云日志服务

产品介绍

文档版本 01

发布日期 2025-02-08

华为云计算技术有限公司

商标声明


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

注意

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

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

目 录

1 图解云日志服务

2 什么是云日志服务

云日志服务（Log Tank Service，简称LTS）是高性能、低成本、功能丰富、高可靠的日志平台。

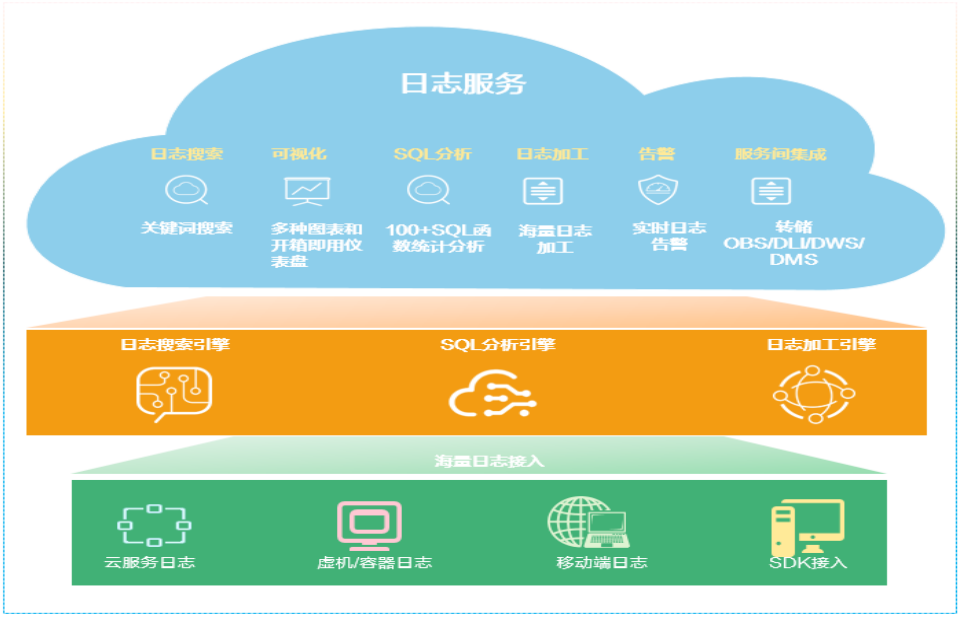
提供全栈日志采集、百亿日志秒搜、PB级存储、日志加工、可视化图表、告警和转储等功能，满足应用运维、等保合规和运营分析等应用场景需求。

LTS 的核心价值

云日志服务提供多种接入方式实现海量日志接入LTS，支持日志搜索引擎、SQL分析引擎、日志加工引擎，详细请参考**图2-1**。

- **端云全场景日志接入：**40+云服务、主机/容器、移动端、跨云、多语言SDK、多账号汇聚，满足全场景客户丰富的日志接入需求。
- **海量日志存储搜索：**百亿日志秒级搜索，千亿日志迭代搜索，PB级智能冷存储。
- **SQL统计和可视化图表：**100+SQL函数、多种可视化图表、10多种开箱即用仪表盘。
- **实时日志告警：**自定义告警内容，短信/邮件/企业微信/钉钉/HTTP多渠道通知。
- **一站式日志加工：**200＋函数、一站式日志规整、富化、脱敏、过滤、分裂加工平台。
- **日志数据服务间集成：**日志转储OBS/DWS/DIS/DLI/DMS，助力用户快速构建水平解决方案。

图 2-1 云日志服务示意图



3 产品功能

在使用云日志服务LTS之前，建议您先通过表3-1了解LTS提供的主要功能。

表 3-1 产品功能

功能	说明
端云全场景日志接入	支持40+云服务、主机/容器、移动端、跨云、多语言SDK、多账号汇聚，满足全场景客户丰富的日志接入需求。
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。
海量日志存储搜索	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，支持百亿日志秒级搜索，千亿日志迭代搜索。
SQL统计和可视化图表	• LTS提供多种开箱即用的日志仪表盘模板，用户接入日志后即可快速分析。 • 将日志分析的结果使用可视化图表呈现出来，支持表格、折线图、饼图、柱状图、地图等统计图表，或将统计图表汇聚在仪表盘上统一呈现，方便运营分析。

功能	说明
日志监控与日志告警	• 支持对存储在云日志服务中的日志数据进行关键词统计或SQL统计，通过在一定时间段内日志中关键字出现次数，实时监控服务运行状态；支持自定义告警内容，支持短信/邮件/企业微信/钉钉/HTTP多渠道通知。 
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。 • 同时LTS还支持转储DWS/DIS/DLI/DMS，让用户实现日志数据便捷在云服务间流转，快速构建水平解决方案。
日志消费与加工	• LTS提供DSL日志加工的能力，内置200＋函数，可以实现一站式日志规整、富化、脱敏、过滤、分裂等功能；另外结合定时SQL统计，可以对数据实现聚合统计。 • 支持用户使用SDK消费LTS日志，可以获取全量日志数据，可以作为流计算的数据源（SDK消费功能邀测中，暂未开放）。

4 应用场景

应用场景 1：应用运维

企业在日常业务运维、审计或等保时，需要收集各种类型的日志，常遇到如下痛点：

- 企业部门多且日志繁杂，日志量大。
- 云服务资源种类数量多，不熟悉监控指标和运维日志，运维难度大。
- 安全合规要求高，等保合规要求日志长期存储，人力不足，维护成本高。

基于云日志服务LTS可以实现：

- 提供全场景日志接入，全面覆盖业务、应用、中间件和基础设施，实现快速收集日志。
- 支持秒级日志查询和分钟级日志监控，通过配置告警规则和告警通知，实现分钟级问题定位和分析。
- 支持将日志转储至OBS实现长期保存，满足网络安全要求。

LTS提供解决方案参考如下**图4-1**，可以实现统一收集生产环境应用日志，开发人员检索分析日志，运维人员基于日志配置告警，实时感知现网业务，及时发现并解决故障问题。

图 4-1 应用运维解决方案

应用场景 2：安全合规

大型企业的每个业务部门都有独立的云账户实现资源隔离，每个业务部门的运维人员需要依赖日志监控告警实现故障定位分析，同时集团安全部门需要统一监控日志，因此多账号的统一日志管理成为企业痛点：

- **分业务独立运维**：客户每个业务模块都有一个独立的账号做资源隔离，依赖日志服务配置监控告警，快速分析发现故障并定位根因。
- **安全部门统一监控日志**：客户使用多账号管理体系，每个业务部门有一个独立的账号，安全部门需要汇聚所有日志到一个账号，并存储180天以上来满足法规要求。

基于云日志服务LTS可以实现：

- **多账号独立管理**：每个账号独立采集各自业务的应用日志、云服务日志，资源互相隔离、权限划分清晰；借助日志告警配置，90%问题定位控制在10分钟。
- **日志数据跨账号集中汇聚**：使用LTS的多账号日志汇聚功能，将各个子账号的日志复制一份到统一监控账号，长期存储180天，便于安全部门集中审计，满足网络安全法规要求。

LTS提供解决方案参考如下图4-2，可以实现统一收集云服务、应用程序日志，支持保存180天以上，满足《网络安全法》、《GDPR》等法律法规要求。

图 4-2 安全合规解决方案

应用场景 3：运营分析

企业在日常经营中，可以上报各种业务日志（例如移动端日志、服务端日志），经过规整、过滤、脱敏、富化等加工处理后，可以融合大数据平台、BI工具进行业务分析，例如获取页面的PV、UV、用户停留时间、交易金额等，用于了解业务运营状况、分析用户行为特征，基于实时的数据分析反馈调整业务决策，提升用户体验，提升经营效率，实现企业的数字化转型。

在业务分析过程中经常遇到如下痛点：

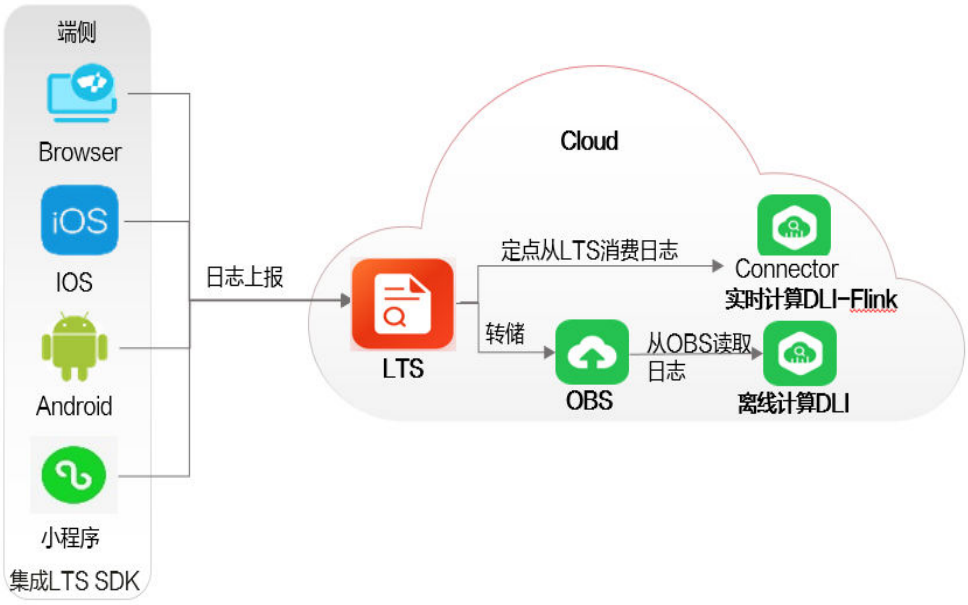
- **移动端数据难采集：**难以快速采集多种移动端设备，例如Web浏览器、IOS、安卓、百度小程序、微信小程序、钉钉小程序、快应用等多类端侧日志无法快速采集。
- **数据传输不可靠：**移动端日志数据量多且频繁，传输速度慢，也极易出现丢失，对业务分析造成一定影响。
- **数据处理不方便：**原始数据不方便处理，不方便快速与大数据平台实现对接。

云日志服务LTS支持采集多种移动端日志，融合大数据完成业务运营分析，基于LTS可以实现：

- **端侧日志全面采集接入：**集成LTS提供的多种移动端SDK，实现了缓存发送、异常重试、批量发送等稳定功能，用户快速集成即可全面采集移动端日志到LTS。
- **秒级上报，高可靠：**端侧采集日志后，经传输链路秒级完成上报，数据无丢失，支撑业务做完整性分析。
- **DLI和DWS快速对接LTS：**DLI-Flink简易集成Connector，定点从LTS实时消费日志；LTS日志可快速配置转储到OBS，供DLI快速从OBS读取日志；LTS支持直接将结构化日志转储到DWS。

LTS提供解决方案参考如下图4-3，可以对日志结构化解析，基于SQL语法分析日志，生成可视化图表，并结合大数据平台帮助企业进一步挖掘数据价值，助力企业数字化转型。

图 4-3 运营分析解决方案



5 安全

5.1 责任共担

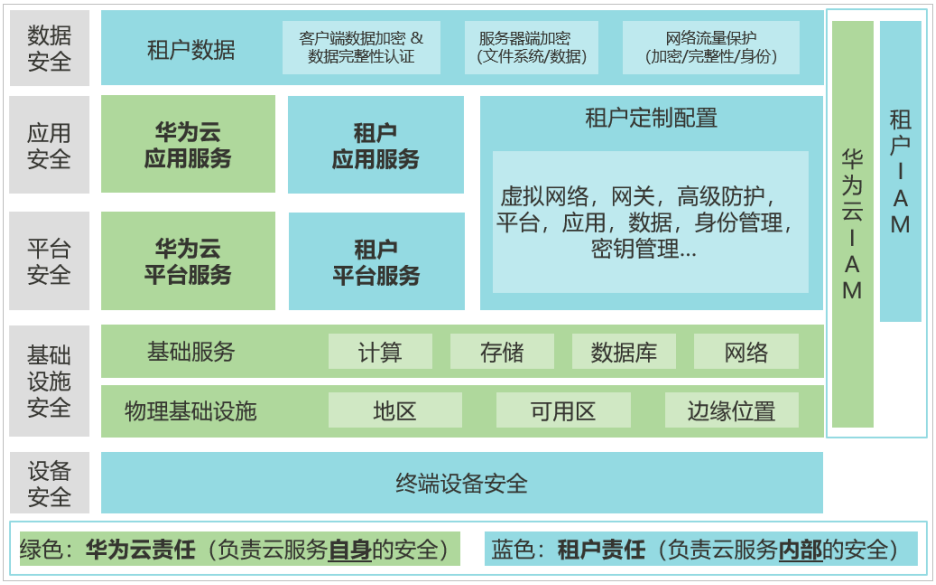
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图5-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 5-1 华为云安全责任共担模型



5.2 身份认证与访问控制

身份认证

无论用户通过LTS控制台还是API访问LTS，都会要求访问请求方出示身份凭证，并进行身份合法性校验，同时提供登录保护和登录验证策略加固身份认证安全。LTS服务基于统一身份认证服务（IAM），支持三种方式身份认证方式：**用户名密码**、**访问密钥**、**临时访问密钥**。同时还提供**登录保护**及**登录验证策略**。

访问控制

对企业中的员工设置不同的LTS访问权限，以达到不同员工之间的权限隔离，使用统一身份认证服务（Identity and Access Management，简称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华为云资源的访问。详细如下：LTS**权限管理**。

5.3 数据保护技术

LTS通过多种数据保护手段和特性，保障LTS的数据安全可靠。

表 5-1 LTS 的数据保护手段和特性

数据保护手段	简要说明	详细介绍
传输加密（HTTPS）	LTS支持HTTPS传输协议，保证数据传输的安全性。	**构造请求**
日志冗余存储	日志数据以多副本方式存储，保障数据可靠性。	/

数据保护手段	简要说明	详细介绍
日志转储OBS	LTS支持将日志转储到对象存储服务OBS，并支持转储到加密OBS桶。用户可以以更低成本保存更长时间的日志，同时可以借助OBS的数据保护技术。	转储OBS

5.4 审计与日志

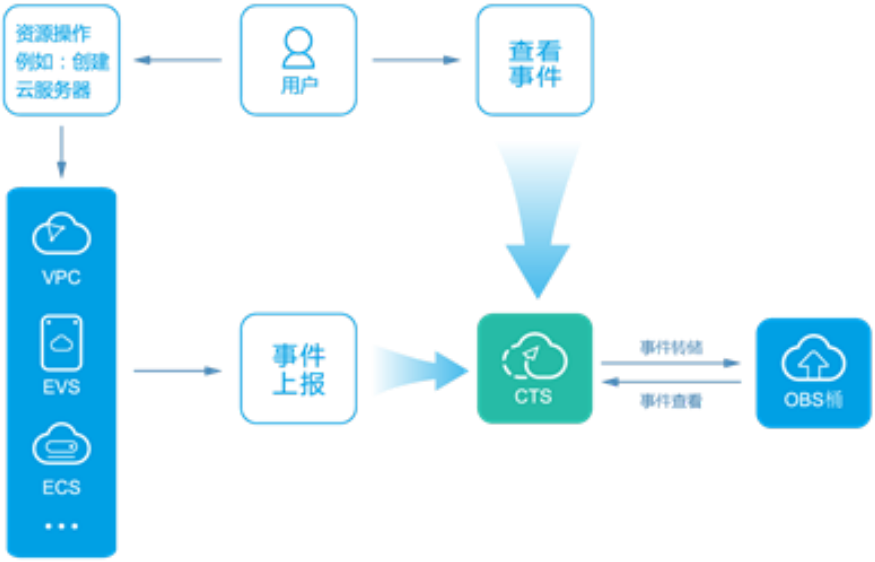
云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务并创建和配置追踪器后，CTS可记录LTS的管理事件用于审计。

CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

CTS支持追踪的LTS管理事件列表，请参见**审计**。

图 5-2 云审计服务



5.5 服务韧性

LTS服务提供了3级可靠性架构，通过AZ内实例容灾、双AZ容灾、日志数据多副本技术方案，保障服务的持久性和可靠性。

表 5-2 LTS 服务可靠性架构

可靠性方案	简要说明
AZ内实例容灾	单AZ内，LTS实例通过多实例方式实现实例容灾，快速剔除故障节点，保障LTS实例持续提供服务。
多AZ容灾	LTS支持跨AZ容灾，当一个AZ异常时，不影响LTS实例持续提供服务。
数据容灾	通过日志数据多副本方式实现数据容灾。

5.6 监控安全风险

LTS通过多种方式监控安全风险，保障数据安全可靠。

表 5-3 LTS 的监控安全风险

监控安全风险	简要说明	详细介绍
日志告警	LTS支持日志告警能力，包括关键词告警和SQL告警。 • 关键词告警：对日志流中的日志数据进行关键词统计，通过设置告警规则，监控日志中的关键词，通过在一定时间段内，统计日志中关键字出现的次数，实时监控服务运行状态。 • SQL告警：支持将日志数据进行结构化，通过配置SQL告警规则，定时查询结构化数据，当且仅当条件表达式返回为true的时候，将告警进行上报，用户可以在LTS控制台查看SQL告警。	**关键词告警** SQL告警
日志资源使用量预警	LTS提供日志资源使用量预警能力，开启自定义日志资源使用量预警开关后，系统将自动为您创建一条告警规则（日志资源使用量预警）。当日志使用量超过当前配置的自定义日志资源使用量额度时，系统会发送告警通知	**日志资源使用量预警**

5.7 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 5-3 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 5-4 资源中心

6 约束与限制

6.1 基础资源限制

本文介绍云日志服务基础资源的使用限制。

表 6-1 基础资源使用限制表

限制项	说明	备注
日志组数量	您在1个华为账号下最多可创建100个日志组。	如您有更大的使用需求，请**提工单**申请。
日志流数量	您在1个日志组中最多可创建100个日志流。 日志流名称不能重复。	如您有更大的使用需求，请**提工单**申请。
日志保存时间	日志支持保存1~365天。	不涉及。
主机组	您在1个华为账号下最多可创建200个主机组。	如您有更大的使用需求，请**提工单**申请。
快速查询	您在1个日志流中最多可创建50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。	
	通过ICAgent采集：单个LogItem最大为500 KB。	

6.2 日志读写限制

本文介绍云日志服务日志读写的限制。

表 6-2 日志读写限制表

类别	限制项	说明	备注
华为账号	日志写入流量	您在1个华为账号下，写入流量最大为500MB/s。	如您有更大的使用需求，请**提工单**申请。
	日志写入次数	您在1个华为账号下，写入次数最大为10000次/s。	如您有更大的使用需求，请**提工单**申请。
	日志查询流量	您在1个华为账号下，通过API查询日志，单次返回日志最大为10MB。	如您有更大的使用需求，请**提工单**申请。
	日志读取次数	您在1个华为账号下，读取次数最大为1000次/min。	如您有更大的使用需求，请**提工单**申请。
日志组	日志写入流量	您在1个日志组下，写入流量最大为200MB/s。	非硬性限制，超过限制不保证服务质量。
	日志写入次数	您在1个日志组下，写入次数最大为1000次/s。	非硬性限制，超过限制不保证服务质量。
	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	您在1个日志组下，读取次数最大为500次/min。	非硬性限制，超过限制不保证服务质量。
日志流	日志写入流量	您在1个日志流下，写入流量最大为100MB/s。	非硬性限制，超过限制不保证服务质量。
	日志写入次数	您在1个日志流下，写入次数最大为500次/s。	非硬性限制，超过限制不保证服务质量。
	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	您在1个日志流下，读取次数最大为100次/min。	非硬性限制，超过限制不保证服务质量。

类别	限制项	说明	备注
	日志时间	日志时间不超过24小时。从当前时间往前推24小时或往后推24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6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8日11:00后的日志无法进行采集	不涉及。
SDK	SDK上报日志流量	推荐使用1.0.0以上SDK正式版本，若有低版本，请尽快升级，否则无法保证SLA。	低版本SDK可能会导致上报失败。
	端侧SDK	当前限制邀测中，不建议在生产环境中使用。	邀测阶段，可能会频繁迭代，需要您配合产品升级。

6.3 ICAgent 限制

本文介绍日志采集器ICAgent的限制。

表 6-3 ICAgent 文件采集限制

限制项	说明	备注
文件编码	仅支持UTF8，其他编码可能会产生乱码。 不支持采集其他类型日志文件，例如：二进制文件。	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。

限制项	说明	备注
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。 **Windows**： ● Windows环境日志采集路径支持递归路径，**表示递归5层目录。配置样例：C:\var\service**\a.log。 ● Windows环境日志采集路径支持模糊匹配，匹配目录或文件名中的任何字符。配置样例：C:\var\service*\a.log、C:\var\service\a*.log。 ● 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。 ● windows事件日志采集不能重复配置，即同一主机下，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	每条日志最大500KB，超出限制部分ICAgent将截断后丢弃。	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。
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 6-4 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 ● ICAgent版本低于5.12.200时，对CPU资源的消耗最大不超过2核。 ● ICAgent版本为5.12.200及以上，节点规格小于等于4核时，对CPU资源的消耗最大不超过2核；节点规格大于4核时，对CPU资源的消耗最大不超过log2(节点核数)。 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 6-5 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或日志重复。 • 日志文件未使用CCE提供的logPolicy轮转策略。 • 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。

表 6-6 ICAgent 支持访问的 IP 地址

组件/服务	IP地址	说明
openstack	http://169.254.169.254/openstack/latest/meta_data.json	获取节点元数据，节点名称和节点id。
	http://169.254.169.254/openstack/latest/securitykey	委托方式获取临时ak/sk和securitytoken。
	http://169.254.169.254/latest/meta-data/public-ipv4	获取节点绑定的弹性IP地址。
CCE	http://127.0.0.1:4194/api/v2.0/ps	cadvisor接口获取进程信息。
	http://127.0.0.1:4194/api/v1.2/docker	cadvisor接口获取容器全量指标。
	http://nodeip:10255/pods	k8s接口获取pod信息。

表 6-7 ICAgent 支持访问的端口号

端口号	说明
#icmgr-service {podlb}:30200	ICAgent注册。
icmgr-controller {podlb}:30201	ICAgent状态配置。
#als-access {podlb}:8102	日志上报。
#ams-access {podlb}:8149	上报监控指标。
#ats-access apm {podlb}:8923	上报数据到APM。

6.4 搜索与分析限制

本文介绍云日志服务查询与分析的限制。

搜索

表 6-8 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。	如您有更大的使用需求，请**提交工单**申请。
操作并发数	您在1个华为账号下支持的最大查询操作并发数为200个。	如您有更大的使用需求，请**提交工单**申请。
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。
返回结果	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。

限制项	说明	备注
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	单次搜索，时间跨度默认不超过30天。	如您有更大的使用需求，请**提交工单**申请。

分析

表 6-9 日志 SQL 分析限制

限制项	说明	备注
操作并发数	您在1个华为账号下日志分析并发数为15个。	如您有更大的使用需求，请**提交工单**申请。
数据量	单个日志流单次最大分析24GB数据。	如果您的数据量远超LTS提供的分析规格，请您购买DWS服务，配置日志转储DWS，使用数据仓库分析。
开启模式	默认不开启。	不涉及。
数据生效机制	日志结构化只对新增结构化配置之后写入的数据生效。	不涉及。
返回结果	默认最多返回100条数据。 如果需要返回更多数据，可以使用**SQL查询语法**单独配置返回查询结果。	不涉及。
	LIMIT上限为5000条。	不涉及。
字段值大小	结构化字段最大大小为16KB，超过部分不参与分析。	不涉及。
超时时间	分析操作的最大超时时间为30秒。	如果您的数据量远超LTS提供的分析规格，请您购买DWS服务，配置日志转储DWS，使用数据仓库分析。
Double类型的字段值位数	Double类型的字段值最多52位。 如果浮点数编码位数超过52位，会造成精度损失。	不涉及。

限制项	说明	备注
IP函数时效性	IP函数是可以分析IP地址所属的国家、省份、城市及对应的网络运营商，该函数依赖的后台数据库每半年更新一次，可能出现少量IP与地理位置映射未及时更新的情况。	不涉及。
SQL分析时间范围	仅支持分析30天内的数据，30天以上的数据不支持SQL分析。	如您有更大的使用需求，请**提交工单**申请。

6.5 日志转储限制

本文介绍云日志服务转储的限制。

表 6-10 日志转储限制

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	转储速率上限为为100 MB/s。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。
转储DIS	单个日志流转储任务数量	1 个日志流只能配置一个转储DIS任务。	不涉及。
	转储周期	实时转储。	不涉及。
	每次转储数据大小	不涉及。	不涉及。
	转储条件已触发，待转储成功时会有时间延迟。	不涉及。	不涉及。

类别	限制项	说明	备注
	转储速率阈值	转储速率上限为DIS通道最大写入流量。 超过DIS通道限制时，转储数据会不稳定。	不涉及。
转储DMS	单个日志流转储任务数量	1 个日志流只能配置一个转储DMS任务。	不涉及。
	转储周期	实时	不涉及。
	每次转储数据大小	不涉及	不涉及。
	转储条件已触发，待转储成功时会有时间延迟。	不涉及	不涉及。
	转储速率阈值	转储速率上限为DMS（kafka）集群流量上限。 超过KAFKA集群流量上限时，转储数据会不稳定。	不涉及。
转储DWS	单个日志流转储任务数量	一个日志流仅可创建一个DWS转储任务	不涉及。
	转储周期	1分钟	不涉及。
	单次转储数据大小	<5MB	不涉及。
	转储条件已触发，待转储成功时会有时间延迟。	延迟5Min。 例如：8:30开始转储，最晚8:35可见转储数据。	不涉及。
	转储速率阈值	转储速率上限为为40 MB/s。 超过限制时，转储数据会不稳定。	不涉及。
	转储数据可靠性	某批次数据格式合法时，保证转储数据至少一次（At Least Once）。当DWS集群负载较高、网络错误时，会有写入响应超时，可能导致数据重复，因此无法保障数据精确一次（Exactly Once）。	不涉及。

类别	限制项	说明	备注
	表结构变更	• 如果投递过程中，在DWS表中添加非必须的新列，则不影响转储； • 如果投递过程中，在DWS表中添加必须的新列，则会导致数据写入失败； • 如果投递过程中，在DWS表中删除已配置转储规则的列，则会导致数据写入失败。	不涉及。
	数据列不合法	常见场景类型为不匹配或者类型转换失败。该批次数据不会写入DWS，其余批次正常写入DWS。	不涉及。
	数据列过长	常见场景为数据超出string类型或者varchar长度限制。该批数据不会写入DWS，其余批次正常写入DWS。	不涉及。

6.6 日志告警限制

本文介绍云日志服务告警的限制。

表 6-11 告警限制说明

类别	限制项	说明	备注
告警监控	告警规则数量	您在1个华为账号下最多可创建200个告警。	如您有更大的使用需求，请**提交工单**申请。
	搜索和分析条件组合个数	关键词搜索为1个，SQL分析个数为1-3个。	不涉及。
	查询时间范围	关键词告警：每条查询语句的查询时间跨度不能超过1小时。	不涉及。
		SQL告警：每条查询语句的查询时间跨度不能超过24小时。	不涉及。
	查询和分析操作一般性限制	查询和分析操作的限制项，关键词告警请参见**搜索语法**。SQL告警请参见**SQL查询语法**。	不涉及。

类别	限制项	说明	备注
告警通知	通知方式	各个通知方式的使用限制如下所示。超出限制，可能导致您无法接收到告警通知。 • 邮件 • 短信 • 语音 仅支持中国内地手机号码（+86）。如需开通，请**提交工单**申请。 • 钉钉 钉钉机器人限制每分钟最多20条消息。 • 企业微信 企业微信机器人限制每分钟最多20条消息。 • 飞书 飞书的功能仅针对白名单用户使用，如需开通，请**提交工单**申请。	不涉及。

类别	限制项	说明	备注
	通知内容	每个通知方式都存在通知内容长度的限制。为了尽量保证告警通知成功，对于超长的内容，系统可能通过适当的内容截断来避免通知失败。内容截断无法保证内容的完整性以及百分百发送成功，这主要是受限于截断后的内容以及各个通知方式的支持能力，例如截断后的内容是不合法的Markdown或者HTML，则可能导致通知失败。对于短信、语音等纯文本格式的内容，一般内容截断不会导致通知失败。 建议根据通知方式的限制合理配置内容模板，避免内容超长导致通知失败。各个通知方式的限制如下（中文、英文、数字或标点符号都算一个字符）： ● 短信 具体限制请**短信发送限制**。 ● 语音 通知内容限制为256个字符。 ● 邮件 通知内容限制为5 KB。 ● 钉钉 通知内容限制为5 KB。 ● 企业微信 通知内容限制为5 KB。	不涉及。
	消息模板	最多100个模板。	不涉及。
	消息模板变量	LTS限制消息内容长度不超过3 KB，超过3 KB部分会被截断。	不涉及。
	消息通知方式额度	每个接收人每天最多可接收额度与用户SMN资源配额有关。	不涉及。

6.7 日志生成指标限制

本文介绍云日志服务日志生成指标的规则总数说明和使用限制。

图 6-1 日志生成指标规则总数说明

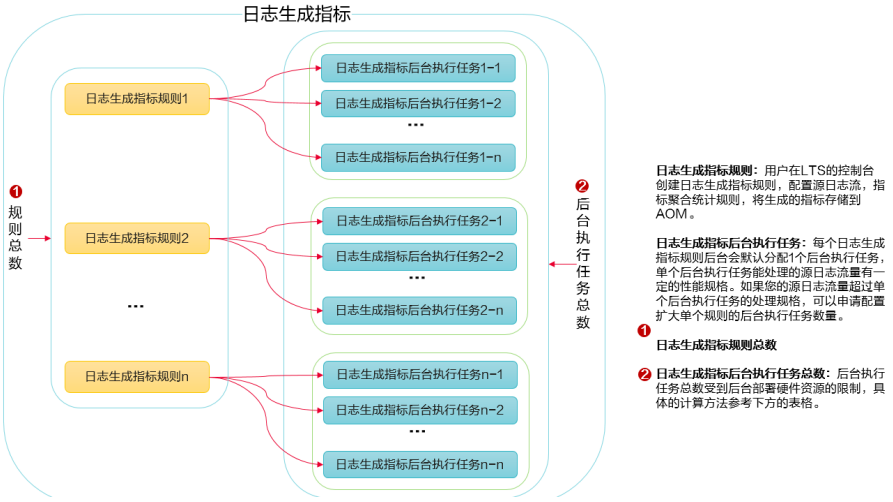


表 6-12 日志生成指标使用限制说明

类别	限制项	说明	备注
日志生成指标	1个账号的日志生成指标-规则总数	单个账号的日志生成指标规则数，默认限制<=10，该限制是软件层面的元数据限制。 ● 每个日志生成指标规则后台会默认分配1个后台执行任务，单个后台执行任务能处理的源日志流量有一定的性能规格。如果您的源日志流量超过单个后台执行任务的处理规格，支持提工单申请配置扩大单个规则的后台执行任务数量。 ● 如果您的日志生成指标规则太多，导致剩余可用的后台执行任务的数量已经耗尽，那么会有部分日志生成指标规则不会被调度执行。	不涉及。
	1个日志生成指标规则的日志稳态速率	<=40MB/s （默认1个日志生成指标规则分配1个后台执行任务）	如果您的源日志流量超过单个后台执行任务的处理规格，支持提工单申请配置扩大单个规则的后台执行任务数量。

类别	限制项	说明	备注
	1个日志生成指标规则的日志峰值速率	<=50MB/s （默认1个日志生成指标规则分配1个后台执行任务）	如果您的源日志流量超过单个后台执行任务的处理规格，支持提工单申请配置扩大单个规则的后台执行任务数量。
	日志生成指标规则配置参数	• 过滤条件分组数量<=10个，每个分组中关联关系数量<=10。 • 分组聚合（Group By）的字段数量<=5。 • 分组聚合（Group By）字段基数<=100。	不涉及。
	日志时间	日志时间与LTS系统时间差<1小时，否则任务执行失败，无法生成指标上报AOM。	日志时间需要保证基本有序，乱序严重或者超时太严重将无法处理。 典型的：当采集端所在机器没有从NTP服务器同步时间，或者日志采集出现严重积压延时，可能导致日志时间无法保证基本有序，影响日志生成指标的聚合统计。

6.8 操作系统限制

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。

- 对于Linux x86_64服务器，LTS支持上表中所有的操作系统及版本。
- 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。

表 6-13 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

操作系统	版本					
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	2.10 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	

表 6-14 LTS 支持的操作系统及版本（Windows）

操作系统	版本
Windows（64位）	Windows Server 2019
	Windows Server 2016 R2 Datacenter
	Windows Server 2016 R2 Standard
	Windows Server 2016 Datacenter English
	Windows Server 2016 R2 Standard English
	Windows Server 2012 R2 Datacenter
	Windows Server 2012 R2 Standard
	Windows Server 2012 Datacenter English
	Windows Server 2012 R2 Standard English
	Windows Server 2008 R2 Enterprise
	Windows Server 2008 R2 Standard
	Windows Server 2008 Enterprise English
	Windows Server 2008 R2 Standard English

7 权限管理

权限说明

如果您需要对华为云上购买的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，您可以使用统一身份认证服务（Identity and Access Management，简称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，可以帮助您安全地控制LTS资源的访问。

通过IAM，您可以在华为账号中给员工创建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。

如果华为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是华为云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**IAM产品介绍**。

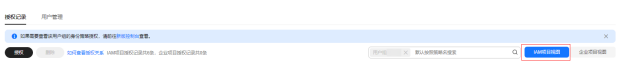
企业项目授权后仍报权限不足的说明

IAM项目(Project)/企业项目(Enterprise Project)：自定义策略的授权范围，包括IAM项目与企业项目。授权范围如果同时支持IAM项目和企业项目，表示此授权项对应的自定义策略，可以在IAM和企业管理两个服务中给用户组授权并生效。如果仅支持IAM项目，不支持企业项目，表示仅能在IAM中给用户组授权并生效，如果在企业管理中授权，则该自定义策略不生效。关于IAM项目与企业项目的区别，详情请参见：**IAM和企业管理的区别**。

LTS当前仅日志组、日志流、仪表盘资源接口支持企业项目方式授权，其他资源的接口仅支持IAM项目方式授权，因此针对仅支持IAM项目方式授权时需注意：

1. 授权时选择“IAM项目视图”。

   图 7-1 IAM 项目视图

2. 选择授权范围时，建议根据最小化授权原则，选择“指定区域项目资源”，具体请根据实际业务情况选择授权范围。

LTS 权限

默认情况下，管理员创建的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。

权限根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 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。

如表7-1所示，包括了LTS的所有系统权限。

表 7-1 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	CCE Administrator、OBS Administrator、AOM FullAccess、FunctionGraph 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	CCE Administrator、OBS Administrator、AOM FullAccess
LTS Administrator	云日志服务的管理员权限。	系统角色	Tenant Guest、Tenant Administrator

表7-2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 7-2 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	√	×	√

操作	LTS FullAccess	LTS ReadOnlyAccess	LTS Administrator
修改日志组	√	×	√
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	√	×	√
查询仪表盘	√	√	√
创建仪表盘	√	×	√
修改仪表盘	√	×	√
删除仪表盘	√	×	√
查询结构化配置	√	√	√
配置结构化	√	×	√
开启快速分析	√	×	√
关闭快速分析	√	×	√
配置分词	√	×	√
查询过滤器	√	√	√
禁用过滤器	√	×	√
启用过滤器	√	×	√
删除过滤器	√	×	√
查询告警规则	√	√	√
创建告警规则	√	×	√
修改告警规则	√	×	√
删除告警规则	√	×	√
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	√	×	√

操作	LTS FullAccess	LTS ReadOnlyAccess	LTS Administrator
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7-3。

表 7-3 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

权限名称	权限描述	权限依赖
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
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

权限名称	权限描述	权限依赖
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
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

权限名称	权限描述	权限依赖
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

8 隐私与敏感信息保护声明

8.1 采集器隐私声明

由于LTS会将运维数据内容展示到LTS控制台，请您在使用过程中，注意您的隐私及敏感信息数据保护，不建议将隐私或敏感数据上传到LTS，必要时请加密保护。

采集器部署

在ECS上手动部署ICAgent过程中，安装命令会使用到您的AK/SK作为输入参数，安装前请您关闭系统的历史记录收集，以免泄露隐私。安装后ICAgent会加密存储您的AK/SK，有效保护敏感信息。

9 基本概念

日志组

日志组（LogGroup）是云日志服务进行日志管理的基本单位，可以创建日志流以及设置日志存储时间。

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，方便对日志进一步分类管理。

日志读写以日志流为单位，您可以在写入时指定日志流，将不同类型的日志分类存储，ICAgent采集日志后，将多条日志数据进行打包，以日志流为单位发往云日志服务，日志流的读写方式可以最大限度地减少读取与写入次数，提高业务效率。

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。

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。

10 与其他云服务的关系

云日志服务与其他服务之间关系，如表1所示。

表 10-1 与其他服务之间关系

交互功能	相关服务
通过CTS服务，您可以记录与云日志服务相关的操作事件，便于日后的查询、审计和回溯。	云审计服务（Cloud Trace Service，简称CTS）
通过OBS服务，您可以将需要长期存储的日志转储至OBS桶中，确保日志不丢失，实现数据持久化。	对象存储服务（Object Storage Service，简称OBS）
通过DIS服务，您可以将需要长期存储的日志转储至DIS，DIS可以将大量日志文件传输到云端做备份，进行离线分析、存储查询及机器学习，还能用于数据丢失或异常后的恢复和故障分析。同时大量小文本文件可合并转储为大文件，提高数据处理性能。	数据接入服务（Data Ingestion Service，简称DIS）
通过AOM服务，可以进行站点访问统计，可以将相关日志上报给AOM，对其进行监控与告警。	应用运维管理（Application Operations Management，简称AOM）
通过IAM服务，您可以给账号中的子用户授予使用云日志服务的权限。	统一身份认证服务（Identity and Access Management，简称IAM）