

云日志服务

产品介绍

文档版本

01

发布日期

2020-12-24



华为技术有限公司



版权所有 © 华为技术有限公司 2020。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为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，华为公司对本文档内容不做任何明示或默示的声明或保证。

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。

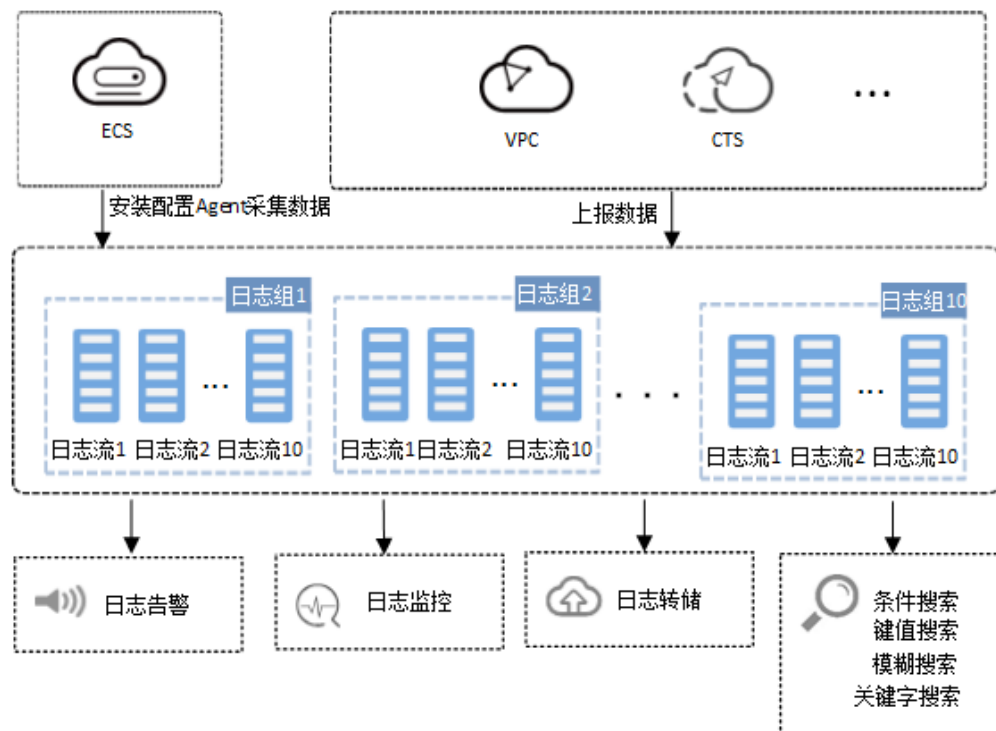
目录

1 什么是 LTS.....	1
2 基本功能.....	3
3 应用场景.....	4
4 使用限制.....	5
5 基本概念.....	8
6 权限管理.....	10
7 与其他云服务的关系.....	12

1 什么是 LTS

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，为您提供一个实时、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



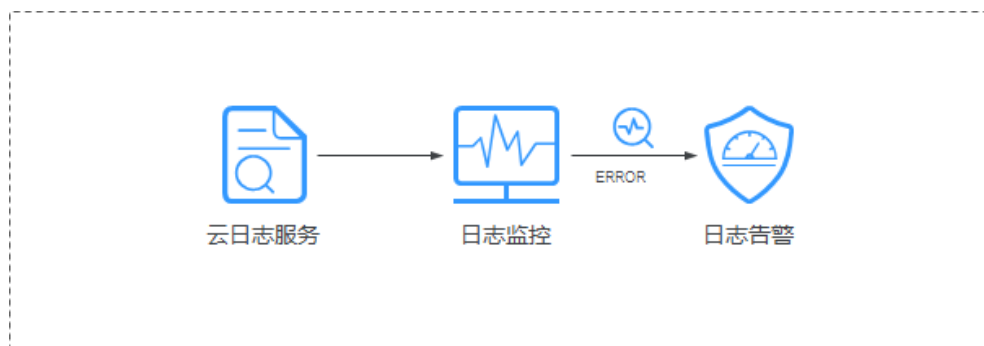
日志采集与分析

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。



日志监控与告警

云日志服务支持对日志数据关键字进行监控与告警，通过在一定时间段内，日志中关键字出现次数，如果关键字达到阈值将会触发告警，实时监控服务运行状态。



日志转储

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，可以在1-30天之间进行设置。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）、数据接入服务（DIS）或分布式消息服务（DMS）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。

计费

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

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

收费详情请参见：[LTS产品价格详情](#)。

如果每月免费赠送的额度已经可以满足您的使用需求，超过后希望暂停日志收集，可以在配置中心进行设置，详情请参见：[配置中心](#)。

2 基本功能

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。

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。

日志监控与告警

云日志服务结合应用运维管理（Application Operations Management，简称AOM），支持对存储在云日志服务中的日志数据进行关键词统计，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。

日志转储

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，可以在1-30天之间进行设置。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）、数据接入服务（DIS）或分布式消息服务（DMS）中长期保存。

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。

4 使用限制

资源使用限制

在使用LTS时，您需注意以下使用限制。使用限制中部分内容属于配额，关于什么是配额以及怎样查看与修改配额，详见[关于配额](#)。

限制项	使用限制
日志组个数	最多创建100个日志组，云服务创建的日志组不占配额。
日志流个数	每个日志组最多创建100个日志流，云服务创建的日志流不占配额。
自定义指标过滤器个数	每个日志流最多可以创建5个自定义指标过滤器。
日志流写入速率	单个日志流写入速率最大不能超过5MB/S，写入条数最多不能超过25K/S，超过此规格可能会导致日志丢失。
单行日志长度	单行日志长度最长为10240字节，超过此规格的单行日志将会被丢弃。
主机	仅支持华为云上购买的主机。
采集路径配置	<ul style="list-style-type: none">● 日志采集路径不能重复配置，即相同主机的同一个日志源不能配置到多个不同的日志流，否则可能会导致日志采集异常。● 相同主机的同一个日志源，如果在AOM进行了配置，则不能在LTS重复配置。● Windows环境中，采集路径暂不支持配置通配符*。
日志存储时间	可以在1~30天之间进行设置，如果不设置，系统默认存储时间为7天。
日志免费额度	500MB/月，超过免费额度后按需收费。收费详情请参见： LTS产品价格详情 。

限制项	使用限制
采集器资源消耗	采集器在采集基础指标时的资源消耗情况和容器、进程数等因素有关，在未运行任何业务的VM上，采集器将消耗30M内存、1% CPU。为保证采集可靠性，单节点上运行的容器个数应小于1000。

操作系统使用限制

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。

表 4-1 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
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	

说明

- 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 4-2 LTS 支持的操作系统及版本（Windows）

操作系统	版本
Windows（64位）	Windows Server 2016 R2 Datacenter

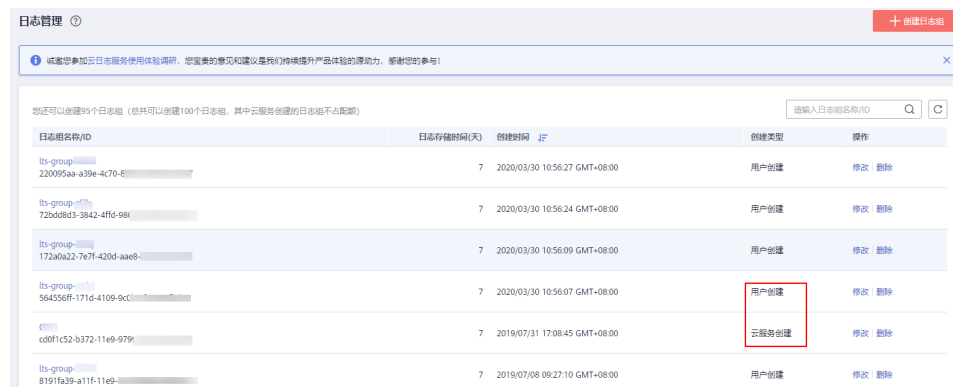
操作系统	版本
	Windows Server 2016 R2 Standard
	Windows Server 2016 Datacenter English
	Windows Server 2016 R2 Standard English
	Windows Server 2012 R2 Datacenter
	Windows Server 2012 R2 Standard
	Windows Server 2012 Datacenter English
	Windows Server 2012 R2 Standard English
	Windows Server 2008 R2 Enterprise
	Windows Server 2008 R2 Standard
	Windows Server 2008 Enterprise English
	Windows Server 2008 R2 Standard English

5 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。

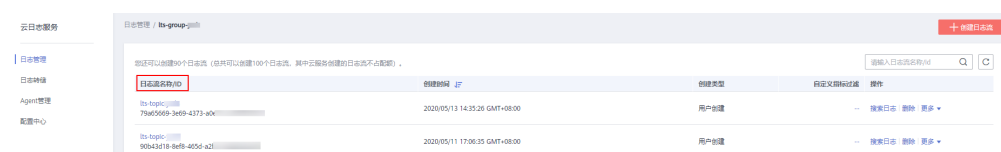
日志组的创建类型分为用户创建（主动）和云服务创建（被动），云服务创建指华为云其他云服务与云日志服务进行系统对接后，系统将自动在云日志服务控制台创建日志组和日志流，云服务的运行日志将发送到对应的日志流中。



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，Agent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。

6 权限管理

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，可以帮助您安全的控制LTS资源的访问。

通过IAM，您可以在华为云账号中给员工创建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。

如果华为云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。

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（如华北-北京1）对应的项目（cn-north-1）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6-1所示，包括了LTS的所有系统权限。

表 6-1 LTS 系统权限

策略名称	描述	策略类别
LTS FullAccess	LTS管理员权限，拥有该权限的用户可以操作并使用LTS。	系统策略
LTS ReadOnlyAccess	LTS只读权限，拥有该权限的用户仅能查看LTS数据。	系统策略
LTS Administrator	云日志服务的管理员权限。	系统角色

7 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 7-1 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）