云日志服务

快速入门

文档版本 01

发布日期 2025-02-27

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 使用 ICAgent 插件采集 ECS 文本日志到云日志服务.....1
2 入门实践.....13

1 使用 ICAgent 插件采集 ECS 文本日志到云日志服务

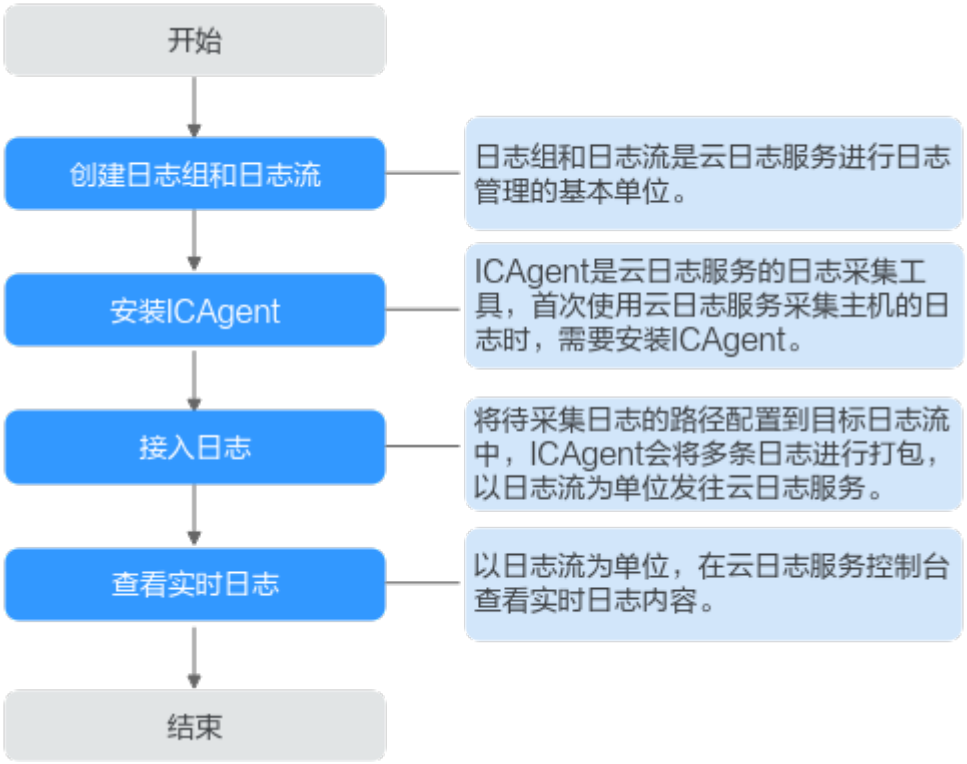
云日志服务（Log Tank Service，LTS）提供一站式的日志数据解决方案，支持日志的采集、日志存储、搜索分析、日志加工、可视化仪表盘、日志告警等功能。LTS提供稳定可靠的服务，您可无需关注扩缩容等资源问题，同时降低了日志运维门槛，帮助您提高问题定位和指标监控的效率。

本文以**云主机 ECS-文本日志接入LTS**为例，帮助您快速上手使用云日志服务。首先需要创建用于存放ECS文本日志的日志组和日志流；然后在需要采集日志的ECS主机上安装ICAgent插件；其次配置ECS文本日志接入LTS，待日志成功上报到LTS后，即可在LTS控制台查看上报的实时日志。

操作流程

操作流程请参考**图1-1**。

图 1-1 流程图



1. **步骤一：创建日志组和日志流**
2. **步骤二：安装ICAgent**
3. **步骤三：ECS接入日志**
4. **步骤四：查看实时日志**

前提条件

- 为用户添加云日志服务LTS的操作权限。

  您需要有LTS的管理员权限“LTS FullAccess”，具体操作请参考**授权IAM用户使用LTS**。
- 本操作以Linux系统的ECS为例，准备好需要采集日志的ECS主机，详细请参考**自定义购买ECS**。如果您已有可用的ECS主机，可重复使用，不需要再次创建。

步骤一：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，然后在日志组中创建日志流。

步骤1 登录**云日志服务控制台**。

步骤2 在“日志管理”页面，单击“创建日志组”，参考**表1-1**填写日志组相关信息。

图 1-2 创建日志组

表 1-1 参数说明

参数	说明	示例
日志组名称	• 日志组名称只支持输入英文、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。 • 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。	lts-group-ECS
企业项目	选择业务需要的企业项目，默认为default。	default
日志存储时间(天)	日志组的存储时间，即日志上报到LTS后日志存储的时间。 日志数据默认存储30天，可以在1~365天之间设置。 云日志服务LTS根据配置的日志存储时间定时清理日志内容，例如日志存储时间为30天，上报到LTS的日志只保存30天，30天后开始删除日志内容。	30
标签	按照业务需求对不同的日志组添加对应的标签。本示例可不设置。	-
备注	自定义填写备注信息，字符长度0-1024个字符。本示例可不填写。	-

步骤3 单击“确定”，日志组创建成功，即可在日志组列表下方生成一条日志组信息。

步骤4 单击目标日志组名称对应的 。

步骤5 单击“创建日志流”，在“创建日志流”页面中，参考表1-2填写日志流相关信息。

图 1-3 创建日志流

表 1-2 参数说明

参数	说明	示例
日志组名称	默认显示目标日志组名称。	-
日志流名称	• 日志流名称只支持输入英文、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。 • 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。	lts-topic-ECS
企业项目	选择业务需要的企业项目，默认为default。	default
日志存储	开启日志存储：日志将会被存入搜索引擎，能使用日志全量功能。 需要开启日志存储，才能开启日志存储时间。	开启

参数	说明	示例
日志存储时间(天)	日志流的存储时间，即日志上报到LTS后日志存储的时间。 日志数据默认存储30天，可以在1~365天之间设置。 • 打开日志流的“日志存储时间”开关：日志的存储时间使用日志流设置的日志存储时间。 • 云日志服务LTS根据配置的日志存储时间定时清理日志内容，例如日志存储时间为30天，上报到LTS的日志只保存30天，30天后开始删除日志内容。	30
标签	按照业务需求对不同的日志组添加对应的标签。本示例可不添加。	-
匿名写入	匿名写入默认关闭，本示例默认关闭。 匿名写入适用于安卓/IOS/小程序/浏览器端上报日志。	关闭
备注	自定义填写备注信息，字符长度0-1024个字符。本示例可不填写。	-

步骤6 单击“确定”。

步骤7 日志流创建成功，即可在目标日志组下方生成一条日志流信息。

----结束

步骤二：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。同一台主机安装ICAgent成功后，后续采集日志时无需重复安装ICAgent。

以主机类型选择区域内主机，安装系统选择Linux，安装方式选择获取AK/SK凭证为例子介绍如何安装ICAgent，具体步骤参考如下。

步骤1 左侧导航栏选择“主机管理 > 主机”，进入“主机”页面。

步骤2 单击右上角“安装ICAgent”。

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。

表 1-3 安装 ICAgent

参数	说明	示例
主机类型	默认选择区域内主机。确保需要采集日志的机器是在区域内还是区域外。 区域内主机就是用户登录云日志服务控制台所在region区，例如北京四。	-

参数	说明	示例
安装系统	默认选择Linux。	-
安装方式	默认选择获取AK/SK凭证。详细操作请参考**如何获取访问密钥AK/SK**。	-

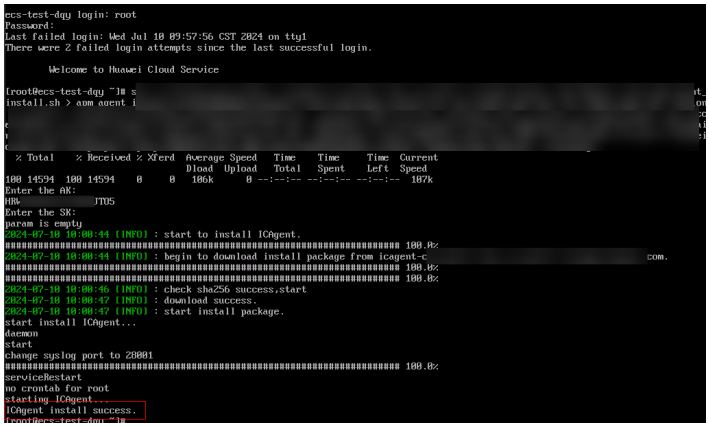
图 1-4 安装 ICAgent

步骤3 单击“复制命令”，复制ICAgent安装命令。

步骤4 登录ECS主机。详细操作请参考**通过VNC登录Linux ECS**。

1. 进入弹性云服务器ECS控制台。
2. 找到需要安装ICAgent的ECS主机，单击目标主机操作列的“远程登录”。
3. 在弹出的“登录Linux云服务器”窗口中，选择“其他方式”下的VNC方式，单击“立即登录”。
4. 在新打开的页面中，根据界面提示，输入用户购买弹性云服务器设置的root用户名和密码。
5. ECS登录成功后，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。（若复制命令时手动替换了AK/SK，则系统不会再提示输入AK/SK）
6. 当显示“ICAgent install success”时，表示安装成功，ICAgent已安装在了/opt/oss/servicemgr/目录。

图 1-5 安装回显



步骤5 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的状态显示“运行”，主机名称为ECS-test-dqy（仅供参考，请以实际安装的主机名称为准）。

图 1-6 主机

----结束

步骤三：ECS 接入日志

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

步骤1 在左侧导航栏中，选择“接入 > 接入中心”，单击“云主机 ECS-文本日志”进行主机接入配置。

步骤2 进入选择日志流页面。

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（例如lts-group-ECS）。
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（例如lts-topic-ECS）。
3. 单击“下一步：选择主机组”。

步骤3 选择主机组。

1. 在主机组列表中，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，参考**表1-4**完成主机组创建，单击“确定”。

图 1-7 新建主机组

表 1-4 新建主机组

参数	说明	示例
主机组名称	自定义设置。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。	testECS
主机组类型	默认选择IP。 创建IP地址的主机组类型：在主机组中添加服务器的IP地址，通过IP地址识别服务器。	IP
主机类型	默认选择Linux主机。此处的主机类型与**步骤二：安装ICAgent**中安装系统保持一致。	Linux主机
备注	自定义填写主机组描述信息，字符长度0-1024个字符。本示例可不填写。	-
添加主机	在主机列表下方选择勾选已安装ICAgent的主机。截图中的主机仅供参考，请以实际环境中的主机信息为准。	ECS-test-dqy

2. 主机组创建成功后，勾选需要采集日志的主机组。
3. 单击“下一步：采集配置”。

步骤4 采集配置，参考**表1-5**对主机日志采集设置具体的采集规则。

图 1-8 采集配置

表 1-5 采集配置

参数	说明	示例
采集配置名称	自定义设置，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。	testECS
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。 例如采集路径配置为/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 • 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。	/var/logs/**/a.log
允许文件多次采集	暂不支持Windows场景。 开启“允许文件多次采集”后，同一主机下的同一日志文件支持被采集到多个日志流。	开启

参数	说明	示例
设置采集黑名单	黑名单配置可在采集时忽略指定的目录或文件，目录和文件名支持完整匹配，也支持通配符模式匹配。指定按目录过滤，可过滤掉该目录下的所有文件。windows主机不支持设置采集黑名单。 本示例默认关闭，采集所有文件。	关闭
采集Windows事件日志	本示例是Linux主机，默认关闭。	关闭
结构化解析配置	开启结构化解析配置，日志结构化解析规则选择单行-全文日志。更多规则请参考**ICAgent结构化解析规则说明**。	开启
最大目录深度	最大目录深度为20层。 采集路径支持使用**配置多层路径模糊匹配，该配置项限制最大目录深度。例如您的日志路径为/var/logs/department/app/a.log，采集路径配置为：/var/logs/**/a.log，当配置为1时日志不会被采集，配置>=2时日志会被采集。	20
日志拆分	用于拆分单行日志，本示例开启“日志拆分”开关。当日志大小超过500KB时，打开“日志拆分”开关，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。	开启
采集二进制文件	用于对接入的二进制文件日志进行采集，本示例开启“采集二进制文件”开关。 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。 打开“采集二进制文件”开关，则对接入的二进制文件日志进行采集，但仅支持UTF-8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。	开启
日志文件编码	日志文件编码为UTF-8。	-
采集策略	本示例采集策略选择增量。 增量采集：ICAgent采集新文件时，从文件的末尾开始读。	-
自定义元数据	本示例默认关闭自定义元数据，ICAgent会根据系统默认的内置字段和自定义键值对上传LTS。	-

参数	说明	示例
日志格式	若开启“结构化解析配置”不用设置该参数。用于设置采集日志上报LTS后显示格式，本示例选择“单行日志”。 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。	单行日志
日志时间	若开启“结构化解析配置”不用设置该参数。用于设置每条日志的行首显示日志的采集时间，本示例开启“系统时间”开关。 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。	系统时间

步骤5 单击“下一步：索引配置”，进入索引配置页面，按照界面默认参数配置即可，通过配置索引后，可对日志进行查询和分析操作。更多信息请参考**设置LTS日志索引配置**。

图 1-9 索引配置

- 全文索引：默认开启全文索引开关，表示创建全文索引。默认开启大小写敏感和包含中文，分词符使用默认分词符, '";=()[]{}@&<>/:\\?\n\t\r
- 日志分析：默认开启“日志分析”，配置的字段索引支持SQL可视化分析。
- 字段索引：云日志服务LTS默认为部分内置保留字段创建字段索引，例如hostIP、hostName、pathFile字段。更多内置保留字段请参考**设置LTS日志索引配置**。

步骤6 单击“提交”，日志接入成功，可以单击“返回接入配置列表”查看日志接入，在接入管理页面，则会生成一条接入配置信息。

----结束

步骤四：查看实时日志

完成日志接入配置后，可以在云日志服务控制台实时查看上报的日志。

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。

步骤1 在“接入管理”页面，单击目标日志接入任务“所属日志流”列的日志流名称，即可进入日志流详情页。

步骤2 单击“实时日志”页签，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。

图 1-10 实时日志

----结束

相关信息

日志接入成功后，在日志接入页面，单击目标日志接入任务“所属日志流”列的日志流名称，即可进入日志流详情页，您可以参考**日志搜索与分析**对上报的日志进行搜索分析。

2 入门实践

当您完成了日志组、日志流等基本操作后，可以根据自身的业务需求使用云日志服务提供的一系列常用实践。

表 2-1 常用最佳实践

实践	描述
对华为云ELB日志进行分析	该解决方案介绍将ELB日志接入LTS后，配置日志结构化后，即可进行日志搜索分析。
无服务器日志实时分析	该解决方案帮助您无服务器架构实现弹性云服务器ECS日志的采集、分析、告警以及存档，基于云日志服务 LTS实时采集弹性云服务器 ECS的日志数据，通过函数工作流 FunctionGraph的LTS触发器自动获取日志数据，并实现对日志中告警信息的分析，通过消息通知服务 SMN将告警信息推送给用户，并存储到对象存储服务 OBS桶中进行存档。