# 云日志服务

# 用户指南

**文档版本** 01

**发布日期** 2023-08-30

**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



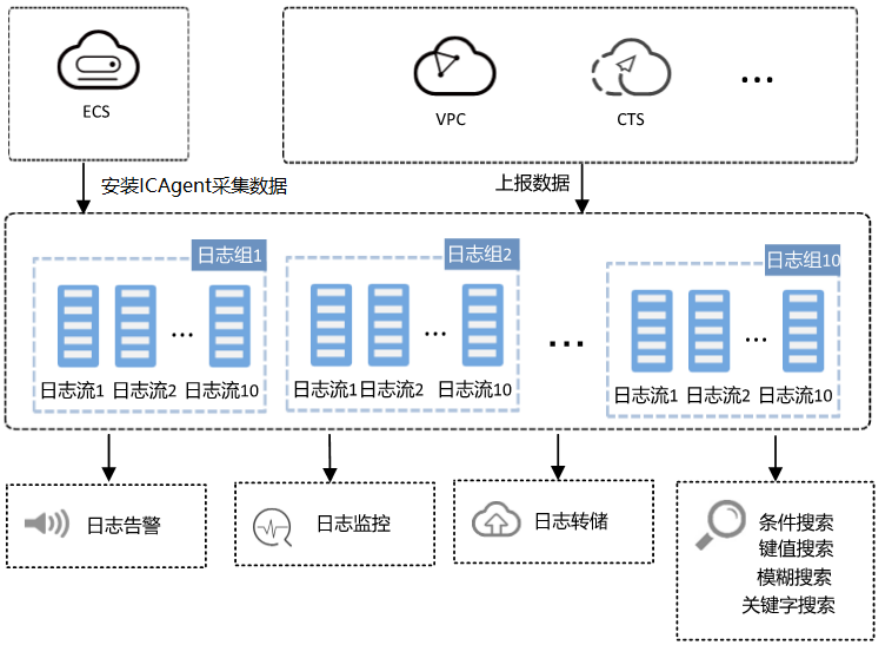
  

# 1 产品介绍

## 1.1 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 基本概念

## 日志组

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。

## 日志流

日志流是日志组的基本单位，每个帐号下可以创建100个日志组，每个日志组下又可以创建100个日志流。

日志通过日志流进行区分，您可以在写入时指定日志流，将不同类型的日志分类存储，便于您进行查询。例如，用户可以使用不同ID命名作为日志流，这样您在查询时可利用已写入的日志流快速查看到自己的日志。

# 1.3 产品功能

## 实时查看日志

您可以通过日志实时查看功能对日志文件内容进行实时查看，方便您诊断与LTS对接的服务日志的当前情况，同时支持对日志文件内容进行预览。

## 日志查询与实时分析

对上报的日志数据，按条件搜索，具有查询历史数据、诊断问题以及对系统进行追踪等作用；以便于进行设备运维管理、用户业务趋势分析等操作。

## 日志转储

日志服务对日志上报的数据默认存储时间为7天，超出存储时间的日志数据将会被自动删除。您若需要长期存储日志数据，可将日志转储至OBS桶中。

# 1.4 使用限制

本文介绍云日志服务日志读写的限制。

**表 1-1** 日志读写限制表

| 类别 | 限制项 | 说明 | 备注 |
| --- | --- | --- | --- |
| 帐号 | 日志写入流量 | 您在1个帐号下，写入流量最大为5MB/s。 | 如您有更大的使用需求，请联系技术支持工程师。 |
| | 日志写入次数 | 您在1个帐号下，写入次数最大为1000次/s。 | 如您有更大的使用需求，请联系技术支持工程师。 |
| | 日志查询流量 | 您在1个帐号下，通过API查询日志，单次返回日志最大为1MB。 | 如您有更大的使用需求，请联系技术支持工程师。 |
| | 日志读取次数 | 您在1个帐号下，读取次数最大为100次/min。 | 如您有更大的使用需求，请联系技术支持工程师。 |
| 日志组 | 日志写入流量 | 您在1个日志组下，写入流量最大为5MB/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100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50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5MB/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50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。 |

| 类别 | 限制项 | 说明 | 备注 |
| --- | --- | --- | --- |
| | 日志读取次数 | 您在1个日志流下，读取次数最大为10次/min。 | 非硬性限制，超过限制不保证服务质量。 |
| | 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。 | 不涉及。 |

# 1.5 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 1-2** 与其他服务之间关系

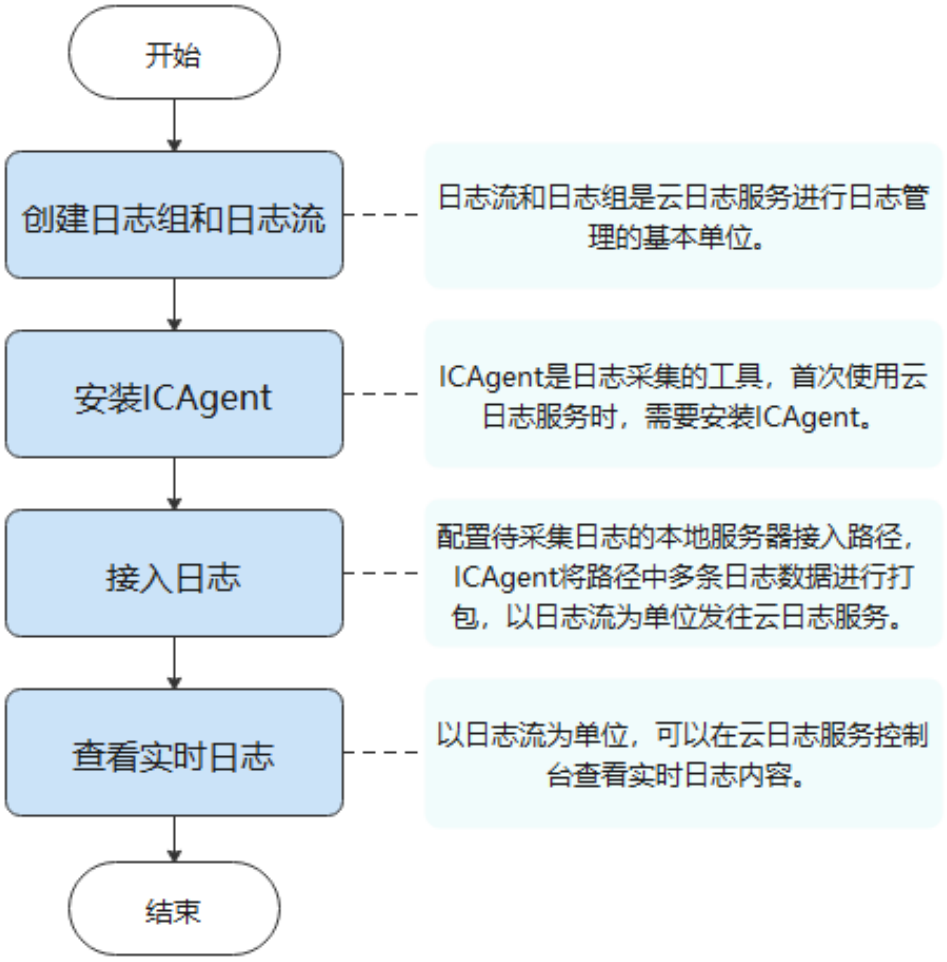
| 交互功能 | 相关服务 |
| --- | --- |
| 通过CTS服务，您可以记录与云日志服务相关的操作事件，便于日后的查询、审计和回溯。 | 云审计服务（Cloud Trace Service，简称CTS） |
| 通过OBS服务，您可以将需要长期存储的日志转储至OBS桶中，确保日志不丢失，实现数据持久化。 | 对象存储服务（Object Storage Service，简称OBS） |
| 通过AOM服务，可以进行站点访问统计，可以将相关日志上报给AOM，对其进行监控与告警。 | 应用运维管理（Application Operations Management，简称AOM） |
| 通过IAM服务，您可以给帐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） |

# 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。

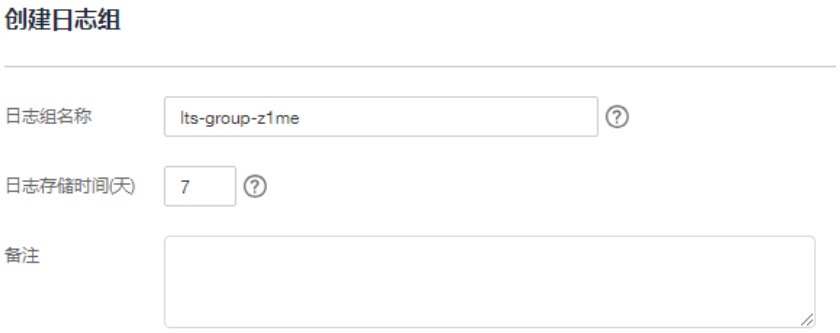
## 前提条件

已获取控制台的登录帐号与密码。

## 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。

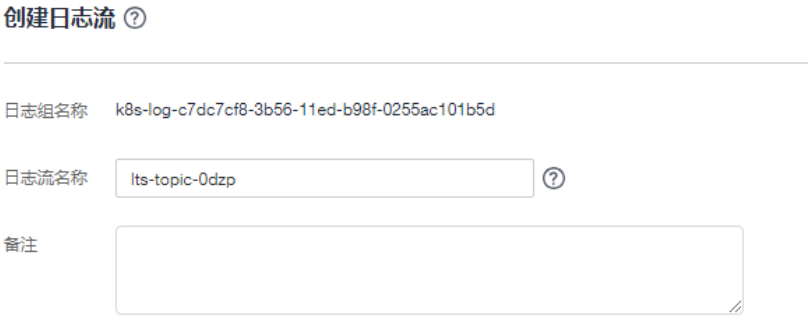
日志组名称需要满足如下要求：

- 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1~30天之间进行设置，如果不设置，系统默认存储时间为7天。
4. 自定义填写“备注”信息。
5. 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. 自定义填写“备注”信息。
5. 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”。

**图 2-2** 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**

请确保公共用户帐号及其创建的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（可选）”。

**图 2-3** 选择日志流


**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”。

**图 2-4** 选择主机组

**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** 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**

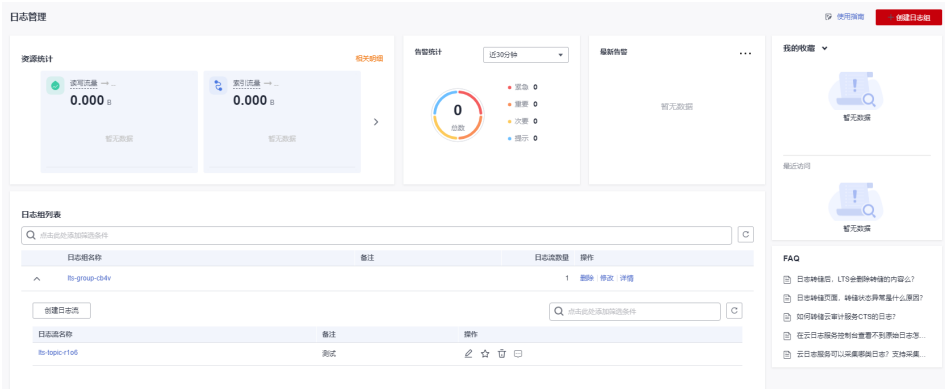
如果您正在使用实时查看功能，请停留在实时查看页面，请勿切换页面。如果您离开实时查看页面，实时查看功能将会被关闭。

# 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、告警统计、最新告警和FAQ等信息。

**图 3-1** 控制台首页




### 资源统计

资源统计展示帐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**。

**图 3-2** 资源统计


详细信息，请参见**资源统计**。

## 告警统计

告警统计展示云服务日志的告警总数及各个告警级别的数量。告警统计时间有：近30分钟、近1小时、近6小时、近1天和近1周；告警级别包括紧急、重要、次要和提示。

**图 3-3** 告警统计


## 最新告警

最新告警展示最新创建的告警规则，最多可显示近30分钟的3条告警规则。如需查看更多告警或添加告警，您可以单击 ··· 。

## 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。当您的帐号开通写权限时，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。所有帐号均显示我的收藏（本地缓存）。

  **说明**

  当您的帐号开通写权限时，**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：

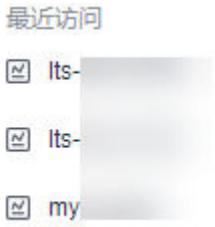
- 在日志流列表中，单击待取消收藏的日志流对应的 ，即可取消收藏。
- 在我的收藏中，鼠标悬浮待取消收藏的日志流，单击 ，即可取消收藏。

**----结束**

## 最近访问

最近访问展示最近访问的日志流。

**图 3-4** 最近访问




**说明**

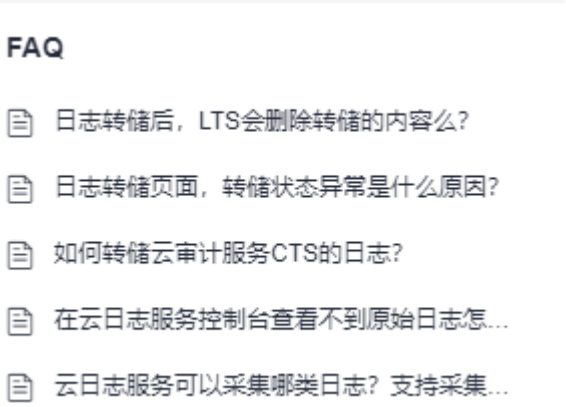
最近访问最多可显示3条日志流访问记录。

## FAQ

FAQ（常见问题）展示经常被询问的问题。

**图 3-5** FAQ




# 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

**图 3-6** 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。

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。

- 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，可以创建日志流以及设置日志存储时间，每个帐号下可以创建100个日志组。

## 前提条件

已获取控制台的登录帐号与密码。

# 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”。

**图 3-7** 创建日志组

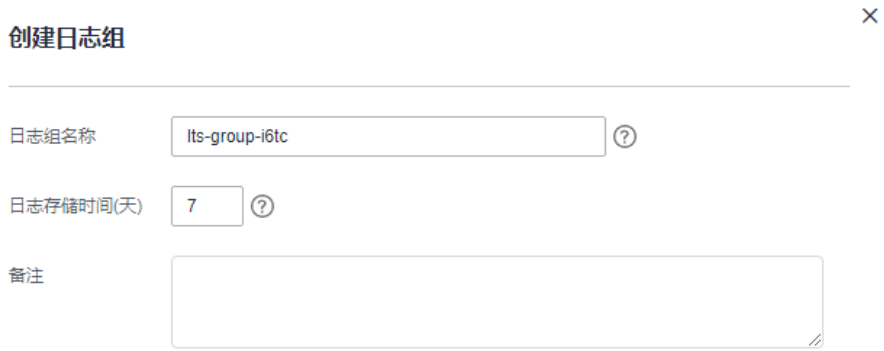

2. 在“创建日志组”页面中，输入日志组名称。

**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1~30天之间进行设置，如果不设置，系统默认存储时间为7天。

**图 3-8** 创建日志组



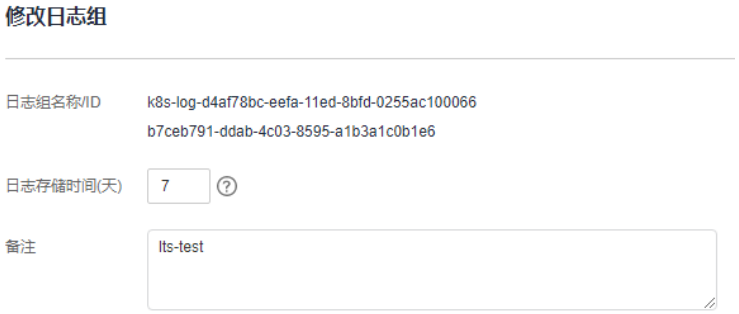

4. 填写“备注”，字符长度0-1024个字符。
5. 单击“确定”，完成日志组的创建。
   - 单击日志组名称，可跳转到日志流详情页面。
   - 并发创建时，可能会偶现创建个数超过限制。
   - 单击日志组操作列的“详情”可以查询日志组详情信息。

## 修改日志组

日志组创建完成后，如果您需要修改日志组的日志存储时间或备注，步骤操作如下：

1. 在日志组列表中，单击待修改日志组操作列下的“修改”。
2. 在弹出的修改日志组页面中 ，修改日志存储时间。

**图 3-9** 修改日志组




3. 完成后，单击“确定”。

## 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
- 备注

**图 3-10** 搜索日志组/日志流

## 其他操作

在日志组列表中，单击待查询流量日志组操作列下的“详情”，可查看该日志组名称、日志组ID、创建时间等详情。

# 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。

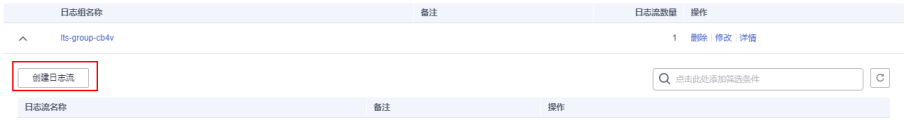
## 前提条件

已创建日志组。

## 创建日志流

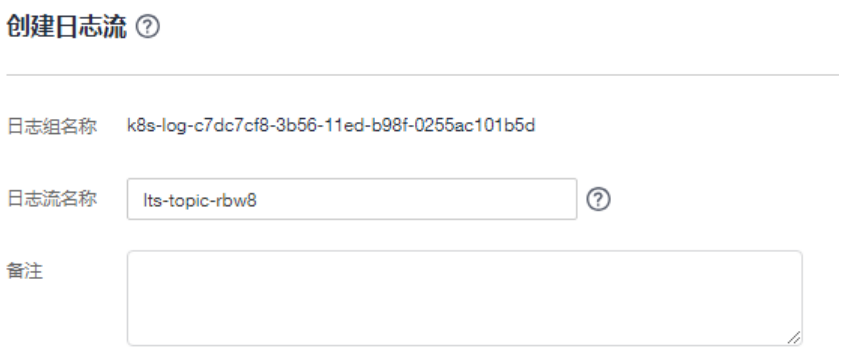
日志流的创建类型分为用户创建（主动）和云服务创建（被动），云服务创建指其他云服务与云日志服务进行系统对接后，系统自动在云日志服务控制台创建的日志流，本操作中日志流的创建类型为用户创建（主动）。

**图 3-11** 创建日志流




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。

**图 3-12** 创建日志流




**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. 填写“备注”，字符长度0-1024个字符。
4. 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。

## 修改日志流

日志流默认的存储时间和日志组保持一致。

1. 在日志流列表中，单击待修改日志流所在行的 按钮。
2. 修改日志流备注信息。
3. 单击“确定”。

## 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。

- **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。

# 4 日志接入

## 4.1 云服务接入

### 4.1.1 CCE 接入

云日志服务支持云容器引擎（Cloud Container Engine）日志接入。

#### 前提条件

- 已**安装ICAgent**并**添加至主机组**。
- 已**关闭采集容器标准输出到AOM的开关**。

#### 使用限制

- 目前不支持ServiceStage托管场景。
- 支持容器引擎为Docker的CCE集群节点。
- 支持使用Containerd作为容器引擎的CCE集群节点（ICAgent 5.12.130及以上版本）。
- 容器内的日志目录如果已挂载到主机目录上，将无法通过配置容器文件路径方式采集到LTS，只能通过配置节点文件路径方式采集到LTS。
- Docker存储驱动限制：容器文件日志采集目前仅支持overlay2存储驱动，不支持devicemapper作为存储驱动的节点。查看存储驱动类型，请使用如下命令：
  ```
  docker info | grep "Storage Driver"
  ```
- 如果选择日志流时，采集方式为采集到集中日志流时，则必须已创建CCE集群。

#### 操作步骤

云日志服务接入方式选择CCE接入时，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“云容器引擎 CCE-应用日志”进行CCE接入配置。

**步骤3** 选择日志流。

有两种采集方式：采集到自定义日志流和采集到集中日志流，您可以根据实际情况选择采集方式。

**采集到自定义日志流**

1. 单击“CCE集群”后的目标框，在下拉列表中选择具体的集群。
2. 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。
3. 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。
4. 单击“下一步：检查依赖项”。

**采集到集中日志流**

集中采集日志到一个固定的日志流。CCE集群默认有四种采集日志流，分别为标准输出/错误stdout-{ClusterID}、节点文件hostfile-{ClusterID}和容器文件containerfile-{ClusterID}。日志流名称会根据ClusterID自动命名，例如：集群ID为Cluster01，则标准输出/错误日志流为stdout-Cluster01。

在一个CCE集群下可创建四条采集日志流，标准输出/错误stdout-{ClusterID}、节点文件hostfile-{ClusterID}、容器文件containerfile-{ClusterID}），如果某个日志组下，已创建某种采集日志流，则不会在其他日志组或当前日志组下再创建该日志流。

1. 单击“CCE集群”后的目标框，在下拉列表中选择具体的集群。
2. 默认所属日志组为k8s-log-集群ID，例如集群ID为c7f3f4a5-bcb8-11ed-a4ec-0255ac100b07，默认所属日志组为k8s-log-c7f3f4a5-bcb8-11ed-a4ec-0255ac100b07。

   **说明**

   当无该日志组时，系统会提示：暂无该日志组，后续操作中，系统将会为您自动创建，创建完成后日志会集中采集到该日志组中。
3. 单击“下一步：检查依赖项”。

**步骤4** 检查依赖项。

系统自动检查以下内容检查项是否符合要求：

1. 已安装ICAgent，且版本 >= 5.12.130。
2. 存在名称和自定义标识都是**k8s-log-集群ID**的主机组。
3. 存在名为**k8s-log-集群ID**的日志组。
4. 存在系统推荐的集中采集的日志流。当选择日志流为**采集到集中日志流**时，会进行该项内容检查。

如果以上内容检查项中，有任意一项不符合要求，需单击“自动修复”按钮进行修复，否则将无法进行下一步操作。

**说明**

- **自动修复**：一键帮您完成以上内容检查项配置。
- **重新检查**：重新检查依赖项。

**说明**

当选择日志流为**采集到自定义日志流**时，“存在名为**k8s-log-集群ID**的日志组”的检查项为可选项。您可以通过开启或关闭开关进行控制，确定是否进行该项检查。

**步骤5** 选择主机组（可选）

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（自定义标识）**。

   **说明**

   - 默认选择集群所在的主机组，您可以根据需要选择其他已创建的主机组。
   - 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6** 采集配置。

设置具体的采集规则，具体可参考**采集配置**。

**步骤7** 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8** 完成。

单击“提交”，完成CCE接入。

**----结束**

## 采集配置

在使用CCE接入完成日志接入时，在采集配置页面的具体配置如下：

1. **基本信息**：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。
2. **数据源配置**：选择数据源类型，进行对应的数据源配置。
   - 容器标准输出：采集集群内指定容器日志，仅支持Stderr和Stdout的日志。

     **说明**

     - 被匹配上的容器的标准输出会采集到指定的日志流，原先采集到的AOM的标准输出会停止采集。
     - 容器标准输出不能重复配置，即使跨日志组和日志流，也只能配置一次。
   - 容器文件路径：采集集群内指定容器内的文件路径日志。
   - 节点文件路径：采集集群内指定节点路径的文件。

**说明**

采集路径不能重复配置，即同一个主机下的同一路径，即使跨日志组和日志流，也只能配置一次。

**表 4-1** 采集配置参数表

| 类型 | 参数配置 |
| --- | --- |
| 容器标准输出 | 采集容器标准输出到AOM、采集容器标准输出（stdout）和采集容器标准错误（stderr）。<br>采集容器标准输出到AOM：默认集群下的主机已安装了ICAgent 且采集日志到AOM，采集容器标准输出到AOM的开关处于开启状态。开启后标准输出只会采集到AOM，不会采集到LTS，建议您手动关闭该开关。<br>采集容器标准输出（stdout）和采集容器标准错误（stderr）两者必须得有一个是开启状态。 |
| 容器文件路径 | • 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。<br>**说明**<br>• 当CCE集群的工作负载中，已配置容器的挂载路径时，此时路径配置里添加的路径将无效。须将CCE集群页面中的挂载路径删除后，该配置才有效。<br>• 采集路径不能重复配置，即同一个主机下的同一路径，即使跨日志组和日志流，也只能配置一次。<br>• 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。 |
| 节点文件路径 | • 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。<br>**说明**<br>采集路径不能重复配置，即同一个主机下的同一路径，即使跨日志组和日志流，也只能配置一次。<br>• 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。 |

3. K8s匹配规则：当数据源类型选择容器标准输出和容器文件路径时，设置K8s匹配规则，非必选项。

**表 4-2** K8s 匹配规则

| 参数名称 | 参数说明 |
| --- | --- |
| K8s Namespace正则匹配 | 通过Namespace名称指定采集的容器，支持正则匹配。<br>**说明**<br>采集名称符合正则规则的Namespace的日志，为空时采集所有Namespace的日志。 |

| 参数名称 | 参数说明 |
| --- | --- |
| K8s Pod正则匹配 | 通过Pod名称指定待采集的容器，支持正则匹配。<br>**说明**<br>采集名称符合正则规则的Pod的日志，为空时采集所有Pod的日志。 |
| K8s容器名称正则匹配 | 通过容器名称指定待采集的容器（Kubernetes容器名称是定义在spec.containers中），支持正则匹配。<br>**说明**<br>采集名称符合正则规则的容器的日志，为空时采集所有容器的日志。 |
| 容器Label白名单 | 通过容器Label白名单指定待采集的容器。如果您要设置容器Label白名单，那么LabelKey必填，LabelValue可选填。<br>**说明**<br>如果LabelValue为空，则容器Label中包含LabelKey的容器都匹配；如果LabelValue不为空，则容器Label中包含LabelKey=LabelValue的容器才匹配；多个白名单之间为或关系，即只要容器Label满足任一白名单即可被匹配。 |
| 容器Label黑名单 | 通过容器Label黑名单排除不采集的容器。如果您要设置容器Label黑名单，那么LabelKey必填，LabelValue可选填。<br>**说明**<br>如果LabelValue为空，则容器Label中包含LabelKey的容器都被排除；如果LabelValue不为空，则容器Label中包含LabelKey=LabelValue的容器才会被排除；多个黑名单之间为或关系，即只要容器Label满足任一黑名单即可被排除。 |
| 容器Label日志标签 | 设置容器Label日志标签后，日志服务将在日志中新增容器Label相关字段。<br>**说明**<br>设置容器 Label日志标签后，lts将在日志中新增相关字段。例如设置LabelKey为app，设置LabelValue为app_alias，当容器中包含app=lts时，将在日志中添加的内容{app_alias：lts}。 |
| 环境变量白名单 | 用于指定待采集的容器。如果您要设置环境变量白名单，那么Label Key必填，Label Value可选填。<br>**说明**<br>如果环境变量Value为空，则容器环境变量中包含环境变量Key的容器都匹配；如果环境变量Value不为空，则容器环境变量中包含环境变量Key=环境变量Value的容器才被匹配；多个白名单之间为或关系，即只要容器的环境变量满足任一键值对即可被匹配。 |
| 环境变量黑名单 | 用于排除不采集的容器。如果您要设置环境变量黑名单，那么Label Key必填，Label Value可选填。<br>**说明**<br>如果环境变量Value为空，则容器环境变量中包含环境变量Key的容器都将被排除；如果环境变量Value不为空，则容器环境变量中包含环境变量Key=环境变量Value的容器才会被排除；多个黑名单之间为或关系，即只要容器的环境变量满足任一键值对即可被排除。 |
| 环境变量日志标签 | 设置环境变量日志标签后，日志服务将在日志中新增环境变量相关字段。<br>**说明**<br>设置环境变量日志标签后，lts将在日志中新增相关字段，例如设置环境变量Key为app，设置环境变量Value为app_alias，当容器中包含环境变量app=lts时，将在日志中添加的内容为{app_alias：lts}。 |

4. 高级配置：日志格式、日志时间具体说明如下：

**表 4-3** 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。<br>● 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。<br>**说明**<br>● 日志采集时间：ICAgent采集日志，并且发送到云日志服务的时间。<br>● 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。<br>● 采集日志时间限制：系统时间的前后24小时内。 |
| | 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。<br>● 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。<br>● 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。<br>**说明**<br>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。<br>填写示例：<br>YY - year (19)<br>YYYY - year (2019)<br>M - month (1)<br>MM - month (01)<br>D - day (1)<br>DD - day (01)<br>hh - hours (23)<br>mm - minutes (59)<br>ss - seconds (59)<br>SSS - millisecond（999）<br>hpm - hours (03PM)<br>h:mmpm - hours:minutes (03:04PM)<br>h:mm:sspm - hours:minutes:seconds (03:04:05PM)<br>hh:mm:ss ZZZZ (16:05:06 +0100)<br>hh:mm:ss ZZZ (16:05:06 CET)<br>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。 |

| 名称 | 说明 |
| --- | --- |
| 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。 |

**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**。

## 4.1.2 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。

**图 4-1** 选择日志流

3. 单击“下一步：选择主机组（可选）”。

**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** 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. 采集Windows事件日志：当选择Windows主机采集日志时，需要开启“采集Windows事件日志”，配置如下参数：

   **表 4-4** 采集 Windows 事件日志参数

| 名称 | 说明 |
| --- | --- |
| 日志类型 | 日志类型有系统、应用程序、安全和启动。 |
| 首次采集时间偏移量 | 如设置为7天，表示从采集开始时间前7天内的日志（7天前的日志被忽略），该时间仅在首次配置采集生效，确保不会重复采集。最大支持设置为7天。 |
| 事件等级 | 事件等级有information、warning、error、critical和verbose。根据Windows事件等级过滤采集。仅支持Windows Vista及以上的操作系统。 |

5. 日志格式、日志时间具体说明如下：

   **表 4-5** 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。<br>• 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。 |

| 名称 | 说明 |
| --- | --- |
| 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。<br>**说明**<br>• 日志采集时间：ICAgent采集日志，并且发送到云日志服务的时间。<br>• 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。<br>• 采集日志时间限制：系统时间的前后24小时内。 |
| | 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。<br>• 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。<br>• 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。<br>**说明**<br>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。<br>填写示例：<br>YY - year (19)<br>YYYY - year (2019)<br>M - month (1)<br>MM - month (01)<br>D - day (1)<br>DD - day (01)<br>hh - hours (23)<br>mm - minutes (59)<br>ss - seconds (59)<br>SSS - millisecond（999）<br>hpm - hours (03PM)<br>h:mmpm - hours:minutes (03:04PM)<br>h:mm:sspm - hours:minutes:seconds (03:04:05PM)<br>hh:mm:ss ZZZZ (16:05:06 +0100)<br>hh:mm:ss ZZZ (16:05:06 CET)<br>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。 |

**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  。

# 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。<br>2. 在主机组列表中，单击待修改的主机组所在行的操作列 。<br>3. 在弹出的修改主机组页面，修改主机组名称、自定义标识。<br>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：**<br>1. 在主机组列表，单击待修改的主机组所在行前的 。<br>2. 在主机页签，单击“添加主机”。<br>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。<br>● 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。<br>● 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**。<br>4. 单击“确定”。<br>**方式二：**<br>1. 在主机管理页面，单击“主机”，切换至主机页签。<br>2. 在主机列表中勾选需要添加的主机，单击“添加到主机组”。<br>3. 在弹出的添加到主机组页面，勾选目标主机组。<br>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 。<br>2. 在主机页签，单击待移除主机所在行操作列的“移除”。<br>3. 在弹出的移除主机页面，单击“确定”，将该主机移除。<br>**说明**<br>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 。<br>2. 在主机页签，单击待移除主机所在行操作列的“取消部署”。<br>3. 在弹出的取消部署页面，单击“确定”，将该主机卸载并移除。<br>**说明**<br>● 自定义标识主机组下的主机不支持该操作。<br>● 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 。<br>2. 在主机页签，勾选待删除的主机，单击“批量移除”。<br>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 。<br>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。<br>3. 单击“新增关联配置”。<br>4. 在弹出的新增关联配置页面，勾选需要关联的接入配置。<br>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”。<br>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”。<br>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”。

**图 5-1** 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帐号的AK/SK，请勿使用个人帐号的AK/SK。

  **须知**

  请确保公共用户帐号及其创建的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”。

   选择“CCE集群”，在右侧下拉框中，选择待升级ICAgent的集群，单击“升级ICAgent”。

**说明**

- 未创建CCE集群时，采集容器标准输出到AOM的开关为置灰状态。
- 当ICAgent版本号为5.12.133及以上时，支持关闭采集容器标准输出到AOM的开关功能。
- 首次创建的CCE集群，默认集群下的主机已安装了ICAgent 且上报日志到AOM，采集容器标准输出到AOM的开关处于开启状态；如需将日志上报至LTS则执行升级ICAgent操作时，关闭采集容器标准输出到AOM的开关。建议使用“接入日志 > 云服务接入 > 云容器引擎CCE”直接采集容器标准输出到LTS，不推荐采集到AOM。
- CCE集群ID（ClusterID）： 每个集群为固定的ID。
- 升级ICAgent时，LTS将为您的CCE集群创建对应的日志组和主机组。且该日志组和主机组的名称为k8s-log-{ClusterID}。您可以创建接入配置（云服务接入>云容器引擎CCE）将当前CCE集群的日志接入到该日志组。
- 当集群里的主机未安装ICAgent或ICAgent版本过低时，单击“升级ICAgent”操作，可对该集群里的所有主机安装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。 |
| 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。 |

# 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。<br>● 手动刷新：单击“手动刷新”可直接对日志进行刷新。<br>● 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。<br>**说明**<br>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”。<br>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。<br>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。<br>**说明**<br>• 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。<br>• 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。<br>**说明**<br>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。<br>• 是否简化显示：开启该按钮，日志的字段内容将简化显示。<br>• 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。<br>**说明**<br>默认开启格式化，JSON默认展开层级为2层。<br>• 开启格式化按钮：设置JSON默认展开层级，最大设置为10层。<br>• 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。<br>● 当日志流未配置版面设置时，将不显示 按钮。<br>● 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。 |

## 搜索语法及样例

**搜索语法：**

**表 6-2** 搜索语法

| 条件 | 说明 |
| --- | --- |
| 关键字精确搜索 | 针对日志中的关键字进行精确搜索，大小写敏感。关键词指相邻两分词符之间的单词。<br>如果对分词符规则不熟悉，建议在关键词后加上*，例如：error*，帮助搜索。 |
| 短语精确搜索 | 针对日志中的短语进行精确搜索，大小写敏感。 |
| && | 搜索结果的交集。 |
| \|\| | 搜索结果的并集。 |
| AND | 搜索结果的交集。 |
| and | 搜索结果的交集。 |
| OR | 搜索结果的并集。 |
| or | 搜索结果的并集。 |
| NOT | 搜索结果不包含NOT后的关键字。 |
| not | 搜索结果不包含not后的关键字。 |
| ? | 模糊搜索能力，?放在关键字中间或末尾，用于替代一个字符。 |
| > | 搜索结构化long或float类型字段大于某个数值，例如：num>10。 |
| < | 搜索结构化long或float类型字段小于某个数值，例如：num < 10。 |
| = | 搜索结构化long或float类型字段等于某个数值，例如：num = 10。 |
| >= | 搜索结构化long或float类型字段大于等于某个数值，例如：num >= 10。 |

| 条件 | 说明 |
| --- | --- |
| <= | 搜索结构化long或float类型字段小于等于某个数值，例如：num <= 10。 |
| : | 用于字段查询（Key:Value），例如：request_method:GET。<br>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"file info":apsara。 |
| "" | 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"。<br>表示查询包含and的日志，此处的and不代表运算符。<br>在字段查询中双引号（""）内的所有词被当成一个整体。 |
| \ | 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。 |
| * | 通配符查询，*只能放在关键字后，可以匹配零个、单个、多个字符。例如：host:abcd*c。<br>**说明**<br>云日志服务会在所有日志中为您查询到符合条件的100个词，返回包含这100个词并满足查询条件的所有日志。 |
| in | 查询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<br>request_time in [100 200]或request_time in (100 200]。<br>**说明**<br>in只能为小写字母；仅支持long或float类型字段。 |
| () | 用于提高括号内查询条件的优先级（支持 and、or、not查询条件）。例如：(request_method:GET or request_method:POST) and status:200。 |
| key:#"abc def" | 字段查询。配置字段索引后，可以指定字段名称和字段值（Key:Value）进行查询。 |
| #"abc def" | 全文查询。配置分词符后，云日志服务根据您设置的分词符将整条日志拆分成多个词。可以指定关键字（字段名、字段值）和查询规则进行查询。 |

**说明**

如果原始日志中本身包含搜索语法的关键字（&&、||、AND、OR、NOT、*、?、:、>、<、=、>=、<=、"），则不支持使用这些关键字来搜索日志。

**搜索规则：**

- 支持模糊搜索能力。

  例如：输入error*，可以查找所有含有error的日志且高亮以error开头的日志内容。

- 支持键与值格式的多条件组合搜索，格式为：key1:value1 AND key2:value2或key1:value1 OR key2:value2。输入或选择key1:value1进行搜索后，需添加AND或OR，才可以在搜索框中继续输入或选择key2:value2对两个条件同时进行搜索。
- 支持单击关键词弹出菜单项，有**复制**、**添加到查询**和**从查询中排出**三种操作。

  复制：复制该字段

  添加到查询：在查询的语句中添加“AND field: value ”

  从查询中排出：在查询的语句中添加“NOT field: value”

**搜索样例：**

- 搜索含有start的所有日志：start。
- 搜索含有start to refresh的所有日志：start to refresh。
- 搜索同时包含start和unexpected的日志数据：start && unexpected。
- 搜索同时包含start和unexpected的日志数据：start AND unexpected。
- 搜索包含start或者unexpected的日志数据：start || unexpected。
- 搜索包含start或者unexpected的日志数据：start OR unexpected。
- 不包含query1的日志数据：NOT content : query1。
- 搜索日志内容中含有error的所有日志：error*。
- 搜索日志内容中以“er”开头，以“or”结尾，并且中间有一个字符的所有日志：er?or。
- 搜索的关键词中含有分词符（:）时，搜索日志： content : "120.46.138.115:80" 或者 content : 120.46.138.115:80 。
- 搜索包含query1而且包含query2，但不包含query3的日志数据：query1 AND query2 AND NOT content : query3。

**说明**

- 输入关键字查询日志时，关键字区分大小写，搜索的日志内容大小写敏感，高亮的日志内容大小写敏感。
- 全文搜索时，模糊搜索 “*”，“?” 不匹配特殊字符，例如：“-”、空格。
- 支持关键词模糊匹配搜索，关键词不能以“?”或“*”开头。例如：关键词可以输入"ER? OR"或"ER*R"。
- 使用关键词搜索时，当单条日志超过255长度时，可能无法精确查询。

# 6.2 结构化配置

## 6.2.1 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**

结构化后的日志数据可理解为数据库中的二维表，接下来就可以使用SQL语句对提取的字段进行查询与分析。

**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**

## 6.2.2 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。

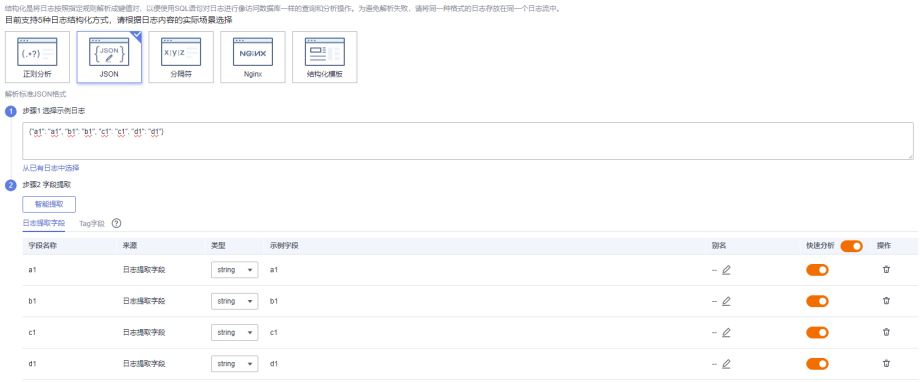
在“步骤2 字段提取”下单击“智能提取”。以如下原始日志为例进行分析：

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。

**图 6-1** 提取结果



**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**。

## 6.2.3 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ELB、VPC、CTS、APIG、DCS审计日志、TOMCAT、NGINX、GAUSSV5审计日志、DDS审计日志、DDS错误日志、DDS慢日志、CFW访问控制日志、CFW攻击日志、CFW流量日志、MYSQL错误日志、MYSQL慢日志、POSTGRESQL慢日志、POSTGRESQL错误日志、SQLSERVER错误日志、GAUSSDB_REDIS慢日志、CDN、SMN、GAUSSDB_MYSQL错误日志、GAUSSDB_MYSQL慢日志、ER企业路由器、MYSQL审计日志、GaussDBforCassandra慢日志、GaussDBforMongo慢日志、GaussDBforMongo错误日志。

**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。

## 6.2.4 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 6-3** 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。<br>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。<br>• 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 |
| ELB模板 | 根据ELB资料中提供的日志字段被定义。 | 否 | 否 |
| VPC模板 | 根据VPC资料中提供的日志字段被定义。 | 否 | 否 |
| CTS模板 | 字段名称为json日志中的key。 | 否 | 否 |
| APIG模板 | 根据APIG资料中提供的日志字段被定义。 | 否 | 否 |
| DCS审计日志 | 根据DCS资料中提供的日志字段被定义。 | 否 | 否 |
| TOMCAT | 根据TOMCAT官网提供的字段名称进行nginx解析的名称 | 否 | 否 |

| 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 |
| --- | --- | --- | --- |
| NGINX | 根据NGINX资料中提供的日志字段被定义。 | 否 | 否 |
| GAUSSV5审计日志 | 根据GAUSSV5资料中提供的日志字段被定义。 | 否 | 否 |
| DDS审计日志 | 根据DDS资料中提供的日志字段被定义。 | 否 | 否 |
| DDS错误日志 | 根据DDS资料中提供的日志字段被定义。 | 否 | 否 |
| DDS慢日志 | 根据DDS资料中提供的日志字段被定义。 | 否 | 否 |
| CFW访问控制日志 | 根据CFW资料中提供的日志字段被定义。 | 否 | 否 |
| CFW攻击日志 | 根据CFW资料中提供的日志字段被定义。 | 否 | 否 |
| CFW流量日志 | 根据CFW资料中提供的日志字段被定义。 | 否 | 否 |
| MYSQL错误日志 | 根据MYSQL资料中提供的日志字段被定义。 | 否 | 否 |
| MYSQL慢日志 | 根据MYSQL资料中提供的日志字段被定义。 | 否 | 否 |
| POSTGRESQL错误日志 | 根据POSTGRESQL资料中提供的日志字段被定义。 | 否 | 否 |
| SQLSERVER错误日志 | 根据SQLSERVER资料中提供的日志字段被定义。 | 否 | 否 |
| GAUSSDB_REDIS慢日志 | 根据GAUSSDB_REDIS资料中提供的日志字段被定义。 | 否 | 否 |
| CDN | 根据CDN资料中提供的日志字段被定义。 | 否 | 否 |
| SMN | 根据SMN资料中提供的日志字段被定义。 | 否 | 否 |
| GAUSSDB_MYSQL错误日志 | 根据GAUSSDB_MYSQL资料中提供的日志字段被定义。 | 否 | 否 |
| GAUSSDB_MYSQL慢日志 | 根据GAUSSDB_MYSQL资料中提供的日志字段被定义。 | 否 | 否 |
| ER企业路由器 | 根据ER企业路由器资料中提供的日志字段被定义。 | 否 | 否 |

| 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 |
| --- | --- | --- | --- |
| MYSQL审计日志 | 根据MYSQL审计日志资料中提供的日志字段被定义。 | 否 | 否 |
| GaussDBforCassandra慢日志 | 根据GaussDBforCassandra慢日志资料中提供的日志字段被定义。 | 否 | 否 |
| GaussDBforMongo慢日志 | 根据GaussDBforMongo慢日志资料中提供的日志字段被定义。 | 否 | 否 |
| GaussDBforMongo错误日志 | 根据GaussDBforMongo错误日志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**

# 6.3 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。

# 6.4 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** 在“原始日志”页签，单击“创建快速分析”或 按钮，在展开的“管理快速分析”界面，选择快速分析的字段。

**图 6-2** 创建快速分析


**步骤4** 单击“确定”，快速分析创建完成。

**说明**

- abc 表示String类型字段。
- 1.2 表示float类型字段。
- 123 表示long类型字段。
- 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。
- 单击快速分析右侧的 ，可以修改或者删除已添加的字段。如果您在结构化界面删除了某一字段，或者对字段名称进行了修改，快速分析会同步更新。

**----结束**

# 6.5 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. 在原始日志页签，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 6-4** 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。 |

| 功能 | 说明 |
| --- | --- |
| 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 告警规则

### 7.1.1 关键词告警

LTS支持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。目前每个帐户最多可以创建关键词告警共200个。

#### 前提条件

已创建日志组、日志流。

#### 创建告警规则

**步骤1** 在云日志服务管理控制台，单击“告警”。

**步骤2** 在告警页面默认显示“告警列表”，单击“告警规则”切换至告警规则页面。

**步骤3** 单击“创建”，在界面右侧弹出“新建告警规则”页面。

**步骤4** 在“新建告警规则”页面，配置告警规则相关参数。

**表 7-1** 配置告警规则参数

| 参数名称 | 说明 | 校验规则 | 样例 |
| --- | --- | --- | --- |
| 规则名称 | 告警规则的名称。 | 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。 | LTS-Alarm |

| 参数名称 | 说明 | 校验规则 | 样例 |
| --- | --- | --- | --- |
| 描述 | 对该规则进行简要描述。 | 长度不能超过64个字符。 | - |
| 统计类型 | 选择关键词统计。 | - | 关键词统计 |
| 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。 | - | - |
| 关键词 | 设置关键词，LTS会根据设置的关键词对日志流中的日志进行监控。 | 关键词支持精确匹配和模糊匹配，区分大小写，输入长度不超过1024个字符。 | hostIP :192 |
| 查询时间 | 指定关键词的查询周期。查询关键词时间范围：从当前时间往前推一个周期。例如：查询时间设置为1小时，当前时间为9:00，则查询关键词的时间范围为8:00-9:00。<br>● 如果查询时间单位为分钟，则取值范围是1-60；<br>● 如果查询时间单位为小时，则取值范围是1-24。 | - | 1小时 |

| 参数名称 | 说明 | 校验规则 | 样例 |
| --- | --- | --- | --- |
| 统计周期 | 条件表达式查询的频率可以设置为：<br>● 每小时：表示整点小时查询。<br>● 每天：需要指定几点整查询。<br>● 每周：需要指定周几的几点整查询。<br>● 固定间隔：自定义间隔周期，需要指定1-60分钟/1-24小时。例如：当前时间为9:00，固定间隔设置为5分钟，则第一次查询时间为9:00，第二次查询时间为9:05，第三次查询时间为9:10.....<br>**说明**<br>当查询时间大于1小时，固定间隔时间最小取值为5分钟。<br>● CRON表达式：CRON表达式的最小精度为分钟，格式为24小时制，示例如下：<br>– 0/10 * * * *从00:00开始，每隔整10分钟查询一次，分别为10分钟、20分钟、30分钟、40分钟、50分钟、60分钟。例如：当前时间为16:37，下一次查询时间为16:50。<br>– 0 0/5 * * *从00:00开始，每隔5小时查询一次，分别为0时、5时、10时、15时、20时。例如：当前时间为16:37，下一次查询时间为20:00。<br>– 0 14 * * *每天14:00查询一次。<br>– 0 0 10 * *每月10日00:00查询一次。 | - | 每天 01:00 |
| 匹配条数 | 当关键词搜索结果的日志条数达到设定的条数时，会触发告警。<br>支持大于（>）、大于等于（>=）、小于（<）、小于等于（<=）4种比较运算符。 | 日志条数支持最小值: 1，最大值: 2147483647。 | >10 |
| 触发条件 | 配置触发条件，即满足该条件时，会触发告警。<br>统计周期次数指上面设置的统计周期；满足条件次数指设置的关键词。配置的统计周期次数须大于等于满足触发条件次数。 | 统计周期次数最小值为1，最大值为10。 | 4，2 |
| 触发告警级别 | 包括“紧急”、“重要”、“次要”、“提示”，默认“紧急”。 | - | 紧急 |

| 参数名称 | 说明 | 校验规则 | 样例 |
| --- | --- | --- | --- |
| 发送通知 | 包括“不发送”、“发送”，默认“不发送”。 | - | 不发送 |
| 告警主题 | 当“发送通知”中选择“发送”时，需要在下拉框选择该告警的主题，其中告警主题可多选。<br>若没有您想要选择的主题，请单击创建主题。<br>若您需要修改时区/语言，可单击“修改”，在帐号中心里进行设置。 | 当“发送通知”中选择“发送”时，该参数为必选。 | - |

**步骤5** 单击“确定”，完成对关键词告警规则的创建。

也可以在**日志管理>日志流>原始日志**页面中单击右上角的，选择“告警规则”页签，可创建告警规则。

**说明**

告警规则创建完成后，默认开启**状态**按钮。当开启该按钮且关联日志流满足告警规则时，会触发告警；当关闭该按钮，即使有满足该告警规则的情况，也不会触发告警。

**----结束**

## 修改告警规则

**步骤1** 单击告警规则所在行后的“修改”，根据表7-1修改具体参数，其中“规则名称”和“统计类型”不可修改。

**步骤2** 单击“确定”。

**----结束**

## 删除告警规则

**步骤1** 单击告警规则所在行后的“删除”，单击“确定”删除该规则。

**----结束**

# 7.2 告警列表

云日志服务支持对日志数据进行监控，通过配置关键词告警规则，定时查询日志数据，当设置的匹配条数或条件表达式满足时，将告警进行上报，用户可以在LTS控制台查看告警。

## 前提条件

已创建告警规则，具体请参见关键词告警。

## 查看告警

**步骤1** 在云日志服务管理控制台，单击“告警”。

**步骤2** 默认显示“告警列表”页面，在该页面默认显示30分钟（相对）的所有告警列表及其趋势图。

**步骤3** 输入查询条件后进行搜索，页面会展示该条件下的所有告警信息及这些告警的趋势图，具体查询条件如下：

- 在页面上方搜索框中可根据日志组、日志流和告警级别进行搜索。
- 设置时间范围，默认时间范围为30分钟（相对）。

  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。

**步骤4** 设置搜索条件后，单击，查找在已设时间范围内满足搜索条件的告警。

**步骤5** 查询的告警默认显示在“活动告警”页签下，将鼠标放在目标告警所在行中的“告警详情”可查看告警详情。单击告警列表中对应的“名称”，界面右侧弹出该告警的详细信息。

告警故障已经解除时，可单击列表中告警所在行后的对该告警进行清除，被执行清除操作后的告警将会显示在“历史告警”页签。

针对已设置好的搜索条件，告警列表默认需要手动刷新，如需设置自动刷新可单击告警界面右上角，在弹出的下拉列表中选择“30秒自动刷新”、“1分钟自动刷新”或“5分钟自动刷新”，若在设置自动刷新后需要手动刷新，也可在下拉列表重新选择“手动刷新”。

**----结束**

# 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，您在创建日志组时，可以对日志存储进行设置（1-30天）。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。

**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**

- 目前此功能仅支持白名单用户使用，需要提交工单申请才能使用。详细操作请参考。
- 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。<br>– 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。<br>– 如果OBS桶为加密桶，则需要选择“密钥名称”，并勾选下方的“我同意在KMS创建授权给LTS帐号，对转储日志加解密”。<br>● LTS目前仅支持存储类别为“标准存储”的OBS桶。 | - |
| 密钥名称 | 对于加密的OBS桶，选择密钥名称。如果没有可选择的密钥，单击“创建密钥并授权”，进入数据加密控制台，创建密钥。 | - |

| 参数名称 | 说明 | 样例 |
| --- | --- | --- |
| 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：<br>– “/LogTanks/RegionName”为系统默认路径，不可以修改。<br>– 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。<br>– 自定义转储路径名称不允许为空，长度限制为1~128个字符。<br>示例：<br>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*。<br>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*。<br>● 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 |
| 日志文件前缀 | 转储至OBS桶中的日志文件前缀。<br>日志文件前缀需符合如下规范：<br>● 名称长度限制为0~64个字符。<br>● 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。<br>示例：输入LTS-log，则日志文件名称为：LTS-log_日志文件名称。 | LTS-log |

| 参数名称 | 说明 | 样例 |
| --- | --- | --- |
| 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”。<br>● 原始日志格式示例：<br>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。<br>Sep 30 07:30:01 ecs-bd70 CRON[3459]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)<br>● JSON格式示例：<br>{"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 |

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”。

**图 9-1** 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。

日志采集关闭后，ICAgent会停止采集日志，且在应用运维管理AOM控制台的“日志采集开关”也会同步关闭。

**----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。

### 10.1.3 在 AOM（应用运维管理）中关闭超额继续采集日志开关，会影响 LTS（云日志服务）收集日志吗?

会。云日志服务与应用运维服务的日志采集开关为同步状态，即如果您在应用运维管理服务关闭了“超额继续采集日志”开关，则云日志服务的开关也同样关闭，关闭后将停止采集日志。

### 10.1.4 CCE 标准输出日志默认采集到 AOM，应该如何关闭?

#### 问题描述

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

使用要求，须在云日志服务（LTS）控制台进行关闭。推荐您将CCE标准输出日志直接采集到云日志服务（LTS），由LTS对日志进行统一管理。

**说明**

关闭CCE标准输出到AOM后，您在云日志服务（LTS）中配置的CCE标准输出采集到LTS才会生效。

### 解决办法

**步骤1** 在云日志服务（LTS）控制台，单击左侧导航栏“主机管理”。

**步骤2** 选择“主机”页签，单击“CCE集群”。

**步骤3** 在CCE集群中，选择您需要关闭标准输出到AOM的CCE集群，关闭**采集容器标准输出到AOM**按钮。

**步骤4** 单击“确定”，待ICAgent重启完成后，已关闭CCE标准输出到AOM。

**----结束**

# 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
- 当前帐号欠费，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自动清理过期的日志数据。

## 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“配置追踪器”页面，在OBS转储下方，选择OBS转储到对应的OBS桶。


4. 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”。

5. 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帐号的AK/SK，请勿使用个人帐号的AK/SK。

### 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“临时访问密钥”。
3. 进入“临时访问密钥”页面，单击密钥操作列的“创建”即可生成访问密钥信息。

   **说明**

   为防止AK/SK泄露，建议您将其保存到安全的位置。