云日志服务

用户指南

文档版本 01

发布日期 2025-02-21

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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 授权 IAM 用户使用云日志服务 LTS

如果需要对您所拥有的云日志服务LTS（Log Tank Service）进行精细的权限管理，可以使用**统一身份认证服务**（Identity and Access Management，简称IAM），通过IAM可以进行如下操作：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用LTS资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将LTS资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用LTS服务的其它功能。

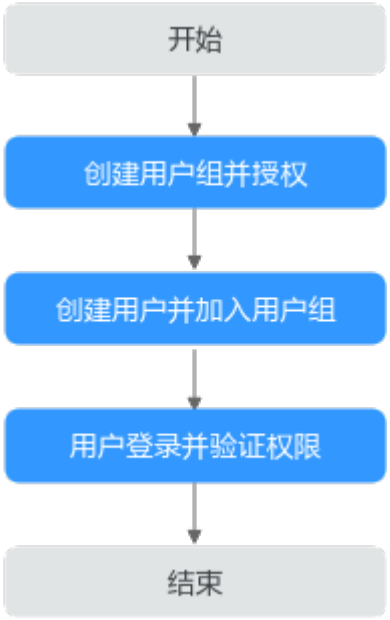
本章节为您介绍对用户授权的方法，操作流程如**图1-1**所示。

前提条件

给用户组授权之前，请您了解用户组可以添加的LTS权限，并结合实际需求进行选择LTS支持的系统权限，请参见：**权限管理**。

示例流程

图 1-1 给用户授权 LTS 权限流程



1. 登录统一身份认证服务IAM控制台。在IAM控制台创建用户组，并授予云日志服务操作权限“LTS FullAccess”。详细操作请参考**创建用户组并授权**。

   说明

   选择“LTS FullAccess”，由于该策略有依赖，除了勾选LTS FullAccess外，还需要在同项目中勾选依赖的策略：Tenant Guest、以及“全局区域 对象存储服务项目”中勾选依赖的策略：Tenant Administrator。

2. 在IAM控制台创建用户，并将其加入**步骤1**中创建的用户组。详细操作请参考**创建用户并加入用户组**。
3. 使用新创建的用户登录控制台，切换至授权区域，进入云日志服务控制台可以正常操作并使用LTS。详细操作请参考**用户登录**并验证权限。

2 购买 LTS 资源包

云日志服务LTS支持购买按需资源包进行计费，在费用结算时，优先从资源包中抵扣用量。先购买资源包，后抵扣费用，适用于业务用量相对稳定的场景。更多计费信息**价格计算器**。

使用规则

- 资源包到期后，按需资源不会自动关闭，将会以按需付费的方式继续使用。
- 超出额度部分的按需用量，将会按需收费。
- 资源包计费周期的起点是用户设置的生效时间，清零和恢复时间点是购买时长到期后当天的23:59:59。
- 资源包到期后，剩余资源不会结余，将会自动清零。更多信息请参考**资源包扣减规则**。

购买 LTS 资源包

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“购买资源包”。

步骤3 在购买资源包页面，请参考**表2-1**或**表2-2**设置参数。

说明

资源包中的冷存储包是白名单功能，同时需要开启智能冷存储，详情请参考**管理日志流**，如有需要请**提交工单**申请开通。

表 2-1 推荐规格参数说明

参数	说明
区域	云日志服务所在的区域，建议选择与业务应用系统相同的地域。
计算方式	推荐规格。
资源包类型	支持读写流量包、索引流量包、标准存储包、冷存储包（白名单功能）。
规格	默认支持100GB。

参数	说明
购买数量	资源包的数量，支持设置1-3000。
规格说明	根据用户选择的数量进行计算，例如购买2个资源包，规格为规格*规格数量=100GB*2=200GB。 **说明** • 在LTS控制台的购买资源包页面，存储量的单位是GB/月。在费用中心控制台，存储量的单位是GB/小时。例如在LTS购买1个数量100GB的标准存储包（100GB/月），在费用中心的资源包页面存储总量有100GB*1个*24小时*30天=72000GB。 • 若只购买1个数量100GB的读写流量包，在费用中心的资源包页面总量显示100GB。 • 若只购买1个数量100GB的索引流量包，在费用中心的资源包页面总量显示100GB。
购买时长	选择资源包的使用时长，支持按月、按年购买。
生效时间	• 支付完成后立即生效，即购买成功后，优先从资源包中抵扣用量。 • 指定生效时间：设置指定生效的具体时间，例如2023/07/11 10:30:00。 **说明** 资源包生效时间非整点时，例如2023/07/11 10:30:00开始生效，开始抵扣时间为下一个整点2023/07/11 11:00:00。
定向使用	• 所有企业项目均可使用。 • 限定企业项目使用套餐包，选择特定企业项目。 **说明** 如果您没有开通企业管理服务，将无法看到企业项目选项。开通方法请参见**如何开通企业项目**。

表 2-2 一键测算参数说明

参数	说明
区域	云日志服务所在的区域，建议选择与业务应用系统相同的地域。
计算方式	一键测算：按照每天新增日志量（GB/天或TB/天）、日志存储时长（天）、标准存储层数据保存时间(天)进行测算读写流量包、索引流量包、标准存储包、冷存储包的使用量。（冷存储包是白名单功能，开通冷存储功能后，才需要设置标准存储层数据保存时间。） 读写流量包和索引流量包与每天新增日志量有关，标准存储包和和冷存储包与每天新增日志量、日志存储时长、标准存储层数据保存时间(天)有关。

参数	说明
测算结果	例如选择每天新增日志量10GB/天，日志存储时长30天，标准存储层数据保存时间7天，云日志服务提供默认规格是100GB，一键测算一个月的结果如下：（若是选择TB/天，先将TB换算为GB）  • 读写流量包100GB*1，读写有5倍的压缩率，因此所需要的数量：（10GB*30天）/5=60GB ，不足100GB的算1个。 • 索引流量包100GB*3，所需要的数量：（10GB*30天）/100GB=3个。 • 标准存储包100GB*1，所需要的数量：10GB*7天=70GB，不足100GB的算1个。 • 冷存储包100GB * 3，冷存储的天数为30-7=23天，所需要的数量：（10GB*23天）/100GB=3个，不足100GB的算1个。
购买时长	选择资源包的使用时长，支持按月、按年购买。
生效时间	• 支付完成后立即生效，即购买成功后，优先从资源包中抵扣用量。 • 指定生效时间：设置指定生效的具体时间，例如2023/07/11 10:30:00。 **说明** 资源包生效时间非整点时，例如2023/07/11 10:30:00开始生效，开始抵扣时间为下一个整点2023/07/11 11:00:00。
定向使用	• 所有企业项目均可使用。 • 限定企业项目使用套餐包，选择特定企业项目。 **说明** 如果您没有开通企业管理服务，将无法看到企业项目选项。开通方法请参见**如何开通企业项目**。

步骤4 设置完成后，单击“加入清单”。

步骤5 确认清单信息无误后，单击“立即购买”。

步骤6 在购买详情页面，根据业务需要调整购买数量购买时长，单击“去支付”。

说明

单次订单中资源包的购买数量总和不超过5000。

步骤7 在购买云日志服务页面选择支付方式，单击“确认付款”，完成后，即可单击“返回云日志服务控制台”。

步骤8 在资源包卡片上方，单击“查看已购买的资源包”，进入资源包页面查看已购买资源包信息。详细操作请参考**资源包**。

----结束

3 日志管理

3.1 日志管理概述

云日志服务LTS是以日志组和日志流为基本单位进行日志管理。使用云日志服务LTS之前，请先创建日志组和日志流。创建日志组后，可以在该日志组下方创建多个日志流，方便对日志做进一步分类管理。创建日志流后，您可以将日志数据采集保存到日志流上，通过日志流对日志数据进行搜索分析、日志告警、日志转储、可视化展示、日志加工等。

为了快速了解并使用云日志服务LTS，建议您按照如下步骤进行操作：

1. 创建日志组，请参考**管理日志组**。
2. 创建日志流，请参考**管理日志流**。
3. 支持多账号日志汇聚多个账号的日志流、日志组集中管理。请参考**设置多账号日志汇聚**。
4. 在日志管理首页查看资源统计、我的收藏/我的收藏（本地缓存）、最近访问等信息。请参考**查看日志管理**。

3.2 管理日志组

日志组（LogGroup）是云日志服务进行日志管理的基本单位，用于对日志流进行分类，一个日志组下面可以创建多个日志流。日志组本身不存储任何日志数据，仅方便您管理日志流，每个账号下可以创建100个日志组。

一个日志组通常对应公司内的某一个项目/业务，建议将某个项目/业务下的多个应用/服务的日志流归属到同一个日志组下。当公司有多个项目时，具体的项目人员只需要查看所属项目对应的日志组下的日志流即可，其它项目的日志流不会对其产生干扰。

LTS支持按照业务需求对不同的日志组添加对应的标签，方便运维人员管理业务。

前提条件

如果您使用华为账号创建的IAM用户进行操作，IAM用户需要具备足够的权限才能使用云日志服务。具体操作请参见**授权IAM用户使用云日志服务LTS**。

创建日志组

步骤1 登录**云日志服务控制台**。

步骤2 进入“日志管理”页面，单击“创建日志组”。

步骤3 在“创建日志组”页面中，参考**表3-1**填写日志组相关信息。

表 3-1 日志组参数说明

参数	说明
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。
企业项目	选择业务需要的企业项目，也可单击“查看企业项目”，在企业项目管理页面查看全部企业项目。 企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。 **说明** • 企业项目需要开通后才能使用，请参考**如何开通企业项目**。 • 支持将该企业项目资源迁出，详细请参考**迁出企业项目资源**。
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。 **说明** • 目前白名单用户的日志存储时间支持1095天，如有需要，请提工单申请。详细操作请参考**提交工单**。 • 创建日志组免费，使用阶段按照日志量收费，详细请参考**价格计算器**。

参数	说明
标签	按照业务需求对不同的日志组添加对应的标签。单击“添加标签”，分别填写标签键key和标签值value，开启应用到日志流。 ● 如需添加多个标签可重复该步骤，最多支持添加20个标签。 ● 如需删除标签可单击标签操作列的“删除”。 ● 标签键长度不能超过128个字符；标签值长度不能超过255个字符。 ● 标签键名称不可重复。 ● 如果配置转储时使用了该标签，删除标签后，请同步修改转储配置信息。 **说明** 若您的组织已经设定云日志服务的相关标签策略，则需按照标签策略规则为日志组、日志流、日志接入、主机组添加标签。标签如果不符合标签策略的规则，则可能会导致日志组、日志流、日志接入、主机组创建失败，请联系组织管理员了解标签策略详情。标签策略详细介绍请参考**标签策略概述**，标签管理详细介绍请参考**标签管理**。
备注	自定义填写备注信息，字符长度0-1024个字符。

步骤4 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。

- 在日志组列表中，可以查看日志组名称、标签、日志流数量等信息。
- 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。

----结束

修改日志组

日志组创建完成后，如果您需要修改日志组名称、日志存储时间、标签等信息，参考如下操作：

步骤1 在日志组列表中，单击待修改日志组操作列下的“修改”。

步骤2 在弹出的修改日志组页面中 ，修改日志组名称、日志存储时间、标签等信息。

步骤3 完成后，单击“确定”。

步骤4 修改成功后，鼠标悬浮在日志组名称上，显示修改后日志组名称和日志组原始名称。

----结束

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。**删除日志组会导致用户日志相关业务异常，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。

步骤1 在日志组列表中，单击待删除日志组操作列下的“删除”。

步骤2 在弹出框中输入“DELETE”后，单击“确定”，完成日志组删除。

图 3-1 删除日志组

----结束

搜索日志组/日志流

在日志组列表中，支持通过如下筛选条件进行搜索：

- 日志组/日志流
- 日志组原始名称/日志流原始名称
- 日志组名称/ID
- 日志流名称/ID
- 日志组标签
- 备注

其他操作

- 在日志组列表中，单击目标日志组操作列的“更多 > 详情”，可查看该日志组名称、日志组ID、创建时间等详情。
- 需要先开启“ICAgent诊断开关”，请参考**设置ICAgent日志采集开关**。单击目标日志组操作列下的“更多 > ICAgent采集诊断”，可查看该日志组的ICAgent异常监控、ICAgent整体状态和ICAgent采集监控。
- 单击搜索框旁边的 ，下载当前展示日志组的所有信息到本地查看。

3.3 管理日志流

云日志服务是以日志流（LogStream）作为日志管理维度。日志采集后，以日志流为单位，将不同类型的日志分类存储在不同的日志流上，方便对日志进一步分类管理。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。例如，您可以将操作日志、访问日志等接入不同的日志流，查询日志时可以进入对应的日志流快速查看日志。支持按照业务需求对不同的日志流添加对应的标签，方便运维人员管理业务。

1个日志组中最多可以创建100个日志流，如果无法创建日志流，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

步骤1 登录**云日志服务控制台**。

步骤2 单击日志组名称对应的 。

步骤3 单击“创建日志流”，在创建日志流页面，参考**表3-2**填写日志流相关信息。

说明

若您的组织已经设定云日志服务的相关标签策略，则需按照标签策略规则为日志组、日志流、日志接入、主机组添加标签。标签如果不符合标签策略的规则，则可能会导致日志组、日志流、日志接入、主机组创建失败，请联系组织管理员了解标签策略详情。标签策略详细介绍请参考**标签策略概述**，标签管理详细介绍请参考**标签管理**。

表 3-2 日志流参数说明

参数	说明
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。
企业项目	选择业务需要的企业项目，默认为default。也可单击“查看企业项目”，在企业项目管理页面查看全部企业项目。 **说明** • 企业项目需要开通后才能使用，请参考**如何开通企业项目**。 • 支持将该企业项目资源迁出，详细请参考**迁出企业项目资源**。
日志存储	若关闭日志存储，则无法开启日志存储时间。 • 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。 • 关闭“日志存储”：日志不会存储到LTS，可节约索引流量和存储费用，只能使用日志生成指标、转储功能，不能使用日志搜索分析、告警、消费加工等其他功能。
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”：日志的存储时间使用日志流设置的日志存储时间。 • 关闭日志流的“日志存储时间”：日志的存储时间使用日志组设置的日志存储时间。

参数	说明
标签	按照业务需求对不同的日志流添加对应的标签，单击“添加标签”，分别填写标签键key和标签值value。 **说明** • 如需添加多个标签可重复该步骤，最多支持添加20个标签。 • 如需删除标签可单击标签操作列的“删除”。 • 标签键长度不能超过128个字符；标签值长度不能超过255个字符。 • 标签键名称不可重复。 • 如果配置转储时使用了该标签，删除标签后，请同步修改转储配置信息。
匿名写入	匿名写入默认关闭，适用于安卓/IOS/小程序/浏览器端上报日志才能使用匿名写入，需要**提交工单**开通白名单。 打开匿名写入则表示该日志流打开匿名写入权限，不会经过有效鉴权，可能产生脏数据。
备注	自定义填写备注信息，字符长度0-1024个字符。

步骤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。

说明

- 支持查看日志流计费状态，日志计费请参考**价格计算器**。
- 按日志流维度上报话单功能目前在友好用户内测中，您可以**提交工单**申请开通。

----结束

修改日志流

日志流默认的存储时间和日志组保持一致。

步骤1 在日志流列表中，单击待修改日志流操作列的“修改”。

步骤2 在弹出框中，支持修改日志流名称、日志存储时间、标签等信息。

说明

- 关闭开关：日志流会使用日志组配置的日志存储时间。
- 打开开关：使用日志流配置的日志存储时间。
- 超出存储时间的日志将会被自动删除，您可以按需将日志数据转储至OBS桶中进行长期存储。
- 目前仅支持白名单用户**提交工单**申请开通日志存储时间为1095天，但是存量Region需要根据底层资源评估是否支持1095天。

步骤3 单击“确定”。

步骤4 修改完成后，鼠标悬浮在日志流名称上，显示修改后日志流名称和日志流原始名称。

----结束

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。**删除日志流会导致用户日志相关业务异常，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。

步骤1 在日志流列表中，单击待删除日志流操作列的“删除”。

步骤2 在弹出框中输入“DELETE”后，单击“确定”，完成日志流删除。

图 3-2 删除日志流

----结束

其他操作

- **收藏日志流**

  单击日志流中操作列“更多 > 编辑收藏”，收藏日志流，即可在我的收藏/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“更多 > 详情”，可查看日志流详情。包括日志流名称、日志流ID、创建时间等信息。

- 采集诊断：需要先开启“ICAgent诊断开关”，请参考**设置ICAgent日志采集开关**。单击目标日志流操作列“更多 > ICAgent采集诊断”，可查看该日志流的ICAgent异常监控、ICAgent整体状态和ICAgent采集监控。

3.4 查看日志管理

在日志管理首页提供资源统计、日志应用、我的收藏/我的收藏（本地缓存）、最近访问、告警统计、最新告警、功能上线公告等信息的展示。

资源统计

在日志资源统计页面，支持查看资源统计、资源详情。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，统计日志资源的数据量仅供参考。

步骤1 登录**云日志服务控制台**。

步骤2 在日志总览下方，单击资源统计旁边的“相关明细”，进入日志资源统计详情页面。

步骤3 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，您可以根据业务需要选择时间范围。

时间范围有三种方式，分别是相对时间、整点时间和自定义。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：表示查询指定时间范围的日志数据。

步骤4 在资源统计下方，查看资源统计数据：

- 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-标准型日志流：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，在日志写入数据库时一次性收取流量费用。
- 标准存储量：日志标准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。

  说明

  标准存储量统计是指在选定时间范围内最新的存储总量。
- 原始日志流量：原始日志数据的大小。
- 基础转储流量：开启日志转储计费功能后，才会显示基础转储流量。日志转储不需要字段映射，转储算力消耗少，例如转储OBS/DMS/DIS。
- 高级转储流量：开启日志转储计费功能后，才会显示高级转储流量。日志转储需要字段映射，转储算力消耗较多，例如转储DWS/DLI。

步骤5 在资源详情下方，查看Top100的日志组资源统计和Top100的日志流资源统计。根据选择的时间范围，支持表格或柱状图展示每日标准存储量（GB）、每日索引流量-标准型日志流（GB）、每日读写流量（GB）、每日基础转储流量 (GB)、每日高级转储流量(GB)的数据。

- 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  ，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。

----结束

告警统计和最新告警

在日志总览下方，支持查看告警统计和最新告警。

- 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。
- 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 ··· 。

日志应用

在日志管理页面的日志总览下方，支持多种日志应用，即LTS提供开箱即用的日志仪表盘模板，用户接入即可进行日志的快速分析，主要有如下几个应用：

- ELB日志中心：支持ELB日志接入LTS和ELB仪表盘模板。
- APIG日志中心：支持APIG日志接入LTS和APIG仪表盘模板。详情请参考**APIG仪表盘模板**。
- VPC日志流中心：支持VPC日志接入LTS和VPC仪表盘模板。详情请参考**VPC仪表盘模板**。
- CFW日志中心：支持CFW日志接入LTS和CFW仪表盘模板。详情请参考**CFW仪表盘模板**。
- CTS日志中心：支持CTS日志接入LTS，暂不支持CTS仪表盘模板，支持CTS接入LTS。详情请参考**云审计服务CTS接入LTS**。
- 多账号日志汇聚中心：支持您将多个账号下的日志流复制到指定的账号中，实现多账号日志的集中存储和分析。详细请参考**设置多账号日志汇聚**。

日志组列表

在日志组列表下方，展示日志组和日志流信息，更多信息请参考**管理日志组**、**管理日志流**。

公告

公告是对新功能的介绍，展示云日志服务功能的最新动态。

如需查看更多功能介绍，您可以单击**更多**。

我的收藏/我的收藏（本地缓存）

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

- **我的收藏**：将日志流保存至数据库中，默认为关闭状态。当您的账号开通写权限时，可显示该功能和我的收藏（本地缓存）。
- **我的收藏（本地缓存）**：将日志流保存至浏览器本地缓存，默认为关闭状态。可写用户和只读用户支持显示我的收藏（本地缓存）。

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

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

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

步骤1 在日志管理页面的日志组列表下方，单击日志组lts-test对应的 ，选择待收藏的日志流。

步骤2 单击日志流操作列的“更多 > 编辑收藏”，选择收藏方式，单击“确定”，即可收藏日志流。

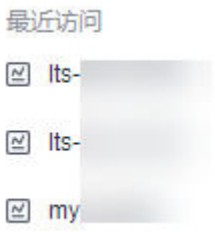
步骤3 收藏成功后，在右侧我的收藏/我的收藏（本地缓存）展示框中，即可展示您收藏的日志流信息。

----结束

最近访问

最近访问展示最近访问的日志流。最近访问最多可显示3条日志流访问记录。

图 3-3 最近访问



FAQ

FAQ（常见问题）展示经常被询问的问题。如需查看更多FAQ，您可以单击**更多**。

视频介绍

通过视频介绍云日志服务的功能、ECS文本日志接入LTS、CCE应用日志接入LTS、安装ICAgent。

3.5 设置多账号日志汇聚

多账号日志汇聚中心支持您将多个账号下的日志流复制到指定的账号中，实现多账号日志的集中存储和分析，满足安全合规、集中分析等不同场景下的诉求。

> **说明**
>
> 目前此功能支持中国-香港、亚太-曼谷、亚太-新加坡、亚太-雅加达、华南-广州、拉美-圣保罗一、华北-北京四、西南-贵阳一、拉美-圣地亚哥、非洲-开罗，其他局点需要提交工单申请才能使用。详细操作请参考**提交工单**。

背景信息

- 集团公司经常采用多账号解决方案（LandingZone），不同的业务部门使用不同的账号，实现权限、资源等的隔离，提高账号的安全性。
- 集团公司的安全合规部门有统一收集日志的诉求，期望将不同账号下各个业务部门的关键日志集中存储和分析，汇聚到一个日志账号中，用于应对不同国家和地区的安全合规审计要求。
- 集团公司的运营部门也可能出于运营分析的诉求，期望将不同账号下各个业务部门的关键日志集中存储和分析，汇聚到一个日志账号中，方便后续进行统一的大数据处理和可视化展示。

方案介绍

- 组织（以下简称Organizations）云服务为企业用户提供多账号关系的管理能力。Organizations支持用户将多个华为云账号整合到创建的组织中，并可以集中管理组织下的所有账号。用户可以在组织中设置访问策略，帮助用户更好地满足业务的安全性和合规性需求。
- 云日志服务LTS联合Organizations推出多账号日志汇聚中心，您可以在Organizations使用管理账号指定某个成员账号成为LTS可信服务的委托管理员账号，然后可以在LTS将组织下某个成员账号的日志流复制到管理账号或者委托管理员账号中，实现多账号日志集中汇聚的目的。
- 某个成员账号的源日志组/日志流实际上是被复制一份到管理账号或者委托管理员账号对应的目标日志组/日志流中，因此两个账号间的日志组/日志流之间不会互相干扰，可以在各自账号下独立配置转储、消费、加工等任务。

前提条件

- 已创建组织。更多信息请参考**创建组织**。
- 已设置service.LTS为可信服务。更多信息请参考**启用、禁用可信服务**。
- 赋予管理账号或者委托管理员账号拥有Organizations服务只读权限。关于委托账号的操作请参考**添加、查看和取消委托管理员**。关于授权的操作请联系企业管理员参考**创建IAM用户并授权管理组织**。

设置多账号日志汇聚任务

步骤1 使用管理账号或者委托管理员账号登录管理控制台，选择“云日志服务 LTS”进入日志管理页面。

步骤2 在日志应用下方，单击“多账号日志汇聚中心”。

步骤3 在多账号日志汇聚配置页面，开启日志接收状态，左侧选择某个成员账号，右侧勾选对应的源日志组/日志流，支持自定义目标日志组/日志流的名称。

说明

- 若不需要使用日志汇聚配置功能时，可以关闭日志接收状态，则所有汇聚配置都会失效，源日志流停止汇聚到目标日志流上。
- 支持创建日志流的数量不超过总数量。更多信息请参考**基础资源**限制。

步骤4 设置完成后，单击“确定”，该账号汇聚配置创建中，预计5分钟左右创建完成，请稍后刷新查看配置。

说明

- 目标日志流初始化时默认采用源账号日志流的索引配置和结构化配置，配置成功后，若源账号日志流修改索引/结构化配置则不会同步到目标日志流。
- 删除源账号的日志组/日志流不会对目标账号的日志组/日志流造成影响。
- 取消勾选日志组/日志流并成功下发配置后，该日志组/日志流将不再继续汇聚。

----结束

4 日志接入

4.1 日志接入概述

日志接入是一个关键的过程，它涉及到收集应用程序或服务在执行过程中生成的各种日志信息，如系统运行状态、错误信息和用户操作记录等。这些信息被存储在特定位置，以便于后续的分析和应用，对于系统的运维、故障排查和业务分析都至关重要。

云日志服务提供实时日志接入功能，通过ICAgent插件、云服务接入、自建软件接入、API接入等多种方式将采集到的日志上报到LTS。日志接入LTS后，用户就可以在云日志服务控制台进行一系列操作，例如搜索与分析日志、使用统计图表或仪表盘可视化展示日志统计结果、设置日志告警、设置日志转储等。

说明

日志接入前，需要确认开启ICAgent采集开关，请参考**设置LTS日志采集配额和使用量预警**。

- 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。

数据来源

支持上报到LTS的日志数据来源如下**表4-1**所示。

表 4-1 数据来源

类别	场景	接入方式
应用	程序输出	**CCE接入**
	访问日志	**WAF接入**
OS	Linux	• **安装ICAgent（区域内主机）** • **安装ICAgent（区域外主机）**
	Windows	
	Docker文件	

类别	场景	接入方式
	Docker输出	
数据库	MySQL	• GaussDB for MySQL接入LTS • 云数据库RDS for MySQL接入LTS
	SQL Server	云数据库RDS for SQLServer接入LTS
	PostgreSQL	云数据库RDS for PostgreSQL接入LTS
	云数据库 GaussDB	数据仓库服务GaussDB(DWS)接入LTS
	云数据库 GeminiDB	• 云数据库GeminiDB接入LTS • 云数据库GeminiDB Mongo接入LTS • 云数据库GeminiDB Cassandra接入LTS
标准协议	HTTP轮询	使用KAFKA协议上报日志到LTS
	Syslog	使用KAFKA协议上报日志到LTS
	Kafka	使用KAFKA协议上报日志到LTS
第三方	Logstash	使用KAFKA协议上报日志到LTS
	Flume	使用KAFKA协议上报日志到LTS
	Beats	使用KAFKA协议上报日志到LTS
云日志服务云产品	ECS、CCE等华为云产品日志	使用云服务接入LTS

4.2 使用 ICAgent 插件采集日志

4.2.1 ICAgent 插件采集日志概述

云日志服务LTS支持通过ICAgent采集方式上报日志。在创建日志接入时设置采集配置策略，例如解析规则、白名单规则、黑名单规则、上传原始日志等参数，实现定制化

的采集策略。ICAgent采集配置定义了如何在服务器上采集同类日志并解析、发送到指定的日志流上。

ICAgent 采集原理

云日志服务安装ICAgent后，会对所关联的日志文件进行实时监听。ICAgent侧收到LTS接入页面下发的采集配置后，会定时解析采集配置信息，获取到采集路径后在节点上进行路径匹配，将节点上对应的文件加入监控任务中，通过轮询和inotify感知目标日志文件的变化。

ICAgent侧发现文件变更后，读取文件的内容，分块发送到处理模块，进行单行、多行、结构化、拆分、添加标签等日志处理动作，再将处理好的任务提交到发送任务池后，上报到LTS。

ICAgent 安装说明

如果需要采集主机指标、容器指标、节点日志、容器日志、标准输出日志等，则需要在采集日志的机器上安装ICAgent。

请参考**安装ICAgent（区域内主机）**和**安装ICAgent（区域外主机）**。

说明

- 区域内主机就是主机所在区域和用户登录云日志服务控制台所在的区域相同，例如中国-香港。
- 区域外主机就是主机所在区域和用户登录云日志服务控制台所在区域不同，例如华为云其他区域、第三方都属于区域外主机。

功能优势

- 基于日志文件，无侵入式采集日志。您无需修改应用程序代码，且采集日志不会影响您的应用程序运行。
- 稳定处理日志采集过程中的各种异常。当遇到网络异常、服务端异常等问题时会采用主动重试、本地缓存数据等措施保障数据安全。
- 基于日志服务的集中管理能力。安装ICAgent后，只需要在日志服务上配置主机组、ICAgent采集配置等信息即可。
- 完善的自我保护机制。为保证运行在服务器上的ICAgent，不会明显影响您服务器上其他服务的性能，ICAgent在CPU、内存及网络使用方面都做了严格的限制和保护机制。

ICAgent 结构化解析规则

日志接入前，您需要提前了解ICAgent采集的结构化解析规则，方便快速操作。支持组合解析，一个日志流的每个采集配置可以配置不同的结构化解析规则。详情请参考**ICAgent结构化解析规则说明**。

4.2.2 安装 ICAgent（区域内主机）

区域内主机是指用户登录云日志服务控制台所在Region区内的主机，例如北京四。如果您想使用云日志服务对区域内主机进行日志采集，例如主机指标、容器指标、采集节点日志、采集容器日志、采集标准输出日志等日志，那么您需要在区域内主机上需要安装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。

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 ICAgent 的限制说明

- Linux环境：ICAgent支持的Linux操作系统，请参考**Linux操作系统**。
- Windows环境：仅支持在如下64位系统的Windows环境中安装ICAgent。

```
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
```

说明

Windows环境不支持在云日志服务主机管理界面对ICAgent进行升级和卸载操作。如果需要使用新版本，请先卸载旧版本ICAgent，再安装新版本ICAgent。请在ICAgent安装包解压目录下，双击执行“*ICAgent安装包解压目录*\ICProbeAgent\bin\manual\win\uninstall.bat”脚本，当显示“ICAgent uninstall success”时，表示卸载成功。

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 4-2 安装方式

方式	适用场景
首次安装	该服务器上未安装过ICAgent。 在服务器上执行**ps -aux | grep icagent**命令，查看没有ICAgent进程，则确认没有安装过ICAgent。 • **首次安装（Linux环境）** • **首次安装（Windows环境）**
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。 • **继承安装（Linux环境）** • **继承批量安装（Linux环境）**

首次安装（Linux 环境）

步骤1 ICAgent安装方式选择委托时，需要提前创建IAM委托。

1. 登录统一身份认证服务控制台。
2. 在左侧导航栏单击“委托”，进入委托页面。
3. 单击右上角“创建委托”，具体操作请参考**委托其他云服务管理资源**，创建委托时参数设置要求参考如下。
   a. 委托类型：选择“云服务”。
   b. 云服务：选择“弹性云服务器 ECS 裸金属服务器 BMS”。
   c. 持续时间：选择“永久”。
   d. 授权权限：需要同时添加LTS Administrator和APM Administrator，授权后需等待15-30分钟才可生效。
   e. 权限的作用范围：指定区域项目资源。
4. 委托创建成功后，设置委托生效。
   a. 进入弹性云服务器控制台。
   b. 单击需要安装ICAgent的弹性云服务器名称，进入弹性云服务器参数配置页面。

      说明

      您可以在购买ECS机器时设置委托，请在“购买弹性云服务器”页面，“高级配置”下方的“委托”中选择已创建的委托名称。待剩余参数配置完成后，单击“立刻购买”即可。

   c. 在管理信息下方的“委托”后，单击，选择已创建的委托名称，单击即可生效。更多关于委托的信息，请参见**委托其他账号管理资源**。

步骤2 登录管理控制台，选择“管理与部署 > 云日志服务 LTS”，进入“日志管理”页面。

步骤3 左侧导航栏选择“主机管理 > 主机”，进入“主机”页面。

步骤4 单击右上角“安装ICAgent”。

说明

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 4-3 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。 **说明** • 区域内主机就是主机所在区域和用户登录云日志服务控制台所在的区域相同，例如中国-香港。 • 区域外主机就是主机所在区域和用户登录云日志服务控制台所在区域不同，例如华为云其他区域、第三方都属于区域外主机。	-
安装系统	默认选择Linux。	-

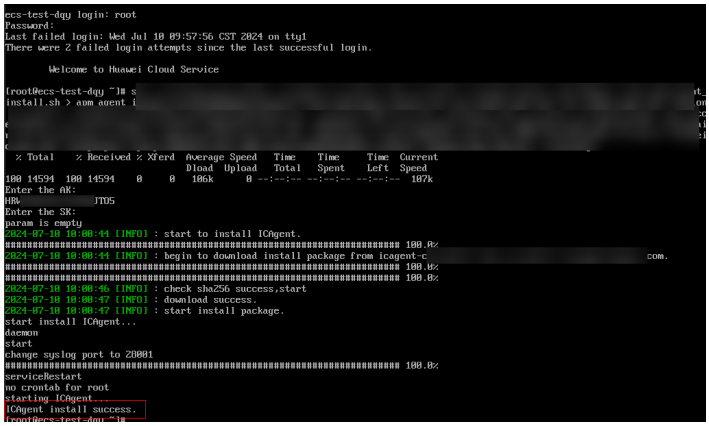
参数	说明	示例
安装方式	• 选择“获取AK/SK凭证”，需要提前获取访问密钥，安装ICAgent时需要输入AK/SK。通过AK识别访问用户的身份，通过SK对请求数据进行签名验证，用于确保请求的机密性、完整性和请求者身份的正确性。请参考**如何获取访问密钥AK/SK**。 **说明** 请确保公共用户账号及其创建的AK/SK不会被删除或禁用。AK/SK被删除，会导致安装的ICAgent无法正常上报数据到LTS。 • 选择“创建IAM委托”，不需要获取访问密钥，通过创建委托ICAgent可以自动获取AK/SK（访问密钥），安装ICAgent时不需要输入AK/SK。请参考**创建IAM委托**。	-

步骤5 在“安装ICAgent”页面，单击“复制命令”，复制ICAgent安装命令。

步骤6 以登录华为云ECS主机为例子进行介绍，请以实际采集主机为准。详细操作请参考**远程登录Linux弹性云服务器（VNC方式）**。

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：
   - “安装方式”选择“获取AK/SK凭证”，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）
   - “安装方式”选择“创建IAM委托”，直接执行ICAgent安装命令进行安装即可。（ICAgent可以自动获取AK/SK，不需要输入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 4-1 安装回显



步骤7 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”。

图 4-2 主机

----结束

首次安装（Windows 环境）

步骤1 单击右上角“安装ICAgent”。

步骤2 主机类型选择“区域内主机”。

步骤3 “安装系统”选择“Windows”。

步骤4 您可以通过单击界面提供的ICAgent压缩包或者下载地址，下载ICAgent安装包到本地。

步骤5 将ICAgent安装包存放到待安装ICAgent服务器的目录（如：C:\ICAgent）并解压。

步骤6 获取AK/SK方法请参考：**如何获取访问密钥AK/SK**。

步骤7 在“安装ICAgent”页面，单击“复制命令”，复制ICAgent安装命令到本地并手动替换AK/SK。

步骤8 打开cmd窗口并进入ICAgent安装包的解压目录，执行ICAgent安装命令进行安装。

当显示“Service icagent installed successfully”时，表示安装成功。

说明

- 如果安装了第三方杀毒软件，需要添加ICAgent为信任程序，否则可能导致ICAgent安装失败。
- 如果需要卸载ICAgent，请在ICAgent安装包解压目录下，双击执行“*ICAgent安装包解压目录*\ICProbeAgent\bin\manual\win\uninstall.bat”脚本，当显示“icagent removed successfully”时，表示卸载成功。

  卸载ICAgent不会删除对应目录的文件，请您根据实际情况自行删除。
- 查询ICAgent的状态，**请在ICAgent安装包解压目录下**，打开cmd窗口，执行命令“sc query icagent”，状态为RUNNING，表示ICAgent正在运行中；提示“The specified service does not exist as an installed service”或者“指定的服务未安装”，表示ICAgent已卸载。
- 卸载后重新安装ICAgent，如果一直处于“pending”状态，可以在任务管理器中结束icagent.exe进程，然后再次重新安装ICAgent。

步骤9 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”。

----结束

继承安装（Linux 环境）

如果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。
   - 如果没有显示“ICAgent install success”代表安装失败，请卸载ICAgent后重新安装。

继承批量安装（Linux 环境）

如果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。

- 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请在服务器上安装python版本后重试。

前提条件

已收集需要安装ICAgent的所有服务器的IP地址、root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地址与服务器root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服务器的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服务器安装操作已完成。

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**查看ICAgent状态**。

4.2.3 安装 ICAgent（区域外主机）

区域外主机指的是华为云非当前Region或非华为云主机，例如自建IDC（Internet Data Center，互联网数据中心）、第三方云厂商或华为云跨Region主机等。如果您想使用云日志服务对区域外主机进行日志采集，那么您需要先保证区域外主机与华为云当前区域LTS网络互通，再在区域外主机上安装ICAgent。ICAgent是云日志服务进行日志采集的工具，运行在待采集日志的主机中。

按照区域外主机上报日志到LTS的网络通路来划分，可分为公网和专线：

- 公网：区域外主机与公网连通，那么区域外主机可以直接通过公网与华为云当前区域LTS进行通信，将日志上报的LTS。但是由于公网的安全性可能较低，因此在实际生产环境中通常选择专线接入方式。

  说明

  区域外主机安装ICAgent选择公网方式时，该局点必须支持公网上报日志。

- 专线：区域外主机与华为云当前区域LTS通过跳板机或VPCEP的方式进行连通，安全性和稳定性都更高。在专线连通场景下，默认区域外主机与当前区域LTS网络不通，安装在区域外主机上的ICAgent无法直接访问华为云管理面上报日志的网段。因此需要配置网络打通方案，使用跳板机或VPCEP的方式去连通LTS后端将数据转发到LTS。
  - 跳板机：跳板机作为数据转发器，将区域外主机ICAgent采集到的数据转发给LTS。当您在进行测试，或者日志流量并不大的情况下，可以使用跳板机的方案。对于大流量日志场景推荐您使用VPCEP。
  - VPCEP：即VPC终端节点，能够提供便捷、安全的通道用于与华为云当前区域LTS进行连接，使VPC中的资源无需弹性公网IP就能够访问终端节点服务。这种方式能够减少数据在公网上传输的风险，提高数据传输的安全性和效率。

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 4-4 安装方式

方式	适用场景
首次安装	该服务器上未安装过ICAgent。

方式	适用场景
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 左侧导航栏选择“主机管理 > 主机”，进入“主机”页面。

步骤2 “主机类型”选择“区域外主机”。

步骤3 “安装系统”选择“Linux”。

步骤4 设置网络连通性方式。区域外主机将日志上报到当前区域LTS的网络通路，建议您优先选择专线，更稳定可靠。

- 若选择“公网”，直接从**步骤6**开始执行。
- 若选择“专线”，需要从**步骤5**开始执行。

步骤5 选择“连通LTS后端方式”，在专线连通场景下，默认区域外主机与当前区域LTS网络不通，安装在区域外主机上的ICAgent无法直接访问华为云管理面上报日志的网段。因此需要配置网络打通方案，使用跳板机或VPCEP的方式去连通LTS。

- 选择“连通LTS后端方式”为“VPCEP”时：

  配置VPCEP域名。请您在华为云网络工程师的协助下，在区域外云上配置VPCEP的DNS域名解析规则，将VPCEP的域名解析到指定IP。配置完成后，在“安装ICAgent”页面根据界面提示复制命令：

  ```
  ping {VPCEP域名}
  ```

  选择一台待采集日志的主机，执行该命令。如果能ping通，表示网络配置连通。跳转到**步骤6**开始执行。

- 选择“连通LTS后端方式”为“跳板机”时：

  a. 创建Linux操作系统的ECS弹性云服务器作为跳板机。

  登录弹性云服务器控制台，创建一个Linux操作系统的ECS。创建ECS的具体步骤，请参考**购买弹性云服务器**。如果您已有符合条件ECS，可直接使用作为跳板机，不需要再次创建。

  说明

  - 推荐CentOS 6.5 64bit及其以上版本的镜像， 最低规格为1vCPUs | 1GB，推荐规格为2vCPUs | 4GB。
  - 如果跳板机使用公网与区域外主机互通，那么需要开通EIP；如果跳板机使用云专线VPC对等连接方式与区域外主机互通，那么不需要开通EIP。
  - 跳板机的区域要与LTS当前Region一致。

  b. 添加跳板机ECS使用的安全组规则，开放入方向对应端口，保证区域外主机到跳板机数据连通。

  i. 登录弹性云服务器控制台，查看弹性云服务器列表，找到作为跳板机的弹性云服务器。

  ii. 单击跳板机名称进入ECS详情，单击安全组名称，进入安全组详情页。

iii. 在该安全组详情页，选择“入方向规则”页签，单击“添加规则 ”。请按照**表4-5**设置端口，更多参数可根据业务网络需求填写。详情请参考**添加安全组规则**。

表 4-5 安全组规则

策略	协议	端口	说明
允许	TCP	8149,8102,8923,30200,30201,80	ICAgent发送数据到跳板机的端口列表，保证非本区域主机到跳板机ECS的数据连通性。

c. 返回弹性云服务器列表，找到**步骤5.a**中作为跳板机的弹性云服务器，可以获取私有IP及弹性公网IP（如跳板机开通EIP，此处会显示弹性公网IP）。

d. 返回云日志服务控制台，在“安装ICAgent”页面中输入获取到的跳板机私有IP，生成跳板机转发命令。

说明

跳板机私有IP是指VPC内网IP。

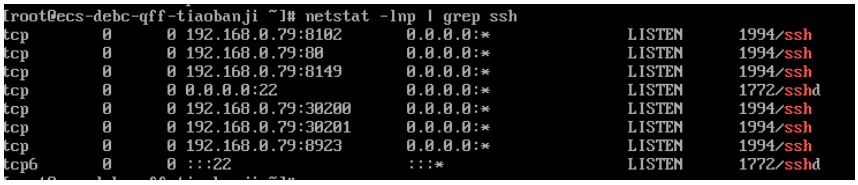
e. 在“安装ICAgent”页面单击“复制命令”，复制SSH Tunnel转发命令。

```
ssh -f -N -L {跳板机私有IP}:8149:{LTS上报IP}:8149 -L {跳板机私有IP}:8102:{LTS上报IP}:8102 -L {跳板机私有IP}:8923:{LTS上报IP}:8923 -L {跳板机私有IP}:30200:{LTS上报IP}:30200 -L {跳板机私有IP}:30201:{LTS上报IP}:30201 -L {跳板机私有IP}:80:icagent-{region}.{obs_domain}:80 {跳板机私有IP}
```

f. 以**root**用户名密码登录跳板机，执行复制的SSH Tunnel转发命令。

g. 执行**netstat -lnp | grep ssh**命令查看对应端口是否被侦听，如果返回结果如**图4-3**所示，说明TCP端口已开通。

图 4-3 TCP 端口验证结果



说明

如果跳板机ECS掉电重启，请重新执行**netstat -lnp | grep ssh**命令。

h. 在“安装ICAgent”页面，填写DC和跳板机连接IP。

- DC：自定义主机节点所属数据中心名称，便于分类查看主机。由数字、大小写字母、中划线、下划线组成，并且最多不超过64个字符。

  跳板机连接IP：如果跳板机使用EIP方式连通区域外主机，此处填写跳板机弹性IP；如果跳板机与区域外主机使用云专线VPC对等连接方式，此处填写跳板机VPC内网IP，即私有IP。弹性IP和私有IP的查看可参考**步骤5.c**。

步骤6 获取AK/SK。详细请参考**如何获取访问密钥AK/SK**。在“安装ICAgent”页面，复制ICAgent安装命令时需要替换AK/SK。

步骤7 使用PuTTY等远程登录工具，以**root**用户登录待安装ICAgent的区域外主机，执行ICAgent安装命令进行安装。

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。

说明

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

首次安装（Windows 环境）

步骤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。

步骤2 左侧导航栏选择“主机管理 > 主机”，进入“主机”页面。

步骤3 “主机类型”选择“区域外主机”。

步骤4 “安装系统”选择“Windows”。

步骤5 设置“网络连通性方式”。区域外主机将日志上报到LTS的网络通路（公网或专线），建议您优先选择专线，更稳定可靠。

- 若选择“公网”，直接从**步骤7**开始执行。
- 若选择“专线”，需要从**步骤6**开始执行。

步骤6 选择“连通LTS后端方式”，在专线连通场景下，默认区域外主机与当前区域LTS网络不通，安装在区域外主机上的ICAgent无法直接访问华为云管理面上报日志的网段。因此需要配置网络打通方案，使用跳板机或VPCEP的方式去连通LTS。

- 选择“连通LTS后端方式”为“VPCEP”时：

  配置VPCEP域名。请您在华为云网络工程师的协助下，在区域外云上配置VPCEP的DNS域名解析规则，将VPCEP的域名解析到指定IP。配置完成后，在“安装ICAgent”页面根据界面提示复制命令：

  ```
  ping {VPCEP域名}
  ```

  选择一台待采集日志的主机，执行该命令。如果能ping通，表示网络配置连通。跳转到**7**开始执行。

- 选择“连通LTS后端方式”为“跳板机”时：

  a. 创建Linux操作系统的ECS弹性云服务器作为跳板机。

  登录弹性云服务器控制台，创建一个Linux操作系统的ECS。创建ECS的具体步骤，请参考**购买弹性云服务器**。如果您已有符合条件ECS，可直接使用作为跳板机，不需要再次创建。

  说明

  - 推荐CentOS 6.5 64bit及其以上版本的镜像， 最低规格为1vCPUs | 1GB，推荐规格为2vCPUs | 4GB。
  - 如果跳板机使用公网与区域外主机互通，那么需要开通EIP；如果跳板机使用云专线VPC对等连接方式与区域外主机互通，那么不需要开通EIP。
  - 跳板机的区域要与LTS当前Region一致。

b. 添加跳板机ECS使用的安全组规则，开放入方向对应端口，保证区域外主机到跳板机数据连通。

i. 登录弹性云服务器控制台，查看弹性云服务器列表，找到作为跳板机的弹性云服务器。

ii. 单击跳板机名称进入ECS详情，单击安全组名称，进入安全组详情页。

iii. 在该安全组详情页，选择“入方向规则”页签，单击“添加规则”。请按照**表4-6**设置端口，更多参数可根据业务网络需求填写。详情请参考**添加安全组规则**。

表 4-6 安全组规则

策略	协议	端口	说明
允许	TCP	8149,8102,8923,30200,30201,80	ICAgent发送数据到跳板机的端口列表，保证非本区域主机到跳板机ECS的数据连通性。

c. 返回弹性云服务器列表，找到**步骤6.a**中作为跳板机的弹性云服务器，可以查看到私有IP及弹性公网IP（如跳板机开通EIP，此处会显示弹性公网IP）。

d. 返回云日志服务控制台，在“安装ICAgent”页面中输入获取到的跳板机私有IP，生成跳板机转发命令。

说明

跳板机私有IP是指VPC内网IP。

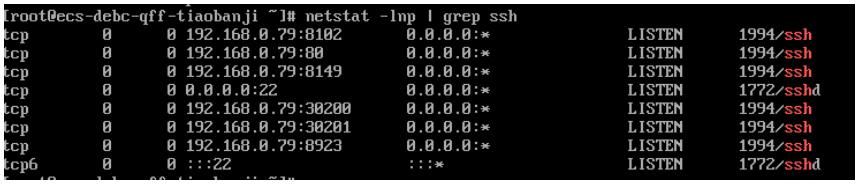
e. 在“安装ICAgent”页面单击“复制命令”，复制SSH Tunnel转发命令。

```
ssh -f -N -L {跳板机私有IP}:8149:{LTS上报IP}:8149 -L {跳板机私有IP}:8102:{LTS上报IP}:8102 -L {跳板机私有IP}:8923:{LTS上报IP}:8923 -L {跳板机私有IP}:30200:{LTS上报IP}:30200 -L {跳板机私有IP}:30201:{LTS上报IP}:30201 -L {跳板机私有IP}:80:icagent-{region}.{obs_domain}:80 {跳板机私有IP}
```

f. 以**root**用户登录跳板机，执行复制的SSH Tunnel转发命令。

g. 执行**netstat -lnp | grep ssh**命令查看对应端口是否被侦听，如果返回结果如**图4-4**所示，说明TCP端口已开通。

图 4-4 TCP 端口验证开通结果



说明

如果跳板机ECS掉电重启，请重新执行如上命令。

步骤7 通过“安装ICAgent”页面提示链接，下载ICAgent安装包。

步骤8 将ICAgent安装包存放到Windows主机目录（如：C:\ICAgent）并解压。

步骤9 获取AK/SK并保存好，复制ICAgent安装命令时需要替换AK/SK。详细请参考**如何获取访问密钥AK/SK**。

如果选择“连通LTS后端方式”为“跳板机”时，那么此处还要填写跳板机连接IP。

跳板机连接IP：如果跳板机使用EIP方式连通区域外主机，此处填写跳板机弹性IP；如果跳板机与区域外主机使用云专线VPC对等连接方式，此处填写跳板机VPC内网IP，即私有IP。弹性IP和私有IP的查看可参考**步骤6.c**。

步骤10 在“安装ICAgent”页面，单击“复制命令”，复制ICAgent安装命令。

步骤11 登录Windows主机，打开cmd窗口并进入ICAgent安装包的解压目录，执行ICAgent安装命令进行安装。

当显示“Service icagent installed successfully”时，表示安装成功。安装成功后，在云日志服务控制台左侧导航栏中选择“主机管理 > 主机”，查看ICAgent状态。

说明

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

创建多台跳板机通过 ELB 进行负载均衡

单跳板机可能发生单点故障带来运维的不稳定性，此时可以创建多个跳板机并通过ELB负载均衡将流量分摊到不同的跳板机上，提高接入的可靠性。

步骤1 创建Linux操作系统的ECS弹性云服务器作为跳板机。

登录弹性云服务器控制台，创建一个Linux操作系统的ECS。创建ECS的具体步骤，请参考**购买弹性云服务器**。如果您已有符合条件ECS，可直接使用作为跳板机，不需要再次创建。

说明

- 推荐CentOS 6.5 64bit及其以上版本的镜像， 最低规格为1vCPUs | 1GB，推荐规格为2vCPUs | 4GB。
- 如果跳板机使用公网与区域外主机互通，那么需要开通EIP；如果跳板机使用云专线VPC对等连接方式与区域外主机互通，那么不需要开通EIP。
- 跳板机的区域要与LTS当前Region一致。

步骤2 添加跳板机ECS使用的安全组规则，开放入方向对应端口，保证区域外主机到跳板机数据连通。

1. 登录弹性云服务器控制台，查看弹性云服务器列表，找到作为跳板机的弹性云服务器。
2. 单击跳板机名称进入ECS详情，单击安全组名称，进入安全组详情页。
3. 在该安全组详情页，选择“入方向规则”页签，单击“添加规则 ”。请按照**表4-7**设置端口，更多参数可根据业务网络需求填写。详情请参考**添加安全组规则**。

表 4-7 安全组规则

策略	协议	端口	说明
允许	TCP	8149,8102,8923,30200,30201,80	ICAgent发送数据到跳板机的端口列表，保证非本区域主机到跳板机ECS的数据连通性。

步骤3 返回弹性云服务器列表，找到**步骤1**中作为跳板机的弹性云服务器，可以查看到私有IP及弹性IP（如跳板机开通EIP，此处会显示弹性IP）。

步骤4 登录云日志服务控制台，在左侧导航栏选择“主机管理 ”，单击“安装ICAgent”，在“安装ICAgent”页面中输入跳板机私有IP，生成跳板机转发命令。

说明

跳板机私有IP是指VPC内网IP。

步骤5 在“安装ICAgent”页面单击“复制命令”，复制SSH Tunnel转发命令。

```
ssh -f -N -L {跳板机私有IP}:8149:{LTS上报IP}:8149 -L {跳板机私有IP}:8102:{LTS上报IP}:8102 -L {跳板机私有IP}:8923:{LTS上报IP}:8923 -L {跳板机私有IP}:30200:{LTS上报IP}:30200 -L {跳板机私有IP}:30201:{LTS上报IP}:30201 -L {跳板机私有IP}:80:icagent-{region}.{obs_domain}:80 {跳板机私有IP}
```

步骤6 以**root**用户登录跳板机，执行复制的SSH Tunnel转发命令。

步骤7 重复以上步骤创建多个跳板机，并且将多个跳板机放入同一个VPC中。即在创建弹性云服务器，进行网络配置时，选择同一个虚拟私有云。

步骤8 登录弹性负载均衡控制台，创建弹性负载均衡ELB。具体请参见**创建弹性负载均衡**，在创建时需注意以下几点。

1. 创建ELB，在网络配置时，选择与跳板机ECS相同的VPC。
2. 新建弹性公网IP，ELB的弹性公网IP将作为跳板机连接IP。
3. 带宽根据业务量申请，并进行适配。

步骤9 分别为TCP的端口30200、30201、8149、8923、8102、80添加监听器。具体请参见**添加TCP监听器**。

步骤10 创建一个后端服务器组，并将所有的跳板机放置在同一个后端服务器组，具体请参见**添加后端云服务器**。

步骤11 返回云日志服务控制台，在“安装ICAgent”页面，将ELB的弹性公网IP填写到“跳板机连接IP”中，复制安装命令，在对应区域外主机上执行即可。

----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。
- 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。

3. 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。

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。

- 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请在服务器上安装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、root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root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”，查看主机的安装状态，详细请参考**查看ICAgent状态**。

4.2.4 管理 ICAgent

ICAgent安装成功后，支持**升级ICAgent**、**卸载ICAgent**、**查看ICAgent状态**、**查看ICAgent版本说明**。

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。

如果需要升级Windows环境中的ICAgent，请先卸载旧版本ICAgent，再安装新版本ICAgent即可。

步骤1 登录管理控制台，选择“管理与部署 > 云日志服务 LTS”，进入“日志管理”页面。

步骤2 左侧导航栏选择“主机管理 > 主机”，进入“主机”页面。

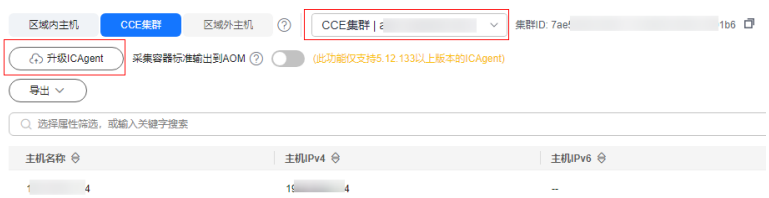
步骤3 选择“区域内主机”或“区域外主机”，当系统提示您有新的ICAgent版本时，在主机列表中选中一个或多个待升级ICAgent前的复选框，单击“升级ICAgent”。

图 4-5 区域内主机升级 ICAgent

步骤4 选择“CCE集群”，在搜索框中选择待升级ICAgent的集群，单击“升级ICAgent”。

- 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。

图 4-6 CCE 集群升级 ICAgent



步骤5 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。

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）。

----结束

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

云日志服务主机管理界面，仅支持卸载安装在Linux环境中的ICAgent，如果需要卸载安装Windows环境中的ICAgent，请在ICAgent安装包解压目录下，双击执行“*ICAgent安装包解压目录*\ICProbeAgent\bin\manual\win\uninstall.bat”脚本，当显示“ICAgent uninstall success”时，表示卸载成功。

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。
  a. 左侧导航栏选择“主机管理 > 主机”，进入“主机”页面。
  b. 勾选一个或多个待卸载ICAgent的服务器的复选框，单击“卸载ICAgent”。
  c. 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：此操作适用于未成功安装ICAgent需卸载重装的场景。
  a. 以**root**用户登录需卸载ICAgent的服务器。
  b. 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：此操作适用于正常安装ICAgent后需远程卸载的场景。
  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。
  a. 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
     ```
  b. 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：此操作适用于正常安装ICAgent后需批量卸载的场景。

  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。

  说明

  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。

  a. 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。

  b. 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。

查看 ICAgent 状态

左侧导航栏选择“主机管理 > 主机”，查看目标主机的ICAgent状态。详细请参见**表4-8**。

表 4-8 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。

查看 ICAgent 版本说明

左侧导航栏选择“主机管理 > 主机”，查看目标主机的ICAgent版本。详细请参见**表 4-9**。

表 4-9 ICAgent 版本说明

版本号	说明	发布时间
7.1.17	优化日志采集流程，调整发送块大小。	2025-01-03
7.1.14	• 优化日志采集流程。 • 日志采集时，持久化保存签名信息。	2024-12-25
7.1.12	解决在某些场景下，Go版本引起的定时器泄漏导致CPU升高的问题。	2024-12-15
7.1.6	• 支持日志上报镜像名称。 • 优化采集日志流程。 • 升级ICAgent基础镜像版本。	2024-11-21
7.1.5	解决用户project下所有配置删除或关闭后，仍然继续采集日志的问题。	2024-11-21
7.1.3	优化发送日志时httpclient组件性能。	2024-11-02
7.1.1	优化ICAgent架构，统一AOM1.0和AOM2.0的Agent。	2024-10-26

版本号	说明	发布时间
5.12.233	• 优化容器日志结构化性能。 • 解决CCE场景错误诊断偶现上报失败的问题。 • 解决虚机场景不活跃文件采集失效的问题。	2024-10-17
5.12.232	• 解析标准输出日志用到的json库替换为sonic，降低CPU使用率。 • LTS发送日志出现超时，解决超时问题。	2024-10-14
5.12.231	• 解决以下条件满足的情况下ICAgent重启的问题：标准输出采集到LTS、LTS不配置日志接入规则、CCE创建新容器并打印标准输出日志。 • 解决游标文件中hisfile变成目录的问题。 • 解决增量采集开关不生效的问题。	2024-10-11
5.12.230	• 解决游标定时刷新功能不生效的问题。 • 查找不到绕接文件的情况下，解决base文件绕接后无法重置游标的问题。 • 解决文件签名导致cpu高的问题。	2024-10-09
5.12.224	在ECS升级场景下，若“.bashrc文件中export HISTSIZE=0”大于1条，则清除“.bashrc文件中的export HISTSIZE=0”。	2024-09-27
5.12.218	• ICAgent上报日志支持GBK编码。 • ICAgent上报日志允许文件多次采集。	2024-09-26
5.12.185	• 解决虚机日志配置中黑名单路径不生效问题。 • 优化containerd标准输出日志采集的问题。	2024-05-20
5.12.184	• 解决容器日志采集功能中无法排除绕接文件的问题。 • 节点日志采集功能并发采集协程调整为32个。	2024-05-16
5.12.183	优化containerd节点采集容器标准输出绕接文件的问题。	2024-05-11
5.12.182	解决syslog开关问题。	2024-04-28
5.12.181	• 解决自建k8s icagent认证失败问题。 • 解决日志截断问题。 • 解决日志速率很大的情况下，查找不到绕接文件导致文件漏采的问题。	2024-04-25
5.12.177	解决绕接死循环问题。	2024-03-28
5.12.176	• zip流式解析优化：检查转储文件是否结束。 • 限制podlb每个主机最大连接数。	2024-03-18
5.12.175	解决了结构化日志采集性能瓶颈问题。	2024-03-13

版本号	说明	发布时间
5.12.172	优化支持的绕接方式。	2024-02-28
5.12.171	解决Docker节点标准输出日志Json解析问题（没有去掉转义字符）。	2024-01-31
5.12.170	• 主机日志，容器日志，标准输出日志支持增量采集。 • 解决主机gpu指标挂断问题。	2024-01-29
5.12.166	• 解决标准输出日志采集插件占用内存高问题。 • 解决虚机日志采集插件重复采集绕接文件问题。 • 游标文件中添加日志组和日志流信息。	2023-12-27
5.12.165	从配置文件获取初始agentID，如果不符合校验要求则使用随机生成的uuid。	2023-12-21
5.12.163	支持UniAgent插件化安装ICAgent。	2023-12-13
5.12.159	• 解决标准输出日志采集协程泄露问题。 • 解决标准输出日志采集到AOM后，不支持采集标准输出绕接日志的问题。	2023-11-27
5.12.158	解决关闭指标开关后容器指标内存泄露导致ICAgent重启的问题。	2023-11-08
5.12.157	• CCE接入LTS的容器日志采集：支持Docker驱动Devicemapper。 • 解决虚机日志量大（转储快）ICAgent内存暴涨导致重启问题。	2023-11-06
5.12.156	解决从OBS拉取安装包问题，将http协议改成https。	2023-11-01
5.12.154	支持结构化功能。	2023-10-31
5.12.153	Release7版本。	2023-10-19
5.12.150	• 解决集群name和集群id not-set问题。 • 支持CCE集群1.27版本。	2023-10-17
5.12.149	支持挂载绕接功能。	2023-10-12
5.12.148	修复gpu多卡场景，解决cpu高的问题。	2023-08-30
5.12.147	修复日志转储无法重启、主机gpu指标适配。	2023-08-17
5.12.142	支持CCE集群1.25及以上版本的容器gpu指标采集。	2023-06-13
5.12.139	解决上报LTS日志出现大量TIME_WAIT状态的TCP连接问题。	2023-04-25

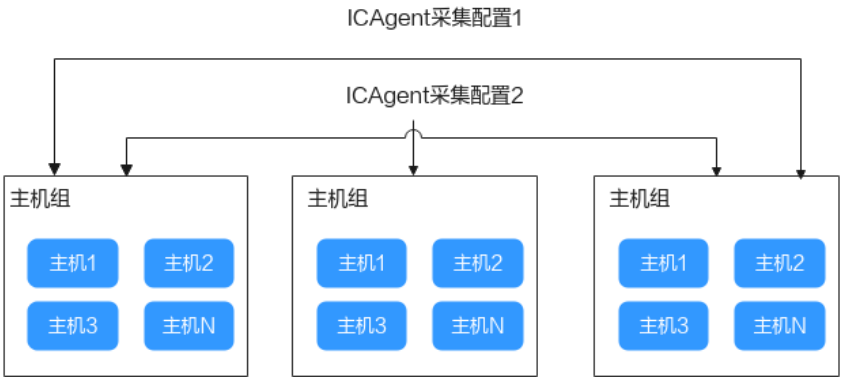
版本号	说明	发布时间
5.12.135	• 解决CPU使用率为0的问题。 • 解决CCE1.23版本集群containerd节点容器网络指标缺失问题。 • 支持采集EulerOS 2.5系统的磁盘分区指标。	2023-02-08
5.12.133	容器的标准输出日志支持多行采集。	2022-12-17
5.12.130	支持将CCE日志直接接入LTS。	2022-11-04
5.12.120	• 增加进程的最大句柄数指标。 • 支持LTS的podlb域名的切换能力。	2022-08-28
5.12.111	新增线程指标、修复“获取lvs磁盘分区指标失败”问题。	2022-06-09
5.12.100	• 上报内存指标增加内存workingset使用量、内存workingset使用率。 • 容器采集支持通过标签区分stderr.log和stdout.log。 • 容器上报增加Pod_ip的tag。 • **配置匹配当前目录文件。	2022-01-15
5.12.98	增加LTS日志黑名单功能，更改容器指标来源为working_set。	2021-09-29
5.12.96	新增云资源发现类型。	2021-09-22
5.12.90	更新gpu指标来源。	2021-07-15
5.12.87	新增磁盘支持类型。	2021-03-30
5.12.75	适配安全容器场景。	2021-03-09

4.2.5 管理 LTS 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，配置日志接入时以主机组为单位下发采集配置，方便您对多台主机日志进行采集。请参考**图4-7**。

- 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。

图 4-7 主机组



支持创建IP类型与自定义标识类型主机组。

- **创建主机组（IP地址）**：创建主机组时，直接勾选同类型主机加入该主机组即可，操作简单。
- **创建主机组（自定义标识）**：创建主机组时，需要在主机组和主机上分别创建标识，若标识存在交集，则会自动将该主机加入主机组内，操作方法复杂。

  说明

  若有以下场景，可以选择使用自定义标识主机组：

  - VPC等自定义网络环境中，可能出现不同服务器IP地址冲突的问题，导致日志服务无法管理ICAgent。使用自定义标识可以避免此类情况的发生。
  - 多台服务器通过同一个自定义标识实现主机组弹性伸缩。您只需为新增的服务器配置相同的自定义标识，日志服务可自动识别，并将其添加至主机组中。

创建主机组（IP 地址）

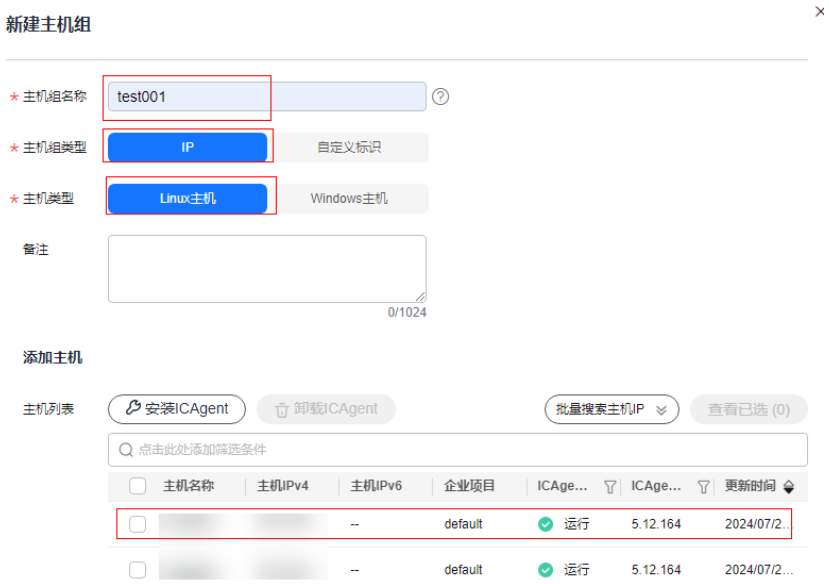
步骤1 登录管理控制台，选择“管理与部署 > 云日志服务 LTS”，进入“日志管理”页面。

步骤2 左侧导航栏选择“主机管理 > 主机组”，进入“主机组”页面。

步骤3 单击右上角“新建主机组”。

步骤4 在弹出的新建主机组页面，输入“主机组名称”，主机组类型选择“IP”，主机类型选择“Linux主机”或“Windows主机”。

图 4-8 创建 IP 地址主机组



步骤5 在列表中勾选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（区域内主机）**或**安装ICAgent（区域外主机）**。

----结束

创建主机组（自定义标识）

选择自定义标识主机组类型时，需要提前规划好需要添加标识的主机。

步骤1 单击右上角“新建主机组”。

步骤2 在弹出的新建主机组页面，输入“主机组名称”，主机组类型选择“自定义标识”，主机类型选择“Linux主机”或“Windows主机”。

步骤3 单击 添加标识 ，输入自定义标识信息。

说明

最多可添加10个自定义标识。

步骤4 单击“确定”，主机组自定义标识创建完成后，请参考5将主机加入自定义标识主机组。

步骤5 执行以下操作创建custom_tag文件，用来保存主机标签。

1. 登录主机执行“cd /opt/cloud”命令，若提示没有/opt/cloud目录，执行“mkdir /opt/cloud/”命令创建/opt/cloud目录。若有/opt/cloud目录，在cloud目录下，执行“mkdir lts”创建lts目录。
2. 继续执行“chmod 750 lts”，修改lts目录权限。
3. 在lts目录下执行“touch custom_tag”，创建custom_tag文件 。

4. 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。
5. 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。
6. 支持以下两种方式将主机加入到自定义标识主机组：

表 4-10 添加方式

类型	方式1（推荐使用）	方式2
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。	- 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。
Windows主机	在主机里***C:|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***C:|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。	- 在主机里***C:|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***C:|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。

----结束

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，具体操作参考如下表4-11。

表 4-11 操作列表

操作	具体步骤
修改主机组名称	1. 在“主机组”页面，默认显示主机组页签。 2. 在主机组列表中，单击待修改的主机组所在行的操作列修改按钮。 3. 在弹出的修改主机组页面，修改主机组名称、自定义标识等信息。 4. 单击“确定”，完成主机名称修改。
添加主机	**方式一：** 1. 在主机组列表，单击待修改的主机组类型为IP的主机组所在行前的 。 2. 在主机页签，单击“添加主机”。 3. 在弹出的添加主机页面，主机列表中显示该主机组所选主机类型下所有未选主机，选择需要加入该主机组的主机。 ● 可以通过主机名称或主机IP对列表进行过滤，也可以单击 批量搜索主机IP ，并在弹出的搜索框中输入多个主机IP，进行批量搜索。 ● 当列表中没有所需主机时，单击“安装ICAgent”，在弹出的页面安装指引完成主机安装，具体操作可参见安装ICAgent。 4. 单击“确定”。 **方式二：** 1. 选择“主机管理 > 主机”页面。 2. 在主机列表中勾选需要添加的主机，单击“添加到主机组”。 3. 在弹出的添加到主机组页面，勾选目标主机组。 4. 单击“确定”，完成主机的添加。
移除主机	1. 在主机组列表，单击待修改的主机组所在行前的 。 2. 在主机页签，单击待移除主机所在行操作列的“移除”。 3. 在弹出的移除主机页面，单击“确定”，将该主机移除。 **说明** 自定义标识主机组下的主机不支持该操作。

操作	具体步骤
取消部署	1. 在主机组列表，单击待修改的主机组所在行前的 。 2. 在主机页签，单击待移除主机所在行操作列的“取消部署”。 3. 在弹出的取消部署页面，单击“确定”，将该主机ICAgent卸载并移除。 **说明** • 自定义标识主机组下的主机不支持该操作。 • 主机取消部署后，其他主机组下的该主机也会被移除。
批量移除	1. 在主机组列表，单击待修改的主机组所在行前的 。 2. 在主机页签，勾选待移除的主机，单击“批量移除”。 3. 单击“确定”。
新增关联配置	1. 在主机组列表，单击待修改的主机组所在行前的 。 2. 默认显示主机页签，单击“相关接入配置”，切换至相关接入配置页签。 3. 单击“新增关联配置”。 4. 在弹出的新增关联配置页面，勾选需要关联的接入配置。 5. 单击“确定”，配置完成后会将所选的接入配置显示在列表中。
解除关联	1. 在相关接入配置页签，单击待解除配置所在行操作列的“解除关联”。 2. 单击“确定”，解除该主机组与该接入配置的关联。
批量解除关联	1. 在相关接入配置页签，勾选待解除的配置，单击“批量解除关联”。 2. 单击“确定”，解除该主机组与所勾选的接入配置的关联。
复制主机组ID	鼠标悬浮在主机组名称上，支持复制主机组ID。
导出主机信息	1. 在“主机”页面的区域内主机、CCE集群或区域外主机下方，勾选需要导出的主机。 2. 单击“导出”，即可将主机信息导出到本地进行查看。

删除主机组

步骤1 左侧导航栏选择“主机管理 > 主机组”，进入“主机组”页面。

步骤2 删除单个主机组。

1. 单击待删除的主机组所在行的操作列删除图标。
2. 在弹出的“删除主机组”页面，单击“确定”，删除该主机组。

步骤3 批量删除主机组。

1. 批量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“删除主机组”页面，单击“确定”，删除所勾选的主机组。

----结束

4.2.6 裸金属服务 BMS 文本日志接入 LTS

裸金属服务器（Bare Metal Server）是一款兼具虚拟机弹性和物理机性能的计算类服务，为您和您的企业提供专属的云上物理服务器，为核心数据库、关键应用系统、高性能计算、大数据等业务提供卓越的计算性能以及数据安全。

当您选择了裸金属服务BMS接入方式时，云日志服务可以将BMS待采集日志的路径配置到日志流中，ICAgent按照日志采集规则采集日志，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查看和分析日志，可以确保服务器的稳定运行和信息安全。

您可以按照如下步骤完成接入配置。

1. **步骤1：选择日志流**
2. **步骤2：选择主机组（可选）**
3. **步骤3：采集配置**
4. **步骤4：索引配置**
5. **步骤5：完成接入配置**

若需要采集多个场景的日志，您可以选择**批量设置多个接入配置**的方式，同时设置多个接入配置。

前提条件

已**安装ICAgent**并**添加至主机组**。开启“ICAgent诊断开关”用于查看ICAgent异常监控、ICAgent整体状态和ICAgent采集监控，请参考**设置ICAgent日志采集开关**。

步骤 1：选择日志流

1. 登录**云日志服务控制台**。
2. 在左侧导航栏中，选择“接入 > 接入中心”，单击“裸金属服务 BMS - 文本日志”。

   或在左侧导航栏中，选择“接入 > 接入管理 > 接入日志”，单击“裸金属服务 BMS - 文本日志”。

   或在左侧导航栏中，选择“日志管理”，单击目标日志流的名称进入日志详情页面。单击右上角  ，在弹出页面中，选择“日志接入”页签，单击“接入日志”，在弹出页面中，单击“裸金属服务 BMS - 文本日志”。
3. 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。详细请参考**管理日志组**。
4. 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。详细请参考**管理日志流**。
5. 单击“下一步：选择主机组（可选）”。

步骤 2：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**管理LTS主机组**。

   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 > 接入管理”页面，单击操作列的“修改”，进入接入配置页面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 3：采集配置

选择主机组信息后，采集配置的具体配置如下：

说明

- 请注意您的敏感信息是否在收集范围内。
- 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。
- LTS暂不支持采集PostgreSQL（数据库）实例的日志。

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。

   若需要复用其他已创建好的采集配置信息，单击输入框后面的“导入其他配置”，在导入其他配置页面勾选已创建好的配置，单击“确定”，即可直接复用该采集配置信息，后面的步骤可以不用设置了。

   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。采集路径设置规则参考如下：

   - **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/a.log
     /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

- 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。
- 添加自定义绕接规则，ICAgent目前是通过文件名规则来判断是否为绕接文件，如果您的绕接规则不符合内置类型时，可以通过单击“添加自定义绕接规则”来进行匹配，避免重复采集和绕接时的日志丢失。

  内置类型为{basename}{连接符}{绕接标识}.后缀，{basename}.{后缀}{连接符}{绕接标识}。其中连接符为-._绕接标识为非字母符号，后缀为字母。

  自定义绕接规则为{basename}+绕接文件的特征正则表达式组成匹配规则。例如您的日志文件名称为test.out.log，绕接后的文件名为test.2024-01-01.0.out.log，test.2024-01-01.1.out.log，因此在路径配置时，采集路径为/opt/*.log，绕接规则为{basename}\.\d{4}-\d{2}-\d{2}\.\d{1}.out.log

3. 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。该功能依赖ICAgent版本，详见**查看ICAgent版本说明**。

   关闭“允许文件多次采集”后，采集路径不能重复配置，即同一主机下的同一日志文件，即使跨日志流，也只能配置一次。

4. 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。

   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。
- 已经加了黑名单的日志，新建日志接入也无法采集黑名单里的日志，除非在设置采集黑名单下方删除采集路径，才能重新采集。
- 过滤指定的目录时，可以过滤掉该目录下的所有文件，但是不能过滤该目录下文件夹里的日志文件。

5. 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 4-12 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（信息）、warning（警告）、error（错误）、critical（严重）和verbose（详细）。根据Windows事件等级过滤采集。仅支持Windows Vista及以上的操作系统。

6. 开启结构化解析配置，详细操作请参考**ICAgent结构化解析规则说明**。

   支持组合解析，一个日志流的每个采集配置可以配置不同的结构化解析规则。

   若已经配置了云端结构化解析，请先删除云端结构化解析后再配置ICAgent结构化解析。

图 4-9 ICAgent 结构化解析配置

7. 其他配置。

表 4-13 其他配置

名称	说明
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。
日志拆分	• 开启日志拆分，支持自定义设置日志拆分大小，设置范围为500KB-1024KB。日志拆分大小为500KB，即单条日志超过500KB会被拆分为多条采集。例如：日志大小为600KB，被拆分为2条日志采集，第一条500KB，第二条100KB。仅支持单行日志，不支持多行日志。 • 不开启日志拆分，单条日志大小限制不超过500KB，超过限制部分会被截断丢弃。
采集二进制文件	云日志服务支持采集二进制文件。 您可以通过命令（*file -i 文件名*）查看文件类型，如果包含charset=binary，那么该日志文件就是二进制文件。 当日志的文件类型为二进制时，开启采集二进制文件按钮，则对接入的二进制文件日志进行采集，但仅支持UTF8编码的字符串，非UFT8编码的字符在LTS控制台页面会显示乱码。 当日志的文件类型为二进制时，未开启采集二进制文件按钮，则对接入的二进制文件日志停止采集，开启后即可进行采集。
日志文件编码	日志文件编码支持UTF-8、GBK（暂不支持Windows场景）。 UTF-8编码是一种变长编码方式，用于表示Unicode字符集。GBK全称《汉字内码扩展规范》，中文计算机编码的一种，是ASCII码和GB2312编码的扩展。
采集策略	采集策略支持增量或全量。 • 增量采集：ICAgent采集新文件时，从文件的末尾开始读。 • 全量采集：ICAgent采集新文件时，从文件的开头开始读。
自定义元数据	• 关闭“自定义元数据”，使用ICAgent系统默认配置的字段上报到LTS，不需要用户配置且ICAgent系统不支持配置。 • 开启“自定义元数据”，根据用户选择的内置字段和自定义键值增加字段上报到LTS。 系统内置字段：勾选需要设置的内置字段。 自定义键值对：单击“添加”，输入键值key和键值Value。

8. 参考**表4-14**配置日志格式、日志时间。

表 4-14 日志采集信息

名称	说明
日志格式	● 单行日志：采集的日志文件中，如果您希望每一行日志在LTS界面中都显示为一条单独的日志数据，则选择单行日志。 ● 多行日志：采集的日志中包含像java异常的日志，如果您希望多行异常的日志显示为一条日志，正常的日志每一行都显示为一条单独的日志数据，则选择多行日志，方便您查看日志并且定位问题。
日志时间	系统时间：表示系统当前时间，默认为日志采集时间，每条日志的行首显示日志的采集时间。 **说明** ● 日志采集时间：ICAgent采集日志，并且发送到云日志服务的时间。 ● 日志打印时间：系统产生并打印日志的时间。ICAgent采集日志并发送日志到云日志平台的频率为1秒钟。 ● 采集日志时间限制：系统时间的前后24小时内。
	时间通配符：用日志打印时间来标识一条日志数据，通过时间通配符来匹配日志，每条日志的行首显示日志的打印时间。 ● 如果日志中的时间格式为：2019-01-01 23:59:59.011，时间通配符应该填写为：YYYY-MM-DD hh:mm:ss.SSS。 ● 如果日志中的时间格式为：19-1-1 23:59:59.011，时间通配符应该填写为：YY-M-D hh:mm:ss.SSS。 **说明** 如果日志中不存在年份信息，则云日志会自动补齐年份数据为当前年份数据。 填写示例： YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond（999） hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)
分行模式	日志格式选择多行日志时，需要选择分行模式，分行模式选择“日志时间”时，是以时间通配符来划分多行日志；当选择“正则模式”时，则以正则表达式划分多行日志。
正则表达式	此配置是用来标识一条日志数据的正则表达式。日志格式选择“多行日志”格式后且“分行模式”已选择“正则模式”后需要设置。

> **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**。

9. 单击“下一步：索引配置”。

步骤 4：索引配置

1. 索引配置（可选项），具体请参考**设置LTS日志索引配置**。
2. 单击“提交”。

步骤 5：完成接入配置

接入成功后会生成一条接入配置信息。

- 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。
- 单击接入配置操作列的“修改”重新修改接入配置信息。
- 单击接入配置操作列的“标签管理”即可添加标签。
- 单击接入配置操作列的“更多 > 复制”复制一条新的接入配置信息。
- 单击接入配置操作列的“更多 > 删除”即可删除接入配置信息。

> **说明**
>
> 删除接入配置后会导致日志无法正常采集，可能会影响用户日志相关业务异常，且删除后无法恢复，请谨慎操作。

- 若不需要采集日志，关闭接入配置状态列的开关  。若需要重新采集日志，需要重新开启接入配置状态列的开关  。

> **说明**
>
> 关闭接入配置后会导致日志无法正常采集，可能会影响用户日志相关业务异常，请谨慎操作。

- 单击接入配置操作列的“更多 > 采集诊断”，可查看ICAgent异常监控、ICAgent整体状态和ICAgent采集监控。

批量设置多个接入配置

支持同时批量设置多个接入配置，操作简单，不用重复配置即可快速完成多个场景的接入配置。

步骤1 在“接入管理”页面，单击“批量接入”，进入配置详情页面，请参考**表4-15**。

表 4-15 批量接入设置

类型	操作	说明
基本配置	接入类型	选择裸金属服务BMS-文本日志。

类型	操作	说明
	接入配置数量	在输入框填写接入配置数量，单击“添加接入配置”。 在接入配置下方默认已有1个接入配置，最多支持再添加99个数量，因此支持同时添加100个接入配置。
接入配置	接入列表	1. 左侧显示接入配置的信息，最多支持添加99个配置。 2. 右侧显示配置接入的内容，详细请参考**步骤3：采集配置**进行设置。 3. 一个接入配置设置完成后，单击“应用于其他接入配置”即可将该接入配置复制到其他接入配置。

步骤2 单击“参数检查”，检查成功后，单击“提交”，批量接入设置完成。

例如添加了4个接入配置，批量创建成功后，在“接入管理”下方，就会显示4条接入配置数量。

步骤3 （可选）支持对接入配置任务进行以下操作：

- 勾选多个已创建成功的接入配置，单击“批量编辑”进入配置详情页面，通过选择不同接入类型，修改对应的接入配置信息。
- 勾选多个已创建成功的接入配置，单击启用或禁用按钮。接入配置状态禁用后不会继续采集日志。
- 勾选多个已创建成功的接入配置，单击删除按钮即可批量删除接入配置。

----结束

4.2.7 云容器引擎 CCE 应用日志接入 LTS

云容器引擎（Cloud Container Engine，简称CCE）提供高度可扩展的、高性能的企业级Kubernetes集群。借助云容器引擎，您可以轻松部署、管理和扩展容器化应用程序。

云容器引擎CCE应用日志接入LTS后，在LTS控制台可以对收集到的日志进行统一管理和分析，还可以将日志报表进行可视化展示，从而更好地监控和管理容器化应用的运行状态，帮助用户能够快速发现容器的问题，提高容器的性能和可靠性。

您可以按照如下步骤完成接入配置。

1. **步骤1：选择日志流**
2. **步骤2：检查依赖项**
3. **步骤3：选择主机组（可选）**
4. **步骤4：采集配置**
5. **步骤5：索引配置**
6. **步骤6：完成接入配置**

若需要采集多个场景的日志，您可以选择**批量设置多个接入配置**的方式，同时设置多个接入配置。

前提条件

- CCE集群已安装ICAgent并且已创建相关节点自定义标识的主机组（如果不满足，配置CCE接入LTS时会自动检查修复）。

  说明

  - 首次使用AOM2.0的用户，请参考**开通AOM2.0**授权使用AOM2.0，进入AOM2.0控制台后，请参考**云服务授权**授予云日志服务 (LTS)、云容器引擎 (CCE)等云服务数据的访问权限。
  - 在“主机”页面，选择“CCE集群”，在搜索框选择目标集群，单击“升级ICAgent”，详细操作请参考**升级ICAgent**。
- 已关闭采集容器标准输出到AOM的开关。
- 开启“ICAgent诊断开关”用于查看ICAgent异常监控、ICAgent整体状态和ICAgent采集监控，请参考**设置ICAgent日志采集开关**。

使用限制

- 支持容器引擎为Docker的CCE集群节点。详情请查看**云容器引擎（CCE）**。
- 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）。
- 支持CCE Turbo集群（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。

步骤 1：选择日志流

1. 登录**云日志服务控制台**。
2. 在左侧导航栏中，选择“接入 > 接入中心”，单击“云容器引擎 CCE-应用日志”进行CCE接入配置。

   或在左侧导航栏中，选择“接入 > 接入管理 > 接入日志”，单击“云容器引擎 CCE-应用日志”进行CCE接入配置。

   或在左侧导航栏中，选择“日志管理”，单击目标日志流的名称进入日志详情页面。单击右上角  ，在弹出页面中，选择“日志接入”页签，单击“接入日志”，在弹出页面中，单击“云容器引擎 CCE-应用日志”进行CCE接入配置。
3. 采集方式：采集到集中日志流和采集到自定义日志流，您可以根据实际情况选择采集方式，推荐您使用采集到集中日志流。

表 4-16 采集方式

采集方式	说明
采集到集中日志流	• 优点：在CCE界面可以根据命名空间、工作负载、容器名称直接查看对应的日志，将所有日志采集到一个日志流。 • 缺点： 不同的工作负载的日志结构不一样，采集到一个日志流后无法配置结构化解析，无法使用SQL可视化分析。 单个日志流的写入速率上限是100MB/S，集中采集对于大流量场景有性能瓶颈。
采集到自定义日志流	• 优点： 不同的工作负载的日志结构不一样，采集到不同日志流后可以配置结构化解析，使用SQL可视化分析。 多个日志流的写入速率累加起来可以线性扩增，自定义采集对于大流量场景没有性能瓶颈。 • 缺点：在CCE界面无法根据命名空间、工作负载、容器名称直接查看对应的日志。

- 若选择“采集到集中日志流”，请执行如下操作步骤：

  集中采集日志到一个固定的日志流。CCE集群默认的采集日志流分别为标准输出/错误stdout-{ClusterID}、节点文件hostfile-{ClusterID}、K8S事件:event-{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集群下可以创建的采集日志流为标准输出/错误stdout-{ClusterID}、节点文件hostfile-{ClusterID}、容器文件containerfile-{ClusterID}）和K8s事件event-{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。

  i. 单击“CCE集群”后的目标框，在下拉列表中选择具体的集群。

  ii. 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。

  iii. 单击“下一步：检查依赖项”。

- 若选择“采集到自定义日志流”，请执行如下操作步骤：

  i. 单击“CCE集群”后的目标框，在下拉列表中选择具体的集群。

  ii. 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。

iii. 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。

iv. 单击“下一步：检查依赖项”。

步骤 2：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. 存在自定义标识符为**k8s-log-集群ID**的主机组。
3. 存在名为**k8s-log-集群ID**的日志组。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。
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。

步骤 3：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。

   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。
   - 对于自定义CCE集群的主机组，自定义标识的格式需要是**k8s-log-集群ID**。
   - 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 > 接入管理”页面，单击操作列的“修改”，进入接入配置页面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 4：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. **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。
2. **数据源配置**：选择数据源类型，进行对应的数据源配置，详细请参考**表4-17**。

   说明

   对挂载的网盘或者共享存储，配置多台机器同时采集，会导致日志重复。

表 4-17 数据源配置参数

类型	参数配置
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。 ● 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。 ● 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。 ● 开启采集容器标准错误（stderr）后，选择采集目前路径：将标准输出和标准错误采集到不同的文件（stdout.log和stderr.log）、将标准输出和标准错误采集到同一个文件（stdout.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。该功能依赖ICAgent版本，详见**查看ICAgent版本说明**。 关闭“允许文件多次采集”后，采集路径不能重复配置，即同一主机下的同一日志文件，即使跨日志流，也只能配置一次。

类型	参数配置
容器文件路径	采集集群内指定容器内的文件日志。 • 添加采集路径：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，更多示例请参考**路径配置**。 **说明** 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。 • 添加自定义绕接规则，ICAgent目前是通过文件名规则来判断是否为绕接文件，如果您的绕接规则不符合内置类型时，可以通过单击“添加自定义绕接规则”来进行匹配，避免重复采集和绕接时的日志丢失。 **内置类型**为{basename}{连接符}{绕接标识}.后缀，{basename}.{后缀}{连接符}{绕接标识}。其中连接符为**-.**_绕接标识为非字母符号，后缀为字母。 **自定义绕接规则**为{basename}+绕接文件的特征正则表达式组成匹配规则。例如您的日志文件名称为test.out.log，绕接后的文件名为test.2024-01-01.0.out.log，test.2024-01-01.1.out.log，因此在路径配置时，采集路径为/opt/*.log，绕接规则为{basename}\.\d{4}-\d{2}-\d{2}\.\d{1}.out.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。该功能依赖ICAgent版本，详见**查看ICAgent版本说明**。 关闭“允许文件多次采集”后，采集路径不能重复配置，即同一主机下的同一日志文件，即使跨日志流，也只能配置一次。 • 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。

类型	参数配置
节点文件路径	采集集群内指定节点的文件。 • 添加采集路径：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，更多示例请参考**路径配置**。 • 添加自定义绕接规则，ICAgent目前是通过文件名规则来判断是否为绕接文件，如果您的绕接规则不符合内置类型时，可以通过单击“添加自定义绕接规则”来进行匹配，避免重复采集和绕接时的日志丢失。 **内置类型**为{basename}{连接符}{绕接标识}.后缀，{basename}.{后缀}{连接符}{绕接标识}。其中连接符为-._绕接标识为非字母符号，后缀为字母。 **自定义绕接规则**为{basename}+绕接文件的特征正则表达式组成匹配规则。例如您的日志文件名称为test.out.log，绕接后的文件名为test.2024-01-01.0.out.log，test.2024-01-01.1.out.log，因此在路径配置时，采集路径为/opt/*.log，绕接规则为{basename}\.\d{4}-\d{2}-\d{2}\.\d{1}.out.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。该功能依赖ICAgent版本，详见**查看ICAgent版本说明**。 关闭“允许文件多次采集”后，采集路径不能重复配置，即同一主机下的同一日志文件，即使跨日志流，也只能配置一次。 • 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。
K8S事件	采集K8S集群内的事件日志。 K8S事件不能重复配置，即一个K8S集群的K8S事件，只能配置接入到一个日志流。

3. （可选）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，需要设置K8s匹配规则。

说明

填写正则匹配规则后，单击校验按钮，支持校验确保正则表达式的正确性。

表 4-18 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。 **说明** 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。
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。 **说明** 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。

参数名称	参数说明
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。 **说明** 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。
K8s Label白名单	通过K8s Label白名单指定待采集的容器。如果您要设置K8s Label白名单，那么LabelKey必填，LabelValue可选填。 新增多条白名单时，支持选择And或or的关系，即全部满足或满足任意白名单就可以被匹配。 **说明** 若LabelValue为空，则K8S Label中包含LabelKey的容器都匹配；若LabelValue不为空，则K8S Label中包含LabelKey=LabelValue的容器才匹配；LabelKey需要全匹配，LabelValue支持正则匹配。
K8s Label黑名单	通过K8s Label黑名单排除不采集的容器。如果您要设置K8s Label黑名单，那么LabelKey必填，LabelValue可选填。 新增多条黑名单时，支持选择And或or的关系，即全部满足或满足任意黑名单就可以被排除。 **说明** 若LabelValue为空，则K8S Label中包含LabelKey的容器都被排除；若LabelValue不为空，则K8S Label中包含LabelKey=LabelValue的容器才会被排除；LabelKey需要全匹配，LabelValue支持正则匹配。
K8s Label日志标签	设置K8s Label日志标签后，日志服务将在日志中新增K8s Label相关字段。 **说明** 设置K8s 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，将在日志中添加内容{app_alias：lts}。
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。 新增多条白名单时，支持选择And或or的关系，即全部满足或满足任意白名单就可以被匹配。 **说明** 若LabelValue为空，则容器 Label中包含LabelKey的容器都匹配；若LabelValue不为空，则容器 Label中包含LabelKey=LabelValue的容器才匹配；LabelKey需要全匹配，LabelValue支持正则匹配。
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。 新增多条黑名单时，支持选择And或or的关系，即全部满足或满足任意黑名单就可以被排除。 **说明** 若LabelValue为空，则容器 Label中包含LabelKey的容器都被排除；若LabelValue不为空，则容器 Label中包含LabelKey=LabelValue的容器才会被排除；LabelKey需要全匹配，LabelValue支持正则匹配。

参数名称	参数说明
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。 **说明** 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。 新增多条白名单时，支持选择And或or的关系，即全部满足或满足任意白名单就可以被匹配。 **说明** 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；LabelKey需要全匹配，LabelValue支持正则匹配。
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。 新增多条黑名单时，支持选择And或or的关系，即全部满足或满足任意黑名单就可以被排除。 **说明** 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；LabelKey需要全匹配，LabelValue支持正则匹配。
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。 **说明** 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. 开启结构化解析配置，详细操作请参考**ICAgent结构化解析规则说明**。

   支持组合解析，一个日志流的每个采集配置可以配置不同的结构化解析规则。

   若已经配置了云端结构化解析，请先删除云端结构化解析后再配置ICAgent结构化解析。

图 4-10 ICAgent 结构化解析配置

5. 其他配置。

表 4-19 其他配置

名称	说明
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。
日志拆分	• 开启日志拆分，支持自定义设置日志拆分大小，设置范围为500KB-1024KB。日志拆分大小为500KB，即单条日志超过500KB会被拆分为多条采集。例如：日志大小为600KB，被拆分为2条日志采集，第一条500KB，第二条100KB。仅支持单行日志，不支持多行日志。 • 不开启日志拆分，单条日志大小限制不超过500KB，超过限制部分会被截断丢弃。
采集二进制文件	云日志服务支持采集二进制文件。 您可以通过命令（*file -i 文件名*）查看文件类型，如果包含charset=binary，那么该日志文件就是二进制文件。 当日志的文件类型为二进制时，开启采集二进制文件按钮，则对接入的二进制文件日志进行采集，但仅支持UTF8编码的字符串，非UFT8编码的字符在LTS控制台页面会显示乱码。 当日志的文件类型为二进制时，未开启采集二进制文件按钮，则对接入的二进制文件日志停止采集，开启后即可进行采集。
日志文件编码	日志文件编码支持UTF-8、GBK（暂不支持Windows场景）。 UTF-8编码是一种变长编码方式，用于表示Unicode字符集。GBK全称《汉字内码扩展规范》，中文计算机编码的一种，是ASCII码和GB2312编码的扩展。
采集策略	采集策略支持增量或全量。 • 增量采集：ICAgent采集新文件时，从文件的末尾开始读。 • 全量采集：ICAgent采集新文件时，从文件的开头开始读。
自定义元数据	• 关闭“自定义元数据”，使用ICAgent系统默认配置的字段上报到LTS，不需要用户配置且ICAgent系统不支持配置。 • 开启“自定义元数据”，根据用户选择的内置字段和自定义键值增加字段上报到LTS。 系统内置字段：勾选需要设置的内置字段。 自定义键值对：单击“添加”，输入键值key和键值Value。

6. 参考**表4-20**配置日志格式、日志时间。

说明

不再推荐使用以下功能，建议使用**结构化解析配置**。

表 4-20 日志采集信息

名称	说明
日志格式	• 单行日志：采集的日志文件中，如果您希望每一行日志在LTS界面中都显示为一条单独的日志数据，则选择单行日志。 • 多行日志：采集的日志中包含像java异常的日志，如果您希望多行异常的日志显示为一条日志，正常的日志每一行都显示为一条单独的日志数据，则选择多行日志，方便您查看日志并且定位问题。
日志时间	系统时间：表示系统当前时间，默认为日志采集时间，每条日志的行首显示日志的采集时间。 **说明** • 日志采集时间：ICAgent采集日志，并且发送到云日志服务的时间。 • 日志打印时间：系统产生并打印日志的时间。ICAgent采集日志并发送日志到云日志平台的频率为1秒钟。 • 采集日志时间限制：系统时间的前后24小时内。
	时间通配符：用日志打印时间来标识一条日志数据，通过时间通配符来匹配日志，每条日志的行首显示日志的打印时间。 • 如果日志中的时间格式为：2019-01-01 23:59:59.011，时间通配符应该填写为：YYYY-MM-DD hh:mm:ss.SSS。 • 如果日志中的时间格式为：19-1-1 23:59:59.011，时间通配符应该填写为：YY-M-D hh:mm:ss.SSS。 **说明** 如果日志中不存在年份信息，则云日志会自动补齐年份数据为当前年份数据。 填写示例： YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)
分行模式	日志格式选择多行日志时，需要选择分行模式，分行模式选择“日志时间”时，是以时间通配符来划分多行日志；当选择“正则模式”时，则以正则表达式划分多行日志。
正则表达式	此配置是用来标识一条日志数据的正则表达式。日志格式选择“多行日志”格式后且“分行模式”已选择“正则模式”后需要设置。

> **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**。

7. 单击“下一步：索引配置”。

步骤 5：索引配置

1. 索引配置（可选项），具体请参考**设置LTS日志索引配置**。
2. 单击“提交”。

步骤 6：完成接入配置

接入成功后会生成一条接入配置信息。

- 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。
- 单击接入配置操作列的“修改”重新修改接入配置信息。
- 单击接入配置操作列的“标签管理”即可添加标签。
- 单击接入配置操作列的“更多 > 复制”复制一条新的接入配置信息。
- 单击接入配置操作列的“更多 > 删除”即可删除接入配置信息。

> **说明**
>
> 删除接入配置后会导致日志无法正常采集，可能会影响用户日志相关业务异常，且删除后无法恢复，请谨慎操作。

- 若不需要采集日志，关闭接入配置状态列的开关  。若需要重新采集日志，需要重新开启接入配置状态列的开关  。

> **说明**
>
> 关闭接入配置后会导致日志无法正常采集，可能会影响用户日志相关业务异常，请谨慎操作。

- 单击接入配置操作列的“更多 > 采集诊断”，可查看ICAgent异常监控、ICAgent整体状态和ICAgent采集监控。

批量设置多个接入配置

支持同时批量设置多个接入配置，操作简单，不用重复配置即可快速完成多个场景的接入配置

步骤1 在“接入管理”页面，单击“批量接入”，进入配置详情页面，请参考**表4-21**。

表 4-21 批量接入设置

类型	操作	说明
基本配置	接入类型	选择云容器引擎 CCE-应用日志。

类型	操作	说明
	接入配置数量	在输入框填写接入配置数量，单击“添加接入配置”。 在接入配置下方默认已有1个接入配置，最多支持再添加99个数量，因此支持同时添加100个接入配置。
接入配置	接入列表	1. 左侧显示接入配置的信息，最多支持添加99个配置。 2. 右侧显示配置接入的内容，详细请参考**步骤4：采集配置**进行设置。 3. 一个接入配置设置完成后，单击“应用于其他接入配置”即可将该接入配置复制到其他接入配置。

步骤2 单击“参数检查”，检查成功后，单击“提交”，批量接入设置完成。

例如添加了4个接入配置，批量创建成功后，在“接入管理”下方，就会显示4条接入配置数量。

步骤3 （可选）支持对接入配置任务进行以下操作：

- 勾选多个已创建成功的接入配置，单击“批量编辑”进入配置详情页面，通过选择不同接入类型，修改对应的接入配置信息。
- 勾选多个已创建成功的接入配置，单击启用或禁用按钮。接入配置状态禁用后不会继续采集日志。
- 勾选多个已创建成功的接入配置，单击删除按钮即可批量删除接入配置。

----结束

4.2.8 云主机 ECS 文本日志接入 LTS

弹性云服务器（Elastic Cloud Server）是一种可随时自助获取、可弹性伸缩的云服务器，可帮助您打造可靠、安全、灵活、高效的应用环境，确保服务持久稳定运行，提升运维效率。

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按照日志采集规则采集日志，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查看和分析日志，可以确保服务器的稳定运行和信息安全。

您可以按照如下步骤完成接入配置。

1. **步骤1：选择日志流**
2. **步骤2：选择主机组（可选）**
3. **步骤3：采集配置**
4. **步骤4：索引配置**
5. **步骤5：完成接入配置**

若需要采集多个场景的日志，您可以选择**批量设置多个接入配置**的方式，同时设置多个接入配置。

前提条件

已**安装ICAgent**并**添加至主机组**。开启“ICAgent诊断开关”用于查看ICAgent异常监控、ICAgent整体状态和ICAgent采集监控，请参考**设置ICAgent日志采集开关**。

步骤 1：选择日志流

1. 登录**云日志服务控制台**。
2. 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ECS接入配置。

   或在左侧导航栏中，选择“接入 > 接入管理 > 接入日志”，单击“云主机 ECS-文本日志”进行ECS接入配置。

   或在左侧导航栏中，选择“日志管理”，单击目标日志流的名称进入日志详情页面。单击右上角  ，在弹出页面中，选择“日志接入”页签，单击“接入日志”，在弹出页面中，单击“云主机 ECS-文本日志”进行ECS接入配置。
3. 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。详细请参考**管理日志组**。
4. 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。详细请参考**管理日志流**。
5. 单击“下一步：选择主机组”。

步骤 2：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**管理LTS主机组**。

   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 > 接入管理”页面，单击操作列的“修改”，进入接入配置页面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 3：采集配置

选择主机组信息后，采集配置的具体配置如下：

说明

- 请注意您的敏感信息是否在收集范围内。
- 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。
- 配置日志接入时可以同时选择多个主机组，同一个主机组又可以添加多个主机。所以不同主机的路径可以通过主机组来控制采集配置接入。
- 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。
- LTS暂不支持采集PostgreSQL（数据库）实例的日志。

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。

若需要复用其他已创建好的采集配置信息，单击输入框后面的“导入其他配置”，在导入其他配置页面勾选已创建好的配置，单击“确定”，即可直接复用该采集配置信息，后面的步骤可以不用设置了。

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。采集路径设置规则参考如下：
   - **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/a.log
     /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
   - 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。
   - 添加自定义绕接规则，ICAgent目前是通过文件名规则来判断是否为绕接文件，如果您的绕接规则不符合内置类型时，可以通过单击“添加自定义绕接规则”来进行匹配，避免重复采集和绕接时的日志丢失。

内置类型为{basename}{连接符}{绕接标识}.后缀，{basename}.{后缀}{连接符}{绕接标识}。其中连接符为-._绕接标识为非字母符号，后缀为字母。

自定义绕接规则为{basename}+绕接文件的特征正则表达式组成匹配规则。例如您的日志文件名称为test.out.log，绕接后的文件名为test.2024-01-01.0.out.log，test.2024-01-01.1.out.log，因此在路径配置时，采集路径为/opt/*.log，绕接规则为{basename}\.\d{4}-\d{2}-\d{2}\.\d{1}.out.log

3. 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。该功能依赖ICAgent版本，详见**查看ICAgent版本说明**。

   关闭“允许文件多次采集”后，采集路径不能重复配置，即同一主机下的同一日志文件，即使跨日志流，也只能配置一次。

4. 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。

   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。
   - 已经加了黑名单的日志，新建日志接入也无法采集黑名单里的日志，除非在设置采集黑名单下方删除采集路径，才能重新采集。
   - 过滤指定的目录时，可以过滤掉该目录下的所有文件，但是不能过滤该目录下文件夹里的日志文件。

5. 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 4-22 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（信息）、warning（警告）、error（错误）、critical（严重）和verbose（详细）。根据Windows事件等级过滤采集。仅支持Windows Vista及以上的操作系统。

6. 开启结构化解析配置，详细操作请参考**ICAgent结构化解析规则说明**。

   支持组合解析，一个日志流的每个采集配置可以配置不同的结构化解析规则。

   若已经配置了云端结构化解析，请先删除云端结构化解析后再配置ICAgent结构化解析。

图 4-11 ICAgent 结构化解析配置

7. 其他配置。

表 4-23 其他配置

名称	说明
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。
日志拆分	• 开启日志拆分，支持自定义设置日志拆分大小，设置范围为500KB-1024KB。日志拆分大小为500KB，即单条日志超过500KB会被拆分为多条采集。例如：日志大小为600KB，被拆分为2条日志采集，第一条500KB，第二条100KB。仅支持单行日志，不支持多行日志。 • 不开启日志拆分，单条日志大小限制不超过500KB，超过限制部分会被截断丢弃。
采集二进制文件	云日志服务支持采集二进制文件。 您可以通过命令（*file -i 文件名*）查看文件类型，如果包含charset=binary，那么该日志文件就是二进制文件。 当日志的文件类型为二进制时，开启采集二进制文件按钮，则对接入的二进制文件日志进行采集，但仅支持UTF8编码的字符串，非UFT8编码的字符在LTS控制台页面会显示乱码。 当日志的文件类型为二进制时，未开启采集二进制文件按钮，则对接入的二进制文件日志停止采集，开启后即可进行采集。
日志文件编码	日志文件编码支持UTF-8、GBK（暂不支持Windows场景）。 UTF-8编码是一种变长编码方式，用于表示Unicode字符集。GBK全称《汉字内码扩展规范》，中文计算机编码的一种，是ASCII码和GB2312编码的扩展。
采集策略	采集策略支持增量或全量。 • 增量采集：ICAgent采集新文件时，从文件的末尾开始读。 • 全量采集：ICAgent采集新文件时，从文件的开头开始读。

名称	说明
自定义元数据	• 关闭“自定义元数据”，使用ICAgent系统默认配置的字段上报到LTS，不需要用户配置且ICAgent系统不支持配置。 • 开启“自定义元数据”，根据用户选择的内置字段和自定义键值增加字段上报到LTS。 系统内置字段：勾选需要设置的内置字段。 自定义键值对：单击“添加”，输入键值key和键值Value。

8. 参考**表4-24**配置日志格式、日志时间。

表 4-24 日志采集信息

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

名称	说明
	时间通配符：用日志打印时间来标识一条日志数据，通过时间通配符来匹配日志，每条日志的行首显示日志的打印时间。 ● 如果日志中的时间格式为：2019-01-01 23:59:59.011，时间通配符应该填写为：YYYY-MM-DD hh:mm:ss.SSS。 ● 如果日志中的时间格式为：19-1-1 23:59:59.011，时间通配符应该填写为：YY-M-D hh:mm:ss.SSS。 **说明** 如果日志中不存在年份信息，则云日志会自动补齐年份数据为当前年份数据。 填写示例： YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)
分行模式	日志格式选择多行日志时，需要选择分行模式，分行模式选择“日志时间”时，是以时间通配符来划分多行日志；当选择“正则模式”时，则以正则表达式划分多行日志。
正则表达式	此配置是用来标识一条日志数据的正则表达式。日志格式选择“多行日志”格式后且“分行模式”已选择“正则模式”后需要设置。

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**。

9. 单击“下一步：索引配置”。

步骤 4：索引配置

1. 索引配置（可选项），具体请参考**设置LTS日志索引配置**。
2. 单击“提交”。

步骤 5：完成接入配置

接入成功后会生成一条接入配置信息。

- 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。
- 单击接入配置操作列的“修改”重新修改接入配置信息。

- 单击接入配置操作列的“标签管理”即可添加标签。
- 单击接入配置操作列的“更多 > 复制”复制一条新的接入配置信息。
- 单击接入配置操作列的“更多 > 删除”即可删除接入配置信息。

  说明

  删除接入配置后会导致日志无法正常采集，可能会影响用户日志相关业务异常，且删除后无法恢复，请谨慎操作。

- 若不需要采集日志，关闭接入配置状态列的开关  。若需要重新采集日志，需要重新开启接入配置状态列的开关  。

  说明

  关闭接入配置后会导致日志无法正常采集，可能会影响用户日志相关业务异常，请谨慎操作。

- 单击接入配置操作列的“更多 > 采集诊断”，可查看ICAgent异常监控、ICAgent整体状态和ICAgent采集监控。

批量设置多个接入配置

支持同时批量设置多个接入配置，操作简单，不用重复配置即可快速完成多个场景的接入配置。

步骤1 在“接入管理”页面，单击“批量接入”，进入配置详情页面，请参考**表4-25**。

表 4-25 批量接入设置

类型	操作	说明
基本配置	接入类型	选择云主机 ECS-文本日志。
	接入配置数量	在输入框填写接入配置数量，单击“添加接入配置”。 在接入配置下方默认已有1个接入配置，最多支持再添加99个数量，因此支持同时添加100个接入配置。
接入配置	接入列表	1. 左侧显示接入配置的信息，最多支持添加99个配置。 2. 右侧显示配置接入的内容，详细请参考**步骤3：采集配置**进行设置。 3. 一个接入配置设置完成后，单击“应用于其他接入配置”即可将该接入配置复制到其他接入配置。

步骤2 单击“参数检查”，检查成功后，单击“提交”，批量接入设置完成。

例如添加了4个接入配置，批量创建成功后，在“接入管理”下方，就会显示4条接入配置数量。

步骤3 （可选）支持对接入配置任务进行以下操作：

- 勾选多个已创建成功的接入配置，单击“批量编辑”进入配置详情页面，通过选择不同接入类型，修改对应的接入配置信息。

- 勾选多个已创建成功的接入配置，单击启用或禁用按钮。接入配置状态禁用后不会继续采集日志。
- 勾选多个已创建成功的接入配置，单击删除按钮即可批量删除接入配置。

----结束

4.2.9 ServiceStage 容器应用日志接入 LTS

云日志服务（Log Tank Service，简称LTS）用于收集来自ServiceStage容器应用的日志数据，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。

您可以按照如下步骤完成接入配置。

1. **步骤1：选择日志流**
2. **步骤2：检查依赖项**
3. **步骤3：选择主机组（可选）**
4. **步骤4：采集配置**
5. **步骤5：索引配置**
6. **步骤6：完成接入配置**

若需要采集多个场景的日志，您可以选择**批量设置多个接入配置**的方式，同时设置多个接入配置。

说明

目前此功能仅支持白名单用户提交工单申请使用。详细操作请参考**提交工单**。

前提条件

- 已安装ICAgent并添加至主机组。
- 已创建ServiceStage应用。详细操作请参考**创建应用**。
- 已创建ServiceStage环境。详细操作请参考**创建环境**。
- 已创建ServiceStage组件。详细操作请参考**创建组件**。
- 开启“ICAgent诊断开关”用于查看ICAgent异常监控、ICAgent整体状态和ICAgent采集监控，请参考**设置ICAgent日志采集开关**。

使用限制

- 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"
```

步骤 1：选择日志流

1. 登录**云日志服务控制台**。
2. 在左侧导航栏中，选择“接入 > 接入中心”，单击自建软件下的“ServiceStage-容器应用日志”进行ServiceStage接入配置。

   或在左侧导航栏中，选择“接入 > 接入管理 > 接入日志”，单击“ServiceStage-容器应用日志”进行ServiceStage接入配置。

   或在左侧导航栏中，选择“日志管理”，单击目标日志流的名称进入日志详情页面。单击右上角  ，在弹出页面中，选择“日志接入”页签，单击“接入日志”，在弹出页面中，单击自建软件下的“ServiceStage-容器应用日志”进行ServiceStage接入配置。
3. 在选择日志流页面，设置如下参数。
   a. 选择ServiceStage应用、ServiceStage环境。
   b. 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。
   c. 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”。

步骤 2：检查依赖项

1. 系统自动检查是否存在自定义标识符为**k8s-log-应用ID**的主机组。

   如果不符合要求，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**：一键帮您完成内容检查项配置。
   - **重新检查**：重新检查依赖项。
2. 单击“下一步：选择主机组（可选）”。

步骤 3：选择主机组（可选）

1. 在主机组列表中，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。
2. 单击“下一步：采集配置”。

步骤 4：采集配置

在ServiceStage容器应用日志接入时，采集配置的具体配置如下：

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。
2. 数据源配置：选择数据源类型，进行对应的数据源配置。支持的数据源类型有容器标准输出、容器文件路径、节点文件路径和K8S事件。

表 4-26 采集配置参数表

类型	参数配置
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。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。 • 开启采集容器标准错误（stderr）后，选择采集目标路径：将标准输出和标准错误采集到不同的文件（stdout.log和stderr.log）、将标准输出和标准错误采集到同一个文件（stdout.log）。 • 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。 • 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。该功能依赖ICAgent版本，详见**查看ICAgent版本说明**。 关闭“允许文件多次采集”后，采集路径不能重复配置，即同一主机下的同一日志文件，即使跨日志流，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日志。 • 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，详细请参考2。 **说明** 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。 • 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。该功能依赖ICAgent版本，详见**查看ICAgent版本说明**。 关闭“允许文件多次采集”后，采集路径不能重复配置，即同一主机下的同一日志文件，即使跨日志流，也只能配置一次。 • 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	采集集群内指定节点的文件。 • 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。 • 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。该功能依赖ICAgent版本，详见**查看ICAgent版本说明**。 关闭“允许文件多次采集”后，采集路径不能重复配置，即同一主机下的同一日志文件，即使跨日志流，也只能配置一次。 • 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。

类型	参数配置
K8S事件	采集K8S集群内的事件日志。无需设置参数，仅支持icagent 5.12.150及以上版本。 **说明** K8S事件不能重复配置，即一个K8S集群的K8S事件，只能配置接入到一个日志流。

3. 当数据源类型选择**容器标准输出**和**容器文件路径**时，需要设置ServiceStage匹配规则，在下拉框选择对应组件。
4. 开启结构化解析配置，详细操作请参考**ICAgent结构化解析规则说明**。

   支持组合解析，一个日志流的每个采集配置可以配置不同的结构化解析规则。

   若已经配置了云端结构化解析，请先删除云端结构化解析后再配置ICAgent结构化解析。

图 4-12 ICAgent 结构化解析配置

5. 其他配置。

表 4-27 其他配置

名称	说明
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。
日志拆分	• 开启日志拆分，支持自定义设置日志拆分大小，设置范围为500KB-1024KB。日志拆分大小为500KB，即单条日志超过500KB会被拆分为多条采集。例如：日志大小为600KB，被拆分为2条日志采集，第一条500KB，第二条100KB。仅支持单行日志，不支持多行日志。 • 不开启日志拆分，单条日志大小限制不超过500KB，超过限制部分会被截断丢弃。

名称	说明
采集二进制文件	云日志服务支持采集二进制文件。 您可以通过命令（*file -i 文件名*）查看文件类型，如果包含charset=binary，那么该日志文件就是二进制文件。 当日志的文件类型为二进制时，开启采集二进制文件按钮，则对接入的二进制文件日志进行采集，但仅支持UTF8编码的字符串，非UFT8编码的字符在LTS控制台页面会显示乱码。 当日志的文件类型为二进制时，未开启采集二进制文件按钮，则对接入的二进制文件日志停止采集，开启后即可进行采集。
日志文件编码	日志文件编码支持UTF-8、GBK（暂不支持Windows场景）。 UTF-8编码是一种变长编码方式，用于表示Unicode字符集。 GBK全称《汉字内码扩展规范》，中文计算机编码的一种，是ASCII码和GB2312编码的扩展。
采集策略	采集策略支持增量或全量。 ● 增量采集：ICAgent采集新文件时，从文件的末尾开始读。 ● 全量采集：ICAgent采集新文件时，从文件的开头开始读。
自定义元数据	● 关闭“自定义元数据”，使用ICAgent系统默认配置的字段上报到LTS，不需要用户配置且ICAgent系统不支持配置。 ● 开启“自定义元数据”，根据用户选择的内置字段和自定义键值增加字段上报到LTS。 系统内置字段：勾选需要设置的内置字段。 自定义键值对：单击“添加”，输入键值key和键值Value。

6. 参考**表4-28**设置日志格式、日志时间。

表 4-28 日志采集信息

名称	说明
日志格式	● 单行日志：采集的日志文件中，如果您希望每一行日志在LTS界面中都显示为一条单独的日志数据，则选择单行日志。 ● 多行日志：采集的日志中包含像java异常的日志，如果您希望多行异常的日志显示为一条日志，正常的日志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。 **说明** • 日志采集时间：ICAgent采集日志，并且发送到云日志服务的时间。 • 日志打印时间：系统产生并打印日志的时间。ICAgent采集日志并发送日志到云日志平台的频率为1秒钟。 • 采集日志时间限制：系统时间的前后24小时内。
	时间通配符：用日志打印时间来标识一条日志数据，通过时间通配符来匹配日志，每条日志的行首显示日志的打印时间。 • 如果日志中的时间格式为：2019-01-01 23:59:59.011，时间通配符应该填写为：YYYY-MM-DD hh:mm:ss.SSS。 • 如果日志中的时间格式为：19-1-1 23:59:59.011，时间通配符应该填写为：YY-M-D hh:mm:ss.SSS。 **说明** 如果日志中不存在年份信息，则云日志会自动补齐年份数据为当前年份数据。 填写示例： YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)
分行模式	日志格式选择多行日志时，需要选择分行模式，分行模式选择“日志时间”时，是以时间通配符来划分多行日志；当选择“正则模式”时，则以正则表达式划分多行日志。
正则表达式	此配置是用来标识一条日志数据的正则表达式。日志格式选择“多行日志”格式后且“分行模式”已选择“正则模式”后需要设置。

7. 单击“下一步：索引配置”。

步骤 5：索引配置

1. 索引配置（可选项），具体请参考**设置LTS日志索引配置**。
2. 单击“提交”。

步骤 6：完成接入配置

接入成功后会生成一条接入配置信息。

- 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。
- 单击接入配置操作列的“修改”重新修改接入配置信息。
- 单击接入配置操作列的“标签管理”即可添加标签。
- 单击接入配置操作列的“更多 > 复制”复制一条新的接入配置信息。
- 单击接入配置操作列的“更多 > 删除”即可删除接入配置信息。

  说明

  删除接入配置后会导致日志无法正常采集，可能会影响用户日志相关业务异常，且删除后无法恢复，请谨慎操作。

- 若不需要采集日志，关闭接入配置状态列的开关  。若需要重新采集日志，需要重新开启接入配置状态列的开关  。

  说明

  关闭接入配置后会导致日志无法正常采集，可能会影响用户日志相关业务异常，请谨慎操作。

- 单击接入配置操作列的“更多 > 采集诊断”，可查看ICAgent异常监控、ICAgent整体状态和ICAgent采集监控。

批量设置多个接入配置

支持同时批量设置多个接入配置，操作简单，不用重复配置即可快速完成多个场景的接入配置。

步骤1 在“接入管理”页面，单击“批量接入”，进入配置详情页面，请参考**表4-29**。

表 4-29 批量接入设置

类型	操作	说明
基本配置	接入类型	选择ServiceStage-容器应用日志。
	接入配置数量	在输入框填写接入配置数量，单击“添加接入配置”。 在接入配置下方默认已有1个接入配置，最多支持再添加99个数量，因此支持同时添加100个接入配置。
接入配置	接入列表	1. 左侧显示接入配置的信息，最多支持添加99个配置。 2. 右侧显示配置接入的内容，详细请参考**步骤4：采集配置**进行设置。 3. 一个接入配置设置完成后，单击“应用于其他接入配置”即可将该接入配置复制到其他接入配置。

步骤2 单击“参数检查”，检查成功后，单击“提交”，批量接入设置完成。

例如添加了4个接入配置，批量创建成功后，在“接入管理”下方，就会显示4条接入配置数量。

步骤3 （可选）支持对接入配置任务进行以下操作：

- 勾选多个已创建成功的接入配置，单击“批量编辑”进入配置详情页面，通过选择不同接入类型，修改对应的接入配置信息。
- 勾选多个已创建成功的接入配置，单击启用或禁用按钮。接入配置状态禁用后不会继续采集日志。
- 勾选多个已创建成功的接入配置，单击删除按钮即可批量删除接入配置。

----结束

4.2.10 ServiceStage 云主机日志接入 LTS

云日志服务（Log Tank Service，简称LTS）用于收集来自ServiceStage云主机的日志数据，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。

您可以按照如下步骤完成接入配置。

1. **步骤1：选择日志流**
2. **步骤2：选择主机组（可选）**
3. **步骤3：采集配置**
4. **步骤4：索引配置**
5. **步骤5：完成接入配置**

若需要采集多个场景的日志，您可以选择**批量设置多个接入配置**的方式，同时设置多个接入配置。

说明

目前此功能仅支持白名单用户提交工单申请才能使用。详细操作请参考**提交工单**。

前提条件

- 已安装ICAgent并添加至主机组。
- 已创建ServiceStage应用。详细操作请参考**创建应用**。
- 已创建ServiceStage环境。详细操作请参考**创建环境**。
- 已创建ServiceStage组件。详细操作请参考**创建组件**。
- 开启“ICAgent诊断开关”用于查看ICAgent异常监控、ICAgent整体状态和ICAgent采集监控，请参考**设置ICAgent日志采集开关**。

步骤 1：选择日志流

1. 登录**云日志服务控制台**。
2. 在左侧导航栏中，选择“接入 > 接入中心”，单击“ServiceStage-云主机日志”进行ServiceStage接入配置。

   或在左侧导航栏中，选择“接入 > 接入管理 > 接入日志”，单击“ServiceStage-云主机日志”进行ServiceStage接入配置。

   或在左侧导航栏中，选择“日志管理”，单击目标日志流的名称进入日志详情页面。单击右上角  ，在弹出页面中，选择“日志接入”页签，单击“接入日志”，在弹出页面中，单击“ServiceStage-云主机日志”进行ServiceStage接入配置。

3. 在选择日志流页面，设置如下参数。
   a. 选择ServiceStage应用、ServiceStage环境。
   b. 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。
   c. 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：选择主机组（可选）”。

步骤 2：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。

   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 > 接入管理”页面，单击操作列的“修改”，进入接入配置页面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 3：采集配置

采集配置参考如下步骤：

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。
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。采集路径设置规则参考如下：
   - **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/a.log
     /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

– 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。

3. 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。该功能依赖ICAgent版本，详见**查看ICAgent版本说明**。

   关闭“允许文件多次采集”后，采集路径不能重复配置，即同一主机下的同一日志文件，即使跨日志流，也只能配置一次。

4. 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。

5. 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 4-30 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。

6. 设置ServiceStage匹配规则，选择对应组件。

7. 开启结构化解析配置，详细操作请参考**ICAgent结构化解析规则说明**。

   支持组合解析，一个日志流的每个采集配置可以配置不同的结构化解析规则。

   若已经配置了云端结构化解析，请先删除云端结构化解析后再配置ICAgent结构化解析。

图 4-13 ICAgent 结构化解析配置

8. 其他配置。

表 4-31 其他配置

名称	说明
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。
日志拆分	• 开启日志拆分，支持自定义设置日志拆分大小，设置范围为500KB-1024KB。日志拆分大小为500KB，即单条日志超过500KB会被拆分为多条采集。例如：日志大小为600KB，被拆分为2条日志采集，第一条500KB，第二条100KB。仅支持单行日志，不支持多行日志。 • 不开启日志拆分，单条日志大小限制不超过500KB，超过限制部分会被截断丢弃。
采集二进制文件	云日志服务支持采集二进制文件。 您可以通过命令（*file -i 文件名*）查看文件类型，如果包含charset=binary，那么该日志文件就是二进制文件。 当日志的文件类型为二进制时，开启采集二进制文件按钮，则对接入的二进制文件日志进行采集，但仅支持UTF8编码的字符串，非UFT8编码的字符在LTS控制台页面会显示乱码。 当日志的文件类型为二进制时，未开启采集二进制文件按钮，则对接入的二进制文件日志停止采集，开启后即可进行采集。
日志文件编码	日志文件编码支持UTF-8、GBK（暂不支持Windows场景）。 UTF-8编码是一种变长编码方式，用于表示Unicode字符集。GBK全称《汉字内码扩展规范》，中文计算机编码的一种，是ASCII码和GB2312编码的扩展。

名称	说明
采集策略	采集策略支持增量或全量。 ● 增量采集：ICAgent采集新文件时，从文件的末尾开始读。 ● 全量采集：ICAgent采集新文件时，从文件的开头开始读。
自定义元数据	● 关闭“自定义元数据”，使用ICAgent系统默认配置的字段上报到LTS，不需要用户配置且ICAgent系统不支持配置。 ● 开启“自定义元数据”，根据用户选择的内置字段和自定义键值增加字段上报到LTS。 系统内置字段：勾选需要设置的内置字段。 自定义键值对：单击“添加”，输入键值key和键值Value。

9. 参考**表4-32**设置日志格式、日志时间。

表 4-32 日志采集信息

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

名称	说明
	时间通配符：用日志打印时间来标识一条日志数据，通过时间通配符来匹配日志，每条日志的行首显示日志的打印时间。 ● 如果日志中的时间格式为：2019-01-01 23:59:59.011，时间通配符应该填写为：YYYY-MM-DD hh:mm:ss.SSS。 ● 如果日志中的时间格式为：19-1-1 23:59:59.011，时间通配符应该填写为：YY-M-D hh:mm:ss.SSS。 **说明** 如果日志中不存在年份信息，则云日志会自动补齐年份数据为当前年份数据。 填写示例： YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)
分行模式	日志格式选择多行日志时，需要选择分行模式，分行模式选择“日志时间”时，是以时间通配符来划分多行日志；当选择“正则模式”时，则以正则表达式划分多行日志。
正则表达式	此配置是用来标识一条日志数据的正则表达式。日志格式选择“多行日志”格式后且“分行模式”已选择“正则模式”后需要设置。

10. 单击“下一步：索引配置”。

步骤 4：索引配置

1. 索引配置（可选项），具体请参考**设置LTS日志索引配置**。
2. 单击“提交”。

步骤 5：完成接入配置

接入成功后会生成一条接入配置信息。

- 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。
- 单击接入配置操作列的“修改”重新修改接入配置信息。
- 单击接入配置操作列的“标签管理”即可添加标签。
- 单击接入配置操作列的“更多 > 复制”复制一条新的接入配置信息。
- 单击接入配置操作列的“更多 > 删除”即可删除接入配置信息。

说明

删除接入配置后会导致日志无法正常采集，可能会影响用户日志相关业务异常，且删除后无法恢复，请谨慎操作。

- 若不需要采集日志，关闭接入配置状态列的开关  。若需要重新采集日志，需要重新开启接入配置状态列的开关  。

  说明

  关闭接入配置后会导致日志无法正常采集，可能会影响用户日志相关业务异常，请谨慎操作。

- 单击接入配置操作列的“更多 > 采集诊断”，可查看ICAgent异常监控、ICAgent整体状态和ICAgent采集监控。

批量设置多个接入配置

支持同时批量设置多个接入配置，操作简单，不用重复配置即可快速完成多个场景的接入配置。

步骤1 在“接入管理”页面，单击“批量接入”，进入配置详情页面，请参考**表4-33**。

表 4-33 批量接入设置

类型	操作	说明
基本配置	接入类型	选择ServiceStage-云主机日志。
	接入配置数量	在输入框填写接入配置数量，单击“添加接入配置”。 在接入配置下方默认已有1个接入配置，最多支持再添加99个数量，因此支持同时添加100个接入配置。
接入配置	接入列表	1. 左侧显示接入配置的信息，最多支持添加99个配置。 2. 右侧显示配置接入的内容，详细请参考**步骤3：采集配置**进行设置。 3. 一个接入配置设置完成后，单击“应用于其他接入配置”即可将该接入配置复制到其他接入配置。

步骤2 单击“参数检查”，检查成功后，单击“提交”，批量接入设置完成。

例如添加了4个接入配置，批量创建成功后，在“接入管理”下方，就会显示4条接入配置数量。

步骤3 （可选）支持对接入配置任务进行以下操作：

- 勾选多个已创建成功的接入配置，单击“批量编辑”进入配置详情页面，通过选择不同接入类型，修改对应的接入配置信息。
- 勾选多个已创建成功的接入配置，单击启用或禁用按钮。接入配置状态禁用后不会继续采集日志。
- 勾选多个已创建成功的接入配置，单击删除按钮即可批量删除接入配置。

----结束

4.2.11 自建 K8s 应用日志接入 LTS

自建K8s（kubernetes）是开源的一个容器编排引擎，它支持自动化部署、大规模可伸缩、应用容器化管理。将自建K8s集群内服务或集群节点特定路径文件的应用日志上报至LTS后，用户可以对Kubernetes集群内服务日志进行存储和分析。

您可以按照如下步骤完成接入配置。

1. **步骤1：选择日志流**
2. **步骤2：检查依赖项**
3. **步骤3：安装日志采集组件**
4. **步骤4：选择主机组（可选）**
5. **步骤5：采集配置**
6. **步骤6：索引配置**
7. **步骤7：完成接入配置**

若需要采集多个场景的日志，您可以选择**批量设置多个接入配置**的方式，同时设置多个接入配置。

前提条件

- 请确保已在Kubernetes集群中执行安装Helm v3的命令。
- 请确保Kubernetes集群已配置kubectl。
- 开启“ICAgent诊断开关”用于查看ICAgent异常监控、ICAgent整体状态和ICAgent采集监控，请参考**设置ICAgent日志采集开关**。

步骤 1：选择日志流

1. 登录**云日志服务控制台**。
2. 在左侧导航栏中，选择“接入 > 接入中心”，单击“自建k8s - 应用日志”进行自建K8s接入配置。

   或在左侧导航栏中，选择“接入 > 接入管理 > 接入日志”，单击“自建k8s - 应用日志”进行自建K8s接入配置。

   或在左侧导航栏中，选择“日志管理”，单击目标日志流的名称进入日志详情页面。单击右上角  ，在弹出页面中，选择“日志接入”页签，单击“接入日志”，在弹出页面中，单击“自建k8s - 应用日志”进行自建K8s接入配置。
3. 采集方式：采集到集中日志流和采集到自定义日志流，您可以根据实际情况选择采集方式，推荐您使用采集到集中日志流。

表 4-34 采集方式

采集方式	说明
采集到集中日志流	• 优点：相同类型的日志在一个日志流中，方便集中搜索。 • 缺点： 不同的工作负载的日志结构不一样，采集到一个日志流后无法配置结构化解析，无法使用SQL可视化分析。 单个日志流的写入速率上限是100MB/S，集中采集对于大流量场景有性能瓶颈。
采集到自定义日志流	• 优点： 不同的工作负载的日志结构不一样，采集到不同日志流后可以配置结构化解析，使用SQL可视化分析。 多个日志流的写入速率累加起来可以线性扩增，自定义采集对于大流量场景没有性能瓶颈。 • 缺点：日志流数量较多，管理起来相对繁琐。

- **若选择“采集到集中日志流”，请执行如下操作步骤：**

  集中采集日志到一个固定的日志流。kubernetes集群默认的采集日志流分别为标准输出/错误stdout-{ClusterID}、节点文件hostfile-{ClusterID}、容器文件containerfile-{ClusterID}、K8S事件: event-{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kubernetes集群下可以创建的采集日志流为标准输出/错误stdout-{ClusterID}、节点文件hostfile-{ClusterID}、容器文件containerfile-{ClusterID}）和K8s事件event-{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。

  i. 选择采集方式“采集到集中日志流”。
  ii. 输入“集群名称”和“集群ID”。
  iii. 选择“所属日志组”。

  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。

  iv. 单击“下一步：检查依赖项”。

- **若选择“采集到自定义日志流”，请执行如下操作步骤：**

  i. 选择采集方式“采集到自定义日志流”。
  ii. 输入“集群名称”和“集群ID”。
  iii. 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。

iv. 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 4-14 采集到自定义日志流

4. 单击“下一步：检查依赖项”。

步骤 2：检查依赖项

1. 系统自动检查以下三项是否符合要求：
   - 存在自定义标识符为**k8s-log-集群ID**的主机组。
   - 存在名为**k8s-log-集群ID**的日志组。支持修改日志组的日志存储时间和备注。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。
   - 存在系统推荐的集中采集的日志流。支持修改日志流的日志存储时间和备注。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。

   如果以上三项中，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**：一键帮您完成以上三项配置。
   - **重新检查**：重新检查依赖项。
2. 单击“下一步：安装日志采集组件”。

步骤 3：安装日志采集组件

在Kubernetes集群中，选择任意一台主机执行如下操作步骤：

1. 获取ICAgent安装包。
   a. 获取ICAgent安装包（以界面上显示的为准）。
   ```
   wget https://icagent-{regionId}.{obsDomainName}/ICAgent_linux/icagentK8s-5.5.1.2.tar.gz
   ```
   b. 解压ICAgent安装包。
   ```
   tar -xzvf icagentK8s-5.5.1.2.tar.gz
   ```


c. 进入目录。
```
cd icagentK8s
```
d. 生成安装命令：

选择接入日志的**区域名**。

选择接入日志的账号的**项目ID**。

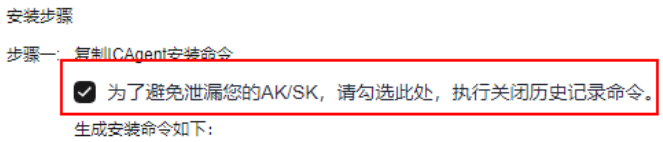
k8s集群所在区域，选择“区域内”。

2. 安装ICAgent。

a. 复制ICAgent安装命令，执行的命令需要填写AK/SK，有两种方式可选择：复制命令时手动替换AK/SK或者直接执行命令时再根据提示替换AK/SK。

为了避免泄漏您的AK/SK，请勾选此处，执行关闭历史记录命令。

图 4-15 安装 ICAgent



b. 使用PuTTY等远程登录工具，以root用户登录待安装主机，执行复制到的命令。

当显示”ICAgent install success”时，表示安装成功，安装成功后，在主机列表下方查看ICAgent状态。

3. 单击“确认安装完毕”。

步骤 4：选择主机组（可选）

1. 在主机组列表中，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。
2. 单击“下一步：采集配置”。

步骤 5：采集配置

在使用自建K8s接入完成日志接入时，采集配置的具体配置如下：

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。
2. **数据源配置**：选择数据源类型，进行对应的数据源配置。

表 4-35 采集配置参数表

类型	参数配置
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。 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。 • 开启后采集容器标准错误（stderr），可以选择采集目前路径：将标准输出和标准错误采集到不同的文件（stdout.log和stderr.log）、将标准输出和标准错误采集到同一个文件（stdout.log）。 • 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。 • 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。该功能依赖ICAgent版本，详见**查看ICAgent版本说明**。 关闭“允许文件多次采集”后，采集路径不能重复配置，即同一主机下的同一日志文件，即使跨日志流，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。 • **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。 **说明** 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。 • 添加自定义绕接规则，ICAgent目前是通过文件名规则来判断是否为绕接文件，如果您的绕接规则不符合内置类型时，可以通过单击“添加自定义绕接规则”来进行匹配，避免重复采集和绕接时的日志丢失。 **内置类型**为{basename}{连接符}{绕接标识}.后缀，{basename}.{后缀}{连接符}{绕接标识}。其中连接符为**-._**绕接标识为非字母符号，后缀为字母。 **自定义绕接规则**为{basename}+绕接文件的特征正则表达式组成匹配规则。例如您的日志文件名称为test.out.log，绕接后的文件名为test.2024-01-01.0.out.log，test.2024-01-01.1.out.log，因此在路径配置时，采集路径为/opt/*.log，绕接规则为{basename}\.\d{4}-\d{2}-\d{2}\.\d{1}.out.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。该功能依赖ICAgent版本，详见**查看ICAgent版本说明**。 关闭“允许文件多次采集”后，采集路径不能重复配置，即同一主机下的同一日志文件，即使跨日志流，也只能配置一次。 • 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。

类型	参数配置
节点文件路径	采集集群内指定节点路径的文件。 • **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。 • 添加自定义绕接规则，ICAgent目前是通过文件名规则来判断是否为绕接文件，如果您的绕接规则不符合内置类型时，可以通过单击“添加自定义绕接规则”来进行匹配，避免重复采集和绕接时的日志丢失。 **内置类型**为{basename}{连接符}{绕接标识}.后缀，{basename}.{后缀}{连接符}{绕接标识}。其中连接符为-._绕接标识为非字母符号，后缀为字母。 **自定义绕接规则**为{basename}+绕接文件的特征正则表达式组成匹配规则。例如您的日志文件名称为test.out.log，绕接后的文件名为test.2024-01-01.0.out.log，test.2024-01-01.1.out.log，因此在路径配置时，采集路径为/opt/*.log，绕接规则为{basename}\.\d{4}-\d{2}-\d{2}\.\d{1}.out.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。该功能依赖ICAgent版本，详见**查看ICAgent版本说明**。 关闭“允许文件多次采集”后，采集路径不能重复配置，即同一主机下的同一日志文件，即使跨日志流，也只能配置一次。 • 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。
K8S事件	采集K8S集群内的事件日志。无需设置参数。仅支持icagent 5.12.150及以上版本。 **说明** K8S事件不能重复配置，即一个K8S集群的K8S事件，只能配置接入到一个日志流。

3. 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。

   说明

   填写正则匹配规则后，单击校验按钮，支持校验确保正则表达式的正确性。

   表 4-36 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。 **说明** 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。 **说明** 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。 **说明** 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。
K8s Label白名单	通过K8s Label白名单指定待采集的容器。如果您要设置K8s Label白名单，那么LabelKey必填，LabelValue可选填。 新增多条白名单时，支持选择And或or的关系，即全部满足或满足任意白名单就可以被匹配。 **说明** 若LabelValue为空，则K8S Label中包含LabelKey的容器都匹配；若LabelValue不为空，则K8S Label中包含LabelKey=LabelValue的容器才匹配；LabelKey需要全匹配，LabelValue支持正则匹配。
K8s Label黑名单	通过K8s Label黑名单排除不采集的容器。如果您要设置K8s Label黑名单，那么LabelKey必填，LabelValue可选填。 新增多条黑名单时，支持选择And或or的关系，即全部满足或满足任意黑名单就可以被排除。 **说明** 若LabelValue为空，则K8S Label中包含LabelKey的容器都被排除；若LabelValue不为空，则K8S Label中包含LabelKey=LabelValue的容器才会被排除；LabelKey需要全匹配，LabelValue支持正则匹配。
K8s Label日志标签	设置K8s Label日志标签后，日志服务将在日志中新增K8s Label相关字段。 **说明** 设置K8s 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，将在日志中添加内容{app_alias：lts}。
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。 新增多条白名单时，支持选择And或or的关系，即全部满足或满足任意白名单就可以被匹配。 **说明** 若LabelValue为空，则容器 Label中包含LabelKey的容器都匹配；若LabelValue不为空，则容器 Label中包含LabelKey=LabelValue的容器才匹配；LabelKey需要全匹配，LabelValue支持正则匹配。

参数名称	参数说明
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。 新增多条黑名单时，支持选择And或or的关系，即全部满足或满足任意黑名单就可以被排除。 **说明** 若LabelValue为空，则容器 Label中包含LabelKey的容器都被排除；若LabelValue不为空，则容器 Label中包含LabelKey=LabelValue的容器才会被排除；LabelKey需要全匹配，LabelValue支持正则匹配。
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。 **说明** 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。 新增多条白名单时，支持选择And或or的关系，即全部满足或满足任意白名单就可以被匹配。 **说明** 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；LabelKey需要全匹配，LabelValue支持正则匹配。
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。 新增多条黑名单时，支持选择And或or的关系，即全部满足或满足任意黑名单就可以被排除。 **说明** 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；LabelKey需要全匹配，LabelValue支持正则匹配。
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。 **说明** 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. 开启结构化解析配置，详细操作请参考**ICAgent结构化解析规则说明**。
   支持组合解析，一个日志流的每个采集配置可以配置不同的结构化解析规则。
   若已经配置了云端结构化解析，请先删除云端结构化解析后再配置ICAgent结构化解析。

图 4-16 ICAgent 结构化解析配置

5. 其他配置。

表 4-37 其他配置

名称	说明
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。
日志拆分	• 开启日志拆分，支持自定义设置日志拆分大小，设置范围为500KB-1024KB。日志拆分大小为500KB，即单条日志超过500KB会被拆分为多条采集。例如：日志大小为600KB，被拆分为2条日志采集，第一条500KB，第二条100KB。仅支持单行日志，不支持多行日志。 • 不开启日志拆分，单条日志大小限制不超过500KB，超过限制部分会被截断丢弃。
采集二进制文件	云日志服务支持采集二进制文件。 您可以通过命令（*file -i 文件名*）查看文件类型，如果包含charset=binary，那么该日志文件就是二进制文件。 当日志的文件类型为二进制时，开启采集二进制文件按钮，则对接入的二进制文件日志进行采集，但仅支持UTF8编码的字符串，非UFT8编码的字符在LTS控制台页面会显示乱码。 当日志的文件类型为二进制时，未开启采集二进制文件按钮，则对接入的二进制文件日志停止采集，开启后即可进行采集。
日志文件编码	日志文件编码支持UTF-8、GBK（暂不支持Windows场景）。 UTF-8编码是一种变长编码方式，用于表示Unicode字符集。GBK全称《汉字内码扩展规范》，中文计算机编码的一种，是ASCII码和GB2312编码的扩展。
采集策略	采集策略支持增量或全量。 • 增量采集：ICAgent采集新文件时，从文件的末尾开始读。 • 全量采集：ICAgent采集新文件时，从文件的开头开始读。

名称	说明
自定义元数据	• 关闭“自定义元数据”，使用ICAgent系统默认配置的字段上报到LTS，不需要用户配置且ICAgent系统不支持配置。 • 开启“自定义元数据”，根据用户选择的内置字段和自定义键值增加字段上报到LTS。 系统内置字段：勾选需要设置的内置字段。 自定义键值对：单击“添加”，输入键值key和键值Value。

6. 参考**表4-38**配置日志格式、日志时间。

表 4-38 日志采集信息

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

名称	说明
	时间通配符：用日志打印时间来标识一条日志数据，通过时间通配符来匹配日志，每条日志的行首显示日志的打印时间。 ● 如果日志中的时间格式为：2019-01-01 23:59:59.011，时间通配符应该填写为：YYYY-MM-DD hh:mm:ss.SSS。 ● 如果日志中的时间格式为：19-1-1 23:59:59.011，时间通配符应该填写为：YY-M-D hh:mm:ss.SSS。 **说明** 如果日志中不存在年份信息，则云日志会自动补齐年份数据为当前年份数据。 填写示例： YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)
分行模式	日志格式选择多行日志时，需要选择分行模式，分行模式选择“日志时间”时，是以时间通配符来划分多行日志；当选择“正则模式”时，则以正则表达式划分多行日志。
正则表达式	此配置是用来标识一条日志数据的正则表达式。日志格式选择“多行日志”格式后且“分行模式”已选择“正则模式”后需要设置。

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**。

7. 单击“下一步：索引配置”。

步骤 6：索引配置

1. 索引配置（可选项），具体请参考**设置LTS日志索引配置**。
2. 单击“提交”。

步骤 7：完成接入配置

接入成功后会生成一条接入配置信息。

- 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。

- 单击接入配置操作列的“修改”重新修改接入配置信息。
- 单击接入配置操作列的“标签管理”即可添加标签。
- 单击接入配置操作列的“更多 > 复制”复制一条新的接入配置信息。
- 单击接入配置操作列的“更多 > 删除”即可删除接入配置信息。

  说明

  删除接入配置后会导致日志无法正常采集，可能会影响用户日志相关业务异常，且删除后无法恢复，请谨慎操作。

- 若不需要采集日志，关闭接入配置状态列的开关  。若需要重新采集日志，需要重新开启接入配置状态列的开关  。

  说明

  关闭接入配置后会导致日志无法正常采集，可能会影响用户日志相关业务异常，请谨慎操作。

- 单击接入配置操作列的“更多 > 采集诊断”，可查看ICAgent异常监控、ICAgent整体状态和ICAgent采集监控。

批量设置多个接入配置

支持同时批量设置多个接入配置，操作简单，不用重复配置即可快速完成多个场景的接入配置。

步骤1 在“接入管理”页面，单击“批量接入”，进入配置详情页面，请参考**表4-39**。

表 4-39 批量接入设置

类型	操作	说明
基本配置	接入类型	选择自建k8s - 应用日志。
	接入配置数量	在输入框填写接入配置数量，单击“添加接入配置”。 在接入配置下方默认已有1个接入配置，最多支持再添加99个数量，因此支持同时添加100个接入配置。
接入配置	接入列表	1. 左侧显示接入配置的信息，最多支持添加99个配置。 2. 右侧显示配置接入的内容，详细请参考**步骤5：采集配置**进行设置。 3. 一个接入配置设置完成后，单击“应用于其他接入配置”即可将该接入配置复制到其他接入配置。

步骤2 单击“参数检查”，检查成功后，单击“提交”，批量接入设置完成。

例如添加了4个接入配置，批量创建成功后，在“接入管理”下方，就会显示4条接入配置数量。

步骤3 （可选）支持对接入配置任务进行以下操作：

- 勾选多个已创建成功的接入配置，单击“批量编辑”进入配置详情页面，通过选择不同接入类型，修改对应的接入配置信息。

- 勾选多个已创建成功的接入配置，单击启用或禁用按钮。接入配置状态禁用后不会继续采集日志。
- 勾选多个已创建成功的接入配置，单击删除按钮即可批量删除接入配置。

----结束

4.2.12 ICAgent 结构化解析规则说明

云日志服务LTS支持通过ICAgent采集方式进行日志上报。在创建日志接入时设置采集配置策略，例如解析规则、白名单规则、黑名单规则、上传原始日志等参数，实现定制化的采集策略。ICAgent采集配置定义了如何在服务器上采集同类日志并解析、发送到指定的日志流上。

功能优势

- 基于日志文件，无侵入式采集日志。您无需修改应用程序代码，且采集日志不会影响您的应用程序运行。
- 稳定处理日志采集过程中的各种异常。当遇到网络异常、服务端异常等问题时会采用主动重试、本地缓存数据等措施保障数据安全。
- 基于日志服务的集中管理能力。安装ICAgent后，只需要在日志服务上配置主机组、ICAgent采集配置等信息即可。
- 完善的自我保护机制。为保证运行在服务器上的ICAgent，不会明显影响您服务器上其他服务的性能，ICAgent在CPU、内存及网络使用方面都做了严格的限制和保护机制。

日志接入前，您可以提前了解ICAgent采集的结构化解析规则，方便您快速操作。支持组合解析，一个日志流的每个采集配置可以配置不同的结构化解析规则。

支持以下日志结构化解析规则：

- **单行-全文日志**：采集的日志文件中，如果您希望每一行日志在LTS界面中都显示为一条单独的日志数据，则选择单行日志。
- **多行-全文日志**：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。
- **JSON**：适用JSON格式的日志，通过提取JSON字段将其拆分为键值对。
- **分隔符**：适用于固定符号（例如空格/逗号/冒号）分隔的日志。
- **单行-完全正则**：适用任意格式的单行日志，使用正则表达式提取字段。填写正则匹配规则后，单击验证按钮，支持校验确保正则表达式的正确性。
- **多行-完全正则**：适用任意格式的多行日志，使用正则表达式提取字段。首行正则表达式支持自动生成和手动输入，填写正则匹配规则后，单击验证按钮，支持校验确保正则表达式的正确性。
- **组合解析**：适用于多格式嵌套的日志（例如：分隔符+JSON）。当您的日志结构太过复杂，涉及多种解析模式，单种解析模式（如 Nginx 模式、完整正则模式、JSON 模式等）无法满足日志解析需求时，您可以使用组合解析格式解析日志，此模式支持用户在控制台输入代码（json 格式）用来定义日志解析的流水线逻辑。您可添加一个或多个插件处理配置，ICAgent会根据处理配置顺序逐一执行。

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。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：表示查询指定时间范围的日志数据。

单行-全文日志

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。

1. 选择单行-全文日志。
2. 日志过滤默认关闭，可根据需要打开日志过滤，进行添加白名单规则或黑名单规则，白名单规则或黑名单规则添加上限为20个。

图 4-17 日志过滤规则

- 开启日志过滤才需要设置，添加白名单规则。

  您可以添加过滤规则筛选出有价值的日志数据，过滤规则为**正则表达式**，应用到指定Key的Value。所创建的过滤规则为命中规则，即匹配上正则表达式的日志才会被采集上报。

  i. 单击“添加”，填写Key值和过滤规则（正则表达式）。单行/多行全文模式下，默认使用content作为全文的键{key}名，多条过滤规则之间关系是“或”逻辑。例如采集日志源文件中包含hello的日志，可配置采集规则为**.*hello.***

  ii. 单击操作列的  可以进行规则校验，输入字段值，单击“校验”，提示校验成功。

图 4-18 校验

- 开启日志过滤才需要设置，添加黑名单规则。

  您可以添加过滤规则筛选出有价值的日志数据，过滤规则为正则表达式，应用到指定Key的Value。所创建的过滤规则为丢弃规则，即匹配上正则表达式的日志会被丢弃。

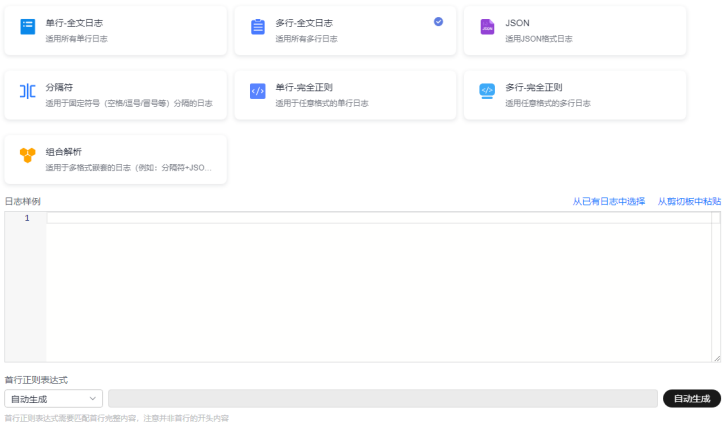
  i. 单击“添加”，填写Key值和过滤规则（正则表达式）。单行/多行全文模式下，默认使用content作为全文的键{key}名，多条过滤规则之间关系是“或”逻辑。例如不采集日志源文件中包含test的日志，可配置采集规则为**.*test.***

  ii. 单击操作列的  可以进行规则校验，输入字段值，单击“校验”，提示校验成功。

多行-全文日志

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。

1. 选择多行-全文日志。
2. 从“从已有日志中选择”或“从剪切板中粘贴”选择日志样例。
   - 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。



3. 在“首行正则表达式”下方支持自动生成或手动输入正则表达式。首行正则表达式需要匹配首行完整内容，注意并非首行的开头内容。

图 4-19 首行正则表达式

4. 日志过滤默认关闭，可根据需要打开日志过滤，进行添加白名单规则或黑名单规则，白名单规则或黑名单规则添加上限为20个。

图 4-20 日志过滤规则

- 开启日志过滤才需要设置，添加白名单规则。

  您可以添加过滤规则筛选出有价值的日志数据，过滤规则为**正则表达式**，应用到指定Key的Value。所创建的过滤规则为命中规则，即匹配上正则表达式的日志才会被采集上报。

  i. 单击“添加”，填写Key值和过滤规则（正则表达式）。单行/多行全文模式下，默认使用content作为全文的键{key}名，多条过滤规则之间关系是“或”逻辑。例如采集日志源文件中包含hello的日志，可配置采集规则为**.*hello.***

  ii. 单击操作列的  可以进行规则校验，输入字段值，单击“校验”，提示校验成功。

  图 4-21 校验

- 开启日志过滤才需要设置，添加黑名单规则。

  您可以添加过滤规则筛选出有价值的日志数据，过滤规则为正则表达式，应用到指定Key的Value。所创建的过滤规则为丢弃规则，即匹配上正则表达式的日志会被丢弃。

  i. 单击“添加”，填写Key值和过滤规则（正则表达式）。单行/多行全文模式下，默认使用content作为全文的键{key}名，多条过滤规则之间关

系是“或”逻辑。例如不采集日志源文件中包含test的日志，可配置采集规则为**.*test.***

ii. 单击操作列的  可以进行规则校验，输入字段值，单击“校验”，提示校验成功。

JSON

适用JSON格式的日志，通过提取JSON字段将其拆分为键值对。

1. 选择JSON格式。
2. 日志过滤默认关闭，可根据需要打开日志过滤，进行添加白名单规则或黑名单规则，白名单规则或黑名单规则添加上限为20个。

图 4-22 日志过滤规则

- 开启日志过滤才需要设置，添加白名单规则。

  您可以添加过滤规则筛选出有价值的日志数据，过滤规则为**正则表达式**，应用到指定Key的Value。所创建的过滤规则为命中规则，即匹配上正则表达式的日志才会被采集上报。

  i. 单击“添加”，填写Key值和过滤规则（正则表达式）。Key值为日志字段名称，多条过滤规则之间关系是“或”逻辑。例如采集日志源文件中包含hello的日志，可配置采集规则为**.*hello.***

  ii. 单击操作列的  可以进行规则校验，输入字段值，单击“校验”，提示校验成功。

  图 4-23 校验

- 开启日志过滤才需要设置，添加黑名单规则。

  您可以添加过滤规则筛选出有价值的日志数据，过滤规则为正则表达式，应用到指定Key的Value。所创建的过滤规则为丢弃规则，即匹配上正则表达式的日志会被丢弃。

i. 单击“添加”，填写Key值和过滤规则（正则表达式）。Key值为日志字段名称，多条过滤规则之间关系是“或”逻辑。例如不采集日志源文件中包含test的日志，可配置采集规则为.*test.*

ii. 单击操作列的  可以进行规则校验，输入字段值，单击“校验”，提示校验成功。

3. 上传原始日志。

   打开上传原始日志开关后，原始日志将作为content字段的值上传到日志服务。

4. 上传解析失败日志。

   打开上传解析失败日志开关后，原始日志将作为_content_parse_fail_字段的值上传到日志服务。

5. **自定义日志时间**。

   开启后可指定某一字段作为日志时间，或关闭此项使用日志被采集时间作为日志时间。

6. json解析层数。增加json解析层数配置，取值范围为1~4，只能整数，默认值为1。

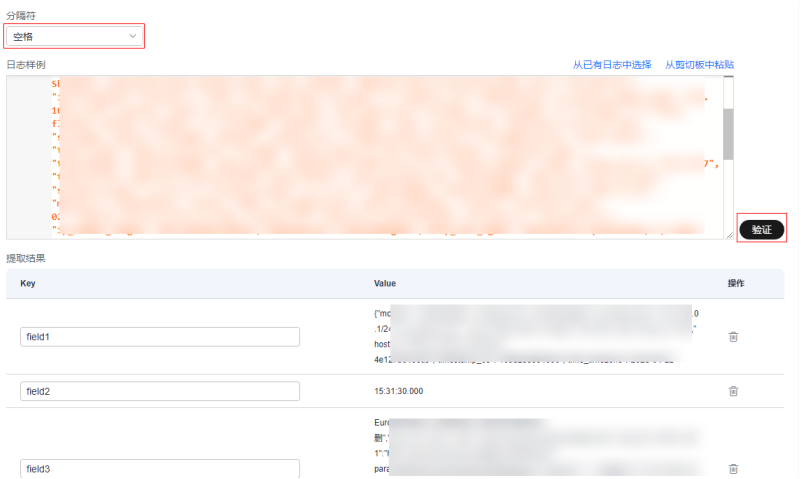
   将json格式日志的字段展开，例如原始日志为{"key1":{"key2":"value"}}，解析1层日志为：{"key1":{"key2":"value"}}，解析2层日志为：{"key1.key2":"value"}。

分隔符

使用分隔符（例如：逗号、空格或字符）提取字段。

1. 选择分隔符。
2. 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。
3. 从“从已有日志中选择”或“从剪切板中粘贴”选择日志样例，单击“验证”，在提取结果下方查看结果。
   - 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。

图 4-24 分隔符



4. 日志过滤默认关闭，可根据需要打开日志过滤，进行添加白名单规则或黑名单规则，白名单规则或黑名单规则添加上限为20个。

图 4-25 日志过滤规则

- 开启日志过滤才需要设置，添加白名单规则。

  您可以添加过滤规则筛选出有价值的日志数据，过滤规则为**正则表达式**，应用到指定Key的Value。所创建的过滤规则为命中规则，即匹配上正则表达式的日志才会被采集上报。

  i. 单击“添加”，填写Key值和过滤规则（正则表达式）。Key值为日志字段名称，多条过滤规则之间关系是“或”逻辑。例如采集日志源文件中包含hello的日志，可配置采集规则为**.*hello.***

  ii. 单击操作列的  可以进行规则校验，输入字段值，单击“校验”，提示校验成功。

  图 4-26 校验

- 开启日志过滤才需要设置，添加黑名单规则。

  您可以添加过滤规则筛选出有价值的日志数据，过滤规则为正则表达式，应用到指定Key的Value。所创建的过滤规则为丢弃规则，即匹配上正则表达式的日志会被丢弃。

  i. 单击“添加”，填写Key值和过滤规则（正则表达式）。Key值为日志字段名称，多条过滤规则之间关系是“或”逻辑。例如不采集日志源文件中包含test的日志，可配置采集规则为**.*test.***

  ii. 单击操作列的  可以进行规则校验，输入字段值，单击“校验”，提示校验成功。

5. 上传原始日志。

   打开上传原始日志开关后，原始日志将作为content字段的值上传到日志服务。

6. 上传解析失败日志。

   打开上传解析失败日志开关后，原始日志将作为_content_parse_fail_字段的值上传到日志服务。

7. **自定义日志时间**。

开启后可指定某一字段作为日志时间，或关闭此项使用日志被采集时间作为日志时间。

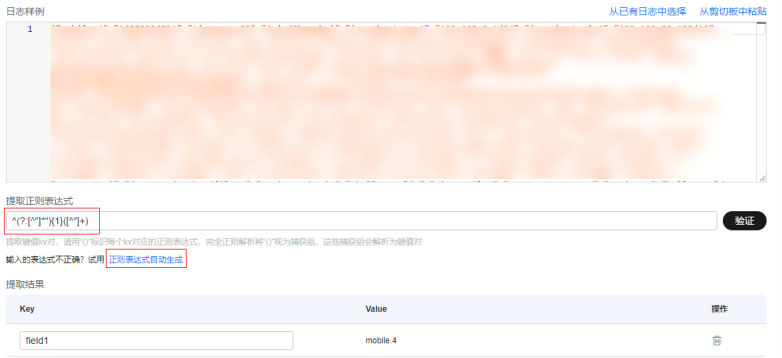
单行-完全正则

适用任意格式的单行日志，使用正则表达式提取字段。

1. 选择单行-完全正则。
2. 从“从已有日志中选择”或“从剪切板中粘贴”选择日志样例。
   - 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。
3. 在“提取正则表达式”下方输入要提取日志的正则表达式，单击“验证”，在提取结果下方查看结果。

   或者单击“正则表达式自动生成”，在新打开的页面根据日志样例提取字段，输入key值，单击“确定”即可自动生成正则表达式，设置完成后，单击“确定”。

图 4-27 提取正则表达式



4. 日志过滤默认关闭，可根据需要打开日志过滤，进行添加白名单规则或黑名单规则，白名单规则或黑名单规则添加上限为20个。

图 4-28 日志过滤规则

   - 开启日志过滤才需要设置，添加白名单规则。

     您可以添加过滤规则筛选出有价值的日志数据，过滤规则为**正则表达式**，应用到指定Key的Value。所创建的过滤规则为命中规则，即匹配上正则表达式的日志才会被采集上报。

     i. 单击“添加”，填写Key值和过滤规则（正则表达式）。Key值为日志字段名称，多条过滤规则之间关系是“或”逻辑。例如采集日志源文件中包含hello的日志，可配置采集规则为.***hello.***

ii. 单击操作列的  可以进行规则校验，输入字段值，单击“校验”，提示校验成功。

图 4-29 校验

- 开启日志过滤才需要设置，添加黑名单规则。

  您可以添加过滤规则筛选出有价值的日志数据，过滤规则为正则表达式，应用到指定Key的Value。所创建的过滤规则为丢弃规则，即匹配上正则表达式的日志会被丢弃。

  i. 单击“添加”，填写Key值和过滤规则（正则表达式）。Key值为日志字段名称，多条过滤规则之间关系是“或”逻辑。例如不采集日志源文件中包含test的日志，可配置采集规则为**.*test.***

  ii. 单击操作列的  可以进行规则校验，输入字段值，单击“校验”，提示校验成功。

5. 上传原始日志。

   打开上传原始日志开关后，原始日志将作为content字段的值上传到日志服务。

6. 上传解析失败日志。

   打开上传解析失败日志开关后，原始日志将作为_content_parse_fail_字段的值上传到日志服务。

7. **自定义日志时间**。

   开启后可指定某一字段作为日志时间，或关闭此项使用日志被采集时间作为日志时间。

多行-完全正则

适用任意格式的多行日志，使用正则表达式提取字段。

1. 选择多行-完全正则。
2. 从“从已有日志中选择”或“从剪切板中粘贴”选择日志样例。
   - 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。
3. 在“首行正则表达式”下方支持自动生成或手动输入正则表达式。首行正则表达式需要匹配首行完整内容，注意并非首行的开头内容。

说明

“首行正则表达式”用于识别多行日志的行首，例如以下日志示例：

```
2024-10-11 10:59:07.000 a.log:1 level:warn
 no.1 log
2024-10-11 10:59:17.000 a.log:2 level:warn
 no.2 log
```

完整的多行是：

```
2024-10-11 10:59:07.000 a.log:1 level:warn
no.1 log
```

首行则是：

```
2024-10-11 10:59:07.000 a.log:1 level:warn
```

首行正则示例：^(\d+-\d+-\d+\s+\d+:\d+:\d+\.\d+)，由于每个首行的日期是唯一的，因此可以根据日期来生成首行正则。

4. 在“提取正则表达式”下方输入要提取日志的正则表达式，单击“验证”，在提取结果下方查看结果。

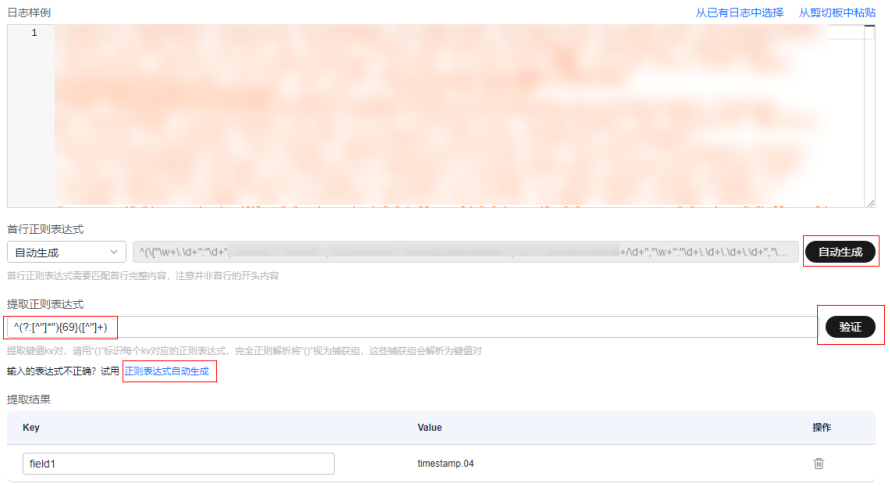
   或者单击“正则表达式自动生成”，在新打开的页面根据日志样例提取字段，输入key值，单击“确定”即可自动生成正则表达式，设置完成后，单击“确定”。

   说明

   提取结果显示的是“提取正则表达式”执行的结果，而不是“首行正则表达式”执行的结果，“首行正则表达式”执行的结果需要到目标日志流查看。

   如果“首行正则表达式”手动输入的正则表达式有误，则会导致无法查看上报的日志流数据。

图 4-30 设置正则表达式



5. 日志过滤默认关闭，可根据需要打开日志过滤，进行添加白名单规则或黑名单规则，白名单规则或黑名单规则添加上限为20个。

图 4-31 日志过滤规则

- 开启日志过滤才需要设置，添加白名单规则。

  您可以添加过滤规则筛选出有价值的日志数据，过滤规则为**正则表达式**，应用到指定Key的Value。所创建的过滤规则为命中规则，即匹配上正则表达式的日志才会被采集上报。

  i. 单击“添加”，填写Key值和过滤规则（正则表达式）。Key值为日志字段名称，多条过滤规则之间关系是“或”逻辑。例如采集日志源文件中包含hello的日志，可配置采集规则为**.*hello.***

  ii. 单击操作列的  可以进行规则校验，输入字段值，单击“校验”，提示校验成功。

  图 4-32 校验

- 开启日志过滤才需要设置，添加黑名单规则。

  您可以添加过滤规则筛选出有价值的日志数据，过滤规则为正则表达式，应用到指定Key的Value。所创建的过滤规则为丢弃规则，即匹配上正则表达式的日志会被丢弃。

  i. 单击“添加”，填写Key值和过滤规则（正则表达式）。Key值为日志字段名称，多条过滤规则之间关系是“或”逻辑。例如不采集日志源文件中包含test的日志，可配置采集规则为**.*test.***

  ii. 单击操作列的  可以进行规则校验，输入字段值，单击“校验”，提示校验成功。

6. 上传原始日志。

   打开上传原始日志开关后，原始日志将作为content字段的值上传到日志服务。

7. 上传解析失败日志。

   打开上传解析失败日志开关后，原始日志将作为_content_parse_fail_字段的值上传到日志服务。

8. **自定义日志时间**。

   开启后可指定某一字段作为日志时间，或关闭此项使用日志被采集时间作为日志时间。

组合解析

适用于多格式嵌套的日志（例如：分隔符+JSON），根据语法自定义配置解析规则。

1. 选择组合解析。
2. 从“从已有日志中选择”或“从剪切板中粘贴”选择日志样例，在插件配置下方输入配置内容。

3. 您可以根据日志内容参考以下插件语法自定义设置：
   - processor_regex

     表 4-40 正则提取

参数	类型	说明
source_key	string	原始字段名。
regex	string	正则表达式()中为提取字段。
keys	string	为提取的内容指定字段名。
keep_source	boolean	是否保留原始字段。
keep_source_if_parse	boolean	解析错误是否保留原始字段。

   - processor_split_string

     表 4-41 分隔符解析

参数	类型	说明
source_key	string	原始字段名。
split_sep	string	分隔符字符串。
keys	string	为提取的内容指定字段名。
keep_source	boolean	被解析后的日志中是否保留原始字段。
split_type	char/special_char/string	分隔类型，支持char-单字符、special_char-不可见字符、string-字符串。
keep_source_if_parse_error	boolean	解析错误是否保留原始字段。

   - processor_split_key_value

     表 4-42 键值对分割

参数	类型	说明
source_key	string	原始字段名。
split_sep	string	键值对之间的分隔符，默认值为制表符\t。
expand_connector	string	单个键值对中键与值之间的分隔符，默认值为半角冒号（:）。

参数	类型	说明
keep_source	boolean	被解析后的日志中是否保留原始字段。

- processor_add_fields

  表 4-43 添加字段

参数	类型	说明
fields	json/object	待添加的字段名和字段值。键值对格式，支持添加多个。

- processor_drop

  表 4-44 丢弃字段

参数	类型	说明
drop_keys	string	丢弃的字段列表。

- processor_rename

  表 4-45 重命名字段

参数	类型	说明
source_keys	string	待重命名的原始字段。
destkeys	string	重命名后的字段。

- processor_json

  表 4-46 json 展开提取

参数	类型	说明
source_key	string	原始字段名。
keep_source	string	被解析后的日志中是否保留原始字段。
expand_depth	int	json展开的深度。默认值为0，表示不限制。1表示当前层级，以此类推。
expand_connector	string	json展开时的连接符，默认值为下划线（_）。
prefix	string	json展开时，对字段名附加的前缀。

参数	类型	说明
keep_source_if_parse_error	boolean	解析错误是否保留原始字段。

- processor_filter_regex

  表 4-47 过滤器

参数	类型	说明
include	json/object	key为日志字段，value为匹配的正则表达式。
exclude	json/object	key为日志字段，value为匹配的正则表达式。

- processor_gotime

  表 4-48 提取时间

参数	类型	说明
source_key	string	原始字段名。
source_format	string	原始时间的格式。
source_location	int	原始时间的时区。参数值为空时，表示logtail所在主机或容器的时区。
dest_key	string	解析后的目标字段。
dest_format	string	解析后的时间格式。
dest_location	int	解析后的时区。参数值为空时，表示本机时区。
set_time	boolean	是否将解析后的时间设置为日志时间。
keep_source	boolean	被解析后的日志中是否保留原始字段。

4. 参考示例：

```
[
    {
        "type": "processor_regex",
        "detail": {
            "source_key": "content",
            "regex": "*",
            "keys": [
                "key1",
                "key2"
            ],
            "multi_line_regex": "*",
            "keep_source": true,
```

```
            "keep_source_if_parse_error": true
        }
    },
    {
        "type": "processor_split_string",
        "detail": {
            "split_sep": ".",
            "split_type": ".",
            "split_keys": [
                "key1",
                "key2"
            ],
            "source_key": "context",
            "keep_source": true,
            "keep_source_if_parse_error": true
        }
    },
    {
        "type": "processor_add_fields",
        "detail": {
            "fields": [
                {
                    "key1": "value1"
                },
                {
                    "key2": "value2"
                }
            ]
        }
    },
    {
        "type": "processor_drop",
        "detail": {
            "drop_keys": [
                "key1",
                "key2"
            ]
        }
    },
    {
        "type": "processor_rename",
        "detail": {
            "source_key": [
                "skey1",
                "skey2"
            ],
            "dest_keys": [
                "dkey1",
                "dkey2"
            ]
        }
    },
    {
        "type": "processor_json",
        "detail": {
            "source_key": "context",
            "expand_depth": 4,
            "expand_connector": "_",
            "prefix": "prefix",
            "keep_source": true,
            "keep_source_if_parse_error": true
        }
    },
    {
        "type": "processor_gotime",
        "detail": {
            "source_key": "skey",
            "source_format": "ydm",
            "source_location": 8,
```



```
            "dest_key": "dkey",
            "dest_format": "ydm",
            "dest_location": 8,
            "set_time": true,
            "keep_source": true,
            "keep_source_if_parse_error": true
        }
    },
    {
        "type": "processor_filter_regex",
        "detail": {
            "include": {
                "ikey1": "*",
                "ikey2": "*"
            },
            "exclude": {
                "ekey1": "*",
                "ekey1": "*"
            }
        }
    }
]
```

自定义日志时间

开启自定义日志时间开关  ，参考**表4-49**设置参数。

说明

- 若时间格式填写错误或指定字段不存在，将使用日志被采集时间作为日志时间。
- 对结构化解析进行字段名称修改、字段删除、字段类型修改等操作，都需要重新校验时间字段。

表 4-49 参数配置表

参数	说明	示例
时间字段key名称	已提取字段的名称。单击下拉框选择已提取的字段，该字段为string或long类型。	test
字段value	已提取的字段value，选择字段key后，将自动填充。 **说明** 配置的字段value必须是当前时间前后24小时内的时间。	2023-07-19 12:12:00
时间格式	请参考**常见日志时间格式**。	yyyy-MM-dd HH:mm:ss
操作	单击  校验图标，提示“时间格式和字段value匹配成功”则表示校验成功。	-

常见日志时间格式

常见日志时间格式如下**表4-50**。

说明

默认情况下，云日志服务LTS中的日志时间戳精确到秒，因此时间格式只需配置到秒，无需配置毫秒、微秒等信息。

表 4-50 时间格式

时间格式	说明	示例
EEE	星期的缩写。	Fri
EEEE	星期的全称。	Friday
MMM	月份的缩写。	Jan
MMMM	月份的全称。	January
dd	每月第几天，十进制，范围为01~31。	07, 31
HH	小时，24小时制。	22
hh	小时，12小时制。	11
MM	月份，十进制，范围为01~12。	08
mm	分钟，十进制，范围为00~59。	59
a	AM或PM。	AM、PM
hh:mm:ss a	12小时制的时间组合。	11:59:59 AM
HH:mm	小时和分钟组合。	23:59
ss	秒数，十进制，范围为00~59。	59
yy	年份，十进制，不带世纪，范围为00~99。	04、98
yyyy	年份，十进制。	2004、1998
d	每月第几天，十进制，范围为1~31。	7、31
DDD	一年中的天数，十进制，范围为001~366。	365
u	星期几，十进制，范围为1~7，1表示周一。	2
w	每年的第几周，星期天是一周的开始，范围为00~53。	23
W	每月的第几周，范围为0~5。	2
U	星期几，十进制，范围为0~6，0代表周日。	5
EEE MMM dd HH:mm:ss yyyy	标准的日期和时间。	Tue Nov 20 14:12:58 2020

时间格式	说明	示例
EEE MMM dd yyyy	标准的日期，不带时间。	Tue Nov 20 2020
HH:mm:ss	标准的时间，不带日期。	11:59:59
%s	Unix时间戳。	147618725

4.3 使用云服务接入 LTS

4.3.1 云服务接入 LTS 概述

云日志服务（LTS）支持采集计算、存储、安全、数据库等多种华为云服务的日志数据，您可以使用LTS对云服务日志进行关键词搜索、运营数据统计分析、运行状况监控告警等多种操作。当前LTS支持采集的云服务日志如下表所示：

表 4-51 云服务接入

云服务简称	云服务名称	日志类型	文档链接	仪表盘
AOM	应用运维管理	全量日志	**应用运维管理AOM接入LTS**	-
APIG	API网关	网关访问日志（APIG）	**API网关APIG接入LTS**	• APIG监控中心 • APIG访问中心 • APIG秒级监控
BMS	裸金属服务器	全量日志	**裸金属服务BMS文本日志接入LTS**	-
CBH	云堡垒机	操作日志	**云堡垒机CBH接入LTS**	-
CCE	云容器引擎	• 用户应用日志 • CCE管理面日志	**云容器引擎CCE应用日志接入LTS**	-
CFW	云防火墙	• 攻击日志（CFW攻击日志） • 访问日志（CFW访问控制日志） • 流量日志（CFW流量日志）	**云防火墙CFW接入LTS**	-
CTS	云审计服务	云服务管理面操作日志（CTS）	**云审计服务CTS接入LTS**	-

云服务简称	云服务名称	日志类型	文档链接	仪表盘
DDS	文档数据库服务	• 审计日志（DDS审计日志） • 错误日志（DDS错误日志） • 慢日志（DDS慢日志）	**文档数据库服务DDS接入LTS**	DDS审计日志中心
DMS	分布式消息服务Kafka版	DMS重平衡日志	**分布式消息服务Kafka版接入LTS**	-
DRS	数据复制服务	访问日志	**数据复制服务DRS接入LTS**	-
DWS	数据仓库服务	• CN节点日志 • DN节点日志 • 操作系统messages日志 • 审计日志	**数据仓库服务GaussDB(DWS)接入LTS**	-
ECS	弹性云服务器	全量日志（ICAgent采集文本日志）	**云主机ECS文本日志接入LTS**	-
ELB	弹性负载均衡	7层访问日志（ELB）	**弹性负载均衡 ELB接入LTS**	• ELB监控中心 • ELB访问中心 • ELB秒级监控
ER	企业路由器	全量日志（ER企业路由器）	**企业路由器ER接入LTS**	-
FunctionGraph	函数工作流	函数执行日志	**函数工作流FunctionGraph接入LTS**	-
GaussDB	云数据库GaussDB	审计日志（GAUSSV5审计日志）	**云数据库GaussDB接入LTS**	-
GES	图引擎服务	审计日志	**图引擎服务GES接入LTS**	-
GaussDB for MySQL	云数据库GaussDB for MySQL	• 错误日志（GAUSSDB_MYSQL错误日志） • 慢日志（GAUSSDB_MYSQL慢日志）	**云数据库TaurusDB接入LTS**	-

云服务简称	云服务名称	日志类型	文档链接	仪表盘
GeminiDB Redis	云数据库 GeminiDB Redis	慢日志（GeminiDB Redis慢日志）	云数据库GeminiDB接入LTS	-
GeminiDB Mongo	云数据库 GeminiDB Mongo	• 错误日志（GeminiDB Mongo错误日志） • 慢日志（GeminiDB Mongo慢日志）	云数据库GeminiDB Mongo接入LTS	-
GeminiDB Cassandra	云数据库 GeminiDB Cassandra	慢日志（GeminiDB Cassandra慢日志）	云数据库GeminiDB Cassandra接入LTS	-
IoTDA	设备接入	设备运行日志	设备接入IoTDA接入LTS	-
ModelArts	ModelArts	运行日志	AI开发平台ModelArts接入LTS	-
MRS	MapReduce服务	全量日志（ICAgent采集文本日志）	MapReduce服务MRS接入LTS	-
RDS for MySQL	云数据库 RDS for MySQL	• 错误日志（MYSQL错误日志） • 慢日志（MYSQL慢日志）	云数据库RDS for MySQL接入LTS	-
RDS for PostgreSQL	云数据库 RDS for PostgreSQL	• 错误日志（POSTGRESQL错误日志） • 慢日志（POSTGRESQL慢日志）	云数据库RDS for PostgreSQL接入LTS	-
RDS for SQLServer	云数据库RDS for SQL Server	错误日志（SQLSERVER错误日志）	云数据库RDS for SQLServer接入LTS	-

云服务简称	云服务名称	日志类型	文档链接	仪表盘
ROMA Connect	应用与数据集成平台	网关访问日志	应用与数据集成平台ROMA Connect接入LTS	-
SMN	消息通知服务	消息传输日志（SMN）	消息通知服务SMN接入LTS	-
SecMaster	安全云脑	全量日志	安全云脑SecMaster接入LTS	-
ServiceStage	应用管理与运维平台	ServiceStage容器应用日志	ServiceStage容器应用日志接入LTS	-
ServiceStage	应用管理与运维平台	ServiceStage云主机日志	ServiceStage云主机日志接入LTS	-
VPC	虚拟私有云	VPC流日志（VPC）	虚拟私有云VPC接入LTS	VPC流日志
WAF	Web应用防火墙	• 攻击日志 • 访问日志	Web应用防火墙WAF接入LTS	-

4.3.2 应用运维管理 AOM 接入 LTS

支持应用运维管理AOM的日志接入LTS。

具体接入方法请参见**接入LTS**。

4.3.3 API 网关 APIG 接入 LTS

支持API网关APIG日志接入LTS。

前提条件

已创建并使用华为云APIG实例。

设置 APIG 接入 LTS

云日志服务接入方式为API网关 APIG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“接入 > 接入中心”，单击“API网关 APIG”进行APIG接入配置。

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”：APIG配置。

步骤4 APIG配置，单击“前往APIG配置”。详细操作请参见**日志分析**。

步骤5 单击下一步：日志流配置。

表 4-52 日志流配置参数表

参数	说明
自动对日志流进行结构化配置和索引配置	开启该按钮，日志流结构化配置为APIG系统模板，索引配置时将所有APIG解析出来的字段打开快速分析按钮。配置结构化和索引后，才能对APIG日志进行SQL分析，并提供可视化图表。
自动为日志流添加标签：log_type=apig_access	开启该按钮，自动为日志流添加标签log_type=apig_access后，APIG仪表盘模板才能匹配该日志流。
自动为日志流创建仪表盘	开启该按钮，自动为日志流创建APIG仪表盘。

步骤6 单击“提交”。

----结束

4.3.4 云堡垒机 CBH 接入 LTS

支持云堡垒机（CBH）日志接入LTS。

具体接入方法请参见**配置LTS日志外发服务**。

4.3.5 云防火墙 CFW 接入 LTS

支持云防火墙CFW日志接入LTS。LTS对于采集的日志数据，通过海量日志数据的分析与处理，可以为您提供一个实时、高效、安全的日志处理能力。

具体接入方法请参见**配置日志**。

4.3.6 云审计服务 CTS 接入 LTS

支持云审计服务CTS日志接入LTS。

前提条件

已购买并使用华为云CTS实例。

设置 CTS 接入 LTS

云日志服务接入方式为云审计 CTS时，按照如下操作完成接入配置。

说明

云审计服务记录的用户操作事件日志接入到云日志服务后，在云日志服务控制台默认存储时间为30天，您在创建存放该日志的日志组时，可以对日志存储周期进行设置（1-365天）。详情请参考**管理日志组**。

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 > 接入中心”，单击“云审计 CTS”进行CTS接入配置。

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”：CTS配置。

步骤4 单击“前往CTS配置”。具体的操作步骤及参数配置，请见**云审计服务《 用户指南 》**。

步骤5 单击下一步：日志流配置。

表 4-53 日志流配置参数表

参数	说明
自动对日志流进行结构化配置和索引配置	开启该按钮，日志流结构化配置为CTS系统模板，索引配置时将所有CTS解析出来的字段打开快速分析按钮。配置结构化和索引后，才能对CTS日志进行SQL分析，并提供可视化图表。

步骤6 单击“提交”。

----结束

4.3.7 文档数据库服务 DDS 接入 LTS

支持文档数据库服务DDS日志接入LTS。

具体接入方法请参见**日志配置管理**。

4.3.8 分布式消息服务 Kafka 版接入 LTS

支持分布式消息服务Kafka日志接入LTS。重平衡日志记录Rebalance的详情，包括Rebalance时间、原因和触发Rebalance的客户端等。重平衡日志存储在云日志服务（Log Tank Service，简称LTS）中，由LTS提供查询功能。

具体接入方法请参见**查看Kafka重平衡日志**。

4.3.9 数据复制服务 DRS 接入 LTS

支持数据复制服务（DRS）日志接入LTS。配置访问日志后，DRS实例（包含实时迁移、备份迁移、实时同步、实时灾备和录制回放实例）新生成的所有日志记录会上传到云日志服务（Log Tank Service，简称LTS）进行管理。

具体接入方法请参见**日志配置管理**。

4.3.10 数据仓库服务 GaussDB(DWS)接入 LTS

支持数据仓库GaussDB（DWS）日志接入LTS。

具体接入方法请参见**集群日志管理**。

4.3.11 弹性负载均衡 ELB 接入 LTS

支持弹性负载均衡ELB日志接入LTS。

前提条件

已创建并使用华为云ELB实例。

使用限制

当前ELB日志仅支持七层独享型负载均衡和七层共享型负载均衡，不支持四层共享型负载均衡。

设置 ELB 接入

云日志服务接入方式为负载均衡 ELB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“接入 > 接入中心”，单击“负载均衡 ELB”进行ELB接入配置。

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”： ELB配置。

步骤4 单击“前往ELB配置”。具体的操作步骤，请见**访问日志**。

步骤5 日志流配置。

表 4-54 日志流配置参数表

参数	说明
自动对日志流进行结构化配置和索引配置	开启该按钮，日志流结构化配置为ELB系统模板，索引配置时将所有ELB解析出来的字段打开快速分析按钮。配置结构化和索引后，才能对ELB日志进行SQL分析，并提供可视化图表。
自动为日志流添加标签：log_type=elb_7layer_access	开启该按钮，自动为日志流添加标签（log_type=elb_7layer_access）后，ELB仪表盘模板才能匹配该日志流。
自动为日志流创建仪表盘	开启该按钮，自动为日志流创建ELB仪表盘。

步骤6 单击“提交”。

----结束

4.3.12 企业路由器 ER 接入 LTS

支持ER企业路由器日志接入LTS。

具体接入方法请参见**创建日志流**。

4.3.13 函数工作流 FunctionGraph 接入 LTS

支持函数工作流FunctionGraph日志接入LTS。

具体接入方法请参见**管理函数日志**。

4.3.14 云数据库 GaussDB 接入 LTS

支持云数据库 GaussDB日志接入LTS。

具体接入方法请参见**对接LTS并查看数据库审计日志**。

4.3.15 图引擎服务 GES 接入 LTS

支持图引擎服务GES日志接入LTS。

具体接入方法请参见**自定义创建图**。

4.3.16 云数据库 TaurusDB 接入 LTS

LTS支持云数据库 TaurusDB日志接入。

具体接入方法请参见**日志配置管理**。

4.3.17 云数据库 GeminiDB 接入 LTS

支持云数据库GeminiDB日志接入LTS。配置访问日志后，GeminiDB Redis实例新生成的日志记录会上传到云日志服务（Log Tank Service，简称LTS）进行管理。

具体接入方法请参见**日志配置管理**。

4.3.18 云数据库 GeminiDB Mongo 接入 LTS

支持云数据库GeminiDB Mongo日志接入LTS。

具体接入方式请参考**日志配置管理**。

4.3.19 云数据库 GeminiDB Cassandra 接入 LTS

支持云数据库GeminiDB Cassandra日志接入LTS。

如果您有需要请提工单给GeminiDB云服务开通。详细操作请参考**提交工单**。

4.3.20 设备接入 IoTDA 接入 LTS

支持设备接入IoTDA日志接入LTS。

具体接入方法请参见**查看运行日志**。

4.3.21 AI 开发平台 ModelArts 接入 LTS

支持AI开发平台ModelArts日志接入LTS。

具体接入方法请参见**部署为在线服务**。

4.3.22 MapReduce 服务 MRS 接入 LTS

支持MapReduce服务MRS日志接入LTS。

具体接入方法请参见**MRS服务对接云日志服务**。

4.3.23 云数据库 RDS for MySQL 接入 LTS

支持云数据库RDS for MySQL日志接入LTS。

具体接入方法请参见**日志配置管理**。

4.3.24 云数据库 RDS for PostgreSQL 接入 LTS

支持云数据库RDSfor PostgreSQL日志接入LTS。

具体接入方法请参见**日志配置管理**。

4.3.25 云数据库 RDS for SQLServer 接入 LTS

支持云数据库RDS for SQLServer日志接入LTS。

具体接入方法请参见**日志管理**。

4.3.26 应用与数据集成平台 ROMA Connect 接入 LTS

支持应用与数据集成平台ROMA Connect日志接入LTS。

具体接入方法请参见**查看API调用日志**。

4.3.27 消息通知服务 SMN 接入 LTS

支持消息通知服务SMN日志接入LTS。

具体接入方法请参见**消息传输日志**。

4.3.28 安全云脑 SecMaster 接入 LTS

支持安全云脑SecMaster日志接入LTS。

具体接入方法请参见**新增数据投递**。

4.3.29 对象存储服务 OBS 接入 LTS（邀测）

支持将对象存储服务桶内的文件一次性或定期导入到云日志服务，OBS服务接入LTS成功后，即可对日志进行搜索分析、日志加工等操作。加密桶的文件不支持导入LTS，若需要导入加密桶的文件，请先删除桶的加密配置，详细请参考**删除桶的加密配置**。

该功能仅支持华北-北京四、华南-广州的白名单用户，如有需要，请**提交工单**，其他区域暂不支持申请开通。

设置单个对象存储 OBS 接入 LTS

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“接入 > 接入中心”，单击“云服务接入-对象存储OBS”进行OBS接入配置。

或在左侧导航栏中，选择“接入 > 接入管理 > 接入日志”，单击“云服务接入-对象存储OBS”进行OBS接入配置。

或在左侧导航栏中，选择“日志管理”，单击目标日志流的名称进入日志详情页面。

单击右上角  ，在弹出页面中，选择“日志接入”页签，单击“接入日志”，在弹出页面中，单击“云服务接入-对象存储OBS”进行OBS接入配置。

步骤3 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。详细请参考**管理日志组**。

步骤4 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。详细请参考**管理日志流**。

步骤5 单击“下一步：采集配置”。

步骤6 在采集配置页面，参考**表4-55**设置参数。

表 4-55 采集配置

参数类型	名称	说明
基本配置	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、下划线及小数点，且不能以小数点、下划线开头或以小数点结尾。

参数类型	名称	说明
	任务监控	默认开启。 开启后会将每次任务执行状态写入日志流 lts-system/lts-obs2lts-statistics，您可以查看OBS文件导入LTS任务监控中心或者配置告警规则，及时发现数据导入过程中可能出现的异常问题。
OBS数据源配置	OBS桶	选择需要导入日志文件到LTS的OBS桶。
	文件夹前缀	输入待导入的OBS文件前缀，用于准确定位待导入的文件，支持输入文件前缀your_prefix/或完整路径your_prefix/file.gz（只支持导入5GB以内的原始文件）。
	文件正则过滤	用于过滤文件的正则表达式，只有文件名匹配该正则表达式的文件才会被导入。若不填写正则表达式，表示不过滤文件。 **说明** 假设目录下有aab和aba文件： ● 只匹配aab文件，正则写法：aab或aa或^aab或者aa. ● 只匹配aba文件，正则写法：aba或^aba或者^ab，不能写ab因为这样aab也是能匹配上的 ● 匹配aab和aba，正则写法：ab或者a.* ● 如果存在正则关键字的字符需要转义，例如{}则需要要转义为\{\}
	压缩格式	支持自动检测、不压缩、压缩gzip、压缩zip、压缩snappy。如果是zip压缩文件，只能包含一个文件，不能有任何文件夹。

参数类型	名称	说明
	导入间隔	• 一次性：只导入一次，云日志服务不会检测新出现的文件。 • 固定间隔：设置固定时间导入文件，云日志服务会检测新出现的文件，并导入云日志服务。 开启“解冻归档文件”：只支持解冻对象存储类别为归档存储的OBS文件。归档存储文件需要激活此选项，归档存储文件激活需要一定时间（归档存储文件加急恢复典型值在1~5分钟，详情请参考**对象恢复方式及耗时**）。首次单击右下角的“预览”可能超时，请再次重试单击“预览”。 **说明** – 周期任务首次开始扫描obs上文件，文件的最后修改时间区间范围是(周期首次运行时间-固定间隔时间，周期首次运行时间]。例如周期任务首次开始12:00:00，obs导入任务配置的固定时间间隔为10分钟，那么首次扫描出来的obs文件其最后修改时间在(11:50:00, 12:00:00]区间内，第二次周期12:10:00运行，则扫描出来的文件其最后修改时间在(12:00:00, 12:10:00]区间内。 – 一次性任务如果处理某个文件失败后，扫描出来的其余文件不会再被解析上报到LTS。 – 固定间隔任务关闭后重新开启，监控数据连续性最多保持一天。 – 固定间隔任务在某个周期时间内处理文件失败后，该周期时间内扫描出来的其余文件不会再被解析上报到LTS。
数据格式配置	日志文件编码	日志文件编码支持UTF-8、GBK。 UTF-8编码是一种变长编码方式，用于表示Unicode字符集。GBK全称《汉字内码扩展规范》，中文计算机编码的一种，是ASCII码和GB2312编码的扩展。

参数类型	名称	说明
	提取模式	根据日志类型选择提取模式，提取OBS日志超过1MB的部分会被截断丢弃。 **说明** • 单行日志单行超过1MB的部分被截断丢弃。 • 多行日志多行块超过1MB的部分被截断丢弃。 • ORC和JSON格式日志是单行解析，如果单行日志超过1MB直接被丢弃。 • 单行全文：采集完整的单行日志全文，不做结构化解析。如果您需要对日志做结构化解析，请在完成OBS文件导入配置后，请参考**设置云端结构化解析日志**设置。 • 多行全文：采集完整的多行日志全文（如堆栈日志），不做结构化解析。如果您需要对日志做结构化解析，请在完成OBS文件导入配置后，请参考**设置云端结构化解析日志**设置。 • ORC：采集ORC格式的日志。 不开启“自定义时间”时，使用日志被采集时间作为日志时间。 开启“自定义时间”时，可指定某一字段作为日志时间。填写时间字段Key名称、字段Value、时间格式，设置完成后，单击 校验。**如果导入的数据写入到css集群，LTS不支持ORC格式日志自定义两天前的时间。自定义时间格式请参考Oracle官网的时间匹配字符。** • JSON：采集JSON格式的日志。 不开启“自定义时间”时，使用日志被采集时间作为日志时间。 开启“自定义时间”时，可指定某一字段作为日志时间。填写时间字段Key名称、字段Value、时间格式，设置完成后，单击 校验。**如果导入的数据写入到css集群，LTS不支持JSON格式日志自定义两天前的时间。自定义时间格式请参考Oracle官网的时间匹配字符。** 设置json解析层数，取值范围为1~4，只能整数，默认值为1。将json格式日志的字段展开，例如原始日志为{"key1":{"key2":"value"}}，解析1层日志为：{"key1":{"key2":"value"}}，解析2层日志为：{"key1.key2":"value"}。

步骤7 设置完成后，单击右下角的“预览”。预览只扫描并返回符合条件的第一个文件的前10行内容。

步骤8 在结果预览下方查看结果，确认无误后，单击“提交”。

步骤9 接入成功后，则会生成一条接入配置信息。邀测期间，最多支持创建10个接入任务。

- 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。
- 单击接入配置操作列的“修改”重新修改接入配置信息。不支持修改导入间隔为一次性的任务。
- 单击接入配置操作列的“标签管理”即可添加标签。
- 单击接入配置操作列的“复制”复制一条新的接入配置信息。
- 单击接入配置操作列的“删除”即可删除接入配置信息。

  说明

  删除接入配置后会导致日志无法正常采集，可能会影响用户日志相关业务异常，且删除后无法恢复，请谨慎操作。
- 单击所属日志流的名称进入日志流详情页，即可对接入LTS的日志进行日志搜索分析。详细请参考**日志搜索与分析**。

----结束

4.3.30 虚拟私有云 VPC 接入 LTS

支持虚拟私有云VPC日志接入LTS。

前提条件

购买并使用华为云VPC实例。

使用限制

目前支持的弹性云服务器，请参见**VPC流日志简介**。

设置 VPC 接入

云日志服务接入方式为虚拟私有云 VPC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“接入 > 接入中心”，单击“虚拟私有云 VPC”进行VPC接入配置。

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”：VPC配置。

步骤4 单击“前往VPC配置”。具体的操作步骤及参数配置，请参见**创建VPC流日志**。

步骤5 单击下一步：日志流配置。

表 4-56 日志流配置参数表

参数	说明
自动对日志流进行结构化配置和索引配置	开启该按钮，日志流结构化配置为VPC系统模板，索引配置时将所有VPC解析出来的字段打开快速分析按钮。配置结构化和索引后，才能对VPC日志进行SQL分析，并提供可视化图表。
自动为日志流添加标签：log_type=vpc_flow	开启该按钮，自动为日志流添加标签log_type=vpc_flow后，VPC仪表盘模板才能匹配该日志流。
自动为日志流创建仪表盘	开启该按钮，自动为日志流创建VPC仪表盘。

步骤6 完成。

----结束

4.3.31 Web 应用防火墙 WAF 接入 LTS

支持Web应用防火墙 WAF接入LTS。

具体接入方法请参见**通过LTS记录WAF全量日志**。

4.4 使用 API 接入 LTS

4.4.1 API 接入概述

您可以通过调用云日志服务LTS提供的REST风格API将日志上报到LTS，具体有上报日志和上报高精度日志两个接口。

以下是两个接口的适用场景和各区域访问IP：

表 4-57 适用场景

API名称	日志时间	举例说明	适用场景

上报日志	用户调用API上传一批日志时，通过log_time_ns字段指定一个初始时间。
	每一条日志的日志时间，使用log_time_ns+顺序计数得到。
		{
		"log_time_ns": "1586850540000000000",
		"contents": [
		"log1",
		"log2"
		],
		"labels": {
		"user_tag": "string"
		}
		}
		上报到LTS后：
		log1的日志时间为：**1586850540000000000**
		log2的日志时间为：**1586850540000000001**
			上传的一批日志是在相近时间点、按顺序产生的。

上报高精度日志	用户调用API上传一批日志时，每一条日志都需要通过log_time_ns字段指定日志时间。	{
		"contents":[
		{
		"log_time_ns":"1586850540000000000",
		"log":"log3"
		},
		{
		"log_time_ns":"1586850540000000008",
		"log":"log4"
		}
		],
		"labels":{
		"user_tag":"string"
		}
		}
		上报到LTS后：
		log3的日志时间为：**1586850540000000000**
		log4的日志时间为：**1586850540000000008**
			上传的一批日志是在不同时间、非顺序产生的，希望每条日志的时间单独指定。

表 4-58 访问 IP（accessip）

区域	访问IP
华北-北京一	100.125.57.101
华北-北京二	100.125.6.108

区域	访问IP
华北-北京四	100.125.12.150
华东-上海一	100.125.11.177
华东-上海二	100.125.140.102
华南-广州	100.125.158.115
西南-贵阳一	100.125.0.27
华南-广州-友好用户环境	100.125.4.30
亚太-新加坡	100.125.4.58

说明

您可以在云日志服务控制台的安装ICAgent页面中的命令里获取访问IP（accessip），详细请参考**安装ICAgent（区域内主机）**。

4.4.2 上报日志接口参考

功能介绍

该接口用于主机上报租户日志给LTS。

接入点IP可在LTS控制台安装ICAgent的安装命令中获取，端口为8102，调用时使用该参数请参见**请求示例**。

说明

关于上报日志的约束与限制请参考**日志读写限制**。

URI

POST /v2/{project_id}/lts/groups/{log_group_id}/streams/{log_stream_id}/tenant/contents

表 4-59 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID，获取方式请参见：**获取账号ID、项目ID、日志组ID、日志流ID**。 缺省值：None 最小长度：32 最大长度：32

参数	是否必选	参数类型	描述
log_group_id	是	String	日志组ID，获取方式请参见：**获取账号ID、项目ID、日志组ID、日志流ID**。 缺省值：None 最小长度：36 最大长度：36
log_stream_id	是	String	日志流ID，获取方式请参见：**获取账号ID、项目ID、日志组ID、日志流ID**。 缺省值：None 最小长度：36 最大长度：36 **说明** 每个logstream写入速率最大不能超过100MB/S，超过此规格可能会导致日志丢失。

请求参数

表 4-60 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	从IAM获取的用户Token，获取方式请参见：**获取用户Token**。 缺省值：None 最小长度：1000 最大长度：2000
Content-Type	是	String	该字段填为：application/json;charset=UTF-8。 缺省值：None 最小长度：30 最大长度：30

表 4-61 请求 Body 参数

参数	是否必选	参数类型	描述
log_time_ns	是	Long	日志数据上报时间，UTC时间（纳秒）。 **说明** 通过接口上报日志到LTS的时间相距当前时间不超过2天，否则上报日志会被LTS删除。
contents	是	Array of String	日志内容。
labels	是	Object	用户自定义label。 **说明** 请不要将字段名称设置为**内置保留字段**，否则可能会造成字段名称重复、查询不精确等问题。
tenant_project_id	否	String	租户项目ID，获取方式请参见：**获取账号ID、项目ID、日志组ID、日志流ID**。

响应参数

状态码为 200 时:

表 4-62 响应 Body 参数

参数	参数类型	描述
errorCode	String	错误码。 枚举值： • SVCSTG.ALS.200.200
errorMessage	String	调用失败响应信息描述。 枚举值： • Report success.
result	String	响应结果。

状态码为 400 时:

表 4-63 响应 Body 参数

参数	参数类型	描述
errorCode	String	错误码。 枚举值： ● SVCSTG.ALS.200.201 ● SVCSTG.ALS.200.210
errorMessage	String	调用失败响应信息描述。 枚举值： ● Request conditions must be json format. ● projectid xxx log's quota has full.
result	String	响应结果。

状态码为 401 时:

表 4-64 响应 Body 参数

参数	参数类型	描述
errorCode	String	错误码。 枚举值： ● SVCSTG.ALS.403.105
errorMessage	String	调用失败响应信息描述。 枚举值： ● Project id is invalid.
result	String	响应结果。

状态码为 500 时:

表 4-65 响应 Body 参数

参数	参数类型	描述
errorCode	String	错误码。 枚举值： ● LTS.200500
errorMessage	String	调用失败响应信息描述。 枚举值： ● Internal error

参数	参数类型	描述
result	String	响应结果。

状态码为 503 时:

表 4-66 响应 Body 参数

参数	参数类型	描述
result	String	ServiceUnavailable。 被请求的服务无效，服务不可用。

请求示例

```
POST https://{接入点IP:8102}/v2/{project_id}/lts/groups/{log_group_id}/streams/{log_stream_id}/tenant/contents

{
    "log_time_ns": 1586850540000000000,
    "contents": [
        "Fri Feb  1 07:48:04 UTC 2019 0\n",
        "Sat Apri 18 16:04:04 UTC 2019"
    ],
    "labels": {
        "user_tag": "string"
    }
}
```

响应示例

状态码： 200

日志上报成功。

```
{
  "errorCode": "SVCSTG.ALS.200.200",
  "errorMessage": "Report success.",
  "result": null
}
```

状态码： 401

在客户端提供认证信息后，返回该状态码，表明服务端指出客户端所提供的认证信息不正确或非法。

```
{
  "errorCode" : "SVCSTG.ALS.403.105",
  "errorMessage" : "Project id is invalid.",
  "result": null
}
```


状态码

状态码	描述
200	请求响应成功。
400	BadRequest。非法请求。建议根据error_msg直接修改该请求，不要重试该请求。
401	在客户端提供认证信息后，返回该状态码，表明服务端指出客户端所提供的认证信息不正确或非法。
500	系统内部错误。
503	ServiceUnavailable。被请求的服务无效，服务不可用。

4.4.3 上报高精度日志接口参考

功能介绍

该接口用于主机上报租户日志给LTS。

接入点IP可在LTS控制台安装ICAgent的安装命令中获取，端口为8102，调用时使用该参数请参见**请求示例**。

说明

每次上报的时候， 每条日志都必须带一个纳秒级的时间戳。在LTS界面查看日志的时候， 会按照时间戳排序展示在页面上。关于上报日志的约束与限制请参考**日志读写限制**。

URI

POST /v2/{project_id}/lts/groups/{log_group_id}/streams/{log_stream_id}/tenant/contents/high-accuracy

表 4-67 路径参数

参数	是否必选	参数类型	描述
project_id	是	String	项目ID，获取方式请参见：**获取账号ID、项目ID、日志组ID、日志流ID**。 缺省值：None 最小长度：32 最大长度：32
log_group_id	是	String	日志组ID，获取方式请参见：**获取账号ID、项目ID、日志组ID、日志流ID**。 缺省值：None 最小长度：36 最大长度：36

参数	是否必选	参数类型	描述
log_stream_id	是	String	日志流ID，获取方式请参见：**获取账号ID、项目ID、日志组ID、日志流ID**。 缺省值：None 最小长度：36 最大长度：36 **说明** 每个logstream写入速率最大不能超过100MB/S，超过此规格可能会导致日志丢失。

请求参数

表 4-68 请求 Header 参数

参数	是否必选	参数类型	描述
X-Auth-Token	是	String	从IAM获取的用户Token，获取方式请参见：**获取用户Token**。 缺省值：None 最小长度：1000 最大长度：2000
Content-Type	是	String	该字段填为：application/json;charset=UTF-8。 缺省值：None 最小长度：30 最大长度：30
Content-Encoding	否	String	日志压缩格式 枚举值： • **GZIP** • **SNAPPY** • **gzip** • **snappy**

表 4-69 请求 Body 参数

参数	是否必选	参数类型	描述
contents	是	Array of **LogContents**	包含上报时间戳的日志内容列表。
labels	是	Object	用户自定义label。 **说明** 请不要将字段名称设置为**内置保留字段**，否则可能会造成字段名称重复、查询不精确等问题。
tenant_project_id	否	String	租户项目ID，获取方式请参见：**获取账号ID、项目ID、日志组ID、日志流ID**。

表 4-70 LogContents

参数	是否必选	参数类型	描述
log_time_ns	是	Long	日志数据上报时间，UTC时间（纳秒）。 **说明** 通过接口上报日志到LTS的时间相距当前时间不超过2天，否则上报日志会被LTS删除。
log	是	String	日志内容。

响应参数

状态码为 200 时:

表 4-71 响应 Body 参数

参数	参数类型	描述
errorCode	String	错误码。 枚举值： • SVCSTG.ALS.200.200
errorMessage	String	调用失败响应信息描述。 枚举值： • Report success.
result	String	响应结果。

状态码为 400 时:

表 4-72 响应 Body 参数

参数	参数类型	描述
errorCode	String	错误码。 枚举值: ● SVCSTG.ALS.200.201 ● SVCSTG.ALS.200.210
errorMessage	String	调用失败响应信息描述。 枚举值: ● Request conditions must be json format. ● projectid xxx log's quota has full.
result	String	响应结果。

状态码为 401 时:

表 4-73 响应 Body 参数

参数	参数类型	描述
errorCode	String	错误码。 枚举值: ● SVCSTG.ALS.403.105
errorMessage	String	调用失败响应信息描述。 枚举值: ● Project id is invalid.
result	String	响应结果。

状态码为 500 时:

表 4-74 响应 Body 参数

参数	参数类型	描述
errorCode	String	错误码。 枚举值: ● LTS.200500

参数	参数类型	描述
errorMessage	String	调用失败响应信息描述。 枚举值： ● Internal error
result	String	响应结果。

状态码为 503 时:

表 4-75 响应 Body 参数

参数	参数类型	描述
result	String	ServiceUnavailable。 被请求的服务无效，服务不可用。

请求示例

```
POST https://{接入点IP:8102}/v2/{project_id}/lts/groups/{log_group_id}/streams/{log_stream_id}/tenant/contents/high-accuracy

{
   "contents": [
      {
         "log_time_ns": 1586850540000000000,
         "log": "Fri Feb  15 15:48:04 UTC 2019"
      },
      {
         "log_time_ns": 1586850540000000001,
         "log": "Sat Apri 18 16:04:04 UTC 2019"
      }
   ],
   "labels": {
      "user_tag": "string"
   }
}
```

响应示例

状态码： 200

日志上报成功。

```
{
  "errorCode": "SVCSTG.ALS.200.200",
  "errorMessage": "Report success.",
  "result": null
}
```

状态码： 401

在客户端提供认证信息后，返回该状态码，表明服务端指出客户端所提供的认证信息不正确或非法。

```
{
  "errorCode" : "SVCSTG.ALS.403.105",
```



```
  "errorMessage" : "Project id is invalid.",
  "result": null
}
```

状态码

状态码	描述
200	请求响应成功。
400	BadRequest。非法请求。建议根据error_msg直接修改该请求，不要重试该请求。
401	在客户端提供认证信息后，返回该状态码，表明服务端指出客户端所提供的认证信息不正确或非法。
500	系统内部错误。
503	ServiceUnavailable。被请求的服务无效，服务不可用。

4.5 跨 IAM 账号接入 LTS

当您选择了跨账号接入-日志流映射方式时，通过创建委托，您可以将委托账号的日志流映射到被委托方账号的日志流下，被委托账号即当前云日志服务登录账号。

说明

跨账号接入成功后，如果账号A在IAM上删除委托，则云日志服务无法感知到该委托被删除，配置的跨账号接入依然生效；如果您不再使用跨账号接入功能，可直接通知账号B删除接入配置。

前提条件

已创建委托关系。

限制条件

数据未同步完成前，目标日志流数据与源日志流可能会有一定偏差。建议1小时后，查看接入数据。

设置跨账号接入

日志服务接入方式选择跨账号接入时，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“接入 > 接入中心”，单击“跨账号接入-日志流映射”进行跨账号接入配置。

或在左侧导航栏中，选择“接入 > 接入管理 > 接入日志”，单击“跨账号接入-日志流映射”进行跨账号接入配置。

或在左侧导航栏中，选择“日志管理”，单击目标日志流的名称进入日志详情页面。

单击右上角  ，在弹出页面中，选择“日志接入”页签，单击“接入日志”，在弹出页面中，单击“跨账号接入-日志流映射”进行跨账号接入配置。

步骤3 选择委托。

配置相关参数，请参见**表4-76**，完成后，单击“下一步：日志流映射”。

表 4-76 委托参数配置

参数	说明
委托名称	填写委托人在IAM中创建的委托名称。委托人账号可通过**创建委托**将资源管理权限委托给其他华为云账号。
委托人账号名称	创建委托时的账号名称，用来验证委托关系。

说明

- 委托账号和被委托账号需是不同租户。
- 被委托账号必须要授权Agent Operator系统角色，用于被委托账号在使用LTS委托功能时进行委托校验。

步骤4 日志流映射。

在日志流映射页面，配置接入规则，有两种方式：自动配置和手动配置。

- **自动配置**
  a. 在日志流映射页面，单击“自动配置”。
  b. 在弹出的自动配置页面中，配置相关参数信息，完成后，单击“确定”。

表 4-77 自动配置接入规则

参数	说明
规则名称前缀	填写规则名称前缀，自动配置将使用您配置的规则名称前缀，产生多条接入规则。 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。可不填写，默认规则名称前缀为rule。
从委托账号中选择您希望接入的日志组/日志流	选择希望接入的日志组/日志流，最多支持选择20条。

说明

通过自动配置的接入规则，被委托方中的目标日志组、目标日志流名称默认同委托方中源日志组、源日志流名称保持一致，也支持手动修改。

  c. 单击“预览”，查看预览结果。

说明

1. 预览结果有两种：
   - **将创建新的目标日志流**：被委托方中新建的目标日志组/日志流。
   - **接入已存在的目标日志流**：被委托方中已存在的目标日志组/日志流。
2. 预览报错情况如下：
   - 源日志流xxx，已配置为目标日志流。
   - 目标日志流xxx，已配置为源日志流。
   - 目标日志流xxx，已存在于其它日志组。
   - 目标日志流xxx，存在于不同目标日志组。
   - 规则名称重复。
   - 源日志流xxx，已存在映射关系。
   - 日志组数量已达上限，请选择存在的日志组进行接入。

   当提示以上报错时，须删除日志流对应的接入规则。

d. 预览完成后，单击“提交”。

- **手动配置**

a. 在日志流映射页面，单击“添加规则”，参考表4-78设置规则。

表 4-78 参数说明

参数		说明
规则名称		默认为rule_xxx，也可根据您的需要进行自主命名。 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。
委托方	源日志组	委托方的日志组，在原有的日志组中进行选择。
	源日志流	委托方的日志流，在原有的日志流中进行选择。
被委托方	目标日志组	被委托方的日志组，可在原有的日志组中进行选择或直接输入名称进行新建日志组。
	目标日志流	被委托方的日志流，可在原有的日志流中进行选择或直接输入名称进行新建日志流。

b. 单击“预览”，查看预览结果。

说明

1. 预览结果有两种：
   - **将创建新的目标日志流**：被委托方中新建的目标日志组/日志流。
   - **接入已存在的目标日志流**：被委托方中已存在的目标日志组/日志流。
2. 预览报错情况有五种：
   - 源日志流xxx，已配置为目标日志流。
   - 目标日志流xxx，已配置为源日志流。
   - 目标日志流xxx，已存在于其它日志组。
   - 目标日志流xxx，存在于不同目标日志组。
   - 规则名称重复。
   - 源日志流xxx，已存在映射关系。
   - 日志组/日志流超过最大创建条数。

   当提示以上报错时，须删除日志流对应的接入规则。

c. 预览完成后，单击“提交”，等待创建日志接入成功。

步骤5 配置接入完成。

说明

配置完成后，数据将会在1小时内完成同步，请您耐心等待。

- 当接入多个日志流时，单击“返回接入配置列表”可查看日志接入列表。
- 当接入单个日志流时，单击“返回接入配置列表”可查看日志接入列表；单击“查看日志流”可查看已接入的日志详情。

----结束

4.6 使用 KAFKA 协议上报日志到 LTS

您可以通过Kafka协议上报日志到日志服务，目前支持各类Kafka Producer SDK或采集工具，仅依赖于Kafka协议。支持以下场景：

- **场景1**：已有基于开源采集的自建系统，仅修改配置文件便可以将日志上报到LTS，例如Logstash。
- **场景2**：希望通过 Kafka producer SDK 来采集日志并上报，不必再安装采集ICAgent。

说明

目前此功能仅支持华北-北京四、华南-广州、华东-上海一、华东-上海二、亚太-新加坡，其他局点需要**提交工单**申请使用。

前提条件

- 使用云日志SDK前，您需要注册用户账号，并开通云日志服务。
- 确认云日志服务的区域，请用户根据所在区域，获取regionid。
- **如何获取访问密钥AK/SK**。
- 获取华为云账号的项目ID（project id），详情请参见“我的凭证 >**API凭证**”。

- 获取需要上报到LTS的日志组ID、日志流ID。
- 当前仅支持内网上报，需要在ECS主机上使用。

相关限制

- 当前仅支持内网上报，端口固定为9095，IP根据所在局点进行配置。
- 支持 Kafka 协议版本为：1.0.X，2.X.X，3.X.X。
- 支持压缩方式：gzip，snappy，lz4。
- KAFKA认证方式为 SASL_PLAINTEXT 认证。
- KAFKA协议的ACKS参数必须设置为0。

配置方式

- 使用Kafka协议上报日志时，需要使用到的通用参数如下。

表 4-79 通用参数

参数名称	描述	类型
projectId	用户账号的项目ID（project id）	String
logGroupId	LTS的日志组ID	String
logStreamId	LTS的日志流ID	String
regionName	云日志服务的区域	String
accessKey	用户账号的AK	String
accessSecret	用户账号的SK	String

- 使用Kafka协议上报日志时，需要配置以下参数。

表 4-80 配置参数

参数名称	说明
连接类型	当前支持SASL_PLAINTEXT
hosts	Kafka的IP和PORT地址，格式为lts-kafka.${regionName}.${external_global_domain_name}:9095或lts-access.${regionName}.${external_global_domain_name}:9095 其中IP根据局点进行配置，PORT固定为9095。详细请参考**参数获取方式**，例如北京四局点对应hosts为 lts-kafka.cn-north-4.myhuaweicloud.com:9095。
topic	Kafka的topic名称，格式为 ${日志组ID}_${日志流ID}，即LTS的日志组ID和日志流ID通过下划线连接，作为topic的名称。
username	Kafka访问用户名，配置为用户账号的项目ID。

参数名称	说明
password	Kafka访问密码，格式为${accessKey}#${accessSecret}，即用户账号的AK和SK通过#连接，作为Kafka的访问密码。
headers	设置自定义label字段时，需要配置headers。 headers中添加header，key值为LTS_LOG_TYPE，value值为FORMAT，用户需要上报符合要求的规范化日志。

- ${message}日志格式

  仅当headers中添加了key为LTS_LOG_TYPE，value为FORMAT的header时，日志需要符合该格式规范。

  表 4-81 日志参数

参数名称	是否必选	参数类型	描述
tenant_project_id	是	String	用户账号的项目ID。
tenant_group_id	是	String	LTS的日志组ID。
tenant_stream_id	是	String	LTS的日志流ID。
log_time_ns	是	Long	日志数据采集时间，UTC时间（纳秒）。 **说明** 采集时间需在日志存储时间范围之内，否则上报日志会被删除。比如日志组的日志存储时间是7天，则此参数不应早于当前时间的7天前。
contents	是	Array of String	日志内容。
labels	是	Object	用户自定义label。 **说明** 请不要将字段名称设置为**内置保留字段**，否则可能会造成字段名称重复、查询不精确等问题。

日志示例

```
{
  "tenant_project_id": "${projectId}",
  "tenant_group_id": "${logGroupId}",
  "tenant_stream_id": "${logStreamId}",
  "log_time_ns": "XXXXXXXXXXXXXXXXXX",
  "contents": [
     "This is a log 1",
     "This is a log 2"
  ],
  "labels": {
     "type": "kafka"
```

```
  }
}
```

调用示例

1. Beat系列软件调用（ FileBeat等 ）。以FileBeat为例，配置参数如下：

```
output.kafka:
hosts: ["${ip}:${port}"]
partition.round_robin:
reachable_only: false
username: "${projectId}"
password: "${accessKey}#${accessSecret}"
topic: "${logGroupId}_${logStreamId}'"
sasl.mechanism: "PLAIN"
security.protocol: "SASL_PLAINTEXT"
acks: "0"
compression: gzip
```

2. 通过Logstash软件上报日志。

```
input {
stdin {}
}
output {
kafka {
# 配置地址
bootstrap_servers => "${ip}:${port}"
# 配置topic
topic_id => "${logGroupId}_${logStreamId}"
# 配置消息确认机制
acks => "0"
# 配置压缩方式
compression_type => "gzip"
# 配置认证方式
security_protocol => "SASL_PLAINTEXT"
sasl_mechanism => "PLAIN"
# 用户名 projectId 密码 accessKey#accessSecret
sasl_jaas_config => "org.apache.kafka.common.security.plain.PlainLoginModule required username='$
{projectId}' password='${accessKey}#${accessSecret}';"
}
}
```

3. 通过Flume软件上报日志。

```
#Name
a1.sources = r1
a1.channels = c1
a1.sinks = k1
#Source
a1.sources.r1.type = TAILDIR
a1.sources.r1.channels = c1
a1.sources.r1.filegroups = f1
a1.sources.r1.filegroups.f1 = /tmp/test.txt
a1.sources.r1.fileHeader = true
a1.sources.r1.maxBatchCount = 1000
#Channel
a1.channels.c1.type = memory
a1.channels.c1.capacity = 10000
a1.channels.c1.transactionCapacity = 100
#Sink
a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";
#Bind
a1.sources.r1.channels = c1
a1.sinks.k1.channel = c1
```

SDK 调用示例

1. Java SDK调用示例。

   maven依赖（示例kafka协议版本为2.7.1）：

```
<dependencies>
    <dependency>
        <groupId>org.apache.kafka</groupId>
        <artifactId>kafka-clients</artifactId>
        <version>2.7.1</version>
    </dependency>
</dependencies>
```

   代码示例：

```
package org.example;
import org.apache.kafka.clients.producer.KafkaProducer;
import org.apache.kafka.clients.producer.Producer;
import org.apache.kafka.clients.producer.ProducerRecord;
import java.util.Properties;
public class ProducerDemo {
public static void main(String[] args) {
Properties props = new Properties();
// 配置地址
props.put("bootstrap.servers", "${ip}:${port}");
// 配置消息确认机制
props.put("acks", "0");
// 配置认证方式
props.put("security.protocol", "SASL_PLAINTEXT");
props.put("sasl.mechanism", "PLAIN");
// 用户名 projectId 密码 accessKey#accessSecret
props.put("sasl.jaas.config",
"org.apache.kafka.common.security.plain.PlainLoginModule required username='${projectId}'
password='${accessKey}#${accessSecret}';");
// 配置压缩方式
props.put("compression.type", "${compress_type}");
props.put("key.serializer", "org.apache.kafka.common.serialization.StringSerializer");
props.put("value.serializer", "org.apache.kafka.common.serialization.StringSerializer");
// 1.创建一个生产者对象
Producer<String, String> producer = new KafkaProducer<>(props);
// 2.调用send方法
for (int i = 0; i < 1; i++) {
ProducerRecord record = new ProducerRecord<>("${logGroupId}_${logStreamId}", "${message}");
// 配置recordHeader
// record.headers().add(new RecordHeader("LTS_LOG_TYPE","FORMAT".getBytes()));
producer.send(record);
}
// 3.关闭生产者
producer.close();
}
}
```

2. Python SDK调用示例。

```
from kafka import KafkaProducer
producer = KafkaProducer(
# 配置地址
bootstrap_servers="${ip}:${port}",
# 配置消息确认机制
acks="0",
# 配置压缩方式
compression_type ="${compression_type}"
# 配置认证方式
sasl_mechanism="PLAIN",
security_protocol="SASL_PLAINTEXT",
# 用户名 projectId 密码 accessKey#accessSecret
sasl_plain_username="${projectId}",
sasl_plain_password="${accessKey}#${accessSecret}"
)
print('start producer')
for i in range(0, 3):
```



```
    data = bytes("${message}", encoding="utf-8")
    future = producer.send("${logGroupId}_{logStreamId}", data)
    result = future.get(timeout=10)
    print(result)
print('end producer')
```

报错说明

当参数错误或不匹配时，会有相应的报错提示。

表 4-82 报错说明

报错信息	报错原因
TopicAuthorizationException	projectId（项目ID）、accessKey（AK）、accessSecret（SK）参数错误或者不匹配。
UnknownTopicOrPartitionException	logGroupId（日志组ID）、logStreamId（日志流ID）参数错误或者不匹配。
InvalidRecordException	仅当配置headers，上报规范化日志时，会出现此类报错： 日志格式错误或者日志中的projectId（项目ID）、logGroupId（日志组ID）、logStreamId（日志流ID）与外部设置参数不一致。

参数获取方式

表 4-83 区域表

区域名称	RegionName
华北-北京四	lts-kafka.cn-north-4.myhuaweicloud.com
华东-上海一	lts-access.cn-east-3.myhuaweicloud.com
华东-上海二	lts-kafka.cn-east-2.myhuaweicloud.com
华南-广州	lts-access.cn-south-1.myhuaweicloud.com
亚太-新加坡	lts-kafka.ap-southeast-3.myhuaweicloud.com

4.7 使用 Flume 采集器上报日志到 LTS

Flume是一个高可用的，高可靠的，分布式的海量日志采集、聚合和传输的系统，Flume支持在日志系统中定制各类数据发送方，用于收集数据；同时，Flume提供对数据进行简单处理，并写到各种数据接受方的能力。

用户使用Flume系统采集日志，并且通过LTS侧提供的KAFKA协议方式上报日志。以下是部分常用数据采集场景示例：

1. **使用Flume采集文本日志上报到LTS**

2. **使用Flume采集数据库表数据并且上报至LTS**
3. **使用Flume采集syslog协议传输的日志上报到LTS**
4. **通过Flume采集TCP/UDP协议传输的日志上报到LTS**
5. **通过Flume采集SNMP协议上报的设备管理数据并发送到LTS**
6. **使用默认拦截器处理日志**
7. **自定义拦截器处理日志**
8. **使用外部数据源丰富日志内容并上报到LTS**

前提条件

- 用户机器已经安装了JDK。
- 用户已经安装Flume，并且需要在Flume中配置文件中配置JDK路径。

使用 Flume 采集文本日志上报到 LTS

支持使用Flume采集文本日志内容上报至LTS，参考如下示例添加采集文本日志的conf文件。以下示例中的参数介绍请参考**使用KAFKA协议上报日志**。

```
#Named
a1.sources = r1
a1.channels = c1
a1.sinks = k1

#Source
a1.sources.r1.type = TAILDIR
a1.sources.r1.channels = c1
a1.sources.r1.filegroups = f1
a1.sources.r1.filegroups.f1 = /tmp/test.txt
a1.sources.r1.fileHeader = true
a1.sources.r1.maxBatchCount = 1000

#Channel
a1.channels.c1.type = memory
a1.channels.c1.capacity = 10000
a1.channels.c1.transactionCapacity = 100

#Sink
a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";

#Bind
a1.sources.r1.channels = c1
a1.sinks.k1.channel = c1
```

使用 Flume 采集数据库表数据并且上报至 LTS

使用Flume采集数据库表数据并且上报至LTS，实现对表数据变动监控。以下示例中的参数介绍请参考**使用KAFKA协议上报日志**。

步骤1 在**https://github.com/keedio/flume-ng-sql-source**页面下载flume-ng-sql-source插件，转换为jar包并取名为flume-ng-sql-source.jar，打包前注意将pom文件中的flume-ng-core 版本与flume安装版本保持一致，并且将jar包放在安装Flume包路径的

lib目录下面，例如**FLUME_HOME/lib**目录下（例子中的**FLUME_HOME**为Flume安装路径，仅供参考，请以实际安装路径为准）。

步骤2 添加MySQL驱动到**FLUME_HOME/lib**目录下：

1. 下载MySQL驱动。
   ```
   wget https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-java-5.1.35.tar.gz
   ```
2. 将驱动包解压并打为jar包。
   ```
   tar xzf mysql-connector-java-5.1.35.tar.gz
   ```
3. 将jar包存放在FLUME_HOME/lib/路径。
   ```
   cp mysql-connector-java-5.1.35-bin.jar  FLUME_HOME/lib/
   ```

步骤3 添加采集MySQL的conf文件。

```
# a1表示agent的名称
# source是a1的输入源
# channels是缓冲区
# sinks是a1输出目的地，本例子sinks使用了kafka
a1.channels = c1
a1.sources = r1
a1.sinks = k1

#source
a1.sources.r1.type = org.keedio.flume.source.SQLSource
# 连接mysql的一系列操作，{mysql_host}改为您虚拟机的ip地址，可以通过ifconfig或者ip addr查看,
{database_name}改为数据库名称
# url中要加入?useUnicode=true&characterEncoding=utf-8&useSSL=false，否则有可能连接失败
a1.sources.r1.hibernate.connection.url = jdbc:mysql://{mysql_host}:3306/{database_name}?
useUnicode=true&characterEncoding=utf-8&useSSL=false
# Hibernate Database connection properties
# mysql账号，一般都是root
a1.sources.r1.hibernate.connection.user = root
# 填入您的mysql密码
a1.sources.r1.hibernate.connection.password = xxxxxxxx
a1.sources.r1.hibernate.connection.autocommit = true
# mysql驱动
a1.sources.r1.hibernate.dialect = org.hibernate.dialect.MySQL5Dialect
a1.sources.r1.hibernate.connection.driver_class = com.mysql.jdbc.Driver
# 存放status文件
a1.sources.r1.status.file.path = FLUME_HOME/bin
a1.sources.r1.status.file.name = sqlSource.status
# Custom query
# 填写需要采集的数据表名{table_name}，也可以使用下面的方法：
a1.sources.r1.custom.query = select * from {table_name}


#Sink
a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";


a1.channels.c1.type = memory
a1.channels.c1.capacity = 10000
a1.channels.c1.transactionCapacity = 10000
a1.channels.c1.byteCapacityBufferPercentage = 20
a1.channels.c1.byteCapacity = 800000
```

步骤4 启动Flume后，即可开始采集数据库中的表数据到LTS。

----结束

使用 Flume 采集 syslog 协议传输的日志上报到 LTS

Syslog协议是一种用于在IP网络中传输日志消息的协议，通过Flume将syslog协议传输的日志采集并上报到LTS。以下示例中的参数介绍请参考**使用KAFKA协议上报日志**。

- 接收UDP日志，参考如下示例添加采集Syslog协议的conf文件。

```
a1.sources = r1
a1.sinks = k1
a1.channels = c1

a1.sources.r1.type=syslogudp
#host_port为syslog服务器的端口
a1.sources.r1.port = {host_port}
#host_ip为syslog服务器的ip地址
a1.sources.r1.host = {host_ip}
a1.sources.r1.channels = c1

a1.channels.c1.type = memory

#Sink
a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule required username="${projectId}" password="${accessKey}#${accessSecret}";
a1.sinks.k1.channel = c1
```

- 接收TCP日志，参考如下示例添加采集Syslog协议的conf文件。

```
a1.sources = r1
a1.sinks = k1
a1.channels = c1

a1.sources.r1.type=syslogtcp
#host_port为syslog服务器的端口
a1.sources.r1.port = {host_port}
#host_ip为syslog服务器的ip地址
a1.sources.r1.host = {host_ip}
a1.sources.r1.channels = c1

a1.channels.c1.type = memory

#Sink
a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule required username="${projectId}" password="${accessKey}#${accessSecret}";
a1.sinks.k1.channel = c1
```

通过 Flume 采集 TCP/UDP 协议传输的日志上报到 LTS

通过Flume采集TCP/UDP协议传输的日志上报到LTS。以下示例中的参数介绍请参考**使用KAFKA协议上报日志**。

- 采集TCP端口日志，参考如下示例添加采集端口的conf文件。

```
a1.sources = r1
a1.sinks = k1
a1.channels = c1
```



```
a1.sources.r1.type = netcat
a1.sources.r1.bind = 0.0.0.0
a1.sources.r1.port = {host_port}

a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";

a1.channels.c1.type = memory
a1.channels.c1.capacity = 1000
a1.channels.c1.transactionCapacity = 100

a1.sources.r1.channels = c1
a1.sinks.k1.channel = c1
```

- 采集UDP端口日志，参考如下示例添加采集端口的conf文件。

```
a1.sources = r1
a1.sinks = k1
a1.channels = c1

a1.sources.r1.type = netcatudp
a1.sources.r1.bind = 0.0.0.0
a1.sources.r1.port = {host_port}

a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";

a1.channels.c1.type = memory
a1.channels.c1.capacity = 1000
a1.channels.c1.transactionCapacity = 100

a1.sources.r1.channels = c1
a1.sinks.k1.channel = c1
```

通过 Flume 采集 SNMP 协议上报的设备管理数据并发送到 LTS

通过Flume采集SNMP协议上报的设备管理数据并发送到LTS。以下示例中的参数介绍请参考**使用KAFKA协议上报日志**。

- 监听SNMP协议通信端口号161。参考如下示例添加SNMP协议接受日志的conf。

```
a1.sources = r1
a1.sinks = k1
a1.channels = c1

a1.sources.r1.type = netcatudp
a1.sources.r1.bind = 0.0.0.0
a1.sources.r1.port = 161

a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
```



```
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";

a1.channels.c1.type = memory
a1.channels.c1.capacity = 1000
a1.channels.c1.transactionCapacity = 100

a1.sources.r1.channels = c1
a1.sinks.k1.channel = c1
```

- 监听SNMP协议陷阱(Trap)通信的端口号162，参考如下示例添加SNMP协议接受日志的conf。

```
a1.sources = r1
a1.sinks = k1
a1.channels = c1



a1.sources.r1.type = netcatudp
a1.sources.r1.bind = 0.0.0.0
a1.sources.r1.port = 162



a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";

a1.channels.c1.type = memory
a1.channels.c1.capacity = 1000
a1.channels.c1.transactionCapacity = 100

a1.sources.r1.channels = c1
a1.sinks.k1.channel = c1
```

使用默认拦截器处理日志

使用Flume采集器时，拦截器是简单的插件式组件，设置在Source和Channel之间。Source接收到的事件Event，在写入Channel之前，拦截器都可以进行转换或者删除这些事件。每个拦截器只处理同一个Source接收到的事件。

- 时间戳拦截器

  该拦截器的作用是将时间戳插入到flume的事件报头中。如果不使用任何拦截器，flume接收到的只有message。时间戳拦截器的配置， 参数默认值描述type，类型名称timestamp，也可以使用类名的全路径preserveExisting为false。如果设置为true，若事件中报头已经存在，不会替换时间戳报头的值。source连接到时间戳拦截器的配置：

  ```
  a1.sources.r1.interceptors = timestamp
  a1.sources.r1.interceptors.timestamp.type=timestamp
  a1.sources.r1.interceptors.timestamp.preserveExisting=false
  ```

- 正则过滤拦截器

  在日志采集的时候，可能有一些数据是不需要的，添加过滤拦截器可以过滤掉不需要的日志，也可以根据需要收集满足正则条件的日志。参数默认值描述type，类型名称REGEX_FILTER。excludeEvents为false时默认收集匹配到的事件。如果为true，则会删除匹配到的event，收集未匹配到的。source连接到正则过滤拦截器的配置：

  ```
  a1.sources.r1.interceptors = regex
  a1.sources.r1.interceptors.regex.type=REGEX_FILTER
  ```



```
a1.sources.r1.interceptors.regex.regex=(today)|(Monday)
a1.sources.r1.interceptors.regex.excludeEvents=false
```

这样配置的拦截器就只会接收日志消息中带有today或者Monday的日志。

- 搜索并替换拦截器

  拦截器基于Java正则表达式提供简单的基于字符串的搜索和替换功能。配置如下：

```
# 拦截器别名
a1.sources.r1.interceptors = search-replace
# 拦截器类型，必须是search_replace
a1.sources.r1.interceptors.search-replace.type = search_replace

# 删除事件正文中的字符，根据正则匹配event内容
a1.sources.r1.interceptors.search-replace.searchPattern = today
# 替换匹配到的event内容
a1.sources.r1.interceptors.search-replace.replaceString = yesterday
# 设置字符集，默认是utf8
a1.sources.r1.interceptors.search-replace.charset = utf8
```

自定义拦截器处理日志

在Flume中自定义拦截器的方式主要流程如下（以java语言为例），以下示例中的FLUME_HOME表示Flume的安装路径，例如/tools/flume（仅供参考），实际配置的时候，请以用户安装Flume的实际路径为准。

步骤1 创建MAVEN工程项目，引入Flume依赖。

根据集群中的 Flume 版本，引入 Flume 依赖，如下所示：

```
<dependencies>
      <dependency>
         <groupId>org.apache.flume</groupId>
         <artifactId>flume-ng-core</artifactId>
         <version>1.10.1</version>
         <scope>provided</scope>
      </dependency>
  </dependencies>
```

无需将该依赖打包进最后的JAR包中，故将其作用域设置为provided。

步骤2 创建类实现拦截器接口Interceptor，并且实现相关方法。

- initialize() 方法：初始化拦截器操作，读取配置信息、建立连接等。
- intercept(Event event) 方法：用于拦截单个事件，并对事件进行处理。接收一个事件对象作为输入，并返回一个修改后的事件对象。
- intercept(List<Event> list) 方法：事件批处理，拦截事件列表，并对事件列表进行处理。
- close() 方法：关闭拦截器，在这里释放资源、关闭连接等。

```
import org.apache.flume.Event;
import org.apache.flume.interceptor.Interceptor;

import java.nio.charset.StandardCharsets;
import java.util.ArrayList;
import java.util.List;

public class TestInterceptor implements Interceptor {
   @Override
   public void initialize() {

   }
   @Override
   public Event intercept(Event event) {
```



```
        // 获取事件数据
        String eventData = new String(event.getBody(), StandardCharsets.UTF_8);
        // 检查事件数据中是否包含指定字符串
        if (eventData.contains("hello")) {
            // 如果包含指定字符串，则过滤掉该事件，返回 null
            return null;
        }

        return event;
    }

    @Override
    public List<Event> intercept(List<Event> events) {
        // 创建一个新的列表，存储处理过后的事件
        List<Event> interceptedEvents = new ArrayList<>();
        for (Event event : events) {
            Event interceptedEvent = intercept(event);
            if (interceptedEvent != null) {
                interceptedEvents.add(interceptedEvent);
            }
        }
        return interceptedEvents;
    }

    @Override
    public void close() {

    }

}
```

步骤3 构建拦截器，拦截器的创建和配置通常是通过 Builder 模式来完成的，完整的代码如下所示：

```
import org.apache.flume.Context;
import org.apache.flume.Event;
import org.apache.flume.interceptor.Interceptor;

import java.nio.charset.StandardCharsets;
import java.util.ArrayList;
import java.util.List;

public class TestInterceptor implements Interceptor {
    @Override
    public void initialize() {
    }
    @Override
    public Event intercept(Event event) {
        // 获取事件数据
        String eventData = new String(event.getBody(), StandardCharsets.UTF_8);
        // 检查事件数据中是否包含指定字符串
        if (eventData.contains("hello")) {
            // 如果包含指定字符串，则过滤掉该事件，返回 null
            return null;
        }
        return event;
    }
    @Override
    public List<Event> intercept(List<Event> events) {
        List<Event> interceptedEvents = new ArrayList<>();
        for (Event event : events) {
            Event interceptedEvent = intercept(event);
            if (interceptedEvent != null) {
                interceptedEvents.add(interceptedEvent);
            }
        }
        return interceptedEvents;
    }
```



```
    @Override
    public void close() {

    }

    // 拦截器构建
    public static class Builder implements Interceptor.Builder {

        @Override
        public void configure(Context context) {

        }

        @Override
        public Interceptor build() {
            return new TestInterceptor();
        }

    }

}
```

步骤4 转换为jar包，并且将其上传至Flume安装路径下的lib文件夹下（请以用户安装Flume的实际路径为准）。

步骤5 编写配置文件，需要将自定义的拦截器配置进去。

拦截器全类名配置时需要注意，格式为拦截器的全类名 + $Builder。

```
# 拦截器配置
# 拦截器定义
a1.sources.r1.interceptors = i1
# 拦截器全类名
a1.sources.r1.interceptors.i1.type = TestInterceptor$Builder
```

步骤6 运行Flume即可。

----结束

KV解析日志：用空格分隔字符串并且转换为Map类型字符串。

```
public class TestInterceptor implements Interceptor {
    @Override
    public void initialize() {
    }

    @Override
    public Event intercept(Event event) {
        // 获取事件数据
        String eventData = new String(event.getBody(), StandardCharsets.UTF_8);
        Map<String, Object> splitMap = new HashMap<>();
        String[] splitList = eventData.split(" ");
        for (int i = 0; i < splitList.length; i++) {
            splitMap.put("field" + i, splitList[i].trim());
        }
        eventData.setBody(splitMap.toString().getBytes(StandardCharsets.UTF_8));
        return event;
    }

    @Override
    public List<Event> intercept(List<Event> events) {
        List<Event> interceptedEvents = new ArrayList<>();
        for (Event event : events) {
            Event interceptedEvent = intercept(event);
            if (interceptedEvent != null) {
                interceptedEvents.add(interceptedEvent);
            }
        }
        return interceptedEvents;
    }
```



```
    @Override
    public void close() {
    }
}
```

使用外部数据源丰富日志内容并上报到 LTS

Flume数据传输的基本单元，以Event的形式将数据从源头传输至目的地。Event由Header和Body两部分组成，Header用来存放该Event的一些属性，为K-V结构，Body用来存放该条数据，形式为字节数组。

有外部数据源时，如果您需要丰富日志内容，例如修改日志内容、添加字段、删除内容等操作，将修改内容添加至Event的body中，Flume才能将日志内容上报到LTS。例如使用Java自定义扩展日志内容。以下示例中的参数介绍请参考**使用KAFKA协议上报日志**。

```
import com.alibaba.fastjson.JSONObject;

import org.apache.flume.Context;
import org.apache.flume.Event;
import org.apache.flume.interceptor.Interceptor;

import java.nio.charset.StandardCharsets;
import java.util.ArrayList;
import java.util.List;

public class TestInterceptor implements Interceptor {
    @Override
    public void initialize() {
    }

    @Override
    public Event intercept(Event event) {
        // 获取事件数据，将原数据转换为json字符串并且添加额外字段
        String eventData = new String(event.getBody(), StandardCharsets.UTF_8);
        JSONObject object = new JSONObject();
        object.put("content", eventData);
        object.put("workLoadType", "RelipcaSet");
        eventData = object.toJSONString();
        eventData.setBody(eventData.getBytes(StandardCharsets.UTF_8));
        return event;
    }

    @Override
    public List<Event> intercept(List<Event> events) {
        List<Event> interceptedEvents = new ArrayList<>();
        for (Event event : events) {
            Event interceptedEvent = intercept(event);
            if (interceptedEvent != null) {
                interceptedEvents.add(interceptedEvent);
            }
        }
        return interceptedEvents;
    }

    @Override
    public void close() {
    }
}
```


5 日志搜索与分析

5.1 日志搜索与分析概述

日志搜索与分析是运维中不可或缺的一环。日志接入成功后，云日志服务（LTS）支持对采集成功的日志数据进行搜索与分析。通过合理的日志收集、高效的搜索方法和专业的分析工具，可以实现对系统或应用的全面监控和精细化管理。

- 执行搜索与分析前，需要将上报的日志进行结构化配置和索引配置，因为结构化后数据具有严格的长度和格式，方便进行搜索与分析。详细请参考**设置云端结构化解析日志**和**设置LTS日志索引配置**。
- 结构化完成后，使用云日志服务（LTS）提供的**搜索语法**用于设置搜索条件，帮助您更有效地搜索日志。详细请参考**搜索日志**。
- 云日志服务（LTS）支持使用**SQL分析语法**，对结构化后的日志字段进行日志分析，通过统计图表的方式对查询和分析的结果进行可视化展示。详细请参考**分析LTS日志**。

5.2 设置云端结构化解析日志

5.2.1 日志结构化概述

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，以便对结构化后的日志按照SQL语法进行查询与分析。

日志结构化解析是一种将日志数据从非结构化或半结构化形式转换为结构化格式的过程，以便于更好地存储、查询和分析，提高日志数据的可读性、可搜索性和查询效率。

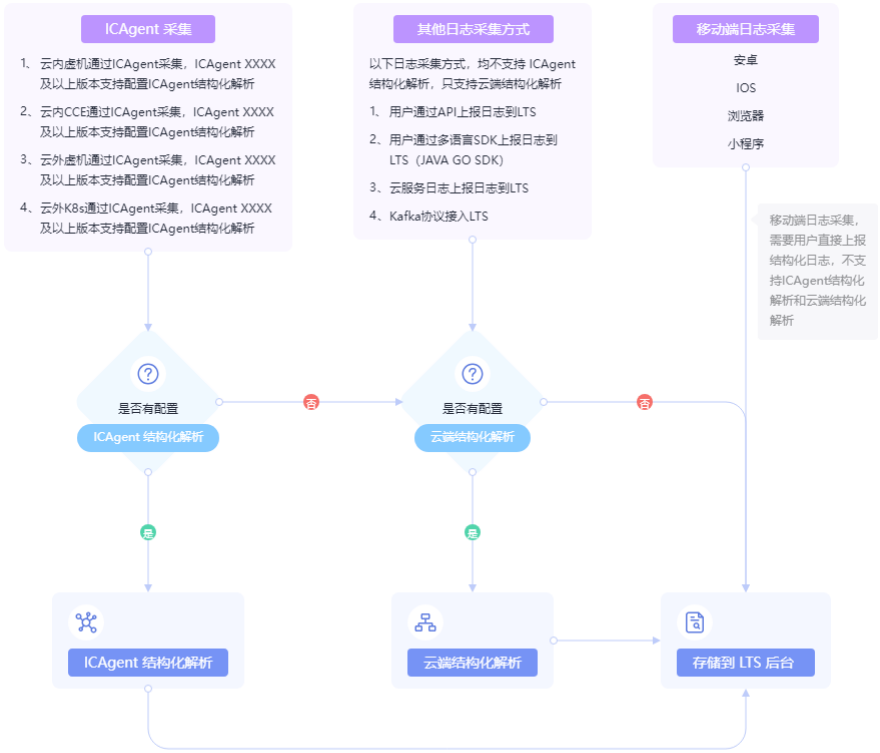
解析方式介绍

云日志服务支持两种日志结构化解析方式：云端结构化解析和ICAgent结构化解析，且一个日志流只能配置一种结构化方式，例如选择云端结构化解析后，不能再选择ICAgent结构化解析，需要删除后，才能重新选择。更多信息请参考图5-1。

若用户在日志接入的时候没有配置结构化解析，可以单独给目标日志流配置ICAgent结构化解析或云端结构化解析。

- ICAgent结构化解析是在采集侧做结构化，支持插件组合解析，单个日志流的多个采集配置支持不同结构化解析规则，推荐使用ICAgent结构化解析的方式，更多内容请参考ICAgent结构化解析规则说明。
- 云端结构化解析是通过不同的日志提取方式将日志流中的日志进行结构化，云端结构化解析会消耗LTS服务端算力，未来会按照日志大小收取日志加工流量费用。

图 5-1 不同解析方式



注意事项

- 日志结构化是以日志流为单位。
- 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。
- 结构化配置修改后，对新写入的日志数据生效，历史日志数据不会生效。

5.2.2 设置日志云端结构化解析

云日志服务LTS目前支持五种日志结构化方式，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**：适用于日志文本中每行内容为一条原始日志，且每条日志可按正则表达式提取为多个key-value键值的日志解析模式。使用正则表达式提取字段，您需要先输入日志样例，再自定义正则表达式。配置完成后，系统将根据正则表达式中的捕获组提取对应的key-value。
- **JSON**：适用于日志文本中每行内容为一条原始日志，且每条日志可按JSON解析规则提取为多个key-value键值的日志解析模式。
- **分隔符**：适用于日志文本中每行内容为一条原始日志，且每条日志可根据指定的分隔符（例如：冒号、空格或字符等）提取为多个key-value键值的日志解析模式。
- **Nginx**：适用于日志文本中每行内容为一条原始日志，每条日志符合Nginx格式，支持通过log_format指令来自定义访问日志的格式。
- **结构化模板**：适用于日志结构比较复杂或需要自定义提取key-value键值的场景，可以通过内置系统模板或者自定义模板提取字段。

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

说明

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。

使用限制

- 若未配置索引配置，结构化字段默认分词符为空，最大长度限制为20KB，超过部分会被截断。
- 若已配置索引配置，结构化字段默认分词符参考**设置LTS日志内容分词**，此时最大长度限制为500KB。

云端结构化解析

步骤1 登录**云日志服务控制台**，进入“日志管理”页面。

步骤2 单击目标日志组和日志流名称。

步骤3 在日志流详情页面，单击右上角  ，在弹出页面中，选择“云端结构化解析”，进行日志结构化配置。

说明

- 开启“保留原始日志”后，原始日志将作为content字段的值存储到云日志服务。同时在资源统计和计费时content字段均会统计在内。
- 开启“上传解析失败日志”后，原始日志将作为_content_parse_fail_字段的值上传到云日志服务。

- **正则分析**：使用正则表达式提取字段。
- **JSON**：通过提取JSON字段将其拆分为键值对。
- **分隔符**：使用分隔符（例如：冒号、空格或字符等）提取字段。
- **Nginx**：通过log_format指令来自定义访问日志的格式。
- **结构化模板**：通过自定义模板或系统内置模板提取字段。

步骤4 云端结构化解析配置完成后，支持修改或删除结构化配置。

- 在云端结构化解析页面中，单击 ，修改结构化配置。
- 在云端结构化解析页面中，单击 ，删除结构化配置。

  说明

  结构化配置删除后，将无法恢复，请谨慎操作。

----结束

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。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：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”。
- 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

- 分词符指将日志内容切分为多个单词的符号，默认分词符包括, '";=()[]{}@&<>/:\\?\n\t\r，在日志搜索或者对日志进行结构化时，可以选取相邻两分词符之间的单词。
- 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 若需要指定某一字段作为日志时间，详细请参考**自定义日志时间**。

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

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。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：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"}
```

说明

- 当日志提取字段的类型为float时，精度为16位有效数字。如果超过16位有效数字，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。
- 当日志提取字段的类型为long时，日志内容超过16位有效数字，只会精确显示前16位有效数字，后面的数字会变为0。
- 当日志提取字段的类型为long时，日志内容超过21位有效数字，则会识别为float类型，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 若需要指定某一字段作为日志时间，详细请参考**自定义日志时间**。

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

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。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：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
```

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 若需要指定某一字段作为日志时间，详细请参考**自定义日志时间**。

步骤5 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。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：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"';
```


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 若需要指定某一字段作为日志时间，详细请参考**自定义日志时间**。

步骤5 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**。

5.2.3 设置云端结构化字段和 tag 字段

设置云端结构化字段

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，详细请参考**表5-1**。

表 5-1 结构化字段设置规则

日志提取方式	字段名称	字段类型是否可修改	字段是否可删除
正则分析（自动生成）	用户自定义。 名称必须以字母开始，且仅包含字母和数字。	是	是
正则分析（手动输入）	• 支持在输入正则表达式时进行命名。 • 支持使用系统默认命名field1、field2、field3等。	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
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，单击“添加字段”。

图 5-2 添加 tag 字段

步骤2 在tag字段列表中，输入需要设置 tag“字段名称”，例如hostIP。

说明

tag字段功能上线前，已设置的结构化配置，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3 如需添加多个字段可单击“添加字段”，继续添加。

步骤4 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

5.2.4 设置云端结构化自定义日志时间

当日志接入云日志服务LTS时，您可以通过开启“自定义日志时间”开关，将日志中的时间字段设置为接入配置的时间。

开启自定义日志时间

步骤1 登录**云日志服务控制台**，进入“日志管理”页面。

步骤2 单击目标日志组和日志流名称。

步骤3 在日志流详情页面，单击右上角  ，在弹出页面中，选择“云端结构化解析”，详细请参考**设置日志云端结构化解析**。

步骤4 配置完成后，开启自定义日志时间开关  ，配置如下参数。

说明

切换自定义日志时间开关时，可能会导致日志搜索界面在切换时间点附近出现时间偏差，请勿频繁切换自定义日志时间开关。

表 5-2 参数配置表

参数	说明	示例
字段key	已提取字段的名称。单击下拉框选择已提取的字段，该字段为string或long类型。	test
字段value	已提取的字段value，选择字段key后，将自动填充。	2022-07-19 12:12:00
时间格式	请参考**常见日志时间格式**。	yyyy-MM-dd HH:mm:ss
操作	单击“校验”，提示“时间格式和字段value匹配成功”则表示校验成功。	-

----结束

常见日志时间格式

常见日志时间格式如下**表5-3**。

说明

默认情况下，云日志服务LTS中的日志时间戳精确到秒，因此时间格式只需配置到秒，无需配置毫秒、微秒等信息。

表 5-3 时间格式

时间格式	说明	示例
EEE	星期的缩写。	Fri
EEEE	星期的全称。	Friday
MMM	月份的缩写。	Jan
MMMM	月份的全称。	January
dd	每月第几天，十进制，范围为01~31。	07, 31

时间格式	说明	示例
HH	小时，24小时制。	22
hh	小时，12小时制。	11
MM	月份，十进制，范围为01~12。	08
mm	分钟，十进制，范围为00~59。	59
a	AM或PM。	AM、PM
hh:mm:ss a	12小时制的时间组合。	11:59:59 AM
HH:mm	小时和分钟组合。	23:59
ss	秒数，十进制，范围为00~59。	59
yy	年份，十进制，不带世纪，范围为00~99。	04、98
yyyy	年份，十进制。	2004、1998
d	每月第几天，十进制，范围为1~31。	7、31
DDD	一年中的天数，十进制，范围为001~366。	365
u	星期几，十进制，范围为1~7，1表示周一。	2
w	每年的第几周，星期天是一周的开始，范围为00~53。	23
W	每月的第几周，范围为0~5。	2
U	星期几，十进制，范围为0~6，0代表周日。	5
EEE MMM dd HH:mm:ss yyyy	标准的日期和时间。	Tue Nov 20 14:12:58 2020
EEE MMM dd yyyy	标准的日期，不带时间。	Tue Nov 20 2020
HH:mm:ss	标准的时间，不带日期。	11:59:59
%s	Unix时间戳。	147618725

示例

常见的时间标准、示例及对应的时间表达式如下**表5-4**。

表 5-4 示例

示例	时间表达式	时间标准
2022-07-14T19:57:36+08:00	yyyy-MM-dd'T'HH:mm:ssXXX	自定义
1548752136	%s	自定义
27/Jan/2022:15:56:44	dd/MMM/yyyy:HH:mm:ss	自定义
2022-08-15 17:53:23+08	yyyy-MM-dd HH:mm:ssX	自定义
2022-08-05T08:24:15.536+0000	yyyy-MM-dd'T'HH:mm:ss.SSSZ	自定义
2022-08-20T10:04:03.204000Z	yyyy-MM-dd'T'HH:mm:ss.SSSZ	自定义
2022-08-22T06:52:08Z	yyyy-MM-dd'T'HH:mm:ssZ	自定义
2022-07-24T10:06:41.000	yyyy-MM-dd'T'HH:mm:ss.SSS	自定义
Monday, 02-Jan-06 15:04:05 MST	EEEE, dd-MMM-yy HH:mm:ss Z	RFC850
Mon, 02 Jan 2006 15:04:05 MST	EEE, dd MMM yyyy HH:mm:ss Z	RFC1123
02 Jan 06 15:04 MST	dd MMM yy HH:mm Z	RFC822
02 Jan 06 15:04 -0700	dd MMM yy HH:mm Z	RFC822Z
2023-01-02T15:04:05Z07:00	yyyy-MM-dd'T'HH:mm:ss Z	RFC3339
2022-12-11 15:05:07	yyyy-MM-dd HH:mm:ss	自定义

5.2.5 设置云端结构化模板

云日志服务（LTS）目前支持的结构化模板有两种，分别为系统模板和自定义模板。

系统模板

支持多种系统模板，不支持修改系统模板的字段类型和删除字段，详情请参考**表5-5**。

步骤1 在云端结构化解析页面中，日志结构化方式选择“结构化模板”。

步骤2 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3 选择模板后，“模板详情”中会自动显示对应的日志解析结果。

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。支持通过模板名称搜索模板，方便用户快速查询模板信息。
- string类型的字段不支持使用运算符（>=<）或 in 语法进行范围查询，建议使用星号（*）或问号（?）进行模糊查询。需要重新配置结构化，将该字段修改为数字类型。

表 5-5 系统模板

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
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
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

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慢日志	根据MYSQL资料中提供的日志字段被定义。	否	否
POSTGRESQL慢日志	根据POSTGRESQL慢日志资料中提供的日志字段被定义。	否	否
POSTGRESQL错误日志	根据POSTGRESQL错误日志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
GeminiDB Redis慢日志	根据GeminiDB 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
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
GeminiDB Cassandra慢日志	根据GeminiDB Cassandra慢日志资料中提供的日志字段被定义。	否	否
GeminiDB Mongo慢日志	根据GeminiDB Mongo慢日志资料中提供的日志字段被定义。	否	否
GeminiDB Mongo错误日志	根据GeminiDB Mongo错误日志资料中提供的日志字段被定义。	否	否
WAF访问日志	根据WAF访问日志资料中提供的日志字段被定义。	否	否
WAF攻击日志	根据WAF攻击日志资料中提供的日志字段被定义。	否	否
DMS重平衡日志	根据DMS重平衡日志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
CCE审计日志	根据CCE审计日志资料中提供的日志字段被定义。	否	否
CCE事件日志	根据CCE事件日志资料中提供的日志字段被定义。	否	否
CCE NGINX-INGRESS日志	根据CCE NGINX-INGRESS日志资料中提供的日志字段被定义。	否	否 -
GeminiDB Redis审计日志	根据GeminiDB Redis审计日志资料中提供的日志字段被定义。	否	否
influx慢日志	根据influx慢日志资料中提供的日志字段被定义。	否	否
METRIC系统日志	根据日志生成指标任务过滤的监控日志字段被定义。	否	否
Microgateway	根据Microgateway应用网关提供的日志字段被定义。	否	否
GeminiDB Mongo接口审计日志	根据GeminiDB Mongo接口审计日志提供的日志字段被定义。	否	否

步骤4 单击“保存”完成结构化配置。

----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。自定义模板主要来源有以下两种：

- 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”，保存自定义模板。该模板会在“自定义模板”下的模板列表展示。
- 新增结构化模板，具体操作如下：
  a. 在“选择模板”下，选择“自定义模板”，单击“新增结构化模板”。
  b. 在“新增结构化模板”页面中，选择正则分析、JSON、分隔符或Nginx方式，进行配置。
  c. 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”下的模板列表展示。

5.3 设置 LTS 日志索引配置

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

索引类型

云日志服务LTS支持全文索引和字段索引，详细请参考**表5-6**。

表 5-6 索引类型

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

注意事项

- 全文索引属性和字段索引属性必须至少启用一种。
- 创建索引会产生索引流量和索引存储空间，费用说明请参见**价格计算器**。
- 关闭索引后，历史索引的存储空间将在当前日志流的数据保存时间到期后，自动被清除。
- 云日志服务默认已为部分内置保留字段创建字段索引，请参见**内置保留字段**。
- 不同的索引配置，会产生不同的查询和分析结果，请根据您的需求，合理创建索引。全文索引和字段索引互不影响。

- 索引配置修改后，对新写入的日志数据生效，历史日志数据不会生效。
- 在字段索引功能上线前，SQL分析支持的字段来自于云端结构化解析；在字段索引功能上线后，只要用户配置了字段索引，SQL分析支持的字段将来自于字段索引，因此修改字段索引可能对现有的可视化图表、仪表盘、SQL告警、定时SQL、Grafana接入中的查询结果产生影响，请谨慎操作！

配置全文索引

步骤1 登录**云日志服务控制台**，进入“日志管理”页面。

步骤2 单击目标日志组和日志流名称。

步骤3 在日志流详情页面，单击右上角  ，在弹出页面中，选择“索引配置”，进入索引配置页面。

步骤4 在索引配置页面中，默认开启“全文索引”按钮，参考**表5-7**配置各参数信息。

说明

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

表 5-7 自定义全文索引配置参数

参数	说明
全文索引	打开全文索引开关，表示创建全文索引。
大小写敏感	查询时是否区分英文字母的大小写。 • 打开大小写敏感开关，则查询时区分大小写。例如示例日志含有Know，那么您只能使用**Know**才能查询到该日志。 • 关闭大小写敏感开关，则查询时不区分大小写。例如示例日志含有Know，那么您使用关键字**KNOW**和**know**都能查到该日志。

参数	说明
包含中文	查询时是否区分中英文。 ● 打开包含中文开关后，如果日志中包含中文，默认按照一元分词法拆分中文内容，按照分词符的设置拆分英文内容。 **说明** – 一元分词是指将中文字符串拆分为单个独立的中文字。 – 使用一元分词符的优点是对海量日志分词效率高，其他中文分词方法对写入速度影响大。 – 打开包含中文功能，会对中文使用一元分词（每个汉字单独分词），如果需要更精确的搜索结果，请用短语搜索，语法为：#"待搜索的短语"。 ● 关闭包含中文开关后，按照分词符的设置拆分所有内容。 例如示例日志内容为： **error,400,I Know 今天是星期一**。 ● 关闭包含中文开关后，按照分词符的设置拆分英文内容，日志会被拆分为**error**、**400**、**I**、**Know**、**今天是星期一**，您可以通过**error**或**今天是星期一**查找该日志。 ● 打开包含中文开关后，日志服务后台分词器将日志拆分为**error**、**400**、**I**、**Know**、**今**、**天**、**是**、**星**、**期**、**一**，您通过**error**或**今天**等词都可以查找到该日志。
分词符	根据指定分词符，将日志内容拆分成多个词。当默认设置不能满足您的需求时，您可以自定义设置分词符。所有的ASCII码包括中文都可被定义为分词符。 如果设置分词符为空，则字段值将被当成一个整体，您只能通过完整字符串或模糊查询查找对应的日志。 单击“预览”，查看分词预览效果。 例如示例日志内容为： **error,400,I Know 今天是星期一**。 ● 如果不设置任何分词符，整条日志被作为一个词**error,400,I Know 今天是星期一**，您只能通过完整字符串**error,400,I Know 今天是星期一**或模糊查询**error,400,I K***查找该日志。 ● 如果设置分词符为逗号（,），则原始日志被拆分为**error**、**400**、**I Know 今天是星期一**3个词，您通过任意一个词或词的模糊查询都可以找到该日志，例如**error**、**400**、**I Kn***、**今天是***。 ● 如果设置分词符为逗号（,）和空格，则原始日志被拆分为**error**、**400**、**I**、**Know**、**今天是星期一**5个词，您通过任意一个词或词的模糊查询都可以找到该日志，例如**Know**、**今天是***。
特殊分词符	单击“添加特殊分词符”，参考**ASCII码对照表**输入ASCII值。

步骤5 完成后，单击“确定”。

----结束

配置字段索引

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

步骤1 设置快速分析采样条数，默认值10万条，最小值为10万条，最大值1000万条。通过采样快速统计字段值取值分布，并非对全量数据进行分析，采样条数越多分析数据越慢。

步骤2 在索引配置页面的字段索引下方，单击“添加字段”，配置字段索引。具体的参数配置请参考**表5-8**。

说明

- 字段索引的参数配置仅对该字段生效。
- 当添加的字段在日志内容中不存在时，则配置的该索引字段无效。
- 更多内置字段请参考**内置保留字段**。

- 自动配置字段索引：单击“自动配置”，云日志服务会根据采集时预览数据中的第一条内容或常见内置保留字段（例如hostIP、hostName、pathFile）自动生成字段索引，您可以根据自己的需要增加或者删除字段。
- 批量配置字段索引：批量勾选字段，单击“批量配置”，进行批量配置字段索引。

表 5-8 自定义字段索引配置参数

参数	说明
字段名称	日志字段名称，例如示例日志中的level。 字段名称只能包括字母、数字或下划线（_），且只能以字母或下划线（_）开头，字段名称中不能含有双下划线。 **说明** • 双下划线（__）在LTS不对用户呈现的内置保留字段中使用，用户自定义日志字段名中不能使用双下划线__，否则无法配置字段索引名称。 • 日志服务默认会对部分内置保留字段开启字段索引，请参见**内置保留字段**。 • 若是内置字段，在字段名称后会显示“内置”字眼，方便用户识别。
执行操作	显示字段的添加状态：新增、不修改、修改、删除。索引字段有变动后，单击“修改对比”，即可查看原配置内容与修改后配置内容的差异。 • 显示新增的字段不支持修改执行操作。 • 修改类型、大小写敏感、自定义分词符、特殊分词符、包含中文、快速分析时，会与原索引配置中的字段进行对比，若任意一项不同，则执行操作变为“修改”。 • 索引配置单击确定后，不会保存执行操作为“删除”的字段。

参数	说明
类型	• 日志字段值（Value）的数据类型，可选值为string、long、float、json。 **说明** 字段json类型只对ICAgent结构化解析生效，对云端结构化解析不生效。 • long类型和float类型不支持设置大小写敏感、包含中文和分词符。
大小写敏感	查询时是否区分英文字母的大小写。 • 打开大小写敏感开关，则查询时区分大小写。例如示例日志message字段中含有Know，那么您只能使用**message:Know**才能查询到该日志。 • 关闭大小写敏感开关，则查询时不区分大小写。例如示例日志message字段中含有Know，那么您使用关键字**message:KNOW**和**message:know**都能查到该日志。
自定义分词符	根据指定分词符，将日志内容拆分成多个词。当默认设置不能满足您的需求时，您可以自定义设置分词符。所有的ASCII码包括中文都可被定义为分词符。 如果设置分词符为空，则字段值将被当成一个整体，您只能通过完整字符串或模糊查询查找对应的日志。 例如示例日志message字段内容为：**I Know 今天是星期一**。 • 如果不设置任何分词符，整条日志被作为一个词**I Know 今天是星期一**，您只能通过完整字符串**message:I Know 今天是星期一**或模糊查询**message:I Know 今天是*查找该日志**。 • 如果设置分词符为空格，则原始日志被拆分为**I**、**Know**、**今天是星期一**3个词，您通过任意一个词或词的模糊查询都可以找到该日志，例如**message:Know**或**message:今天是星期一**。
特殊分词符	单击“添加特殊分词符”，参考**ASCII码对照表**输入ASCII值。

参数	说明
包含中文	查询时是否区分中英文。 • 打开包含中文开关后，如果日志中包含中文，默认按照一元分词法拆分中文内容，按照分词符的设置拆分英文内容。 **说明** – 一元分词是指将中文字符串拆分为单个独立的中文字。 – 使用一元分词符的优点是对海量日志分词效率高，其他中文分词方法对写入速度影响大。 – 打开包含中文功能，会对中文使用一元分词（每个汉字单独分词），如果需要更精确的搜索结果，请用短语搜索，语法为：#"待搜索的短语"。 • 关闭包含中文开关后，按照分词符的设置拆分所有内容。 例如示例日志message字段内容为：**I Know 今天是星期一**。 • 关闭包含中文开关后，按照分词符的设置拆分英文内容，日志会被拆分为**I**、**Know**、**今天是星期一**，您可以通过**message:Know**或**message:今天是星期一**查找该日志。 • 打开包含中文开关后，日志服务后台分词器将日志拆分为**I**、**Know**、**今**、**天**、**是**、**星**、**期**、**一**，您通过**message:Know**或**message:今天**等词都可以查找到该日志。
快速分析	默认为开启状态，开启后，可以对字段值做采样统计，请参见11.6.4-快速分析。 **说明** • 快速分析的原理是对搜索命中的日志采样10万条进行数据统计，不是全量统计。 • 快速分析的字段长度最大为2000字节。 • 快速分析字段展示前100条数据。
操作	单击  ，删除添加的自定义字段。

图 5-3 批量配置

步骤3 完成后，单击“确定”。

----结束

内置保留字段

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

说明

- 使用API写入日志数据或添加ICAgent配置时，请不要将字段名称设置为内置保留字段，否则可能会造成字段名称重复、查询不精确等问题。
- 日志服务为日志数据增加的内置保留字段当前免费，后续会按照按量付费方式正常收费（为其开启索引时也会产生少量索引流量及存储费用）。更多信息请参见**价格计算器**。
- 用户自定义日志字段名称中不能使用双下划线__，否则无法配置索引。

表 5-9 内置保留字段说明

内置保留字段	数据格式	索引与统计设置	说明
collectTime	整型，Unix时间戳（毫秒）	索引设置：开启索引后，日志服务默认为collectTime创建字段索引，索引数据类型为long类型。 查询时输入collectTime : xxx。	采集时间，指日志被采集器ICAgent采集时的时间。 例如示例中的"collectTime":"1681896081334"，转换成标准时间是2023-04-19 17:21:21
__time__	整型，Unix时间戳（毫秒）	索引设置：开启索引后，日志服务默认为time创建字段索引，索引数据类型为long类型。该字段不支持查询。	日志时间，指的是日志在控制台页面展示的日志时间。 例如示例中的"__time__":"1681896081334"，转换成标准时间是2023-04-19 17:21:21 日志时间默认使用采集时间，也支持自定义日志时间。

内置保留字段	数据格式	索引与统计设置	说明
lineNum	整型	索引设置：开启索引后，日志服务默认为lineNum创建字段索引，索引数据类型为long类型。	行号（偏移量），用来排序日志。 非高精度日志会根据collectTime生成，默认是collectTime * 1000000 + 1，高精度日志就是用户上报的纳秒值。 例如示例中的"lineNum":"1681896081333991900"。
category	字符串	索引设置：开启索引后，日志服务默认为category创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入category: xxx。	日志类型，表示该日志的来源。 例如ICAgent采集的日志该字段为LTS，某云服务例如DCS上报的日志该字段为DCS。
clusterName	字符串	索引设置：开启索引后，日志服务默认为clusterName创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入clusterName: xxx。	集群名称，k8s场景下集群名称。 例如示例中的"clusterName":"epstest"。
clusterId	字符串	索引设置：开启索引后，日志服务默认为clusterId创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入clusterId: xxx。	集群ID，k8s场景下集群ID。例如示例中的"clusterId":"c7f3f4a5-xxxx-11ed-a4ec-0255ac100b07"。
nameSpace	字符串	索引设置：开启索引后，日志服务默认为nameSpace创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入nameSpace: xxx。	命名空间，k8s场景下命名空间。 例如示例中的"nameSpace":"monitoring"。

内置保留字段	数据格式	索引与统计设置	说明
appName	字符串	索引设置：开启索引后，日志服务默认为appName创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入appName: xxx。	组件名称，k8s场景下工作负载的名称。 例如示例中的"appName":"alertmanager-alertmanager"。
serviceID	字符串	索引设置：开启索引后，日志服务默认为serviceID创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入serviceID: xxx。	工作负载ID，k8s场景下工作负载ID。 例如示例中的"serviceID":"cf5b453xxxad61d4c483b50da3fad5ad"。
podName	字符串	索引设置：开启索引后，日志服务默认为podName创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入podName: xxx。	POD名称，k8s场景下POD名称。 例如示例中的"podName":"alertmanager-alertmanager-0"。
podIp	字符串	索引设置：开启索引后，日志服务默认为podIp创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入podIp: xxx。	pod的ip，k8s场景下pod的IP地址。 例如示例中的"podIp":"10.0.0.145"。
containerName	字符串	索引设置：开启索引后，日志服务默认为containerName创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入containerName: xxx。	容器名称，k8s场景下容器名称。 例如示例中的"containerName":"config-reloader"。
hostName	字符串	索引设置：开启索引后，日志服务默认为hostName创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入hostName: xxx。	主机名称，ICAgent所在主机的名称。 例如示例中的"hostName":"epstest-xx518"。

内置保留字段	数据格式	索引与统计设置	说明
hostId	字符串	索引设置：开启索引后，日志服务默认为hostId创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入hostId: xxx。	主机ID，ICAgent所在主机的id，该id由ICAgent生成。例如示例中的"hostId":"318c02fe-xxxx-4c91-b5bb-6923513b6c34"。
hostIP	字符串	索引设置：开启索引后，日志服务默认为hostIP创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入hostIP: xxx。	主机IP，日志采集器所在主机的ip（适用于ipv4场景） 例如示例中的"hostIP":"192.168.0.31"。
hostIPv6	字符串	索引设置：开启索引后，日志服务默认为hostIPv6创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入hostIPv6: xxx。	主机IP，日志采集器所在主机的ip（适用于ipv6场景） 例如示例中的"hostIPv6":""。
pathFile	字符串	索引设置：开启索引后，日志服务默认为pathFile创建字段索引，索引数据类型为string类型，分词字符为空。查询时输入pathFile: xxx。	文件路径，采集的日志文件的路径。 例如示例中的"pathFile":"stdout.log"。
content	字符串	索引设置：开启全文索引后，会使用全文索引定义的分词符对content字段的value进行分词；不支持将content字段配置到字段索引中。	日志原文， 例如示例中的"content":"level=error ts=2023-04-19T09:21:21.333895559Z"
__receive_time__	整型，Unix时间戳（毫秒）	索引设置：开启索引后，日志服务默认为__receive_time__创建字段索引，索引数据类型为long类型。	上报日志的服务端时间，相当于LTS采集端接收到日志的时间。

内置保留字段	数据格式	索引与统计设置	说明
__client_time__	整型，Unix时间戳（毫秒）	索引设置：开启索引后，日志服务默认为__client_time__创建字段索引，索引数据类型为long类型。	端侧日志的客户端上报时间。
_content_parse_fail_	字符串	索引设置：开启索引后，日志服务默认为_content_parse_fail_创建字段索引，索引数据类型为string类型，分词字符为默认分词符。查询时输入_content_parse_fail_:xxx。	上报日志解析失败的日志内容。
__time	整型，Unix时间戳（毫秒）	不支持将__time字段配置到字段索引中。	不涉及。
logContent	字符串	不支持将logContent字段配置到字段索引中。	不涉及。
logContentSize	整型	不支持将logContentSize字段配置到字段索引中。	不涉及。
logIndexSize	整型	不支持将logIndexSize字段配置到字段索引中。	不涉及。
groupName	字符串	不支持将groupName字段配置到字段索引中。	不涉及。
logStream	字符串	不支持将logStream字段配置到字段索引中。	不涉及。

ASCII 码对照表

表 5-10 ASCII 码对照表

ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符
0	NUL（空字符）	32	空格	64	@	96	`

ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符
1	SOH（标题开始）	33	!	65	A	97	a
2	STX（正文开始）	34	"	66	B	98	b
3	ETX（正文结束）	35	#	67	C	99	c
4	EOT（传输结束）	36	$	68	D	100	d
5	ENQ（询问字符）	37	%	69	E	101	e
6	ACK（确认回应）	38	&	70	F	102	f
7	BEL（响铃）	39	'	71	G	103	g
8	BS（退格）	40	(	72	H	104	h
9	HT（水平定位符号，制表符）	41	)	73	I	105	i
10	LF（换行）	42	*	74	J	106	j
11	VT（垂直定位符号）	43	+	75	K	107	k
12	FF（换页键）	44	,	76	L	108	l
13	CR（归位键）	45	-	77	M	109	m
14	SO（取消变换）	46	.	78	N	110	n
15	SI（启用变换）	47	/	79	O	111	o
16	DLE（跳出数据通讯）	48	0	80	P	112	p
17	DC1（设备控制1）	49	1	81	Q	113	q
18	DC2（设备控制2）	50	2	82	R	114	r
19	DC3（设备控制3）	51	3	83	S	115	s

ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符
20	DC4（设备控制4）	52	4	84	T	116	t
21	NAK（确认失败回应）	53	5	85	U	117	u
22	SYN（同步用暂停）	54	6	86	V	118	v
23	ETB（区块传输结束）	55	7	87	W	119	w
24	CAN（取消）	56	8	88	X	120	x
25	EM（连接介质中断）	57	9	89	Y	121	y
26	SUB（替换）	58	:	90	Z	122	z
27	ESC（跳出）	59	;	91	[	123	{
28	FS（文件分割符）	60	<	92	\	124	|
29	GS（组群分隔符）	61	=	93	]	125	}
30	RS（记录分隔符）	62	>	94	^	126	~
31	US（单元分隔符）	63	?	95	_	127	DEL（删除）

5.4 搜索日志

5.4.1 进入搜索 LTS 日志页面

当您配置完成日志结构化解析和索引后，就可以通过输入搜索语句，在日志数据中查找包含特定关键词的日志记录。或者根据时间范围来检索日志数据，帮助您定位特定时间段内发生的事件和问题。

搜索语句用于指定日志查询时的过滤规则，返回符合条件的日志。搜索语句可以为关键词、数值、数值范围、空格、星号（*）等。 如果为空格或星号（*），表示无过滤条件。更多信息请参见**LTS搜索语法介绍**。

搜索日志

步骤1 登录**云日志服务控制台**，进入“日志管理”页面。

步骤2 在“日志管理”页面，单击目标日志组或日志流名称，进入日志详情页面。

步骤3 您可以根据自己的实际需求，在搜索框上方选择时间范围，即可查看不同时间段的日志数据。

时间范围有三种方式，分别是相对时间、整点时间和自定义。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：表示查询指定时间范围的日志数据。支持选择3个月的范围，白名单用户支持选择6个月的范围。如有需要，请**提交工单**申请。

步骤4 根据**LTS搜索语法介绍**在搜索框输入查询条件，用于日志数据的查看、简单搜索和过滤。

- 在页面搜索区域中，单击搜索框，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。

  说明

  - 内置保留字段有appName、category、clusterId、clusterName、collectTime等，默认简化显示，并且hostIP、hostName、pathFile默认显示在最前面。更多内置保留字段请参考**设置LTS日志索引配置**。
  - 结构化配置的字段按照key:value显示。
  - 日志搜索框内容过多时支持自动换行并多行显示。
  - 支持固定搜索框高度。
- 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。
- 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。请参考**创建LTS快速分析**开启快速分析。

  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。

步骤5 在“日志搜索”页签，您可以进行如下操作，更多操作请参考**日志搜索的常用操作**。

1. 在日志统计下方，展示不同时间段的日志总条数柱状图，柱状图旁边显示日志条数刻度。

   说明

   若使用了内嵌功能，支持设置收起或展开式日志条数统计图。关于内嵌参数请参考**云日志服务地址**。
2. 在日志内容下方，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，支持以下方式搜索日志：复制、添加到查询、从查询中排除、添加到查询（交互模式）、从查询中排除（交互模式）、新建查询、隐藏。
3. 在日志内容下方，支持选择列表或原始日志方式展示日志内容。

> **说明**
>
> 日志高亮的实现原理是当查询条件命中日志后，再将日志与查询条件进行字符串匹配，相同日志部分增加高亮标签，该部分会在界面高亮展示。因此当查询条件比较复杂，尤其是存在或关系时，在界面高亮显示的内容可能会比实际查询结果显示的多。

步骤6 支持设置日志数据的版面展示，主要设置字段是否显示或简化显示。

1. 在下拉框单击编辑版面，进入版面设置页面，版面列表自带默认版面、纯净版面、容器日志默认版面，可以设置字段在版面是否显示。
   - 云端：适用于有写权限的用户，版面配置信息保存在云端。
   - 本地缓存：适用于只有读权限的用户，版面配置信息缓存在本地浏览器。
2. 单击 新增自定义版面，设置版面名称和版面字段的可见性。
3. 设置完成后，单击“确定”，返回下拉框显示新增的自定义版面。

----结束

交互模式

使用交互模式之前，请确保日志正常上报，且已经完成结构化分析和索引配置，详细请参考**设置云端结构化解析日志**和**设置LTS日志索引配置**。

交互式搜索适用于生成简单的搜索语句，操作简单，通过在界面上设置搜索条件和指定日志查询时的过滤规则，从而筛选日志中满足条件的记录。如果您需要使用更多的函数或者嵌套查询，请手动输入SQL语句。详细请参考**SQL分析语法介绍**。

步骤1 单击搜索框前面的“交互模式”，进入交互式搜索页面。

图 5-4 交互模式

步骤2 在下拉框选择日志搜索的字段和条件，搜索框则会展示对应字段的值。根据业务需要，用户可以自定义设置搜索方式，添加关联关系或添加组进行搜索。

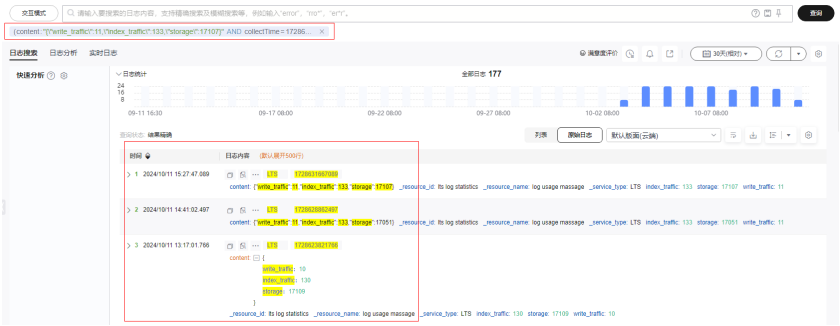
- 下拉框显示的字段为索引配置字段、结构化字段、**内置保留字段**。
- 且（AND）表示在多个条件中需要同时满足所有条件才能成立。
- 或（OR）表示在多个条件中只需满足其中一个条件即可。

例如在界面上选择content、collectTime、category字段，设置不同的条件，随时可以预览搜索语句，如有问题，可以修改搜索条件，操作简单。

（截图仅供参考，请以实际搜索结果为准）

```
(content:"{\"write_traffic\":11,\"index_traffic\":133,\"storage\":17107}" AND collectTime=1728631667089) OR category:LTS
```


步骤3 设置完成后，单击“确定”，LTS根据搜索语句进行日志搜索，在日志搜索下方即可查看搜索结果。（截图仅供参考，请以实际搜索结果为准）



----结束

日志搜索的常用操作

在日志内容展示区域，支持分享日志、查看上下文、下载日志等操作，具体参考**表5-11**。

表 5-11 常用操作

操作	说明
创建快速查询	单击 按钮，创建快速查询。
查看仪表盘	单击 按钮，在弹出来的仪表盘页面中，可查看已创建的仪表盘。
添加告警	单击 按钮，在弹出的页面中，支持**新建告警规则**。
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。

操作	说明
刷新日志	单击 对日志进行刷新，有两种方式刷新方式：手动刷新和自动刷新。 ● 手动刷新：单击“手动刷新”，可直接对日志进行刷新。 ● 自动刷新：选择自动刷新的间隔时间，将对日志进行自动刷新。间隔时间范围为15秒、30秒、1分钟和5分钟。
复制	单击 复制日志内容。
查看上下文	单击 查看日志上下文。 **说明** 支持选择简洁模式查看日志上下文。支持下载上下文内容。
更多操作	单击 进入该时间段的日志详情页，查看更多日志信息。 ● 在“扩展字段”页签，查看字段名称、字段值，在对应字段操作列，支持对该字段进行添加到查询、从查询中排除、字段存在、字段不存在、隐藏的方式搜索日志。 ● 在“json格式”页签，查看日志的json格式。 ● 在“上下文日志”页签，支持设置查询行数、过滤字段、下载日志、简洁模式等操作。
换行/取消换行	单击 按钮，搜索的日志内容将换行显示。若不需要换行， 单击 按钮，取消换行。 **说明** 默认开启换行按钮。
下载日志	该功能仅支持白名单用户使用，如有需要，请**提交工单**申请开通。 鼠标悬浮在 按钮上，单击“下载日志”，在弹出的下载日志页面中支持“本地下载”和“前往创建转储”。开通一次性转储后才能看到“前往创建转储”功能。 ● 本地下载：将日志文件直接下载到本地，白名单用户单次下载支持最大2000万条日志。非白名单用户单次下载支持最大5,000条日志。 在下拉框中选择“.csv”或“.txt”，单击“开始下载日志”，可将日志导出至本地。 ● 前往创建转储（白名单功能）：通过OBS转储任务下载日志文件，单次下载支持最大2,000万条日志。单击“前往创建转储”，跳转至配置转储页面，详细请参考**日志转储至OBS**。 ● 鼠标悬浮在 按钮上，单击“日志下载历史”，在日志下载历史页面，支持查看、下载、删除日志下载记录。

操作	说明
全部折叠/全部展开	单击 设置日志内容展示的行数。若不需要展示日志内容，再单击一次 按钮即可关闭展示的日志内容。 **说明** 默认不折叠。折叠后，默认显示2行，最多支持展示6行。
JSON设置	鼠标悬浮在 按钮上，单击“JSON设置”，在弹出的JSON设置页面中，设置格式化显示。 **说明** 默认开启格式化，JSON默认展开层级为2层。若日志包含多个反斜杠，当日志展示为json格式时，会丢失一个反斜杠，因为json解析会将第一个反斜杠作为转义符处理。 ● 开启格式化按钮：设置JSON默认展开层级，最大设置为10层。 ● 关闭格式化按钮：对于JSON格式的日志，将不会格式化层级显示。
日志折叠设置	鼠标悬浮在 按钮上，单击“日志折叠设置”，在弹出的日志折叠设置页面中，设置长日志字符个数。 日志超过设置的长日志字符个数时，超出字符将被隐藏，单击“展开”按钮可查看全部内容。 **说明** 默认开启自动折叠长日志，字符个数默认为400个。
日志时间展示	鼠标悬浮在 按钮上，单击“日志时间展示”，在弹出的日志折叠设置页面中，设置是否展示毫秒、是否展示时区。 **说明** 默认开启展示毫秒。
虚拟滚动设置	鼠标悬浮在 按钮上，单击“虚拟滚动设置”，在弹出的虚拟滚动设置页面中，设置是否开启虚拟滚动、填写缓冲区大小。 **说明** ● 虚拟滚动可以避免或减少滚动时卡顿的情况，提升操作体验，防止页面卡死。 ● 滚动时数据会重新渲染，一定程度上影响数据流畅性。 ● 缓冲区决定同时加载的数据量大小，缓冲区越大，同时加载的数据越多，但滚动性能会越差。
不可见字段列表	该列表展示版面设置中配置的不可见性字段。 ● 当日志流未配置版面设置时，将不显示 按钮。 ● 当日志内容为“CONFIG_FILE”且未配置版面设置时，不可见字段默认有appName、clusterId、clusterName、containerName、hostIPv6、NameSpace、podName和serviceID。

跨流搜索（白名单功能）

目前此功能仅支持白名单用户使用，如有需要请**提交工单**申请开通。

在当前日志流详情页面，支持跨流搜索日志，即无需退出当前日志搜索页面，即可选择其他日志流搜索日志。

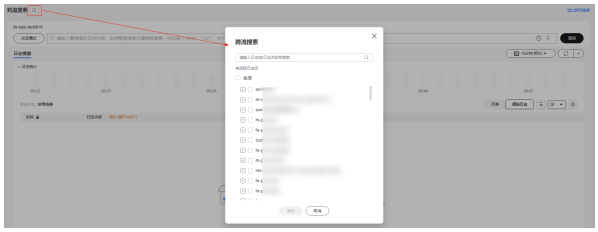
步骤1 在当前日志流详情页面，单击 。

步骤2 在弹出的跨流搜索页面，选择需要搜索的目标日志流。

步骤3 单击“确定”。

步骤4 进入目标日志流详情页，根据业务需要参考**LTS搜索语法介绍**进行搜索日志。

若需要更换日志流，单击左上角跨流搜索旁边 ，在弹出的页面重新选择日志流进行搜索。



步骤5 搜索完成后，单击右上角的“退出跨流搜索”，即可返回当前日志流搜索页面。

- 当跨流搜索的日志流的分词配置不同时，会导致跨流日志关键词高亮不一致。
- 最多可同时搜索50个日志流。

- 仅支持搜索原始日志，暂不支持使用SQL进行统计分析。
- 支持跨日志组选择日志流，但不支持跨区域选择日志流。
- 跨流搜索选择多个索引配置不一致的日志流，例如A日志流配置了字段索引Key1，B日志流没有配置该字段，使用搜索语句**Key1:xxx**搜索日志时，仅能查看A日志流的相关日志，B日志流搜索日志失败，请根据界面报错提示修改后再重新搜索日志。

----结束

5.4.2 LTS 搜索语法介绍

云日志服务（LTS）提供一套搜索语法用于设置搜索条件和指定日志查询时的过滤规则，从而筛选日志中满足条件的记录，筛选结果可以用于分析语句，进行更复杂的分析处理。

为了快速了解并使用搜索语法，建议您了解以下信息：**搜索方式**、**短语搜索**、**运算符**、**搜索语句示例**。

说明

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

  搜索语句不支持区分分词符，例如搜索语句**var/log**，其中/为分词符，搜索语句等同于**var log**，搜索的是同时包含**var**和**log**的所有日志。同理，搜索语句**"var:log"**、**var;log**等搜索的也是同时包含**var**和**log**的所有日志。
- 查询日志使用搜索语法的常见问题和相关报错的处理方法请参考**日志搜索相关问题**。

搜索方式

搜索语句是用来指定日志搜索时的过滤规则，返回符合条件的日志。

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

表 5-12 搜索方式说明

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

搜索方式	说明	示例
字段搜索	配置字段索引后，您可以指定字段名称和字段值（key:value）进行搜索。根据字段索引中设置的数据类型，您可以进行多种类型的基础搜索和组合搜索。 **说明** • value参数不可为空，通过搜索语句**key:""**匹配字段值为空的日志。 • 字段搜索和 not 运算符配合使用时，还会匹配到不包含该字段的日志。	• request_time>60 and request_method:po*表示搜索request_time字段值大于60且request_method字段值以po开头的日志。 • request_method:""表示搜索request_method字段值为空的日志。 • not request_method:GET表示搜索不包含request_method字段和request_method字段值不为GET的日志。
精确搜索	使用精确的词进行搜索。 日志服务搜索采用的是分词法，搜索时不会保证关键词出现的顺序。 **说明** 搜索语句为abc def，会匹配所有同时包含abc和def的日志，日志abc def或者def abc都会命中，如果需要确保关键词出现的顺序，请您采用**短语搜索#"abc def"**。	• GET POST表示搜索同时包含关键词GET和POST的日志。 • request_method:GET表示搜索request_method字段值包含GET的日志。 • #"/var/log"表示搜索包含短语/var/log的日志。

搜索方式	说明	示例
模糊搜索	在搜索语句中指定一个词，在词的中间或者末尾加上模糊搜索关键字，即星号（*）或问号（?），云日志服务会在所有日志中查询到符合条件的100个词，返回包含这100个词并满足查询条件的所有日志。指定的词越精确，查询结果越精确。 **说明** • 星号（*）代表匹配多个字符，问号（?）代表匹配1个字符。 • 当星号（*）和问号（?）作为分词符时，不具备模糊搜索功能，其中问号（?）为默认的分词符，使用其模糊搜索功能前需将其从分词符中移除。 • 星号（*）或问号（?）不能用在词的开头。 • long数据类型和float数据类型不支持使用星号（*）或问号（?）进行模糊搜索。 • 当模糊条件前缀很短且日志中符合条件的词超过100个时，查询结果会不精确。	• GE*表示在所有日志中查找以GE开头的词，并返回包含这些词的日志。 • request_method:GE*表示在所有日志中查找request_method字段值以GE开头的词，并返回包含这些词的日志。
范围搜索	long数据类型和float数据类型支持范围搜索。 • 方式1：通过 =（等于）>（大于）<（小于） 运算符搜索日志。 • 方式2：通过 in 运算符搜索日志，支持修改开闭区间。 **说明** string类型的字段不支持范围查询。	• request_time>=60表示在所有日志中查找request_time字段值大于等于60的日志。 • request_time in (60 120]表示在所有日志中查找request_time字段值大于60且小于等于120的日志。
短语搜索	短语搜索用于完全匹配日志中的目标短语，可以确保关键词出现的顺序。 **说明** 短语搜索不支持模糊搜索。	**#"abc def"**表示在所有日志中查找包含目标短语 abc def 的日志。

- 分词符

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

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

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

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

- 关键词顺序

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

  例如：**request_method:GET POST**查询的是同时包含GET和POST的日志，不会保证GET和POST的顺序。如有需要推荐采用**短语搜索**。

- 中文搜索

  中文搜索时不需要采用模糊查询，如有需要推荐采用短语搜索，可以匹配到更精确的结果。

  云日志服务LTS的英文是以单词的形式进行拆分的，单词的长度不一致，因此可以通过模糊搜索匹配拥有相同前缀英文单词的日志。

  中文采用的是一元分词，每个字都是独立的，拆分后每部分的长度都是1。

  例如：搜索语句**星期一**，代表搜索同时包含**星**、**期**、**一**的日志；搜索语句**#"星期一"**，代表搜索包含目标短语**星期一**的日志。

- 语法关键词

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

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

  如果日志中本身包含语法关键词且需要搜索时，搜索语句需要用**双引号**包裹，否则可能会导致语法错误或搜索到错误的结果。

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

短语搜索

短语搜索用于准确匹配目标短语，例如搜索语句**#"abc def"**，区分先后顺序，将匹配所有同时包含abc、def，且abc位于def前面的日志。短语搜索和关键词搜索的区别请参考**表5-13**。

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

表 5-13 搜索区别

搜索方式	说明	示例
短语搜索	区分关键词的顺序，用于精准匹配目标短语，搜索结果更加精确。	假设您的日志流中存在两条原始日志，如下： ● 原始日志1：this service is lts ● 原始日志2：lts is service 则搜索：#"is lts"，会命中1条日志；搜索：#"lts is"，会命中1条日志。
关键词搜索	不区分关键词的顺序，按照搜索逻辑命中关键词即可。	假设您的日志流中存在两条原始日志，如下： ● 原始日志1：this service is lts ● 原始日志2：lts is service 则搜索：is lts，会命中2条日志；搜索：lts is，会命中2条日志。

使用限制如下：

- 短语搜索不支持搭配模糊搜索。

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

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

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

运算符

搜索语句支持的运算符请参考**表5-14**。

说明

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

表 5-14 运算符说明

运算符	说明	示例
and	与运算符，如果多个关键词之间没有语法关键词，默认为and关系。 **说明** and作为运算符使用时前后需要使用空格分隔。例如 **1 and 2** 代表搜索同时包含**1** 和**2**的日志；**1and2**代表搜索包含词语**1and2**的日志。	GET 200等同于GET and 200
AND	与运算符，等同于and。	GET AND 200
&&	与运算符。 **说明** &&作为运算符使用时不需要使用空格分隔。例如**：1 && 2** 等同于**1&&2**，代表搜索同时包含**1** 和**2**的日志。	1&&2
or	or运算符。 **说明** or 作为运算符使用时前后需要使用空格分隔。	request_method:GET or status:200
OR	或运算符，等同于or。	request_method:GET OR status:200
||	或运算符。|| 作为运算符使用时不需要使用空格分隔。	request_method:GET || status:200
not	非运算符。 **说明** • not 作为运算符使用时需要使用空格分隔。 • not 运算符和字段搜索配合使用时还会匹配到不包含对应字段的日志。	request_method:GET not status:200、not status:200
( )	用于提高括号内搜索条件的优先级。	(request_method:GET or request_method:POST) and status:200

运算符	说明	示例
:	用于字段搜索（key:value）。 **说明** 如果字段名称（key）或者字段值（value）内有空格或冒号（:）等保留字符，请使用双引号（""）包裹字段名称（key）或者字段值（value）。例如： • **"request method":GET** • **message:"This is a log"** • **time:"09:00:00"** • **ipv6:"2024:AC8:2ac::d09"**	request_method:GET
""	使用双引号（""）包裹一个语法关键词，可以将该语法关键词转换成普通字符，例如："and"表示搜索包含and的日志，此处的and不代表运算符。	request_method:"GET"
\	转义符号，用于转义双引号（""），转义后的引号表示符号本身。	例如：日志内容为instance_id:nginx"01"，您可以使用instance_id:nginx\"01\"进行查询。
*	通配符搜索，匹配零个、单个、多个字符。 **说明** *不支持放在关键词开头，推荐放在关键词的中间部分或者结尾。	request_method:P*T
?	通配符搜索，匹配单个字符。 **说明** ?不支持放在关键词开头，推荐放在关键词的中间部分或者结尾。	例如：request_method:P?T，可以匹配到PUT，无法匹配到POST。
>	搜索某字段值大于某数值的日志。	request_time>100
>=	搜索某字段值大于或等于某数值的日志。	request_time>=100
<	搜索某字段值小于某数值的日志。	request_time<100
<=	搜索某字段值小于或等于某数值的日志。	request_time<=100
=	搜索某字段值等于某数值的日志，仅适用于float、long类型的字段。对于该类型的字段，等号（=）和冒号（:）作用相同。	request_time=100等同于request_time:100

运算符	说明	示例
in	搜索某字段值处于某数值范围内的日志，中括号表示闭区间，小括号表示开区间，两个数字之间使用空格分隔。 **说明** in只能为小写字母，且作为运算符使用时前后需要使用空格分隔。	• request_time in [100 200] • request_time in (100 200]
#""	用于搜索包含目标短语的日志，可以保证关键词出现的顺序。 **说明** 短语搜索中的星号（*）和问号（？）会被视为普通字符，因此短语搜索不支持模糊搜索，可以用来搜索日志中的星号（*）和问号（？）。	request_method:#"GET POST"

搜索语句示例

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

图 5-5 搜索示例

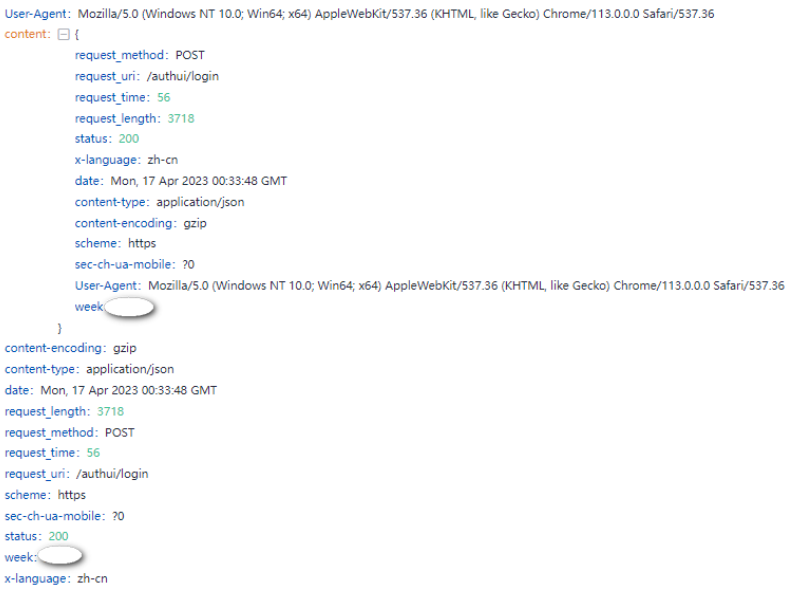


表 5-15 普通搜索示例

搜索需求	搜索语句
搜索POST请求且状态码为200的日志。	request_method:POST and status=200

搜索需求	搜索语句
搜索GET请求或POST请求成功（状态码为200~299）的日志。	(request_method:POST or request_method:GET) and status in [200 299]
搜索GET请求或POST请求失败的日志。	(request_method:POST or request_method:GET) not status in [200 299]
搜索非GET请求的日志。	not request_method:GET
搜索GET请求成功且请求时间小于60秒的日志。	request_method:GET and status in [200 299] not request_time>=60
搜索请求时间为60秒的日志。	• request_time:60 • request_time=60
搜索请求时间大于等于60秒，并且小于200秒的日志。	• request_time>=60 and request_time<200 • request_time in [60 200)
搜索包含and的日志。	content:"and" **说明** 此处使用双引号将and包裹，and为普通字符串，不代表运算符。
搜索不存在user字段的日志。	not user:*
搜索user字段值为空的日志。	user:""
搜索星期字段值不为星期一的日志。	not week:星期一
搜索sec-ch-ua-mobile字段值为?0的日志。	sec-ch-ua-mobile:#"?0" **说明** 日志内容中包含*或?且需要搜索时，需要采用短语查询。

更复杂的搜索示例请参考**表5-16**。

表 5-16 模糊搜索

搜索需求	搜索语句
搜索包含以GE开头的词的日志。	GE*
搜索包含以GE开头，结尾只有一个字符的词的日志。	GE?
搜索request_method字段值包含以G开头的词的日志。	request_method:G*

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

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

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

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

  表 5-17 基于分词符的搜索

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

5.4.3 创建 LTS 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，查询指定日志关键词，云服务日志LTS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。

说明

- 支持对前100000条日志进行分析。

  快速分析的目的是快速返回字段值的分布情况和变化趋势，并没有对全量数据进行分析，是一种采样结果。
- 支持通过查询时间和查询条件过滤日志进行分析。

  快速分析是对通过查询语句查询到的日志进行分析，当查询到的日志数目为零时，快速分析没有结果。
- 支持将快速分析生成查询语句。

  单击快速分析的某一行分析结果，可自动生成查询语句，查询日志并生成新的快速分析。
- 快速分析的字段长度最大为2KB字节。
- 快速分析字段分布统计展示前100条数据。
- 在快速分析的字段中，当分析时间范围内未开启快速分析、字段不存在或字段值为null时，分析结果为null。
  - 当字段为string类型时，单击null添加到搜索框中将显示为字段 : "null"OR NOT 字段 : *。
  - 当字段为float或long类型时，单击null添加到搜索框中将显示为NOT 字段 : *。
  - 未开启快速分析期间，不会存储分析所用的列存数据，分析结果对应为null，此时查询日志没有实际含义，不一定能匹配到日志。

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**设置云端结构化解析日志**。

创建快速分析

快速分析以日志流为单位，请参考如下步骤创建快速分析。

步骤1 登录**云日志服务控制台**，进入“日志管理”页面。

步骤2 单击目标日志组或日志流名称，进入日志详情页面。

步骤3 在“日志搜索”页签，单击 进入“索引配置”页面，在字段索引下方，添加字段时开启快速分析。

步骤4 单击“确定”，快速分析创建完成。

说明

- 表示String类型字段。
- 表示float类型字段。
- 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。
- 支持显示当前字段的采样数量。
- 单击  即可查看一键生成的图表展示，string类型的字段支持展示字段分布值统计和智能聚合时间折线图，long和float数值类型的字段只支持展示智能聚合时间折线图。单击图表即可进入详情页面。
- 单击字段分布值统计或智能聚合时间折线图，会自动跳转到可视化界面并生成对应的SQL查询语句进行查询，更加直观地展示字段值的分布和变化趋势。更多信息请参见**可视化**。

----结束

二次分析

快速分析功能支持对float类型和long类型的字段进行二次分析，具体如下：

快速统计最大项、最小项、平均值和总和，分别单击目标字段下的**Max**、**Min**、**Avg**、**Sum**，快速查找所有项中的最大项、最小项、平均值和总和。

5.4.4 保存 LTS 快速查询日志条件

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，通过保存的快速查询语句，可实现对日志的快速执行查询和分析操作。

保存 LTS 快速查询日志条件

步骤1 登录**云日志服务控制台**，进入“日志管理”页面。

步骤2 单击目标日志组或日志流名称，进入日志详情页面。

步骤3 在“日志搜索”页签，单击，输入“快速查询名称”和“快速查询语句”。默认开启快速查询和快速查询（保存本地）。

图 5-6 创建快速查询

- 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*”。

步骤4 单击“确定”，完成快速查询条件的创建。在左侧导航栏的快速查询页签，即可查看到保存成功的语句。

单击快速查询语句的名称，查看日志详情。

----结束

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。

步骤1 在日志详情页面的“日志搜索”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。

步骤2 在弹出的查看上下文页面中，请参考**表5-18**。

表 5-18 查看上下文日志功能介绍

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

----结束

5.5 查看 LTS 实时日志

日志接入云日志服务后，每隔大约1分钟上报一次。因此，在实时日志页面，您最多需要等待1分钟左右，即可查看实时上报的日志，实现对日志数据的快速检索与分析。

- 若实时日志大于1MB且总数小于2000条时时，LTS会清空前500KB的日志，保留最新的500KB日志。
- 若实时日志未超过1MB，但总数超过2000条时，LTS会清空前1000条日志，保留最新的1000条日志。

说明

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。

前提条件

- 已创建日志组和日志流。
- 已完成**安装ICAgent（区域内主机）**。

- 已配置日志采集规则。

查看 LTS 实时日志

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。

步骤1 登录云日志服务控制台，进入“日志管理”页面。

步骤2 单击目标日志组或日志流名称，进入日志详情页面。

步骤3 选择“实时日志”页签，可查看实时日志。

说明

通过来源类型分别筛选主机和K8S的日志。

- 来源类型选择主机时， 设置主机IP和文件路径。
- 来源类型选择K8S时，设置实例名称、容器名称和文件路径。

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。

- 字段过滤：从索引配置、结构化配置、最新日志获取。
- 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。

----结束

5.6 分析 LTS 日志

可视化提供对结构化后的日志字段进行SQL查询与分析的功能。对原始日志结构化后，等待1~2分钟左右，即可对结构化后的日志进行SQL查询与分析。

说明

目前此功能支持全部用户使用的局点有：华南-广州、华北-北京四、华东-上海一、华东-上海二、中国-香港、西南-贵阳一、亚太-新加坡、华北-北京一；支持部分白名单用户使用的局点有：亚太-曼谷、华南-深圳、中东-利雅得、亚太-雅加达，其他局点暂不支持该功能。

前提条件

- 已成功采集到日志。
- 对日志内容已完成结构化配置，具体操作请参考设置云端结构化解析日志。

说明

日志结构化后字段名称与系统SQL内置保留字段名称相同，或者字段名称中带有中划线、下划线、小数点这三种特殊字符时，SQL查询需要加英文双引号。系统SQL内置保留字段名称包括："time"、"select"、"where"等。

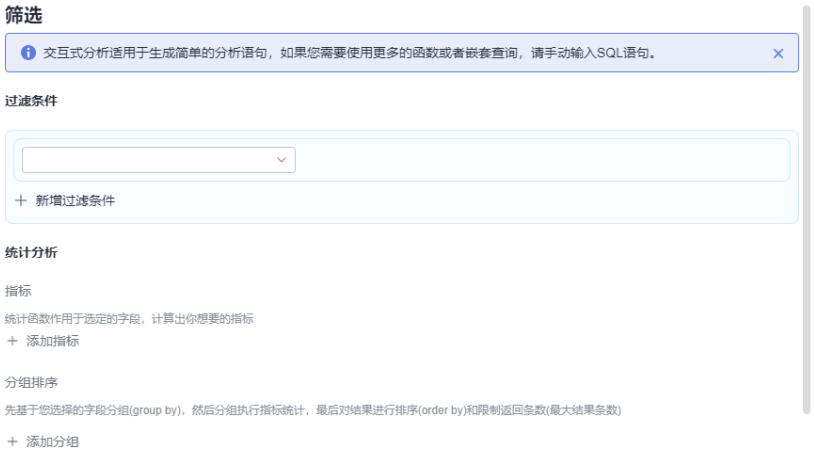
分析日志

步骤1 登录**云日志服务控制台**，进入“日志管理”页面。

步骤2 单击目标日志组或日志流名称，进入日志详情页面。

步骤3 选择“日志分析”页签。

步骤4 在可视化页面支持交互式分析，通过该模块配置简单的分析语句，查询可视化数据，配置可视化图表。设置过滤条件，通过添加指标、添加分组、添加排序进行数据分析，方便用户操作。



步骤5 选择时间范围，参考**SQL分析语法介绍**输入SQL语句，单击“查询”，在下方区域通过不同类型图表展示搜索结果。

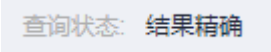
时间范围有三种方式，分别是相对时间、整点时间和自定义。您可以根据自己的实际需求，选择时间范围。

- 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：表示查询指定时间范围的日志数据。

说明

- SQL查询约束有：
  1. 单次查询返回结果最多10W条。
  2. 当聚合结果超过10W时，聚合结果可能存在误差。
- SQL查询语句中，string类型的where条件的键值有限制：
  1. 精确查找value需添加英文单引号， 模糊查找value需添加英文单引号或者双引号，key与SQL内置保留字段名称相同时需添加英文双引号。
  2. 建议使用where条件时，使用where "key"='value'，或者where "key" like '%value%'。
- SQL查询语句中，float和long类型的where条件不受限制，但当与关键词冲突时可能会导致查询异常，建议使用where "key"='value'，或者where "key" like '%value%'进行查询。
- 日志搜索框支持自定义上下拖动调整高度。
- 输入搜索语法后，单击 设置格式化sql和反格式化sql，优化搜索语句，提高搜索效率。

步骤6 当设置时间范围内日志量超过10亿行时会触发迭代查询，可以通过迭代查询分多次完成全部日志的查询，界面会显示“查询状态：结果精确”。



步骤7 根据SQL查询返回的数据，依照业务需求选择不同图表类型，呈现查询结果。详细请参考**使用统计图表将日志可视化**。

步骤8 对查询结果可执行如下操作：

- 单击“新建”，在弹出的“创建可视化图表”中，根据业务需求填写“图表名称”，开启“同时添加到仪表盘”，单击“确定”，可视化图表保存成功。
- 单击“保存”，对在弹出的“保存可视化图表”中，根据业务需求填写“图表名称”，开启“同时添加到仪表盘”，单击“确定”，可视化图表保存成功；当选中某个可视化图表时，单击“保存”，可对该图表进行修改。
- 单击“另存为”，在弹出的“另存为可视化图表”中，根据业务需求填写“图表名称”，开启“同时添加到仪表盘”，单击“确定”，对已有可视化图表进行复制。

  说明

  须先保存一个图表后，才可另存为可视化图表。
- 单击“下载”，可下载当前SQL查询结果的可视化数据，该文件为.csv。
- 单击 按钮添加告警，在弹出的“新建告警规则”中，为选中的可视化图表配置**创建SQL告警规则**。

  说明

  须先保存一个图表后，才能新建告警规则。
- 单击“展开图表”，可对当前日志流下的可视化图表展开；单击“收起图表”，可收起当前日志流下展开的可视化图表。

----结束

5.7 SQL 分析语法介绍

5.7.1 SQL 查询语法概述

SQL是用于访问和处理数据库的标准计算机语言。LTS SQL提供了查询日志流中结构化数据的语句, 以下均将 LTS SQL 称为 SQL。

SQL语言由用于处理数据库和数据库对象的命令和函数组成。使用该语言时需遵循有关表达式和文本使用的规则。因此在SQL参考章节，除了SQL语法参考外，还会看到有关表达式、函数和操作符等信息。SQL基本查询语句如下：

说明

目前此功能支持全部用户使用的局点有：华南-广州、华北-北京四、华东-上海一、华东-上海二、中国-香港、西南-贵阳一、亚太-新加坡、华北-北京一；支持部分白名单用户使用的局点有：亚太-曼谷、华南-深圳、中东-利雅得、亚太-雅加达，其他局点暂不支持该功能。

语法格式

```
SELECT [ ALL | DISTINCT ] { * | exprs }
FROM { <subquery>}
[ WHERE where_condition ]
[ GROUP BY [ col_name_list ]
[ HAVING expr ]
[ ORDER BY expr [ ASC | DESC ], expr [ ASC | DESC ], ... ]
[ LIMIT limit ]
[ OFFSET offset ]
```

数据类型

SQL查询中支持的数据类型如表5-19。如果当前字段数据类型需要改为其他数据类型，我们会进行数据类型的转换。例如STRING类型的字段转为LONG类型。字段数据类型转换之后的结果将会显示默认值，如STRING类型的数据转换为LONG类型的数据，结果会显示为LONG类型的默认值0。同理，当空值被转换为非空类型值时，也会使用默认值进行替换。例如，当把STRING类型空值转换为数字类型时，将会返回默认值0。

说明

SQL语法中，字符必须被单引号（''）包裹，无符号或双引号（""）包裹的为字段或表名称，如：'msg'表示字符串msg，msg或"msg"表示日志结构化msg字段。

表 5-19 SQL 查询支持的数据类型

原生数据类型	默认值	说明
STRING	""	原生STRING类型
FLOAT	0.0	原生FLOAT类型
LONG	0	原生LONG类型

查询语句

表 5-20 SQL 查询语句

语句	说明	示例
DISTINCT	返回去重后的结果。	SELECT DISTINCT visitCount
FROM	表示当前查询数据的源数据集， 可以是当前日志流的结构化数据, 也可以是当前日志流结构化数据的一个子集。 不加FROM的时候默认从当前日志流结构化数据查询，如果查询的数据源是一个子集， 则需要自己编写子查询语句。	SELECT visitCount

语句	说明	示例
WHERE	指定查询的过滤条件，支持算术运算符、关系运算符和逻辑运算符。具体过滤条件可填在where_condition处。	SELECT visitCount WHERE visitCount > 0
GROUP BY	指定作为分组依据的结构化字段，支持根据单字段或多字段分组。具体的结构化字段列表可填入col_name_list处。	SELECT host, count(*) AS pv WHERE visitCount > 0 GROUP BY host
HAVING	只能与GROUP BY配合使用。指定用于过滤GROUP BY结果的结构化字段。	SELECT host, count(*) AS pv GROUP BY host HAVING pv > 10
ORDER BY	后面的字段必须是用于GROUP BY分组的字段，对GROUP BY的查询结果进行排序，用于排序的可以是任意一个结构化字段。	SELECT host, count(*) AS pv GROUP BY host ORDER BY pv
ASC/DESC	ASC为升序，DESC为降序，默认为ASC。	SELECT host, count(*) AS pv GROUP BY host ORDER BY pv DESC
LIMIT	对查询结果进行限制，用于限制返回的结构化日志条数。一次查询最多返回100000条结构化日志。 **说明** 如果不使用LIMIT语句，默认返回查询结果中最新的100条数据。	SELECT host LIMIT 100

示例

表 5-21 常用 SQL 查询语句示例

查询需求	查询语句
标准查询	SELECT "field" WHERE "field" = 'value'
统计行数	SELECT count(*)
列的别名	SELECT count(*) AS "pv"
去重查询	SELECT DISTINCT("field")
分页查询	SELECT "field" LIMIT 100
排序查询	SELECT "__time" ORDER BY "__time"

查询需求	查询语句
分组查询	SELECT "field" GROUP BY "field"
分组统计	SELECT "field",count(*) GROUP BY "field"
模糊查询	SELECT "field" LIKE 'value%'
查询总和	SELECT sum("field")
查询最大值	SELECT max("field")
查询最小值	SELECT min("field")
查询平均值	SELECT avg("field")
SQL嵌套子查询	SELECT sum(pv) FROM (SELECT "field",count(*) AS "pv" GROUP BY "field")
HAVING子句过滤	SELECT "field",count(*) AS "pv" GROUP BY "field" HAVING "pv" > 10
查询包含GET，POST请求	SELECT * WHERE "request_method" IN ('GET', 'POST')
查询不包含GET，POST请求	SELECT * WHERE "request_method" NOT IN ('GET', 'POST')
查询非GET请求的日志	SELECT * WHERE "request_method" != 'GET'
查询GET请求成功并且状态码为200且请求时间小于60秒的日志	SELECT * WHERE "request_method" = 'GET' AND "request_time" < 60
查询请求时间大于等于60秒，并且小于200秒的日志	SELECT * WHERE "request_ time" >=60 and "request_time" < 200
查询GET请求或POST请求的日志	SELECT * WHERE "request_method" = 'GET' OR "request_method" = 'POST'

下面的语句是根据ELB结构化日志构造出的查询语句， 它包含所有的基础查询语法，仅供参考。

```
SELECT url AS Url, host AS Host, failure_rate AS FailureRate,
CONCAT(CAST(access_count AS varchar), ' times') AS "All",
CONCAT(CAST(rsp_200_count AS varchar), ' times') AS "COUNT_200"
FROM ( SELECT
CONCAT(host, CASE WHEN STRPOS(router_request_uri, '?') = 0 THEN router_request_uri ELSE
SUBSTR(router_request_uri, 1, 1) END) AS url,
host,count(1) AS access_count,
SUM(CASE WHEN status = 200 THEN 1 ELSE 0 END) AS "rsp_200_count",
(CASE WHEN COUNT(1) < 30 THEN 0 ELSE round(SUM(CASE WHEN status >= 400 THEN 1 ELSE 0 END) *
100.0 / COUNT(1), 2) END) AS failure_rate
WHERE host NOT IN ('monitor-new.olayc.cn')
GROUP BY host,router_request_uri
HAVING router_request_uri NOT IN ('/robots.txt', '/null', '/undefined')
```

```
)
ORDER BY FailureRate DESC
LIMIT 100
```

5.7.2 SQL 聚合函数

聚合函数是对结构化后的日志的指定列进行的统计运算。聚合函数返回的是单个值，经常与SELECT语句和GROUP BY语句一起使用。LTS支持如下表格所示聚合函数，具体请参考**表5-22**。

在聚合函数的使用中请注意以下几点：

- 聚合函数可用在任何查询的SELECT子句中。您可以使用如AGG(expr) FILTER(WHERE whereExpr)的语法在聚合之前进行过滤，即聚合函数只会聚合满足过滤条件的列。
- 在同一个SQL查询语句中，根据过滤条件的不同，对应的聚合函数所呈现的结果会不同。
- 只有COUNT函数可以跟DISTINCT搭配使用。
- 聚合操作没有固定的执行顺序。如果在执行具有多个聚合函数的SQL语句查询时，执行聚合函数的顺序对运算结果有影响，即结果会因执行顺序的不同而不同，那么每次执行这个查询，得出的结果可能会不一致。
- 如果需要聚合的数据为FLOAT类型时，数次执行同一个查询可能也会因此得出不同的聚合结果。如果您希望执行同一个查询时都能得出同样的结果，建议使用ROUND函数来消除多次查询之间的不一致。

语法格式

```
SELECT COUNT(fieldname1)
```

聚合函数语句

表 5-22 聚合函数语句

语句	说明	示例
COUNT(*)	统计行数。	SELECT COUNT(*)
COUNT(DISTINCT expr)	统计字段中去重后的行数，字段值可以是字符串或者数字，返回值为估算值（**默认存在2.3%的标准误差**）。	SELECT COUNT(DISTINCT host)
SUM(expr)	返回数字总和。	SELECT SUM(visitCount)
MIN(expr)	返回数字中的最小值。	SELECT MIN(visitCount)
MAX(expr)	返回数字中的最大值。	SELECT MAX(visitCount)
AVG(expr)	返回平均值。	SELECT AVG(visitCount)
EARLIEST(expr)	表达式必须是数值类型的， 返回expr的最早的值， 即查询的时候最先遇到的值。	SELECT EARLIEST(visitCount)

语句	说明	示例
LATEST(expr)	表达式必须是数值类型的， 返回expr的最新的值， 即查询的时候最后遇到的值。	SELECT LATEST(visitCount)
APPROX_QUANTILE_DS(expr, probability)	计算数值expr的近似分位数，probability应介于0和1之间。	APPROX_QUANTILE_DS(expr, probability)

5.7.3 SQL 同比和环比函数

本文介绍同比和环比函数的基础语法和示例。

compare 函数

compare函数用于对比当前时间周期内的计算结果与n秒之前时间周期内的计算结果。

语法格式

- 对比当前时间周期内的计算结果与n秒之前时间周期内的计算结果。
  ```
  compare(x,n)
  ```
- 对比当前时间周期内的计算结果与n1、n2、n3秒之前时间周期内的计算结果。
  ```
  compare(x, n1, n2, n3...)
  ```

参数说明

表 5-23 同比函数参数说明

参数	说明
x	目标列的列名，参数值为double类型或long类型。
n	时间窗口，单位为秒。例如3600（1小时）、86400（1天）、604800（1周）、31622400（1年）。

返回类型

JSON数组。格式为[当前计算结果,n秒前的计算结果,当前计算结果与n秒前计算结果的比值]。

示例说明

计算当前1小时和昨天同时段的访问量比值。

1. 选择查询和分析的时间范围为**1小时（整点时间）**，并执行如下查询和分析语句。其中**86400**表示当前时间减去86400秒(1天)。
   ```
   SELECT
   compare(PV, 86400)
   FROM  (SELECT count(*) AS PV )
   ```
2. 查询和分析结果

图 5-7 查询和分析结果

说明

- **5994.0**表示当前1小时（例如2021-01-02 00:00:00~2021-01-02 01:00:00）的网站访问量。
- **6000.0**表示昨天同时段（例如2021-01-01 00:00:00~2021-01-01 01:00:00）的网站访问量。
- **0.999**表示当前1小时与昨天同时段的网站访问量比值。

3. 分列显示查询和分析结果

```
SELECT
diff[1] as "today",
diff[2] as "yesterday",
diff[3] as "ratio"
FROM(SELECT compare(pv, 86400) AS diff FROM (SELECT count(*) AS pv ))
```

图 5-8 查询和分析结果

ts_compare 函数

ts_compare函数用于对比当前时间周期内的计算结果与n秒之前时间周期内的计算结果。

说明

ts_compare函数必须按照时间列进行分组（GROUP BY）。

语法格式

- 对比当前时间周期内的计算结果与n秒之前时间周期内的计算结果。
  ```
  ts_compare(x, n)
  ```
- 对比当前时间周期内的计算结果与n1、n2、n3秒之前时间周期内的计算结果。
  ```
  ts_compare(x, n1, n2, n3...)
  ```

参数说明

表 5-24 环比函数参数说明

参数	说明
x	参数值为double类型或long类型。
n	时间窗口，单位为秒。例如3600（1小时）、86400（1天）、604800（1周）、31622400（1年）。

返回类型

JSON数组。格式为[当前计算结果, n秒前的计算结果, 当前计算结果与n秒前计算结果的比值, n秒前的UNIX时间戳]。

示例说明

环比今天3小时与昨天3小时的网站访问量。

选择查询和分析的时间范围为今天某3小时，并执行如下查询和分析语句。其中86400表示当前时间减去86400秒（1天），date_trunc('hour',__time)表示使用date_trunc函数将时间对齐到小时。

- 查询和分析语句

```
SELECT
  t_time,
  ts_compare(PV, 86400) AS data
FROM(
    SELECT
      date_trunc('hour', __time) AS t_time,
      count(*) AS PV
    GROUP BY
      t_time
    ORDER BY
      t_time
  )
GROUP BY
  t_time
```

- 查询和分析结果

t_time	data
2021-10-26T06:00:00.000Z	[159.0,224.0,0.7098214285714286,1.6351416E9]
2021-10-26T07:00:00.000Z	[100.0,148.0,0.6756756756756757,1.6351452E9]
2021-10-26T08:00:00.000Z	[100.0,100.0,1.0, 1.6016544E9, 1.6351488E9]

5.7.4 SQL JSON 函数

功能描述

JSON函数用于解析JSON对象或JSON数组，并从中提取值。

语法格式

```
SELECT json_extract(Results, '$.[0].EndTime')
```

JSON 函数语句

表 5-25 JSON 函数语句

语句	说明	示例	返回值类型
json_extract	用于从JSON对象或JSON数组中提取一组JSON值（数组或对象）。	json_extract(x, json_path)	JSON格式的string类型
json_extract_scalar	用于从JSON对象或JSON数组中提取一组标量值（字符串、整数或布尔值）。如果指定JSON路径下不是标量，则返回null。	json_extract_scalar(x,json_path)	varchar类型

示例及说明

- **json_extract函数**

  获取Results字段中EndTime字段的值。

  a. 字段样例
  ```
  Results:[{"EndTime":1626314520},{"FireResult":2}]
  ```

  b. 查询和分析语句
  ```
  SELECT json_extract(Results, '$.[0].EndTime')
  ```

  c. 查询和分析结果

  表 5-26 查询和分析结果

EXPR$0
1626314520

- **json_extract_scalar函数**

  从Results字段中获取RawResultCount字段的值，并将这些值转换为bigint类型进行求和。

  a. 字段样例
  ```
  Results:[{"EndTime":1626314520},{"RawResultCount":1}]
  ```

  b. 查询和分析语句
  ```
  SELECT sum(cast(json_extract_scalar(Results,'$.[1].RawResultCount') AS bigint) )
  ```

  c. 查询和分析结果

  表 5-27 查询和分析结果

EXPR$0
1546

5.7.5 SQL IP 函数

使用限制

LTS提供的IP与地域之间的关系，来自于第三方IP库，且数据是周期性更新（约半年），不承诺IP与地域关系完全正确；后续LTS会优化，缩短IP库的更新周期，为用户提供更好的体验。

单IP函数聚合查询的数据量上限为500万，查询的数据超出上限可能导致查询超时。

功能描述

IP函数是分析目标IP地址所属的国家、省份、城市及对应的网络运营商。

语法格式

```
SELECT count(*) AS PV, ip_to_province(client_ip) AS province GROUP BY province
```

IP 函数语句

表 5-28 IP 函数语句

语句	说明	示例
ip_to_province	分析目标IP地址所属省份。	ip_to_province(x)
ip_to_country	分析目标IP地址所属国家或地区。	ip_to_country(x)
ip_to_city	分析目标IP地址所属城市。	ip_to_city(x)
ip_to_provider	分析目标IP地址所对应的网络运营商。	ip_to_provider(x)
ip_to_geo	根据传入的ip返回ip所在的经纬度。	ip_to_geo(x)

示例及说明

- **ip_to_province函数**

  统计请求总数Top3的省份。

  a. 查询和分析语句

  ```
  SELECT count(*) AS PV, ip_to_province(client_ip) AS province GROUP BY province ORDER BY PV desc LIMIT 3
  ```

  b. 查询和分析结果

  表 5-29 查询和分析结果

PV	province
101	广东

PV	province
83	上海
78	山东

- **ip_to_country函数**

  统计请求总数的Top3的国家或地区。

  a. 查询和分析语句

  ```
  SELECT count(*) AS PV, ip_to_country(client_ip) AS country GROUP BY country ORDER BY PV desc LIMIT 3
  ```

  b. 查询和分析结果

  表 5-30 查询和分析结果

PV	country
100	中国
76	美国
55	加拿大

- **ip_to_city函数**

  统计请求总数的Top3的城市。

  a. 查询和分析语句

  ```
  SELECT count(*) AS PV, ip_to_city(client_ip) AS city GROUP BY city ORDER BY PV desc LIMIT 3
  ```

  b. 查询和分析结果

  表 5-31 查询和分析结果

PV	city
109	广州
89	上海
23	西安

- **ip_to_provider函数**

  统计请求总数的Top3的运营商。

  a. 查询和分析语句

  ```
  SELECT count(*) AS PV, ip_to_provider(client_ip) AS provider GROUP BY provider ORDER BY PV desc LIMIT 3
  ```

  b. 查询和分析结果

表 5-32 查询和分析结果

PV	provider
115	电信
65	att.com
44	联通

- **ip_to_geo函数**

  根据传入的ip返回经纬度。

  a. 查询和分析语句

  ```
  SELECT count(*) AS PV, ip_to_geo (client_ip) AS geo GROUP BY geo ORDER BY PV desc LIMIT 3
  ```

  b. 查询和分析结果

  表 5-33 查询和分析结果

PV	geo
101	*, *
83	47.369013, -68.326674
78	32.715891, -117.161588

5.7.6 SQL 数学函数

功能描述

数学函数为标量函数中的一种，只支持数值类型的字段，能够实现对数值进行取整、取绝对值、求余等功能，具体请参考表5-34。

在数学运算中，如果表达式里涉及的操作数皆为整数，那么SQL将会采用整数运算，否则便会切换到浮点运算。您可以将其中一个操作数转换为FLOAT类型来强制进行切换，运行时SQL会将大多数表达式中的32位浮点数扩展到64位。

语法格式

```
SELECT ABS(fieldname1) AS fieldname1_abs
```

数学函数语句

表 5-34 数学函数语句

语句	说明	示例
ABS(expr)	取绝对值。	SELECT ABS(fieldname1)
CEIL(expr)	向上取整，即向上取最接近的整数值	SELECT CEIL(fieldname1)

语句	说明	示例
FLOOR(expr)	向下取整，即向下取最接近的整数值。	SELECT FLOOR(fieldname1)
TRUNCATE(expr, digits)	将expr截断为特定的digits位数。如果数字为负数，则会截断小数点左侧的许多位置。如果未指定，数字默认为零。	SELECT TRUNCATE(fieldname1, 2)
ROUND(expr, digits)	ROUND(expr, digits)对expr值进行四舍五入，保留小数位数由digits指定。expr可以是整数或浮点数，但digits必须是整数。返回值的类型由expr的类型决定。如果没有指定digits，则使用默认值0。如果digits是负数，则返回expr四舍五入后的整数。当expr是非数字值时，会被转换为数字0。如果expr是无限位数的数字，则被转换为最接近的DOUBLE类型的有限位数数字。	SELECT ROUND(fieldname1, 2)
x + y	加法。	SELECT fieldname1 + fieldname2
x - y	减法。	SELECT fieldname1 - fieldname2
x * y	乘法。	SELECT fieldname1 * fieldname2
x / y	除法。	SELECT fieldname1 / fieldname2
MOD(x, y)	求余，即取x除以y后的余数。	SELECT MOD(fieldname1, fieldname2)
LN(expr)	对数(以e为底)。	SELECT ln(expr)
LOG10(expr)	对数(以10为底)。	SELECT LOG10(expr)
POWER(expr,power)	expr的power次幂。	SELECT POWER(expr ,2)
SQRT(expr)	expr的平方根	SELECT SQRT(expr)
SIN(expr)	正弦	SELECT SIN(expr)
COS(expr)	余弦	SELECT COS(expr)
TAN(expr)	正切	SELECT TAN(expr)

语句	说明	示例
COT(expr)	余切	SELECT COT(expr)
ASIN(expr)	反正弦	SELECT ASIN(expr)
ACOS(expr)	反余弦	SELECT ACOS(expr)
ATAN(expr)	反正切	SELECT ATAN(expr)

示例及说明

ACOS(expr)函数

求参数值的反余弦，y=arccosx，x的取值范围[-1,1]。

1. 字段样例
   x:0.5
2. 查询和分析语句
   ```
   select  ACOS(x)
   ```
3. 查询和分析结果

表 5-35 查询和分析结果

x	EXPR$1
0.5	1.0471975511965979

ATAN(expr)函数

ATAN求参数值的反正切，y= arctanx，x的取值范围R。

1. 字段样例
   x:0.5
2. 查询和分析语句
   ```
   select  ATAN(X)
   ```
3. 查询和分析结果

表 5-36 查询和分析结果

x	EXPR$1
0.5	1.0471975511965979

ATAN2(expr)函数

ATAN2从直角坐标（x，y）到极坐标（r，θ）的转换角度θ。

1. 字段样例
   x:3；y:4

2. 查询和分析语句
```
SELECT x , y, ATAN2(x,y)
```
3. 查询和分析结果

表 5-37 查询和分析结果

x	y	EXPR$0
3	4	0.6435011087932844

5.7.7 SQL 时间函数

功能描述

时间函数可以与__time一起使用，任何存储为毫秒时间戳的列都可以使用 MILLIS_TO_TIMESTAMP 函数，或者任何存储为字符串时间戳的列都可以使用 TIME_PARSE 函数。默认情况下，时间操作使用UTC时区，您可以通过参数"timezone"设置为另一个时区的名称（如"Asia/Shanghai"）或设置为偏移量（如"+08:00"）来更改时区。

语法格式

语句	说明	示例
CURRENT_DATE	在连接时区的当期日期。	SELECT CURRENT_DATE
CURRENT_TIMESTAMP	在连接时区的当前时间戳。	SELECT CURRENT_TIMESTAMP
DATE_TRUNC(<unit>,<expr>)	截断时间戳，将其作为新时间戳返回。	SELECT DATE_TRUNC('minute',__time)
TIME_FORMAT(<expr>,<patten>,<timezone>))	使用给定的 pattern 或 ISO8601（例如 2000-01-02T03:04:05Z）将字符串解析为时间戳。timezone（如果提供）应为时区名称，如"America/Los_Angeles"或偏移量，如"+08:00"，并将用作不包括时区偏移量的字符串的时区。模式和时区必须是字面量。无法解析为时间戳的字符串将返回空值。	SELECT TIME_FORMAT(__time,'yyyy-MM-dd HH:mm:ss','+08:00')

语句	说明	示例
TIME_PARSE(<expr>,<pattern>,<timezone>)	使用给定的 pattern 或 ISO8601（例如 2000-01-02T03:04:05Z）将字符串解析为时间戳。时区（如果提供）应为时区名称，如 "America/Los_Angeles"或偏移量，如"+08:00"，并将用作不包括时区偏移量的字符串的时区。模式和时区必须是字面量。无法解析为时间戳的字符串将返回空值。	SELECT TIME_PARSE("timestamp",'yyyy-MM-dd HH:mm:ss','+08:00')
MILLIS_TO_TIMESTAMP(expr)	将时间戳转换为时间格式。	SELECT MILLIS_TO_TIMESTAMP(expr)
TIMESTAMP_TO_MILLIS(expr)	将时间转换为时间戳格式	SELECT TIMESTAMP_TO_MILLIS (expr)
EXTRACT(<extract_unit>FROM expr)	从expr中提取时间部分，并将其作为数字返回。	SELECT EXTRACT(MINUTE FROM __time)
TIMESTAMPDIFF(<unit>,<expr1>,<expr2>)	返回expr1和expr2之间的unit	SELECT TIMESTAMPDIFF (minute, expr1, expr2)
TIME_SERIES	补全您查询时间窗口内缺失的数据。	TIME_SERIES(__time, period, time_format, [padding_value],<timezone>)

TIME_SERIES 函数

time_series函数用于补全您查询时间窗口内缺失的数据。

说明

- 必须搭配ORDER BY语法使用，并且time_series函数是ORDER BY的第一个参数
- 查询语句中不能使用OFFSET语句
- time_series函数不支持作为子查询使用

语法格式

```
time_series(__time, period, time_format, [padding_value], <timezone>)
```

参数说明

表 5-38

参数	说明
__time	时间序列。
period	ISO 8601标准的时间窗口大小。例如P1M（1月）、P1D（1天）、PT1H（1小时）、PT1M（1分钟）、PT1S（1秒钟）。
time_format	返回结果的时间格式。（参考**Joda DateTimeFormat**模式）。
padding_value	补全的内容。包括： • 0 或 zero：将缺失的值设置为0（默认值）。 • null：将缺失的值设置为null。 • last：将缺失的值设置了上一个时间点对应的值。 • next：将缺失的值设置了下一个时间点对应的值。 • avg：将缺失的值设置为前后两个时间点的平均值。
timezone	时区。例如：北京时区：+08:00

返回类型

bigint类型。

示例说明

按照一天的时间粒度进行数据补全，将缺失的值设置为0，并添加时区。

- 查询和分析语句

```
select time_series(__time, 'P1D', 'yyyy-MM-dd HH:mm:ss', '0', '+08:00') as t_time, count(*) as num
group by t_time order by t_time
```

- 查询和分析结果

t_time	num
2021-10-01 08:00:00	5
2021-10-02 08:00:00	0
2021-10-03 08:00:00	0
2021-10-04 08:00:00	21
2021-10-05 08:00:00	17
2021-10-06 08:00:00	0
2021-10-07 08:00:00	34

CURRENT_DATE/ CURRENT_TIMESTAMP 函数

CURRENT_DATE返回查询当天的凌晨零点的ISO8601时间，返回的为UTC时间，该函数可直接参与时间戳之间的运算。

CURRENT_TIMESTAMP返回查询当前的ISO8601时间，返回的为UTC时间，该函数可直接参与时间戳之间的运算。

1. 字段样例

   __time: 2023-02-14T02:35:56.706Z

2. 查询和分析语句

```
select __time,CURRENT_DATE, CURRENT_TIMESTAMP,CURRENT_TIMESTAMP
```

3. 查询和分析结果

表 5-39 查询和分析结果

__time	CURRENT_DATE	CURRENT_TIMESTAMP
2023-02-14T02:35:56.706Z	2023-02-14T00:00:00.000Z	2023-02-14T14:35:57.000Z

DATE_TRUNC(<unit>, <timestamp_expr>)函数

舍去时间戳<timestamp_expr>中精度大于所选单位<unit>的值，将其置为零，并作为新时间戳返回。单位可以是'milliseconds'（毫秒）, 'second'（秒）, 'minute'（分）, 'hour'（时）, 'day'（日）, 'week'（周）, 'month'（月）, 'quarter'（季）, 'year'（年）, 'decade'（十年）, 'century'（千年）,'millennium'（世纪）, unit不区分大小写。

1. 字段样例

   __time: 2023-02-14T02:35:56.706Z

2. 查询和分析语句

```
SELECT __time,DATE_TRUNC('minute', __time),DATE_TRUNC('day', __time),DATE_TRUNC('year', __time)
```

3. 查询和分析结果

表 5-40 查询和分析结果

__time	EXPR$1	EXPR$2	EXPR$3
2023-02-14T02:35:56.706Z	2023-02-15T08:50:00.000Z	2023-02-15T00:00:00.000Z	2023-01-01T00:00:00.000Z

TIME_PARSE(<string_expr>, [<pattern>, [<timezone>]])/ TIME_FORMAT(<timestamp_expr>, [<pattern>, [<timezone>]])函数

TIME_PARSE将给定的字符串<timestamp_expr>，依据用户自定义的<pattern>参数以**Joda DateTimeFormat**模式解析为时间戳。若<pattern>未填写则以默认的ISO8601将字符串解析。<timezone>为时区，可省略。

TIME_FORMAT将给定的时间戳< timestamp_expr>，依据用户自定义的<pattern>参数以 **Joda DateTimeFormat**模式解析为字符串。若<pattern>未填写则以默认的ISO8601将时间戳解析。<timezone>为时区，可省略。

1. 字段样例

   __time: 2023-02-16T07:38:25.306Z

   start_time:2023-02-14 02:35:56

2. 查询和分析语句

```
SELECT __time,TIME_PARSE(start_time,'yyyy-MM-dd HH:mm:ss'),TIME_FORMAT(__time,'yyyy-MM-dd HH:mm:ss')
```

3. 查询和分析结果

表 5-41 查询和分析结果

__time	EXPR$1	EXPR$2
2023-02-16T07:38:25.306Z	2023-02-14T02:35:56.000Z	2023-02-16 07:38:25

MILLIS_TO_TIMESTAMP(millis_expr)/ TIMESTAMP_TO_MILLIS(timestamp_expr)函数

MILLIS_TO_TIMESTAMP函数将毫秒值转化为ISO8601格式的时间戳，转化后的参数可进行时间戳之间的运算。TIMESTAMP_TO_MILLIS将时间戳转化为毫秒值。

1. 字段样例

   __time: 2023-02-16T07:54:15.106Z，start_time: 1676534055106

2. 查询和分析语句

```
SELECT __time,MILLIS_TO_TIMESTAMP(start_time),TIMESTAMP_TO_MILLIS(__time)
```

3. 查询和分析结果

表 5-42 查询和分析结果

__time	EXPR$1	EXPR$2
2023-02-16T07:54:15.106Z	2023-02-16T07:54:05.000Z	1676534055106

TIME_EXTRACT(<timestamp_expr>,[<unit>,[<timezone>]])/ EXTRACT(<unit> FROM timestamp_expr)函数

TIME_EXTRACT函数，从timestamp_expr中提取时间部分，并将其作为数字返回。单位可以是EPOCH（返回纪元以来的秒值unix）、SECOND（当前分钟的秒值）、MINUTE（当前小时中的分钟值）、HOUR（当天的小时值）、DAY（当月的天数）、DOW（当前周的天数）、DOY（当前年的天数）、WEEK（当前年的周数）、MONTH（当前的月数）、QUARTER（当年的季度）或YEAR（返回当前年份）。<timezone>为时区，可省略。EXTRACT函数为TIME_EXTRACT的简写形式。

1. 字段样例

   __time: 2023-02-16T07:54:15.106Z，start_time: 1676534055106

2. 查询和分析语句
```
SELECT __time,MILLIS_TO_TIMESTAMP(start_time),TIMESTAMP_TO_MILLIS(__time)
```
3. 查询和分析结果

表 5-43 查询和分析结果

__time	EXPR$1	EXPR$2
2023-02-16T07:54:15.106Z	2023-02-16T07:54:05.000Z	1676534055106

参考信息

- **unit说明**

unit	说明
second	秒
minute	分
hour	时
day	日
week	周
month	月
quarter	季
year	年

- **extract_unit说明**

extract_unit	说明
SECOND	秒
MINUTE	分
HOUR	时
DAY	每月的第几天
DOW	每周的第几天
DOY	每年的第几天
WEEK	每年的第几周
MONTH	月
QUARTER	季
YEAR	年

5.7.8 SQL 最值函数

功能描述

SQL提供最值函数，对字段进行最值求解，具体请参见表5-44

最值函数对零个或多个字段进行操作，并返回单个值。

在最值函数的使用中请注意以下几点：

- 如果没有设置字段，则返回空值。字段必须能够转换为常见的数据类型。
- 如果所有字段都为空值，则返回空值。如果只有部分字段为空值，这些字段会被忽略。
- 如果字段中既有数字也有字符串，则函数将它们作为字符串进行比较。
- 如果所有字段都是整数，则函数将它们作为LONG值进行比较。
- 如果所有字段都是数字且至少有一个是FLOAT值，则函数将它们作为FLOAT值进行比较。

语法格式

```
SELECT GREATEST(fieldname1,fieldname2) AS the_greatest_field
```

最值函数语句

表 5-44 最值函数语句

语句	说明	示例
GREATEST([expr1, ...])	返回零个或多个字段间的最大值。	SELECT GREATEST(fieldname1,fieldname2)
LEAST([expr1, ...])	返回零个或多个字段间的最小值。	SELECT LEAST(fieldname1,fieldname2)

5.7.9 SQL 字符串函数

功能描述

SQL提供字符串函数，用于对字符类型的数据执行拼接、大小写转换等操作，具体请参见表5-45。

说明

SQL语法中，字符必须被单引号（''）包裹，无符号或双引号（""）包裹的为字段或表名称，如：'msg'表示字符串msg，msg或"msg"表示日志结构化msg字段。

语法格式

```
SELECT (fieldname1 || fieldname2) AS fieldname1_fieldname2
```

字符串函数语句

表 5-45 字符串函数语句

语句	说明	示例
CONCAT(expr1, expr2...)	拼接列举的所有字符串。	SELECT str1, str2, str3, CONCAT(str1, str2, str3) WHERE str1 IS NOT NUll
TEXTCAT(expr, expr)	拼接两个字符串。	SELECT str1, str2, TEXTCAT(str1, str2) WHERE str1 IS NOT NUll
STRING_FORMAT(pattern[, args...])	根据JAVA的String格式对字符串进行格式化。	SELECT str1, STRING_FORMAT(str1, '%s') WHERE str1 IS NOT NUll
LENGTH(expr)	返回字符串的长度，即字符串中UTF-16字符个数。	SELECT LENGTH(str1) WHERE str1 IS NOT NUll
LOWER(expr)	将字符串转换为小写形式。	SELECT LOWER(str1) WHERE str1 IS NOT NUll
POSITION(string1 IN string2 [FROM fromIndex])	返回string1在string2中首次出现位置的索引。搜索从指定索引开始，如果没有指定索引，则从索引1开始。如果string1不存在于string2中，则返回0。	SELECT POSITION(str1 IN str2 FROM 5)
REGEXP_EXTRACT(expr, pattern, [index])	返回字符串中匹配指定正则表达式的子字符串。索引从1开始。如果没匹配，则返回空值。如果没有指定索引，或者索引为0，则返回第一个匹配的子字符串。如想精确匹配，请在正则表达式前后分别加上符号^和$。	SELECT REGEXP_EXTRACT(str1, '[A-Za-z]+://[A-Za-z0-9.-]+(/[^]*)', 5)
REGEXP_LIKE(expr, pattern)	判断字符串是否匹配指定的正则表达式。如想精确匹配，请在正则表达式前后分别加上符号^和$。该函数与LIKE语句用法类似，区别在于LIKE语句搜索的是匹配指定模式的内容。	SELECT REGEXP_LIKE(str1, '\.(jpg|jpeg|png|gif)$')
REPLACE(expr, pattern, replacement)	使用replacement替换expr中与pattern相同的子字符串。	SELECT REPLACE(expr,pattern, replacement)

语句	说明	示例
STRPOS(string1, string2)	返回string2在string1中首次出现位置的索引。查找从索引1开始。如果查找没有结果，则返回0。	SELECT STRPOS(str1, str2) WHERE str1 IS NOT NUll AND str2 IS NOT NUll
SUBSTRING(expr, index, [length])	截取字符串。从指定索引处开始截取，结束位置由指定长度决定。长度按照UTF-16字符个数计算。	SELECT SUBSTRING(str1, 3, 10) WHERE str1 IS NOT NUll
RIGHT(expr, [length])	从字符串最右处开始往左截取指定长度。	SELECT RIGHT(str1, 5) WHERE str1 IS NOT NUll
LEFT(expr, [length])	从字符串最左处开始往右截取指定长度。	SELECT LEFT(str1, 5) WHERE str1 IS NOT NUll
SUBSTR(expr, index, [length])	与SUBSTRING相同。	SELECT SUBSTR(str1, 3, 10) WHERE str1 IS NOT NUll
UPPER(expr)	将字符串转换为大写形式。	SELECT UPPER(str1) WHERE str1 IS NOT NUll
REVERSE(expr)	反转字符串。	SELECT REVERSE(str1) WHERE str1 IS NOT NUll
LPAD(expr, length, chars)	在字符串左侧填充指定字符，直至字符串达到指定长度。如果指定长度小于字符串本身的长度，则按照指定长度对字符串执行截断操作。如果字符串或指定字符为空值，则返回空值。如果指定字符为空白，不会执行填充操作，但如有必要可能会删减字符。	SELECT LPAD(str1, 50, 'testStr') WHERE str1 IS NOT NUll
RPAD(expr, length, chars)	在字符串右侧填充指定字符，直至字符串达到指定长度。如果指定长度小于字符串本身的长度，则按照指定长度对字符串执行截断操作。如果字符串或指定字符为空值，则返回空值。如果指定字符为空白，不会执行填充操作，但如有必要可能会删减字符。	SELECT RPAD(str1, 50, 'testStr') WHERE str1 IS NOT NUll
CONTAINS_STRING(<expr>, str)	判断expr是否包含str字符串	SELECT CONTAINS_STRING(log_level,'warn')

语句	说明	示例
ICONTAINS_STRING(<expr>, str)	判断expr是否包含str字符串，不区分字符串大小写	SELECT ICONTAINS_STRING(log_level,'WARN')

示例及说明

REPEAT函数

REPEAT(expr, [N])函数将expr重复N次。

1. 字段样例

   field4:is

2. 查询和分析语句

```
select field4,REPEAT(field4,3)
```

3. 查询和分析结果

表 5-46 查询和分析结果

field4	EXPR$1
Is	isisis

5.7.10 SQL SPLIT 函数

功能描述

SPLIT函数用于通过指定的分隔符拆分字符串，并返回拆分后的子串集合。

语法格式

```
SELECT split_to_map(x, delimiter01, delimiter02)
```

SPLIT 函数语句

语句	说明	示例	参数
split	split函数用于通过指定的分隔符拆分字符串，并返回拆分后的子串集合。	split(x, delimeter,[limit])	• x：参数值为varchar类型。 • delimeter：分隔符。 • limit：限制字符串拆分的个数，大于0的整数。

语句	说明	示例	参数
split_part	split_part函数通过指定的分隔符拆分字符串，并返回指定索引的内容。	split_part(x, delimeter, part)	• x：参数值为varchar类型。 • delimeter：分隔符。 • part：指定要返回字段的索引值。
split_to_map	split_to_map函数用于使用指定的第一个分隔符拆分字符串，然后再使用指定的第二个分隔符进行第二次拆分。	split_to_map(x, delimiter01, delimiter02)	• x：参数值为varchar类型。 • delimeter01：分隔符1。 • delimeter02：分隔符2。

示例及说明

- **split函数**

  将目标字符串按指定字符串分割，limit用于限制分割后的最大单词数，若不填写，则默认全部分割。

  a. 字段样例

     Id：dc1dab7e-b045-4e77-bda4-914d083d1bf7

  b. 查询和分析语句

  ```
  SELECT split(Id,'-'), split(Id,'-',2)
  ```

  c. 查询和分析结果

  表 5-47 split 函数查询和分析结果

EXPR$0	EXPR$1
["dc1dab7e","b045","4e77","bda4","914d083d1bf7"]	["dc1dab7e","b045-4e77-bda4-914d083d1bf7"]

- **split_part函数**

  通过指定的分隔符拆分字符串，并返回指定索引的内容字段样例，索引下标从0开始。若索引下标超过分割数量或者为负数，则返回空字符串。

  a. 字段样例

     Id: dc1dab7e-b045-4e77-bda4-914d083d1bf7

  b. 查询和分析语句

  ```
  SELECT split_part(Id,'-',1)
  ```

  c. 查询和分析结果

表 5-48 split_part 函数查询和分析结果

EXPR$0
b045

- **split_to_map函数**

  用于使用指定的第一个分隔符拆分字符串，然后再使用指定的第二个分隔符进行第二次拆分，展示形式为{“KEY1”:”VALUE1”,”KEY2”:”VALUE2”}。无法被二次分割的value值为空。

  a. 字段样例

  Request:request_id:"e3ac4b70c7d244f080d434e300d8065a”;request_time: "1674965051000”

  b. 查询和分析语句

  ```
  SELECT split_to_map(Request,';',':')
  ```

  c. 查询和分析结果

  表 5-49 split_to_map 函数查询和分析结果

EXPR$0
{"request_id ":"e3ac4b70c7d244f080d434e300d8065a ","request_time":"1674965051000"}

5.7.11 SQL 比较运算符

功能描述

比较运算符用于比较两个值，并返回真(true)或假(false)。比较运算符可以对数值类型进行大小比较，对STRING类型进行包含比较，比如数值类型的字段num1 < num2是否为真，STRING类型的str1是否存在于字符串strs中等，具体请参见**表5-50**。

语法格式

```
SELECT fieldname1 WHERE fieldname1 > fieldname2
```

比较运算符语句

表 5-50 比较运算符语句

语句	说明	示例
`x = y`	等于。	SELECT num1 < num2
`x <> y`	不等于。	SELECT num1 <> num2
`x > y`	大于。	SELECT num1 > num2

语句	说明	示例
x >= y	大于或等于。	SELECT num1 >= num2
x < y	小于。	SELECT num1 < num2
x <= y	小于或等于。	SELECT num1 <= num2
x BETWEEN y AND z	等同于x >= y AND x <= z。	SELECT num1 BETWEEN num2 AND num3
x NOT BETWEEN y AND z	等同于x < y OR x > z。	SELECT num1 NOT BETWEEN num2 AND num3
x LIKE pattern	如果x匹配SQL LIKE模式，则返回true。	SELECT str1 LIKE '*'
x NOT LIKE pattern	如果x不匹配SQL LIKE模式，则返回true。	SELECT str1 NOT LIKE '*'
x IS NULL	如果x是空值或空白字符串，则返回true。	SELECT str1 IS NULL
x IS NOT NULL	如果x既不是空值也不是空白字符串，则返回true。	SELECT str1 IS NOT NULL
x IN (values)	如果x为其中一个列举值，则返回true。	SELECT str1 IN ('testStr1', 'testStr2')
x NOT IN (values)	如果x不在列举值中，则返回true。	SELECT str1 NOT IN ('testStr1', 'testStr2')
x IN (subquery)	如果x是通过指定子查询返回，则返回true。	SELECT str1 WHERE str2 IN (SELECT DISTINCT str2 LIMIT 100)
x NOT IN (subquery)	如果x不是通过指定子查询返回，则返回True。	SELECT str1 NOT IN (SELECT str2 LIMIT 100)

5.7.12 SQL IP 地址函数

功能函数

对于IPv4地址函数，地址参数可以是IPv4点分十进制字符串（例如"192.168.0.1"）或表示为整数的IP地址（例如3232235521）。subnet 参数应该是一个字符串，格式为CIDR表示法中的IPv4地址子网（例如"192.168.0.0/16"）。

IP 函数语句

语句	说明	示例
IPV4_MATCH(address,subnet)	如果subnet属于address的子网地址则返回true，否则返回false。如果 address不是有效的IPv4地址，则返回false。如果address是整数而不是字符串，则此函数更效率。	SELECT IPV4_MATCH (address,subnet)
IPV4_PARSE(address)	将address解析为整数的IPv4地址。如果address是有效的IPv4地址，则它可以被解析。如果address不是有效的IPv4地址，则返回null。	SELECT IPV4_PARSE(address)
IPV4_STRINGIFY(address)	将整数address转换为以点分隔的IPv4地址字符串。如果address是有效的IPv4地址的整数，则它可以被解析。如果address不能表示为IPv4地址，则返回null。	SELECT IPV4_STRINGIFY(address)

示例及说明

IPV4_MATCH(address, subnet)函数

IPV4_MATCH函数，如果address属于subnet的子网ip，则返回true，否则返回false。如果address不是有效的IPv4地址，则返回false。如果address 是整数而不是字符串，则此函数具有更高的执行效率。

1. 字段样例

   Ipv4: 192.168.1.18

2. 查询和分析语句
```
select IPV4,IPV4_MATCH(Ipv4, '192.168.0.0/16')
```
3. 查询和分析结果

表 5-51 查询和分析结果

IPV4	EXPR$1
192.168.1.18	true

IPV4_PARSE(address)/ IPV4_STRINGIFY(address)函数

将address解析为整数的IPv4地址。如果address是有效的IPv4地址，则它可以被解析。如果address不是有效的IPv4地址，则返回null。

1. 字段样例

   Ipv4: 192.168.0.1

   Num: 3232235521
2. 查询和分析语句
```
select  IPV4_PARSE(Ipv4), IPV4_STRINGIFY(Num)
```
3. 查询和分析结果

表 5-52 查询和分析结果

EXPR$0	EXPR$1
-1062731775	192.168.0.1

5.7.13 SQL 归约函数

功能描述

归约函数对零个或多个表达式进行操作，并返回单个表达式。如果没有表达式作为参数传递，则结果为 NULL。表达式必须全部转换为公共数据类型，即结果的类型有：

- 如果所有的参数都是 NULL，结果是 NULL，否则，NULL 参数被忽略。
- 如果所有的参数包含了数字和字符串的混合，参数都被解释为字符串。
- 如果所有的参数是整型数字，参数都被解释为长整型。
- 如果所有的参数是数值且至少一个参数是double，则参数都被解释为double。

语法格式

```
GREATEST([expr1, ...])/ LEAST([expr1, ...])
```

示例及说明

GREATEST([expr1, ...])/ LEAST([expr1, ...])函数

GREATEST函数，计算零个或多个表达式，并根据上述比较返回最大值。

LEAST函数，计算零个或多个表达式，并根据上述比较返回最小值。

1. 字段样例

   Num: 11785730

2. 查询和分析语句

```
select  Num,GREATEST( "Num"/10,(select count(1)) ),LEAST("Num"/10,(select count(1)))
```

3. 查询和分析结果

表 5-53 归约函数查询和分析结果

Num	EXPR$1	EXPR$2
11785730	1178573	1

5.7.14 SQL 其他函数

功能描述

SQL提供的函数，还支持一些转换类型和CASE WHEN等逻辑运算，具体请参见**表 5-54**。

语法格式

```
SELECT CAST(fieldname1 AS VARCHAR) AS fieldname1_str
```

其他函数语句

表 5-54 其他函数语句

关键字	说明	示例
CAST(value AS TYPE)	转换数据类型。只支持转换为VARCHAR、FLOAT。	SELECT fieldname1, CAST(fieldname1 AS VARCHAR)
CASE WHEN boolean_expr1 THEN result1 \[WHEN boolean_expr2 THEN result2 ... \] \[ELSE resultN \] END	简单CASE函数。	SELECT CASE WHEN httpStatus = 200 THEN 1 ELSE 0 END
NULLIF(value1, value2)	如果value1和value2相等，返回空值，否则返回value1。	SELECT fieldname1, fieldname2, NULLIF(fieldname1, fieldname2)
NVL(expr,expr-for-null)	如果"expr"为空值或空白字符串，则返回"expr-for-null"。	SELECT NVL(str1, 'expr-for-null')

5.7.15 SQL JOIN 语法

JOIN子句可以关联查询两个或多个表数据，本文介绍JOIN子句的基本使用方法。

语法

```
select key
from t1
LEFT|RIGHT|INNER JOIN t2
on t1.key=t2.key
```

当前日志服务支持LEFT JOIN、RIGHT JOIN和INNER JOIN三种JOIN子句方式。具体功能如下：

表 5-55

JOIN方式	说明
LEFT JOIN	以左表（t1）的结果为基础，关联右表（t2）数据。 **说明** 当表名为纯数字时，需要给表名加上双引号转换成字符串。例如：表名是123，JOIN语句中该表应写成“123”。
RIGHT JOIN	以右表（t2）的结果为基础，关联左表（t1）数据。 **说明** 当表名为纯数字时，需要给表名加上双引号转换成字符串。例如：表名是123，JOIN语句中该表应写成“123”。
INNER JOIN	两个表的结果（elb1，elb2）交集数据

示例

有两个表，access表示主机的接入指标包含路径，时延，状态码，host为主机指标包含cpu和内存。通过JOIN可以关联接入和主机指标，查看相同主机的不同维度的指标情况。

- **LEFT JOIN**
  a. 查询语句
  ```
  SELECT
    "access".__time,
    "access".host_ip,
    "access".cost,
    "host".cpu,
    "host".memory
  FROM
    log "access"
    LEFT JOIN (select memory,cpu,host_ip from log) host ON "access".host_ip = "host".host_ip
  ```
  b. 返回结果，总共60条数据。
- **RIGHT JOIN**
  a. 查询语句
  ```
  SELECT
    "access".__time,
    "host".host_ip,
    "access".cost,
    "host".cpu,
    "host".memory
  FROM
    log "access"
    RIGHT  JOIN (select memory,cpu,host_ip from log) host ON "access".host_ip = "host".host_ip
  ```
  b. 返回结果，总共60条数据。

- **INNER JOIN**

  a. 查询语句

```
SELECT
    "access".__time,
    "host".host_ip,
    "access".cost,
    "host".cpu,
    "host".memory
FROM
    log "access"
    INNER  JOIN (select memory,cpu,host_ip from log) host ON "access".host_ip = "host".host_ip
```

  b. 返回结果，总共45条数据。

5.7.16 SQL 查询样例

本章以ELB日志为例进行介绍，对LTS中的ELB原始日志进行查询，具体查询步骤如下。

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“日志管理”，单击目标日志组和日志流名称，进入日志详情页面。

步骤3 系统获取ELB原始日志，在日志搜索页面查看具体日志。

步骤4 单击右上角  ，在弹出页面中，选择“云端结构化解析”。

步骤5 选择结构化模板，根据ELB模板进行结构化配置。其他日志内容可选择其他结构化模板。

步骤6 在“可视化”页签下输入SQL查询语句对相应的字段进行查询，即可返回所需的日志内容。

----结束

查询结果呈现

表格

下面的语句查询请求的host，request_uri所对应的日志各有多少条，发送的请求体的大小（MB），请求返回的状态码分别是2xx, 3xx, 4xx, 5xx的占比，并按照日志条数降序排列。

```
SELECT "router_request_uri" as "request_uri", "host", COUNT(*) as pv,
round(sum(body_bytes_sent) / 1024.0 , 5) as "body_bytes_sent(MB)",
round(sum(case when status >= 200 and status < 300 then 1 else 0 end ) * 100.0 / COUNT(1), 6) as "2xx ratio(%)",
round(sum(case when status >= 300 and status < 400 then 1 else 0 end ) * 100.0 / count(1), 6) as "3xx ratio(%)",
round(sum(case when status >= 400 and status < 500 then 1 else 0 end ) * 100.0 / count(1), 6) as "4xx ratio(%)",
round(sum(case when status >= 500 and status < 600 then 1 else 0 end ) * 100.0 / count(1), 6) as "5xx ratio(%)"
GROUP BY "host", "router_request_uri"
ORDER BY pv DESC
LIMIT 100
```

柱状图

根据以下语句查询结果绘制柱状图，x轴选择"request_uri"，y轴选择"pv"，表示每种requestURL请求分别有多少条。

```
SELECT "router_request_uri" as "request_uri", "host", COUNT(*) as pv,
round(sum(body_bytes_sent) / 1024.0 , 5) as "body_bytes_sent(MB)",
round(sum(case when status >= 200 and status < 300 then 1 else 0 end ) * 100.0 / COUNT(1), 6) as "2xx ratio(%)",
round(sum(case when status >= 300 and status < 400 then 1 else 0 end ) * 100.0 / count(1), 6) as "3xx ratio(%)",
round(sum(case when status >= 400 and status < 500 then 1 else 0 end ) * 100.0 / count(1), 6) as "4xx ratio(%)",
round(sum(case when status >= 500 and status < 600 then 1 else 0 end ) * 100.0 / count(1), 6) as "5xx ratio(%)"
GROUP BY "host", "router_request_uri"
ORDER BY pv DESC
LIMIT 100
```

折线图

根据以下语句查询结果绘制折线图，x轴选择"_time_"，y轴选择"QPS"。表示查询时间段内间隔5s的QPS变化。

```
select TIME_FORMAT(TIME_CEIL(TIME_PARSE(SUBSTRING(time_iso8601, 2, 25) ,'yyyy-MM-dd''T''HH:mm:ssZZ'),'PT5S'),'yyyy-MM-dd HH:mm:ss','+08:00') AS _time_ , COUNT(*) as QPS from log group by _time_
```

饼图

根据以下语句查询结果绘制饼图，类目选择"status"，数据选择"rm"，表示查询时间段内status不同值的占比。

```
SELECT status, COUNT(1) AS rm GROUP BY status
```

数字图

根据以下语句查询结果绘制数字图，查看最近一小时一共有多少次正常的请求。

```
SELECT count(*) AS normalRequest WHERE status = 200
```

6 日志可视化

6.1 日志可视化概述

云日志服务支持用户使用**SQL查询语法**对结构化日志进行统计分析，同时将分析结果以图表方式可视化展示，提供多种图表类型，满足不同场景的可视化呈现需求，用于运维和运营分析。

LTS提供40多种开箱即用仪表盘模板、预置样例数据，配置丰富，简单易用，降低使用门槛，减少用户重复开发。其他云服务日志只要接入LTS即可直接使用仪表盘模板，帮助企业基于日志数据进行数字化运营，助力企业数字化转型。

表 6-1 可视化方式

可视化方式	说明
统计图表	统计图表是云日志服务根据**SQL查询语法**渲染出的结果，包括表格、柱状图、折线图等多种图表类型，详细请参考**使用统计图表将日志可视化**。
仪表盘	• 仪表盘是云日志服务提供的实时数据分析大盘。您可以在仪表盘查看多个基于SQL语句查询分析结果的统计图表，并能将多张统计图表同步保存到仪表盘中。详细请参考**使用仪表盘将日志可视化**。

说明

目前此功能支持全部用户使用的局点有：华南-广州、华北-北京四、华东-上海一、华东-上海二、中国-香港、西南-贵阳一、亚太-新加坡、华北-北京一；支持部分白名单用户使用的局点有：亚太-曼谷、华南-深圳、中东-利雅得、亚太-雅加达，其他局点暂不支持该功能。

6.2 使用统计图表将日志可视化

6.2.1 统计图表概述

日志上报LTS后，支持通过**SQL分析语法**搜索关键日志数据，并将查询结果通过统计图表的方式进行可视化展示，帮助用户更容易地理解日志数据之间的变化。用户还可以将图表分析结果保存到仪表盘，进行长期监控。

限制说明

- 一个日志流最多可创建100个图表。
- 一个仪表盘最多可添加50个图表。

统计图表类型

支持使用表格、柱状图、折线图等图表类型展示不同场景数据，详细请参考**表6-2**。

表 6-2 图表类型

图表类型	使用场景
表格	表格是最常见的数据展示类型，通过对数据结构化的整理，实现数据的对比与统计。大多数场景均适用。
柱状图	柱状图描述的是分类数据，直观表现每一个分类项的大小对比关系。统计近一天各错误码类型出现的次数等分类统计场景适用。
折线图	折线图需要统计数据具备时序字段，依据时间顺序组织与聚合指标。可直观反映指标随时间的变化趋势。
饼图	饼图描述的是不同分类的占比情况，通过扇区大小来衡量各分类项的占比情况。错误码占比情况分析等占比统计场景适用。
数字图	数字图描述的是单个指标，一般选择具备有业务价值的关键性指标。统计天、周、月PV、UV等单指标场景适用。
数字折线图	折线图和数字图的组合。折线图用于表示数据趋势和变化的，数字图则展示关键性指标。在一些需要同时显示趋势和关键数据点的场合适用。
地图	地图通过图形的位置来表现数据的地理位置，通常来展示数据在不同地理区域上的分布情况。攻击IP地理分布等地理位置统计场景适用。
漏斗图	漏斗图适用于单流向单路径的业务流程，对各环节进行统计并用梯形面积表示某个环节业务量与上一个环节之间的差异。

统计图表操作说明

支持对图表进行新建、保存、另存为等操作。详细请参考**表6-3**。

表 6-3 操作说明

功能名称	功能描述
新建	选择不同的图表类型，将图表分析结果保存到仪表盘。
保存	对当前可视化图表进行保存。
另存为	对已有可视化图表进行复制。
下载	将图表分析结果下载到excel。
展开图表	可展开当前日志流下的可视化图表。
收起图表	可收起当前日志流下的可视化图表。

6.2.2 LTS 表格

表格作为最常见的数据展示类型，是组织整理数据最基本的手段，通过对数据的整理，达到快速引用和分析的目的。通过查询分析语法得到的数据结果默认以表格方式进行展示。

查看表格

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“日志管理”，进入日志管理页面。

步骤3 在日志管理页面中，选择目标日志组和日志流，进入日志流详情页面。

步骤4 选择“日志分析”。

步骤5 请参考**SQL分析语法**输入查询和分析语句，设置查询和分析的时间范围，单击“查询”。

步骤6 日志下方默认使用表格展示日志数据查询结果，在通用配置下方，参考**表6-4**配置参数。

图 6-1 表格

表 6-4 表格参数说明

类别	参数	说明
标准配置	格式化	将表格数据按照指定格式进行显示。
	单位	自定义配置表格数据的单位。
	小数点位数	设置显示数值小数点位数。
	图表名称字号	设置图表名称的字号大小。
查询分析设置	隐藏字段	选择目标字段，将该字段在表格中隐藏。
表格配置	每页显示	每页显示的数据条数。
	显示总数	显示表格数据的总条目数。
列配置	对齐方式	表格数据的对齐方式，支持左对齐，右对齐以及居中。
	开启搜索	开启后，即可对表格列数据进行搜索功能。
	开启排序	开启后，即可对表格列数据进行排序功能。
	字体大小	表格字体的大小，取值范围为12px~24px 。

----结束

6.2.3 LTS 柱状图

柱状图是使用垂直或水平的柱子显示类别之间的数值比较，用于描述分类数据，并统计每一个分类中的数量。

云日志服务（LTS）提供的柱状图，有垂直柱子和水平柱子，矩形块宽度一定，高度代表数值大小。有多列数据映射到Y轴时，采用分组柱状形式显示。

默认采用垂直柱子，您可以根据自己的需要进行选择。基本构成如下：

- X轴（横轴）
- Y轴（纵轴）
- 矩形块
- 图例

查看柱状图

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“日志管理”，进入日志管理页面。

步骤3 在日志管理页面中，选择目标日志组和日志流，进入日志流详情页面。

步骤4 选择“日志分析”。

步骤5 请参考**SQL分析语法**输入查询和分析语句，设置查询和分析的时间范围，单击“查询”。

步骤6 单击 图标，使用柱状图展示查询数据。在通用配置下方，参考表6-5配置参数。

图 6-2 柱状图

表 6-5 柱状图参数说明

类别	参数	说明
标准配置	格式化	将Y轴按照指定格式进行显示。
	单位	自定义配置Y轴的单位。
	小数点位数	设置显示数值小数点位数。
	图表名称字号	设置图表名称的字号大小。
柱配置	方向	选择基础柱状图或横向柱状图。
	柱宽度	设置柱宽度。
	是否显示值	开启后，显示各个条形体对应的数值。
	值字体大小	设置各个条形体对应的数值字体大小
	是否堆叠	开启后，将堆叠显示Y轴数据。
查询分析设置	X轴数据	支持数字或字符串数据。
	Y轴数据	支持数字或字符串数据，可以选择多个数据。
图例配置	隐藏图例	开启后，可以隐藏图例和对比值的显示。
	图例位置	图例在图表中的位置，选择图表顶部或图表右边。
	对比数值	选择显示最大值、最小值、平均值、求和值等，可勾选多个。
图形配置	上边距	坐标轴距离图表上边界距离。
	下边距	坐标轴距离图表下边界距离。
	左边距	坐标轴距离图表左边界距离。
	右边距	坐标轴距离图表右边界距离。

类别	参数	说明
Tooltip配置	不排序、升序、降序	提示框配置，当Y轴数据选择多个时，可对其进行排序显示。
X轴	显示X轴	开启后，显示X轴数据。
	X轴名称	设置X轴名称。
Y轴	显示Y轴	开启后，显示Y轴数据。
	Y轴名称	设置Y轴名称。
	Y轴位置	设置Y轴位置，左边或者右边。

----结束

6.2.4 LTS 折线图

折线图属于趋势类分析图表，一般用于表示一组数据在一个有序数据类别（多为连续时间间隔）上的变化情况，用于直观分析数据变化趋势。在折线图中，可以清晰的观测到数据在某一个周期内的变化，主要反映在：

- 递增性或递减性
- 增减的速率情况
- 增减的规律（如周期变化）
- 峰值和谷值

所以，折线图是用于分析数据随时间变化趋势的最佳选择。同时，也可以绘制多条线用于分析多组数据在同一时间周期的变化趋势，进而分析数据之间的相互作用和影响（如同增同减，成反比等）。

查看折线图

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“日志管理”，进入日志管理页面。

步骤3 在日志管理页面中，选择目标日志组和日志流，进入日志流详情页面。

步骤4 选择“日志分析”。

步骤5 请参考**SQL分析语法**输入查询和分析语句，设置查询和分析的时间范围，单击“查询”。

步骤6 单击  图标，使用折线图展示查询数据。在通用配置下方，参考**表6-6**配置参数。

图 6-3 折线图

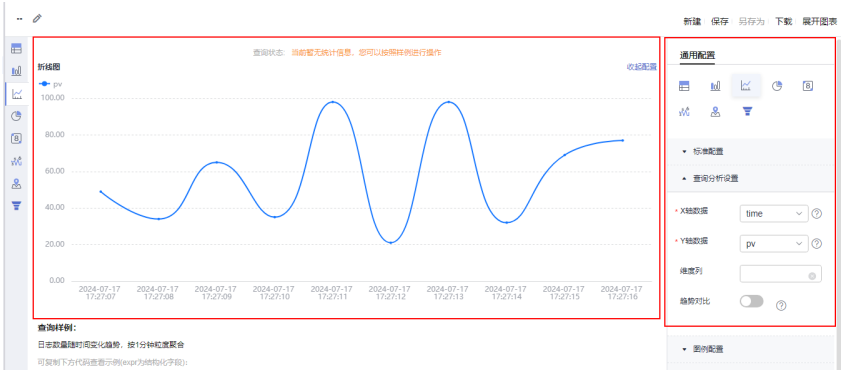


表 6-6 折线图参数说明

类别	参数	说明
标准配置	格式化	在下拉框选择**K,Mil,Bil**、**1000000**或**Byte,KB,MB**等格式，将Y轴按照指定格式进行显示。
	单位	自定义配置Y轴的单位。
	小数点位数	设置显示数值小数点位数。
	图表名称字号	设置图表名称的字号大小。
查询分析设置	X轴数据	支持数字或字符串数据。
	Y轴数据	支持数字或字符串数据，可以选择多个数据。
	维度列	请从下拉列表中选择，一般为有序数据类别。
	趋势对比	当X轴为时间数据时，且不设置维度列时，可开启该按钮。 开启后，设置比较对象时间，时间小于等于24小时。设置完成后，将当前时间的数据与对象时间数据进行比较。
图例配置	隐藏图例	开启后，可以隐藏图例和对比值的显示。
	图例位置	选择图表顶部或图表右边。
	对比数值	选择显示最大值、最小值、平均值、求和值等，可勾选多个。
图形配置	连接方式	设置线图显示格式，可选择直线或曲线。
	线宽	折线的线宽。
	是否显示点	开启该功能后，显示折线的连接点。
	上边距	坐标轴距离图表上边界距离。
	下边距	坐标轴距离图表下边界距离。
	左边距	坐标轴距离图表左边界距离。

类别	参数	说明
	右边距	坐标轴距离图表右边界距离。
Tooltip配置	排序方式	提示框配置，当Y轴数据选择多个时，可对其进行排序显示。
X轴	显示X轴	开启后，显示X轴数据。
	X轴名称	设置X轴名称。
Y轴	显示Y轴	开启后，显示Y轴数据。
	Y轴名称	设置Y轴名称。
	Y轴位置	设置Y轴位置，左边或者右边。

----结束

6.2.5 LTS 饼图

饼图用于表示不同分类的占比情况，通过弧度大小来对比各种分类。饼图通过将一个圆饼按照分类的占比划分成多个区块，整个圆饼代表数据的总量，每个区块表示该分类占总体的比例大小，所有区块的加和等于100%。基本构成如下：

- 扇形
- 文本百分比
- 图例

查看饼图

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“日志管理”，进入日志管理页面。

步骤3 在日志管理页面中，选择目标日志组和日志流，进入日志流详情页面。

步骤4 选择“日志分析”。

步骤5 请参考**SQL分析语法**输入查询和分析语句，设置查询和分析的时间范围，单击“查询”。

步骤6 单击  图标，使用饼图展示查询数据。在通用配置下方，参考**表6-7**配置参数。

图 6-4 饼图

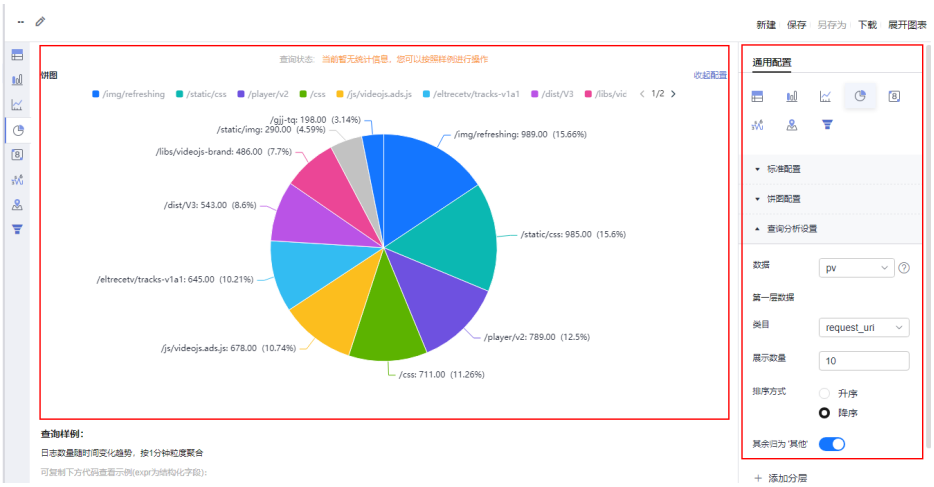


表 6-7 饼图参数说明

类别	参数	说明
标准配置	格式化	在下拉框选择**K,Mil,Bil**、**1000000**或**Byte,KB,MB**等格式，将Y轴按照指定格式进行显示。
	单位	自定义配置Y轴的单位。
	小数点位数	设置显示数值小数点位数。
	图表名称字号	设置图表名称的字号大小。

类别	参数	说明
饼图配置	饼图类型	包括饼图、环图和南丁格尔玫瑰图。 ● 饼图 饼图是一种用于展示各部分组成在整体中所占百分比的图形。它通过将一个圆形划分为不同的扇区，每个扇区的面积（或弧长和圆心角）大小对应所表示的数据的比例，从而直观地展示出各部分与整体之间的关系。 ● 环图 环图本质上是将饼图中心挖空，相比于饼图来说有如下优点： – 在原有构成的基础上增加了总数显示，展示了更多的信息。 – 两个饼图直接进行比较是非常不直观的，两个环图间可以通过环状条长度进行简单的对比。 ● 南丁格尔玫瑰图 南丁格尔玫瑰图本质上并不是环图，而是在极坐标系下画出来的柱状图，每一个分类数据被圆弧平分，使用圆弧的半径长短表示数据的大小，相比于饼图来说有如下优点： – 饼图适用于不超过10条的分类数据，南丁格尔玫瑰图则适用于分类较多的场景（10-30条数据）。 – 由于半径和面积是成平方的关系，南丁格尔玫瑰图放大了各个分类数据之间值的差异，尤其适合对比大小相近的数值。 – 由于圆形有周期的特性，南丁格尔玫瑰图也适用于表示一个周期的时间概念，比如星期、月份。
	是否显示刻度	开启后，显示饼图上的文本标签，可用于说明图形的一些数据信息，比如值，名称等。
	刻度文本格式	可配置为分类、百分比、分类：百分比或分类：数值（百分比）。
	标签位置	开启是否显示刻度后，可配置此参数，调整标签在图表中的位置。
查询分析设置	数据	分类数据对应的数值。
	第一层数据	
	类目	分类数据。
	展示数量	显示分类数据的个数。
	排序方式	升序或降序。

类别	参数	说明
	其余归为其他	开启后，除了展示的数据，其余归为其他方式展示。
	添加分层	单击添加分层，设置第二层数据，每层数据包括类目、展示数量、排序方式、其余归为其他。
图例配置	隐藏图例	开启后，可以隐藏图例和图例内容的显示。
	图例内容	选择显示值和百分比，可勾选多个。
	图例位置	图例在图表中的位置，选择图表顶部或图表右边。
图形配置	外半径	指定饼图外半径值。取值范围为40~100 。
	内半径	指定饼图内半径值。取值范围为0~100。
	上边距	坐标轴距离图表上边界距离。
	下边距	坐标轴距离图表下边界距离。
	左边距	坐标轴距离图表左边界距离。
	右边距	坐标轴距离图表右边界距离。

----结束

6.2.6 LTS 数字图

数字图通常用来表示单一数据点或关键性指标，能够更好地展示单一信息和数据的相对大小，是一种非常清晰的信息展示方式，适用于需要重点突出关键信息和数据的场合。通过数字图可以快速地呈现信息和数据，使得用户能够快速、直观地理解数据的趋势和关键指标。

查看数字图

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“日志管理”，进入日志管理页面。

步骤3 在日志管理页面中，选择目标日志组和日志流，进入日志流详情页面。

步骤4 选择“日志分析”。

步骤5 请参考**SQL分析语法**输入查询和分析语句，设置查询和分析的时间范围，单击“查询”。

步骤6 单击  图标，使用数字图展示查询数据。在通用配置下方，参考**表6-8**配置参数。

图 6-5 数字图

表 6-8 数字图参数说明

类别	参数	说明
查询分析设置	数值列	支持数字或字符串数据。
	同比数据	选择待对比的字段，在图表中显示该字段对应的值。
主体设置	图表名称字号	设置图表名称的字号大小。
	格式化	将数据按照指定格式进行显示。
	数值字号	显示值的字号，取值范围为12px~80px。
	数值单位	显示值的单位
	单位字号	显示值单位的字号，取值范围为12px~50px。
	小数点位数	设置显示数值小数点位数。
	添加对比值	开启后，显示待对比字段对应的值。
	对比值格式化	将待对比数据按照指定格式进行显示。
	对比值字号	待对比值的字号，取值范围为12px~50px。
	对比值单位	待对比值的单位。
	对比值单位字号	显示待对比值单位的字号，取值范围为12px~50px。
	描述	对显示的数值及对比值趋势的描述，显示在数值下方。
背景配置	背景色	图表的背景颜色，支持深色或浅色。

----结束

6.2.7 LTS 数字折线图

数字图和折线图组合，同时显示趋势和关键数据点。可以帮助用户更好的理解数据和趋势变化，从而更好的进行业务决策。

查看数字折线图

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“日志管理”，进入日志管理页面。

步骤3 在日志管理页面中，选择目标日志组和日志流，进入日志流详情页面。

步骤4 选择“日志分析”。

步骤5 请参考SQL分析语法输入查询和分析语句，设置查询和分析的时间范围，单击“查询”。

步骤6 单击  图标，使用数字折线图展示查询数据。在通用配置下方，参考表6-9配置参数。

图 6-6 数字折线图

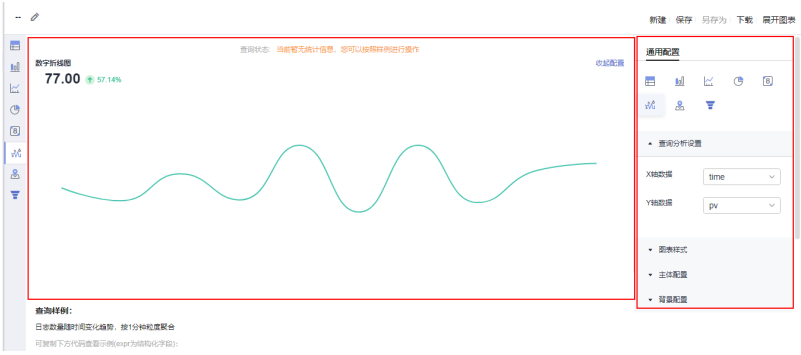


表 6-9 数字折线图参数说明

类别	参数	说明
查询分析设置	X轴数据	支持数字或字符串数据。
	Y轴数据	支持数字或字符串数据，可以选择多个数据。
图表样式	连接方式	设置线图显示格式，可选择直线或曲线。
主体设置	图表名称字号	设置图表名称的字号大小。
	数据格式	将数据按照指定格式进行显示。
	数值字号	显示值的字号，取值范围为12px~80px。
	数值单位	显示值的单位。
	单位字号	显示值单位的字号，取值范围为12px~50px。
	小数点位数	设置显示数值小数点位数。
背景配置	背景色	图表的背景颜色，支持深色或浅色。

----结束

6.2.8 LTS 地图

以地图作为背景，通过图形颜色、图像标记的方式展示地理数据信息。云日志服务（LTS）提供的地图，包括中国地图和世界地图。您在查询和分析语句中使用特定函数（中国地图：ip_to_province函数，世界地图：ip_to_country函数）后，云日志服务（LTS）将以地图形式展示分析结果。

基本构成如下：

- 地图画布
- 色块

查看地图

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“日志管理”，进入日志管理页面。

步骤3 在日志管理页面中，选择目标日志组和日志流，进入日志流详情页面。

步骤4 选择“日志分析”。

步骤5 请参考**SQL分析语法**输入查询和分析语句，设置查询和分析的时间范围，单击“查询”。

步骤6 单击  图标，使用地图展示查询数据。在通用配置下方，参考**表6-10**配置参数。

图 6-7 地图

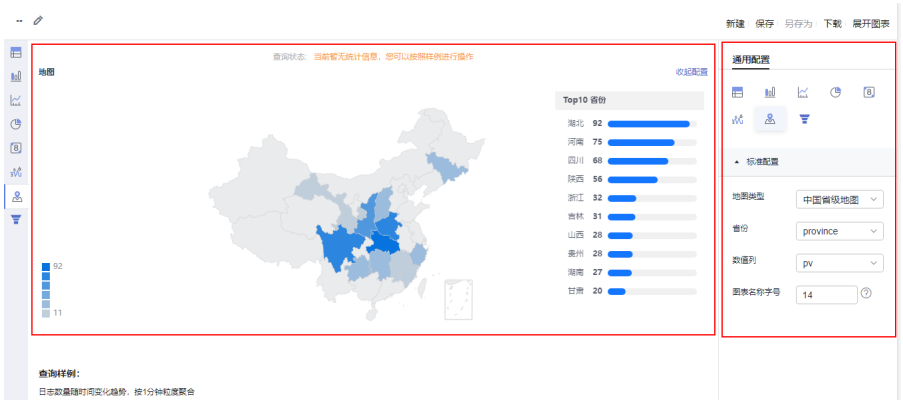


表 6-10 地图参数说明表

参数	说明
地图类型	区域定位：设置地图显示的区域范围，包含中国省级地图和世界地图两种。
省份	地图类型为中国省级地图，该字段为具体省份。例如浙江省
国家	地图类型为世界地图，该字段为具体国家。例如中国
数值列	选择用于展示数值的字段。

参数	说明
图表名称字号	设置图表名称的字号大小。

----结束

6.2.9 LTS 漏斗图

漏斗图适用于业务流程比较规范、周期长、环节多的单流程单向分析，通过漏斗各环节业务数据的比较能够直观地发现和说明问题所在的环节，进而做出决策。漏斗图用梯形面积表示某个环节业务量与上一个环节之间的差异。

查看漏斗图

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“日志管理”，进入日志管理页面。

步骤3 在日志管理页面中，选择目标日志组和日志流，进入日志流详情页面。

步骤4 选择“日志分析”。

步骤5 请参考SQL分析语法输入查询和分析语句，设置查询和分析的时间范围，单击“查询”。

步骤6 单击 图标，使用漏斗图展示查询数据。在通用配置下方，参考表6-11配置参数。

图 6-8 漏斗图

表 6-11 漏斗图参数说明

参数	说明
系列名称	漏斗图的名称。
数值列	选择数值字段，某个字段对应的数值越大，在越上面。
隐藏图例	开启后，可以隐藏漏斗图上方的字段名显示。

----结束

6.3 使用仪表盘将日志可视化

6.3.1 创建日志仪表盘

仪表盘是一种数据可视化工具，它汇总并呈现关键性能指标、重要数据和分析结果，为用户提供了一目了然的业务或系统运行状况概览。

云日志服务提供多种仪表盘模板，用户可以直接使用LTS提供的仪表盘模板展示日志数据，或者将查询分析结果的统计图表同步保存到仪表盘中进行展示。

说明

目前此功能支持全部用户使用的局点有：华南-广州、华北-北京四、华东-上海一、华东-上海二、中国-香港、西南-贵阳一、亚太-新加坡、华北-北京一；支持部分白名单用户使用的局点有：亚太-曼谷、华南-深圳、中东-利雅得、亚太-雅加达，其他局点暂不支持该功能。

前提条件

- 已成功采集到日志。
- 对日志内容已完成结构化配置，具体操作请参考**结构化配置**。

限制条件

- 一个账号最多可创建100个仪表盘。
- 一个日志流最多可创建100个图表。
- 一个仪表盘最多可添加50个图表。

创建仪表盘

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 单击  ，在“添加仪表盘分组”对话框，自定义填写“分组名称”。

说明

分组名称只支持英文、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，长度不超过64。

步骤3 单击“确定”，创建分组成功后。

步骤4 单击“添加仪表盘”，进入“创建仪表盘”页面，参考**表6-12**填写仪表盘相关参数。

表 6-12 创建仪表盘参数

参数名称	说明
仪表盘名称	自定义仪表盘名称，用于区分日志流下不同的仪表盘。 仅支持中英文、数字、中划线、下划线、小数点，不能以小数点开头和结尾，长度不超过255。

参数名称	说明
企业项目	选择业务需要的企业项目，默认为default。也可单击“查看企业项目”，在企业项目管理页面查看全部企业项目。 **说明** • 企业项目需要开通后才能使用，请参考**如何开通企业项目**。 • 支持将该企业项目资源迁出，详细请参考**迁出企业项目资源**。
添加到仪表盘分组	将新建的仪表盘进行分组管理。 不开启“添加到仪表盘分组”，新建仪表盘会添加到系统自带的“默认分组”中。 开启“添加到仪表盘分组”，新建仪表盘按“分组类型”进行添加： • 已有分组：选择已有的仪表盘分组。 • 新建分组：输入新建仪表盘分组名称。
简洁模式	仪表盘页面简介模式。 • 开启“简洁模式”，仪表盘界面不显示编辑、删除、添加过滤器等按钮。 • 关闭“简洁模式”，仪表盘界面显示编辑、删除、添加过滤器等按钮。
添加图表	添加可视化图表：将日志流的可视化图表加入仪表盘。 1. 在“添加图表”区域中，鼠标悬浮在添加可视化图表模块，单击“开始添加图表”，进入添加可视化图表界面。 2. 选择业务需要的日志流，根据业务需要勾选一个或多个图表名称前的☐，单击“确定”，进入仪表盘详情页后，调整图表信息，单击“保存设计”。 3. 如果当前日志流未配置或没有当前需要的可视化图表，单击“前往添加图表”，新建图表。
	使用仪表盘模板：支持选择自定义模板（用户从已创建的仪表盘中提取的模板）和系统模板（LTS提供的系统内置模板，用户无法修改）： 1. 在“添加图表”区域中，鼠标悬浮在使用仪表盘模板模块，单击“使用仪表盘模板”，进入使用仪表盘模板界面。 2. 根据业务需要选择仪表盘模板，单击下一步选择业务需要的日志流，根据业务需要勾选一个或多个日志流名称前的☐，单击“确定”。

步骤5 仪表盘创建成功后，在仪表盘列表生成一条仪表盘信息。

- 单击仪表盘操作列的编辑，修改仪表盘名称和简洁模式。
- 单击仪表盘操作列的移动分组，修改仪表盘分组。
- 单击仪表盘操作列的删除按钮即可删除删除仪表盘。

----结束

新建可视化图表到仪表盘

步骤1 在仪表盘目录下方，选中仪表盘分组，单击待操作的仪表盘名称进入详情页。

步骤2 单击  ，在添加可视化图表界面中，选择相应日志流。单击“前往添加图表”。

步骤3 在“添加图表”页面，单击“新建”，参照表6-13填写相关参数，填写完成后单击“确定”。

表 6-13 创建图表

参数	说明
图表名称	自定义图表名称，用于区分日志流下不同的图表。 仅支持中英文、数字、中划线、下划线、空格、括号、小数点，不能以小数点、空格开头或结尾。长度为1-64个字符。
可视化对象	• 默认语句“SELECT * ”，表示查询该日志流内的结构化数据，其中*为结构化字段。 • 如需自行编辑SQL语句，请参考SQL分析语法介绍。
图表类型	LTS提供表格、柱状图、折线图等多种图表类型供用户选择。
同时添加到仪表盘	• 开启“同时添加到仪表盘”，勾选一个或多个仪表盘前面的  ，可将图表同步添加至勾选的仪表盘中。 • 关闭“同时添加到仪表盘”，则表示新建图表不在仪表盘显示。

步骤4 单击“确定”，可视化图表创建成功。

----结束

相关操作

创建仪表盘后，单击仪表盘名称进入详情页，您可以编辑仪表盘中的图表、移除仪表盘中的图表、调整仪表盘中图表的位置等，详细请参考表6-14。

表 6-14 相关操作

操作	说明
编辑仪表盘中的图表	将光标移至图表框右上角，单击，在下拉框中选择“编辑图表”，在可视化页面编辑图表，具体操作请参考分析LTS日志。
移除仪表盘中的图表	将光标移至图表框右上角，单击  ，在下拉框中选择“移除图表”，单击“保存设计”，可将已创建图表删除。
调整仪表盘中图表的位置	将光标移至待操作的图表框内，选中该图表，可将该图表移动至仪表盘内任意位置，单击“保存设计”，调整当前图表布局。

操作	说明
调整仪表盘中图表的大小	将光标移至待操作的图表框右下角边缘，选中该图表，可根据业务展示内容需求调整图表大小，单击“保存设计”，调整当前图表布局。
编辑仪表盘中的过滤器	将光标移至过滤器框右上角，单击 ，在下拉框中选择“编辑”，在添加过滤器页面编辑过滤器，具体操作请参考**添加过滤器**。
复制仪表盘中的过滤器	将光标移至过滤器框右上角，单击 ，在下拉框中选择“复制”，跳转到添加过滤器页面，单击“确定”即可复制过滤器。
删除仪表盘中的过滤器	将光标移至过滤器框右上角，单击 ，在下拉框中选择“删除”，在弹出的“删除过滤器”提示框中，单击“确定”即可删除过滤器。
调整仪表盘中过滤器的大小	将光标移至待操作的过滤器右下角边缘，可根据业务展示内容需求调整过滤器大小，单击“保存设计”，调整当前过滤器布局。
自动刷新	单击右上角的 ，开启仪表盘自动刷新功能，选择自动刷新的时间，可使仪表盘中的所有图表数据自动进行刷新。自动刷新的时间有1分钟、5分钟、15分钟。
手动刷新	选择待操作的仪表盘，单击 可手动刷新当前页面。
全屏显示	选择待操作的仪表盘，单击 ，可全屏显示仪表盘。全屏后，勾选保持在线按钮，可以保持在线状态，会话一直有效，当前账号不会退出。
退出全屏显示	将光标移至屏幕上方，单击弹出的 ，或者单击 ，或者按键盘中的“Esc”可退出全屏模式。
全屏显示单个图表	选择待操作的仪表盘，单击取消退出编辑模式。将光标移至图表框右上角，单击 ，在下拉框中选择“全屏”，可全屏显示图表数据。
退出全屏显示单个图表	将光标移至屏幕上方，单击弹出的 ，或者单击 ，在下拉框中选择“退出全屏”，或者按键盘中的“Esc”可退出全屏模式。
手动刷新单个图表	选择待操作的仪表盘，将光标移至图表框右上角，单击 ，在下拉框中选择“刷新”，或者在全屏模式下，单击 ，在下拉框中选择“刷新”，可手动刷新当前图表页面。

操作	说明
查询时间设置	选择待操作的仪表盘，单击 前面的下拉框  。 时间范围有三种方式，分别是相对时间、整点时间和自定义。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：表示查询指定时间范围的日志数据。
查看图表详情	选择待操作的仪表盘，将光标移至图表框右上角，单击 ，在下拉框中选择“查看图表详情”，可查看图表详情。
添加告警	选择待操作的仪表盘，将光标移至图表框右上角，单击 ，在下拉框中选择“添加告警”，可新建告警规则。
复制	选择待操作的仪表盘，将光标移至图表框右上角，单击 ，在下拉框中选择“复制”，可复制图表到当前仪表盘。
复制到其他仪表盘	选择待操作的仪表盘，将光标移至图表框右上角，单击 ，在下拉框中选择“复制到其他仪表盘”，可将该图表复制到其他仪表盘。
复制搜索分析语句	选择待操作的仪表盘，将光标移至图表框右上角，单击 ，在下拉框中选择“复制搜索分析语句”，可复制该图表的搜索分析语句。
导出图表数据	选择待操作的仪表盘，将光标移至图表框右上角，单击 ，在下拉框中选择“导出图表数据”，可导出图表数据。

6.3.2 添加日志仪表盘过滤器

在云日志服务仪表盘中添加过滤器，即对整个仪表盘进行查询过滤或变量替换操作。

过滤器用于为仪表盘中的所有统计图表批量修改查询条件。每张统计图表实际为一个查询和分析语句，过滤器实质上是操作该查询和分析语句。

- 过滤器类型：通过日志字段的Key和Value进行过滤。在执行过滤器操作时，将其作为过滤条件增加到查询和分析语句前，使用AND或NOT连接。例如Key: Value AND [search query] | [sql query]，表示在原查询和分析语句的结果中，查找包

含Key:Value的日志。在过滤器类型的过滤器中，Value可以多选，也可以直接输入。多选时过滤条件之间为或（or）关系。

- 时序过滤器类型：动态添加Label和Value进行过滤。在添加过滤器时，可以添加过滤条件，各个过滤条件之间使用AND连接。

前提条件

- 已成功采集到日志。
- 已添加图表到仪表盘。
- 日志流已配置结构化规则，具体操作请参考**结构化配置**。

限制条件

一个仪表盘最多可添加10个过滤器。

添加过滤器

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘”，选择待操作的仪表盘。

步骤2 单击仪表盘名称进入详情页。

步骤3 单击  ，在“过滤器”页面中，参考**添加日志仪表盘过滤器**配置过滤器的相关参数。

说明

不支持过滤数值型的字段。

表 6-15 添加过滤器参数

参数	说明
过滤器名称	仅支持输入英文、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。
查询方式	过滤器选中的条件与已有图表查询条件组合方式。支持AND和NOT两种方式，默认为AND。
Key值	配置需要过滤的字段。仅支持输入英文、数字、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，且不能是纯数字。
别名	Key值的别名，用于区分不同字段。仅支持输入英文、数字、中文、中划线、下划线及小数点，且不能以小数点开头、下划线开头或以小数点结尾。

参数	说明
静态列表项	设置Key值对应的Value，多次单击“添加静态列表项”可添加多个Value。 单击“添加静态列表项”可添加Value，需配置如下参数： ● 列表项名称：需要过滤的Key值对应的Value字段名称。仅支持输入英文、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。 ● 别名：Value的别名。 ● 默认选中：开启“默认选中”，可直接对添加的Value进行过滤选中。 ● 操作：单击  删除添加的Value。
添加动态列表项	动态列表项为对应查询和分析语句的查询结果，在不同的时间范围，查询结果是动态变化的。 ● 关闭“添加动态列表项”，无法设置查询结果的动态变化。 ● 开启“添加动态列表项”，通过添加动态列表项显示查询结果的动态变化，即为Key值配置动态Value。需配置如下参数： 日志组：选择待查询的日志组。 日志流：选择待查询的日志流。 SQL引擎：支持管道符版本和非管道符版本。管道符版本的SQL查询默认语法为*** | select ***，非管道符版本的SQL查询默认语法为**select *** 动态列表来源：支持**字段模糊匹配**和**SQL查询**。 字段模糊匹配：选择当前日志流中配置的结构化字段。 SQL查询：输入SQL查询语句。单击“查询”，可预览动态列表项。

步骤4 设置完成后，单击“确定”即可完成过滤器的添加。

----结束

6.3.3 日志仪表盘模板

6.3.3.1 APIG 仪表盘模板

APIG（API Gateway）提供高性能、高可用、高安全的API托管服务，能快速将企业服务能力包装成标准API服务，帮助您轻松构建、管理和部署任意规模的API，并上架API云商店进行售卖。借助API网关，可以简单、快速、低成本、低风险地实现内部系统集成、业务能力开放及业务能力变现。API网关帮助您变现服务能力的同时，降低企业研发投入，让您专注于企业核心业务，提升运营效率。

APIG仪表盘模板支持**查看APIG访问中心**、**查看APIG监控中心**、**分析APIG秒级监控**。

前提条件

- 已采集APIG日志，详情请参见**API网关APIG接入LTS**。
- 日志配置结构化，详情请参见**设置云端结构化解析日志**。

查看 APIG 访问中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘”。

步骤2 在仪表盘模板下方，选择“APIG仪表盘模板 > APIG访问中心”，查看图表详情。

- 过滤请求域名，所关联的查询分析语句如下所示：
```
select distinct(host)
```
- 过滤app_id，所关联的查询分析语句如下所示：
```
select distinct(app_id)
```
- **访问量PV分布(世界)**图表所关联的查询分析语句如下所示：
```
SELECT ip_to_country(my_remote_addr) as country,sum(ori_pv) as PV from (select my_remote_addr, count(1) as ori_pv
 group by my_remote_addr
 ORDER BY ori_pv desc
 LIMIT 10000) GROUP BY country HAVING country not in ('','保留地址','*')
```
- **平均时延分布（中国）**所关联的查询分析语句如下所示：
```
SELECT province,round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)"FROM (SELECT ip_to_province(my_remote_addr) as province,sum(rt)/sum(ori_pv) * 1000 AS "平均延迟(ms)" from (select my_remote_addr, sum(request_time) as rt,count(1) as ori_pv
 group by my_remote_addr
 ORDER BY ori_pv desc
 LIMIT 10000) WHERE  IP_TO_COUNTRY (my_remote_addr) = '中国' GROUP BY province )
 where province not in ('','保留地址','*')
```
- **平均时延分布（世界）**所关联的查询分析语句如下所示：
```
SELECT country,round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 2 ) AS "平均延迟(ms)"FROM (SELECT ip_to_country(my_remote_addr) as country,sum(rt)/sum(ori_pv)  * 1000 AS "平均延迟(ms)" from (select my_remote_addr, sum(request_time) as rt,count(1) as ori_pv
 group by my_remote_addr
 ORDER BY ori_pv desc
 LIMIT 10000) GROUP BY country )
where  country not in ('','保留地址','*')
```
- **今日PV/UV**所关联的查询分析语句如下所示：
```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss' ) as _time_,PV,UV FROM (select TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT600S') AS _time_ , count(1) as PV,  APPROX_COUNT_DISTINCT(my_remote_addr) as UV from log WHERE __time <= CURRENT_TIMESTAMP  and __time >= DATE_TRUNC( 'DAY',(CURRENT_TIMESTAMP + INTERVAL '8' HOUR)) - INTERVAL '8' HOUR group by _time_ order by _time_)
```
- **区域访问TOP10(省份)**所关联的查询分析语句如下所示：
```
select ip_to_province(my_remote_addr) as "province", sum(ori_pv) as "访问次数" from(select my_remote_addr, count(1) as ori_pv
 group by my_remote_addr
 ORDER BY ori_pv desc
 LIMIT 10000)group by "province" HAVING "province" <> '-1' order by "访问次数" desc limit 10
```
- **区域访问TOP10(城市)**图表所关联的查询分析语句如下所示：
```
select ip_to_city(my_remote_addr) as "city", sum(ori_pv) as "访问次数" from(select my_remote_addr, count(1) as ori_pv
 group by my_remote_addr
 ORDER BY ori_pv desc
 LIMIT 10000) group by "city" HAVING  "city" <> '-1' order by "访问次数" desc  limit 10
```
- **Host访问TOP10**图表所关联的查询分析语句如下所示：
```
select  host as "Host", count(1) as "PV" group by "Host" order by "PV" desc limit 10
```


- **UserAgent访问TOP10**图表所关联的查询分析语句如下所示：
```
select http_user_agent as "UserAgent", count(1) as "PV" group by "UserAgent" order by "PV" desc limit 10
```
- **设备占比(终端)**图表所关联的查询分析语句如下所示：
```
select case when regexp_like(lower(http_user_agent), 'iphone|ipod|android|ios') then '移动端' else 'PC端' end as type , count(1) as total group by  type
```
- **设备占比(系统)**图表所关联的查询分析语句如下所示：
```
select case when regexp_like(lower(http_user_agent), 'iphone|ipod|ios') then 'IOS' when regexp_like(lower(http_user_agent), 'android') then 'Android' else 'other' end as type , count(1) as total group by  type HAVING type != 'other'
```
- **TOP URL**图表所关联的查询分析语句如下所示：
```
select router_uri , count(1) as pv, APPROX_COUNT_DISTINCT(my_remote_addr) as UV, round(sum( case when status < 400 then 1 else 0 end  ) * 100.0 / count(1), 2) as "访问成功率" group by router_uri ORDER by pv desc
```
- **TOP 访问IP**图表所关联的查询分析语句如下所示：
```
select my_remote_addr as "来源IP",ip_to_country(my_remote_addr) as "国家",ip_to_province(my_remote_addr) as "省份",ip_to_city(my_remote_addr) as "城市",ip_to_provider(my_remote_addr) as "运营商",count(1) as "PV" group by my_remote_addr ORDER by "PV" desc limit 100
```

----结束

查看 APIG 监控中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘”。

步骤2 在仪表盘模板下方，选择“APIG仪表盘模板 > APIG监控中心”，查看图表详情。

- 过滤请求域名，所关联的查询分析语句如下所示：
```
select distinct(host)
```
- 过滤app_id，所关联的查询分析语句如下所示：
```
select distinct(app_id)
```
- **访问量PV**图表所关联的查询分析语句如下所示：
```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss' ) as _time_,PV FROM ( SELECT TIME_CEIL ( TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'), 'PT300S' ) AS _time_, count( 1 ) AS PV FROM log GROUP BY _time_ )
```
- **请求成功率**图表所关联的查询分析语句如下所示：
```
select ROUND(sum(case when status < 400 then 1 else 0 end) * 100.0 / count(1),2) as cnt
```
- **平均延迟**图表所关联的查询分析语句如下所示：
```
select round(avg(request_time) * 1000, 3) as cnt
```
- **4XX请求数**图表所关联的查询分析语句如下所示：
```
SELECT COUNT(1) as cnt WHERE "status" >= 400 and "status" < 500
```
- **404请求数**图表所关联的查询分析语句如下所示：
```
SELECT COUNT(1) as cnt WHERE "status" = 404
```
- **429请求数**图表所关联的查询分析语句如下所示：
```
SELECT COUNT(1) as cnt WHERE "status" = 429
```
- **504请求数**图表所关联的查询分析语句如下所示：
```
SELECT COUNT(1) as cnt WHERE "status" = 504
```
- **5XX请求数**图表所关联的查询分析语句如下所示：
```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss') as _time_,cnt FROM ( SELECT TIME_CEIL ( TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'), 'PT300S' ) AS _time_, count( 1 ) AS cnt FROM log where "status" >= 500 GROUP BY _time_ )
```
- **状态码分布**图表所关联的查询分析语句如下所示：
```
SELECT status, COUNT(1) AS rm GROUP BY status
```
- **访问量UV**图表所关联的查询分析语句如下所示：


```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss' ) as _time_,UV FROM (select
TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT600S') AS _time_ ,
APPROX_COUNT_DISTINCT(my_remote_addr) as UV  from log group by _time_)
```

- **流量**图表所关联的查询分析语句如下所示：

```
select TIME_FORMAT(_time_,'yyyy-MM-dd HH:mm:ss') AS _time_,round( CASE WHEN "入流量" > 0
THEN "入流量" ELSE 0 END, 2 ) AS "入流量",round( CASE WHEN "出流量" > 0 THEN "出流量" ELSE 0
END, 2 ) AS "出流量" FROM (SELECT TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss
ZZ'),'PT600S') AS _time_,sum(request_length) / 1024.0 AS "入流量",sum(bytes_sent) / 1024.0 AS "出流
量" group by  _time_)
```

- **访问失败率**图表所关联的查询分析语句如下所示：

```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss') as _time_,round( CASE WHEN "失败率" > 0
THEN "失败率" ELSE 0 END, 2 ) AS "失败率",round( CASE WHEN "5XX比例" > 0 THEN "5XX比例" ELSE
0 END, 2 ) AS "5XX比例" from (select TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss
ZZ'),'PT600S') AS _time_,sum(case when status >= 400 then 1 else 0 end) * 100.0 / count(1) as '失败
率' , sum(case when status >=500 THEN 1 ELSE 0 END)*100.0/COUNT(1) as '5XX比例' group by
_time_)
```

- **延迟**图表所关联的查询分析语句如下所示：

```
select TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss') as _time_,round( CASE WHEN "平均" > 0
THEN "平均" ELSE 0 END, 2 ) AS "平均",round( CASE WHEN "P50" > 0 THEN "P50" ELSE 0 END, 2 )
AS "P50",round( CASE WHEN "P90" > 0 THEN "P90" ELSE 0 END, 2 ) AS "P90",round( CASE WHEN
"P99" > 0 THEN "P99" ELSE 0 END, 2 ) AS "P99",round( CASE WHEN "P9999" > 0 THEN "P9999" ELSE
0 END, 2 ) AS "P9999" from (select TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss
ZZ'),'PT600S') as _time_,avg(request_time) * 1000 as "平均", APPROX_QUANTILE_DS("request_time",
0.50)*1000 as "P50", APPROX_QUANTILE_DS("request_time", 0.90)*1000 as
"P90" ,APPROX_QUANTILE_DS("request_time", 0.99)*1000 as
'P99',APPROX_QUANTILE_DS("request_time", 0.9999)*1000 as 'P9999' group by  _time_)
```

- **Host请求TOP**图表所关联的查询分析语句如下所示：

```
SELECT "host", pv, uv, round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END,
2 ) AS "访问成功率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END,
3 ) AS "平均延迟(ms)", round( CASE WHEN "入流量(KB)" > 0 THEN "入流量(KB)" ELSE 0 END, 3 ) AS
"入流量(KB)", round( CASE WHEN "出流量(KB)" > 0 THEN "出流量(KB)" ELSE 0 END, 3 ) AS "出流量
(KB)"  FROM ( SELECT "host", count( 1 ) AS pv, APPROX_COUNT_DISTINCT ( my_remote_addr ) AS
uv, sum( CASE WHEN "status" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)",
avg( request_time ) * 1000 AS "平均延迟(ms)", sum( request_length ) / 1024.0 AS "入流量(KB)",
sum( bytes_sent ) / 1024.0 AS "出流量(KB)"  WHERE "host" != ''  GROUP BY "host" ) ORDER BY pv
DESC
```

- **Host延迟TOP**图表所关联的查询分析语句如下所示：

```
SELECT "host", pv, round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 )
AS "访问成功率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 )
AS "平均延迟(ms)", round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS
"P90延迟(ms)", round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99
延迟(ms)" FROM ( SELECT "host", count( 1 ) AS pv, sum( CASE WHEN "status" < 400 THEN 1 ELSE 0
END ) * 100.0 / count( 1 ) AS "访问成功率(%)", avg( request_time ) * 1000 AS "平均延迟
(ms)",APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90延迟(ms)",
APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99延迟(ms)" WHERE "host" != ''  GROUP BY
"host" ) ORDER BY "平均延迟(ms)" desc
```

- **Host失败率TOP**图表所关联的查询分析语句如下所示：

```
SELECT "host", pv,round( CASE WHEN "访问失败率(%)" > 0 THEN "访问失败率(%)" ELSE 0 END, 2 )
AS "访问失败率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 )
AS "平均延迟(ms)", round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS
"P90延迟(ms)", round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99
延迟(ms)"  FROM ( SELECT "host", count( 1 ) AS pv, sum( CASE WHEN "status" >= 400 THEN 1 ELSE
0 END ) * 100.0 / count( 1 ) AS "访问失败率(%)", avg( request_time ) * 1000 AS "平均延迟(ms)",
APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90延迟(ms)",
APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99延迟(ms)" WHERE "host" != ''  GROUP BY
"host"  ) ORDER BY "访问失败率(%)" desc
```

- **URL请求TOP**图表所关联的查询分析语句如下所示：

```
SELECT upstream_uri, pv,uv, round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0
END, 2 ) AS "访问成功率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0
END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "入流量(KB)" > 0 THEN "入流量(KB)" ELSE 0 END,
3 ) AS "入流量(KB)", round( CASE WHEN "出流量(KB)" > 0 THEN "出流量(KB)" ELSE 0 END, 3 ) AS "出
流量(KB)"  FROM ( SELECT upstream_uri, count( 1 ) AS pv, APPROX_COUNT_DISTINCT
( my_remote_addr ) AS uv, sum( CASE WHEN "status" < 400 THEN 1 ELSE 0 END ) * 100.0 /
count( 1 ) AS "访问成功率(%)", avg( request_time ) * 1000 AS "平均延迟(ms)",
```



```
sum( request_length ) / 1024.0 AS "入流量(KB)", sum( bytes_sent ) / 1024.0 AS "出流量(KB)"  WHERE "host" != ''  GROUP BY upstream_uri  ) ORDER BY pv desc
```

- **URL失败率TOP**图表所关联的查询分析语句如下所示：

```
SELECT upstream_uri, pv, round( CASE WHEN "访问失败率(%)" > 0 THEN "访问失败率(%)" ELSE 0 END, 2 ) AS "访问失败率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90延迟(ms)", round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟(ms)" FROM( SELECT upstream_uri, count( 1 ) AS pv, sum( CASE WHEN "status" >= 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问失败率(%)", avg( request_time ) * 1000 AS "平均延迟(ms)", APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90延迟(ms)", APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99延迟(ms)" WHERE "host" != '' GROUP BY upstream_uri  ) ORDER BY "访问失败率(%)" desc
```

- **后端请求TOP**图表所关联的查询分析语句如下所示：

```
SELECT addr, pv, uv, round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS "访问成功率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "入流量(KB)" > 0 THEN "入流量(KB)" ELSE 0 END, 3 ) AS "入流量(KB)", round( CASE WHEN "出流量(KB)" > 0 THEN "出流量(KB)" ELSE 0 END, 3 ) AS "出流量(KB)"  FROM ( SELECT my_remote_addr as addr, count( 1 ) AS pv, APPROX_COUNT_DISTINCT ( my_remote_addr ) AS uv, sum( CASE WHEN "status" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)", avg( request_time ) * 1000 AS "平均延迟(ms)", sum( request_length ) / 1024.0 AS "入流量(KB)", sum( bytes_sent ) / 1024.0 AS "出流量(KB)"  WHERE "host" != ''  GROUP BY addr  having length(my_remote_addr) > 2) ORDER BY "pv" desc
```

- **后端延迟TOP**图表所关联的查询分析语句如下所示：

```
SELECT addr,pv,round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS "访问成功率(%)",round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)",round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90延迟(ms)",round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟(ms)" FROM (SELECT my_remote_addr as addr,count( 1 ) AS pv,sum( CASE WHEN "status" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)",avg( request_time ) * 1000 AS "平均延迟(ms)",APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90延迟(ms)",APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99延迟(ms)" WHERE "host" != '' and "my_remote_addr" != '-' GROUP BY addr ) ORDER BY "平均延迟(ms)" desc
```

- **后端失败率TOP**图表所关联的查询分析语句如下所示：

```
SELECT addr, pv, round( CASE WHEN "访问失败率(%)" > 0 THEN "访问失败率(%)" ELSE 0 END, 2 ) AS "访问失败率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90延迟(ms)", round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟(ms)"  FROM ( SELECT my_remote_addr as addr, count( 1 ) AS pv, sum( CASE WHEN "status" >= 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问失败率(%)", avg( request_time ) * 1000 AS "平均延迟(ms)", APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90延迟(ms)", APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99延迟(ms)" WHERE "host" != '' and "my_remote_addr" != '-' GROUP BY addr) ORDER BY "访问失败率(%)" desc
```

- **URL延迟TOP**图表所关联的查询分析语句如下所示：

```
SELECT upstream_uri, pv,round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS "访问成功率(%)",round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)",round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90延迟(ms)",round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟(ms)" FROM (SELECT upstream_uri, count( 1 ) AS pv, sum( CASE WHEN "status" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)", avg( request_time ) * 1000 AS "平均延迟(ms)", APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90延迟(ms)", APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99延迟(ms)" WHERE "host" != ''  GROUP BY upstream_uri  ) ORDER BY "平均延迟(ms)" desc
```

----结束

查看 APIG 秒级监控

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘”。

步骤2 在仪表盘模板下方，选择“APIG仪表盘模板 > APIG秒级监控”，查看图表详情。

- 过滤请求域名，所关联的查询分析语句如下所示：

```
select distinct(host)
```


- 过滤app_id，所关联的查询分析语句如下所示：
```
select distinct(app_id)
```
- **QPS**图表所关联的查询分析语句如下所示：
```
SELECT TIME_FORMAT(TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT1S'),'yyyy-MM-dd HH:mm:ss') AS _time_ , COUNT(*) as QPS from log group by _time_
```
- **成功率**图表所关联的查询分析语句如下所示：
```
select __time,round(CASE WHEN "成功率" > 0 THEN "成功率" else 0 end,2) as "成功率" from (select TIME_FORMAT(TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT5S'),'yyyy-MM-dd HH:mm:ss') as __time, sum(case when status < 400 then 1 else 0 end) * 100.0 / count(1) as '成功率' from log group by __time)
```
- **延迟**图表所关联的查询分析语句如下所示：
```
select __time,round(CASE WHEN "访问延迟" > 0 THEN "访问延迟" else 0 end,2) as "访问延迟",round(CASE WHEN "Upstream延迟" > 0 THEN "Upstream延迟" else 0 end,2) as "Upstream延迟" from (select TIME_FORMAT(TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT5S'),'yyyy-MM-dd HH:mm:ss') as __time, avg(request_time)* 1000 as '访问延迟',avg(upstream_response_time)* 1000 as 'Upstream延迟' from log group by __time)
```
- **流量**图表所关联的查询分析语句如下所示：
```
select __time,round( CASE WHEN "请求流量" > 0 THEN "请求流量" ELSE 0 END, 3 ) AS "请求流量",round( CASE WHEN "返回body流量" > 0 THEN "返回body流量" ELSE 0 END, 3 ) AS "返回body流量" from (select TIME_FORMAT(TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT5S'),'yyyy-MM-dd HH:mm:ss') as __time , sum("request_length") / 1024.0 as "请求流量", sum("body_bytes_sent") / 1024.0 as "返回body流量" group by __time)
```
- **状态码**图表所关联的查询分析语句如下所示：
```
SELECT TIME_CEIL ( TIME_PARSE ( time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ' ), 'PT5S' ) AS "time", SUM( CASE WHEN "status" >= 200 AND "status" < 300 THEN 1 ELSE 0 END ) AS "2XX", SUM( CASE WHEN "status" >= 300 AND "status" < 400 THEN 1 ELSE 0 END ) AS "3XX", SUM( CASE WHEN "status" >= 400 AND "status" < 500 THEN 1 ELSE 0 END ) AS "4XX", SUM( CASE WHEN "status" >= 500 AND "status" < 600 THEN 1 ELSE 0 END ) AS "5XX", SUM( CASE WHEN "status" < 200 OR "status" >= 600 THEN 1 ELSE 0 END ) AS "其他" FROM log  WHERE TIME_PARSE ( time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ' ) IS NOT NULL GROUP BY "time"  ORDER BY "time" ASC LIMIT 100000
```
- **后端响应码**图表所关联的查询分析语句如下所示：
```
SELECT TIME_CEIL ( TIME_PARSE ( time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ' ), 'PT5S' ) AS "time", SUM( CASE WHEN "upstream_status" >= 200 AND "upstream_status" < 300 THEN 1 ELSE 0 END ) AS "2XX", SUM( CASE WHEN "upstream_status" >= 300 AND "upstream_status" < 400 THEN 1 ELSE 0 END ) AS "3XX", SUM( CASE WHEN "upstream_status" >= 400 AND "upstream_status" < 500 THEN 1 ELSE 0 END ) AS "4XX", SUM( CASE WHEN "upstream_status" >= 500 AND "upstream_status" < 600 THEN 1 ELSE 0 END ) AS "5XX", SUM( CASE WHEN "upstream_status" < 200 OR "upstream_status" >= 600 THEN 1 ELSE 0 END ) AS "其他" FROM log  WHERE TIME_PARSE ( time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ' ) IS NOT NULL GROUP BY "time"  ORDER BY "time" ASC LIMIT 100000
```

----结束

6.3.3.2 CCE 仪表盘模板

云容器引擎（Cloud Container Engine，简称CCE）提供高度可扩展的、高性能的企业级Kubernetes集群。

CCE仪表盘模板支持**查看CCE日志节点操作**、**查看CCE日志K8s对象操作**、**查看CCE日志K8s事件查询**、**查看CCE日志K8s事件中心**、**查看CCE日志聚合检索**、**查看CCE日志账号操作审计**和**查看CCE日志审计中心**。

前提条件

- 已采集CCE日志，详情请参见**云容器引擎CCE应用日志接入LTS**。
- 日志配置结构化，详情请参见**设置云端结构化解析日志**。

查看 CCE 日志节点操作

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“CCE仪表盘模板 > CCE日志节点操作”，查看图表详情。

- 过滤节点名称，所关联的查询分析语句如下所示：
  ```
  select distinct("objectRef.name")
  ```
- 过滤操作用户，所关联的查询分析语句如下所示：
  ```
  select distinct("user.username")
  ```
- 过滤状态码，所关联的查询分析语句如下所示：
  ```
  select distinct("responseStatus.code")
  ```
- 过滤操作类型，所关联的查询分析语句如下所示：
  ```
  select distinct("verb")
  ```
- **节点数趋势**图表所关联的查询分析语句如下所示：
  ```
  SELECT  time_series( TIME_PARSE(LEFT(requestReceivedTimestamp, 23),'yyyy-MM-dd"T"HH:mm:ss.SSS'), 'PT1H', 'yyyy-MM-dd HH', '0' ) as "dt",  count(DISTINCT("objectRef.name")) as "节点数" where "objectRef.resource" = 'nodes'  and "objectRef.subresource" = 'status'  and "verb" in ('update', 'patch') and "user.username" = 'system:node' group by  "dt" order by  "dt" desc limit  10000
  ```
- **非系统用户操作趋势**图表所关联的查询分析语句如下所示：
  ```
  SELECT time_series( TIME_PARSE(LEFT(requestReceivedTimestamp, 23),'yyyy-MM-dd"T"HH:mm:ss.SSS'), 'PT1H', 'yyyy-MM-dd HH', '0' ) as "dt", count(*) as "请求", "user.username" where "objectRef.resource" = 'nodes' and "user.username" not in ( 'kube-controller-manager','kube-apiserver-kubelet-client','apiserver') and "user.username" not like  'system:%' and "verb" in ('create','delete','update','patch') group by "dt", "user.username" order by "dt","请求" desc limit 10000
  ```
- **create操作状态码分布**图表所关联的查询分析语句如下所示：
  ```
  select cast("responseStatus.code" as varchar) as "状态码", count(*) as "count" where "objectRef.resource" = 'nodes' and "verb" = 'create' group by "状态码"
  ```
- **delete操作状态码分布**图表所关联的查询分析语句如下所示：
  ```
  select cast("responseStatus.code" as varchar) as "状态码", count(*) as "count" where "objectRef.resource" = 'nodes' and "verb" = 'delete' group by "状态码"
  ```
- **patch操作状态码分布**图表所关联的查询分析语句如下所示：
  ```
  select cast("responseStatus.code" as varchar) as "状态码", count(*) as "count" where "objectRef.resource" = 'nodes' and "verb" = 'patch' group by "状态码"
  ```
- **update操作状态码分布**图表所关联的查询分析语句如下所示：
  ```
  select cast("responseStatus.code" as varchar) as "状态码", count(*) as "count" where "objectRef.resource" = 'nodes' and "verb" = 'update' group by "状态码"
  ```
- **节点封锁/解除封锁操作状态码分布**图表所关联的查询分析语句如下所示：
  ```
  select cast("responseStatus.code" as varchar) as "状态码", count(*)  as "count" where "requestObject" in ('{"spec":{"unschedulable":false}}','{"spec":{"unschedulable":true}}')  group by "状态码"
  ```
- **Label操作状态码分布**图表所关联的查询分析语句如下所示：
  ```
  select cast("responseStatus.code" as varchar) as "状态码", count(*) as "count" where "objectRef.resource" = 'nodes' and "verb" in ('patch','update') and "requestObject" = 'labels' and "requestObject" = 'metadata' group by "状态码"
  ```
- **Taint操作状态码分布**图表所关联的查询分析语句如下所示：
  ```
  select cast("responseStatus.code" as varchar) as "状态码", count(*) as "count" where "objectRef.resource" = 'nodes' and "verb" in ('patch','update') and "requestObject" = 'taints' group by "状态码"
  ```
- **驱逐操作状态码分布**图表所关联的查询分析语句如下所示：
  ```
  select cast("responseStatus.code" as varchar) as "状态码", count(*) as "count" where "objectRef.subresource" = 'eviction' and "objectRef.resource" = 'pods' and "verb" = 'create' group by "状态码"
  ```
- **节点增删操作列表**图表所关联的查询分析语句如下所示：
  ```
  select  "auditID" AS "Audit ID", "objectRef.name" AS "节点名", "verb" AS "操作动作", "stageTimestamp" AS "操作时间", "user.username" AS "操作账号", "responseStatus.code" AS "状态码" where "objectRef.resource" = 'nodes' and "verb" in ('create','delete')
  ```
- **Taint操作列表**图表所关联的查询分析语句如下所示：


```
select  "auditID" AS "Audit ID", "objectRef.name" AS "节点名","requestObject" AS "Taints", "requestReceivedTimestamp" AS "操作时间", "user.username" AS "操作账号", "responseStatus.code" AS "状态码"  where "objectRef.resource" = 'nodes' and "verb" = 'patch' and "requestObject" = 'taints'
```

- **驱逐操作列表**图表所关联的查询分析语句如下所示：

```
select  "auditID" AS "Audit ID", "objectRef.name" AS "pod", "sourceIPs" AS "源地址", "requestReceivedTimestamp" AS "操作时间", "user.username" AS "操作账号", "responseStatus.code" AS "状态码"  where "objectRef.resource" = 'pods' and "verb" = 'create' and "objectRef.subresource" = 'eviction'
```

- **Label操作列表**图表所关联的查询分析语句如下所示：

```
select  "auditID" AS "Audit ID", "objectRef.name" AS "节点名", "requestObject" AS "Label", "requestReceivedTimestamp" AS "操作时间", "user.username" AS "操作账号", "responseStatus.code" AS "状态码"  where "objectRef.resource" = 'nodes' and "verb" = 'patch' and "requestObject" = 'labels'
```

- **封锁操作列表**图表所关联的查询分析语句如下所示：

```
select "auditID" AS "Audit ID", "objectRef.name" AS "节点名",  "requestReceivedTimestamp" AS "操作时间", "user.username" AS "操作账号", "responseStatus.code" AS "状态码" where "verb" = 'patch' and "objectRef.resource" = 'nodes' and "requestObject" ='true' and "requestObject" = 'unschedulable'
```

- **取消封锁操作列表**图表所关联的查询分析语句如下所示：

```
select "auditID" AS "Audit ID", "objectRef.name" AS "节点名",  "requestReceivedTimestamp" AS "操作时间", "user.username" AS "操作账号", "responseStatus.code" AS "状态码" where "verb" = 'patch' and "objectRef.resource" = 'nodes' and "requestObject" not in ('true','taints','unschedulable')
```

----结束

查看 CCE 日志 K8s 对象操作

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“CCE仪表盘模板 > CCE日志K8s对象操作”，查看图表详情。

- 过滤命名空间，所关联的查询分析语句如下所示：

```
select distinct("objectRef.namespace")
```

- 过滤操作类型，所关联的查询分析语句如下所示：

```
select distinct("verb")
```

- 过滤状态码，所关联的查询分析语句如下所示：

```
select distinct("responseStatus.code")
```

- 过滤资源对象，所关联的查询分析语句如下所示：

```
select distinct("objectRef.name")
```

- 过滤资源类型，所关联的查询分析语句如下所示：

```
select distinct("objectRef.resource")
```

- 过滤操作用户，所关联的查询分析语句如下所示：

```
select distinct("user.username")
```

- **重要操作趋势**图表所关联的查询分析语句如下所示：

```
SELECT REPLACE(LEFT(requestReceivedTimestamp, 16),'T',' ') AS "dt", "verb" as "操作类型", count(*) as "count" where "verb" in ('create','delete','update','patch') and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "dt","操作类型" order by "dt" limit 10000
```

- **非系统用户操作趋势**图表所关联的查询分析语句如下所示：

```
SELECT REPLACE(LEFT(requestReceivedTimestamp, 16),'T',' ') AS "dt", count(*) as "请求次数","user.username" WHERE "user.username" not in ('kube-controller-manager','kube-apiserver-kubelet-client','apiserver') and "user.username" not like 'system:%'  and  "verb" in ('create','delete','update','patch')  and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresss','configmaps','secrets','pvcs')  group by "dt", "user.username"  limit 10000
```

- **create操作资源类型分布**图表所关联的查询分析语句如下所示：

```
select "objectRef.resource" as "资源类型", count(*) as "count" where "verb" = 'create' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims')  group by  "objectRef.resource"
```


- **delete操作资源类型分布**图表所关联的查询分析语句如下所示：
```
select "objectRef.resource" as "资源类型", count(*) as "count" where "verb" = 'delete' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims')  group by  "objectRef.resource"
```
- **update操作资源类型分布**图表所关联的查询分析语句如下所示：
```
select "objectRef.resource" as "资源类型", count(*) as "count" where "verb" = 'update' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims')  group by  "objectRef.resource"
```
- **patch操作资源类型分布**图表所关联的查询分析语句如下所示：
```
select "objectRef.resource" as "资源类型", count(*) as "count" where "verb" = 'patch' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims')  group by  "objectRef.resource"
```
- **create操作用户分布**图表所关联的查询分析语句如下所示：
```
select "user.username" as "操作用户", count(*)  as "count" where "verb" = 'create' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by  "user.username"
```
- **delete操作用户分布**图表所关联的查询分析语句如下所示：
```
select "user.username" as "操作用户", count(*) as "count" where "verb" = 'delete' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by  "user.username"
```
- **update操作用户分布**图表所关联的查询分析语句如下所示：
```
select "user.username" as "操作用户", count(*)  as "count" where "verb" = 'update' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by  "user.username"select "user.username" as "操作用户", count(*)  as "count" where "verb" = 'update' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by  "user.username"
```
- **patch操作用户分布**图表所关联的查询分析语句如下所示：
```
select "user.username" as "操作用户", count(*)  as "count"  where "verb" = 'patch' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by  "user.username"
```
- **create操作状态码分布**图表所关联的查询分析语句如下所示：
```
select cast("responseStatus.code" as varchar) as "状态码", count(*) as "count" where "verb" = 'create' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by  "responseStatus.code"
```
- **delete操作状态码分布**图表所关联的查询分析语句如下所示：
```
select cast("responseStatus.code" as varchar) as "状态码", count(*) as "count" where "verb" = 'delete' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by  "responseStatus.code"
```
- **update操作状态码分布**图表所关联的查询分析语句如下所示：
```
select cast("responseStatus.code" as varchar) as "状态码", count(*) as "count" where "verb" = 'update' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by  "responseStatus.code"
```
- **patch操作状态码分布**图表所关联的查询分析语句如下所示：
```
select cast("responseStatus.code" as varchar) as "状态码", count(*)  as "count" where "verb" = 'patch' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by  "responseStatus.code"
```
- **create操作趋势**图表所关联的查询分析语句如下所示：
```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "资源类型", count(*) as "count" where "verb" = 'create' and "objectRef.resource" in
```



```
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims')  group by dt, "objectRef.resource" order by dt limit 10000
```

- **delete操作趋势**图表所关联的查询分析语句如下所示：

```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "资源类型", count(*)
as "count" where "verb" = 'delete' and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims')  group by dt, "objectRef.resource" order by dt limit 10000
```

- **update操作趋势**图表所关联的查询分析语句如下所示：

```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "资源类型", count(*)
as "count" where "verb" = 'update' and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims')  group by dt, "objectRef.resource" order by dt limit 10000
```

- **patch操作趋势**图表所关联的查询分析语句如下所示：

```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "资源类型", count(*)
as "count" where "verb" = 'patch' and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims')  group by dt, "objectRef.resource" order by dt limit 10000
```

----结束

查看 CCE 日志 K8s 事件查询

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“CCE仪表盘模板 > CCE日志K8s对象操作”，查看图表详情。

- 过滤命名空间，所关联的查询分析语句如下所示：

```
select distinct("objectRef.namespace")
```

- 过滤操作类型，所关联的查询分析语句如下所示：

```
select distinct("verb")
```

- 过滤状态码，所关联的查询分析语句如下所示：

```
select distinct("responseStatus.code")
```

- 过滤资源对象，所关联的查询分析语句如下所示：

```
select distinct("objectRef.name")
```

- 过滤资源类型，所关联的查询分析语句如下所示：

```
select distinct("objectRef.resource")
```

- 过滤操作用户，所关联的查询分析语句如下所示：

```
select distinct("user.username")
```

- **重要操作趋势**图表所关联的查询分析语句如下所示：

```
SELECT REPLACE(LEFT(requestReceivedTimestamp, 16),'T',' ') AS "dt", "verb" as "操作类型", count(*)
as "count" where "verb" in ('create','delete','update','patch') and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by "dt","操作类型" order by "dt" limit 10000
```

- **非系统用户操作趋势**图表所关联的查询分析语句如下所示：

```
SELECT REPLACE(LEFT(requestReceivedTimestamp, 16),'T',' ') AS "dt", count(*) as "请求次数
","user.username" WHERE "user.username" not in ('kube-controller-manager','kube-apiserver-kubelet-
client','apiserver') and "user.username" not like 'system:%'  and  "verb" in
('create','delete','update','patch')  and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresss','configmaps','secrets',
'pvcs')  group by "dt", "user.username"  limit 10000
```

- **create操作资源类型分布**图表所关联的查询分析语句如下所示：

```
select "objectRef.resource" as "资源类型", count(*) as "count" where "verb" = 'create' and
"objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims')  group by  "objectRef.resource"
```

- **delete操作资源类型分布**图表所关联的查询分析语句如下所示：

```
select "objectRef.resource" as "资源类型", count(*) as "count" where "verb" = 'delete' and
"objectRef.resource" in
```



```
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims')  group by  "objectRef.resource"
```

- **update操作资源类型分布**图表所关联的查询分析语句如下所示：

```
select "objectRef.resource" as "资源类型", count(*) as "count" where "verb" = 'update' and
"objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims')  group by  "objectRef.resource"
```

- **patch操作资源类型分布**图表所关联的查询分析语句如下所示：

```
select "objectRef.resource" as "资源类型", count(*) as "count" where "verb" = 'patch' and
"objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims')  group by  "objectRef.resource"
```

- **create操作用户分布**图表所关联的查询分析语句如下所示：

```
select "user.username" as "操作用户", count(*)  as "count" where "verb" = 'create' and
"objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by  "user.username"
```

- **delete操作用户分布**图表所关联的查询分析语句如下所示：

```
select "user.username" as "操作用户", count(*) as "count" where "verb" = 'delete' and
"objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by  "user.username"
```

- **update操作用户分布**图表所关联的查询分析语句如下所示：

```
select "user.username" as "操作用户", count(*)  as "count" where "verb" = 'update' and
"objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by  "user.username"select "user.username" as "操作用户",
count(*)  as "count" where "verb" = 'update' and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by  "user.username"
```

- **patch操作用户分布**图表所关联的查询分析语句如下所示：

```
select "user.username" as "操作用户", count(*)  as "count"  where "verb" = 'patch' and
"objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by  "user.username"
```

- **create操作状态码分布**图表所关联的查询分析语句如下所示：

```
select cast("responseStatus.code" as varchar) as "状态码", count(*) as "count" where "verb" = 'create'
and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by  "responseStatus.code"
```

- **delete操作状态码分布**图表所关联的查询分析语句如下所示：

```
select cast("responseStatus.code" as varchar) as "状态码", count(*) as "count" where "verb" = 'delete'
and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by  "responseStatus.code"
```

- **update操作状态码分布**图表所关联的查询分析语句如下所示：

```
select cast("responseStatus.code" as varchar) as "状态码", count(*) as "count" where "verb" = 'update'
and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by  "responseStatus.code"
```

- **patch操作状态码分布**图表所关联的查询分析语句如下所示：

```
select cast("responseStatus.code" as varchar) as "状态码", count(*)  as "count" where "verb" = 'patch'
and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by  "responseStatus.code"
```

- **create操作趋势**图表所关联的查询分析语句如下所示：

```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "资源类型", count(*)
as "count" where "verb" = 'create' and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims')  group by dt, "objectRef.resource" order by dt limit 10000
```


- **delete操作趋势**图表所关联的查询分析语句如下所示：
```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "资源类型", count(*) as "count" where "verb" = 'delete' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims')  group by dt, "objectRef.resource" order by dt limit 10000
```
- **update操作趋势**图表所关联的查询分析语句如下所示：
```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "资源类型", count(*) as "count" where "verb" = 'update' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims')  group by dt, "objectRef.resource" order by dt limit 10000
```
- **patch操作趋势**图表所关联的查询分析语句如下所示：
```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "资源类型", count(*) as "count" where "verb" = 'patch' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims')  group by dt, "objectRef.resource" order by dt limit 10000
```

----结束

查看 CCE 日志 K8s 事件中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“CCE仪表盘模板 > CCE日志K8s事件中心”，查看图表详情。

- 事件等级分为Warning和Normal。
- 过滤事件类型，所关联的查询分析语句如下所示：
```
select distinct("name")
```
- 过滤集群ID，所关联的查询分析语句如下所示：
```
select distinct("cluster_id")
```
- 过滤命名空间，所关联的查询分析语句如下所示：
```
select distinct("namespace")
```
- 过滤名称，所关联的查询分析语句如下所示：
```
select distinct("resource_name")
```
- **Conntrack Full**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( "total", 3600) as diff from( select count(1) as "total" from log where  "name"= 'ConntrackFull'  ) )
```
- **事件同步异常**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( "total", 3600) as diff from( select count(1) as "total" from log where  "name"= 'NTPIsDown') )
```
- **节点Pid不足**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( "total", 3600) as diff from( select count(1) as "total" from log where  "name" in ('PIDPressure','NodeHasPIDPressure') ) )
```
- **节点FD不足**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( "total", 3600) as diff from( select count(1) as "total" from log where  "name"= 'NodeHasFDPressure') )
```
- **节点磁盘空间不足**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( "total", 3600) as diff from( select count(1) as "total" from log where  "name"= 'NodeHasDiskPressure') )
```
- **Pod OOM**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( "total", 3600) as diff from( select count(1) as "total" from log where   "reason" in ('OOMKilling','PodOOMKilling')) )
```


- **DockerHung**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( "total", 3600) as diff from( select count(1) as "total" from log where  "name"= 'Failed' and "reason" = 'DockerHung') )
```
- **节点重启**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( "total", 3600) as diff from( select count(1) as "total" from log where  "name"= 'NodeRebooted') )
```
- **镜像拉取失败**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( "total", 3600) as diff from( select count(1) as "total" from log where  "name"= 'Failed' and "reason" = 'ImagePullBackOff') )
```
- **节点OOM**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( "total", 3600) as diff from( select count(1) as "total" from log where  "name" = 'SystemOOM') )
```
- **Pod启动失败**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( "total", 3600) as diff from( select count(1) as "total" from log where  "name"= 'Failed' and "resource_kind" = 'Pod' and  "reason" = 'ImagePullBackOff') )
```
- 事**件分布**图表所关联的查询分析语句如下所示：
```
select "type", count(*) as "事件数" group by "type"
```
- **Warning事件趋势**图表所关联的查询分析语句如下所示：
```
select time_series(__time, 'PT1H', 'yyyy-MM-dd HH', '0') as "dt",count(1) as "count"  from log  where "type" = 'Warning'  group by "dt" order by "dt"
```
- **Error事件趋势**图表所关联的查询分析语句如下所示：
```
select time_series(__time, 'PT1H', 'yyyy-MM-dd HH', '0') as "dt",count(1) as "count" from log  where "type" = 'Error' group by "dt" order by "dt"
```
- **Pod OOM事件列表**所关联的查询分析语句如下所示：
```
select TIME_FORMAT( __time, 'yyyy-MM-dd HH:mm:ss', '+08:00') as "Time", "resource_kind" as "事件目标", "name" as "类型", "resource_name" as "目标名", "reason" as "详细内容" from log where "name" in ('OOMKilling','PodOOMKilling') order by __time desc limit 100
```
- **Pod驱动事件列表**所关联的查询分析语句如下所示：
```
select TIME_FORMAT( __time, 'yyyy-MM-dd HH:mm:ss', '+08:00' ) as "Time", "resource_kind" as "事件目标", "name" as "类型", "resource_name" as "目标名", "reason" as "详细内容" from log where "name" = 'NodeControllerEviction' order by __time desc limit 100
```
- **重要事件列表**所关联的查询分析语句如下所示：
```
select TIME_FORMAT( __time, 'yyyy-MM-dd HH:mm:ss', '+08:00' ) as "Time", "type" as "等级", "resource_kind" as "事件目标", "name" as "类型", "resource_name" as "目标名", "reason" as "详细内容" from log where "type" in ('Warning','Error') order by __time desc limit 100
```

----结束

查看 CCE 日志聚合检索

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“CCE仪表盘模板 > CCE日志聚合检索”，查看图表详情。

- 过滤命名空间，所关联的查询分析语句如下所示：
```
select distinct("objectRef.namespace")
```
- 过滤操作用户，所关联的查询分析语句如下所示：
```
select distinct("user.username")
```
- 过滤状态码，所关联的查询分析语句如下所示：
```
select distinct("responseStatus.code")
```
- 过滤操作类型，所关联的查询分析语句如下所示：
```
select distinct("verb")
```


- 过滤资源对象，所关联的查询分析语句如下所示：
```
select distinct("objectRef.name")
```
- 过滤资源类型，所关联的查询分析语句如下所示：
```
select distinct("objectRef.resource")
```
- 过滤请求URL，所关联的查询分析语句如下所示：
```
select distinct("requestURI")
```
- 过滤userAgent，所关联的查询分析语句如下所示：
```
select distinct("userAgent")
```
- **操作用户分布趋势**图表所关联的查询分析语句如下所示：
```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "user.username" as "操作用户", count(*) as "count" group by dt, "user.username" order by dt limit 10000
```
- **命名空间分布趋势**图表所关联的查询分析语句如下所示：
```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.namespace" as "命名空间", count(*) as "count"  group by dt, "objectRef.namespace" order by dt limit 10000
```
- **操作类型分布趋势**图表所关联的查询分析语句如下所示：
```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.namespace" as "命名空间", count(*) as "count"  group by dt, "objectRef.namespace" order by dt limit 10000
```
- **状态码分布趋势**图表所关联的查询分析语句如下所示：
```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, cast("responseStatus.code" as varchar) as "返回码", count(*)  as "count" group by dt, "返回码" order by dt limit 10000
```
- **资源类型分布趋势**图表所关联的查询分析语句如下所示：
```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "资源类型", count(*) as "count" group by dt, "objectRef.resource" order by dt limit 10000    SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "资源类型", count(*) as "count" group by dt, "objectRef.resource" order by dt limit 10000
```
- **重要操作列表**所关联的查询分析语句如下所示：
```
select  "auditID" AS "Audit ID", "verb" AS "操作类型", "requestReceivedTimestamp" AS "开始时间", "stageTimestamp" AS "结束时间", "user.username" AS "操作账号", "sourceIPs" AS "操作源","userAgent","objectRef.namespace" AS "命名空间", CONCAT(CONCAT("objectRef.resource", '/'), "objectRef.subresource") AS "操作对象", "objectRef.name" AS "资源名", "responseStatus.code" AS "返回码"
```

----结束

查看 CCE 日志账号操作审计

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“CCE仪表盘模板 > CCE日志账号操作审计”，查看图表详情。

- 过滤用户名，所关联的查询分析语句如下所示：
```
select distinct("user.username")
```
- 过滤命名空间，所关联的查询分析语句如下所示：
```
select distinct("objectRef.namespace")
```
- 过滤状态码，所关联的查询分析语句如下所示：
```
select distinct("responseStatus.code")
```
- **资源创建数**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(1) as total from log where "verb" = 'create') )
```
- **资源修改数**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(*)    as "total" from log where "verb" in ('update','patch')) )
```
- **资源删除数**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(*)    as "total" from log where "verb" = 'delete') )
```


- **操作命名空间分布**图表所关联的查询分析语句如下所示：
```
select case when "objectRef.namespace" is null then '_all__' else "objectRef.namespace" end as ns, count(1) as total group by  ns  limit 10000
```
- **删除资源分布**图表所关联的查询分析语句如下所示：
```
SELECT "objectRef.resource" as "resource", count(1) as "count" where  "verb" = 'delete' group by "resource"
```
- **操作轨迹**图表所关联的查询分析语句如下所示：
```
select case  when "操作" is null then '无' else "操作" end as "操作", "时间", v from  (select concat(CASE WHEN "objectRef.subresource" is null then "objectRef.resource" else "objectRef.subresource"  end, '[', verb, ']'  ) as "操作", time_series(__time, 'PT1H', 'yyyy-MM-dd HH', '0') as "时间", count(1) as v  from  log where "verb" in ('create', 'patch',  'update', 'delete')  group by "操作", "时间" order by "时间" desc  limit  10000  )
```
- **资源操作分布**图表所关联的查询分析语句如下所示：
```
select CASE WHEN "objectRef.subresource" is null then "objectRef.resource" else "objectRef.subresource" end as "资源", verb as "操作", count(1) as total where "verb" in ('create','update','patch','delete') group by "资源", "操作" limit 10000
```
- **创建资源列表**所关联的查询分析语句如下所示：
```
SELECT "auditID" as "事件ID", time_format("__time",'yyyy-MM-dd HH:mm:ss') as "操作时间", "requestURI" as "资源", "objectRef.name" as "资源名", "responseStatus.code" as "状态码","sourceIPs" as "源地址", "requestObject" as "详细内容" where "verb" = 'create' order by __time desc limit 1000
```
- **修改资源列表**所关联的查询分析语句如下所示：
```
SELECT auditID as "事件ID", time_format("__time",'yyyy-MM-dd HH:mm:ss') as "操作时间","requestURI" as "资源", "objectRef.name" as "资源名", "responseStatus.code" as "状态码","sourceIPs" as "源地址", requestObject as "详细内容" where "verb" in ('upate','patch') order by __time desc limit 1000
```
- **资源访问列表**所关联的查询分析语句如下所示：
```
SELECT auditID as "事件ID", time_format("__time",'yyyy-MM-dd HH:mm:ss') as "操作时间", "requestURI" as "资源", "objectRef.name" as "资源名", "responseStatus.code" as "状态码","sourceIPs" as "源地址", requestObject as "详细内容" where "verb" in ('get','list') order by __time desc limit 1000
```
- **资源删除列表**所关联的查询分析语句如下所示：
```
SELECT auditID as "事件ID", time_format("__time",'yyyy-MM-dd HH:mm:ss') as "操作时间", "requestURI" as "资源", "objectRef.name" as "资源名", "responseStatus.code" as "状态码","sourceIPs" as "源地址", requestObject as "详细内容" where "verb" = 'delete' order by __time desc limit 1000
```

----结束

查看 CCE 日志审计中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“CCE仪表盘模板 > CCE日志审计中心”，查看图表详情。

- 过滤命名空间，所关联的查询分析语句如下所示：
```
select distinct("objectRef.namespace")
```
- 过滤操作用户，所关联的查询分析语句如下所示：
```
select distinct("user.username")
```
- 过滤操作类型，所关联的查询分析语句如下所示：
```
select distinct("verb")
```
- 过滤状态码，所关联的查询分析语句如下所示：
```
select distinct("responseStatus.code")
```
- 过滤资源对象，所关联的查询分析语句如下所示：
```
select distinct("objectRef.name")
```
- 过滤资源类型，所关联的查询分析语句如下所示：
```
select distinct("objectRef.resource")
```
- 过滤请求URL，所关联的查询分析语句如下所示：
```
select distinct("requestURI")
```


- 过滤UserAgent，所关联的查询分析语句如下所示：
```
select distinct("userAgent")
```
- **总审计记录数**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total" , round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(1) as total from log ) )
```
- **操作用户数**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total" , round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc"  from (select compare( total , 86400) as diff from( select count(distinct("user.username")) as total from log ) )
```
- **活跃节点数**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(DISTINCT "user.username") as total     from log where "objectRef.resource" = 'nodes' and "objectRef.subresource" = 'status' and "verb" in ('update','put','patch') and "user.username" in ('node','system')) )
```
- **异常访问次数**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(1) as total from log where "responseStatus.code" >= 400) )
```
- **敏感操作次数**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total" , round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(1)  as "total" from log where ("verb" = 'create' AND "objectRef.subresource" = 'exec') OR ("verb" = 'create' AND "objectRef.subresource" = 'attach' AND "objectRef.resource" = 'pods') OR ("objectRef.resource" = 'secrets' AND "verb"= 'get' AND ( "user.username" != 'apiserver') AND ("user.username" not like 'system:node:%')) OR ("verb"= 'delete' AND ( "user.username" not like 'system:node:%') AND ( "user.username" not like 'system:serviceaccount:kube-system:%') AND ( "user.username" != 'system:apiserve') AND ( "user.username" != 'system:apiserve') AND ( "user.username" != 'system:kube-scheduler') AND ("user.username" != 'system:kube-controller-manager'))) )
```
- **创建操作次数**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(1) as total from log where verb = 'create') )
```
- **更新操作次数**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total" , round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc"  from (select compare( total , 86400) as diff from( select count(1) as total from log where verb in ('update','patch')) )
```
- **删除操作次数**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(1) as total from log where verb = 'delete') )
```
- **操作用户分布**图表所关联的查询分析语句如下所示：
```
select "user.username" as "用户名", count(*) as "count"  group by "用户名" order by "count" desc
```
- **命名空间分布**图表所关联的查询分析语句如下所示：
```
select "objectRef.namespace" as "命名空间", count(*) as "count"  group by "命名空间"
```
- **资源类型分布**图表所关联的查询分析语句如下所示：
```
select "objectRef.resource" as "资源类型", count(*) as "count"  group by "资源类型" order by "count" desc limit 20
```
- **操作类型分布**图表所关联的查询分析语句如下所示：
```
select verb as "操作类型", count(*) as "count" group by "操作类型" order by "count" desc
```
- **节点操作分布**图表所关联的查询分析语句如下所示：
```
select "verb" as "操作类型", count(*) as "count" where  "objectRef.resource" = 'nodes' AND ("verb" in ('create','delete') ) group by "操作类型" order by "count" desc
```
- **工作负载操作分布**图表所关联的查询分析语句如下所示：
```
select "verb" as "操作类型", count(*) as "count" where "verb" in ('create', 'delete') and "objectRef.resource" in ('deployments','statefulsets','daemonsets','jobs','cronjobs') group by "操作类型" order by "count" desc
```
- **Service/Ingress操作分布**图表所关联的查询分析语句如下所示：
```
select "verb" as "操作类型", count(*) as "count" where "verb" in ('create', 'delete') and "objectRef.resource" in ('ingressess','services') group by "verb"  order by "count" desc
```


- **重要操作趋势**图表所关联的查询分析语句如下所示：
```
SELECT REPLACE(LEFT("stageTimestamp", 16),'T',' ') AS "dt", "verb", count(*) as "count" where "verb" in ('create','delete','update','patch') group by "dt", "verb" order by "dt" limit 10000
```
- **非系统用户操作趋势**图表所关联的查询分析语句如下所示：
```
SELECT REPLACE(LEFT("stageTimestamp", 16),'T',' ') AS "dt", count(*) as "count", "user.username" as "用户名称" where "user.username" not in ('kube-controller-manager','kube-apiserver-kubelet-client','system','apiserver') group by "dt", "用户名称" order by "dt" limit 10000
```

----结束

6.3.3.3 CDN 仪表盘模板

CDN（Content Delivery Network，内容分发网络）记录了所有域名（包括已删除域名，如果您开通了企业项目，则已删除域名不支持此功能）被网络用户访问的详细日志，您可以将日志接入LTS，对您的业务资源被访问情况进行详细分析。

CDN仪表盘模板支持**查看CDN错误分析**、**查看CDN基础数据**、**查看CDN用户分析**和**查看CDN热门资源**。

前提条件

- 日志配置结构化，详情请参见**设置云端结构化解析日志**。

查看 CDN 错误分析

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘”。

步骤2 在仪表盘模板下方，选择“CDN仪表盘模板 > CDN错误分析”，查看图表详情。

- **错误域名访问Top5**图表所关联的查询分析语句如下所示：
```
select domain , count(*) as c where http_code > 400 group by domain order by c desc limit 5
```
- **错误URI访问Top5**图表所关联的查询分析语句如下所示：
```
select uri , count(*) as c where http_code > 400 group by uri order by c desc limit 5
```
- **错误请求状态分布**图表所关联的查询分析语句如下所示：
```
select http_code , count(*) as c where http_code > 400 group by http_code order by c desc
```
- **错误按运营商统计**图表所关联的查询分析语句如下所示：
```
select ip_to_provider(client_ip) as isp , count(*) as c where http_code > 400 group by isp having ip_to_provider(client_ip) != '' order by c desc limit 10
```
- **错误按客户端统计**图表所关联的查询分析语句如下所示：
```
select user_agent as "客户端版本", count(*) as "错误次数" where http_code > 400 group by user_agent order by "错误次数" desc limit 10
```
- **错误按省份统计**图表所关联的查询分析语句如下所示：
```
select ip_to_province(client_ip) as province , count(*) as c where http_code > 400 and IP_TO_COUNTRY (client_ip) = '中国' group by province order by c desc limit 50
```
- **4XX错误详情**图表所关联的查询分析语句如下所示：
```
SELECT
    province AS "省份",
    isp AS "运营商",
    c AS "错误次数",
    round( c * 100.0 / sum( c ), 2 ) AS "错误比率(%)"
  FROM
   (
   SELECT
    ip_to_province ( client_ip ) AS province,
    ip_to_provider ( client_ip ) AS isp,
    count(*) AS c
   FROM
    log
   WHERE
```



```
    http_code >= 400
    AND http_code < 500
   GROUP BY
    province,
    isp
   HAVING
    (
    ip_to_provider ( client_ip )) != ''
   ORDER BY
    c DESC
   )
  GROUP BY
   province,
   isp,
   c
```

- **5XX错误详情**图表所关联的查询分析语句如下所示：

```
SELECT
    province AS "省份",
    isp AS "运营商",
    c AS "错误次数",
    round( c * 100.0 / sum( c ), 2 ) AS "错误比率(%)"
   FROM
    (
    SELECT
     ip_to_province ( client_ip ) AS province,
     ip_to_provider ( client_ip ) AS isp,
     count(*) AS c
    FROM
     log
    WHERE
        http_code >= 500
    GROUP BY
     province,
     isp
    HAVING
     (
     ip_to_provider ( client_ip )) != ''
    ORDER BY
     c DESC
    )
   GROUP BY
    province,
    isp,
    c
```

- **错误按国家统计**图表所关联的查询分析语句如下所示：

```
select ip_to_country(client_ip) as country , count(*) as c where http_code > 400  group by country order by c desc limit 50
```

----结束

查看 CDN 基础数据

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘”。

步骤2 在仪表盘模板下方，选择“CDN仪表盘模板 > CDN基础数据”，查看图表详情。

- **缓存命中率**图表所关联的查询分析语句如下所示：

```
select round(diff[1],2) as Hit_ratio, round(diff[2],2) as diff, round((diff[3]-1)*100, 2) from (select compare(Hit_ratio, 86400) as diff from (select sum(s) * 100.0/count(*) as Hit_ratio from (select case when hit_info = 'HIT' then 1 else 0 end as s from log)))
```

- **下载速度**图表所关联的查询分析语句如下所示：

```
select round(diff[1],2) as speed, round(diff[2],2) as diff, round((diff[3]-1)*100, 2) from (select compare(speed, 86400) as diff from (select sum(response_size) * 1.0 /sum(response_time) as speed from log ))
```

- **访问状态**图表所关联的查询分析语句如下所示：


```
select http_code , count(*) as c group by http_code order by c desc
```

- **访问延时分布**图表所关联的查询分析语句如下所示：

```
select
    case when response_time < 100 then '~100ms'
    when response_time < 500 then '100~500ms'
    when response_time < 1000 then '500ms~1s'
    when response_time < 5000 then '1~5s'
    when response_time < 6000 then '5~6s'
    when response_time < 7000 then '6~7s'
    when response_time < 8000 then '7~8s'
    when response_time < 10000 then '8~10s'
    when response_time < 15000 then '10~15s'
    else '15s~' end as latency ,
    count(*) as cnt
    group by latency
    order by  cnt
```

- **请求带宽**图表所关联的查询分析语句如下所示：

```
select TIME_FORMAT (TIME_FLOOR(__time,'PT1M'), 'HH:mm', '+08:00') as thisdate,
    sum(response_size) * 8/1000000000.0 as "带宽Gbit/min"
    group by TIME_FLOOR(__time,'PT1M')
    order by TIME_FLOOR(__time,'PT1M')
```

- **访问次数/人数**图表所关联的查询分析语句如下所示：

```
select TIME_FORMAT (TIME_FLOOR(__time,'PT1M'), 'HH:mm', '+08:00') as thisdate,
    count(*) as pv, APPROX_COUNT_DISTINCT(client_ip) as uv group by TIME_FLOOR(__time,'PT1M')
order by TIME_FLOOR(__time,'PT1M')
```

- **访问平均延时**图表所关联的查询分析语句如下所示：

```
select TIME_FORMAT (TIME_FLOOR(__time,'PT1M'), 'HH:mm', '+08:00') as thisdate,
    avg(response_time) as "平均延时(ms)" group by TIME_FLOOR(__time,'PT1M') order by
TIME_FLOOR(__time,'PT1M')
```

- **请求命中率**图表所关联的查询分析语句如下所示：

```
select
    TIME_FORMAT (TIME_FLOOR(m_time,'PT1M'), 'HH:mm', '+08:00' ) as thisdate ,
    sum(is_hit)*100.0/count(*) as hit_ratio
    from  (select  TIME_FLOOR(__time,'PT1M') as m_time ,  case when hit_info = 'HIT'
     then 1 else 0 end as is_hit from log ) group by m_time order by m_time
```

----结束

查看 CDN 用户分析

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘”。

步骤2 在仪表盘模板下方，选择“CDN仪表盘模板 > CDN用户分析”，查看图表详情。

- **访问次数**图表所关联的查询分析语句如下所示：

```
select diff[1] as pv,diff[2] as diff, round(100*(diff[3]-1), 2) from (select compare(pv, 86400) as diff
from (select count(*) as pv from log))
```

- **访问人数**图表所关联的查询分析语句如下所示：

```
select diff[1] as uv, diff[2] as diff, round((diff[3]-1)*100, 2) from (select compare(uv , 86400) as diff
from (select APPROX_COUNT_DISTINCT(client_ip) as uv from log))
```

- **访问客户端统计**图表所关联的查询分析语句如下所示：

```
select ua as "客户端" , sum(c) as "访问次数" from (select case when strpos(ua , 'iphone') > 1 then
'iphone' when strpos(ua, 'ipad') > 1 then 'ipad' when strpos(ua, 'android') > 1 then 'android' when
strpos(ua, 'windows') > 1 then 'windows' when strpos(ua , 'mac') > 1 then 'mac' when strpos(ua,
'linux') > 1 then 'linux' else ua end as ua , c from (select count(*) as c , lower(user_agent) as ua from
log group by ua order by c desc limit 2000) ) group by "客户端" order by "访问次数" desc limit 100
```

- **运营商次数统计**图表所关联的查询分析语句如下所示：

```
select ip_to_provider(client_ip) as isp ,count(*) as "访问次数" group by isp order by "访问次数" desc
limit 100
```

- **访问地区分布**图表所关联的查询分析语句如下所示：

```
select ip_to_province(client_ip) as province , count(*) as cnt where IP_TO_COUNTRY (client_ip) = '中
国' group by province HAVING province not in ('','保留地址','*') order by cnt desc limit 100
```


- **有效访问用户TOP**图表所关联的查询分析语句如下所示：

```
SELECT  CASE    WHEN ip_to_country(client_ip) = '上海' THEN concat(client_ip, ' ( shanghai )') WHEN ip_to_province(client_ip) = '' THEN concat(client_ip, ' ( Unknown IP )')    WHEN ip_to_provider(client_ip) = '内网IP' THEN concat(client_ip, ' ( Private IP )')    ELSE concat(     client_ip,     ' ( ',     ip_to_country(client_ip),     '/',     ip_to_province(client_ip),     '/',     CASE       WHEN ip_to_city(client_ip) = '-1' THEN 'Unknown city'       ELSE ip_to_city(client_ip)     END,     ' ',     ip_to_provider(client_ip),     ' )'    ) END AS client,  pv as "总访问数",  (pv - success_count) as "错误访问数",  round( CASE WHEN "throughput" > 0 THEN "throughput" ELSE 0 END, 1 ) AS "下载总量(GB)"from  (   select     client_ip,     count(*) as pv,     sum(response_size) / 1024.0 / 1024 / 1024.0 AS throughput,     sum(       CASE         WHEN http_code < 400 THEN 1         ELSE 0       END     ) AS success_count    from     log     group by     client_ip     order by     success_count desc    limit     100  )
```

- **下载量TOP用户**图表所关联的查询分析语句如下所示：

```
SELECT CASE WHEN ip_to_country(client_ip)='上海' THEN concat(client_ip, ' ( shanghai )') WHEN ip_to_province(client_ip)='' THEN concat(client_ip, ' ( Unknown IP )') WHEN ip_to_provider(client_ip)='内网IP' THEN concat(client_ip, ' ( Private IP )') ELSE concat(client_ip, ' ( ', ip_to_country(client_ip), '/', ip_to_province(client_ip), '/',       CASE WHEN ip_to_city(client_ip)='-1' THEN 'Unknown city' ELSE ip_to_city(client_ip) END, ' ',ip_to_provider(client_ip), ' )') END AS client,       pv as "总访问数", error_count as "错误访问数" ,      round( CASE WHEN "throughput" > 0 THEN "throughput" ELSE 0 END, 1 ) AS "下载总量(GB)"      from (      select client_ip ,       count(*) as pv, sum(response_size)/1024.0/1024/1024.0 AS throughput ,       sum(CASE WHEN http_code > 400 THEN 1 ELSE 0 END) AS error_count       from log       group by client_ip       order by throughput desc       limit 100)
```

----结束

查看 CDN 热门资源

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘”。

步骤2 在仪表盘模板下方，选择“CDN仪表盘模板 > CDN热门资源”，查看图表详情。

- **域名访问次数Top5**图表所关联的查询分析语句如下所示：

```
select domain ,count(*) as cnt group by domain order by cnt desc limit 5
```

- **域名下载流量Top5**图表所关联的查询分析语句如下所示：

```
select domain , sum(response_size) as "下载总量" group by domain order by "下载总量" desc limit 5
```

- **热门访问（URI）**图表所关联的查询分析语句如下所示：

```
select uri as URI, "访问次数", "访问人数", round( CASE WHEN "下载总量(GB)" > 0 THEN "下载总量(GB)" ELSE 0 END, 2 ) AS "下载总量(GB)" from (       select uri ,count(*) as "访问次数" , APPROX_COUNT_DISTINCT(client_ip) as "访问人数", sum(response_size)/1024.0/1024.0/1024.0 as "下载总量(GB)" where http_code < 400 group by uri order by "访问次数" desc limit 100)
```

- **热门访问（来源）**图表所关联的查询分析语句如下所示：

```
select refer_domain as "来源",c as "次数",uv as "人数", round(c * 100.0 / sum(c), 2) as  "百分比%" from (select refer_domain as refer_domain,count(*) as c,APPROX_COUNT_DISTINCT(client_ip) as uv from log where refer_domain != '' group by refer_domain order by c desc limit 100 ) GROUP BY refer_domain, c, uv
```

- **全国访问次数分布统计**图表所关联的查询分析语句如下所示：

```
select ip_to_province(client_ip) as province , count(*) as cnt where IP_TO_COUNTRY (client_ip) = '中国' group by province HAVING province not in ('','保留地址','*') order by cnt desc limit 1000
```

- **全国下载网速统计**图表所关联的查询分析语句如下所示：

```
select province, round( CASE WHEN "speed" > 0 THEN "speed" ELSE 0 END, 3 ) AS "speed" from (select ip_to_province(client_ip) as province , sum(response_size)* 1.0 /(sum(response_time)+1) as "speed" , count(*) as c where IP_TO_COUNTRY (client_ip) = '中国' group by province HAVING province not in ('','保留地址','*') order by c desc limit 40)
```

- **省份统计**图表所关联的查询分析语句如下所示：

```
select ip_to_province(client_ip) as "省份" ,count(*) as "访问次数", sum(response_size)/1024.0/1024.0/1024.0 as "下载流量(GB)" , sum(response_size) * 1.0 /sum(response_time) as "下载速度(KB/s)" group by "省份" having ip_to_province(client_ip) != '' order by "下载流量(GB)" desc limit 200
```

- **运营商流量和速度**图表所关联的查询分析语句如下所示：

```
select ip_to_provider(client_ip) as isp , sum(response_size)* 1.0 /(sum(response_time)+1) as "下载速度(KB/s)" , sum(response_size)/1024.0/1024.0/1024.0 as "下载总量(GB)", count(*) as c group by isp having ip_to_provider(client_ip) != '' order by c desc limit 10
```


- **运营商统计**图表所关联的查询分析语句如下所示：
```
select "运营商", "访问次数", round( CASE WHEN "下载流量(GB)" > 0 THEN "下载流量(GB)" ELSE 0 END, 2 ) AS "下载流量(GB)",  round( CASE WHEN "下载速度(KB/s)" > 0 THEN "下载速度(KB/s)" ELSE 0 END, 2 ) AS "下载速度(KB/s)" from (  select ip_to_provider(client_ip) as "运营商" ,count(*) as "访问次数", sum(response_size)/1024.0/1024.0/1024.0 as "下载流量(GB)" , sum(response_size) * 1.0 /sum(response_time) as "下载速度(KB/s)" group by "运营商" having ip_to_provider(client_ip) != '' and "运营商" not in ('*') order by "下载流量(GB)" desc limit 200)
```

----结束

6.3.3.4 CFW 仪表盘模板

云防火墙（Cloud Firewall，CFW）是新一代的云原生防火墙，提供云上互联网边界和VPC边界的防护，包括实时入侵检测与防御、全局统一访问控制、全流量分析可视化、日志审计与溯源分析等，同时支持按需弹性扩容、AI提升智能防御能力、灵活扩展满足云上业务的变化和扩张需求，极简应用让用户快速灵活应对威胁。云防火墙可以通过攻击事件日志查看检测到的危险流量的危险等级、受影响的端口、命中的规则、攻击事件类型等信息；通过访问控制日志查看根据访问控制策略放行或阻断的所有流量，以便更好的调整访问控制策略。

CFW仪表盘模板支持**查看CFW访问日志中心**、**查看CFW流量日志中心**和**查看CFW攻击日志中心**。

前提条件

- 已采集CFW日志，详情请参见**云防火墙CFW接入LTS**。
- 日志配置结构化，详情请参见**设置云端结构化解析日志**。

查看 CFW 访问日志中心

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 在“日志应用”模块中，单击“CFW日志中心”，选择“进入仪表盘”。

步骤3 在仪表盘模板下方，选择“CFW仪表盘模板 > CFW访问日志中心”，查看图表详情。

- **互联网访问-拦截趋势**图展示互联网访问-拦截趋势的变化情况，所关联的查询分析语句如下所示：
```
select time_series(MILLIS_TO_TIMESTAMP(hit_time), 'PT1M', 'yyyy-MM-dd HH:mm:ss', '0') as t_time,COUNT(*) as frequency WHERE action='deny' AND direction='out2in' group by t_time order by t_time
```
- **主动外联-拦截趋势**图展示主动外联-拦截趋势的变化情况，所关联的查询分析语句如下所示：
```
select time_series(MILLIS_TO_TIMESTAMP(hit_time), 'PT1M', 'yyyy-MM-dd HH:mm:ss', '0') as t_time,COUNT(*) as frequency WHERE action='deny' AND direction='in2out' group by t_time order by t_time
```
- **互联网阻断应用TOP5**图展示互联网阻断应用TOP5的变化情况，所关联的查询分析语句如下所示：
```
SELECT app, COUNT(*) as frequency WHERE action='deny' AND direction='out2in' GROUP BY app ORDER BY frequency DESC LIMIT 5
```
- **互联网阻断目的TOP5**图展示互联网阻断目的TOP5的变化情况，所关联的查询分析语句如下所示：
```
SELECT dst_ip, COUNT(*) as frequency WHERE action='deny' AND direction='out2in' GROUP BY dst_ip ORDER BY frequency DESC LIMIT 5
```
- **互联网阻断来源TOP5**图展示互联网阻断来源TOP5的变化情况，所关联的查询分析语句如下所示：
```
SELECT src_ip, COUNT(*) as frequency WHERE action='deny' AND direction='out2in' GROUP BY src_ip ORDER BY frequency DESC LIMIT 5
```


- **主动外联阻断应用TOP5**图展示主动外联阻断应用TOP5的变化情况，所关联的查询分析语句如下所示：
```
SELECT app, COUNT(*) as frequency WHERE action='deny' AND direction='in2out' GROUP BY app ORDER BY frequency DESC LIMIT 5
```
- **主动外联阻断目的TOP5**图展示主动外联阻断目的TOP5的变化情况，所关联的查询分析语句如下所示：
```
SELECT dst_ip, COUNT(*) as frequency WHERE action='deny' AND direction='in2out' GROUP BY dst_ip ORDER BY frequency DESC LIMIT 5
```
- **主动外联阻断来源TOP5**图展示主动外联阻断来源TOP5的变化情况，所关联的查询分析语句如下所示：
```
SELECT src_ip, COUNT(*) as frequency WHERE action='deny' AND direction='in2out' GROUP BY src_ip ORDER BY frequency DESC LIMIT 5
```

----结束

查看 CFW 流量日志中心

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 在“日志应用”模块中，单击“CFW日志中心”，选择“进入仪表盘”。

步骤3 在仪表盘模板下方，选择“CFW仪表盘模板 > CFW流量日志中心”，查看图表详情。

- **互联网访问流量趋势**图展示互联网访问流量趋势的变化情况，所关联的查询分析语句如下所示：
```
select time_series(MILLIS_TO_TIMESTAMP(start_time), 'PT1M', 'yyyy-MM-dd HH:mm:ss', '0') as t_time, SUM(to_s_bytes) AS '入流量', SUM(to_c_bytes) AS '出流量' WHERE direction='out2in' group by t_time order by t_time
```
- **互联网访问流入地域分布(中国)**图展示互联网访问流入地域分布(中国)的变化情况，所关联的查询分析语句如下所示：
```
SELECT count(*) AS PV, ip_to_province(src_ip) AS province WHERE direction='out2in' and IP_TO_COUNTRY (src_ip) = '中国' GROUP BY province HAVING province not in ('','保留地址','*') ORDER BY PV DESC
```
- **互联网访问流入地域分布(世界)**图展示互联网访问流入地域分布(世界)的变化情况，所关联的查询分析语句如下所示：
```
SELECT count(*) AS PV, ip_to_country(src_ip) AS country WHERE direction='out2in' GROUP BY country HAVING country not in ('','保留地址','*') ORDER BY PV DESC
```
- **互联网访问应用分布**图展示互联网访问应用分布的变化情况，所关联的查询分析语句如下所示：
```
SELECT app, COUNT(*) AS num WHERE direction='out2in' GROUP BY app ORDER BY num DESC
```
- **互联网访问源IP TOP5**图展示互联网访问源IP TOP5的变化情况，所关联的查询分析语句如下所示：
```
select src_ip, SUM(bytes)/1024 as sum_bytes WHERE direction='out2in' GROUP BY src_ip ORDER BY sum_bytes DESC LIMIT 5
```
- **互联网访问目的IP TOP5**图展示互联网访问目的IP TOP5的变化情况，所关联的查询分析语句如下所示：
```
select dst_ip, SUM(bytes)/1024 as sum_bytes WHERE direction='out2in' GROUP BY dst_ip ORDER BY sum_bytes DESC LIMIT 5
```
- **主动外联流量趋势**图展示主动外联流量趋势的变化情况，所关联的查询分析语句如下所示：
```
select time_series(MILLIS_TO_TIMESTAMP(start_time), 'PT1M', 'yyyy-MM-dd HH:mm:ss', '0') as t_time, SUM(to_c_bytes) AS '入流量', SUM(to_s_bytes) AS '出流量' WHERE direction='in2out' group by t_time order by t_time
```
- **主动外联目的地域分布(中国)**图展示主动外联目的地域分布(中国)的变化情况，所关联的查询分析语句如下所示：
```
SELECT count(*) AS PV, ip_to_province(dst_ip) AS province WHERE direction='in2out' and IP_TO_COUNTRY (dst_ip) = '中国' GROUP BY province HAVING province not in ('','保留地址','*') ORDER BY PV DESC
```


- **目的地域分布(世界)**图展示目的地域分布(世界)的变化情况，所关联的查询分析语句如下所示：
  ```
  SELECT count(*) AS PV, ip_to_country(dst_ip) AS country WHERE direction='in2out' GROUP BY country HAVING country not in ('','保留地址','*') ORDER BY PV DESC
  ```
- **主动外联-应用分布**图展示主动外联-应用分布的变化情况，所关联的查询分析语句如下所示：
  ```
  SELECT app, COUNT(*) AS num WHERE direction='in2out' GROUP BY app ORDER BY num DESC
  ```
- **主动外联源IP TOP5**图展示主动外联源IP TOP5的变化情况，所关联的查询分析语句如下所示：
  ```
  select src_ip, SUM(bytes)/1024 as sum_bytes WHERE direction='in2out' GROUP BY src_ip ORDER BY sum_bytes DESC LIMIT 5
  ```
- **主动外联目的IP TOP5**图展示主动外联目的IP TOP5的变化情况，所关联的查询分析语句如下所示：
  ```
  select dst_ip, SUM(bytes)/1024 as sum_bytes WHERE direction='in2out' GROUP BY dst_ip ORDER BY sum_bytes DESC LIMIT 5
  ```

----结束

查看 CFW 攻击日志中心

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 在“日志应用”模块中，单击“CFW日志中心”，选择“进入仪表盘”。

步骤3 在仪表盘模板下方，选择“CFW仪表盘模板 > CFW攻击日志中心”，查看图表详情。

- **攻击趋势**图表所关联的查询分析语句如下所示：
  ```
  select time_series(MILLIS_TO_TIMESTAMP(event_time), 'PT1M', 'yyyy-MM-dd HH:mm:ss', '0') as t_time, count(*) as frequency group by t_time order by t_time
  ```
- **攻击来源分布(中国)**图表所关联的查询分析语句如下所示：
  ```
  SELECT count(*) as PV,ip_to_province(src_ip) as province WHERE  IP_TO_COUNTRY (src_ip) = '中国' GROUP BY province HAVING province not in ('','保留地址','*')
  ```
- **攻击来源分布(世界)**图表所关联的查询分析语句如下所示：
  ```
  SELECT count(*) AS PV,ip_to_country(src_ip) AS country GROUP BY country HAVING country not in ('','保留地址','*')
  ```
- **攻击类型分布**图表所关联的查询分析语句如下所示：
  ```
  SELECT attack_type, COUNT(*) as num GROUP BY attack_type ORDER BY num
  ```
- **攻击目的TOP5**图表所关联的查询分析语句如下所示：
  ```
  SELECT dst_ip, COUNT(*) as frequency GROUP BY dst_ip ORDER BY frequency  DESC LIMIT 5
  ```
- **攻击来源TOP5**图表所关联的查询分析语句如下所示：
  ```
  SELECT src_ip, COUNT(*) as frequency GROUP BY src_ip ORDER BY frequency DESC LIMIT 5
  ```

----结束

6.3.3.5 CSE 仪表盘模板

微服务引擎（Cloud Service Engine，CSE）是用于微服务应用的云中间件。用户可结合其他云服务，快速构建云原生微服务体系，实现微服务应用的快速开发和高可用运维。

CSE仪表盘模板支持**查看CSE层级访问中心**、**查看CSE层级监控中心**和**查看CSE层级秒级监控**。

前提条件

- 已采集CSE日志。

- 日志配置结构化，详情请参见**设置云端结构化解析日志**。

查看 CSE 层级访问中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“CSE仪表盘模板 > CSE层访问中心”，查看图表详情。

- 过滤上游IP，所关联的查询分析语句如下所示：
```
select distinct(upstream_host)
```
- 过滤调用链trace_id，所关联的查询分析语句如下所示：
```
select distinct(trace_id)
```
- **PV对比昨日**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100, 2) as inc from(select compare( "pv" , 86400) as diff from (select count(1) as "pv" from log))
```
- **PV对比上周**图表所关联的查询分析语句如下所示
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100, 2) as inc from(select compare( "pv" , 604800) as diff from (select count(1) as "pv" from log))
```
- **UV对比昨日**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100, 2) as inc from(select compare( "uv" , 86400) as diff from (select APPROX_COUNT_DISTINCT(authority) as "uv" from log))
```
- **UV对比上周**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100, 2) as inc from(select compare( "uv" , 604800) as diff from (select APPROX_COUNT_DISTINCT(authority) as "uv" from log))
```
- **访问量PV分布(中国)**图表所关联的查询分析语句如下所示：
```
select ip_to_province(authority) as province, sum(ori_pv) as pv from (select authority, count(1) as ori_pv  group by authority  ORDER BY ori_pv desc  LIMIT 10000)  where IP_TO_COUNTRY (authority) = '中国'  group by province HAVING province not in ('','保留地址','*')
```
- **访问量PV分布(世界)**图表所关联的查询分析语句如下所示：
```
SELECT ip_to_country(authority) as country,sum(ori_pv) as PV from (select authority, count(1) as ori_pv  group by authority  ORDER BY ori_pv desc  LIMIT 10000) GROUP BY country HAVING country not in ('','保留地址','*')
```
- **平均时延分布（中国）**图表所关联的查询分析语句如下所示：
```
SELECT province,round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)" FROM (SELECT ip_to_province(authority) as province,sum(rt)/sum(ori_pv) * 1000 AS "平均延迟(ms)" from (select authority, sum(duration) as rt,count(1) as ori_pv  group by authority ORDER BY ori_pv desc  LIMIT 10000) WHERE  IP_TO_COUNTRY (authority) = '中国' GROUP BY province )  where province not in ('','保留地址','*')
```
- **平均时延分布（世界）**图表所关联的查询分析语句如下所示：
```
SELECT country,round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 2 ) AS "平均延迟(ms)" FROM (SELECT ip_to_country(authority) as country,sum(rt)/sum(ori_pv)  * 1000 AS "平均延迟(ms)" from (select authority, sum(duration) as rt,count(1) as ori_pv  group by authority  ORDER BY ori_pv desc LIMIT 10000) GROUP BY country ) where  country not in ('','保留地址','*')
```
- **今日PV/UV**图表所关联的查询分析语句如下所示：
```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss') as _time_,PV,UV FROM (select TIME_CEIL(TIME_PARSE(start_time),'PT600S') AS _time_ , count(1) as PV, APPROX_COUNT_DISTINCT(authority) as UV from log WHERE __time <= CURRENT_TIMESTAMP  and __time >= DATE_TRUNC( 'DAY',(CURRENT_TIMESTAMP + INTERVAL '8' HOUR)) - INTERVAL '8' HOUR group by _time_ order by _time_)
```
- **区域访问TOP10(省份)**图表所关联的查询分析语句如下所示：
```
select ip_to_province(authority) as "province", sum(ori_pv) as "访问次数" from (select authority, count(1) as ori_pv  group by authority  ORDER BY ori_pv desc  LIMIT 10000) group by "province" HAVING "province" <> '-1' order by "访问次数" desc limit 10
```
- **区域访问TOP10(城市)**图表所关联的查询分析语句如下所示：
```
select ip_to_city(authority) as "city", sum(ori_pv) as "访问次数" from (select authority, count(1) as ori_pv  group by authority ORDER BY ori_pv desc LIMIT 10000) group by "city" HAVING  "city" <> '-1' order by "访问次数" desc  limit 10
```


- **Host访问TOP10**图表所关联的查询分析语句如下所示：
```
select  upstream_host as "Host", count(1) as "PV" group by "Host" order by "PV" desc limit 10
```
- **UserAgent访问TOP10**图表所关联的查询分析语句如下所示：
```
select user_agent as "UserAgent", count(1) as "PV" group by "UserAgent" order by "PV" desc limit 10
```
- **设备占比(终端)**图表所关联的查询分析语句如下所示：
```
select case when regexp_like(lower(user_agent), 'iphone|ipod|android|ios') then '移动端' else 'PC端' end as type , count(1) as total group by  type
```
- **设备占比(系统)**图表所关联的查询分析语句如下所示：
```
select case when regexp_like(lower(user_agent), 'iphone|ipod|ios') then 'IOS' when regexp_like(lower(user_agent), 'android') then 'Android' else 'other' end as type , count(1) as total group by  type HAVING type != 'other'
```
- **TOP URL**图表所关联的查询分析语句如下所示：
```
select path , count(1) as pv, APPROX_COUNT_DISTINCT(authority) as UV, round(sum( case when response_code < 400 then 1 else 0 end  ) * 100.0 / count(1), 2) as "访问成功率" group by path ORDER by pv desc
```
- **TOP 访问IP**图表所关联的查询分析语句如下所示：
```
select authority as "来源IP",ip_to_country(authority) as "国家",ip_to_province(authority) as "省份",ip_to_city(authority) as "城市",ip_to_provider(authority) as "运营商",count(1) as "PV" group by authority ORDER by "PV" desc limit 100
```

----结束

查看 CSE 层级监控中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“CSE仪表盘模板 > CSE层监控中心”，查看图表详情。

- 过滤上游IP，所关联的查询分析语句如下所示：
```
select distinct(upstream_host)
```
- 过滤调用链trace_id，所关联的查询分析语句如下所示：
```
select distinct(trace_id)
```
- **访问量PV**图表所关联的查询分析语句如下所示：
```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss') as _time_,PV FROM ( SELECT TIME_CEIL ( TIME_PARSE(start_time), 'PT300S' ) AS _time_, count( 1 ) AS PV FROM log GROUP BY _time_ )
```
- **请求成功率**图表所关联的查询分析语句如下所示：
```
select ROUND(sum(case when response_code < 400 then 1 else 0 end) * 100.0 / count(1),2) as cnt
```
- **平均延迟**图表所关联的查询分析语句如下所示：
```
select round(avg(duration) * 1000, 3) as cnt
```
- **4XX请求数**图表所关联的查询分析语句如下所示：
```
SELECT COUNT(1) as cnt WHERE "response_code" >= 400 and "response_code" < 500
```
- **404请求数**图表所关联的查询分析语句如下所示：
```
SELECT COUNT(1) as cnt WHERE "response_code" = 404
```
- **429请求数**图表所关联的查询分析语句如下所示：
```
SELECT COUNT(1) as cnt WHERE "response_code" = 429
```
- **504请求数**图表所关联的查询分析语句如下所示：
```
SELECT COUNT(1) as cnt WHERE "response_code" = 504
```
- **5XX请求数**图表所关联的查询分析语句如下所示：
```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss') as _time_,cnt FROM ( SELECT TIME_CEIL ( TIME_PARSE(start_time), 'PT300S' ) AS _time_, count( 1 ) AS cnt FROM log where "response_code" >= 500 GROUP BY _time_ )
```
- **状态码分布**图表所关联的查询分析语句如下所示：
```
SELECT response_code, COUNT(1) AS rm GROUP BY response_code
```
- **访问量UV**图表所关联的查询分析语句如下所示：


```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss') as _time_,UV FROM (select TIME_CEIL(TIME_PARSE(start_time),'PT600S') AS _time_ , APPROX_COUNT_DISTINCT(authority) as UV  from log group by _time_)
```

- **流量**图表所关联的查询分析语句如下所示：

```
select TIME_FORMAT(_time_,'yyyy-MM-dd HH:mm:ss') AS _time_,round( CASE WHEN "入流量" > 0 THEN "入流量" ELSE 0 END, 2 ) AS "入流量",round( CASE WHEN "出流量" > 0 THEN "出流量" ELSE 0 END, 2 ) AS "出流量" FROM (SELECT TIME_CEIL(TIME_PARSE(start_time),'PT600S') AS _time_,sum(bytes_received) / 1024.0 AS "入流量",sum(bytes_sent) / 1024.0 AS "出流量" group by _time_)
```

- **访问失败率**图表所关联的查询分析语句如下所示：

```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss') as _time_,round( CASE WHEN "失败率" > 0 THEN "失败率" ELSE 0 END, 2 ) AS "失败率",round( CASE WHEN "5XX比例" > 0 THEN "5XX比例" ELSE 0 END, 2 ) AS "5XX比例" from (select TIME_CEIL(TIME_PARSE(start_time),'PT600S') AS _time_,sum(case when response_code >= 400 then 1 else 0 end) * 100.0 / count(1) as '失败率' , sum(case when response_code >=500 THEN 1 ELSE 0 END)*100.0/COUNT(1) as '5XX比例' group by _time_)
```

- **延迟**图表所关联的查询分析语句如下所示：

```
select TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss') as _time_,round( CASE WHEN "平均" > 0 THEN "平均" ELSE 0 END, 2 ) AS "平均",round( CASE WHEN "P50" > 0 THEN "P50" ELSE 0 END, 2 ) AS "P50",round( CASE WHEN "P90" > 0 THEN "P90" ELSE 0 END, 2 ) AS "P90",round( CASE WHEN "P99" > 0 THEN "P99" ELSE 0 END, 2 ) AS "P99",round( CASE WHEN "P9999" > 0 THEN "P9999" ELSE 0 END, 2 ) AS "P9999" from (select TIME_CEIL(TIME_PARSE(start_time),'PT600S') as _time_,avg(duration) * 1000 as "平均", APPROX_QUANTILE_DS("duration", 0.50)*1000 as "P50", APPROX_QUANTILE_DS("duration", 0.90)*1000 as "P90" ,APPROX_QUANTILE_DS("duration", 0.99)*1000 as 'P99',APPROX_QUANTILE_DS("duration", 0.9999)*1000 as 'P9999' group by  _time_)
```

- **Host请求TOP**图表所关联的查询分析语句如下所示：

```
SELECT "upstream_host", pv, uv, round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS "访问成功率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "入流量(KB)" > 0 THEN "入流量(KB)" ELSE 0 END, 3 ) AS "入流量(KB)", round( CASE WHEN "出流量(KB)" > 0 THEN "出流量(KB)" ELSE 0 END, 3 ) AS "出流量(KB)"  FROM ( SELECT "upstream_host", count( 1 ) AS pv, APPROX_COUNT_DISTINCT ( authority ) AS uv, sum( CASE WHEN "response_code" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)", avg( duration ) * 1000 AS "平均延迟(ms)", sum( bytes_received ) / 1024.0 AS "入流量(KB)", sum( bytes_sent ) / 1024.0 AS "出流量(KB)"  WHERE "upstream_host" != '' GROUP BY "upstream_host" ) ORDER BY pv DESC
```

- **Host延迟TOP**图表所关联的查询分析语句如下所示：

```
SELECT "upstream_host", pv, round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS "访问成功率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90延迟(ms)", round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟(ms)" FROM ( SELECT "upstream_host", count( 1 ) AS pv, sum( CASE WHEN "response_code" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)", avg( duration ) * 1000 AS "平均延迟(ms)",APPROX_QUANTILE_DS(duration, 0.9) * 1000 AS "P90延迟(ms)", APPROX_QUANTILE_DS(duration, 0.99) * 1000 AS "P99延迟(ms)" WHERE "upstream_host" != '' GROUP BY "upstream_host" ) ORDER BY "平均延迟(ms)" desc
```

- **Host失败率TOP**图表所关联的查询分析语句如下所示：

```
SELECT "upstream_host", pv,round( CASE WHEN "访问失败率(%)" > 0 THEN "访问失败率(%)" ELSE 0 END, 2 ) AS "访问失败率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90延迟(ms)", round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟(ms)"  FROM ( SELECT "upstream_host", count( 1 ) AS pv, sum( CASE WHEN "response_code" >= 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问失败率(%)", avg( duration ) * 1000 AS "平均延迟(ms)", APPROX_QUANTILE_DS(duration, 0.9) * 1000 AS "P90延迟(ms)", APPROX_QUANTILE_DS(duration, 0.99) * 1000 AS "P99延迟(ms)" WHERE "upstream_host" != ''  GROUP BY "upstream_host") ORDER BY "访问失败率(%)" desc
```

- **URL请求TOP**图表所关联的查询分析语句如下所示：

```
SELECT path, pv,uv, round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS "访问成功率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "入流量(KB)" > 0 THEN "入流量(KB)" ELSE 0 END, 3 ) AS "入流量(KB)", round( CASE WHEN "出流量(KB)" > 0 THEN "出流量(KB)" ELSE 0 END, 3 ) AS "出流量(KB)"  FROM ( SELECT path, count( 1 ) AS pv, APPROX_COUNT_DISTINCT ( authority ) AS uv, sum( CASE WHEN "response_code" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)", avg( duration ) * 1000 AS "平均延迟(ms)", sum( bytes_received ) / 1024.0 AS "入流量(KB)", sum( bytes_sent ) / 1024.0 AS "出流量(KB)"  WHERE "upstream_host" != ''  GROUP BY path  ) ORDER BY pv desc
```


- **URL失败率TOP**图表所关联的查询分析语句如下所示：
```
SELECT path, pv, round( CASE WHEN "访问失败率(%)" > 0 THEN "访问失败率(%)" ELSE 0 END, 2 ) AS "访问失败率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90延迟(ms)", round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟(ms)" FROM( SELECT path, count( 1 ) AS pv, sum( CASE WHEN "response_code" >= 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问失败率(%)", avg( duration ) * 1000 AS "平均延迟(ms)", APPROX_QUANTILE_DS(duration, 0.9) * 1000 AS "P90延迟(ms)", APPROX_QUANTILE_DS(duration, 0.99) * 1000 AS "P99延迟(ms)" WHERE "upstream_host" != '' GROUP BY path ) ORDER BY "访问失败率(%)" desc
```
- **后端请求TOP**图表所关联的查询分析语句如下所示：
```
SELECT addr, pv, uv, round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS "访问成功率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "入流量(KB)" > 0 THEN "入流量(KB)" ELSE 0 END, 3 ) AS "入流量(KB)", round( CASE WHEN "出流量(KB)" > 0 THEN "出流量(KB)" ELSE 0 END, 3 ) AS "出流量(KB)"  FROM ( SELECT authority as addr, count( 1 ) AS pv, APPROX_COUNT_DISTINCT ( authority ) AS uv, sum( CASE WHEN "response_code" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)", avg( duration ) * 1000 AS "平均延迟(ms)", sum( bytes_received ) / 1024.0 AS "入流量(KB)", sum( bytes_sent ) / 1024.0 AS "出流量(KB)"  WHERE "upstream_host" != ''  GROUP BY addr  having length(authority) > 2) ORDER BY "pv" desc
```
- **后端延迟TOP**图表所关联的查询分析语句如下所示：
```
SELECT addr,pv,round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS "访问成功率(%)",round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)",round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90延迟(ms)",round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟(ms)" FROM (SELECT authority as addr,count( 1 ) AS pv,sum( CASE WHEN "response_code" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)",avg( duration ) * 1000 AS "平均延迟(ms)",APPROX_QUANTILE_DS(duration, 0.9) * 1000 AS "P90延迟(ms)",APPROX_QUANTILE_DS(duration, 0.99) * 1000 AS "P99延迟(ms)" WHERE "upstream_host" != '' and "authority" != '-' GROUP BY addr ) ORDER BY "平均延迟(ms)" desc
```
- **后端失败率TOP**图表所关联的查询分析语句如下所示：
```
SELECT addr, pv, round( CASE WHEN "访问失败率(%)" > 0 THEN "访问失败率(%)" ELSE 0 END, 2 ) AS "访问失败率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90延迟(ms)", round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟(ms)"  FROM ( SELECT authority as addr, count( 1 ) AS pv, sum( CASE WHEN "response_code" >= 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问失败率(%)", avg( duration ) * 1000 AS "平均延迟(ms)", APPROX_QUANTILE_DS(duration, 0.9) * 1000 AS "P90延迟(ms)", APPROX_QUANTILE_DS(duration, 0.99) * 1000 AS "P99延迟(ms)" WHERE "upstream_host" != '' and "authority" != '-' GROUP BY addr) ORDER BY "访问失败率(%)" desc
```
- **URL延迟TOP**图表所关联的查询分析语句如下所示：
```
SELECT path, pv,round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS "访问成功率(%)",round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)",round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90延迟(ms)",round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟(ms)" FROM (SELECT path, count( 1 ) AS pv, sum( CASE WHEN "response_code" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)", avg( duration ) * 1000 AS "平均延迟(ms)", APPROX_QUANTILE_DS(duration, 0.9) * 1000 AS "P90延迟(ms)", APPROX_QUANTILE_DS(duration, 0.99) * 1000 AS "P99延迟(ms)" WHERE "upstream_host" != ''  GROUP BY path  ) ORDER BY "平均延迟(ms)" desc
```

----结束

查看 CSE 层级秒级监控

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“CSE仪表盘模板 > CSE层秒级监控”，查看图表详情。

- 过滤上游IP，所关联的查询分析语句如下所示：
```
select distinct(upstream_host)
```
- 过滤调用链trace_id，所关联的查询分析语句如下所示：
```
select distinct(trace_id)
```


- **QPS**图表所关联的查询分析语句如下所示：
```
SELECT TIME_FORMAT(TIME_CEIL(TIME_PARSE(start_time),'PT5S'),'yyyy-MM-dd HH:mm:ss') AS _time_ , COUNT(*) as QPS from log group by _time_
```
- **成功率**图表所关联的查询分析语句如下所示：
```
select __time,round(CASE WHEN "成功率" > 0 THEN "成功率" else 0 end,2) as "成功率" from (select TIME_FORMAT(TIME_CEIL(TIME_PARSE(start_time),'PT5S'),'yyyy-MM-dd HH:mm:ss') as __time, sum(case when response_code < 400 then 1 else 0 end) * 100.0 / count(1) as '成功率' from log group by __time)
```
- **延迟**图表所关联的查询分析语句如下所示：
```
select __time,round(CASE WHEN "访问延迟" > 0 THEN "访问延迟" else 0 end,2) as "访问延迟",round(CASE WHEN "Upstream延迟" > 0 THEN "Upstream延迟" else 0 end,2) as "Upstream延迟" from (select TIME_FORMAT(TIME_CEIL(TIME_PARSE(start_time),'PT5S'),'yyyy-MM-dd HH:mm:ss') as __time, avg(duration)* 1000 as '访问延迟',avg(upstream_service_time)* 1000 as 'Upstream延迟' from log group by __time)
```
- **流量**图表所关联的查询分析语句如下所示：
```
select __time,round( CASE WHEN "请求流量" > 0 THEN "请求流量" ELSE 0 END, 3 ) AS "请求流量",round( CASE WHEN "返回body流量" > 0 THEN "返回body流量" ELSE 0 END, 3 ) AS "返回body流量" from (select TIME_FORMAT(TIME_CEIL(TIME_PARSE(start_time),'PT5S'),'yyyy-MM-dd HH:mm:ss') as __time , sum("bytes_received") / 1024.0 as "请求流量", sum("bytes_sent") / 1024.0 as "返回body流量" group by __time)
```
- **状态码**图表所关联的查询分析语句如下所示：
```
SELECT TIME_CEIL ( TIME_PARSE ( start_time ), 'PT5S' ) AS "time", SUM( CASE WHEN "response_code" >= 200 AND "response_code" < 300 THEN 1 ELSE 0 END ) AS "2XX", SUM( CASE WHEN "response_code" >= 300 AND "response_code" < 400 THEN 1 ELSE 0 END ) AS "3XX", SUM( CASE WHEN "response_code" >= 400 AND "response_code" < 500 THEN 1 ELSE 0 END ) AS "4XX", SUM( CASE WHEN "response_code" >= 500 AND "response_code" < 600 THEN 1 ELSE 0 END ) AS "5XX", SUM( CASE WHEN "response_code" < 200 OR "response_code" >= 600 THEN 1 ELSE 0 END ) AS "其他" FROM log  WHERE TIME_PARSE ( start_time ) IS NOT NULL GROUP BY "time" ORDER BY "time" ASC LIMIT 100000
```

----结束

6.3.3.6 DCS 仪表盘模板

分布式缓存服务（Distributed Cache Service，简称DCS）是一款内存数据库服务，兼容了Redis内存数据库引擎，满足用户高并发及数据快速访问的业务诉求。云日志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。

云日志服务支持日志采集向导一站式采集DCS日志，DCS审计日志中心仪表盘支持展示访问用户数、访问客户端数、审计日志条数等图表。

前提条件

日志配置结构化，详情请参见**设置云端结构化解析日志**。

DCS 审计日志中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘”。

步骤2 在仪表盘模板下方，选择“DCS仪表盘模板 > DCS审计日志中心”，查看图表详情。

- **访问用户数**图表所关联的查询分析语句如下所示：
```
select count(distinct(user)) as user_num
```
- **访问客户端数**图表所关联的查询分析语句如下所示：
```
select count(distinct(client_addr)) as client_num
```
- **审计日志条数**图表所关联的查询分析语句如下所示：
```
select count(1) as log_num
```


- **平均响应时间**图表所关联的查询分析语句如下所示：
```
select avg(use_time) as avg_time
```
- **平均QPS**图表所关联的查询分析语句如下所示：
```
select count(*) / CAST((TIMESTAMPDIFF (minute, MIN(__time),MAX(__time))+1) as FLOAT)
```
- **TOP5 用户**图表所关联的查询分析语句如下所示：
```
select user, count(1) as 'user_count' group by user order by count(1) desc LIMIT 5
```
- **TOP5 客户端**图表所关联的查询分析语句如下所示：
```
select client_addr, count(1) as 'remote_count' group by client_addr order by count(1) desc limit 5
```
- **TOP5 执行命令**图表所关联的查询分析语句如下所示：
```
select command_name, count(1) as 'command_count' group by command_name order by count(1) desc
```
- **热Key**图表所关联的查询分析语句如下所示：
```
SELECT count(*) as 'count',  command_keys GROUP by command_keys order by count(*) desc limit 5
```
- **审计日志详情**图表所关联的查询分析语句如下所示：
```
select  "client_addr" as '客户端IP',"client_type" as '客户端类型',"server_addr" as '服务端IP',"command_name" as '执行命令',"command_keys" as '命令KEYS',"command_param" as '命令内容',"command_type" as '命令类型',"use_time" as '执行耗时',"time" as '执行时间',"db" as 'DB',"user" as '账号名',"instance_id" as '实例ID',"role" as '节点角色',"extend" as '扩展信息'
```

----结束

6.3.3.7 DDS 仪表盘模板

文档数据库服务（Document Database Service）完全兼容MongoDB协议，提供安全、高可用、高可靠、弹性伸缩和易用的数据库服务，同时提供一键部署、弹性扩容、容灾、备份、恢复、监控和告警等功能。云日志服务进行分析日志、搜索日志、日志可视化、下载日志和查看实时日志等操作。

云日志服务支持日志采集向导一站式采集DDS日志，DDS审计日志中心展示审计日志条数、访问用户数、访问客户端数等图表。

前提条件

- 已采集DDS日志，详情请参见**文档数据库服务DDS接入LTS**。
- 日志配置结构化，详情请参见**设置云端结构化解析日志**。

DDS 审计日志中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘”。

步骤2 在仪表盘模板下方，选择“DDS仪表盘模板 > DDS审计日志中心”，查看图表详情。

- 过滤操作类型，所关联的查询分析语句如下所示：
```
select distinct(optype)
```
- 过滤客户端IP，所关联的查询分析语句如下所示：
```
select distinct(user_ip)
```
- 过滤数据库名，所关联的查询分析语句如下所示：
```
select distinct(db)
```
- 过滤用户名，所关联的查询分析语句如下所示：
```
select distinct(user)
```
- 过滤集合名，所关联的查询分析语句如下所示：
```
select distinct(coll)
```
- **审计日志条数**图表所关联的查询分析语句如下所示：
```
select count(1) as log_num
```

- **访问用户数**图表所关联的查询分析语句如下所示：
```
select count(distinct(user)) as user_num
```
- **访问客户端数**图表所关联的查询分析语句如下所示：
```
select count(distinct(user_ip)) as client_num
```
- **TOP5 执行命令**图表所关联的查询分析语句如下所示：
```
select optype, count(1) as 'command_count' group by optype order by count(1) desc LIMIT 5
```
- **TOP5 用户**图表所关联的查询分析语句如下所示：
```
select user, count(1) as 'user_count' group by user order by count(1) desc LIMIT 5
```
- **TOP5 客户端**图表所关联的查询分析语句如下所示：
```
select user_ip, count(1) as 'remote_count' group by user_ip order by count(1) desc LIMIT 5
```
- **审计日志详情**图表所关联的查询分析语句如下所示：
```
select "time" as "执行时间","user" as "用户名","param" as "查询语句","instanceid" as "实例ID","db" as "DB","coll" as "集合名","user_ip" as "客户端IP"
```

----结束

6.3.3.8 DMS 仪表盘模板

分布式消息服务Kafka版（Distributed Message Service for Kafka）是一款基于开源社区版Kafka提供的消息队列服务，向用户提供计算、存储和带宽资源独占式的Kafka专享实例。重平衡日志记录Rebalance的详情，包括Rebalance时间、原因和触发Rebalance的客户端等。

云日志服务支持日志采集向导一站式采集DMS重平衡日志，支持多维度分析，并为DMS-Rebalance日志配置结构化和仪表盘。该仪表盘主要展示DMS重平衡日志的重平衡消费组个数、重平衡次数、消费组重平衡次数、重平衡原因及组详情。

前提条件

- 已采集DMS日志，详情请参见**云防火墙CFW接入LTS**。
- 日志配置结构化，详情请参见**设置云端结构化解析日志**。

DMS 重平衡日志中心

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“仪表盘 ”。

步骤3 在仪表盘模板下方，选择“DMS仪表盘模板 > DMS重平衡日志中心”，查看图表详情。

- 消费组ID，所关联的查询分析语句如下所示：
```
select distinct("message.groupId")
```
- 过滤重平衡原因。
- **重平衡消费组个数**图表所关联的查询分析语句如下所示：
```
select count(distinct("message.groupId"))  as "total" from log where ("message.type"!='RESPONSE' and "message.type" !='REQUEST')
```
- **重平衡次数**图表所关联的查询分析语句如下所示：
```
select count(*) as 'total'  where ("message.type" !='RESPONSE' and "message.type" !='REQUEST')
```
- **消费组重平衡次数**图表所关联的查询分析语句如下所示：
```
select "message.groupId" as 'GroupId', count(*) as 'Count' where ('message.type' !='RESPONSE' and 'message.type' !='REQUEST')  group by "message.groupId"
```
- **重平衡原因及组详情**图表所关联的查询分析语句如下所示：


```
select __time  as 'Time', "message.type" as 'Type' ,"message.groupId" as 'GroupId', "message.reason" as 'Reason',"message.group" as 'Group' where ('message.type' !='RESPONSE' and 'message.type' !='REQUEST')
```

----结束

6.3.3.9 DSL 仪表盘模板

DSL加工是LTS为您提供的一站式日志加工平台，基于领域自定义的脚本语言和200多个内置函数，您可以在LTS控制台实现端到端的日志规整、富化、流转、脱敏、过滤等加工任务。

云日志服务支持DSL（Domain Specific Language）仪表盘模板，DSL加工任务监控中心主要展示加工任务ID、加工任务名称、输入行数、输出行数等信息。

前提条件

- 已创建DSL加工任务。
- 日志配置结构化，详情请参见**设置云端结构化解析日志**。

DSL 加工任务监控中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘”。

步骤2 在仪表盘模板下方，选择“DSL仪表盘模板 > DSL加工任务监控中心”，查看图表详情。

- 过滤加工任务ID，所关联的查询分析语句如下所示：
  ```
  select distinct(task_id)
  ```
- 过滤加工任务名称，所关联的查询分析语句如下所示：
  ```
  select distinct(task_name)
  ```
- **输入行数**图表所关联的查询分析语句如下所示：
  ```
  SELECT CASE  WHEN  "input" < 1000 THEN concat( cast( "input" AS VARCHAR ), '行' )  WHEN "input" < 1000 * 1000 THEN concat( cast( round( "input"/ 1000, 1 ) AS VARCHAR ), '千行' ) WHEN "input" < 1000000000 THEN concat( cast( round( "input"/ 1000000.0, 1 ) AS VARCHAR ), '百万行' ) WHEN "input"/ 1000.0 < 1000000000 THEN concat( cast( round( "input"/ 1000 / 1000000.0, 1 ) AS VARCHAR ), '十亿行' ) ELSE concat( cast( round( "input"/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), '万亿行' )  END AS  "total"  from (select sum("process.accept") as "input")
  ```
- **输出行数**图表所关联的查询分析语句如下所示
  ```
  SELECT CASE  WHEN  "delivered" < 1000 THEN concat( cast( "delivered" AS VARCHAR ), '行' ) WHEN "delivered" < 1000 * 1000 THEN concat( cast( round( "delivered"/ 1000, 1 ) AS VARCHAR ), '千行' ) WHEN "delivered" < 1000000000 THEN concat( cast( round( "delivered"/ 1000000.0, 1 ) AS VARCHAR ), '百万行' )  WHEN "delivered"/ 1000.0 < 1000000000 THEN concat( cast( round( "delivered"/ 1000 / 1000000.0, 1 ) AS VARCHAR ), '十亿行' ) ELSE concat( cast( round( "delivered"/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), '万亿行' )  END AS  "total"  from (select sum("process.delivered") as "delivered")
  ```
- **过滤行数**图表所关联的查询分析语句如下所示：
  ```
  SELECT CASE  WHEN  "drop" < 1000 THEN concat( cast( "drop" AS VARCHAR ), '行' )  WHEN "drop" < 1000 * 1000 THEN concat( cast( round( "drop"/ 1000, 1 ) AS VARCHAR ), '千行' ) WHEN "drop" < 1000000000 THEN concat( cast( round( "drop"/ 1000000.0, 1 ) AS VARCHAR ), '百万行' )  WHEN "drop"/ 1000.0 < 1000000000 THEN concat( cast( round( "drop"/ 1000 / 1000000.0, 1 ) AS VARCHAR ), '十亿行' ) ELSE concat( cast( round( "drop"/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), '万亿行' )  END AS  "total"  from (select sum("process.drop") as "drop")
  ```
- **失败行数**图表所关联的查询分析语句如下所示：
  ```
  SELECT CASE  WHEN  "failed" < 1000 THEN concat( cast( "failed" AS VARCHAR ), '行' )  WHEN "failed" < 1000 * 1000 THEN concat( cast( round( "failed"/ 1000, 1 ) AS VARCHAR ), '千行' ) WHEN "failed" < 1000000000 THEN concat( cast( round( "failed"/ 1000000.0, 1 ) AS VARCHAR ), '百万行' ) WHEN "failed"/ 1000.0 < 1000000000 THEN concat( cast( round( "failed"/ 1000 / 1000000.0, 1 ) AS VARCHAR ), '十亿行' ) ELSE concat( cast( round( "failed"/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), '万亿行' )  END AS  "total"  from (select sum("process.failed") as "failed")
  ```


- **执行记录**图表所关联的查询分析语句如下所示：
```
select TIME_FORMAT( MILLIS_TO_TIMESTAMP("start"), 'yyyy-MM-dd HH:mm:ss:SSS', '+08:00') as "统计开始时间",TIME_FORMAT( MILLIS_TO_TIMESTAMP("end"), 'yyyy-MM-dd HH:mm:ss:SSS', '+08:00') as "统计结束时间", "process.accept" as "输入行数", "process.delivered" as "输出行数", "process.drop" as "过滤行数", "process.failed" as "失败行数" limit 1000
```

----结束

6.3.3.10 ER 仪表盘模板

企业路由器（Enterprise Router, ER）可以连接虚拟私有云（Virtual Private Cloud, VPC）或本地网络来构建中心辐射型组网，是云上大规格、高带宽、高性能的集中路由器。企业路由器使用边界网关协议（Border Gateway Protocol, BGP），支持路由学习、动态选路以及链路切换，极大的提升网络的可扩展性及运维效率，从而保证业务的连续性。

云日志服务支持日志采集向导一站式采集ER日志，支持多维度分析，并为ER日志配置结构化和仪表盘。该仪表盘主要展示ER日志的TOP20包数统计、TOP20流量统计、流日志条数等信息。

前提条件

- 已采集ER流量日志，详情请参见**企业路由器ER接入LTS**。
- 日志配置结构化，详情请参见**设置云端结构化解析日志**。

ER 流量日志中心

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“仪表盘 ”。

步骤3 在仪表盘模板下方，选择“ER仪表盘模板 > ER流量日志中心”，查看图表详情。

- 过滤实例ID图，所关联的查询分析语句如下所示：
```
SELECT DISTINCT(instance_id)
```
- 过滤连接ID图，所关联的查询分析语句如下所示：
```
SELECT DISTINCT(resource_id)
```
- 流量方向图展示为静态过滤器，可按照入方向和出方向的流量进行过滤，所关联的查询分析语句如下所示：
- 过滤源IP图，所关联的查询分析语句如下所示：
```
SELECT DISTINCT(srcaddr)
```
- 过滤目的IP图，所关联的查询分析语句如下所示：
```
SELECT DISTINCT(dstaddr)
```
- 过滤协议类型图，所关联的查询分析语句如下所示：
```
SELECT DISTINCT(protocol)
```
- **TOP20包数统计**图表所关联的查询分析语句如下所示：
```
SELECT "srcaddr" as "源地址", "dstaddr" as "目的地址", sum("packets") as "包数", "resource_id" as "连接ID", "instance_id" as "实例ID" group by "instance_id", "resource_id", "srcaddr", "dstaddr" order by "包数" desc limit 20
```
- **TOP20流量统计**图表所关联的查询分析语句如下所示：
```
SELECT "srcaddr" as "源地址", "dstaddr" as "目的地址", sum("bytes") as "字节数", "resource_id" as "连接ID", "instance_id" as "实例ID" group by "instance_id", "resource_id", "srcaddr", "dstaddr" order by "字节数" desc limit 20
```
- **流日志条数**图表所关联的查询分析语句如下所示：
```
select time_series(__time, 'PT1H', 'yyyy-MM-dd HH:mm:ss', '0', '+08:00') as "时间", count(*) as "流日志条数" group by "时间" order by "时间"
```

- **流日志详情**图表所关联的查询分析语句如下所示：
```
SELECT "instance_id" as "实例ID", "resource_id" as "连接ID", "project_id" as "项目ID", "srcaddr" as "源IP", "dstaddr" as "目的IP", "srcport" as "源端口",  "dstport" as "目的端口", "protocol" as "协议类型", "direct" as "流量方向", "packets" as "包数", "bytes" as "字节数",
TIME_FORMAT( MILLIS_TO_TIMESTAMP("start"*1000), 'yyyy-MM-dd HH:mm:ss', '+08:00') as "开始时间", TIME_FORMAT( MILLIS_TO_TIMESTAMP("end"*1000) , 'yyyy-MM-dd HH:mm:ss', '+08:00') as "结束时间"
```

----结束

6.3.3.11 METRIC 仪表盘模板

用户在LTS页面只需按照业务需要创建指标规则即可生成自己的统计报表，设置单个日志过滤条件或通过添加关联关系和添加组设置多个日志过滤条件，保留符合条件的日志，对用户特定时间范围内已结构化的日志进行动态统计，并将统计结果动态呈现到aom的Prometheus实例，操作简单且功能强大。

前提条件

- 已创建日志生成指标，详情请参见**日志生成指标（邀测）**。
- 日志配置结构化，详情请参见**设置云端结构化解析日志**。

日志生成指标任务监控中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“METRIC仪表盘模板 > 日志生成指标任务监控中心”，查看图表详情。

- 过滤规则ID，所关联的查询分析语句如下所示：
```
select distinct(task_set)
```
- **输入行数**图表所关联的查询分析语句如下所示：
```
SELECT CASE  WHEN  "input" < 1000 THEN concat( cast( "input" AS VARCHAR ), '行' )  WHEN "input" < 1000 * 1000 THEN concat( cast( round( "input"/ 1000, 1 ) AS VARCHAR ), '千行' ) WHEN "input" < 1000000000 THEN concat( cast( round( "input"/ 1000000.0, 1 ) AS VARCHAR ), '百万行' ) WHEN "input"/ 1000.0 < 1000000000 THEN concat( cast( round( "input"/ 1000 / 1000000.0, 1 ) AS VARCHAR ), '十亿行' ) ELSE concat( cast( round( "input"/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), '万亿行' )  END AS  "total"  from (select sum("input") as "input")
```
- **输出行数**图表所关联的查询分析语句如下所示
```
SELECT CASE  WHEN  "output" < 1000 THEN concat( cast( "output" AS VARCHAR ), '行' )  WHEN "output" < 1000 * 1000 THEN concat( cast( round( "output"/ 1000, 1 ) AS VARCHAR ), '千行' ) WHEN "output" < 1000000000 THEN concat( cast( round( "output"/ 1000000.0, 1 ) AS VARCHAR ), '百万行' )  WHEN "output"/ 1000.0 < 1000000000 THEN concat( cast( round( "output"/ 1000 / 1000000.0, 1 ) AS VARCHAR ), '十亿行' ) ELSE concat( cast( round( "output"/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), '万亿行' )  END AS  "total"  from (select sum("output") as "output")
```
- **满足过滤条件行数**图表所关联的查询分析语句如下所示：
```
SELECT CASE  WHEN  "filters" < 1000 THEN concat( cast( "filters" AS VARCHAR ), '行' )  WHEN "filters" < 1000 * 1000 THEN concat( cast( round( "filters"/ 1000, 1 ) AS VARCHAR ), '千行' ) WHEN "filters" < 1000000000 THEN concat( cast( round( "filters"/ 1000000.0, 1 ) AS VARCHAR ), '百万行' ) WHEN "filters"/ 1000.0 < 1000000000 THEN concat( cast( round( "filters"/ 1000 / 1000000.0, 1 ) AS VARCHAR ), '十亿行' ) ELSE concat( cast( round( "filters"/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), '万亿行' )  END AS  "total"  from (select sum("filters") as "filters")
```
- **不满足过滤条件行数**图表所关联的查询分析语句如下所示：
```
SELECT CASE  WHEN  "filter_drops" < 1000 THEN concat( cast( "filter_drops" AS VARCHAR ), '行' ) WHEN "filter_drops" < 1000 * 1000 THEN concat( cast( round( "filter_drops"/ 1000, 1 ) AS VARCHAR ), '千行' ) WHEN "filter_drops" < 1000000000 THEN concat( cast( round( "filter_drops"/ 1000000.0, 1 ) AS VARCHAR ), '百万行' )  WHEN "filter_drops"/ 1000.0 < 1000000000 THEN concat( cast( round( "filter_drops"/ 1000 / 1000000.0, 1 ) AS VARCHAR ), '十亿行' ) ELSE concat( cast( round( "filter_drops"/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), '万亿行' )  END AS  "total"  from (select sum("filter_drops") as "filter_drops")
```


- **采样行数**图表所关联的查询分析语句如下所示：
```
SELECT CASE  WHEN  "samples" < 1000 THEN concat( cast( "samples" AS VARCHAR ), '行' )  WHEN "samples" < 1000 * 1000 THEN concat( cast( round( "samples"/ 1000, 1 ) AS VARCHAR ), '千行' ) WHEN "samples" < 1000000000 THEN concat( cast( round( "samples"/ 1000000.0, 1 ) AS VARCHAR ), '百万行' )  WHEN "samples"/ 1000.0 < 1000000000 THEN concat( cast( round( "samples"/ 1000 / 1000000.0, 1 ) AS VARCHAR ), '十亿行' ) ELSE concat( cast( round( "samples"/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), '万亿行' )  END AS "total"  from (select sum("samples") as "samples")
```
- **采样丢弃行数**图表所关联的查询分析语句如下所示：
```
SELECT CASE  WHEN  "sample_drops" < 1000 THEN concat( cast( "sample_drops" AS VARCHAR ), '行' )  WHEN "sample_drops" < 1000 * 1000 THEN concat( cast( round( "sample_drops"/ 1000, 1 ) AS VARCHAR ), '千行' ) WHEN "sample_drops" < 1000000000 THEN concat( cast( round( "sample_drops"/ 1000000.0, 1 ) AS VARCHAR ), '百万行' )  WHEN "sample_drops"/ 1000.0 < 1000000000 THEN concat( cast( round( "sample_drops"/ 1000 / 1000000.0, 1 ) AS VARCHAR ), '十亿行' ) ELSE concat( cast( round( "sample_drops"/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), '万亿行' )  END AS  "total"  from (select sum( "sample_drops" ) as "sample_drops")
```
- **超过日志时间范围行数**图表所关联的查询分析语句如下所示：
```
SELECT CASE  WHEN  "out_of_bounds" < 1000 THEN concat( cast( "out_of_bounds" AS VARCHAR ), '行' )  WHEN "out_of_bounds" < 1000 * 1000 THEN concat( cast( round( "out_of_bounds"/ 1000, 1 ) AS VARCHAR ), '千行' ) WHEN "out_of_bounds" < 1000000000 THEN concat( cast( round( "out_of_bounds"/ 1000000.0, 1 ) AS VARCHAR ), '百万行' )  WHEN "out_of_bounds"/ 1000.0 < 1000000000 THEN concat( cast( round( "out_of_bounds"/ 1000 / 1000000.0, 1 ) AS VARCHAR ), '十亿行' ) ELSE concat( cast( round( "out_of_bounds"/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), '万亿行' )  END AS  "total"  from (select sum("out_of_bounds") as "out_of_bounds")
```
- **执行记录**图表所关联的查询分析语句如下所示：
```
select TIME_FORMAT( "__time", 'yyyy-MM-dd HH:mm:ss:SSS', '+08:00') as "统计时间", sum("input") as "输入行数",sum("output") as "输出行数",sum("filters") as "满足过滤条件行数",sum("filter_drops") as "不满足过滤条件行数",sum("samples") as "采样行数",sum("sample_drops") as "采样丢弃行数",sum("out_of_bounds") as "超过日志时间范围行数" group by __time order by __time desc limit 1000
```

----结束

6.3.3.12 NGINX 仪表盘模板

日志服务支持采集NGINX日志，并进行多维度分析。云日志服务支持日志采集向导一站式采集NGINX日志，并为NGINX日志配置结构化和仪表盘。Nginx (engine x) 是一个高性能的HTTP和反向代理web服务器，同时也提供了IMAP/POP3/SMTP服务。

NGINX仪表盘模板支持**查看NGINX秒级监控**、**查看NGINX访问中心**和**查看NGINX监控中心**。

前提条件

日志配置结构化，详情请参见**设置云端结构化解析日志**。

查看 NGINX 秒级监控

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“NGINX仪表盘模板 > NGINX秒级监控”，查看图表详情。

- **QPS**图表所关联的查询分析语句如下所示：
```
SELECT TIME_FORMAT(TIME_CEIL(__time,'PT1S'),'yyyy-MM-dd HH:mm:ss','+08:00') AS _time_ , COUNT(*) as QPS from log group by _time_
```
- **成功率**图表所关联的查询分析语句如下所示：
```
select __time,round(CASE WHEN "成功率" > 0 THEN "成功率" else 0 end,2) as "成功率" from (select TIME_FORMAT(TIME_CEIL(__time,'PT5S'),'yyyy-MM-dd HH:mm:ss','+08:00') as __time, sum(case when status < 400 then 1 else 0 end) * 100.0 / count(1) as '成功率' from log group by __time)
```
- **延迟**图表所关联的查询分析语句如下所示：


```
select __time,round(CASE WHEN "访问延迟" > 0 THEN "访问延迟" else 0 end,2) as "访问延迟
",round(CASE WHEN "Upstream延迟" > 0 THEN "Upstream延迟" else 0 end,2) as "Upstream延迟"
from (select TIME_FORMAT(TIME_CEIL(__time,'PT5S'),'yyyy-MM-dd HH:mm:ss','+08:00') as __time,
avg(request_time)* 1000 as '访问延迟',avg(upstream_response_time)* 1000 as 'Upstream延迟' from
log group by __time)
```

- **流量**图表所关联的查询分析语句如下所示：

```
select TIME_FORMAT(TIME_CEIL(__time,'PT5S'),'yyyy-MM-dd HH:mm:ss','+08:00') as __time ,
sum("request_length") as "请求流量", sum("body_bytes_sent") as "返回body流量" group by __time
```

- **状态码**图表所关联的查询分析语句如下所示：

```
select t.t as "time",
    CASE WHEN a."2XX" IS NOT NULL THEN  CAST(a."2XX" AS BIGINT) ELSE 0 END as "2XX",
    CASE WHEN b."3XX" IS NOT NULL THEN  CAST(b."3XX" AS BIGINT) ELSE 0 END as "3XX",
    CASE WHEN c."4XX" IS NOT NULL THEN  CAST(c."4XX" AS BIGINT) ELSE 0 END as "4XX",
    CASE WHEN d."5XX" IS NOT NULL THEN  CAST(d."5XX" AS BIGINT) ELSE 0 END as "5XX",
    CASE WHEN e."其他" IS NOT NULL THEN  CAST(e."其他" AS BIGINT)  ELSE 0 END as "其他"
    from (select TIME_CEIL(__time,'PT5S') as t from log group by t order by t asc  ) t left join (select
TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "2XX" from log WHERE "status" >=
200 and "status" < 300 group by t order by t asc ) a on t.t =a.t left join (select
TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "3XX" from log WHERE "status" >=
300 and "status" < 400 group by t order by t asc) b on t.t =b.t left join (select
TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "4XX" from log WHERE "status" >=
400 and "status" < 500 group by t order by t asc) c on t.t =c.t left join (select
TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "5XX" from log WHERE "status" >=
500 and "status" < 600 group by t order by t asc) d on t.t =d.t left join (select
TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "其他" from log WHERE "status" <
200 or "status" >= 600 group by t order by t asc) e on t.t =e.t
```

- **后端响应码**图表所关联的查询分析语句如下所示：

```
select t.t as "time",
    CASE WHEN a."2XX" IS NOT NULL THEN  CAST(a."2XX" AS BIGINT) ELSE 0 END as "2XX",
    CASE WHEN b."3XX" IS NOT NULL THEN  CAST(b."3XX" AS BIGINT) ELSE 0 END as "3XX",
    CASE WHEN c."4XX" IS NOT NULL THEN  CAST(c."4XX" AS BIGINT) ELSE 0 END as "4XX",
    CASE WHEN d."5XX" IS NOT NULL THEN  CAST(d."5XX" AS BIGINT) ELSE 0 END as "5XX",
    CASE WHEN e."其他" IS NOT NULL THEN  CAST(e."其他" AS BIGINT)  ELSE 0 END as "其他"
    from (
    select TIME_CEIL(__time,'PT5S') as t from log group by t order by t asc
    ) t
    left join(
    select TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "2XX" from log WHERE
"upstream_status" >= 200 and "upstream_status" < 300 group by t order by t asc) a
    on t.t = a.t
    left join (
    select TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "3XX" from log WHERE
"upstream_status" >= 300 and "upstream_status" < 400 group by t order by t asc) b
    on t.t =b.t
    left join (
    select TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "4XX" from log WHERE
"upstream_status" >= 400 and "upstream_status" < 500 group by t order by t asc) c
    on t.t =c.t
    left join (
    select TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "5XX" from log WHERE
"upstream_status" >= 500 and "upstream_status" < 600 group by t order by t asc) d
    on t.t =d.t
    left join (
    select TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "其他" from log WHERE
"upstream_status" < 200 or "upstream_status" >= 600 group by t order by t asc) e
    on t.t =e.t
```

----结束

查看 NGINX 访问中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“NGINX仪表盘模板 > NGINX访问中心”，查看图表详情。

- **PV对比昨日**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100, 2) as inc from(select compare( "pv" , 86400) as diff from (select count(1) as "pv" from log))
```
- **PV对比上周**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100, 2) as inc from(select compare( "pv" , 604800) as diff from (select count(1) as "pv" from log))
```
- **UV对比昨日**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100, 2) as inc from(select compare( "uv" , 86400) as diff from (select APPROX_COUNT_DISTINCT(my_remote_addr) as "uv" from log))
```
- **UV对比上周**图表所关联的查询分析语句如下所示：
```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100, 2) as inc from(select compare( "uv" , 604800) as diff from (select APPROX_COUNT_DISTINCT(my_remote_addr) as "uv" from log))
```
- **访问量PV分布(中国)**图表所关联的查询分析语句如下所示：
```
select ip_to_province(remote_addr) as province, count(1) as pv where IP_TO_COUNTRY (remote_addr) = '中国'  group by province HAVING province not in ('','保留地址','*')
```
- **访问量PV分布(世界)**图表所关联的查询分析语句如下所示：
```
SELECT ip_to_country(remote_addr) as country,COUNT(1) as PV GROUP BY country HAVING country not in ('','保留地址','*')
```
- **访问量UV分布(中国)**图表所关联的查询分析语句如下所示：
```
select ip_to_province(remote_addr) as province, APPROX_COUNT_DISTINCT(remote_addr) as UV where IP_TO_COUNTRY (remote_addr) = '中国'  group by province HAVING province not in ('','保留地址','*')
```
- **访问量UV分布(世界)**图表所关联的查询分析语句如下所示：
```
select ip_to_country(remote_addr) as country, APPROX_COUNT_DISTINCT(remote_addr) as uv group by country HAVING country not in ('','保留地址','*')
```
- **平均时延分布（中国）**图表所关联的查询分析语句如下所示：
```
SELECT province,round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)"FROM (SELECT ip_to_province(remote_addr) as province,avg(request_time) * 1000 AS "平均延迟(ms)"WHERE  IP_TO_COUNTRY (remote_addr) = '中国'GROUP BY province HAVING province not in ('','保留地址','*'))
```
- **平均时延分布（世界）**图表所关联的查询分析语句如下所示：
```
SELECT country,round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 2 ) AS "平均延迟(ms)"FROM (SELECT ip_to_country(remote_addr) as country,avg(request_time) * 1000 AS "平均延迟(ms)" GROUP BY country HAVING country not in ('','保留地址','*'))
```
- **今日PV/UV**图表所关联的查询分析语句如下所示：
```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss', '+08:00' ) as _time_,PV,UV FROM (select TIME_CEIL(__time,'PT600S') AS _time_ , count(1) as PV, APPROX_COUNT_DISTINCT(my_remote_addr) as UV from log WHERE __time <= CURRENT_TIMESTAMP  and __time >= DATE_TRUNC( 'DAY',(CURRENT_TIMESTAMP + INTERVAL '8' HOUR)) - INTERVAL '8' HOUR group by _time_ order by _time_) WHERE _time_ <= CURRENT_TIMESTAMP LIMIT 100000 OFFSET 1
```
- **7日PV/UV**图表所关联的查询分析语句如下所示：
```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss', '+08:00' ) as _time_,PV,UV FROM (select TIME_CEIL(__time,'PT600S') AS _time_ , count(1) as PV,  APPROX_COUNT_DISTINCT(remote_addr) as UV from log WHERE __time <= CURRENT_TIMESTAMP  and __time >= DATE_TRUNC( 'DAY', (CURRENT_TIMESTAMP + INTERVAL '8' HOUR)) - INTERVAL '8' HOUR - INTERVAL '7' DAY group by _time_ order by _time_ ) WHERE _time_ <= CURRENT_TIMESTAMP LIMIT 100000 OFFSET 1
```
- **区域访问TOP10(省份)**图表所关联的查询分析语句如下所示：
```
select ip_to_province(remote_addr) as "province", count(1) as "访问次数" group by "province" HAVING "province" <> '-1' order by "访问次数" asc limit 10
```
- **区域访问TOP10(城市)**图表所关联的查询分析语句如下所示：
```
select ip_to_city(remote_addr) as "city", count(1) as "访问次数" group by "city" HAVING  "city" <> '-1' order by "访问次数" asc  limit 10
```
- **Host访问TOP10**图表所关联的查询分析语句如下所示：
```
select  host as "Host", count(1) as "PV" group by "Host" order by "PV" asc limit 10
```
- **UserAgent访问TOP10**图表所关联的查询分析语句如下所示：
```
select http_user_agent as "UserAgent", count(1) as "PV" group by "UserAgent" order by "PV" asc limit 10
```


- **设备占比(终端)**图表所关联的查询分析语句如下所示：
```
select case when regexp_like(lower(http_user_agent), 'iphone|ipod|android|ios') then '移动端' else 'PC端' end as type , count(1) as total group by  type
```
- **设备占比(系统)**图表所关联的查询分析语句如下所示：
```
select case when regexp_like(lower(http_user_agent), 'iphone|ipod|ios') then 'IOS' when regexp_like(lower(http_user_agent), 'android') then 'Android' else 'other' end as type , count(1) as total group by  type HAVING type != 'other'
```
- **TOP URL**图表所关联的查询分析语句如下所示：
```
select request_uri , count(1) as PV, APPROX_COUNT_DISTINCT(remote_addr) as UV, round(sum( case when status < 400 then 1 else 0 end ) * 100.0 / count(1), 2) as "访问成功率" group by request_uri ORDER by PV desc
```
- **TOP 访问IP**图表所关联的查询分析语句如下所示：
```
select remote_addr as "来源IP",ip_to_country(remote_addr) as "国家",ip_to_province(remote_addr) as "省份",ip_to_city(remote_addr) as "城市",ip_to_provider(remote_addr) as "运营商",count(1) as "PV",http_user_agent as "UserAgent采样",request_uri as "URL采样" group by remote_addr,http_user_agent,request_uri ORDER by "PV" desc
```

----结束

查看 NGINX 监控中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“NGINX仪表盘模板 > NGINX监控中心”，查看图表详情。

- **访问量PV**图表所关联的查询分析语句如下所示：
```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss', '+08:00' ) as _time_,PV FROM ( SELECT TIME_CEIL ( __time, 'PT300S' ) AS _time_, count( 1 ) AS PV FROM log GROUP BY _time_ )  WHERE _time_ <= CURRENT_TIMESTAMP LIMIT 100 OFFSET 1
```
- **请求成功率**图表所关联的查询分析语句如下所示：
```
select ROUND(sum(case when status < 400 then 1 else 0 end) * 100.0 / count(1),2) as cnt
```
- **平均延迟**图表所关联的查询分析语句如下所示：
```
select round(avg(request_time) * 1000, 3) as cnt
```
- **4XX请求数**图表所关联的查询分析语句如下所示：
```
SELECT COUNT(1) as cnt WHERE "status" >= 400 and "status" < 500
```
- **404请求数**图表所关联的查询分析语句如下所示：
```
SELECT COUNT(1) as cnt WHERE "status" = 404
```
- **429请求数**图表所关联的查询分析语句如下所示：
```
SELECT COUNT(1) as cnt WHERE "status" = 429
```
- **504请求数**图表所关联的查询分析语句如下所示：
```
SELECT COUNT(1) as cnt WHERE "status" = 504
```
- **5XX请求数**图表所关联的查询分析语句如下所示：
```
select TIME_FORMAT(TIME_CEIL(__time,'PT300S'),'yyyy-MM-dd HH:mm:ss','+08:00') AS _time_ , count(1) as cnt where "status" >= 500 group by _time_
```
- **状态码分布**图表所关联的查询分析语句如下所示：
```
SELECT status, COUNT(1) AS rm GROUP BY status
```
- **访问量UV**图表所关联的查询分析语句如下所示：
```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss', '+08:00' ) as _time_,UV FROM (select TIME_CEIL(__time,'PT600S') AS _time_ , APPROX_COUNT_DISTINCT(remote_addr) as UV  from log group by _time_) WHERE _time_ <= CURRENT_TIMESTAMP LIMIT 100000 OFFSET 1
```
- **流量**图表所关联的查询分析语句如下所示：
```
select TIME_FORMAT(_time_,'yyyy-MM-dd HH:mm:ss','+08:00') AS _time_,round( CASE WHEN "入流量" > 0 THEN "入流量" ELSE 0 END, 2 ) AS "入流量",round( CASE WHEN "出流量" > 0 THEN "出流量" ELSE 0 END, 2 ) AS "出流量" FROM (SELECT TIME_CEIL(__time,'PT600S') AS _time_,sum(request_length) / 1024.0 AS "入流量",sum(bytes_sent) / 1024.0 AS "出流量" group by _time_) WHERE _time_ <= CURRENT_TIMESTAMP LIMIT 100000 OFFSET 1
```


- **访问失败率**图表所关联的查询分析语句如下所示：

```
SELECT TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss', '+08:00' ) as _time_,round( CASE WHEN "失败率" > 0 THEN "失败率" ELSE 0 END, 2 ) AS "失败率",round( CASE WHEN "5XX比例" > 0 THEN "5XX比例" ELSE 0 END, 2 ) AS "5XX比例" from (select TIME_CEIL(__time,'PT600S') AS _time_,sum(case when status >= 400 then 1 else 0 end) * 100.0 / count(1) as '失败率' , sum(case when status >=500 THEN 1 ELSE 0 END)*100.0/COUNT(1) as '5XX比例' group by  _time_) WHERE _time_ <= CURRENT_TIMESTAMP LIMIT 100000 OFFSET 1
```

- **延迟**图表所关联的查询分析语句如下所示：

```
select TIME_FORMAT( _time_, 'yyyy-MM-dd HH:mm:ss', '+08:00' ) as _time_,round( CASE WHEN "平均" > 0 THEN "平均" ELSE 0 END, 2 ) AS "平均",round( CASE WHEN "P50" > 0 THEN "P50" ELSE 0 END, 2 ) AS "P50",round( CASE WHEN "P90" > 0 THEN "P90" ELSE 0 END, 2 ) AS "P90",round( CASE WHEN "P99" > 0 THEN "P99" ELSE 0 END, 2 ) AS "P99",round( CASE WHEN "P9999" > 0 THEN "P9999" ELSE 0 END, 2 ) AS "P9999" from (select TIME_CEIL(__time,'PT600S') as _time_,avg(request_time) * 1000 as "平均", APPROX_QUANTILE_DS("request_time", 0.50)*1000 as "P50", APPROX_QUANTILE_DS("request_time", 0.90)*1000 as "P90" ,APPROX_QUANTILE_DS("request_time", 0.99)*1000 as 'P99',APPROX_QUANTILE_DS("request_time", 0.9999)*1000 as 'P9999' group by  _time_) WHERE _time_ <= CURRENT_TIMESTAMP LIMIT 100000 OFFSET 1
```

- **Host请求TOP**图表所关联的查询分析语句如下所示：

```
SELECT "host", pv, uv, round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS "访问成功率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "入流量(KB)" > 0 THEN "入流量(KB)" ELSE 0 END, 3 ) AS "入流量(KB)", round( CASE WHEN "出流量(KB)" > 0 THEN "出流量(KB)" ELSE 0 END, 3 ) AS "出流量(KB)"  FROM ( SELECT "host", count( 1 ) AS pv, APPROX_COUNT_DISTINCT ( remote_addr ) AS uv, sum( CASE WHEN "status" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)", avg( request_time ) * 1000 AS "平均延迟(ms)", sum( request_length ) / 1024.0 AS "入流量(KB)", sum( bytes_sent ) / 1024.0 AS "出流量(KB)"  WHERE "host" != ''  GROUP BY "host" ) ORDER BY pv DESC
```

- **Host延迟TOP**图表所关联的查询分析语句如下所示：

```
SELECT "host", pv, round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS "访问成功率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90延迟(ms)", round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟(ms)" FROM ( SELECT "host", count( 1 ) AS pv, sum( CASE WHEN "status" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)", avg( request_time ) * 1000 AS "平均延迟(ms)",APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90延迟(ms)", APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99延迟(ms)" WHERE "host" != ''  GROUP BY "host" ) ORDER BY "平均延迟(ms)" desc
```

- **Host失败率TOP**图表所关联的查询分析语句如下所示：

```
SELECT "host", pv,round( CASE WHEN "访问失败率(%)" > 0 THEN "访问失败率(%)" ELSE 0 END, 2 ) AS "访问失败率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90延迟(ms)", round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟(ms)"  FROM ( SELECT "host", count( 1 ) AS pv, sum( CASE WHEN "status" >= 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问失败率(%)", avg( request_time ) * 1000 AS "平均延迟(ms)", APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90延迟(ms)", APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99延迟(ms)" WHERE "host" != ''  GROUP BY "host"  ) ORDER BY "访问失败率(%)" desc
```

- **URL请求TOP**图表所关联的查询分析语句如下所示：

```
SELECT request_uri, pv,uv, round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS "访问成功率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)", round( CASE WHEN "入流量(KB)" > 0 THEN "入流量(KB)" ELSE 0 END, 3 ) AS "入流量(KB)", round( CASE WHEN "出流量(KB)" > 0 THEN "出流量(KB)" ELSE 0 END, 3 ) AS "出流量(KB)"  FROM ( SELECT request_uri, count( 1 ) AS pv, APPROX_COUNT_DISTINCT ( remote_addr ) AS uv, sum( CASE WHEN "status" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)", avg( request_time ) * 1000 AS "平均延迟(ms)", sum( request_length ) / 1024.0 AS "入流量(KB)", sum( bytes_sent ) / 1024.0 AS "出流量(KB)"  WHERE "host" != ''  GROUP BY request_uri  ) ORDER BY pv desc
```

- **URL延迟TOP**图表所关联的查询分析语句如下所示：

```
SELECT request_uri, pv,round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS "访问成功率(%)",round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS "平均延迟(ms)",round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90延迟(ms)",round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟(ms)" FROM (SELECT request_uri, count( 1 ) AS pv, sum( CASE WHEN "status" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)", avg( request_time ) * 1000 AS "平均延迟
```



```
(ms)", APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90延迟(ms)",
APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99延迟(ms)" WHERE "host" != ''  GROUP BY
request_uri  ) ORDER BY "平均延迟(ms)" desc
```

- **URL失败率TOP**图表所关联的查询分析语句如下所示：

```
SELECT request_uri, pv, round( CASE WHEN "访问失败率(%)" > 0 THEN "访问失败率(%)" ELSE 0 END,
2 ) AS "访问失败率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END,
3 ) AS "平均延迟(ms)",round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 )
AS "P90延迟(ms)", round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS
"P99延迟(ms)" FROM( SELECT request_uri, count( 1 ) AS pv, sum( CASE WHEN "status" >= 400 THEN
1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问失败率(%)", avg( request_time ) * 1000 AS "平均延迟
(ms)", APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90延迟(ms)",
APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99延迟(ms)" WHERE "host" != '' GROUP BY
request_uri  )ORDER BY "访问失败率(%)" desc
```

- **后端请求TOP**图表所关联的查询分析语句如下所示：

```
SELECT addr, pv, uv, round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 )
AS "访问成功率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 )
AS "平均延迟(ms)", round( CASE WHEN "入流量(KB)" > 0 THEN "入流量(KB)" ELSE 0 END, 3 ) AS "入
流量(KB)", round( CASE WHEN "出流量(KB)" > 0 THEN "出流量(KB)" ELSE 0 END, 3 ) AS "出流量
(KB)"  FROM ( SELECT upstream_addr as addr, count( 1 ) AS pv, APPROX_COUNT_DISTINCT
( remote_addr ) AS uv, sum( CASE WHEN "status" < 400 THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS
"访问成功率(%)", avg( request_time ) * 1000 AS "平均延迟(ms)", sum( request_length ) / 1024.0 AS
"入流量(KB)", sum( bytes_sent ) / 1024.0 AS "出流量(KB)"  WHERE "host" != ''  GROUP BY addr
having length(upstream_addr) > 2) ORDER BY "pv" desc
```

- **后端延迟TOP**图表所关联的查询分析语句如下所示：

```
SELECT addr,pv,round( CASE WHEN "访问成功率(%)" > 0 THEN "访问成功率(%)" ELSE 0 END, 2 ) AS
"访问成功率(%)",round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS
"平均延迟(ms)",round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90
延迟(ms)",round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟
(ms)" FROM (SELECT upstream_addr as addr,count( 1 ) AS pv,sum( CASE WHEN "status" < 400 THEN
1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问成功率(%)",avg( request_time ) * 1000 AS "平均延迟
(ms)",APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90延迟
(ms)",APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99延迟(ms)" WHERE "host" != ''
GROUP BY addr having length(upstream_addr) > 2) ORDER BY "平均延迟(ms)" desc
```

- **后端失败率TOP**图表所关联的查询分析语句如下所示：

```
SELECT addr, pv, round( CASE WHEN "访问失败率(%)" > 0 THEN "访问失败率(%)" ELSE 0 END, 2 ) AS
"访问失败率(%)", round( CASE WHEN "平均延迟(ms)" > 0 THEN "平均延迟(ms)" ELSE 0 END, 3 ) AS
"平均延迟(ms)", round( CASE WHEN "P90延迟(ms)" > 0 THEN "P90延迟(ms)" ELSE 0 END, 3 ) AS "P90
延迟(ms)", round( CASE WHEN "P99延迟(ms)" > 0 THEN "P99延迟(ms)" ELSE 0 END, 3 ) AS "P99延迟
(ms)"  FROM ( SELECT upstream_addr as addr, count( 1 ) AS pv, sum( CASE WHEN "status" >= 400
THEN 1 ELSE 0 END ) * 100.0 / count( 1 ) AS "访问失败率(%)", avg( request_time ) * 1000 AS "平均延
迟(ms)", APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90延迟(ms)",
APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99延迟(ms)" WHERE "host" != ''  GROUP BY
addr having length(upstream_addr) > 2)ORDER BY "访问失败率(%)" desc
```

----结束

6.3.3.13 VPC 仪表盘模板

虚拟私有云（Virtual Private Cloud，VPC）是隔离的、私密的虚拟网络环境。用户可以自由配置VPC内的IP地址段、子网、安全组等子服务，也可以申请弹性带宽和弹性公网IP搭建业务系统。 VPC日志流中记录了虚拟私有云中的流量信息，可以帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。

云日志服务支持日志采集向导一站式采集VPC日志，并为VPC日志配置结构化和仪表盘。该仪表盘主要展示VPC日志的Action总次数，ACCEPT总字节数、ACCEPT总包数、REJECT总字节数、REJECT总包数、源地址的Action次数分布、总分钟Action次数、Action分布、流日志记录状态分布、Action次数的源地址运行商分布、Top5字节数的源地址、Top5字节数的目标地址、Top5包数的目标端口、各协议的每分钟包数、弹性网卡。

前提条件

- 已采集VPC日志，详情请参见**虚拟私有云VPC接入LTS**。
- 日志配置结构化，详情请参见**设置云端结构化解析日志**。

查看 VPC 流日志

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 在“日志应用”模块中，单击“VPC日志流中心”，选择“进入仪表盘”。

步骤3 在仪表盘模板下方，选择“VPC仪表盘模板 > VPC流日志”，查看图表详情。

- **Action总次数**图表所关联的查询分析语句如下所示：

```
select CASE WHEN total_actions < 1000 THEN concat(cast( total_actions AS VARCHAR), '次') WHEN total_actions < 1000 * 1000 THEN concat(cast(round(total_actions / 1000.0, 2) AS VARCHAR),'千次') WHEN total_actions < 1000000000 THEN concat(cast(round(total_actions / 1000000.0, 2) AS VARCHAR),'百万次') WHEN total_actions / 1000.0 < 1000000000 THEN concat(cast(round(total_actions / 1000 / 1000000.0, 1) AS VARCHAR),'十亿次') ELSE concat(cast(round(total_actions / 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR),'万亿次') END AS "total_actions" from (select count(1) as total_actions where log_status='OK' and version=1)
```

- **ACCEPT总字节数**图表所关联的查询分析语句如下所示：

```
select CASE WHEN accept_bytes < 1024 THEN concat(cast( accept_bytes AS VARCHAR), 'B') WHEN accept_bytes < 1024 * 1024 THEN concat(cast(round(accept_bytes / 1024, 2) AS VARCHAR),'KB') WHEN accept_bytes < 1000000000 THEN concat(cast(round(accept_bytes /1024.0 /1024, 2) AS VARCHAR),'MB') WHEN accept_bytes / 1000.0 < 1000000000 THEN concat(cast(round(accept_bytes / 1024 / 1000000.0, 2) AS VARCHAR),'GB') ELSE concat(cast(round(accept_bytes / 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR),'TB') END AS "accept_bytes" from (select sum(bytes) as accept_bytes where log_status='OK' and version=1 and action='ACCEPT')
```

- **ACCEPT总包数**图表所关联的查询分析语句如下所示：

```
select CASE WHEN accept_packets < 1024 THEN concat(cast( accept_packets AS VARCHAR), 'B') WHEN accept_packets < 1024 * 1024 THEN concat(cast(round(accept_packets / 1024, 2) AS VARCHAR),'KB') WHEN accept_packets < 1000000000 THEN concat(cast(round(accept_packets / 1024.0 /1024, 2) AS VARCHAR),'MB') WHEN accept_packets / 1000.0 < 1000000000 THEN concat(cast(round(accept_packets / 1024 / 1000000.0, 2) AS VARCHAR),'GB') ELSE concat(cast(round(accept_packets / 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR),'TB') END AS "accept_packets" from (select sum(packets) as accept_packets where log_status='OK' and version=1 and action='ACCEPT')
```

- **REJECT总字节数**图表所关联的查询分析语句如下所示：

```
select CASE WHEN reject_bytes < 1024 THEN concat(cast( reject_bytes AS VARCHAR), 'B') WHEN reject_bytes < 1024 * 1024 THEN concat(cast(round(reject_bytes / 1024, 2) AS VARCHAR),'KB') WHEN reject_bytes < 1000000000 THEN concat(cast(round(reject_bytes /1024.0 /1024, 2) AS VARCHAR),'MB') WHEN reject_bytes / 1000.0 < 1000000000 THEN concat(cast(round(reject_bytes / 1024 / 1000000.0, 2) AS VARCHAR),'GB') ELSE concat(cast(round(reject_bytes / 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR),'TB') END AS "reject_bytes" from (select sum(bytes) as reject_bytes where log_status='OK' and version=1 and action='REJECT')
```

- **REJECT总包数**图表所关联的查询分析语句如下所示：

```
select CASE WHEN reject_packets < 1024 THEN concat(cast( reject_packets AS VARCHAR), 'B') WHEN reject_packets < 1024 * 1024 THEN concat(cast(round(reject_packets / 1024, 2) AS VARCHAR),'KB') WHEN reject_packets < 1000000000 THEN concat(cast(round(reject_packets /1024.0 /1024, 2) AS VARCHAR),'MB') WHEN reject_packets / 1000.0 < 1000000000 THEN concat(cast(round(reject_packets / 1024 / 1000000.0, 2) AS VARCHAR),'GB') ELSE concat(cast(round(reject_packets / 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR),'TB') END AS "reject_packets" from (select sum(packets) as reject_packets where log_status='OK' and version=1 and action='REJECT')
```

- **源地址的Action次数分布**图表所关联的查询分析语句如下所示：

```
select IP_TO_PROVINCE(srcaddr) as province, count(1) as total_actions where IP_TO_COUNTRY(srcaddr) = '中国'  group by province HAVING province not in ('','保留地址','*')
```

- **每分钟Action次数**图表所关联的查询分析语句如下所示：

```
select TIME_FORMAT(date_trunc('minute', MILLIS_TO_TIMESTAMP("start" * 1000)),'MM-dd HH:mm') as "t", "action", count(1) as "total_actions" where log_status='OK' and version=1 group by "t", "action" order by t asc limit 1000
```

- **Action分布**图表所关联的查询分析语句如下所示：
  ```
  select action, count(1) as total_actions where log_status='OK' and version=1 group by action
  ```
- **流日志记录状态分布**图表所关联的查询分析语句如下所示：
  ```
  select log_status, count(1) as total_actions where version=1 group by log_status
  ```
- **Action次数的源地址运营商分布**图表所关联的查询分析语句如下所示：
  ```
  select ip_to_provider(srcaddr) as src_addr_provider, count(1) as total_actions where log_status='OK' and version=1 group by src_addr_provider order by total_actions desc limit 5
  ```
- **Top5字节数的源地址**图表所关联的查询分析语句如下所示：
  ```
  select ip_to_provider(srcaddr) as src_addr_provider, count(1) as total_actions where log_status='OK' and version=1 group by src_addr_provider order by total_actions desc limit 5
  ```
- **Top5字节数的目标地址**图表所关联的查询分析语句如下所示：
  ```
  select dstaddr, sum(bytes) as total_bytes where log_status='OK' and version=1 group by dstaddr order by total_bytes desc limit 5
  ```
- **Top5包数的目标端口**图表所关联的查询分析语句如下所示：
  ```
  select dstport, sum(packets) as total_packets where log_status='OK' and version=1 group by dstport order by total_packets desc limit 5
  ```
- **各协议的每分钟包数**图表所关联的查询分析语句如下所示：
  ```
  select TIME_FORMAT(date_trunc('minute', MILLIS_TO_TIMESTAMP("start" * 1000)),'MM-dd HH:mm') as t, protocol, sum(packets) as total_packets where log_status='OK' and version=1 group by t, protocol order by t asc limit 1000
  ```
- **弹性网卡**图表所关联的查询分析语句如下所示：
  ```
  select interface_id as "ID", sum(packets) as '数据包总数量', sum(bytes) as '数据包总大小' where log_status='OK' and version=1 group by "ID"
  ```

----结束

6.3.3.14 WAF 仪表盘模板

Web应用防火墙（Web Application Firewall， WAF），通过对HTTP(S)请求进行检测，识别并阻断SQL注入、跨站脚本攻击、网页木马上传、命令/代码注入、文件包含、敏感文件访问、第三方应用漏洞攻击、CC攻击、恶意爬虫扫描、跨站请求伪造等攻击，保护Web服务安全稳定。

使用**日志搜索与分析**时，对应的WAF仪表盘模板支持**查看WAF安全日志中心**和**查看WAF访问日志中心**。

前提条件

- 已采集WAF日志，详情请参考**Web应用防火墙WAF接入LTS**。
- 日志配置结构化，详情请参见**设置云端结构化解析日志**。

查看 WAF 安全日志中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“WAF仪表盘模板 > WAF安全日志中心”，查看图表详情。

- **被攻击网站**图表所关联的查询分析语句如下所示：
  ```
  SELECT diff [ 1 ] AS  "VALUE", COALESCE ( diff [ 1 ]- diff [ 2 ], 0 ) AS "BEFORE" FROM
      (
      SELECT
      compare ( "DATA", 86400 ) AS diff
      FROM
      ( SELECT count( DISTINCT "host" ) AS "DATA" FROM log
      WHERE action != ''
      ))
  ```
- **攻击来源国家**图表所关联的查询分析语句如下所示：


```
SELECT
    diff [ 1 ] AS
    "VALUE"
    ,
    COALESCE ( diff [ 1 ]- diff [ 2 ], 0 ) AS "BEFORE"
    FROM
    (
    SELECT
    compare ( "DATA", 86400 ) AS diff
    FROM
    ( SELECT count( DISTINCT ip_to_country ( CASE WHEN sip = '-' THEN remote_ip ELSE sip END) )
AS "DATA" FROM log
    WHERE action != ''
    )
    )
```

- **Web攻击拦截**图表所关联的查询分析语句如下所示：

```
SELECT
    CASE

    WHEN
    diff [ 1 ] < 1000 THEN
    concat( cast( diff [ 1 ] AS VARCHAR ), ' 次' )
    WHEN diff [ 1 ] < 1000 * 1000 THEN
    concat( cast( round( diff [ 1 ]/ 1000, 1 ) AS VARCHAR ), ' 千次' )
    WHEN diff [ 1 ] < 1000000000 THEN
    concat( cast( round( diff [ 1 ]/ 1000000.0, 1 ) AS VARCHAR ), ' 百万次' )
    WHEN diff [ 1 ]/ 1000.0 < 1000000000 THEN
    concat( cast( round( diff [ 1 ]/ 1000.0 / 1000000, 1 ) AS VARCHAR ), ' 十亿次' ) ELSE
concat( cast( round( diff [ 1 ]/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), ' 万亿次' )
    END AS
    "value"
    ,
    CASE WHEN diff [ 2 ]= 0 THEN 0 ELSE round( diff [ 3 ]- 1, 2 ) END AS ratio
    FROM
    ( SELECT compare ( "data", 86400 ) AS diff FROM ( SELECT count( 1 ) AS "data" FROM log
WHERE action = '' ) )
```

- **CC攻击拦截**图表所关联的查询分析语句如下所示：

```
SELECT
    CASE

    WHEN
    diff [ 1 ] < 1000 THEN
    concat( cast( diff [ 1 ] AS VARCHAR ), ' 次' )
    WHEN diff [ 1 ] < 1000 * 1000 THEN
    concat( cast( round( diff [ 1 ]/ 1000, 1 ) AS VARCHAR ), ' 千次' )
    WHEN diff [ 1 ] < 1000000000 THEN
    concat( cast( round( diff [ 1 ]/ 1000000.0, 1 ) AS VARCHAR ), ' 百万次' )
    WHEN diff [ 1 ]/ 1000.0 < 1000000000 THEN
    concat( cast( round( diff [ 1 ]/ 1000.0 / 1000000, 1 ) AS VARCHAR ), ' 十亿次' ) ELSE
concat( cast( round( diff [ 1 ]/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), ' 万亿次' )
    END AS
    "value"
    ,
    CASE WHEN diff [ 2 ]= 0 THEN 0 ELSE round( diff [ 3 ]- 1, 2 ) END AS ratio
    FROM
    ( SELECT compare ( "data", 86400 ) AS diff FROM ( SELECT count( 1 ) AS "data" FROM log
WHERE attack != 'default') )
```

- **攻击者UV**图表所关联的查询分析语句如下所示：

```
SELECT
    CASE
    WHEN
    diff [ 1 ] < 1000 THEN
    concat( cast( cast ( diff [ 1 ] AS INTEGER ) AS VARCHAR ), ' 个' )
    WHEN diff [ 1 ] < 1000 * 1000 THEN
    concat( cast( round( diff [ 1 ]/ 1000, 1 ) AS VARCHAR ), ' 千个' )
    WHEN diff [ 1 ] < 1000000000 THEN
    concat( cast( round( diff [ 1 ]/ 1000000.0, 1 ) AS VARCHAR ), ' 百万个' )
```

```
    WHEN diff [ 1 ]/ 1000.0 < 1000000000 THEN
    concat( cast( round( diff [ 1 ]/ 1000.0 / 1000000, 1 ) AS VARCHAR ), ' 十亿' ) ELSE
concat( cast( round( diff [ 1 ]/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), ' 万亿' )
    END AS "value",
    CASE WHEN diff [ 2 ]= 0 THEN 0 ELSE round( diff [ 3 ]- 1, 2 ) END AS ratio
    FROM
    (
    SELECT
    compare ( "data", 86400 ) AS diff
    FROM
    ( SELECT count( DISTINCT CASE WHEN sip = '-' THEN remote_ip ELSE sip END ) AS "data"
    FROM log
    ))
```

- **攻击拦截**图表所关联的查询分析语句如下所示：

```
SELECT
    CASE
    WHEN
    diff [ 1 ] < 1000 THEN
    concat( cast( diff [ 1 ] AS VARCHAR ), ' 次' )
    WHEN diff [ 1 ] < 1000 * 1000 THEN
    concat( cast( round( diff [ 1 ]/ 1000, 1 ) AS VARCHAR ), ' 千次' )
    WHEN diff [ 1 ] < 1000000000 THEN
    concat( cast( round( diff [ 1 ]/ 1000000.0, 1 ) AS VARCHAR ), ' 百万次' )
    WHEN diff [ 1 ]/ 1000.0 < 1000000000 THEN
    concat( cast( round( diff [ 1 ]/ 1000.0 / 1000000, 1 ) AS VARCHAR ), ' 十亿次' ) ELSE
concat( cast( round( diff [ 1 ]/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), ' 万亿次' )
    END AS
    "value",
    CASE WHEN diff [ 2 ]= 0 THEN 0 ELSE round( diff [ 3 ]- 1, 2 ) END AS "ratio"
    FROM
    (
    SELECT
    compare ( "data", 86400 ) AS diff
    FROM
    ( SELECT count( 1 ) AS "data" FROM log WHERE action != '')
    )
```

- **CC攻击**图表所关联的查询分析语如下所示：

```
SELECT
    ip_to_province (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS province,
    count( 1 ) AS "攻击次数"
    WHERE attack != 'default' and ip_to_country(CASE WHEN sip = '-' THEN remote_ip ELSE sip END)
= '中国'
    GROUP BY
    province
```

- **攻击类型分布**图表所关联的查询分析语句如下所示：

```
SELECT time_format( MILLIS_TO_TIMESTAMP( TIMESTAMP_TO_MILLIS(__time) -
MOD(TIMESTAMP_TO_MILLIS(__time), 3600)), 'HH:mm' ) AS dt, count( 1 ) AS cnt, CASE WHEN
action = 'block' THEN '拦截'  WHEN action = 'log' THEN '仅记录'  WHEN action = 'captcha' THEN '人机
验证' END AS attack FROM log WHERE action != '' GROUP BY TIMESTAMP_TO_MILLIS(__time) -
MOD(TIMESTAMP_TO_MILLIS(__time), 3600), attack ORDER BY cnt DESC
```

- **Web攻击**图表所关联的查询分析语句如下所示：

```
SELECT
    ip_to_province (
    CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS province,
    count( 1 ) AS "攻击次数"
    WHERE action = 'block' and ip_to_country(CASE WHEN sip = '-' THEN remote_ip ELSE sip END) =
'中国'
    GROUP BY
    province
```

- **CC攻击(世界)**图表所关联的查询分析语句如下所示：

```
SELECT
    ip_to_country (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS country,
    count( 1 ) AS "攻击次数"
    WHERE attack != 'default'
    GROUP BY
    country
```


- **Web攻击(世界)**图表所关联的查询分析语句如下所示：

```
SELECT
    ip_to_country (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS country,
    count( 1 ) AS "攻击次数"
    WHERE action = 'block'
    GROUP BY
    country
```

----结束

查看 WAF 访问日志中心

步骤1 登录云日志服务控制台，在左侧导航栏中选择“仪表盘 ”。

步骤2 在仪表盘模板下方，选择“WAF仪表盘模板 > WAF访问日志中心”，查看图表详情。

- **PV**图表所关联的查询分析语句如下所示：

```
SELECT CASE WHEN diff [ 1 ] < 1000 THEN concat( cast( diff [ 1 ] AS VARCHAR ), ' 次' ) WHEN diff [ 1 ] < 1000 * 1000 THEN concat( cast( round( diff [ 1 ]/ 1000, 1 ) AS VARCHAR ), ' 千次' ) WHEN diff [ 1 ] < 1000000000 THEN concat( cast( round( diff [ 1 ]/ 1000000.0, 1 ) AS VARCHAR ), ' 百万次' ) WHEN diff [ 1 ]/ 1000.0 < 1000000000 THEN concat( cast( round( diff [ 1 ]/ 1000 / 1000000.0, 1 ) AS VARCHAR ), ' 十亿次' ) ELSE concat( cast( round( diff [ 1 ]/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), ' 万亿次' ) END AS "VALUE" , CASE WHEN diff [ 2 ]= 0 THEN 0 ELSE round( diff [ 3 ]- 1, 2 ) END AS ratio FROM ( SELECT compare ( DATA, 86400 ) AS diff FROM ( SELECT count( 1 ) AS DATA FROM log ) )
```

- **UV**图表所关联的查询分析语句如下所示：

```
SELECT CASE WHEN diff [ 1 ] < 1000 THEN concat( cast( diff [ 1 ] AS VARCHAR ), ' 次' ) WHEN diff [ 1 ] < 1000 * 1000 THEN concat( cast( round( diff [ 1 ]/ 1000, 1 ) AS VARCHAR ), ' 千次' ) WHEN diff [ 1 ] < 1000000000 THEN concat( cast( round( diff [ 1 ]/ 1000000.0, 1 ) AS VARCHAR ), ' 百万次' ) WHEN diff [ 1 ]/ 1000.0 < 1000000000 THEN concat( cast( round( diff [ 1 ]/ 1000 / 1000000.0, 1 ) AS VARCHAR ), ' 十亿次' ) ELSE concat( cast( round( diff [ 1 ]/ 1000.0 / 1000 / 1000 / 1000, 1 ) AS VARCHAR ), ' 万亿次' ) END AS "VALUE" , CASE WHEN diff [ 2 ]= 0 THEN 0 ELSE round( diff [ 3 ]- 1, 2 ) END AS ratio FROM ( SELECT compare ( DATA, 86400 ) AS diff FROM ( SELECT count( DISTINCT CASE WHEN sip = '-' THEN remote_ip ELSE sip END ) AS "DATA" FROM log ) )
```

- **流入流量**图表所关联的查询分析语句如下所示：

```
SELECT CASE WHEN diff [ 1 ] < 102 THEN concat( cast( diff [ 1 ] AS VARCHAR ), ' B' ) WHEN diff [ 1 ] < 1024 * 1024 THEN concat( cast( round( diff [ 1 ]/ 1024, 1 ) AS VARCHAR ), ' KB' ) WHEN diff [ 1 ] < 1024 * 1024 * 1024 THEN concat( cast( round( diff [ 1 ]/ 1024.0 / 1024, 1 ) AS VARCHAR ), ' MB' ) WHEN diff [ 1 ]/ 1024.0 < 1024 * 1024 * 1024 THEN concat( cast( round( diff [ 1 ]/ 1024.0 / 1024 / 1024, 1 ) AS VARCHAR ), ' GB' ) ELSE concat( cast( round( diff [ 1 ]/ 1024.0 / 1024 / 1024 / 1024, 1 ) AS VARCHAR ), ' TB' ) END AS "VALUE" , CASE WHEN diff [ 2 ]= 0 THEN 0 ELSE round( diff [ 3 ]- 1, 2 ) END AS ratio FROM ( SELECT compare ( "DATA", 86400 ) AS diff FROM ( SELECT COALESCE ( sum( request_length ), 0 ) AS "DATA" FROM log ) )
```

- **网络in带宽峰值**图表所关联的查询分析语句如下所示：

```
SELECT CASE WHEN diff [ 1 ] < 102 THEN concat( cast( round( diff [ 1 ], 2 ) AS VARCHAR ), ' B/s' ) WHEN diff [ 1 ] < 1024 * 1024 THEN concat( cast( round( diff [ 1 ]/ 1024, 1 ) AS VARCHAR ), ' KB/s' ) WHEN diff [ 1 ] < 1024 * 1024 * 1024 THEN concat( cast( round( diff [ 1 ]/ 1024.0 / 1024, 1 ) AS VARCHAR ), ' MB/s' ) WHEN diff [ 1 ]/ 1024.0 < 1024 * 1024 * 1024 THEN concat( cast( round( diff [ 1 ]/ 1024.0 / 1024 / 1024, 1 ) AS VARCHAR ), ' GB/s' ) ELSE concat( cast( round( diff [ 1 ]/ 1024.0 / 1024 / 1024 / 1024, 1 ) AS VARCHAR ), ' TB/s' ) END AS "VALUE" , CASE WHEN diff [ 2 ]= 0 THEN 0 ELSE round( diff [ 3 ]- 1, 2 ) END AS ratio FROM ( SELECT compare ( "DATA", 86400 ) AS diff FROM ( SELECT COALESCE ( max( "DATA" ), 0 ) AS "DATA" FROM ( SELECT TIME_FLOOR(__time,'PT1M') AS dt, sum( request_length )/ 60.0 AS "DATA" FROM log GROUP BY dt LIMIT 10000 )) )
```

- **网络out带宽峰值**图表所关联的查询分析语句如下所示：

```
SELECT CASE WHEN diff [ 1 ] < 102 THEN concat( cast( round( diff [ 1 ], 2 ) AS VARCHAR ), ' B/s' ) WHEN diff [ 1 ] < 1024 * 1024 THEN concat( cast( round( diff [ 1 ]/ 1024, 1 ) AS VARCHAR ), ' KB/s' ) WHEN diff [ 1 ] < 1024 * 1024 * 1024 THEN concat( cast( round( diff [ 1 ]/ 1024.0 / 1024, 1 ) AS VARCHAR ), ' MB/s' ) WHEN diff [ 1 ]/ 1024.0 < 1024 * 1024 * 1024 THEN concat( cast( round( diff
```



```
[ 1 ]/ 1024.0 / 1024 / 1024, 1 ) AS VARCHAR ), ' GB/s' ) ELSE concat( cast( round( diff [ 1 ]/ 1024.0 / 1024 / 1024 / 1024, 1 ) AS VARCHAR ), ' TB/s' ) END AS "value", case when diff [ 2 ]= 0 then 0 else round( diff [ 3 ]- 1, 2 ) END AS "ratio" FROM ( SELECT compare ( "DATA", 86400 ) AS diff FROM ( SELECT COALESCE ( max( bytes_out ), 0 ) AS "DATA" FROM ( SELECT time_ceil( __time,'PT1M') AS dt, sum( body_bytes_sent )/ 60.0 AS bytes_out FROM log GROUP BY dt LIMIT 10000 )))
```

- **流量带宽趋势**图表所关联的查询分析语句如下所示：

```
SELECT TIME_FORMAT( MILLIS_TO_TIMESTAMP( TIMESTAMP_TO_MILLIS(__time) - MOD(TIMESTAMP_TO_MILLIS(__time) , 600000)), 'HH:mm' ) AS dt,
round( sum( request_length )/ 1024.0 / 600, 2 ) AS "流入流量(KB/s)",
round( sum( body_bytes_sent )/ 1024.0 / 600, 2 ) AS "流出流量(KB/s)" where request_length is not null GROUP BY TIMESTAMP_TO_MILLIS(__time) - MOD(TIMESTAMP_TO_MILLIS(__time) , 600000) ORDER BY dt LIMIT 1000
```

- **PV/UV趋势**图表所关联的查询分析语句如下所示：

```
SELECT TIME_FORMAT(MILLIS_TO_TIMESTAMP( TIMESTAMP_TO_MILLIS(__time) - MOD(TIMESTAMP_TO_MILLIS(__time) , 3600000)) , 'HH:mm' ) AS dt, count( 1 ) AS PV, APPROX_COUNT_DISTINCT (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS UV FROM log GROUP BY TIMESTAMP_TO_MILLIS(__time) - MOD(TIMESTAMP_TO_MILLIS(__time) , 3600000) ORDER BY dt LIMIT 1000
```

- **访问状态分布**图表所关联的查询分析语句如下所示：

```
SELECT TIME_FORMAT(MILLIS_TO_TIMESTAMP( TIMESTAMP_TO_MILLIS(__time) - MOD(TIMESTAMP_TO_MILLIS(__time) , 3600000)) , 'HH:mm' ) AS dt, count( 1 ) AS cnt, concat( cast( "response_code" / 100 AS VARCHAR ), 'XX' ) AS "status" GROUP BY TIMESTAMP_TO_MILLIS(__time) - MOD(TIMESTAMP_TO_MILLIS(__time) , 3600000) , "response_code" / 100 ORDER BY dt DESC LIMIT 10000
```

- **访问来源**图表所关联的查询分析语句如下所示：

```
SELECT ip_to_province (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS country, count( 1 ) AS "访问次数" where ip_to_country(CASE WHEN sip = '-' THEN remote_ip ELSE sip END) = '中国' GROUP BY country
```

- **流入流量来源（中国）**图表所关联的查询分析语句如下所示：

```
SELECT ip_to_province (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS region, round( sum( request_length )/ 1024.0 / 1024, 4 ) AS "流入流量(MB)" where ip_to_country(CASE WHEN sip = '-' THEN remote_ip ELSE sip END) = '中国' GROUP BY region
```

- **流入流量来源（世界）**图表所关联的查询分析语句如下所示：

```
SELECT ip_to_country (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS region, round( sum( request_length )/ 1024.0 / 1024, 4 ) AS "流入流量(MB)" where request_length is not null GROUP BY region
```

- **来源网络提供商**图表所关联的查询分析语句如下所示：

```
SELECT ip_to_provider (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS provider, round( sum( request_length )/ 1024.0 / 1024.0, 3 ) AS mb_in GROUP BY provider HAVING ip_to_provider (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) != '*' ORDER BY mb_in DESC LIMIT 10
```

- **访问域名**图表所关联的查询分析语句如下所示：

```
SELECT http_host, count( 1 ) AS "被访问次数" GROUP BY http_host ORDER BY "被访问次数" DESC LIMIT 30
```

- **响应最慢的URL**图表所关联的查询分析语句如下所示：

```
SELECT http_host AS "网站",url_extract_path (COALESCE ( url, '/' )) AS URL,sum( request_time )/ count( 1 ) AS "响应时间(毫秒)",count( 1 ) AS "访问次数" GROUP BY http_host, url ORDER BY "响应时间(毫秒)" DESC LIMIT 100
```

- **访问最多的客户端**图表所关联的查询分析语句如下所示：

```
SELECT ip AS "客户端", client AS "地理网络", concat( cast( (CASE WHEN pv IS NULL THEN 0 ELSE pv END) AS VARCHAR ), ' (', cast( case when head_pv = 'null' then 0 else (case when head_pv > 0 then head_pv else 0 end) end AS VARCHAR ), '/', cast( case when get_pv = 'null' then 0 else (case when get_pv > 0 then get_pv else 0 end) end AS VARCHAR ), '/', cast( case when put_pv = 'null' then 0 else (case when put_pv > 0 then put_pv else 0 end) end AS VARCHAR ), '/', cast( case when post_pv = 'null' then 0 else (case when post_pv > 0 then post_pv else 0 end) end AS VARCHAR ), '/', cast( case when delete_pv = 'null' then 0 else (case when delete_pv > 0 then delete_pv else 0 end) end AS VARCHAR ), '/', ')' ) AS "PV (Head, Get, Put, Post, Delete方法)", error_count AS "错误访问次数" FROM ( SELECT ip, client, sum( CASE WHEN "method" = 'PUT' AND "status" < 400 THEN pv ELSE 0 END ) AS put_pv, sum( CASE WHEN "method" = 'GET' AND "status" < 400 THEN pv ELSE 0 END ) AS get_pv, sum( CASE WHEN "method" = 'POST' AND "status" < 400 THEN pv ELSE 0 END ) AS post_pv, sum( CASE WHEN "method" = 'DELETE' AND "status" < 400 THEN pv ELSE 0 END ) AS delete_pv, sum( CASE WHEN "method" = 'HEAD' AND "status" < 400 THEN pv ELSE 0 END ) AS
```



```
head_pv,  sum( throughput ) AS throughput,  sum( pv ) AS pv,  sum( CASE WHEN "status" < 400
THEN 1 ELSE 0 END ) AS error_count   FROM  (  SELECT  CASE    WHEN  sip = '-' THEN  remote_ip
ELSE sip   END AS ip,  "method",  CASE    WHEN ip_to_country ( CASE WHEN sip = '-' THEN
remote_ip ELSE sip END )= '上海' THEN  '中国上海'   WHEN ip_to_province ( CASE WHEN sip = '-'
THEN remote_ip ELSE sip END )= '*' THEN  '未知IP'   WHEN ip_to_provider ( CASE WHEN sip = '-'
THEN remote_ip ELSE sip END )= '内网IP' THEN  '内网IP' ELSE concat(  ip_to_country ( CASE WHEN
sip = '-' THEN remote_ip ELSE sip END ),  '/',  ip_to_province ( CASE WHEN sip = '-' THEN remote_ip
ELSE sip END ),  '/',  CASE    WHEN ip_to_city ( CASE WHEN sip = '-' THEN remote_ip ELSE sip
END )= '*' THEN  ' ' ELSE ip_to_city ( CASE WHEN sip = '-' THEN remote_ip ELSE sip END )   END,  ' ',
ip_to_provider ( CASE WHEN sip = '-' THEN remote_ip ELSE sip END ))   END AS client,  sum( CASE
WHEN "response_code" < 400 THEN 1 ELSE 0 END ) AS pv,  round( sum( request_length )/ 1024.0 /
1024, 1 ) AS throughput,  "response_code" AS "status"   FROM    log  GROUP BY  ip,  client,
"method",  "response_code"   ORDER BY  pv DESC,  client,  "method"   LIMIT 1000  )  GROUP BY  ip,
client   ORDER BY  pv DESC   )  LIMIT 100
```

----结束

7 日志告警

7.1 日志告警概述

云日志服务支持创建关键词统计类型、SQL统计类型的日志告警规则，根据设置的告警规则触发告警，可以在告警列表查看上报的告警详情，实时监控服务运行状态。或者通过告警行动规则将上报告警以短信，手机，邮件等多种形式发送告警通知，方便用户及时处理告警问题。

功能优势

- 易于开始，便于复制。

  日志接入LTS后，即可创建告警规则和通知策略，支持实时接收潜在的告警事件并响应。
- 高可用性与可靠性。

  依托于LTS的高可用性与数据可靠性，告警服务的可用性达到99.9%，告警相关的数据可靠性高于99.99999999%。
- 低成本与免运维。

  目前LTS暂时不收取告警规则、告警管理等其他费用，降低告警系统的运维成本和运维人员的时间成本。后续如有收费计划将至少提前1个月通知您。

  短信通知按实际用量付费，详细请参考消息通知服务的**计费说明**。语音是白名单功能，具体收费请参考**计费说明**。
- 快速响应异常问题。

  更全面、更智能的告警监控能力与告警行动规则能力，使告警的响应变得更迅速，提高问题解决的速度，减少因业务异常造成的损失。

使用限制

使用限制请参考**日志告警**。

7.2 配置日志告警规则

LTS支持对日志流中的日志数据进行**关键词告警**、**SQL告警**，通过设置告警规则，实时监控服务运行状态。目前每个账号最多可以创建关键词告警与SQL告警共200个。

支持批量创建多个告警规则，请参考**创建多个告警规则**。

前提条件

已创建日志组、日志流，请参考**管理日志组**和**管理日志流**。

创建关键词告警规则

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，统计一定时间段内的日志中关键字出现的次数，实时监控服务运行状态。

步骤1 登录**云日志服务控制台**。

步骤2 左侧导航选择“日志告警”。

步骤3 单击“告警规则”。

步骤4 在“告警规则”页签，单击“创建”，在界面右侧弹出“新建告警规则”页面。

步骤5 在“新建告警规则”页面，配置告警规则相关参数。

表 7-1 关键词告警参数说明

参数类别	参数名称	参数说明
基本信息	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，且不能以中划线、下划线开头或结尾。长度为 1-64个字符。 **说明** 告警创建完成后，支持修改规则名称，修改完成后，鼠标悬浮在规则名称上，显示修改后的规则名称和原始名称，不支持修改首次创建的原始名称。
	描述	对该规则进行简要描述，长度不能超过64个字符。
统计分析	统计类型	勾选关键词统计：适用于使用关键词搜索配置日志告警的场景。
	查询条件	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。 **说明** 当日志组下有多个日志流时，支持选择多个日志流，即可批量创建关键词告警。
		查询时间：指定语句的查询周期。查询语句的时间范围：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，则查询语句的时间范围为8:00-9:00。 • 如果查询时间单位为分钟，则取值范围是1-60； • 如果查询时间单位为小时，则取值范围是1-24。
		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。如何设置关键词搜索请参考**LTS搜索语法介绍**。

参数类别	参数名称	参数说明
	检测规则	配置触发条件，即满足该条件时，会触发告警。 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。支持大于（>）、大于等于（>=）、小于（<）、小于等于（<=）4种比较运算符。 ● 单击+增加条件表达式（or），最多支持增加20条。 ● 单击 删除条件表达式。 统计周期次数指高级设置的统计周期；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。 **说明** ● 触发告警级别包括“紧急”、“重要”、“次要”、“提示”，默认“紧急”。 ● 统计周期次数最小值为1，最大值为10。
高级设置	统计周期	条件表达式查询的频率可以设置为： ● 每小时：表示整点小时查询。 ● 每天：需要指定几点整查询。 ● 每周：需要指定周几的几点整查询。 ● 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..... **说明** 当查询时间大于1小时，固定间隔时间最小取值为5分钟。 ● 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： – 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。 – 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。 – 0 14 * * *每天14:00查询一次。 – 0 0 10 * *每月10日00:00查询一次。
高级设置	恢复策略	配置恢复策略，即满足该策略时，会发送告警恢复通知。 配置的最近统计周期次数内，如果不满足触发条件且开启恢复时通知开关，则会发送恢复告警通知。 最近统计周期次数最小值为1，最大值为10。

参数类别	参数名称	参数说明
高级设置	通知场景	• 告警触发时：用于发送触发告警通知。开启该按钮，当满足触发条件时，会发送告警通知；未开启该按钮，当满足触发条件时，不会发送告警通知。 • 告警恢复时：用于发送恢复告警通知。开启该按钮，当满足恢复策略时，会发送恢复告警通知；未开启该按钮，当满足恢复策略时，不会发送恢复告警通知。
高级设置	通知频率	支持选择立即通知、每5分钟、每10分钟、每15分钟、每30分钟、每1小时、每3小时、每6小时发送告警。 立即通知指只要产生告警就发送通知，每10分钟指的是两次通知之间最小时间间隔为10分钟，可避免告警轰炸。
高级设置	告警行动规则	请从下拉列表中选择已创建的告警行动规则。 若没有，请单击右侧“创建告警行动规则”。
高级设置	语言	发送告警的语言，支持中文（简体）和英文。

步骤6 单击“确定”，关键词告警规则创建成功。详细示例请查看**参考示例1：出现关键字即触发告警**。

说明

告警规则创建完成后，告警状态默认显示“已开启”。关闭告警规则后，告警状态显示“已关闭”，临时关闭告警后，告警状态显示“临时关闭到2023/05/30 16:21:24.000 GMT+08:00”。（临时关闭的时间仅供参考，请以设置临时关闭告警的时间为准）

当开启告警规则且关联日志流满足告警规则时，会触发告警；当关闭告警规则时，即使有满足该告警规则的情况，也不会触发告警。

----结束

创建 SQL 告警规则

云日志服务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。每条SQL告警规则可以关联1到3个图表，每个图表包含一条查询某个日志流的SQL查询语句。

说明

目前此功能支持全部用户使用的局点有：华南-广州、华北-北京四、华东-上海一、华东-上海二、中国-香港、西南-贵阳一、亚太-新加坡、华北-北京一；支持部分白名单用户使用的局点有：亚太-曼谷、华南-深圳、中东-利雅得、亚太-雅加达，其他局点暂不支持该功能。

步骤1 在云日志服务管理控制台，单击“日志告警”。

步骤2 单击“告警规则”。

步骤3 在“告警规则”页签，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，参考**表7-2**配置告警规则相关参数。

表 7-2 SQL 告警参数说明

参数类别	参数名称	参数说明
基本信息	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，且不能以中划线、下划线开头或结尾。长度为 1-64个字符。 **说明** 告警创建完成后，支持修改规则名称，修改完成后，鼠标悬浮在规则名称上，显示修改后的规则名称和原始名称。不支持修改首次创建的原始名称。
	描述	对该规则进行简要描述。长度不能超过64个字符。
统计分析	统计类型	勾选SQL统计：使用SQL分析配置告警。
	相关图表	有两种添加方式：直接添加和从图表导入。 • **直接添加**：单击“直接添加”，可选择日志组、日志流。具体的参数配置信息如下： 日志组名称：日志组的名称，必选项。 日志流名称：日志组下的日志流名称，必选项。 **说明** 若所选日志流未配置结构化规则，请先**设置云端结构化解析日志**。 查询时间：当前所选日志的查询时间，可选项。查询时间（1 ~ 60分钟/1 ~ 24小时），单位为分钟或小时。 查询语句：可视化查询语句，必填项。 • **从图表导入**：单击 ＋从图表导入 ，进入“添加可视化图表”页面，选择对应日志组、日志流下的可视化图表，单击“确定”。若该日志流下没有图表或没有所需的图表，单击界面上的“前往添加图表”，进入可视化界面，设置完成后单击“保存并返回”返回到告警规则界面，自动打开创建规则弹框，填充新创建的图表及图表的查询语句。 可以指定图表的查询时间（1 ~ 60分钟/1 ~ 24小时），单位为分钟或小时，每个图表最多可以查询最近一天的数据，当统计周期选择1~4分钟时，图表查询时间不能超过1小时。 若想添加多个图表，可单击 ＋从图表导入 继续添加。 **说明** – 单击 跳转到日志流的可视化查看详情界面。 – 单击 删除该直接添加的图表。 – 单击“预览”可查看可视化分析后的数据。必须要执行“预览”，否则将无法保存该告警规则。 – 最多支持添加3个图表。 – 图表不能为空，且图表中的sql查询语句不能为空。

参数类别	参数名称	参数说明
	检测规则	输入具体的条件表达式，当条件表达式返回为true的时候，产生告警，否则不产生告警。 **说明** • 条件表达式支持中文。 • 条件表达式不支持纯数字，不支持以数字开头的。 • 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条件表达式。配置的统计周期次数须大于等于满足触发条件次数。 • 触发告警级别包括“紧急”、“重要”、“次要”、“提示”，默认“紧急”。 • 统计周期次数最小值为1，最大值为10。 ● 单击+增加条件表达式（or），最多支持增加20条。 ● 单击 删除条件表达式。 条件表达式支持的基础语法和多表组合语法。 ● 基础语法： – 基础运算符：支持加（+）、减（-）、乘（*）、除（/）、取模运算（%）。 示例：x * 10 + y > 100。 – 比较运算符：支持大于（>）、大于等于（>=）、小于（<）、小于等于（<=）、等于（==）、不等于（!=）。示例：x >= 100。 – 逻辑运算符：支持与（&&）、或（||）。示例：x > 0 && y < 200。 – 取反前缀：支持取反前缀（!）。 示例：!(x < 1 && x > 100)。 – 数值常量：支持数值常量，并作为64位浮点数处理。示例：x > 10。 – 字符串常量：支持字符串常量（"字符串"），例如"string"。示例：str =="string"。 – 布尔常量：支持布尔常量(true、false)。示例：(x < 100)!=true。 – 括号：支持使用括号改变计算的优先级。示例：x *(y + 10)<200。 – contains函数：支持使用contains函数判断是否包含子串，例如contains(str, "hello")返回true则表示str中包含hello子串。 ● 多表组合语法： – 基础运算符：（+-*/%）。 – 比较运算符：大于（>）、大于等于（>=）、小于（<）、小于等于（<=）、等于（==）、不等于（!=）。 – 逻辑运算符：与（&&）、或（||）。 – 取反前缀（!）。

参数类别	参数名称	参数说明
		– contains函数。 – 括号（ ）。
高级设置	统计周期	条件表达式查询的频率可以设置为： ● 每小时：表示整点小时查询。 ● 每天：需要指定几点整查询。 ● 每周：需要指定周几的几点整查询。 ● 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..... **说明** 当查询时间大于1小时，固定间隔时间最小取值为5分钟。 ● 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： – 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。 – 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。 – 0 14 * * *每天14:00查询一次。 – 0 0 10 * *每月10日00:00查询一次。
高级设置	恢复策略	配置恢复策略，即满足该策略时，会发送告警恢复通知。 配置的最近统计周期次数内，如果不满足触发条件且开启恢复时通知开关，则会发送恢复告警通知。 最近统计周期次数最小值为1，最大值为10。
高级设置	通知场景	● 告警触发时：用于发送触发告警通知。开启该按钮，当满足触发条件时，会发送告警通知；未开启该按钮，当满足触发条件时，不会发送告警通知。 ● 告警恢复时：用于发送恢复告警通知。开启该按钮，当满足恢复策略时，会发送恢复告警通知；未开启该按钮，当满足恢复策略时，不会发送恢复告警通知。
高级设置	通知频率	支持选择立即通知、每5分钟、每10分钟、每15分钟、每30分钟、每1小时、每3小时、每6小时发送告警。 立即通知指只要产生告警就发送通知，每10分钟指的是两次通知之间最小时间间隔为10分钟，可避免告警轰炸。
高级设置	告警行动规则	请从下拉列表中选择已创建的告警行动规则。 若没有，请单击右侧“创建告警行动规则”，详细操作请见**创建告警行动规则**。

参数类别	参数名称	参数说明
高级设置	语言	发送告警的语言，支持中文（简体）和英文。

步骤5 单击“确定”，SQL告警规则创建成功。详细示例请查看**参考示例2：根据关键字出现的次数设置告警**。

----结束

创建多个告警规则

支持批量创建多个告警规则。

步骤1 在“告警规则”页面，批量导入告警规则。

1. 单击“导入”，进入导入告警规则页面。
2. 下载告警模板到本地填写完成。
3. 单击“选择文件”，选择本地填写好的文件。
4. 确认导入的规则信息无误后，单击“导入”。
5. 导入成功后，在规则列表下方显示告警规则明细。

步骤2 单击“批量编辑”，进入批量编辑告警规则页面。

步骤3 在基本配置下方，输入告警规则数量，单击“添加告警规则”。

或者单击“导入”，批量导入告警规则。

说明

在规则列表下方默认已有1个告警规则，最多支持再添加199个数量，因此支持同时添加200个告警规则。

步骤4 在规则列表下方，请参考**创建关键词告警规则**、**创建SQL告警规则**设置告警规则，设置完成后，单击“提交”。

- 一个告警规则设置完成后，单击“应用于其他告警规则”即可将该告警规则复制到其他告警规则。
- 例如添加了4个告警规则，批量创建成功后，在告警规则页签下方，就会显示4条告警规则。

----结束

告警规则后续操作

创建告警规则后，支持对告警规则进行修改、开启/关闭、复制、删除等操作，可能会导致原有告警规则发生变化，请谨慎操作。

- 支持对单个告警规则进行如下操作：

  修改告警规则：单击目标告警规则操作列的“修改”，在“修改告警规则”页面，修改规则名称、查询条件、检测规则等信息，修改完成后，单击“确定”。

  开启告警规则：单击目标告警规则操作列的“更多 > 开启告警规则”，开启告警规则。

  关闭告警规则：单击目标告警规则操作列的“更多 > 关闭告警规则”，关闭告警规则。

临时关闭告警规则：单击目标告警规则操作列的“更多 > 临时关闭告警规则”，设置临时关闭的截止时间。

复制告警规则：单击目标告警规则操作列的“更多 > 复制”，即可直接复制告警规则。

删除告警规则：单击目标告警规则操作列的“删除”，在弹出的对话框中，单击“确定”删除该告警规则。

说明

删除告警规则后不可恢复，请谨慎操作。

- 勾选多个告警规则后，支持对多个告警进行批量操作：开启、关闭、临时关闭、取消临时关闭、告警恢复开启、告警恢复关闭、删除、导出。
- 鼠标悬浮在规则名称上，显示修改后的规则名称和原始名称。不支持修改首次创建的原始名称。

参考示例 1：出现关键字即触发告警

如果您希望日志中出现目标关键字时，就能触发告警，则您可以参考本示例设置查询语句和关键词告警规则。以下示例仅供参考，请以实际业务为准。

设置的关键字一定是日志流存在的关键字，例如Error关键字。

图 7-1 查询结果

- 查询语句：选择查询时间范围为15分钟，然后执行如下语句，查询包含Error关键字的日志。更多搜索语法请参考**LTS搜索语法介绍**。

图 7-2 查询语句

- 告警通知：创建上述告警规则后，只要日志中出现Error关键字，您就可以在“告警列表”收到告警通知。您还可以单击告警名称，查看告警详情，进行溯源。

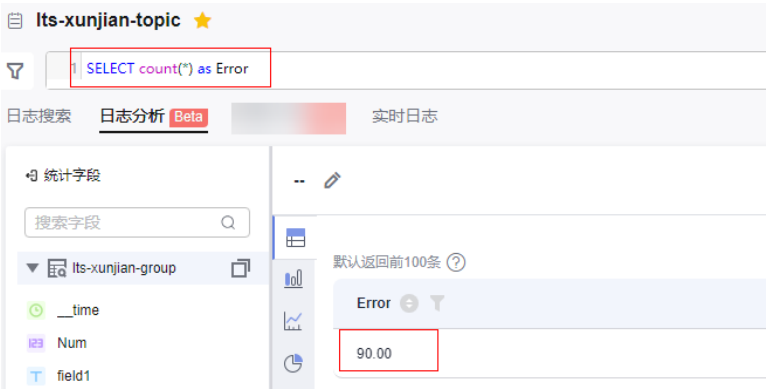
图 7-3 告警报错

参考示例 2：根据关键字出现的次数设置告警

如果您希望在一定时间范围内日志关键字出现的次数达到指定次数时，才触发告警，则您可以参考本示例设置查询分析语句和SQL告警规则。以下示例仅供参考，请以实际业务为准。

使用“SELECT count(*) as Error”在目标日志流查询当前Error总共出现90次。

图 7-4 查询结果



- 查询语句：选择查询时间范围为5分钟，然后执行如下语句“SELECT count(*) as Error”，统计5分钟内出现Error关键字的次数。更多搜索语法请参考**SQL分析语法介绍**。

图 7-5 查询语句

- 告警通知：创建上述告警规则后，只要日志中出现Error关键字超过2次，您就可以在“告警列表”收到告警通知。您还可以单击告警名称，查看告警详情，进行溯源。

图 7-6 告警报错

7.3 配置日志告警行动规则

7.3.1 在 LTS 页面创建消息模板

消息模板是告警通知消息的固定格式，系统发送告警通知消息必须使用消息模板向订阅者发送。支持内置消息模板，不同协议的订阅者优先选择模板名称对应的协议模板，如果对应的协议模板不存在，则采用内置的消息模板。使用消息模板发送告警通知消息时，系统会自动将模板变量替换为告警规则中的内容。

创建消息模板

步骤1 登录云日志服务控制台。

步骤2 左侧导航选择“日志告警”，进入告警页面，选择“告警行动规则”。

说明

消息模板默认有以下内置模板，当您所选择的消息模板中未配置消息内容时，云日志服务默认使用内置模板。

- 关键词模板：关键词告警模板
- keywords_template：关键词告警英文模板
- sql模板：sql告警模板
- sql_template：sql告警英文模板

步骤3 在消息模板页签，单击“创建”，在界面右侧弹出的“创建消息模板”页面中，配置消息模板的相关参数。

说明

- 邮件内容支持html标签和消息预览。
- 企业微信、钉钉、飞书支持markdown语法和消息预览。
- 针对AOM和LTS，最多可以创建100（包含）条消息模板，如果消息模板数量已达上限100个时，请删除不需要的消息模板后重新创建。

表 7-3 配置消息模板参数

参数名称	说明	校验规则	样例
模板名称	消息模板的名称	输入内容只能是数字、字母、下划线、汉字、中划线，且不能以下划线、中划线等特殊符号开头和结尾。长度不能超过100个字符。	LTS-test
模板描述	对消息模板的描述	输入内容只能是数字、字母、下划线、汉字，且不能以下划线等特殊符号开头和结尾。长度不能超过1024个字符。	-
消息头语言	系统在发送消息时会默认添加消息头	• 中文（简体） • 英文	• 中文：“尊敬的用户...” • 英文：“Dear User...”
通知方式	消息的通知方式类型	• 邮件 • 短信 • HTTP/HTTPS • 钉钉 • 飞书 • 企业微信 • 语音 **说明** 语音功能仅针对白名单用户提交工单申请使用。详细操作请参考**提交工单**。	-
主题	消息的主题	支持自定义主题名称和使用变量命名主题两种方式。主题名称长度不能超过512个字符。 仅邮件类型支持配置消息主题。	test

参数名称	说明	校验规则	样例
正文	消息的内容	**添加变量：** • 规则原始名称：${event_name} • 告警级别：${event_severity} • 发生时间：${starts_at} • 发生区域：${region_name} • 华为云账号：${domain_name} • 告警源：$event.metadata.resource_provider • 资源类型：$event.metadata.resource_type • 资源标识：${resources} • 告警状态：$event.annotations.alarm_status • 表达式：$event.annotations.condition_expression • 当前值：$event.annotations.current_value • 表达式带值：$event.annotations.condition_expression_with_value • 统计周期：$event.annotations.frequency • 规则名称：$event.annotations.alarm_rule_alias • 通知频率：$event.annotations.notification_frequency • 日志组原始名称：$event.annotations.results[0].log_group_name • 日志流原始名称：$event.annotations.results[0].log_stream_name • 关键词告警支持的变量	${event_name} ${event_severity} ${starts_at} ${region_name}

参数名称	说明	校验规则	样例
		1. 查询时间：$event.annotations.results[0].time 2. 查询日志：（日志长度最多2KB，超过2KB被截断丢弃）$event.annotations.results[0].raw_results 3. 查询URL：$event.annotations.results[0].url 4. 日志组/日志流名称：$event.annotations.results[0].resource_id **说明** 只支持添加首次创建的日志组/日志流原始名称，不支持添加修改后的日志组/日志流名称。 5. 日志流的企业项目ID：$event.annotations.results[0].eps_id 6. 查询自定义字段 $event.annotations.results[0].fields.xxx **说明** xxx表示原始日志的结构化字段和内置字段（hostIP、hostName等），日志字段长度最多1KB，超过1KB被截断丢弃。 ● SQL告警支持的变量 1. 图表0的日志组/流名称：$event.annotations.results[0].resource_id **说明** 只支持添加首次创建的日志组/日志流原始名称，不支持添加修改后的日志组/日志流名称。 0代表第一个图表，1代表第二个图表，以此类推。 2. 图表0的查询语句：$event.annotations.results[0].sql 3. 图表0的查询时间：$event.annotations.results[0].time	

参数名称	说明	校验规则	样例
		4. 图表0的查询URL：$event.annotations.results[0].url 5. 图表0的查询日志：$event.annotations.results[0].raw_results 6. 图表0的日志流的企业项目ID：$event.annotations.results[0].eps_id **复制模板：** • keywords_template • sql_template • sql模板 • 关键词模板 • 自定义模板（用户通过添加变量创建的消息模板）	

步骤4 配置完成后，单击“确定”。

说明

在LTS页面创建消息模板时提示“创建消息模板失败，名称不能重复”，可以参考如下步骤进行排查处理。

1. 请检查消息模板名称是否有重复。

   若有重复，请重新修改消息模板名称。因为，LTS的消息模板数据源与AOM消息模板数据源为同一个，消息模板名称不能重复，如果在AOM中创建了名称为test的消息模板，在LTS页面不能创建同名的消息模板。

2. 请检查消息模板数量是否超过100个。

   针对AOM和LTS，最多可以创建100（包含）条消息模板，当消息模板数量已达上限100个时，请删除不需要的消息模板后重新创建。

----结束

编辑消息模板

步骤1 在消息模板列表中，单击消息模板名称行后的“修改”，根据表7-3进行修改，其中“模板名称”不可修改。

说明

内置消息模板不支持编辑。

步骤2 编辑完成后，单击“确定”。

----结束

复制消息模板

步骤1 在消息模板列表中，单击消息模板名称行后的“复制”，修改消息模板的模板名称。

步骤2 完成后，单击“确定”。

----结束

删除消息模板

步骤1 在消息模板列表中，单击消息模板名称行后的“删除”。

说明

内置消息模板不支持删除。

步骤2 在弹出的对话框中，单击“确认”删除该消息模板。

----结束

批量删除消息模板

步骤1 在消息模板列表中，勾选待删除的消息模板，单击列表左上方“批量删除”。

步骤2 在弹出的删除消息模板页面，单击“确定”，删除所勾选的消息模板。

----结束

导出消息模板

步骤1 在消息模板列表中，勾选待导出的消息模板，单击列表左上方“导出”。

步骤2 选择“导出全部数据到XLSX”或“导出已选中数据到XLSX”，导出成功后即可到本地查看消息模板数据。

----结束

7.3.2 创建告警行动规则

LTS提供告警行动规则定制功能，您可以通过创建告警行动规则关联SMN主题与消息模板，创建消息模板时，自定义通知消息配置。

前提条件

- 已创建一个主题。详细操作请参考**创建主题**。
- 已设置主题策略。详细操作请参考**设置主题策略**。
- 已为主题添加相关的订阅者，即通知的接收人（例如：邮件或短信）。详细操作请参考**订阅主题**。

注意事项

您最多可创建1000个告警行动规则，如果告警行动规则数量已达上限1000时，请删除不需要的行动规则。

创建告警行动规则

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“日志告警”。

步骤3 单击“告警行动规则”页签。

步骤4 在告警行动规则页签，单击“创建”。设置行动规则名称、行动规则配置等信息。

图 7-7 创建告警行动规则

表 7-4 告警行动规则参数说明

参数名称	说明
行动规则名称	只能由数字、字母、中文、下划线、中划线组成，且不能以下划线、中划线开头结尾，长度为1到64个字符。
企业项目	选择已创建的企业项目。 如果当前账号未开通企业项目则不显示该参数。
描述	自定义行动规则的描述，字符长度0-1024个字符。
主题	SMN主题，请从下拉列表中选择。 若没有合适的主题，请单击主题选择栏下方“创建主题”，在SMN界面创建。

参数名称	说明
消息模板	通知消息的模板，请从下拉列表中选择。 若没有合适的消息模板，请单击消息模板选择栏右侧“创建消息模板”，新建消息模板。详细操作请参考**创建消息模板**。

步骤5 设置完成后，单击“确定”。

----结束

更多操作

告警行动规则创建完成后，您还可以执行**表7-5**中的相关操作。

表 7-5 相关操作

操作	说明
修改告警行动规则	单击“操作”列的“修改”。
导出告警行动规则	选中单个或多个告警行动规则，单击“导出”，若没有选中告警行动规则，则导出全部告警行动规则。
删除告警行动规则	• 删除单条规则：单击对应规则“操作”列的“删除”，随后在提示页面单击“确定”即可删除。 • 删除单条或多条规则：勾选对应规则前的复选框，单击“批量删除”，随后在提示页面单击“确定”即可删除。 **说明** 删除告警行动规则前需要先删除该行动规则绑定的告警规则。
搜索告警行动规则	在右上角的搜索框中输入规则名称关键字，单击  后显示匹配对象。

7.4 查看 LTS 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或sql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。

查看告警

步骤1 登录**云日志服务控制台**。

步骤2 左侧导航选择“日志告警”。

步骤3 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4 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、告警级别、规则名称进行搜索。
- 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。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：表示查询指定时间范围的日志数据。

步骤5 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6 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删除按钮对该告警进行清除，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 日志转储概述

主机和云服务的日志数据上报至云日志服务LTS后，LTS会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。请以创建日志组或日志流时设置的日志存储时间为准，详情请参考**管理日志组**和**管理日志流**。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，可以将日志转储至其他云服务中进行长期保存。

说明

日志转储功能只能拷贝已有日志，不会删除日志。云日志服务LTS根据用户配置的日志存储时间定时清理日志文件，不会影响转储后的日志。

当前LTS支持以下**表8-1**，请根据您的业务场景进行日志转储服务选择。

表 8-1 转储服务类型

转储服务类型	使用场景
对象存储服务 OBS	对象存储服务（Object Storage Service，OBS）提供海量、安全、高可靠、低成本的数据存储能力，可供用户存储任意类型和大小的数据。适合企业备份/归档、视频点播、视频监控等多种数据存储场景。 OBS提供了标准存储、低频访问存储、归档存储、深度归档存储（受限公测中）四种存储类别，满足不同场景下客户对存储性能和成本的不同诉求。

转储服务类型	使用场景
分布式消息服务Kafka版（DMS）	分布式消息服务Kafka版（Distributed Message Service for Kafka）是一款基于开源社区版Kafka提供的消息队列服务，具备高效可靠的消息异步传递机制，向用户提供计算、存储和带宽资源独占式的Kafka专享实例。 主要用于不同系统间的数据交流和传递，在企业解决方案、金融支付、电信、电子商务、社交、即时通信、视频、物联网、车联网等众多领域都有广泛应用。 Kafka可以应对大量日志传输场景，应用通过异步方式将日志消息同步到消息服务，再通过其他组件对日志做实时或离线分析，也可用于关键日志信息收集进行应用监控。
数据接入服务 DIS	数据接入服务（Data Ingestion Service，简称DIS）为处理或分析流数据的自定义应用程序构建数据流管道，主要解决云服务外的数据实时传输到云服务内的问题。数据接入服务每小时可从数十万种数据源（如IoT数据采集、日志和定位追踪事件、网站点击流、社交媒体源等）中连续捕获、传送和存储数TB数据。

8.2 日志转储至 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。支持将日志周期性或一次性的转储至对象存储服务（OBS）中长期保存。

- 创建日志转储（周期性）
- 创建日志转储（一次性）

说明

- 创建日志转储时，除需拥有LTS使用权限外，还需要拥有以下OBS桶相关授权项：设置桶ACL（obs:bucket:PutBucketAcl）、获取桶列表（obs:bucket:ListAllMyBuckets）、获取桶元数据（obs:bucket:HeadBucket）、获取桶ACL（obs:bucket:GetBucketAcl）、获取桶的加密配置（obs:bucket:GetEncryptionConfiguration）。更多信息请参见桶相关授权项。
- 云日志服务配置的日志转储是将最新产生的日志转储到OBS桶中，不会对历史日志进行转储。

前提条件

- 日志已接入LTS。详细请参考日志接入。
- 已创建OBS桶。

说明

OBS存储独立收费，收费详情请参见：华为云定价。

创建日志转储（周期性）

步骤1 登录云日志服务控制台。

步骤2 左侧导航选择“日志转储”。

步骤3 在“日志转储”页面右上角，单击“配置转储”。

步骤4 在“配置转储”页面，设置转储日志相关参数。

表 8-2 配置转储参数说明

参数名称	说明	示例
日志源	• 当前账号：对用户所在账号下所产生的日志进行转储。 • 其他账号：对委托人账号下所产生的日志进行转储，如需转储其他账号日志，需该账号使用者在IAM中**创建委托**。	当前账号
委托名称	当转储其他账号时，需填写委托人在IAM中创建的委托名称。	-
委托人账号名称	当转储其他账号时，需填写委托人的账号名称。	-
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。	-
企业项目	选择已创建的企业项目。 • 如果当前账号未开通企业项目则不显示该参数。 • 如果当前账号已开通企业项目，则存在以下情况： – 当转储当前账号日志时，下拉框显示当前账号的全部企业项目。 – 当转储其他账号日志时，若委托账号未开通企业项目，则默认显示“default”。 – 当转储其他账号日志时，若委托账号已开通企业项目，则显示委托账号的全部企业项目。	-
日志流名称	选择已创建的日志流。 **说明** 已配置过OBS转储的日志流不能重复配置。	-

参数名称	说明	示例
OBS桶	● 选择已创建的OBS桶。 – 如果没有可选择的OBS桶，单击“查看OBS”，进入对象存储服务管理控制台，创建OBS桶。 – 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账号，对转储日志加解密”。 – 选中的桶会将读写策略授权给云日志服务，请谨慎修改桶策略，防止转储失败。 ● LTS目前仅支持单AZ存储策略、标准存储类别的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	示例
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/%GroupName/%StreamName/*自定义转储路径*。自定义转储路径默认为lts/%Y/%m/%d，其中%Y代表年，%m代表月，%d代表日，格式需要符合如下规范： – “/LogTanks/RegionName”为系统默认路径，不可以修改。 – 新增%GroupName代表日志组名称，%StreamName代表日志流名称。 – 名称只能由英文字母、数字及特殊字符“&”“$”“@”“;”“:”“,”“=”“+”“?”“-”“.”“_”“/”和“%”组成，且“%”后只可跟Y（年）、m（月）、d（日）、H（时）、M（分），在%Y、%m、%d、%H和%M前后可以添加任意长度字符，并且可对其先后顺序进行调换。 – 自定义转储路径名称不允许为空，长度限制为1~128个字符。 示例： 1. 输入LTS-test/%Y/%m/%d/%H/%*M*，则日志转储路径为*：LogTanks/RegionName/LTS-test/Y/m/d/H/M/日志文件名称。* 2. 输入LTS-test/%d/%H/%m/%Y，则日志转储路径为：*LogTanks/RegionName/LTS-test/d/H/m/Y/日志文件名称。* • 不开启：将日志转储至系统默认路径中。系统默认路径为：LogTanks/RegionName/*2019/01/01/日志组/日志流/日志文件名称*。	LTS-test/%GroupName/%StreamName/%Y/%m/%d/%H/%M
日志文件前缀	转储至OBS桶中的日志文件前缀。 日志文件前缀需符合如下规范： • 名称长度限制为0~64个字符。 • 名称只能由英文大小写字母、数字、中划线“-”、下划线“_”和小数点“.”组成。 示例：输入LTS-log，则日志文件名称为：LTS-log_日志文件名称。	LTS-log

参数名称	说明	示例

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

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

步骤5 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。

步骤6 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。

----结束

创建日志转储（一次性）

说明

目前此功能支持亚太-新加坡，其他局点如有需要请**提交工单**申请开通。

步骤1 在“日志转储”页面右上角，单击“配置转储”。

步骤2 在“配置转储”页面，设置转储日志相关参数。

表 8-3 配置转储参数说明

参数名称	说明	示例
转储方式	一次性转储：日志将一次性的转储至对象存储服务（OBS）中长期保存。	一次性转储
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。	-
企业项目	选择已创建的企业项目。 • 如果当前账号未开通企业项目则不显示该参数。 • 如果当前账号已开通企业项目，则存在以下情况： – 当转储当前账号日志时，下拉框显示当前账号的全部企业项目。 – 当转储其他账号日志时，若委托账号未开通企业项目，则默认显示“default”。 – 当转储其他账号日志时，若委托账号已开通企业项目，则显示委托账号的全部企业项目。	-
日志流名称	选择已创建的日志流。 **说明** 已配置过OBS转储的日志流不能重复配置。	-
过滤条件	默认关键词过滤，在输入框填写需要过滤的关键词。	-

参数名称	说明	示例
转储时间范围	时间范围有三种方式，分别是相对时间、整点时间和自定义。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：表示查询指定时间范围的日志数据。	-
日志总条数	日志总条数。	-
转储文件个数	单次一次性转储日志条数上限2000万条，转储文件个数上限200个。	-
OBS桶	● 选择已创建的OBS桶。 如果没有可选择的OBS桶，单击“查看OBS”，进入对象存储服务管理控制台，创建OBS桶。 ● LTS目前仅支持存储类别为“标准存储”的OBS桶。 ● 不支持转储到存储类型为归档存储或配置了跨区域复制的OBS桶。 **说明** 首次配置一次性转储到未授权的OBS桶中时，LTS服务会授权给OBS桶ACL规则，授权生效需要15分钟，如果您第一次配置一次性转储后失败，任务会在15分钟后重试。请谨慎修改桶策略，防止转储失败。	-
所属桶目录	所属OBS桶目录。	-
转储文件名称	自定义转储文件名称，只能由英文字母、数字、中划线、下划线、小数点组成。	-

参数名称	说明	示例
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、CSV格式。 ● 原始日志格式示例： 云日志服务控制台展示的日志内容的格式为原始日志格式。 Sep 30 07:30:01 ecs-bd70 CRON[3459]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1) ● Json格式示例： {"host_name":"ecs-bd70","ip":"192.168.0.54","line_no":249,"message":"Sep 30 14:40:01 ecs-bd70 CRON[4363]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)\n","path":"/var/log/syslog","time":1569825602303} ● CSV格式：以表格的形式展示日志内容。	Json

步骤3 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。

步骤4 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。

步骤5 转储到OBS后的日志，支持从OBS下载到本地进行查看。

----结束

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“更多>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“确定”，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。

8.3 日志转储至 DIS

DIS提供丰富的大数据分析能力，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。您可以根据业务场景选择是否使用DIS进行日志转储。

说明

- 建议您优先使用**转储至DMS**。
- 目前此功能仅支持华北-北京四、华北-北京一、华东-上海二、华南-广州、中国-香港、亚太-新加坡局点，其他局点需要给DIS服务提交工单申请开通才能使用。详细操作请参考**提交工单**。

前提条件

- 日志已接入LTS，详细请参考**日志接入**。
- 已开通DIS，详细请参考**开通DIS通道**。

说明

DIS存储独立收费，收费详情请参见：**华为云定价**。

日志转储至 DIS

步骤1 在云日志服务管理控制台，左侧导航栏中，单击“日志转储”。

步骤2 在“日志转储”页面右上角，单击“配置转储”。

步骤3 在“配置转储”页面，设置转储日志相关参数。

表 8-4 配置转储参数说明

参数名称	说明	示例
日志源	• 当前账号：对用户所在账号下所产生的日志进行转储。 • 其他账号：对委托人账号下所产生的日志进行转储，如需转储其他账号日志，需该账号使用者在IAM中**创建委托**，创建完成后，请记下委托名称和委托人账号名称。	当前账号
委托名称	当转储其他账号时，需填写委托人在IAM中创建的委托名称。	-
委托人账号名称	当转储其他账号时，需填写委托人的账号名称。	-
是否开启转储	选择开启转储。	开启
转储对象	选择转储的云服务。	DIS
日志组名称	选择已创建的日志组。	-
企业项目	选择已创建的企业项目。 • 如果当前账号未开通企业项目则不显示该参数。 • 如果当前账号已开通企业项目，则存在以下情况： – 当转储当前账号日志时，下拉框显示当前账号的全部企业项目。 – 当转储其他账号日志时，若委托账号未开通企业项目，则默认显示“default”。 – 当转储其他账号日志时，若委托账号已开通企业项目，则显示委托账号的全部企业项目。	-
日志流名称	选择已创建的日志流。 **说明** 已配置过DIS转储的日志流不能重复配置。	-
通道名称	选择已创建的DIS通道。如果没有可选择的通道，单击“查看DIS通道”，进入数据接入服务管理控制台，创建接入通道。	-

参数名称	说明	示例
转储格式	用于配置日志的转储格式，可选择“原始日志格式”和“JSON格式”。 ● 原始日志格式示例： 云日志服务控制台展示的日志内容的格式为原始日志格式。 Sep 30 07:30:01 ecs-bd70 CRON[3459]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1) ● JSON格式示例： {"host_name":"ecs-bd70","ip":"192.168.0.54","line_no":249,"message":"Sep 30 14:40:01 ecs-bd70 CRON[4363]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh > /dev/null 2>&1)\n","path":"/var/log/syslog","time":1569825602303}	JSON
转储周期	日志将实时转储至DIS通道中。	实时
是否投递tag	如主机日志，转储时会增加采集器收集的tag字段。 ● 不开启：不会投递tag。 ● 开启：默认的投递tag有：主机信息（hostIP、hostId、hostName、pathFile、collectTime）；kubernetes信息（clusterName、clusterId、nameSpace、podName、appName、containerName）。可选择公共tag有：regionName、projectId、logStreamName、logGroupName。 **说明** 当开启投递tag后，转储格式必须是JSON格式。 ● 转储标签：开启后，会将日志流标签添加至转储内容。	开启

步骤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。当选择对其他账号日志进行转储时，被委托人的转储界面，日志组和日志流属于委托人，前端单击日志组名称、日志流名称时，需要通过委托跳转到委托人的日志组、日志流界面。

步骤5 单击“转储对象”列的DIS通道名称，可以跳转至DIS控制台，查看转储的日志文件。

转储后的日志，支持下载到本地进行查看。

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DIS。
- 当删除该转储任务时，请在数据接入服务（Data Ingestion Service，DIS）中，单击“通道管理”，选择该DIS实例进入实例详情页面。在授权管理中，删除上传权限。

----结束

8.4 日志转储至 DMS

分布式消息服务 DMS提供日志实时处理管道，您可以通过分布式消息服务API实时消费处理日志。

说明

目前此功能仅支持白名单用户提交工单申请使用。详细操作请参考**提交工单**。

前提条件

- 日志已接入LTS。
- 已购买DMS。

  说明

  DMS存储独立收费，收费详情请参见：**华为云定价**。
- 在注册DMS Kafka实例前，需在安全组中，开放**入方向规则**198.19.128.0/17和9011端口。如果DMS的子网关联了网络ACL，需要放开网络ACL入方向规则，协议为TCP， 入方向规则源地址198.19.128.0/17，端口范围为1-65535，目的地址为全放开，目的端口为9011。

日志转储至 DMS

步骤1 在云日志服务管理控制台，左侧导航栏中，单击“日志转储”。

步骤2 在“日志转储”页面右上角，单击“配置转储”。

步骤3 在“配置转储”页面，设置转储日志相关参数。

表 8-5 配置转储参数说明

参数名称	说明	示例
日志源	• 当前账号：对用户所在账号下所产生的日志进行转储。 • 其他账号：对委托人账号下所产生的日志进行转储，如需转储其他账号日志，需该账号使用者在IAM中**创建委托**。	当前账号
委托名称	当转储其他账号时，需填写委托人在IAM中创建的委托名称。	-
委托人账号名称	当转储其他账号时，需填写委托人的账号名称。	-
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。	DMS
日志组名称	选择已创建的日志组。	-

参数名称	说明	示例
企业项目	选择已创建的企业项目。 ● 如果当前账号未开通企业项目则不显示该参数。 ● 如果当前账号已开通企业项目，则存在以下情况： – 当转储当前账号日志时，下拉框显示当前账号的全部企业项目。 – 当转储其他账号日志时，若委托账号未开通企业项目，则默认显示“default”。 – 当转储其他账号日志时，若委托账号已开通企业项目，则显示委托账号的全部企业项目。	-
日志流名称	选择已创建的日志流。 **说明** 已配置过DMS转储的日志流不能重复配置。	-
Kafka实例	选择Kafka实例。如果没有可选择的实例，单击“查看Kafka实例”，进入分布式消息管理控制台，创建Kafka实例。 如果Kafka实例已注册（如果未注册，请注册Kafka实例，操作指导请参见：**注册Kafka实例**），可以选择修改Kafka实例。 **说明** 创建Kafka实例时，设置实例的访问方式：内网访问开启密文接入，“kafka安全协议”选择“SASL_SSL”，设置用户名和密码。同时开启“SASL PLAIN机制”。详细操作请参考**购买实例**。	-
Topic	选择Kafka实例的topic，如果没有可选择的topic，进入分布式消息管理控制台，创建专享版Kafka的topic	topic-01

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

转储周期	日志将实时转储至Kafka实例中。	实时

参数名称	说明	示例
用户日志字段	当转储格式选择JSON时，需要设置该参数。 是否开启转储用户日志字段。 选择转储所有字段后将转储日志下所有的字段，选择自定义转储字段后将手动配置用户日志字段。	-
LTS内置字段和用户自定义Tag	当转储格式选择JSON时，需要设置该参数。 是否开启LTS内置字段和用户自定义Tag。 选择转储所有字段后将转储日志下所有的内置字段和用户自定义字段，选择自定义转储字段后将手动配置LTS内置字段和自定义字段。	-
日志流标签字段	当转储格式选择JSON时，需要设置该参数。 是否开启日志流标签字段。开启后，转储类型支持转储所有字段或自定义转储字段。 选择转储所有字段后将转储日志下所有的日志流标签字段，选择自定义转储字段后将手动配置日志流标签字段。如何设置标签请参考**管理日志流**。	-
更多配置	当转储格式选择JSON时，需要设置该参数。 若日志中无值与上方配置的键值对应，则会用无效字段填充。	-

步骤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。当选择对其他账号日志进行转储时，被委托人的转储界面，日志组和日志流属于委托人，前端单击日志组名称、日志流名称时，需要通过委托跳转到委托人的日志组、日志流界面。

步骤5 单击“转储对象”列的名称，可跳转到专享版Kafka实例的基本信息页面。

说明

创建转储任务成功后，支持查看、修改、删除转储任务。

- 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DMS。

----结束

注册 Kafka 实例

1. 如果选择Kafka实例未注册，单击“注册”，跳转到注册Kafka实例页面。
2. 注册Kafka实例相关参数说明。

表 8-6 参数说明

参数名称	说明	示例
Kafka实例	dms实例名称。	Kafka-01

参数名称	说明	示例
打通DMS网络	打通Kafka实例和LTS服务的网络，用户LTS服务通过该网络发送转储数据。	-
用户名	如果Kafka实例开启了sasl认证，需要输入sasl认证的用户名。	DMS
密码	如果Kafka实例开启了sasl认证，需要输入sasl认证的密码。	-

3. 单击“确定”，完成注册Kafka实例。

8.5 日志转储至 DWS

数据仓库服务GaussDB(DWS) 是一种基于华为云基础架构和平台的在线数据处理数据库，提供即开即用、可扩展且完全托管的分析型数据库服务。转储至数据仓库服务GaussDB(DWS) ，可以将日志中的结构化字段转储到DWS数据库表中，您可以根据业务场景选择是否使用DWS进行日志转储。

说明

目前此功能仅支持华北-北京四、华东-上海一、华南-广州、亚太-新加坡局点，其他局点需要提交工单申请使用。详细操作请参考**提交工单**。

前提条件

- 日志已接入云日志服务（ LTS ）。
- 日志流已配置结构化规则。
- 购买**购买独享型负载均衡器**。
- **创建GaussDB(DWS)存算一体集群**，并且绑定弹性负载均衡（ ELB ）。

  说明

  暂不支持DWS集群跨VPC绑定弹性负载均衡（ ELB ）。

日志转储至 DWS

步骤1 登录云日志服务控制台，在左侧导航栏中选择“日志转储 ”。

步骤2 在“日志转储”页面中，单击右上角“配置转储”。

步骤3 在“配置转储”页面中，选择转储对象“DWS集群”，并配置各参数信息。

表 8-7 配置转储参数说明

参数名称	说明	示例
是否开启转储	选择是否开启转储。	开启
转储对象	选择转储的云服务。	DWS集群

参数名称	说明	示例
日志组名称	选择已创建的日志组。	-
企业项目	选择已创建的企业项目。 ● 如果当前账号未开通企业项目则不显示该参数。 ● 如果当前账号已开通企业项目，则存在以下情况： – 当转储当前账号日志时，下拉框显示当前账号的全部企业项目。 – 当转储其他账号日志时，若委托账号未开通企业项目，则默认显示“default”。 – 当转储其他账号日志时，若委托账号已开通企业项目，则显示委托账号的全部企业项目。	default
日志流名称	选择已创建的日志流。 **说明** 已配置过DWS集群转储的日志流不能重复配置。	-
集群名称	已创建的集群名称。	test
数据库名称	集群的数据库名称。有两种数据库，分别是“gaussdb”和“postgres”。默认集群数据库为“gaussdb”。	gaussdb
用户名	数据库的管理员用户名。	lts-test
密码	数据库的管理员密码。	-
schema名称	数据库对象的集合名称。	-
表名	schema中的表名称。	-

参数名称	说明	示例
字段映射	将内置字段以及日志中配置的结构化字段和类型，映射到数据库字段。 **说明** 内置字段有13个，分别是hostIP、 hostId、hostName、pathFile、collectTime、clusterName、clusterId、 podName、containerName、regionName、projectId、logGroupName和logStreamName。 当结构化字段类型和数据库表字段类型一致时，支持将日志的结构化字段转储至数据仓库服务GaussDB(DWS)，否则转储无效。 ● 在结构化字段和表字段的下拉框，选择您需要转储的字段。 ● 单击操作列下的，删除不需要的转储字段。 ● 单击 添加 ，添加需要转储的字段。	hostIP

步骤4 完成后单击“确定”。

创建转储任务成功后，支持查看、修改、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DWS。

----结束

9 日志加工

9.1 使用定时 SQL 进行日志加工

云日志服务提供定时SQL功能，用于定时分析日志内容。定时SQL支持标准的SQL语法，按照调度规则周期性执行日志分析，并将分析结果存储到目标日志流。

说明

目前此功能仅在华北-北京四、华南-广州、华东-上海一局点支持白名单用户提交工单申请使用，详细操作请参考**提交工单**，其他局点暂不支持该功能。

前提条件

- 已成功采集到日志。
- 对源日志内容已完成结构化配置，具体操作请参考**结构化配置**。

限制条件

最多可创建20个定时SQL任务。

创建定时 SQL

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“日志加工>定时SQL”，单击“创建定时SQL” 。

或在左侧导航栏中选择“日志管理 ”，单击日志组或日志流名称，进入日志流详情页面，单击  ，在弹出页面中，选择“定时SQL”，单击“创建定时SQL”。

说明

- 通过该方式创建定时SQL时，源日志组/日志流为当前所选的日志组/日志流，且无法修改。
- 通过该方式创建的定时SQL任务，会同步显示在定时SQL列表中，单击任务名称可**查看详细信息**。

步骤3 在创建定时SQL页面中，配置相关参数。

- 在计算配置中，完成如下配置后，然后单击“下一步”。

表 9-1 计算配置参数

参数	说明
任务名称	定时SQL任务的名称。仅支持输入英文、数字、中文、中划线、下划线，且不能以中划线、下划线开头或结尾，长度范围为1~64个字符。
描述	定时SQL任务的描述。长度不超过1000个字符。
源日志组/流名称	选择已完成结构化配置的日志组/流，即表示源日志组/流中的日志内容通过定时SQL处理后，将存储到目标日志组/日志流中。
统计类型	SQL统计（使用旧SQL引擎）
SQL代码	输入的查询和分析语句，定时SQL运行时，云日志服务将执行该查询和分析语句分析日志。 选择时间范围，对该范围内的日志内容进行SQL查询；单击“预览”可查询预览结果。
目标日志组/流名称	存储SQL分析结果的日志组/日志流。

- 在调度配置中，完成如下配置。

表 9-2 调度配置参数

参数	说明
调度间隔	调度定时SQL任务的频率，每调度一次定时SQL任务将产生一个执行实例。调度间隔决定每个执行实例的调度时间。 – 每小时：每隔一小时调度一次定时SQL任务。 – 每天：在每天的某个固定时间点调度一次定时SQL任务。 – 每周：在周几的某个固定时间点调度一次定时SQL任务。 – 固定间隔：按照固定间隔调度定时SQL任务。 – CRON：通过CRON表达式指定时间间隔，按照指定的时间间隔调度定时SQL任务。CRON表达式的最小精度为分钟，格式为24小时制，示例如下： ■ 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。 ■ 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。 ■ 0 14 * * *每天14:00查询一次。 ■ 0 0 10 * *每月10日00:00查询一次。
调度时间范围	调度的时间范围，具体说明如下： – 某时间开始：实例调度的开始时间，不设时间范围。当该作业被删除时，则不产生新实例。 – 特定时间范围：按照调度间隔生成的实例调度时间必须在该范围内，超出范围则不产生新实例。
起始时间	调度的起始时间。 当调度时间范围选择某时间开始时，需要设置开始时间；当调度时间范围选择特定时间范围时，需要设置起始时间。

参数	说明
SQL时间窗口	定时SQL任务运行时，仅分析该时间范围内的日志。时间窗口表达式的最小精度为秒（s：秒，m：分，h：小时），且SQL时间窗口设置不能超过24小时。可在下拉框中，选择5分钟、15分钟、1小时和1天。如果需要设置其他时间，可在下拉框中选择自定义，通过时间窗口表达式进行设置。时间表达式为：[+/-{num}h+/-{num}m+/-{num}s@s,+/-{num}@h)。具体说明如下： – “[”表示包含边界。 – “)”表示不包含边界。 – “+”表示时间从当前时间开始往后算起，例如：当前时间是16：00，+1h则表示17：00。不建议使用“+”。 – “-”表示时间从当前时间往前算起，例如：当前时间时间是16：00，-1h则表示15：00. – “{num}”表示时间取值，为任意整数。逗号前后的时间差值不能超过24小时。 – “@”表示取整。@h：小时取整，分钟和秒忽略不计；@m：分钟取整，秒忽略不计；@s：秒取整。 时间表达式，举例如下： – 5分钟：[-5m@m,@m) – 15分钟：[-15m@m,@m) – 1小时：[-1h@h,@h) – 1天：[-24h@h,@h) – 自定义（不超过一天）：[-65m@h,-5m@h) **说明** 时间表达式最大值为调度间隔的五倍。
SQL超时	执行SQL分析操作失败时，自动重试的阈值。当超时时间超过指定的最大时间和超时次数超过最大次数时，该执行实例结束，状态为失败。 – SQL超时时间取值为60~180秒之间。 – SQL超时次数取值为1~10次之间。

步骤4 完成后，单击“确定”。

----结束

查看定时 SQL

步骤1 在“定时SQL”页签，单击目标作业名称进入详情页面，可查看定时SQL任务的基本信息和执行实例。

说明

每一个实例的上报的日志条数最多为100行。

----结束

修改定时 SQL

步骤1 在“定时SQL”页签，单击目标作业名称操作列对应的“修改”。

步骤2 在弹出的页面中，修改**表9-2**。

说明

定时SQL的任务名称和源日志组/流名称无法进行修改。

----结束

删除定时 SQL

步骤1 在“定时SQL”页签，单击目标作业名称操作列对应的“删除”。

或单击目标作业名称，进入定时SQL任务的基本信息页面中，单击右上角“删除”。

步骤2 在弹出的页面中，单击“确定”可删除定时SQL任务。

----结束

9.2 使用 FunctionGraph 服务提供的函数模板进行日志加工

云日志服务提供函数加工，您可以基于函数服务提供的函数模板或者自定义函数，实现日志规整、流转、脱敏、过滤等功能。

说明

目前此功能仅支持以下局点，其他局点需要提交工单申请使用。详细操作请参考**提交工单**。

华北-北京一、华北-北京四、华东-上海一、华东二、中国-香港、亚太-曼谷、亚太-新加坡、亚太-雅加达、非洲-约翰内斯堡、土耳其-伊斯坦布尔、拉美-墨西哥城一、拉美-墨西哥城二、拉美-圣保罗一、拉美-圣地亚哥

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“日志加工 >函数加工”，进入函数模板页面。

步骤3 根据实际需要，选择函数模板创建函数。

说明

具体的操作步骤，请参见**函数工作流《 用户指南 》**。

----结束

9.3 日志生成指标（ 邀测 ）

支持创建日志指标规则，将上报到LTS的日志数据提取为指标来统一管理，便于后续在应用运维管理控制台的指标浏览、仪表盘界面实时查看数据。

说明

目前此功能在邀测中，支持华北-北京四、华北-乌兰察布一局点，针对白名单用户内测使用，后续将全网开放，敬请期待！

背景信息

- 用户在LTS页面只需按照业务需要创建指标规则即可生成自己的统计报表，设置单个日志过滤条件或通过添加关联关系和添加组设置多个日志过滤条件，保留符合条件的日志，对用户特定时间范围内已结构化的日志进行动态统计，并将统计结果动态呈现到aom的Prometheus实例，操作简单且功能强大。
- 创建的每个指标规则只能生成一个结果，多个结果则需要创建多条指标规则。

前提条件

- 已在应用运维管理控制台创建Prometheus实例。
- 已将日志接入到LTS。
- 已配置结构化数据，当前仅支持已配置结构化的数据进行处理。

  说明

  日志生成指标要求日志时间的顺序偏差在较小范围内（5s统计频率允许偏差5s，1min统计频率允许偏差1min，5min统计频率允许偏差1min30s），建议优先使用ICAgent结构化方式上报日志，云端结构化方式会引起日志时间乱序严重从而导致无法在统计周期内处理日志，使得统计结果存在偏差。

限制条件

单个用户最多可创建10个日志指标规则，所有规则中添加的指标总数不能超过10。

创建日志指标规则

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“日志加工”。

步骤3 在“生成指标”页签，单击“创建规则”。

步骤4 配置日志的基本信息。

1. 填写规则名称，最多256位，只能包含字母、数字、下划线、中划线。
2. 填写描述信息。
3. 启用状态默认打开。
4. 默认勾选委托授权，创建日志生成指标任务，需要您授权LTS和AOM创建云服务委托：lts_admin_trust、aom_admin_trust
5. 任务监控，开启后会将每次任务执行状态写入日志流lts-system/lts-logtometric-statistics，您可以查看日志生成指标任务监控中心或者配置告警规则，及时发现加工过程中可能出现的异常问题。

步骤5 配置数据源。

1. 选择源日志组，若没有，则单击创建日志组。

   说明

   - 超出存储时间的日志将会被自动删除，您可以按需将日志数据转储至OBS桶中长期存储。
   - 如果您的日志尚未接入LTS，请参考**日志接入**，创建日志接入规则，并配置结构化解析规则。
2. 选择日志流，若没有，则单击创建日志流。

3. 日志采样，开启后会对日志源进行随机采样，采样率支持设置为0.1～0.9。

步骤6 配置指标存储位置。

1. 日志生成的指标会被存储到AOM中为自定义指标，请选择要存储的Prometheus实例。若没有，则单击创建实例。
2. 自定义日志生成指标的名称。只支持输入英文、数字、下划线、冒号，且不能以数字、下划线、冒号开头。
3. 填写指标含义。

步骤7 单击“下一步”。

步骤8 在“指标预览”下方预览信息。该预览信息是基于用户配置的日志过滤和统计规则，对日志流执行SQL查询模拟生成的指标结果，依赖用户先将日志采集到LTS，并配置好结构化解析规则和索引配置 ，否则此处预览结果展示为空。

步骤9 配置日志的统计方式。

1. 日志过滤的规则，设置完成后，支持预览效果。如果您无法在日志过滤和日志统计处选择到想要的日志字段，请您先在采集配置中配置好，详细操作请参考**设置云端结构化解析日志**。

   说明

   - 支持“或”“且”两种方式交互式过滤日志。
   - 不同字段支持的过滤规则不同。
   - 日志过滤和日志统计字段的类型仅支持string、float、long，不支持json。
   - 日志过滤是保留符合条件的日志，不符合条件的日志将被丢弃。
   - group by分组字段只支持字符串和整数类型。

2. 设置日志统计的字段，选择统计类型、支持选择或者自定义输入被统计的字段和分组字段。数据迟到1分钟，将不参与统计。

   说明

   - 支持以下统计类型：

     Count: 统计日志条数，CountKeyword: 统计关键词出现的次数， Sum: 统计指定字段求和值，Avg: 统计指定字段平均值，Max: 统计指定字段最大值，Min: 统计指定字段最小值，P50: 统计指定字段50%的值，P75: 统计指定字段75%的值，P90: 统计指定字段90%的值，P95: 统计指定字段95%的值，P99: 统计指定字段99%的值。
   - P系列统计类型是将数字排序后取xx%位置的值作为统计结果。
   - 日志统计是针对符合条件的日志进行操作，执行过程中会在日志组system生成一个日志流，如果删除该日志流将导致所有日志生成指标的规则执行详情无法查看。

3. 选择频率，支持5秒钟、1分钟、5分钟。频率不仅代表上报数据间隔，也代表统计操作的时间窗口，例如：频率5分钟具体含义为到达5分钟间隔后，取当前时间前5分钟数据进行统计操作并上报。
4. 设置完成后，根据查询中选择的内容自动生成维度。
5. 选择单位，例如选择角度、带宽、频率等数据的单位。

步骤10 （可选）单击“实时日志预览”查看实时日志。

步骤11 单击“确定”。

步骤12 创建成功后，在生成指标页签下方，新增一条规则记录。

说明

- 指标可视化和告警：创建成功后，您可以前往应用运维管理AOM控制台的仪表盘配置指标可视化图表，或者前往AOM告警规则配置指标告警。
- 建议每个日志流配置规则数量<= 5个。
- 在对应规则的操作列，支持复制、修改、删除规则。

----结束

10 LTS 配置中心管理

10.1 设置 LTS 日志采集配额和使用量预警

配置超额采集

当日志超过每月免费赠送的额度（500M）时，超过的部分将按需收费。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。

说明

- 该开关默认为开启状态，开启后表示当日志超过免费赠送的额度（500M）时，继续采集日志，超过的部分按需收费。
- 云日志服务的计费依据为日志使用量，包括日志读写、日志索引和日志存储。超过免费额度后，如果关闭日志采集开关，将无法再进行日志读写和索引，同时也不再产生日志读写和索引费用。关闭日志采集开关后，超额部分的日志继续存储在LTS，LTS收取日志存储费用，系统将根据配置的日志存储时间老化日志，日志老化后将不再产生任何费用。
- 云日志服务与应用运维管理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步关闭。

步骤1 登录**云日志服务控制台**。

步骤2 左侧导航选择“配置中心”，进入“配额设置”页面。

步骤3 选择关闭“超额继续采集日志”。

关闭后表示当日志超过每月免费赠送的额度(500M)时，将暂停采集日志。支持在日志总览页查看当前资源使用情况，详情请参考**查看日志管理**。

----结束

配置日志资源使用量预警

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。日志使用量包括日志读写流量、索引流量和标准存储量。

步骤1 在“配额设置”页签，单击“自定义日志资源使用量预警”开关。

开启后，云日志服务首页的资源统计数据将投递到自动创建的日志流下（lts-system/lts-resource-statistics），可以通过日志告警功能实现自定义日志资源使用量预警。

表 10-1 参数配置说明表

参数	说明
最近1小时日志读写流量	设置最近1小时内云日志服务的日志读写流量额度。默认值为1024GB，单位为GB，只能输入数字和小数点，保留4位小数，且不能以小数点开头和结尾，最小值为0，最大值输入长度不能超过10个字符。 当日志读写流量超过设置额度时，会触发日志告警功能。
最近1小时日志索引流量	设置最近1小时内云日志服务的日志索引流量额度。默认值为1024GB，单位为GB，只能输入数字和小数点，保留4位小数，且不能以小数点开头和结尾，最小值为0，最大值输入长度不能超过10个字符。 当日志索引流量超过设置额度时，会触发日志告警功能。
日志最新标准存储量	设置最近1小时日志的最新标准存储量额度。默认值为1024GB，单位为GB，只能输入数字和小数点，保留4位小数，且不能以小数点开头和结尾，最小值为0，最大值输入长度不能超过10个字符。 当日志最新标准存储量超过设置额度时，会触发日志告警功能。

说明

- 参数为“或”关系，当任意一个参数满足条件时，告警列表会产生一条告警。
- 该开关默认为关闭状态，当开启后表示当日志资源使用量超过1024GB时，会触发告警规则。
- 开启该开关后，默认会自动创建日志组/日志流（lts-system/lts-resource-statistics）和告警规则（log-statistics-alarm）；关闭该开关，则会自动删除告警规则（log-statistics-alarm）。
- 日志资源使用量会每小时统计一次。
- 系统自动创建一条告警规则（日志资源使用量预警），SQL告警语句为：select write_traffic,index_traffic,storage，条件表达为：write_traffic > 1024E12 || index_traffic > 1024E12 || storage > 1024E13，如果您希望产生的告警以短信、邮件等方式通知您，您可以修改告警规则配置发送通知。
- 如果告警规则不存在，重新开启自定义日志资源使用量预警开关，系统会默认创建规则。

----结束

10.2 设置 LTS 日志内容分词

通过配置分词可将日志内容按照分词符切分为多个单词，在日志搜索时可使用切分后的单词进行搜索。初次使用时，LTS已默认进行了分词配置，默认配置的分词符为：

```
, '";=()[]{}@&<>/:\\?\n\t\r
```

若默认分词符不能满足您的需求时，可按照如下操作进行自定义配置。

注意事项

- 分词配置只会对配置时间点以后生成的日志生效，之前的日志按照之前配置的分词符进行处理。
- 在“分词配置”页签设置分词符后会对当前Region区域内的所有日志流生效，若需要单独配置单个日志流的分词符，请参考**设置LTS日志索引配置**。

配置分词

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“配置中心”，选择“分词配置”页签。

步骤3 配置分词。

LTS提供了如下两种配置分词的方法。若同时使用了这两种配置方法，则分词符取并集。

- 自定义分词符：单击“编辑”，在文本框中自定义输入需要的分词符。
- 特殊分词符：单击“编辑 > 添加特殊分词符”，参考**ASCII码对照表**输入ASCII值。

步骤4 预览分词效果。

在文本框中输入待预览的日志内容，单击“预览”。

步骤5 预览确认配置无误后，单击“保存”。

说明

单击“重置”，可恢复到系统默认分词配置。

----结束

ASCII 码对照表

表 10-2 ASCII 码对照表

ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符
0	NUL（空字符）	32	空格	64	@	96	`

ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符
1	SOH（标题开始）	33	!	65	A	97	a
2	STX（正文开始）	34	"	66	B	98	b
3	ETX（正文结束）	35	#	67	C	99	c
4	EOT（传输结束）	36	$	68	D	100	d
5	ENQ（询问字符）	37	%	69	E	101	e
6	ACK（确认回应）	38	&	70	F	102	f
7	BEL（响铃）	39	'	71	G	103	g
8	BS（退格）	40	(	72	H	104	h
9	HT（水平定位符号，制表符）	41	)	73	I	105	i
10	LF（换行）	42	*	74	J	106	j
11	VT（垂直定位符号）	43	+	75	K	107	k
12	FF（换页键）	44	,	76	L	108	l
13	CR（归位键）	45	-	77	M	109	m
14	SO（取消变换）	46	.	78	N	110	n
15	SI（启用变换）	47	/	79	O	111	o
16	DLE（跳出数据通讯）	48	0	80	P	112	p
17	DC1（设备控制1）	49	1	81	Q	113	q
18	DC2（设备控制2）	50	2	82	R	114	r
19	DC3（设备控制3）	51	3	83	S	115	s

ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符	ASCII值	控制字符
20	DC4（设备控制4）	52	4	84	T	116	t
21	NAK（确认失败回应）	53	5	85	U	117	u
22	SYN（同步用暂停）	54	6	86	V	118	v
23	ETB（区块传输结束）	55	7	87	W	119	w
24	CAN（取消）	56	8	88	X	120	x
25	EM（连接介质中断）	57	9	89	Y	121	y
26	SUB（替换）	58	:	90	Z	122	z
27	ESC（跳出）	59	;	91	[	123	{
28	FS（文件分割符）	60	<	92	\	124	|
29	GS（组群分隔符）	61	=	93	]	125	}
30	RS（记录分隔符）	62	>	94	^	126	~
31	US（单元分隔符）	63	?	95	_	127	DEL（删除）

10.3 设置 ICAgent 日志采集开关

在“ICAgent采集开关”页签，支持设置ICAgent采集开关（控制ICAgent是否对日志数据进行采集）、采集Syslog日志到AOM、采集容器标准输出到AOM、ICAgent诊断开关。

设置采集开关

步骤1 登录云日志服务控制台。

步骤2 左侧导航选择“配置中心”，单击“ICAgent采集开关”。

步骤3 ICAgent采集开关是用来控制ICAgent是否对日志数据进行采集。

- “ICAgent采集开关”默认打开，当您不需要采集日志时，通过关闭“ICAgent采集开关”停止日志采集，以减少资源占用。
- “ICAgent采集开关”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。

步骤4 采集Syslog日志到AOM用来控制ICAgent是否采集Syslog日志到AOM1.0。开关关闭后，ICAgent将不会采集Syslog日志到AOM1.0，此功能仅支持5.12.182以上版本的ICAgent。

步骤5 采集容器标准输出到AOM。选择CCE集群，开启或关闭应用到该集群。开关关闭后，ICAgent将不会采集标准输出日志到AOM，此功能仅支持5.12.133以上版本的ICAgent。建议使用**云容器引擎CCE应用日志接入LTS**直接采集容器标准输出到LTS，不推荐采集到AOM。

步骤6 ICAgent诊断开关用来控制是否开启采集诊断功能。开关开启后ICAgent运行日志将上报到日志组/日志流lts-system/lts-icagent-statistics，然后您可以使用采集诊断功能查看ICAgent运行状态，及时发现异常情况，此功能仅支持5.12.196及以上版本的ICAgent。

----结束

11 查看 LTS 审计事件

概述

云审计服务（Cloud Trace Service，CTS）可以记录LTS相关的操作事件，便于日后的查询、审计和回溯。

开通了云审计服务后，系统开始记录LTS资源的操作。云审计服务管理控制台保存最近7天的操作记录。

开通云审计服务

云审计服务的开通请参见**开通云审计服务**。

开通云审计服务后，如果需要查看LTS相关操作事件，请参见**查询审计事件**。

云审计支持的 LTS 操作列表

表 11-1 云审计服务支持的 LTS 操作列表

操作名称	资源类型	事件名称
创建日志组	group	createLogGroup
修改日志组	group	updateLogGroup
删除日志组	group	deleteLogGroup
创建日志流	topic	createLogStream
修改日志流	topic	updateLogStream
删除日志流	topic	deleteLogStream
删除日志桶	logPailSetting	deleteLogPail
添加日志转储至OBS	als	addLogPailToOBS
修改日志转储至OBS	als	updateLogPailToOBS
删除日志转储至OBS	als	deleteLogPailToOBS

操作名称	资源类型	事件名称
批量启动暂停周期性日志转储	als	batchActionLogPailToOBS
创建指标过滤器	filter	createLogFilter
修改指标过滤器	filter	updateLogFilter
删除指标过滤器	filter	deleteLogFilter
修改指标过滤器状态	filter	updateLogFilterStatus
创建转储	transfer	createLogTransfer
修改转储	transfer	updateLogTransfer
删除转储	transfer	deleteLogTransfer
创建快速查询	searchCriteria	createLogSearchCriteria
修改快速查询	searchCriteria	updateLogSearchCriteria
删除快速查询	searchCriteria	deleteLogSearchCriteria
新增采集路径	LogAgent	createLogAgent
修改采集路径	LogAgent	updateLogAgent
删除采集路径	LogAgent	deleteLogAgent
创建结构化模板	structLogConfig	createLogStreamStructConfig
修改结构化模板	structLogConfig	updateLogStreamStructConfig
删除结构化模板	structLogConfig	deleteLogStreamStructConfig
创建快速分析	wordFreqConfig	updateWordFreqConfig
存储日志路径配置	path	addLogPath
添加统计规则	rule	addRuleStatistics
修改统计规则	rule	updateRuleStatistics
删除统计规则	rule	deleteRuleStatistics
创建结构化	structurization	addStructurization
删除结构化	structurization	deleteStructurization
添加kafka实例	dmsKafka	registerKafkaInfo
修改kafka实例	dmsKafka	updateKafkaInfo
删除kafka实例	dmsKafka	deleteKafkaInfo
创建dis转储	transfer	createDisTransfer

操作名称	资源类型	事件名称
修改dis转储	transfer	updateDisTransfer
删除dis转储	transfer	deleteDisTransfer
创建kafka转储	kafkaTransfer	createKafkaTransfer
修改kafka转储	kafkaTransfer	updateKafkaTransfer
删除kafka转储	kafkaTransfer	deleteKafkaTransfer
创建日志清洗	logFilter	createLogFilterRules
修改日志清洗	logFilter	updateLogFilterRules
删除日志清洗	logFilter	deleteLogFilterRules
创建图表	logChart	createLogChart
修改图表	logChart	updateLogChart
删除图表	logChart	deleteLogChart
创建仪表盘	logDashboard	createLogDashboard
修改仪表盘	logDashboard	updateLogDashboard
删除仪表盘	logDashboard	deleteLogDashboard
打开日志超额采集开关	LogCollectionSwitchOperation	LogCollectionSwitchOperation
关闭日志超额采集开关	LogCollectionSwitchOperation	LogCollectionSwitchOperation
创建ELB日志桶	elbPailType	createElbPail
修改ELB日志桶	elbPailType	updateElbPail
删除ELB日志桶	elbPailType	deleteElbPail
添加日志路径采集规则	logPathCollectionType	createLogPathCollection
修改日志路径采集规则	logPathCollectionType	updateLogPathCollection
删除日志路径采集规则	logPathCollectionType	deleteLogPathCollection
清理Redis缓存	cleanTenantResourceType	deleteCleanTenantResource

