ALIBABA CLOUD

Alibaba Cloud

日志服务

应用中心（App）

文档版本：20201120

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.日志审计服务

1.1. 简介

本文介绍日志审计服务的应用场景、技术优势及覆盖的云产品。

日志审计服务在继承现有日志服务所有功能外，还支持多账户下实时自动化、中心化采集云产品日志并进行审计，以及支持审计所需的存储、查询及信息汇总。覆盖基础（ActionTrail、容器服务Kubernetes版）、存储（OSS、NAS）、网络（SLB、API网关）、数据库（关系型数据库RDS、云原生分布式数据库PolarDB-X、PolarDB MySQL云原生数据库）、安全（WAF、云防火墙、云安全中心）等产品以及支持自由对接其他生态产品或自有SOC中心。

背景信息

- 日志审计是法律刚性需求。

  无论国内外，企业落实日志审计越来越迫切。尤其中国内地于2017年实施了《网络安全法》、于2019年12月实施《网络安全等保2.0标准》。

- 日志审计是客户安全合规依赖的基础。

  很多企业自身有成熟的法规条例以及合规审计团队，对账号设备操作、网络行为、日志进行审计。客户可以直接消费原生各类日志，也可以使用日志审计服务提供的审计功能，构建并输出合规的审计信息。如果客户有安全中心（SOC），则可以直接消费日志审计中的日志，也可以使用阿里云安全中心消费日志。

- 日志审计是安全防护的重要一环。

  根据FireEye M-Trends 2018报告，企业安全防护管理能力薄弱，尤其是亚太地区。全球范围内企业组织的攻击从发生到发现所需时长平均101天，而亚太地域平均需要498天。企业需要长期、可靠、无篡改的日志记录与审计支持来持续缩短这个时间。

应用场景

- 日志服务与审计场景

  日志服务作为行业领先的日志大数据解决方案，提供一站式数据采集、清洗、分析、可视化和告警功能。支持日志服务相关场景：DevOps、运营、安全、审计。

- 典型日志审计场景

  日志审计一般分成如下4层需求。

  - 基础需求：大部分中小企业客户需要自动化采集存储日志。他们的主要诉求是满足《网络安全等保2.0标准》中的最低要求，并脱离手工维护。
  - 高级需求：跨国企业、大企业以及部分中型企业，存在多个部门之间独立结算并且在阿里云账号的使用上各自隔离，但是在审计的时候，需要自动化、统一采集相关日志。他们的主要诉求是除上述的基础诉求外，还希望中心化采集日志并支持多个账号的简单管理。这部分企业一般拥有审计系统，因此对日志审计的需求是能够实时、简单的对接。

- 更上层的需求：拥有专门合规团队的大公司，他们需要对日志进行监控、告警和分析。一部分客户采集数据到审计系统中进行操作。另一部分客户（尤其是计划在云上搭建一套新审计系统的客户）可以使用日志服务提供的审计支持（查询、分析、告警、可视化等）进行审计操作。
- 最顶端需求：拥有专业成熟审计合规团队的大企业，一般拥有自己的安全中心或审计系统，他们的核心需求是对接数据进行统一操作。

针对以上4类客户需求，日志服务的日志审计服务都可以比较好的满足。

技术优势

- 中心化采集
  - 跨账号：支持将多个主账号下的日志采集到一个主账号下的Project中。
  - 一键式采集：一次性配置采集策略后，即可完成跨账号自动实时发现新资源（例如新创建的RDS、SLB、OSS Bucket实例等）并实时采集日志。
  - 中心化存储：将采集到的日志存储到某个地域的中心化Project中，方便后续查询分析、可视化与告警、二次开发等。
- 支持丰富的审计功能
  - 继承日志服务现有的所有功能，包括查询分析、加工、报表、告警、导出等功能，支持审计场景下中心化的审计等需求。
  - 生态开放对接：与开源软件、阿里云大数据产品、第三方SOC软件无缝对接，充分发挥数据价值。

云产品覆盖及相关资源

日志审计服务支持采集基础（ActionTrail、容器服务Kubernetes版）、存储（OSS、NAS）、网络（SLB、API网关）、数据库（关系型数据库RDS、云原生分布式数据库PolarDB-X、PolarDB MySQL云原生数据库）、安全（WAF、云防火墙、云安全中心）等云产品日志，采集完成后，会自动存储到对应Logstore中，并生成对应的仪表盘，详情如下表所示。

云产品	审计相关日志	采集地域	使用前提	日志服务资源
操作审计	RAM登录日志、阿里云产品的资源操作日志、通过OpenAPI的操作行为	所有在售地域	无	• Logstore名称 actiontrail_log • 仪表盘名称 ◦ ActionTrail审计中心 ◦ ActionTrail核心配置中心 ◦ ActionTrail登录中心
负载均衡	HTTP或HTTPS侦听实例的7层网络日志	所有在售地域	无	• Logstore名称 slb_log • 仪表盘名称 ◦ SLB审计中心 ◦ SLB访问中心 ◦ SLB全局数据

云产品	审计相关日志	采集地域	使用前提	日志服务资源
API网关	访问日志	所有在售地域	无	• Logstore名称 apigateway_log • 仪表盘名称 API网关审计中心

Web应用防火墙	访问日志、攻击日志	所有在售地域	• 高级版本及以上
			• 需在WAF控制台中购买**日志服务**模块。更多信息，请参见开通WAF日志服务。
				• Logstore名称
				waf_log
				• 仪表盘
				  ○ WAF审计中心
				  ○ WAF安全中心
				  ○ WAF访问中心

云安全中心	7种主机日志、4种网络日志、3种安全日志	所有在售地域	• 企业版本
			• 需在SAS控制台中开通**日志分析**功能。更多信息，请参见开通日志分析功能。
				• Logstore名称
				sas_log
				• 仪表盘名称
				  ○ 主机
				  ■ 账户快照
				  ■ 进程快照
				  ■ 网络连接中心
				  ○ 网络
				  ■ 网络会话
				  ■ DNS中心
				  ○ 安全
				  ■ Web访问漏洞中心
				  ■ 基线中心
				  ■ 安全告警中心

云防火墙	互联网流量日志	不涉及	• 高级版本及以上 • 需在云防火墙控制台中购买**日志分析**模块。更多信息，请参见开通日志分析功能。	• Logstore名称 cloudfirewall_log • 仪表盘名称 云防火墙审计中心
堡垒机	操作命令日志	华东1（杭州）、华东2（上海）、华南2（河源）、西南1（成都）	V3.2版本及以上	• Logstore名称 baston_log • 仪表盘名称 无

云产品	审计相关日志	采集地域	使用前提	日志服务资源
对象存储	资源操作日志、数据操作日志、数据访问日志、计量日志、过期文件删除日志、CDN回流日志	所有在售地域	无	• Logstore名称 oss_log • 仪表盘名称 ◦ OSS审计中心 ◦ OSS访问中心 ◦ OSS运维中心 ◦ OSS性能中心 ◦ OSS全局数据
关系数据库RDS	MySQL、SQL Server、PostgreSQL审计日志	• 中国：华北1（青岛）、华北2（北京）、华北3（张家口）、华北5（呼和浩特）、华东1（杭州）、华东2（上海）、华南1（深圳）、西南1（成都）、中国（香港） • 海外：新加坡、马来西亚（吉隆坡）、印度尼西亚（雅加达）、德国（法兰克福）、澳大利亚（悉尼）、印度（孟买）、日本（东京）	• MySQL：不支持基础版 • PostgreSQL、Microsoft SQL Server：无限制 • 均需开启SQL洞察或审计功能，由日志审计服务自动开启。	• Logstore名称 rds_log • 仪表盘名称 ◦ RDS审计中心 ◦ RDS审计安全中心 ◦ RDS审计性能中心 ◦ RDS全局数据
云原生分布式数据库PolarDB-X	审计日志	华北1（青岛）、华南1（深圳）、华东2（上海）、华北2（北京）、华东1（杭州）、华北3（张家口）、西南1（成都）、中国（香港）	无	• Logstore名称 drds_log • 仪表盘名称 ◦ PolarDB-X运营中心 ◦ PolarDB-X安全中心 ◦ PolarDB-X性能中心
PolarDB MySQL云原生数据库	PolarDB审计日志	华北1（青岛）、华北2（北京）、华东1（杭州）、华东2（上海）、华南1（深圳）、中国（香港）	需开启SQL洞察或审计功能，由日志审计服务自动开启。	• Logstore名称 polardb_log • 仪表盘名称 无

云产品	审计相关日志	采集地域	使用前提	日志服务资源
文件存储	访问日志	所有在售地域	无	• Logstore名称 nas_log • 仪表盘 ◦ NAS概览 ◦ NAS审计中心 ◦ NAS运维中心
移动推送	推送回调事件	中国内地	无	• Logstore名称 cps_log • 仪表盘名称 ◦ Android回执中心 ◦ iOS回执中心

云产品	审计相关日志	采集地域	使用前提	日志服务资源

容器服务Kubernetes版	• Kubernetes审计日志
	• Kubernetes事件中心
	• Ingress访问日志
		华东2（上海）、华北2（北京）、华东1（杭州）、华南1（深圳）、华北5（呼和浩特）、华北3（张家口）、西南1（成都）、中国（香港）	针对Kubernetes的采集，需要您先手动开通对应的日志采集功能。
			说明
			• 必须使用自动创建的专属Project（k8s-log-{ClusterID}），暂不支持自定义Project。
			• Kubernetes相关日志采集依赖于数据加工功能，会产生相应的加工费用。更多信息，请参见计费概述。
			• Kubernetes审计日志的使用前提请参见通过日志服务采集Kubernetes容器日志。
			• Kubernetes事件中心的使用前提请参见创建并使用Kubernetes事件中心。
			• Ingress访问日志的使用前提请参见Ingress访问日志分析与监控。
				• Logstore名称
				  ◦ k8s_log
				  ◦ k8s_ingress_log
				• 仪表盘名称
				  ◦ Kubernetes审计中心概览
				  ◦ Kubernetes事件中心
				  ◦ Kubernetes资源操作概览
				  ◦ Ingress概览
				  ◦ Ingress访问中心

1.2. 使用前须知

本文介绍日志审计服务的使用限制、费用说明等信息。

使用限制

- 存储方式与地域限制
  - 中心化存储

    从各个主账号的各个地域采集到的日志，会存储到中心主账号下的一个中心化Project中，目前中心化存储可供选择的地域如下所示。

    - 中国：华北2（北京）、华北5（呼和浩特）、华东1（杭州）、华东2（上海）、华南1（深圳）

    - 海外：新加坡、日本（东京）
  - 区域化存储

    对于SLB、OSS、PolarDB-X的访问日志，日志审计服务支持将各个主账号采集到的日志存储到中心主账号下的各个与SLB、OSS、PolarDB-X实例处于相同地域的日志服务Project中（例如：杭州的OSS访问日志，存储到杭州的日志服务Project中）。
  - 同步到中心

    对于SLB、OSS、PolarDB-X的区域化存储，支持将各个地域的Logstore同步到一个中心化的Logstore中，以便做中心化查询、分析、告警、可视化、二次开发等。

    同步机制依赖日志服务数据加工，支持的地域：支持除华北1（青岛）、华南2（河源）外的所有地域。
- 资源限制
  - 中心主账号下对应的中心化Project只有一个，名为slsaudit-center-*中心化主账号ID-配置的地域*，例如：slsaudit-center-1234567890-cn-beijing。无法通过控制台删除中心化Project，只能通过命令行、API删除。
  - 对于SLB、OSS、PolarDB-X，可以有多个区域化Project，名为slsaudit-region-*中心化主账号ID-各个采集的地域*，例如：slsaudit-region-1234567890-cn-beijing。无法通过控制台删除区域化Project，只能通过命令行、API删除。
  - 配置云产品日志采集后，日志审计服务会创建专属Logstore，具备日志服务Logstore所有的功能，除以下操作限制。
    - 保护数据不被篡改，您无法自行写入数据，修改或删除索引。
    - 只能通过日志审计服务的配置页面或接口修改存储周期、删除Logstore。
    - 对于SLB、OSS、PolarDB-X，如果开启了**同步到中心**功能，在对应的区域化Project中，会生成数据加工任务。
      - 数据加工任务名为Internal Job: SLS Audit Service Data Sync for OSS Access、Internal Job: SLS Audit Service Data Sync for SLB、Internal Job: SLS Audit Service Data Sync for DRDS。
      - 您只能通过日志审计服务的配置页面或接口关闭该数据加工任务。
      - 开启了**同步到中心**功能的区域化Logstore会变成同步专属的Logstore，您无法进行任何操作，如果需要查询等操作时，可以直接在中心化Logstore中操作。

费用说明

- 日志服务

  中心主账号需要开通日志服务与日志审计服务App，从其他主账号采集日志到中心主账号下。除特定云产品日志依赖外，其他主账号默认无需开通日志服务，也不会在其账号的日志服务下产生特定费用。目前日志审计服务免费，其涉及的数据存储、读写流量、数据加工等按量付费，详情请参见计费概述。

  > **说明** 特定云产品（例如负载均衡SLB、对象存储OSS、云原生分布式数据库PolarDB-X、容器服务Kubernetes版）的日志，在开启同步到中心后，会使用数据加工功能进行同步，其涉及的加工与跨网流量费用等按量付费，详情请参见计费概述。

  支持免费额度，支持用已购买的资源包抵扣相应的费用。
- 云产品

  开通日志审计服务与对应云产品的日志采集后，在云产品侧可能会产生额外的费用，如下所示。

云产品	额外费用
Web应用防火墙（WAF）	在Web应用防火墙控制台上购买**日志服务**模块，费用详情请参见计费方式。
云安全中心（SAS）	在云安全中心控制台开通**日志分析**功能，费用详情请参见计费模式。
云防火墙（Coud Firewall）	在云防火墙控制台上购买**日志分析**模块，费用详情请参见日志分析计费方式。
关系数据库（RDS）	开启RDS日志采集功能后，会自动开启符合条件的RDS实例的SQL洞察（SQL审计）功能，费用详情请参见价格、收费项与计费方式。
PolarDB MySQL云原生数据库	开启PolarDB MySQL云原生数据库日志采集功能后，会自动开启符合条件的PolarDB MySQL集群的SQL洞察（SQL审计）功能，费用详情请参见SQL洞察价格。

1.3. 配置日志采集

本文介绍如何在日志审计服务中选择云产品进行日志采集。

前提条件

- 已注册阿里云账号。

  建议使用阿里云RAM用户，该RAM用户需具备RAM读权限（例如已被授权AliyunRAMReadOnlyAccess策略），且对日志服务有读写权限（例如被授权AliyunLogFullAccess策略）。

- 已开通日志服务。

  首次登录日志服务控制台时，根据页面提示开通日志服务。

- 待采集日志的云产品已开启相应的服务，详情请参见云产品覆盖及相关资源。

首次配置

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**日志审计服务**中的**进入应用**。
3. 在**云产品接入 > 全局配置**页面，配置如下信息。
   i. 在**中心项目Project所在区域**下拉列表中，选择日志中心化存储的目标地域。目前支持华北2（北京）、华北5（呼和浩特）、华东1（杭州）、华东2（上海）、华南1（深圳）、新加坡、日本（东京）。
   ii. 在云产品列表中，选择需开启日志审计功能的云产品，并配置存储时间。如果是SLB 7层访问日志、OSS访问日志、PolarDB-X审计日志，还可以选择**同步到中心**。开启**同步到中心**后，区域化Project将作为中转，不需要存储很长时间，控制台会自动调整成推荐的时间。
   iii. 配置采集同步授权。日志审计服务支持手动授权和通过账号密钥辅助授权。
      - 手动授权：详情请参见同一账号：手动授权。
      - 通过账号密钥辅助授权：输入账号的AK信息，AK信息不会被保存，仅临时使用。

        此处AK对应的RAM用户需具备RAM读写权限（例如已被授权AliyunRAMFullAccess策略）。

   iv. 单击**确定**。

4. 在左侧导航栏，选择**云产品接入 > 接入状态**，查看日志接入状态。配置完成后，需要2分钟左右完成初始同步。如果出现异常，请根据页面提示信息进行调整，详情请参见常见问题及错误排查。

配置多账号

日志审计服务支持跨账号采集云产品日志到当前账号下的日志库中。在开始采集前，您需要先完成多账号配置。

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**日志审计服务**中的**进入应用**。
3. 在**多账号配置 > 全局配置**页面，配置如下信息。日志审计服务支持手动授权和通过账号密钥服务授权。
   - 手动授权：输入主账号ID，可配置多个。对应的账号权限配置请参见多账号配置：手动授权。
   - 通过账号密钥辅助授权：在**其他账号授权日志服务采集**文本框中输入其他账号的AK信息及其主账号ID。AK信息不会被保存，仅临时使用。

     此处AK对应的RAM用户需具备RAM读写权限（例如已被授权AliyunRAMFullAccess策略）。
4. 在左侧导航栏，选择**云产品接入 > 接入状态**，查看日志接入状态。配置完成后，需要2分钟左右完成初始同步。如果出现异常，请根据页面提示信息进行调整，详情请参见常见问题及错误排查。

停止采集日志

如果您不再需要采集云产品日志但想要保留已采集的日志，可参见以下步骤。

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**日志审计服务**中的**进入应用**。
3. 在**云产品接入 > 全局配置**页面，单击右上角的**修改**。
4. 关闭目标日志选项，单击**确定**。

删除审计资源

如果您需要清理并删除日志审计服务相关的所有日志资源（如Logstore、仪表盘、告警等），可参见以下操作。

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**日志审计服务**中的**进入应用**。
3. 在**云产品接入 > 全局配置**页面，单击右上角的**删除审计资源**。
4. 根据页面提示，完成删除。

常见问题及错误排查

- 如何查看接入状态？

  在**云产品接入 > 接入状态**中查看接入状态。
- 显示账号没有权限或密钥错误，怎么处理？

  请检查账号权限是否配置正确。如果是同一账号下的采集，请参见同一账号：手动授权，如果是跨账号采集，请参见多账号配置：手动授权。例如：账号中的sls-audit-service-monitor角色没有被授予**系统策略**下的**ReadOnlyAccess**策略。
- 显示账号没有开启特定服务，怎么处理？

一般是由于某个云产品没有开启特定服务，详情请参见云产品覆盖及相关资源，例如：已开通云安全中心，但未开通**日志分析**功能。

1.4. 审计操作

本文介绍日志审计服务在采集到日志后的审计操作。

前提条件

- 已完成日志审计配置，详情请参见配置日志采集。
- 已有对应权限的账号，权限配置请参见配置权限助手。
  - 如果您需要查询日志、查看报表，则当前登录的账号需要对日志审计服务以及Project下的资源具有读权限。
  - 如果您需要创建报表、创建告警、二次对接，则当前登录的账号需要对日志审计服务以及Project下的资源具有读写权限。

使用审计报表

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**日志审计服务**中的**进入应用**。
3. 在左侧导航栏中，单击**审计报表**。
4. 单击目标报表，进入审计中心。您可以在审计中心查看数据报表，仪表盘操作请参见仪表盘。

> **说明** 对于OSS、SLB和PolarDB-X，如果没有在**全局配置**中开启**同步到中心**功能，则只能在**区域化**页签中查看各个地域下的报表。如果开启了**同步到中心**功能，则可在**中心化**页签中查看除华北1（青岛）、华南2（河源）外的报表，地域限制请参见简介。

使用审计查询

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**日志审计服务**中的**进入应用**。
3. 在左侧导航栏中，单击**审计查询**。
4. 单击目标云产品，进入查询分析页面。具体的查询、分析操作请参见查询与分析。

> **说明** 对于OSS、SLB和DRDS，如果没有在**全局配置**中开启**同步到中心**功能，则只能在**区域化**页签中查看各个地域下的日志。如果开启了**同步到中心**功能，则可在**中心化**页签中查看除华北1（青岛）、华南2（河源）外的日志，地域限制请参见简介。

创建审计报警

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**日志审计服务**中的**进入应用**。
3. 创建告警。
   - 基于日志创建告警
     a. 在左侧导航栏中，单击**审计查询**。
     b. 单击目标云产品，进入查询分析页面。

c. 单击**另存为告警**创建告警，详情请参见配置告警。

- 基于报表创建告警
  a. 在左侧导航栏中，单击**审计报表**。
  b. 单击目标报表，进入仪表盘页面。
  c. 选择目标图表，单击 > **新建告警**创建告警，详情请参见配置告警。

操作Logstore

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**日志审计服务**中的**进入应用**。
3. 单击**审计配置** > **云产品接入** > **全局配置**。
4. 单击Project名称，进入日志库列表页面。

后续步骤

完成日志审计后，可通过数据消费、数据投递功能将日志与第三方系统进行对接。

- 数据投递

  使用数据投递与第三方系统对接，包括OSS、MaxCompute、AnalyticDB for MySQL、TSDB、Splunk或其他SIEM，详情请参见数据投递。

- 数据消费

  使用第三方流计算系统实时消费日志，包括Storm、Flume、ARMS、Blink、Logstash、Spark streaming、Cloud Monitor或消费组等，详情请参见实时消费。

1.5. 手动授权日志采集与同步

在使用日志审计服务时，需先授予日志服务采集相关云产品日志的权限以及授权多个主账号之间的同步汇集。您可以在配置日志采集时使用具备特定权限的子账号的密钥直接完成授权，或者参考本文的操作步骤完成授权。

背景信息

日志审计服务支持采集同一主账号下的云产品日志，也支持跨主账号采集云产品日志。

进行跨账号采集云产品日志时，当前主账号和其他主账号需要进行双向授权。

- 当前主账号允许其他账号同步数据到当前主账号的审计Logstore。
- 其他主账号允许同步数据到当前主账号的审计Logstore。

使用日志审计服务涉及多个授权角色和策略，对应关系如下所示：

- 当前主账号

角色	权限策略
sls-audit-service-dispatch	AliyunLogAuditServiceDispatchPolicy

角色	权限策略
sls-audit-service-monitor	○ ReadOnlyAccess ○ AliyunLogAuditServiceMonitorAccess ○ AliyunLogAuditServiceK8sAccess（仅开启Kubernetes采集时需要配置）

- 其他主账号

角色	权限策略
sls-audit-service-monitor	○ ReadOnlyAccess ○ AliyunLogAuditServiceMonitorAccess ○ AliyunLogAuditServiceK8sAccess（仅开启Kubernetes采集时需要配置）

同一账号：手动授权

1. 登录RAM 控制台。建议使用子账号登录，且该子账号需具备RAM读写权限（例如已被授予AliyunRAMFullAccess策略）。
2. 创建AliyunLogAuditServiceDispatchPolicy策略。
   i. 在左侧导航栏中，选择**权限管理 > 权限策略管理**，单击**创建权限策略**。
   ii. 在**新建自定义权限策略**页面，配置如下参数，并单击**确定**。

参数	说明
策略名称	配置为**AliyunLogAuditServiceDispatchPolicy**。
配置模式	选择**脚本配置**。

策略内容	将配置框中的原有脚本替换为如下内容。
	{
	"Version": "1",
	"Statement": [
	{
	"Action": "log:*",
	"Resource": [
	"acs:log:*:*:project/slsaudit-*"
	],
	"Effect": "Allow"
	}
	]
	}

3. 参见步骤2，创建AliyunLogAuditServiceMonitorAccess策略。参数配置如下所示。

参数	说明
策略名称	配置为**AliyunLogAuditServiceMonitorAccess**。
配置模式	选择**脚本配置**。

策略内容	将配置框中的原有脚本替换为如下内容。
	{
	"Version": "1",
	"Statement": [
	{
	"Action": "log:*",
	"Resource": [
	"acs:log:*:*:project/slsaudit-*",
	"acs:log:*:*:app/audit"
	],
	"Effect": "Allow"
	},
	{
	"Action": [
	"rds:ModifySQLCollectorPolicy",
	"vpc:*FlowLog*",
	"drds:*SqlAudit*",
	"kvstore:ModifyAuditLogConfig",
	"polardb:ModifyDBClusterAuditLogCollector"
	],
	"Resource": "*",
	"Effect": "Allow"
	}
	]
	}

> **说明** 如果您要采集Kubernetes数据，还需创建AliyunLogAuditServiceK8sAccess策略，策略内容如下所示。创建成功后，还需创建sls-audit-service-monitor角色并授予AliyunLogAuditServiceK8sAccess，详情请参见步骤5。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "log:*",
      "Resource": [
        "acs:log:*:*:project/k8s-log-*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

4. 创建sls-audit-service-dispatch角色并授予AliyunLogAuditServiceDispatchPolicy策略。
   i. 在左侧导航栏中，选择**RAM角色管理**，单击**创建RAM角色**。
   ii. 在**选择类型**页签中，选择**阿里云服务**，单击**下一步**。

iii. 在**配置角色**页签中，配置如下参数后，单击**完成**。

参数	说明
角色类型	选择**普通服务角色**。
角色名称	配置为sls-audit-service-dispatch。

选择受信服务	选择**日志服务**，对应的信任策略如下所示。
	{
	"Statement": [
	{
	"Action": "sts:AssumeRole",
	"Effect": "Allow",
	"Principal": {
	"Service": [
	"log.aliyuncs.com"
	]
	}
	}
	],
	"Version": "1"
	}

iv. 单击**为角色授权**。

v. 在**添加权限**页面，进行授权。选择**自定义策略**下的AliyunLogAuditServiceDispatchPolicy策略。

5. 创建sls-audit-service-monitor角色并授予AliyunLogAuditServiceMonitorAccess策略。

i. 在左侧导航栏中，选择**RAM角色管理**，单击**创建RAM角色**。

ii. 在**选择类型**页签中，选择**阿里云服务**，单击**下一步**。

iii. 在**配置角色**页签中，配置如下参数，单击**完成**。

参数	说明
角色类型	选择**普通服务角色**。
角色名称	配置为sls-audit-service-monitor。

选择受信服务	选择**日志服务**，对应的信任策略如下所示。
	{
	"Statement": [
	{
	"Action": "sts:AssumeRole",
	"Effect": "Allow",
	"Principal": {
	"Service": [
	"log.aliyuncs.com"
	]
	}
	}
	],
	"Version": "1"
	}

iv. 单击**为角色授权**。

v. 在**添加权限**页面，进行授权。选择**自定义策略**下的AliyunLogAuditServiceMonitorAccess策略和**系统策略**下的ReadOnlyAccess策略。

多账号配置：手动授权

1. 获取主账号ID。
   i. 登录账号管理控制台。使用当前主账号和其他主账号分别登录获取主账号ID。
   ii. 在**安全设置**页面，获取账号ID。
2. 配置当前主账号。
   i. 登录RAM 控制台。建议使用子账号登录，且该子账号需具备RAM读写权限（例如已被授予*AliyunRAMFullAccess*策略）。
   ii. 单击**RAM角色管理**。
   iii. 找到并单击sls-audit-service-dispatch角色，进入详情页面。

iv. 在**信任策略管理**页签，将配置框中的原有脚本替换为如下内容。

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "log.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}
```

3. 配置其他主账号。

i. 登录RAM 控制台。建议使用子账号登录，且该子账号需具备RAM读写权限（例如已被授予*AliyunRAMFullAccess*策略）。

ii. 在左侧导航栏中，选择**权限管理 > 权限策略管理**，单击**创建权限策略**。

iii. 在**新建自定义权限策略**页面，配置如下参数，并单击**确定**。

参数	说明
策略名称	配置为AliyunLogAuditServiceMonitorAccess。
配置模式	选择**脚本配置**。
	将配置框中的原有脚本替换为如下内容。

参数	说明

策略内容	{
	"Version": "1",
	"Statement": [
	{
	"Action": "log:*",
	"Resource": [
	"acs:log:*:*:project/slsaudit-*",
	"acs:log:*:*:app/audit"
	],
	"Effect": "Allow"
	},
	{
	"Action": [
	"rds:ModifySQLCollectorPolicy",
	"vpc:*FlowLog*",
	"drds:*SqlAudit*",
	"kvstore:ModifyAuditLogConfig",
	"polardb:ModifyDBClusterAuditLogCollector"
	],
	"Resource": "*",
	"Effect": "Allow"
	}
	]
	}

> **说明** 如果您要采集Kubernetes数据，还需创建*AliyunLogAuditServiceK8sAccess*策略，策略内容如下所示。创建成功后，还需创建*sls-audit-service-monitor*角色并授予*AliyunLogAuditServiceK8sAccess*，详情请参见步骤3.iv。

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": "log:*",
      "Resource": [
        "acs:log:*:*:project/k8s-log-*"
      ],
      "Effect": "Allow"
    }
  ]
}
```

iv. 创建*sls-audit-service-monitor*角色并授予*AliyunLogAuditServiceMonitorAccess*策略。

a. 在左侧导航栏中，选择**RAM角色管理**，单击**创建RAM角色**。

b. 在**选择类型**页签中，选择**阿里云服务**，单击**下一步**。

c. 在**配置角色**页签中，配置如下参数后，单击**完成**。

参数	说明
角色类型	选择**普通服务角色**。
角色名称	配置为sls-audit-service-monitor。
选择受信服务	选择**日志服务**。

d. 单击**为角色授权**。

e. 在**添加权限**页面，进行授权。

选择**自定义策略**下的AliyunLogAuditServiceMonitorAccess策略和**系统策略**下的ReadOnlyAccess策略。

f. 返回**RAM角色管理**页面，单击sls-audit-service-monitor角色。

g. 在**信任策略管理**页签，将配置框中的原有脚本替换为如下内容。

其中，中心主账号ID请根据步骤1中获取的当前主账号ID进行替换。

```
{
  "Statement": [
    {
      "Action": "sts:AssumeRole",
      "Effect": "Allow",
      "Principal": {
        "Service": [
          "中心主账号ID@log.aliyuncs.com",
          "log.aliyuncs.com"
        ]
      }
    }
  ],
  "Version": "1"
}
```

1.6. 日志字段详情

本文列举了云产品日志的字段详情。

操作审计（ActionTrail）

日志字段	说明
__topic__	日志主题，固定为actiontrail_event
owner_id	主账号ID
event	事件主体，JSON格式，事件主体的内容随事件变化。
event.eventId	事件ID，事件的唯一标示
event.eventName	事件名称
event.eventSource	事件来源
event.eventType	事件类型
event.eventVersion	ActionTrail的数据格式版本，固定为1
event.acsRegion	事件所在的地域
event.requestId	操作云产品的请求ID
event.apiVersion	相关API的版本

日志字段	说明
event.errorMessage	事件失败的错误信息
event.serviceName	事件相关服务名称
event.sourceIpAddress	事件相关的源IP地址
event.userAgent	事件相关的客户端Agent
event.requestParameters.HostId	请求参数中的主机ID
event.requestParameters.Name	请求参数中的名称
event.requestParameters.Region	请求参数中的域
event.userIdentity.accessKeyId	请求所使用的AccessKey ID
event.userIdentity.accountId	请求账户的ID
event.userIdentity.principalId	请求相关账户的凭证ID
event.userIdentity.type	请求相关账户的类型
event.userIdentity.userName	请求相关账户的账户名
event.errorCode	事件失败的错误码
addionalEventData.isMFAChecked	登录账号是否开启MFA
addionalEventData.loginAccount	登录账号

负载均衡（SLB）

日志字段	说明
owner_id	主账号ID
region	实例所在地域
instance_id	实例ID
instance_name	实例名
network_type	网络类型，包括VPC、Classic
vpc_id	VPC ID
body_bytes_sent	发送给客户端的http body的字节数。
client_ip	请求客户端IP地址

日志字段	说明
client_port	请求客户端端口
host	优先从request请求参数中获取host，如果获取不到，则从host header中取值，如果还是获取不到，则以处理请求的后端服务器IP作为host。
http_host	请求报文host header的内容。
http_referer	proxy收到的请求报文中http的referer header的内容。
http_user_agent	proxy收到的请求报文中http的user-agent header的内容。
http_x_forwarded_for	proxy收到的请求报文中x-forwarded-for header的内容。
http_x_real_ip	真实的客户端IP地址
read_request_time	proxy读取request时间，单位：毫秒
request_length	请求报文的长度，包括startline、http头报文和http body。
request_method	请求报文的方法
request_time	proxy收到第一个请求报文的时间到proxy返回应答之间的间隔时间，单位：秒。
request_uri	proxy收到的请求报文的URI。
scheme	请求的schema，例如：http或https
server_protocol	proxy收到的http协议的版本，例如HTTP/1.0或HTTP/1.1。
slb_vport	SLB的监听端口
slbid	SLB实例ID
ssl_cipher	使用的cipher，例如ECDHE-RSA-AES128-GCM-SHA256。
ssl_protocol	建立SSL连接使用的协议，例如TLSv1.2。
status	proxy应答报文的状态
tcpinfo_rtt	客户端的tcp rtt时间，单位：微秒
time	日志记录时间
upstream_addr	后端服务器的IP地址和端口
upstream_response_time	从SLB向后端建立连接开始到接受完数据然后关闭连接为止的时间，单位：秒。
upstream_status	proxy收到的后端服务器的响应状态码。
vip_addr	vip地址

日志字段	说明
write_response_time	proxy写的响应时间，单位：毫秒

API网关

日志字段	说明
owner_id	API提供者的帐户ID
apiGroupUid	API的分组ID
apiGroupName	API分组名称
apiUid	API ID
apiName	API名称
apiStageUid	API环境ID
apiStageName	API环境名称
httpMethod	调用的HTTP方法
path	请求的PATH
domain	调用的域名
statusCode	Http的状态码
errorMessage	错误信息
appId	调用者应用ID
appName	调用者应用名称
clientIp	调用者客户端IP
exception	后端返回的具体错误信息
region	地域，例如cn-hangzhou
requestHandleTime	请求时间，格林威治时间
requestId	请求ID，全局唯一
requestSize	请求大小，单位：字节
responseSize	返回数据大小，单位：字节
serviceLatency	后端延迟，单位：毫秒

Web应用防火墙（WAF）

字段	说明
__topic__	日志主题，固定为waf_access_log。
owner_id	阿里云主账号ID。
acl_action	WAF精准访问控制规则行为，例如pass、drop、captcha。 **说明** 空值或短划线（-）也表示pass。
acl_blocks	是否被精准访问控制规则拦截，包括： • 1表示拦截。 • 其他值均表示通过。
antibot	触发的爬虫风险管理防护策略类型。 • ratelimit：频次控制 • sdk：APP端增强防护 • algorithm：算法模型 • intelligence：爬虫情报 • acl：精准访问控制 • blacklist：黑名单
antibot_action	爬虫风险管理防护策略执行的操作。 • challenge：嵌入JS进行验证 • drop：拦截 • report：记录 • captcha：滑块验证
block_action	触发拦截的WAF防护类型。 • tmd：CC攻击防护 • waf：Web应用攻击防护 • acl：精准访问控制 • geo：地区封禁 • antifraud：数据风控 • antibot：防爬封禁
body_bytes_sent	发送给客户端的HTTP Body的字节数。
cc_action	CC防护策略行为，例如none、challenge、pass、close、captcha、wait、login、n等。
cc_blocks	是否被CC防护功能拦截，包括： • 1表示拦截。 • 其他值均表示通过。

字段	说明
cc_phase	触发的CC防护策略，包括seccookie、server_ip_blacklist、static_whitelist、server_header_blacklist、server_cookie_blacklist、server_args_blacklist、qps_overmax等。
content_type	访问请求内容类型。
host	源站服务器。
http_cookie	访问请求头部中带有的访问来源客户端Cookie信息。
http_referer	访问请求头部中带有的访问请求的来源URL信息。如果无来源URL信息，则显示为短划线（-）。
http_user_agent	访问请求头部中的User Agent字段，一般包含来源客户端浏览器标识、操作系统标识等信息。
http_x_forwarded_for	访问请求头部中带有的XFF头信息，用于识别通过HTTP代理或负载均衡方式连接到Web服务器的客户端最原始的IP地址。
https	访问请求是否为HTTPS请求。 • true：HTTPS请求 • false：HTTP请求
matched_host	匹配到的已接入WAF防护配置的域名，可能是泛域名。如果无法匹配到相关域名配置，则显示短划线（-）。
querystring	请求中的查询字符串。
real_client_ip	访问的客户端的真实IP地址。如果无法获取，则显示为短划线（-）。
region	WAF实例地域信息。
remote_addr	访问请求的客户端IP地址。
remote_port	访问请求的客户端端口。
request_length	访问请求长度，单位：字节。
request_method	访问请求的HTTP请求方法。
request_path	请求的相对路径（不包含查询字符串）。
request_time_msec	访问请求时间，单位：毫秒。
request_traceid	WAF记录的访问请求唯一ID标识。
server_protocol	源站服务器响应的协议及版本号。
status	WAF返回给客户端的HTTP响应状态信息。
time	访问请求的发生时间。

字段	说明
ua_browser	访问请求来源的浏览器信息。
ua_browser_family	访问请求来源所属浏览器系列。
ua_browser_type	访问请求来源的浏览器类型。
ua_browser_version	访问请求来源的浏览器版本。
ua_device_type	访问请求来源客户端的设备类型。
ua_os	访问请求来源客户端的操作系统信息。
ua_os_family	访问请求来源客户端所属操作系统系列。
upstream_addr	WAF使用的回源地址列表，格式为IP:Port，多个地址用逗号分隔。
upstream_ip	访问请求所对应的源站IP。例如，WAF回源到ECS的情况，该参数即返回源站ECS的IP。
upstream_response_time	源站响应WAF请求的时间，单位：秒。如果返回短划线（-），代表响应超时。
upstream_status	源站返回给WAF的响应状态。如果返回短划线（-），表示没有响应，例如该请求被WAF拦截。
user_id	阿里云主账号ID。
waf_action	Web攻击防护策略行为，block：表示拦截，bypass或其它值均表示放行。
web_attack_type	Web攻击类型，例如xss、code_exec、webshell、sqli、lfilei、rfilei、other等。
waf_rule_id	匹配的WAF的相关规则ID。
ssl_cipher	SSL加密套件。
ssl_protocol	SSL协议版本。

云安全中心（SAS）

- 网络日志
  - DNS日志

日志字段	说明
__topic__	主题，固定为sas-log-dns
owner_id	阿里云主账号ID
additional	additional字段，竖线分隔

日志字段	说明
additional_num	additional字段数量
answer	DNS回答信息，竖线分隔
answer_num	DNS回答信息数量
authority	authority字段
authority_num	authority字段数量
client_subnet	客户端子网
dst_ip	目标IP地址
dst_port	目标端口
in_out	数据的传输方向 ■ in：入方式 ■ out：出方向
qid	查询ID
qname	查询域名
qtype	查询类型
query_datetime	查询时间戳，单位：毫秒
rcode	返回代码
region	来源区域ID ■ 1：北京 ■ 2：青岛 ■ 3：杭州 ■ 4：上海 ■ 5：深圳 ■ 6：其它
response_datetime	返回时间
src_ip	源IP地址
src_port	源端口

- 本地DNS日志

字段名	名称
__topic__	主题，固定为local-dns
owner_id	阿里云主账号ID
answer_rda	DNS回答信息，竖线分隔
answer_ttl	DNS回答的时间周期，竖线分隔
answer_type	DNS回答的类型，竖线分隔
anwser_name	DNS回答的名称，竖线分隔
dest_ip	目标IP地址
dest_port	目标端口
group_id	分组ID
hostname	主机名
id	主机IP地址
instance_id	实例ID
internet_ip	互联网IP地址
ip_ttl	IP的周期
query_name	查询域名
query_type	查询类型
src_ip	源IP地址
src_port	源端口
time	查询时间戳，单位：秒
time_usecond	响应耗时，单位：微秒
tunnel_id	通道ID

- 网络会话日志

日志字段	说明
__topic__	日志主题，固定为sas-log-session
owner_id	阿里云主账号ID
asset_type	关联的资产类型，例如ECS、SLB、RDS等
dst_ip	目标IP地址
dst_port	目标端口
proto	协议类型，例如tcp、udp
session_time	Session时间
src_ip	源IP地址
src_port	源端口

- Web日志

日志字段	说明
__topic__	日志主题，固定为sas-log-http
owner_id	阿里云主账号ID
content_length	内容长度
dst_ip	目标IP地址
dst_port	目标端口
host	访问主机名
jump_location	重定向地址
method	HTTP访问
referer	客户端向服务器发送请求时的HTTP referer，告知服务器访问来源的HTTP链接。
request_datetime	请求时间
ret_code	返回状态值
rqs_content_type	请求内容类型
rsp_content_type	响应内容类型
src_ip	源IP地址
src_port	源端口
uri	请求URI
user_agent	向用户客户端发起的请求
x_forward_for	路由跳转信息

- 安全日志

- 漏洞日志

日志字段	说明
__topic__	日志主题，固定为sas-vul-log
owner_id	阿里云主账号ID
name	漏洞名称
alias_name	漏洞别名
op	操作信息 ■ new：新增 ■ verify：验证 ■ fix：修复
status	状态信息，请参见安全日志状态码。
tag	漏洞标签，例如oval、system、cms，主要用于区分EMG紧急漏洞。
type	漏洞类型 ■ sys：windows漏洞 ■ cve：Linux漏洞 ■ cms：Web CMS漏洞 ■ EMG：紧急漏洞
uuid	客户端号

- 基线日志

日志字段	说明
__topic__	日志主题，固定为sas-hc-log
owner_id	阿里云主账号ID
level	级别，例如low、mediam、high
op	操作信息 ■ new：新增 ■ verify：验证
risk_name	风险名称
status	状态信息，请参见安全日志状态码。
sub_type_alias	子类型别名，中文
sub_type_name	子类型名称

日志字段	说明
type_name	类型名称
type_alias	类型别名，中文
uuid	客户端号
check_item	检查项名称
check_level	检查项级别
check_type	检查项类型

基线type-sub-type列表

type_name	sub_type_name
system	baseline
weak_password	postsql_weak_password
database	redis_check
account	system_account_security
account	system_account_security
weak_password	mysq_weak_password
weak_password	ftp_anonymous
weak_password	rdp_weak_password
system	group_policy
system	register
account	system_account_security
weak_password	sqlserver_weak_password
system	register
weak_password	ssh_weak_password
weak_password	ftp_weak_password
cis	centos7
cis	tomcat7
cis	memcached-check

type_name	sub_type_name
cis	mongodb-check
cis	ubuntu14
cis	win2008_r2
system	file_integrity_mon
cis	linux-httpd-2.2-cis
cis	linux-docker-1.6-cis
cis	SUSE11
cis	redhat6
cis	bind9.9
cis	centos6
cis	debain8
cis	redhat7
cis	SUSE12
cis	ubuntu16

安全日志状态码

状态值	说明
1	未修复
2	修复失败
3	回滚失败
4	修复中
5	回滚中
6	验证中
7	修复成功
8	修复成功待重启
9	回滚成功
10	忽略

状态值	说明
11	回滚成功待重启
12	已不存在
20	已失效

- 安全告警日志

日志字段	说明
__time__	连接时间，例如2018-02-27 11:58:15
__topic__	日志主题，固定为sas-security-log
data_source	数据源，详情请参见安全告警data_source列表。
level	告警级别
name	名称，例如Suspicious Process-SSH-based Remote Execution of Non-interactive Commands
op	操作信息 ■ new：新增 ■ dealing：处理
status	状态信息，详情请参见安全日志状态码。
uuid	客户端号
detail	告警详情，例如{"loginSourceIp":"120.27.28.118","loginTimes":1,"type":"login_common_location","loginDestinationPort":22,"loginUser":"aike","protocol":2,"protocolName":"SSH","location":"青岛市"}
unique_info	单服务器该类型告警的唯一标识，例如2536dd765f804916a1fa3b9516b5d512

安全告警data_source列表

值	描述
aegis_suspicious_event	主机异常
aegis_suspicious_file_v2	Webshell
aegis_login_log	异常登录
security_event	安全中心异常事件

- 主机日志

- 进程启动日志

日志字段	说明
__topic__	日志主题，固定为aegis-log-process
owner_id	阿里云主账号ID
uuid	客户端号
ip	客户端主机的IP地址
cmdline	用户启动完整命令行
username	用户名
uid	用户ID
pid	进程ID
filename	进程文件名
filepath	进程文件完整路径
groupname	用户组
ppid	父进程ID
pfilename	父进程文件名
pfilepath	父进程文件完整路径

- 进程快照日志

日志字段	说明
__topic__	日志主题，固定为aegis-snapshot-process
owner_id	阿里云主账号ID
uuid	客户端号
ip	客户端主机的IP地址
cmdline	用户启动完整命令行
pid	进程ID
name	进程文件名
path	进程文件完整路径
md5	进程文件进行MD5计算，超过1MB的进程文件不进行计算。
pname	父进程文件名
start_time	进程启动时间，内置字段
user	用户名
uid	用户ID

- 登录日志

  1分钟内重复登录会被合并为1条日志。

日志字段	说明
__topic__	日志主题，固定为aegis-log-login
owner_id	阿里云主账号ID
uuid	客户端号
ip	客户端主机的IP地址
warn_ip	登录来源IP地址
warn_port	登录端口
warn_type	登录类型，例如SSHLOGIN、RDPLOGIN、IPCLOGIN
warn_user	登录用户名
warn_count	登录次数，例如：3次表示这次登录前1分钟内还发送了2次。

- 暴力破解日志

字段名	名称
__topic__	日志主题，固定为aegis-log-crack
owner_id	阿里云主账号ID
uuid	客户端号
ip	客户端主机的IP地址
warn_ip	登录来源IP地址
warn_port	登录端口
warn_type	登录类型，例如SSHLOGIN、RDPLOGIN、IPCLOGIN
warn_user	登录用户名
warn_count	失败登录次数

- 主机网络连接日志

  主机上每隔10秒到1分钟会收集变化的网络连接。

日志字段	说明
__topic__	日志主题，固定为aegis-log-network
owner_id	阿里云主账号ID

日志字段	说明
uuid	客户端号
ip	客户端主机的IP地址
src_ip	源IP地址
src_port	源端口
dst_ip	目标IP地址
dst_port	目标端口
proc_name	进程名
proc_path	进程路径
proto	协议，例如tcp、udp和raw（表示raw socket）
status	连接状态，详情请参见网络连接状态描述列表。

网络连接状态描述列表

状态值	描述
1	closed
2	listen
3	syn send
4	syn recv
5	establisted
6	close wait
7	closing
8	fin_wait1
9	fin_wait2
10	time_wait
11	delete_tcb

- 端口监听快照

日志字段	说明
__topic__	主题，固定为aegis-snapshot-port
owner_id	阿里云主账号ID
uuid	客户端号
ip	客户端机器IP地址
proto	协议，例如tcp、udp和raw（表示raw socket）
src_ip	监听IP地址
src_port	监听端口
pid	进程ID
proc_name	进程名

- 账户快照

日志字段	说明
__topic__	日志主题，固定为aegis-snapshot-host
owner_id	阿里云主账号ID
name	漏洞名称
alias_name	漏洞别名
op	操作信息 ■ new：新增 ■ verify：验证 ■ fix：修复
status	连接状态，详情请参见网络连接状态描述列表。
tag	漏洞标签，例如oval、system、cms等，主要用于区分EMG紧急漏洞。
type	漏洞类型 ■ sys：windows漏洞 ■ cve：Linux漏洞 ■ cms：Web CMS漏洞 ■ EMG：紧急漏洞
uuid	客户端号

分布式关系型数据库（PolarDB-X）

字段名称	字段说明
__topic__	日志主题，固定为drds_audit_log。
instance_id	PolarDB-X实例ID。
instance_name	PolarDB-X实例名。
owner_id	阿里云主账户ID。
region	PolarDB-X实例所在地域。
db_name	PolarDB-X数据库名。
user	执行SQL的用户名。
client_ip	访问PolarDB-X实例的客户端IP地址。
client_port	访问PolarDB-X实例的客户端端口。
sql	执行的SQL语句。
trace_id	SQL执行的TRACE ID。如果是事务，会以跟踪ID、横杠（-）、数字进行，例如drdsabcdxyz-1，drdsabcdxyz-2等。
sql_code	模板SQL的HASH值。
hint	SQL执行的HINT。
table_name	查询涉及的表名，多表之间以逗号（,）分隔。
sql_type	SQL类型。包括Select、Insert、Update、Delete、Set、Alter、Create、Drop、Truncate、Replace和Other。
sql_type_detail	SQL解析器的名称。
response_time	响应时间，单位为ms。
affect_rows	SQL执行返回行数，增删改时表示影响的行数，查询语句表示返回的行数。
fail	SQL执行是否出错。 • 0：成功 • 1：失败
sql_time	SQL开始执行的时间。

云防火墙（Coud Firewall）

日志字段	说明
__topic__	日志主题，固定为cloudfirewall_access_log

日志字段	说明
owner_id	阿里云主账号ID
log_type	日志类型
app_name	访问流量应用的协议名称，例如HTTPS、NTP、SIP、SMB、NFS、DNS等，未知时为Unknown。
direction	流量的方向 • in：入方向 • out：出方向
domain	域名
dst_ip	目的IP地址
dst_port	目的端口
end_time	会话结束时间，单位：秒（Unix时间戳）
in_bps	入流量大小，单位：bps
in_packet_bytes	入流量总字节数
in_packet_count	入流量总报文数
in_pps	入流量大小，单位：pps
ip_protocol	IP协议类型，支持TCP或UDP协议
out_bps	出方向流量大小，单位：bps
out_packet_bytes	出方向总流量字节数
out_packet_count	出方向报文数
out_pps	出方向流量大小，单位：pps
region_id	访问流量所属的区域
rule_result	命中规则结果 • pass：通过 • alert：告警 • drop：丢弃
src_ip	源IP地址
src_port	源端口，流量数据发出的主机端口
start_time	会话开始时间，单位：秒（Unix时间戳）

日志字段	说明
start_time_min	会话开始时间，分钟取整数，单位：秒（Unix时间戳）
tcp_seq	TCP序列号
total_bps	出入方向访问总流量的大小，单位：bps
total_packet_bytes	出入方向的访问总流量，单位：字节
total_packet_count	总流量，以报文数表示
total_pps	出入方向访问总流量的大小，单位：bps
src_private_ip	私网IP地址
vul_level	漏洞风险等级 • 1：低危 • 2：中危 • 3：高危
url	URL地址
acl_rule_id	命中ACL的规则ID
ips_rule_id	命中IPS的规则ID
ips_ai_rule_id	命中AI的规则ID

堡垒机（Baston Host）

日志字段	说明
__topic__	日志主题
owner_id	阿里云主账号ID
content	日志内容
event_type	事件类型，详情请参见事件类型。
instance_id	堡垒机实例ID
log_level	日志级别
resource_address	资源地址
resource_name	资源名称
result	操作结果
session_id	会话ID

日志字段	说明
user_client_ip	用户来源IP地址
user_id	用户ID
user_name	用户名称

事件类型

值	含义
cmd.Command	字符命令
file.Upload	上传文件
file.Download	下载文件
file.Rename	重命名
file.Delete	删除
file.DeleteDir	删除目录
file.CreateDir	创建目录
graph.Text	图形文字
graph.Keyboard	键盘事件

对象存储（OSS）

日志类型	说明
访问日志	记录对应的Bucket的所有访问日志，实时收集。
批量删除日志	记录批量删除日志时具体的删除信息，实时收集。 **说明** 当您调用DeleteObjects时，访问日志中会有一条请求记录。但因为删除的文件信息存放在请求的HTTP Body中，访问日志中的object会是-，如果查看具体的删除文件的列表，就需要查看批量删除的日志，可以通过request_id关联。
每小时计量日志	记录特定Bucket每个小时累计的计量日志，延迟为数小时，用于辅助分析。

Bucket存储类型

存储类型	描述
standard	标准存储类型

存储类型	描述
archive	归档存储类型
infrequent_access	低频访问存储类型

每个操作的具体信息，请参见API概览。

访问类型

操作值	描述
AbortMultiPartUpload	中止断点上传。
AppendObject	追加上传文件。
CompleteUploadPart	完成断点上传。
CopyObject	复制文件。
DeleteBucket	删除Bucket。
DeleteLiveChannel	删除LiveChannel。
DeleteObject	删除文件。
DeleteObjects	删除多个文件。
GetBucket	列举文件。
GetBucketAcl	获取Bucket权限。
GetBucketCors	查看Bucket的CORS规则。
GetBucketEventNotification	获取Bucket通知配置。
GetBucketInfo	查看Bucket信息。
GetBucketLifecycle	查看Bucket的Lifecycle配置。
GetBucketLocation	查看Bucket区域。
GetBucketLog	查看Bucket访问日志配置。
GetBucketReferer	查看Bucket防盗链设置。
GetBucketReplication	查看跨区域复制。
GetBucketReplicationProgress	查看跨区域复制进度。
GetBucketStat	获取bucket的相关信息。
GetBucketWebSite	查看Bucket的静态网站托管状态。

操作值	描述
GetLiveChannelStat	获取LiveChannel状态信息。
GetObject	读取文件。
GetObjectAcl	获取文件访问权限。
GetObjectInfo	获取文件信息。
GetObjectMeta	查看文件信息。
GetObjectSymlink	获取symlink文件的详细信息。
GetPartData	获取断点文件块数据。
GetPartInfo	获取断点文件块信息。
GetProcessConfiguration	获取Bucket图片处理配置。
GetService	列举Bucket。
HeadBucket	查看Bucket信息。
HeadObject	查看文件信息。
InitiateMultipartUpload	初始化断点上传文件。
ListMultiPartUploads	列举断点事件。
ListParts	列举断点块状态。
PostObject	表单上传文件。
PostProcessTask	提交相关的数据处理，例如截图等。
PostVodPlaylist	创建LiveChannel点播列表。
ProcessImage	图片处理。
PutBucket	创建Bucket。
PutBucketCors	设置Bucket的CORS规则。
PutBucketLifecycle	设置Bucket的Lifecycle配置。
PutBucketLog	设置Bucket访问日志。
PutBucketWebSite	设置Bucket静态网站托管模式。
PutLiveChannel	创建LiveChannel。
PutLiveChannelStatus	设置LiveChannel状态。

操作值	描述
PutObject	上传文件。
PutObjectAcl	修改文件访问权限。
PutObjectSymlink	创建symlink文件。
RedirectBucket	bucket endpoint重定向。
RestoreObject	解冻文件。
UploadPart	断点上传文件。
UploadPartCopy	复制文件块。
get_image_exif	获取图片的exif信息。
get_image_info	获取图片的长宽等信息。
get_image_infoexif	获取图片的长宽以及exif信息。
get_style	获取Bucket样式。
list_style	列举Bucket的样式。
put_style	创建Bucket样式。

同步请求类型

同步请求类型	描述
-	一般请求
cdn	CDN回源

关于签名的更多信息，请参见用户签名验证

签名类型

签名类型	描述
NotSign	未签名
NormalSign	一般方式签名
UriSign	通过URL签名
AdminSign	管理员账号

- 访问日志

日志字段	说明
__topic__	日志主题，固定为oss_access_log
owner_id	阿里云主账号ID
region	Bucket所在区域
access_id	访问者的AccessKey ID
time	访问时间，即OSS收到请求的时间，如果需要时间戳可以使用__time__。
owner_id	Bucket拥有者的阿里云ID
User-Agent	HTTP的User-Agent头
logging_flag	是否开启了日志定期导出到OSS Bucket的功能。
bucket	Bucket名称
content_length_in	请求头中Content-Length的值，单位：Byte
content_length_out	回应头中Content-Length的值，单位：Byte
object	用户请求的object，URL编码，查询时可以使用select url_decode(object)解码。
object_size	对象大小，即对应请求对象的大小，单位：Byte
operation	访问类型，详情请参见访问类型。
request_uri	用户请求的URI，包括query-string，路径是URL编码，查询时可以使用select url_decode(request_uri)解码。
error_code	OSS返回的错误码，详情请参见错误响应。
request_length	HTTP请求的大小，包括header，单位：Byte
client_ip	请求发起的IP地址，即客户端IP地址、其网络防火墙或者Proxy的IP地址。
response_body_length	HTTP响应中body的大小，即HTTP response的body的大小，不包括header。
http_method	HTTP请求方法
referer	请求的HTTP Referer
requester_id	请求者的阿里云主账号ID，匿名访问时为短划线（-）。
request_id	请求ID
response_time	请求响应时间，单位：毫秒

日志字段	说明
server_cost_time	OSS服务器处理时间，即OSS服务器处理本次请求所花的时间，单位：毫秒。
http_type	HTTP请求类型，http或https
sign_type	签名类型，详情请参见签名类型。
http_status	HTTP状态，即OSS请求返回的HTTP状态。
sync_request	同步请求类型，详情请参见同步请求类型。
bucket_storage_type	Bucket存储类型，详情请参见Bucket存储类型。
host	请求访问域名
vpc_addr	访问OSS的域名对应的VPC IP地址
vpc_id	VPC ID
delta_data_size	object大小的变化量，若没有变化为0；如果不是上传请求，则为短划线（-）。
acc_access_region	如果是传输加速请求，这个字段为请求接入点所在区域名，否则为短划线（-）。

- 批量删除日志

日志字段	说明
__topic__	日志主题，固定为oss_batch_delete_log
owner_id	阿里云主账号ID
region	Bucket所在区域
client_ip	请求发起的IP地址，客户端IP地址、网络防火墙或者Proxy的IP地址
user_agent	HTTP的User-Agent头
bucket	Bucket名称
error_code	OSS返回的错误码，详情请参见错误响应。
request_length	request的大小，HTTP请求的大小，包括header，单位：Byte。
response_body_length	response的body的大小，HTTP response的body的大小，不包括header。
object	用户请求的object，URL编码，查询时可以使用select url_decode(object)解码。
object_size	请求对象的大小，单位：Byte

日志字段	说明
operation	访问类型，详情请参见访问类型。
bucket_location	Bucket所在集群
http_method	HTTP请求方法
referer	请求的HTTP Referer
request_id	请求ID
http_status	OSS请求返回的HTTP状态。
sync_request	同步请求类型，详情请参见同步请求类型。
request_uri	用户请求的URI，包括query-string，路径是URL编码，查询时可以使用select url_decode(request_uri)解码。
host	请求访问域名
logging_flag	是否开启logging，即是否开启了原来的日志定期导出功能。
server_cost_time	OSS服务器处理时间，单位：毫秒
owner_id	Bucket拥有者的阿里云主账号ID
requester_id	请求者阿里云ID，匿名访问为短划线（-）。
delta_data_size	object大小的变化量，如果没有变化为0；如果不是上传请求，则为短划线（-）。

- 每小时计量日志

日志字段	说明
__topic__	日志主题，固定为oss_metering_log
owner_id	Bucket拥有者的阿里云主账号ID
bucket	Bucket名称
cdn_in	CDN流入量，单位：Byte
cdn_out	CDN流出量，单位：Byte
get_request	GET请求次数
intranet_in	内网流入量，单位：Byte
intranet_out	内网流出量，单位：Byte
network_in	外网流入量，单位：Byte

日志字段	说明
network_out	外网流出量，单位：Byte
put_request	PUT请求次数
storage_type	Bucket存储类型，详情请参见Bucket存储类型。
storage	Bucket存储量，单位：Byte
metering_datasize	非标准存储的计量数据大小
process_img_size	处理的图像大小，单位：Byte
process_img	处理的图像
sync_in	同步流入量，单位：Byte
sync_out	同步流出量，单位：Byte
start_time	计量开始时间戳
end_time	计量截止时间戳
region	Bucket所在区域

关系数据库（RDS）

日志字段	说明
__topic__	日志主题，固定为rds_audit_log
owner_id	阿里云主账号ID
region	实例所在地域
instance_name	RDS实例名
instance_id	RDS实例ID
db_type	RDS实例类型，例如：mysql、mssql、pgsql
db_version	实例版本号
check_rows	扫描的行数
db	数据库名
fail	SQL执行是否出错。 • 0：成功 • 1：失败

日志字段	说明
client_ip	访问RDS实例的客户端IP地址
latency	延迟，单位：微秒
origin_time	操作时间，单位：微秒
return_rows	返回行数
sql	执行的SQL语句
thread_id	线程ID
user	执行SQL的用户名
update_rows	更新行数

文件存储（NAS）

日志字段	说明
owner_id	阿里云主账号ID
ArgIno	文件系统inode号
AuthRc	授权返回码
NFSProtocolRc	NFS协议返回码
OpList	NFSv4 Procedures编号
Proc	NFSv3 Procedures编号
RWSize	读写大小，单位：Byte
RequestId	请求ID
ResIno	lookup的资源inode号
SourceIp	客户端IP地址
Vers	NFS协议版本号
Vip	服务端IP地址
Volume	文件系统ID
microtime	请求发生时间，单位：微秒

移动推送

日志字段	说明
__topic__	日志主题，固定为cps_callback_event
owner_id	阿里云主账号ID
app_key	AppKey
message_id	消息ID
event_time	回执事件时间
event_type	回执事件类型
device_id	设备ID
device_type	设备类型
last_active_time	设备最后活跃时间
app_version	应用版本号
client_ip	客户端IP地址
brand	设备品牌
network_type	设备网络类型
os	设备操作系统
os_version	设备操作系统版本
isp	设备所属运营商
job_key	任务Key
event_channel	推送通道
vendor_message_id	厂商通道消息ID
reason	发送失败的原因

PolarDB MySQL云原生数据库

日志字段	说明
__topic__	日志主题，固定为polardb_audit_log
owner_id	阿里云主账号ID
region	PolarDB MySQL集群所在地域
cluster_id	PolarDB MySQL集群ID

日志字段	说明
node_id	PolarDB MySQL结点ID
check_rows	扫描的行数
db	数据库名
fail	SQL执行是否出错。 • 0：成功 • 1：失败
client_ip	访问PolarDB MySQL集群的客户端IP地址
latency	延迟，单位：微秒
origin_time	操作时间，单位：微秒
return_rows	返回行数
sql	执行的SQL语句
thread_id	线程ID
user	执行SQL的用户名
update_rows	更新行数

1.7. 查看全局数据

本文介绍如何在日志审计服务中查看从云产品接入的全局数据。

查看日志审计全局数据视图

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**日志审计服务**中的**进入应用**。
3. 单击**审计配置 > 云产品接入 > 全局数据**，查看日志审计全局数据视图。

查看云产品全局数据视图

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**日志审计服务**中的**进入应用**。
3. 单击**审计报表 > 中心化 > 云产品 > 云产品全局数据**，查看云产品全局数据视图。

> **说明** 目前仅支持查看RDS、SLB、OSS的全局数据视图。

报表详情

- 日志审计全局数据视图

仪表盘	描述	说明
活跃账户数	审计监控的账号总数	无
总日志量、小时日志量、天日志量	日志量统计	最多半小时延迟
日志审计全局数据视图、产品存量日志分布	所有采集云产品的日志全局数据汇总	最多半小时延迟
日志量整体趋势、产品日志量趋势	过去30天的日志量趋势	当天的统计有一小时延迟

- OSS全局数据

仪表盘	描述
总日志量、小时日志量、天日志量	OSS日志全局统计
访问日志总日志量、小时日志量、天日志量	访问日志统计
计量日志总志量、小时日志量、天日志量	计量日志统计
OSS全局信息	全局监控统计
日志量整体趋势、子类型日志量趋势	OSS过去30天的日志量趋势

- SLB全局数据

仪表盘	描述
总日志量、小时日志量、天日志量	SLB日志全局统计
经典网络日志总日志量、小时日志量、天日志量	经典网络日志统计
VPC网络日志总志量、小时日志量、天日志量	VPC网络日志统计
SLB全局信息	全局监控统计
日志量整体趋势、网路类型日志量趋势	SLB过去30天的日志量趋势

- RDS全局数据

仪表盘	描述
总日志量、小时日志量、天日志量	RDS日志全局统计
MySQL日志总日志量、小时日志量、天日志量	MySQL日志统计
PgSQL日志总志量、小时日志量、天日志量	PgSQL日志统计
MSSQL日志总志量、小时日志量、天日志量	MSSQL日志统计
RDS全局信息	全局监控统计

仪表盘	描述
日志量整体趋势、子产品日志量趋势	RDS过去30天的日志量趋势

1.8. 使用Terraform配置日志审计

本文介绍如何使用Terraform调用接口配置日志审计。

操作步骤

1. 操作RAM授权。 使用Terraform调用RAM接口完成RAM授权，接口详情请参见alicloud_ram_policy。在调用RAM接口时，需配置审计相关权限（策略内容、角色名称等），详情请参见手动授权日志采集与同步。
2. 配置日志采集。 使用Terraform调用日志审计接口配置日志采集，接口详情请参见alicloud_log_audit，具体示例请参见terraform-provider-alicloud。

1.9. 采集策略

日志审计提供一键式跨账号采集云产品日志及中心化存储功能。对于已开通日志审计的阿里云产品，日志服务默认采集所有符合限定条件的云产品日志。而通过采集策略，可对账号、地域或实例等因素进行限制，实现精细化的日志采集目的。本文介绍如何配置采集策略。

产品支持

采集策略目前支持RDS、DRDS、SLB、Kubernetes容器，详细说明如下所示。

云产品	采集对象	属性	说明
RDS	RDS实例	账号：account.id	RDS实例所属的阿里云账号ID。
		地域：region	RDS实例所属的地域，例如：cn-shanghai。
		实例ID：instance.id	RDS实例ID。
		实例名：instance.name	RDS实例名。
		DB类型：instance.db_type	DB类型，可取值为mysql、pgsql、mssql。
		DB版本号：instance.db_version	DB版本号，例如：8.0。
		标签：tag.*	用户自定义的标签名。 将tag.*中的星号（*）替换为您自定义的标签名。
		账号：account.id	DRDS实例所属的阿里云账号ID。

云产品	采集对象	属性	说明
DRDS	DRDS实例	地域：region	DRDS实例所属的地域，例如：cn-shanghai。
		实例ID：instance.id	DRDS实例ID。
		实例名：instance.name	DRDS实例名。
SLB	SLB实例	账号：account.id	SLB实例所属的阿里云账号ID。
		地域：region	SLB实例所属的地域，例如：cn-shanghai。
		实例ID：instance.id	SLB实例ID。
		实例名：instance.name	SLB实例名。
		网络类型：instance.network_type	SLB网络类型，包括专有网络（VPC）和经典网络（Classic）。
		VPC ID：instance.vpc_id	SLB实例所属的专有网络VPC ID。
		地址类型：instance.address_type	SLB实例的地址类型，包括阿里云内网（intranet）和公网（internet）。
		标签：tag.*	用户自定义的标签名。 将tag.*中的星号（*）替换为您自定义的标签名。
Kubernetes容器（Kubernetes审计日志）	Kubernetes集群	地域：region	Kubernetes集群所属地域，例如：cn-shanghai。
		集群ID：cluster.id	Kubernetes集群ID。
		集群名：cluster.name	Kubernetes集群名称。
		集群类型：cluster.type	Kubernetes集群类型，包括专有版Kubernetes Kubernetes、托管版Kubernetes ManagedKubernetes、Serverless Kubernetes ASK。
		网络类型：cluster.network_mode	Kubernetes集群的网络类型，包括专有网络（VPC）和经典网络（Classic）。
		标签：tag.*	用户自定义的标签名。 将tag.*中的星号（*）替换为您自定义的标签名。

云产品	采集对象	属性	说明
Kubernetes容器（Kubernetes事件中心）	Kubernetes集群	地域：region	Kubernetes集群所属地域，例如：cn-shanghai。
		集群ID：cluster.id	Kubernetes集群ID。
		集群名：cluster.name	Kubernetes集群名称。
		集群类型：cluster.type	Kubernetes集群类型，包括专有版Kubernetes Kubernetes、托管版Kubernetes ManagedKubernetes、Serverless Kubernetes ASK。
		网络类型：cluster.network_mode	Kubernetes集群的网络类型，包括专有网络和经典网络。
		标签：tag.*	用户自定义的标签名。 将tag.*中的星号（*）替换为您自定义的标签名。
Kubernetes容器（ Ingress访问日志）	Kubernetes集群	地域：region	Kubernetes集群所属地域，例如：cn-shanghai。
		集群ID：cluster.id	Kubernetes集群ID。
		集群名：cluster.name	Kubernetes集群名称。
		集群类型：cluster.type	Kubernetes集群类型，包括专有版Kubernetes Kubernetes、托管版Kubernetes ManagedKubernetes、Serverless Kubernetes ASK。
		网络类型：cluster.network_mode	Kubernetes集群的网络类型，包括专有网络（VPC）和经典网络（Classic）。
		标签：tag.*	用户自定义的标签名。 将tag.*中的星号（*）替换为您自定义的标签名。
		日志内容：log.*	日志内容。

配置采集策略

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**日志审计服务**中的**进入应用**。
3. 在**云产品接入 > 全局配置**页面，单击**修改**。
4. 单击目标云产品右侧的**采集策略**。

5. 配置采集策略。日志服务支持通过简易编辑模式或高级编辑模式配置采集策略。简易编辑模式配置简单，当简易编辑模式无法满足您的需求时，可开启高级编辑模式，灵活配置复杂的采集策略。

   > **说明**
   > - 您可以根据实际需求，配置多条采集策略。
   > - 在高级编辑模式下，您可以手动编辑策略语句，但在手动编辑策略语句后，无法返回到简易编辑模式。
   > - 在高级编辑模式下，清空策略语句并保存，再次打开可恢复到简易编辑模式。

   - 简易编辑模式

     a. 在**待添加策略**区域，配置如下参数，并单击**添加策略**。

参数	说明
动作	通过您配置的采集策略，执行相应的动作，详情请参见策略语法。
属性	选择采集对象的属性，不同采集对象对应的属性不同，详情请参见产品支持。
操作符	选择操作符，例如选择**完全匹配**，则对应的操作符为==，详情请参见策略语法。
属性取值	输入属性的值，支持配置多个值。

     b. 在**已添加策略**区域，确认策略配置结果。

     您也可以修改已添加的采集策略以及调整采集策略的顺序。

     - 单击目标采集策略右侧的**编辑**，修改已添加的采集策略。
     - 单击目标采集策略右侧的上下箭头，调整采集策略的顺序。

     > **说明** 日志服务默认添加accept "*"策略，用于接受所有的采集项，不可编辑与删除。

     c. 确认无误后，单击**确定**。

   - 高级编辑模式

     a. 开启**高级编辑模式**。

     b. 在**规则**文本框中，配置采集策略，并单击**确定**。

     详细的语法说明请参见策略语法。

6. 在**全局配置**页面，单击**保存**。

策略语法

- 动作

- 保持（keep）：当采集对象满足采集策略时继续执行下一条策略，由后续策略判断是否采集日志。不满足则拒绝采集日志，不再做后续策略判断。
- 拒绝（drop）：当采集对象满足采集策略时拒绝采集日志，不再执行下一条策略。不满足则继续执行下一条策略，由后续策略判断是否采集。
- 接受（accept）：当采集对象满足采集策略时采集日志，不再执行下一条策略。不满足则继续执行下一条策略，由后续策略判断是否采集。

- 匹配模式

匹配模式	说明
完全匹配	通过字符串的完全匹配，进行采集策略的匹配。 ○ 操作符：== ○ 示例：**keep instance.db_type == "mysql"**表示mysql类型的RDS实例通过当前判断。
通配符匹配	通过通配符星号（*）和问号（?）进行采集策略的匹配。星号（*） 表示0个或多个字符，问号（?）表示一个字符。 ○ 操作符：== ○ 示例： ■ **keep instance.name == "backend*"** 表示实例名以backend开头的实例，通过当前判断。 ■ **keep instance.name == "active?"**表示实例名以active开头且其后面还有一个任意字符的实例，通过当前判断。
正则表达式匹配	通过正则表达式进行采集策略的匹配。 ○ 操作符：~= ○ 示例：**keep instance.name ~= "^\d+$"**表示纯数字的实例名通过当前判断。 **说明** 默认为部分匹配，如果需要完全匹配，需要在开头和结尾加上^和$。
数值比较	对数值进行比较。 ○ 操作符： ■ 直接比较：>、>=、=、<=、< ■ 闭区间比较：：[*, 100]，支持用星号（*）表示无边界。 ○ 示例： ■ **keep tag.level >= 2**表示tag.level大于等于2的实例，通过当前判断。 ■ **keep tag.level：[*, 10]**表示tag.level小于等于10的实例，通过当前判断。 ■ **keep tag.level：[1, 10]**表示tag.level位于[1, 10]之间的实例，通过当前判断。

匹配模式	说明
逻辑关系	○ 关键字： ■ 且：使用and、AND、&&等关键词，不区分大小写。 ■ 或：使用or、OR等关键词，不区分大小写。 ■ 否：使用not，NOT，感叹号（!）等关键词，不区分大小写。 ○ 示例： ■ keep (tag.level > 10) and (region == "cn-shanghai")表示tag.level大于10且位于上海的实例，通过当前判断。 ■ keep (tag.level > 10) or (region == "cn-shanghai")表示tag.level大于10或位于上海的实例，通过当前判断。 ■ keep not region == "cn-shanghai"表示非上海的示例，通过当前判断。
全局匹配	如果策略中没有指定对象名，则表示全局匹配。例如： ○ keep "abc"表示含有abc字符的采集项都可以通过当前判断。 ○ accept "*"表示接受所有采集项。 说明 ○ 全局匹配，必须带双引号（" "）。 ○ 仅在高级编辑模式下，支持全局匹配。

- 字符转义

  采集策略中，需要对星号（*）、反斜线（\）等特殊字符进行转义，例如：keep instance.name == "abc*"表示实例名为abc*的实例通过当前判断。

常见案例

- 采集特定区域的实例日志

  例如：只采集中国区域的实例日志，采集策略如下所示。

```
# only scan cn region
keep region == "cn-*"
# accept by default
accept "*"
```

- 采集特定标签的实例日志

  例如：只采集所有标签打上type值是production（大小写不敏感）的实例日志，采集策略如下所示。

```
# only scan "production" instances
keep tag.type ~= "(?i)^production$"
# accept by default
accept "*"
```

- 复杂场景

  例如：只采集RDS MySQL实例日志，但是如果标签打上level: high的实例，无论数据库类型是MySQL、SQL Server或PostgreSQL，都采集，采集策略如下所示。

```
# accept all high level instances
accept tag.level == "high"
# only scan mysql
keep instance.db_type == "mysql"
# accept by default
accept "*"
```

2.成本管家

2.1. 成本管家

日志服务推出成本管家功能，一键开通后自动导入账单，并提供可视化的账单分析报表，帮助您提高账单分析的效率。

背景信息

阿里云资源具备随时可用、规模弹性、规格丰富的特征，保证您在任意时刻都有足够的资源使用。在您使用云资源的同时，成本是个不容忽视的问题。阿里云的计费方式有按量付费和包年包月。对于按量付费方式，手工对账单进行统计分析不仅耗费时间和精力，准确性也没办法保证。日志服务的成本管家功能很好的解决了这个问题，将您从低效的账单获取和整理工作中解放出来，提高账单分析效率。

功能特点

日志服务提供的成本管家功能，一键开通后，会自动将账单从账单中心导入到日志库中。账单是一种时间序列的数据，而日志服务的主要功能就是对时间序列数据的采集、存储和分析，实现与账单数据的无缝对接，减少了账单分析人员80%的人力投入。成本管家的特点如下：

- 近实时采集：账单产生后一小时内上传到日志服务中。
- 定制报表：提供常见的账单分析场景，支持自动发送报告。
- 交互式分析：使用SQL分析账单数据，分析结果秒级可见。支持将分析规则保存到自定义报表中。
- 可视化：以图表的形式展示分析结果，更加直观。
- 机器学习算法：智能预测未来费用趋势，挖掘异常账单。
- 自定义告警：支持自定义告警功能，实时了解账单详情。
- 免费：账单分析涉及的数据存储和分析功能均不收费。

导入账单

1. 登录日志服务控制台。
2. 在**日志应用**中单击**成本管家**下的**进入应用**。
3. 在**成本管家**左侧，单击**设置**。
4. 导入账单设置。在导入账单步骤中进行如下设置。
   - **阿里云账单导入**：勾选后，会将本账号下所有的阿里云账单导入到日志服务中。
   - **首次导入历史账单**：首次导入您可以选择要导入历史账单的时间。
   - 访问账单权限：如果当前账号没有账单访问权限，请根据提示进行授权。
5. 订阅报告设置。在订阅报告步骤中进行如下设置。
   - **频率**：订阅后报告的发送频率。
   - **添加水印**：打开后会对账单中的敏感数据添加水印，以免关键信息泄露。
   - **通知列表**：可以选择**邮件**或者**WebHook-钉钉机器人**的方式发送订阅的报告。钉钉机器人的请求地址请参见WebHook-钉钉机器人进行获取。
6. （可选）设置告警。您可以针对不同云产品设置不同的告警条件，当账单达到设置的告警条件，则触发告警，帮助您及时了解账单的使用量。
   i. 单击**添加告警**。

ii. 设置告警条件。根据需求配置以下参数：**选择产品**、**账单类型**、**判断条件**、**判断值类型**和**判断值大小**。

> **说明** 可以多次单击**添加告警**添加多个告警信息。

iii. 选择通知方式。关于告警通知方式的操作及说明请参见通知方式。

7. 单击**创建/修改告警**完成账单设置。

功能说明

导入账单后，您可以单击**成本管家**下的**说明**，查看成本管家功能说明信息。包含产品说明、产品分析账单的使用、限制说明、账单字段说明等。

自定义分析

在自定义分析界面，您可以和操作其他日志库一样，对导入的账单进行查询分析，设置快速查询、保存仪表盘、设置告警等。

1. 单击左侧**成本管家**下的**自定义分析**。
2. 在**自定义分析**界面的查询分析输入框中，输入查询分析语句，对导入的账单进行查询分析。该操作与其他日志库查询分析操作相同，具体请参见查询分析简介。

账单总览

成本管家提供内置的账单总览报表，展示当月及过去三个月的费用组成，并根据当前费用预测未来的费用趋势，帮助您合理的规划未来预算。该报表拥有和日志服务仪表盘相同的功能，详细介绍请参见简介。

1. 单击左侧**成本管家**下的**总览**。
2. 在**总览**界面查看账单总览和预测信息。

账单明细

成本管家提供内置的账单明细报表，展示每个产品的账单明细和趋势，以及异常的账单信息。该报表拥有和日志服务仪表盘相同的功能，详细介绍请参见简介。

1. 单击左侧**成本管家**下的**明细**。
2. 在**明细**界面查看产品消费明细。

账单优化

成本管家提供内置的账单优化报表，根据产品账单详情，对按量付费产品自动推出包年包月的节省额度。

1. 单击左侧**成本管家**下的**优化**。
2. 在**优化**界面查看账单优化建议。

资源成本分摊

通过资源成本分摊报表，可以查看主要云资源的使用数目，以及按照tag、昵称等进行分账管理。

ECS 账单分析报表

通过ECS账单分析报表，可以查看ECS的使用情况，以及按照各个维度（region、Tag、昵称）进行分析。通过报表，可以整体把握ECS的使用有，适用于费用优化，成本分摊等场景。

OSS账单分析

通过OSS账单分析报表，可以查看OSS整体费用，费用趋势，以及标准型存储、低频存储、归档型存储等不同类型的存储费用，各个计费项目的使用量和费用。您可根据实际使用情况调整存储类型，节省费用。

SLS账单分析

通过SLS账单分析报表，可以查看SLS的整体费用、费用趋势、各个计费项的用量以及存储空间和索引流量最多的Project和Logstore，可帮助客户优化SLS的使用成本。

2.2. 使用SQL语句自定义分析账单

本文介绍在日志服务控制台上如何使用SQL语句自定义分析账单。

账单数据详情

账单数据包括以下两类数据：

- 左侧为账单数据，标识为 `source:bill` ，每个云产品在每个账单周期中产生一条记录。
- 右侧为实例账单数据，每个实例对应一条数据，包含实例的使用量、属性（TAG、NickName、名称等）、费用。标识为 `source:instance_bill` 。

案例

成本管家中内置的报表仅是分析模板，提供分析案例。实际使用中，您可能有多种多样的需求，同一个模板无法满足。您可以通过SQL语句自定义分析账单，这里以ECS账单为例进行说明。

- 搜索关心的账单

  在所有的账单中，您可能只关心某些账单，例如：只想要获取ECS实例账单，那么只需要在名为aliyun_bill的Logstore中使用SQL语句 `source:instance_bill and ProductCode:ECS` 即可获取结果，如下图所示。更多搜索语法请参见查询语法。

- 简单聚合，获取总的账单费用

  使用以下SQL语句获取ECS实例的总费用。在计算结果中单击**添加到仪表盘**，即可创建一个专属的仪表盘。

  ```
  source:instance_bill and ProductCode:ECS | select sum(PretaxAmount)
  ```

- 分组聚合。

  使用以下SQL语句，获取每个ECS实例的账单总额。

```
source:instance_bill and ProductCode:ECS | select InstanceID, sum(PretaxAmount) as Amount group by InstanceId order by Amount desc
```

本案例通过实例维度进行分析，如果您想要通过其他维度（例如Region、昵称等）分析，只需更换SQL语句中 `group by` 后面的维度。

- 同比环比分析
  - 计算本月费用，同比上月的增长率。

```
source:bill | select diff[1] as "本月费用", diff[2] as "上月费用", diff[3]*100-100 as "同比增加%" from(select compare(amount,604800) as diff from( select sum(PretaxAmount) as amount from log ))
```

  - 按照产品，与上月进行同比分析。

```
source:bill | select ProductCode, diff[1] as "本月费用", diff[2] as "上月费用", diff[3]*100-100 as "同比增加%" from(select productcode, compare(amount,604800) as diff from( select ProductCode, sum(PretaxAmount) as amount from log group by ProductCode ) group by productcode )
```

- 利用Tag做分账管理

  目前多种产品已支持Tag，您可以通过Tag完成分账。Tag中包含多个key-value，通过解析不同的key-value，计算每一对key-value的费用额度。

```
source: instance_bill and ecs | select k,v , round(sum(PretaxAmount),3) "金额" from( select split_to_map(Tag,';',' ') as tags ,PretaxAmount from log where tag <>'' ),unnest(tags) as t(k,v) group by k,v order by "金额" desc limit 1000
```

2.3. 子账号授权

本文档为您介绍子账号使用成本管家所需的权限。

为子账号授权后，可以通过子账号来使用成本管家功能，详情请参见授权RAM用户。

权限策略内容如下。关于每个动作具体的说明请参见动作列表。

```
{
 "Version": "1",
 "Statement": [
  {
   "Action": "log:CreateLogStore",
   "Resource": "acs:log:*:*:project/bill-analysis-*/logstore/*",
   "Effect": "Allow"
  },
  {
   "Action": "log:CreateIndex",
```

```
    "Resource": "acs:log:*:*:project/bill-analysis-*/logstore/aliyun_bill",
    "Effect": "Allow"
  },
  {
    "Action": "log:UpdateIndex",
    "Resource": "acs:log:*:*:project/bill-analysis-*/logstore/aliyun_bill",
    "Effect": "Allow"
  },
  {
    "Action": "log:CreateDashboard",
    "Resource": "acs:log:*:*:project/bill-analysis-*/dashboard/*",
    "Effect": "Allow"
  },
 {
    "Action": "log:UpdateDashboard",
    "Resource": "acs:log:*:*:project/bill-analysis-*/dashboard/*",
    "Effect": "Allow"
  },
 {
    "Action": "log:CreateSavedSearch",
    "Resource": "acs:log:*:*:project/bill-analysis-*/savedsearch/*",
    "Effect": "Allow"
  },
 {
    "Action": "log:UpdateSavedSearch",
    "Resource": "acs:log:*:*:project/bill-analysis-*/savedsearch/*",
    "Effect": "Allow"
  },
{
    "Action": "log:CreateJob",
    "Resource": "acs:log:*:*:project/bill-analysis-*/job/*",
    "Effect": "Allow"
  },
 {
    "Action": "log:UpdateJob",
    "Resource": "acs:log:*:*:project/bill-analysis-*/job/*",
    "Effect": "Allow"
  },
 {
    "Action": "log:CreateApp",
    "Resource": "acs:log:*:*:app/bill",
```

```
    "Effect": "Allow"
  },
{
    "Action": "log:UpdateApp",
    "Resource": "acs:log:*:*:app/bill",
    "Effect": "Allow"
  },
{
    "Action": "log:GetApp",
    "Resource": "acs:log:*:*:app/bill",
    "Effect": "Allow"
  },
{
    "Action": "log:DeleteApp",
    "Resource": "acs:log:*:*:app/bill",
    "Effect": "Allow"
  }
 ]
}
```

3.新冠病毒疫情分析

3.1. 简介

本文主要介绍新冠病毒疫情分析应用及其相关亮点。

简介

新冠病毒疫情分析应用是基于阿里云日志服务中台提供的一站式的数据处理可视化分析系统。借助它，可以在全球范围内了解国家/地区、省份/州的疫情动态。目前该能力全面开放给政府、社区、第三方平台和开发者进行广泛应用，完全免费，应用详情请参见详细说明。

关于日志服务

阿里云日志服务（Log Service）是针对日志类数据的一站式服务，无需开发就能快捷完成海量日志数据的采集、消费、投递以及查询分析等功能，提升运维、运营效率。日志服务主要包括实时采集与消费、数据投递、查询与实时分析等功能，适用于从实时监控到数据仓库的各种开发、运维、运营与安全场景。

作为日志分析中台，日志服务提供了一站式的数据采集、加工、查询分析、AI计算、可视化，并支持互联互通。

亮点

- 定时同步疫情数据，并形成可视化平台覆盖全球各个国家/地区、省份/州的疫情信息。

  > **说明** 图中各种数据源表示日志服务支持客户自行接入其他合法合规的多方面数据，目前App提供的数据来源于Novel Coronavirus (COVID-19) Cases、provided by JHU CSSE（实际信息以官方为准）。

- 内置多份数据大盘并支持自定义。

  提供全球各个国家/地区、省份/州疫情态势。支持交互式查询分析、自定义报表、深钻与告警等。

  - 全球疫情概览

    

    

  - 各个国家/地区的疫情详情

    

    

- 数据平台开放，互联互通

  日志服务是开放的，可以和大量其他环境的系统、三方应用或开源进行对接。提供易扩展的数据分析、存储、可视化平台能力，如DataV、Blink、OSS、流计算、Grafana、SOC等。

  

- 完全免费

  疫情服务应用以及相关资源数据，包括仪表盘、告警等功能完全免费。

其他参考

- 新冠病毒疫情分析应用的资源说明
- 新冠病毒疫情分析应用的限制说明
- 新冠病毒疫情分析应用的日志格式说明
- 新冠病毒疫情分析应用的使用说明

3.2. 详细说明

本文介绍新冠病毒疫情分析应用的详细信息，包括应用说明、资源说明、限制说明、数据说明和使用说明等。

应用说明

- 首次使用该功能需要完成初始化配置（2分钟左右）。
- 每天自动更新同步数据，无需手动同步。
- Data sources: Novel Coronavirus (COVID-19) Cases, provided by JHU CSSE.
- Update frequency: Once a day around 23:59 (UTC).
- 数据仅供参考，以官方最新公告为准。
- 完全免费。
- 如果本应用中相关免费资源长期无活跃操作，本服务保留回收的权利。您可以重启应用再次创建应用。
- 技术支持。

  由阿里云日志服务提供技术支持，扫码了解更多。

资产说明

应用会创建以下日志服务项目资源，不会产生费用。

- 日志项目：ncp-{阿里云主账号UID}-cn-chengdu
- 日志库：ncp
- 仪表盘: covid-19_global、covid-19_detail。

限制说明

- 专属日志库，您无法修改删除Logstore、索引或写入数据。其他操作与一般日志库没有差别。
- 您可以在该项目中创建自己的Logstore并写入自己的数据，但这部分Logstore产生的费用不在免费范围内。
- 专属仪表盘，不推荐修改，可能在后续应用升级中自动覆盖任何改动。您可以在日志服务的项目中复制仪表盘再做修改，详情请参见如何复制仪表盘。

仪表盘说明

提供如下多张内置仪表盘。仪表盘是基于日志库中的数据构建的，您也可以基于数据构建新的仪表盘。

仪表盘	ID	描述
COVID-19 Global	covid-19_global	提供全球各个国家、地区的疫情指标、趋势与列表汇总。

仪表盘	ID	描述
COVID-19 Detail	covid-19_detail	提供全球各个国家、地区所涉及的省份、州的疫情指标、趋势与列表汇总。

数据说明

- 数据版本与使用说明

  各种疫情相关数据均放在一个日志库ncp中，每天有多次版本自动同步到本地导入日志库中，通过字段version标示更新时间，例如：v2020-01-26T12:30:00。

  每个版本的数据都包含了全量数据，因此只需要使用最新版本的数据进行查询、分析统计即可。

  一般情况，可以在查询统计时指定一个版本，如下所示。

  ```
  Version: "v2020-01-26T12:30:00" and Type : "Province/State Cases" | select .... from log
  ```

  但推荐将以上查询统计语句改成如下SQL模式，这样可以在版本更新后自动使用最新版本。

  ```
  Type : "Province/State Cases" | select .... from log l right join (select max(Version) as Version from log) r on l.Version = r.Version
  ```

  > 说明
  > - |前的是查询语句，一般用type过滤特定类型的日志，查询语法详情请参见查询语法。
  > - |后的是标准SQL92语法，其中from log表示从当前日志库中查询，也支持多库join等，并提供额外扩展，如IP地理库、外表OSS/MySQL协同查询功能，详情请参见统计语法。
  > - 每天自动更新同步数据，因此查询统计的时间选择器，选择相对1天即可。

- 概览

  各种疫情相关数据均放在一个日志库ncp中，通过字段type作为类型区分：Global Cases、Country/Region Cases、Province/State Cases。

- Global Cases

  > 说明 其中Hist会在表格的迷你图中使用，而Trend类数据会在各个趋势中使用。

字段名	说明	样例
Type	数据类型	固定为Global Cases
Version	数据版本	v2020-01-26T12:30:00
Last Update	最新来源新闻发布时间	2020-01-26 18:23
Confirmed	最新确诊病例累计数据	1058
Confirmed Hist	确诊病例累计数据（从2020.01.23到当前的历史数据数组）	[270, 444, 444, 549, 729, 1058]

字段名	说明	样例
Confirmed Trend	确诊病例累计数据（从2020.01.23到当前的历史趋势数据字典）	{"2020-01-21": 1, "2020-01-22": 1, "2020-01-23": 1, "2020-01-24": 2, "2020-01-25": 2, "2020-01-26": 3}
Recovered	最新治愈病例累计数据	42
Recovered Hist	治愈病例累计数据（从2020.01.23到当前的历史数据数组）	[0, 28, 28, 31, 32, 42]
Recovered Trend	治愈病例累计数据（从2020.01.23到当前的历史趋势数据字典）	{"2020-01-21": 1, "2020-01-22": 1, "2020-01-23": 1, "2020-01-24": 2, "2020-01-25": 2, "2020-01-26": 3}
Deaths	最新死亡病例累计数据	52
Deaths Hist	死亡病例累计数据（从2020.01.23到当前的历史数据数组）	[3, 17, 17, 24, 39, 52]
Deaths Trend	死亡病例累计数据（从2020.01.23到当前的历史趋势数据字典）	{"2020-01-21": 1, "2020-01-22": 1, "2020-01-23": 1, "2020-01-24": 2, "2020-01-25": 2, "2020-01-26": 3}
New Confirmed Hist	疑似病例现有数据（从2020.01.23到当前的历史数据数组）	[11, 0, 41, 0, 56, 127]
New Confirmed Trend	疑似病例现有数据（从2020.01.23到当前的历史趋势数据字典）	{"2020-01-21": 1, "2020-01-22": 1, "2020-01-23": 1, "2020-01-24": 2, "2020-01-25": 2, "2020-01-26": 7}

- Country/Region Cases

> **说明** 其中Hist会在表格的迷你图中使用，而Trend类数据会在各个趋势中使用。

字段	说明	样例
Type	数据类型	固定为Country/Region Cases
Version	数据版本	v2020-01-26T12:30:00
Last Update	最新来源新闻发布时间	2020-01-26 18:23
Country/Region	国家或地区名称	China, US
LatLng	数据条目中区域的经纬度组成的字符串，格式：lat,lng	51.7283857,-2.2085499
Confirmed	最新确诊病例累计数据	1058

字段	说明	样例
Confirmed Hist	确诊病例累计数据（从2020.01.23到当前的历史数据数组）	[270, 444, 444, 549, 729, 1058]
Confirmed Trend	确诊病例累计数据（从2020.01.23到当前的历史趋势数据字典）	{"2020-01-21": 1, "2020-01-22": 1, "2020-01-23": 1, "2020-01-24": 2, "2020-01-25": 2, "2020-01-26": 3}
Recovered	最新治愈病例累计数据	42
Recovered Hist	治愈病例累计数据（从2020.01.23到当前的历史数据数组）	[0, 28, 28, 31, 32, 42]
Recovered Trend	治愈病例累计数据（从2020.01.23到当前的历史趋势数据字典）	{"2020-01-21": 1, "2020-01-22": 1, "2020-01-23": 1, "2020-01-24": 2, "2020-01-25": 2, "2020-01-26": 3}
Deaths	最新死亡病例累计数据	52
Deaths Hist	死亡病例累计数据（从2020.01.23到当前的历史数据数组）	[3, 17, 17, 24, 39, 52]
Deaths Trend	死亡病例累计数据（从2020.01.23到当前的历史趋势数据字典）	{"2020-01-21": 1, "2020-01-22": 1, "2020-01-23": 1, "2020-01-24": 2, "2020-01-25": 2, "2020-01-26": 3}
New Confirmed Hist	疑似病例现有数据（从2020.01.23到当前的历史数据数组）	[11, 0, 41, 0, 56, 127]
New Confirmed Trend	疑似病例现有数据（从2020.01.23到当前的历史趋势数据字典）	{"2020-01-21": 1, "2020-01-22": 1, "2020-01-23": 1, "2020-01-24": 2, "2020-01-25": 2, "2020-01-26": 7}

- Province/State Cases

> **说明**
> - 对于源数据中未明确说明具体所属省份/州的数据，将放入到一个叫做Unspecified*的省份/州中。
> - 其中Hist会在表格的迷你图中使用，而Trend类数据会在各个趋势中使用。

字段	说明	样例
Type	数据类型	固定为Province/State Cases
Version	数据版本	v2020-01-26T12:30:00
Last Update	最新来源新闻发布时间	2020-01-26 18:23

字段	说明	样例
Country/Region	国家/地区名称	China, US
Province/State	省份/州名称	Shanghai, New York
LatLng	数据条目中区域的经纬度组成的字符串，格式：lat,lng	51.7283857,-2.2085499
Confirmed	最新确诊病例累计数据	1058
Confirmed Hist	确诊病例累计数据（从2020.01.23到当前的历史数据数组）	[270, 444, 444, 549, 729, 1058]
Confirmed Trend	确诊病例累计数据（从2020.01.23到当前的历史趋势数据字典）	{"2020-01-21": 1, "2020-01-22": 1, "2020-01-23": 1, "2020-01-24": 2, "2020-01-25": 2, "2020-01-26": 3}
Recovered	最新治愈病例累计数据	42
Recovered Hist	治愈病例累计数据（从2020.01.23到当前的历史数据数组）	[0, 28, 28, 31, 32, 42]
Recovered Trend	治愈病例累计数据（从2020.01.23到当前的历史趋势数据字典）	{"2020-01-21": 1, "2020-01-22": 1, "2020-01-23": 1, "2020-01-24": 2, "2020-01-25": 2, "2020-01-26": 3}
Deaths	最新死亡病例累计数据	52
Deaths Hist	死亡病例累计数据（从2020.01.23到当前的历史数据数组）	[3, 17, 17, 24, 39, 52]
Deaths Trend	死亡病例累计数据（从2020.01.23到当前的历史趋势数据字典）	{"2020-01-21": 1, "2020-01-22": 1, "2020-01-23": 1, "2020-01-24": 2, "2020-01-25": 2, "2020-01-26": 3}
New Confirmed Hist	疑似病例现有数据（从2020.01.23到当前的历史数据数组）	[11, 0, 41, 0, 56, 127]
New Confirmed Trend	疑似病例现有数据（从2020.01.23到当前的历史趋势数据字典）	{"2020-01-21": 1, "2020-01-22": 1, "2020-01-23": 1, "2020-01-24": 2, "2020-01-25": 2, "2020-01-26": 7}

使用说明

1. 登录阿里云日志服务控制台。
2. 在**日志应用**区域，单击**新冠病毒疫情分析**中的**进入应用**。

   

3. 根据页面提示，完成初始化配置，开始使用新冠病毒疫情分析应用。 只在首次使用时，需进行初始化配

置。

常见问题

- 如何删除所属项目？

  应用及其相关专属资源完全免费，如需删除所属项目，可直接打开Cloud Shell执行如下命令行删除项目。

  ```
  aliyunlog log delete_project --project_name=ncp-$ALICLOUD_ACCOUNT_ID-cn-chengdu --region-endpoint=cn-chengdu.log.aliyuncs.com
  ```

  > 注意 如果项目中创建了自己的日志库，也会一并被删除，请谨慎操作。

- 如何从现有仪表盘复制新的仪表盘？

  i. 在阿里云控制台右上角，打开阿里云Cloud Shell。

  ii. 复制仪表盘配置到本地。

  ```
  aliyunlog log get_dashboard --project=ncp-$ALICLOUD_ACCOUNT_ID-cn-chengdu --entity=covid-19_global --region-endpoint=cn-chengdu.log.aliyuncs.com > covid-19_global.json
  aliyunlog log get_dashboard --project=ncp-$ALICLOUD_ACCOUNT_ID-cn-chengdu --entity=covid-19_detail --region-endpoint=cn-chengdu.log.aliyuncs.com > covid-19_detail.json
  sed -i "s/\"dashboardName\": \"/\"dashboardName\": \"v2/g" covid-19_global.json
  sed -i "s/\"description\": \"\", \"displayName\": \"/\"description\": \"\", \"displayName\": \"v2/g" covid-19_global.json
  sed -i "s/\"dashboardName\": \"/\"dashboardName\": \"v2/g" covid-19_detail.json
  sed -i "s/\"description\": \"\", \"displayName\": \"/\"description\": \"\", \"displayName\": \"v2/g" covid-19_detail.json
  aliyunlog log create_dashboard --project=ncp-$ALICLOUD_ACCOUNT_ID-cn-chengdu --detail=file://./covid-19_global.json --region-endpoint=cn-chengdu.log.aliyuncs.com
  aliyunlog log create_dashboard --project=ncp-$ALICLOUD_ACCOUNT_ID-cn-chengdu --detail=file://./covid-19_detail.json --region-endpoint=cn-chengdu.log.aliyuncs.com
  ```

  iii. 查看创建的仪表盘。

  在**新冠病毒疫情分析**应用的**设置**页签中单击**跳转到Project控制台**，单击**仪表盘**，查看新建的仪表盘。

其他参考

- 日志服务文档
- 构建仪表盘

4.K8S事件中心

4.1. 创建并使用Kubernetes事件中心

本文介绍如何创建Kubernetes事件中心及相关操作，包括查看事件总览、查询事件详情、查看Pod生命周期、配置告警和自定义查询等操作。

背景信息

Kubernetes事件中心记录了集群的状态变更，包括创建Pod、运行Pod、删除Pod、组件异常等。
Kubernetes事件中心实时汇聚Kubernetes中的所有事件并提供存储、查询、分析、可视化、告警等能力。

免费策略

Kubernetes事件中心关联的Logstore在90天内免费（每天允许免费写入256M数据，相当于25万条事件。默认一个Kubernetes线上集群每天产生的事件在1000条左右）。事件存储时间默认为90天，因此如果您不调整事件保存时间，可一直免费使用Kubernetes事件中心。例如：

- 不调整存储时间（默认90天），集群每天产生1000条事件，则事件中心永久免费。
- 调整存储时间为105天，集群每天产生1000条事件，则超过90天后，事件中心每天收取的费用约0.1元，费用详情请参见按量付费。

步骤一：创建事件中心

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**K8s事件中心**中的**进入应用**。
3. 在**事件中心管理**页面，单击**添加**。
4. 在**添加事件中心**页面，配置相关参数。
   - 选择**已有Project**，可从**Project**下拉框中选择已创建的Project。
   - 选择**从容器服务选择K8s集群**，可从**K8s集群**下拉框中选择已创建的K8s集群。通过此方式创建事件中心，默认创建一个名为k8s-log-{cluster-id}的Project。
5. 单击**下一步**，完成创建。

> **说明** 创建事件中心后，默认在您选择的日志服务Project中创建一个名为k8s-event的Logstore，并创建相关联的报表和告警等。

步骤二：部署Eventer和NodeProblemDetector

您需要在Kubernetes集群中配置事件采集和node-problem-detector后才能正常使用K8s事件中心。

- 阿里云Kubernetes配置方式

  阿里云Kubernetes应用市场中的ack-node-problem-detector已集成node-problem-detector和事件采集功能，您只需要部署该组件即可，该组件详细部署请参见场景3：使用node-problem-detector与eventer实现节点异常告警。

  i. 登录容器服务控制台。
  ii. 在左侧导航栏中，选择**市场** > **应用目录**。
  iii. 在**阿里云应用**页签下，单击**ack-node-problem-detector**。
  iv. 在**参数**页签下，修改eventer节点中的相关信息。

- enabled：将**eventer > sinks > sls**下的enabled设置为true。
- topic：可选，设置为您的集群名称，只支持英文字母a-z、下划线（_）、连接号（-）。
- project：设置为您创建事件中心时的Project名称。
- logstore：只能设置为k8s-event。

```
sinks:
  sls:
    enabled: true
    # If you want the monitoring results to be notified by sls, set enabled to true.
    topic: "my-cluster"
    project: "{sls-project-name}"
    # You can view the project information by logging in to the
    # SLS console. Please fill in the name of the project here.
    # eg: your project name is k8s-log-cc18a5f3443dhdss22654da,
    # then you can fill k8s-log-cc18a5f3443dhdss22654da to project label.
    logstore: "k8s-event"
    # You can view the project information by logging in to the
    # SLS console. Please fill the logstore address in here.
```

v. 单击**创建**，完成部署。

- 自建Kubernetes配置方式
  i. 配置事件采集，详情请参见采集Kubernetes事件。
  ii. 配置node-problem-detector，详情请参见Github。

步骤三：使用事件中心

创建K8s事件中心并部署Eventer和NodeProblemDetector后，即可使用K8s事件中心，包括查看事件总览、查询事件详情、查看Pod生命周期、配置告警和自定义查询等操作。

在**K8s事件中心**页面，找到目标事件中心实例，单击 图标，可进行如下操作。

操作	说明
查看事件总览	单击**事件总览**，查看核心事件的汇总统计信息。例如：总体错误数以及和昨天/上周的对比、告警项统计、重要事件趋势、Pod OOM详细信息等。 **说明** 目前Pod OOM信息不能精确到Pod，只能定位到事件发生的节点、进程名、进程号。您可以通过自定义查询查找Pod OOM发生时间点附近的Pod重启事件，以此定位到具体的Pod。
查询事件详情	单击**事件详情查询**，查看按照各种维度（事件等级、事件类型、事件目标、Host、Namespace、Name）过滤后的事件的统计信息以及详情。
查看Pod生命周期	单击**Pod生命周期**，以图形化方式展示Pod整个生命周期中的事件信息，还可通过事件等级筛选重要的Pod事件。

操作	说明
配置告警	单击**告警配置**，配置事件的告警，具体操作请参见表格下方的操作步骤。
自定义查询	单击**自定义查询**，自定义查询条件查询相关信息，查询条件请参见查询与分析语法规则。 事件中心的所有事件都保存在Logstore中，您可以使用Logstore中的所有功能，例如自定义查询、消费事件进行自定义处理、创建自定义报表、创建自定义告警等。 如果您要访问事件中心所在的Project，可通过以下两种方式获取Project名称。 • 通过**自定义查询**页面的URL定位到Project。URL规则为 `https://sls.console.aliyun.com/lognext/app/k8s-event/project/k8s-log-xxxx/logsearch/k8s-event` ，Project字段的后一个字段即为日志服务Project名称，例如k8s-log-xxxx。 • 在**集群管理**页签的事件中心列表中，查看目标事件中心对应的Project名称。
配置自定义告警	除了内置的告警外，事件中心还支持配置自定义告警。 在**自定义查询**页面，输入对应K8s事件的查询语句，单击**另存为告警**完成自定义告警配置，详情请参见告警简介。 例如：创建一个FailedPreStopHook的告警，您可以在查询页面中输入 `* and FailedPreStopHook | SELECT "object-namespace", "object-name", "reason", "message"` ，单击**另存为告警**，配置参数后保存即可。 **说明** 如果您自定义配置的告警名称是前缀K8s，则该告警配置会在目标事件的**告警配置**页签的**全部告警事件**显示中，否则只显示在告警详情中。

配置告警具体操作如下所示。

1. 在**K8s事件中心**，找到目标事件中心实例，单击 图标。
2. 单击**告警配置**，进入**告警配置页面**。
3. 添加通知方式。
   i. 单击**添加通知方式**。
   ii. 在**添加通知方式**页面，配置相关参数。

参数	说明
通知方式名称	通知方式的名称。
告警间隔	两次告警通知之间的时间间隔，默认为5分钟。 **说明** 建议告警间隔最小设置为2分钟，防止收到过多的告警信息。
通知类型	包括短信、语音、邮件、钉钉机器人、WebHook自定义和通知中心，可选择一种或多种通知类型，详情请参见通知方式。

iii. 单击**确定**。

4. 开启告警通知

i. 在**全部告警事件**区域，单击**修改**。

ii. 找到待开启的告警事件，单击开启图标，并选择合适的告警通知。

> **说明** 建议您先开启所有告警，若发现告警通知太多，可适当关闭告警或调整通知间隔。

iii. 单击**保存**。

删除事件中心

在**K8s事件中心 > 集群管理**页面中，找到目标事件中心实例，单击 图标，删除事件中心。

常见问题

- K8s事件中心无数据。

  部署好K8s事件中心后，新产生的事件会自动采集到K8s事件中心，您可以在**自定义查询**页面进行搜索（建议将右上角时间范围调整到1天）。如果无数据，一般有两个原因：

  - 部署K8s事件中心后，K8s集群还未产生事件。

    您可以通过 `kubectl get events --all-namespaces` 命令检查集群内是否有新事件产生。

  - 部署Eventer和NodeProblemDetectors时，参数填写错误。
    - 如果您使用的是阿里云Kubernetes集群，请在**容器服务控制台 > 应用 > 发布**中，找到对应的集群，单击**ack-node-problem-detector**后的**更新**，检查参数配置，详情配置请参见步骤二：部署Eventer和NodeProblemDetector。
    - 如果您使用的是自建Kubernetes集群，参数配置请参见采集Kubernetes事件。

- 如何查看事件对应容器的日志？
  - 如果您使用的是阿里云Kubernetes集群，请在**容器服务控制台 > 应用 > 容器组**中，找到目标集群，将**命名空间**选择为**kube-system**，在搜索框中输入eventer关键词找到目标容器，在其详情页面查看日志。
  - 如果您使用的是自建Kubernetes集群，请查看namespace为**kube-system**下文件名前缀为eventer-sls的Pod日志。