ALIBABA CLOUD

Alibaba Cloud

日志服务

应用中心（App）

文档版本：20210906

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

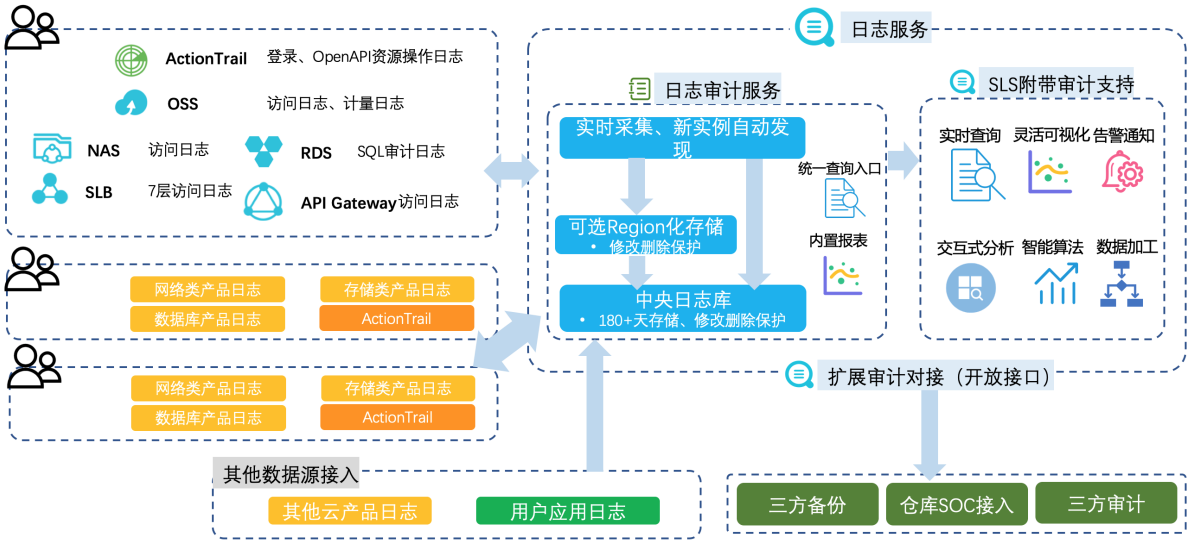
1.日志审计服务

1.1. 日志审计服务概述

本文介绍日志审计服务的功能特性、背景信息、应用场景、技术优势及覆盖的云产品。

功能特性

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。日志审计服务覆盖基础（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DRDS、云原生数据库PolarDB）、安全（WAF、DDoS防护、云防火墙、云安全中心）等产品，并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》。

《网络安全法》（2017年6月1日 实施）

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月

（第三章第一节第二十一条）

《GDPR》（2018年5月25日实施）

惩罚力度较强（2%/4%营收-可叠加），但有模糊空间
覆盖大部分国际业务的公司：
- 在欧盟境内拥有业务；或在欧盟境内没有业务，但是存储或处理欧盟公民的个人信息；
- 超过250名员工；或少于250名员工，但是其数据处理方式影响数据主体的权利和隐私，或是包含某些类型的敏感个人数据。

较明确规定了数据保护的一些细节：
- 网络数据（IP地址或cookie数据）等信息也被纳入保护范围
- 规定了数据是否需要离开信息拥有者所在地
- 规定了3年后客户敏感信息的脱敏要求等

《网络安全等保2.0标准》
（2019年5月13日发布，12月1日实施）

规定了哪些行为、事件需要审计：
- 网络边界、重要网络节点
- 覆盖每个用户、支持重要用户行为、重要安全事件
- 远程访问的用户行为、访问互联网用户行为等单独行为
- 网络系统操作、重要存储操作、计算系统操作、安全系统操作需详细记录
- 审计管理员的操作本身也需要记录并审计

对审计系统提出要求：
- 集中收集、集中分析，集中存储时长要求（180天以上）
- 对审计数据的保护（备份、防修改、覆盖、防止中断等）
- 需提供分析、监控报警等支持可疑行为发现
- 需要提供数据汇集接口，供第三方审计

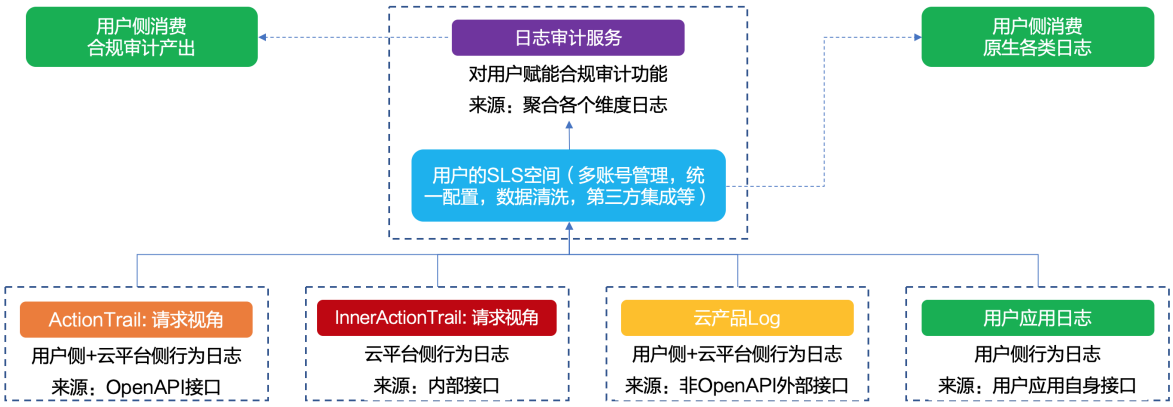
也覆盖云平台内部操作日志的审计

通过HIPAA、GLBA、PCI DSS、SOX、FISMA和ISO 27001/2等审计

- 日志数据保存180天
- 可以被溯源
- 无法篡改

- 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，对账号设备的操作、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。



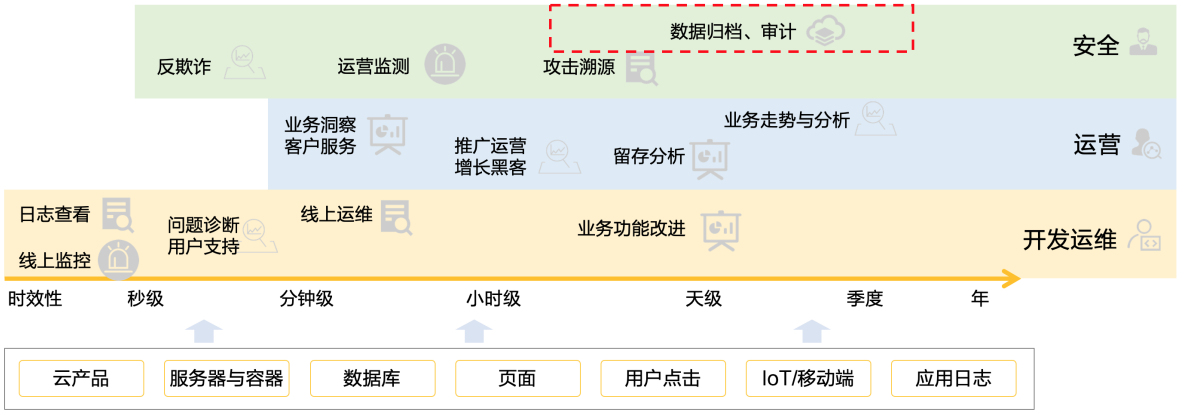
- 日志审计是安全防护的重要一环。

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

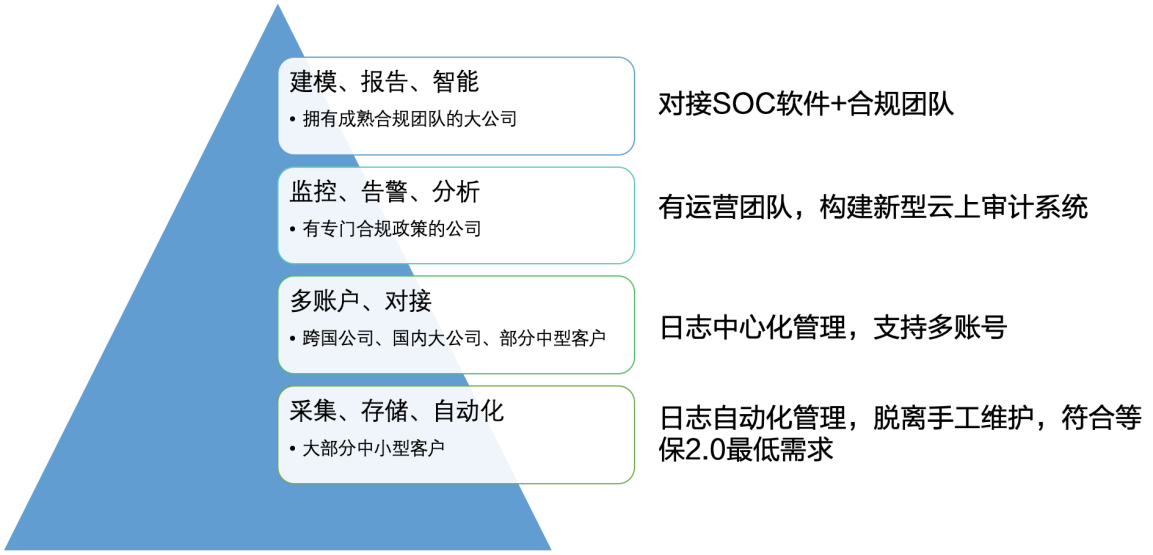
- 日志服务与审计场景

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：支持将多个阿里云账号下的日志采集到一个阿里云账号下的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DRDS、PolarDB MySQL云原生数据库）、安全（WAF、云防火墙、云安全中心、DDoS防护）等云产品日志。采集完成后，会自动存储到对应Logstore或Metricstore中，并生成对应的仪表盘。详细信息如下：

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的操作行为日志	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
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

云产品	审计相关日志	采集地域	使用前提	日志服务资源
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	• 主机日志（7种） • 网络日志（4种） • 安全日志（3种）	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	互联网边界防火墙流量日志、VPC边界防火墙流量日志	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	所有在售地域	V3.2版本及以上	• Logstore名称 bastion_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
云数据库RDS	• RDS审计日志 • MySQL慢日志 • MySQL性能日志	除本地云以外的其他在售地域	• 审计日志 ◦ 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。 • 慢日志、性能日志 只支持非基础版的MySQL实例。	• 审计日志 ◦ 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 • 慢日志 ◦ Logstore名称 rds_log ◦ 仪表盘名称 无 • 性能日志 ◦ Metricstore名称 rds_metrics ◦ 仪表盘名称 RDS性能监控

云产品	审计相关日志	采集地域	使用前提	日志服务资源

云数据库PolarDB	• PolarDB审计日志
	• PolarDB MySQL慢日志
	• PolarDB MySQL性能日志
		所有在售地域	• 审计日志
			  ○ 支持MySQL集群和PostgreSQL集群。
			  ○ 需开启SQL洞察或审计功能。由日志审计服务自动开启。
			• 慢日志、性能日志
			只支持MySQL集群。
				• 慢日志、审计日志
				  ○ Logstore名称
				polardb_log
				  ○ 仪表盘名称
				无
				• 性能日志
				  ○ Metricstore名称
				polardb_metrics
				  ○ 仪表盘名称
				PolarDB性能监控

云原生分布式数据库DRDS	DRDS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
				  ○ DRDS运营中心
				  ○ DRDS安全中心
				  ○ DRDS性能中心

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

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，请参见计费项。
			• 暂不支持跨账号采集K8s相关的日志。
			• 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

云产品	审计相关日志	采集地域	使用前提	日志服务资源
DDoS防护	• DDoS高防（新BGP）访问日志 • DDoS高防（国际）访问日志 • DDoS原生访问日志	不涉及	• DDoS高防（新BGP）：已在DDoS高防（新BGP）控制台上购买全量日志分析模块。更多信息，请参见开通全量日志分析功能。 • DDoS高防（国际）：已在DDoS高防（国际）控制台上购买全量日志分析模块。更多信息，请参见开通全量日志分析功能。 • DDDoS原生：已在DDoS原生控制台上购买全量日志分析模块。更多信息，请参见开通原生防护日志。	• Logstore名称 ddos_log • 仪表盘名称 ◦ DDoS高防（国际）访问中心 ◦ DDoS高防（国际）运营中心 ◦ DDoS高防（新BGP）访问中心 ◦ DDoS高防（新BGP）运营中心 ◦ DDoS原生防护事件报表 ◦ DDoS原生清洗分析报表
应用集成	操作日志	不涉及	无	• Logstore名称 appconnect_log • 仪表盘名称 无

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

    从各个阿里云账号、各个地域采集到的日志，会存储到中心账号下的一个中心Project中，目前中心化存储可供选择的地域如下所示。

    > **说明** 当您切换中心账号所在地域时，日志服务为您创建一个新的中心Project，原Project不会被删除。

    - 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）、德国（法兰克福）、印尼（雅加达）
  - 区域化存储

    对于SLB、OSS、DRDS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、DRDS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、DRDS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）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、DRDS，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、DRDS，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。更多信息，请参见计费项。

  > **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DRDS、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。更多信息，请参见计费项。

  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。

云产品	额外费用
云防火墙（Cloud 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 MySQL审计日志采集功能后，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云原生数据库的审计日志采集功能后，会自动开启符合条件的PolarDB MySQL集群的SQL洞察（SQL审计）功能，费用详情请参见计费项概览。
DDoS防护	在DDoS高防（新BGP）控制台上购买**全量日志分析**模块，费用详情请参见概述。

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。

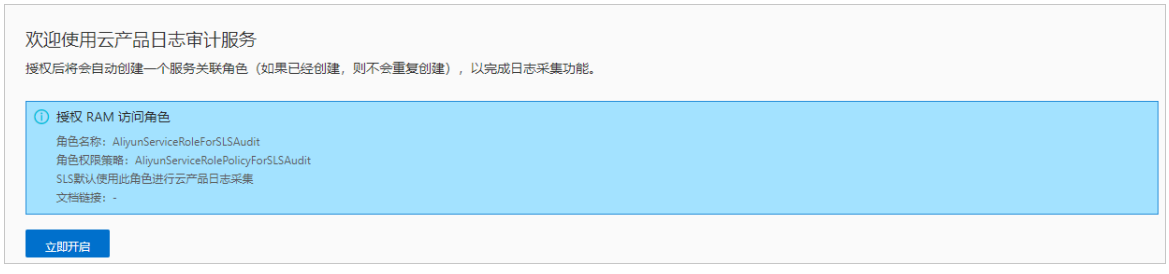
  建议使用阿里云RAM用户，该RAM用户需具备RAM读权限（例如已被授权AliyunRAMReadOnlyAccess策略），且对日志服务有读写权限（例如被授权AliyunLogFullAccess策略）。
- 待采集日志的云产品已开启相应的服务。更多信息，请参见云产品覆盖及相关资源。

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**。
3. 根据页面提示完成授权。

   完成授权后，日志审计服务将使用服务关联角色AliyunServiceRoleForSLSAudit进行云产品的日志采集。更多信息，请参见管理服务关联角色AliyunServiceRoleForSLSAudit。

   > **注意**
   > - 执行该操作的账号具备AliyunRamFullAccess权限。
   > - 本操作只需执行一次。
   > - RDS审计中心和日志审计服务都需使用服务关联角色AliyunServiceRoleForSLSAudit进行日志采集，如果您已在RDS审计中心中执行此操作，则无需在日志审计服务中再次执行。



配置单账号采集

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**。
3. 在**云产品接入 > 全局配置**页面，开启日志采集功能。
   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。
      - 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）、德国（法兰克福）、印尼（雅加达）
   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、DRDS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. 单击**保存**。
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。更多信息，请参见常见问题及错误排查。

配置多账号采集

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。

> **注意** 暂不支持跨账号采集K8s相关的日志。

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**。
3. 在**云产品接入 > 全局配置**页面，开启日志采集功能。
   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。
      - 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）、德国（法兰克福）、印尼（雅加达）
   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、DRDS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. 单击**保存**。
4. 在**多账号配置 > 全局配置**页面，配置账号信息。

   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操作步骤。
   - 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）。
5. 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。更多信息，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**。
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**。
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，请参见首次配置，如果是跨账号采集，请参见操作步骤。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。更多信息，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。具体操作，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**。
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）外的报表，地域限制请参见日志审计服务概述。

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**。
3. 在左侧导航栏中，单击**审计查询**。
4. 单击目标云产品，进入查询与分析页面。

   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）外的日志，地域限制请参见日志审计服务概述。

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**。
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。更多信息，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。更多信息，请参见实时消费。

1.5. 自定义授权日志采集与同步

在使用日志审计服务进行跨账号采集云产品日志时，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数据同步。您可以直接使用具备特定权限的RAM用户的密钥或者参见本文进行自定义授权。

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。

> **说明** 当前主账号的授权在创建服务关联角色AliyunServiceRoleForSLSAudit时，自动完成。具体操作，请参见首次配置。其他主账号要使用自定义权限时，需参见本文完成授权。

- 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
AliyunServiceRoleForSLSAudit	AliyunServiceRolePolicyForSLSAudit

- 其他账号

角色	权限策略
sls-audit-service-monitor	ReadOnlyAccess AliyunLogAuditServiceMonitorAccess

操作步骤

1. 使用其他账号登录RAM 控制台。

   建议使用RAM用户登录，且该RAM用户需具备RAM读写权限（例如已被授予*AliyunRAMFullAccess*策略）。

2. 创建权限策略AliyunLogAuditServiceMonitorAccess。

   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"
	}
	]
	}

3. 创建*sls-audit-service-monitor*角色。

i. 在左侧导航栏中，选择**身份管理 > 角色**，然后单击**创建RAM角色**。

ii. 在**选择类型**配置向导中，选择**阿里云服务**，单击**下一步**。

iii. 在**配置角色**配置向导中，配置如下参数后，然后单击**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**。

iv. 在**创建完成**配置向导中，单击**为角色授权**。

4. 授予sls-audit-service-monitor角色AliyunLogAuditServiceMonitorAccess策略。

在**添加权限**面板中，选择**自定义策略**下的AliyunLogAuditServiceMonitorAccess策略和**系统策略**下的ReadOnlyAccess策略。单击**确定**。

5. 修改sls-audit-service-monitor角色的信任策略。
   i. 在RAM角色列表中，单击**sls-audit-service-monitor**角色。
   ii. 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，然后单击**确定**。

   其中，中心主账号ID请根据实际值替换，您可以在账号中心查看阿里云账号的ID。

```
{
  "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

1.6.1. 操作审计

本文介绍操作审计的操作日志的字段详情。

日志字段	说明
__topic__	日志主题，固定为actiontrail_event。
owner_id	阿里云账号ID
event	事件主体内容，JSON格式。事件主体的内容随事件变化。
event.eventId	事件ID，事件的唯一标识。
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

日志字段	说明
event.apiVersion	相关API的版本
event.errorMessage	事件失败的错误信息
event.serviceName	事件相关的服务名称
event.sourceIpAddress	事件相关的源IP地址
event.userAgent	事件相关的客户端
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	请求参数中的地域
event.userIdentity.accessKeyId	请求所使用的AccessKey ID
event.userIdentity.accountId	请求账号的ID
event.userIdentity.principalId	请求账号的凭证ID
event.userIdentity.type	请求账号的类型
event.userIdentity.userName	请求账号的名称
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

1.6.2. 对象存储

本文介绍对象存储OSS相关日志的字段详情。

- 访问日志

  记录对应Bucket的所有访问日志，实时采集。

日志字段	说明
__topic__	日志主题，固定为oss_access_log。
owner_id	阿里云账号ID
region	Bucket所在地域
access_id	访问者的阿里云AccessKey ID
time	访问时间，即OSS收到请求的时间。如果需要时间戳，可使用__time__。

日志字段	说明
owner_id	Bucket拥有者的阿里云账号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	响应头中Content-Length的值，单位：Byte。
object	OSS Object，URL编码。查询时，您可使用select url_decode(object)解码。
object_size	OSS Object大小，单位：Byte。
operation	访问类型。更多信息，请参见访问类型。
request_uri	请求URI，包括query-string，路径是URL编码。查询时，您可使用select url_decode(request_uri)解码。
error_code	OSS返回的错误码。更多信息，请参见错误响应。
request_length	HTTP请求的大小，包括header，单位：Byte。
client_ip	发起请求的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	响应Body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。
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。更多信息，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。更多信息，请参见同步请求类型。
bucket_storage_type	Bucket存储类型。更多信息，请参见Bucket存储类型。

日志字段	说明
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	OSS Object大小的变化量。如果没有变化则为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地域名，否则为短划线（-）。
restore_priority	Restore恢复优先级

- 批量删除日志

  记录批量删除Object时具体的删除信息，实时采集。

  > **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字段显示为短划线（-）。如果需要查看具体的删除文件的列表，可查看批量删除的日志，通过request_id关联。

日志字段	说明
__topic__	日志主题，固定为oss_batch_delete_log。
owner_id	阿里云账号ID
region	Bucket所在地域
client_ip	发起请求的IP地址，例如客户端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。更多信息，请参见同步请求类型。
request_length	请求Body大小，包括header，单位：Byte。
response_body_length	响应Body大小，不包括header。
object	OSS Object，URL编码。查询时，您可使用select url_decode(object)解码。
object_size	请求对象的大小，单位：Byte。
operation	访问类型。更多信息，请参见访问类型。
bucket_location	Bucket所在集群

日志字段	说明
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。更多信息，请参见同步请求类型。
request_uri	请求URI，包括query-string，路径是URL编码。查询时，您可使用select url_decode(request_uri)解码。
host	请求访问域名
logging_flag	是否开启了日志定期导出到OSS Bucket的功能。
server_cost_time	OSS服务器处理时间，单位：毫秒。
owner_id	Bucket拥有者的阿里云账号ID
requester_id	请求者的阿里云账号ID，匿名访问为短划线（-）。
delta_data_size	OSS Object大小的变化量。如果没有变化则为0；如果不是上传请求，则为短划线（-）。

- 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。

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。
network_out	外网流出量，单位：Byte。

日志字段	说明
put_request	PUT请求次数
storage_type	Bucket存储类型。更多信息，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
end_time	计量截止时间
region	Bucket所在地域

Bucket存储类型

存储类型	描述
standard	标准存储类型
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

操作值	描述
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的生命周期规则
GetBucketLocation	查看Bucket地域
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
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	查看元信息
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

操作值	描述
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
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

操作值	描述
put_style	创建Bucket样式

同步请求类型

同步请求类型	描述
短划线（-）	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

1.6.3. 云数据库RDS

本文介绍云数据库RDS SQL审计日志、慢日志和性能日志的字段详情。

SQL审计日志

日志字段	说明
__topic__	日志主题，固定为rds_audit_log。
owner_id	阿里云账号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
db_version	实例版本号
check_rows	扫描的行数
db	数据库名

日志字段	说明
fail	SQL执行是否出错。包括： • 0：成功 • 1：失败
client_ip	访问RDS实例的客户端IP地址
latency	执行SQL操作后，多久返回结果，单位：微秒。
origin_time	执行操作的时间点
return_rows	返回的行数
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

慢日志

日志字段	说明
__topic__	日志主题，固定为rds_slow_log
owner_id	阿里云账号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
db_version	实例版本号
db_name	数据库名
rows_examined	扫描的行数
rows_sent	返回的行数
start_time	开始执行的时间
query_time	执行的耗时，单位：秒。
lock_time	锁等待的耗时，单位：秒。

日志字段	说明
user_host	客户端信息
query_sql	慢日志SQL语句

性能日志

指标名称	说明
mysql_perf_active_session	活跃连接数，单位：个。
mysql_perf_com_delete	平均每秒Delete语句执行次数
mysql_perf_com_insert	平均每秒Insert语句执行次数
mysql_perf_com_insert_select	平均每秒Insert Select语句执行次数
mysql_perf_com_replace	平均每秒Replace语句执行次数
mysql_perf_com_replace_select	平均每秒Replace Select语句执行次数
mysql_perf_com_select	平均每秒Select语句执行次数
mysql_perf_com_update	平均每秒Update语句执行次数
mysql_perf_conn_usage	实例连接使用率，单位：百分比。
mysql_perf_cpu_usage	实例CPU使用率，单位：百分比。
mysql_perf_data_size	实例数据使用量，单位：MB。
mysql_perf_disk_usage	实例磁盘使用率，单位：百分比。
mysql_perf_ibuf_dirty_ratio	缓冲池脏块的百分率，单位：百分比。
mysql_perf_ibuf_read_hit	缓冲池的读命中率
mysql_perf_ibuf_request_r	平均每秒钟从InnoDB缓冲池的读次数
mysql_perf_ibuf_request_w	平均每秒钟向InnoDB缓冲池的写次数
mysql_perf_ibuf_use_ratio	缓冲池的利用率，单位：百分比。
mysql_perf_inno_data_read	InnoDB平均每秒钟读取的数据量，单位：KB。
mysql_perf_inno_data_written	InnoDB平均每秒钟写入的数据量，单位：KB。
mysql_perf_inno_row_delete	平均每秒从InnoDB表删除的行数
mysql_perf_inno_row_insert	平均每秒从InnoDB表插入的行数
mysql_perf_inno_row_readed	平均每秒从InnoDB表读取的行数

指标名称	说明
mysql_perf_inno_row_update	平均每秒从InnoDB表更新的行数
mysql_perf_innodb_log_write_requests	平均每秒日志写请求数
mysql_perf_innodb_log_writes	平均每秒向日志文件的物理写次数
mysql_perf_innodb_os_log_fsyncs	平均每秒向日志文件完成的fsync()写数量
mysql_perf_ins_size	实例磁盘使用量，单位：MB。
mysql_perf_iops	IOPS，单位：次/秒。
mysql_perf_iops_usage	实例IOPS使用率，单位：百分比。
mysql_perf_kbytes_received	平均每秒钟的输入流量，单位：KB。
mysql_perf_kbytes_sent	平均每秒钟的输出流量，单位：KB。
mysql_perf_log_size	实例binlog使用量，单位：MB。
mysql_perf_mem_usage	实例内存使用率，单位：百分比。
mysql_perf_open_tables	当前打开表数量
mysql_perf_other_size	实例其他空间使用量，单位：MB。
mysql_perf_qps	平均每秒SQL语句执行次数
mysql_perf_slow_queries	平均每秒慢查询数量
mysql_perf_tb_tmp_disk	MySQL执行语句时每秒在磁盘上自动创建的临时表的数量
mysql_perf_threads_connected	MySQL线程连接数
mysql_perf_threads_running	MySQL活跃线程
mysql_perf_tmp_size	实例临时空间使用量，单位：MB。
mysql_perf_total_session	总连接数，单位：个。
mysql_perf_tps	平均每秒事务数

1.6.4. PolarDB MySQL云原生数据库

本文介绍PolarDB MySQL云原生数据库审计日志、慢日志和性能日志的字段详情。

审计日志

日志字段	说明
__topic__	日志主题，固定为polardb_audit_log。
owner_id	阿里云账号ID
region	PolarDB MySQL集群所在地域
cluster_id	PolarDB MySQL集群ID
node_id	PolarDB MySQL节点ID
check_rows	扫描的行数
db	数据库名称
fail	SQL执行是否出错。包括： • 0：成功 • 1：失败
client_ip	访问PolarDB MySQL集群的客户端IP地址
latency	执行SQL操作后，多久返回结果，单位：微秒。
origin_time	执行操作的时间
return_rows	返回的行数
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

慢日志

日志字段	说明
__topic__	日志主题，固定为rds_slow_log。
owner_id	阿里云账号ID
region	PolarDB MySQL集群所在地域
cluster_id	PolarDB MySQL集群ID
node_id	PolarDB MySQL节点ID
db_type	PolarDB数据库类型

日志字段	说明
db_name	PolarDB数据库名
version	PolarDB数据库版本号
rows_examined	扫描的行数
rows_sent	返回的行数
start_time	开始执行的时间
query_time	执行的耗时，单位：秒。
lock_time	锁等待的耗时，单位：秒。
user_host	客户端信息
query_sql	慢日志SQL语句

性能日志

指标名称	说明
mysql_perf_active_session	每秒活跃连接数
mysql_perf_binlog_size	本地Binlog使用量，单位：MB。
mysql_perf_com_delete	每秒DELETE语句执行次数
mysql_perf_com_delete_multi	每秒Multi-DELETE语句执行次数
mysql_perf_com_insert	每秒INSERT语句执行次数
mysql_perf_com_insert_select	每秒INSERT-SELECT语句执行次数
mysql_perf_com_replace	每秒REPLACE语句执行次数
mysql_perf_com_replace_select	每秒REPLACE-SELECT语句执行次数
mysql_perf_com_select	每秒SELECT语句执行次数
mysql_perf_com_update	每秒UPDATE语句执行次数
mysql_perf_com_update_multi	每秒Multi-UPDATE语句执行次数
mysql_perf_cpu_ratio	CPU使用率，单位：百分比。
mysql_perf_created_tmp_disk_tables	每秒创建临时表个数
mysql_perf_data_size	数据空间使用量，单位：MB。

指标名称	说明
mysql_perf_innodb_buffer_dirty_ratio	缓冲池脏块率，单位：百分比。
mysql_perf_innodb_buffer_read_hit	缓冲池读命中率，单位：百分比。
mysql_perf_innodb_buffer_use_ratio	缓冲池使用率，单位：百分比。
mysql_perf_innodb_data_read	每秒从存储引擎读取数据量，单位：Byte。
mysql_perf_innodb_data_reads	每秒缓冲池读取次数
mysql_perf_innodb_data_writes	每秒缓冲池写次数
mysql_perf_innodb_data_written	每秒往存储引擎写入数据量，单位：Byte。
mysql_perf_innodb_log_write_requests	每秒日志写请求数
mysql_perf_innodb_os_log_fsyncs	每秒向日志文件完成的fsync()写数量
mysql_perf_innodb_rows_deleted	每秒删除的行数
mysql_perf_innodb_rows_inserted	每秒插入的行数
mysql_perf_innodb_rows_read	每秒读取的行数
mysql_perf_iops	每秒IOPS
mysql_perf_iops_r	每秒读IOPS
mysql_perf_iops_throughput	每秒总IO吞吐量，单位：MB。
mysql_perf_iops_throughput_r	每秒读IO吞吐量，单位：MB。
mysql_perf_iops_throughput_w	每秒写IO吞吐量，单位：MB。
mysql_perf_iops_w	每秒写IOPS
mysql_perf_kbytes_received	每秒输入流量，单位：KB。
mysql_perf_kbytes_sent	每秒输出流量，单位：KB。
mysql_perf_mem_ratio	内存使用率，单位：百分比。
mysql_perf_mps	每秒数据操作数
mysql_perf_other_log_size	其他日志使用量，单位：MB。

指标名称	说明
mysql_perf_qps	每秒请求数
mysql_perf_redolog_size	本地Redolog使用量，单位：MB。
mysql_perf_slow_queries	平均每秒慢查询数量
mysql_perf_sys_dir_size	系统空间使用量，单位：MB。
mysql_perf_tmp_dir_size	临时空间使用量，单位：MB。
mysql_perf_total_session	当前平均总连接数
mysql_perf_tps	每秒事务数

1.6.5. 分布式关系型数据库DRDS

本文介绍分布式关系型数据库DRDS SQL审计日志的字段详情。

字段名称	字段说明
__topic__	日志主题，固定为drds_audit_log。
instance_id	DRDS实例ID
instance_name	DRDS实例名
owner_id	阿里云账户ID
region	DRDS实例所在地域
db_name	DRDS数据库名
user	执行SQL的用户名
client_ip	访问DRDS实例的客户端IP地址
client_port	访问DRDS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，则显示为跟踪ID、短划线（-）和数字，例如drdsabcdxyz-1。
sql_code	模板SQL的HASH值
hint	SQL执行的HINT
table_name	查询涉及的表名。多表之间以英文逗号（,）分隔。
sql_type	SQL类型。包括Select、Insert、Update、Delete、Set、Alter、Create、Drop、Truncate、Replace和Other。

字段名称	字段说明
sql_type_detail	SQL解析器名称
response_time	响应时间，单位：微秒。
affect_rows	SQL执行返回的行数。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。包括： • 0：成功 • 1：失败
sql_time	SQL开始执行的时间

1.6.6. 负载均衡

本文介绍负载均衡七层访问日志的字段详情。

日志字段	说明
owner_id	阿里云账号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：专有网络 • Classic：经典网络
vpc_id	VPC ID
body_bytes_sent	发送给客户端的Body字节数
client_ip	客户端IP地址
client_port	客户端端口
host	优先从请求参数中获取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地址作为host。
http_host	请求报文host header的内容
http_referer	Proxy收到的请求报文中HTTP referer header的内容
http_user_agent	Proxy收到的请求报文中HTTP user-agent的内容
http_x_forwarded_for	Proxy收到的请求报文中HTTP forwarded-for header的内容

日志字段	说明
http_x_real_ip	真实的客户端IP地址
read_request_time	Proxy读取请求的时间，单位：毫秒。
request_length	请求报文的长度，包括startline、HTTP header和HTTP Body。
request_method	请求方法
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Scheme
server_protocol	Proxy收到的HTTP协议的版本
slb_vport	SLB的监听端口
slbid	SLB实例ID
ssl_cipher	使用的cipher
ssl_protocol	建立SSL连接所使用的协议
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
write_response_time	Proxy写的响应时间，单位：毫秒。

1.6.7. 堡垒机

本文介绍堡垒机操作日志的字段详情。

日志字段	说明
__topic__	日志主题
owner_id	阿里云账号ID

日志字段	说明
content	日志内容
event_type	事件类型。更多信息，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
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	重命名文件
file.Delete	删除文件
file.DeleteDir	删除目录
file.CreateDir	创建目录
graph.Text	图形文字
graph.Keyboard	键盘事件

1.6.8. Web应用防火墙

本文介绍Web应用防火墙访问日志的字段详情。

字段	说明
__topic__	日志主题，固定为waf_access_log。
owner_id	阿里云账号ID
acl_action	WAF精准访问控制规则行为，例如pass、drop、captcha。 空值或短划线（-）也表示pass。
block_action	触发拦截的WAF防护类型，详细说明如下： • tmd：CC攻击防护 • waf：Web应用攻击防护 • acl：精准访问控制 • geo：地域封禁 • antifraud：数据风控 • antibot：防爬封禁
body_bytes_sent	发送给客户端的HTTP Body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。
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，包括： • 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

字段	说明
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	访问请求发生的时间
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。 多个地址之间以英文逗号（,）分隔。
upstream_response_time	源站响应WAF请求的时间，单位：秒。 如果返回短划线（-），表示响应超时。
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	阿里云账号ID

字段	说明
waf_action	Web攻击防护策略行为。包括： • block表示拦截。 • by pass或其它值均表示放行。
bypass_matched_ids	客户端请求命中的WAF放行类规则的ID，具体包括白名单规则、设置了放行动作的自定义防护策略规则。 如果请求同时命中了多条放行类规则，该字段会记录所有命中的规则ID。多个规则ID间使用半角逗号（,）分隔。
final_plugin	WAF对客户端请求最终执行的防护动作（final_action）对应的防护模块。 如果一个请求未触发任何防护模块（包括命中了放行类规则、客户端完成滑块或JS校验后触发放行的情况），则不会记录该字段。 如果一个请求同时触发了多个防护模块，则仅记录最终执行的防护动作（final_action）对应的防护模块。
final_action	WAF对客户端请求最终执行的防护动作。 如果一个请求未触发任何防护模块（包括命中了放行类规则、客户端完成滑块或JS校验后触发放行的情况），则不会记录该字段。 如果一个请求同时触发了多个防护模块，则仅记录最终执行的防护动作。防护动作的优先级由高到低依次为：拦截（block）、严格滑块校验（captcha_strict）、普通滑块校验（captcha）和JS校验（js）。
final_rule_id	WAF对客户端请求最终应用的防护规则的ID，即final_action对应的防护规则的ID。
final_rule_type	WAF对客户端请求最终应用的防防护规则（final_rule_id）的子类型。例如在*final_plugin:waf*类型下有final_rule_type:sqli、final_rule_type:xss等细分的规则类型。
waf_rule_id	匹配的WAF的相关规则ID
waf_rule_type	WAF对客户端请求最终应用的防防护规则（final_rule_id）的子类型。 例如在 `final_plugin:waf` 类型下有 `final_rule_type:sqli` 、 `final_rule_type:xss` 等细分的规则类型。
acl_rule_type	客户端请求命中的IP黑名单、自定义防护策略（ACL访问控制）规则的类型。取值： • custom：表示自定义防护策略（ACL访问控制）规则。 • blacklist：表示IP黑名单规则。
cc_rule_id	CC攻击规则拦截ID。

字段	说明
cc_rule_type	客户端请求命中的CC安全防护、自定义防护策略（CC攻击防护）规则的类型。取值： • custom：表示自定义防护策略（CC攻击防护）规则。 • system：表示CC安全防护规则。
ssl_cipher	SSL加密套件
ssl_protocol	SSL协议版本

1.6.9. 云防火墙

本文介绍云防火墙的互联网边界防火墙流量日志和VPC边界防火墙流量日志的字段详情。

互联网边界防火墙流量日志

日志字段	说明
__topic__	日志主题，固定为cloudfirewall_access_log。
owner_id	阿里云账号ID
log_type	日志类型，固定为internet_log。
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，包括： • 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，Unix时间戳格式，单位：秒。
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。

日志字段	说明
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	访问流量所属的地域
rule_result	命中规则结果，包括： • 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，Unix时间戳，单位：秒。
start_time_min	会话开始时间的分钟取整，Unix时间戳，单位：秒。
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：pps。
src_private_ip	私网IP地址
vul_level	漏洞风险等级，包括： • 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
ips_rule_name	命中IPS的规则名称（中文）

日志字段	说明
ips_rule_name_en	命中IPS的规则名称（英文）
attack_type_name	攻击类型的名称（中文）
attack_type_name_en	攻击类型的名称（英文）
proxy_acl_rule_id	命中正向代理ACL的规则ID

VPC边界防火墙流量日志

日志字段	说明
__topic__	主题，固定为cloudfirewall_vpc_log。
log_type	日志类型，固定为vpc_firewall_log。
aliuid	阿里云账号ID
app_name	应用名。值可能为HTTPS、NTP、SIP、SMB、NFS、DNS等，未知时为Unknown。
domain	域名
dst_ip	目的IP地址
dst_port	目的端口
dst_region	目的地域ID
dst_network_instance_id	目的网络实例ID，可能为VPC、VBR、CCN的网络实例ID。
end_time	会话结束时间，Unix时间戳格式，单位：秒。
firewall_id	VPC防火墙ID。 • 云企业网场景下，显示的是云企业网ID，例如cen-6srj4tvjjovhbc。 • 高速通道场景下，显示的是防火墙实例ID，例如vfw-123。
in_bps	入流量大小，单位：bps。
in_packet_bytes	入流量总子节数
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，TCP或UDP。
out_bps	出方向流量大小，单位：bps。
out_packet_bytes	出方向总流量字节数

日志字段	说明
out_packet_count	出方向报文数
out_pps	出方向流量大小，单位：pps。
rule_result	命中规则结果。包括： • pass：通过 • alert：告警 • drop：丢弃
src_ip	源IP地址
src_port	源端口
src_region	源地域ID
src_network_instance_id	源网络实例ID，可能为VPC、VBR、CCN的网络实例ID。
start_time	会话开始时间，Unix时间戳格式，单位：秒。
start_time_min	会话开始时间的分钟取整，Unix时间戳格式，单位：秒。
tcp_seq	TCP序列号
total_bps	总流量大小，单位：bps。
total_packet_bytes	流量总字节数，单位：字节。
total_packet_count	流量总报文数
total_pps	总流量大小，单位：pps。
vul_level	漏洞风险等级，包括： • 1：低危 • 2：中危 • 3：高危
ips_rule_name	命中IPS规则中文名称
ips_rule_name_en	命中IPS规则英文名称
attack_type_name	攻击类型中文名称
attack_type_name_en	攻击类型英文名称

1.6.10. DDoS防护

本文介绍DDoS防护访问日志的字段详情。

DDoS高防（新BGP）

日志字段	说明
__topic__	日志主题，固定为ddoscoo_access_log。
owner_id	阿里云账号ID
body_bytes_sent	请求Body的大小，单位：字节。
cc_action	CC防护策略行为，例如none、challenge、pass、close、captcha、wait、login等。
cc_phase	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。
cc_blocks	是否被CC防护策略阻断。包括： • 1表示阻断。 • 其他内容表示通过。
content_type	内容类型
host	源网站
http_cookie	请求Cookie
http_referer	请求Referer。如果HTTP Header中没有Referer，则显示为短划线（-）。
http_user_agent	请求User Agent
http_x_forwarded_for	通过代理跳转的上游用户的IP地址。
https	该请求是否为HTTPS请求。取值如下： • true：该请求是HTTPS请求。 • false：该请求是HTTP请求。
isp_line	线路信息，例如BGP、电信、联通等。
matched_host	匹配到的源站，可能是泛域名。如果未匹配，则显示为短划线（-）。
real_client_ip	客户端的真实IP地址。如果获取不到，则显示为短划线（-）。
remote_addr	请求连接的客户端IP地址
remote_port	请求连接的客户端端口号
request_length	请求长度，单位：字节。
request_method	请求的HTTP方法
request_time_msec	请求时间，单位：微秒。
request_uri	请求路径

日志字段	说明
server_name	匹配到的host名。如果未匹配，则显示为default。
status	HTTP状态
time	时间
ua_browser	浏览器
ua_browser_family	浏览器系列
ua_browser_type	浏览器类型
ua_device_type	客户端设备类型
ua_os	客户端操作系统
ua_os_family	客户端操作系统系列
upstream_addr	回源地址列表，格式为IP:Port。 多个地址之间以英文逗号（,）分隔。
upstream_ip	实际回源地址IP地址
upstream_response_time	回源响应时间，单位：秒。
upstream_status	回源请求HTTP状态

DDoS高防（国际）

日志字段	说明
__topic__	日志主题，固定为ddosdip_access_log。
owner_id	阿里云账号ID
body_bytes_sent	请求Body的大小，单位：字节。
cc_action	CC防护策略行为，例如none、challenge、pass、close、captcha、wait、login等。
cc_phase	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。
cc_blocks	是否被CC防护策略阻断。包括： • 1表示阻断。 • 其他内容表示通过。
content_type	内容类型

日志字段	说明
host	源网站
http_cookie	请求Cookie
http_referer	请求Referer。如果HTTP Header中没有Referer，则显示为短划线（-）。
http_user_agent	请求User Agent
http_x_forwarded_for	通过代理跳转的上游用户的IP地址。
https	该请求是否为HTTPS请求。取值如下： • true：该请求是HTTPS请求。 • false：该请求是HTTP请求。
isp_line	线路信息，例如BGP、电信、联通等。
matched_host	匹配到的源站，可能是泛域名。如果未匹配，则显示为短划线（-）。
real_client_ip	客户端的真实IP地址。如果获取不到，则显示为短划线（-）。
remote_addr	请求连接的客户端IP地址
remote_port	请求连接的客户端端口号
request_length	请求长度，单位：字节。
request_method	请求的HTTP方法
request_time_msec	请求时间，单位：微秒。
request_uri	请求路径
server_name	匹配到的Host名。如果未匹配，则显示为default。
status	HTTP状态
time	时间
ua_browser	浏览器
ua_browser_family	浏览器系列
ua_browser_type	浏览器类型
ua_device_type	客户端设备类型
ua_os	客户端操作系统
ua_os_family	客户端操作系统系列

日志字段	说明
upstream_addr	回源地址列表，格式为IP:Port。 多个地址之间以英文逗号（,）分隔。
upstream_ip	实际回源地址IP地址
upstream_response_time	回源响应时间，单位：秒。
upstream_status	回源请求HTTP状态

DDoS原生

字段	说明
__topic__	日志主题，固定为ddosbqp_access_log。
data_type	日志类型
event_type	事件类型
ip	事件发生的IP地址
subnet	代播的网段
event_time	事件发生时的时间，例如2020-01-01。
qps	事件发生时的每秒查询率
pps_in	事件发生时的入流量，单位：pps。
new_con	事件发生时的新连接
kbps_in	事件发生时的入流量，单位：bps。
instance_id	实例ID
time	日志时间，例如2020-07-17 10:00:30。
destination_ip	目的IP地址
port	目的端口
total_traffic_in_bps	总入流量，单位：bps。
total_traffic_drop_bps	总入流量的丢弃量，单位：bps。
total_traffic_in_pps	总入流量，单位：pps。
total_traffic_drop_pps	总入流量的丢弃量，单位：pps。
pps_types_in_tcp_pps	按协议统计的tcp类型入流量，单位：pps。

字段	说明
pps_types_in_udp_pps	按协议统计的udp类型入流量，单位：pps。
pps_types_in_icmp_pps	按协议统计的icmp类型入流量，单位：pps。
pps_types_in_syn_pps	按协议统计的syn类型入流量，单位：pps。
pps_types_in_ack_pps	按协议统计的ack类型入流量，单位：pps。
user_id	阿里云账号ID

1.6.11. 云安全中心

本文介绍云安全中心网络日志、安全日志和主机日志的字段详情。

网络日志

- DNS日志

日志字段	说明
__topic__	日志主题，固定为sas-log-dns。
owner_id	阿里云账号ID
additional	additional字段，各个值之间以竖线（|）分隔。
additional_num	additional字段数量
answer	DNS回答信息，各个值之间以竖线（|）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，包括： ◦ in：入方式 ◦ out：出方向
qid	查询ID
qname	查询域名

日志字段	说明
qtype	查询类型
query_datetime	查询时间戳，单位：毫秒。
rcode	返回代码
region	来源地域ID，包括： ○ 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	说明
__topic__	日志主题，固定为local-dns。
owner_id	阿里云账号ID
answer_rda	DNS回答信息，各个值之间以竖线（|）分隔。
answer_ttl	DNS回答的时间周期，各个值之间以竖线（|）分隔。
answer_type	DNS回答的类型，各个值之间以竖线（|）分隔。
anwser_name	DNS回答的名称，各个值之间以竖线（|）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

字段名	说明
ip_ttl	IP地址的周期
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	阿里云账号ID
content_length	内容长度
dst_ip	目标IP地址
dst_port	目标端口

日志字段	说明
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
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	阿里云账号ID
name	漏洞名称
alias_name	漏洞别名
op	操作信息，包括： ○ new：新增 ○ verify：验证 ○ fix：修复
status	状态。更多信息，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。

日志字段	说明
type	漏洞类型，包括： ○ 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	阿里云账号ID
level	风险级别
op	操作信息，包括： ○ new：新增 ○ verify：验证
risk_name	风险名称
status	状态。更多信息，请参见安全日志状态码。
sub_type_alias	子类型别名
sub_type_name	子类型名称
type_name	类型名称。更多信息，请参见基线type-sub-type列表。
type_alias	类型别名
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

type_name	sub_type_name
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
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

type_name	sub_type_name
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
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
__topic__	日志主题，固定为sas-security-log。
data_source	数据源。更多信息，请参见安全告警data_source列表。
level	告警级别
name	名称

日志字段	说明
op	操作信息，包括： ○ new：新增 ○ dealing：处理
status	状态。更多信息，请参见安全日志状态码。
uuid	客户端号
detail	告警详情
unique_info	告警的唯一标识

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。
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

日志字段	说明
pfilename	父进程文件名
pfilepath	父进程文件完整路径
cmd_chain	进程链
containerhostname	容器主机名
containerpid	容器PID
containerimageid	镜像ID
containerimagename	镜像名称
containername	容器名称
containerid	容器ID
cwd	进程运行目录

- 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1 MB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	说明
__topic__	日志主题，固定为aegis-log-crack。
owner_id	阿里云账号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	连接协议
status	连接状态。更多信息，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__	日志主题，固定为aegis-snapshot-port。

日志字段	说明
owner_id	阿里云账号ID
uuid	客户端号
ip	客户端IP地址
proto	监听协议
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	阿里云账号ID
name	漏洞名称
alias_name	漏洞别名
op	操作信息，包括： ○ new：新增 ○ verify：验证 ○ fix：修复
status	连接状态。更多信息，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，包括： ○ sys：windows漏洞 ○ cve：Linux漏洞 ○ cms：Web CMS漏洞 ○ EMG：紧急漏洞
uuid	客户端号

1.6.12. API网关

本文介绍API网关访问日志的字段详情。

日志字段	说明
owner_id	API提供者的阿里云账号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	HTTP请求方法
path	请求路径
domain	调用的域名
statusCode	HTTP状态码
errorMessage	错误信息
appId	调用者的应用ID
appName	调用者的应用名称
clientIp	调用者的客户端IP地址
exception	返回的错误信息
region	地域
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	返回的数据大小，单位：字节。
serviceLatency	后端延迟，单位：毫秒。

1.6.13. 文件存储

本文介绍文件存储NAS访问日志的字段详情。

日志字段	说明
owner_id	阿里云账号ID

日志字段	说明
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。

1.6.14. 应用集成

本文介绍应用集成操作日志的字段详情。

日志字段	说明
__topic__	日志主题，固定为appconnect_oplog。
uid	阿里云账号ID
execution_id	单次请求或者触发的唯一标识
status	本次集成流的执行状态，仅包含begin、done。
flow_name	集成流名称
step	集成流中步骤的名称，步骤的唯一标识。
id	步骤执行ID。集成流每次执行的唯一索引，可解码为stepTime时间戳字段。 在包含循环的业务场景中，同一步骤可执行多次，步骤名称相同，id不同。
type	步骤类型
duration	步骤执行持续时间，单位：纳秒。

日志字段	说明
message	步骤执行过程中，输出的信息，字符串文本格式。
step_time	集成流每次触发步骤开始执行的时间
container_ip	集成pod的IP地址
integration_name	集成pod的名称
failed	步骤运行是否成功

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**。
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**。
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

仪表盘	描述
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
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服务。

前提条件

已安装和配置Terraform。具体操作，请参见在Cloud Shell中使用Terraform、在本地安装和配置Terraform。

背景信息

Terraform是一种开源工具，用于安全高效地预览、配置和管理云基础架构和资源。Terraform的命令行接口（CLI）提供了一种简单机制，用于将配置文件部署到阿里云或其他任意支持的云上，并对其进行版本控制。

阿里云是中国国内第一家与Terraform集成的云厂商。目前terraform-provider-alicloud已经提供了超过163个Resource和113个Data Source，覆盖计算、存储、网络、负载均衡、CDN、容器服务、中间件、访问控制和数据库等阿里云产品，满足大量大客户的自动化上云需求。

使用Terraform的优势

- 将基础结构部署到多个云

  Terraform适用于多云方案，将类似的基础结构部署到阿里云、其他云厂商或者本地数据中心。开发人员能够使用相同的工具和相似的配置文件同时管理不同云厂商的资源。

- 自动化管理基础结构

  您可以使用Terraform创建配置文件模板，用于重复、可预测的方式定义、预配和配置ECS资源，减少因人为因素导致的部署和管理错误。您可以多次部署同一模板，创建相同的开发、测试和生产环境。

- 基础架构即代码（Infrastructure as Code）

  Terraform支持通过代码来管理、维护资源，允许保存基础设施状态，从而使您能够跟踪对系统（基础设施即代码）中不同组件所做的更改，并与其他人共享这些配置 。

- 降低开发成本

  您通过按需创建开发和部署环境来降低成本。并且，您可以在系统更改之前进行评估。

步骤一：配置身份信息以及日志审计服务的中心化地域

在环境变量中配置用户身份信息以及日志审计服务的中心Project所在地域。

```
export ALICLOUD_ACCESS_KEY="LTAIUrZCw3****"
export ALICLOUD_SECRET_KEY="zfwwWAMWIAiooj14GQ2****"
export ALICLOUD_REGION="cn-huhehaote"
```

参数	说明
ALICLOUD_ACCESS_KEY	阿里云访问密钥AccessKey ID。更多信息，请参见访问密钥。
ALICLOUD_SECRET_KEY	阿里云访问密钥AccessKey Secret。更多信息，请参见访问密钥。
ALICLOUD_REGION	日志审计服务的中心Project所在地域。目前支持如下地域： • 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）、德国（法兰克福）、印尼（雅加达）

步骤二：RAM授权

使用Terraform完成RAM授权。具体操作，请参见alicloud_ram_policy。在授权中所涉及的权限策略信息请参见自定义授权日志采集与同步。

步骤三：配置日志采集

1. 创建一个Terraform工作目录*sls*，并在该目录下创建一个名为*terraform.tf*的文件。
2. 在*terraform.tf*文件中，添加如下内容。

```
resource "alicloud_log_audit" "example" {
  display_name = "tf-audit-test"
  aliuid     = "12345678"
}
```

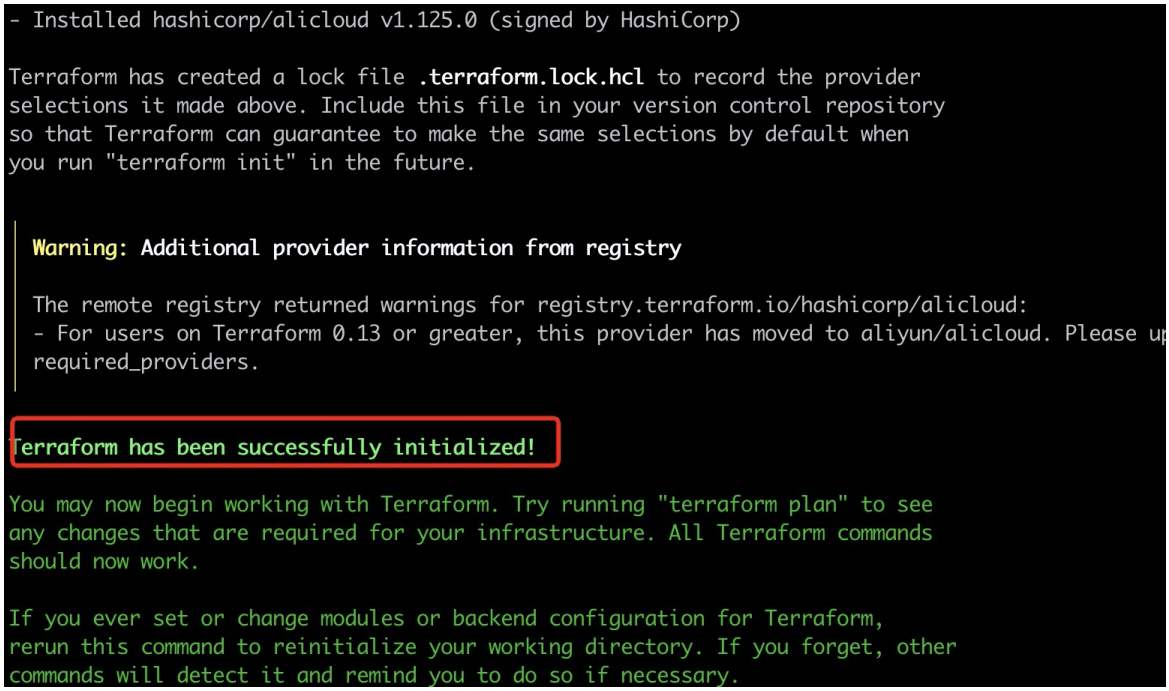
相关参数说明如下：

参数	说明
example	Resource名称。自定义配置。
display_name	采集配置名称。自定义配置。
aliuid	阿里云账号ID。

3. 在*sls*目录下，执行如下命令，初始化terraform工作目录。

```
terraform init
```

如果返回结果中提示 `Terraform has been successfully initialized!` ，表示初始化成功。



4. 编辑*terraform.tf*文件，配置日志审计服务相关参数。

配置示例如下。Terraform中日志审计采集配置的完整参数说明，请参见Terraform-Aliyun Log Audit。

- 单账号采集

```
resource "alicloud_log_audit" "example" {
 display_name = "tf-audit-test"
 aliuid     = "12345678"
 variable_map = {
  "actiontrail_enabled" = "true",
  "actiontrail_ttl" = "180"
 }
}
```

- 多账号采集

```
resource "alicloud_log_audit" "example" {
 display_name = "tf-audit-test"
 aliuid     = "12345678"
 variable_map = {
  "actiontrail_enabled" = "true",
  "actiontrail_ttl" = "180"
 }
 multi_account = ["123456789123", "12345678912300123"]
}
```

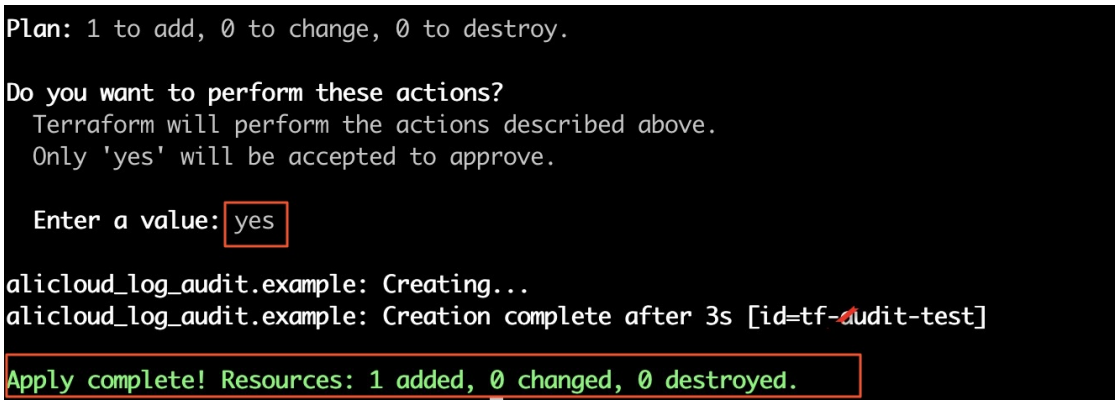
参数	说明
actiontrail_enabled	是否开启操作审计（Actiontrail）日志的采集，取值： - *true*：开启。 - *false*：关闭。
actiontrail_ttl	设置操作审计日志的存储时间。
multi_account	多账号采集时，需配置多个阿里云账号ID。

5. 使*terraform.tf*文件中的采集配置生效。
   i. 执行如下命令。

   ```
   terraform apply
   ```

   ii. 输入*yes*。

   如果返回结果中提示 `Apply complete!` ，表示应用采集配置成功，日志审计服务将按照采集配置进行日志采集和存储。



相关操作

您还可以通过Terraform完成如下相关操作。

- 导入已有审计配置。

  ```
  terraform import alicloud_log_audit.example tf-audit-test
  ```

  其中，*example*和*tf-audit-test*，请根据实际情况替换。

  ```
  lichang@B-QPJTMD6M-0104 terrafrom % terraform import alicloud_log_audit.example tf-audit-test
  alicloud_log_audit.example: Importing from ID "tf-audit-test"...
  alicloud_log_audit.example: Import prepared!
    Prepared alicloud_log_audit for import
  alicloud_log_audit.example: Refreshing state... [id=tf-audit-test]

  Import successful!

  The resources that were imported are shown above. These resources are now in
  your Terraform state and will henceforth be managed by Terraform.
  ```

  执行完毕后，您可以查看terraform工作目录下的*terraform.tfstate*文件内容。*terraform.tfstate*文件内容即为导入的采集配置。

  > **注意**
  >
  > - 如果您想要将导入的采集配置迁移到*terraform.tf*文件中，需要手动拷贝，并对格式做适当调整，满足*terraform.tf*文件的格式要求。
  > - 如果您已经在当前的terraform工作目录执行过terrraform apply或者terraform import命令，则此时再次执行terraform import命令会失败。您需要删除当前目录下的*terraform.tfstate*文件后再重新执行terraform import命令。

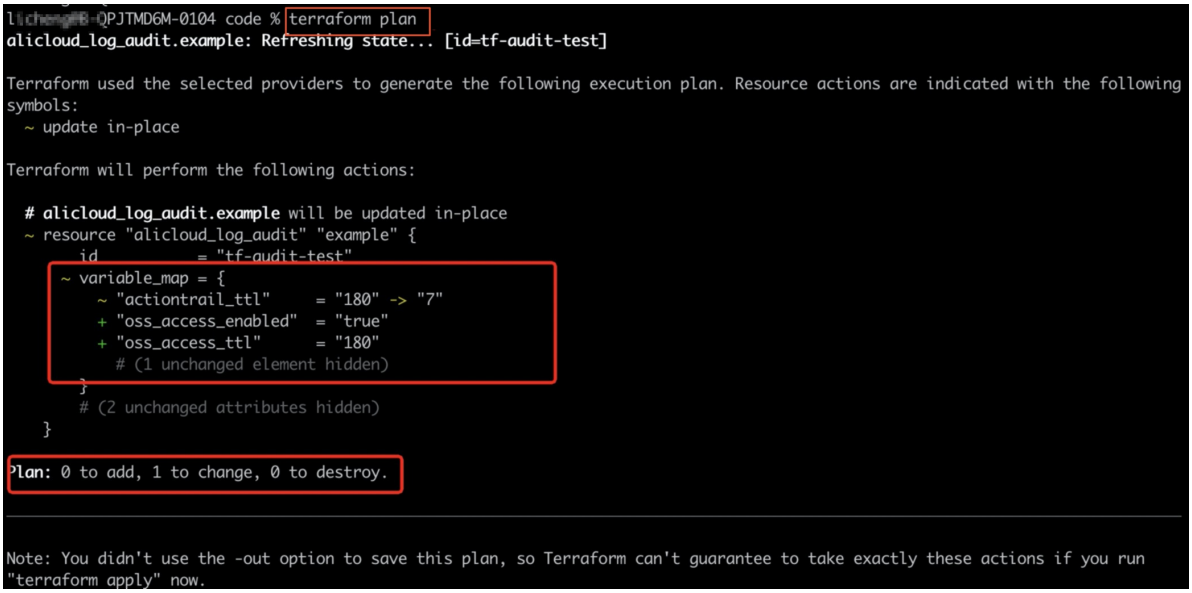
- 查看当前采集配置。

  ```
  terraform show
  ```

  ```
  li[redacted]0104 terrafrom % terraform show
  # alicloud_log_audit.example:
  resource "alicloud_log_audit" "example" {
      aliuid       = "1[redacted]0"
      display_name = "tf-audit-test"
      id           = "tf-audit-test"
      variable_map = {
          "actiontrail_enabled" = "true"
          "actiontrail_ttl"     = "180"
      }
  }
  ```

- 查看当前terraform工作目录下的*terraform.tf*文件与已生效的采集配置的差异。

  ```
  terraform plan
  ```



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、PolarDB、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	PolarDB集群所属的阿里云账号ID。

云产品	采集对象	属性	说明
PolarDB	PolarDB集群	地域：region	PolarDB集群所属的地域，如cn-shanghai。
		集群ID：cluster.id	PolarDB集群ID。
		集群名：cluster.name	PolarDB集群名称。
		集群兼容的DB类型：cluster.db_type	PolarDB集群兼容的DB类型，目前只支持MySQL。
		集群兼容的DB版本：cluster.db_version	DB版本号，可选值为8.0、5.7和5.6。
		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。
DRDS	DRDS实例	账号：account.id	DRDS实例所属的阿里云账号ID。
		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。

云产品	采集对象	属性	说明
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。
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。
		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。

云产品	采集对象	属性	说明
Kubernetes容器（ Ingress访问日志）	Kubernetes集群	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

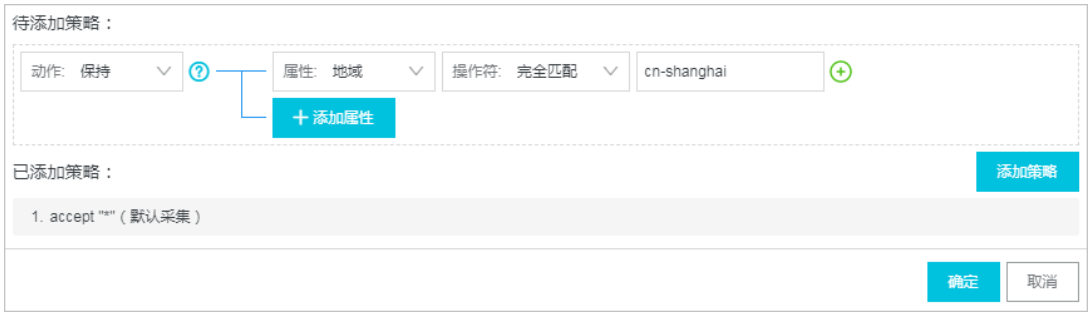
1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**日志审计服务**。
3. 选择**云产品接入 > 全局配置**，单击**修改**。
4. 单击目标云产品右侧的**采集策略**。
5. 配置采集策略。

   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。更多信息，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。更多信息，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==。更多信息，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**。

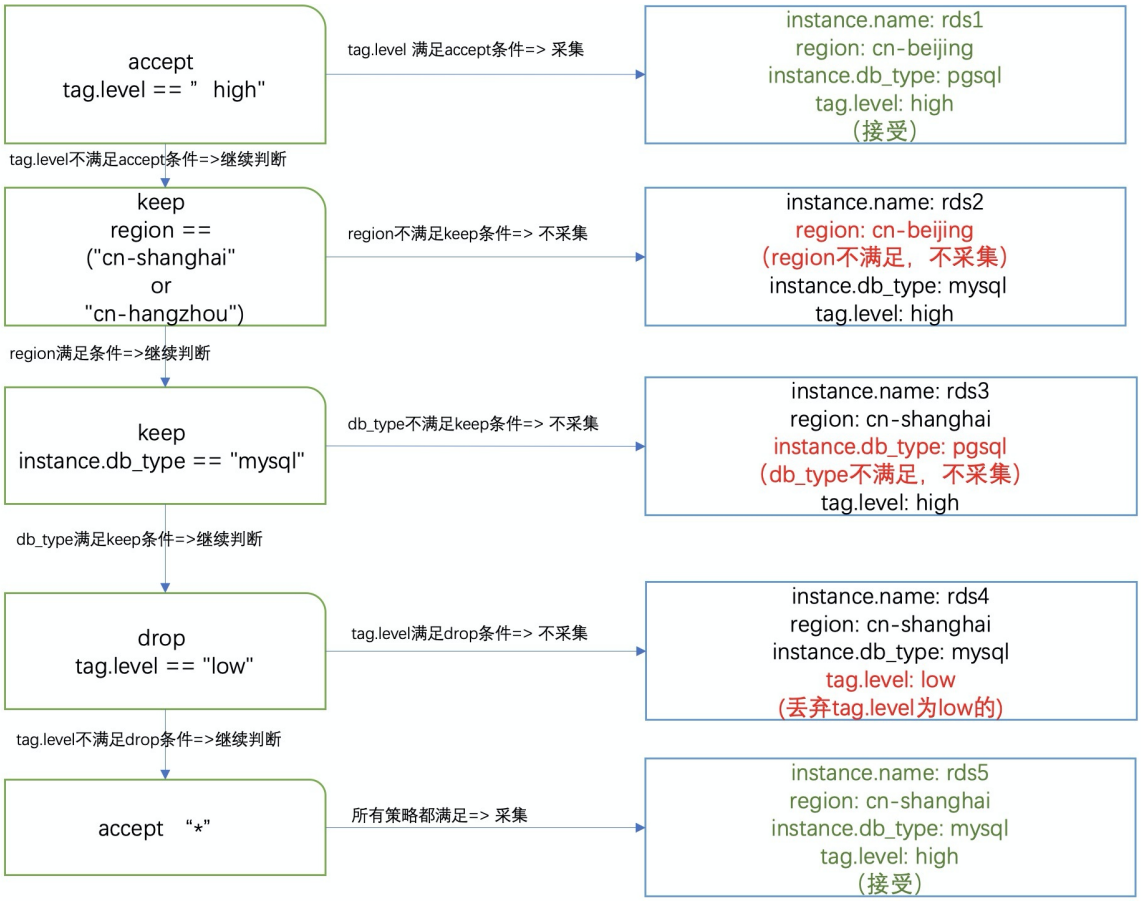
b. 在**规则**文本框中，配置采集策略，并单击**确定**。

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，半角问号（?）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 "*"
```

1.10. 告警

1.10.1. 设置告警

日志审计服务已内置告警规则，您开启对应的告警实例即可实时监控日志审计服务。本文介绍设置告警的相关操作。

前提条件

已在**全局配置**页面中开启目标云产品的审计功能。具体操作，请参见配置日志采集。

背景信息

日志审计服务中已内置告警规则、SLS审计内置告警策略、SLS审计内置行动策略、SLS审计内置用户组和SLS审计内置内容模板。它们之间的关联如下：

- 通过告警规则指定SLS审计内置告警策略。

  > **说明** 日志审计服务中的告警规则已绑定SLS审计内置告警策略，无法解绑和更换绑定。

- 通过SLS审计内置告警策略指定SLS审计内置行动策略。
- 通过SLS审计内置行动策略指定SLS审计内置用户组和SLS审计内置内容模板。

配置流程

您可以直接使用内置的告警资源，也可以自定义告警资源，具体设置告警的流程如下：

- 使用内置的告警资源

  如果您希望快速完成告警设置，通过语音、短信或邮件接收到告警通知，您可以根据如下流程完成设置。

  i. 创建用户
  ii. 将用户添加到SLS审计内置用户组
  iii. 开启告警实例

- 自定义告警资源

  如果您希望根据实际场景自定义告警资源，您可以根据如下流程完成设置。

  i. 创建用户和用户组
  ii. 创建内容模板
  iii. 创建行动策略

iv. 修改内置告警策略所绑定的行动策略

v. 设置白名单

vi. 开启告警实例

日志服务提供的内置资源可满足大部分告警场景，在实际场景中，你可以综合上述两种方式设置告警。本文以内置的告警资源为例。

步骤一：创建用户

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**。
3. 在左侧导航栏中，选择**审计告警 > 用户管理 > 用户管理**。
4. 创建用户。

   具体操作，请参见创建用户。

步骤二：将用户添加到SLS审计内置用户组

1. 在左侧导航栏中，选择**审计告警 > 用户管理 > 用户组管理**。
2. 在用户组列表中，单击**SLS审计内置用户组**对应的**修改**。
3. 在**修改用户组**中，将已创建的用户从**待添加成员**区域添加到**已添加成员**区域，然后单击**确认**。

步骤三：开启告警实例

1. 在左侧导航栏中，选择**审计告警 > 规则配置 > 告警规则**。
2. 在告警规则列表中，找到目标告警规则，单击**开启**。

   开启告警实例后，日志服务开始实时监控日志审计服务。如果您需要开启多个告警实例，可单击**添加**。

   告警规则的参数说明请参见告警规则总览。

相关操作

操作	说明
设置白名单	针对特定告警规则，如果您希望某些用户（或者实例ID、IP地址）进行操作时不触发告警，可将其设置为白名单。 不同告警规则对应的白名单配置不同。更多信息，请参见告警规则总览。
关闭告警实例	关闭告警实例后，告警实例不会再触发告警，**状态**变更为**未开启**。 该操作不会删除实例参数中已设置的信息。需要再次监控时，无需重新设置实例参数。
临时关闭告警实例	临时关闭告警实例后，在指定时间内不再触发告警。
恢复告警实例	处于临时关闭状态的告警实例，可随时恢复告警。
删除告警实例	删除告警实例，**状态**变更为**未创建**。 该操作会删除实例参数中已设置的信息（例如阿里云账号）。需要再次监控时，需要重新设置实例参数。

操作	说明
升级告警实例	当日志服务对告警规则进行较大的功能升级或升级后需要您额外配置时，系统会提示您升级告警规则。一般情况下，系统会自动完成升级。
手动初始化告警	如果误删除告警初始化产生的资产或者发生首次初始化告警资产失败的情况，可通过此操作强制重新初始化告警相关内容。
修改内置告警策略所绑定的行动策略	如果您要使用自定义的行动策略，则在创建行动策略后，需在**告警策略**页面，修改SLS审计内置告警策略的所绑定的行动策略。

1.10.2. 告警规则

1.10.2.1. 告警规则总览

本文介绍日志审计服务的内置告警规则，包括日志审计合规、账号安全、权限控制和流量安全等。了解告警规则，有助于您快速发现审计相关问题。

告警规则列表

支持的告警规则类型如下表所示。设置告警参数、设置白名单相关操作，请参见设置告警。

类型	告警规则
日志审计合规	云安全中心日志审计配置检测
	RDS日志审计配置检测
	PolarDB（DRDS）日志审计配置检测
	K8s日志审计配置检测
	应用防火墙（WAF）日志审计配置检测
	堡垒机日志审计配置检测
	API网关日志审计配置检测
	云防火墙日志审计配置检测
	日志审计状态检测
	ActionTrail日志审计配置检测
	RAM子账号无MFA登录告警
	RAM密码过期策略异常设置告警
	Root账号无MFA登录告警
	RAM密码登录重试策略异常设置告警
	Root账户连续登录告警

类型	告警规则
安全	RAM历史密码检查策略异常设置告警
	密钥配置变更告警
	账号连续登录失败告警
	Root账号AK使用检测
	RAM密码长度策略异常设置告警
权限控制	OSS Bucket权限变更告警
	RAM策略变更告警
	RAM策略异常添加告警
OSS操作合规	OSS Bucket加密关闭告警
	OSS新创建的Bucket加密未开启告警
	OSS Bucket访问日志记录关闭告警
	OSS新创建的Bucket访问日志记录未开启告警
RDS操作合规	RDS实例SQL洞察关闭告警
	RDS实例访问白名单异常设置告警
	新创建的RDS实例的SSL未开启告警
	新创建的RDS实例的TDE未开启告警
	RDS实例SSL关闭告警
	RDS实例配置变更告警
SLB操作合规	负载均衡修改保护关闭告警
	负载均衡健康检查关闭告警
ECS操作合规	ECS磁盘加密关闭告警
	ECS自动快照策略关闭告警
	安全组配置变更告警
	ECS网络类型检测
VPC操作合规	VPC网络路由变更告警
	VPC流日志配置异常变更告警

类型	告警规则
	VPC通用配置变更告警
云防火墙操作合规	云防火墙控制策略变更告警
API调用	未授权的API调用告警
TDI操作合规	云安全中心网页防篡改功能关闭告警
K8s安全	K8s Warning事件数过多告警
	K8s频繁删除事件告警
	K8s错误事件数过多告警
RDS安全	RDS慢SQL检测
	RDS大批量数据删除告警
	RDS外网访问检测
	RDS查询SQL平均执行时间监控告警
	RDS数据库更新峰值监控告警
	RDS数据库查询峰值监控告警
	RDS实例释放告警
	RDS高频访问IP检测
	RDS更新SQL平均执行时间监控告警
	RDS登录失败次数过多告警
	RDS大批量数据修改事件告警
	RDS危险的SQL执行告警
	RDS SQL执行错误数过多告警
SLB流量安全	负载均衡响应报文长度异常检测
	负载均衡请求报文长度异常检测
	负载均衡平均响应延迟过高告警
	负载均衡HTTP访问协议开启告警
	负载均衡访问UV异常检测
	负载均衡访问PV异常检测

类型	告警规则
API网关流量安全	API网关服务端平均延时过高告警
	API网关后端服务器错误率过高告警
	API网关请求成功率过低告警
OSS流量安全	OSS流入流量异常检测
	OSS Bucket有效请求率过低告警
	OSS外网访问检测
	OSS访问PV异常检测
	OSS流量异常检测
	OSS流出流量异常检测
	OSS访问UV异常检测
K8s流量安全	K8s非法访问次数过多告警
	K8s Ingress平均请求延迟过高告警
	K8s Ingress后端平均响应延迟过高告警
	K8s Ingress请求成功率过低告警
OSS数据安全	OSS Bucket账号访问控制
	OSS频繁删除对象告警
NAS数据安全	文件存储操作错误检测
	文件存储大批量删除文件告警
WAF安全事件	应用防火墙有效请求率过低告警
	应用防火墙防护网站被攻击次数过多告警
TDI安全事件	云安全中心高优先级告警数过多
	云安全中心新增漏洞数过多
	云安全中心有效请求率过低告警
	云安全中心新增告警数过多
	云安全中心外网DNS请求成功率过低告警
	云防火墙流出流量拦截告警

云防火墙安全事件类型	告警规则
	云防火墙流入流量拦截告警

1.10.2.2. 日志审计合规

本文介绍日志审计合规的告警规则，包括OSS、RDS、PolarDB、SLB、NAS、K8s等云产品的日志审计合规规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现日志审计合规问题。

告警规则列表

支持的告警规则列表如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- 云安全中心日志审计配置检测
- RDS日志审计配置检测
- 日志审计状态检测
- PolarDB（DRDS）日志审计配置检测
- K8s日志审计配置检测
- ActionTrail日志审计配置检测
- OSS（对象存储）日志审计配置检测
- 应用防火墙（WAF）日志审计配置检测
- 堡垒机日志审计配置检测
- NAS（文件存储）日志审计配置检测
- API网关日志审计配置检测
- SLB日志审计配置检测
- 云防火墙日志审计配置检测

云安全中心日志审计配置检测

告警ID	sls_app_audit_cis_at_sas_audit_check
告警名称	云安全中心日志审计配置检测
版本号	1
类别	云平台、阿里云、CIS、日志审计合规
作用	检测云安全中心日志在日志审计服务中的配置是否正常。确保云安全中心日志的审计开关已开启，且其存储时长大于等于规则参数中存储时长（ttl）最小值。
执行频率	固定时间间隔1分钟
查询范围	过去2分钟
参数配置	存储时长（ttl）最小值：存储时长最小值，默认为180天。
外部配置	无

消除方法	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中开启云安全中心日志的审计开关，并确保存储时长大于规则参数配置中设定的存储时长（ttl）最小值。
前提条件	无

RDS日志审计配置检测

告警ID	sls_app_audit_cis_at_rds_audit_check
告警名称	RDS日志审计配置检测
版本号	1
类别	云平台、阿里云、CIS、日志审计合规
作用	检测RDS日志在日志审计服务中的配置是否正常。确保RDS日志的审计开关已开启，且其存储时长大于等于规则参数中存储时长（ttl）最小值。
执行频率	固定时间间隔1分钟
查询范围	过去2分钟
参数配置	存储时长（ttl）最小值：存储时长最小值，默认为180天。
外部配置	无
消除方法	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中开启RDS日志的审计开关，并确保存储时长大于规则参数配置中设定的存储时长（ttl）最小值。
前提条件	无

日志审计状态检测

告警ID	sls_app_audit_cis_at_audit_status_check
告警名称	日志审计状态检测
版本号	1
类别	云平台、阿里云、CIS、日志审计合规
作用	日志审计服务总体状态检测，总体状态异常时会触发告警。
执行频率	固定时间间隔1分钟
查询范围	过去2分钟
参数配置	无
外部配置	无
消除方法	在日志审计服务中的**审计配置 > 云产品接入 > 接入状态**中查看日志审计服务的状态，定位状态异常的原因。

前提条件	无

PolarDB（DRDS）日志审计配置检测

告警ID	sls_app_audit_cis_at_drds_audit_check
告警名称	PolarDB（DRDS）日志审计配置检测
版本号	1
类别	云平台、阿里云、CIS、日志审计合规
作用	检测PolarDB日志在日志审计服务中的配置是否正常。确保PolarDB（DRDS）日志的审计开关已开启，且其存储时长大于等于规则参数中存储时长（ttl）最小值。
执行频率	固定时间间隔1分钟
查询范围	过去2分钟
参数配置	存储时长（ttl）最小值：存储时长最小值，默认为180天。
外部配置	无
消除方法	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中开启Polar（DRDS）日志的审计开关，并确保存储时长大于规则参数配置中设定的存储时长（ttl）最小值。
前提条件	无

K8s日志审计配置检测

告警ID	sls_app_audit_cis_at_k8s_audit_check
告警名称	K8s日志审计配置检测
版本号	1
类别	云平台、阿里云、CIS、日志审计合规
作用	检测K8s相关日志（K8s审计日志、K8s事件中心和Ingress访问日志）在日志审计服务中的配置是否正常。确保K8s日志的审计开关已开启，且其存储时长大于等于规则参数中存储时长（ttl）最小值。
执行频率	固定时间间隔1分钟
查询范围	过去2分钟
参数配置	存储时长（ttl）最小值：存储时长最小值，默认为180天。
外部配置	无
消除方法	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中开启K8s相关日志（K8s审计日志、K8s事件中心和Ingress访问日志）的审计开关，并确保存储时长大于规则参数配置中设定的存储时长（ttl）最小值。

前提条件	无

ActionTrail日志审计配置检测

告警ID	sls_app_audit_cis_at_actiontrail_audit_check
告警名称	ActionTrail日志审计配置检测
版本号	1
类别	云平台、阿里云、CIS、日志审计合规
作用	检测操作审计（ActionTrail）日志在日志审计服务中的配置是否正常。确保ActionTrail日志的审计开关已开启，且其存储时长大于等于规则参数中存储时长（ttl）最小值。
执行频率	固定时间间隔1分钟
查询范围	过去2分钟
参数配置	存储时长（ttl）最小值：存储时长最小值，默认为180天。
外部配置	无
消除方法	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中开启操作审计（ActionTrail）日志开关，并确保存储时长大于规则参数配置中设定的存储时长（ttl）最小值。
前提条件	无

OSS（对象存储）日志审计配置检测

告警ID	sls_app_audit_cis_at_oss_audit_check
告警名称	OSS（对象存储）日志审计配置检测
版本号	1
类别	云平台、阿里云、CIS、日志审计合规
作用	检测OSS相关日志（访问日志和计量日志）在日志审计服务中的配置是否正常。确保OSS（对象存储）日志的审计开关已开启，且其存储时长大于等于规则参数中存储时长（ttl）最小值。
执行频率	固定时间间隔1分钟
查询范围	过去2分钟
参数配置	存储时长（ttl）最小值：存储时长最小值，默认为180天。
外部配置	无

消除方法	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中开启OSS相关日志（访问日志和计量日志）的审计开关，并确保存储时长大于规则参数配置中设定的存储时长（ttl）最小值。
前提条件	无

应用防火墙（WAF）日志审计配置检测

告警ID	sls_app_audit_cis_at_waf_audit_check
告警名称	应用防火墙（WAF）日志审计配置检测
版本号	1
类别	云平台、阿里云、CIS、日志审计合规
作用	检测应用防火墙（WAF）日志在日志审计服务中的配置是否正常。确保应用防火墙（WAF）日志的审计开关已开启，且其存储时长大于等于规则参数中存储时长（ttl）最小值。
执行频率	固定时间间隔1分钟
查询范围	过去2分钟
参数配置	存储时长（ttl）最小值：存储时长最小值，默认为180天。
外部配置	无
消除方法	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中开启应用防火墙（WAF）日志的审计开关，并确保存储时长大于规则参数配置中设定的存储时长（ttl）最小值。
前提条件	无

堡垒机日志审计配置检测

告警ID	sls_app_audit_cis_at_bastion_audit_check
告警名称	堡垒机日志审计配置检测
版本号	1
类别	云平台、阿里云、CIS、日志审计合规
作用	检测堡垒机日志在日志审计服务中的配置是否正常。确保堡垒机日志的审计开关已开启，且其存储时长大于等于规则参数中存储时长（ttl）最小值。
执行频率	固定时间间隔1分钟
查询范围	过去2分钟
参数配置	存储时长（ttl）最小值：存储时长最小值，默认为180天。
外部配置	无

消除方法	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中开启堡垒机日志的审计开关，并确保存储时长大于规则参数配置中设定的存储时长（ttl）最小值。
前提条件	无

NAS（文件存储）日志审计配置检测

告警ID	sls_app_audit_cis_at_nas_audit_check
告警名称	NAS（文件存储）日志审计配置检测
版本号	1
类别	云平台、阿里云、CIS、日志审计合规
作用	检测NAS（文件存储）日志在日志审计服务中的配置是否正常。确保NAS（文件存储）日志的审计开关已开启，且其存储时长大于等于规则参数中存储时长（ttl）最小值。
执行频率	固定时间间隔1分钟
查询范围	过去2分钟
参数配置	存储时长（ttl）最小值：存储时长最小值，默认为180天。
外部配置	无
消除方法	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中开启NAS（文件存储）日志的审计开关，并确保存储时长大于规则参数配置中设定的存储时长（ttl）最小值。
前提条件	无

API网关日志审计配置检测

告警ID	sls_app_audit_cis_at_apigateway_audit_check
告警名称	API网关日志审计配置检测
版本号	1
类别	云平台、阿里云、CIS、日志审计合规
作用	检测API网关日志在日志审计服务中的配置是否正常。确保API网关日志的审计开关已开启，且其存储时长大于等于规则参数中存储时长（ttl）最小值。
执行频率	固定时间间隔1分钟
查询范围	过去2分钟
参数配置	存储时长（ttl）最小值：存储时长最小值，默认为180天。
外部配置	无

消除方法	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中开启API网关日志的审计开关，并确保存储时长大于规则参数配置中设定的存储时长（ttl）最小值。
前提条件	无

SLB日志审计配置检测

告警ID	sls_app_audit_cis_at_slb_audit_check
告警名称	SLB日志审计配置检测
版本号	1
类别	云平台、阿里云、CIS、日志审计合规
作用	检测SLB日志在日志审计服务中的配置是否正常。确保SLB日志的审计开关已开启，且其存储时长大于等于规则参数中存储时长（ttl）最小值。
执行频率	固定时间间隔1分钟
查询范围	过去2分钟
参数配置	存储时长（ttl）最小值：存储时长最小值，默认为180天。
外部配置	无
消除方法	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中开启SLB日志的审计开关，并确保存储时长大于规则参数配置中设定的存储时长（ttl）最小值。
前提条件	无

云防火墙日志审计配置检测

告警ID	sls_app_audit_cis_at_cloudfirewall_audit_check
告警名称	云防火墙日志审计配置检测
版本号	1
类别	云平台、阿里云、CIS、日志审计合规
作用	检测云防火墙日志在日志审计服务中的配置是否正常。确保云防火墙日志的审计开关已开启，且其存储时长大于等于规则参数中存储时长（ttl）最小值。
执行频率	固定时间间隔1分钟
查询范围	过去2分钟
参数配置	存储时长（ttl）最小值：存储时长最小值，默认为180天。
外部配置	无

消除方法	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中开启云防火墙日志的审计开关，并确保存储时长大于规则参数配置中设定的存储时长（ttl）最小值。
前提条件	无

1.10.2.3. 账号安全

本文介绍账号安全的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现账号安全相关问题。

告警规则列表

支持的告警规则列表如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- RAM子账号无MFA登录告警
- RAM密码过期策略异常设置告警
- Root账号无MFA登录告警
- RAM密码登录重试策略异常设置告警
- Root账户连续登录告警
- RAM历史密码检查策略异常设置告警
- 密钥配置变更告警
- 账号连续登录失败告警
- Root账号AK使用检测
- RAM密码长度策略异常设置告警

RAM子账号无MFA登录告警

告警ID	sls_app_audit_cis_at_ram_mfa
告警名称	RAM子账号无MFA登录告警
版本号	1
类别	云平台、阿里云、CIS、账号安全
作用	监控RAM用户无MFA（多登录因素验证）登录的行为。RAM用户登录控制台时需要开启MFA，且其登录次数小于等于规则参数配置中设定最大登录次数，否则会触发告警。
执行频率	固定时间间隔：4分钟
查询范围	过去5分钟
参数配置	• 严重度：严重、高、中、低、报告。默认值为中。 • 最大登录次数：每5分钟内，允许未开启MFA的RAM用户登录的最大次数。默认值为0。
外部配置	无MFA登录的RAM用户白名单。白名单中RAM用户无MFA登录行为不会触发该告警。

消除方法	确保RAM用户5分钟内无MFA登录次数小于等于规则参数配置中设定的最大登录次数。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

RAM密码过期策略异常设置告警

告警ID	sls_app_audit_cis_at_pwd_expire_policy
告警名称	RAM密码过期策略异常设置告警
版本号	1
类别	云平台、阿里云、CIS、账号安全
作用	监控RAM密码策略中的密码过期策略的设置是否正常。RAM密码策略中，RAM密码的有效期应该小于等于规则参数中设定的密码有效期最大值，否则会触发告警。
执行频率	固定时间间隔：5分钟
查询范围	过去5分钟
参数配置	• 严重度：严重、高、中、低、报告。默认值为中。 • 密码有效期最大值：默认值为90天。根据阿里云CIS规则，该值建议设置为小于等于90。
外部配置	无
消除方法	确保RAM密码策略中密码有效期的值小于等于规则参数配置中设定的密码有效期最大值。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

Root账号无MFA登录告警

告警ID	sls_app_audit_cis_at_root_mfa
告警名称	Root账号无MFA登录告警
版本号	1
类别	云平台、阿里云、CIS、账号安全
作用	监控Root账号无MFA（多登录因素验证）登录的行为。Root账号登录控制台时需要开启MFA，且其登录次数小于等于规则参数配置中设定的最大登录次数，否则会触发告警。
执行频率	固定时间间隔：4分钟

查询范围	过去5分钟
参数配置	• 严重度：严重、高、中、低、报告。默认值为中。 • 最大登录次数：Root账号每天未开启MFA登录的最大次数，默认值0。
外部配置	无MFA登录的Root账号白名单。白名单中的账号无MFA登录行为不会触发该告警。
消除方法	确保Root账号5分钟内无MFA登录次数小于等于规则参数配置中设定的最大登录次数。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

RAM密码登录重试策略异常设置告警

告警ID	sls_app_audit_cis_at_pwd_login_attemp_policy
告警名称	RAM密码登录重试策略异常设置告警
版本号	1
类别	云平台、阿里云、CIS、账号安全
作用	监控RAM密码策略中的登录重试策略的设置是否正常。RAM密码登录重试策略中，允许一小时内使用错误密码尝试登录次数不能大于规则参数中设定的最大登录失败次数/h，否则会触发告警。
执行频率	固定时间间隔：5分钟
查询范围	过去5分钟
参数配置	• 严重度：严重、高、中、低、报告。默认值为中。 • 最大登录失败次数/h：密码登录重试策略中，允许一小时内使用错误密码尝试登录次数的最大值。默认值为5。根据阿里云CIS规则，该值建议设置为5。
外部配置	无
消除方法	确保RAM密码登录重试策略中，允许一小时内最大连续失败登录次数的值小于等于规则参数配置中设定的最大登录失败次数/h。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

Root账户连续登录告警

告警ID	sls_app_audit_cis_at_root_login
告警名称	Root账户连续登录告警

版本号	1
类别	云平台、阿里云、CIS、账号安全
作用	监控Root账号的连续登录行为。Root用户登录不能过于频繁，5分钟内登录次数超过规则参数中设定的最大登录次数会触发告警。
执行频率	固定时间间隔：5分钟
查询范围	过去5分钟
参数配置	• 严重度：严重、高、中、低、报告。默认值为中。 • 最大登录次数：Root账号5分钟内的最大登录次数，默认值为2。
外部配置	Root账号登录白名单。白名单中账号的登录行为不会触发告警。
消除方法	确保Root账号每天登录次数小于等于规则参数配置中设定的最大登录次数。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

RAM历史密码检查策略异常设置告警

告警ID	sls_app_audit_cis_at_pwd_reuse_policy
告警名称	RAM历史密码检查策略异常设置告警
版本号	1
类别	云平台、阿里云、CIS、账号安全
作用	监控RAM密码策略中的历史密码检查策略的设置是否正常。RAM历史密码检查策略中，禁止使用前N次密码。可在告警规则参数中配置N的最小值，小于该值会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	• 严重度：严重、高、中、低、报告。默认值为高。 • 密码重用最小值：历史密码检查策略中，**禁止使用前N次密码**中N的最小值。默认值为4。根据阿里云CIS规则，该值建议设为4。
外部配置	无
消除方法	确保RAM历史密码检查策略**禁止使用前N次密码**中N的值大于等于规则参数配置中设定密码重用最小值。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

密钥配置变更告警

告警ID	sls_app_audit_cis_at_ak_conf_change
告警名称	密钥配置变更告警
版本号	1
类别	云平台、阿里云、CIS、账号安全
作用	监控账号密钥配置变更事件。账号密钥的配置发生变更后（如删除或禁用等）会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许进行密钥配置变更的RAM用户白名单。使用白名单中的RAM用户进行密钥配置变更不会触发告警。
消除方法	禁止使用白名单以外的账号进行账号密钥配置变更。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

账号连续登录失败告警

告警ID	sls_app_audit_cis_at_abnormal_login_count
告警名称	账号连续登录失败告警
版本号	1
类别	云平台、阿里云、CIS、账号安全
作用	监控连续登录失败行为。5分钟内连续失败登录次数大于规则参数中设定的最大失败登录次数后触发告警。
执行频率	固定时间间隔：4分钟
查询范围	过去5分钟
参数配置	• 严重度：严重、高、中、低、报告。默认值为高。 • 最大失败登录次数：一个账号5分钟内的失败登录最大次数，默认值为5。
外部配置	无
消除方法	确保账号5分钟内的失败登录次数小于等于规则参数配置中设定的最大失败登录次数。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

Root账号AK使用检测

告警ID	sls_app_audit_cis_at_root_ak_usage
告警名称	Root账号AK使用检测
版本号	1
类别	云平台、阿里云、CIS、账号安全
作用	监控Root账号的密钥（AccessKey）使用行为。Root账号不应该创建和使用AccessKey密钥，否则会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	Root账号密钥使用白名单。使用白名单中的Root账号密钥不会触发告警。
消除方法	确保Root账号密钥不被使用。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

RAM密码长度策略异常设置告警

告警ID	sls_app_audit_cis_at_pwd_length_policy
告警名称	RAM密码长度策略异常设置告警
版本号	1
类别	云平台、阿里云、CIS、账号安全
作用	监控RAM密码策略中的密码长度策略的设置是否正常。RAM密码策略中，RAM密码的最小长度不能小于规则参数中设定的密码最小长度，否则会触发告警。
执行频率	固定时间间隔：5分钟
查询范围	过去5分钟
参数配置	• 严重度：严重、高、中、低、报告。默认值为高。 • 密码最小长度：密码策略中的密码最小长度的最小值。默认值为14。根据阿里云CIS规则，该值建议设置为14。
外部配置	无
消除方法	确保RAM密码策略中设置的密码最小长度大于等于规则参数配置中设定密码最小长度。

前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

1.10.2.4. 权限控制

本文介绍权限控制的告警规则，包括RAM用户策略变更、异常和OSS Bucket权限变更的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现权限控制相关问题。

告警规则列表

支持的告警规则列表如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- OSS Bucket权限变更告警
- RAM策略变更告警
- RAM策略异常添加告警

OSS Bucket权限变更告警

告警ID	sls_app_audit_cis_at_oss_policy_change
告警名称	OSS Bucket权限变更告警
版本号	1
类别	云平台、阿里云、CIS、权限控制
作用	监控OSS Bucket权限变更行为。OSS Bucket的权限发生变更后会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许进行OSS Bucket权限变更的RAM用户白名单。使用白名单中的RAM用户进行Bucket权限变更不会触发告警。
消除方法	禁止使用白名单以外的账号进行OSS Bucket权限变更。
前提条件	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

RAM策略变更告警

告警ID	sls_app_audit_cis_at_ram_policy_change
告警名称	RAM策略变更告警
版本号	1
类别	云平台、阿里云、CIS、权限控制

作用	监控RAM策略变更行为。RAM策略发生变更后会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为中。
外部配置	允许进行RAM策略变更的RAM用户白名单。使用白名单中的RAM用户进行RAM策略变更不会触发告警。
消除方法	禁止使用白名单以外的账号进行RAM策略变更。
前提条件	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

RAM策略异常添加告警

告警ID	sls_app_audit_cis_at_ram_policy_attach
告警名称	RAM策略异常添加告警
版本号	1
类别	云平台、阿里云、CIS、权限控制
作用	监控RAM策略是否存在异常添加行为。禁止将RAM策略添加到用户，只能添加到用户组或角色，否则会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为中。
外部配置	允许添加RAM策略的RAM用户白名单。使用白名单中的RAM用户添加RAM策略不会触发告警。
消除方法	禁止将RAM策略添加到用户，只能添加到用户组或角色。
前提条件	在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

1.10.2.5. OSS操作合规

本文介绍OSS操作合规的告警规则，包括OSS Bucket加密关闭和新创建加密未开启等告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现OSS操作合规问题。

告警规则列表

支持的告警规则列表如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- OSS Bucket加密关闭告警

- OSS新创建的Bucket加密未开启告警
- OSS Bucket访问日志记录关闭告警
- OSS新创建的Bucket访问日志记录未开启告警

OSS Bucket加密关闭告警

告警ID	sls_app_audit_cis_at_oss_encry_config
告警名称	OSS Bucket加密关闭告警
版本号	1
类别	云平台、阿里云、CIS、OSS操作合规
作用	监控OSS Bucket加密关闭行为。所有OSS Bucket都应该在服务端开启加密，不建议关闭。关闭加密会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许OSS Bucket不开启加密的账号白名单。白名单账号下的OSS Bucket加密被关闭后，不会触发告警。
消除方法	禁止白名单以外的账号下的OSS Bucket关闭加密功能。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开OSS**访问日志**的开关。

OSS新创建的Bucket加密未开启告警

告警ID	sls_app_audit_cis_at_oss_bucket_encry_off
告警名称	OSS新创建的Bucket加密未开启告警
版本号	1
类别	云平台、阿里云、CIS、OSS操作合规
作用	监控新创建的OSS Bucket加密未开启行为。OSS Bucket在创建时应该打开加密开关，或者在创建后（1小时内）尽快打开加密开关，否则会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去1小时
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许OSS Bucket不开启加密的账号白名单。使用白名单中的账号下的OSS Bucket在创建后可以不开启加密。

消除方法	OSS Bucket在创建时打开加密开关，或者创建后尽快（1小时内）打开加密开关。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开OSS**访问日志**的开关。

OSS Bucket访问日志记录关闭告警

告警ID	sls_app_audit_cis_at_oss_log_config
告警名称	OSS Bucket访问日志记录关闭告警
版本号	1
类别	云平台、阿里云、CIS、OSS操作合规
作用	监控OSS Bucket访问日志记录关闭行为。所有OSS Bucket都应该开启访问日志记录功能，不建议关闭。关闭日志记录后会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为中。
外部配置	允许不开启OSS访问日志的账号白名单。使用白名单中账号下的OSS Bucket访问日志记录被关闭后，不会触发告警。
消除方法	禁止白名单以外的账号下的OSS Bucket关闭日志记录功能。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开OSS**访问日志**的开关。

OSS新创建的Bucket访问日志记录未开启告警

告警ID	sls_app_audit_cis_at_oss_log_off
告警名称	OSS新创建的Bucket访问日志记录未开启告警
版本号	1
类别	云平台、阿里云、CIS、OSS操作合规
作用	监控新创建的OSS Bucket的访问日志记录未开启行为。OSS Bucket在创建后应该尽快开启访问日志记录功能。在Bucket创建1小时后还未打开访问日志记录会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去1小时
参数配置	严重度：严重、高、中、低、报告。默认值为中。

外部配置	允许不开启OSS访问日志的账号白名单。使用白名单中的账号下的OSS Bucket在创建后可以不开启访问日志记录功能。
消除方法	白名单以外的账号下的OSS Bucket在创建后尽快（1小时内）打开访问日志记录功能。
前提条件	确保已在日志审计服务中的**审计配置** > **云产品接入** > **全局配置**中打开OSS**访问日志**的开关。

1.10.2.6. RDS操作合规

本文介绍RDS操作合规的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现RDS操作合规问题。

告警规则列表

支持的告警规则列表如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- RDS实例SQL洞察关闭告警
- RDS实例访问白名单异常设置告警
- 新创建的RDS实例的SSL未开启告警
- 新创建的RDS实例的TDE未开启告警
- RDS实例SSL关闭告警
- RDS实例配置变更告警

RDS实例SQL洞察关闭告警

告警ID	sls_app_audit_cis_at_rds_sql_audit
告警名称	RDS实例SQL洞察关闭告警
版本号	1
类别	云平台、阿里云、CIS、RDS操作合规
作用	监控RDS实例的SQL洞察关闭行为。RDS实例的SQL洞察功能应该保持开启，关闭后会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许RDS SQL洞察功能关闭的账号白名单。白名单账号下RDS实例的SQL洞察功能关闭后，不会触发告警。
消除方法	禁止白名单以外的账号下的RDS实例关闭SQL洞察功能。
前提条件	确保已在日志审计服务中的**审计配置** > **云产品接入** > **全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

RDS实例访问白名单异常设置告警

告警ID	sls_app_audit_cis_at_rds_access_whitelist
告警名称	RDS实例访问白名单异常设置告警
版本号	1
类别	云平台、阿里云、CIS、RDS操作合规
作用	监控RDS实例的访问白名单的异常设置行为。RDS实例的访问白名单不应该设置为0.0.0.0，否则会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许RDS访问白名单设置为0.0.0.0的账号白名单。白名单账号下RDS实例的访问白名单设置为0.0.0.0后，不会触发告警。
消除方法	禁止白名单以外的账号下的RDS实例将访问白名单设置为0.0.0.0。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

新创建的RDS实例的SSL未开启告警

告警ID	sls_app_audit_cis_at_rds_ssl_off
告警名称	新创建的RDS实例的SSL未开启告警
版本号	1
类别	云平台、阿里云、CIS、RDS操作合规
作用	监控新创建的RDS实例SSL未开启行为。RDS实例创建后应该尽快（1小时内）开启SSL，否则会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去1小时
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许RDS不开启SSL的账号白名单。白名单账号下RDS实例在创建后可以不开启SSL。
消除方法	白名单以外账号下的RDS实例在创建后尽快（1小时内）打开SSL。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

新创建的RDS实例的TDE未开启告警

告警ID	sls_app_audit_cis_at_rds_tde_off
告警名称	新创建的RDS实例的TDE未开启告警
版本号	1
类别	云平台、阿里云、CIS、RDS操作合规
作用	监控新创建的RDS实例TDE未开启行为。RDS实例在创建后应该尽快（1小时）打开TDE功能，否则会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去1小时
参数配置	严重度：严重、高、中、低、报告。默认值为中。
外部配置	允许RDS不开启TDE的账号白名单。白名单账号下的RDS实例在创建后可以不开启TDE。
消除方法	白名单以外账号下的RDS实例在创建后尽快（1小时内）打开TDE。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

RDS实例SSL关闭告警

告警ID	sls_app_audit_cis_at_rds_ssl_config
告警名称	RDS实例SSL关闭告警
版本号	1
类别	云平台、阿里云、CIS、RDS操作合规
作用	监控RDS实例的SSL关闭行为。RDS实例的SSL应该保持开启，关闭后会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允允许RDS不开启SSL的账号白名单。白名单账号下RDS实例的SSL功能关闭后，不会触发告警。
消除方法	禁止白名单以外的账号下的RDS实例关闭SSL。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

RDS实例配置变更告警

告警ID	sls_app_audit_cis_at_rds_conf_change
告警名称	RDS实例配置变更告警
版本号	1
类别	云平台、阿里云、CIS、RDS操作合规
作用	监控RDS实例的配置变更行为。RDS实例的配置发生变更后会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为低。
外部配置	RDS配置变更不会触发告警的账号白名单。白名单账号下RDS实例的配置发生变更后，不会触发告警。
消除方法	检查发生配置变更的RDS实例及其配置变更项是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

1.10.2.7. SLB操作合规

本文介绍负载均衡（SLB）操作合规的告警规则，包括SLB健康检测关闭和关闭修改保护告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现SLB操作合规问题。

告警规则列表

支持的告警规则列表如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- 负载均衡修改保护关闭告警
- 负载均衡健康检查关闭告警

负载均衡修改保护关闭告警

告警ID	sls_app_audit_cis_at_slb_mod_protec
告警名称	负载均衡修改保护关闭告警
版本号	1
类别	云平台、阿里云、CIS、SLB操作合规
作用	监控负载均衡（SLB）实例的修改保护关闭行为。负载均衡（SLB）实例的修改保护功能应该保持开启，关闭后会触发告警。
执行频率	固定时间间隔：1分钟

查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许关闭修改保护的SLB实例白名单。白名单中SLB实例的修改保护功能关闭后，不会触发告警。
消除方法	禁止白名单以外的SLB实例关闭修改保护功能。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

负载均衡健康检查关闭告警

告警ID	sls_app_audit_cis_at_slb_health_check
告警名称	负载均衡健康检查关闭告警
版本号	1
类别	云平台、阿里云、CIS、SLB操作合规
作用	监控负载均衡（SLB）实例的健康检查关闭行为。负载均衡（SLB）实例的健康检查功能应该保持开启，关闭后会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许关闭健康检查的SLB实例白名单。关闭白名单中SLB实例的健康检查功能后，不会触发告警。
消除方法	禁止白名单以外的SLB实例关闭健康检查功能。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

1.10.2.8. ECS操作合规

本文介绍ECS操作合规的告警规则，包括ECS磁盘加密、自动快照策略、安全组变更等告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现ECS操作合规问题。

告警规则列表

支持的告警规则列表如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- ECS磁盘加密关闭告警
- ECS自动快照策略关闭告警
- 安全组配置变更告警
- ECS网络类型检测

ECS磁盘加密关闭告警

告警ID	sls_app_audit_cis_at_ecs_disk_encry_detection
告警名称	ECS磁盘加密关闭告警
版本号	1
类别	云平台、阿里云、CIS、ECS操作合规
作用	监控ECS磁盘加密关闭行为。ECS磁盘应该在服务端开启加密，关闭加密会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许磁盘不加密的账号白名单。关闭白名单账号下磁盘的加密功能后，不会触发告警。
消除方法	禁止白名单以外账号下的磁盘关闭加密功能。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

ECS自动快照策略关闭告警

告警ID	sls_app_audit_cis_at_ecs_auto_snapshot_policy
告警名称	ECS自动快照策略关闭告警
版本号	1
类别	云平台、阿里云、CIS、ECS操作合规
作用	监控ECS自动快照策略的关闭行为。ECS磁盘建议使用自动快照策略进行自动备份，关闭自动快照策略会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许取消磁盘自动快照策略的账号白名单。白名单账号下磁盘的自动快照策略被关闭后，不会触发告警。
消除方法	禁止白名单以外账号下的磁盘关闭自动快照策略。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

安全组配置变更告警

告警ID	sls_app_audit_cis_at_securitygroup_change
告警名称	安全组配置变更告警
版本号	1
类别	云平台、阿里云、CIS、ECS操作合规
作用	监控安全组配置变更行为。ECS安全组的配置发生变更时会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许进行安全组配置变更的子账号白名单。白名单中的账号进行安全组配置变更时，不会触发告警。
消除方法	禁止白名单以外的账号进行安全组配置变更。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

ECS网络类型检测

告警ID	sls_app_audit_cis_at_ecs_network_type
告警名称	ECS网络类型检测
版本号	1
类别	云平台、阿里云、CIS、ECS操作合规
作用	监控ECS网络类型是否存在异常。ECS建议使用专有网络VPC，创建经典网络的ECS会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为中。
外部配置	允许ECS使用经典网络的账号白名单。白名单账号下创建使用经典网络的ECS，不会触发告警。
消除方法	禁止白名单以外的账号创建经典网络的ECS。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

1.10.2.9. VPC操作合规

本文介绍VPC操作合规的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现VPC操作合规问题。

告警规则列表

支持的告警规则列表如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- VPC网络路由变更告警
- VPC流日志配置异常变更告警
- VPC通用配置变更告警

VPC网络路由变更告警

告警ID	sls_app_audit_cis_at_vpc_route_change
告警名称	VPC网络路由变更告警
版本号	1
类别	云平台、阿里云、CIS、VPC操作合规
作用	监控VPC网络路由的变更行为。VPC网络路由的配置发生变更后会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为低。
外部配置	允许VPC网络路由配置变更的账号白名单。白名单中的账号进行VPC网路路由配置变更时，不会触发告警。
消除方法	禁止白名单以外的账号进行VPC网络路由配置变更。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

VPC流日志配置异常变更告警

告警ID	sls_app_audit_cis_at_vpc_flowlog_detection
告警名称	VPC流日志配置异常变更告警
版本号	1
类别	云平台、阿里云、CIS、VPC操作合规
作用	监控VPC流日志的异常变更行为。所有VPC都应该开启流日志，关闭或者删除流日志会触发告警。
执行频率	固定时间间隔：1分钟

查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许不开启VPC流日志的账号白名单。白名单中的账号可以不开启VPC流日志。
消除方法	禁止白名单以外的账号关闭或删除VPC流日志。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

VPC通用配置变更告警

告警ID	sls_app_audit_cis_at_vpc_conf_change
告警名称	VPC通用配置变更告警
版本号	1
类别	云平台、阿里云、CIS、VPC操作合规
作用	监控VPC的配置变更行为。VPC配置发生变更后触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为低。
外部配置	允许VPC配置变更的账号白名单。白名单中的账号进行VPC配置变更时，不会触发告警。
消除方法	禁止白名单以外的账号进行VPC配置变更。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

1.10.2.10. TDI操作合规

本文介绍TDI操作合规的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现TDI操作合规问题。

云安全中心网页防篡改功能关闭告警

告警ID	sls_app_audit_cis_at_sas_webshell_detection
告警名称	云安全中心网页防篡改功能关闭告警
版本号	1
类别	云平台、阿里云、CIS、TDI操作合规

作用	监控云安全中心网页防篡改功能的关闭行为。云安全中心网页防篡改功能应该保持开启，关闭后会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许关闭网页防篡改功能的账号白名单。白名单账号关闭云安全中心网页防篡改功能，不会触发告警。
消除方法	禁止白名单以外的账号关闭云安全中心的网页防篡改功能。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

1.10.2.11. 云防火墙操作合规

本文介绍云防火墙操作合规的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现云防火墙操作合规问题。

云防火墙控制策略变更告警

告警ID	sls_app_audit_cis_at_cloudfirewall_conf_change
告警名称	云防火墙控制策略变更告警
版本号	1
类别	云平台、阿里云、CIS、云防火墙操作合规
作用	监控云防火墙的控制策略变更行为。云防火墙的控制策略发生变更后会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为中。
外部配置	允许云防火墙控制策略变更的账号白名单。白名单中的账号进行云防火墙控制策略变更时，不会触发告警。
消除方法	禁止白名单以外的账号进行云防火墙控制策略变更。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

1.10.2.12. API调用

本文介绍API调用的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现API调用问题。

未授权的API调用告警

告警ID	sls_app_audit_cis_at_unauth_apicall
告警名称	未授权的API调用告警
版本号	1
类别	云平台、阿里云、CIS、API调用
作用	监控未授权的API调用行为。未授权API调用次数小于等于规则参数配置中设定的未授权调用的最大次数，否则会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	• 严重度：严重、高、中、低、报告。默认值为中。 • 未授权调用的最大次数：每2分钟，允许每个IP地址对同一个服务发起未授权API调用的最大次数。默认值为5。
外部配置	允许未授权API调用的IP地址白名单。白名单中的IP地址对服务发起未授权API调用时，不会触发告警。
消除方法	禁止白名单以外的IP地址发起过多的未授权API调用。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

1.10.2.13. K8s安全

本文介绍K8s安全的告警规则，包括K8s错误事件过多、频繁删除事件等。通过设置并开启告警规则，可及时触发告警，有助于您快速发现K8s安全问题。

告警规则列表

支持的告警规则列表如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- K8s Warning事件数过多告警
- K8s频繁删除事件告警
- K8s错误事件数过多告警

K8s Warning事件数过多告警

告警ID	sls_app_audit_container_at_k8s_warn
告警名称	K8s Warning事件数过多告警
版本号	1

类别	云平台、阿里云、容器安全、K8s安全
作用	监控K8s集群的Warning事件。K8s集群上的Warning事件大于等于规则参数Warning事件数的阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为K8s Warning事件数过多告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为中。
	• Warning事件数的阈值：每2分钟内，一个K8s集群上报Warning事件的最大次数。默认值为10。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• K8s集群名称：待监控的K8s集群名称（支持正则表达式）。默认值 `.*` ，表示监控该阿里云账号下的所有K8s集群。

外部配置	无
消除方法	检查Warning事件数过多的K8s集群是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开Kubernetes **K8s事件中心**的开关。

K8s频繁删除事件告警

告警ID	sls_app_audit_container_at_k8s_del
告警名称	K8s频繁删除事件告警
版本号	1
类别	云平台、阿里云、容器安全、K8s安全
作用	监控K8s集群的频繁删除事件。K8s集群上的删除事件大于等于规则参数频繁删除的次数阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为K8s频繁删除事件告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 频繁删除的次数阈值：每2分钟内，一个K8s集群删除事件的最大次数。默认值为5。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• K8s集群名称：待监控的K8s集群名称（支持正则表达式）。默认值 `.*` ，表示监控该阿里云账号下的所有K8s集群。

外部配置	无
消除方法	检查发生频繁删除事件的K8s集群是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开Kubernetes **K8s审计日志**的开关。

K8s错误事件数过多告警

告警ID	sls_app_audit_container_at_k8s_err
告警名称	K8s错误事件数过多告警
版本号	1
类别	云平台、阿里云、容器安全、K8s安全
作用	监控K8s集群的错误事件。K8s集群上的Error事件大于规则参数错误事件数的阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为K8s错误事件数过多告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 错误事件数的阈值：每2分钟内，一个K8s集群上报错误事件的最大次数。默认值为5。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• K8s集群名称：待监控的K8s集群名称（支持正则表达式）。默认值 `.*` ，表示监控该阿里云账号下的所有K8s集群。

外部配置	无
消除方法	检查错误事件数过多的K8s集群是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开Kubernetes **K8s事件中心**的开关。

1.10.2.14. RDS安全

本文介绍RDS安全的告警规则。通过设置告警规则，可及时触发告警，有助于您快速发现RDS安全问题。

告警规则列表

支持的告警规则列表如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- RDS慢SQL检测
- RDS大批量数据删除告警
- RDS外网访问检测
- RDS查询SQL平均执行时间监控告警
- RDS数据库更新峰值监控告警
- RDS数据库查询峰值监控告警
- RDS实例释放告警
- RDS高频访问IP检测
- RDS更新SQL平均执行时间监控告警
- RDS登录失败次数过多告警
- RDS大批量数据修改事件告警
- RDS危险的SQL执行告警
- RDS SQL执行错误数过多告警

RDS慢SQL检测

告警ID	sls_app_audit_db_at_rds_slow_sql

告警名称	RDS慢SQL检测
版本号	1
类别	云平台、阿里云、数据库安全、RDS安全
作用	监控RDS SQL执行是否为慢SQL。RDS SQL执行时间大于等于规则参数慢SQL时间阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为RDS慢SQL检测。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 慢SQL时间阈值：SQL执行时间大于该阈值时，判定为慢SQL。默认值为5000微妙。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• RDS实例ID：待监控的RDS实例ID（支持正则表达式）。默认值 `.*` ，表示监控阿里云账号下的所有RDS实例。
	• 数据库名称：待监控的数据库名称（支持正则表达式）。默认值 `.*` ，表示监控阿里云账号下的所有数据库。

外部配置	无
消除方法	检查出现慢SQL的RDS数据库是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开RDS **SQL审计日志**的开关。

RDS大批量数据删除告警

告警ID	sls_app_audit_db_at_rds_batch_del_sql
告警名称	RDS大批量数据删除告警
版本号	1
类别	云平台、阿里云、数据库安全、RDS安全
作用	监控RDS是否大量删除数据。删除的RDS数据行数大于等于规则参数大批量删除界定阈值时，会触发告警。
执行频率	固定时间间隔：1分钟

查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为RDS大批量数据删除告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 大批量删除界定阈值：删除数据行数的最大值。默认值为10。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• RDS实例ID：待监控的RDS实例ID（支持正则表达式）。默认值 `.*` ，表示监控阿里云账号下的所有RDS实例。
	• 数据库名称：待监控的数据库名称（支持正则表达式）。默认值 `.*` ，表示监控阿里云账号下的所有数据库。

外部配置	无
消除方法	检查发生大批量删除事件的RDS数据库是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开RDS SQL审计日志的开关。

RDS外网访问检测

告警ID	sls_app_audit_db_at_rds_internet_access
告警名称	RDS外网访问检测
版本号	1
类别	云平台、阿里云、数据库安全、RDS安全
作用	监控RDS是否被外网IP地址访问。RDS被外网IP地址访问时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许通过外网访问的RDS实例白名单。白名单中的RDS实例被外网IP地址访问时，不会触发告警。
消除方法	禁止白名单以外的RDS实例被外网IP地址访问。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开RDS SQL审计日志的开关。

RDS查询SQL平均执行时间监控告警

告警ID	sls_app_audit_db_at_rds_select_speed
告警名称	RDS查询SQL平均执行时间监控告警
版本号	1
类别	云平台、阿里云、数据库安全、RDS安全
作用	监控RDS每条查询SQL执行平均时间。RDS SQL查询语句平均执行时间大于等于规则参数SQL平均执行时间阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为RDS查询SQL平均执行时间监控告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• SQL平均执行时间阈值：查询语句SQL平均执行时间的最大值。默认值为0.005秒/条。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• RDS实例ID：待监控的RDS实例ID（支持正则表达式）。默认值 `.*` ，表示监控所有RDS实例。
	• 数据库名称：待监控的数据库名称（支持正则表达式）。默认值 `.*` ，表示监控该阿里云账号下的所有数据库。

外部配置	无
消除方法	检查查询SQL的平均执行时间过长的RDS数据库是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开RDS SQL审计日志的开关。

RDS数据库更新峰值监控告警

告警ID	sls_app_audit_db_at_rds_update_peak
告警名称	RDS数据库更新峰值监控告警
版本号	1
类别	云平台、阿里云、数据库安全、RDS安全

作用	监控RDS更新（增删改）峰值。RDS更新（增删改）峰值大于等于规则参数更新峰值阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为RDS数据库更新峰值监控告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 更新峰值阈值：RDS更新（增删改）峰值。默认值为100行/秒。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• RDS实例ID：待监控的RDS实例ID（支持正则表达式）。默认值 `.*` ，表示监控所有RDS实例。
	• 数据库名称：待监控的数据库名称（支持正则表达式）。默认值 `.*` ，表示监控所有数据库。

外部配置	无
消除方法	检查更新峰值过高的RDS数据库是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开RDS SQL审计日志的开关。

RDS数据库查询峰值监控告警

告警ID	sls_app_audit_db_at_rds_query_peak
告警名称	RDS数据库查询峰值监控告警
版本号	1
类别	云平台、阿里云、数据库安全、RDS安全
作用	监控RDS查询峰值。RDS查询峰值大于等于规则参数查询峰值阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为RDS数据库查询峰值监控告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 查询峰值阈值：RDS查询峰值。默认值为1000行/秒。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• RDS实例ID：待监控的RDS实例ID（支持正则表达式）。默认值 `.*` ，表示监控所有RDS实例。
	• 数据库名称：待监控的数据库名称（支持正则表达式）。默认值 `.*` ，表示监控所有数据库。

外部配置	无
消除方法	检查查询峰值过高的RDS数据库是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开RDS SQL审计日志的开关。

RDS实例释放告警

告警ID	sls_app_audit_db_at_rds_instance_del
告警名称	RDS实例释放告警
版本号	1
类别	云平台、阿里云、数据库安全、RDS安全
作用	监控RDS实例释放异常。RDS实例被释放时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	无
消除方法	检查被释放的RDS实例是否属于正常释放。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开RDS SQL审计日志的开关。

RDS高频访问IP检测

告警ID	sls_app_audit_db_at_rds_visit

告警名称	RDS高频访问IP检测
版本号	1
类别	云平台、阿里云、数据库安全、RDS安全
作用	监控同一个IP地址对RDS实例访问频率是否异常。同一个IP地址对RDS实例访问频率大于等于规则参数高频访问阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为RDS高频访问IP检测。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 高频访问阈值：每2分钟内，同一个IP地址对一个RDS实例的访问次数最大值。默认值为30次。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• RDS实例ID：待监控的RDS实例ID（支持正则表达式）。默认值 `.*` ，表示监控所有RDS实例。

外部配置	RDS高频访问IP地址白名单。白名单中的IP地址对RDS实例发起高频访问时，不会触发告警。
消除方法	检查高频访问RDS实例的IP地址是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开RDS **SQL审计日志**的开关。

RDS更新SQL平均执行时间监控告警

告警ID	sls_app_audit_db_at_rds_update_speed
告警名称	RDS更新SQL平均执行时间监控告警
版本号	1
类别	云平台、阿里云、数据库安全、RDS安全
作用	监控RDS每条更新（增删改）SQL执行平均时间。RDS更新（增删改）SQL平均执行时间大于等于规则参数SQL平均执行时间阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为RDS更新SQL平均执行时间监控告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• SQL平均执行时间阈值：更新（增删改）SQL平均执行时间的最大值。默认值为0.005秒/条。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• RDS实例ID：待监控的RDS实例ID（支持正则表达式）。默认值 `.*` ，表示监控所有RDS实例。
	• 数据库名称：待监控的数据库名称（支持正则表达式）。默认值 `.*` ，表示监控所有数据库。

外部配置	无
消除方法	检查更新（增删改）SQL的平均执行时间过长的RDS数据库是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开RDS **SQL审计日志**的开关。

RDS登录失败次数过多告警

告警ID	sls_app_audit_db_at_rds_login_err_cnt
告警名称	RDS登录失败次数过多告警
版本号	1
类别	云平台、阿里云、数据库安全、RDS安全
作用	监控登录RDS实例失败次数是否异常。一个RDS实例在5分钟内登录失败次数大于等于规则参数最大失败登录次数时，会触发告警。
执行频率	固定时间间隔：4分钟
查询范围	过去5分钟

参数配置	• 告警名称：告警实例的名称，默认为RDS登录失败次数过多告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 最大失败登录次数：一个RDS实例5分钟内允许登录失败次数的最大值。默认值为3次。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• RDS实例ID：待监控的RDS实例ID（支持正则表达式）。默认值 `.*` ，表示监控所有RDS实例。

外部配置	无
消除方法	检查登录失败次数过的RDS实例是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开RDS SQL审计日志的开关。

RDS大批量数据修改事件告警

告警ID	sls_app_audit_db_at_rds_batch_update_sql
告警名称	RDS大批量数据修改事件告警
版本号	1
类别	云平台、阿里云、数据库安全、RDS安全
作用	监控RDS大量修改数据是否异常。RDS大量修改数据行数大于等于规则参数大规模修改界定阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为RDS大批量数据修改事件告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 大规模修改界定阈值：修改数据行数的最大值。默认值为10。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• RDS实例ID：待监控的RDS实例ID（支持正则表达式）。默认值 `.*` ，表示监控所有RDS实例。
	• 数据库名称：待监控的数据库名称（支持正则表达式）。默认值 `.*` ，表示监控所有数据库。

外部配置	无
消除方法	检查发生大批量数据修改事件的RDS数据库是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开RDS SQL审计日志的开关。

RDS危险的SQL执行告警

告警ID	sls_app_audit_db_at_rds_danger_sql
告警名称	RDS危险的SQL执行告警
版本号	1
类别	云平台、阿里云、数据库安全、RDS安全
作用	监控RDS是否存在执行危险SQL。RDS出现执行危险SQL时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为RDS危险的SQL执行告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• RDS实例ID：待监控的RDS实例ID（支持正则表达式）。默认值 `.*` ，表示监控所有RDS实例。
	• 数据库名称：待监控的数据库名称（支持正则表达式）。默认值 `.*` ，表示监控所有数据库。

外部配置	无
消除方法	检查执行危险SQL的RDS数据库是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开RDS SQL审计日志的开关。

RDS SQL执行错误数过多告警

告警ID	sls_app_audit_db_at_rds_sql_err_cnt
告警名称	RDS SQL执行错误数过多告警
版本号	1
类别	云平台、阿里云、数据库安全、RDS安全
作用	监控RDS SQL执行错误次数是否异常。一个RDS实例的SQL执行错误次数大于等于规则参数最大错误次数时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为RDS SQL执行错误数过多告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 最大错误次数：一个RDS实例2分钟内允许SQL执行错误的最大次数。默认值为10。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• RDS实例ID：待监控的RDS实例ID（支持正则表达式）。默认值 `.*` ，表示监控所有RDS实例。
	• 数据库名称：待监控的数据库名称（支持正则表达式）。默认值 `.*` ，表示监控所有数据库。

外部配置	无
消除方法	检查SQL执行错误次数过多的RDS数据库是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开RDS SQL审计日志的开关。

1.10.2.15. SLB流量安全

本文介绍SLB（阿里云负载均衡）流量安全的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现SLB流量安全问题。

告警规则列表

支持的告警规则列表如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- 负载均衡响应报文长度异常检测
- 负载均衡请求报文长度异常检测
- 负载均衡平均响应延迟过高告警
- 负载均衡HTTP访问协议开启告警
- 负载均衡访问UV异常检测
- 负载均衡访问PV异常检测

负载均衡响应报文长度异常检测

告警ID	sls_app_audit_dataflow_at_slb_resp_detc
告警名称	负载均衡响应报文长度异常检测
版本号	1
类别	云平台、阿里云、流量安全、SLB流量安全

作用	检测负载均衡（SLB）响应报文长度异常。响应报文长度的异常点个数大于等于规则参数异常点个数的阈值时，会触发告警。
执行频率	固定时间间隔：4小时
查询范围	过去4小时

参数配置	• 告警名称：告警实例的名称，默认为负载均衡响应报文长度异常检测。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 异常点个数的阈值：每分钟统计一个平均的响应报文长度，4小时内响应报文长度的异常点个数的最大值。默认值为10。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• SLB实例名称：待监控的SLB实例名称（支持正则表达式）。默认值 `.*` ，表示监控您操作账号绑定的所有SLB实例。

外部配置	无
消除方法	检查响应报文长度异常点过多的负载均衡实例是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开SLB**7层访问日志**的开关。

负载均衡请求报文长度异常检测

告警ID	sls_app_audit_dataflow_at_slb_req_detc
告警名称	负载均衡请求报文长度异常检测
版本号	1
类别	云平台、阿里云、流量安全、SLB流量安全
作用	检测负载均衡（SLB）请求报文长度异常。请求报文长度的异常点个数大于等于规则参数异常点个数的阈值时，会触发告警。
执行频率	固定时间间隔：4小时
查询范围	过去4小时

参数配置	• 告警名称：告警实例的名称，默认为负载均衡请求报文长度异常检测。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 异常点个数的阈值：每分钟统计一个平均的请求报文长度，4小时内请求报文长度的异常点个数的最大值。默认值为10。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• SLB实例名称：待监控的SLB实例名称（支持正则表达式）。默认值 `.*` ，表示监控您操作账号绑定的所有SLB实例。

外部配置	无
消除方法	检查请求报文长度异常点过多的负载均衡实例是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开SLB**7层访问日志**的开关。

负载均衡平均响应延迟过高告警

告警ID	sls_app_audit_dataflow_at_slb_latency
告警名称	负载均衡平均响应延迟过高告警
版本号	1
类别	云平台、阿里云、流量安全、SLB流量安全
作用	检测负载均衡（SLB）实例平均响应延迟过高。负载均衡实例平均响应时长大于等于规则参数平均响应延迟阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为负载均衡平均响应延迟过高告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 平均响应延迟阈值：每2分钟内，负载均衡实例响应延迟的最大值。默认值为0.5秒。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• SLB实例名称：待监控的SLB实例名称（支持正则表达式）。默认值 `.*` ，表示监控您操作账号绑定的所有SLB实例。

外部配置	无
消除方法	检查平均响应延迟过高的负载均衡实例是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开SLB**7层访问日志**的开关。

负载均衡HTTP访问协议开启告警

告警ID	sls_app_audit_dataflow_at_slb_http
告警名称	负载均衡HTTP访问协议开启告警
版本号	1
类别	云平台、阿里云、流量安全、SLB流量安全
作用	检测负载均衡（SLB）是否通过HTTPS协议访问服务端。负载均衡通过HTTP协议访问服务端时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	严重度：严重、高、中、低、报告。默认值为高。
外部配置	允许开启HTTP访问协议的负载均衡实例白名单。白名单中的负载均衡实例开启HTTP访问协议后，不会触发告警。
消除方法	禁止白名单以外的负载均衡实例开启HTTP访问协议。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开操作审计（ActionTrail）**操作日志**的开关。

负载均衡访问UV异常检测

告警ID	sls_app_audit_dataflow_at_slb_uv_detc

告警名称	负载均衡访问UV异常检测
版本号	1
类别	云平台、阿里云、流量安全、SLB流量安全
作用	检测负载均衡（SLB）访问UV是否异常。负载均衡实例访问UV个数大于等于规则参数UV异常点个数的阈值时，会触发告警。
执行频率	固定时间间隔：4小时
查询范围	过去4小时

参数配置	• 告警名称：告警实例的名称，默认为负载均衡访问UV异常检测。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• UV异常点个数的阈值：每分钟统计1个UV值，每4小时内负载均衡访问UV异常的最大值。默认值为10。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• SLB实例名称：待监控的SLB实例名称（支持正则表达式）。默认值 `.*` ，表示监控您操作账号绑定的所有SLB实例。

外部配置	无
消除方法	检查UV异常点过多的负载均衡实例是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开SLB**7层访问日志**的开关。

负载均衡访问PV异常检测

告警ID	sls_app_audit_dataflow_at_slb_pv_detc
告警名称	负载均衡访问PV异常检测
版本号	1
类别	云平台、阿里云、流量安全、SLB流量安全
作用	检测负载均衡（SLB）访问PV是否异常。负载均衡实例访问PV个数大于等于规则参数PV异常点个数的阈值时，会触发告警。
执行频率	固定时间间隔：4小时
查询范围	过去4小时

参数配置	• 告警名称：告警实例的名称，默认为负载均衡访问PV异常检测。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• UV异常点个数的阈值：每分钟统计1个PV值，每4小时内负载均衡访问PV异常的最大值。默认值为10。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• SLB实例名称：待监控的SLB实例名称（支持正则表达式）。默认值 `.*` ，表示监控您操作账号绑定的所有SLB实例。

外部配置	无
消除方法	检查PV异常点过多的负载均衡实例是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开SLB**7层访问日志**的开关。

1.10.2.16. API网关流量安全

本文介绍API网关流量安全的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现API网关流量安全问题。

告警规则列表

支持的告警规则列表如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- API网关服务端平均延时过高告警
- API网关后端服务器错误率过高告警
- API网关请求成功率过低告警

API网关服务端平均延时过高告警

告警ID	sls_app_audit_dataflow_at_api_latency
告警名称	API网关服务端平均延时过高告警
版本号	1
类别	云平台、阿里云、流量安全、API网关流量安全
作用	监控API网关中的API请求的服务端平均延时。API网关中的API请求的服务端平均延时大于等于规则参数服务端平均延时阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为API网关服务端平均延时过高告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 服务端平均延时阈值：每2分钟内，API请求的服务端平均延时的最大值。默认值为100毫秒。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• API名称：待监控的API名称（支持正则表达式）。默认值 `.*` ，表示监控所有API。

外部配置	无
消除方法	检查服务端平均延时过高的API是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开API网关**访问日志**的开关。

API网关后端服务器错误率过高告警

告警ID	sls_app_audit_dataflow_at_api_err_rate
告警名称	API网关后端服务器错误率过高告警
版本号	1
类别	云平台、阿里云、流量安全、API网关流量安全
作用	监控API网关中API请求的后端服务器错误率。API网关中API请求的后端服务器错误率大于等于规则参数后端服务器错误率阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为API网关后端服务器错误率过高告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• 后端服务器错误率阈值：每2分钟内，API请求的后端服务器错误率最大值。默认值为0%。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• API名称：待监控的API名称（支持正则表达式）。默认值 `.*` ，表示监控所有API。

外部配置	无
消除方法	检查后端服务器错误率过高的API是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开API网关**访问日志**的开关。

API网关请求成功率过低告警

告警ID	sls_app_audit_dataflow_at_api_req_rate
告警名称	API网关请求成功率过低告警
版本号	1
类别	云平台、阿里云、流量安全、API网关流量安全
作用	监控API网关中API的请求成功率。API网关的API请求成功率低于规则参数API请求成功率阈值时，会触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	• 告警名称：告警实例的名称，默认为API网关请求成功率过低告警。您可以根据不同监控对象，命名不同的告警名称便于识别。
	• 严重度：严重、高、中、低、报告。默认值为高。
	• API请求成功率阈值：API请求的成功率最小值。默认值为95%。
	• 阿里云账号ID：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• API名称：待监控的API名称（支持正则表达式）。默认值 `.*` ，表示监控所有API。

外部配置	无
消除方法	检查请求成功率过低的API是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置** > **云产品接入** > **全局配置**中打开API网关**访问日志**的开关。

1.10.2.17. OSS流量安全

本文介绍OSS流量安全的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现OSS流量安全问题。

告警规则列表

支持的告警规则如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- OSS流量异常检测
- OSS流入流量异常检测
- OSS流出流量异常检测
- OSS访问PV异常检测
- OSS访问UV异常检测
- OSS Bucket有效请求率过低告警
- OSS外网访问检测

OSS流量异常检测

告警ID	sls_app_audit_dataflow_at_oss_flow_detc
告警名称	OSS流量异常检测
版本号	1
类别	云平台、阿里云、流量安全、OSS流量安全
作用	监控OSS的流入流量和流出流量。当流量的异常点个数超过指定的阈值时，触发告警。
执行频率	固定时间间隔：4小时
查询范围	过去4小时

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **流量异常点个数的阈值**：OSS流量异常点个数的阈值，默认值为10个。如果4小时内的流量异常点个数超过该阈值，则触发告警。
	每分钟统计一个流量值。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。
	• **Bucket名称**：需要监控的OSS Bucket名称（支持正则）。
	  ○ 您可以使用正则表达式 `.*` 进行配置。
	  ○ 默认值为 `.*`，表示监控目标阿里云账号下的所有的OSS Bucket。

外部配置	无
消除办法	检查触发告警的OSS Bucket是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开OSS**访问日志**开关。

OSS流入流量异常检测

告警ID	sls_app_audit_dataflow_at_oss_inflow_detc
告警名称	OSS流入流量异常检测
版本号	1
类别	云平台、阿里云、流量安全、OSS流量安全
作用	监控OSS的流入流量。当流入流量的异常点个数超过指定的阈值时，触发告警。
执行频率	固定时间间隔：4小时
查询范围	过去4小时

参数配置	告警参数说明如下：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **入流量异常点个数的阈值**：OSS流入流量异常点个数的阈值，默认值为10个。如果4小时内的流入流量异常点个数超过该阈值，则触发告警。
	每分钟统计一个流入流量值。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。
	• **Bucket名称**：需要监控的OSS Bucket名称（支持正则）。
	  ○ 您可以使用正则表达式 `.*` 进行配置。
	  ○ 默认值为 `.*`，表示监控目标阿里云账号下的所有的OSS Bucket。

外部配置	无
消除办法	检查触发告警的OSS Bucket是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开OSS**访问日志**开关。

OSS流出流量异常检测

告警ID	sls_app_audit_dataflow_at_oss_outflow_detc
告警名称	OSS流出流量异常检测
版本号	1
类别	云平台、阿里云、流量安全、OSS流量安全
作用	监控OSS的流出流量。当流出流量的异常点个数超过指定的阈值时，触发告警。
执行频率	固定时间间隔：4小时
查询范围	过去4小时

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **出流量异常点个数的阈值**：OSS流出流量异常点个数的阈值，默认值为10个。如果4小时内的流出流量异常点个数超过该阈值，则触发告警。
	每分钟统计一个流量值。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。
	• **Bucket名称**：需要监控的OSS Bucket名称（支持正则）。
	  ○ 您可以使用正则表达式 `.*` 进行配置。
	  ○ 默认值为 `.*`，表示监控目标阿里云账号下的所有的OSS Bucket。

外部配置	无
消除办法	检查触发告警的OSS Bucket是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开OSS**访问日志**开关。

OSS访问PV异常检测

告警ID	sls_app_audit_dataflow_at_oss_pv_detc
告警名称	OSS访问PV异常检测
版本号	1
类别	云平台、阿里云、流量安全、OSS流量安全
作用	监控OSS的访问PV。当OSS访问PV的异常点个数超过指定的阈值时，触发告警。
执行频率	固定时间间隔：4小时
查询范围	过去4小时

参数配置	告警参数说明如下所示： • **告警名称**：告警实例的名称，支持创建多个告警实例。 • **严重度**：告警严重度，包括严重、高、中、低、报告。 • **PV异常点个数阈值**：OSS访问PV异常点个数的阈值，默认值为10个。如果4小时内的PV异常点个数超过该阈值，则触发告警。 每分钟统计一个PV值。 • **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。 ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。 ◦ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。 • **Bucket名称**：需要监控的OSS Bucket名称（支持正则）。 ◦ 您可以使用正则表达式 `.*` 进行配置。 ◦ 默认值为 `.*`，表示监控目标阿里云账号下的所有的OSS Bucket。
外部配置	无
消除办法	检查触发告警的OSS Bucket是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开OSS**访问日志**开关。

OSS访问UV异常检测

告警ID	sls_app_audit_dataflow_at_oss_uv_detc
告警名称	OSS访问UV异常检测
版本号	1
类别	云平台、阿里云、流量安全、OSS流量安全
作用	监控OSS的访问UV。当OSS访问UV的异常点个数超过指定阈值时，触发告警。
执行频率	固定时间间隔：4小时
查询范围	过去4小时

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **UV异常点个数阈值**：OSS访问UV异常点个数的阈值，默认值为10个。如果4小时内的UV异常点个数超过该阈值，则触发告警。
	每分钟统计一个PV值。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。
	• **Bucket名称**：需要监控的OSS Bucket名称（支持正则）。
	  ○ 您可以使用正则表达式 `.*` 进行配置。
	  ○ 默认值为 `.*`，表示监控目标阿里云账号下的所有的OSS Bucket。

外部配置	无
消除办法	检查触发告警的OSS Bucket是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开OSS**访问日志**开关。

OSS Bucket有效请求率过低告警

告警ID	sls_app_audit_dataflow_at_oss_req_rate
告警名称	OSS Bucket有效请求率过低告警
版本号	1
类别	云平台、阿里云、流量安全、OSS流量安全
作用	监控OSS Bucket有效请求率。当OSS Bucket有效请求率低于指定的阈值时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **有效请求率阈值**：OSS Bucket的有效请求率的阈值，默认值为95%。如果OSS Bucket的有效请求率低于该阈值，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。
	• **Bucket名称**：需要监控的OSS Bucket名称（支持正则）。
	  ○ 您可以使用正则表达式 `.*` 进行配置。
	  ○ 默认值为 `.*`，表示监控目标阿里云账号下的所有的OSS Bucket。

外部配置	无
触发告警时的推荐**消除办法**	检查触发告警的OSS Bucket是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开OSS**访问日志**开关。

OSS外网访问检测

告警ID	sls_app_audit_dataflow_at_oss_internet_access
告警名称	OSS外网访问检测
版本号	1
类别	云平台、阿里云、流量安全、OSS流量安全
作用	监控OSS Bucket外网访问情况。当OSS被外网访问时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	告警参数说明如下： **严重度**：告警严重度，包括严重、高、中、低、报告。
外部配置	添加阿里云账号和OSS Bucket白名单，白名单中的OSS Bucket被外网访问时，不会触发告警。
消除方法	请勿使用外网访问白名单以外的OSS Bucket。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开OSS**访问日志**开关。

1.10.2.18. K8s流量安全

本文介绍K8s流量安全的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现K8s流量安全问题。

告警规则列表

支持的告警规则如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- K8s Ingress后端平均响应延迟过高告警
- K8s Ingress请求成功率过低告警
- K8s Ingress平均请求延迟过高告警
- K8s非法访问次数过多告警

K8s Ingress后端平均响应延迟过高告警

告警ID	sls_app_audit_dataflow_at_ingress_resp
告警名称	K8s Ingress后端平均响应延迟过高告警
版本号	1
类别	云平台、阿里云、流量安全、K8s流量安全
作用	监控K8s Ingress的后端平均响应延迟。当K8s Ingress后端平均响应延迟高于指定阈值时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **后端平均响应延迟阈值**：K8s Ingress后端平均响应延迟的阈值，默认值为500毫秒。如果2分钟内K8s Ingress的后端平均响应延迟高于该阈值，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。
	• **K8s集群名称**：需要监控的K8s集群名称。
	  ○ 您可以使用正则表达式 `.*` 进行配置。
	  ○ 默认值为 `.*`，表示监控目标阿里云账号下所有的K8s集群名称。

外部配置	无
消除办法	检查触发告警的K8s集群是否存在异常。

前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开Kubernetes **Ingress访问日志**的开关。

K8s Ingress平均请求延迟过高告警

告警ID	sls_app_audit_dataflow_at_ingress_latency
告警名称	K8s Ingress平均请求延迟过高告警
版本号	1
类别	云平台、阿里云、流量安全、K8s流量安全
作用	监控K8s Ingress的平均请求延迟。当K8s Ingress的平均请求延迟高于指定阈值时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **平均请求延迟阈值**：K8s Ingress平均请求延迟的阈值，默认值为200毫秒。如果2分钟内K8s Ingress的平均响应延迟高于该阈值，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• **K8s集群名称**：需要监控的K8s集群名称。
	  ◦ 您可以使用正则表达式 `.*` 进行配置。
	  ◦ 默认值为 `.*` ，表示监控目标阿里云账号下所有的K8s集群名称。

外部配置	无
消除办法	检查触发告警的K8s集群是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开Kubernetes **Ingress访问日志**的开关。

K8s Ingress请求成功率过低告警

告警ID	sls_app_audit_dataflow_at_ingress_rate
告警名称	K8s Ingress请求成功率过低告警
版本号	1

类别	云平台、阿里云、流量安全、K8s流量安全
作用	监控K8s Ingress的请求成功率。当K8s Ingress请求成功率低于指定阈值时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **后端平均响应延迟阈值**：K8s Ingress请求成功率的阈值，默认值为90%。如果2分钟内K8s Ingress的请求成功率低于该阈值，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。
	• **K8s集群名称**：需要监控的K8s集群名称。
	  ○ 您可以使用正则表达式 `.*` 进行配置。
	  ○ 默认值为 `.*`，表示监控目标阿里云账号下所有的K8s集群名称。

外部配置	无
消除办法	检查触发告警的K8s集群是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开Kubernetes **Ingress访问日志**的开关。

K8s非法访问次数过多告警

告警ID	sls_app_audit_dataflow_at_k8s_visit
告警名称	K8s非法访问次数过多告警
版本号	1
类别	云平台、阿里云、流量安全、K8s流量安全
作用	监控K8s集群的访问情况。当K8s集群被非法访问的次数多于指定的阈值时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **非法访问次数阈值**：K8s集群被非法访问的次数的阈值，默认值为3次。如果2分钟内K8s集群被非法访问的次数超过该阈值时，触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。
	• **K8s集群名称**：需要监控的K8s集群名称。
	  ○ 您可以使用正则表达式 `.*` 进行配置。
	  ○ 默认值为 `.*`，表示监控目标阿里云账号下所有的K8s集群名称。

外部配置	无
消除办法	检查触发告警的K8s集群是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开Kubernetes **Ingress访问日志**的开关。

1.10.2.19. OSS数据安全

本文介绍OSS数据安全的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现OSS数据安全问题。

告警规则列表

支持的告警规则如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- OSS频繁删除对象告警
- OSS Bucket账号访问控制

OSS频繁删除对象告警

告警ID	sls_app_audit_storage_at_oss_obj_del
告警名称	OSS频繁删除对象告警
版本号	1
类别	云平台、阿里云、数据安全、OSS数据安全
作用	监控OSS Bucket的删除操作。当OSS Bucket中删除操作的次数超过指定的阈值时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **频繁删除的阈值**：删除操作的阈值。默认值为10次。如果2分钟内某个OSS Bucket中删除操作的次数超过该阈值，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。
	• **Bucket名称**：需要监控的OSS Bucket名称（支持正则）。
	  ○ 您可以使用正则表达式 `.*` 进行配置。
	  ○ 默认值为 `.*`，表示监控目标阿里云账号下的所有的OSS Bucket。

外部配置	无
消除办法	检查触发告警的OSS Bucket是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开OSS**访问日志**开关。

OSS Bucket账号访问控制

告警ID	sls_app_audit_storage_at_oss_access_control
告警名称	OSS Bucket账号访问控制
版本号	1
类别	云平台、阿里云、数据安全、OSS数据安全
作用	监控OSS Bucket的访问控制。当目标OSS Bucket只能被指定的阿里云账号或RAM用户访问时，如果不在允许范围内的阿里云账号或RAM用户访问该OSS Bucket，则触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟
参数配置	告警参数说明如下所示： **严重度**：告警严重度，包括严重、高、中、低、报告。
外部配置	添加阿里云账号（RAM用户）和OSS Bucket白名单。白名单中的阿里云账号或RAM用户访问指定的OSS Bucket时，不会触发告警。
消除办法	请勿使用白名单以外的阿里云账号或RAM用户访问OSS Bucket。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开OSS**访问日志**开关。

1.10.2.20. NAS数据安全

本文介绍NAS数据安全的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现NAS数据安全问题。

告警规则列表

支持的告警规则如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- 文件存储操作错误检测
- 文件存储大批量删除文件告警

文件存储操作错误检测

告警ID	sls_app_audit_storage_at_nas_err_op
告警名称	文件存储操作错误检测
版本号	1
类别	云平台、阿里云、数据安全、NAS数据安全
作用	监控NAS Volume的错误操作情况。当NAS Volume中错误操作的次数多于指定的阈值时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	参数如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **操作错误数的阈值**：操作错误的次数的阈值，默认值为5。如果2分钟内一个Volume中的操作错误次数大于该阈值，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• **Volume名称**：需要监控的Volume名称（支持正则）。
	  ◦ 您可以使用正则表达式 `.*` 进行配置。
	  ◦ 默认值为 `.*` ，表示监控目标阿里云账号下所有的Volume。

外部配置	无
消除办法	检查触发告警的NAS Volume是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置** > **云产品接入** > **全局配置**中打开NAS**访问日志**的开关。

文件存储大批量删除文件告警

告警ID	sls_app_audit_storage_at_nas_file_del
告警名称	文件存储大批量删除文件告警
版本号	1
类别	云平台、阿里云、数据安全、NAS数据安全
作用	监控NAS Volume的删除操作情况。当NAS Volume中删除操作的次数超过指定的阈值时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	参数如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **大批量删除阈值**：删除操作的阈值。如果2分钟内某个NAS Volume中的删除操作次数超过该阈值，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• **Volume名称**：需要监控的Volume名称（支持正则）。
	  ◦ 您可以使用正则表达式 `.*` 进行配置。
	  ◦ 默认值为 `.*` ，表示监控目标阿里云账号下所有的Volume。

外部配置	无
消除办法	检查触发告警的NAS Volume是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开NAS**访问日志**的开关。

1.10.2.21. WAF安全事件

本文介绍WAF安全事件的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现WAF安全事件问题。

告警规则列表

支持的告警规则如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- 应用防火墙防护网站被攻击次数过多告警
- 应用防火墙有效请求率过低告警

应用防火墙防护网站被攻击次数过多告警

告警ID	sls_app_audit_secure_at_waf_attack
告警名称	应用防火墙防护网站被攻击次数过多告警
版本号	1
类别	云平台、阿里云、安全事件、WAF安全事件
作用	监控网站被攻击的情况。当应用防火墙所防护的网站被攻击的次数超过指定的阈值时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **被攻击次数阈值**：网站被攻击次数的阈值，默认值为5次。如果2分钟内一个网站被攻击的次数超过该阈值时，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• **网站（host）**：需要监控的网站名称。
	  ◦ 您可以使用正则表达式 `.*` 进行配置。
	  ◦ 默认值 `.*` 表示监控目标阿里云账号下所有被应用防火墙防护的网站。

外部配置	无
消除办法	检查触发告警的网站是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开应用防火墙（WAF）**访问日志**的开关。

应用防火墙有效请求率过低告警

告警ID	sls_app_audit_secure_at_waf_rate
告警名称	应用防火墙有效请求率过低告警
版本号	1
类别	云平台、阿里云、安全事件、WAF安全事件
作用	监控应用防火墙有效请求率。经应用防火墙（WAF）拦截过滤后，如果对网站的有效请求率低于指定的阈值，则触发告警。

执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **有效请求率阈值**：网站有效请求率的阈值，默认值为90%。过去2分钟内经应用防火墙拦截过滤后，如果对网站的有效请求率低于该阈值，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• **网站（host）**：需要监控的网站名称。
	  ○ 您可以使用正则表达式 `.*` 进行配置。
	  ○ 默认值 `.*` 表示监控目标阿里云账号下所有被应用防火墙防护的网站。

外部配置	无
消除办法	检查触发告警的网站是否存在异常，是否存在被攻击的事件。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开应用防火墙（WAF）**访问日志**的开关。

1.10.2.22. TDI安全事件

本文介绍TDI安全事件的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现TDI安全事件问题。

告警规则列表

支持的告警规则如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- 云安全中心外网DNS请求成功率过低告警
- 云安全中心有效请求率过低告警
- 云安全中心新增告警数过多
- 云安全中心新增漏洞数过多
- 云安全中心高优先级告警数过多

云安全中心外网DNS请求成功率过低告警

告警ID	sls_app_audit_secure_at_sas_dns_rate
告警名称	云安全中心外网DNS请求成功率过低告警
版本号	1

类别	云平台、阿里云、安全事件、TDI安全事件
作用	监控云安全中心外网DNS请求成功率。当云安全中心的外网DNS请求成功率低于指定的阈值时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **请求成功率阈值**：请求成功率的阈值，默认值为90%。如果2分钟内云安全中心的外网DNS请求成功率低于该阈值，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。

外部配置	无
消除办法	检查云安全中心的外网DNS请求事件是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开云安全中心日志的开关。

云安全中心有效请求率过低告警

告警ID	sls_app_audit_secure_at_sas_rate
告警名称	云安全中心有效请求率过低告警
版本号	1
类别	云平台、阿里云、安全事件、TDI安全事件
作用	监控云安全中心的有效请求率。经云安全中心防护过滤后，如果对网站的有效请求率低于指定的阈值时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **有效请求率阈值**：有效请求率的阈值，默认值为90%。如果过去2分钟内经云安全中心防护过滤后，对网站的有效请求率低于该阈值，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。
	• **网站（host）**：需要监控的网站名称（支持正则）。
	  ○ 您可以使用正则表达式 `.*` 进行配置。
	  ○ 默认值 `.*` 表示监控目标阿里云账号下所有的网站。

外部配置	无
消除办法	检查云安全中心的请求事件是否存在异常，是否存在过多攻击事件。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开云安全中心日志的开关。

云安全中心新增告警数过多

告警ID	sls_app_audit_secure_at_sas_new_alert
告警名称	云安全中心新增告警数过多
版本号	1
类别	云平台、阿里云、安全事件、TDI安全事件
作用	监控云安全中心告警情况。当云安全中心新增告警数超过指定的阈值时，则触发告警。
执行频率	固定时间间隔：4分钟
查询范围	过去5分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **新增告警数阈值**：新增告警数的阈值，默认值为2。如果5分钟内云安全中心新增告警数超过该阈值时，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。

外部配置	无
消除办法	检查云安全中心中新增的告警。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开云安全中心日志的开关。

云安全中心新增漏洞数过多

告警ID	sls_app_audit_secure_at_sas_new_vul
告警名称	云安全中心新增漏洞数过多
版本号	1
类别	云平台、阿里云、安全事件、TDI安全事件
作用	监控云安全中心的漏洞情况。当云安全中心新增的漏洞数超过指定的阈值时，触发告警。
执行频率	固定时间间隔：4分钟
查询范围	过去5分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **新增漏洞数阈值**：新增漏洞数的阈值，默认值为1。如果5分钟内云安全中心新增漏洞数超过该阈值时，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。

外部配置	无

消除办法	检查云安全中心中新增的漏洞。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开云安全中心日志的开关。

云安全中心高优先级告警数过多

告警ID	sls_app_audit_secure_at_sas_ser_alert
告警名称	云安全中心高优先级告警数过多
版本号	1
类别	云平台、阿里云、安全事件、TDI安全事件
作用	监控云安全中心高优先级告警的情况。当云安全中心高优先级告警数超过指定的阈值时，触发告警。
执行频率	固定时间间隔：4分钟
查询范围	过去5分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **高优先级告警数阈值**：高优先级告警数的阈值，默认值为1。如果云安全中心内的高优先级告警数超过该阈值，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ◦ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ◦ 默认值为 `.*` ，表示监控审计服务下配置的所有阿里云账号。

外部配置	无
消除办法	检查云安全中心中的高优先级告警。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开云安全中心日志的开关。

1.10.2.23. 云防火墙安全事件

本文介绍云防火墙安全事件的告警规则。通过设置并开启告警规则，可及时触发告警，有助于您快速发现云防火墙安全事件问题。

告警规则列表

支持的告警规则如下所示。设置告警参数、设置白名单等相关操作，请参见设置告警。

- 云防火墙流入流量拦截告警

- 云防火墙流出流量拦截告警

云防火墙流入流量拦截告警

告警ID	sls_app_audit_secure_at_cfw_in_block
告警名称	云防火墙流入流量拦截告警
版本号	1
类别	云平台、阿里云、安全事件、云防火墙安全事件
作用	监控云防火墙的流入流量拦截情况。当云防火墙对一个访问协议流入流量的拦截次数超过指定阈值时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **流入流量拦截次数阈值**：流入流量拦截次数的阈值，默认值为10次。如果2分钟内云防火墙对一个访问协议的流入流量的拦截次数超过该阈值，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。
	• **访问协议名称**：需要监控的访问协议名称（支持正则）。
	  ○ 您还可以使用正则表达式 `.*` 进行配置。
	  ○ 默认值 `.*` 表示监控目标阿里云账号下所有的访问协议。

外部配置	无
消除办法	检查云防火墙对流入流量的拦截事件，确认是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开云防火墙**互联网访问日志**的开关。

云防火墙流出流量拦截告警

告警ID	sls_app_audit_secure_at_cfw_out_block
告警名称	云防火墙流出流量拦截告警
版本号	1
类别	云平台、阿里云、安全事件、云防火墙安全事件

作用	监控云防火墙的流出流量拦截情况。当云防火墙对一个访问协议流出流量的拦截次数超过指定阈值时，触发告警。
执行频率	固定时间间隔：1分钟
查询范围	过去2分钟

参数配置	告警参数说明如下所示：
	• **告警名称**：告警实例的名称，支持创建多个告警实例。
	• **严重度**：告警严重度，包括严重、高、中、低、报告。
	• **流出流量拦截次数阈值**：流出流量拦截次数的阈值，默认值为10次。如果2分钟内云防火墙对一个访问协议的流出流量的拦截次数超过该阈值，则触发告警。
	• **阿里云账号ID**：需要监控的阿里云账号ID（支持正则）。
	  ○ 多个阿里云账号ID之间可以使用竖线（|）分隔。您还可以使用正则表达式 `.*` 进行配置，例如156133.*，表示监控以156133开头的阿里云账号。
	  ○ 默认值为 `.*`，表示监控审计服务下配置的所有阿里云账号。
	• **访问协议名称**：需要监控的访问协议名称（支持正则）。
	  ○ 您还可以使用正则表达式 `.*` 进行配置。
	  ○ 默认值 `.*` 表示监控目标阿里云账号下所有的访问协议。

外部配置	无
消除办法	检查云防火墙对流出流量的拦截事件，确认是否存在异常。
前提条件	确保已在日志审计服务中的**审计配置 > 云产品接入 > 全局配置**中打开云防火墙**互联网访问日志**的开关。

1.11. 最佳实践

1.11.1. 使用资源目录进行跨账号日志采集与同步授权

日志审计服务支持将多个阿里云账号下的日志采集到一个阿里云账号下的Project中。在多账号场景下，您可以使用资源目录管理账号。本文介绍如何使用资源目录进行跨账号日志采集与同步授权。

前提条件

- 已创建成员，即待采集日志的云产品涉及的所有阿里云账号均已加入资源目录中。

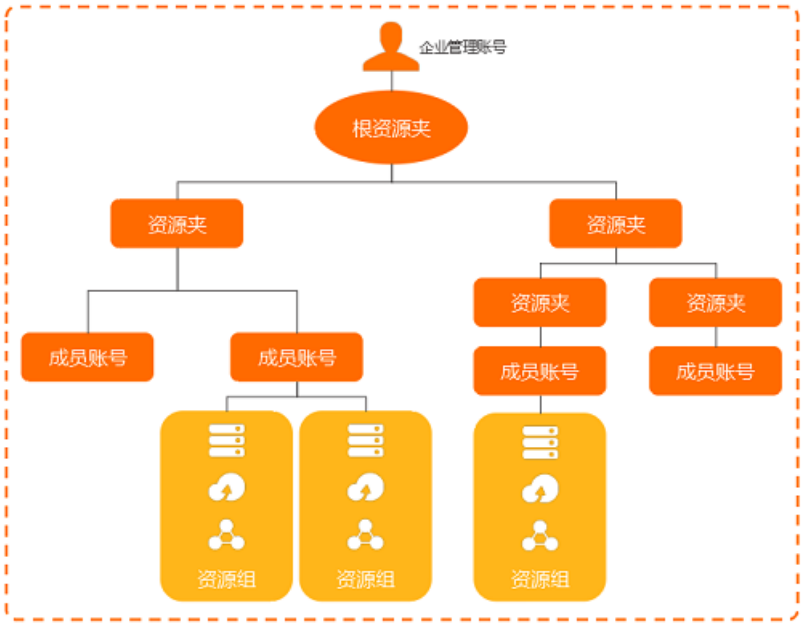
  您可通过创建或邀请成员的方式将阿里云账号加入到资源目录中。更多信息，请参见创建成员、邀请阿里云账号加入资源目录。
- 中心Project所在账号已开通日志服务。
- 待采集日志的云产品已开启相应的服务。更多信息，请参见云产品覆盖及相关资源。

背景信息

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。在使用日志审计服务时，您可以使用账号密钥辅助授权方式和手动授权方式完成授权，授予日志服务采集相关云产品日志的权限以及授权多个阿里云账号之间的同步汇集。在多账号场景下，您可以使用资源目录管理账号。更多信息，请参见日志审计服务。

资源目录是阿里云面向企业客户提供的一套多级资源（账号）关系管理服务。资源目录服务的本质：建立一套与您的企业相关的，基于资源使用的关系结构。资源目录具有全局一致性的特点，方便您基于此关系结构，对企业内多个应用服务所对应的各种资源进行高效的规划、构建和管理。是阿里云面向企业客户提供的一套多级资源（账号）关系管理服务。更多信息，请参见资源目录。

资源目录支持您基于企业的业务或生态环境，让您方便的构建出体现资源关系的目录结构，并将企业多个账号分布到这个目录结构中的相应位置，从而形成资源间的多层级关系。企业可依赖设定的组织关系进行资源的集中管理，满足企业资源在财资、安全、审计及合规方面的管控需要。下图展示了资源目录的基本结构。



- 企业管理账号是资源目录的超级管理员，也是开通资源目录的初始账号，对其创建的资源目录和成员账号拥有完全控制权限。每个资源目录有且只有一个企业管理账号。为了确保企业管理账号的安全，建议您创建一个新的阿里云账号作为企业管理账号，避免将已有用途的云账号作为企业管理账号。更多信息，请参见企业管理账号。
- 资源夹是资源目录内的组织单元，通常用于指代企业的分公司、业务线或产品项目。每个资源夹下可以放置成员账号，并允许嵌套子资源夹，最终形成树形的资源组织关系。更多信息，请参见资源夹。
- 成员账号是阿里云账号在资源目录中的一种称呼。在资源目录内，成员账号作为资源容器，是一种资源分组单位。成员账号通常用于指代一个项目或应用，每个成员账号中的资源相对其他成员账号中的资源是物理隔离的。更多信息，请参见成员账号。

操作步骤

1. 通过资源目录访问中心Project所在账号。

   在资源目录内创建或邀请成员后，您可以从资源目录的成员账号中选取一个账号作为日志审计服务中心Project所在的阿里云账号。然后通过RAM用户、RAM角色或根用户访问中心Project所在的阿里云账号。

   - 通过RAM角色访问成员
   - 通过RAM用户访问成员
   - 通过根用户访问成员

2. 登录日志服务控制台。
3. 在**日志应用**区域，单击**日志审计服务**。
4. 在中心Project所在账号内进行日志审计采集的首次配置。

   如果该账号已完成首次配置，可跳过此步骤。

   i. 在左侧导航栏，单击**云产品接入 > 全局配置**。

   ii. 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。

   - 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）、德国（法兰克福）、印尼（雅加达）

   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。

   - 通过账号密钥辅助授权：输入账号的AccessKey信息，AccessKey信息不会被保存，仅临时使用。

     此处AccessKey对应的RAM用户需具备RAM读写权限（例如已被授权AliyunRAMFullAccess策略）。具体操作，请参见授权RAM用户。

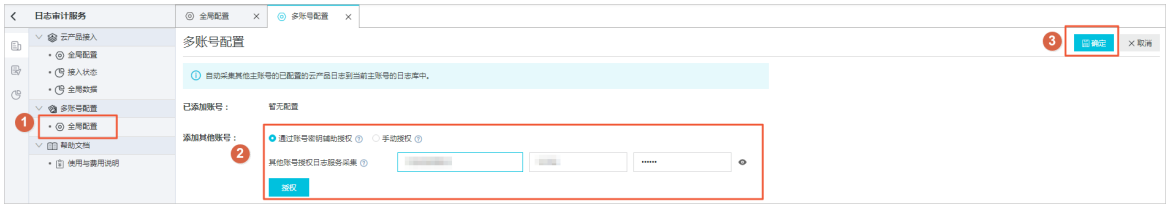
   - 手动授权：更多信息，请参见自定义授权日志采集与同步。

   iv. 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、DRDS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。

   v. 单击**保存**。

5. 在中心Project所在账号内进行多账号采集配置。



   i. 在左侧导航栏中，单击**多账号配置 > 全局配置**。

   ii. 在**多账号配置**页面，单击**修改**。

   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。

   - 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AccessKey信息及其阿里云账号ID。AccessKey信息不会被保存，仅临时使用。

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

   - 手动授权：输入阿里云账号ID，可配置多个。对应的账号权限配置请参见操作步骤。

6. 通过资源目录依次访问其他需要被采集同步的阿里云账号，并进行手动授权。

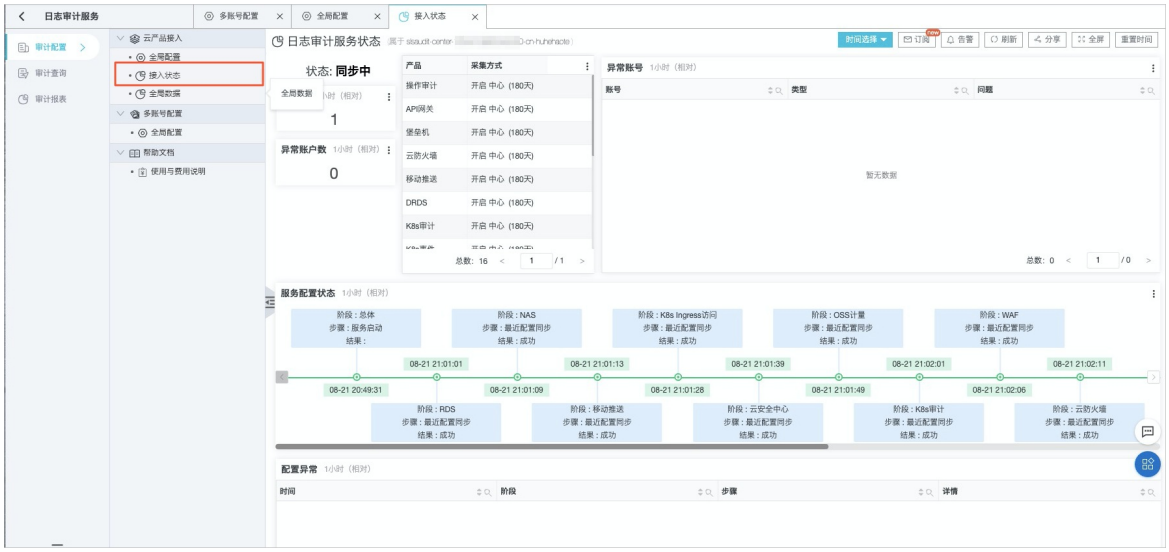
   在步骤5中，如果使用的是手动授权方式完成授权，则需要配置此步骤；如果使用的是通过账号密钥辅助授权方式完成授权，请跳过此步骤。

   i. 通过资源目录访问待授权的账号。更多信息，请参见步骤1。

   ii. 在该账号内进行跨账号采集配置手动授权。更多信息，请参见操作步骤中的步骤3。

7. 查看配置结果。

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。更多信息，请参见常见问题及错误排查。



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。

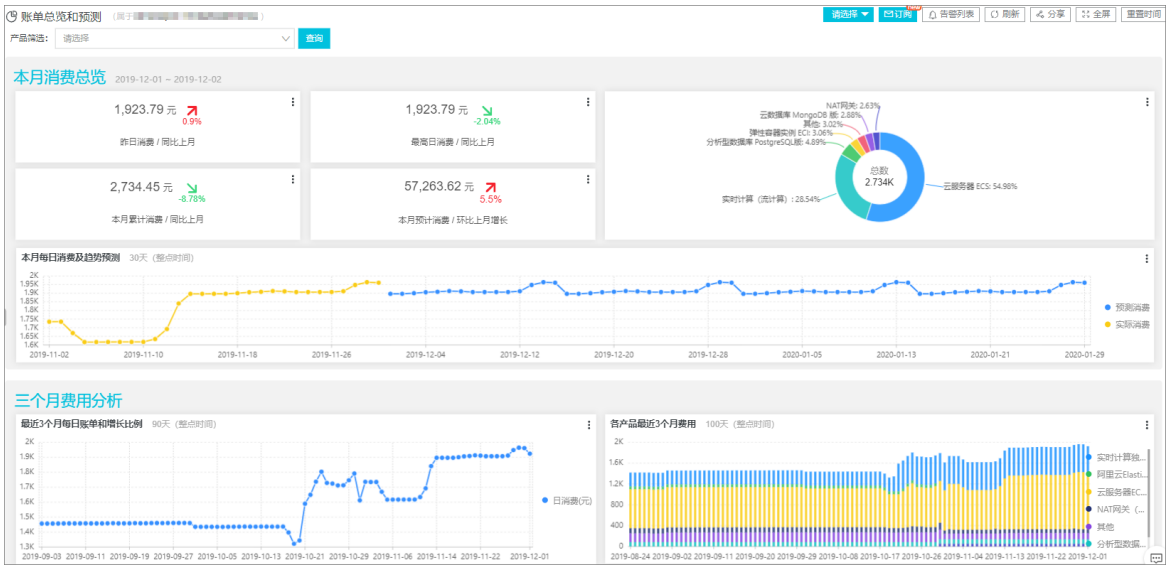
1. 单击左侧**成本管家**下的**自定义分析**。
2. 在**自定义分析**界面的查询分析输入框中，输入查询分析语句，对导入的账单进行查询分析。

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，详细介绍请参见可视化概述。

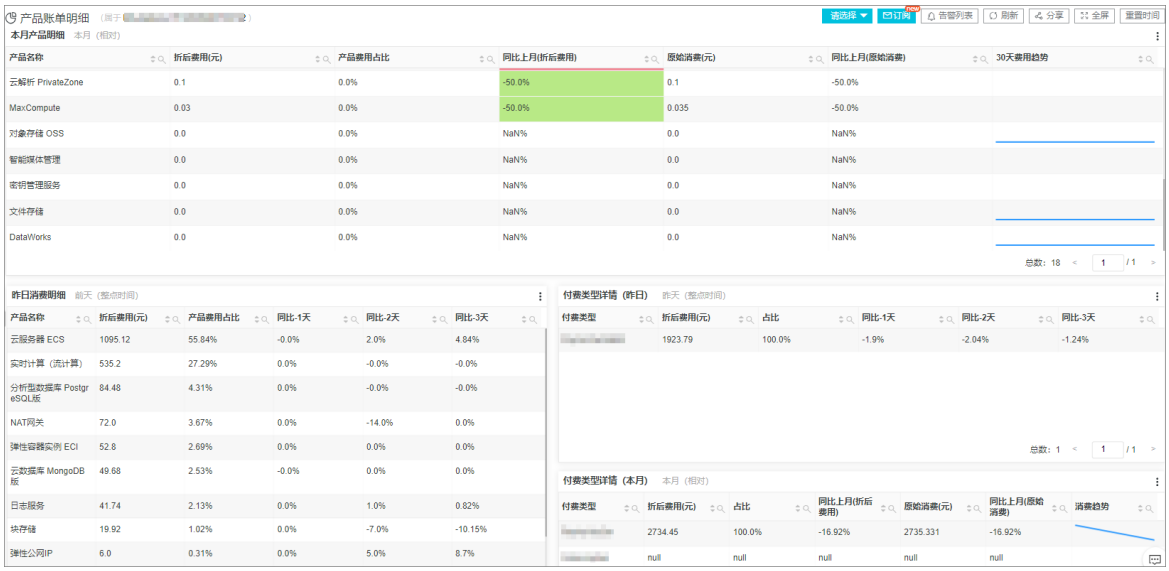
1. 单击左侧**成本管家**下的**总览**。
2. 在**总览**界面查看账单总览和预测信息。



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，详细介绍请参见可视化概述。

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。



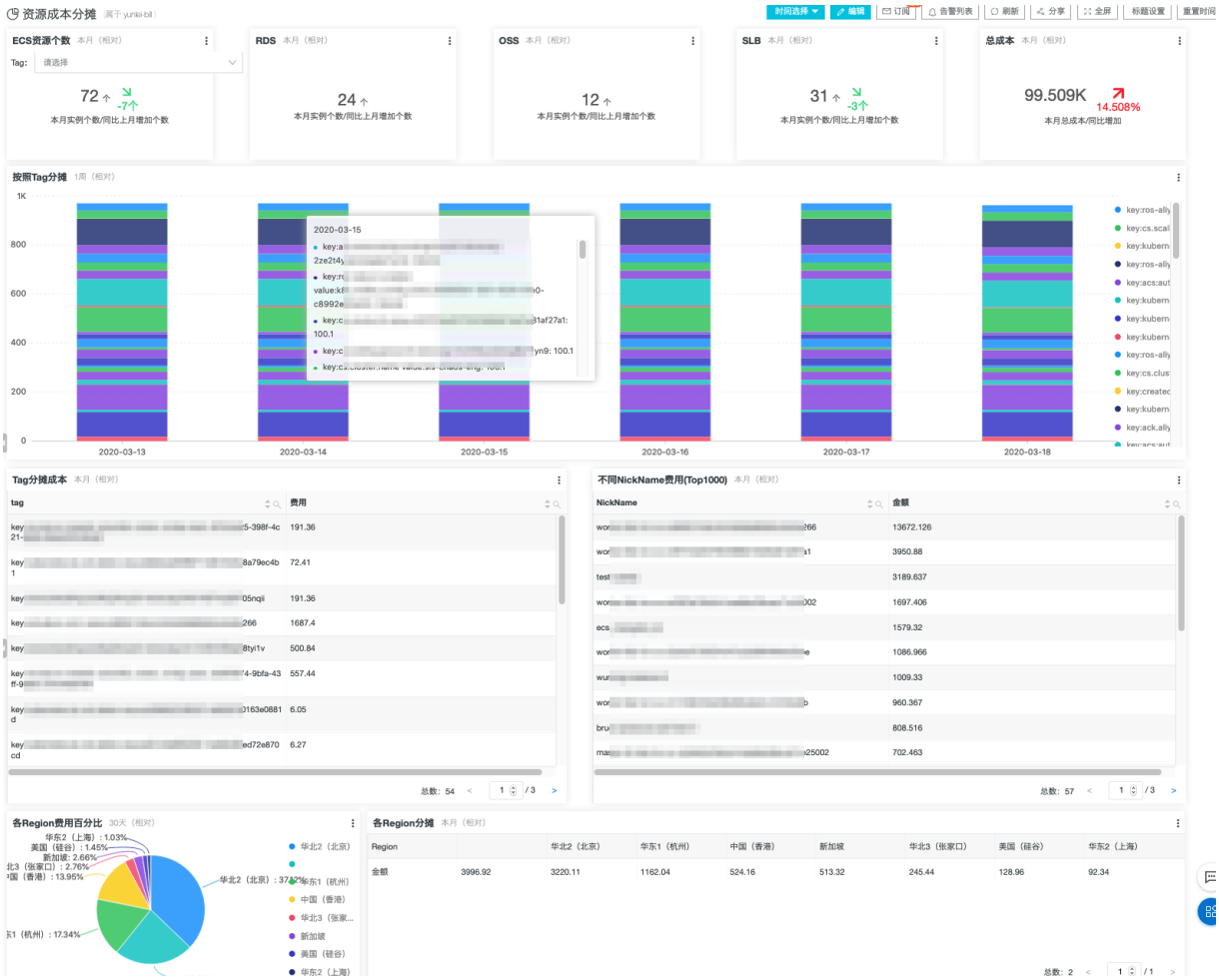
账单优化

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。

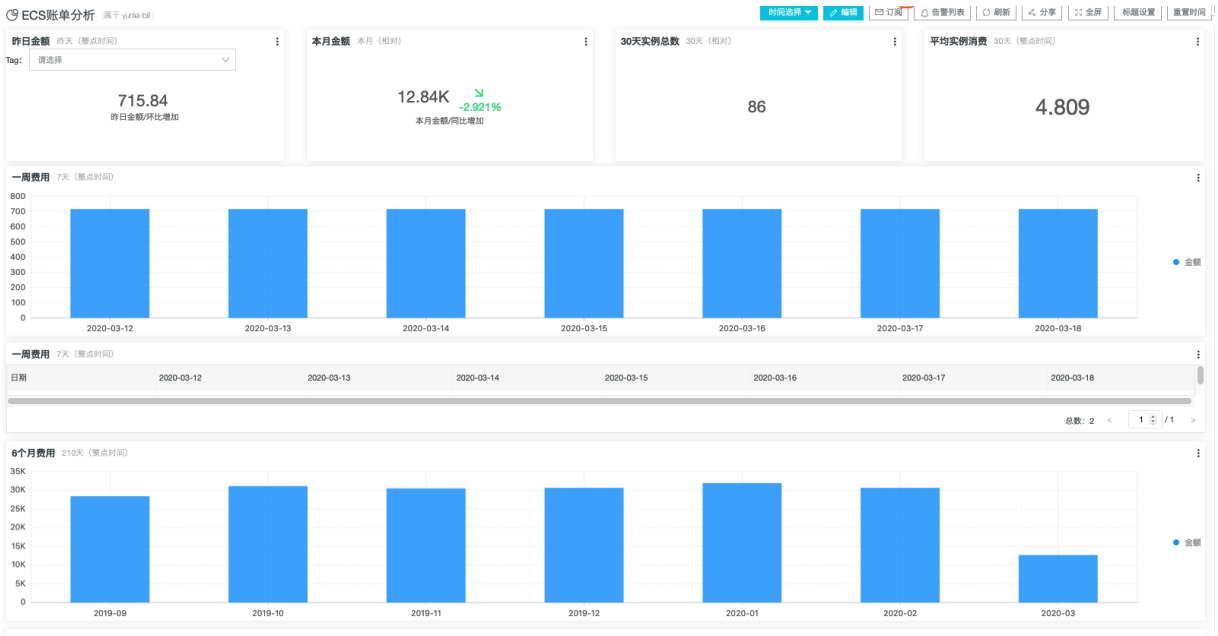
资源成本分摊

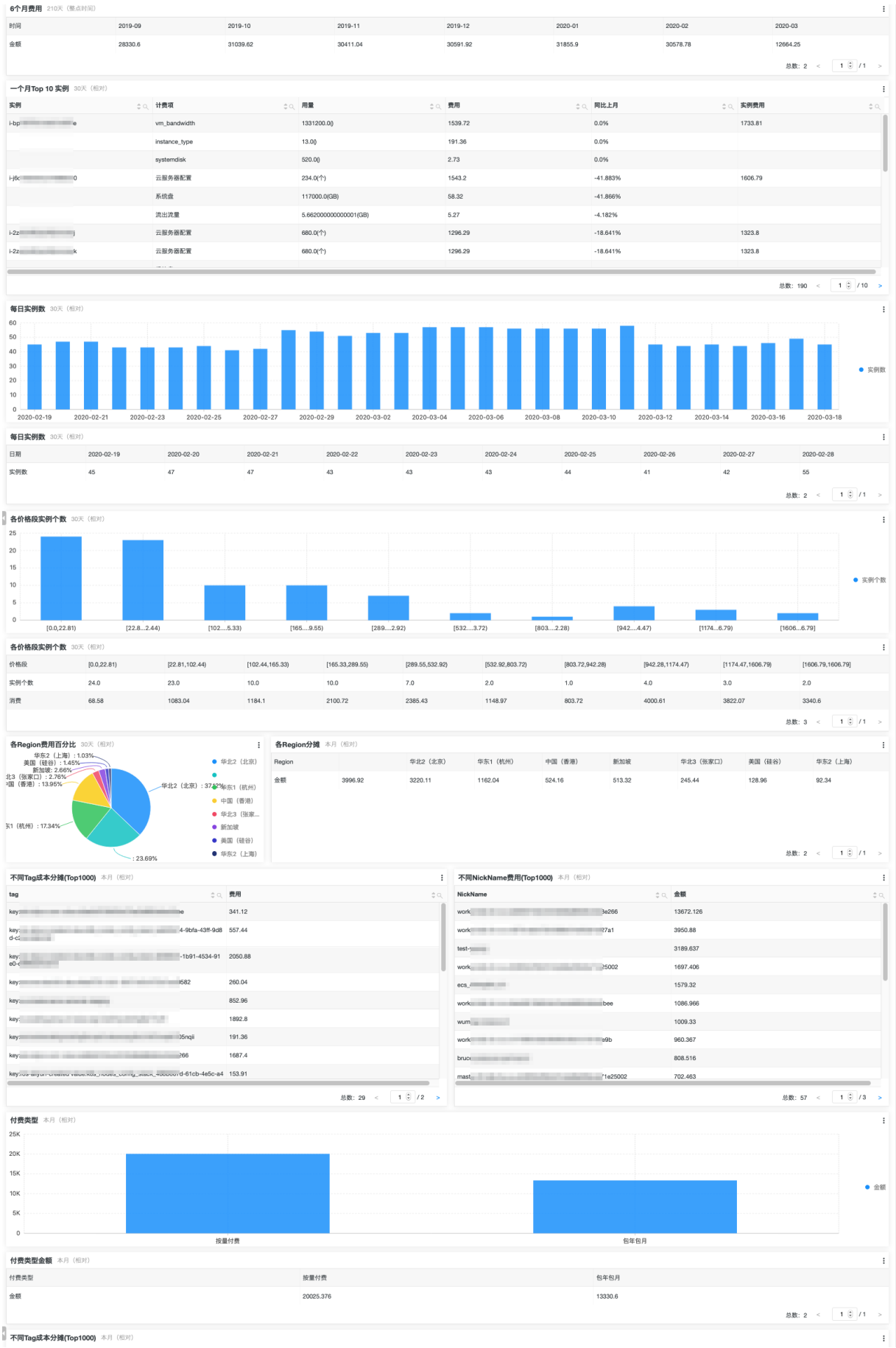
通过资源成本分摊报表，可以查看主要云资源的使用数目，以及按照tag、昵称等进行分账管理。

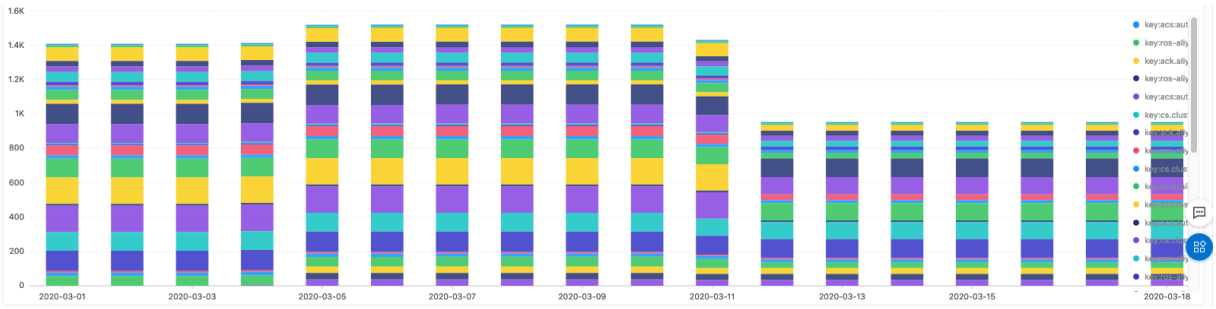


ECS 账单分析报表

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。

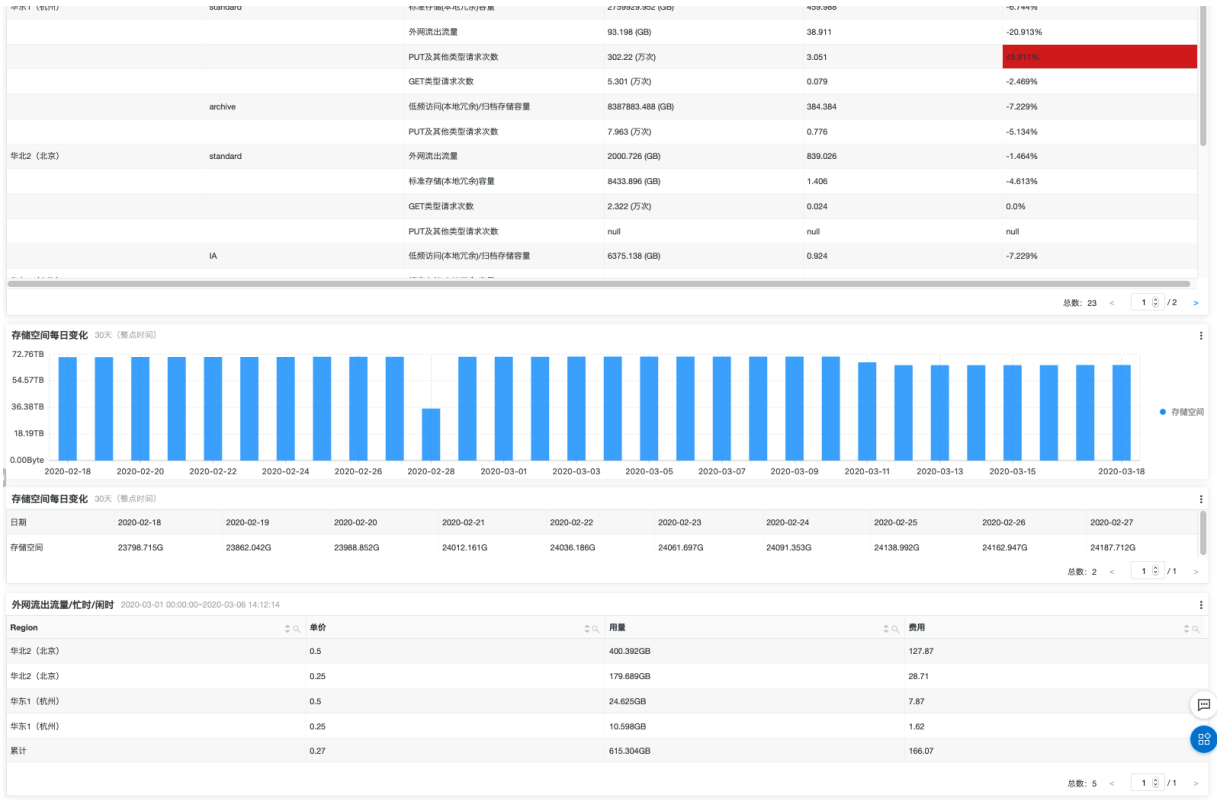



6个月费用 210天（整点时间）
时间 2019-09 2019-10 2019-11 2019-12 2020-01 2020-02 2020-03
金额 28330.6 31039.62 30411.04 30591.92 31855.9 30578.78 12664.25
一个月Top 10 实例 30天（相对）
实例 计费项 用量 费用 同比上月 实例费用
每日实例数 30天（相对）
实例数
每日实例数 30天（相对）
日期 2020-02-19 2020-02-20 2020-02-21 2020-02-22 2020-02-23 2020-02-24 2020-02-25 2020-02-26 2020-02-27 2020-02-28
实例数 45 47 47 43 43 43 44 41 42 55
各价格段实例个数 30天（相对）
[0.0,22.81) [22.8...2.44) [102....5.33) [165....9.55) [289....2.92) [532....3.72) [803....2.28) [942....4.47) [1174...6.79) [1606...6.79]
实例个数
各价格段实例个数 30天（相对）
价格段 [0.0,22.81) [22.81,102.44) [102.44,165.33) [165.33,289.55) [289.55,532.92) [532.92,803.72) [803.72,942.28) [942.28,1174.47) [1174.47,1606.79) [1606.79,1606.79]
实例个数 24.0 23.0 10.0 10.0 7.0 2.0 1.0 4.0 3.0 2.0
消费 68.58 1083.04 1184.1 2100.72 2385.43 1148.97 803.72 4000.61 3822.07 3340.6
各Region费用百分比 30天（相对）
华北2（北京）：37.22%
华东1（杭州）：17.34%
华北2（北京）
华东1（杭州）
中国（香港）
新加坡
美国（硅谷）
华东2（上海）
各Region分摊 本月（相对）
Region 华北2（北京） 华东1（杭州） 中国（香港） 新加坡 华北3（张家口） 美国（硅谷） 华东2（上海）
金额 3996.92 3220.11 1162.04 524.16 513.32 245.44 128.96 92.34
不同Tag成本分摊(Top1000) 本月（相对）
tag 费用
不同NickName费用(Top1000) 本月（相对）
NickName 金额
付费类型 本月（相对）
按量付费
包年包月
付费类型金额 本月（相对）
付费类型 按量付费 包年包月
金额 20025.376 13330.6
不同Tag成本分摊(Top1000) 本月（相对）



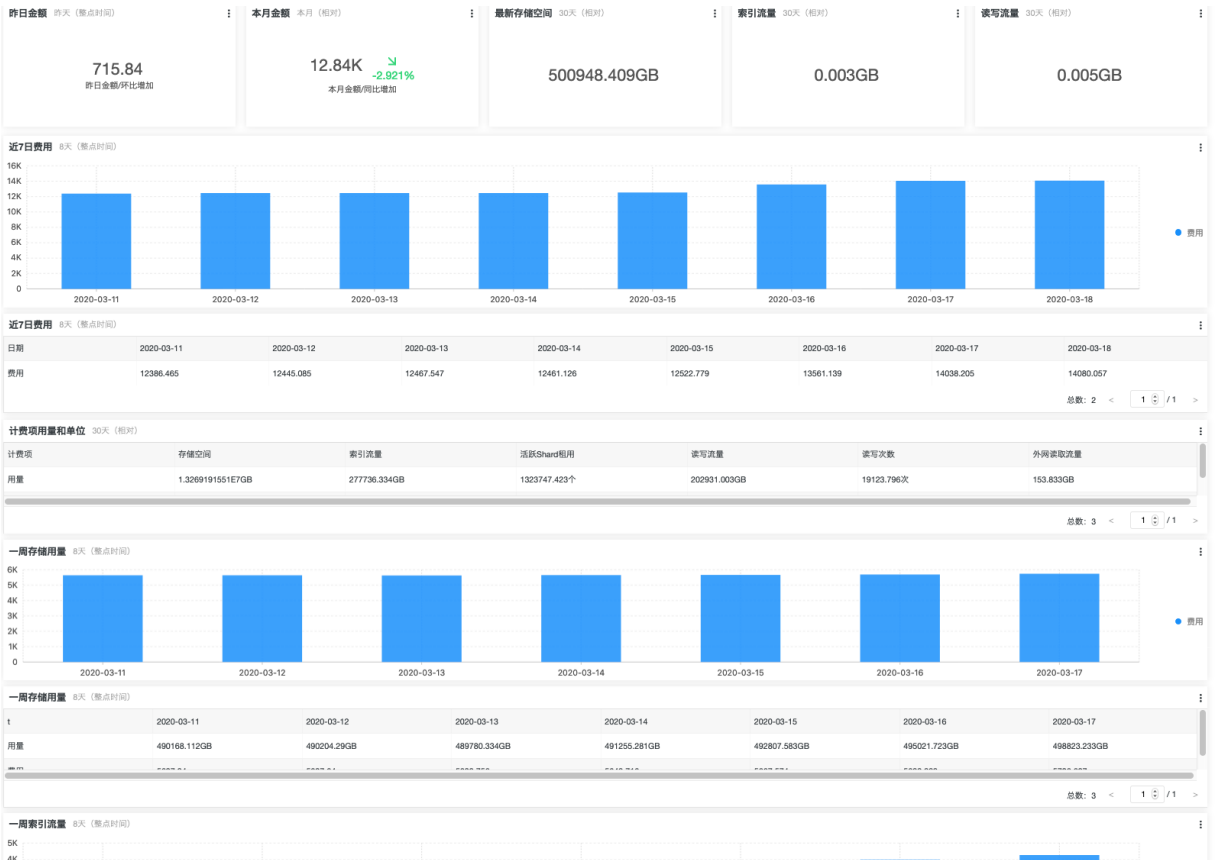
OSS账单分析

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。



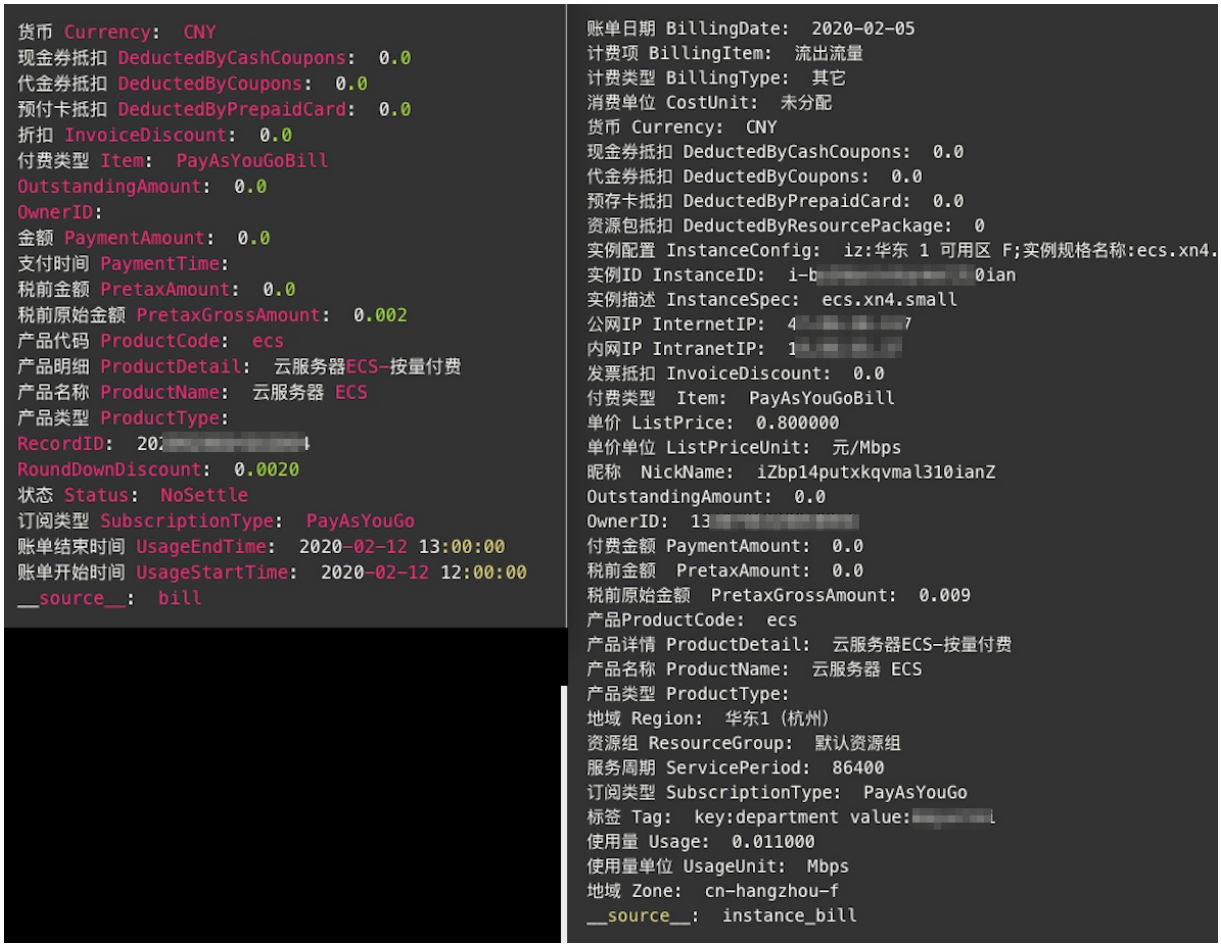
2.2. 使用SQL语句自定义分析账单

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` 。

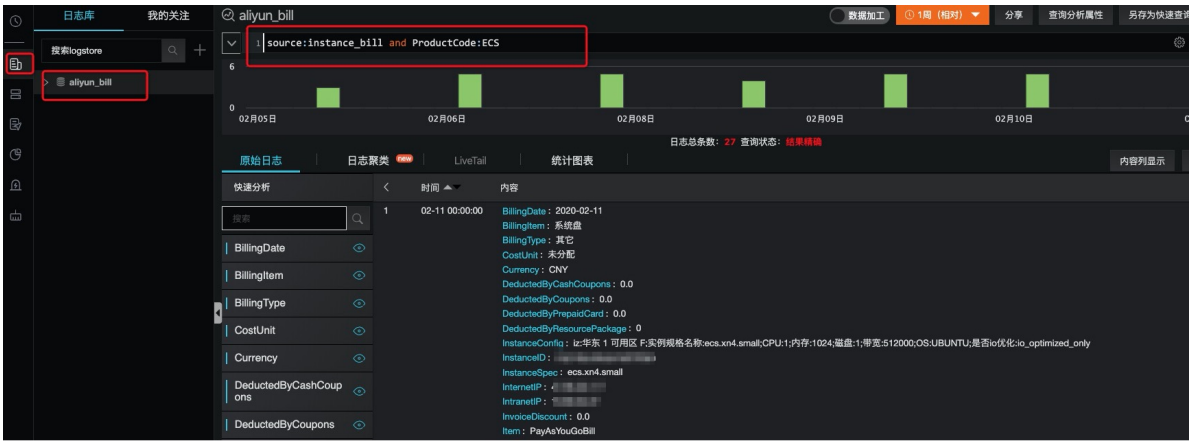


案例

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。

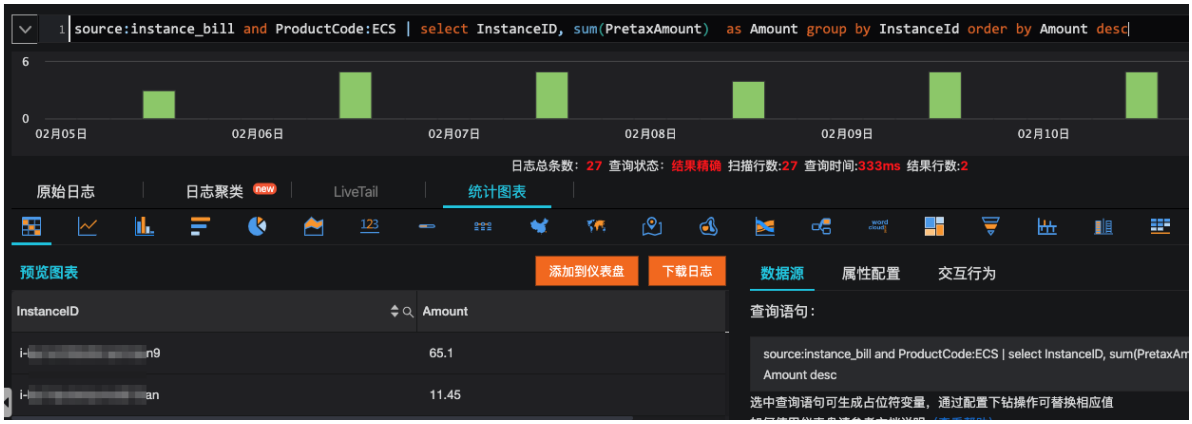
```
source:instance_bill and ProductCode:ECS | select sum(PretaxAmount)
```

- 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 ))
    ```

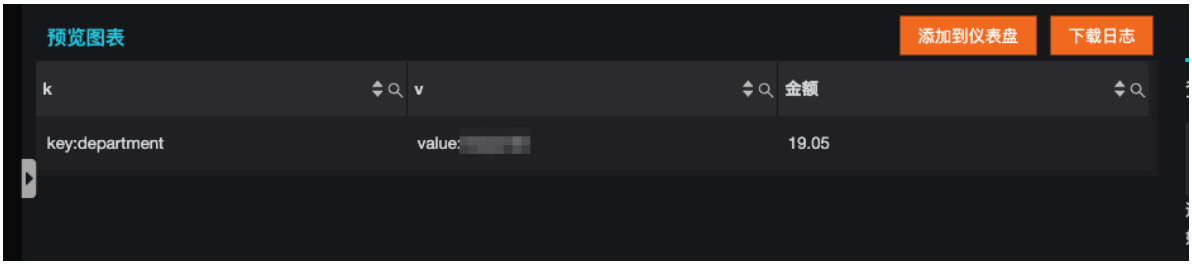
  - 按照产品，与上月进行同比分析。

    ```
    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。

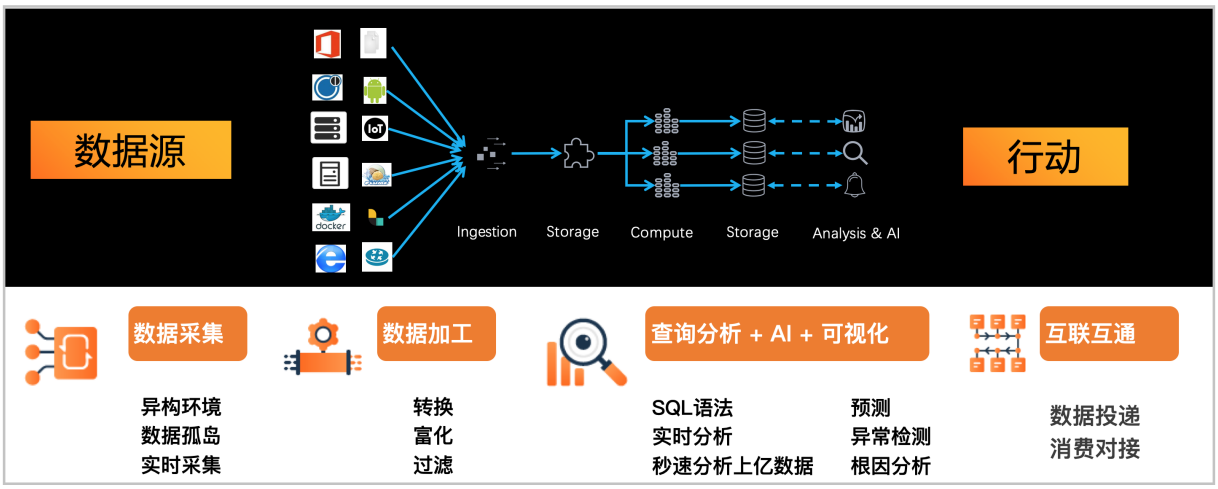
简介

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，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

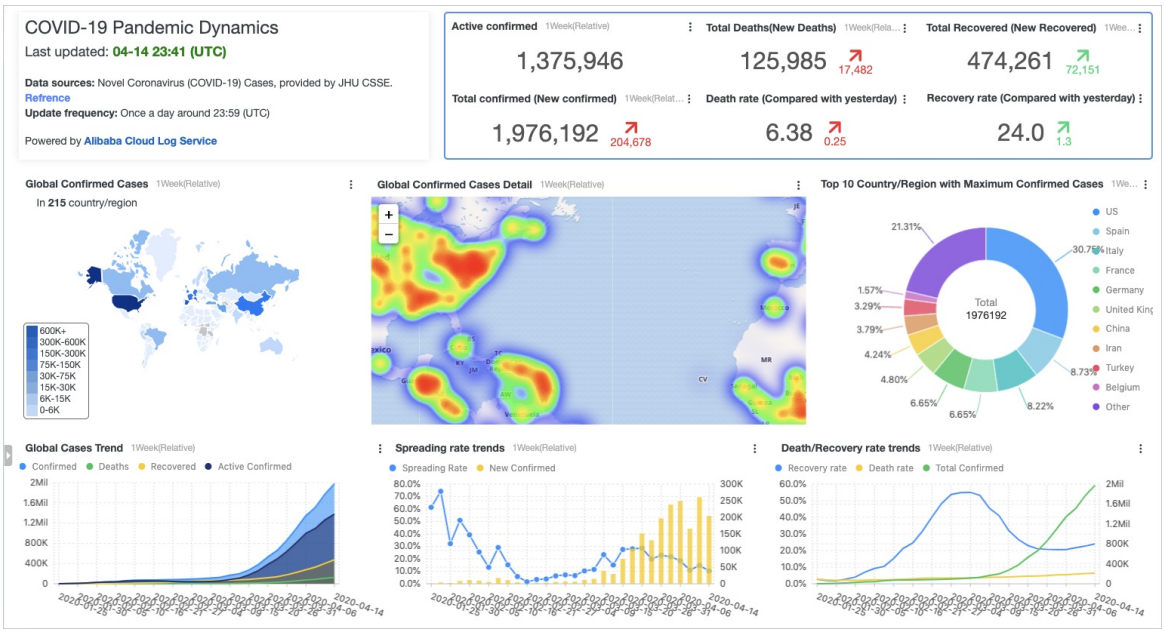
- 定时同步疫情数据，并形成可视化平台覆盖全球各个国家/地区、省份/州的疫情信息。

  > **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）。

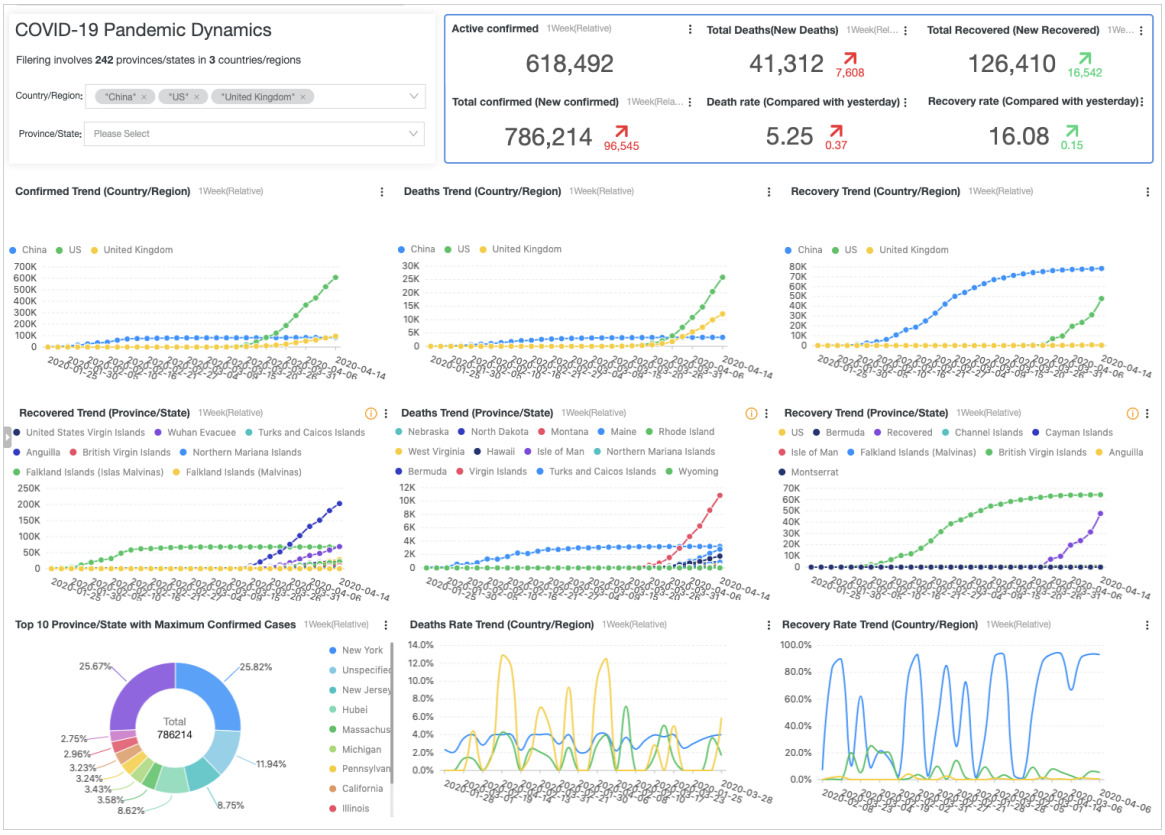
- 内置多份数据大盘并支持自定义。

  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

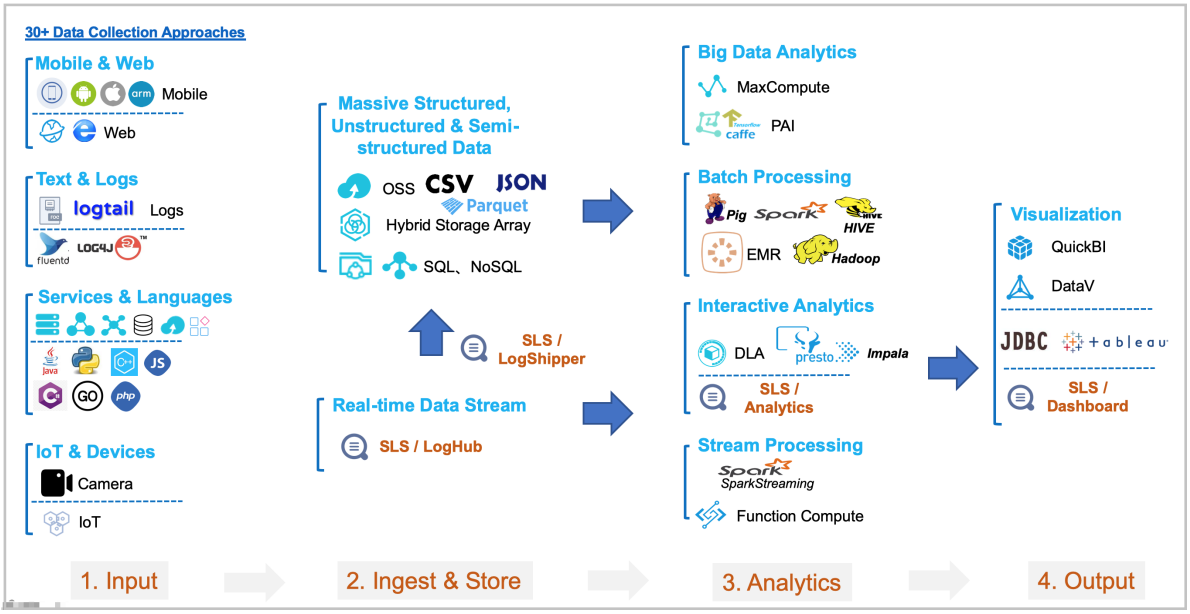


- 各个国家/地区的疫情详情



- 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。



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。
- 数据存储和分析功能不收费。
- 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。更多信息，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。
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。更多信息，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]
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

字段名	说明	样例
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
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]

字段	说明	样例
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
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]

字段	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}

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**。

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？

  如果您需删除所属项目，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**。
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事件监控。

  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。更多信息，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。
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。

操作	说明
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。更多信息，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。更多信息，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。

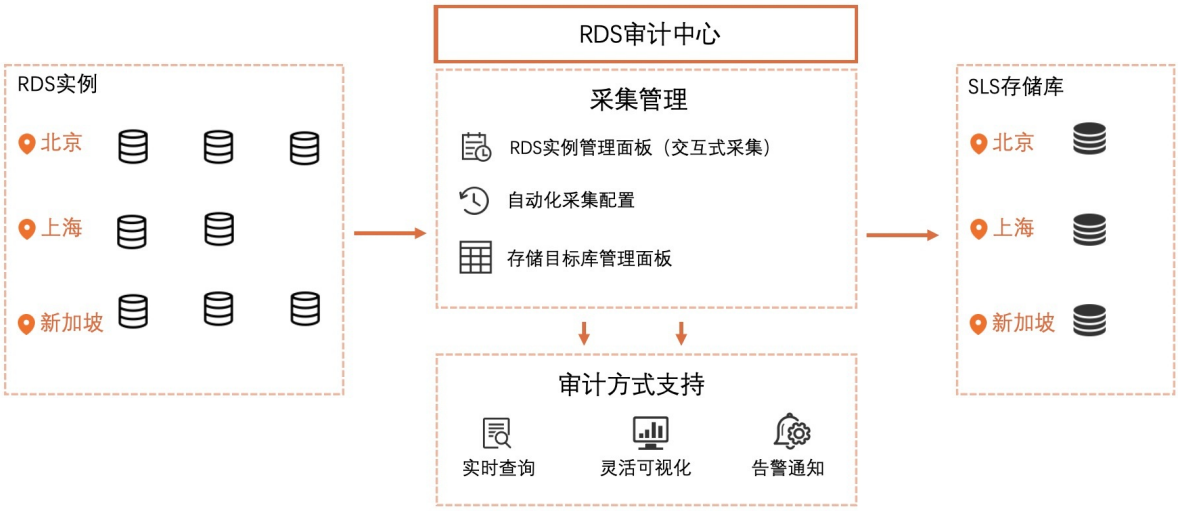
5.RDS审计中心

5.1. 使用前须知

阿里云日志服务与云数据库RDS联合推出RDS审计中心。您可以通过RDS审计中心实时查看RDS SQL审计日志的采集状态，集中管理采集配置，并可基于采集到的日志进行后续的审计、分析、告警等操作。

功能说明

RDS审计中心支持如下功能：



- 采集管理
  - 支持集中管理RDS SQL审计日志的采集状态。
  - 支持自动采集现有或未来新增RDS实例的SQL审计日志。
  - 支持集中管理存储目标库（Project、Logstore）。
- 日志审计
  - 提供RDS SQL审计日志的实时存储、查询与分析。
  - 提供丰富的可视化报表，支持报表邮件、钉钉群订阅。
  - 提供丰富的内置告警规则，支持灵活配置告警策略，及时精准地发送告警消息。

支持的日志类型

RDS SQL审计日志记录了对数据库执行的所有操作，这些信息是系统通过网络协议分析所得，对系统CPU消耗极低，不影响SQL执行效率。RDS SQL审计日志包括但不限于如下操作：

- 数据库的登录和退出操作。
- DDL（Data Definition Language）操作：对数据库结构定义的SQL语句，包括CREATE、ALTER DROP、TRUNCATE、COMMENT等。
- DML（Data Manipulation Language）操作：SQL操作语句，包括SELECT、INSERT、UPDATE、DELETE等。
- 其他SQL执行操作，包括任何其他通过SQL执行的控制，例如回滚、控制等。
- SQL执行的延迟、执行结果、影响的行数等信息。

资产详情

- 自定义日志服务Project和Logstore

  > **注意** 请勿删除RDS SQL审计日志对应的日志服务Project和Logstore，否则将无法正常推送日志到日志服务。

- 专属仪表盘

  默认生成3个仪表盘。

  > **说明** 专属仪表盘可能随时进行升级与更新，建议您不要修改专属仪表盘。您可以自定义仪表盘用于查询结果展示。更多信息，请参见创建仪表盘。

仪表盘	说明
RDS审计运营中心	展示整体访问情况、活跃数据库等信息，包括操作的数据库数量、操作表格数、执行错误、累计插入行数、累计更新行数、累计删除行数、累计查询行数等。
RDS审计性能中心	展示运维可靠性相关指标，包括SQL执行峰值、查询带宽峰值、插入开端峰值、更新带宽峰值、删除带宽峰值、SQL平均时间、查询SQL平均时间、更新SQL平均时间、删除SQL平均时间等。
RDS审计安全中心	展示数据库安全相关指标，包括错误数、登录失败次数、大批量删除事件、大批量修改事件数、危险SQL执行次数、错误操作类型分布、出错客户端外网分布、错误最多的客户端等。

费用说明

- RDS审计中心中的日志采集功能依赖于RDS实例的SQL洞察（MySQL）功能。SQL洞察功能，在RDS产品侧产生相关费用。更多信息，请参见价格、收费项与计费方式。

  > **说明** 三节点企业版（原金融版）实例的SQL洞察功能免费。

- 采集RDS SQL审计日志到日志服务后，日志服务根据存储空间、读取流量、请求数量、数据加工、数据投递等进行收费，费用说明请参见按量付费。

限制说明

- 目前支持投递RDS SQL审计日志到日志服务的RDS类型如下所示。

  MySQL：基础版本不支持，其他在售版本均支持。

- RDS审计中心中的日志采集功能依赖于RDS实例的或SQL洞察（MySQL）功能。

  在RDS审计中心开启RDS SQL审计日志采集功能后，系统自动开启对应RDS实例的SQL洞察（MySQL）功能。

- RDS实例和日志服务Project需处于同一地域。
- 除本地云以外的其他地域都支持。

RDS审计日志采集方式比较？

目前，日志服务支持通过如下三种方式采集RDS SQL审计日志。

> **说明** RDS审计中心方式和接入数据-RDS审计方式中的采集配置是互通的。日志审计服务中的RDS SQL审计日志采集配置为独立的采集渠道，不受另外两种采集方式影响。

- RDS审计中心
  - 入口：在日志服务控制台首页的**日志应用**区域，单击**RDS审计中心**。
  - 推荐场景：建议在单账号采集场景下使用。
- 日志审计服务
  - 入口：在日志服务控制台首页的**日志应用**区域，单击**日志审计服务**。
  - 推荐场景：建议在跨账号、跨地域采集场景下使用。
- 接入数据-RDS审计
  - 入口：在日志服务控制台首页的**接入数据**区域，单击**RDS审计**。
  - 推荐场景：无，可由RDS审计中心代替。

属性	接入数据-RDS审计	RDS审计中心	日志审计服务
指定RDS实例粒度	支持	支持	支持
灵活指定存储目标库	支持	支持	不支持
跨地域采集	不支持	不支持	支持
跨账号采集	不支持	不支持	支持
自动采集	不支持	支持	支持
手动采集	支持	支持	不支持
查看采集状态视图	不支持	支持	不支持

5.2. 授予RAM用户操作权限

本文介绍如何授予阿里云RAM用户操作RDS审计中心的权限。

前提条件

已创建RAM用户。具体操作，请参见创建RAM用户。

背景信息

您可以通过如下两种方式给RAM用户授予RDS审计中心的操作权限。

- 极简授权：权限较大，操作简单。
- 自定义权限策略：权限精细，配置复杂。

极简授权

使用阿里云账号登录RAM控制台，为RAM用户授予全部管理权限（AliyunLogFullAccess、AliyunRAMFullAccess）。具体操作，请参见为RAM用户授权。

自定义权限策略

1. 使用阿里云账号登录RAM控制台。
2. 创建权限策略。
   i. 在左侧导航栏中，选择**权限管理 > 权限策略管理**。
   ii. 单击**创建权限策略**。
   iii. 在**新建自定义权限策略**页面中，配置如下参数，并单击**确定**。

参数	说明
策略名称	配置策略名称。
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。 您可以授予RAM用户使用RDS审计中心的只读权限或读写权限，具体权限策略说明如下： ■ 只读权限（只允许查看RDS审计中心中的各个页面。） { "Version": "1", "Statement": [{ "Action": ["rds:DescribeSqlLogInstances", "rds:DisableSqlLogDistribution"], "Resource": "*", "Effect": "Allow" }, { "Effect": "Allow", "Action": ["log:CreateLogStore", "log:CreateIndex", "log:UpdateIndex", "log:ListLogStores", "log:GetLogStore", "log:GetLogStoreLogs", "log:CreateDashboard", "log:CreateChart", "log:UpdateDashboard"], "Resource": ["acs:log:*:*:project/sls-alert-*/logstore/*", "acs:log:*:*:project/sls-alert-*/dashboard/*"] }, { "Effect": "Allow", "Action": ["log:CreateProject"

参数	说明

策略内容	■ 读写权限（允许操作RDS审计中心中的各个功能。）
	{
	"Version": "1",
	"Statement": [
	{
	"Action": [
	"rds:DescribeSqlLogInstances",
	"rds:DisableSqlLogDistribution",
	"rds:DisableSqlLogDistribution",
	"rds:EnableSqlLogDistribution",
	"rds:ModifySQLCollectorPolicy"
	],
	"Resource": "*",
	"Effect": "Allow"
	},
	{
	"Effect": "Allow",
	"Action": [
	"log:CreateLogStore",
	"log:CreateIndex",
	],
	"Resource": [
	"acs:log:*:*:project/sls-alert-*"
	]
	},
	{
	"Effect": "Allow",
	"Action": [
	"log:GetLogStore",
	"log:ListLogStores",
	"log:GetIndex",
	"log:GetLogStoreHistogram",
	"log:GetLogStoreLogs",
	"log:GetDashboard",
	"log:ListDashboard",
	"log:ListSavedSearch",
	"log:GetProjectLogs"
	],
	"Resource": [
	"acs:log:*:*:project/*/logstore/*",
	"acs:log:*:*:project/*/dashboard/*",
	"acs:log:*:*:project/*/savedsearch/*"
	]
	},
	{
	"Action": [
	"ram:GetRole"
	],
	"Resource": "acs:ram:*:*:role/aliyunlogarchiverole",
	"Effect": "Allow"
	}
	]
	}

参数	说明

```
        "log:UpdateIndex",
        "log:ListLogStores",
        "log:GetLogStore",
        "log:GetLogStoreLogs",
        "log:CreateDashboard",
        "log:CreateChart",
        "log:UpdateDashboard"
      ],
      "Resource": [
        "acs:log:*:*:project/sls-alert-*/logstore/*",
        "acs:log:*:*:project/sls-alert-*/dashboard/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "log:CreateProject"
      ],
      "Resource": [
        "acs:log:*:*:project/sls-alert-*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "log:GetLogStore",
        "log:ListLogStores",
        "log:GetIndex",
        "log:GetLogStoreHistogram",
        "log:GetLogStoreLogs",
        "log:GetDashboard",
        "log:ListDashboard",
        "log:ListSavedSearch",
        "log:CreateLogStore",
        "log:CreateIndex",
        "log:UpdateIndex",
        "log:ListLogStores",
        "log:GetLogStore",
        "log:GetLogStoreLogs",
        "log:CreateDashboard",
        "log:CreateChart",
        "log:UpdateDashboard",
        "log:UpdateLogStore",
        "log:GetProjectLogs"
      ],
      "Resource": [
        "acs:log:*:*:project/*/logstore/*",
        "acs:log:*:*:project/*/dashboard/*",
        "acs:log:*:*:project/*/savedsearch/*"
      ]
    },
    {
      "Action": [
        "log:SetGeneralDataAccessConfig"
```

参数	说明

	],
	"Resource": [
	"acs:log:*:*:resource/sls.general_data_access.rds.global_conf.single_account_channel/record"
	],
	"Effect": "Allow"
	},
	{
	"Action": "ram:CreateServiceLinkedRole",
	"Resource": "*",
	"Effect": "Allow",
	"Condition": {
	"StringEquals": {
	"ram:ServiceName": "audit.log.aliyuncs.com"
	}
	}
	},
	{
	"Action": [
	"ram:*"
	],
	"Resource": [
	"acs:ram:*:*:role/aliyunlogarchiverole",
	"acs:ram:*:*:policy/AliyunLogArchiveRolePolicy"
	],
	"Effect": "Allow"
	}
	]
	}

3. 为RAM用户授权。
   i. 在左侧导航栏中，选择**身份管理 > 用户**。
   ii. 找到目标RAM用户，单击**添加权限**。
   iii. 在**添加权限**面板的**选择权限**区域，单击**自定义策略**，选中步骤中创建的策略。
   iv. 单击**确定**。

5.3. 开启日志采集功能

RDS审计中心支持手动开启采集功能和自动化采集功能。手动开启采集功能针对单个RDS实例，自动化采集功能支持多个RDS实例，自动采集符合条件的RDS实例（包括未来创建的）的审计日志。本文介绍开启采集功能的操作步骤及相关操作。

前提条件

- 如果是手动开启采集功能，则需要在RDS实例所在地域创建日志服务Project和Logstore。具体操作，请参见创建Project和Logstore。
- 如果您使用的是RAM用户，则需要先授予RAM用户RDS审计中心操作权限。具体操作，请参见授予RAM用户操作权限。

首次配置

> **注意**
> - 执行该操作的账号具备AliyunRamFullAccess权限。
> - 本操作只需执行一次。

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**RDS审计中心**。
3. 根据页面提示，完成AliyunLogArchiveRole角色授权。

   完成此操作后，阿里云自动为您创建一个系统角色AliyunLogArchiveRole，并授予RDS审计中心使用该角色访问其他云产品中的资源。

4. 根据页面提示，完成AliyunServiceRoleForSLSAudit角色授权。

   完成此操作后，阿里云自动为您创建一个服务关联角色AliyunServiceRoleForSLSAuditRDS，并授予RDS审计中心使用该角色采集RDS审计日志。更多信息，请参见管理服务关联角色AliyunServiceRoleForSLSAudit。

> **注意** RDS审计中心和日志审计服务都需使用服务关联角色AliyunServiceRoleForSLSAudit进行日志采集，如果您已在日志审计服务中执行此操作，则无需在RAN审计中心中再次执行。

手动开启采集功能

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**RDS审计中心**。
3. 在**数据接入**页签中，单击目标RDS实例对应的**开启**。
4. 在**选择投递目标**对话框中，选择目标Project和Logstore，然后单击**确认**。

   开启采集功能后，日志服务开始采集目标RDS实例的审计日志。

设置自动化采集

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**RDS审计中心**。
3. 在**数据接入**页签中，单击**自动化采集配置**。
4. 单击图标。
5. 设置采集条件。

   您可以使用阿里云账号ID、地域、实例ID、实例名、DB类型、DB版本号、标签等属性设置采集条件。

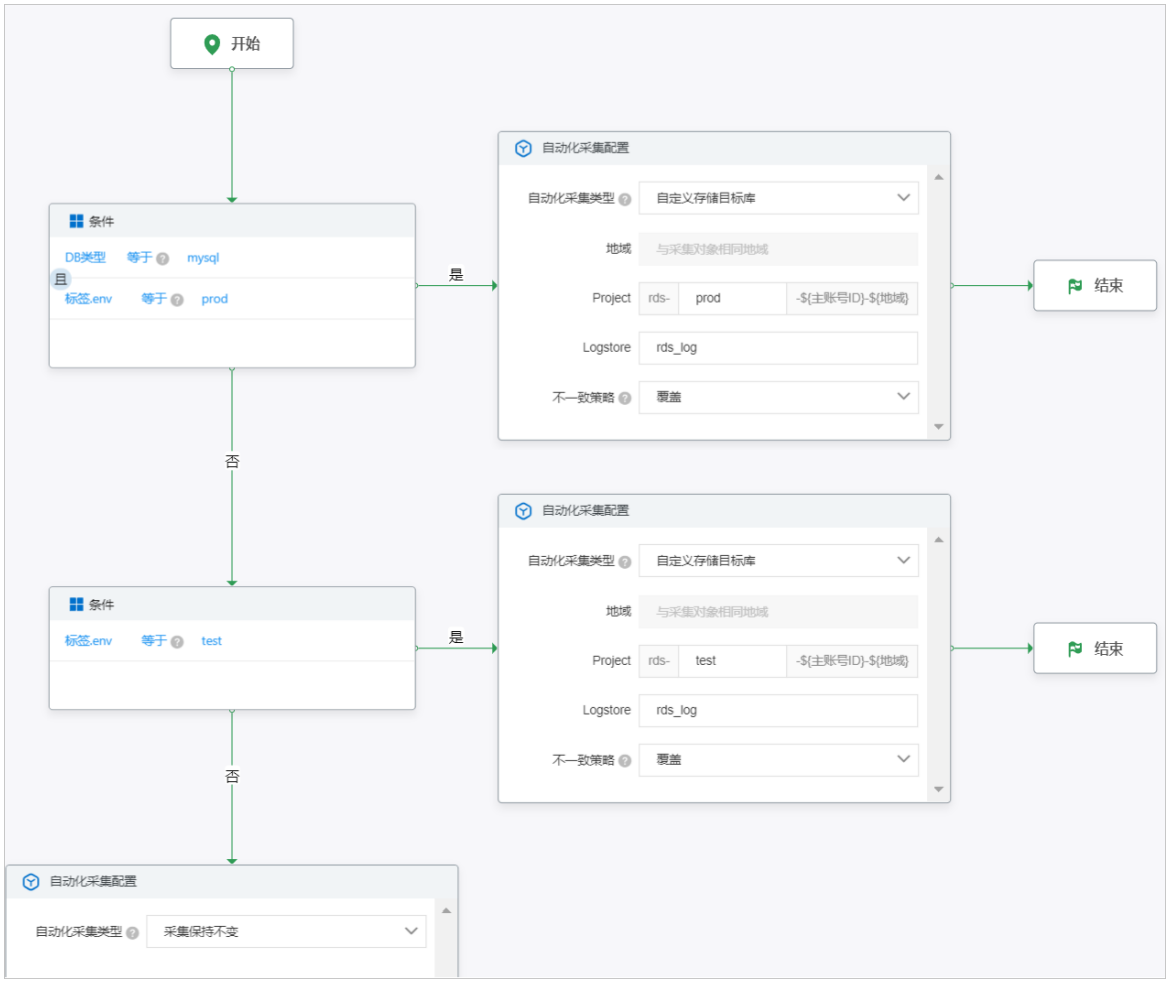
   标准模式下各个条件之间为且关系。高级模式下，您可以灵活组合与嵌套条件。
6. 设置自动化采集配置。

参数	说明
自动化采集类型	选择自动化采集类型，具体说明如下： ○ **自定义存储目标库**：自动采集符合条件的RDS实例的审计日志到目标Logstore中。 如果存储目标库（Project、Logstore）不存在，会自动创建对应的日志库目标。 ○ **采集保持不变**：选择**采集保持不变**时，无需设置**地域**、**Project**、**Logstore**和**不一致策略**参数。 ■ 符合条件的RDS实例，如果未开启采集，则不会自动开启。 ■ 符合条件的RDS实例，如果已开启采集，则不会改变其目标日志库。
地域	系统自动默认选择目标RDS实例所在地域，无法修改。
Project	在RDS实例所在地域，自动创建一个名为`rds-xxx-${主账号ID}-${地域}`的Project。例如rds-test-12345674523-cn-hangzhou。
Logstore	在名为`rds-xxx-${主账号ID}-${地域}`的Project下，自动创建一个名为`rds_log`的Logstore。

参数	说明
不一致策略	当此次设置的存储目标库与当前已生效的存储目标库不一致时，系统将根据如下选择进行判断，具体说明如下： ○ **忽略**：以当前已生效的存储目标库为准。 ○ **覆盖**：以此次设置的存储目标库为准。

例如：

- 绑定 `env==prod` 标签的RDS MySQL实例的审计日志投递到名为 `rds-prod-${主账号ID}-${地域}` 的Project下的 `rds_log` Logstore中。
- 绑定 `env==test` 标签的RDS MySQL实例的审计日志投递到名为 `rds-test-${主账号ID}-${地域}` 的Project下的 `rds_log` Logstore中。
- 其他RDS实例的审计日志的存储目标库以当前已生效的存储目标库为准。



7. 单击图标。
8. 在页面右上角，单击**保存**。

相关操作

操作	说明
管理RDS实例	您可以在**数据接入**页签的**RDS实例**区域，查看您阿里云账号所拥有的所有RDS实例、RDS所在地域、RDS实例的采集状态等。
关闭采集功能	您可以在**数据接入**页签的**RDS实例**区域，单击目标RDS实例对应的**关闭**，关闭采集功能。
修改存储目标库（Project、Logstore）	您可以在**数据接入**页签的**RDS实例**区域，单击目标RDS实例对应的**变更**，修改该RDS实例的审计日志所要投递的Project和Logstore。
管理存储目标库（Project、Logstore）	您可以在**数据接入**页签的**存储目标库**区域，查看用于存储RDS审计日志的Logstore、修改目标logstore中数据的保存时长。

后续步骤

采集到RDS审计日志后，您可以执行如下操作：

- 在**查询**页签中，选择目标Logstore，执行查询和分析操作。更多信息，请参见查询和分析日志。
- 在**审计运营中心**页签、**审计安全中心**页签或**审计性能中心**页签中，选择目标Logstore，查看对应的仪表盘。

5.4. 设置告警

RDS审计中心已内置告警规则，您开启对应的告警实例即可实时监控RDS审计中心。本文介绍设置告警的相关操作。

前提条件

已完成数据接入配置。具体操作，请参见开启日志采集功能。

背景信息

RDS审计中心中已内置告警规则、SLS审计内置告警策略、SLS审计内置行动策略、SLS审计内置用户组和SLS审计内置内容模板。它们之间的关联如下：

- 通过告警规则指定SLS审计内置告警策略。

  > **说明** RDS审计中心中的告警规则已绑定SLS审计内置告警策略，无法解绑和更换绑定。

- 通过SLS审计内置告警策略指定SLS审计内置行动策略。
- 通过SLS审计内置行动策略指定SLS审计内置用户组和SLS审计内置内容模板。

您可以直接使用内置的告警资源，也可以自定义告警资源，本文以使用内置告警资源为例。自定义告警资源的操作，请参见日志审计服务。

步骤一：创建用户

1. 登录日志服务控制台。
2. 在**日志应用**区域，单击**RDS审计中心**。
3. 在左侧导航栏中，单击**告警**。
4. 在**告警**页签中，选择**告警管理 > 用户管理**。
5. 创建用户。

具体操作，请参见创建用户。

步骤二：将用户添加到SLS审计内置用户组

1. 在**告警**页签中，选择**告警管理 > 用户组管理**
2. 在用户组列表中，单击**SLS审计内置用户组**对应的**修改**。
3. 在**修改用户组**中，将已创建的用户从**待添加成员**区域添加到**已添加成员**区域，然后单击**确认**。

步骤三：开启告警实例

1. 在**告警**页签中，单击**规则/事务**。
2. 在告警规则列表中，找到目标告警规则，单击**开启**。

   开启告警实例后，日志服务开始实时监控RDS审计中心。如果您需要开启多个告警实例，可单击**添加**。

   告警规则的参数说明请参见RDS安全。

相关操作

操作	说明
设置白名单	针对特定告警规则，如果您希望某些用户（或者实例ID、IP地址）进行操作时不触发告警，可将其设置为白名单。 不同告警规则对应的白名单配置不同。更多信息，请参见RDS安全。
关闭告警实例	关闭告警实例，告警规则不会再触发告警，**状态**变更为**未开启**。 该操作不会删除规则参数中已设置的信息。需要再次监控时，无需重新设置规则参数。
临时关闭告警实例	临时关闭告警实例后，在指定时间内不再触发告警。
恢复告警实例	处于临时关闭状态的监控实例，可随时恢复告警。
删除告警实例	删除告警实例，**状态**变更为**未创建**。 该操作会删除规则参数中已设置的信息（例如阿里云账号）。需要再次监控时，需要重新设置规则参数。
升级告警实例	当日志服务对告警规则进行较大的功能升级或升级后需要您额外配置时，系统会提示您升级告警规则。一般情况下，系统会自动完成升级。
手动初始化告警	如果误删除告警初始化产生的资产或者发生首次初始化告警资产失败的情况，可通过此操作强制重新初始化告警相关内容。

5.5. 日志字段详情

本文介绍RDS SQL审计日志字段详情。

字段名称	说明
__topic__	日志主题，固定为rds_audit_log。

字段名称	说明
instance_id	RDS实例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RDS实例的客户端IP地址。
latency	执行SQL操作后，多久返回结果，单位：微秒。
origin_time	执行操作的时间点。
return_rows	返回的行数。
sql	执行的SQL语句。
thread_id	线程ID。
user	执行操作的用户名。
update_rows	更新的行数。