日志审计（原生版）

用户指南

天翼云科技有限公司

目录

1 产品介绍

1.1 产品定义

日志审计（原生版）（LAS，Log Audit Service）通过实时不间断采集设备、主机、操作系统、数据库以及应用系统产生的海量日志信息，进行集中化存储，为您提供安全存储、检索、审计、告警、报表等能力，帮助您满足等保合规要求。

产品功能

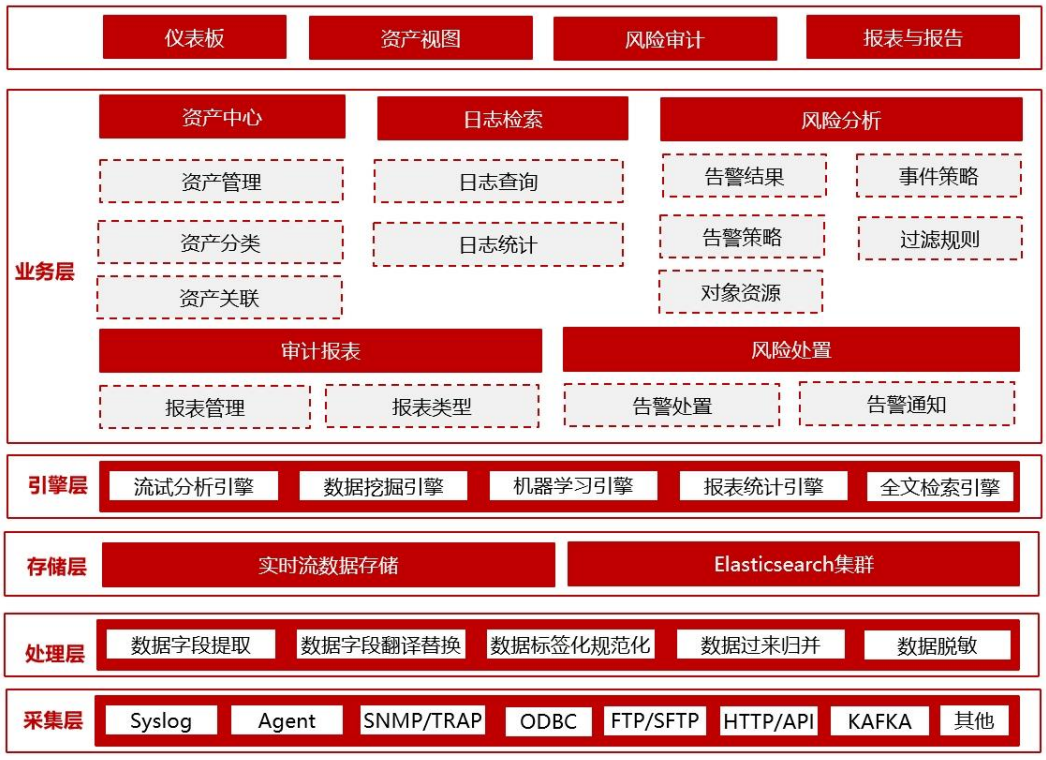
天翼云日志审计（原生版）系统具备资产管理、日志检索、日志审计、多维报表等功能。

- 资产集中管理：提供集中化的统一管理平台，将所有的日志信息收集到平台中，进行信息资产的统一日志管理。
- 高速日志检索：基于海量数据的高速检索能力，可以实现多重条件组合的快速检索和精确定位。
- 实时日志审计报警：对归并处理的日志进行实时动态分析，及时发现网络非法访问、数据违规操作、系统进程异常、设备故障等高危安全事件通过邮件、短信等方式进行报警。
- 丰富多维日志报表：丰富合规报表预设，支持全方位自定义报表导出，实现数据库系统、数据库服务器、网络设备的多维立体审计。

产品架构

天翼云日志审计（原生版）系统产品架构包含数据采集层、处理层、存储层、引擎层、业务层、可视化。

- 采集层：提供开放式的信息采集接口，实现对用户环境内各类 IT 资产以及所采用的各厂商安全产品或安全系统进行主动或被动的日志采集。
- 处理层：实现对采集到的数据做统一规范化，对数据进行关键信息提取，标签化分类，过滤，归并等数据 ETL 操作，为后续的数据分析做准备。
- 存储层：实现海量安全大数据的分布式存储，提供结构化数据和非结构化数据的存储能力，并为上层的数据分析应用提供高效的数据库功能支撑。
- 引擎层：综合数据处理分析的能力提供层，提供由大数据技术和架构支撑的快速检索和数据关联发掘功能。是支撑上层数据呈现和分析结果输出的计算引擎层，提供丰富的大数据统计、关联分析、数据挖掘以及态势分析能力，是系统的分析处理的核心。该层提供了基础数据处理引擎，包括流式计算引擎、复杂事件处理引擎、全文检索引擎、关联分析引擎等。
- 业务层：实现用户基于平台的标准化数据，依托平台报表工具，日志检索工具，分析引擎，实现用户自身业务相关的安全管理以及数据分析，监控，处置，保障业务的安全稳定。
- 可视化：实现对平台的数据处理，数据分析，报表分析，处置结果等通过图表可视化的方式呈现。



1.2 产品优势

- **一站式审计**

  具备日志采集范围广、检索速度快、审计分析维度深、数据展示视图全、风险报表模板多、响应处置效率高等一站式日志审计功能。

  - 强大的关联分析能力，可以让安全运维人员从几十分钟甚至小时级别的日志审计溯源耗时缩小到分钟级别，甚至秒级，大大提升安全审计效率。
  - 搜索引擎是针对日志所设计的架构，比通用的 ES 搜索引擎更安全，效率更高，稳定性更好，还可节省一半硬件资源。

- **满足等保合规**

  符合国家等级保护制度中对于安全审计的技术要求，具备完整的日志审计分析报告，满足用户多样化报表和监管要求。

  - 通过统一数据采集，统一数据备份，满足企业合规要求，如中国电信《中国电信云运〔2021〕58 号》。
  - 满足《网络安全法》对日志审计要求，满足等级保护二级，三级对日志的相关要求。

- **便捷部署**

  为用户提供开箱即用的自动化配置、更新和管理功能，减少了人工干预和操作的需要，降低了用户在部署和配置方面的难度。

  - 通过自动化配置、更新和管理功能，用户可以快速设置和调整系统，无需手动进行繁琐的配置过程。这大大简化了系统的部署和配置过程，并减少了人为错误的可能性。
  - 确保部署流程简单高效，减少人工干预，提高管理工作效率，降低运维工作负担，让安全运维部署工作效益上升一个台阶。

- **弹性降低成本**

为用户提供按需付费的模式，可以节省昂贵的硬件设备购买和维护成本，同时具备更高的灵活性和可扩展性。

- 用户可以根据实际需求选择所需的功能和服务。避免了一次性投入大量资金购买和维护硬件设备的需求，用户可以更加灵活地根据自身业务发展和预算情况进行调整。
- 根据系统的需求变化，用户可以随时添加或调整相应功能模块，以满足不断变化的业务需求。同时，由于部署在云端具有高可用性和容错性，即使出现故障或意外中断，也可以快速恢复并继续提供服务。

1.3 功能特性

日志采集

全面采集网络行为及数据库操作日志、服务器主机及网络设备日志、常规应用及业务系统日志，并对日志进行统一归并处理，便于后续分析。

采集是日志审计（原生版）系统的重要功能模块，它承载了日志或事件采集标准化、过滤、归并功能，是系统进行分析的第一步，用户通过指定需要采集的目标、相关采集参数（Syslog、SNMPTrap 等被动方式无需指定）、相关的过滤策略和归并策略等创建日志采集器，以收集相关设备或系统的日志。

不同的系统或设备所产生的日志格式是不尽相同的，这给分析和统计带了巨大的麻烦，所以在日志审计（原生版）系统中内置了众多的标准化脚本以处理这种情形；即便对于某些特殊的设备，如某个系统的新型号，您没有发现相关的解析脚本，日志审计（原生版）系统也提供了相应的定制方法以解决这些问题。

日志检索

基于海量数据的高速检索能力，可以实现多重条件组合的快速检索和精确定位，并且支持事件的交互式检索分析快速生成图表直观呈现分析内容，并能直接保存成仪表板展示。

- 亿级（TB）原始日志查询耗时低于 1 秒；

- 支持简单易用的日志查询普通模式，根据系统预置的查询条件，根据用户需求查询对应的日志，并且支持查询条件的保存，供后续快捷使用；
- 支持更加精确的高级模式查询，根据页面的指导提示，通过组合查询表达式完成精确查询。

审计分析

对实时动态分析的日志进行归并处理和监测，可及时发现高危安全事件，如用户违规行为、数据泄露、攻击利用和主机通信异常。

关联分析策略是系统中的核心功能之一，主要关注各类日志之间的逻辑关联关系。它不仅支持以预定义规则进行事件关联，还能基于状态、时序和归并等方式发现关联。

系统可审计以下不同类型日志或事件（需结合相关设备，如防火墙和 IPS 等）：网络攻击、有害代码、漏洞、用户访问存取、系统运行、设备故障、配置状态、网络连接和数据库操作等。

关联事件的结果将在关联事件中显示，如果符合关联策略，将以告警形式在实时监控模块呈现给用户。用户可以对告警进行处理，以确保及时应对潜在的安全问题。

数据展示

提供可视化的总体概览，通过仪表板可以直观地展示日志数据的统计和分析结果，帮助用户快速了解系统的运行状态和问题。用户可以自定义展示安全事件以及各类审计分析信息，提供实时的审计分析可视化界面。

全局监视仪表板，可展示不同设备类型、不同安全区域的实时日志流曲线、统计图，以及网络整体运行态势、待处理告警信息等。

风险报表

用户可以根据自己的需求，自由选择需要包含在报表中的指标和数据，以便更好地满足特定的业务需求。系统还提供了对预置报表模板的选择和预览功能。用户可以浏览系统中已经存在的报表模板，并选择其中的一个进行生产。这有助于用户快速生成符合自己需求的报表，节省了手动设计和生成报表的时间和工作量。

在报表中，系统以柱状图、曲线图和饼状图的方式统计安全报警和原始日志情况。这种可视化的报表展示方式使得数据更加直观易懂，用户可以更轻松地分析和理解报表中的信息。报表格式方面，系统支持 PDF、Word 等文件格式的导出。用户可以根据需要选择合适的文件格式，以便将报表分享给其他人或保存到本地进行进一步分析。

此外，系统还支持周期性生成报表并通过邮件推送给用户。用户可以设置报表的生成周期，例如每天、每周或每月定期生成报表，并通过电子邮件将其发送给用户。这样，用户可以及时获得最新的安全报警和日志信息，以便及时采取相应的措施。

响应处置

对实时审计产生的告警，系统还支持通过配置规则来指定场景告警进行响应通知。这意味着用户可以根据自身需求，将不同类型的告警划分为不同的场景，并设置相应的规则和通知方式。在邮件通知方面，系统提供了丰富的内容配置选项。用户可以根据需要填充事件相关信息，以便在通知邮件中提供更详细的上下文信息。此外，还可以配置邮件通知的时段，以确保及时通知用户。系统能够自动实时地发送告警通知给用户，使用户能够及时了解安全报警和日志异常情况。用户可以通过查看告警通知的内容，迅速判断是否存在潜在的安全问题，并采取相应的措施进行处理。

通过以上功能的支持，系统能够帮助用户实现对实时审计中的告警进行快速、准确、有效的响应和处理。用户的响应时间得到缩短，安全问题能够得到及时解决，从而提升了系统的安全性和可靠性。

1.4 应用场景

场景一：响应合规场景

采用日志审计监测、记录和存储网络运行状态和安全事件等信息，实现对系统的全面监控和细致记录，配合多种审计策略，快速定位溯源，全面提升系统服务水平以及网络安全管理水平，满足网络安全法规及等级保护的相关要求。

产品优势能力：

- 产品具备海量日志存储能力，并可以长时间地保存大量日志信息，同时采用了多种技术手段，实现高效地日志数据处理和存储，降低性能负担，确保用户在实现合规性的同时，仍能维持系统的服务水平。
- 通过深度分析安全设备的日志信息，可以及时检测潜在的安全威胁，并结合溯源分析追踪攻击者的行为路径和攻击手法，更好地了解攻击者的意图和方法，帮助快速发现并阻止潜在的攻击，减少安全事件造成的损失。

场景二：运维分析场景

针对中大型企业设备多，系统多，难以统一监管问题，采用日志审计将所有设备、用户行为日志统一监管，贯穿从边界到核心资产的全流程运维监控，以及扩展对关键数据等资产的保护。

产品优势能力：

- 提供实时流的日志分析监控，通过邮件方式及时通知用户，提高运维的响应及时率。
- 仪表盘灵活查看不同设备的整体运行情况，通过定时任务，统计一天到一周、月、季度的业务数据运维情况。
- 借助统计报表掌握业务趋势，通过接口调用统计为扩容、性能问题排查提供参考信息。

场景三：审计分析场景

基于大数据架构的日志审计系统，针对各类系统的日志进行集中采集、管理、存储、统计，分析的系统，实现高效统一管理资产日志并提供实时检索，可视化交互分析，聚合分析，实时告警，报表等功能。

产品优势能力：

- 日志统一采集，集中管理，挖掘数据价值，解决日志散乱，记录不集中，导致对日志的利用较为单一，没有更深层次的数据挖掘和分析。
- 支持实时的字段检索，模糊检索查询，支持交互式选择事件任意属性字段，可以该字段为条件对事件进行统计分析，借助统计报表掌握业务趋势。

1.5 使用限制

在使用日志审计过程中，您需要了解日志审计（原生版）系统的使用限制。

数据接入前置条件

- 数据接入前，请务必在平台资产管理模块配置好数据采集的对象，尤其是 ip 地址信息和设备大类和小类信息。这将影响到数据的接收和数据的处理模板；
- 被采集对象的设备与平台网络可达；
- Syslog 接收端口监听正常，平台服务运行正常；
- 在解析接入规则模块能找到被采集对象的设备类型解析模板。

告警产生前置条件

- 日志数据接入正常；
- 采集接入数据能找到对应设备解析模板，正常解析出关键字段信息；
- 告警规则配置逻辑正确；

- 告警规则配置的规则匹配字段信息有值且正确。

支持的设备类型

支持主机设备、网络设备、安全设备、应用系统、虚拟机、存储设备。

支持的主机设备型号

设备子类	设备型号
windows 系列	Win2000、win2003、xp 等
unix&linux	Linux 系列、solaris8、solaris9 等
Pc 服务器	小型机

支持网络设备型号

设备子类	设备型号
交换机	Extreme、Juniper、神舟数码等
交换机/思科	100 系列、200E 系列、200 系列、300 系列、500 系列、90 系列、Catalyst2918 系列、Catalyst2960-CX 系列等
交换机/华为	12800 系列、16800 系列、2350&5300&6300 系列等
交换机/H3C	S1000 系列、S10500 系列等
交换机/中兴	1000 系列、2900E 系列、2950 系列等
路由器	Extreme、Juniper、神舟数码等
负载均衡设备器	F5、信安世纪、array

支持的区域

区域	一类节点	二类节点
华东地区	杭州 2/杭州 7/合肥 2/华东 1/九江/南昌 5/南京 3/南京 4/南京 5/上海 15/上海 36/上海 7/芜湖 2/芜湖 4	杭州/南昌/上海 4/苏州/芜湖

区域	一类节点	二类节点
华南地区	长沙 3/长沙 42/郴州 2/佛山 3/福州 25/广州 6/海口 2/华南 2/南宁 2/南宁 23/武汉 3/武汉 4/武汉 41/厦门 3	长沙 2/福州 1/广州 4/海口/南宁/深圳/武汉 2
西北地区	兰州 2/庆阳 2/乌鲁木齐 27/乌鲁木齐 4/乌鲁木齐 7/西安 3/西安 4/西安 5/西安 7/西宁 2/中卫 2/中卫 5	兰州/乌鲁木齐/西安 2/西宁/中卫
西南地区	成都 4/重庆 2/贵州 3/昆明 2/拉萨 3/西南 1/西南 2-贵州	成都 3/重庆/贵州 1/昆明
北方地区	北京 5/华北 2/呼和浩特 3/晋中/辽阳 1/内蒙 6/青岛 20/沈阳 8/石家庄 20/太原 4/郑州 5	北京 2/长春/哈尔滨/华北/内蒙 3/青岛/石家庄/太原/郑州

1.6 术语解释

日志采集

实现第三方安全设备、网络设备、windows/linux 主机日志、web 服务器日志、虚拟化平台日志以及自定义等日志采集。

日志存储

实现原始日志、范式化日志的存储，可定义存储周期。

日志检索

实现全文、key-value、括弧、正则、模糊等检索方式；支持保存检索、从已保存的检索导入见多条件。

可视化统计

实现趋势图、折线图、柱状图、饼图、表格等统计项展示。

事件告警

自定义事件规则，可按照日志、字段布尔逻辑关系等方式自定义规则，实现时间的查询、查询结果统计以及统计结果的展示。

2 计费说明

2.1 计费方式

计费模式

日志审计（原生版）支持**包年/包月**（预付费）计费方式，购买时长越久越便宜。

计费项

日志审计（原生版）根据**资产规格、数据盘扩容**量进行计费。

计费项	说明
资产规格	按购买资产规格和时长计费，包含 5/10/15/20/50/100/200/500，共 8 种规格类型。 说明： 资产规格表示日志审计（原生版）可以接入设备资产的数量。
数据盘扩容	按存储扩容大小和时长计费。 说明： **仅“一类节点”区域的实例支持数据盘扩容。**日志审计（原生版）支持的区域请参见“支持的区域。”

产品价格-资产规格

注意：

- 仅“一类节点”区域的实例支持标准版。
- 仅“二类节点”区域的实例支持基础版。如下基础版价格仅为日志审计（原生版）实例的价格，购买时实际结算会包含云主机的价格；根据您所选择的云主机规格，云主机价格有所不同，云主机规格价格可参考云主机价格。
- 针对一次性包年付费，日志审计（原生版）的优惠政策为：1 年 8.5 折、2 年 7.5 折、3、4、5 年 6.5 折。

版本	资产规格	标准价格（元/月）	1 年付价格（元/年）	2 年付价格（元/2 年）	3 年付价格（元/3 年）
标准版	5 资产	1,600	16,320	28,800	37,440
	10 资产	1,750	17,850	31,500	40,950
	15 资产	2,000	20,400	36,000	46,800
	20 资产	3,400	34,680	61,200	79,560
	50 资产	4,600	46,920	82,800	107,640
	100 资产	6,100	62,200	109,800	142,740
	200 资产	9,100	92,820	163,800	212,940
	500 资产	18,100	184,620	325,800	423,540
基础版	5 资产	1,000	10,200	18,000	23,400
	10 资产	1,200	12,240	21,600	28,080
	15 资产	1,400	14,280	25,200	32,760
	20 资产	1,600	16,320	28,800	37,440
	50 资产	3,200	32,650	57,600	74,880
	100 资产	4,265	43,503	76,770	99,801
	200 资产	6,395	65,229	115,110	149,643
	500 资产	12,785	130,407	230,130	299,169

产品价格-数据盘扩容

说明：

- 仅“一类节点”区域的实例支持数据盘扩容。日志审计（原生版）支持的区域请参见“支持的区域”。
- 针对一次性包年付费，日志审计（原生版）的优惠政策为：1 年包年 8.5 折、2 年包年 7.5 折、3、4、5 年包年 6.5 折。

计费项	标准价格（元/月/TB）	1 年付价格（元/年/TB）	2 年付价格（元/2 年/TB）	3 年付价格（元/3 年/TB）
数据盘扩容	500	5,100	9,000	11,700

2.2 购买实例

2.2.1 规格说明

日志审计（原生版）为您提供 5、10、15、20、50、100、200、500 资产数八种规格，您可以根据自身业务的每秒事件指标（Evert Per Second-EPS）选择相应的规格。

资产规格	最高支持 EPS 值	CPU	内存	系统盘	数据盘
5 个	50	4 核	16GB	40GB	256GB
10 个	100	4 核	16GB	40GB	512GB
15 个	150	4 核	16GB	40GB	1TB
20 个	200	8 核	32GB	40GB	1TB
50 个	500	8 核	32GB	40GB	2TB
100 个	800	16 核	32GB	40GB	4TB
200 个	1000	16 核	64GB	40GB	6TB
500 个	2000	16 核	64GB	40GB	10TB

2.2.2 支持的区域

根据所选购买区域，购买步骤略有不同，日志审计（原生版）支持的区域请参见“产品介绍 > 使用限制 > 支持的区域”。

2.2.3 前提条件

购买日志审计（原生版）前，您需要注册天翼云账号并完成实名认证。

2.2.4 购买步骤（一类节点）

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在服务列表选择“安全 > 日志审计（原生版）”，进入日志审计（原生版）实例列表界面。
4. 在界面右上角，单击“立即购买”，选择地区、可用区域、资产规格。

参数	参数说明
地区/可用区域	选择日志审计（原生版）需要部署的区域和可用区，实际可选择地区请根据购买页选择。
CPU 分类	根据您需要部署日志审计（原生版）主机的 CPU 规格选择。
实例名称	输入您的实例名称。
版本及资产规格	选择日志审计（原生版）的版本及规格，资产规格请您根据自身业务的每秒事件指标（Evert Per Second-EPS）进行选择，具体可参考“规格说明”。
企业项目	选择实例所属的企业项目。 企业项目通过将云资源、带有权限的用户组绑定到一起，用户使用企业项目内云资源时，权限将受用户组的权限限制。
虚拟私有云	选择日志审计（原生版）所属的虚拟私有云，请您确保你需要进行审计的设备和日志审计处于同一 VPC 下，若不在需确保和日志审计所在的 VPC 网络互通。
子网	选择日志审计（原生版）所属的子网。
数据盘扩容	选择您需要增加的存储空间，可选 0-25TB。
购买时长	选择日志审计（原生版）购买的时长。 可选：1-3 个月、6 个月、1 年、2 年、3 年、4 年、5 年。
到期自动续费	根据您业务要求勾选是否自动续费。

5. 确认参数配置无误后，阅读并同意相关协议，单击“提交订单”。

6. 在订单详情页确认内容是否正确，确认无误后单击“立即支付”，在后续跳转页中完成支付即成功购买日志审计（原生版）服务。

2.2.5 购买步骤（二类节点）

购买实例

1. 登录天翼云控制中心。
2. 在控制中心页面顶部选择区域。
3. 在服务列表选择“安全 > 日志审计（原生版）”，进入日志审计（原生版）实例列表界面。
4. 在界面右上角，单击“立即购买”，进入订购页面。
5. 配置基础信息和资产规格。

参数	参数说明
地区/可用区域	选择日志审计（原生版）需要部署的区域和可用区，实际可选择地区请根据购买页选择。
CPU 分类	根据您需要部署日志审计（原生版）主机的 CPU 规格选择。
实例名称	输入您的实例名称。
版本及资产规格	选择日志审计（原生版）的版本及规格，资产规格请您根据自身业务的每秒事件指标（Evert Per Second-EPS）进行选择，具体可参考“规格说明”。

6. 选择选择配套的弹性云主机规格。具体云主机规格需求可参考“规格说明”。
   - 云主机规格默认选择最低规格，您可在下拉框中选择主机规格或者输入规格名称进行搜索（支持模糊搜索）。
   - 系统盘和数据盘默认选择最低规格，您可根据业务实际需求进行适量提升。

说明：

- 在选定资产规格的情况下，若您的 EPS 值高于当前规格支持的最高 EPS 值，请您根据实际业务需求提升主机的规格。
- 若您需要将旧合作产品的日志审迁移至日志审计（原生版）服务，并且需要将数据也同步迁移，选购云主机时内存至少选择 64G。

7. 配置日志审计（原生版）实例的网络信息。

参数	参数说明
虚拟私有云	选择日志审计（原生版）所属的虚拟私有云，请您确保你需要进行审计的设备和日志审计处于同一 VPC 下，若不在需确保和日志审计所在的 VPC 网络互通。
子网	选择日志审计（原生版）所属的子网。
安全组	选择日志审计（原生版）所属的安全组。 注意： 安全组规则需要放通如下端口，请您在选择安全组的时候注意是否已放通该端口。 - TCP 协议“10443”的入方向端口。 - UDP 协议“514”的入方向端口。
弹性 IP	为日志审计（原生版）实例绑定弹性 IP。

8. 选择“购买时长”。支持开启“到期自动续费”，当服务到期前，系统会自动按照默认的续订周期生成续费订单并进行续费，无须用户手动续费。

   若您未勾选“到期自动续费”，在日志审计（原生版）到期后需要手动续费，且需要同步去云主机服务页面续费配套的弹性云主机。

9. 确认参数配置无误后，阅读并同意相关协议，单击“提交订单”。

10. 在订单详情页确认内容是否正确，确认无误后单击“立即支付”，在后续跳转页中完成支付即成功购买日志审计（原生版）服务。

    日志审计（原生版）实例在您购买后会自动启用，若您的实例未正常启用，请参考“手动启用实例”进行启用。

手动启用实例

1. 登录日志审计（原生版）控制台。
2. 选择需要待启动的实例，单击“启用”。
3. 在弹出的对话框中填写相关参数。

参数	参数说明
实例 ID	创建实例时自动生成的实例 ID
弹性 IP	输入在购买弹性云主机的过程中，绑定的弹性 IP。
机器码	在 Web 浏览器中输入 https://<弹性 IP>:10443 获取机器码。机器码获取请参见“机器码获取示例”。
用户名	输入本台日志审计服务器的管理员账户名。长度限制：2-16 位，仅可使用数字、字母、“_”和“-”。
密码	输入本台日志审计服务器的管理员密码。密码长度限制：8-16 位，密码必须含有“小写字母”、“大写字母”、“数字”、“特殊符号”中的任意三种，特殊字符支持：`~!@#$^&*()。
确认密码	二次确认本台日志审计服务器的管理员密码。密码长度限制：8-16 位，密码必须含有“小写字母”、“大写字母”、“数字”、“特殊符号”中的任意三种，特殊字符支持：`~!@#$^&*()。

4. 输入完成后，单击“启用”即可完成实例启动。

机器码获取示例

在 Web 浏览器中输入 https://<弹性 IP>:10443，进入下图页面，复制红框中的内容即可获取机器码。

2.3 续订与退订

注意：

对于“二类节点”区域的实例【日志审计（原生版）支持的区域请参见“支持的区域”】，如需退订/手动续费，还需在对应云主机服务页面退订/手动续费开通服务时同步购买的云主机服务。

续费操作步骤

1. 登录管理控制台。
2. 选择“安全 > 日志审计（原生版）”，进入日志审计实例管理页面。
3. 单击待续费的实例，“操作”列的“更多 > 续费”，进入“续费”配置页面。
4. 根据需要选择续费时长。
5. 单击“去支付”，在支付页面完成付款。

退订操作步骤

1. 登录管理控制台。

2. 选择“安全 > 日志审计（原生版）”，进入日志审计实例管理页面。
3. 选择待退订的实例，单击所在行“操作”列的“更多 > 退订”，弹出的退订实例对话框。
4. 确认实例信息无误后，单击“确定”。
5. 在退订资源页面完成退订。

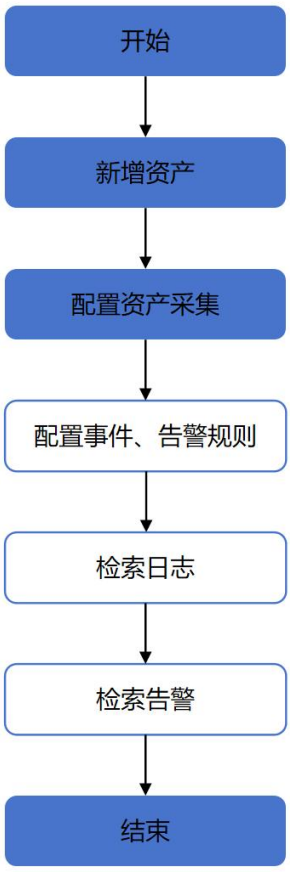
3 快速入门

3.1 背景信息

本文档将以部署一台日志审计（原生版）为场景，帮助您快速入门掌握如何创建和使用日志审计（原生版）。

主要包括：新增资产、配置事件规则、配置告警规则、检索日志、配置检索告警五方面。

注意：需订购日志审计（原生版）后，进入控制台查看实例的状态为“运行中”，点击“登陆”按钮进入日志审计（原生版）实例中使用。



3.2 新增资产

新增资产组

单击“资产”后再点击“资产管理”进入资产管理页面，单击“新增组”按钮，新增资产组。

新增资产

1.单击“资产”后再点击“资产管理”进入资产管理页面后，选择资产组，单击“新增”，新增需要采集的资产设备。也可批量导入资产，单击“导入数据”，下载的导入模板中，填写资产，将 excel 上传提交。

2.新增或导入后的资产，在资产列表中看到，并且可以对该资产进行查看、编辑、删除操作。

3.3 配置事件规则

配置接入解析规则

解析接入规则是对采集日志的分析，符合解析接入规则的日志才能被采集到日志审计平台。选择“风险分析 > 事件策略 > 解析接入规则”，配置需要采集的日志规则。其中设备类型与资产中的资产类型匹配，日志分析的格式可分为正则表达式、分隔符、key-value、json 格式，请根据实际日志格式选择。

配置事件分类规则

事件分类规则是对采集到的日志进行一个分组分类。选择“风险分析 > 事件策略 > 事件分类规则”，点击“新增”，填写分类名称、日志分组、日志等级、关键字/正则表达式、规则所属设备。其中关键字和正则表达式任意填写一个，采集到的日志将符合填写的关键字内容或者正则表达式，归纳到该分类分组中。

配置事件过滤规则

事件过滤规则是对采集到日志过滤，将不需要的日志条件填入规则。选择“风险分析 > 事件策略 > 事件过滤规则”，点击“新增规则”，选填需要过滤的条件，比如事件名称填写 Unix 用户登录成功，填写完成后，在采集过程中，将 Unix 用户登录成功的日志过滤，不采集该日志。

配置事件归并规则

事件归并规则是对采集到日志进行归并。点击“风险分析 > 事件策略 > 事件归并规则”，点击“新增规则”，填写需要归并的日志条件，比如事件名称为 rsyslogd 日志信息的日志归并在一起，不独立展示。

3.4 配置告警规则

配置告警策略

告警策略，对采集到的日志进行告警判断，符合告警策略的日志进行告警。选择“风险分析 > 告警策略”，点击“新增规则”，填写告警条件。

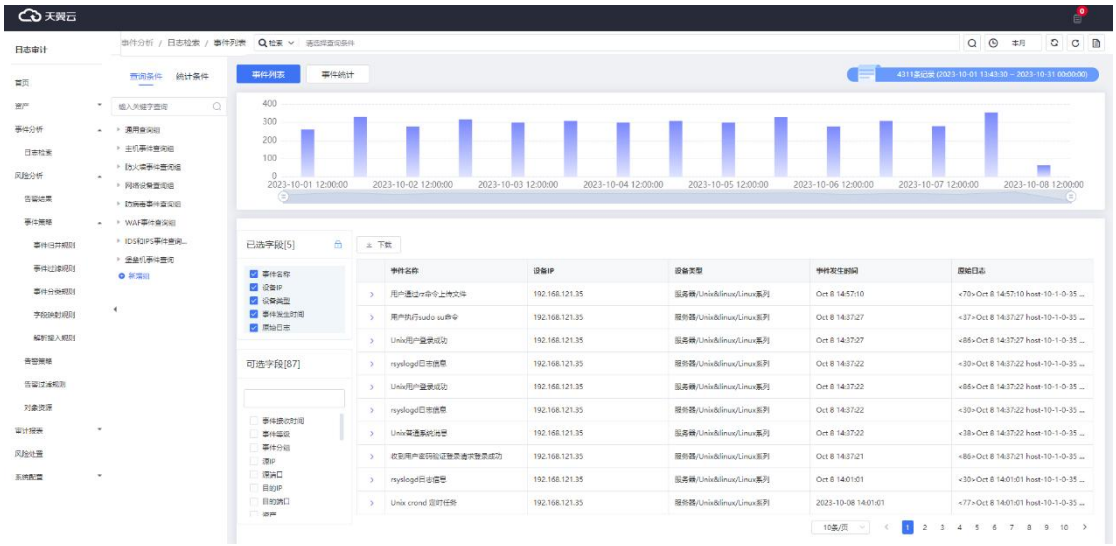
配置告警过滤规则

告警过滤规则，对符合告警规则的日志再进行一层过滤。选择“风险分析 > 告警过滤规则”，点击“新

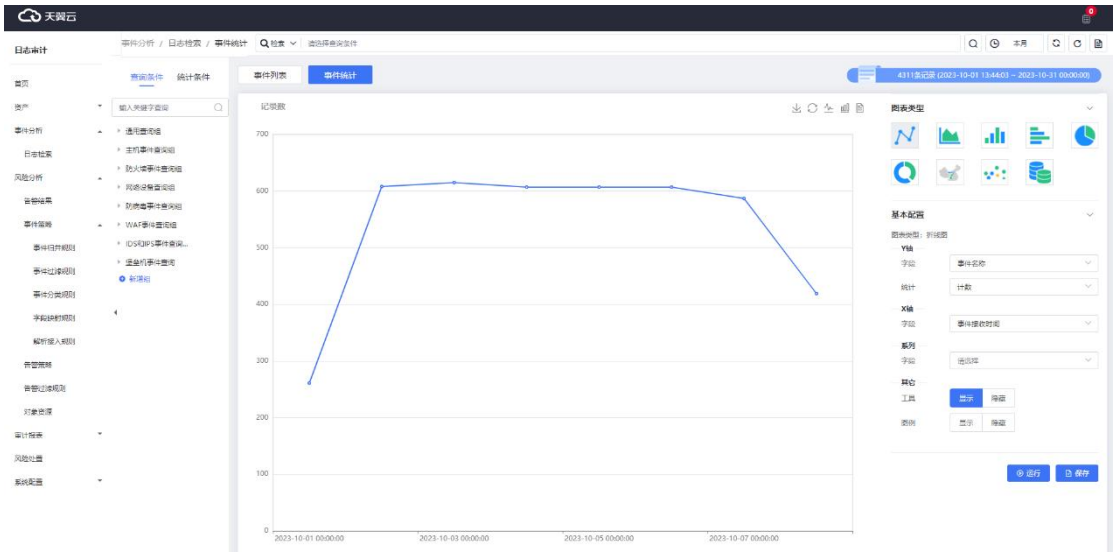
增”，填写告警过滤条件。

3.5 日志检索

通过列表/统计图方式，查看采集的日志数据。点击“事件分析”进行日志检索，系统默认展示事件列表并且显示最近 5 分钟日志。用户可在查询框中输入想要查看的日志（建议使用 csl 查询），选择查询时间，点击查询按钮，会在列表中展示查询后的日志。



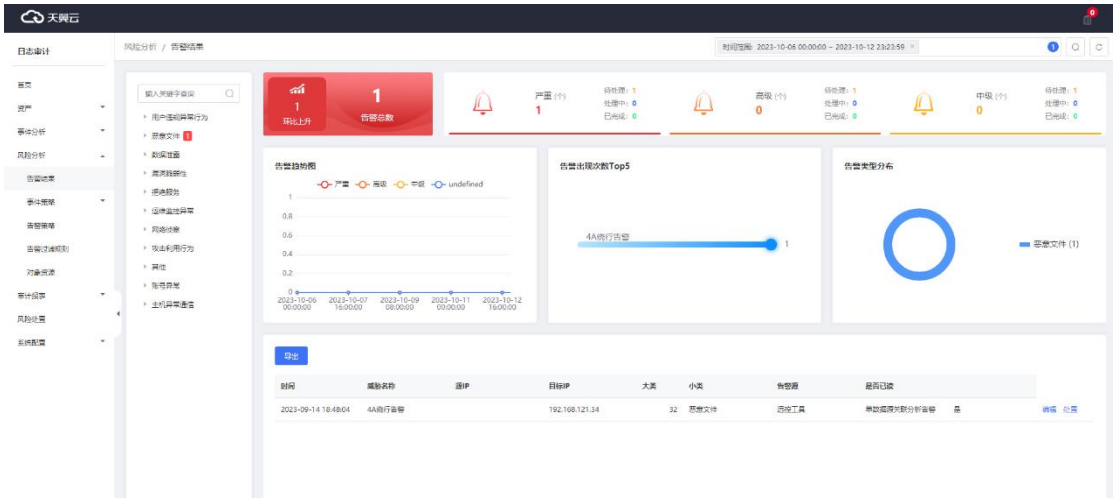
点击事件统计，同样可以根据 csl 查询日志结果，并且选择不同的图表类型，展示字段，更能直观看到日志数据情况。系统支持折线图、面积图、柱形图、横向柱形图、饼形、环状图、地图、散点图、数值图。



3.6 配置检索告警

在“风险分析”的“告警结果”页面中，查看告警结果，默认展示当天告警。展示模块分为告警等级统计数量模块、告警趋势图、告警出现次数、告警类型分布以及告警列表展示。

点击处理按钮，可对该告警进行处理，处理方式为已处理、已清除、已忽略（误报）。



3.7 升级实例版本

新版本的日志审计（原生版）对系统进行了功能优化或添加了新功能，请及时升级版本。

- 最新系统版本说明，请参见产品动态。
- 查看系统当前版本，请参见系统运维的“系统信息”模块或直接在天翼云控制台界面查看系统版本。

升级版本注意事项

- 在您开始升级一小时后，启动升级的实例还处于“升级中”的状态，请你联系天翼云支撑工程师查看实例升级情况。

- 版本升级后您可正常继续使用原有配置和存储数据，升级不影响系统原有配置和存储数据。
- 仅 2.0.0 及以上版本支持升级实例。

升级步骤

1.登录日志审计（原生版）控制台。

2.单击  图标，选择您待升级日志审计实例的资源池。

3.选择需要升级的版本，单击“版本”列的“升级”按钮。

4.在弹出的对话框中单击“确定”，即可升级实例。

4 用户指南

4.1 权限管理

天翼云提供统一身份认证（Identity and Access Management，简称 IAM）服务，是提供用户进行权限管理的基础服务，可以帮助您安全的控制云服务和资源的访问及操作权限。通过 IAM 服务定义企业项目、创建子用户，轻松实现 IAM 子用户对日志审计（原生版）资源的访问控制、权限分配等。

默认情况下，天翼云主账号拥有管理员权限，而主账号创建的 IAM 用户没有任何权限。IAM 用户需要加入用户组，并给用户组授权相应策略后，IAM 用户才能获得策略对应的权限，才可以基于被授予的权限对云服务进行操作。

日志审计（原生版）支持企业项目管理，若您需要对日志审计（原生版）资源进行分组和管理，形成逻辑隔离，您可以创建企业项目，并将资源划分至不同的企业项目中，不同的企业项目可以绑定不同的用户组，并给用户组授予日志审计（原生版）产品的权限策略（包括系统策略和自定义策略），从而实现对特定资源的授权。

> 说明：
>
> 仅“一类节点”区域的实例支持企业项目管理。

IAM 应用场景

IAM 策略主要面向同一主账号下，对不同 IAM 用户授权的场景：

- 您可以为不同操作人员或应用程序创建不同 IAM 用户，并授予 IAM 用户刚好能完成工作所需的权限，比如查看权限，进行最小粒度授权管理。
- 新创建的 IAM 用户可以使用自己的登录名和密码登录控制台，实现多用户协同操作时无需分享账号密码的安全要求。

日志审计（原生版）IAM 策略说明

天翼云为日志审计（原生版）提供如下系统策略。如果系统策略不满足授权要求，可以创建自定义策略，自定义策略是对系统策略的扩展和补充，详情请参见“创建自定义策略”。

策略名称	策略描述	类别	授权范围
las-admin	日志审计（原生版）系统管理员策略。	系统策略	全局级
las-audit	日志审计（原生版）审计管理员策略，只具备查看权限。	系统策略	全局级
las-security	日志审计（原生版）安全管理员策略。	系统策略	全局级

日志审计（原生版）权限及授权项

策略支持的操作与授权项相对应，授权项列表说明如下：

- 权限：允许或拒绝 IAM 用户某项操作。
- 授权项：授权操作对应的权限三元组，创建自定义策略时，支持可视化 JSON 视图写入权限三元组实现策略配置。
- 权限类型：授权操作对应的读写类型。

权限	授权项	权限类型（读/写）	las-admin	las-audit	las-security
实例列表	las:vm:list	读	√	√	√
实例状态检查	las:vmCheckAlive:get	读	√	√	√
实例关闭	las:vmShutdown:access	写	√	×	√
实例启动	las:vmStart:access	写	√	×	√

权限	授权项	权限类型（读/写）	las-admin	las-audit	las-security
实例升级	las:vmUpgradeVersion:access	写	√	×	√
实例切换子网	las:vmChangeSubnet:access	写	√	×	√
实例更新	las:vmUpdate:access	写	√	×	√

通过 IAM 授权使用日志审计（原生版）

详细操作请参考：

1. 创建用户组和授权
2. 创建 IAM 用户和登录
3. 创建企业项目并基于企业项目完成授权

4.2 概览

快速启用日志审计服务

本文档将以部署一台日志审计（原生版）为场景，帮助您快速入门掌握如何创建和使用日志审计（原生版）。

主要包括：新增资产、新增资产采集、开启采集配置。

步骤	任务内容	说明	相关文档
1	新增资产	您需要将您的资产添加至日志审计（原生版）控制台中，以便您的后续操作及管理。	新增资产
2	新增资产采集	您需要资产的采集方式，需要在采集管理中添加对应的采集方式。	采集配置
3	开启采集配置	配置完采集资产后，您需要在系统中开启采集配置才可以通过日志审计服务采集到服务器中的信息。	开启采集

4.3 资产管理

4.3.1 资产管理

日志审计（原生版）提供集中化的统一管理平台，将所有的需要审计的设备统一纳管入平台中，进行信息资产的统一日志管理。

在使用日志审计（原生版）之前，您先需要将资产纳管，以便服务可以进行日志管理。

新增资产

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“资产 > 资产管理”。

3.选择需要新增资产的资产组，进入资产组页面后，单击“新增资产”。

4.进入“新增”页面，填写待新增的资产内容。

参数	参数说明	取值样例
资产名称	填写您的资产名称，最大长度不超过 64 个字符。	资产示例
管理 IP	填写待纳管设备的主识别 IP，请确保 IP 真实有效。	0.0.0.0
生产厂商	（可选）输入您设备的生产厂商关键字，在下拉框中选择。	-
资产大类	在下拉框中选择待纳管资产的设备类别。	主机
资产小类	在下拉框中选择待纳管资产的具体设备类型。	服务器/其他
产品名称	（可选）输入您待纳管资产的产品名称。	-
产品版本号	（可选）输入您待纳管资产的版本号。	-
资产状态	（可选）选择您纳管资产目前的状态，可选“在线”或“离线”。	在线
所属宿主机	（可选）选择您纳管资产所属的宿主机 IP，若没有宿主机可不选择	-

参数	参数说明	取值样例
地理位置	（可选）选择您纳管资产所在地理位置，仅支持选择中国境内地区。	北京
设备联系人	（可选）填写待纳管资产的联系人信息。	-
序列号	（可选）填写待纳管资产的序列号。	-
质保期	（可选）选择待纳管资产的质保期	-
描述	（可选）填写待纳管资产的描述	-
资产标签	（可选）填写待纳管资产的标签，方便您可通过标签进行资产查询。	-
机密性	选择待纳管资产的机密等级，可选 1-10 级，默认选择 1 级。	1 级
完整性	选择待纳管资产的完整等级，可选 1-10 级，默认选择 1 级。	1 级
可用性	选择待纳管资产的可用等级，可选 1-10 级，默认选择 1 级。	1 级
资产价值	选择待纳管资产的资产价值，可选“低”、“中”、“高”，默认为“低”。	低
等保级别	选择待纳管资产的等保等级，可选 1-10 级，默认选择 1 级。	1 级
IP	与“管理 IP”一致，请确保 IP 真实有效。	0.0.0.0
IP 类型	选择纳管资产的 IP 类型，请如实选择。	公网
MAC 地址	（选填）输入待纳管资产的 MAC 接口地址。	-

注意：新增资产时，日志采集方式、资产类型和 IP 需要根据实际情况选择。

编辑资产

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“资产 > 资产管理”。

3.选择需要编辑资产所在的资产组，进入资产组页面后，单击“操作”列的“修改”。

4.在修改页选择需要修改的参数，修改完成后单击“确认”。

删除资产

注意：删除的资产无法恢复，请您谨慎操作。

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“资产 > 资产管理”。

3.选择需要删除资产所在的资产组，进入资产组页面后，单击“操作”列的“更多 > 删除”。

4.在弹出的对话框中单击“确认”，即可删除资产。

4.3.2 资产组管理

日志审计（原生版）提供集中化的统一管理平台，将所有的需要审计的设备统一纳管入平台中，进行信息资产的统一日志管理。

在使用日志审计（原生版）之前，您先需要将资产纳管，以便服务可以进行日志管理。

新增资产组

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“资产 > 资产管理”。

3.单击页面上的“新增组”按钮。

4.在弹出的对话框中填写“资产组名称”，填写完成后单击“确认”即可新增资产组。

参数	参数说明
父资产组	不可选择，系统默认填写。
资产组名称	填写您需要创建的资产组名称，最大长度不超过 64 个字符。

编辑资产组

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“资产 > 资产管理”。

3.将鼠标放在待编辑的资产组上，单击 按钮。

4.在弹出的对话框中修改资产组名称，修改完成后单击“确认”保存。

删除资产组

注意：删除资产组后，会同步删除资产组下的所有资产，请您谨慎操作。

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“资产 > 资产管理”。

3.将鼠标放在待删除的资产组上，单击 按钮。

4.在弹出的对话框中单击“确认”，完成删除操作。

4.3.3 资产类型管理

您可以在日志审计（原生版）控制台添加资产的类型，资产类型可以方便您对需采集日志的设备类型的管理。

日志审计已经预置了部分资产类型，您可以根据自己的业务需求自行添加。

新增资产类型

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“资产 > 资产类型管理”，进入“资产类型管理”页面。

3.单击页面左上角的“新增”，在弹出的对话框中填写相关参数。

参数	参数说明	取值样例
父级资产类型	系统自动选择，根据您选择添加的节点自动选择。	根节点

参数	参数说明	取值样例
资产类型名称	填写需要新增的资产类型名称，建议用中文说明	服务器
资产类型值	填写需要新增的资产类型值，建议用英文说明	Windows
描述	填写需要新增的资产类型的描述	-

添加子级

添加子级是在日志审计（原生版）已有资产类型中添加子类。

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“资产 > 资产类型管理”，进入“资产类型管理”页面。

3.选择需要添加子级的资产类型，单击“操作”列的“添加子级”，在弹出的对话框中填写相关参数。

参数	参数说明	取值样例
父级资产类型	系统自动选择，根据您选择添加的节点自动选择。	根节点
资产类型名称	填写需要新增的资产类型名称，建议用中文说明	服务器
资产类型值	填写需要新增的资产类型值，建议用英文说明	Windows
描述	填写需要新增的资产类型的描述	-

4.填写完成后单击“提交”，即可添加新的资产类型

4.4 采集配置

新增采集资产

Syslog 资产

1. 登录日志审计控制台。
2. 选择“系统配置 > 采集管理 > syslog-udp”，进入 syslog-udp 资产配置页。

3. 选择待采集设备的“资产组”和“资产 IP”，单击“新增”完成资产配置。

Snmptrap 资产

同上，区别于采集方式选择 Snmptrap。配置 Snmptrap 采集资产：

1. 新增 MIB 文件任务。在菜单“系统配置> 采集管理 > MIB 管理”页面中，单击“新增”，上传 MIB 文件。
2. 在菜单“系统配置 > 采集管理 > SnmpTrap 管理”页面中，单击“新增”，对弹出的对话框中填写相关参数，详情见下表。
3. 单击“提交”，完成 Snmptrap 资产的对接。

参数名称	填写说明
资产 IP	选择待采集资产的 IP 地址。
数据接收端口	选择待采集资产的数据接收端口。
关联资产	自动关联，无需填写。
SNMP 版本	选择 SNMP 版本，当前仅支持“v1”和“v2c”版本。
Community	自定义发送的团队名称。
MIB 选择文件	选择步骤 1 上传的 MIB 文件。
发送 Topic 名称	自定义发送 Topic 的名称。
MIB 文件内容	查询 MIB 中文件的内容。关键字查询，多个关键字符请使用英文","进行分隔。

Linux 设备和 Windows 设备

Linux 设备

针对 Linux 操作系统的 syslog 采集配置，为减轻运维人员工作，编写了自动化配置脚本，由运维人员执行脚本即可完成配置，将系统日志上报到服务端，该文档主要对配置脚本提供使用说明。

注意：

- 脚本和详细步骤控制台左上角单击  图标，选择“帮助手册”下载。
- 在上传脚本前需要修改脚本中第 50 行左右的“IP_LIST”中的 IP 地址，IP 地址需要跟实例界面的“私有 IP 地址”保持一致。
- 脚本中端口号默认值为“2511”，需要改为和采集页面一致的端口，默认值为“514”。

安装步骤：

1. 上传脚本到服务器任意目录下；
2. 使用 root 用户登陆：**su - root**，并切换到上传目录下；
3. 增加脚本执行权限：**chmod 744 cmd_syslog_config_20201027.sh;**
4. 执行安装脚本：**sh cmd_syslog_config_20201027.sh;**
5. 执行 **source /etc/profile** 指令，若看到如下提示则表示 Syslog 配置完成：

syslog restart complete!

syslog config complete!

Windows 设备

Windows 系统以管理员身份运行安装 eventlog_win 安装包。

注意：详情可单击控制台右上角图标，下载“Windows 代理下载”，安装包内包含相关说明。

规则配置

配置日志的解析接入规则：点击“风险分析 > 事件策略 > 解析接入规则”，目前已经配置常见的日志规则可在该页面中查看，若需要新增自定义规则，可单击“新增”进行配置。选择需要采集的设备类型和日志样本。

可对日志样本先进行一层过滤，如：通过正则表达式，过滤端口等信息。默认不过滤。

选择日志格式解析的方式：正则表达式解析、分隔符解析、key-value 解析、json 格式解析。优先为 json>key-value>分隔符>正则表达式。

鼠标左击选中样本信息中需要提取的字段内容，选择对应字段，添加到字段列表中。

填写实际采集日志，验证日志解析规则是否添加有误（可跳过）。

最后检查保存即可。

配置告警规则：点击“风险分析 > 告警策略”，目前已经配置常见的告警规则可在该页面中查看，若需要新增自定义规则，可点击新增进行配置。

其中告警规则逻辑关系可选择 and、or、fb、rule。

条件可引用菜单“风险分析 > 对象资源”的内容作为字段值引用。

4.5 日志检索

日志检索

通过列表和统计图的方式，更直观的展示采集到的日志情况。默认显示查询条件组以及事件列表 tab 页面

事件列表

单击 “事件分析”>”日志检索”>“查询条件“，显示查询条件组以及事件列表 tab 页面。可对日志进行查询、保存、下载等操作。

查询日志：在查询栏中，通过检索/csl 检索方式查询日志，填写查询条件，点击 ，页面展示过滤后的日

志信息。

查询条件：左侧 “查询条件”为已保存的查询条件，点击具体查询条件，事件列表自动按该查询条件过滤日志。

新增查询条件组：点击新增组，填写查询条件组名称和描述，点击“确定 “，可在左侧查询条件列中看到该查询条件组。或者，在”保存“按钮中，也可以通过条件分组下拉框中，点击”+“添加查询条件组。

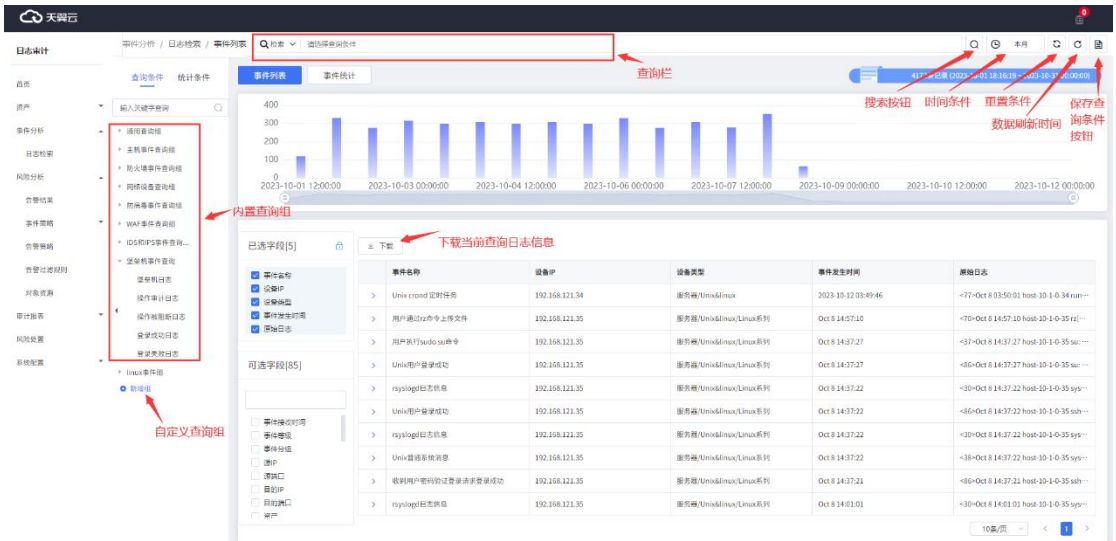
保存查询条件：点击“保存“按钮，选择是否另存，填写条件名称和条件分组等信息，将当前查询条件保存到左侧查询条件列中。下次直接点击该查询条件即可自动查询日志信息。

事件列表页面交互：点击 “ ”,可通过勾选可选字段，展示勾选的字段内容。

下载日志：将当前查询日志信息，以 excel 形式保存本地。

注意：

- 内置查询条件组无法做新增、编辑、删除的操作。
- 是否另存为是时，新增一个查询条件；为否时，覆盖原来相同的条件名称的查询条件。



事件统计

点击 “事件分析”>”日志检索”>“统计条件 “，显示统计条件组以及事件统计 tab 页面。可对日志进行查询、保存等操作。

查询日志：在查询栏中，通过检索/csl 检索方式查询日志，填写查询条件，点击 ，页面展示过滤后的日

志统计图。

统计条件：左侧 “统计条件”为已保存的统计条件，点击具体统计条件，事件统计图自动按该统计条件展示过滤后的统计图。

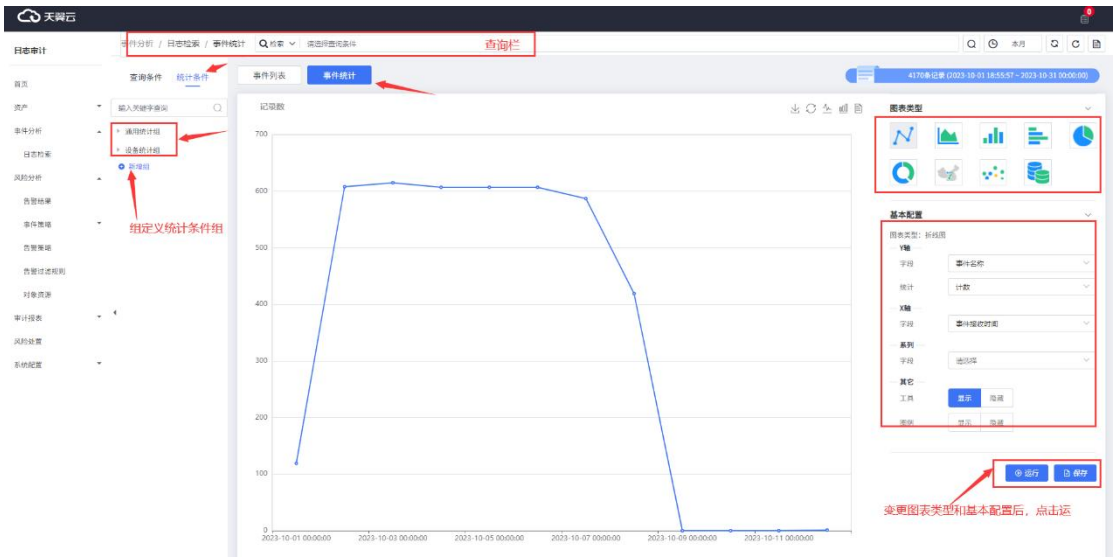
新增统计条件组：点击新增组，填写统计条件组名称和描述，点击“确定 “，可在左侧统计条件列中看到该统计条件组。或者，在”保存“按钮中，也可以通过条件分组下拉框中，点击” + “添加统计条件组。

保存统计条件：点击“保存“按钮，选择是否另存，填写条件名称和条件分组等信息，将当前统计条件保存到左侧统计条件列中。下次直接点击该统计条件即可自动查询日志信息。

图表类型：选择折线图、面积图、柱形图、横向柱形图、饼形、环状图、地图、散点图、数值图等统计图，和要展示和统计的字段后，点击“运行“按钮，页面展示新的统计图。

注意:

- 内置统计条件组无法做新增、编辑、删除的操作。
- 要保存变更后的统计图，必须先点击运行，再保存。
- 是否另存为是时，新增一个统计条件；为否时，覆盖原来相同的条件名称的统计条件。

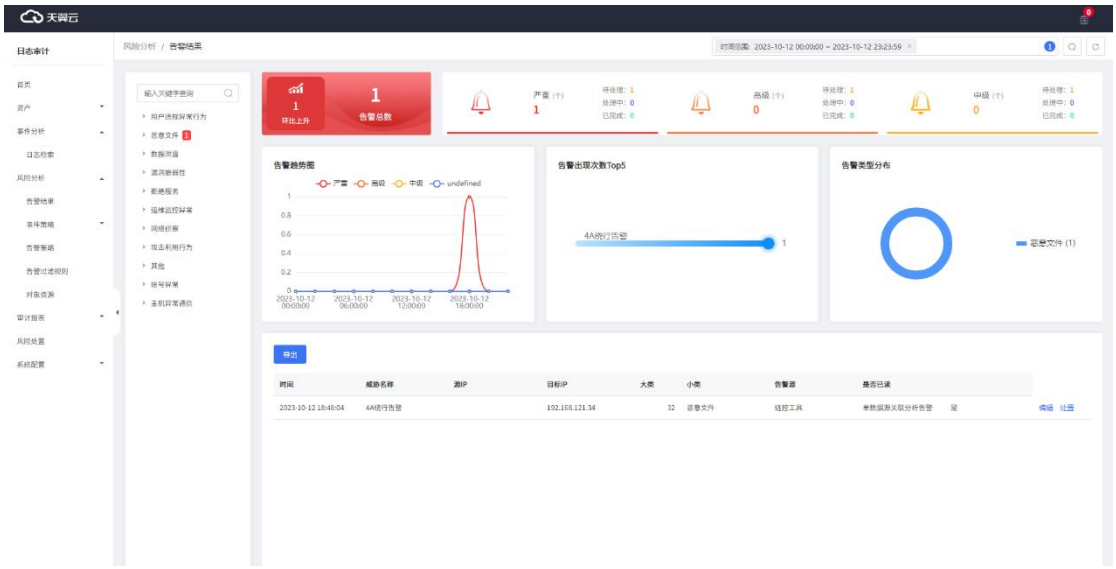


4.6 风险分析

4.6.1 告警结果

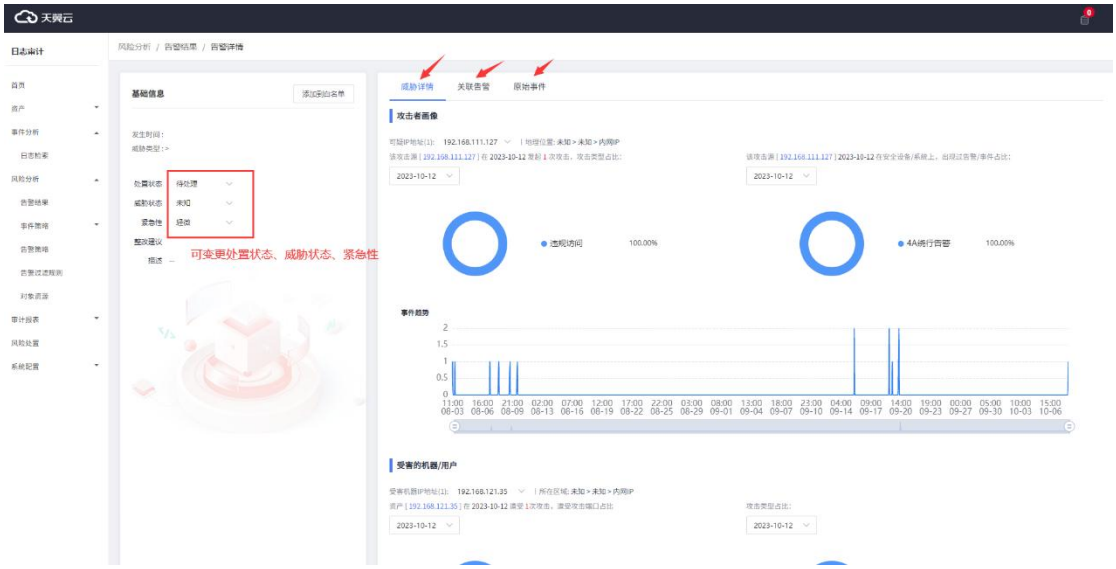
告警结果

点击 “风险分析” >”告警结果”，进入告警结果页面，展示告警类型、告警总数、告警趋势图、告警出现次数 Top5、告警类型分布，并且对告警进行查询、编辑、处理操作。



告警结果编辑

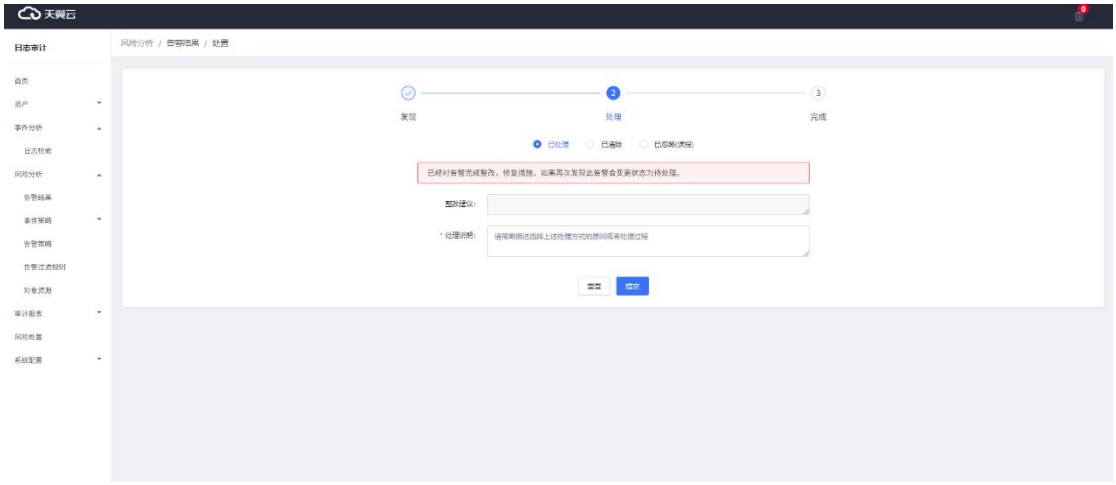
点击 “ 编辑 ” 按钮，可查看告警基本信息、威胁详情（攻击者画像、事件趋势、受害的机器/用户）、关联告警、原始事件。



告警结果处置

点击“处置”按钮，进入处置界面，选择告警处置方式，已处理、已清除、已忽略（误报），并且填写处理说明，点击提交后，处置方式变更。

注意：已清除的告警再次触发后，不再变更处理状态，其他处理方式变更为待处理，需要重新处置。

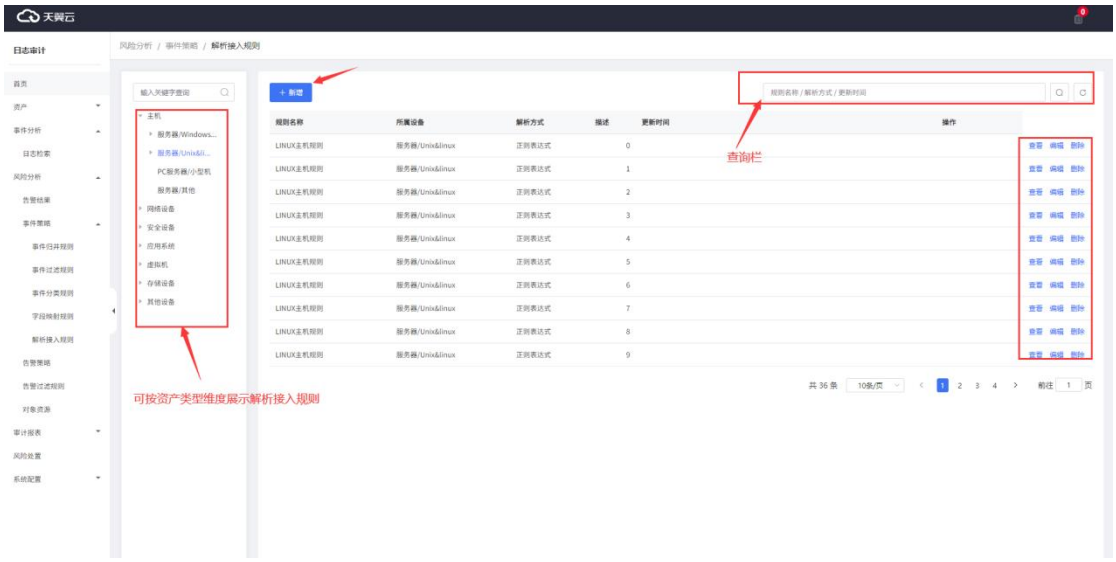


4.6.2 事件策略

4.6.2.1 配置解析接入规则

解析接入规则是对采集日志的分析，符合解析接入规则的日志才能被采集到日志审计平台。可对解析接入规则进行新增、查看、编辑、删除、查询操作。

点击“风险分析 >事件策略 > 解析接入规则”，配置需要采集的日志规则。



新增解析接入规则

点击“新增”按钮，弹出解析接入规则添加界面，根据页面提示填写相应的信息，*号标识的为必填属性，点击提交，即可添加成功。

详情步骤如下：

1. 基本信息：填写规则名称和选择需要采集的设备类型。

基本信息	是否必选	说明
解析规则名称	必选	自定义，注意名称不能与其他规则重复。
设备类型	必选	通过下拉框进行选择。此处选择的设备类型应与资产的设备类型保持一致。
优先级	可选	自定义，注意不能与其他规则优先级重复。
描述	可选	规则的具体说明。

2. 提取样本：将原始日志复制到该文本框。

提取样本	是否必选	说明
原始样本	必选	输入原始日志样本。

3. 前置过滤：可对日志样本通过正则表达式先进行一层过滤，默认不过滤。

前置过滤	是否必选	说明
原始样本	-	提取样本中的原始样本，只支持查看。

前置过滤	是否必选	说明
是否过滤	必选	原始样本过滤参数，开启过滤，还需配置后续参数。
过滤方式	-	默认“正则匹配”，不支持已修改。
正则表达式	必选	自行填写正则表达式。
过滤后样本	-	后续将在过滤后的样本中提取字段，只支持查看。

4. 选择方法：解析方法支持正则表达式解析、分隔符解析、key-value 解析、json 格式解析。优先为 json>key-value>分隔符>正则表达式。

方法	说明
正则表达式	将使用正则表达式提取字段。
分隔符	将使用分隔符（例如逗号、空格或者字符）提取字段。
Key-Value	将对 key-value 类型数据进行提取字段。
JSON	将对 json 类型数据进行提取字段。

5. 提取字段：根据选择的不同方法，填写需要提取的内容。

提取方法	提取字段
正则表达式	方式一：手动输入正则表达式 在**正则表达式**下方，单击“编辑”，输入正则表达式后单击“保存”。会根据所填正则表达式提取字段。
	方式二：选取需要提取的字段自动填入正则表达式 1. 鼠标左击在样本信息中选取需要提取的字段内容。 2. 在弹出的提取字段对话框中配置如下参数。 ● 目标字段：下拉选择字段标签，必填。 ● 目标字段名：选择目标字段后，自动填入。 ● 目标字段类型：选择目标字段后，自动填入。 ● 样本字段类型：默认字符型，必填。 ● 长度模式：固定长度为所选中长度，非固定长度按需选择前置或后置锚点。 ● 示例值：默认为鼠标选中的数据。
分隔符	选择**分隔符**，通过分隔符提取字段。 1. 在分隔符选择一个分隔符，或手动输入其他分隔符。 2. 在提取字段列表中，单击“目标字段”列的“快速选择”，指定目标。
key-value	选择键值对分隔符、键值分隔符。 ● 键值对分隔符：将样本信息分割成若干对键值对。 ● 键值分隔符：用户分割键值对内部的键与值。

提取方法	提取字段
	示例：样本信息为 "name=张三&age=18" ，此时键值对分隔符为 "&" ，键值分隔符为 "=" 。
json 格式	自动按照 json 格式将字段提取到提取字段列表中，单击“目标字段”列的“快速选择”，指定目标。

6. 验证规则：填写实际采集日志，验证日志解析规则是否添加有误（可跳过）。

7. 预览保存：检查填写内容是否正确，确定无误后点击保存。

管理解析接入规则

规则配置完成后，在规则列表，支持查看规则详情、编辑规则、删除规则。

- 查询规则：在查询栏中，填写需要查询的条件，点击“搜索”按钮，列表展示过滤后的规则。
- 查看规则详情：单击规则列表操作列的“查看”按钮，进入解析接入规则的详情界面。
- 编辑规则：单击规则列表操作列的“编辑”按钮，弹出编辑界面，修改解析接入规则。
- 删除规则：单击规则列表操作列的“删除”按钮，在弹出的提示框中，单击“确定”。

4.6.2.2 配置事件分类规则

事件分类规则是对采集到的日志进行一个分组分类。点击“风险分析 > 事件策略 > 事件分类规则”，可对事件分类规则进行新增、查看、编辑、删除、查询操作。

新增事件分类规则

点击“新增”按钮，弹出事件分类规则添加界面，根据页面提示填写相应的信息，*号标识的为必填属性，点击提交，即可添加成功。

参数	是否必选	参数说明
分类名称	必选	自定义事件分类规则的名称。
日志分组	必选	在下拉框中选择该事件分类中，日志划分的类型。 例如：分组根节点 / 策略违规 / 策略违规/应用策略违规 / 策略违规/应用策略违规/密码策略

参数	是否必选	参数说明
日志等级	必选	在下拉框中选择该日志的影响等级。支持轻微、低级、中级、高级、严重。
判断类别	必选	选择日志的判断类型，可选“关键字”或“正则表达式”。 ● 若选择“关键字”，还需填写关键字，多个关键字用英文字符的逗号隔开。 ● 若选择“正则表达式”，还需填写正则表达式。 注意： 关键字和正则表达式任意填写一个，采集到的日志将符合填写的关键字内容或者正则表达式，归纳到该分类分组中。
规则所属设备	必选	在下拉框中选择此事件分类规则所属的设备。 例如：根结点 / 主机 / 服务器/Windows 系列 / 服务器/Windows 系列/Windows 8
规则描述	可选	填写此事件分类规则的描述。
建议措施	可选	填写此事件分类规则的建议处理措施。

管理事件分类规则

规则配置完成后，在规则列表，支持查询规则、查看规则详情、编辑规则、删除规则。

说明：

内置规则不支持修改、删除。

- 查询规则：在查询栏中，填写需要查询的条件，点击搜索图标，列表展示过滤后的规则。
- 查看规则详情：单击规则列表操作列的“查看”按钮，进入事件分类规则的详情界面。
- 修改规则：单击规则列表操作列的“修改”按钮，弹出编辑界面，修改事件分类规则。
- 删除规则：勾选需要删除的规则，单击规则列表右上方的“删除”按钮，在弹出的提示框中，单击“确定”。

4.6.2.3 配置字段映射规则

字段映射规则是对采集到的日志字段内容映射，如等级字段，接收到的可能是数值 1、2、3，可以通过字

段映射成：低、中、高。

可对字段映射规则进行新增、查看、编辑、删除、查询操作。

新增字段映射规则

1. 登录日志审计（原生版）控制台。
2. 在左侧导航栏选择“风险分析 > 事件策略 >字段映射规则”。
3. 单击“新增”，弹窗新增规则窗口。
4. 配置字段映射规则的相关参数。

参数	参数说明	取值样例
设备类型	在下拉框中选择需要配置字段映射的设备类型。	主机 / 服务器/其他
字段名	在下拉框中选择配置字段映射规则的字段名。	业务系统
字段原始值	填写配置规则设备类型下字段的原始值。	1
字段映射值	填写原始值映射后的内容。	低

5. 填写完成后，单击“提交”完成字段映射规则配置。

相关操作

规则配置完成后，在规则列表，支持查询规则、查看规则详情、编辑规则、删除规则。

- 查询规则：在查询栏中，填写需要查询的条件，点击搜索图标，列表展示过滤后的规则。
- 查看规则详情：单击规则列表操作列的“查看”按钮，进入规则的详情界面。
- 编辑规则：单击规则列表操作列的“编辑”按钮，弹出编辑界面，修改规则。
- 删除规则：单击规则列表操作列的“删除”按钮，在弹出的提示框中，单击“确定”。

4.6.2.4 配置事件归并规则

事件归并规则是对采集到日志进行归并。点击“风险分析 > 事件策略 > 事件归并规则”，可对事件归并规则进行新增、查看、编辑、删除、查询操作。

新增事件归并规则

点击“新增”按钮，弹出事件归并规则添加界面，根据页面提示填写相应的信息，*号标识的为必填属性，点击提交，即可添加成功。

参数	是否必选	参数说明	取值样例
归并规则名称	必选	自定义归并规则名称。	Test
相关采集器	必选	选择日志采集器，目前仅可选择“log_p”。	log_p
过滤字段选择	必选	根据业务实际情况填写过滤字段。	目标端口等于 8080
归并字段选择	必选	根据业务实际情况选择归并字段。	EVENTNAME
归并时间（秒）	必选	选择日志每次归并的时间，时间越长归并的日志越多。	30
归并后事件名	可选	自定义归并后的事件名称。若不配置，则默认为原事件名称。	Event1
归并后事件等级	可选	选择归并后日志事件的等级。若不选择，则默认为原事件等级。	轻微
归并后设置	必选	选择归并后日志数据是选择第一条数据，还是最后一条数据。	第一条

管理事件分类规则

规则配置完成后，在规则列表，支持查询规则、查看规则详情、编辑规则、删除规则。

- 查询规则：在查询栏中，填写需要查询的条件，点击搜索图标，列表展示过滤后的规则。
- 查看规则详情：单击规则列表操作列的“查看”按钮，查看事件归并规则详情。
- 修改规则：单击规则列表操作列的“修改”按钮，弹出修改界面，修改事件归并规则。
- 删除规则：单击规则列表操作列的“更多 > 删除”按钮，在弹出的提示框中，单击“确定”。

4.6.2.5 配置事件过滤规则

事件过滤规则是对采集到的日志进行过滤，将不需要审计的日志条件填入规则，不再审计过滤的日志。可对事件过滤规则进行新增、查看、编辑、删除操作。

新增事件过滤规则

1. 登录日志审计（原生版）控制台。

2. 在左侧导航栏选择“风险分析 > 事件策略 > 事件过滤规则”。

3. 单击“新增规则”，弹出新增规则窗口。

4. 配置过滤规则，填写完成后单击“提交”。

参数	参数说明	取值样例
规则名称	自定义过滤规则名称。	Test
相关采集器	选择日志采集器，目前仅可选择“log_p”	log_p
过滤规则	根据业务实际情况填写过滤规则。	目标端口等于 8080

相关操作

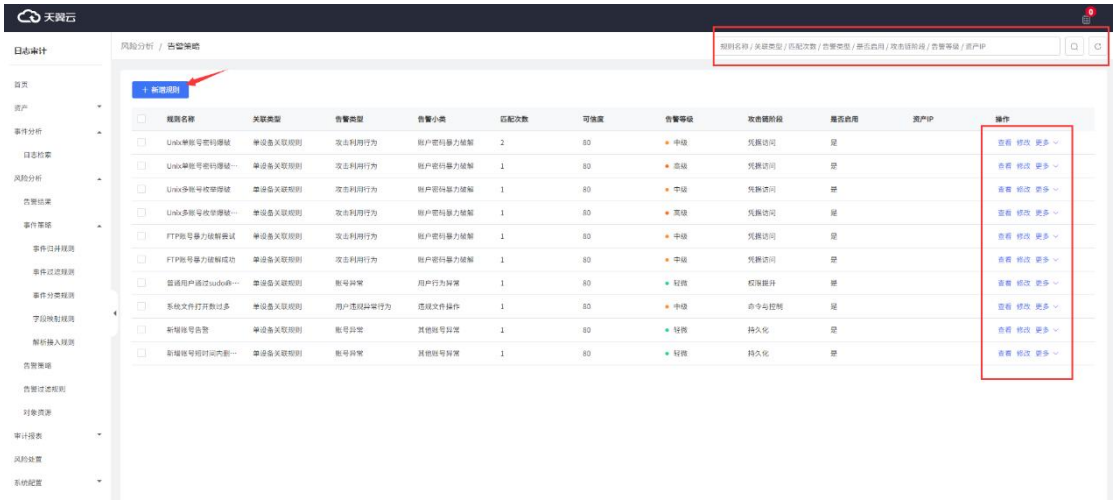
规则配置完成后，在规则列表，支持查询规则、查看规则详情、编辑规则、删除规则。

- 查询规则：在查询栏中，填写需要查询的条件，点击搜索图标，列表展示过滤后的规则。
- 查看规则详情：单击规则列表操作列的“查看”按钮，查看事件过滤规则详情。
- 修改规则：单击规则列表操作列的“修改”按钮，弹出修改界面，修改事件过滤规则。
- 删除规则：单击规则列表操作列的“更多 > 删除”按钮，在弹出的提示框中，单击“确定”。

4.6.3 告警策略

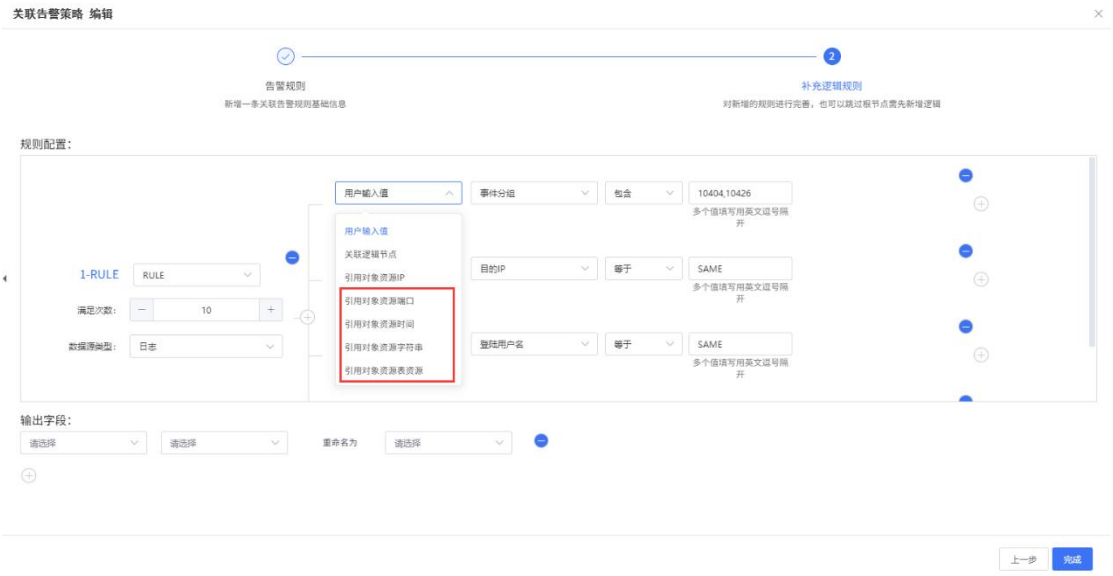
告警策略，对采集到的日志进行告警判断，符合告警策略的日志进行告警。

点击“风险分析”>“告警策略”，可对告警策略进行新增、查看、编辑、删除、查询、停用操作。



- 新增：点击“新增”按钮，弹出告警策略添加界面，根据页面提示填写相应的信息，*号标识的为必填属性，点击提交，即可添加成功。
- 查看：点击“查看”按钮，弹出告警策略的详情界面。
- 编辑：点击“编辑”按钮，弹出编辑界面，修改告警策略。
- 查询：在查询栏中，填写需要查询的条件，点击“搜索”按钮，列表展示过滤后的规则。
- 停用/启用：点击“停用”按钮，该告警规则停用，触发该日志时，不产生告警；反之，点击“启用”按钮时，该告警规则有效。

注意：在告警策略中，可直接引用菜单“风险分析”>“对象资源”中的值作为条件替换。

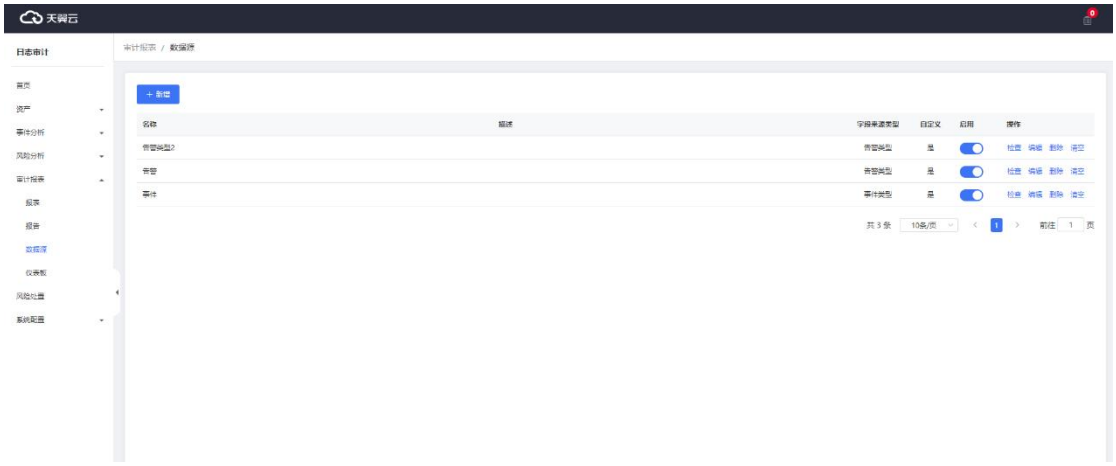


4.7 审计报表

4.7.1 数据源

数据源

数据源是获取需要展示日志/告警字段条件数据。点击“审计报表”>“数据源”，可对数据源进行新增、检查、编辑、删除、清空等操作。



- 新增：点击“新增”按钮，弹出新增界面，根据页面提示填写相应的信息，字段类型为事件类型/告警类型，其中字段配置根据选择的字段类型不同，显示不同的字段。
- 检查：点击“检查”按钮，数据源已录入，则提示“数据源数据存在“。反之，提示” 数据源数据不存在“ 。
- 编辑：点击“编辑”按钮，弹出编辑界面，修改数据源。
- 删除：点击“删除“按钮，提示”确定删除当前项“，确定后，该数据源被删除。
- 清空：点击“清空“按钮，提示”确认清空数据源已有数据“。确定后，该数据源内容被清空。
- 启用/禁用。点击 “启用/禁用”，弹窗提示语，已启用/已禁用，启用每天定时获取该任务数据。已禁用，不再每天定时获取该任务数据。

注意

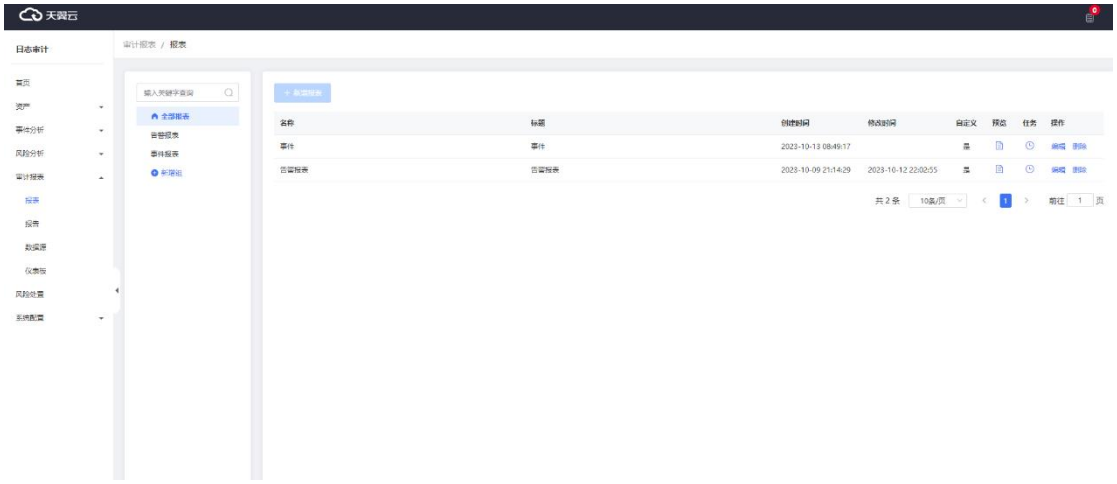
- 数据源添加完成，每天凌晨 3 点定时跑任务，获取昨天符合条件的数据。
- 无法对统计字段和分组字段进行修改。
- 若存在报表已经已经引用，则无法删除该数据源，提示“报表存在引用的数据源，不可删除！”。

4.7.2 报表

报表

报表是将获取到的数据源数据，按报表的形式展示。点击“审计报表”>“报表”，对报表组底下的报表

进行新增、预览、下发任务、编辑、删除等操作。



- 新增组：新增报表组。点击“新增组”按钮，弹出新增界面，根据页面提示填写相应的信息，确定后，页面添加完成。
- 新增：新增报表。选择报表组，点击“新增”按钮，弹出新增界面，根据页面提示填写相应的信息，点击“提交 “，报表添加完成。
- 下发任务：下发生成报表文件的任务。点击“任务“按钮，对报表任务进行新增、复制、下载、删除操作。
- 编辑：点击“编辑”按钮，弹出编辑界面，修改数据源。
- 删除：点击“删除“按钮，提示”确定删除当前项 “，确定后，报表被删除。
- 预览：点击“预览“按钮，选择时间，可预览该时间范围内报表内容。

注意

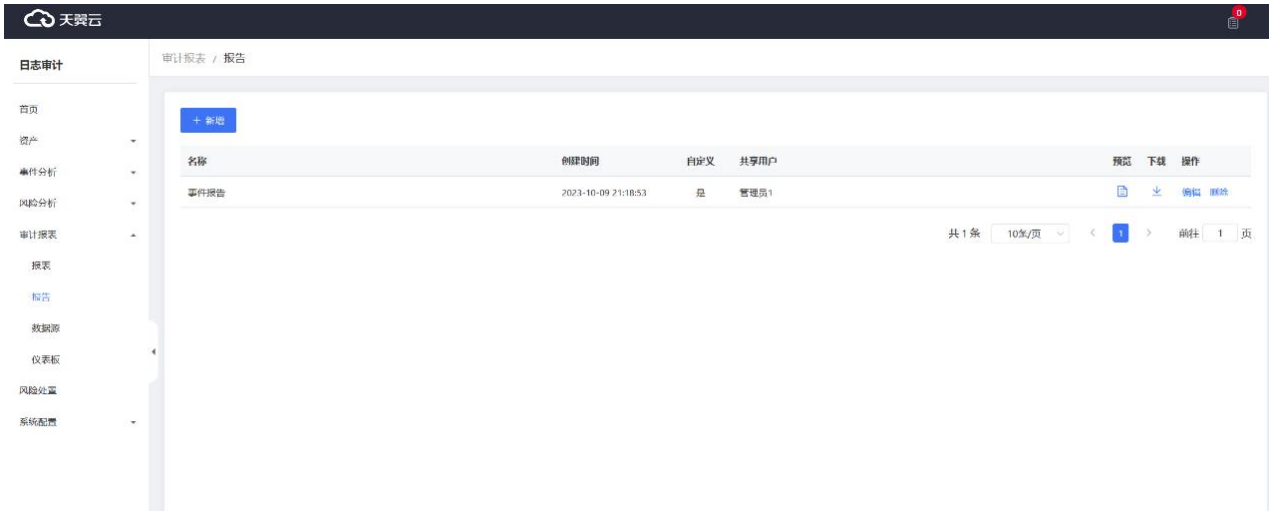
- 支持 word、pdf 格式。
- 无法变更数据源。

4.7.3 报告

报告

报告是将获取到的多个报表整合在一份文档中。点击“审计报表”>“报告” ，报告进行新增、预览、下

发任务、编辑、删除等操作。



- 新增：新增报告。点击“新增”按钮，弹出新增界面，根据页面提示填写相应的信息，点击“确认“，报告添加完成。
- 编辑：点击“编辑”按钮，弹出编辑界面，修改报告。
- 删除：点击“删除“按钮，提示”确定删除当前项“，确定后，报告被删除。
- 预览：点击“预览“按钮，选择时间，可预览该时间范围内报告内容。

注：周报每周一定时生成报告文件，月报每月初定时生成报告文件。

4.8 风险处置

您可以添加风险通知规则，配置规则后，发生相应的事件日志审计服务可以第一时间通过邮件或短信的形式通知到您。

新增风险规则

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“风险处置”，进入“风险处置”页面。

3.单击“新增规则”按钮，在跳转的“新增规则”页面填写相关参数。

参数	参数说明	取值样例
规则名称	自定义风险规则名称。	Test
有效开始时间	选择新建风险规则开始生效的日期。	2024-09-01 10:00:00
有效结束时间	选择新建风险规则失效的日期。	2025-09-01 10:00:00
来源	选择风险规则的事件来源，目前仅支持选择“告警”。	告警
过滤规则	请您根据业务实际需求填写。	-
发送时间范围	选择发送通知的时间范围。	周一-17:00:00-18:00:00
工单时限	选择工单存在的时间范围，单位为“小时”。	12
通知方式	目前新建的风险规则仅支持邮件通知。 预设的风险支持通信通知。	-

说明：短信通知告警暂不支持自定义模板。

4.单击“确认”，完成风险规则配置。

后续操作

启停风险规则：勾选需要启停的风险规则，单击“规则启停”，完成操作。

修改风险规则：单击“操作”列的“修改”按钮，修改需要变动的内容后单击“确认”完成修改。

4.9 系统配置

4.9.1 角色管理

在“二类节点”区域购买的实例【日志审计（原生版）支持的区域请参见“支持的区域”】，支持角色管理功能。通过给用户关联不同的角色，赋予用户在系统中不同模块的操作权限。

注意：

只有初始用户具有删除角色的权限。

创建角色

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“系统配置 > 角色管理”，进入“角色管理”页面。

3.单击页面上方的“新增”，在弹出的对话框中填写内容以新建角色。

参数	参数说明	取值样例
角色编码	填写新建角色的自定义编码，由 3-16 位的数字字母下划线组成。	Operation
角色名称	填写新建角色的自定义名称。	运维人员
可授出角色	选择可赋予该角色的角色。	普通用户

4.单击“提交”，完成角色的创建。

修改角色

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“系统配置 > 角色管理”，进入“角色管理”页面。

3.选择需要修改的角色，单击“操作”列的“修改”。

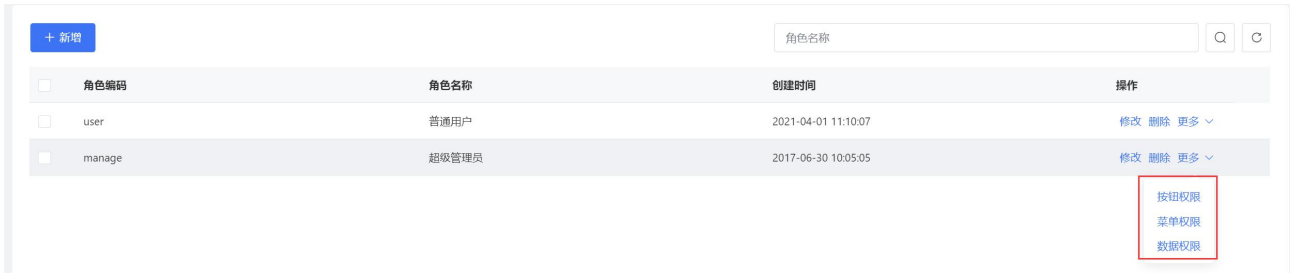
4.在弹出的对话框中修改需要调整内容，单击“提交”，完成角色修改。

配置角色模块权限

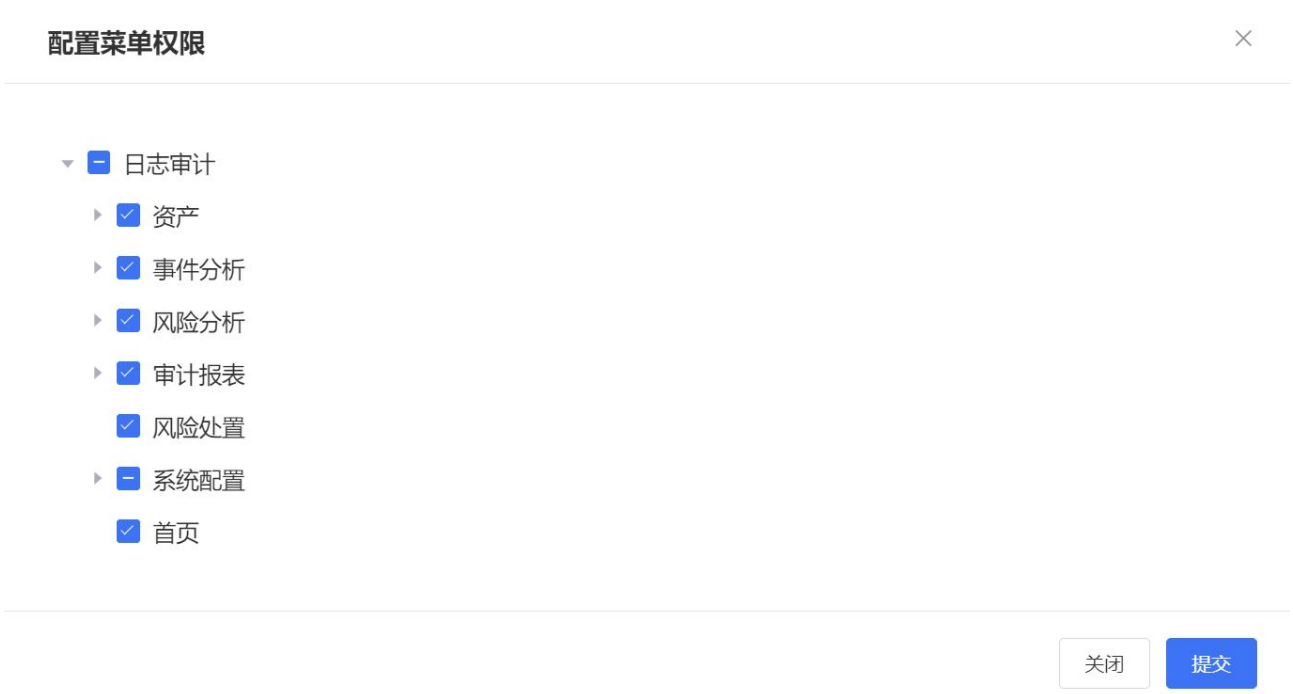
1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“系统配置 > 角色管理”，进入“角色管理”页面。

3.选择需要配置权限的角色，单击“操作”列的“更多”，选择待配置的权限。



4.根据角色的业务需求，勾选需要配置的模块。



5.单击“提交”，完成权限配置。

4.9.2 用户管理

在“二类节点”区域购买的实例【日志审计（原生版）支持的区域请参见“支持的区域”】，支持用户管理功能。日志审计（原生版）的一个用户代表一个可登录自然人，支持新建本地用户。

新建用户

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“系统配置 > 用户管理”。

3.单击“新增”，在弹出对话框中填写新建用户的相关参数。

参数	参数说明	取值样例
用户类型	请选择“系统用户”。	系统用户
用户名称	填写新建用户的名称（非登录名）。	-
登录名	填写新建用户的登录名称。	Test
密码	填写新建用户的密码。	-
再次输入密码	二次填写新建用户的密码。	-
手机号	填写新建用户的手机号码。	13000000000
固定电话	填写新建用户的固定电话号码。	010-XXXXXXXX
电子邮箱	填写新建用户的电子邮箱。	Test@chinatelecom.cn
资产组	选择新建用户所属的资产组。	资产组
地域	选择新建用户所在的地域，仅支持选择中国境内地区。	中国北京
安全域	选择新建用户所属的域。	安全域
专业	选择新建用户的专业。	数据
角色	选择新建用户的角色，角色配置请参考：角色管理章节	普通用户
授权截止时间	选择新建用户的到期时间，请谨慎选择，到期后不可再次登录。	-

4.单击“提交”，完成创建角色。

修改用户信息

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“系统配置 > 用户管理”。

3.单击待修改角色的“操作”列的“修改”按钮，在弹出对话框中修改用户的相关参数。

4.修改完成后单击“提交”，完成角色修改。

删除用户

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“系统配置 > 用户管理”。

3.选择待删除角色的“操作”列的“更多 > 删除”，在弹出对话框中单击“确定”完成删除操作。

4.9.3 操作日志

选择“系统配置 > 操作日志”，可查看系统内所有用户的操作情况包括访问的模块和操作的内容。

用户名称：进行此操作的用户。

登录 IP：进行操作用户登录的 IP 地址。

访问模块：用户进行操作的模块。

操作内容：用户进行的动作。

详细内容：用户进行具体操作的详细数据内容。

发生时间：此操作发生的时间。

是否成功：操作是否成功进行。

4.9.4 邮件服务器

邮件服务器，为系统告警、审计报表等通知提供邮件发送服务。

配置邮件服务器

1.登录日志审计（原生版）控制台。

2.在左侧导航栏选择“系统配置 > 邮件服务器”。

3.单击“编辑”按钮，配置相关参数，详见下表。

参数	参数说明
SMTP 邮件服务器地址	填写发送邮件账号所属的 SMTP 服务器地址，请确认是否填写正确，否则会造成邮件无法发送。
邮件发送账号地址	填写发送系统通知的邮件地址。
邮件发送账号密码	填写发送系统通知的邮件密码。

4.9.5 采集管理

Snmtrap 资产

1.新增 MIB 文件任务。在菜单“系统配置> 采集管理 > MIB 管理”页面中，单击“新增”，上传 MIB 文件。

2.在菜单“系统配置 > 采集管理 > SnmpTrap 管理”页面中，单击“新增”，对弹出的对话框中填写相关参数，详情见下表。

3.单击“提交”，完成 Snmptrap 资产的对接。

参数名称	填写说明
资产 IP	选择待采集资产的 IP 地址。
数据接收端口	选择待采集资产的数据接收端口。
关联资产	自动关联，无需填写。
SNMP 版本	选择 SNMP 版本，当前仅支持“v1”和“v2c”版本。
Community	自定义发送的团队名称。
MIB 选择文件	选择步骤 1 上传的 MIB 文件。
发送 Topic 名称	自定义发送 Topic 的名称。
MIB 文件内容	查询 MIB 中文件的内容。关键字查询，多个关键字符请使用英文","进行分隔。

Syslog-udp

1.登录日志审计控制台。

2.选择“系统配置 > 采集管理 > syslog-udp”，进入 syslog-udp 资产配置页。

3.选择待采集设备的“资产组”和“资产 IP”，单击“新增”完成资产配置。

JDBC 管理

1.选择“系统配置 > 采集管理 > JDBC 管理”，进入 JDBC 管理配置页。

2.单击左上角的“新增”，在弹出的对话框中填写相关参数。

注意：在填写查询 SQL 语句的时候，切勿使用“;”进行结尾，否则服务无法识别到该 SQL 语句。

3.填写完成后，单击“测试连接”确认是否可以和数据库建立起通信。

4.若测试连接通过，单击“提交”完成新增。

Kafka 管理

1.选择“系统配置 > 采集管理 > Kafka 管理”，进入 Kafka 管理配置页。

2.单击左上角的“新增”，在弹出的对话框中填写相关参数。

参数	参数说明	取值样例
资产组	选择需要使用 Kafka 管理资产所在的资产组。	资产组
资产 IP	选择需要使用 Kafka 管理资产的 IP。	0.0.0.0
服务端地址	填写 Kafka 服务端所在的 IP 地址。	0.0.0.0
服务端端口	填写 Kafka 服务端所在的端口。	8080
采集 Topic	填写 Kafka 已创建的 Topic，以便进行数据采集。	Test
Topci 消费组 ID	默认为 logaudit_1，请您根据自身业务情况填写。	1
采集偏量	（选填）可选择 From Latest 或 From begining。	From begining
协议	（选填）可选 PLAINTEXT、SSL/TSL、SASL/PLAIN 协议。	SLL/TSL
发送 Topic	选择采集日志发送的 Topic，默认填写 log-topic。	log-topic

3.填写完成后，单击“测试连接”确认是否可以建立起通信。

4.若测试连接通过，单击“提交”完成新增。

FTP/SFTP 管理

说明：

FTP/SFTP 采集仅针对当前目录下的新文件进行采集，且同一文件只采集一次。

1.选择“系统配置 > 采集管理 > FTP/SFTP 管理”，进入 FTP/SFTP 管理配置页。

2.单击左上角的“新增”，在弹出的对话框中填写相关参数。

参数	参数说明	取值样例
资产组	选择需要使用 FTP/SFTP 管理资产所在的资产组。	资产组
资产 IP	选择需要使用 FTP/SFTP 管理资产的 IP。	0.0.0.0
数据 IP	填写需要进行 FTP/STPF 采集服务器的 IP 地址。	0.0.0.0
数据源名称	自定义采集到的数据源名称。	Test
采集方式	在下拉框中选择新添加的采集方式： - FTP - SFTP - 本地采集	FTP
采集格式	根据业务需求选择采集格式： - 单行：获取单行的日志信息，以换行符为结尾。 - 多行：获取多行的日志信息，匹配行首正则表达式。	单行
行首正则表达式	仅“采集格式”选择**多行**时可填写，填写正则表达式。	-
端口	仅在“采集方式”选择 **FTP** 或 **SFTP** 时可填写。 FTP 默认使用 21 端口，SFTP 默认使用 22 端口，请您根据业务实际情况填写。	21
用户名	填写连接服务器使用的登录用户。	root
密码	填写连接服务器使用的登录用户密码。	-
文件路径/目录	选择需要采集日志文件所在的路径/目录（配置的用户需要有相应的访问权限），使用*号多可查询多个路径/目录。 - 目录的路径仅最后一级支持填写通配符。	-
文件名	选择需要采集日志的文件名，使用*可采集多个文件，支持 json、xml、txt、csv、	-

参数	参数说明	取值样例
	log 后缀格式。	
子文件日志	选择是否读取子文件目录下一级文件。	是
删除模式	可选择保留或删除采集产生的文件。	保留
传输模式	仅“采集方式”选择 **FTP** 时可选择。 选择主动传输模式或被动传输模式。	主动
服务器字符集	根据业务情况选择字符集，支持 UTF-8 和 GBK。	GBK
Cron 表达式	设置定时任务，默认每分钟执行一次。	0 50 23
发送 Topic	选择采集日志发送的 Topic，默认填写 log-topic。	log-topic
描述	填写此采集方式的描述。	-

3.填写完成后，单击“测试连接”查看是否可以正常连接至服务器。

4.若可以正常连接，单击“提交”，完成配置。

4.9.6 日志备份

日志备份功能通过自动化归档、多副本存储及生命周期管理，确保业务连续性与合规性，优化存储资源并支持长期追溯分析。

注意：仅 V3.0.0 版本及以上的日志审计实例支持日志备份功能。

新增日志备份任务

1.登录日志审计（原生版）实例。

2.在左侧导航栏选择“系统配置 > 日志备份”，进入“日志备份”页面。

3.单击页面左上方的“新增”按钮，开始新增新的日志备份任务。

参数	参数说明	填写示例
任务名称	自定义任务名称	Test
备份方式	可选择“原始日志”、“索引快照”。 **原始日志**：只备份原始日志； **索引快照**：包括格式规范化后的数据以及原始日志。	原始日志
备份任务类型	可选择“单次执行”或“周期执行”。 **单次执行**：选择执行日志备份的时间、日志备份的日期范围。 **周期执行**：选择每天或每周为周期，选取每次执行的时间。	单次执行
单文件大小	备份过程中生成的文件大小设置，范围在 100-1000M，默认 500M	500M
远端服务器地址	填写远端服务器合法的 IP 地址。	192.168.0.1
保存目录	以根目录/开头，且拥有远端机器创建目录的权限，保存目录不能包含特殊字符`~!@#$^&*()|{}:;,.<>?)和中文。 说明： Windows 机器根目录以 sftp 服务设置的路径为准，如 sftp 服务路径为 C:/Windows/sftpuser，则根目录就是 C:/Windows/sftpuser。	/tmp
用户名	填写连接远端机器的用户名	root
密码	填写连接远端机器的密码	-
端口	填写远端机器连接端口且为正整数	8080

4.填写完成后，单击提交即可完成日志备份任务新增。

查看日志备份记录

每次日志备份任务进行一次操作之后，会在系统生成一次记录，您可以通过任务记录查看日志备份的情况。

1.登录日志审计（原生版）实例。

2.在左侧导航栏选择“系统配置 > 日志备份”，进入“日志备份”页面。

3.选择需要查看备份记录的日志任务，选择操作列的“更多 > 任务记录”，可在“任务界面”查看日志备份的情况。

其他操作

- 删除日志备份任务：选择需要删除的日志任务，选择操作列的“更多 > 删除”，阅读对话框中内容，确认无误需要删除后单击“确定”即可完成日志备份删除。
- 启用日志备份任务：日志备份任务的状态为“已禁用”，选择操作列的“更多 > 启用”即可启用日志备份任务。

> 说明：
>
> 若启用日志备份任务提示：备份时间早于当前时间，无法备份！请修改备份时间。
>
> 需要编辑日志备份任务，确保首次备份的事件晚于当前时间。

- 禁用日志备份任务：日志备份任务的状态为“已启用”，选择操作列的“更多 > 禁用”即可禁用日志备份任务。

4.9.7 系统运维

在系统运维模块，您可以直观的查看日志审计（原生版）的硬件运行情况、系统巡检情况。

系统监控

系统监控实时展示设备的“CPU 利用率”、“内存利用率”和“磁盘使用情况”。

系统巡检

单击“立即执行”可以立即开始系统巡检。

将定时执行按钮调整至开启状态，每日可以定时巡检，在右侧“每天执行时间”处设定每日巡检的时间。

服务管理

单击“一键重启”可以重启所有服务器。

说明：重启需谨慎，请确保业务可以正常使用。

4.9.8 日志转发

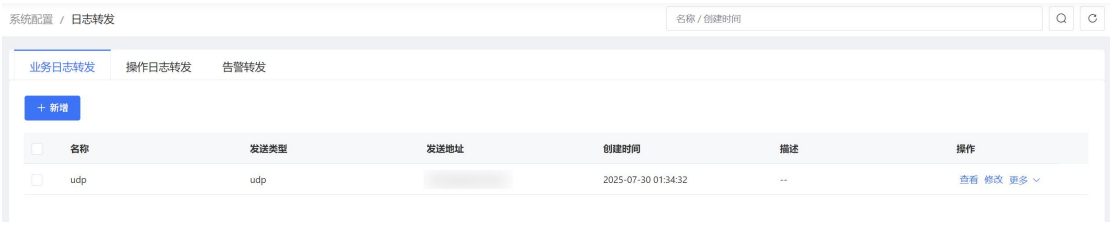
日志转发是指将日志数据从日志审计服务实时或准实时地传输到外部服务器的过程。

新增日志转发任务

1.登录日志审计控制台。

2.在左侧导航栏选择“系统配置 > 日志转发”，进入“日志转发”页面。

3.根据业务需求，选择需要转发的日志或告警，单击“新增”按钮。



4.在弹出的窗口中填写相关参数。填写完成后单击“提交”即可。

参数	说明
名称	自定义名称，不超过 50 个字符长度
数据过滤规则	通过配置过滤参数，筛选要转发的日志： ● 业务日志转发：支持通过事件名称、设备 IP、设备类型、事件等级、事件分组字段进行筛选。 ● 操作日志转发：不涉及。 ● 告警日志转发：支持通过源/目的 IP、源/目的端口、告警名称、告警大/小类、告警等级、开始/结束时间进行筛选。
描述	自定义内容，不超过 512 个字符长度
日志发送类型	可选 udp 和 kafka 方式，配置后该参数不可修改。 ● udp 转发方式：支持添加多个目标。 ■ 目标地址：请输入合法的 IP 地址，暂不支持 IPv6 地址。 ■ 目标端口：请输入 1~65535 之间的端口。 ● Kafka 转发方式： ■ IP：请输入合法的 IP 地址，暂不支持 IPv6 地址。 ■ 端口：请输入 1~65535 之间的端口。 ■ 发送 Topic：Kafka 的 Topic。 ■ 协议：支持 PLANINTEXT 和 SSL/TLS 协议。 若选择 SSL/TLS 协议，还需要配置如下参数： ◆ Keystore 文件：仅支持上传.jks 类型文件。 ◆ Keystore.Password：请输入正确的 Keystore 认证密码。 ◆ Key.Password：请输入正确的 Key 认证密码。 ◆ Truststore 文件：仅支持上传.jks 类型文件。

参数	说明
	◆ Truststore.Password：请输入正确的 Truststore 认证密码。

日志格式说明

业务日志

外发采集到的日志原文，请前往日志源服务查看日志说明。

告警日志

日志示例：

{ "from_ana_single": { "alarm_name": "新增账号告警", "alert_source": "9", "alarm_level": "1", "merge_way": "1,4", "alert_type": "180", "alert_type_sub": "1802", "attack_stage": "4", "protocol": "", "alert_count": "1", "rule_id": "9", "reliability": "80", "success_tag": "1", "src_ip": "", "src_port": "0", "dst_ip": "192.168.101.3", "dst_port": "0", "signature": "", "cve_id": "", "file_name": "", "file_path": "", "file_md5": "", "url": "", "cookie": "", "user_name": "test", "process_name": "", "mail_from": "", "mail_to": "", "src_zone": "", "dst_zone": "", "status_tag": "0", "rectification": "", "index_name": "", "occur_time": "2025-08-05 11:12:35", "update_time": "2025-08-05 11:12:35", "description": "新增账号告警", "event_type_count": "1", "event_count": "1", "vul_id": "", "componentId": "1", "user_group": "", "domain": "", "class_dga": "", "attack_result": "", "is_white": "", "attack_type": "", "payload": "", "attack_main_type": "" } }

日志字段说明：

日志字段	说明
alarm_name	告警名称
alarm_level	告警等级 ● 1：轻微 ● 2：低级 ● 3：中级 ● 4：高级 ● 5：严重
alert_source	告警来源
merge_way	归并方式
alert_type	告警类型
alert_type_sub	告警小类
attack_stage	攻击链阶段

日志字段	说明
protocol	协议
alert_count	告警次数
rule_id	告警规则 ID
reliability	可信度。取值范围 0-100，数字越大，代表可信度越高。
success_tag	攻击是否成功 ● 1：是 ● 0：否 ● 2：未知
src_ip	源 IP
src_port	源端口
dst_ip	目的 IP
dst_port	目的端口
signature	特征码
cve_id	CVEID
file_name	文件名
file_path	文件路径
file_md5	文件 MD5
url	URL
cookie	Cookie
user_name	登录用户名
process_name	进程名称
mail_from	发件人地址
mail_to	收件人地址
src_zone	源域
dst_zone	目的域
status_tag	告警的状态 ● 0：待处理 ● 1：已指派 ● 2：已确认 ● 3：已处理 ● 4：已清除

日志字段	说明
	● 5：已忽略
rectification	整改建议
index_name	索引名称
occur_time	发生时间
update_time	更新时间
description	规则描述
event_type_count	事件类型数量
event_count	事件次数
vul_id	漏洞 ID
componentId	组件 ID
user_group	用户组
domain	域名
class_dga	dga 域名
attack_result	攻击结果
is_white	是否白名单
attack_type	攻击类型
payload	payload
attack_main_type	攻击主类型

操作日志

日志示例：

{"LOG_ID":"389","MODULE_NAME":"首页模块管理","OPERATION_CONTENT":"查询首页模块","OPERATION_TYPE":"sys","SUCCESS_TAG":"1","IP_ADDRESS":"10.144.243.22, 100.126.9.148","VALID_TAG":"","USER_ID":"1","CREATE_TIME":"2025-08-14 16:33:20","REQUEST_PARAM":"请求路径=/homePage/realTimeAlarm; beanName=com.soc.cloud.homepage.controller.HomePageController; IP 地址=10.144.243.22, 100.126.9.148; 方法名=getRealTimeAlarm","REVIEWER":""}

日志字段说明：

日志字段	说明
LOG_ID	日志 ID
MODULE_NAME	操作模块名称
OPERATION_CONTENT	操作内容
OPERATION_TYPE	操作类型
SUCCESS_TAG	是否成功 0：否 1：是
IP_ADDRESS	来源 IP 地址
USER_ID	操作用户
CREATE_TIME	操作时间

4.10 使用云监控服务监控日志审计实例

4.10.1 查看监控数据

为保证日志审计实例的可靠性、可用性和可观测性，对日志审计进行监控已经成为一种必要且重要的手段。天翼云控制平台提供的日志审计监控功能，可方便用户更快、更直观的了解日志审计的运行情况、使用情况及其他性能指标，同时可根据实时监控情况，执行告警通知等操作，帮助客户更好的管理日志审计实例。

当用户开通日志审计（原生版）服务后，即可通过云监控来查看监控指标。

> **说明**：
>
> **目前仅支持监控“一类节点”区域的实例。**日志审计（原生版）支持的区域请参见“支持的区域。”

实例支持的监控指标

监控指标	指标说明	单位	是否支持告警	监控周期
CPU 利用率	该指标用于统计日志审计实例的 CPU 利用率。	%	是	5 分钟
内存总大小	该指标用于统计日志审计实例的实际内存大小。	GB	是	5 分钟

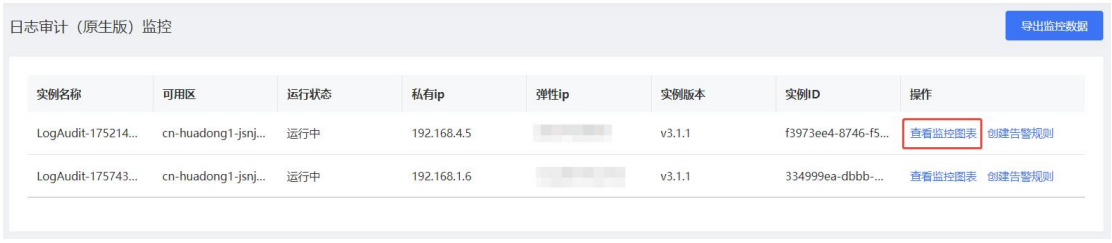
监控指标	指标说明	单位	是否支持告警	监控周期
剩余内存大小	该指标用于统计日志审计实例的空闲的内存大小。	GB	是	5 分钟
内存利用率	该指标用于统计日志审计实例的内存利用率。 内存利用率 = 100% - （剩余内存大小/内存总大小）	%	是	5 分钟
系统盘大小	该指标用于统计日志审计实例的实际系统盘大小。	GB	是	5 分钟
剩余系统盘大小	该指标用于统计日志审计实例的空闲的系统盘大小。	GB	是	5 分钟
系统盘利用率	该指标用于统计日志审计实例的系统盘利用率。 系统盘利用率 = 100% - （剩余系统盘大小/系统盘大小）	%	是	5 分钟
数据盘大小	该指标用于统计日志审计实例的实际数据盘大小。	GB	是	5 分钟
剩余数据盘大小	该指标用于统计日志审计实例的空闲的数据盘大小。	GB	是	5 分钟
数据盘利用率	该指标用于统计日志审计实例的数据盘利用率。 系统盘利用率 = 100% - （剩余数据盘大小/数据盘大小）	%	是	5 分钟

查看监控图表

1. 登录天翼云控制中心。
2. 在产品服务列表中“管理与部署 > 云监控服务”，进入云监控服务主页面。
3. 在左侧导航栏，选择“云服务监控”，单击“日志审计（原生版）”产品。

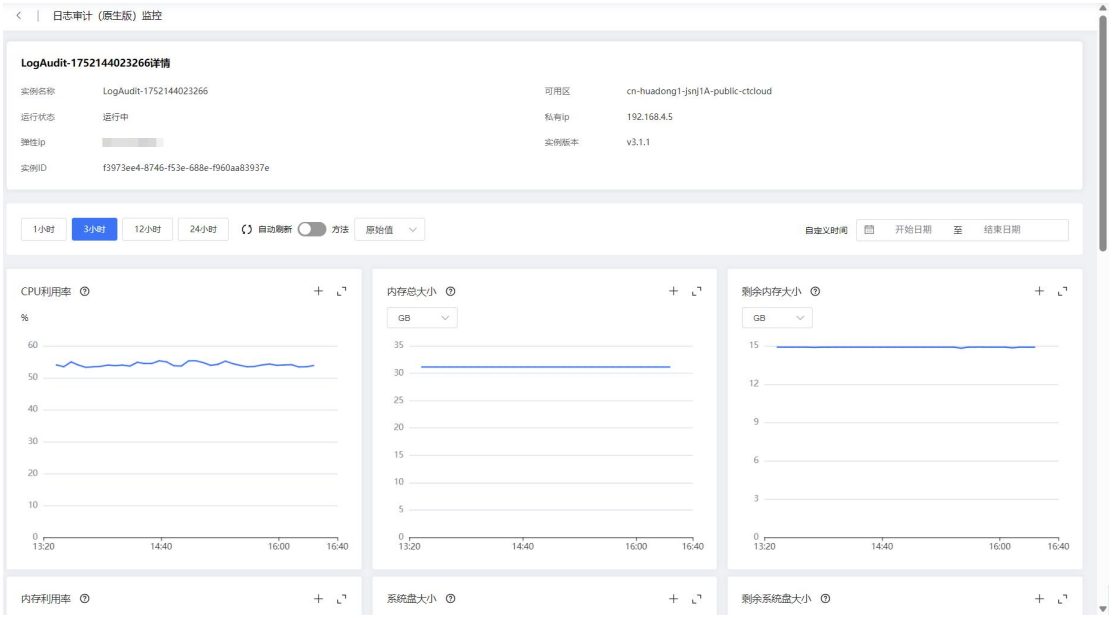
4. 在日志审计（原生版）监控列表中选择目标的实例，单击操作列的“查看监控图表”，进入监控详情

页。



5. 在监控详情页，可以查看实例详情和监控图表。

6. 切换不同的时间周期，查看不同周期内监控指标的情况。



4.10.2 创建告警监控规则

云监控支持灵活的创建告警规则。您既可以根据实际需要对某个监控指标设置自定义告警规则，同时也能够使用告警模板为多个资源或者云服务批量创建告警规则。

> **说明**：
>
> **目前仅支持监控“一类节点”区域的实例。**日志审计（原生版）支持的区域请参见“支持的区域。”

操作步骤

1. 登录天翼云控制中心。

2. 在产品服务列表中“管理与部署 > 云监控服务”，进入云监控服务主页面。

3. 在左侧导航栏，选择“云服务监控”，单击“日志审计（原生版）”产品。

4. 在日志审计（原生版）监控列表中选择目标的实例，单击操作列的“创建告警规则”。

5. 在“创建告警规则”页面，根据界面提示配置参数。

配置参数及相关含义说明如下：

模块	参数	参数说明	配置示例
选择监控对象	规则类型	选择规则的类型，主要包括指标监控、事件监控、站点监控、自定义监控、自定义事件五种。	指标监控
	服务	配置告警规则监控的云服务资源类型。	日志审计（原生版）
	维度	用于指定告警规则对应指标的维度名称。	日志审计实例
	监控对象类型	具体实例/资源分组/全部资源	具体实例
	监控对象	用来配置该告警规则针对的具体资源，可以是一个或多个。	实例名称
定义告警策略	选择类型	支持**自定义创建**、**从模板导入**。	自定义创建
	策略	支持选择满足全部或任意策略。	满足全部以下条件：若 CPU 利

模块	参数	参数说明	配置示例
		策略信息包括： ● 监控指标，支持的监控指标请参见“实例支持的监控指标”。 ● 数据类型（原始值） ● 判断条件（>、≥、<、≤、=、环比上升、环比下降、环比变化） ● 值 ● 单位 ● 发生次数 ● 级别（普通、警示、紧急） **说明**： 同一告警规则，告警条件最多支持添加 20 条。	用率的原始值>=80%，连续发生 1 次，普通
	无数据处理	不做处理/视为告警/视为恢复。	不做处理
配置告警通知	发送通知	配置是否发送邮件通知用户，可以选择开启 （推荐选择）或者关闭。	开启
	通知方式	仅支持“通知联系人组”。	通知联系人组
	告警联系组	选择发生告警通知时通知的用户组。支持选择联系组或者云账户默认联系人。	-
	触发场景	触发告警邮件的场景，可在出现告警和告警恢复时发送提醒信息。	出现告警
	通知渠道	配置告警通知的通知渠道，支持邮箱、短信、语音（语音需要单独订购）。	邮箱
	重复告警	指告警发生后如果未恢复正常，将重复发送告警通知次数。	不重复
	通知频率	指告警发生后如果未恢复正常，间隔多久重复发送一次告警通知。 若重复告警选择“不重复”时，无需配置该参数。	每 24 小时通知一次
	通知周期	配置告警通知的周期时间。	星期天、星期一、星期二、星期三、星期四、星期五、星期六
	通知时段	配置告警通知的时间段。	00:00:00-23:59:59
	告警回调	配置告警通知 webhook 地址。	-
	通知模板	告警信息默认使用系统模板；也可以选择用户自定义创建的通知模板，自定义模板详细操作请参见	系统模板

模块	参数	参数说明	配置示例
		“创建自定义告警模板”。	
规则信息	名称	该告警规则的自定义名称。	evs-alarm-note
	企业项目	选择告警规则适用的企业项目。	default
	描述	添加对该告警规则描述。	-

6. 配置完成后，单击“确定”完成操作。

   告警规则添加完成后，当监控指标触发设定的阈值时，云监控会在第一时间通过邮件实时告知您云上资源异常，以免因此造成业务损失。关于云监控的其他操作和更多信息，请参考《云监控服务》。

5 最佳实践

通过本章，我们可以了解管理员的基本功能，以及给用户创建账号并授权的基本流程。管理员的基础功能包括“管理账号”、“管理资产”、“管理授权”以及“查看审计”。

5.1 程序定位采集日志异常

应用场景

有产生日志，但日志审计（原生版）平台未看到该日志，如何定位问题。

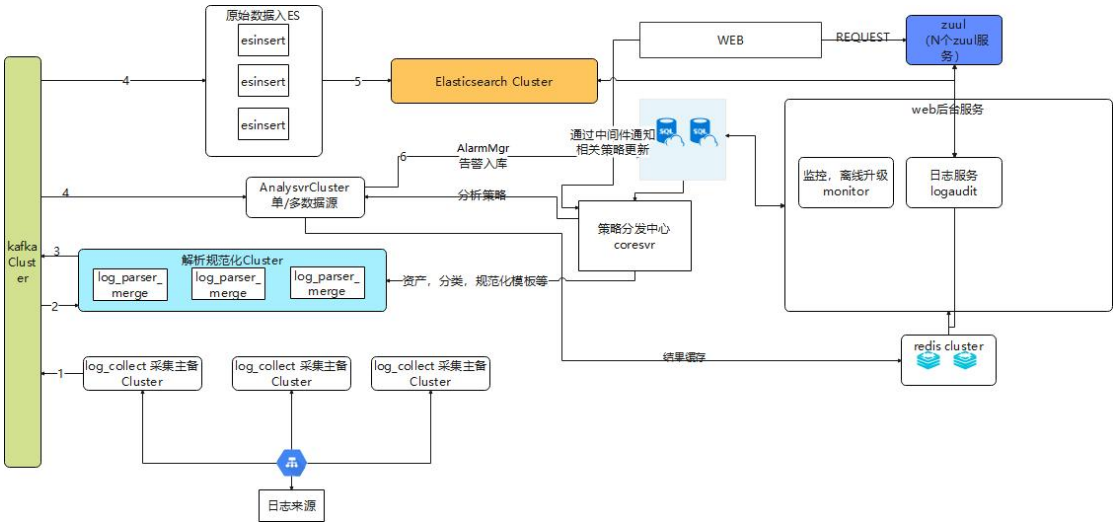
前提准备

通过控制台进入日志审计（原生版）实例。

日志采集涉及服务逻辑

日志采集涉及服务：log_c、logp、coresvr、esinset。

日志采集涉及流程：



Log_c（日志采集）接收日志并通过 kafka 将接收的日志转发 log_p。

Log_p（日志解析分类）接收 log_c 转发的原始日志根据解析规则等进行解析，并通过 kafka 将解析后的日志发送给 esinsert。

Esinsert（录入 elasticsearch）将解析后的日志录入 elasticsearch。

Coresvr（页面更新程序）将页面下发的规则等变更，通过 kafka 下发给对应的服务。

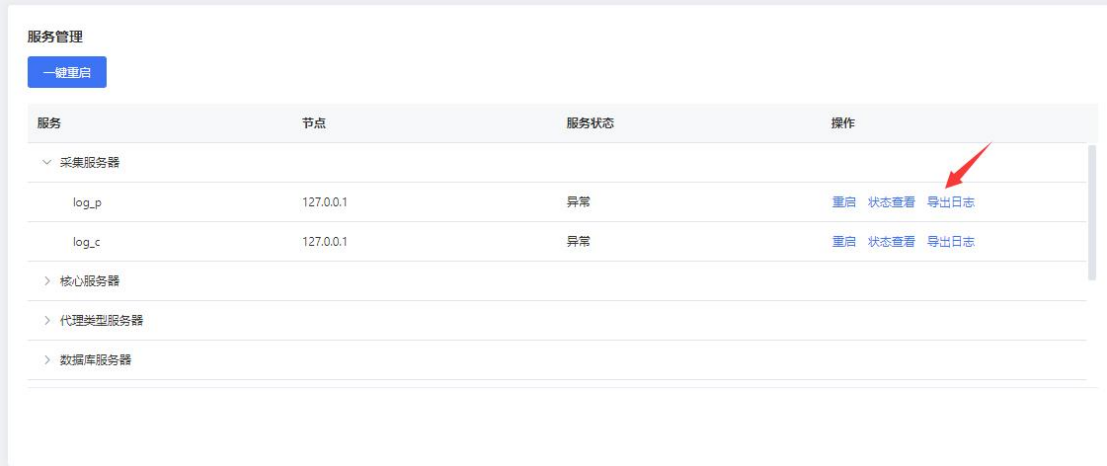
查看程序

点击“系统配置”>“系统运维”,在服务管理中，点击导出日志，可导出服务日志。将 log_c、logp、coresvr、esinsert 等服务日志按流程步骤依次查看是否有异常信息。

查看程序日志

点击“系统配置”>“系统运维”,在服务管理中，点击导出日志，可导出服务日志。将 log_c、logp、coresvr、

esinsert 等服务日志按流程步骤依次查看是否有异常信息。



Logc 的服务日志报错

Logc 的服务日志出现如下报错：2023-07-26 10:10:27 src/LogMgr.cpp:694 "handle log but can not find asset by ip 192.168.121.35"

日志分析：平台页面未存在 ip 为 192.168.121.35 的资产。点击菜单“资产”>"资产管理"，在查询栏查询资产 ip 为 192.168.121.35，若未查询到该资产，则新增一条。新增后，再次查看 logc 日志。

注意：

新增的资产，采集方式、资产类型、资产 ip 都要按实际情况填写。

中间件故障

各程序报告日志出现如下报错：

Broker transport failure: 127.0.0.1:9092/0: Connect to ipv4#127.0.0.1:9092 failed。

日志分析：9092 为 kafka 服务端口，该提示为 kafka 出现异常。

5.2 程序日志定位告警异常

应用场景

日志审计（原生版）已经采集到日志，但未触发对应告警。

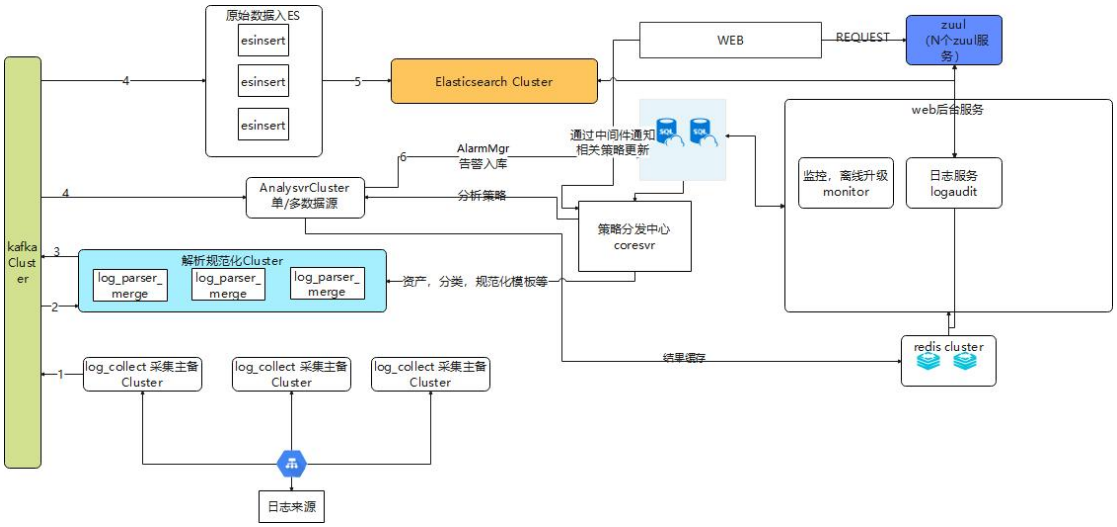
前提准备

进入日志审计（原生版）平台。

告警服务逻辑

告警涉及服务：esinsert、alarmMgr、event_analysvr。

告警涉及流程：



event_ana（告警解析）：通过 kafka 接收 logp 解析的日志，根据告警规则解析该日志是否符合告警条件，符合条件则将该告警信息转发给 alarm。

alarm：通过 kafka 接收 event_ana 的告警信息，并触发告警，产生告警。

esinsert（录入 elasticsearch）将产生的告警录入 elasticsearch。

查看程序

点击“系统配置”>“系统运维”,在服务管理中，查看相关服务状态，出现异常时，点击重启程序，过 1min，刷新页面，查看服务状态是否正常。

查看程序日志

点击“系统配置”>“系统运维”,在服务管理中,点击导出日志,可导出服务日志。将 esinsert、alarmMgr、event_analysvr 等服务日志按流程步骤依次查看是否有异常信息。

中间件故障

各程序报告日志出现如下报错：Broker transport failure: 127.0.0.1:9092/0: Connect to ipv4#127.0.0.1:9092 failed。

日志分析，9092 为 kafka 服务端口，该提示为 kafka 出现异常。

eventana 服务故障

例如下打印：src/LogDispatcher.cpp:45"recevice log event count = 9412"。

日志分析，出现 count 表示有正常接收到解析后的日志，若没有该打印日志，确定对应日志是否采集到日志审计（原生版）平台。可通过“事件分析”>“日志检索”中查询。

6 常见问题

6.1 介绍类

日志审计（原生版）是什么?

- 日志审计（原生版）系统能够实时不间断地采集汇聚企业中不同厂商不同种类的安全设备、网络设备、主机、操作系统、用户业务系统的日志信息，协助用户进行安全分析及合规审计，及时、有效的发现异常安全事件及违规事件。
- 系统提供了众多基于日志分析的强大功能，如安全日志的集中采集、分析挖掘、合规审计、实时监控及安全告警等，系统配备了全球 IP 归属及地理位置信息数据，为安全事件的分析、溯源提供了有力支撑，综合日志审计分析系统能够同时满足企业实际运维分析需求及审计合规需求，是企业日常信息安全工作的重要支撑平台。

日志审计（原生版）市场需求有哪些?

日志审计需求主要源自于两个方面的驱动力：

- 一方面，从企业和组织自身安全的需要出发，日志审计能够帮助用户获悉信息系统的安全运行状态，识别针对信息系统的攻击和入侵，以及来自内部的违规和信息泄露，能够为事后的问题分析和调查取证提供必要的信息；
- 另一方面，从国家法律法规、行业标准和规范的角度出发，日志审计已经成为了满足合规与内控需求

的必备功能。

日志审计（原生版）适用范畴?

日志审计（原生版）系统提供了众多基于日志分析功能，系统具有广泛的应用范围和客户群，在政府、企业、电信、金融、电力、公安、军工、等行业均有成功的应用，满足企业实际运维分析需求及审计合规需求，是企业日常信息安全工作的重要支撑平台。

日志审计（原生版）有哪些核心功能和能力?

- 支持各类厂商多源异构的数据统一采集，进行支持正则表达式、分隔符，Key-Value、JSON 日志解析解析，分类，过滤归并等操作，进行规范化成统一的结构化数据。
- 支持全文检索，条件检索对所有原始日志内容进行即时在线查询，多条件嵌套逻辑查询，收敛事件范围和事件时候溯源审计。依托大数据底层存储，支持查询结果秒级响应。
- 支持用户交互式检索审计，并通过柱状图、饼图、折线图、面积图、堆积图、环状图、数值图、地图等形式的统计信息可视化展示，并可将统计结果保存为仪表板和报表。
- 支持多事件的序列关系，逻辑关系，字段条件逻辑判断等配置，进行实时流的审计分析，关联分析，产生异常审计告警，并实时通知用户处置。
- 支持对系统中预置报表模板选择生产的时间进行预览、生成报表。支持在报表中以柱状图、曲线图、饼状图方式统计安全报警情况；报表格式支持 PDF、Word 等。

日志审计（原生版）有哪些应用场景?

- 采用日志审计监测、记录和存储网络运行状态和安全事件等信息，实现对系统的全面监控和细致记录，配合多种审计策略，快速定位溯源，全面提升系统服务水平以及网络安全管理水平，满足网络安全法规及等级保护的相关要求。
- 针对中大型企业设备多，系统多，难以统一监管问题，采用日志审计将所有设备、用户行为日志统一监管，贯穿从边界到核心资产的全流程，扩展对关键数据等资产的保护。

- 通过对多个不同来源的日志数据进行关联和分析，揭示隐藏在数据背后的模式和趋势，帮助企业识别异常行为和潜在威胁。在当前复杂多变的网络环境中，日志关联分析已经成为了保障网络安全和信息安全的一项重要技术手段。

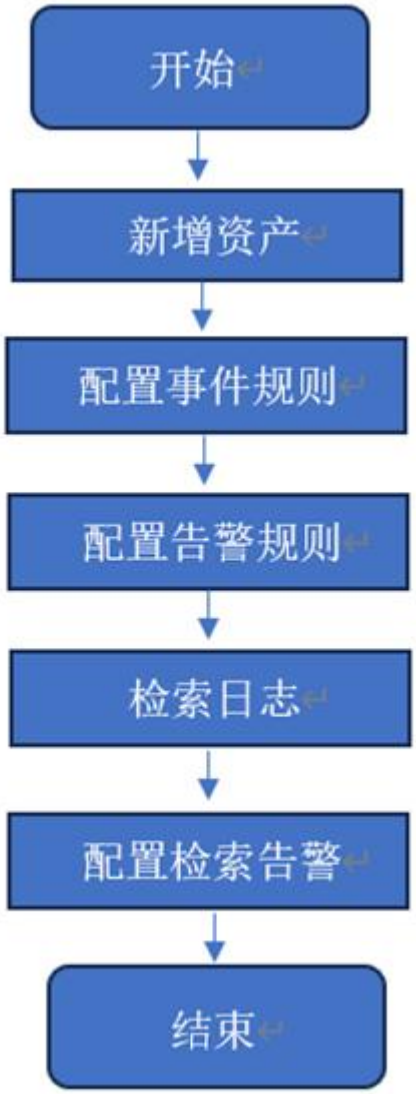
6.2 功能类

日志审计（原生版）采用何种接入方案?

- windows 设备通过 agent 采集，优点在于能够快速地集成现有数据，形成数据能力。
- 其他设备通过 syslog 采集 snmptrap 方式采集，优点在于不侵入应用系统，相关数据的准备由数据源系统自行准备，有利于数据源系统开展数据责任授权及控制扩散范围。

日志审计（原生版）采集日志需要做哪些操作?

进入日志审计后，您需要先配置采集资产，针对采集日志样式进行配置，以及配置对应告警规则。配置完成后，触发日志，可在平台中检索采集到的日志和告警结果。涉及配置流程如下：



日志审计（原生版）如何实现自适应采集解析能力?

通过数据自适应，将采集到多种类型、多种格式的原始事件信息根据预先配置的解析规则进行解析，支持正则解析，分隔符解析，json 解析，key-value 形式解析，实现新增日志类型无需开发能力。且日志解析结果已内置支持 80+个字段，并支持动态扩展。

日志审计（原生版）如何实现检索分析?

检索分析功能底层基于 elasticsearch 索引支持检索功能，为用户提供日志检索及分析能力，支持字段高级逻辑搜索和全文检索，提供丰富的字段用于索引、检索，字段可由用户自定义添加配置，可支持用户自定义时间范围内检索数据，并支持对检索数据进行导出。

6.3 操作类

6.3.1 如何进行实时图表分析？

问题描述

日志审计（原生版）如何进行实时图表分析?

解决方案

点击菜单“事件分析”>日志检索，进入检索界面。通过事件检索模块，事件统计功能，选择对应的图表以及事件字段属性进行实时图表生成。

- 在查询框中输入想要查看的日志，建议使用 csl 查询，选择查询时间，点击 ，页面展示筛选后的日志信息。
- 点击“事件列表”tab，通过列表的方式展示日志，对日志进行分析。
- 点击事件统计，同样可以根据 csl 查询日志结果，并且选择不同的图表类型，展示字段，更能直观看到日志数据情况。其中支持折线图、面积图、柱形图、横向柱形图、饼形、环状图、地图、散点图、数值图。

6.3.2 采集 snmptrap 日志需要在哪配置？

问题描述

发送 snmptrap 日志，发现 snmp 日志未采集到日志审计（原生版）平台上。

可能原因

- nmp 资产未添加或添加错误
- Mib 文件上传错误
- Snmptrap 配置未配置或配置错误

解决方法

检查 snmp 资产

1.在菜单“资产 > 资产管理”中，选择资产组，点击新增 snmptrap 资产。

2.点击“查看”按钮。检查 snmptrap 资产的资产大类、资产小类、资产 ip 是否正确。

检查 MIB 文件

1.在菜单“系统配置”>“采集管理”>“MIB 文件管理”中，上传 mib 文件。

2.点击“查看”按钮，检查 mib 文件上传是否正确。

6.3.3 如何排查日志未采集？

问题描述

日志审计（原生版）采集日志配置配好后，仍未采集到日志，如何排查?

可能原因

- 采集日志相关程序未正常启动。
- 中间件出现故障。
- 采集资产未配置。

解决方案

了解采集日志程序的作用

- Log_c（日志采集）接收日志并通过 kafka 将接收的日志转发 log_p。
- Log_p（日志解析分类）接收 log_c 转发的原始日志根据解析规则等进行解析，并通过 kafka 将解析后的日志发送给 esinsert。
- Esinsert（录入 elasticsearch）将解析后的日志录入 elasticsearch。
- Coresvr（页面更新程序）将页面下发的规则等变更，通过 kafka 下发给对应的服务。

查看程序是否启动

点击“系统配置”>“系统运维”,在服务管理中,查看相关服务状态,出现异常时,点击重启程序,过 1min,刷新页面，查看服务状态是否正常。

查看程序日志

点击“系统配置”>“系统运维”,在服务管理中，点击导出日志，可导出服务日志。将 log_c、log_p、coresvr、esinsert 等服务日志按流程步骤依次查看是否有异常信息。

中间件故障

各程序报告日志出现如下报错：Broker transport failure: 127.0.0.1:9092/0:Connect to ipv4#127.0.0.1:9092 failed。

日志分析，9092 为 kafka 服务端口，该提示为 kafka 出现异常。

6.4 故障类

登录报错：当前实例无法访问，请检查是否在安全组开放端口 8181

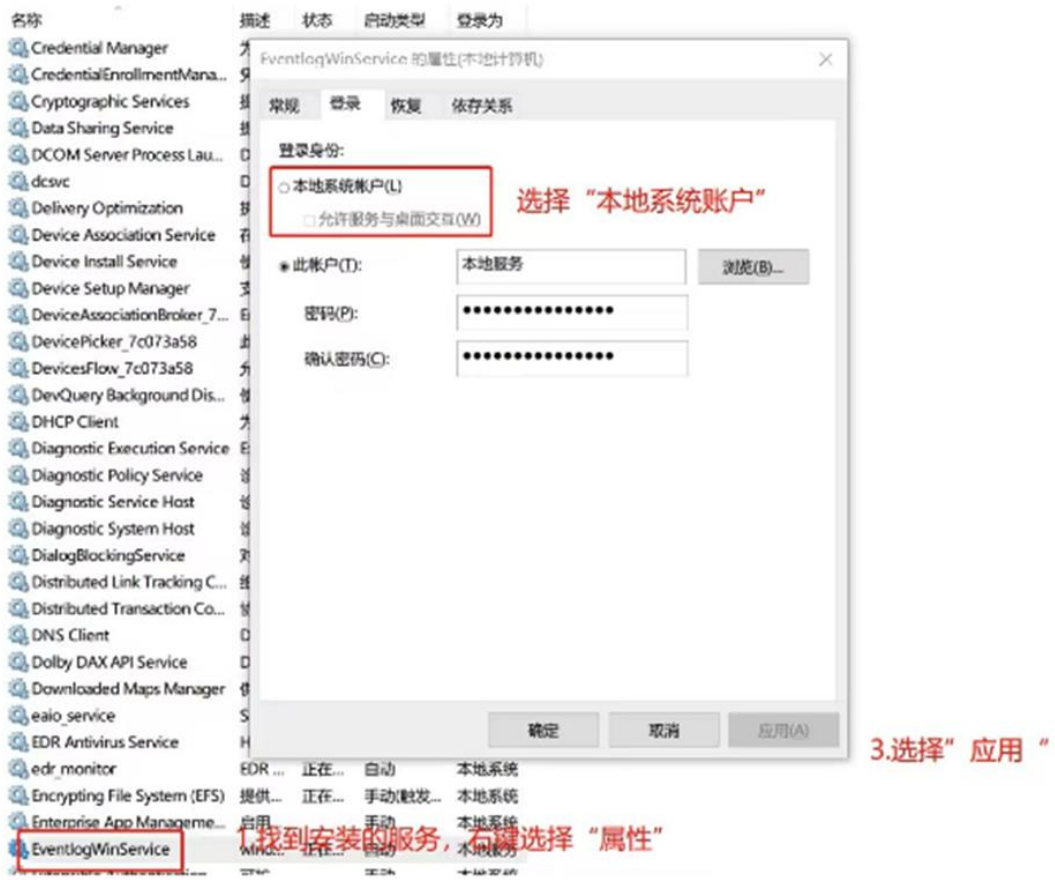
问题现象：登录和日志审计实例相同 vpc 的机器 telnet 8181 端口可以连通，说明日志审计实例已启动完毕、状态正常。

解决方法：通过浏览器开发工具获取登录地址，手动替换地址中的 ip 地址后在浏览器中访问。

安装 Windows 采集代理服务后服务启动报错

问题现象：安装 Windows 采集服务后，日志审计（原生版）服务启动报错

解决方法：请按照下图修改配置。



Linux 配置脚本报错怎么解决?

问题现象：Linux 采集脚本执行报错，无法正常执行。

解决方案：重新 rsyslog 的配置文件后重启服务。

操作步骤：

1.linux 主机配置日志审计流程：

使用以下指令打开/etc/rsyslog.conf 文件

vi /etc/rsyslog.conf

2.在 ryslog 文件末尾添加以下内容：

***.* @192.168.x.x**

说明： “*.*”表示所有级别的日志都发给日志审计，IP 地址填写日志审计的服务器 IP 地址。

3.重启 rsyslog 服务

Cenots7 后的重启命令：**systemctl restart rsyslog.service**

Centos6 前的重启命令：**service rsyslog restart**

4.配置完成后，请查看日志检索否显示出日志的 IP 信息。

若没有收到查看到日志源 IP，请查看端口开放建议，配置完成后，需重新按照步骤 3 的操作重启 rsyslog 服务。

6.5 等保类

密码安全相关

密码复杂度策略：密码必须含有“小写字母”、“大写字母”、“数字”、“特殊符号”中的任意三种(长度至少为 8 位，最大 16 位，特殊字符支持：`~!@#$^&*()|{}:;,.<>?)。

密码定期更换策略：密码若 90 天未修改，登录后系统会强制要求修改密码。

登录安全相关

登录超时自动退出时间：若用户 30 分钟未进行任何操作，则该用户会自动登出。

登录失败处理策略：同一个 IP 使用使用不存在的用户名连续登录 5 次，限制该 IP 登录 10 分钟。

密码若连续三次输入错误，该用户会被锁定。

存储内容相关

鉴别数据、审计数据、配置数加密存储方式：审计鉴别数据存 ES，配置的数据存放 mysql 数据库，涉及到敏感信息如密码会进行加密存储。

日志存储时限：最高可存储 180 天，可根据业务需求进行修改。