日志审计（原生版）

用户操作指南

天翼云科技有限公司

目录

1 产品概述

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。

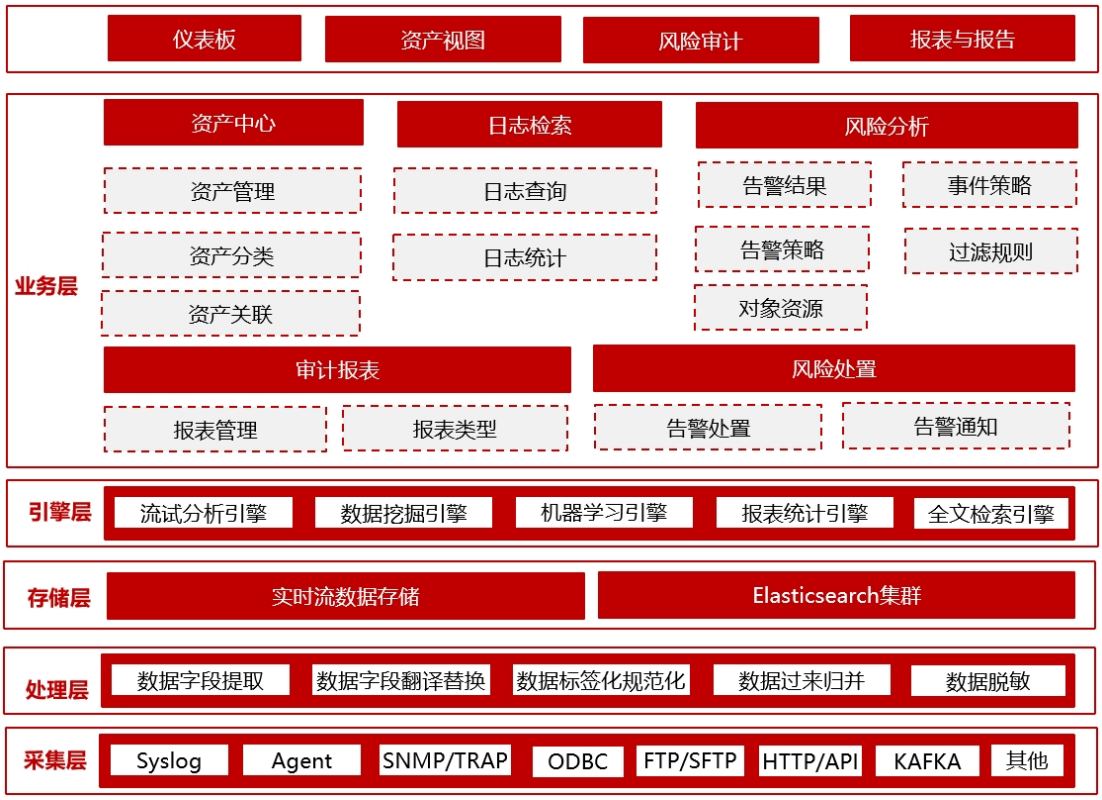
处理层：实现对采集到的数据做统一规范化，对数据进行关键信息提取，标签化分类，过滤，归并等数据 ETL 操作，为后续的数据分析做准备。

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

设备类型
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
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

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 计费项

云堡垒机实例按选购的产品规格和购买时长计费。

计费项目	单位	计费说明	计费类型
资产数	个	按购买资产数计费，包含 5/10/15/20/50 五种规格类型	包周期

2.2 计费方式

计费方式

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。

标准版规格

日志审计（原生版）提供单机标准版，为您提供 5、10、15、20、50 资产数五种规格，您可以根据业务需求选择相应的版本规格。

资产规格	CPU	内存	系统盘	数据盘
5 个	8 核	32G	50G	256G
10 个	8 核	32G	50G	512G
15 个	8 核	32G	50G	1024G

20 个	16 核	64G	50G	2048G
50 个	16 核	64G	50G	4096G

产品价格

版本	规格	标准价格（元/月）	年付价格（元/年）	2 年付价格（元/年）	3 年付价格（元/年）
标准版	5（资源数）	1600	16320	28800	37440
标准版	10（资源数）	1750	17850	31500	40950
标准版	15（资源数）	2000	20400	36000	46800
标准版	20（资源数）	3400	34680	61200	79560
标准版	50（资源数）	4600	46920	82800	107640

2.3 购买方式

购买流程

操作步骤

注意：

- 仅支持重庆、兰州、上海 4、长沙 2、广州 4、福州 1、贵州 2、北京 2、石家庄、苏州、芜湖资源池。
- 上述资源池的日志审计服务需要通过创建弹性云主机开启，需自行前往购买弹性云主机。

1.登录管理控制台，单击左上角的，选择区域。

2.选择“计算 > 弹性云主机”，进入弹性云主机实例列表界面。

3.单击右上角的“创建弹性云主机”，进入“创建弹性云主机”页面。

说明

- 弹性云主机规格选择请参考：日志审计规格。
- 镜像选择“公共镜像 > 安全产品 > 日志审计（原生版）(40G)”

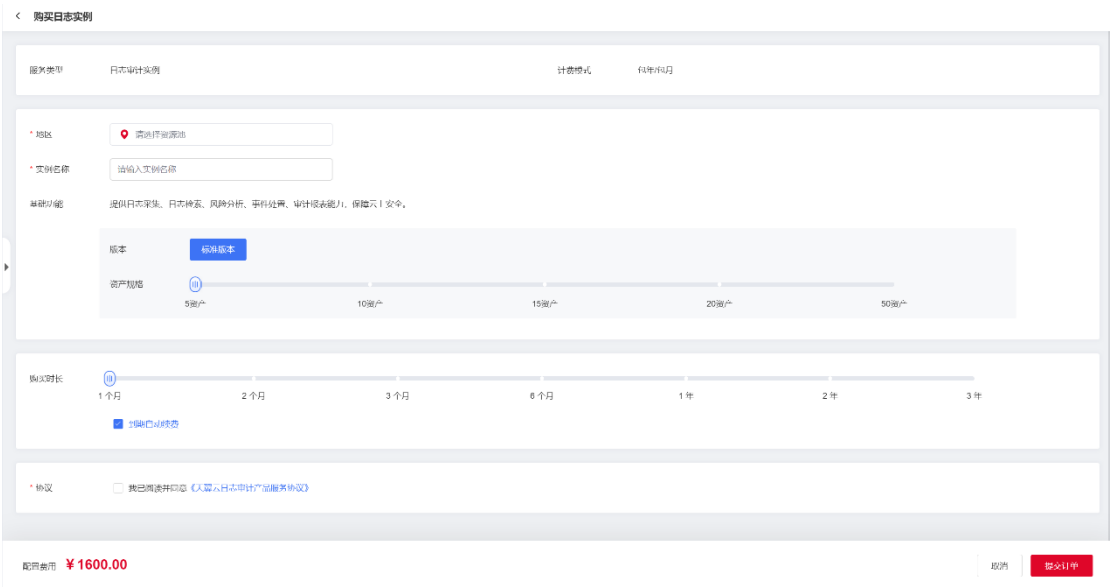
4.选择完规格后，单击“下一步：网络配置”进行网络配置。

注意：安全组规则需要放通“10443”端口，请您在选择安全组的时候注意是否已放通该端口。

5.完成网络配置后单击“下一步：高级配置”进行最后的配置，完成弹性云主机的配置。

6.弹性云主机购买成功后，需要 30 分钟左右进行机器启动、日志审计组件安装/启动。

7.进入日志审计（原生版）控制台，购买日志审计实例。



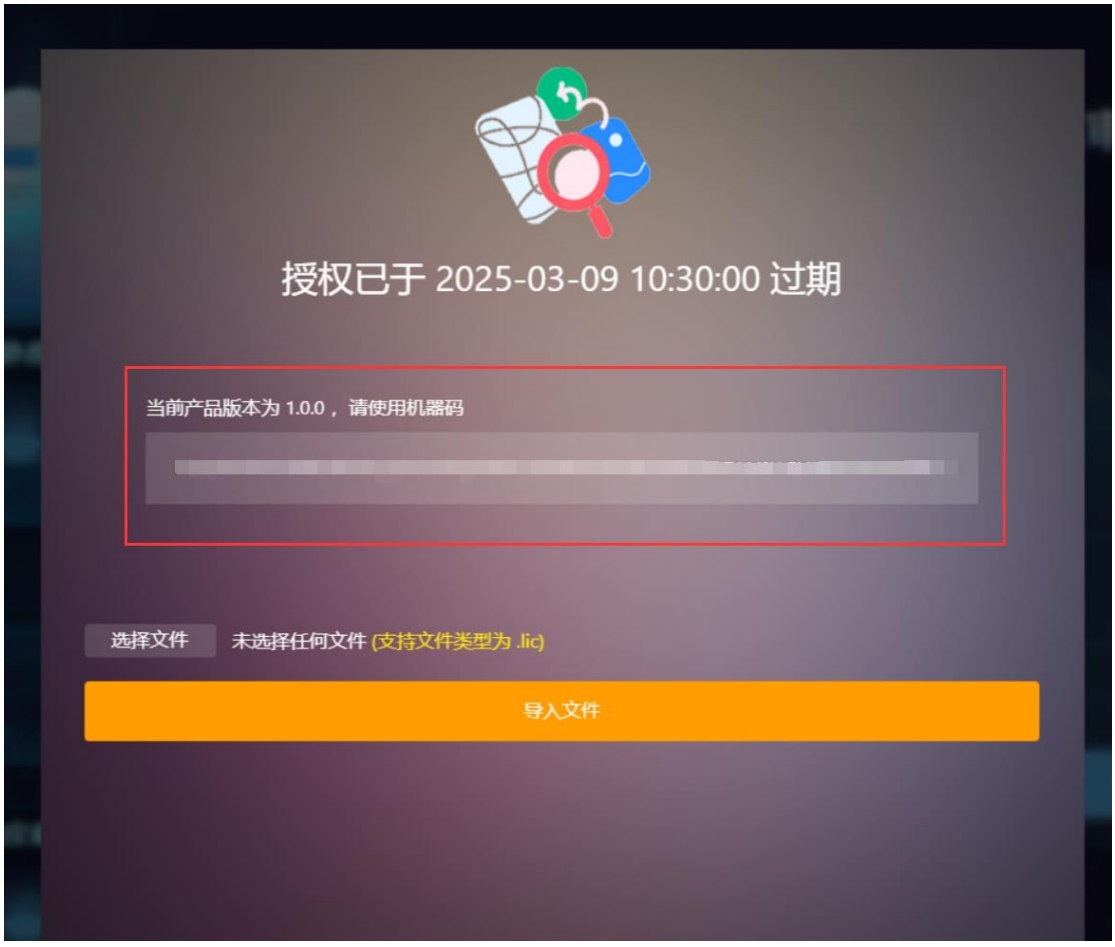
8.购买完成后，返回日志审计（原生版）控制台，在“操作”列单击“启用”，进入启用日志审计操作步骤。

9.在弹出的对话框中输入相关参数说明。

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。机器码获取请参见下文示例。
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“-”。

参数	参数说明
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：`~!@#$^&*()。
确认密码	二次确认本台日志审计服务器的管理员密码。密码长度限制：8-16 位，密码必须含有“小写字母”、“大写字母”、“数字”、“特殊符号”中的任意三种，特殊字符支持：`~!@#$^&*()。

机器码获取示例：



10.激活完成后即可登录日志审计服务器。

2.4 续费与退订

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

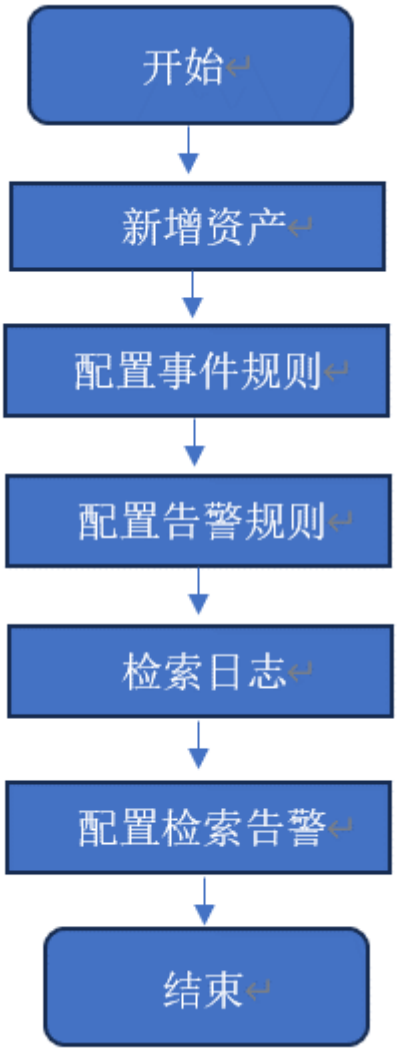
1. 登录管理控制台。
2. 选择“安全 > 日志审计（原生版）”，进入日志审计实例管理页面。
3. 选择待退订的实例，单击所在行“操作”列的“更多 > 退订”，弹出的退订实例对话框。
4. 确认实例信息无误后，单击“确定”。
5. 在退订资源页面完成退订。

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

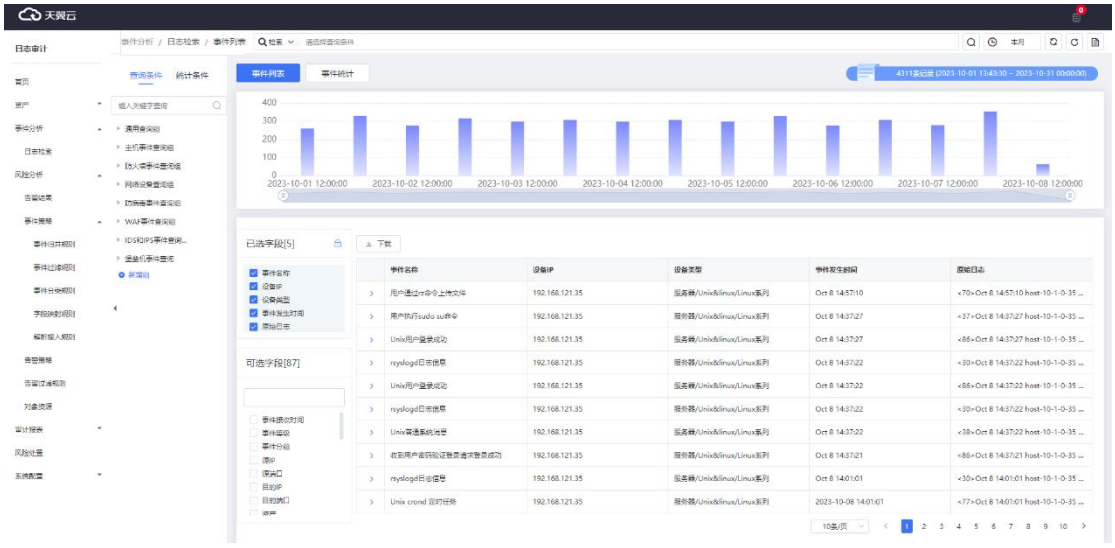
告警策略，对采集到的日志进行告警判断，符合告警策略的日志进行告警。选择“风险分析 > 告警策略” ，点击“新增规则”，填写告警条件。

配置告警过滤规则

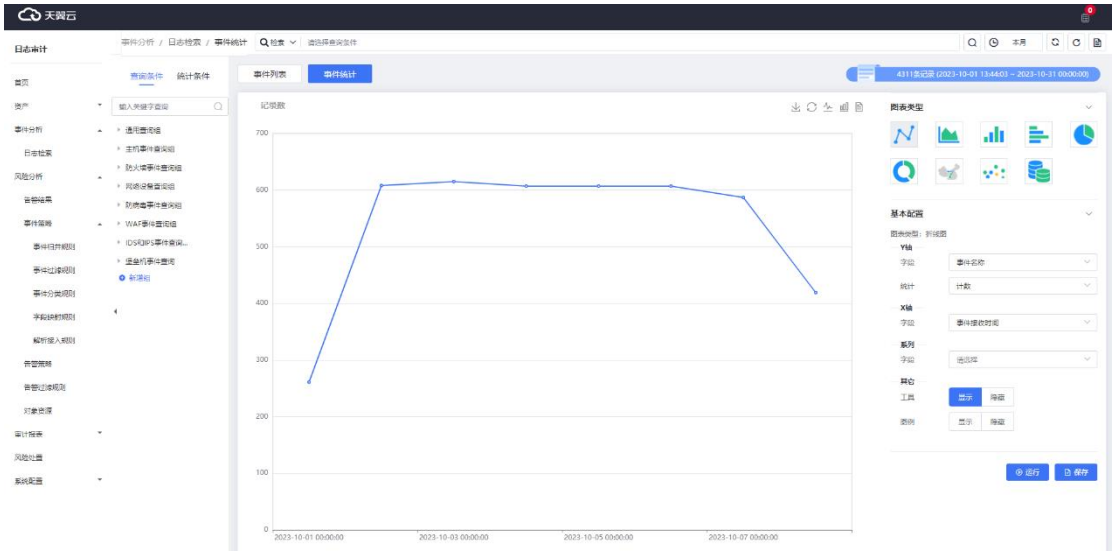
告警过滤规则，对符合告警规则的日志再进行一层过滤。选择“风险分析 > 告警过滤规则”，点击“新增”，填写告警过滤条件。

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。



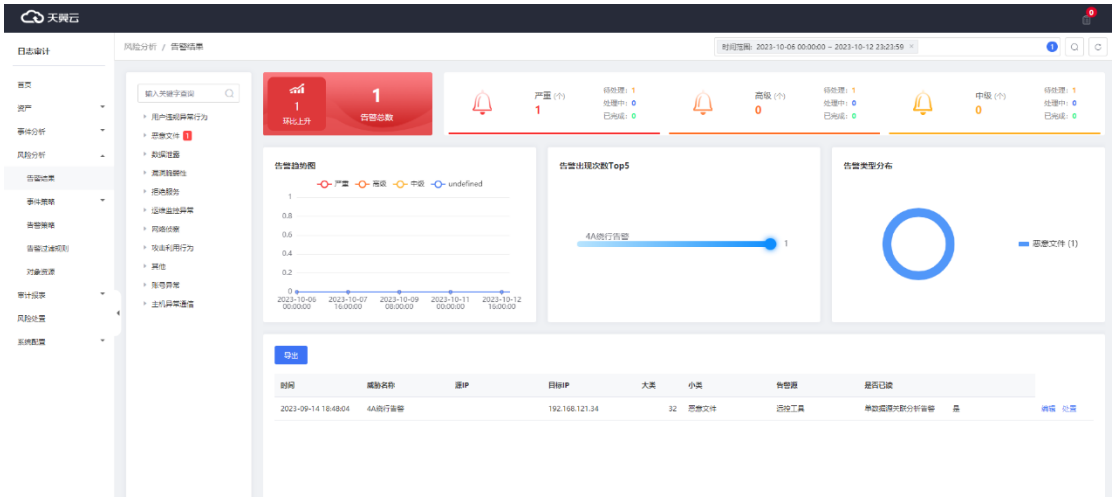
点击事件统计，同样可以根据 csl 查询日志结果，并且选择不同的图表类型，展示字段，更能直观看到日志数据情况。系统支持折线图、面积图、柱形图、横向柱形图、饼形、环状图、地图、散点图、数值图。



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）。



4 用户指南

4.1 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。

参数名称	填写说明
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。

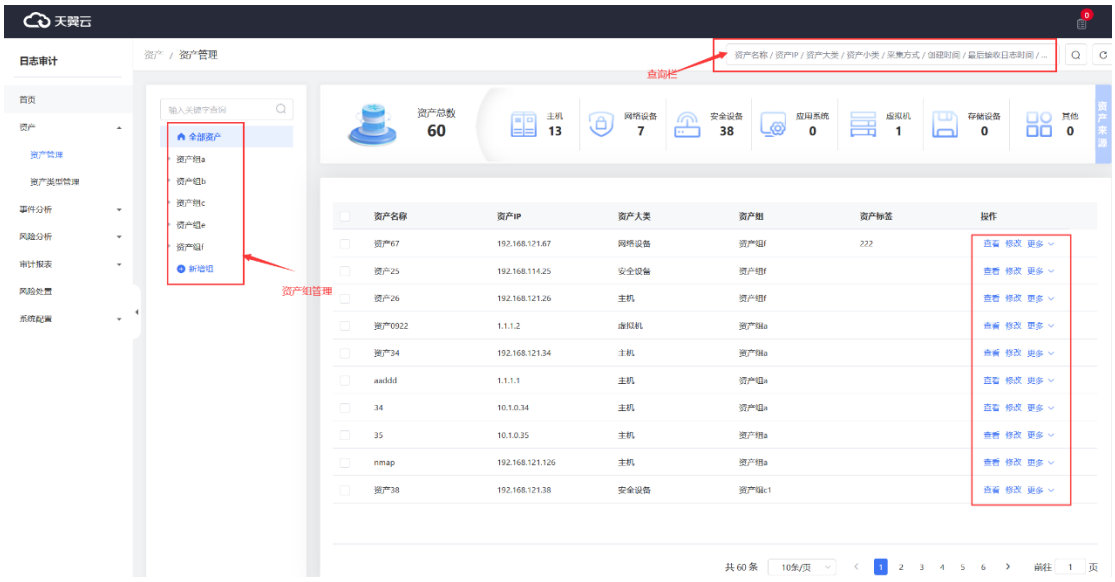
其中告警规则逻辑关系可选择 and、or、fb、rule。

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。

4.2 资产管理

资产管理是对需采集日志的设备管理，展示资产来源模块和资产列表。

单击“资产 > 资产管理”，对资产进行新增、删除、导入、编辑、 查看等操作。



- 新增组：新增资产组。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，单击“确定”后，页面添加完成。
- 新增：新增资产。选择资产组，点击“新增资产”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“，资产添加完成。
- 编辑：点击“编辑”按钮，弹出编辑界面，修改资产。
- 删除：点击资产的“删除“按钮，提示”确定删除当前项“，确定后，资产被删除。
- 导入：选择资产组，点击“导入数据”按钮，下载导入模板，按要求填写导入模板，上传文件后点击“提交”，资产批量新增。
- 查询：在查询栏中，填写需要查询的条件，点击“搜索”按钮，列表展示过滤后的资产。

4.3 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。

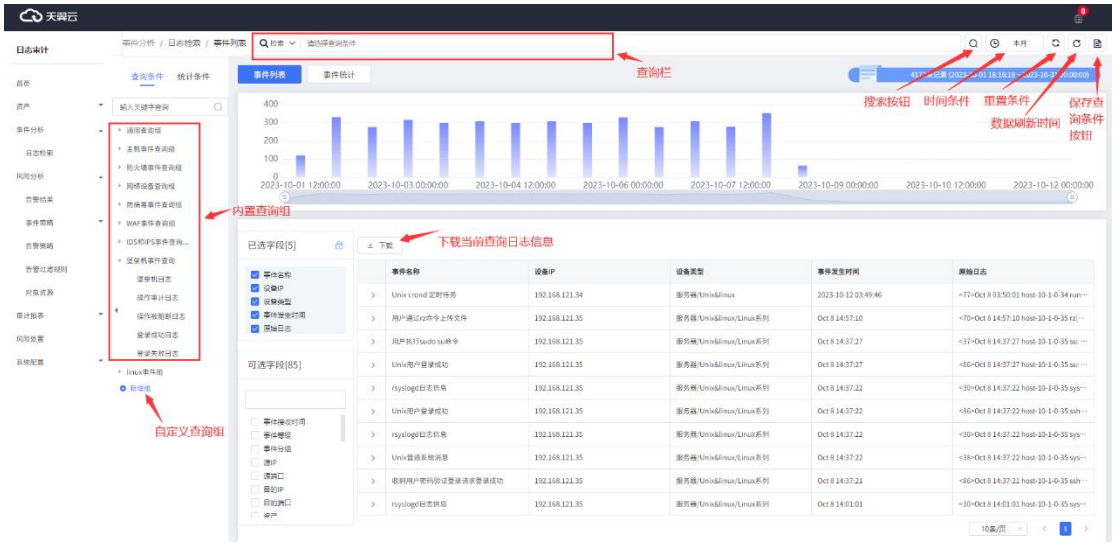
保存查询条件：点击“保存“按钮，选择是否另存，填写条件名称和条件分组等信息，将当前查询条件保存到左侧查询条件列中。下次直接点击该查询条件即可自动查询日志信息。

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。

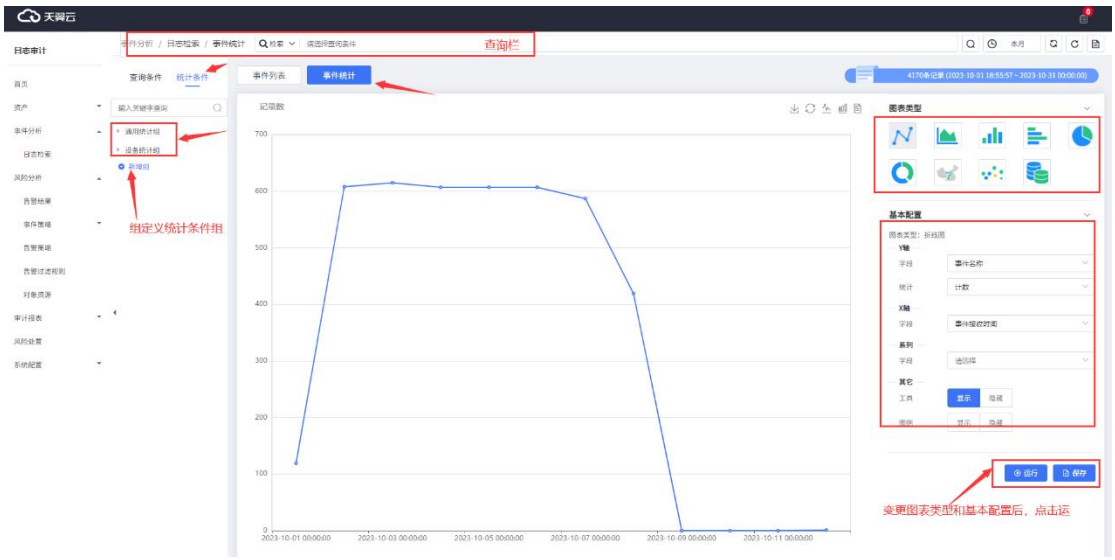
新增统计条件组：点击新增组，填写统计条件组名称和描述，点击“确定 “，可在左侧统计条件列中看到该统计条件组。或者，在”保存“按钮中，也可以通过条件分组下拉框中，点击” + “添加统计条件组。

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。

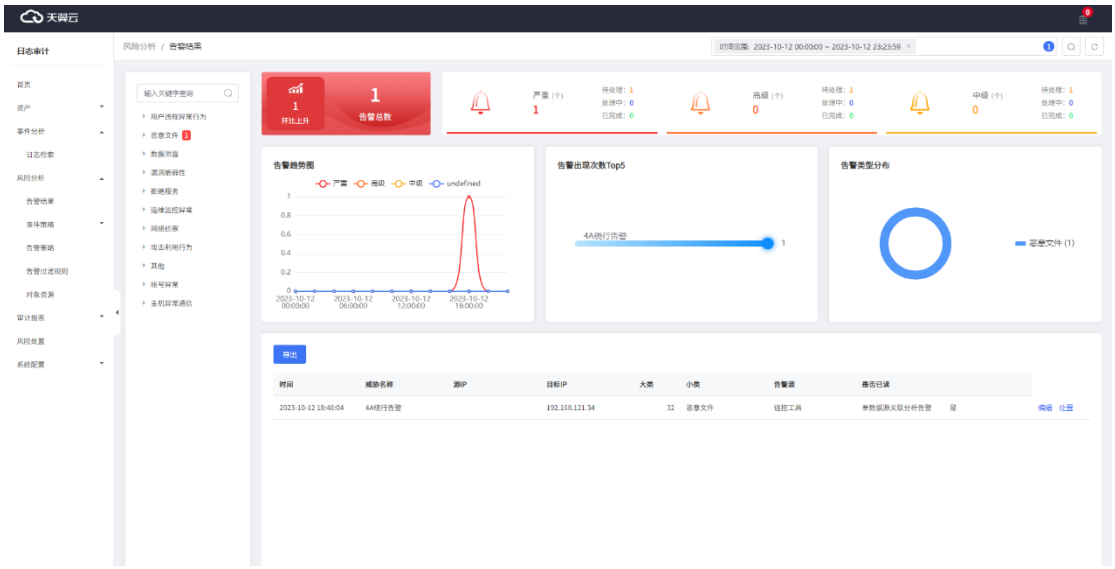


4.4 风险分析

4.4.1 告警结果

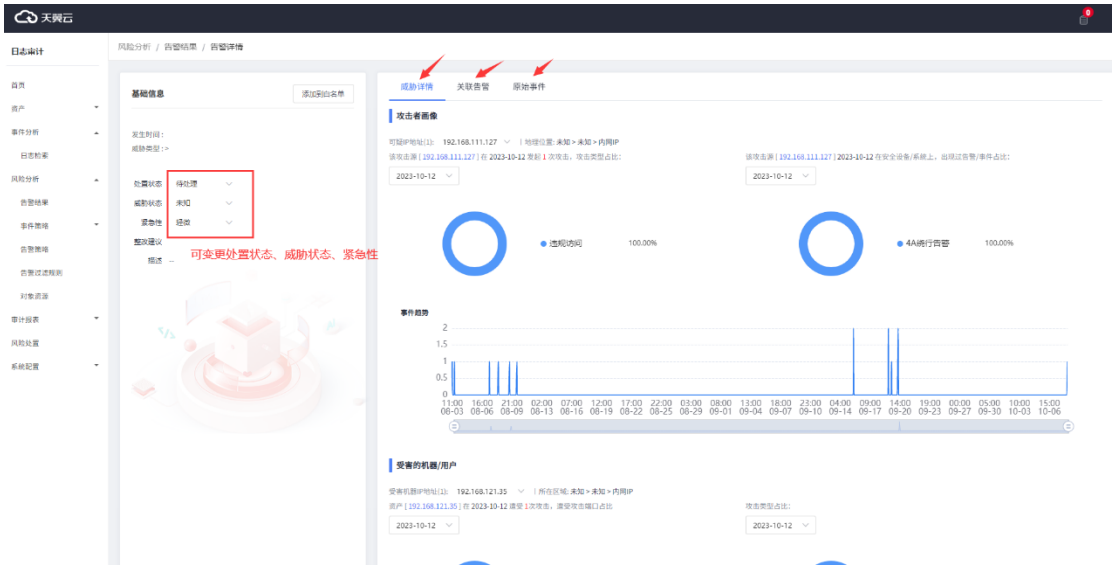
告警结果

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

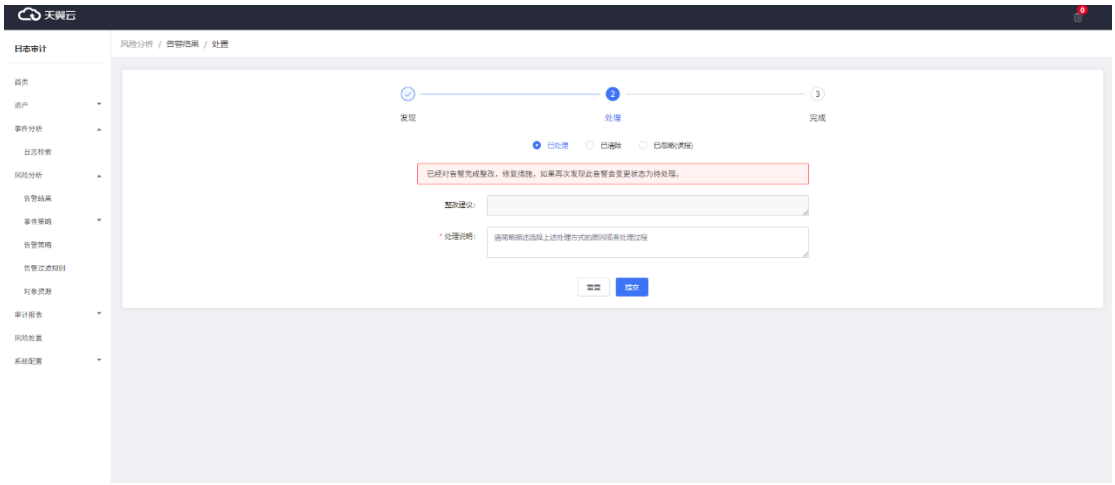
点击“ 编辑 ” 按钮，可查看告警基本信息、威胁详情（攻击者画像、事件趋势、受害的机器/用户）、关联告警、原始事件。



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。



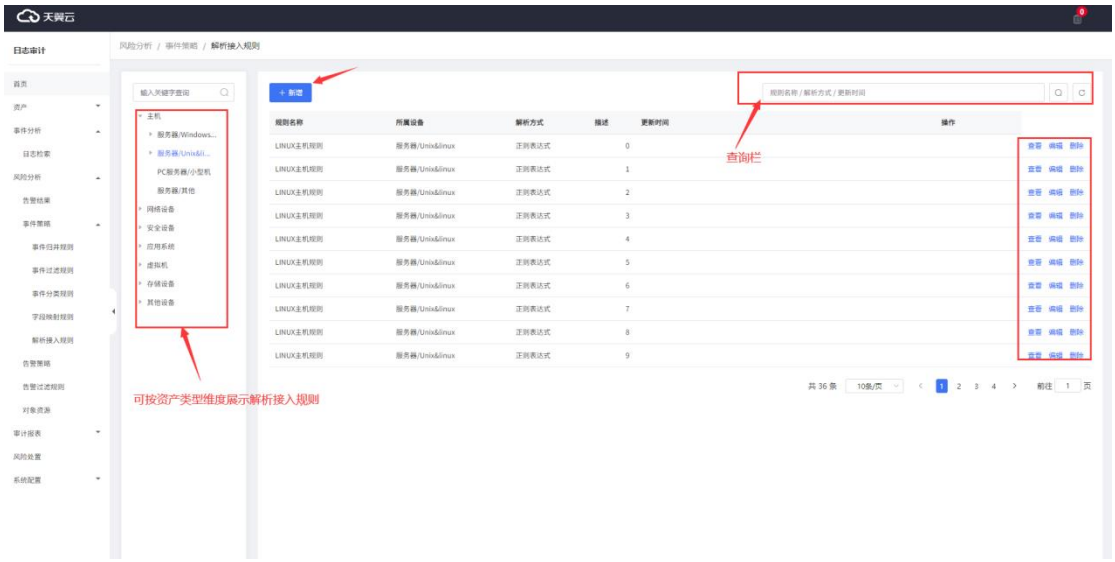
4.4.2 事件策略

事件策略

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。

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。可对解析接入规则进行新增、查看、编辑、删除、查询操作。



- 新增：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：

  基本信息：填写规则名称和选择需要采集的设备类型。

  提取样本：将原始日志复制到该文本框。

  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。

  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。

  提取字段：根据选择的不同方法，填写需要提取的内容。

- 查看：点击“查看”按钮，弹出解析接入规则的详情界面。
- 编辑：点击“编辑”按钮，弹出编辑界面，修改解析接入规则。
- 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。

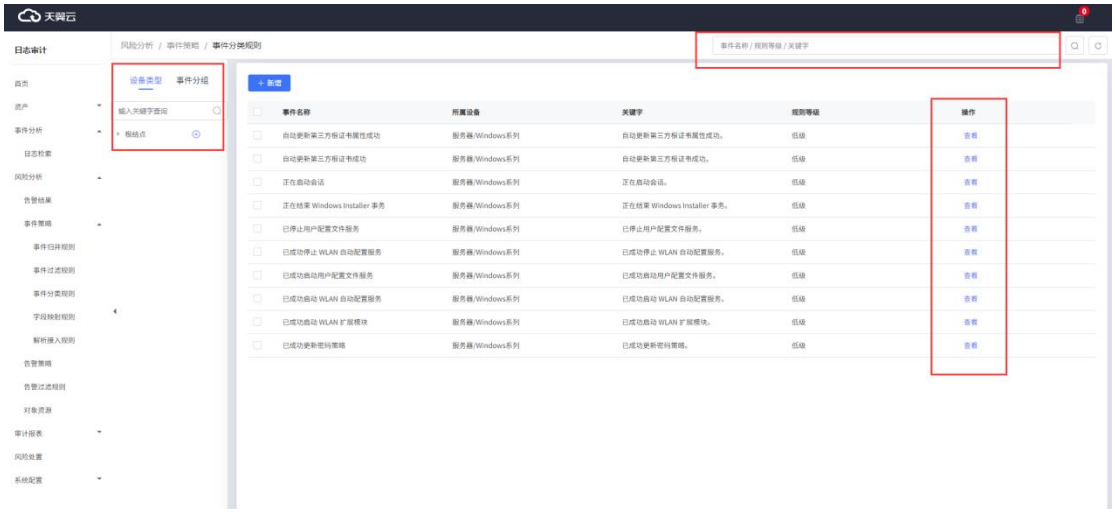
注意：

- 正则表达式提取方式：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。
- 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）。
- 预览保存：检查填写内容是否正确，确定无误后点击保存。

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：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。
- 查看：点击“查看”按钮，弹出事件分类规则的详情界面。
- 编辑：点击“编辑”按钮，弹出编辑界面，修改事件分类规则。
- 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。



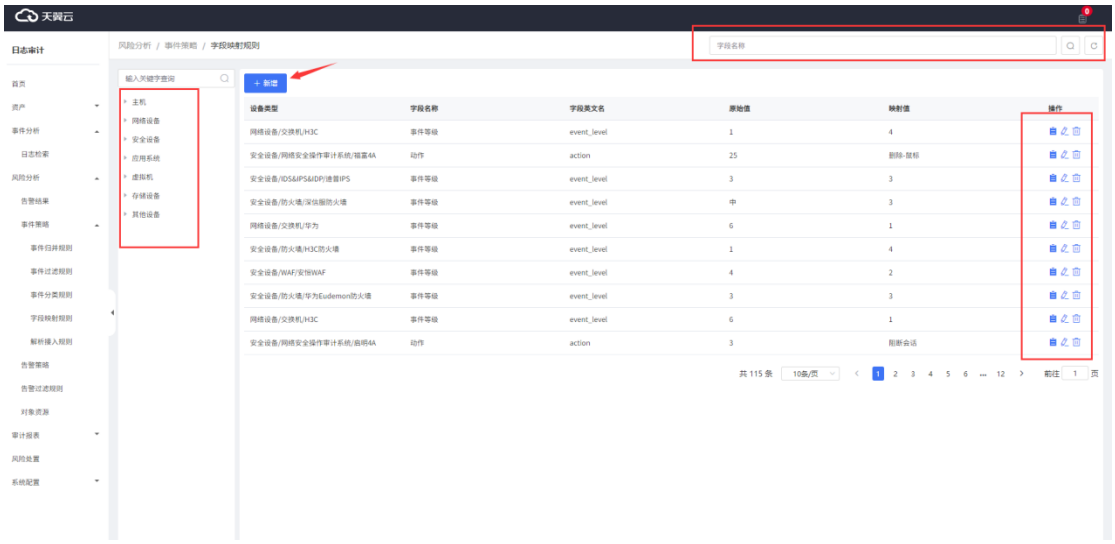
事件归并规则

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：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。

- 查看：点击“查看”按钮，弹出事件归并规则的详情界面。
- 编辑：点击“编辑”按钮，弹出编辑界面，修改事件归并规则。
- 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。

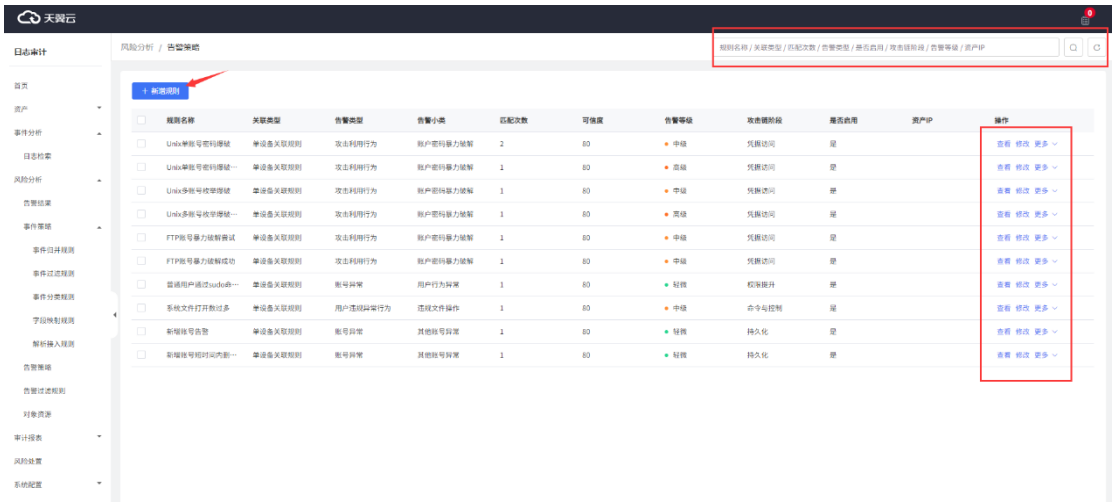


4.4.3 告警策略

告警策略

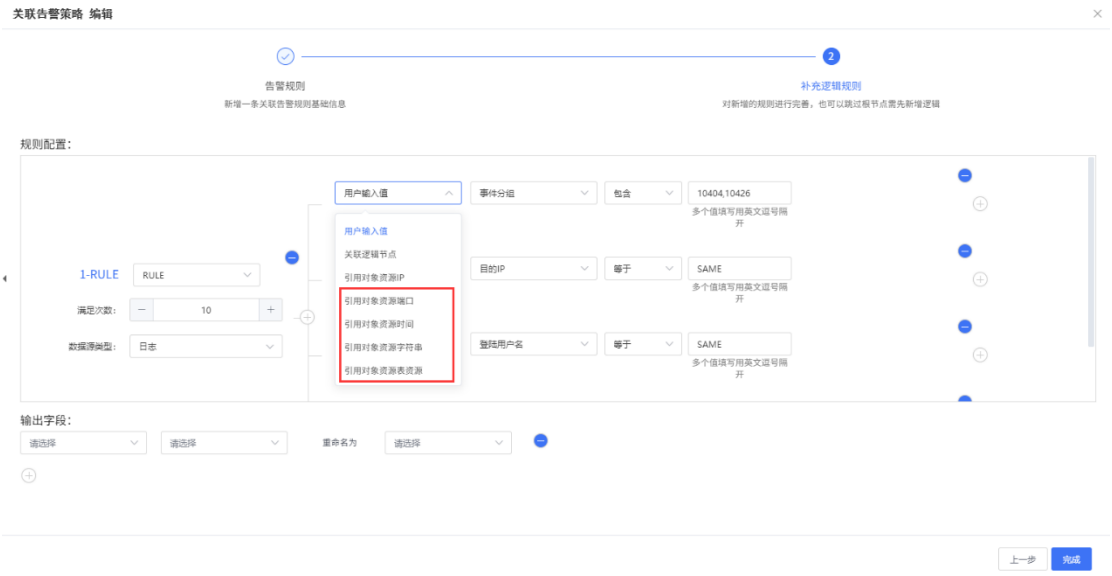
告警策略，对采集到的日志进行告警判断，符合告警策略的日志进行告警。

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。

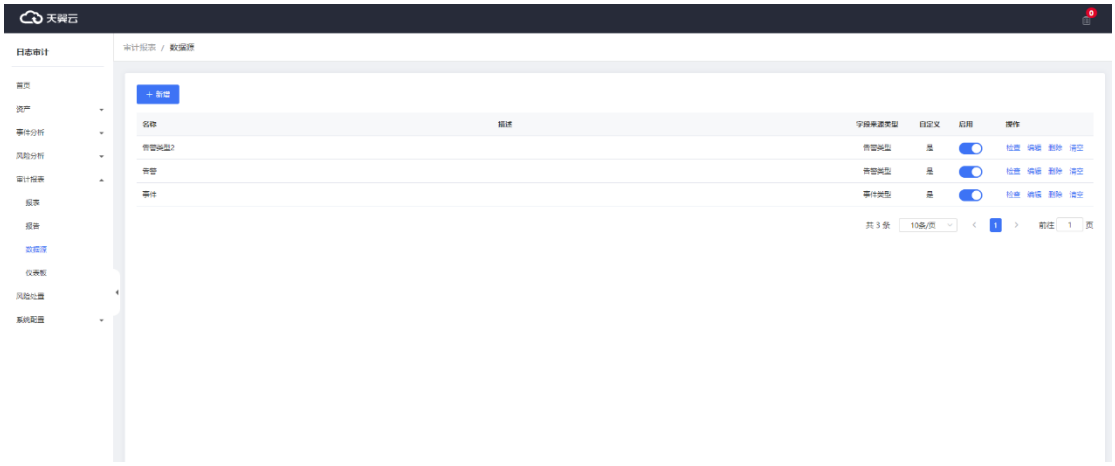


4.5 审计报表

4.5.1 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。

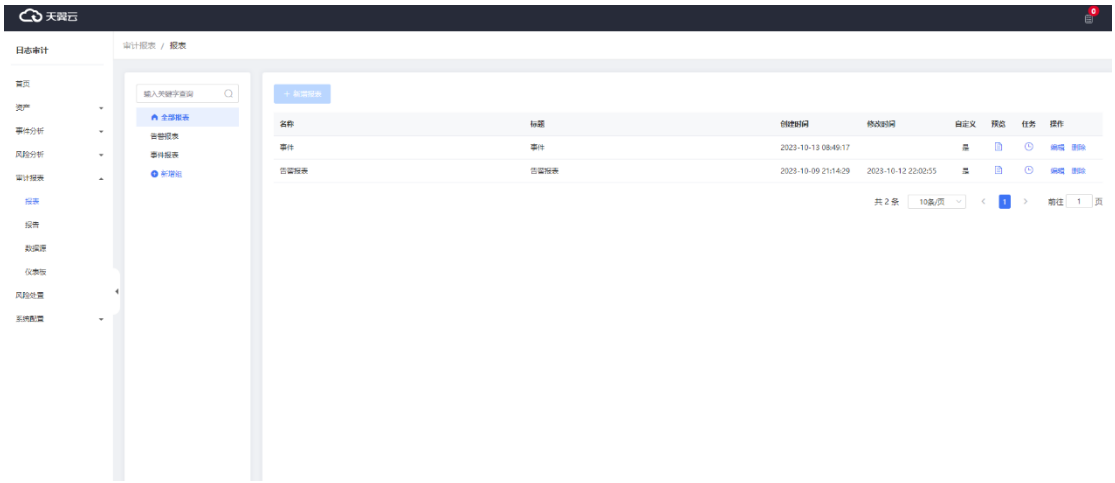
注意

- 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!”。

4.5.2 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。

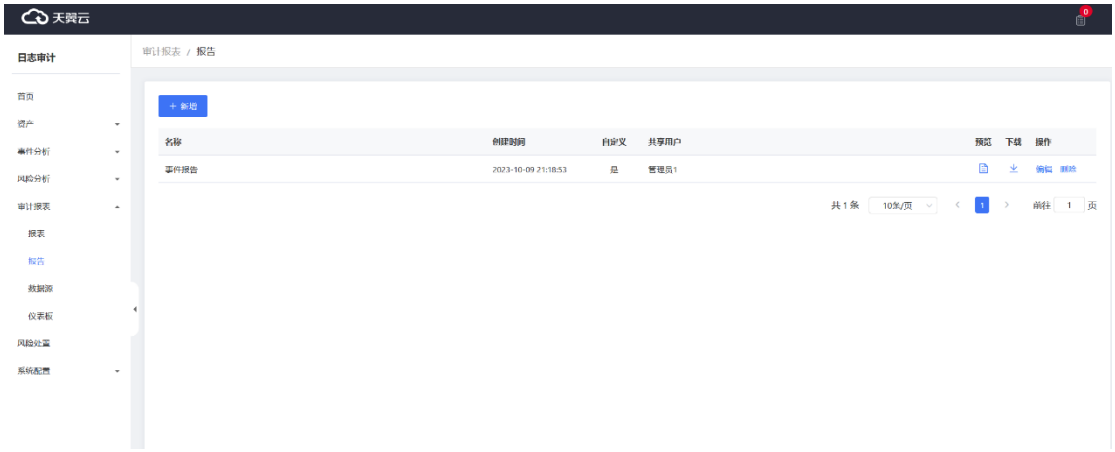
注意

- 支持 word、pdf 格式。
- 无法变更数据源。

4.5.3 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。

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。

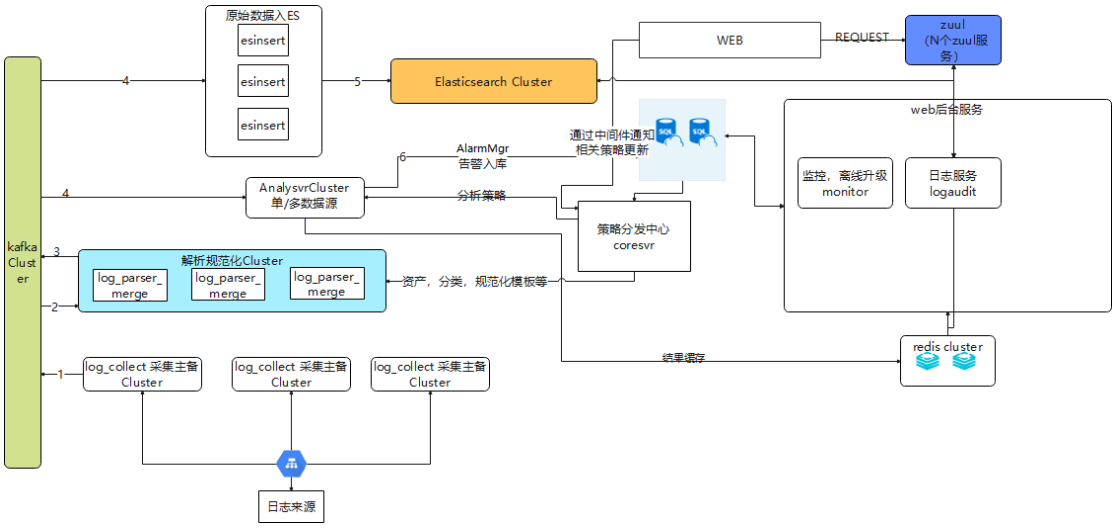
前提准备

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。

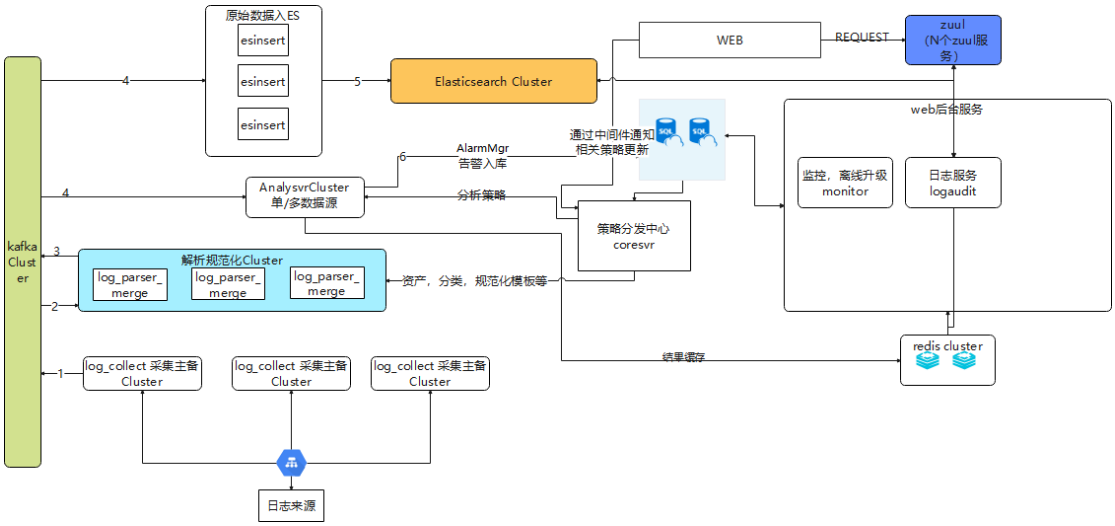
前提准备

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 常见问题

6.1.1 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。

6.1.2 功能类

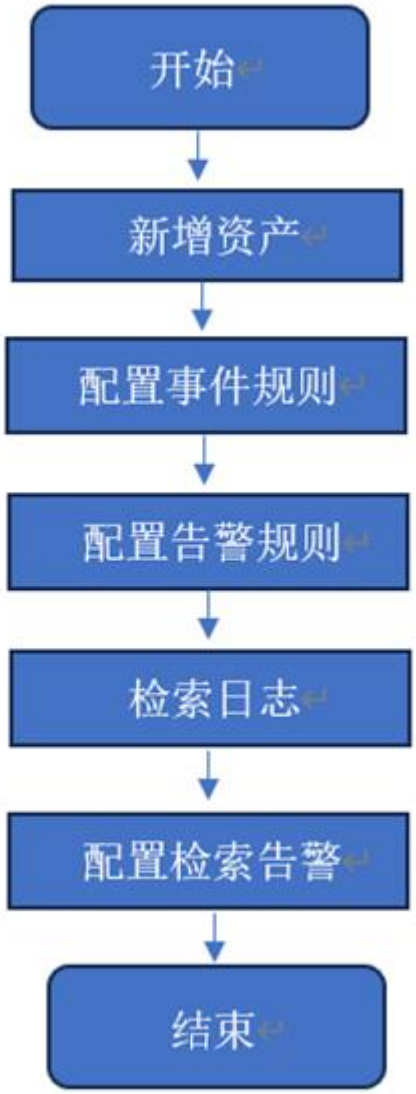
日志审计（原生版）采用何种接入方案?

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。