



SANGFOR
深信服科技



深信服智安全
SANGFOR SECURITY

深信服日志分析管理系统

SIP-Logger 用户手册

产品版本 3.0.5

文档版本 v2.0

发布日期 2021-07-07

深信服科技股份有限公司

版权声明

本文档版权归深信服科技股份有限公司所有，并保留对本文档及本声明的最终解释权和修改权。

本文档中出现的任何文字叙述、文档格式、插图、照片、方法、过程等内容，除另有特别注明外，其著作权或其它相关权利均属于深信服科技股份有限公司。未经深信服科技股份有限公司书面同意，任何人不得以任何方式或形式对本文档内的任何部分进行复制、摘录、备份、修改、传播、翻译成其他语言、将其全部或部分用于商业用途。

免责条款

本文档仅用于为最终用户提供信息，其内容如有更改，恕不另行通知。

深信服科技股份有限公司在编写本文档的时候已尽最大努力保证其内容准确可靠，但深信服科技股份有限公司不对本文档中的遗漏、不准确、或错误导致的损失和损害承担责任。

联系我们

售前咨询热线：400-860-6868

售后服务热线：400-630-6430（中国大陆）

香港：(+852) 3427 9160

英国：(+44) 8455 332 371

新加坡：(+65) 9189 3267

马来西亚：(+60) 3 2201 0192

泰国：(+66) 2 254 5884

印尼：(+62) 21 5695 0789

您也可以访问深信服科技官方网站：www.sangfor.com.cn获得最新技术和产品信息

修订记录

修订记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

日期	文档版本	修改内容
2021.07.26	v2.0	3.0.5 版本新增 POC 测试工具和常用工具

符号说明

在本文中可能出现下列标志，它们所代表的含义如下。

图形	文字	使用原则
 危险	危险	若用户忽略危险标志，可能会因误操作发生危害人身安全、环境安全等严重后果。
 警告	警告	该标志后的注释需给予格外的关注，不当的操作可能会给人身造成伤害。
 小心	小心	若用户忽略警告标志，可能会因误操作发生严重事故（如损坏设备）或人身伤害。
 注意	注意	提醒操作中应注意的事项，不当的操作可能会导致设置无法生效、数据丢失或者设备损坏。。
 说明	说明	对操作内容的描述进行必要的补充和说明。

在本文中会出现图形界面格式，它们所代表的含义如下。

文字描述	代替符号	举例
窗口名、菜单名等	方括号 “[]”	弹出[新建用户]窗口。
		选择[系统设置/接口配置]。
按钮名、键名	尖括号 “< >”	单击<确定>按钮。

目 录

1. 产品说明.....	5
1.1. 产品简介.....	5
1.2. 产品体系架构.....	6
1.3. 产品关键特性.....	7
1.4. 使用场景.....	8
2. 安装部署.....	9
2.1. 注意事项.....	9
2.2. 部署前准备.....	9
2.3. 部署模式.....	11
3. 配置指南.....	12
3.1. 首页介绍.....	12
3.2. 资产管理.....	16
3.3. 告警.....	28
3.4. 日志检索.....	30
3.5. 知识库.....	33
3.6. 策略管理.....	34
3.7. 报表管理.....	39
3.8. 系统管理.....	40
4. 运维管理.....	57
4.1. 日常运维注意事项及高危操作.....	57
4.2. 日常巡检.....	57
4.3. 常见问题排查.....	58
4.4. 突发事件应急处理.....	60

1. 产品说明

1.1. 产品简介

深信服日志分析管理系统针对信息安全事件的“可发现”、“可处理”、“可审计”、“可度量”四大目标进行规划和设计，提供众多基于日志分析功能，如安全日志的集中采集、分析挖掘、合规审计、实时监控、日志二次转发及安全告警等，能够同时满足企业审计合规需求及实际运维分析需求，及时有效的发现异常及违规事件，是企业日常信息安全工作的重要支撑平台。

1.1.1. 产品特点

此产品作为用户网络中所有设备日志的集中地，把成千上万条原始日志汇聚于此进行系统分析，极大地展示了它的强大之处，其特点如下：审计与数据可视化，根据等级保护要求从安全审计、入侵防范及管理等维度，对网络安全设备、主机安全、应用安全和系统运营管理等多方面进行细化，用户也可以根据需要，通过简单的拖拽操作实现仪表盘或审计报表的调整。提升日常安全运维的水平，实现信息系统IT计算环境日志信息的集中管理，全面掌握IT计算环境运行过程中出现的隐患。

1.1.2. 产品优势

日志分析系统相比于目前业界的产品来说，优势如下：

- (1) 专业的日志分析：品具备高性能吞吐和丰富的数据源采集能力，内置多种解析规则和审计关联策略，企业用户只需将日志数据接入，即可实现自动分析、报表和告警。
- (2) 日志全生命周期管理：根据不同的数据源生命周期管理需求对数据进行分级管理、数据备份，且支持数据按需恢复。
- (3) 运维将本增效：日志旁路模式抓取，通过采集和分析日志时对业务并无影响；日志中包含丰富信息，可直观反馈信息系统的状态、安全事件或业务特征；通过进行日志分析或故障定位可以有效规避人为操作风险。并提高运维效率。
- (4) 高性能搜索引擎和灵活的分析模式：通过强大的检索分析功能强化用户自定义分析需求，ES的高性能吞吐能力、低资源消耗以及高稳定性已经得到了各行业客户的认可。客户可根据自身数据日增量情况，采用分布式集群部署，来保障日志的高性能吞吐、实时监控等需求。

(5) 开放的数据接口：可以随时通过syslog/Kafka对接第三方数据平台的输入与输出数据。为提高安全事件的处理能力，安全事件可以无缝对接到 SIEM/安全运营平台进行监测管理。

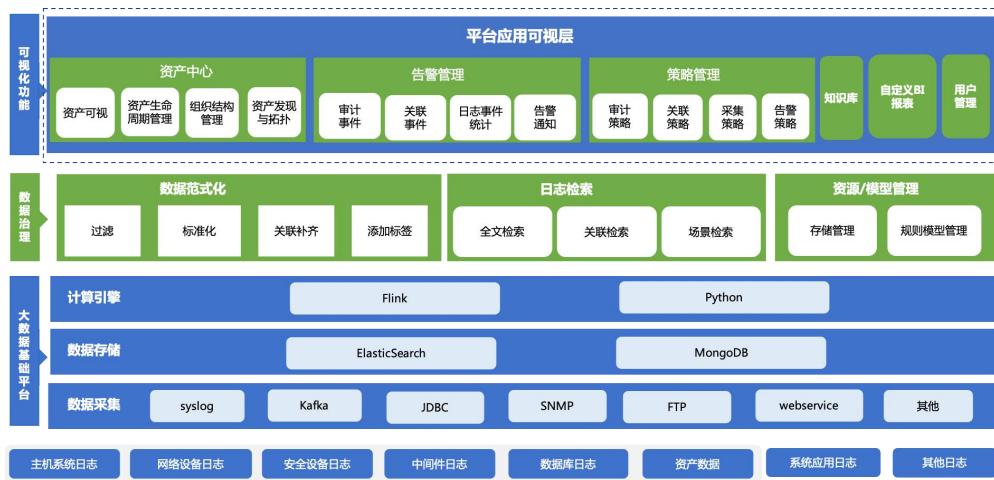
1.1.3. 产品相关概念

为了便于读者更好的阅读产品说明和用户手册，以下将产品中涉及的基本概念作简单介绍：

- (1) eps：是指设备平均每秒能处理的最大日志数，可在界面首页中的日志实时监控中看到。
- (2) 资产拓扑：代表用户网络中的资产，通过拓扑的形式展现在设备界面。
- (3) 资产扫描：通过ICMP协议探测用户网络中存活的设备。
- (4) 采集策略：产品本身内置了标准化的解析规则，采集到的日志通过命中策略来翻译日志。
- (5) 个性化定制：基于用户的实际需要，定制平台文案和LOGO。

1.2. 产品体系架构

深信服日志分析管理系统，采用基于大数据组件架构，采用分层的数据处理结构设计，从数据采集到最终的数据分析呈现形成完整的处理逻辑过程。层次划分如下：



(1) 数据采集层

采集包括主机数据、中间件数据、数据库、第三方网络和安全设备日志。该层提供多种接口进行多源日志数据的采集和对接，支持主动、被动相结合的数据采集方式，支持通过Agent采集日志数据，支持通过syslog、SNMP Trap、JDBC、WMI、webservice、FTP、文件/文件夹读取、Kafka等多种方式完成日志收集。

(2) 数据预处理层

对采集的数据进行预处理，包括数据清洗、数据归并、数据富化，最终数据转换为平台可理解的格式化数据，以文件的形式进行存在，等待分析。

(3) 大数据分析层

读取经过预处理后的数据进行离线计算，或读取ES（Elastic Search）数据进行实时机算。在此进行全网安全数据的检测、分析和统计，并结合多源数据智能分析，发现安全威胁现状，同时，内置的多条安全关联规则可将数据进行归并告警。

(4) 数据存储层

分析数据和结果存储在ES引擎（Elastic Search）中，可提供快速的检索能力。同时，对用于近期需要快速呈现的统计结果数据存放到MongoDB，可快速读取，相比ES引擎无需渲染和消耗内存。

(5) 数据服务层

基于APP的方式设计整个数据可视化的展示，基于从数据存储层获取数据的接口，读取展示数据，提供各种数据的安全可视服务及对外接口服务。

可视化使用ext作为JS框架，基于ECharts作为图形库，以vue架构作为数据可视化呈现支撑。

1.3. 产品关键特性

本节主要讲解产品的关键特性。对于比较大的特性可以采用列表的方式单独写作。对于比较小的特性，特别是大特性下的小子项可以通过表格的形式列出，更清晰。

1.3.1. 攻击快速溯源

统一收集用户系统日志，通过历史数据的比对，找到异常地访问行为，同时利用登录的外网IP关联安全设备、操作系统、中间件等日志进行快速取证，帮助用户快速定位源头。

1.3.2. 运维增效

用户前期在等保自查过程中采用人工登记比对测评指标的情况，每次都需要登录系统查看各种配置状态，并做记录。该工作每天多次重复，耗时长，人工成本高且巡检效率低。应用日志审计后，仅需5分钟即可完成自动巡检，巡检效率大幅提升，故障定位也不再需要登录设备，有效避免了人员误操作风险。

1.3.3. 数据泄露追溯

某制造企业，内部存在违规拷贝敏感信息导致数据泄露的情况。应用日审审计以后，用户将人员信息、IP、操作系统、文件审计以及数据库审计应用等信息进行集中采集，并利用规则建模，进行关联分析。通过产品实时发现用户异常行为并实时告警，有效提高了审计效率，对非法访问数据也形成了强有力的威慑。

1.4. 使用场景

此日志分析和管理系统主要适用于以下三种场景：

- (1) 等保合规场景：集中采集IT系统日志，满足保存6个月以上要求；可水平弹性扩展，及时的查询与检索，满足调查和取证要求；保留原始日志，多种合规报表报告。
- (2) 简化运维场景：第三方设备日志接入场景，通过建立主机、数据库、网络设备、安全设备场景，同时内置一键等保合规自检能力，提高运维效率与竞争力。
- (3) 方案探针场景：多分支日志采集与分布式采集的场景，可配合SIP/NGSOC/其他大数据平台，做日志采集转发。

2. 安装部署

本章主要讲解设备安装与升级过程中的流程、注意事项、准备工作以及操作步骤。

2.1. 注意事项

- (1) 告警灯在设备启动期间是红灯长亮的。通常一分钟后红灯熄灭，说明正常启动。如红灯长时间不灭，请关闭设备等待5分钟后重新开机。
- (2) 如果还是长亮，请联系深信服科技客服确认是否设备损坏。正常启动后，有时红灯会闪烁，属于正常现象，红灯闪烁表示设备正在写系统日志。
- (3) 控制口仅供开发和测试调试使用。最终用户需从网口通过控制台接入。

2.2. 部署前准备

本节主要写作安装前的准备工作，包括准备工具、环境、软硬件材料要求等。

2.2.1. 环境要求

为保证系统能长期稳定地运行，应保证电源有良好的接地措施、防尘措施、保持使用环境的空气通畅和室温稳定，建议环境温度10~35°C、湿度35%~80%。本产品符合关于环境保护方面的设计要求，产品的安放、使用和报废应遵照国家相关法律、法规要求进行。

SIP-Logger系列硬件设备使用交流110V到230V电源。在您接通电源之前，请确保您的电源有良好的接地措施。

2.2.1.1. 产品外观

深信服日志分析管理系统SIP-Logger的前面板（以SIP-Logger-A600为例）。



表1 SIP-Logger-A600前面板对照表

设备名称	编号	说明
SIP-Logger-A600	1	console 口
	2	USB 口
	3	管理接口（ETH0）
	4	ETH1
	5	ETH2
	6	ETH3
	7	ETH4
	8	ETH5

深信服日志分析管理系统SIP-Logger的背面板（以SIP-Logger-A600为例）。



表2 SIP-Logger背面板对照表

设备名称	序号（背面）	说明
SIP-Logger-A600	1	VGA 口
	2	电源开关
	3	电源口

2.2.1.2. 配置与管理

在配置设备之前，您需要配备一台计算机，配置之前请确认该计算机的网页浏览器能正常使用（如Chrome、Firefox），然后把计算机与SIP-Logger连接在同一个局域网内，通过网络对设备进行配置。

2.2.1.3. WEB 控制台登录介绍

日志分析管理系统设备的管理口为MANAGE(ETH0)口，管理口默认出厂IP为10.251.251.252/24。初次登陆设备，请用网线连接MANAGE(ETH0)口到局域网或直接连接计算机。

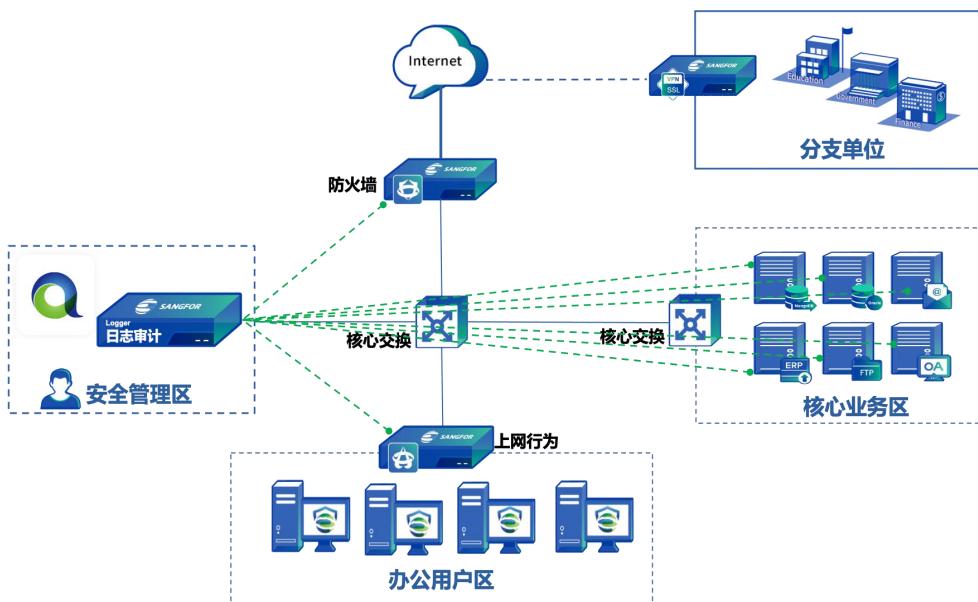
2.3. 部署模式

本节用一张流程图全面展示整个安装的流程。如果升级的流程图与安装的流程图有较大的差异，可以用第二张图展示升级的流程图。

安装与升级的流程图的作用是清晰的展示整个安装的流程。

2.3.1. 旁路部署

如下图所示，SIP-Logger作为日志审计设备，通常旁路部署在客户的核心网络，便于多角度、多方位收集用户各个区域的日志，只要保证网络可达即可。



3. 配置指南

3.1. 首页介绍

用户登录平台后默认进入首页的数据概要页面。默认主页可查看日志存储概况、告警总览、设备概况、日志实时监控、数据分布、审计事件总览、告警事件总览、日志统计情况、日志传输趋势。

3.1.1. 总览

1. 日志存储概况

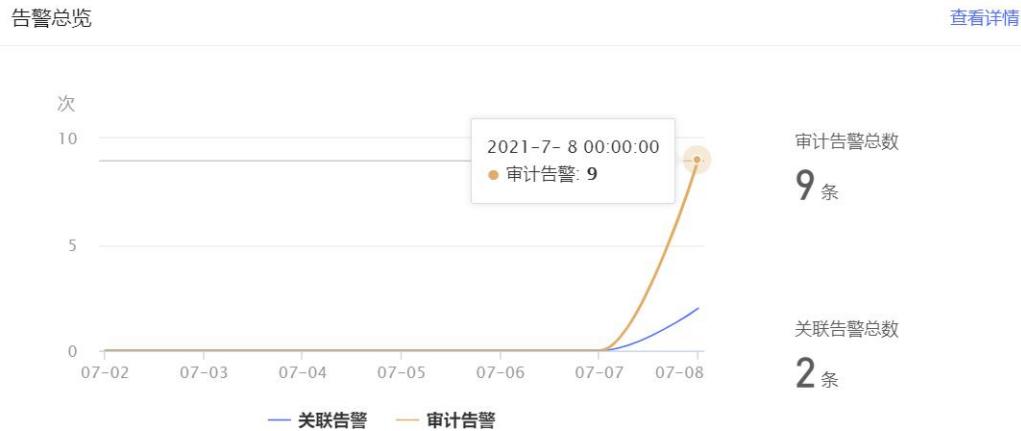
查看等保存储要求合规情况，日志存储天数与可存天数，日志存储占用空间和系统状况。

日志存储概况



2. 告警总览

查看告警分布情况，以日志关联告警与日志审计告警的时间轴角度展示，点击【查看详情】可进入到具体告警列表详情。



3. 设备概况

查看设备资源与使用情况，展示设备的CPU、内存与硬盘情况及设备接入类型、命中规则情况。

设备概况

◆ 接入设备概况



15%



1%



60%

◆ 设备使用情况



接入类型：7 种

类型总数：767 种



命中数：2 个

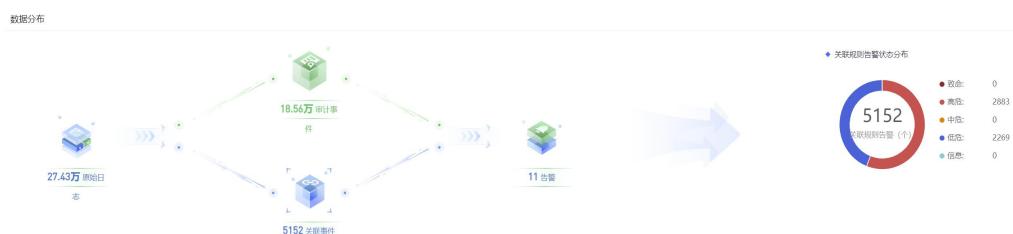
规则总数：362 个

4. 日志实时监控

查看日志数据接收概况，展示日志接收总数、每秒传输日志量信息与日志每天接收的折线趋势，其中日志接收总数指用户打开SIP-Logger界面控制台开始计算，每秒传输的日志量为当前设备的eps。

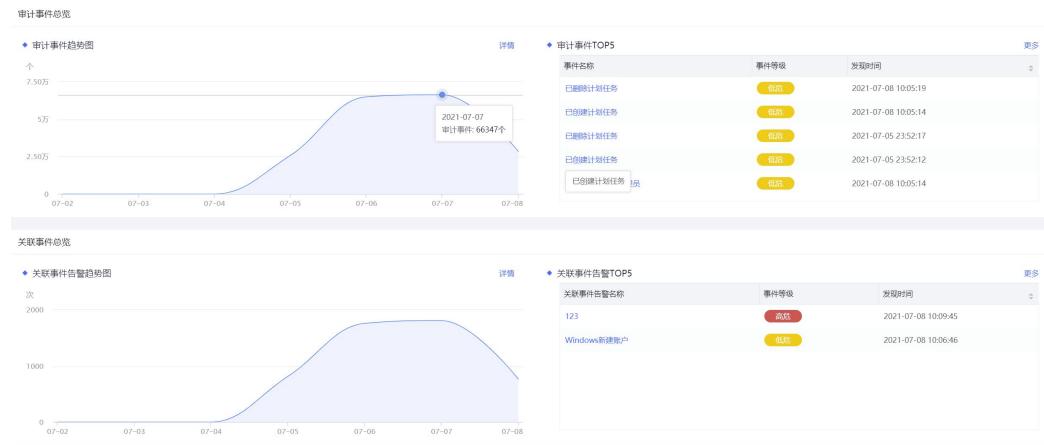


可直观查看数据分布情况，展示原始日志数在经过审计与规则分析后的告警数据，统计数据最终分布，点击对应的图标，可跳转查看对应的原始日志来源分布情况。



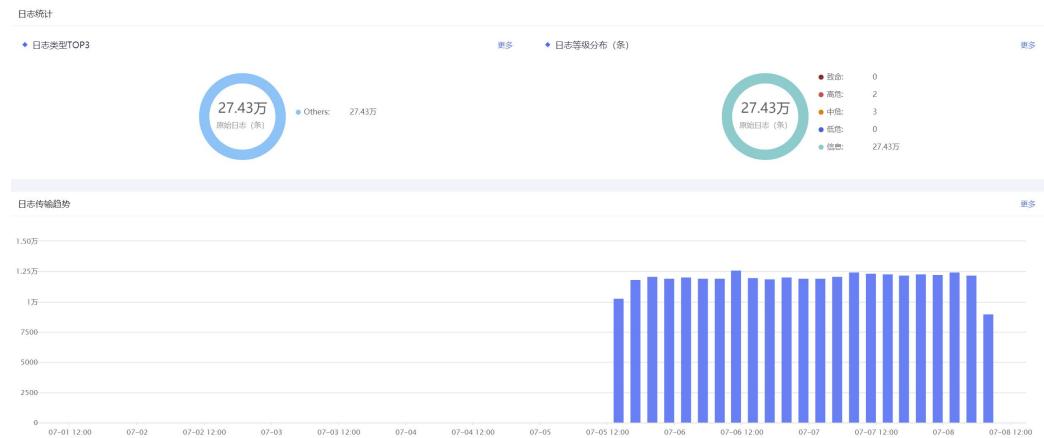
6. 审计事件与关联事件的总览

查看审计事件与关联事件的趋势图与TOP5的信息，可通过【更多】查看事件列表详情。



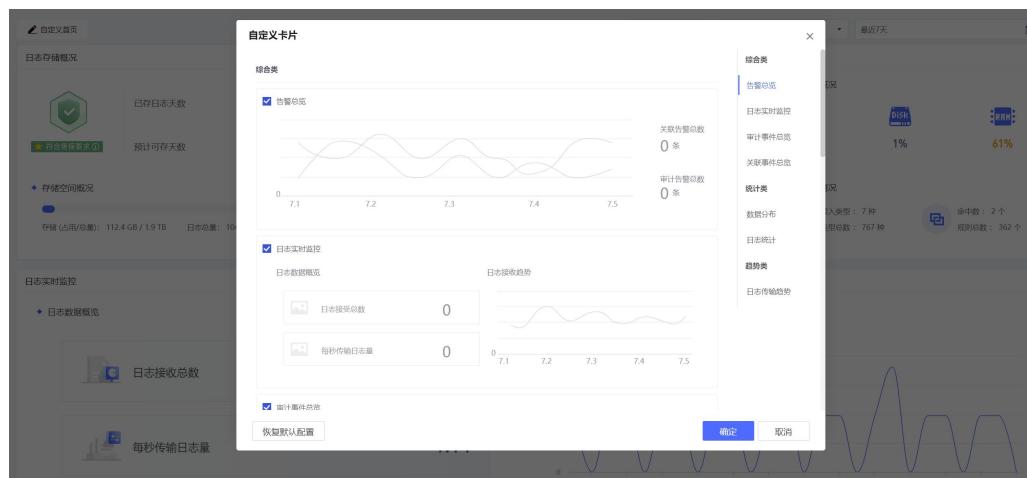
7. 日志统计与日志传输趋势

查看日志类型与等级的统计信息与日志数据的信息统计。



3.1.2. 自定义首页

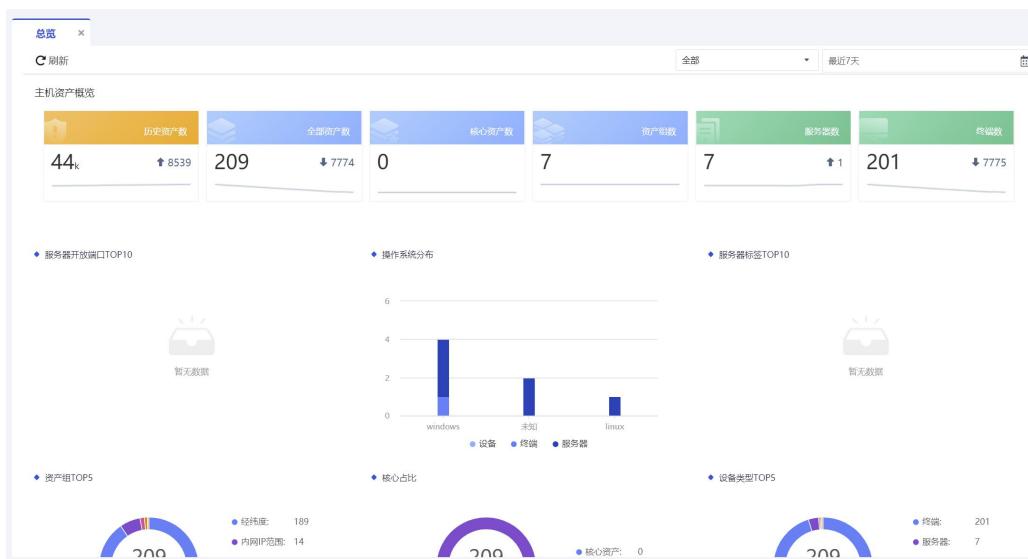
系统在默认内置面板页面外，支持对面板信息的自定义，其中定义类型包含统计类、趋势类、综合类，通过勾选关注卡片信息进行展示内容确定。



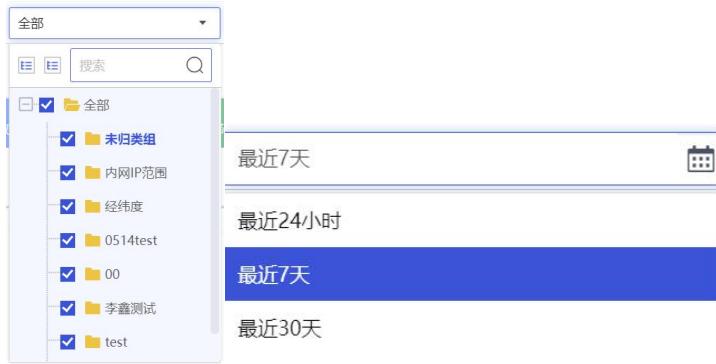
3.2. 资产管理

3.2.1. 资产总览

资产管理模块提供资产总览页面，方便管理员以各个维度统计内网资产和变化趋势，整体掌握资产情况与状态，同时支持筛选特定资产组及统计时间，如下图所示。



资产总览支持通过选择/搜索资产与资产组进行资产可视，同时可通过时间范围进行资产信息可视，包含最近24小时、最近7天、最近30天与自定义时间。



3.2.2. 生命周期管理

3.2.2.1. 资产管理

资产管理可进行标签管理、IP范围管理、自定义资产属性、导入、导出、资产组与资产的增删改查、资产组织结构管理。

The screenshot shows the '资产管理' (Asset Management) section. At the top, there are tabs for '标签管理' (Label Management), 'IP范围定义' (IP Range Definition), '历史资产' (Historical Assets), '自定义属性' (Custom Properties), '导入' (Import), '导出' (Export), and '刷新' (Refresh). Below these are search and filter fields for '资产类型' (Asset Type), '标签' (Label), '重要级别' (Importance Level), '端口' (Port), and '操作系统' (Operating System). The main area displays a table of assets with columns: 序号 (Index), IP, 机名 (Name), MAC地址 (MAC Address), 操作系统 (Operating System), 类型 (Type), 服务与端口 (Service and Port), 责任人 (Responsible Person), 标签 (Label), and 所属组 (Group). The table contains 10 rows of asset information. At the bottom right, there is a pagination control showing '共203项' (203 items) and a page number '1'.

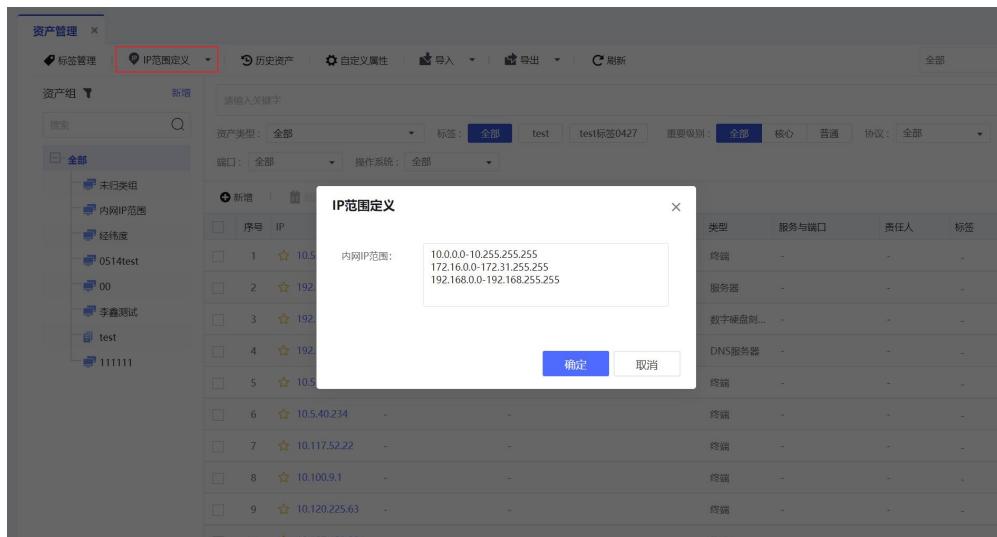
1. 标签管理

通过资产标签可进行资产所属划分，通过标签的方式进行资产分组分层管理。点击【新增】在新增窗口，选择资产/组类型，并添加标签名称。

The screenshot shows the '标签管理' (Label Management) dialog box. It includes a '新增' (Add) button and a table with columns: 序号 (Index), 标签 (Label), 类型 (Type), 应用范围 (Scope), 操作 (Operation), 服务与端口 (Service and Port), and 责任人 (Responsible Person). The table lists 7 items. A new label 'test' is being added in the first row. At the bottom right of the dialog is a '确定' (Confirm) button.

2. IP范围定义

自动识别资产如果在定义的IP范围内，则会自动加入，手动添加资产不受此设置的限制。



3. 历史资产

序号	IP	主机名	MAC地址	操作系统	类型	服务与端口	责任人	标签	操作
1	10.222.81.166	-	-	-	终端	-	-	-	删除
2	10.42.223.112	-	-	-	终端	-	-	-	删除
3	10.113.236.25	-	-	-	终端	-	-	-	删除
4	10.32.91.20	-	-	-	终端	-	-	-	删除
5	10.136.149.117	-	-	-	终端	-	-	-	删除
6	10.219.171.105	-	-	-	终端	-	-	-	删除
7	10.40.130.59	-	-	-	终端	-	-	-	删除
8	10.34.190.30	-	-	-	终端	-	-	-	删除
9	10.52.131.220	-	-	-	终端	-	-	-	删除
10	10.45.149.26	-	-	-	终端	-	-	-	删除

4. 自定义属性

点击新增可自定义属性并关联到对应资产

序号	属性名称	适用资产范围	适用资产类别	描述信息	是否必填	展示到资产列表	操作
1	test	全部	全部	test	是	是	编辑 删除

新增自定义属性

* 属性名称:

* 是否必填: 是 否

描述信息:

* 适用资产范围:

* 适用资产类型:

* 展示到资产列表: 是 否

[保存并新增](#) [确定](#) [取消](#)

5. 批量导入

批量导入资产分为“资产组”与“资产”批量导入两种。

(1) 资产组导入

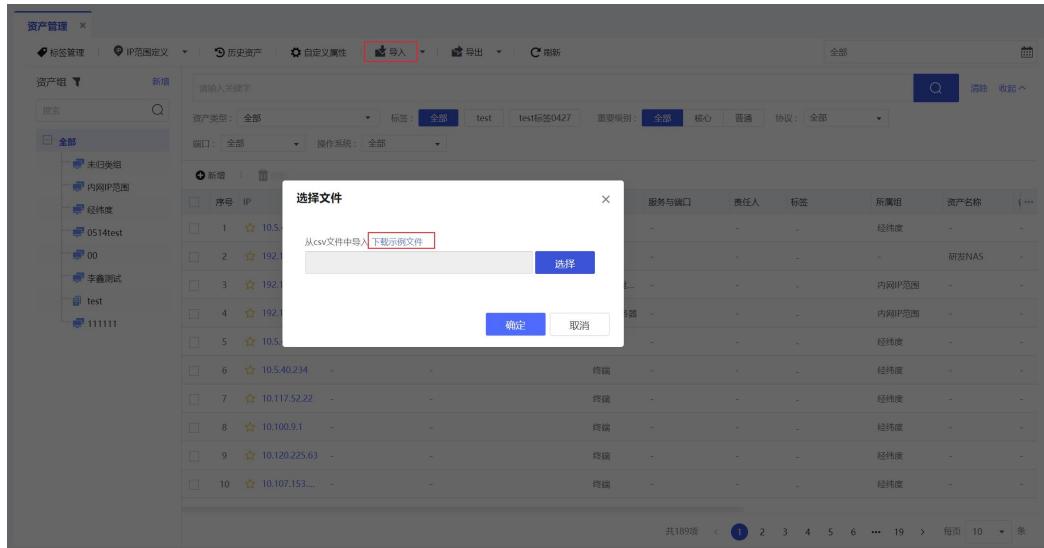
可在【资产管理】页面，点击【导入资产/导入组】，在弹出页面下载csv示例文件进行离线编辑，再选择从csv文件导入的方式进行资产导入，如下图所示。

The screenshot shows the 'Asset Management' interface. In the top navigation bar, there is a red box around the 'Import' button. Below the navigation bar, there is a search bar and several filter dropdowns. On the left, there is a sidebar with a tree view of asset groups, including '全部', '未归类组', '内网IP范围', '经纬度', and several specific group names like '0514test', '00', '李鑫测试', 'test', and '111111'. The main area displays a table of assets with columns: 序号 (Index), IP, 主机名 (Host Name), MAC地址 (MAC Address), 操作系统 (Operating System), 类型 (Type), 服务与端口 (Service & Port), 责任人 (Responsible Person), 标签 (Label), 所属组 (Group), 资产名称 (Asset Name), and more. There are 10 rows of data in the table. At the bottom right of the table, there is a pagination control showing '共189项' (Total 189 items) and a page number '1'.

This screenshot shows the same 'Asset Management' interface as the previous one, but with a modal dialog box overlaid. The dialog is titled '选择文件' (Select File). Inside the dialog, there is a text input field containing the placeholder '从csv文件中导出' (Export from CSV file) and a red box highlighting the '从csv文件中导出' text. Below the input field is a blue '选择' (Select) button. At the bottom of the dialog are two buttons: '确定' (Confirm) and '取消' (Cancel). The background of the main interface is dimmed.

(2) 资产导入

可在【资产管理】页面，直接点击【导入资产】，在弹出页面下载csv示例文件进行离线编辑后，再选择从csv文件导入的方式进行资产导入，如下图所示。

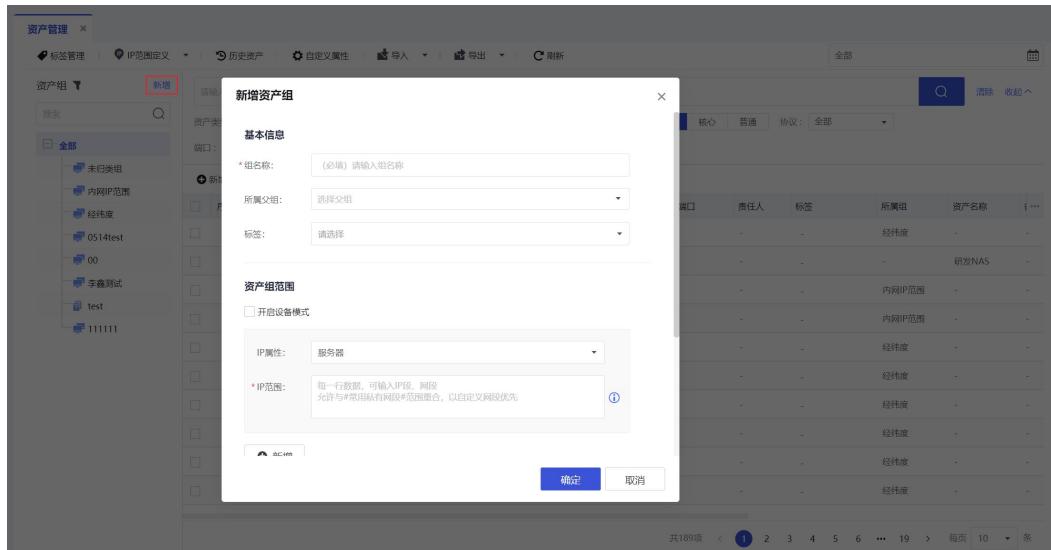


注意：

- (1) 导入资产组最大支持3000个，导入资产单次上限为2w，导出资产单次上限为1w，如资产量大，可分次进行导入导出；
- (2) 不支持旧版本资产导出格式的文件导入操作，请下载全新示例文件进行重新编辑后，再进行导入操作。

6. 新增资产组

通过资产组可针对不同用户组织架构资产进行归类并匹配对应的识别场景，识别场景包括IP端划分资产场景、设备划分资产场景及IP设备混合划分资产场景等，资产组支持多层级，最多支持15层级。



在弹出页面进行资产组信息配置，配置信息包括：

- (1) 基本信息：包括组名称（必填）、所属父组、标签；

(2) 资产组范围：仅配置IP范围方式需对IP属性及IP范围进行配置，可逐条进行新增，其中：

I: IP属性：包括自动识别（根据端口等信息进行服务器/终端类型的识别）、服务器与终端三类；

II: IP范围：每一行数据，可输入IP段、网段，允许与#常用私有网段#范围重合，以自定义网段优先，格式举例：

IPV4格式：

IP范围：如192.168.1.1-192.168.1.10

IP网段：192.168.1.0/24或192.168.1.0/255.255.255.0

IPV6格式：

IP范围：如2005::1-2005::2

IP网段：2005::1/64

III: 地理位置：可通过弹出地图页面进行搜索指定；

IV: 责任人：可选择已有责任人或全新添加；

V: 高级设置：包括内外网访问权限及备注信息。

7.资产详情

针对已有资产进行信息更新的场景，资产管理包括主机资产和互联网资产的管理。

主机资产

在【资产管理】页面，点击对应资产IP可查看详情，可针对已有或空白信息进行更新或补充，也可在该界面做资产对比、退库及删除资产的操作，如下图所示。

资产删除后，会导致对应的安全事件和脆弱性数据会被删除，建议优先以更新资产属

性，平台会同步更新资产历史数据。

编辑信息包括：

(1) 基础信息：包括资产ID、创建时间、资产名称、对外Web域名等信息，如下图所示。

资产ID :	51	创建时间:	2021-04-22 13:30:48
标签:	请选择	资产名称 :	请输入内容
对外WEB域名 :	请输入内容	备注 :	请输入内容

(2) 设备信息：可查看设备类型、所属组、重要级别等信息，重要级别可设置为核心/普通，也可在资产页面标星，如下图所示。

设备类型 :	终端	所属组 :	经纬度
主机名 :	请输入内容	设备发行版 :	请输入,示例: ThinkPad
设备厂商 :	请输入,示例: 联想	重要级别:	普通
设备版本 :	请输入,示例: t450s		

(3) 关联IP：可查看网络的IP地址、IP类型、关联的MAC地址、IP所属运营商、暴露程度等信息，其中暴露程度包括位置、主机内可访问、内网可访问以及外网可访问，如下图所示。

* 网口IP :	10.5.40.232	子网掩码 :	请输入
关联MAC地址 :	-	IP类型:	静态
IP所属运营商:	未知	暴露程度:	未知
创建时间:	2021-04-22 13:30:48		

(4) 地理位置：可以补充资产的实际详细位置，便于快速定位资产。

资产位置:	中国	全部	全部	全部	请输入详细地址
-------	----	----	----	----	---------

(5) 操作系统：可以补充资产的系统类型、厂商、系统版本、版本号等信息。

系统类型:	未知	厂商:	请输入内容
系统发行版 :	请输入,示例: windows 7	系统位数:	请选择
系统版本 :	请输入,示例: 旗舰版	操作系统详情 :	请输入内容
版本号 :	请输入,示例: 6.1	系统补丁包 :	请输入,示例: service pack 1
build版本号 :	请输入内容	内核版本 :	请输入内容
激活状态:	未知	语言 :	请输入内容
安装时间:	请选择日期	授权时间:	请选择日期

(6) 虚拟机：此信息指从虚拟化平台视角，给GUEST OS分配的虚拟机参数和获取到

的虚拟机状态。



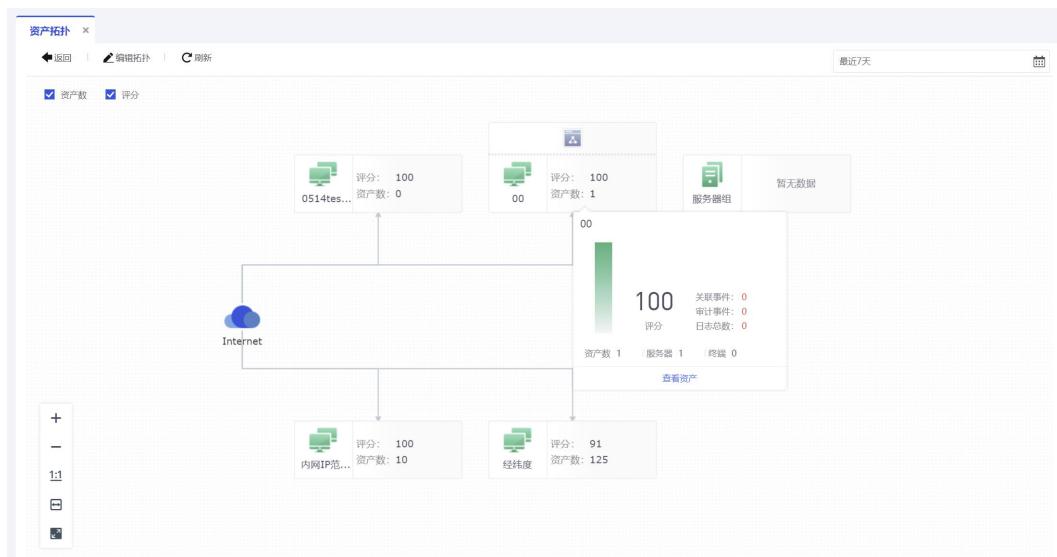
3.2.2.2. 全局搜索

资产感知模块可实现全局全字段搜索，助力资产管理员筛选效率，管理员可在搜索框内填入欲搜索的关键字进行相关搜索，关键字涵盖主机名、MAC地址、IP、责任人等基础信息的同时，还可进行操作系统、服务应用、端口等信息进行检索，如下图所示。

序号	IP	主机名	MAC地址	操作系统	类型	服务与端口	责任人	标签	所属组	资产名称
1	192.168.1.10	研发NAS	-	linux	服务器	-	-	-	-	研发NAS

3.2.2.3. 资产拓扑

资产管理是从安全域维度对资产进行分组得到的拓扑结构。安全域是指同一环境内有相同的安全保护需求、相互信任、并具有相同的安全访问控制 和边界控制策略的网络或系统。每个安全域具有基本相同的安全特性，如安全级别、安全威胁、风险等，依据这些特性，将资产归入不同的安全域中，实施不同的安全保护。



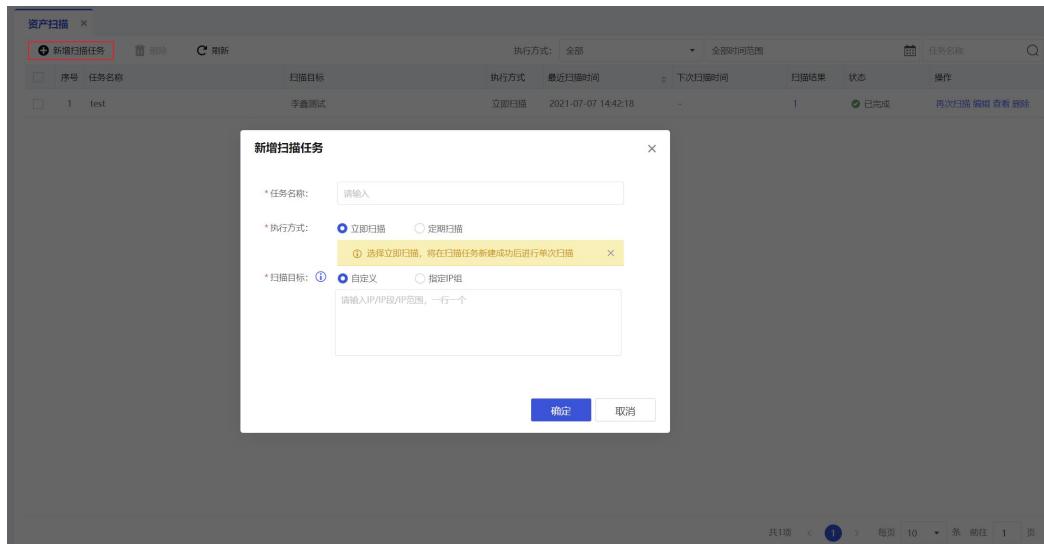
3.2.2.4. 待审核资产

如用户业务系统中未添加的资产，通过已采集到的其他业务系统日志中的详细信息获取到内网IP，这样的资产将进入待审核列表，可根据用户的实际需要选择入库或忽略。

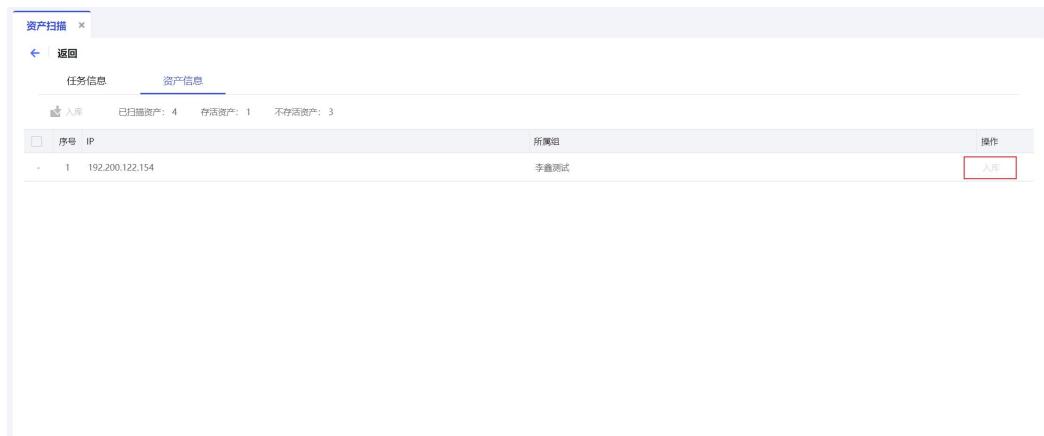
The screenshot shows a search interface for pending review assets. At the top is a search bar with placeholder text '请输入关键字' and a search button. Below it are several filter dropdowns: '资产类型' (全部), '标签' (全部, test, test标签0427), '重要级别' (全部), '操作系统' (全部), '协议' (全部), and '端口' (全部). A table below has columns: 序号, IP, 主机名, MAC地址, 操作系统, 类型, 服务与端口, 责任人, 标签, and 操作. The table body displays a single row with a warning icon and the text '暂无数据'.

3.2.2.5. 资产扫描

资产扫描是基于ICMP协议通过SIP-Logger发送ping包来探测内网存活IP数量，可新增扫描任务，执行方式为定时和立即执行，扫描目标可选择已创建好的资产组或自定义IP地址段。



扫描完成后可查看资产信息，并人工识别是否需要入库操作。



3.2.3. 资产配置

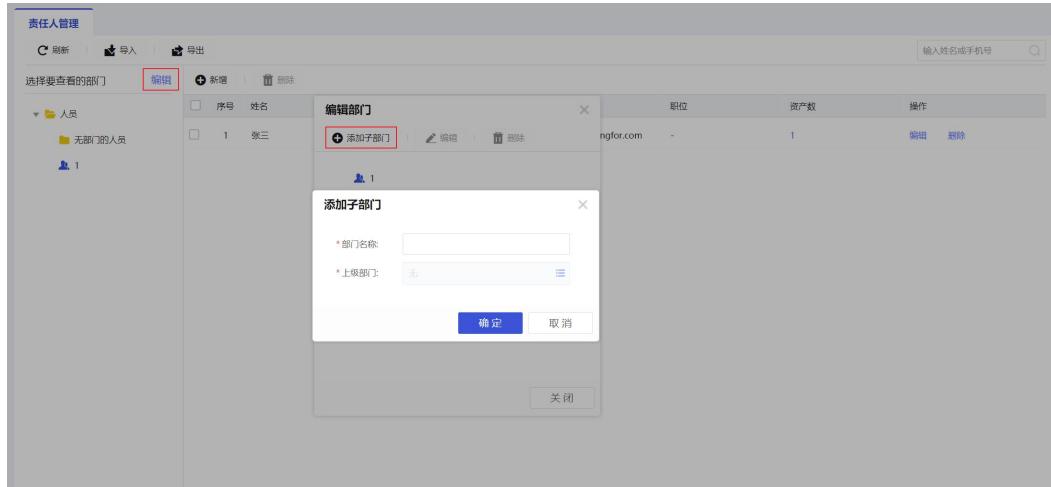
3.2.3.1. 责任人管理

在【资产配置/责任人管理】页下，可以查看责任人的姓名、性别、手机号码、邮箱、资产数等详细信息，可以对责任人进行编辑、新增与删除的操作。



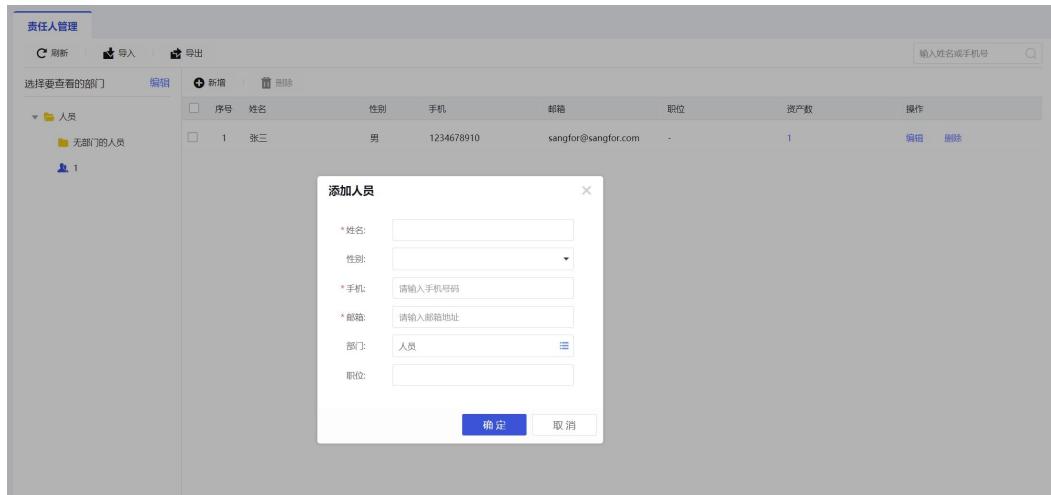
(1) 部门管理

点击页面的【编辑部门】，可以新增子部门操作，如下图所示。



(2) 责任人新增

点击新增，填写姓名、手机、邮箱以及部门等相关信息，完成后点击<确定>即可。



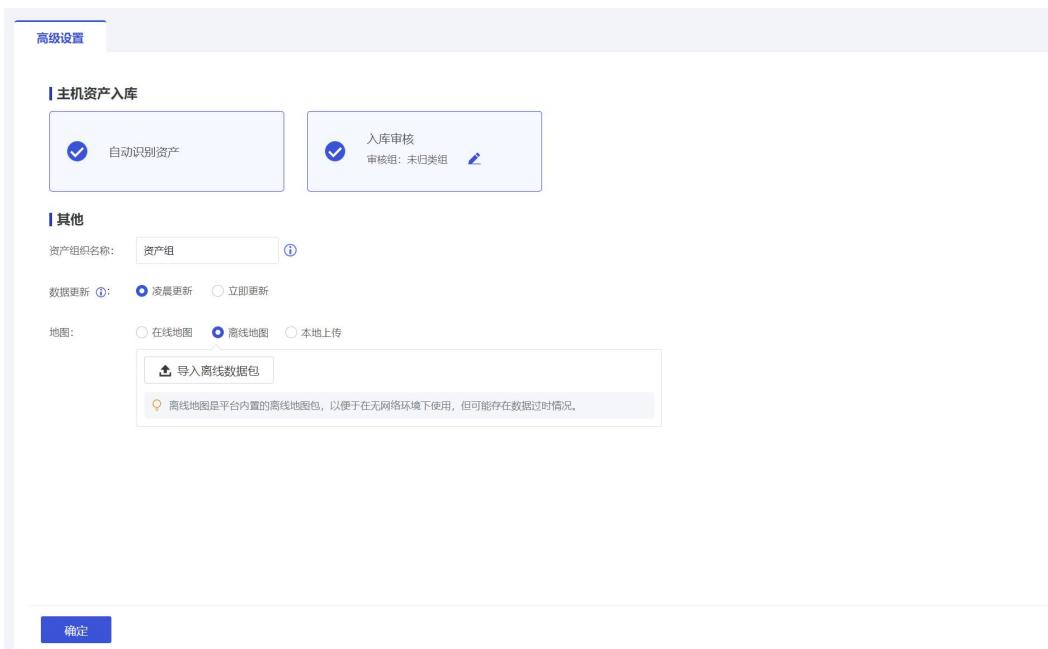
(3) 责任人管理

勾选单个对应的责任人，点击<编辑>，可修改责任人信息。

勾选单个/多个对应的责任人，可以点击<删除>，删除的单个/多个责任人。

3.2.3.2. 高级设置

如要求对指定资产组新增资产进行审核后才可入库，则需配置入库审核策略，如不配置入库审核策略，则自动识别的资产默认自动入库，配置步骤如下，在页面勾选“入库审核”，并点击配置按钮进行审核组指定，如下图所示。



(1) 资产组织名称自定义：可实现对资产总组织名称（即资产页面左树名称）进行自定义，自定义设置成功后全局生效，组织名称如下图所示。

序号	IP	主机名	MAC地址	操作系统	类型	服务与端口
1	10.5.40.232	-	-		终端	-
2	192.168.1.10	研发NAS	-	linux	服务器	-
3	192.168.209.21	-	-		数字硬盘刻...	-
4	192.168.7.156	-	-		DNS服务器	-
5	10.5.40.233	-	-		终端	-
6	10.5.40.234	-	-		终端	-
7	172.16.0.22	财务PC-1	-	windows	台式电脑	-
8	192.200.122.157	lzg-test1	-	windows	服务器	-
9	192.200.122.156	lzg-test	-	windows	服务器	-
10	192.200.122.154	李鑫电脑 测试	-	windows	服务器	-

(2) 数据更新机制：数据更新机制指资产修改属性后，在全平台展示（包括报告数据展示）修改后结果的更新机制，本机制分为“凌晨更新”和“立即更新”两种模式，为保障平台性能稳定，建议选择凌晨更新模式，同时，如选择立即更新模式，当资产属性有变更后，需1-2小时才可生效。

(3) 地图数据来源：地图数据来源可设置为在线地图、离线地图或本地上传三种模式

3.3. 告警

所谓告警是指用户特别需要关注的安全问题，这些问题来源于事件分析、审计分析的结果。告警监控中包括了如下功能：

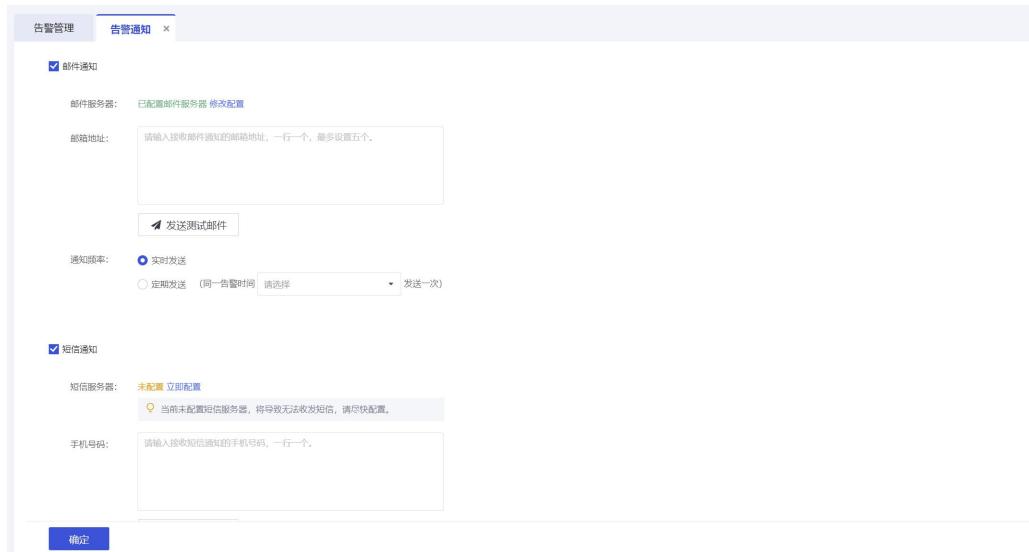
- (1) 告警监控：用户可以通过定义过滤器以监控需要特别关注的告警信息，用户也可以根据个人需求，设置告警的提示音、界面显示方式等；
- (2) 告警处理：处理监控列表中相关告警；针对告警，用户可以清除（不予关注）、确认（已知告警可后续处理）。

3.3.1. 告警管理

告警管理中包括审计告警和关联告警，其中审计告警是命中审计策略后产生的，关联告警是命中关联策略后产生，告警数量很庞大时，可根据告警等级，告警状态，资产类型、告警对象等进行全局查询。亦可单独/批量标记为已处理告警和归档等操作，其中，归档后的告警将进入已归档功能栏。

(1) 告警通知

告警通知可通过邮件和短信的方式发送，可填写正确的邮箱地址和手机号码并选择项定时和定期发送。



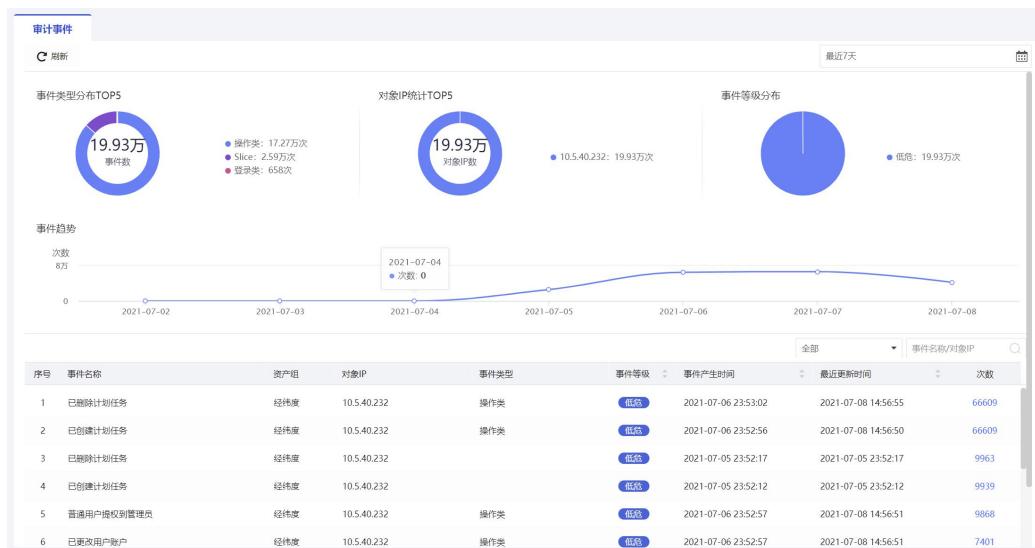
3.3.2. 关联事件

默认展示最近7天的关联事件，可通过规则等级、事件分类进行筛选，也可单独通过搜索框检索某条事件

关联事件								
C 新增		事件名称	事件分类	规则等级	对象IP	开始时间	结束时间	操作
1	123	账号异常	高危	0.0.0.0(互联网)	2021-07-08 14:49:18	2021-07-08 14:49:18		查看日志
2	123	账号异常	高危	0.0.0.0(互联网)	2021-07-08 14:47:49	2021-07-08 14:47:53		查看日志
3	Windows新建账户	账号异常	低危	10.5.40.232(经纬度)	2021-07-08 14:46:19	2021-07-08 14:46:19		查看日志
4	Windows新建账户	账号异常	低危	10.5.40.232(经纬度)	2021-07-08 14:46:19	2021-07-08 14:46:19		查看日志
5	123	账号异常	高危	0.0.0.0(互联网)	2021-07-08 14:46:19	2021-07-08 14:46:23		查看日志
6	Windows新建账户	账号异常	低危	10.5.40.232(经纬度)	2021-07-08 14:46:18	2021-07-08 14:46:18		查看日志
7	123	账号异常	高危	0.0.0.0(互联网)	2021-07-08 14:44:48	2021-07-08 14:44:53		查看日志
8	123	账号异常	高危	0.0.0.0(互联网)	2021-07-08 14:43:18	2021-07-08 14:43:23		查看日志
9	Windows新建账户	账号异常	低危	10.5.40.232(经纬度)	2021-07-08 14:41:49	2021-07-08 14:44:49		查看日志
10	Windows新建账户	账号异常	低危	10.5.40.232(经纬度)	2021-07-08 14:41:49	2021-07-08 14:44:48		查看日志
11	123	账号异常	高危	0.0.0.0(互联网)	2021-07-08 14:41:49	2021-07-08 14:41:53		查看日志
12	Windows新建账户	账号异常	低危	10.5.40.232(经纬度)	2021-07-08 14:41:48	2021-07-08 14:44:48		查看日志
13	123	账号异常	高危	0.0.0.0(互联网)	2021-07-08 14:40:19	2021-07-08 14:40:23		查看日志
14	123	账号异常	高危	0.0.0.0(互联网)	2021-07-08 14:38:48	2021-07-08 14:38:53		查看日志
15	Windows新建账户	账号异常	低危	10.5.40.232(经纬度)	2021-07-08 14:37:19	2021-07-08 14:40:19		查看日志

3.3.3. 审计事件

默认展示最近7天的审计事件，首页分别展示了事件类型分布TOP5、对象IP统计TOP5、事件等级分布、事件趋势以及详细的事件。



3.3.4. 日志统计

日志统计直观地展示了最近7天每个日志源命中的告警事件等级条目，可以通过检索采集器名称来查看对应的事件。



3.4. 日志检索

3.4.1. 日志查询

在查询页面，管理可通过“类型筛选检索”与“搜索框检索”两种检索方式相结合，得到精准的检索结果。

(1) 类型筛选检索

在日志检索页面下，管理员可针对日志类型、访问方向及重点字段进行筛选，同时重点字段支持搜索，如下图所示。

The screenshot shows the SIP-Logger log search interface. At the top, there are buttons for export, import, QR code helper, search tips, and refresh. The date range is set from 2021-07-08 00:00:00 to 2021-07-08 15:22:37, and the search term is '全部日志'. Below the search bar, there's a note about using wildcards for search terms. The results table has columns: 序号 (Index), 标记 (Mark), 时间 (Time), 描述 (Description), 日志类型 (Log Type), 事件名称 (Event Name), 日志等级 (Log Level), 源IP (Source IP), 源所属类型 (Source Type), 源端口 (Source Port), 目的IP (Destination IP), 目的所属类型 (Destination Type), 目的端口 (Destination Port). The results show 10 log entries related to '重点字段'.

(2) 搜索框检索

在日志检索页面下，管理员可通过搜索框，进行“不指定字段模式检索”和“指定字段检索”两种方式搜索，同时，支持单次搜索多个过滤条件，如下图所示。

This screenshot shows the SIP-Logger log search interface with the search term '基础字段'. The results table has the same columns as the previous screenshot. The results show 10 log entries related to '基础字段'.

不指定字段模式检索：支持IP模糊检索、数据包模糊检索及组合模糊检索；

指定字段检索：支持多字段组合检索、指定字段的模糊检索，如下图所示：

This screenshot shows the SIP-Logger log search interface with the search term '基础字段'. The interface includes a sidebar for '基础字段' and a detailed view of the search filters. The results table is identical to the previous ones.

新增过滤条件检索：支持多IP、IP段及模糊检索、应用/协议检索、源/目的MAC地址检索等字段检索，可点击字段框进行详细字段查看，如下图所示。

+ 新建过滤条件

源IP	= ▾	支持多IP、IP段查询；支持模糊查询	① 新增
目的IP	= ▾	支持多IP、IP段查询；支持模糊查询	①
源端口	= ▾	请输入字段值	
目的端口	= ▾	请输入字段值	
数据来源设备	= ▾		▼
源IP	= ▾	支持多IP、IP段查询；支持模糊查询	①

说明：管理员可点击搜索框右侧的“？”标志，跳转至帮助文档查看具体检索规范。

(3) 检索结果

检索结果包括时间、日志类型、源/目的IP、源/目的端口及数据来源等信息，管理员可点击左侧“+”号，展开具体信息进行查看，如下图所示。

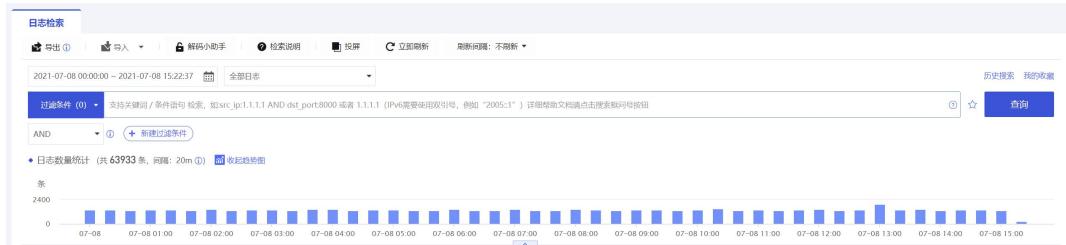
3.4.2. 目志投屏

在日志检索页面，管理员点击“投屏”后，会弹出新的页面，隐藏平台标题栏，方便管理员高效查看日志，如下图所示。

日志检索																
导出	导入	将码小助手	检索说明	C 立即刷新	刷新间隔: 不刷新											
序号	标记	时间	描述	日志类型	事件名称	日志等级	源IP	源所属类型	源端口	目的IP	目的所属类型	目的所属端	目的端口	原始日志内容	数据来源	采集
1	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	计划任务已刷...	10.5.40.232(1...	W	
2	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	计划任务已刷...	10.5.40.232(1...	W	
3	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	计划任务已刷...	10.5.40.232(1...	W	
4	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	计划任务已刷...	10.5.40.232(1...	W	
5	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	计划任务已刷...	10.5.40.232(1...	W	
6	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	计划任务已刷...	10.5.40.232(1...	W	
7	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	已从应用中安...	10.5.40.232(1...	W	
8	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	已从应用中安...	10.5.40.232(1...	W	
9	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	已从应用中安...	10.5.40.232(1...	W	
10	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	已删除用户名...	10.5.40.232(1...	W	
11	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	已共享用户的...	10.5.40.232(1...	W	
12	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	计划任务已刷...	10.5.40.232(1...	W	
13	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	计划任务已刷...	10.5.40.232(1...	W	
14	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	计划任务已刷...	10.5.40.232(1...	W	
15	■■■	2...	数据源日志	-	信息	0.0.0.0	互联网	-	10.5.40.232	终端	经纬度	-	计划任务已刷...	10.5.40.232(1...	W	

3.4.3. 日志导出

针对已检索结果，管理员可通过左上角<导出>按钮进行日志的整体导出操作，目前仅支持导出重点字段内容，如下图所示。



3.4.4. 解码小助手

解码小助手用于解码数据包为可读的内容，支持url, base64, unicode, HEX编码的字符串解码。如查看日志是发现编码数据包，将其复制到解码小助手进行解码，转换为可读信息，如下图所示。

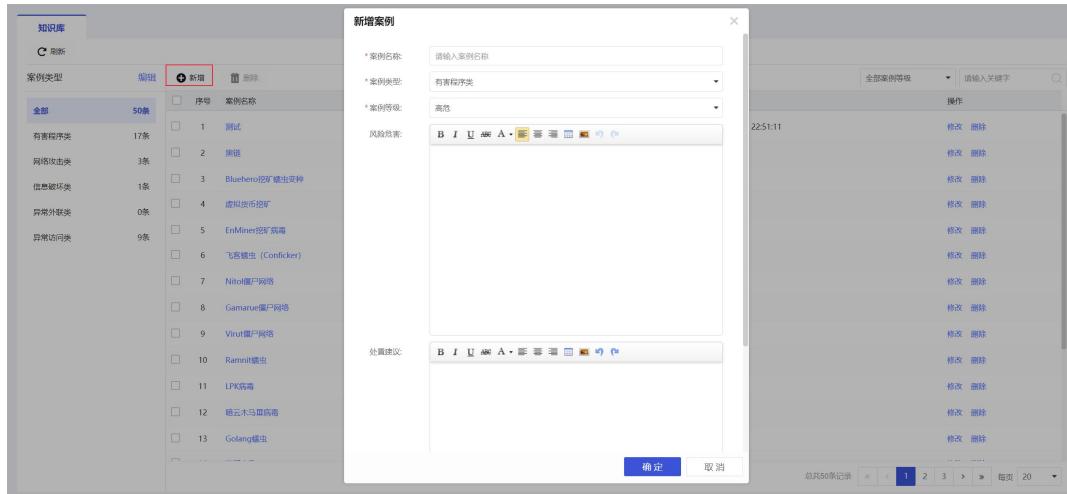


3.5. 知识库

用户可对内外部法律/部制度等文档进行归档与查看，主要查看内容包括文档年份、文档类型、文档名称等，如下图所示。

案例类型	操作	序号	案例名称	案例类型	案例等级	更新时间	操作
全部	新增	1	测试	有害程序类	高危	2021-07-05 22:51:11	修改 删除
有害程序类		2	黑链	信息破坏类	高危	-	修改 删除
网络攻击类		3	Bluehero挖矿链虫变种	-	-	-	修改 删除
信息破坏类		4	虚拟货币挖矿	有害程序类	低危	-	修改 删除
异常外联类		5	EnMine挖矿病毒	-	-	-	修改 删除
异常访问类		6	飞客链虫 (Conficker)	有害程序类	中危	-	修改 删除
		7	Nitol僵尸网络	有害程序类	中危	-	修改 删除
		8	Gamarue僵尸网络	有害程序类	中危	-	修改 删除
		9	Virut僵尸网络	有害程序类	中危	-	修改 删除
		10	Ramnit蠕虫	有害程序类	中危	-	修改 删除
		11	LPK病毒	有害程序类	中危	-	修改 删除
		12	暗云木马病毒	有害程序类	中危	-	修改 删除
		13	GoLang蠕虫	-	-	-	修改 删除

同时，管理员可点击<新增>，进行文档条目的创建与上传，新增页面如下图所示。



3.6. 策略管理

3.6.1. 关联规则

关联规则是指可根据不同时间节点、不同设备的多条日志进行相互关联，触发关联规则条件后会产生对应的关联事件。

在【关联规则】页面下，管理员可对关联规则进行新增、编辑、启用与禁用的管理操作，同时支持通过右上角搜索栏进行规则检索。

管理员可点击<新增>进行关联规则创建，创建流程主要包括基础信息、规则内容、告警设定等。

关联规则		编辑						
规则类型	全部	362条	新增	启用	禁用	操作	请输入关键字	搜索
主机异常	91条	1 123 2 非工作时间通过堡垒机登录服务器 3 非工作时间登录堡垒机 4 堡垒机账户连续多次登录失败 5 Linux系统发现sshd软连接后门 6 Linux用户在异常时间段SSH登录 7 SSL VPN发现新建管理员账号 8 Linux系统发现修改账号配置/密码文件 9 Linux系统新建ssh秘钥 10 SSL VPN发现用户修改密码 11 发现Linux系统端口外SSH登录 12 SSL VPN发现新建用户账号 13 Linux系统发现添加新用户	高危 低危 低危 中危 低危 低危 信息 中危 低危 低危 信息 低危 信息 低危	源主机 目的主机 目的主机 目的主机 目的主机 目的主机 目的主机 目的主机 目的主机 目的主机 目的主机 目的主机 目的主机	否 是 是 是 是 是 是 是 是 是 是 是 是	2021-06-04 10:... 2020-02-28 12:... 2020-02-28 12:... 2020-02-28 12:... 2020-01-08 12:... 2020-01-08 12:... 2020-01-08 12:... 2020-01-08 12:... 2020-01-08 12:... 2020-01-08 12:... 2020-01-08 12:... 2020-01-08 12:...	✓ ✓ ✗ ✗ ✗ ✗ ✗ ✗ ✗ ✗ ✗ ✗ ✗	作为模板新建 更多操作 作为模板新建 调整规则等级 作为模板新建 调整规则等级
主机脆弱性	4条							
账号异常	31条							
权限异常	11条							
侦察探测	24条							
暴力破解	62条							
网站攻击	66条							
漏洞利用	50条							
拒绝服务	1条							
恶意软件	5条							
C&C链路	17条							
设备监控	0条							
其它	0条							

共有 362 条记录

新增关联规则： 定义多个事件并顺序发生，场景如：Linux系统发现1分钟内多次ssh登录失败则产生中危告警，具体配置步骤如下：

(1) 填写规则基础信息

新建统计关联规则

基础信息 完成

① ② ③

* 规则名称:

* 规则类型:

* 规则等级:

启用状态: 启用

规则描述: 分析secure日志,发现有多个ssh登录失败记录

下一步 **取消**

(2) 制定规则内容

条件设定为数据来源设备即日志源设备为用户网络中的Linux (apache) 设备，目的端口设定为实际的22端口，动作状态为失败，对ABC三个条件做与运算，保证三者必须都满足，此规则才生效。

新建统计关联规则

基础信息 → 规则内容 → 完成

条件设定

A:	目的端口	=	22
B:	动作状态	=	失败
C:	数据来源设备	=	apache linux(1.1.1.1)

+ 新增条件

条件逻辑

逻辑表达式 ① : (A and B and C)

A B C

+ 新增 or 关系

上一步 下一步 取消

定义1分钟内发生次数大于等于3次，则命中此关联策略。

新建统计关联规则

A: 目的端口 = <=

B: 动作状态 = 失败

C: 数据来源设备 = apache linux(1.1.1.1)

+ 新增条件

条件逻辑

逻辑表达式 ① : (A and B and C)

A B C

+ 新增 or 关系

告警对象: 目的主机
时间窗口: 1 分钟
发生次数: >= 3

上一步 下一步 取消

(3) 保存配置



3.6.2. 审计策略

审计策略是指对单一设备的多个维度的策略，比如Linux主机类审计策略：针对的就是主机的多个维度，如登陆类、操作类等维度的审计，触发审计策略后会产生对应的审计事件。

在【审计策略】页面下，管理员可对审计策略进行新增、编辑、启用与禁用的管理操作，同时支持通过右上角[搜索栏]进行策略检索。

审计策略									
策略类型		编辑							
全部		45条		新增		启用		禁用	
linux主机	15条	<input type="checkbox"/>	序号	策略名称	通用设备类型	策略等级	是否内置	策略修改时间	状态
		<input type="checkbox"/>	1	su切换命令失败	linux主机	中危	是	2021-07-01 16:07:23	✓
		<input type="checkbox"/>	2	Telnet登出成功	linux主机	中危	是	2021-06-02 16:06:23	✓
		<input type="checkbox"/>	3	SSH登录失败	linux主机	中危	是	2021-04-28 20:57:03	✓
		<input type="checkbox"/>	4	su切换用户成功	linux主机	中危	是	2021-04-25 09:41:12	✓
		<input type="checkbox"/>	5	FTP登录失败	linux主机	中危	是	2021-04-25 09:41:12	✓
		<input type="checkbox"/>	6	sudo下授权后执行命令成功	linux主机	中危	是	2021-04-25 09:41:12	✓
		<input type="checkbox"/>	7	sudo下授权后执行命令失败	linux主机	中危	是	2021-04-25 09:41:12	✓
		<input type="checkbox"/>	8	SSH登录成功	linux主机	中危	是	2021-04-25 09:41:12	✓
		<input type="checkbox"/>	9	SSH操作失败：账号被锁定	linux主机	中危	是	2021-04-25 09:41:12	✓
		<input type="checkbox"/>	10	SSH登出成功	linux主机	中危	是	2021-04-25 09:41:12	✓
		<input type="checkbox"/>	11	sudo下授权失败	linux主机	中危	是	2021-04-25 09:41:12	✓
		<input type="checkbox"/>	12	sudo下授权成功	linux主机	中危	是	2021-04-25 09:41:12	✓
		<input type="checkbox"/>	13	Telnet登录成功	linux主机	中危	是	2021-04-25 09:41:12	✓

3.6.3. 采集策略

展示日志分析管理系统平台当前支持接入的数据源采集器，即对目标设备的解析规则。

3.6.4. 告警策略

1. 审计告警策略：

- (1) 告警条件：告警条件分为“AND/OR”两种，对下方两个条件进行约束。
- (2) 审计事件等级：审计事件等级为包括“致命、高危、中危、低危、信息”5种，为多选标签，默认选中“致命、高危、中危”三种。

2. 关联告警策略：

- (1) 生效时间：告警的生效时间范围，默认为“永久生效”，支持自定义生效时间，点击“自定义”选项时，仅允许选择当前日期之后的时间范围，默认选择从当天开始的30天时间，到达用户设置的默认生效时间后，自动关闭告警策略复选框。

注：告警策略可手动关闭，关闭后默认产生的审计和关联事件不告警。

3.7. 报表管理

对于SIP-Logger设备中的报表功能主要是对接入的数据进行统计与展示。报表分为内置报表和自定义报表，内置报表无需手动配置，会按每日、每周、每月的规则自动生成报告数据。自定义报表则可根据模板类型选择需要的报表内容导出数据。

The screenshot shows the 'Report Management' section of the SIP-Logger user interface. It includes a toolbar with '刷新' (Refresh), '导出历史' (Export History), and '新增自定义报表' (Add Custom Report). Below this are two main sections: '内置报表' (Built-in Reports) and '自定义报表' (Custom Reports).
The '内置报表' section contains five items:

- 主机安全报表 (Linux) - 主机 (linux) 接入统计与审计详情, with '导出报表' (Export Report) and '去下载' (Download) buttons.
- 主机安全报表 (Windows) - 主机 (windows) 接入统计与审计详情, with '去下载' (Download) button.
- 数据库安全报表 - 数据库接入统计与审计详情, with '导出报表' (Export Report) button.
- 网络设备安全报表 - 网络设备接入统计与审计详情, with '导出报表' (Export Report) button.
- 应用安全报表 - 应用接入统计与审计详情, with '导出报表' (Export Report) button.

The '自定义报表' section contains several items, each with a preview icon and a '...' button:

- WEB
- SOX
- ISO27001
- ceshi1111
- ceshi

Each item has a detailed description below it, such as '数据安全日志统计' (Data Security Log Statistics) for the WEB template.

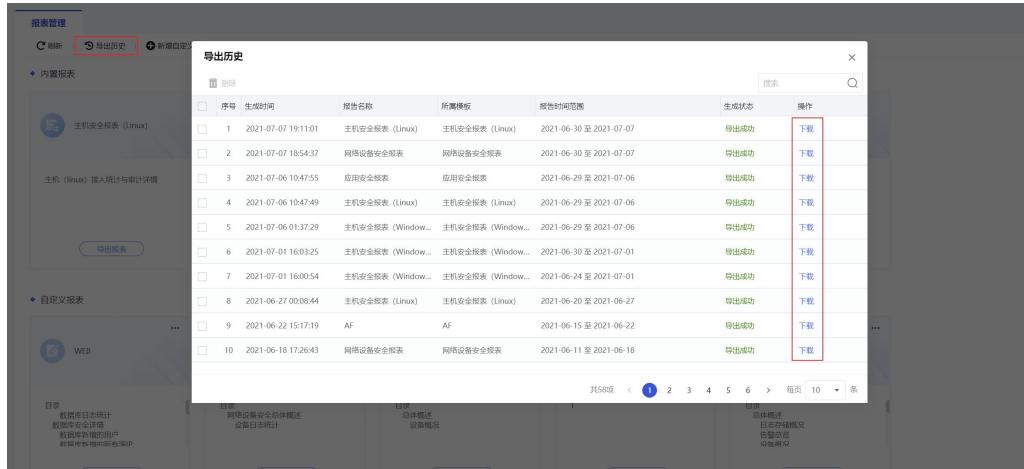
1. 导出报表

内置报表可选择每日、每周、每月进行报告生成，统计所选择时间周期的数据。

The dialog box is titled '导出报表'. It contains the following fields:
* 时间范围: A dropdown menu set to '最近7天' (Last 7 Days) with a calendar icon.
* 报告名称: A field with radio buttons for '默认' (Default) and '自定义' (Custom), with '默认' selected.
At the bottom are '确定' (Confirm) and '取消' (Cancel) buttons.

2. 下载并查看报表

点击去下载或者导出历史，可查看最近生成的报告，导出格式为.pdf。这里的报表LOGO可通过个性化的定制满足用户的需要，具体内容如下图。



主机安全报表 (Windows)

深信服日志分析系统

主机安全 (Windows) 总体概述

主机接入状态统计

共3台Windows主机接入，其中0台主机正常（24小时内有数据同步），3台主机异常（超过24小时没有同步数据）

序号	名称	IP地址	运行状态	最近一次同步时间
1	192.168.10.101	win7_合规跳板机	异常	2021-05-28 20:23:16
2	192.168.30.10	Winserver2008	异常	2021-05-28 20:39:49
3	192.168.20.107	win10-陈泽鑫	异常	2021-05-28 22:54:59

主机日志统计

共1台Windows主机接入，接入日志总数为47234条。

序号	主机IP地址	名称	致命	高危	中危	低危	信息	日志总数
1	192.168.10.101	win7_合规跳板机	-	2908	46	-	44280	47234

主机安全详情

主机登录的所有用户

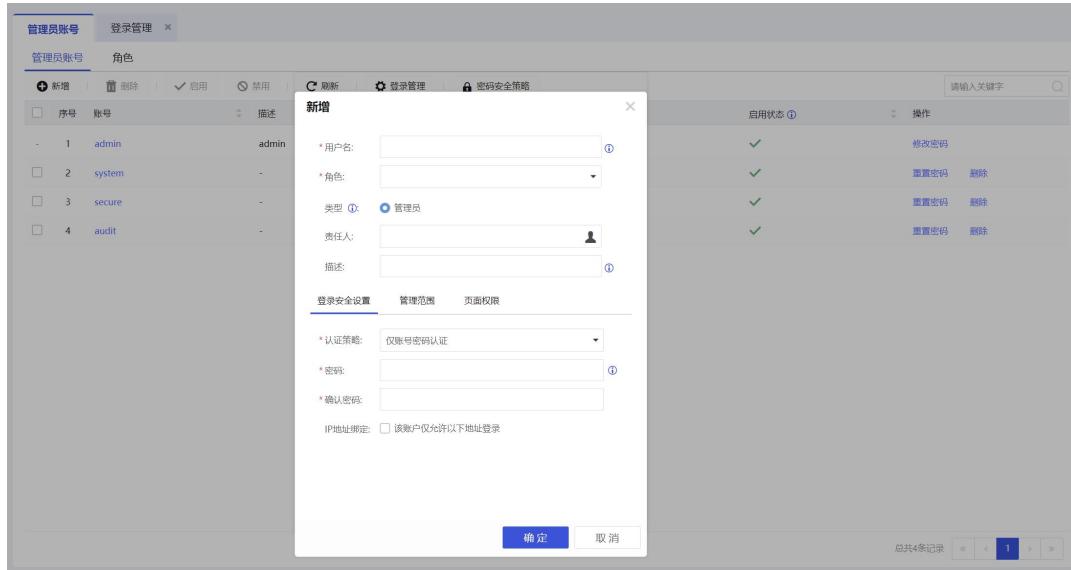
3.8. 系统管理

3.8.1. 系统设置

系统设置包括管理员账号、序列号设置、网络配置、通用配置。

3.8.1.1. 管理员账号

- 可以添加账号，修改账号密码，以及给账号分配权限，admin账号拥有最高权限。在[管理员账号]页面下，可以查看管理员账号、描述、管理范围、角色、责任人、启用状态以及操作信息，如下图所示。



其中：

角色：可以选择为普通管理员，系统管理员，安全管理员，审计管理员；

责任人：账号所有者；

描述：可以说明账号的用途；

登录安全设置：用于定义账号的登录方式；

认证策略：可以选择“仅账号密码认证”或“账号密码+USB-KEY认证”；

密码：用户名登录时使用的密码；

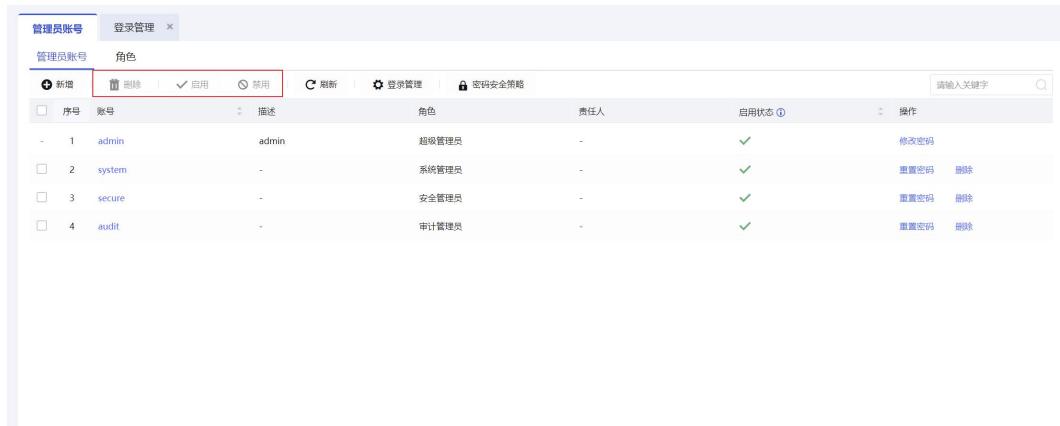
确认密码：对密码进行确认；

IP地址绑定：可以对当前账号进行IP绑定，只有绑定的IP才能登录平台；

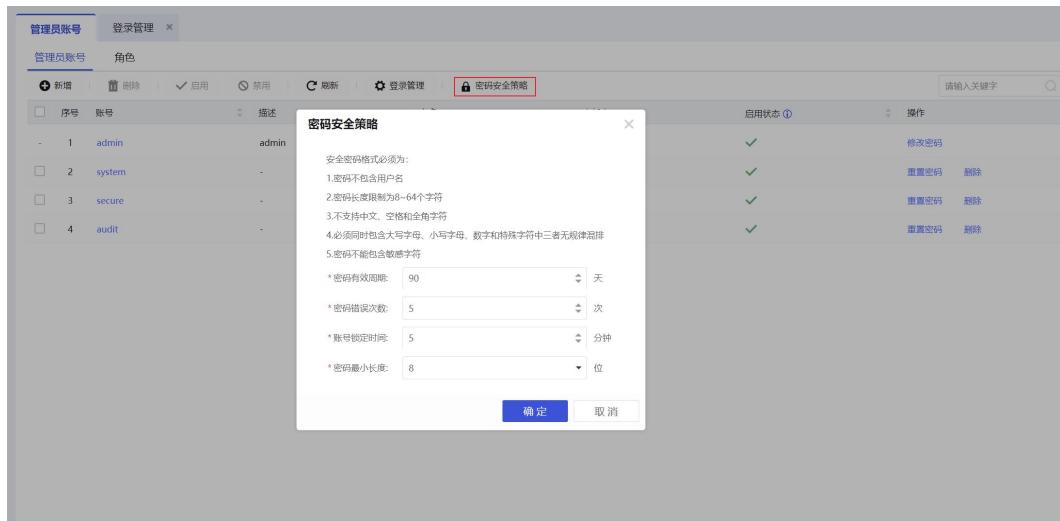
管理范围：可以选择账号可以管理的分支，只限于普通管理员可以选择分支，其它账号强制选择所有分支；

页面权限：对于普通管理员账号，可以对平台的功能模块赋予编辑或查看的权限。

对于已经建立的账号，可以点击<用户名>，对账号权限进行修改，也可以进行删除、启用、禁用等操作，便于运维管理，如下图。



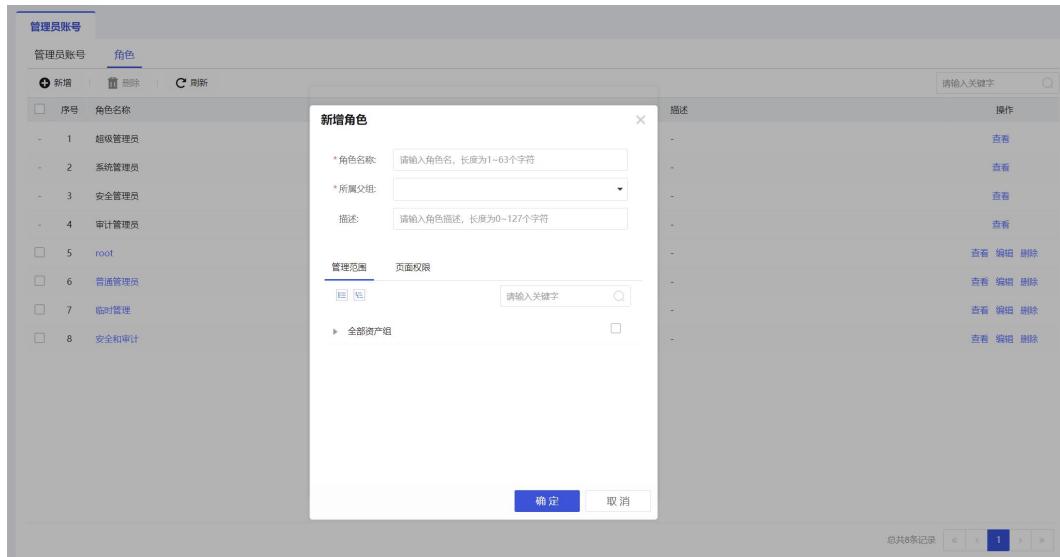
密码安全策略功能，符合电子政务网络标准，用户可以自定义密码复杂度，密码有效周期、密码错误次数、账号锁定时间、密码最小长度。对应设置值如下图。



密码不包含用户名；密码长度限制为8-15个字符；不支持中文、空格和全角字符；必须同时包含字母、数字、特征字符中两者。

2. 角色

默认系统存在超级管理员、系统管理员、安全管理员、审计管理员四个角色，可新增角色名称并赋予页面权限。



3.8.1.2. 序列号设置

查看功能序列号和序列号使用时间是否正确。【序列号设置】分为【基础项】和【增值项】。

【基础项】包括平台序列号、升级序列号，【增值项】为接入序列号，如下如所示。

接入序列号控制全部的设备接入，主要包括设备、系统；

设备：是指网络设备如路由器、交换机等、网络安全设备如防火墙、waf等；

系统：是指操作系统如linux、winodws等、中间件如apache、数据库如mysql、系统等；

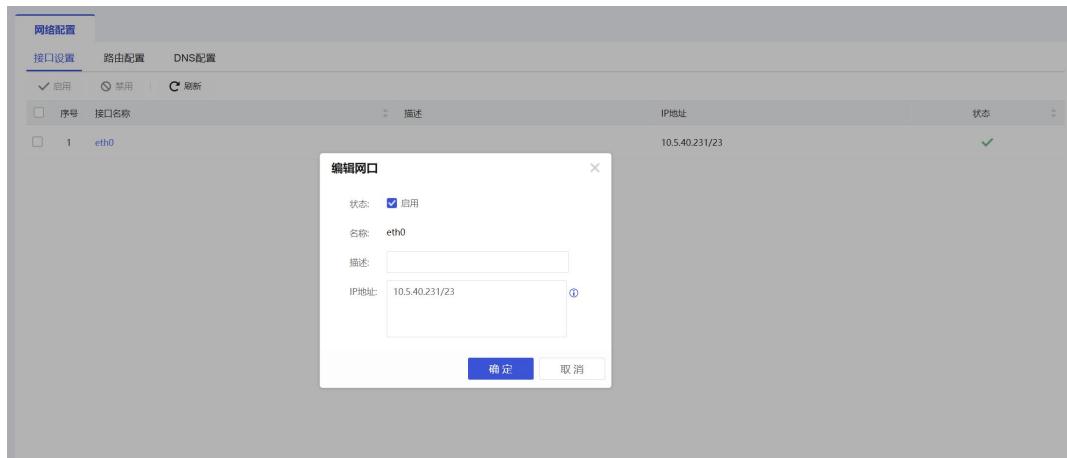
3.8.1.3. 网络配置

网络配置包括接口设置、路由设置、DNS设置。

1. 接口设置

需要先启用网口，再配置接口地址，启用网口时必需网口接入网线使网口灯亮起。

默认管理口为eth0，可以添加客户使用的IP地址，支持IPV6地址，支持一个接口配置多个IP地址。



2. 路由配置

默认情况下配置一条默认路由指向接口的网关即可，可以支持IPV6。

3. DNS配置

可配置DNS服务器，用于设备进行解析。

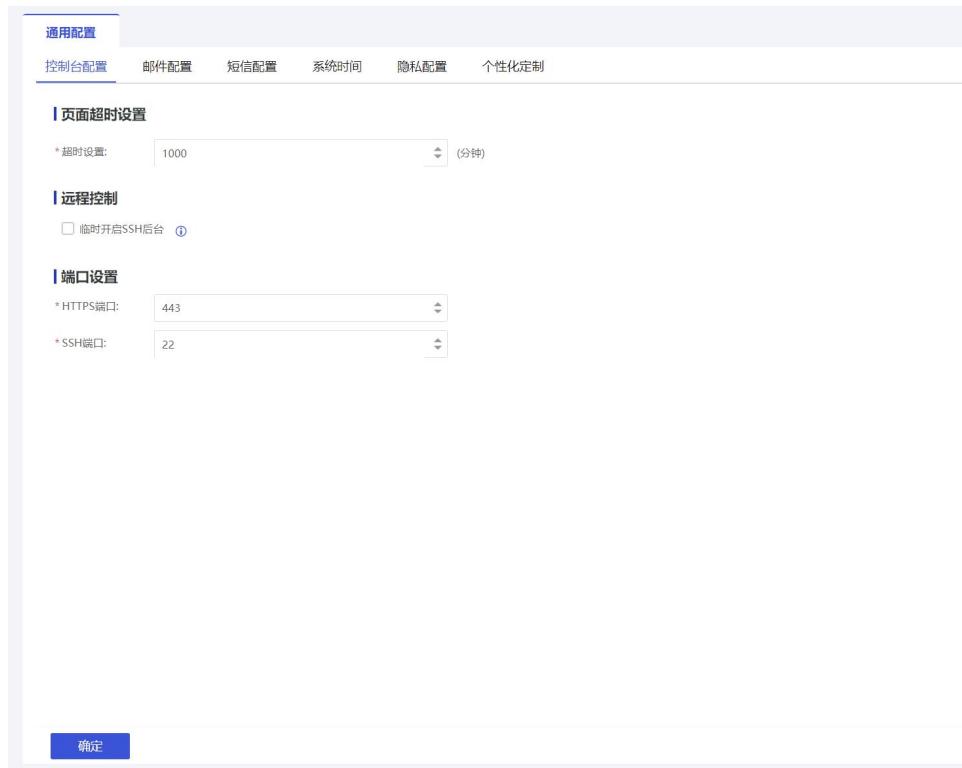


3.8.1.4. 通用配置

通用配置包括控制台配置、邮件配置、短信配置、系统时间、隐私配置，个性化定制。

1. 控制台配置

对控制台进行配置，如下图所示。



其中：

页面超时设置：管理员登录平台时，超过设置时间后会被即出登录；

远程控制：用于研发登录SIP-Logger平台的后台排查问题使用；

升级控制：用于升级，需注意若勾选临时开启，则8小时后自动关闭；

服务控制：勾选允许ICMP响应；

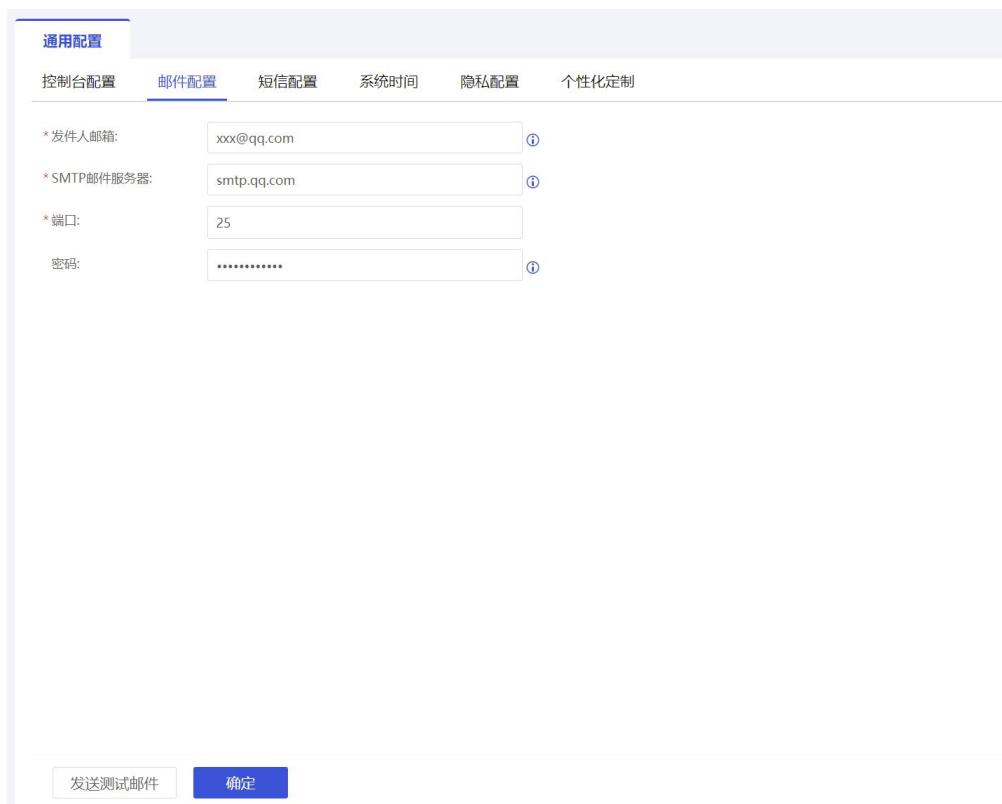
高性能设置：开启高性能模式，平台界面的响应速度更快；

检测模式：正常使用情况下使用标准模式，在POC测试时再开启POC模式；

当前平台名称：修改当前平台的名称。

2. 邮件配置

发送邮件所使用的邮箱信息配置。包括收件人邮箱、端口等配置。



其中：

发件人邮箱：发送告警或报告的邮箱；

SMTP邮件服务器：用于发送邮件的邮件服务器地址；

端口：邮件服务器的端口，默认情况下是25端口；

密码：用于登录邮箱的密码。

3. 短信配置

发送短信所使用的信息配置。支持阿里云、腾讯云短信网关，以及短信猫发送短信，如下图所示。

The screenshot shows the 'SMS Configuration' tab selected under the 'General Configuration' section. It includes fields for Aliyun SMS platform selection, AccessKey ID, Access Key Secret, and SMS signature. Below these are sections for alert message templates and a button to send a test message.

* 短信平台: 阿里云
* AccessKey ID: 请输入AccessKey ID
* Access Key Secret: 请输入Access Key Secret
* 短信签名: 请输入短信签名
安全告警-短信模板配置 帮助
* 补丁包更新告警模版CODE: 请输入补丁包更新告警模版CODE
* 告警通知模版CODE: 请输入告警通知模版CODE
发送测试短信 确定

4. 系统时间

需要配置当前的时间，错误的时间会对平台的安全事件或展示有不良影响。或平台可以联网，建议开启NTP时间同步，如下图所示。

The screenshot shows the 'System Time' tab selected under the 'General Configuration' section. It includes fields for date/time selection, NTP synchronization, and NTP server configuration.

日期/时间
系统日期/时间: 2021-07-08 19:17:59 获取本地时间 获取系统时间
开启NTP时间同步
NTP服务器: pool.ntp.org

5. 隐私配置

建议勾选，参与用户体验改进计划，优化用户的体验。

The screenshot shows the 'Privacy Configuration' tab selected under the 'General Configuration' section. It includes a checkbox for participating in user experience improvement plans.

隐私设置
参与用户体验改进计划 ① 了解用户隐私保护条款

6.个性化定制

可通过自定义的方式实现平台文案和LOGO的定制

通用配置

个性化定制

平台文案定制

* 平台名称： 可自定义新的平台名称，将替换平台内登录页、导航栏等所有涉及到“深信服日志分析管理系统”字眼的地方

* 公司名称： 可自定义新的公司名称，将替换平台内登录页、报告内等所有涉及到“深信服”字眼的地方

深信服相关信息： 我已查看并同意[深信服相关条款](#)

保存

平台LOGO定制

新上传的图片将替换之前的平台LOGO、平台小LOGO、网页LOGO、企业LOGO [查看替换区域](#)

平台LOGO 下载示例文件	平台小LOGO 下载示例文件	网页LOGO 下载示例文件	企业LOGO 下载示例文件
支持：仅 png 格式，不超过 500KB 建议尺寸：241*32（像素）	支持：仅 png 格式，不超过 500KB 建议尺寸：80*80（像素）	支持：仅 png 格式，不超过 500KB 建议尺寸：41*40（像素）	支持：仅 png 格式，不超过 500KB 建议尺寸：101*35（像素）
替换			
恢复默认			

3.8.2. 系统维护

3.8.2.1. 恢复/重启

用于平台的恢复出厂设置与平台的重启操作。

- 在[系统设置/系统维护/恢复/重启]页面下，点击<恢复出厂设置>，将删除平台所有的数据以及配置，需谨慎操作。
- 点击<立即重启>，将重启安全感知平台，由于安全感知平台为单臂部署在网络中，重启不会对网络造成影响。
- 点击<恢复用户配置>，可以将平台的配置进行导出备份，并可导入恢复配置。

系统选项

恢复出厂设置

立即重启

恢复用户配置 ①

导入用户配置 **导出用户配置**

3.8.2.2. 数据备份

数据备份，当前支持对审计到的原始日志、自身操作日志进行备份，上传到FTP服务器。

备份策略的配置

1. 点击<新增>，可以设置数据备份的策略。
2. 设置策略名称以及存放路径，点击<测试连接>，测试连通性。
3. 输入FTP账号密码，选择备份时间，点击<确认>，当前的数据备份策略配置完成。

其中：

策略名称：备份策略的名称；

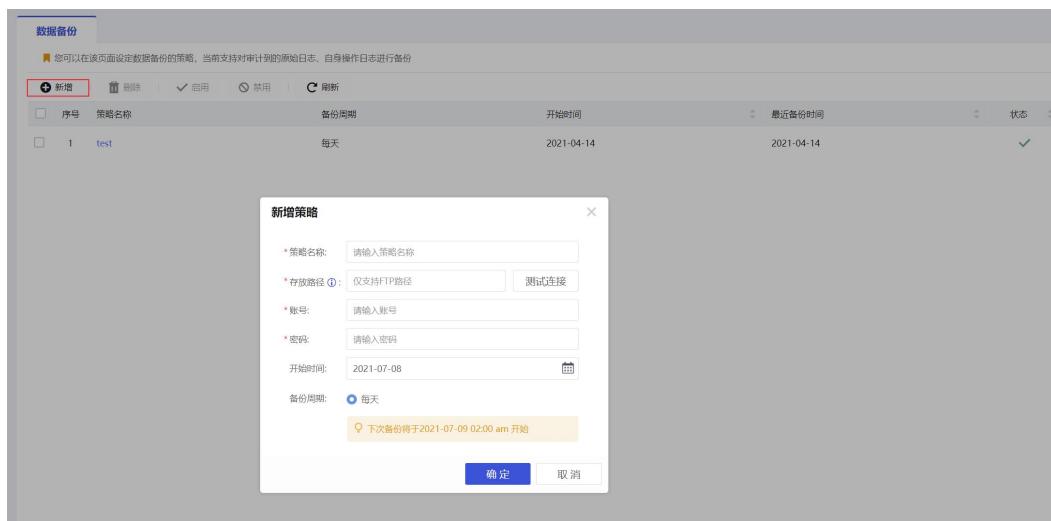
存放路径：配置FTP服务器上存放备份文件的路径；

账号：FTP服务器的账号；

密码：FTP服务器对应账号的密码；

开始时间：选择开始备份的时间；

备份周期：每天将进行备份。



3.8.3. 升级管理

3.8.3.1. 系统升级

日志分析管理系统升级步骤：

1. 在深信服社区（<https://bbs.sangfor.com.cn>）下载升级包，并校验MD5值；

2. 登录日志分析管理系统，在[设置/升级管理/系统升级]页面，将已下载并验证完成升级包导入平台。
3. 升级包导入完成后，日志分析管理系统会进行自动升级，等待升级完成即可。

3.8.3.2. 补丁更新

此位置可更新和加载.zip的补丁包，用于临时解决问题。

3.8.3.3. 规则库升级

默认升级包中自带规则库升级策略，这里仅可查看版本。

3.8.3.4. 升级设置

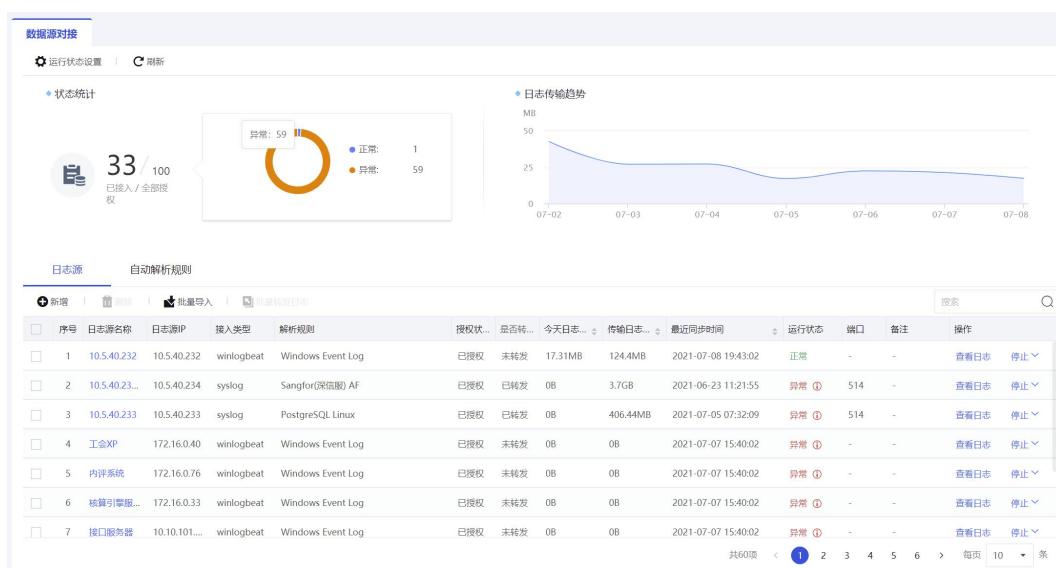
在【系统设置/升级管理/升级设置/升级服务器设置】页面下，点击<测试服务器>进行升级服务器连通性确认，如需使用http代理访问互联网，可进行[代理设置]，启用代理服务器功能，配置页面如下图所示。

说明：

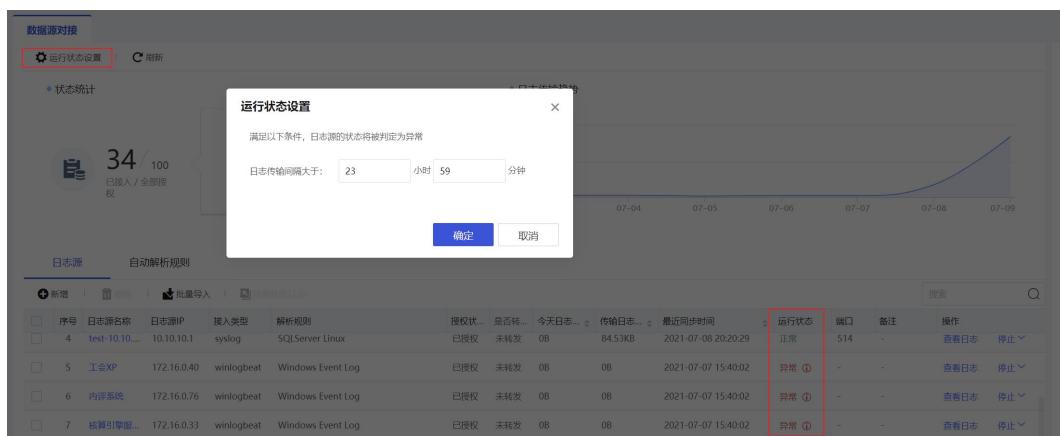
升级服务器无固定IP，若只放通升级时，需以域名的方式放通，深信服全国有三个升级服务器，地址分别为：update1.sangfor.net；update2.sangfor.net；update3.sangfor.net。

3.8.4. 数据源对接

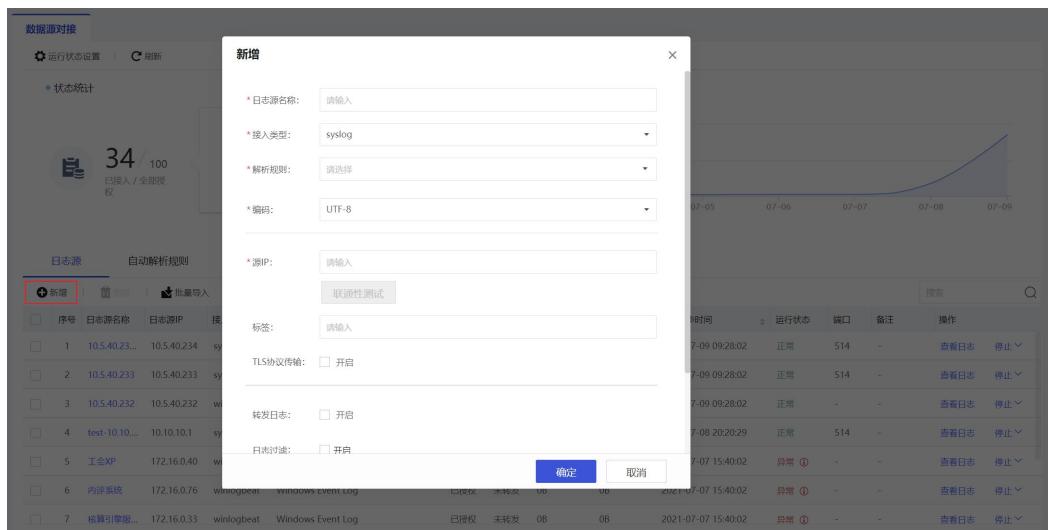
平台通过接入数据源对接实现众多第三方产品SYSLOG日志及操作系统的日志信息采集，管理员可查看当前日志接入的情况。通过状态统计，展示出当前已接入设备数，并以天为单位展示日志传输趋势。



运行状态设置表示，满足设定的日志传输间隔时，日志源状态就被判定为异常，如下图所示的日志源运行状态。



3.8.4.1. 新增日志源



其中：

日志源名称：输入自定义名称

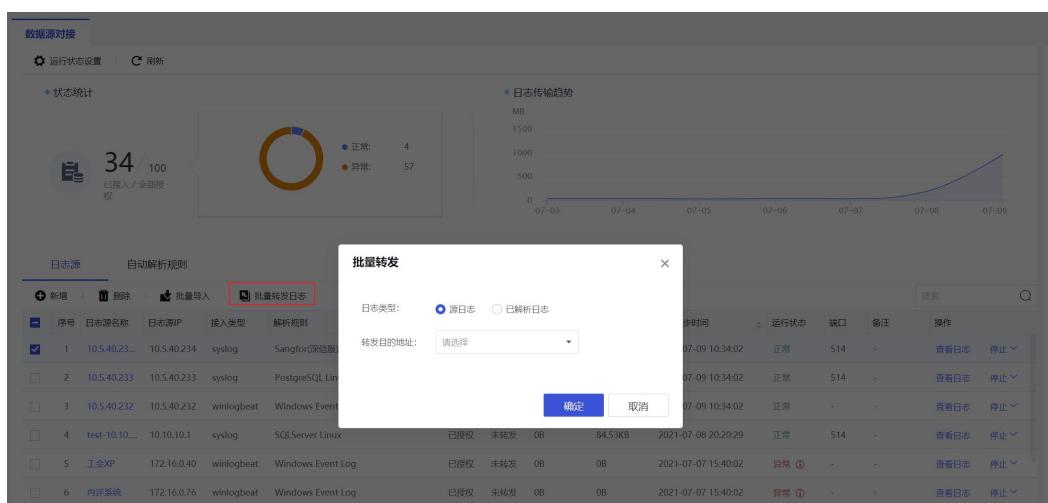
接入方式：采集器接入方式，如Syslog、winlogbeat、WMI、jdbc、FTP等；

解析规则：即采集类型或名称，如360SNA NDAS、Alcatel NOC等；

编码方式：支编码方式一般为UTF-8，同时也支持GBK、ASCII-88IT等上百种编码。

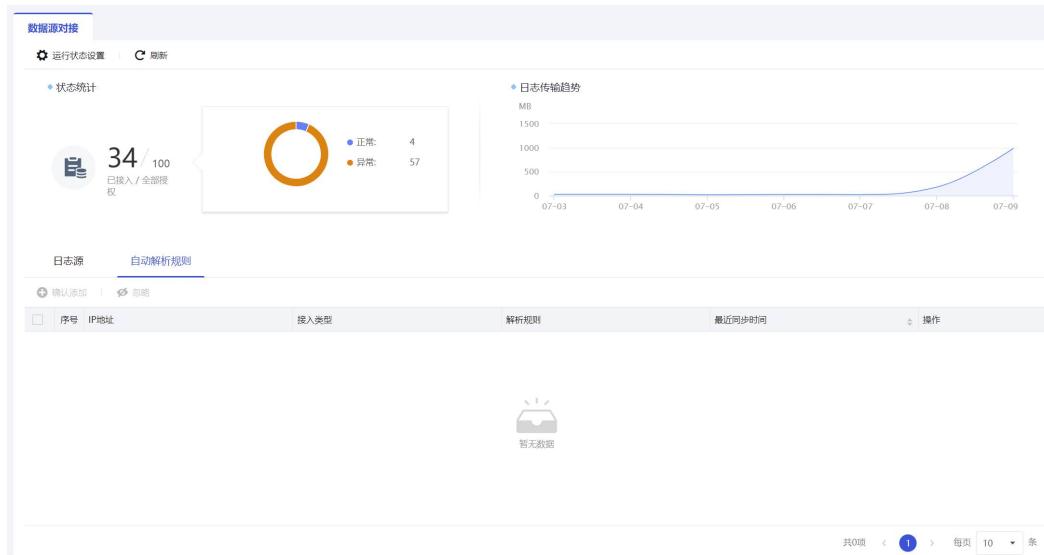
3.8.4.2. 批量日志转发

用户可通过设置转发目的服务器，将采集到的原始日志和解析后日志分别进行转发。



3.8.4.3. 自动解析规则

目标设备通过syslog或者插件的方式发送到SIP-Logger之后，若没有配置日志源和解析规则，就会使用默认的Other规则解析并放入自动解析规则栏，用户通过实际需要可选择确认添加或忽略。

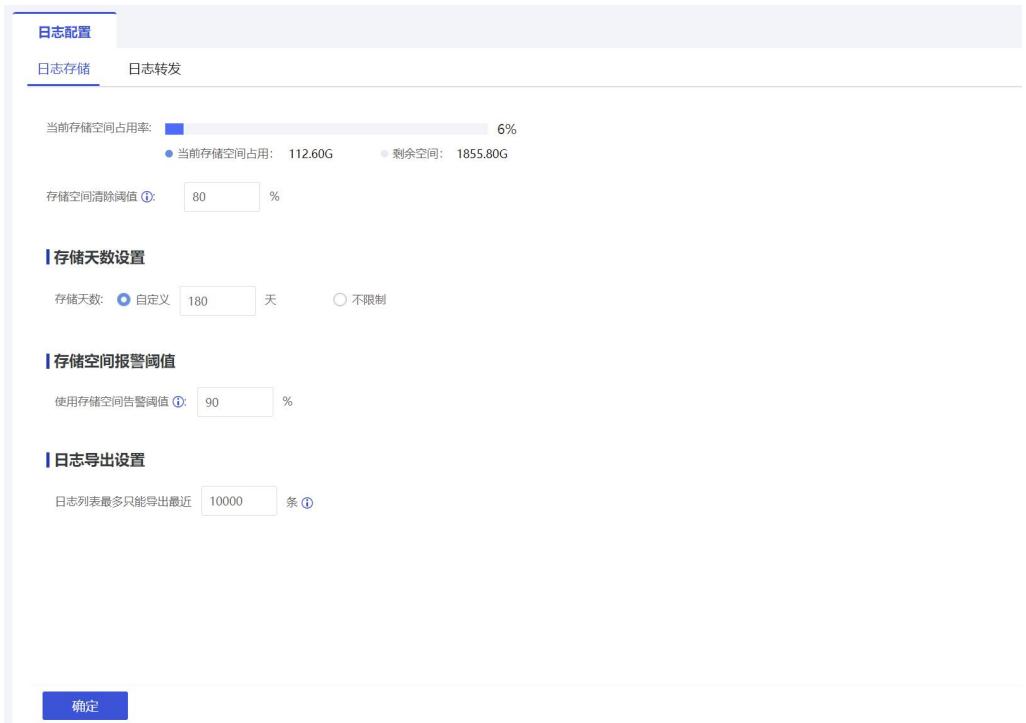


3.8.5. 系统工具

3.8.5.1. 日志配置

1、日志存储

可以直观的展示存储空间利用率，存储天数等相关设置。



2、日志转发

前置条件：SIP-Logger已经收到目标设备发送过来的日志且需要客户提前准备好服务器并保证服务可达。

注意：

- (1) SIP-Logger支持单个日志源转发和多个日志源批量转发；
- (2) 日志转发要设置定时转发，建议选择凌晨进行转发操作，避免影响业务运行。

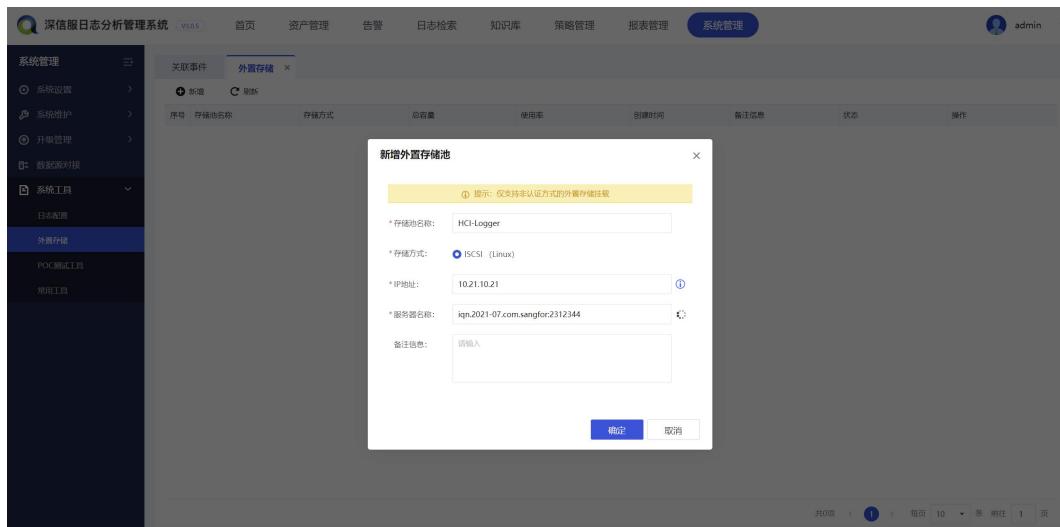
日志配置						
日志存储		日志转发				
+ 新增		X 删除		定时转发		C 刷新
序号	服务器名称	服务器类型	IP地址/kafka集群地址	发送端口/kafka主题	最近修改时间	操作
1	深信服态势感知SIP平台	kafka	1.1.1.12	1	2021-04-23 14:25:34	X
2	test	syslog	1.1.1.1	514	2021-04-30 15:05:13	X

3.8.5.2. 外置存储

如果通过接收的日志量计算磁盘剩余空间无法满足存储要求，可使用外置存储方式，目前仅支持ISCSI免密认证外置存储挂载方式。

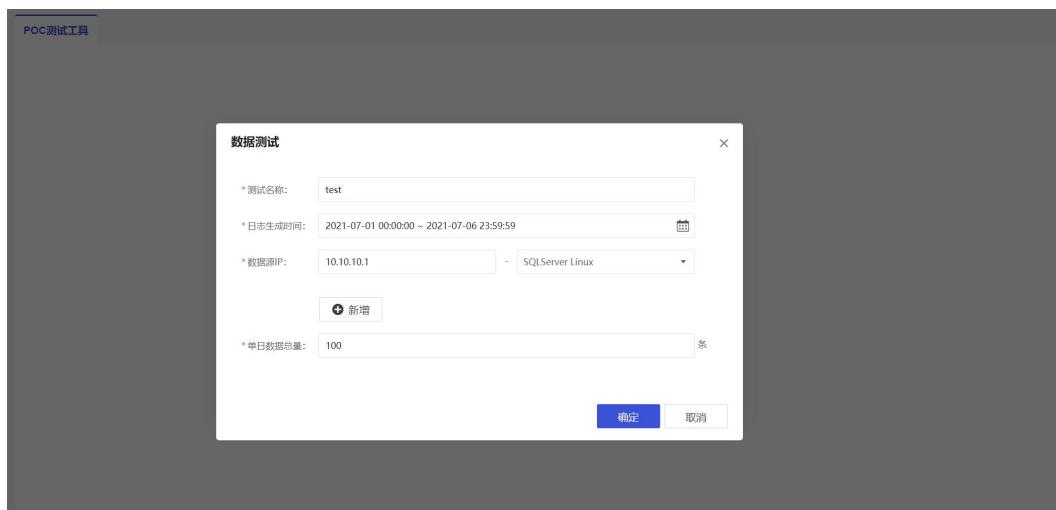
注意：

- (1) 外置存储挂载时，尽量保持被挂载路径下无其他内容，请勿对目标共享路径内的文件进行任何操作；
- (2) 挂载成功后，设备本身的存储空间达到50%，才会将后续日志转移到外置服务器，转移时，优先转移稍早前数据；
- (3) 存储池挂载期间将重启ES，重启时产生的日志将无法保存。

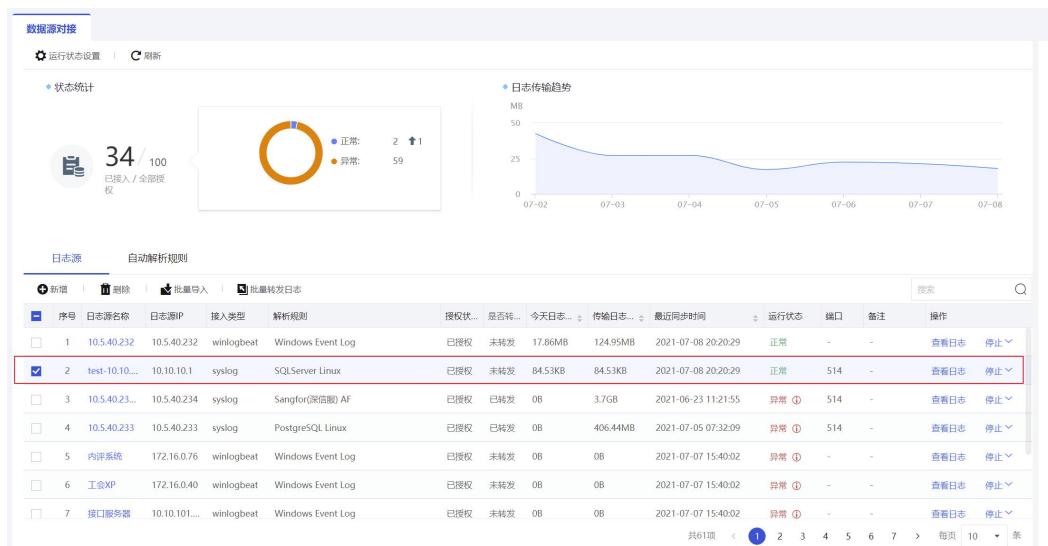


3.8.5.3. POC 测试工具

此功能主要是通过POC的方式构造日志数据，前期为客户测试做相应的数据支撑。新增数据测试时，日志生成时间必须为当前时间之前。



测试任务完成后，可在日志源对接处查看到对应的条目。



3.8.5.4. 常用工具

为SIP-Logger产品排障设计了相应的模块，支持ping、telnet命令，可探测SIP-Logger到目标设备的网络连通性和端口是否可达，其中ping命令支持合法IP和域名。

The screenshot shows the 'Common Tools' module. At the top is a search bar with the placeholder '请输入合法IP或域名, 支持IPv4、IPv6' and a '立即查询' button. Below it is a large input field labeled 'ping' with a dropdown arrow. The main area is titled 'Basic Information' and contains a 'Query Result' section which is currently empty.

4. 运维管理

本章主要讲解产品的运维管理，为管理员例行维护设备以及简单故障排除提供指导。

4.1. 日常运维注意事项及高危操作

风险操作	风险级别	风险说明	风险应对
修改 IP 会重启设备，设备暂不可用，恢复时间大概 5 分钟	高风险	会导致设备无法登陆	联系售后工程师处理
在只有一个网口状态为启用时，将启用设置为禁用	高风险	会导致设备无法登陆	联系售后工程师处理
恢复出厂设置	高风险	将会删除选中的数据与配置信息，对有保存日志合规要求的客户有极大的影响（等保要求保留 180 天的日志）	删除后无法恢复，操作时需获得平台相关方同意后再操作
升级未完成进行重启操作	高风险	升级时错误操作严重可能导致设备无法正常使用	等待升级列表出现升级成功，在根据升级需求进行重启操作
点击重启系统	高风险	设备受影响，不可使用	设备正常运行不需要重启，请谨慎使用该功能

4.2. 日常巡检

此产品暂无自动巡检功能，需要人工定期手动巡检。

4.2.1. 硬件检查

检查项	检查内容
设备灯	查看设备前面板显示灯是否正常
网口灯	查看设备接入网线网口工作是否正常

4.2.2. 软件检查

检查项	检查内容
控制台	查看控制台是否可以通过浏览器远程登录并管理
日志源接入状态	查看接入状态是否异常

设备情况	查看平台显示CPU、内存、磁盘是否显示正常
每秒传输日志量	查看平台每秒传输日志量(eps)是否超过平台可承受范围
序列号	查看平台序列号是否过期
接口设置	查看网络接口是否工作正常

4.3. 常见问题排查

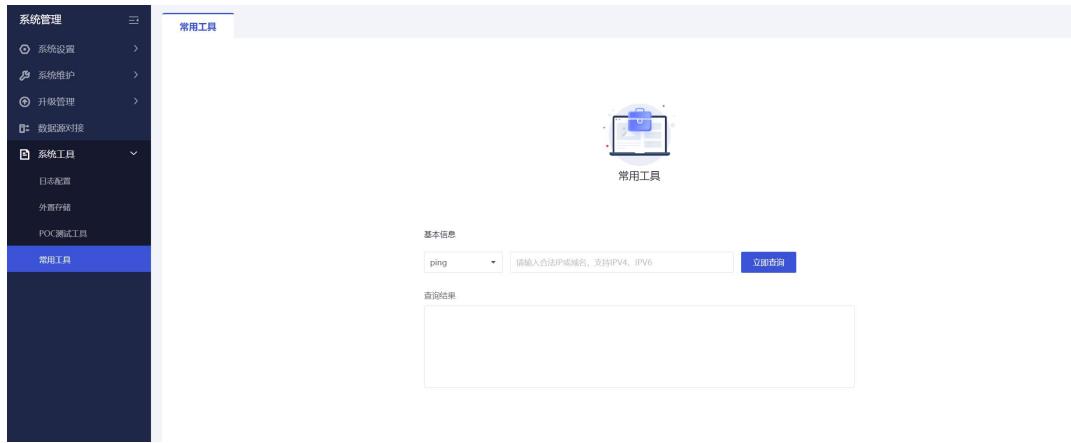
4.3.1. 日志检索问题

针对常见日志检索问题，管理员可在平台右上角点击<帮助>，跳转至【日志检索】页面进行查询与并依指导进行相应处置，如下图所示。

The screenshot displays two main sections of the SIP-Logger interface:

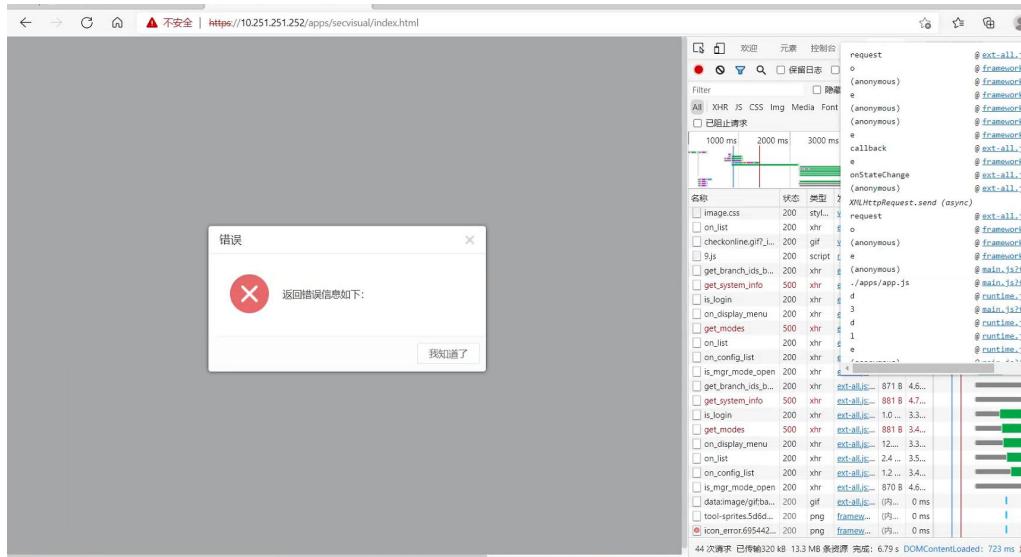
- Top Section (Homepage):** Shows real-time log storage statistics (100 days stored, 1685 days available), log reception trends (2762 total, 46.03 eps), and device status (CPU 13%, Disk 1%, Memory 67%). It also includes a 'Help' menu icon.
- Bottom Section (Help Documentation):** Titled '帮助文档' (Help Document), it shows the '操作手册' (Operation Manual) section. This section includes a search bar, a sidebar with navigation links like '日志检索', and a main content area for '新增过滤条件检索' (Add Filter Condition Search). The content area contains a detailed guide with numbered steps and examples for querying multiple IPs and IP ranges.

针对常见部署环境问题，可通过下图位置的常用工具协助排查。



4.3.2. 无法登录设备控制台

问题描述：到设备网路可达，443端口可以telnet上，无法登录控制台，提示“返回错误信息如下”

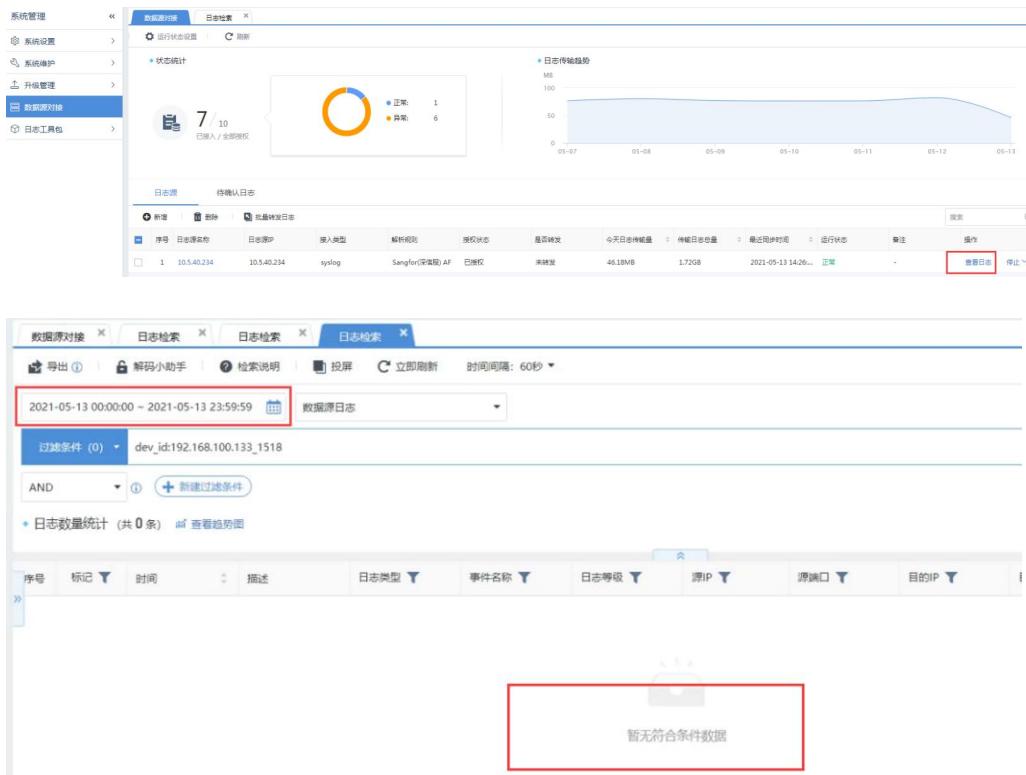


解决方案：

- 1、更换浏览器测试；
- 2、多次尝试登录前端都是报错，可联系研发解决。

4.3.3. 无法检索日志

问题描述：在设备的数据源对接找到有传输日志的设备并点击“查看日志”，在跳转的日志检索页面中提示“暂无符合条件数据”，如下图所示



解决方案：

- 1、调整设备系统时间与实际时间保持一致即可
- 2、跟踪观察，如果还是无法检索，可联系研发解决

4.4. 突发事件应急处理

如遇设备硬件故障和软件问题，请第一时间联系深信服工程师或深信服售后服务热线
400-630-6430。