用户手册

四叶草安全日志收集与分析系统

西安四叶草信息技术有限公司

版权声明

商标声明

本手册中所谈及的产品名称仅做识别之用，而这些名称可能属于其他公司的注册商标或是版权，其他提到的商标，均属各该商标注册人所有，恕不逐一列明。

产品声明

本手册中提到的产品功能或性能可能因产品具体型号、配备环境、配置方法不同而有所差异，由此可能产生的差异为正常现象，相关问题请咨询四叶草安全公司技术服务人员。

免责声明

若因本手册或其所提到的任何信息引起的直接或间接的资料流失、利益损失，四叶草安全公司及其员工均不承担任何责任。

目录

一、前言

1.1 导言

本用户手册主要介绍四叶草安全日志收集与分析系统的安装、配置、使用和管理。通过阅读本文档，用户可以了解日志审计系统的基本配置方法及如何使用 web 控制台对安全设备、网络设备、主机、操作系统、用户业务系统及其它设备和应用的日志、事件、报警等信息进行审计分析。

1.2 产品概述

西安四叶草信息技术有限公司自主研发的四叶草安全日志收集与分析系统是新一代综合安全事件分析平台。该系统采用先进的大数据采集、建模、分析技术，通过对各种网络资源的多维度信息采集和自动化的关联分析，及时发现网络当中的威胁和异常行为。四叶草安全日志收集与分析系统实现对多种设备以及多种采集方式的日志和事件支持，并提供强大的日志和事件处理、统计、分析、查询及告警等功能。同时以图形化、可视化技术将识别到的各种威胁和异常通过图形化方式直观的展现给用户，有利于用户全面掌握网络总体安全态势，并迅速做出判断和决策。

四叶草安全日志收集与分析系统是一个全面的、智能的网络日志和事件管理、分析工具。产品安装简单，操作方便，提供丰富的日志和事件管理、分析功能。

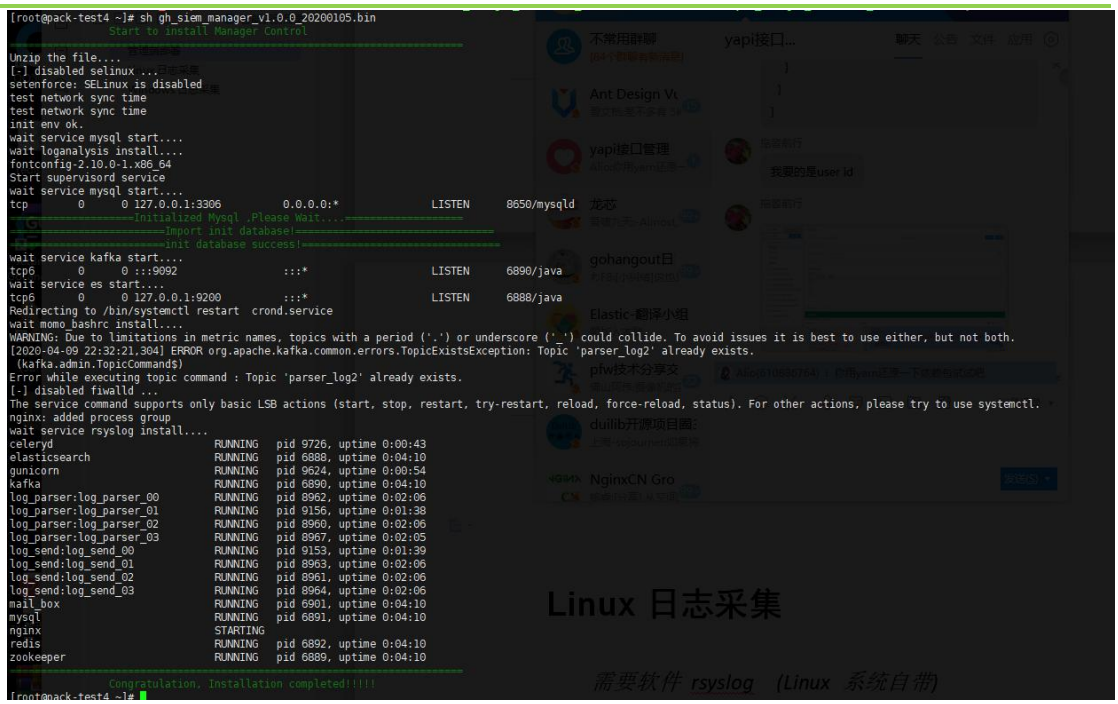
1.3 产品安装与卸载

1.3.1 运行环境

管控中心操作系统支持 centos7 以上，建议使用 centos7.2，最小化安装，配置至少 2 核 CPU、8G 内存及 500G 硬盘。

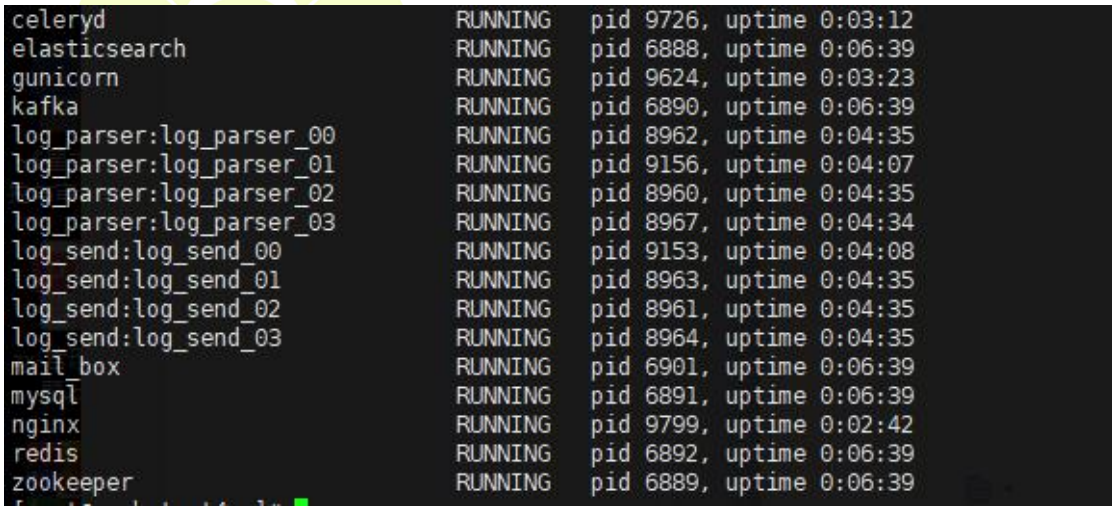
1.3.2 管控中心安装

执行 #sh gh_siem_manager_v1.0.0_20200105.bin



执行成功后，查看管控中心相关服务状态：

执行 #supervisorctl status



1.3.3 管控中心卸载

卸载执行：

```
#cd /opt/ghsoc/script/
#sh uninstall.sh
```

1.3.4 Linux 日志采集

注：需要软件 rsyslog (一般情况下 Linux 系统会自带该软件)。

- UDP 协议发送

修改 rsyslog 配置文件/etc/rsyslog.conf

追加: *.* @report-ip

例如:

vim /etc/rsyslog.conf

. @192.168.21.111

- TCP 协议发送

修改 rsyslog 配置文件/etc/rsyslog.conf

追加: *.* @report-ip

```
#
# An on-disk queue is created for this action. If the remote host is
# down, messages are spooled to disk and sent when it is up again.
#$ActionQueueFileName fwdRule1 # unique name prefix for spool files
#$ActionQueueMaxDiskSpace 1g   # 1gb space limit (use as much as possible)
#$ActionQueueSaveOnShutdown on # save messages to disk on shutdown
#$ActionQueueType LinkedList   # run asynchronously
#$ActionResumeRetryCount -1    # infinite retries if host is down
# remote host is: name/ip:port, e.g. 192.168.0.1:514, port optional
#*.* @@remote-host:514
# ### end of the forwarding rule ###

*.* @192.168.21.111
~
```

1.3.5 Windows 日志采集

注：需要安装软件 nxlog-ce-2.10.2150.msi。

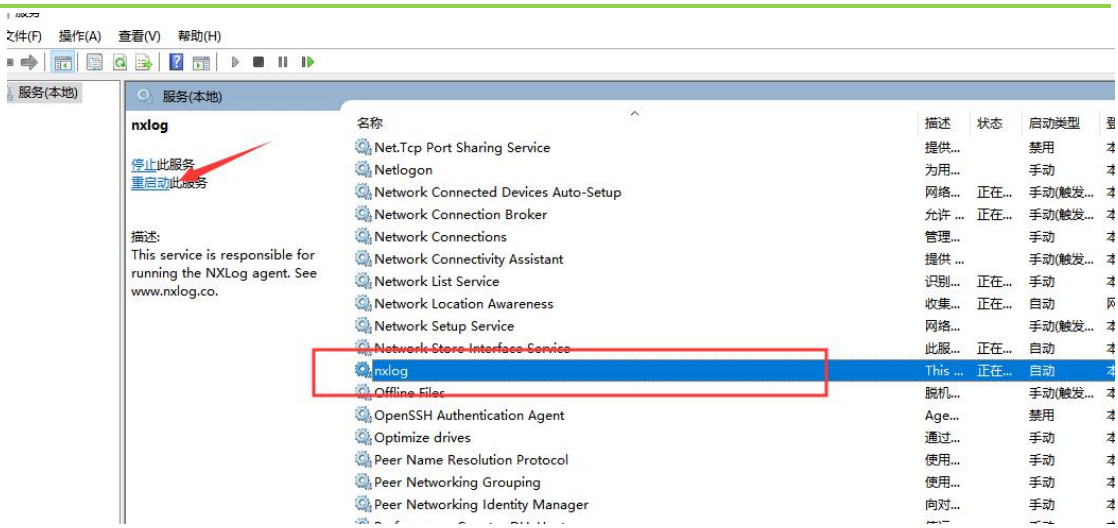
安装完成后进入安装目录 默认:C:\Program Files (x86)\nxlog\，进入 conf 文件夹，修改 nxlog.conf 配置并保存。

```
Panic Soft
#NoFreeOnExit TRUE


define ROOT     C:\Program Files (x86)\nxlog
```

```
define CERTDIR  %ROOT%\cert
define CONFDIR  %ROOT%\conf
define LOGDIR   %ROOT%\data
define LOGFILE  %LOGDIR%\nxlog.log
LogFile %LOGFILE%


Moduledir %ROOT%\modules
CacheDir  %ROOT%\data
Pidfile   %ROOT%\data\nxlog.pid
SpoolDir  %ROOT%\data


<Extension syslog>
    Module          xm_syslog
</Extension>


<Input eventlog>
    Module          im_msvistalog
</Input>


<Output tcp>
    Module          om_tcp
    Host            192.168.21.197  # 这里替换成接受日志服务器 ip
    Port            514
    Exec            to_syslog_bsd();
</Output>


<Route eventlog_to_tcp>
    Path            eventlog => tcp
</Route>
```

打开服务管理(win + r 输入 services.msc)

找到 nxlog 服务，重启服务即可。



1.4 访问 Web 界面

四叶草安全日志收集与分析系统管控中心登录方式默认使用安全的 https 登录。默认的登录地址是：https://IP。（IP 为安装管控中心的 Linux 服务器 IP 地址）。浏览器支持火狐、谷歌等主流浏览器，打开浏览器，输入登录地址后，会有一个安全提示，点击 接受风险并继续 ，会跳转至登录界面：

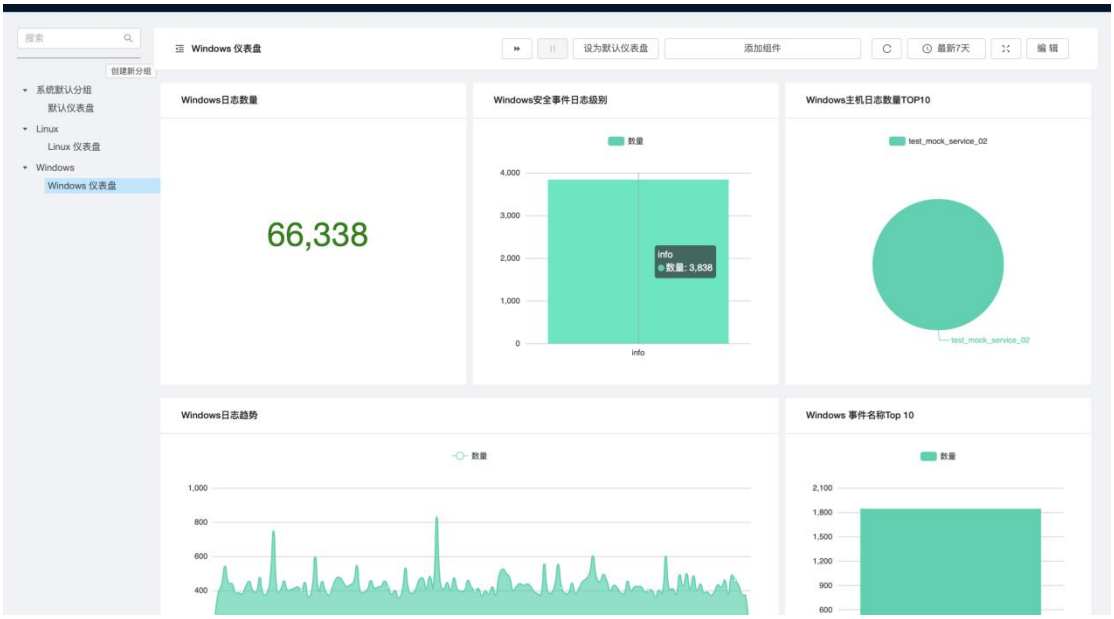
默认登录用户名和密码是：admin/Seclover1234!@#$

二、 仪表盘

仪表盘共分为 2 个部分：工作台和组件管理。

2.1 工作台

工作台主要以分组的形式展示系统的关键图表信息，工作台支持个性化设置，并能够分组展示不同来源设备或不同类型的日志统计信息。不同的系统管理员也可通过分组来单独创建工作台，帮助他们快速查看其关注的统计信息。



- 仪表盘分组

通过分组显示预定义以及管理员用户自定义的图表内容，点击该分组名称，则在

分组显示区显示该分组的内容。

支持对分组名称进行新建、删除及重命名操作。

- 仪表盘内容

支持管理员在分组内自定义编辑组件内容，同时可以通过选择时间范围展示最近 30 分钟、1 小时、1 天、3 天、7 天、15 天、30 天的图表统计信息，也可根据需要进行自定义时间配置。

仪表盘界面支持全屏显示。

2.2 组件管理

支持对组件进行统一分组管理，将不同类型组件归类到一组。支持新增、重命名及删除等操作。

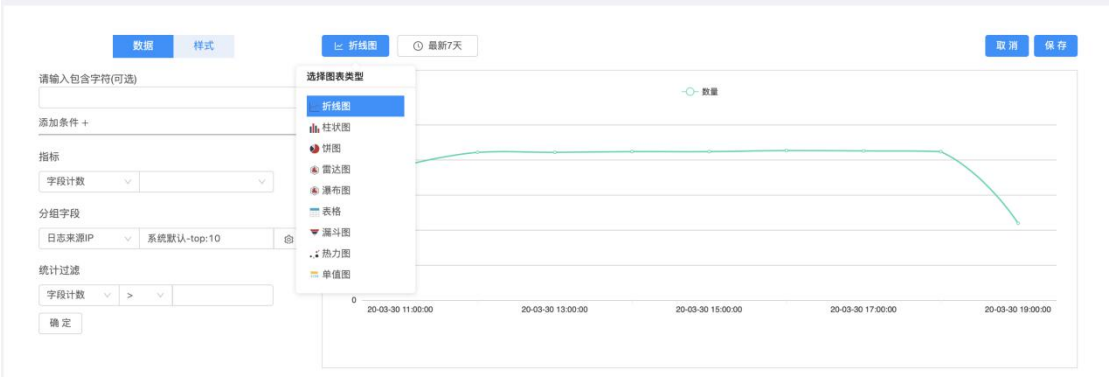
组件以列表形式展示，列信息包括组件名、组件类别、描述信息、创建时间及编辑、删除操作。

除了系统内置的图表组件之外，还支持自定义添加图表组件，能够自定义数据信息及图表样式设置。

数据信息包括：自定义组件名称、添加条件、图表类型定义、数据统计类型、分组字段定义及统计过滤条件定义等；其中，图表类型包括折线图、柱状图、饼图、雷

达图、瀑布图、表格、漏斗图、单值图及热力图等；数据统计类型包括计数、字段计数、求和、平均值、最大值及最小值等。

样式设置包括：图例位置、是否填充及 x 轴标签的样式。



三、 资产管理

资产管理共分为 2 个部分：资产维护和资产列表。

3.1 资产维护

管理员可以通过资产维护对资产设备进行管理，并可以进行修改、查询等操作。

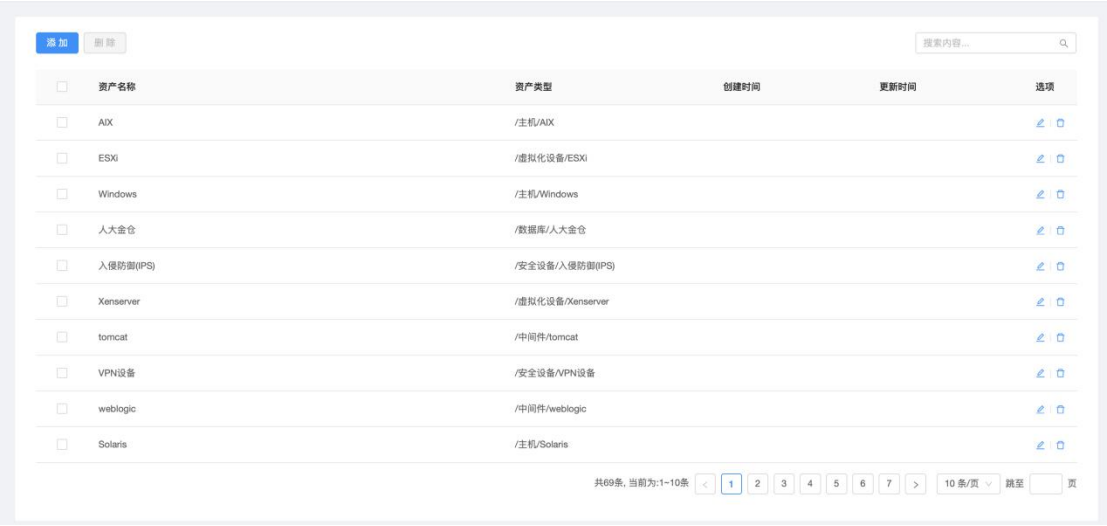
点击【添加】按钮，支持手动添加资产信息。添加资产时，需要填写资产名称、资产类型、IP 地址、资产组、机密性、完整性、可用性、资产价值、保密级别、生产厂商、序列号、MAC 地址、地理位置、负责人及描述等信息。

同时支持资产与告警事件进行关联，能够从资产列表中查看与该资产相关联的告警信息。告警列表信息包括：告警名称、级别、阶段、开始时间、结束时间、告警类型、告警次数及告警主机数量。

支持资产批量导入、导出操作。

3.2 资产列表

系统内置主机、网络设备、安全设备、数据库、中间件、存储设备、应用系统、虚拟化设备、机房设备及其他等多种类型的资产，便于统一管理维护添加的资产信息及日志源设备信息。支持自定义添加资产类型操作。



四、 设备

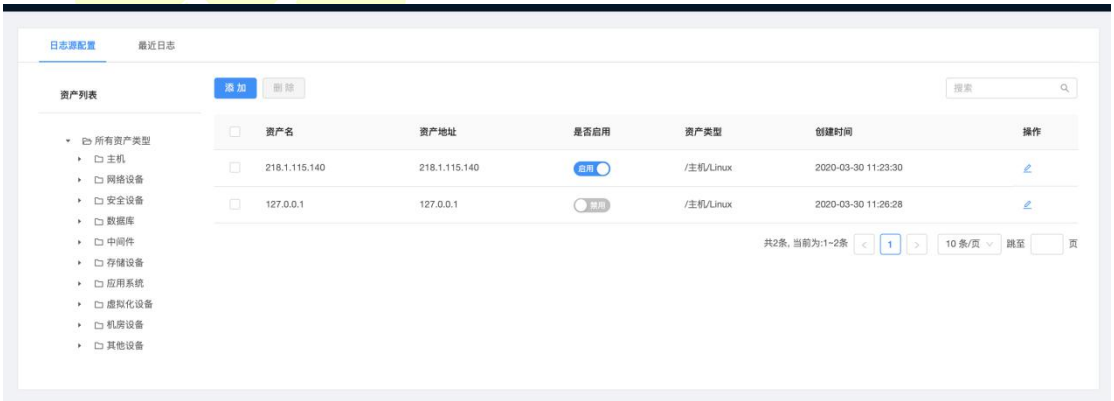
设备共分为 2 个部分：日志源和过滤器

4.1 日志源

管理员可以手动添加日志源设备，右边是系统内置的资产类型，管理员可根据需要在某类型下添加该类型的设备。只有添加设备信息并启用，系统才会接收该设备对应的日志。

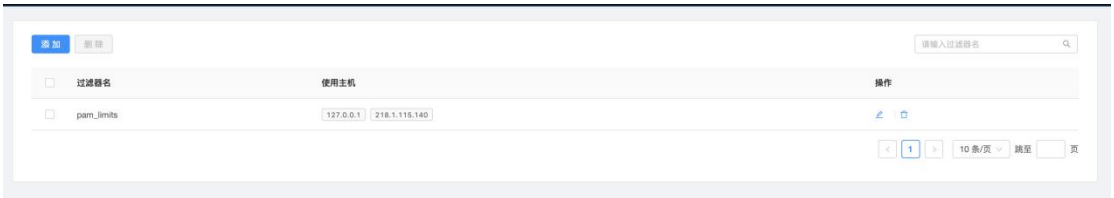
点击【添加】按钮，进行设备添加，填写设备名称、设备 IP、资产类型、设备是否启用及描述信息。同时需要配置该设备产生日志的范化规则，系统支持自定义组合规则。管理员可根据实际业务情况在「日志管理」-「规则管理」中自定义添加日志范化规则。

对已添加的资产设备支持删除、编辑及启用/禁用操作。如对某设备进行禁用操作，则系统不再接收该设备的日志。



4.2 过滤器

支持对日志来源进行过滤，管理员可根据需要添加过滤条件从而过滤部分无用日志。



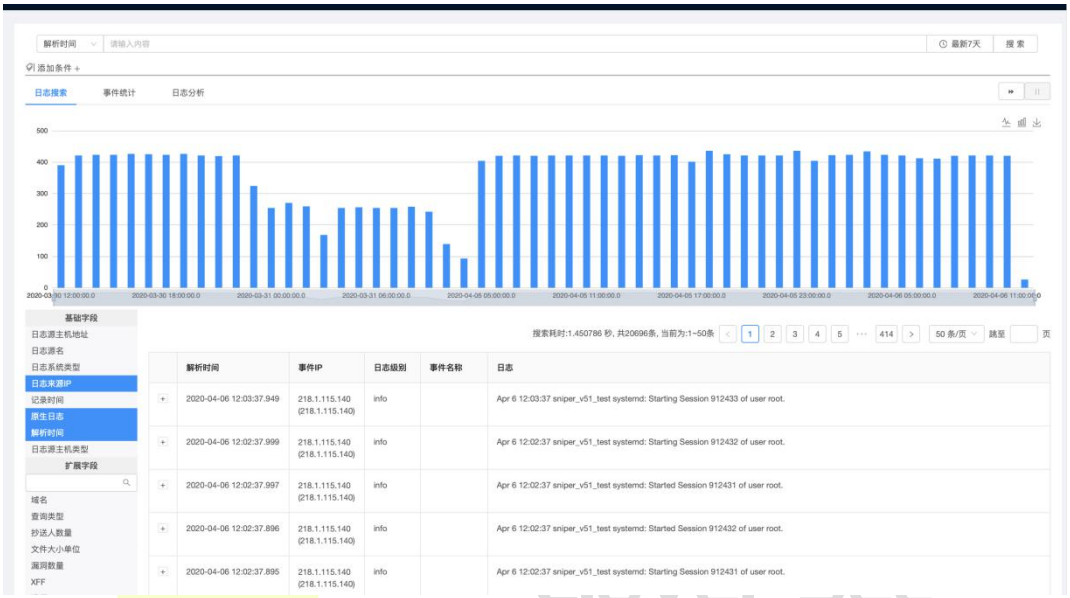
点击【添加】按钮，可添加过滤条件，添加过滤添加时需要配置过滤器名，包含值以及应用主机等信息。

五、 日志管理

日志管理共分为 5 个部分：日志搜索、规则管理、事件分类、字段管理及索引管理。

5.1 日志列表

日志以列表形式展示，并通过图表展示近期日志的数量趋势。



5.1.1 日志搜索

支持多种搜索方式对日志进行查询。

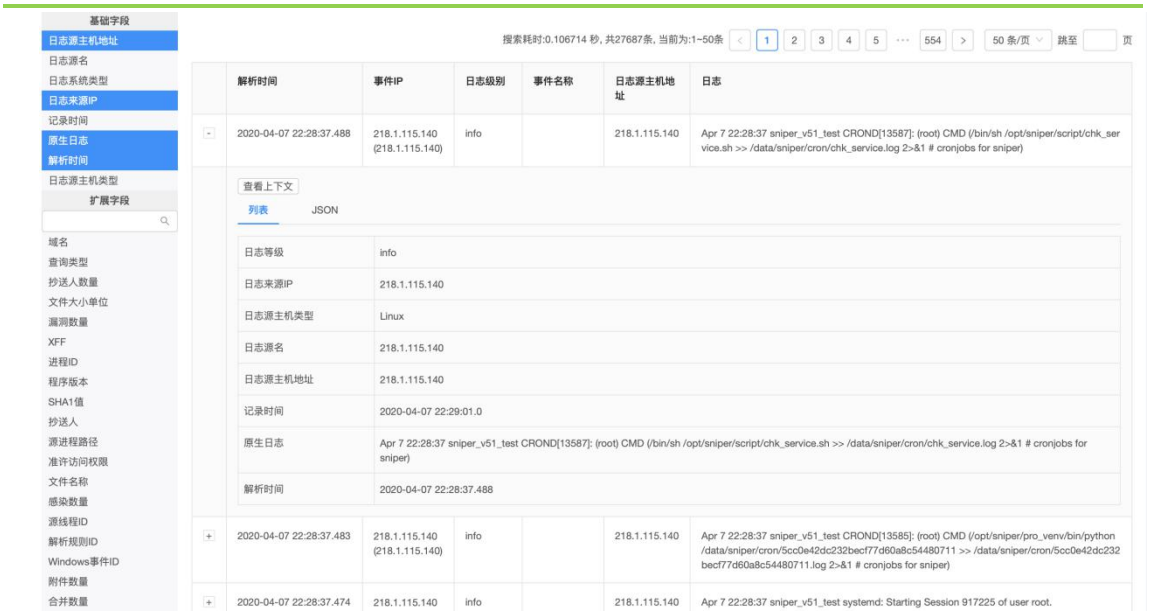
- 模糊搜索：支持输入关键字对日志进行模糊检索，并支持快速查看近 7 天、15 天等时间范围的日志；

- 内置查询条件：系统内置多个查询条件，帮助管理员快速查询对应的关键日志；

- 自定义查询条件：系统支持自定义添加查询条件；

- 上下文查询：支持查看某条日志的上下文信息；

同时日志列表支持自定义字段设置，字段包括基础字段和扩展字段 2 种，管理员可根据需要选择日志字段。

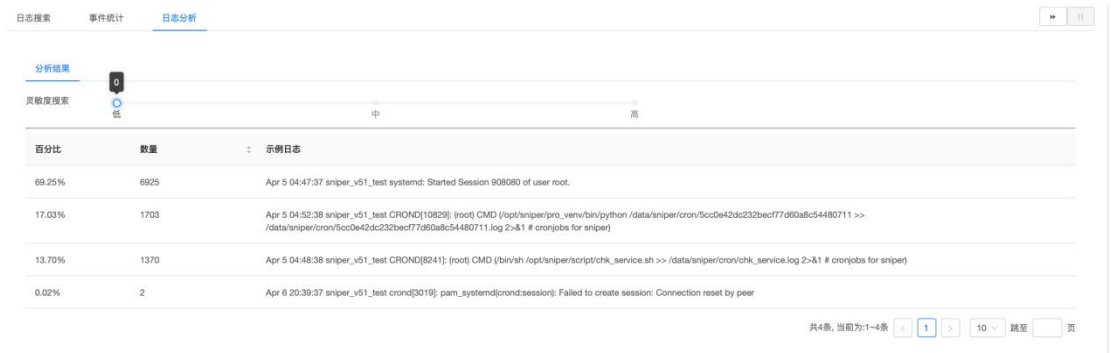


5.1.2 事件统计

支持将日志自定义生成统计图表。图表类型包括折线图、柱状图、饼图、雷达图、瀑布图、表格、漏斗图、单值图及热力图等。同时支持将新建图表添加到组件。

5.1.3 日志分析

支持对日志进行统计归类分析。



5.2 规则管理

系统内置 340+条日志范化规则，支持的资产类型包括主机、网络设备、安全设备、数据库、中间件、存储设备、应用系统、虚拟化设备、机房设备及其他等多种类型。

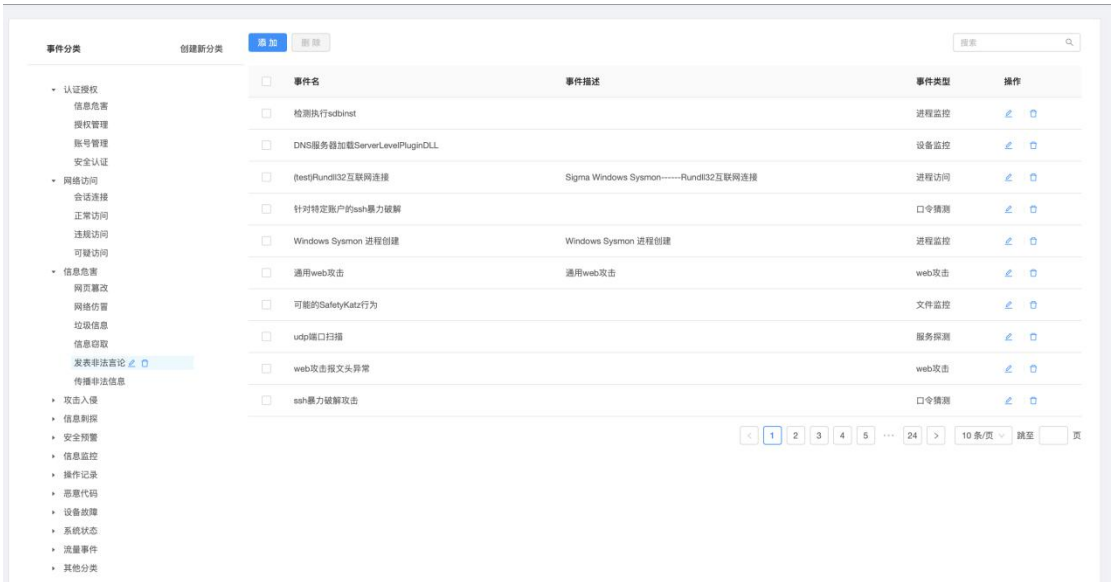
点击【添加】按钮，支持自定义添加规则，添加规则时需要填写规则名、描述、事件分类、资产类型、原生日志及解析方式。解析方式支持正则解析、正则 Json 解析、键值解析。

点击【编辑】按钮，支持对已有规则进行修改编辑。

点击【删除】按钮，支持对规则进行删除操作。

5.3 事件分类

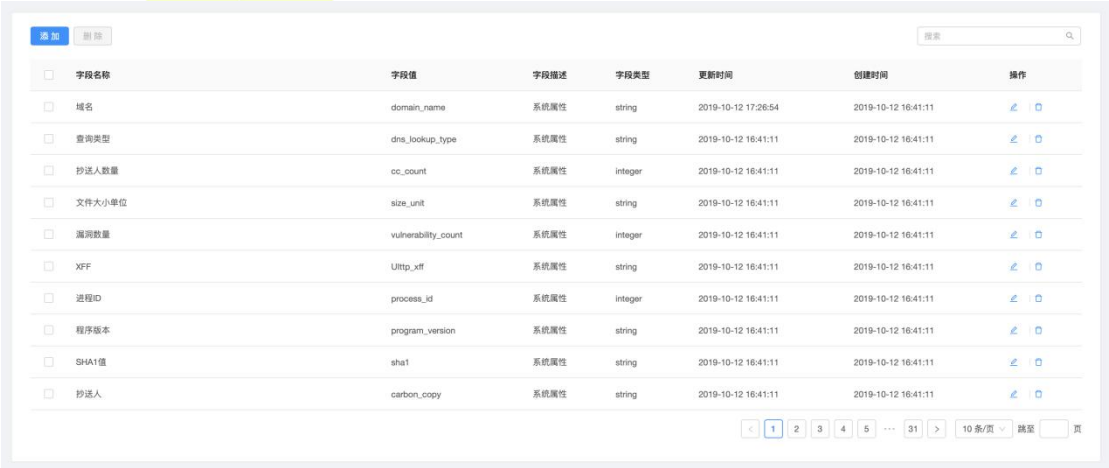
系统内置 230+种事件规则，事件类别共 13 种，包括认证授权、网络访问、信息危害、攻击入侵、信息刺探、安全预警、信息监控、操作记录、恶意代码、设备故障、系统状态、流量事件及其他等。



点击【添加】按钮，支持自定义添加事件。添加事件时需要填写事件名、关键字、事件分类及事件描述，同时对已有事件支持修改和删除操作。

5.4 字段管理

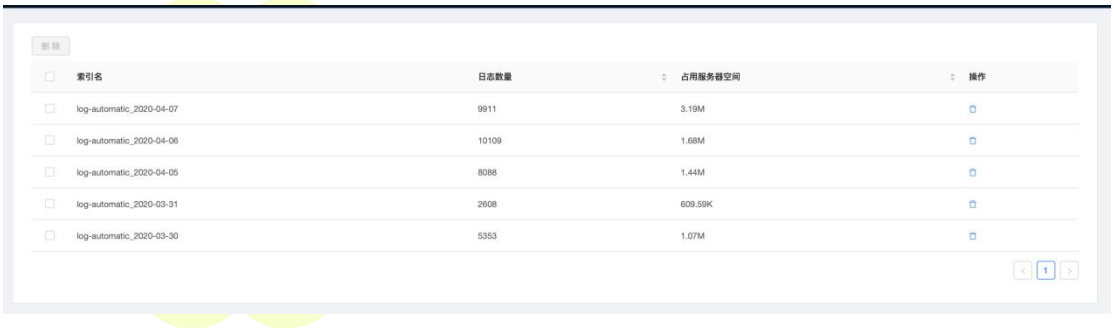
系统内置 300+个字段，支持对字段的统一管理。



点击【添加】按钮，支持自定义添加字段信息。添加字段时需要填写字段名称、字段值、描述及字段类型。支持的字段类型包括字符串、数字、日期及 ipv4/ipv6。同时支持对字段进行编辑和删除操作。

5.5 索引管理

系统支持对日志索引的统一管理。能够查看各个索引的日志数量及占用服务器空间信息。并支持对索引进行删除操作。



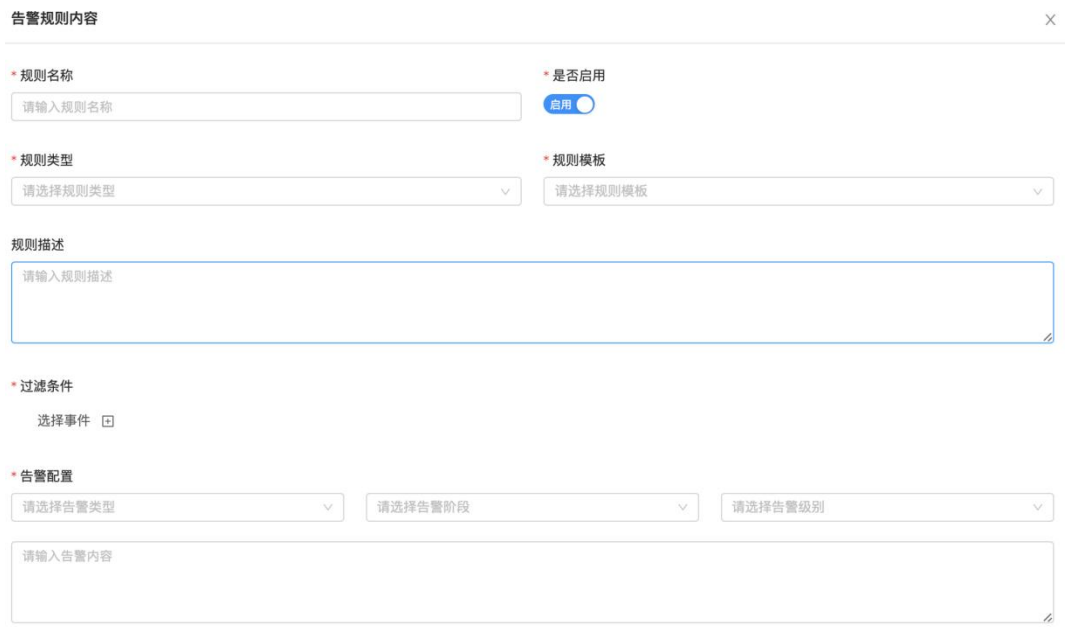
六、 告警管理

告警管理共分为 3 个部分：规则列表、告警列表及资源管理。

6.1 规则列表

系统内置 180+条告警规则，帮助管理员通过告警规则快速从大量日志中提取关键有用信息从而生成告警事件。目前系统支持 7 种规则类型，分别是：配置错误和故障告警、违规行为、网络攻击、恶意代码、数据安全、账户安全及其他。

点击【添加】按钮，支持自定义新建告警规则，新建告警规则时需要填写规则名称、规则类型、规则模板、规则描述、是否启用、过滤条件、告警配置等信息。规则模板支持普通计数模板、普通模板及管理模板 3 种；告警类型包括主机安全、恶意软件、网络安全、访问控制、数据安全及其他；告警阶段包括侦查、投放、利用、安装、控制及攻击 6 种；告警级别包括低危、中危及高危。



点击【编辑】和【删除】按钮，支持对已有告警规则进行编辑和删除操作。点击【启用/停用】按钮，能够对该告警规则进行启用或停用设置。

6.2 告警列表

系统支持将告警事件以列表形式展示。系统提供多种条件进行组合查询，查询条件分别有：告警时间、告警级别、告警类型、告警阶段及告警状态。同时支持关键字模糊搜索。

告警列表分为聚合模式和列表模式，系统内置聚合算法，将多个同类型事件聚合为一个聚合事件。

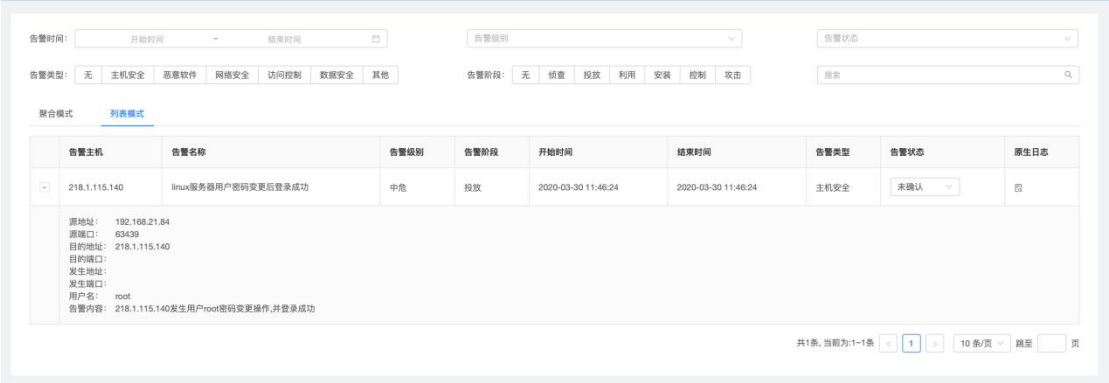
在聚合模式下点击【 】按钮，能够查看该聚合事件对应的子事件信息详情，如下图所示。

点击【 + 】按钮，能够查看每个子事件的源地址、端口，目的地址、端口及用户名、告警内容等信息。

点击【未确认/已确认】按钮，可以针对该告警事件进行确认处理操作。

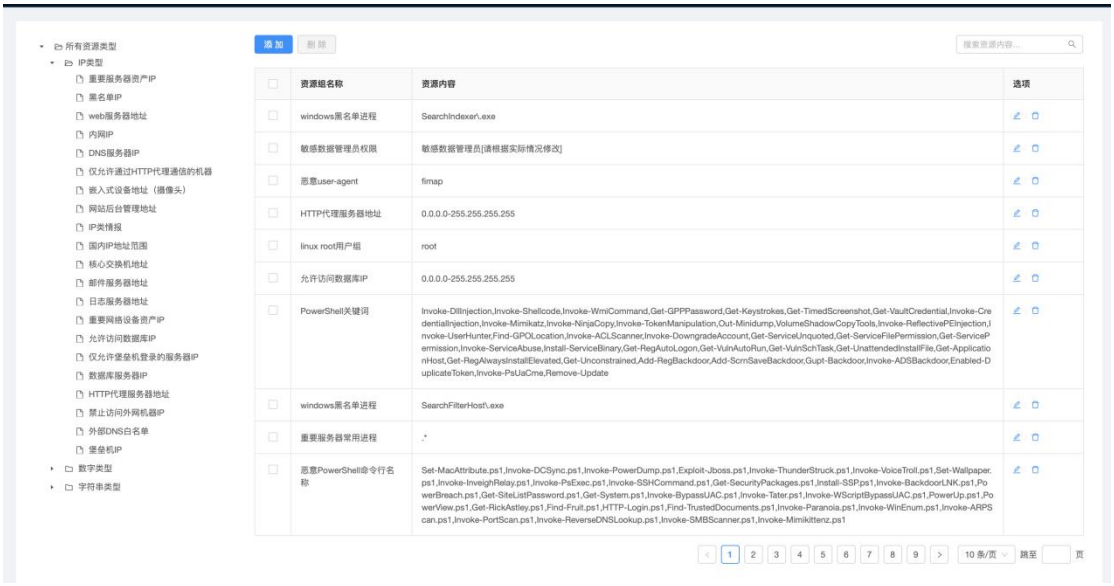
点击【原生日志】按钮，可以查看该告警事件的原生日志信息。

列表模式展示了每个子事件的详细信息。操作和聚合模式一致。

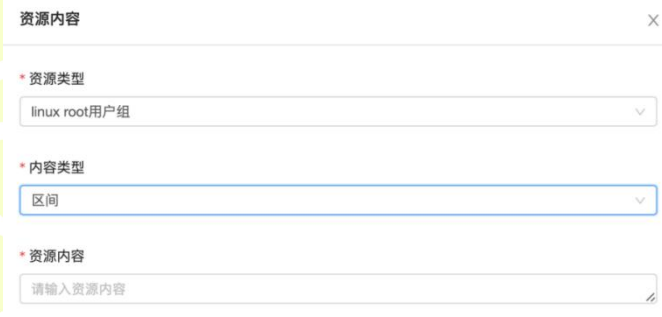


6.3 资源管理

系统内置 800+资源情报信息，资源类型包括 IP 类型、数字类型及字符串类型 3 种。方便管理员进行策略规则配置时直接统一关联调用。



点击【添加】按钮，支持自定义新增资源情报。添加资源时，需要填写资源类型、内容类型及资源内容等信息。内容类型包括值、区间及列表 3 种。



点击【编辑】和【删除】按钮，支持对已有资源信息进行编辑和删除操作。

七、 报表管理

报表管理共分为 2 个部分：报表列表和报表设置。

7.1 报表列表

系统支持自定义添加报表设置。报表类型分为自定义报表、日报、周报及月报 4 种。

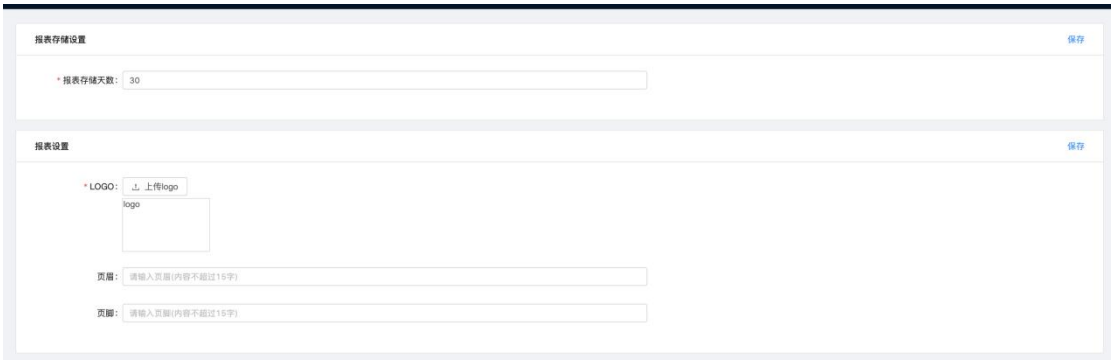
点击【生成记录】按钮，支持查看该报表的历史生成记录，并对历史生成的报表提供下载按钮。

点击【添加】按钮，支持添加报表。添加报表时需要配置报表名称、报表标题、副标题、报表描述、报表类型、报表组件及是否发送邮件通知等信息。报表类型分为一次性报表、日报、周报及月报 4 种；报表组件可根据管理员实际运维需要自定义选择，管理员也可通过「仪表盘」-「组件管理」自定义添加组件信息。同时若开启邮件通知且勾选附件，则能够将生成的报表作为附件发送给收件人，收件人邮箱可手动输入，也可关联管理员邮箱。

7.2 报表设置

系统支持对报表存储时间进行设置，超过存储天数后系统会自动删掉最早一天的报表。

同时支持对报表的 logo 自定义设置，页眉、页脚自定义设置。

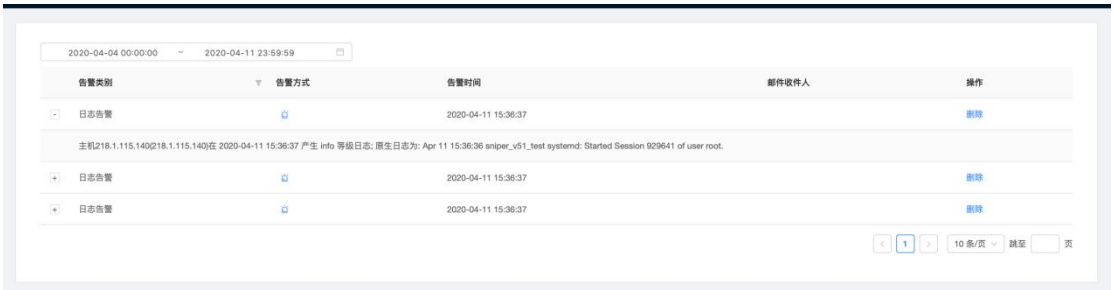


八、 系统管理

系统管理共分为 3 个部分：告警通知、管理员管理和系统设置。

8.1 告警通知

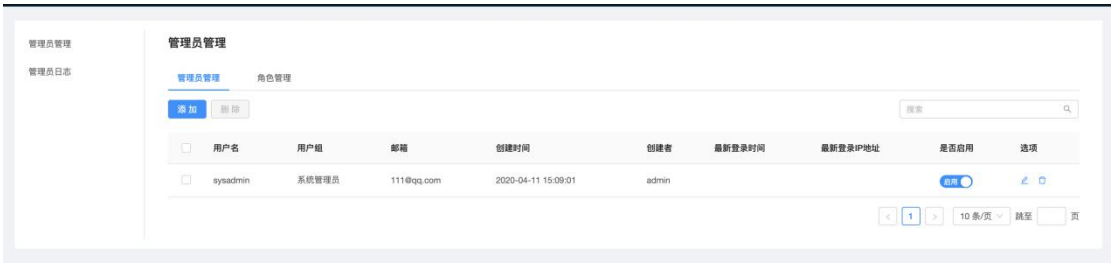
系统支持查看所有的告警通知信息。管理员可以通过「系统管理」-「系统设置」-「告警配置」进行自定义告警配置。



8.2 管理员管理

8.2.1 管理员管理

系统支持自定义添加管理员。支持设置管理员是否启用。同时能够查看该管理员最近登录时间和登录 IP 地址。



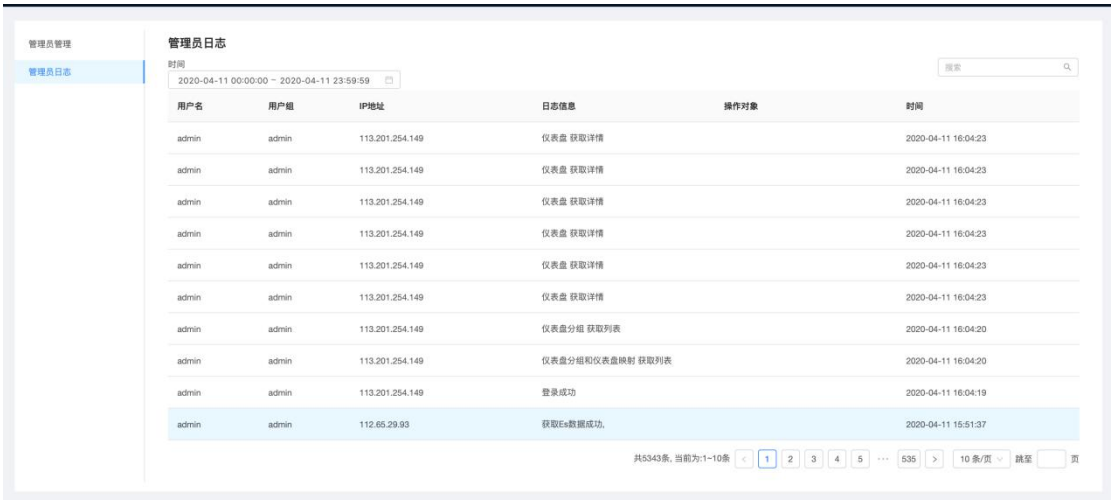
管理员的功能权限由其关联的角色决定。

8.2.2 角色管理

系统支持自定义添加管理员角色。同时支持设置每个角色的管理权限。

8.2.3 管理员日志

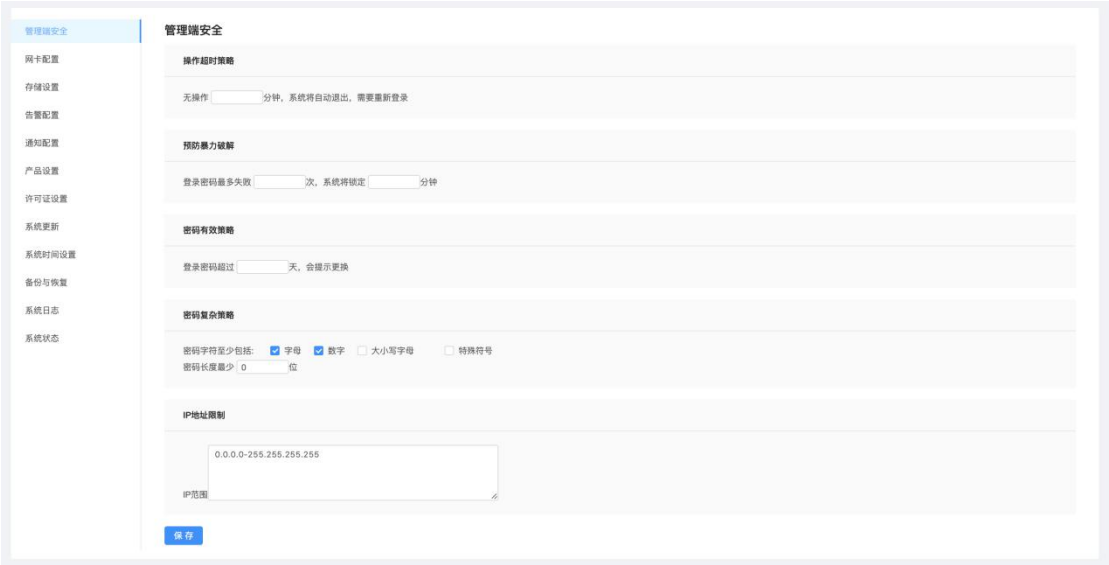
支持查看系统所有管理员的操作日志。



8.3 系统设置

8.3.1 管理端安全

系统支持提供管控中心的安全策略，包括 5 类：操作超时策略、预防暴力破解、密码有效期策略、密码复杂度策略以及管理员登录 IP 地址限制。



8.3.2 网卡配置

系统支持查看服务器网卡信息。

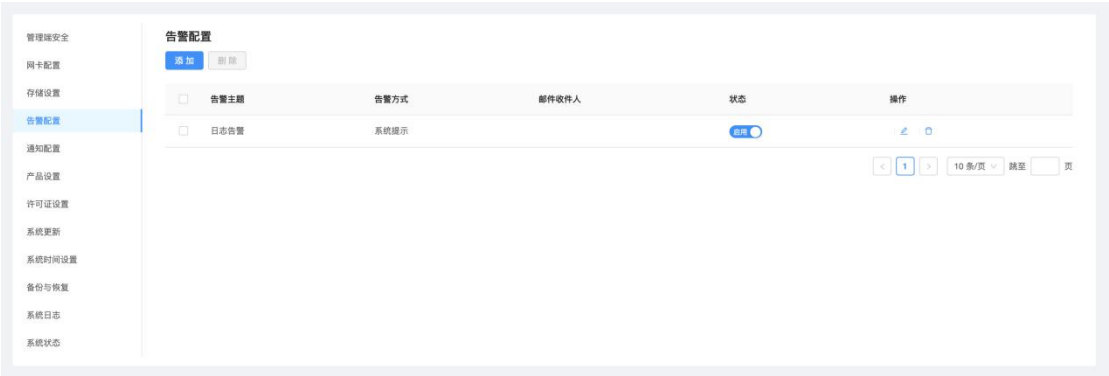
点击【编辑】按钮，支持配置网卡地址协议和子网掩码信息。

8.3.3 存储设置

系统支持配置日志存储配置，能够从存储周期和存储剩余空间两方面对日志进行管控。

8.3.4 告警配置

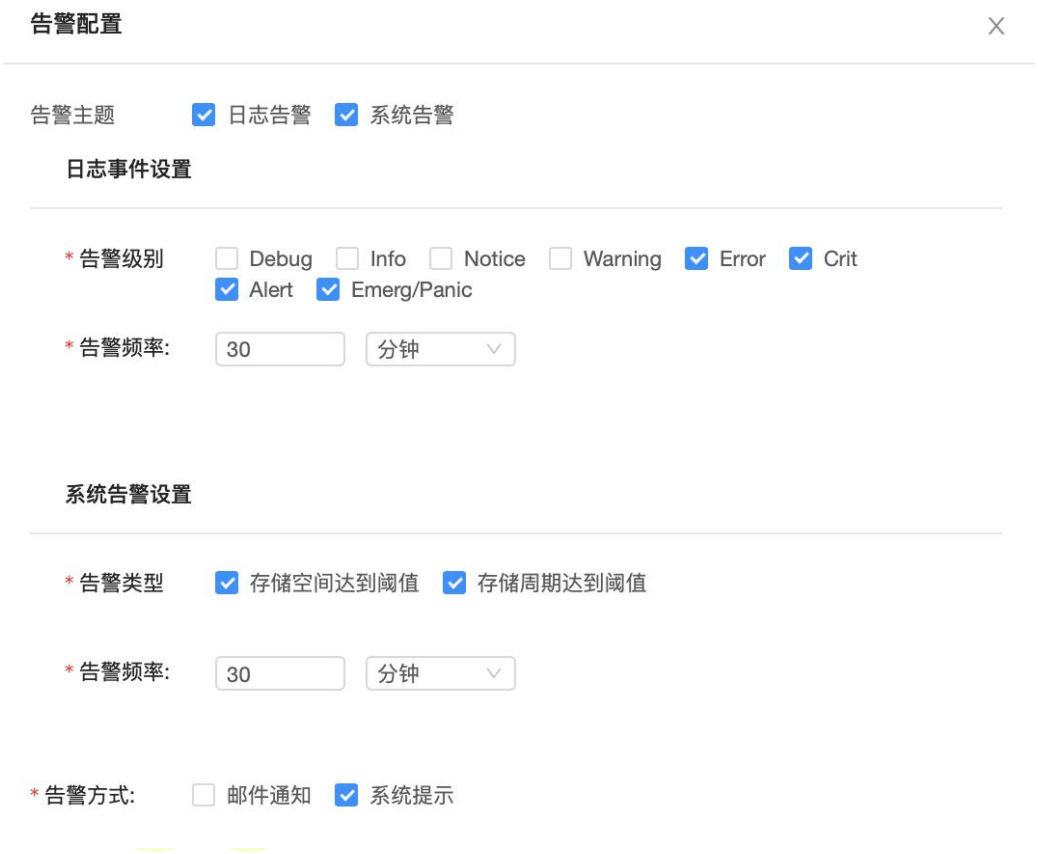
系统支持告警配置，告警主题包含：日志告警和系统告警。告警方式包括邮件通知和系统提示。同时支持对该告警配置进行启用/停用操作。



针对日志告警，支持设置告警级别和告警频率。告警级别共 8 种，分别为：Debug、Info、Notice、Warning、Error、Crit、Alert、Emerg/Panic。系统接收对应级别日

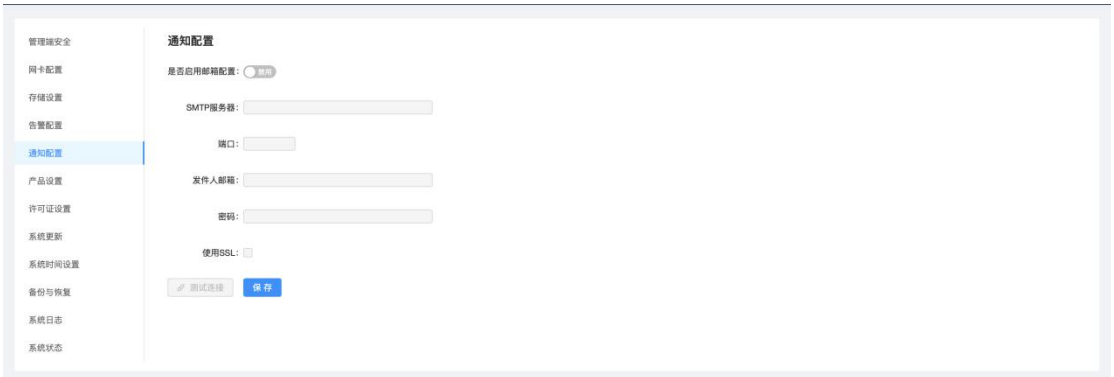
志则会产品告警通知。

针对系统告警，可设置告警类型：存储空间达到阈值和存储周期达到阈值。系统存储空间满足对应条件则会产生告警通知。



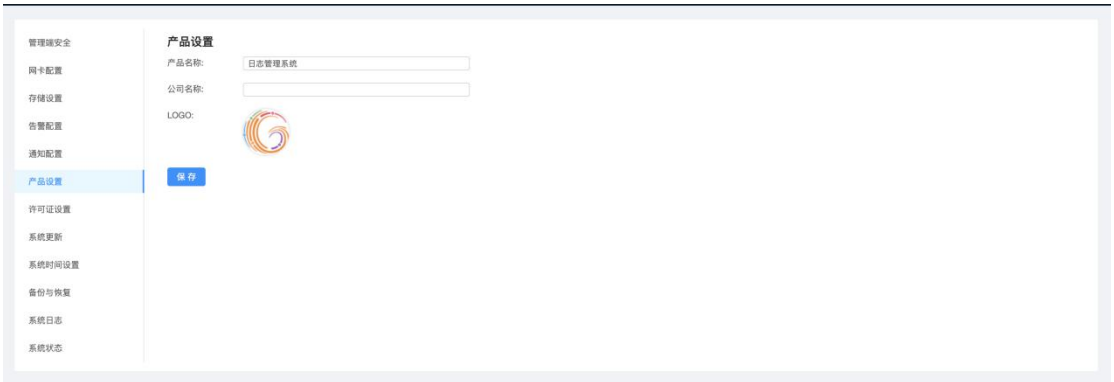
8.3.5 邮件配置

邮件告警通知需要配置邮箱信息。需要填写 SMTP 服务器、SMTP 端口、邮件账户、密码以及是否使用 SSL。



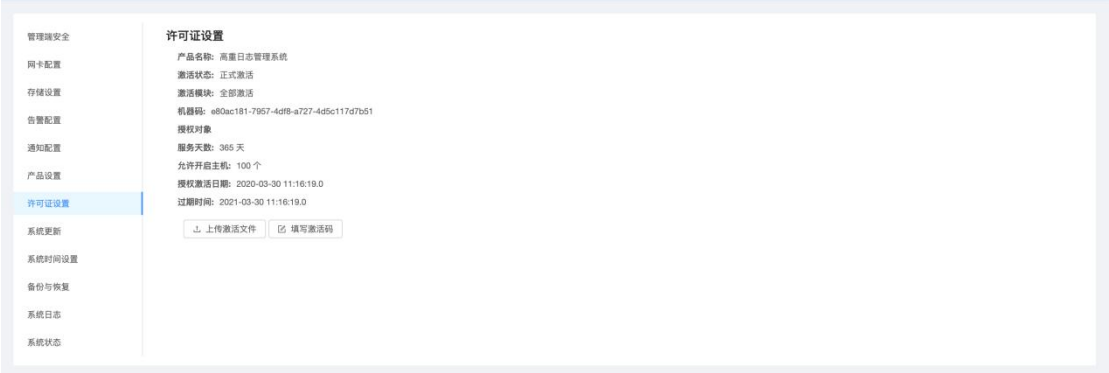
8.3.6 产品设置

系统支持自定义配置产品名称、公司名称及 logo 信息。



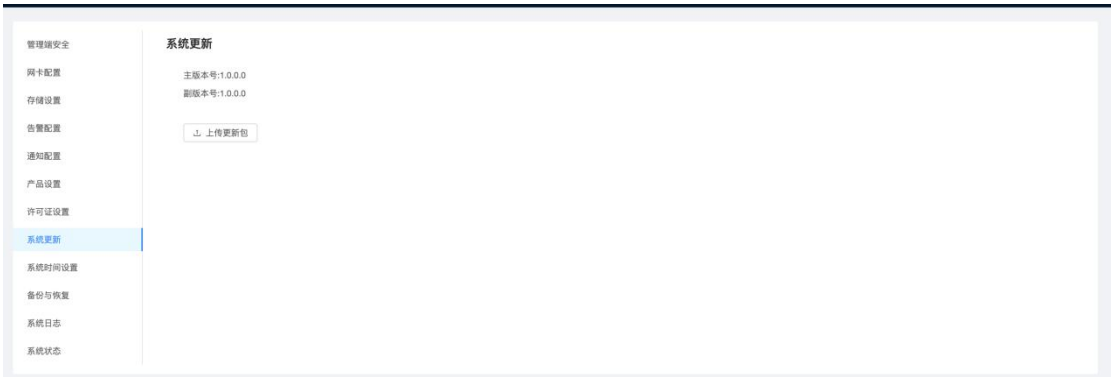
8.3.7 许可证设置

系统支持查看当前激活的许可证信息，并能够进行重新激活操作。



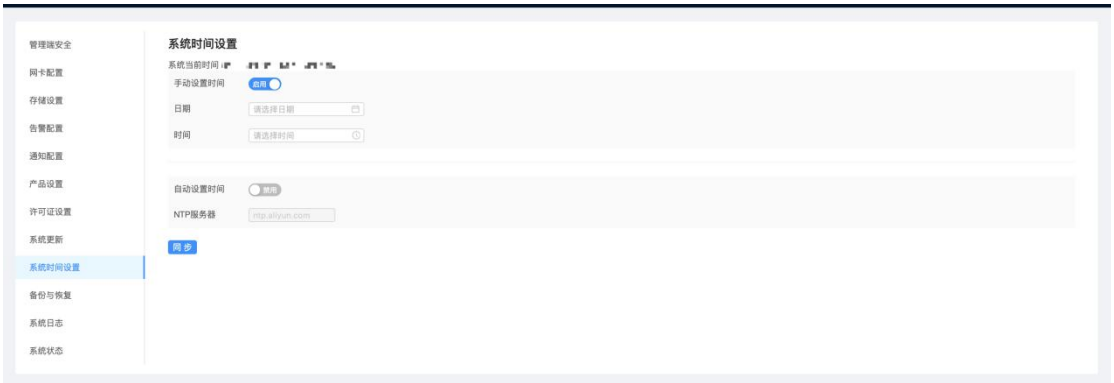
8.3.8 系统更新

支持对管控中心的升级。



8.3.9 系统时间设置

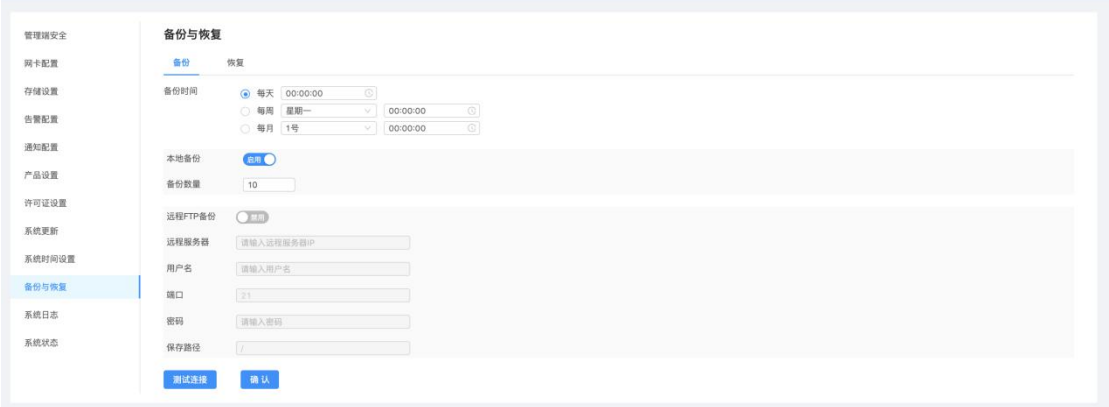
系统提供手动设置时间和自动设置时间的配置。



8.3.10 备份与恢复

8.3.10.1 备份

系统支持 3 种备份方式：立即备份、本地备份以及远程备份。



立即备份：能够对系统的配置进行立即备份操作；

本地备份：能够按照设置的周期将系统的配置备份到本地；其中备份数量是指本地保存的备份数量，超过该数量，则删除最早的备份；

远程备份：能够按照设置的周期将系统的配置备份到远端服务器中。

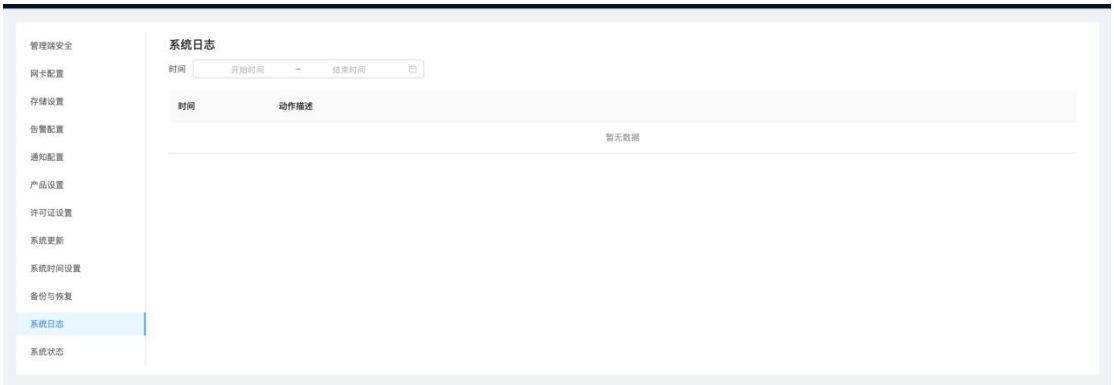
8.3.10.2 恢复

系统支持 3 种恢复方式：从本地恢复、从文件恢复以及恢复出厂设置。

注：恢复出厂设置将会清空系统所有数据，包括激活信息。因此请谨慎操作！

8.3.11 系统日志

管理员能够通过系统日志查看系统定期备份及定期清理日志的操作记录。



8.3.12 系统状态

支持查看当前系统的相关信息，包括：系统基本信息、CPU 使用率、系统负载、内存使用率、网络流量。

九、公司介绍

9.1 公司简介

西安四叶草信息技术有限公司（以下简称：四叶草安全）是一家专业的漏洞风险检测与网络安全解决方案提供商。公司秉承“以攻促防”的安全理念，深耕网络攻防实战型人才培养，为客户提供一体化网络信息安全解决方案，致力于帮助客户以攻击者的视角先于黑客发现并及时解决安全隐患。

四叶草安全成立于 2012 年 8 月，聚集了华为、启明星辰、绿盟、奇安信、BAT3 等众多网络安全人才，立足西安、服务全国，目前在北京、上海、成都、兰州、郑州、武汉、沈阳等地成立办事处和售后服务机构。凭借着在网络安全领域的专注与创新，为客户提供更专业的网络安全产品、网络安全服务、网络安全解决方案、网络安全认证培训及网络安全赛事支撑等。业务覆盖政府、运营商、互联网、教育、金融、能源、企业等。

经过 7 年多的发展，四叶草安全已是国家高新技术企业、入选硬科技优秀企业、培育独角兽企业、西安未来之星 TOP10、科技小巨人、CNCERT 技术支持单位、CNNVD 技术支撑单位、CNVD 技术组单位、拥有数十项技术专利和完善的网络安全服务资质；与中国信息安全测评中心、西安电子科技大学、成都信息工程大学等单位高校联合成立网络安全人才培养实验室；与华为、百度、腾讯、阿里、蚂蚁金服等企业达成战略合作；并于 2019 年获得蚂蚁金服亿级战略投资，服务过几十万用户及政府、央企、互联网等数百个大型项目，业务范围覆盖 20 多个省份的政府、运营商、金融、电力和能源行业等；保障过党的十九大、“一带一路”高峰论坛、金砖国家峰会、G20、文博会、贵阳大数据等大型活动的网络信息安全。

四叶草安全多年来坚持自主创新和掌握核心技术，让安全风险可控，让防御更简单。研究领域涉及渗透测试、代码审计、逆向分析、移动终端安全、物联网安全、工控安全、黑客行为分析、智能算法、漏洞数据的建模和安全人工智能等。

9.2 联系方式

西安四叶草信息技术有限公司

地址：西安市高新区软件新城 天谷八路 156 号 云汇谷 C2 楼 1701 室

邮编：710000

电话：029-88894789

邮箱：support@seclover.com

网址：www.seclover.com