

奇固科威
HKW-LAS1000 日志审计与分析系统
用户手册
V1.0.10

杭州奇固科威信息安全技术有限公司
2025年3月29日

目 录

1 安装与部署.....	5
2 授权.....	6
管理员.....	6
3 系统配置.....	6
3.1 网络配置.....	6
3.1.1 IP 配置.....	6
3.1.2 路由配置.....	6
3.2 升级管理.....	7
3.3 系统配置.....	7
3.3.1 基本信息.....	7
3.3.2 基础配置.....	8
3.3.3 邮件服务.....	8
3.3.4 校时配置.....	9
3.3.5 数据库维护.....	9
3.3.6 数据库备份.....	10
3.3.7 系统快照.....	10
3.3.8 License 管理.....	10
3.3.9 情报库.....	11
3.3.10 系统告警通知.....	11
3.4 白名单.....	12
4 系统管理.....	12
4.1 用户管理.....	12
4.2 角色管理.....	13
4.3 转发策略.....	15
操作员.....	16
5 日志管理.....	16
5.1 日志源类别.....	16
6 审计管理.....	17
6.1 审计事件.....	16
6.2 审计策略.....	16
6.3 审计类型.....	20
7 采集管理.....	21
7.1 代理服务器.....	21

7.2	采集过滤策略.....	211
7.3	采集器管理.....	22
7.4	日志源设备.....	24
8	报表管理.....	25
8.1	报表列表.....	25
8.2	报表任务.....	25
8.3	报表查询.....	26
8.4	自定义报表模板.....	26
9	资产管理.....	26
9.1	资产列表.....	28
9.2	资产类型.....	29
9.3	资产属性.....	300
9.4	区域管理.....	30
9.5	网络管理.....	31
9.6	资产发现.....	31
9.7	厂商.....	32
10	事件管理.....	32
10.1	安全事件.....	32
10.2	聚合策略.....	33
10.3	关联策略.....	33
10.4	原始日志.....	34
10.5	通用日志.....	34
10.6	自定义解析.....	35
10.7	事件.....	35
10.8	事件类型.....	36
10.9	事件特征值.....	36
11	告警管理.....	37
11.1	审计告警.....	37
11.2	告警策略.....	37
11.3	系统告警.....	38

11.4 系统告警级别配置.....	38
审计员.....	38
12 日志管理.....	38
12.1 日志备份.....	38
13 情报库.....	39
13.1 威胁情报库.....	39
14 漏洞库.....	39
14.1 CNNVD 漏洞信息.....	39
15 系统日志.....	40
15.1 操作日志.....	40
15.2 错误日志.....	40
15.1 登录日志.....	40

1 安装与部署

1、系统要求

系统名称	系统版本
Ubuntu	18.04 x64 及以上

2、环境要求

服务	版本	备注
MySQL 数据库	5.7.38	默认账号: root 默认密码: Linkqi@123
JAVA	1.8.x	-

3、解压

将压缩包上传到服务器的任意普通用户的 home 目录，例如/home/linkqi 目录下，然后执行下述命令：

- a) 解压 las-2000xxxxxxx.tar.gz


```
cd /home/linkqi
tar -zxvf las-2000*.tar.gz
./las_install.sh
```

4、安装

- a) 数据库自行安装
- b) 进入解压后的目录，执行 install 脚本安装（请使用 root 权限安装）：


```
su root
cd las-2000
./las_install.sh
```

5、运行

安装完成后，执行一下命令运行服务：

```
./las_start.sh
```

6、升级

通过 web 升级，点击上传按钮，选择升级的安装包，上传完成后点击升级即可完成升级。



7、默认用户名密码：

账号	权限	密码
superuser	超级管理员	Linkqi@000
operator	超级操作员	Linkqi@111
auditor	超级审计员	Linkqi@222

2 授权

系统配置->License 管理；复制机器码给平台维护人员；上传维护人员给的认证文件即可



管理员

用户名: superuser

密码: Linkqi@000

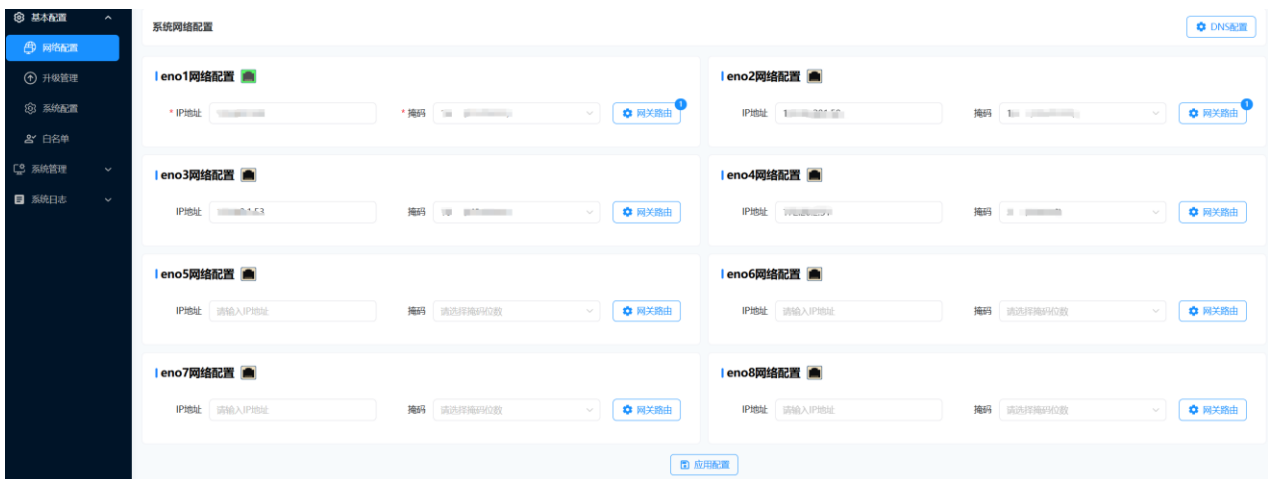
3 基本配置

3.1 网络配置

3.1.1 IP 配置

基本配置->网络配置

绿色闪烁网口表示当前网线连接的网口。



3.1.2 路由配置

点击路由配置可进入配置页面，添加完成点击完成



3.2 升级管理

基本配置->升级管理->上传文件->升级
可以升级软件版本



3.3 系统配置

3.3.1 基本信息

产品信息展示可重启或者关机

产品名称	奇固科威日志审计与分析系统
产品版本	V1.0.10
build号	20230807
产品型号	HKW-LAS1000

3.3.2 安全设置

解锁时间 * 小时

是否开启验证码

密码过期时间 * 天

CPU阈值 * %

MEM阈值 * %

token过期时间 * 小时

3.3.3 邮件服务

可发送至邮件服务器接受消息

置 邮件服务 校时配置 数据库维护 数据库备份 系统快照 License管理 情报库 系统告警通知

发送邮件服务器 * 输入服务器或IP地址

端口 * 输入端口 - +

用户名 * 用户名

密码 * 密码

ssl

测试 保存 重置

3.3.4 校时配置

邮件服务 校时配置 数据库维护 数据库备份 系统快照 License管理 情报库 系统告警通知

校时 手动校时 自动校时

设置中心服务器时间 * 2025-01-14 16:03:04

查看服务器时间 保存

3.3.5 数据库维护

可设置数据库维护时间以及数据保留时间

查看机器码
复制

License管理

序列号	0000-0000-0000-0000-0000-0000
创建时间	2018-08-10 10:00:00
有效时间	永久
可配置采集器数量	1000

3.3.9 情报库

上传情报库文件

3.3.10 系统告警通知

可自行选择通知方式

通知方式

邮件

邮件地址*

snmp trap

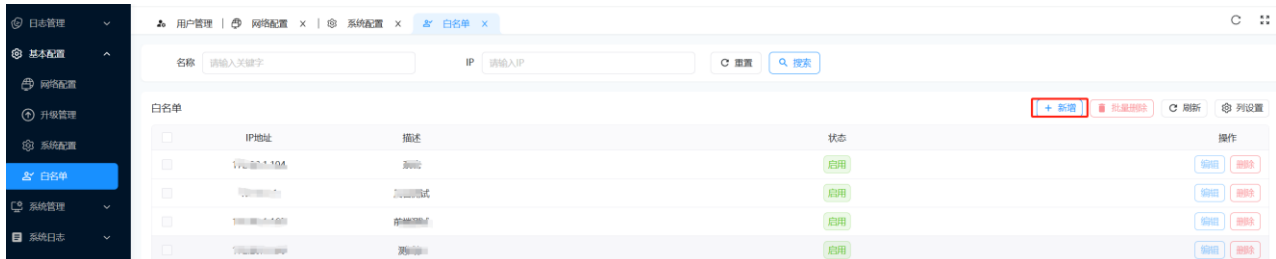
通知服务器

3.4 白名单

只有添加了白名单的 ip 可以访问平台

基本配置->白名单->新增

默认是不开启的状态



输入 IP 启用立即生效;



4 系统管理

4.1 用户管理

用户名	用户类型	用户描述	创建时间	用户状态	操作
	管理员	超级管理员		正常	系统用户不允许操作
	操作员			正常	系统用户不允许操作
	审计员			正常	系统用户不允许操作

4.1.1 新增

新增用户 ×

用户名 *

密码 *

确认密码 *

用户类型

起止日期 *
 →

有效开始时间 *

有效结束时间 *

用户描述

用户状态

4.1.2 编辑

编辑前需要输入当前账号的密码认证

编辑用户

用户名 *
ceshi001

起止日期 *
2025-03-12 00:00:12 → 2025-03-24 00:00:24

有效开始时间 *
03:00

有效结束时间 *
23:00

用户描述
请输入用户描述

用户状态
正常

取消 确认

4.1.3 删除

用户名	角色	描述	状态	操作
ceshi001	审计员		正常	编辑 分配角色 锁定 修改 取消 确认
ceshi002	管理员	测试003	正常	编辑 分配角色 锁定 修改密码 删除

4.1.4 锁定与解锁

用户名	角色	描述	状态	操作
ceshi003	管理员	测试003	正常	编辑 分配角色 锁定 修改密码 删除

4.2 角色管理

按照需要创建角色，可自行分配角色权限，每个用户都有与之对应的角色

角色列表

角色名称	角色描述	类型	操作
操作001	操作001	操作员	编辑 分配权限 删除
管理员01	管理员01	管理员	编辑 分配权限 删除

4.2.1 新增

新增角色 ×

角色名称 *

角色描述

角色所属类型

4.2.2 删除

角色列表

<input type="checkbox"/>	角色名称	角色描述	角色所属类型				
<input type="checkbox"/>	ttt		管理员	编辑	分配权限	删除	

新增 确认删除吗? 取消 确认 列设置

4.2.3 编辑

编辑角色 ×

角色名称 *

角色描述

角色所属类型

4.3 转发策略

可以转发系统告警到指定服务器上有 snmp 和 syslog 两种方式

用户管理 转发策略 x

转发策略

+ 新增 批量删除 刷新 列设置

<input type="checkbox"/>	转发方式	Community	企业节点号	oid节点号	其它服务器IP	端口号	用户描述	操作
<input type="checkbox"/>	SNMP Trap							编辑 删除
<input type="checkbox"/>	syslog							编辑 删除

操作员

用户名: operator

密码: Linkqi@111

5 日志管理

5.1 日志源类别

系统自带的无法操作，可自行添加

日志源类别

+ 新增 批量删除 刷新 列设置

<input type="checkbox"/>	名称	操作
<input type="checkbox"/>	IDS/IPS	
<input type="checkbox"/>	操作系统	
<input type="checkbox"/>	防病毒	
<input type="checkbox"/>	防火墙/VPN	
<input type="checkbox"/>	隔离设备	
<input type="checkbox"/>	加密设备	
<input type="checkbox"/>	审计设备	
<input type="checkbox"/>	网络设备	
<input type="checkbox"/>	应用系统	
<input type="checkbox"/>	综合管理	
<input type="checkbox"/>	漏洞扫描	
<input type="checkbox"/>	流量监控	
<input type="checkbox"/>	网页监控	
<input type="checkbox"/>	邮件检查	
<input type="checkbox"/>	其它	

共 15 条 < 1 > 20 / 页

5.1.1 新增

新增日志源类别

名称 *

5.1.2 删除

<input type="checkbox"/>	邮件检查	是	
<input type="checkbox"/>	其它	是	
<input type="checkbox"/>	测试	否	

确认删除吗?

6 审计管理

6.1 审计事件

事件等级 请选择事件等级 审计类型 请选择审计类型 审计策略 请选择审计策略

产生时间 开始日期时间 → 结束日期时间

导出已加载

审计事件名称	审计类型	产生时间	更新时间	审计策略	事件等级	事件总数	操作
无数据							

6.2 审计策略

策略名称	审计事件级别	策略描述	系统内置	使用状态	操作
策略测试1	一般		否	<input checked="" type="checkbox"/>	<input type="button" value="编辑"/> <input type="button" value="删除"/>
ceshi005	一般		否	<input checked="" type="checkbox"/>	<input type="button" value="编辑"/> <input type="button" value="删除"/>

6.2.1 新增

添加审计策略 ✕

策略名称 *

审计事件类型

安全事件 关联事件 威胁事件

事件

有效时间段 *

每天 星期 日期

至

审计事件名称

审计事件级别

审计类型 *

转发策略

策略描述

6.2.2 删除

策略名称	审计事件级别	策略描述	系统内置	使用状态	操作
<input type="checkbox"/> 策略测试1	<input type="button" value="一般"/>		<input type="button" value="否"/>	<input checked="" type="checkbox"/>	<input type="button" value="编辑"/> <input type="button" value="删除"/>

+ 新增

6.2.3 编辑

编辑审计策略 ×

策略名称 *

审计事件类型
 安全事件 关联事件 威胁事件

事件

有效时间段 *
 每天 星期 日期

至

审计事件名称

审计事件级别

审计类型 *

转发策略

策略描述

6.3 审计类型

6.3.1 新增

添加审计类型

审计类型名称 *

类型描述

排序

6.3.2 删除

审计类型	审计类型名称	类型描述	排序	系统内置	操作
<input type="checkbox"/>	测试2		2	<input type="checkbox"/>	编辑 删除

6.3.3 编辑

编辑审计类型

审计类型名称 *

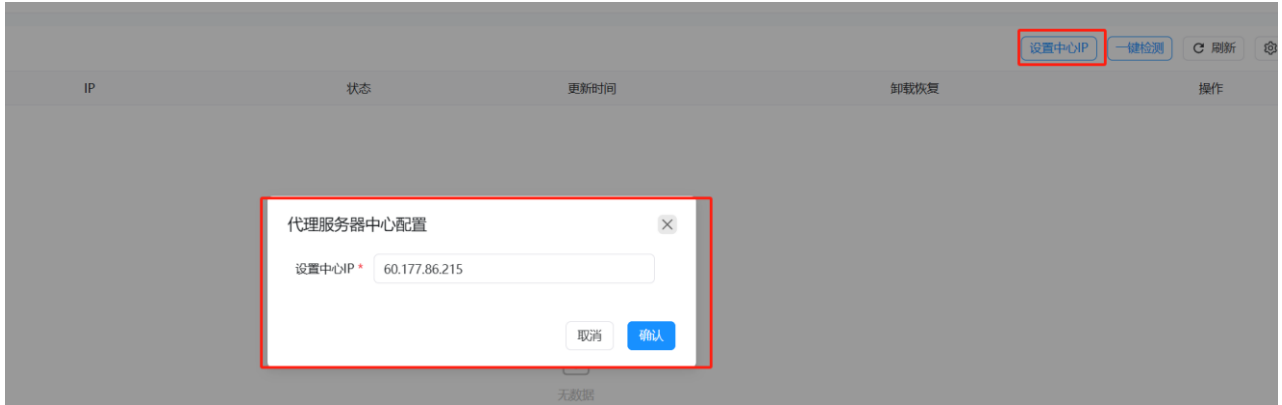
类型描述

排序

7 采集管理

7.1 代理服务器

可以设置中心 IP



7.2 采集过滤策略

可自行添加过滤策略

新增策略 ×

策略名称 *
请输入策略名称

日志级别 *
请选择日志级别

事件类型 *
请选择日志级别

源IP *
源起始IP - 源终止IP

目的IP *
目的起始IP - 目的终止IP

描述
请输入描述

7.3 采集器管理

一、接入方式 snmp 和 syslog 的采集器需要填写采集的地址

Snmp

新增采集器

采集器名称 *	<input type="text" value="请输入采集器名称"/>	编码格式 *	<input type="text" value="自动"/>
接入方式 *	<input type="text" value="SNMP"/>	代理服务器	<input type="text" value="请选择代理服务器"/>
采集地址 *	<input type="text" value="请输入采集地址"/>	日志源设备 *	<input type="text" value="Linux"/>
过滤策略	<input type="text" value="请选择过滤策略"/>	生成资产	<input checked="" type="radio"/> 是 <input type="radio"/> 否
是否启用	<input checked="" type="radio"/> 是 <input type="radio"/> 否		
描述	<input type="text" value="请输入描述"/>		

Syslog

新增采集器

采集器名称 *	<input type="text" value="请输入采集器名称"/>	编码格式 *	<input type="text" value="自动"/>
接入方式 *	<input type="text" value="Syslog"/>	代理服务器	<input type="text" value="请选择代理服务器"/>
采集地址 *	<input type="text" value="请输入采集地址"/>	日志源设备 *	<input type="text" value="Linux"/>
过滤策略	<input type="text" value="请选择过滤策略"/>	生成资产	<input checked="" type="radio"/> 是 <input type="radio"/> 否
是否启用	<input checked="" type="radio"/> 是 <input type="radio"/> 否		
描述	<input type="text" value="请输入描述"/>		

二、Ssh 接入方式需要填写采集地址，端口，用户名和密码

新增采集器 ×

采集器名称 *	<input type="text" value="请输入采集器名称"/>	编码格式 *	自动 ▼
接入方式 *	SSH ▼	代理服务器	请选择代理服务器 ▼
采集地址 *	<input type="text" value="请输入采集地址"/>	日志源设备 *	Linux ▼
过滤策略	请选择过滤策略 ▼	端口 *	<input type="text" value="请输入端口"/>
用户名 *	<input type="text" value="请输入用户名"/>	密码 *	<input type="password" value="请输入密码"/>
生成资产 <input checked="" type="radio"/> 是 <input type="radio"/> 否		是否启用 <input checked="" type="radio"/> 是 <input type="radio"/> 否	
描述	<input type="text" value="请输入描述"/>		

三、Wmi 接入方式需要填写采集地址，用户名密码

Wmi 接入的是 windows 系统需要目标计算机开启 opensshservice 才可以实现连接

具体方法如下

1、Windows 界面中设置

- 打开 **设置**，点击 **应用**。
- 选择 **可选功能**。
- 点击 **添加功能**。
- 搜索 “OpenSSH 服务器”，然后点击 **安装**。
- 打开 **服务**：按 Win + R，输入 services.msc 并按 Enter。
- 找到 **OpenSSH SSH Server** 服务，右键点击，选择 **启动**。
- 为了让 SSH 服务器开机自启，可以右键点击该服务，选择 **属性**，将启动类型设置为 **自动**

2、命令行方法

管理员打开 powershell 执行下列操作

#安装 openssh 服务器组件

1)Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0

#启动 ssh

2)Start-Service sshd

#设置开机自启

3)Set-Service -Name sshd -StartupType Automatic

#防火墙放行

4)New-NetFirewallRule -Name sshd -DisplayName 'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol TCP -Action Allow -LocalPort 22

#查看服务运行状态

5)Get-Service sshd

配置完成后添加采集器

新增采集器 ×

采集器名称 *	<input type="text" value="请输入采集器名称"/>	编码格式 *	<input type="text" value="自动"/>
接入方式 *	<input type="text" value="WMI"/>	代理服务器	<input type="text" value="请选择代理服务器"/>
采集地址 *	<input type="text" value="请输入采集地址"/>	日志源设备 *	<input type="text" value="Linux"/>
过滤策略	<input type="text" value="请选择过滤策略"/>	用户名 *	<input type="text" value="请输入用户名"/>
密码 *	<input type="password" value="请输入密码"/>	生成资产	<input checked="" type="radio"/> 是 <input type="radio"/> 否

是否启用 是 否

描述

四、Sftp 和 ftp 的接入方式类似，需要填写地址，端口(sftp: 22/ftp: 21)，用户名和密码以及采集的日志路径例如/var/log/auth.log

新增采集器 ×

采集器名称 *	<input type="text" value="请输入采集器名称"/>	编码格式 *	<input type="text" value="自动"/>
接入方式 *	<input type="text" value="SFTP"/>	代理服务器	<input type="text" value="请选择代理服务器"/>
采集地址 *	<input type="text" value="请输入采集地址"/>	日志源设备 *	<input type="text" value="Linux"/>
过滤策略	<input type="text" value="请选择过滤策略"/>	目录 *	<input type="text" value="请输入"/>
端口 *	<input type="text" value="请输入端口"/>	用户名 *	<input type="text" value="请输入用户名"/>
密码 *	<input type="password" value="请输入密码"/>	生成资产	<input checked="" type="radio"/> 是 <input type="radio"/> 否

是否启用 是 否

描述

7.4 日志源设备

可自行添加

新增日志源设备

日志源类型 *

请输入日志源类型

日志源类别 *

请选择日志源类别

厂商 *

请选择厂商

描述

请输入备注

8 报表管理

8.1 报表列表

报表实例展示

实例名称	实例类型	实例数量	操作
sq	资源		清空
	资源		清空

8.2 报表任务

可添加定时任务，将报表发送给收件人

新增任务 ✕

* 任务名称

* 实例选择 资产 审计

* 任务类型 每日 每周 每月

* 开始时间

* 收件人

* 发送类型

PDF ▼

任务描述

PDF ✓

Word

Excel

8.3 报表查询

有资产信息报表和综合报表

资产信息报表

资产类型

查询日期 →

综合报表

查询日期 →

8.4 自定义报表模板

对审计信息报表和综合报表进行自定义展示:

模板

资产信息报表

综合报表

资产信息报表

一、资产基本信息

资产类型	资产名称	网段名称	主IP	创建时间
XXX	XXX	XXX	XXX	XXX
XXX	XXX	XXX	XXX	XXX

二、资产类型分布统计

组件库

保存全部更改

文本信息

类型

文本

添加

表格

图表

(主界面)

组件

数据组件

资产

数据来源

资产基本信息

表头

请选择

资产名称

资产类型

网段名称

主IP

创建时间

确定

取消

组件库

保存全部更改

文本信息

类型

文本

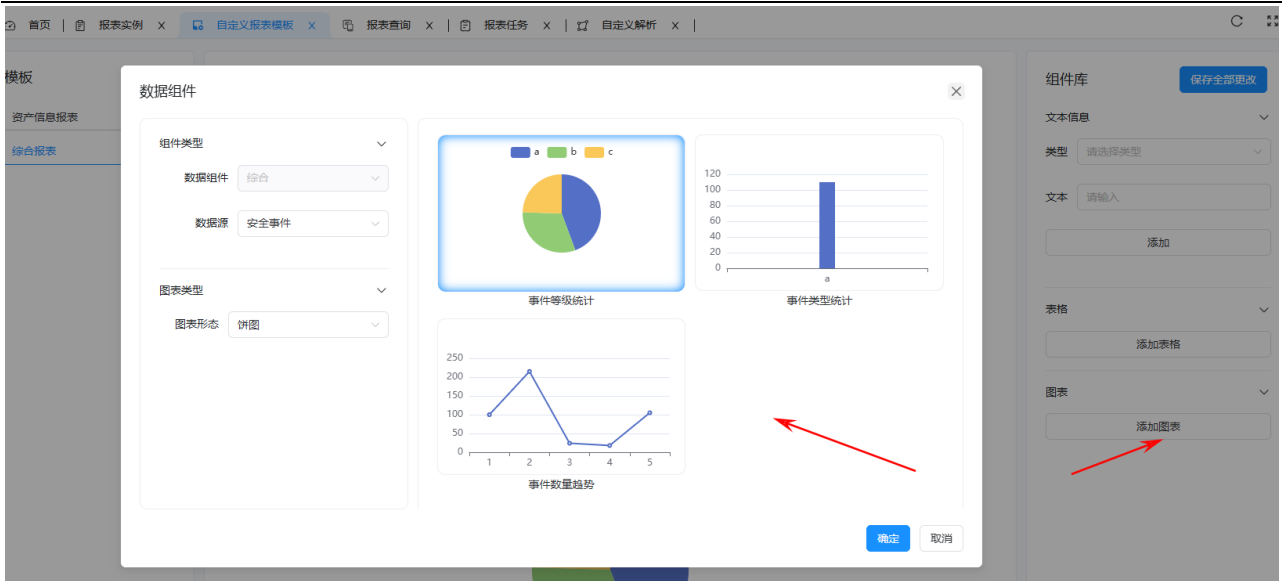
添加

表格

添加表格

图表

(添加表格)



(添加图表)

9 资产管理

9.1 资产列表

可以管理自己的资产，可以单独查看资产的日志

资产列表

[+ 新增](#)
[批量删除](#)
[刷新](#)
[资产导出](#)
[资产导入](#)
[列设置](#)

资产名称	资产类型	网段	备注	制造商	负责人	所属区域	操作
[模糊]	操作系统						日志 查看 编辑 删除
[模糊]	数据库						日志 查看 编辑 删除
[模糊]	网络设备						查看 编辑 删除
[模糊]	[模糊]						日志 查看 编辑 删除
[模糊]	[模糊]						日志 查看 编辑 删除

日志概览

事件类型 请选择事件 事件等级 请选择事件等级 接收时间 请选择接收时间 用户 请选择用户

源IP 源起始IP - 源终止IP 目的IP 目的起始IP - 目的终止IP 发生源IP 发送源起始IP - 发送源终止IP

日志源设备 Microsoft Windows 目标对象 请输入目标对象 C 重置 Q 搜索

原始日志 [导出已加载](#)

事件类别	事件类型	事件等级	设备类别	设备类型	接收时间	发生源IP	操作	
1	Windows日志	Windows安全日志	严重	操作系统	Microsoft Windows	2025-01-16 10:28:31	172.17.0.1	详情
2	Windows日志	Windows安全日志	严重	操作系统	Microsoft Windows	2025-01-16 10:28:31	172.17.0.1	详情
3	Windows日志	Windows安全日志	严重	操作系统	Microsoft Windows	2025-01-16 10:28:31	172.17.0.1	详情
4	Windows日志	Windows安全日志	严重	操作系统	Microsoft Windows	2025-01-16 10:28:31	172.17.0.1	详情
5	Windows日志	Windows安全日志	严重	操作系统	Microsoft Windows	2025-01-16 10:28:31	172.17.0.1	详情
6	Windows日志	Windows安全日志	严重	操作系统	Microsoft Windows	2025-01-16 10:28:31	172.17.0.1	详情
7	Windows日志	Windows安全日志	严重	操作系统	Microsoft Windows	2025-01-16 10:28:31	172.17.0.1	详情
8	Windows日志	Windows安全日志	严重	操作系统	Microsoft Windows	2025-01-16 10:28:31	172.17.0.1	详情
9	Windows日志	Windows安全日志	严重	操作系统	Microsoft Windows	2025-01-16 10:28:31	172.17.0.1	详情

已加载100条 预计还有更多

9.2 资产类型

可自行添加资产

新增资产类型

资产一级分类 *

请选择资产一级分类

资产二级分类 *

请输入资产二级分类

资产类型 + 新增 批量删除 刷新 列设置

<input type="checkbox"/>	资产一级分类	资产二级分类	操作
<input type="checkbox"/>	其他设备	复印机	
<input type="checkbox"/>	其他设备	碎纸机	
<input type="checkbox"/>	其他设备	打印机	
<input type="checkbox"/>	其他设备	个人终端办公	
<input type="checkbox"/>	网络设备	防病毒	
<input type="checkbox"/>	网络设备	光纤交换机	
<input type="checkbox"/>	网络设备	网络设备	
<input type="checkbox"/>	网络设备	应用系统	
<input type="checkbox"/>	网络设备	身份认证网关	
<input type="checkbox"/>	网络设备	流量监控	
<input type="checkbox"/>	网络设备	utm	
<input type="checkbox"/>	网络设备	路由器	
<input type="checkbox"/>	网络设备	集线器	
<input type="checkbox"/>	网络设备	三层交换机	
<input type="checkbox"/>	网络设备	核心交换机	

9.3 资产属性

略

9.4 区域管理

管理区域资源，自行添加

区域列表 + 新增 批量删除 刷新 列设置

<input type="checkbox"/>	区域名称	简称	办公电话	电子邮箱	职能	地址	备注	操作
<input type="checkbox"/>			1			HZ		编辑 删除

9.5 网络管理

管理网络资源

网络管理 + 新增 批量删除 刷新 列设置

<input type="checkbox"/>	名称	IP类型	IP范围	描述	操作
<input type="checkbox"/>	内网测试		172.20.1.1		编辑 删除

9.6 资产发现

展示发现的资产列表

发现任务 + 新增 批量删除 刷新 列设置

<input type="checkbox"/>	任务名称	网段	状态	操作
<input type="checkbox"/>	实时	172.20.1.1~172.20.1.255		立即发现 删除

也可以设置发现任务

发现任务

+ 新增 批量删除 刷新 列设置

任务名称	网段	状态	操作
实时	172.20.1.1-172.20.1.255		立即发现 删除

9.7 厂商

9.7.1 新增

新增厂商

名称 *

请输入名称

9.7.2 删除

厂商列表

+ 新增 批量删除 刷新 列设置

名称	系统内置	操作
测试	是	
测试	是	
测试	是	
测试	否	编辑 删除

确认删除吗?
取消 确认

9.7.3 编辑

编辑厂商

名称 *

测试

10 事件管理

10.1 安全事件

按照聚合策略聚合到一起的事件：

安全事件

导出已加载

事件名称	事件类型	聚合开始时间	事件类别	日志源设备	事件等级	聚合数量	发生源IP	聚合结束时间	操作
1	系统状态		系统状况/配置	Linux	严重	5			查看
2	系统状态		系统状况/配置	Linux	严重	2	1		查看
3	系统状态		系统状况/配置	Linux	严重	5			查看
4	系统状态		系统状况/配置	Linux	严重	5			查看
5	系统状态		系统状况/配置	Linux	严重	2	1		查看
6	系统状态		系统状况/配置	Linux	严重	5	1		查看
7	系统状态		系统状况/配置	Linux	严重	2			查看
8	系统状态		系统状况/配置	Linux	严重	6	1		查看
9	系统状态		系统状况/配置	Linux	严重	5			查看

10.2 聚合策略

按照匹配规则把采集到的日志消息归类聚合到一起，可自行添加聚合规则：

聚合策略

[+ 新增](#)
[批量删除](#)
[刷新](#)
[导出](#)
[列设置](#)

<input type="checkbox"/>	策略名称	最大限定时间(秒)	最大聚合次数	匹配规则	操作
<input type="checkbox"/>	未定义拒绝服务器事件	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	畸形Dos数据包	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	洪水攻击	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	邮件服务攻击	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	利用拒绝服务漏洞	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	SYN Flood	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	UDP Flood	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	ICMP Flood	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	Teardrop	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	Land	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	Smurf	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	Fraggle	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	DDoS攻击	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	DNS Flood	86400	20000	事件等级, 设备种类, 发生源IP	
<input type="checkbox"/>	WINNLUKE攻击	86400	20000	事件等级, 设备种类, 发生源IP	

共 429 条 1 2 3 4 5 6 7 ... 22 20 / 页

10.3 关联策略

关联策略

策略名称	策略描述	事件等级	更新时间	使用状态	系统内置	操作
测试		低	2025-05-11 10:00:00	开启	否	编辑 删除

新增关联策略

新增关联策略

策略名称 *

策略描述

条件

无数据

||或 &&与

10.4 原始日志

存放 ssh、ftp、sftp、wmi 接入方式的数据

事件类型 事件等级 接收时间 用户

源IP 源终止IP 目的IP 目的终止IP 发生源IP 发生源终止IP

日志源设备 目标对象

原始日志

事件类别	事件类型	事件等级	设备类别	设备类型	接收时间	发生源IP	日志原文	操作
1	系统状况/配置	系统状态	操作系统	Linux	2025-01-17 09:30:00	172.17.0.107	...	<input type="button" value="详情"/>
2	系统状况/配置	系统状态	操作系统	Linux	2025-01-17 09:30:00	<input type="button" value="详情"/>
3	认证/授权/访问	会话中断	操作系统	Linux	2025-01-17 09:30:00	<input type="button" value="详情"/>
4	系统状况/配置	系统状态	操作系统	Linux	<input type="button" value="详情"/>
5	系统状况/配置	系统状态	操作系统	Linux	<input type="button" value="详情"/>
6	认证/授权/访问	会话中断	操作系统	Linux	<input type="button" value="详情"/>
7	系统状况/配置	系统状态	操作系统	Linux	<input type="button" value="详情"/>
8	系统状况/配置	系统状态	操作系统	Linux	<input type="button" value="详情"/>
9	认证/授权/访问	会话中断	操作系统	Linux	<input type="button" value="详情"/>

10.5 通用日志

存放 syslog 和 snmp 接入方式的数据

日志源设备 级别 日志模块

时间 开始日期时间 结束日期时间 IP 发生源起始IP 发生源终止IP

通用日志

设备类型	主机名称	接收时间	模块	级别	发生源IP	日志原文	操作
1	Linux	xusi-ubuntu	2025-1-14 11:40:40	DAEMON	WARNING	...	<input type="button" value="详情"/>
2	Linux	xusi-ubuntu	2025-1-14 11:40:40	DAEMON	WARNING	...	<input type="button" value="详情"/>
3	Linux	xusi-ubuntu	2025-1-14 11:40:40	DAEMON	WARNING	...	<input type="button" value="详情"/>
4	Linux	xusi-ubuntu	2025-1-14 11:40:40	DAEMON	WARNING	...	<input type="button" value="详情"/>
5	Linux	xusi-ubuntu	2025-1-14 11:40:40	DAEMON	WARNING	...	<input type="button" value="详情"/>
6	Linux	xusi-ubuntu	2025-1-14 11:40:40	DAEMON	WARNING	...	<input type="button" value="详情"/>
7	Linux	xusi-ubuntu	2025-1-14 11:40:40	DAEMON	WARNING	...	<input type="button" value="详情"/>

10.6 自定义解析

可设置解析策略

新增自定义解析 ×

1 基本信息

2 日志划词

3 生成解析

使用状态

日志源设备 *

日志原文 *

新增自定义解析

1 基本信息

2 日志划词

3 生成解析

日志原文 *

<38>Mar 20 15:47:44 xusl-ubuntu sshd[70063]:ssh.service: Failed with result 'timeout'.

划词信息

字段值	对应规则	操作
<38>	优先级 ▼	删除
Mar 20 15:47:44	日志时间 ▼	删除
xusl-ubuntu	主机名 ▼	删除

新增自定义解析

1 基本信息

2 日志划词

3 生成解析

表达式

<(?(priority>\d+)>\s*(?(dbtime>[A-Za-z]{3}\s{1,2}\d{1,2}\s\d{2}:\d{2}:\d{4}[-]/\d{2}[-]/\d{2}\s\d{2}:\d{2}:\d{2}\d{1,2}-[A-Za-z]{3}-\d{4})\s\d{2}:\d{2}:\d{2}:\d{2}:\d{2}:\d{2}\s\d{4}(?:[-]/\d{2}){2})\s*(?<hname>[a-zA-Z0-9.-])+\s*[a-zA-Z0-9_-]+(?:=[\d+;])\s*\[\d+\];(.*)

解析结果

设备ID: null
 接收时间: 2025-03-29 11:31:43
 模块ID: 4
 级别ID: 6
 发生源IP: null
 应用名称: null
 PROCID: null
 MSGID: null
 日志时间: 2025-03-20 15:47:44
 主机名称: xusl-ubuntu
 结构数据: null
 日志内容: null
 日志原文: <38>Mar 20 15:47:44 xusl-ubuntu sshd[70063]:ssh.service: Failed with result 'timeout'.

10.7 事件

事件	事件名称	系统内置	操作
<input type="checkbox"/>	admx	否	编辑 删除

10.8 事件类型

事件类型 + 新增

事件类别	事件类型	系统内置	操作
拒绝服务	未定义拒绝服务器事件	是	
拒绝服务	畸形Dos数据包	是	
拒绝服务	洪水攻击	是	
拒绝服务	邮件服务攻击	是	
拒绝服务	利用拒绝服务漏洞	是	
拒绝服务	SYN Flood	是	
拒绝服务	UDP Flood	是	
拒绝服务	ICMP Flood	是	
拒绝服务	Teardrop	是	
拒绝服务	Land	是	
拒绝服务	Smurf	是	
拒绝服务	Fraggle	是	
拒绝服务	DDoS攻击	是	
拒绝服务	DNS Flood	是	
拒绝服务	WINNUKE攻击	是	
拒绝服务	攻击告警	是	

430条

10.9 事件特征值

事件特征值 + 新增 批量删除 刷新 列设置

特征值	日志源设备	事件类型	入库时间	操作
<input type="checkbox"/>	ceshixoo	纵向加密装置	洪水攻击	2025-03-15 17:01:00 编辑 删除

11 告警管理

11.1 审计报告警

审计报告警 批量确认 刷新

审计名称	事件级别	审计类型	告警策略	事件总数	产生时间	更新时间	状态	操作
<input type="checkbox"/>								

11.2 告警策略

自行添加告警策略

新增告警策略
✕

策略名称 *

审计事件名称包含

审计类型 *

审计等级 *

转发类型

外转邮箱

使用状态

备注

11.3 系统告警

可以批量确认或者删除

系统告警						批量确认	批量删除	刷新	列设置
<input type="checkbox"/>	告警名称	用户	状态	发生时间	告警描述	操作			
<input type="checkbox"/>	系统有效时间已过期	系统	未确认	2025-01-15 00:00:00	系统有效时间已过期,已停止日志采集	<input type="button" value="确认"/>	<input type="button" value="删除"/>		
<input type="checkbox"/>	存储时间达到阈值	系统	未确认	2025-01-14 01:00:00	清理存储时长达到阈值数据	<input type="button" value="确认"/>	<input type="button" value="删除"/>		
<input type="checkbox"/>	系统有效时间已过期	系统	未确认	2025-01-14 00:00:00	系统有效时间已过期,已停止日志采集	<input type="button" value="确认"/>	<input type="button" value="删除"/>		
<input type="checkbox"/>	存储时间达到阈值	系统	未确认	2025-01-11 01:00:00	清理存储时长达到阈值数据	<input type="button" value="确认"/>	<input type="button" value="删除"/>		
<input type="checkbox"/>	系统有效时间已过期	系统	未确认	2025-01-11 00:00:00	系统有效时间已过期,已停止日志采集	<input type="button" value="确认"/>	<input type="button" value="删除"/>		

11.4 系统告警级别配置

配置系统告警的级别对应:

告警级别配置				添加	批量删除	刷新
<input type="checkbox"/>	名称	名称	操作			
<input type="checkbox"/>	网络连接	低级	<input type="button" value="编辑"/> <input type="button" value="删除"/>			
<input type="checkbox"/>	软件安装与卸载	低级	<input type="button" value="编辑"/> <input type="button" value="删除"/>			
<input type="checkbox"/>	外设 (USB)	中级	<input type="button" value="编辑"/> <input type="button" value="删除"/>			

审计员

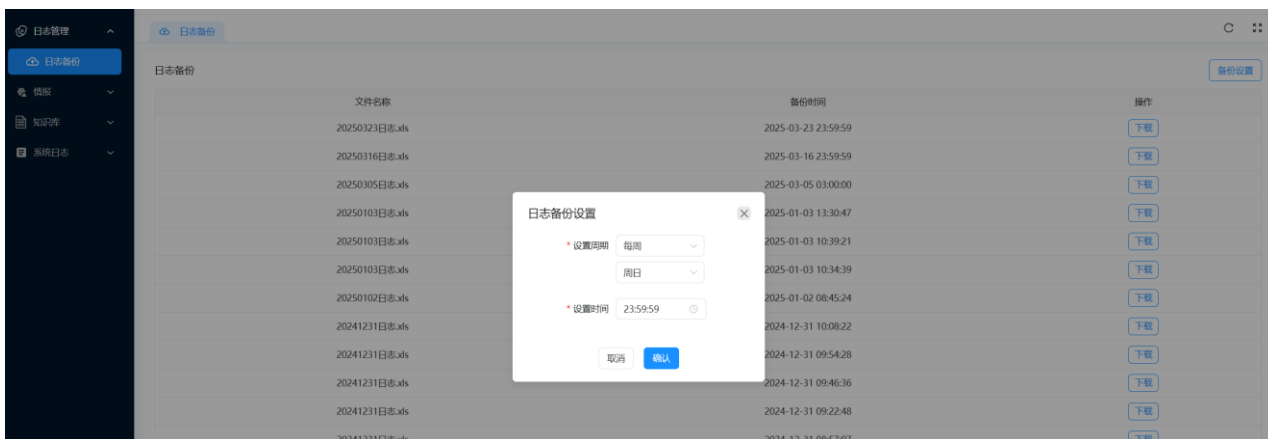
账号: auditor

密码: Linkqi@222

12 日志管理

12.1 日志备份

可以设置备份的时间和周期



13 情报库

13.1 威胁情报库



14 漏洞库

14.1 CNNVD 漏洞信息

登录日志 | 日志备份 | CNNVD漏洞信息 | 威胁情报库

CNNVD编号: 漏洞名称: CVE编号: 收录时间: →

危害等级:

CNNVD漏洞信息

CNNVD编号	漏洞名称	危害等级	CVE编号	厂商	收录时间	操作
CNNVD-202503-2834	China Mobile P22g-Clac 路径遍历漏洞	未定义	CVE-2025-2716	中国移动	2025-03-24	详情
CNNVD-202503-2833	GNOME 安全漏洞	未定义	CVE-2025-2721	GNOME	2025-03-24	详情
CNNVD-202503-2832	webERP 代码注入漏洞	未定义	CVE-2025-2715	个人开发者	2025-03-24	详情
CNNVD-202503-2831	Kubernetes ingress-nginx 输入验证错误...	未定义	CVE-2025-24514	云原生计算基金会	2025-03-24	详情
CNNVD-202503-2830	JoomlaUX JUX Real Estate 代码注入漏洞	未定义	CVE-2025-2714	JoomlaUX	2025-03-24	详情
CNNVD-202503-2829	Yonyou UFIDA ERP-NC 代码注入漏洞	未定义	CVE-2025-2712	Yonyou	2025-03-24	详情
CNNVD-202503-2828	NetApp SnapCenter 安全漏洞	未定义	CVE-2025-26512	网络器械	2025-03-24	详情
CNNVD-202503-2827	Yonyou UFIDA ERP-NC 代码注入漏洞	未定义	CVE-2025-2711	Yonyou	2025-03-24	详情
CNNVD-202503-2826	Kubernetes Ingress-nginx 安全漏洞	未定义	CVE-2025-1974	云原生计算基金会	2025-03-24	详情
CNNVD-202503-2825	Yonyou UFIDA ERP-NC 代码注入漏洞	未定义	CVE-2025-2710	Yonyou	2025-03-24	详情
CNNVD-202503-2824	OpenDaylight (ODL) 安全漏洞	未定义	CVE-2025-29315	OpenDaylight	2025-03-24	详情

共 50 条

15 系统日志

15.1 操作日志

操作日志

用户名	用户操作	请求URL	请求方式	请求参数	请求时长(ms)	状态	操作IP	User-Agent	创建时间
audit	日志备份	/logAudit/logBack...	GET	1	3	成功	172.20.1.100	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML...	2025-03-24 10:06:07
audit	日志备份	/logAudit/logBack...	GET	1	2	成功	172.20.1.100	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML...	2025-03-24 10:06:06
audit	日志备份	/logAudit/logBack...	GET	1	3	成功	172.20.1.100	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML...	2025-03-24 10:06:05
audit	日志备份	/logAudit/logBack...	GET	1	2	成功	172.20.1.100	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML...	2025-03-24 10:06:03
audit	日志备份	/logAudit/logBack...	GET	1	2	成功	172.20.1.100	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML...	2025-03-24 10:06:01
audit	日志备份	/logAudit/logBack...	GET	1	3	成功	172.20.1.100	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML...	2025-03-24 10:05:55
audit	日志备份	/logAudit/logBack...	GET	1	5	成功	172.20.1.100	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML...	2025-03-24 10:05:55
audit	日志备份	/logAudit/logBack...	GET	1	4	成功	172.20.1.100	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML...	2025-03-24 10:05:54
audit	日志备份	/logAudit/logBack...	GET	1	3	成功	172.20.1.100	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML...	2025-03-24 10:05:53
audit	日志备份	/logAudit/logBack...	GET	1	2	成功	172.20.1.100	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML...	2025-03-24 10:05:52

15.2 错误日志

错误日志 导出

请求URL	请求方式	请求参数	操作IP	User-Agent	创建时间	操作
-------	------	------	------	------------	------	----

15.3 登录日志

登录日志 导出

用户名	操作类型	状态	操作IP	User-Agent	创建时间
admin	登录	成功	172.17.0.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36	2025-03-24 10:04:46
admin	登录	成功	172.17.0.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36	2025-03-24 09:46:40
admin	登录	成功	172.17.0.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36	2025-03-24 09:45:57
admin	登录	成功	172.17.0.1	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36	2025-03-24 09:21:48