

奇固科威 HKW-OSAS200 运维安全审计系统 使用说明书 V1.1.12

杭州奇固科威信息安全技术有限公司

2025.01.21

目 录

系统概述.....	3
1. 首页.....	3
2. 资产管理.....	3
2.1 主机管理.....	3
2.2 主机密钥.....	4
2.3 主机身份.....	4
2.4 资产授权.....	5
3. 主机运维.....	5
3.1 主机终端.....	5
4. 运维审计.....	6
4.1 连接日志.....	6
4.2 在线会话.....	7
4.3 文件操作日志.....	7
5. 批量执行.....	8
5.1 命令执行.....	8
5.2 执行日志.....	9
5.3 批量上传.....	9
5.4 上传任务.....	9
5.5 执行模板.....	10
6. 计划任务.....	10
6.1 任务列表.....	10
6.2 任务日志.....	11
7. 系统管理.....	11
7.1 菜单管理.....	11
7.2 角色管理.....	11
7.3 用户管理.....	12
7.4 标签管理.....	12
7.5 SYSLOG 外发.....	12
7.6 系统设置.....	13
7.7 授权管理.....	13
8. 日志管理.....	14
8.1 系统操作日志.....	14
9. 消息通知.....	15
注意事项.....	16

系统概述

运维安全审计系统，以下简称堡垒机，是一款功能强大的网络访问控制系统，旨在提供安全、高效的服务器及网络资源管理。通过精细的权限控制、实时的操作监控和全面的日志审计，本系统能够确保企业信息安全，提升运维效率。

1. 首页

功能简介

首页展示了系统的关键信息，包括：

- 最近资产访问量
- 最近终端连接记录
- 用户登录日志
- 操作日志
- 用户数量
- 设备数量
- 在线会话占比
- 今日批量执行次数



使用说明

管理员可以通过首页快速了解系统运行状态和用户活动情况，及时发现异常行为。

2. 资产管理

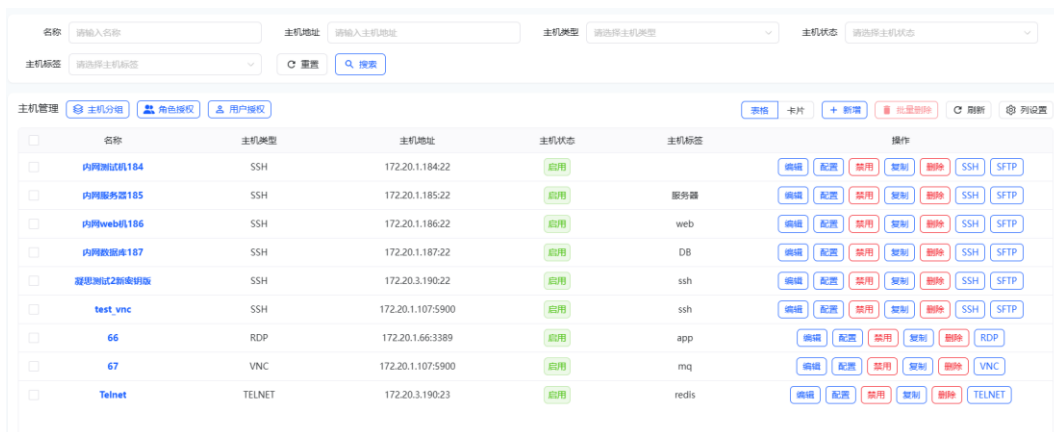
2.1 主机管理

功能简介

提供主机的增删改查功能，支持配置默认登录方式和远程连接按钮。

主机信息包括：

- 名称
- 主机类型
- 主机地址
- 主机状态
- 主机标签



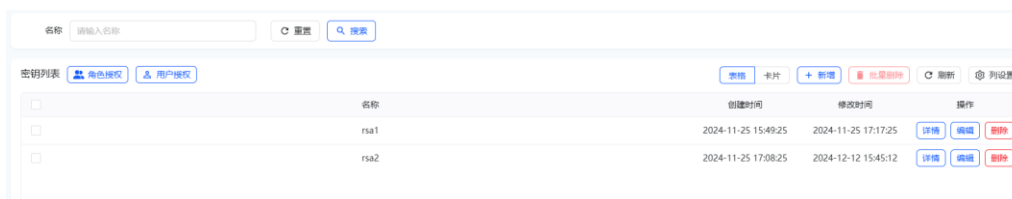
使用说明

- 添加主机：点击“新增”按钮，填写主机信息并保存。
- 编辑主机：选择主机，点击“编辑”按钮修改信息。
- 删除主机：选择主机，点击“删除”按钮。
- 远程连接：点击主机右侧的“连接”按钮，快速登录主机。

2.2 主机密钥

功能简介

用于配置通用的主机登录密钥，方便用户快速登录主机。



使用说明

- 点击“新增密钥”，填写密钥信息并保存。
- 支持密钥的导入和导出。

2.3 主机身份

功能简介

配置通用的主机登录用户，简化登录流程。



使用说明

- 点击“新增身份”，填写用户名和密码信息并保存。

2.4 资产授权

功能简介

提供主机分组授权、主机密钥授权和主机身份授权功能，支持按角色和用户进行授权。



使用说明

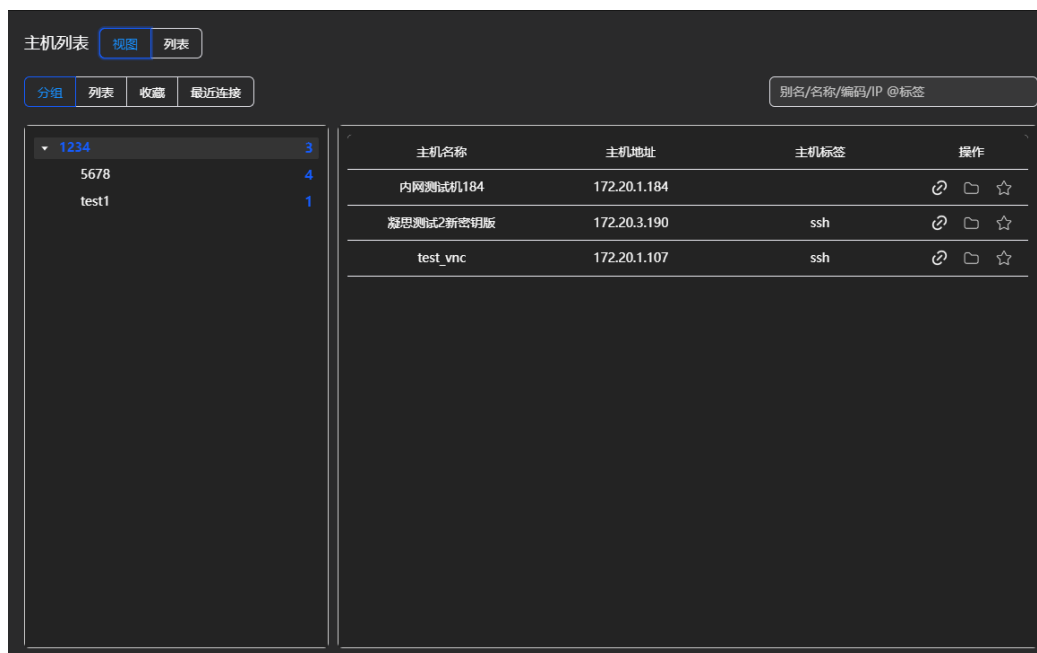
- 选择主机或主机组，配置授权用户或角色。
- 支持批量授权和取消授权。

3. 主机运维

3.1 主机终端

功能简介

提供主机终端访问功能，用户可以通过该功能远程连接并管理主机。



使用说明

- 选择主机，点击“连接”按钮，进入终端界面。
- 支持多种终端协议（如 SSH、RDP 等）。

4. 运维审计

4.1 连接日志

功能简介

记录并查询连接日志，支持视频回放和强制下线功能。

连接信息包括：

- 连接用户
- 连接主机
- 类型
- 状态
- 留痕地址
- 连接时间
- 操作

终端连接日志

连接用户	连接主机	类型	状态	留痕地址	连接时间	操作
wangl	内网测试机184 172.20.1.184	SSH	连接中	内网IP 172.20.1.66	从2025-02-06 14:18:06 至: 2025-02-06 14:18:06	视频回放 详情 下线 删除
admin	内网测试机184 172.20.1.184	SFTP	完成	内网IP 172.20.1.107	从2025-01-15 14:44:15 至: 2025-01-15 14:49:15	详情 删除
wangl	内网测试机184 172.20.1.184	SFTP	完成	内网IP 172.20.1.66	从2025-01-14 14:32:14 至: 2025-01-14 14:45:14	详情 删除
wangl	内网测试机184 172.20.1.184	SFTP	强制下线	内网IP 172.20.1.66	从2025-01-14 14:31:14 至: 2025-01-17 17:17:17	详情 删除
wangl	蓝思测试机-新密码版 172.20.3.190	SFTP	完成	内网IP 172.20.1.66	从2025-01-14 14:30:14 至: 2025-01-14 14:31:14	详情 删除
wangl	内网测试机184 172.20.1.184	SFTP	强制下线	内网IP 172.20.1.66	从2025-01-14 14:29:14 至: 2025-01-17 17:18:17	详情 删除
wangl	蓝思测试机-新密码版 172.20.3.190	SFTP	完成	内网IP 172.20.1.66	从2025-01-14 09:12:14 至: 2025-01-14 10:10:14	详情 删除
wangl	蓝思测试机-新密码版 172.20.3.190	SFTP	完成	内网IP 172.20.1.66	从2025-01-14 08:56:14 至: 2025-01-14 09:01:14	详情 删除
admin	蓝思测试机-新密码版 172.20.3.190	SSH	完成	内网IP 172.20.1.107	从2025-01-09 17:07:09 至: 2025-01-09 17:08:09	视频回放 详情 删除

共 710 条

使用说明

- 查询日志：选择时间范围、用户或主机进行筛选。
- 视频回放：点击“回放”按钮，查看连接过程的录像。
- 强制下线：选择会话，点击“强制下线”按钮。

4.2 在线会话

功能简介

管理正在连接的会话，支持强制下线功能。

会话信息包括：

- 连接用户
- 连接主机
- 类型
- 留痕地址
- 开始时间
- 操作

主机在线会话

连接用户	连接主机	类型	留痕地址	开始时间	操作
wangl	内网测试机184 172.20.1.184	SSH	内网IP 172.20.1.66	2025-02-06 16:02:06	下线

使用说明

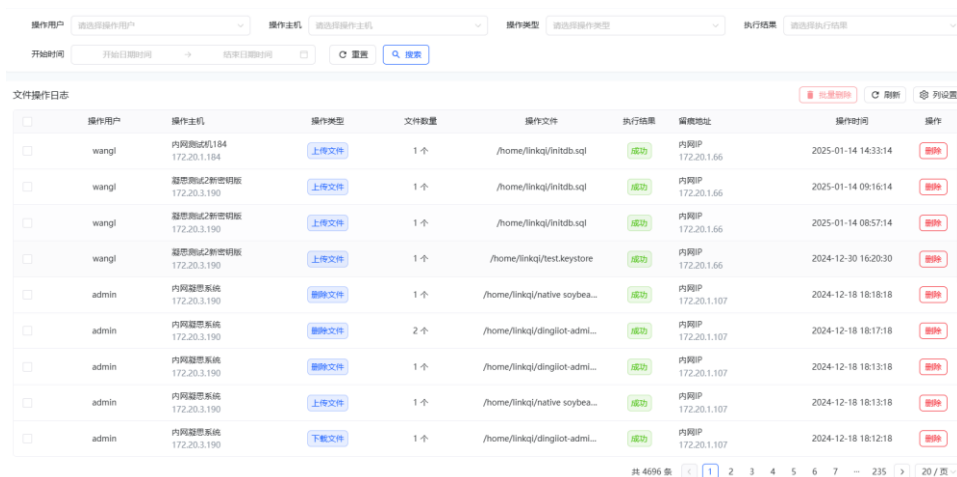
- 查看在线会话：实时显示当前连接的主机会话。
- 强制下线：选择会话，点击“强制下线”按钮。

4.3 文件操作日志

功能简介

分页展示上传和下载的文件日志，包括：

- 操作用户
- 操作主机
- 操作类型
- 文件数量
- 操作文件
- 执行结果
- 留痕地址
- 操作时间



操作用户	操作主机	操作类型	文件数量	操作文件	执行结果	留痕地址	操作时间	操作
wangl	内网测试机184 172.20.1.184	上传文件	1个	/home/linkq/initdb.sql	成功	内网IP 172.20.1.66	2025-01-14 14:33:14	删除
wangl	蓝思测试新密机版 172.20.3.190	上传文件	1个	/home/linkq/initdb.sql	成功	内网IP 172.20.1.66	2025-01-14 09:16:14	删除
wangl	蓝思测试新密机版 172.20.3.190	上传文件	1个	/home/linkq/initdb.sql	成功	内网IP 172.20.1.66	2025-01-14 08:57:14	删除
wangl	蓝思测试新密机版 172.20.3.190	上传文件	1个	/home/linkq/testkeystore	成功	内网IP 172.20.1.66	2024-12-30 16:20:30	删除
admin	内网测试系统 172.20.3.190	删除文件	1个	/home/linkq/native soybea...	成功	内网IP 172.20.1.107	2024-12-18 18:18:18	删除
admin	内网测试系统 172.20.3.190	删除文件	2个	/home/linkq/dingliot-admi...	成功	内网IP 172.20.1.107	2024-12-18 18:17:18	删除
admin	内网测试系统 172.20.3.190	删除文件	1个	/home/linkq/dingliot-admi...	成功	内网IP 172.20.1.107	2024-12-18 18:13:18	删除
admin	内网测试系统 172.20.3.190	上传文件	1个	/home/linkq/native soybea...	成功	内网IP 172.20.1.107	2024-12-18 18:13:18	删除
admin	内网测试系统 172.20.3.190	下载文件	1个	/home/linkq/dingliot-admi...	成功	内网IP 172.20.1.107	2024-12-18 18:12:18	删除

使用说明

- 查询日志：选择时间范围、用户或主机进行筛选。

5. 批量执行

5.1 命令执行

功能简介

选择主机并输入预执行的命令，点击执行即可批量执行命令。



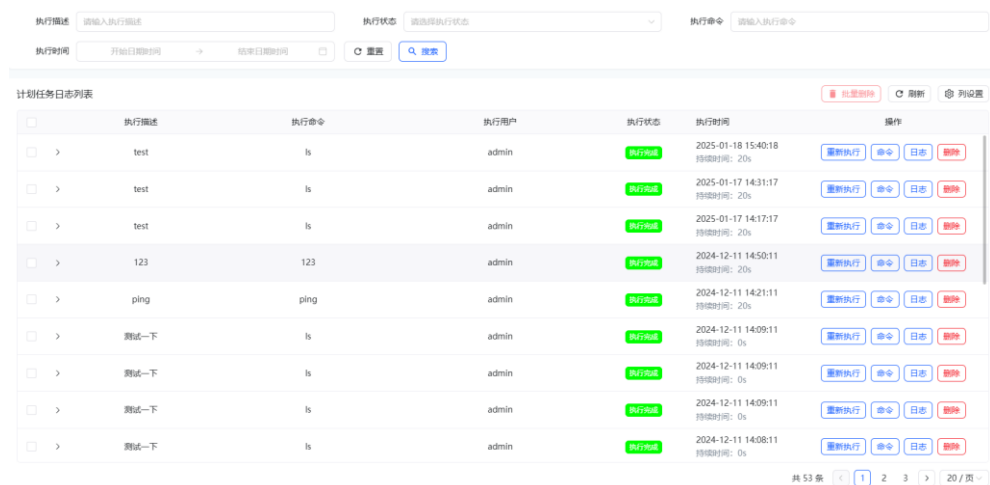
使用说明

- 选择主机，输入命令，点击“执行”按钮。

5.2 执行日志

功能简介

分页展示执行命令的日志，方便管理员查看命令执行情况。



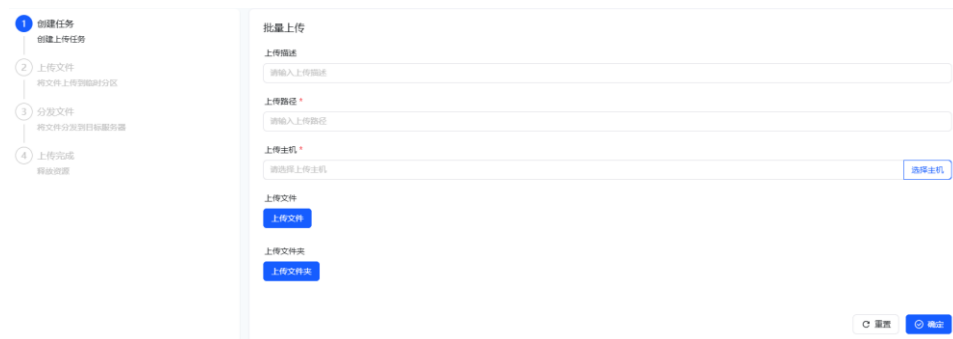
使用说明

- 查询日志：选择时间范围、用户或主机进行筛选。

5.3 批量上传

功能简介

选择多个文件和文件夹，然后选择多个主机进行批量上传。



使用说明

- 选择文件和主机，点击“上传”按钮。

5.4 上传任务

功能简介

分页展示上传任务，包括：

- 上传用户
- 上传描述
- 远程路径
- 上传状态
- 文件数量

- 主机数量
- 上传时间

<input type="checkbox"/>	上传用户	上传描述	远程路径	上传状态	文件数量	主机数量	上传时间	操作
<input type="checkbox"/>	admin	finallyTest	/home/linkqj	已完成	6	2	2025-01-16 10:56:16	删除
<input type="checkbox"/>	admin	finallyTest	/home/linkqj	已完成	6	2	2025-01-16 10:14:16	删除
<input type="checkbox"/>	admin	test	/home/linkqj	已完成	5	1	2025-01-16 10:09:16	删除
<input type="checkbox"/>	admin	test	/home/linkqj	已完成	3	1	2025-01-16 10:06:16	删除
<input type="checkbox"/>	admin	test	/home/linkqj	已完成	2	1	2025-01-16 10:01:16	删除
<input type="checkbox"/>	wangl	0116	/home/linkqj	已完成	4	1	2025-01-16 10:00:16	删除
<input type="checkbox"/>	admin	test	/home/linkqj	已完成	2	1	2025-01-16 09:55:16	删除
<input type="checkbox"/>	admin	ceshi	/home/linkqj	已完成	2	1	2025-01-16 09:53:16	删除
<input type="checkbox"/>	admin	ceshi	/home/linkqj	已完成	2	1	2025-01-16 09:43:16	删除
<input type="checkbox"/>	admin	test	/home/linkqj	等待中	3	1	2025-01-15 20:22:15	删除
<input type="checkbox"/>	admin	test	/home/linkqj	已完成	3	1	2025-01-15 20:08:15	删除
<input type="checkbox"/>	admin	test	/home/linkqj	已完成	3	1	2025-01-15 20:07:15	删除

使用说明

- 查询任务：选择时间范围、用户或主机进行筛选。

5.5 执行模板

功能简介

提供执行模板的增删改查功能，方便管理员配置和管理常用的执行命令。

<input type="checkbox"/>	模板名称	模板命令	修改时间	操作
<input type="checkbox"/>	test	123	2024-11-28 15:38:28	执行 编辑 删除

使用说明

- 点击“新增模板”，填写命令信息并保存。

6. 计划任务

6.1 任务列表

功能简介

分页展示和配置动态定时的执行命令。

任务信息包括：

- 任务名称
- cron 表达式
- 执行命令
- 任务状态
- 最近执行时间
- 创建时间



使用说明

- 点击“新增任务”，填写任务信息并保存。

6.2 任务日志

功能简介

分页展示执行任务的日志，方便管理员查看任务执行情况。



使用说明

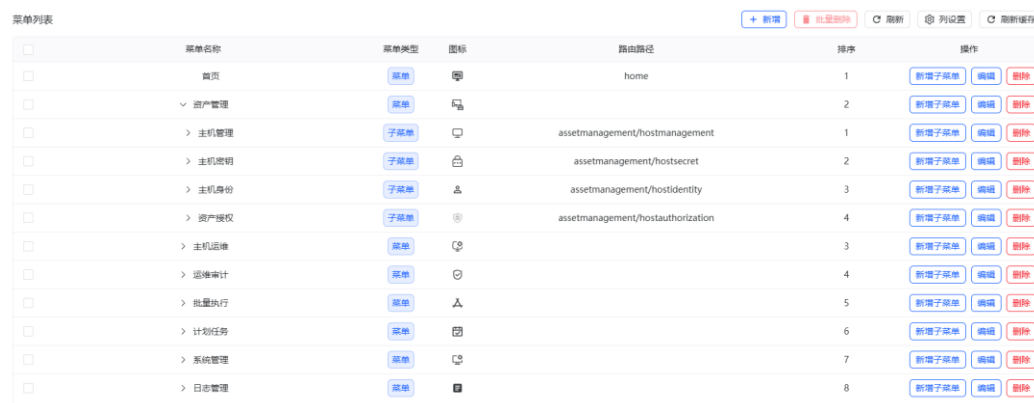
- 查询日志：选择时间范围、任务名称进行筛选。

7. 系统管理

7.1 菜单管理

功能简介

配置菜单和对应的权限码，方便管理员管理系统的菜单结构。



使用说明

- 点击“新增菜单”，填写菜单信息并保存。

7.2 角色管理

功能简介

分页展示角色信息，并提供增删改查功能。



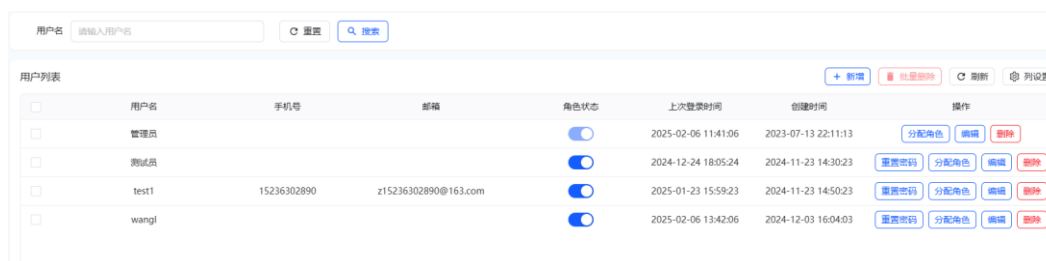
使用说明

- 点击“新增角色”，填写角色信息并保存。

7.3 用户管理

功能简介

分页展示用户信息，提供增删改查功能、重置密码和配置角色等。



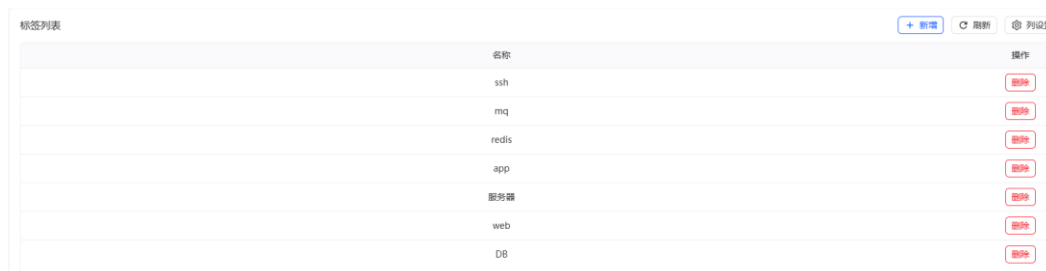
使用说明

- 点击“新增用户”，填写用户信息并保存。

7.4 标签管理

功能简介

管理主机的标签，方便对主机进行分类和管理。



使用说明

- 点击“新增标签”，填写标签信息并保存。

7.5 SYSLOG 外发

功能简介

动态配置 SYSLOG 向外推送，实现日志的集中管理和分析。



使用说明

- 配置 SYSLOG 服务器地址和端口，点击“保存”。

7.6 系统设置

功能简介

配置 sftp 文件预览数量等系统设置。



使用说明

- 修改设置后，点击“保存”。

7.7 授权管理

功能简介

进行正版授权激活，确保系统的合法使用。

注册流程

步骤1: 点击【获取注册码】按钮, 获取唯一注册码

步骤2: 输入授权码字符串或者选择授权码key文件。输入授权码字符串后执行步骤3、选择授权码key文件即可完成注册

步骤3: 点击【注册】按钮, 完成注册

状态 已注册

证书信息

证书名称	测试项目名称
证书编码	DA01-8674-C1E8-483B-D9CD-69D9-1817-D3D8
证书校验码	88BDCBF84599CFD9C16BF2BE91B1CA2E
证书签发机构	杭州领祺科技有限公司
是否永久有效	否
截止有效期	2026-12-31

使用说明

- 输入授权码, 点击“激活”。
- 上传授权证书进行激活

8. 日志管理

8.1 系统操作日志

功能简介

分页展示系统操作日志, 包括:

- 操作用户
- 操作模块
- 风险等级
- 执行结果
- 操作日志
- 留痕地址
- 操作时间

操作用户: 风险等级: 执行结果:

执行时间: ->

系统操作日志

<input type="checkbox"/>	操作用户	操作模块	风险等级	执行结果	操作日志	源端地址	操作时间	操作
<input type="checkbox"/>	wangl	terminalconnect/assetterminal	高风险	成功	连接主机 SSH 内网测试机104	内网IP 172.20.1.66	2025-02-06 14:18:06	<input type="button" value="详情"/> <input type="button" value="删除"/>
<input type="checkbox"/>	wangl	authenticationlogin/infraauthentication	高风险	成功	登录系统	内网IP 172.20.1.66	2025-02-06 13:42:06	<input type="button" value="详情"/> <input type="button" value="删除"/>
<input type="checkbox"/>	wangl	authenticationlogout/infraauthentication	高风险	成功	退出系统	内网IP 172.20.1.66	2025-02-06 13:38:06	<input type="button" value="详情"/> <input type="button" value="删除"/>
<input type="checkbox"/>	wangl	authenticationlogin/infraauthentication	高风险	成功	登录系统	内网IP 172.20.1.66	2025-02-06 13:33:06	<input type="button" value="详情"/> <input type="button" value="删除"/>
<input type="checkbox"/>	admin	authenticationlogin/infraauthentication	高风险	成功	登录系统	内网IP 172.20.1.107	2025-02-06 11:41:06	<input type="button" value="详情"/> <input type="button" value="删除"/>
<input type="checkbox"/>	admin	authenticationlogin/infraauthentication	高风险	成功	登录系统	内网IP 172.20.1.107	2025-02-06 08:49:06	<input type="button" value="详情"/> <input type="button" value="删除"/>
<input type="checkbox"/>	admin	authenticationlogin/infraauthentication	高风险	成功	登录系统	内网IP 172.20.1.107	2025-02-06 08:31:06	<input type="button" value="详情"/> <input type="button" value="删除"/>
<input type="checkbox"/>	test1	authenticationlogout/infraauthentication	高风险	成功	退出系统	内网IP 172.20.1.107	2025-01-23 15:59:23	<input type="button" value="详情"/> <input type="button" value="删除"/>
<input type="checkbox"/>	test1	authenticationlogin/infraauthentication	高风险	成功	登录系统	内网IP 172.20.1.107	2025-01-23 15:59:23	<input type="button" value="详情"/> <input type="button" value="删除"/>
<input type="checkbox"/>	test1	authenticationlogin/infraauthentication	高风险	失败	登录系统	内网IP 172.20.1.107	2025-01-23 15:59:23	<input type="button" value="详情"/> <input type="button" value="删除"/>
<input type="checkbox"/>	test1	authenticationlogout/infraauthentication	高风险	成功	退出系统	内网IP 172.20.1.107	2025-01-23 15:50:23	<input type="button" value="详情"/> <input type="button" value="删除"/>

共 6216 条

使用说明

- 查询日志：选择时间范围、用户或模块进行筛选。

9. 消息通知



点击右上角区域如图所示小图标，可以查看系统通知的内容。

注意事项

1. 请勿将管理员账号泄露给无关人员。
2. 定期更换管理员密码和用户密码。
3. 定期检查系统日志，及时发现并处理异常行为。
4. 如遇紧急情况，请立即联系技术支持人员。

本说明书仅供参考，具体操作可能因系统版本和配置环境的不同而有所差异。如有任何疑问或需要进一步的帮助，请随时联系我们的技术支持团队。