

山石网科日志审计平台用户手册

Version 2.0



目录

设备控制	1
业务控制台说明	1
管理控制台说明	2
系统信息	3
账号口令管理	3
网络管理	4
系统工具	5
日期时间管理	9
数据库备份与恢复	9
日志备份与恢复	9
系统恢复	10
重置平台初始口令	10
系统停止与重启	11
系统参数配置	11
CLI 控制台	12
修改 CLI 用户密码	13
查看组件状态	13
重启组件	13
关闭设备	13
重启设备	14
进入 Console 口	14
重置业务控制台密码	14
重置管理控制台密码	14
查看版本信息	14
查看运行时间	14
查看网卡信息	14
配置网卡 IPV4 地址	14
配置设置网卡 IPV6 地址	14
修改管理控制平台 WEB 端口	15
修改业务控制平台 WEB 端口	15
业务系统配置	15
资产管理配置	15
资产管理简介	15
资产添加	16
资产批量导入	17
自定义产品添加	18
日志标准化配置	19
日志接入说明	19
syslog 方式（常见）	20
WMI 方式（常见）	23
文件方式（常见）	28
数据库方式	29
日志归并	30
日志过滤	30
关联策略配置	31
关联策略说明	31

具体配置.....	35
审计策略配置.....	42
审计策略说明.....	42
具体配置.....	42
审计对象管理.....	45
事件查看.....	49
安全仪表盘查看.....	49
告警监控.....	52
实时监控.....	53
日志列表.....	54
关联事件.....	56
审计事件.....	56
日常维护.....	57
修改密码.....	57
软件版本升级.....	57
修改 IP 地址.....	58
日志查看.....	59
恢复出厂设置.....	60
实施后设备运行检查.....	60
整体运行状态检测.....	60
主要功能使用情况检查.....	62
常见问题处理.....	62
配置了采集器，却没有收到相应数据.....	62
接收到日志，但是日志名为通用日志.....	63

关于本手册

手册约定

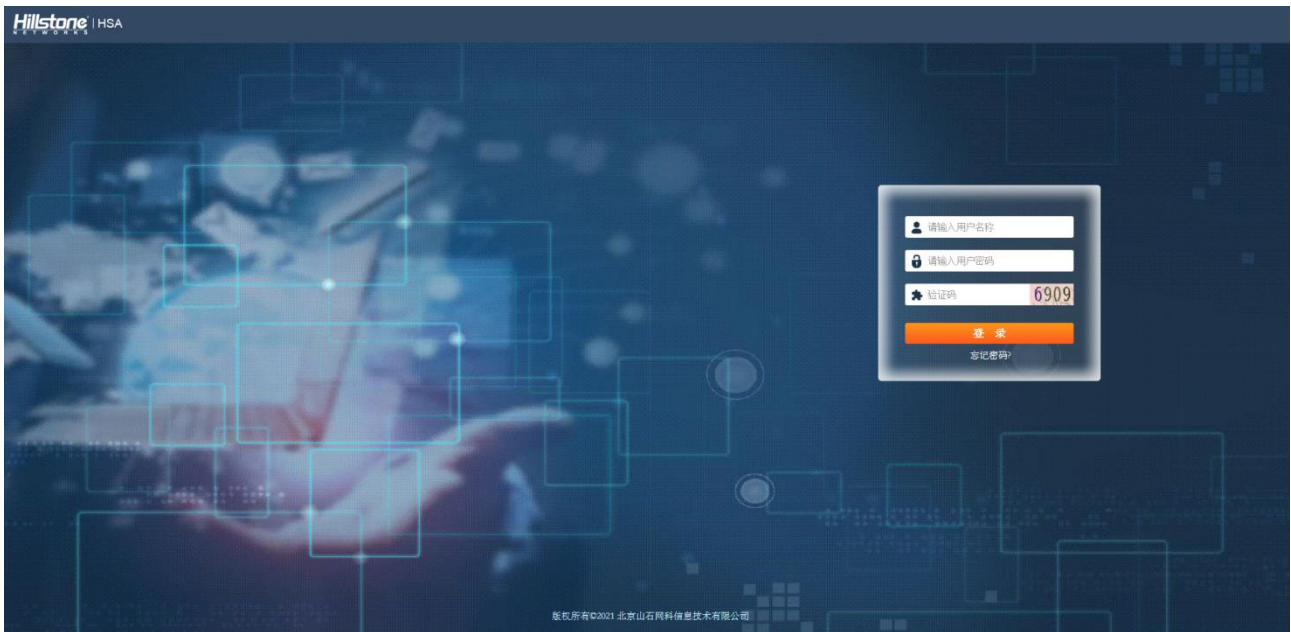
本手册内容约定如下：

- ◆ 提示：为用户提供相关参考信息。
- ◆ 注意：如果该操作不正确，会导致系统出错。
- ◆ 『 』：用该方式表示 Hillstone 设备 WebUI 界面上的按钮。例如：点击『保存』按钮保存操作。

设备控制

业务控制台说明

用户对山石网科日志审计平台的绝大部分操作主要通过业务控制台完成。通过业务控制台可以对山石网科日志审计平台的具体业务模块进行设置、安全内容进行查看，主要包含授权更新、日志标准化设置、资产管理、告警策略配置、安全事件查看等等。



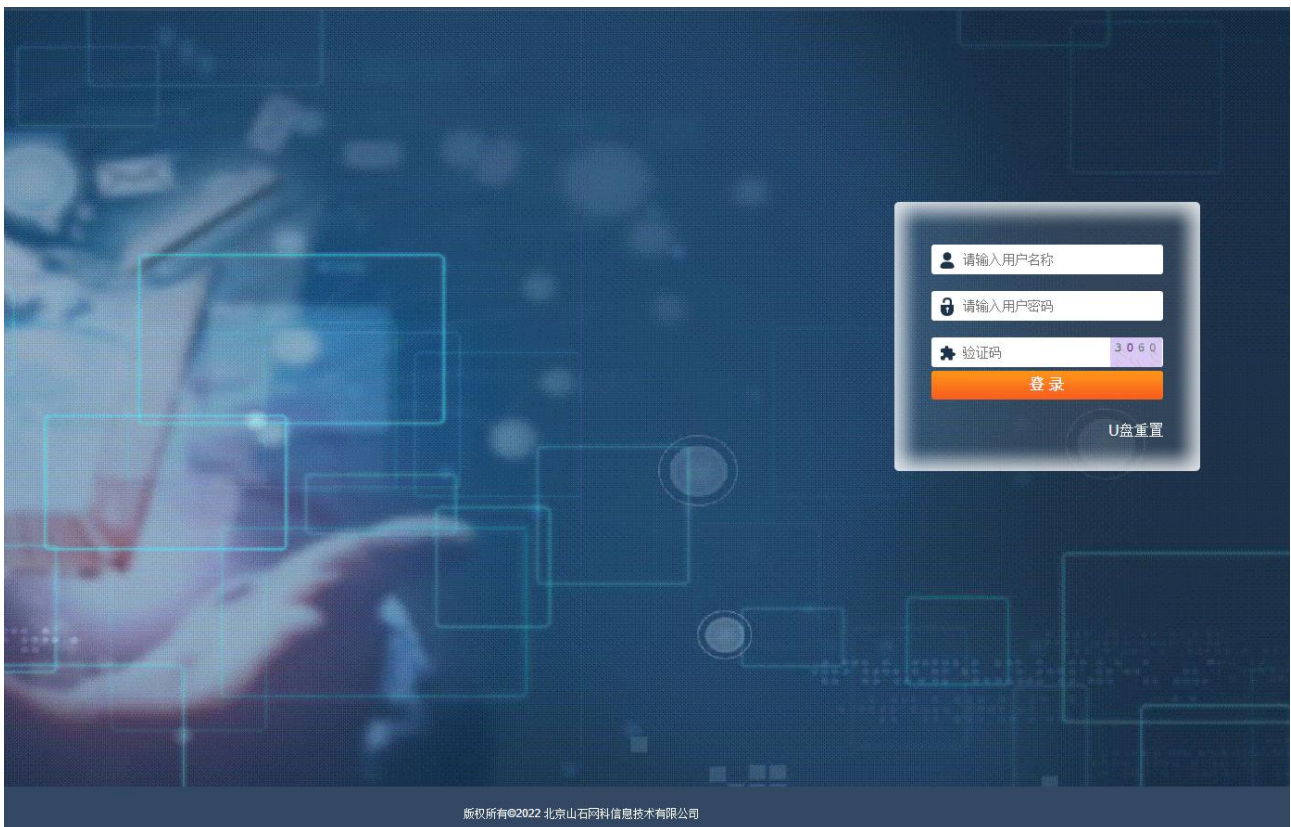
操作步骤：

1. 用网线连接安装软件时设定 IP 的物理网口（假设安装时为服务器的第一块网卡设定 IP 地址为

192.168.1.1)。

2. 确管理计算机的 IP 地址与服务器同网段，这里设置为 192.168.1.2，子网掩码为 255.255.255.0。
3. 在电脑上打开浏览器（建议使用 Chrome、Firefox 其中一种）。
4. 地址栏输入 https://192.168.1.1。
5. 默认用户名/密码：admin/hillstone（首次登录需要修改密码）。

管理控制台说明



操作步骤：

1. 用网线连接安装软件时设定 IP 的物理网口（假设安装时为服务器的第一块网卡设定 IP 地址为 192.168.1.1）。
2. 确管理计算机的 IP 地址与服务器同网段，这里设置为 192.168.1.2，子网掩码为 255.255.255.0。
3. 在电脑上打开浏览器（建议使用 Chrome、Firefox 其中一种）。
4. 地址栏输入 https://192.168.1.1:8082。
5. 默认用户名/密码：admin/hillstone（首次登录需要修改密码）。

系统信息

展示产品硬件、版本等信息。

系统信息

CPU型号	Intel(R) Xeon(R) CPU E5-2678 v3 @ 2.50GHz
CPU线程数	4
内存总量	8 GB
硬盘总量	41.35 GB
设备型号	HSA
硬件标识	445EB-F7AA4-B822C-51E71-FD7B1
软件版本号	V2.0
硬件版本号	V1.0
软件序列号	F912E-EB764-74E59-6B4DB-EF63E

账号口令管理

修改管理控制平台用户密码。

账号口令管理

账号	admin
原密码	<input type="password"/>
新密码	<input type="password"/>
确认密码	<input type="password"/>

网络管理

提示：安全资源池版本采用 DHCP 方式，不支持此功能。

网络配置

配置网卡地址信息，业务口为访问业务系统的 IP。

网络管理

网络配置 路由配置

主机名

业务口IP

网关 DNS

序号	名称	MAC	IPV4	IPV6
1	eth0	00:0C:29:D5:B8:05	<input type="text" value="192.168.100.126"/> IPV4掩码 <input type="text" value="255.255.255.0"/>	<input type="text"/> IPV6地址 <input type="text"/> 子网前缀长度
2	eth1		<input type="text"/> IPV4掩码 <input type="text"/>	<input type="text"/> IPV6地址 <input type="text"/> 子网前缀长度
3	eth2		<input type="text"/> IPV4掩码 <input type="text"/>	<input type="text"/> IPV6地址 <input type="text"/> 子网前缀长度

路由配置

配置系统路由信息。

网络管理

网络配置 **路由配置**

系统路由表

目的IP地址	网关	掩码	接口
192.168.100.0	0.0.0.0	255.255.255.0	eth0
192.168.20.0		255.255.255.0	eth0
0.0.0.0		0.0.0.0	eth0
fe80::		64	eth0
::		0	eth0
::		0	eth0
ff02::1		128	eth0
ff00::	::	8	eth0
fe80::		64	eth5
::	fe80:a00:27ff:fec4:ff2b	0	eth5
::	fe80::1:1	0	eth5
ff02::1	ff02::1	128	eth5
ff00::	::	8	eth5

添加路由

接口: eth0

目的IP: 请输入地址信息

网关: 请输入网关

保存 取消

静态路由表

目的IP地址	网关	掩码	接口	操作
当前无可用记录				
+ 新增静态路由				

系统工具

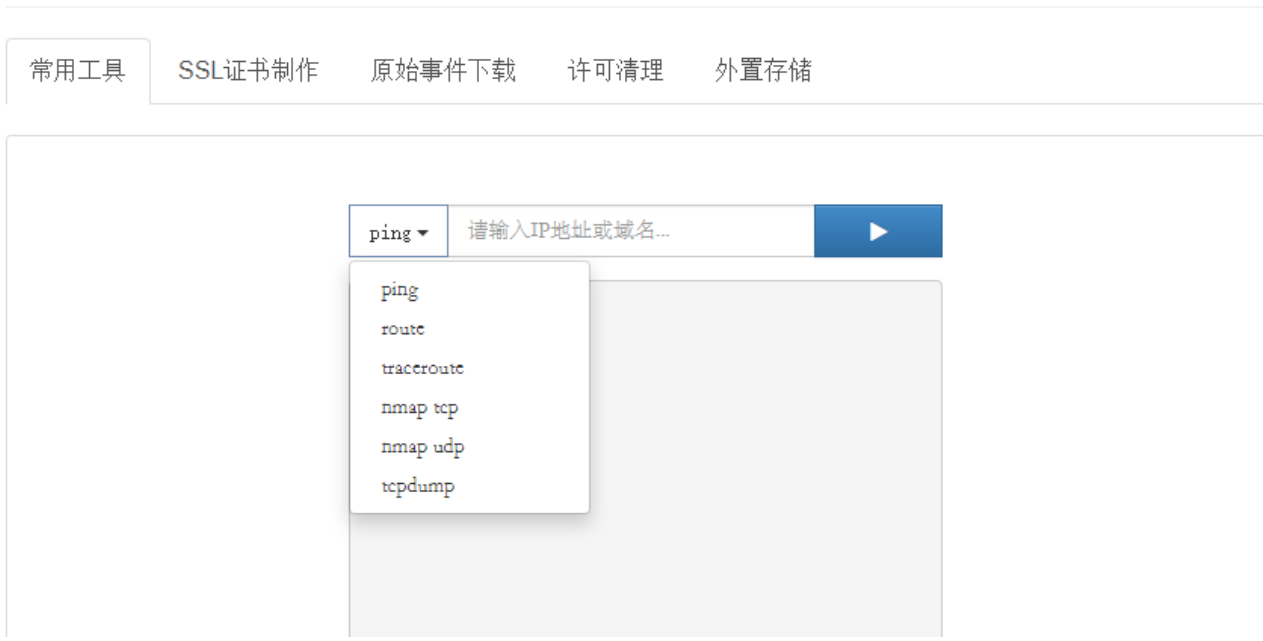
常用工具

对目标地址进行 traceroute、ping、tcpdump 操作。

系统工具



系统工具



SSL 证书制作

系统工具

常用工具 **SSL证书制作** 原始事件下载 许可清理 外置存储

① 双向认证证书使用步骤: 1.制作证书,证书制作完成后将会自动下载 → 2.点击证书生效按钮,导入下载完成的证书,系统将会自动重启(请务必保存证书,否则你将无法进入系统) → 3.系统重启后,手动向浏览器导入客户端证书,访问系统

设置密码

确认密码

IP地址或域名一

IP地址或域名二

IP地址或域名三

IP地址或域名四

IP地址或域名五

证书制作 证书下载 证书生效

原始日志下载

下载原始日志及通用日志。

系统工具

常用工具 SSL证书制作 **原始事件下载** 许可清理 外置存储

日志选择 所有日志 通用日志

设备地址 需要下载的日志条数,最多不能超过200000条

下载条数

原始日志文件

序号	文件名	大小 (KB)	操作
----	-----	---------	----

开始

许可清理

清理产品当前许可信息，重新获取授权（用户一般无需此操作，仅生产使用）。

系统工具

常用工具 SSL证书制作 原始事件下载 **许可清理** 外置存储

验证码

外置存储

当系统内置存储不足以支撑用户的存储需求时，可以通过该功能进行外置存储扩容。

系统工具

常用工具 SSL证书制作 原始事件下载 许可清理 **外置存储**

⚠ 如果挂载失败或连接异常，请查看规则 ?

当前使用情况： NFS:未使用 NAS:未使用 ISCSI:未使用

NFS 磁盘使用情况	NAS 磁盘使用情况	ISCSI 磁盘使用情况

存储方式 NFS(linux) NAS(linux) ISCSI(linux)

IP地址

NFS路径

提示：

1. 挂载外置存储后，内置硬盘数据只读，新日志将写入外置存储内。
2. 当 NFS 服务器死亡后，对我们的设备将造成影响，需要卸载 NFS 后才能使用。

日期时间管理

修改时间、日期及时区信息（仅限平台服务器）。

日期时间管理

当前日期	<input type="text" value="2022-08-09"/>
当前时间	<input type="text" value="12:35:22"/>
当前时区	<input type="text" value="Shanghai"/>
<input type="button" value="当前时间"/> <input type="button" value="保存"/>	

数据库备份与恢复

将数据库数据备份至其他系统，用户可设置数据的备份方式（仅限平台服务器）。

数据库备份与恢复

ⓘ 数据库备份支持立即备份或者定期备份全量数据，当数据库出现异常导致无法使用的情况，可以通过数据库恢复功能恢复到指定时间点。

备份	恢复					
配置						
序号	备份方式	备份服务器地址	备份时间	进度	状态	操作
当前无可用记录						

日志备份与恢复

将日志数据备份至其他系统，用户可设置数据的备份方式（仅限平台服务器）。

以上内容仅为本文档的试下载部分，为可阅读页数的一半内容。如要下载或阅读全文，请访问：<https://d.book118.com/288042047060006135>