山石网科日志审计平台用户手册

Version 2.0

目录

关于本手册

手册约定

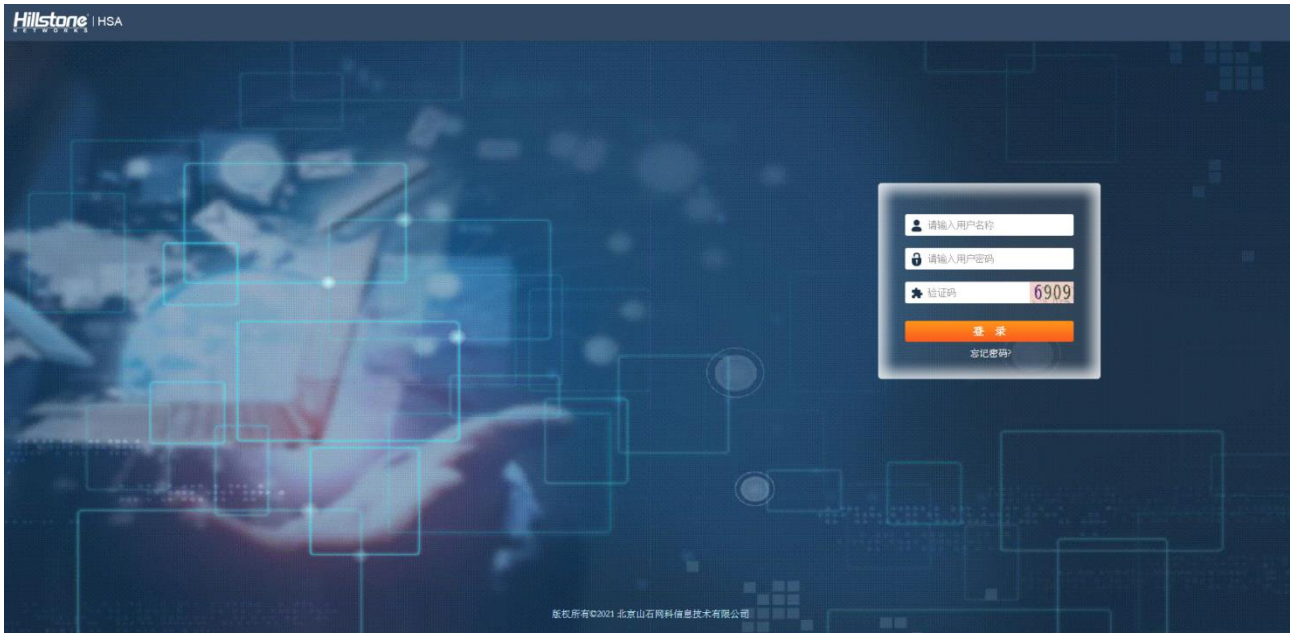
本手册内容约定如下：

- 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。



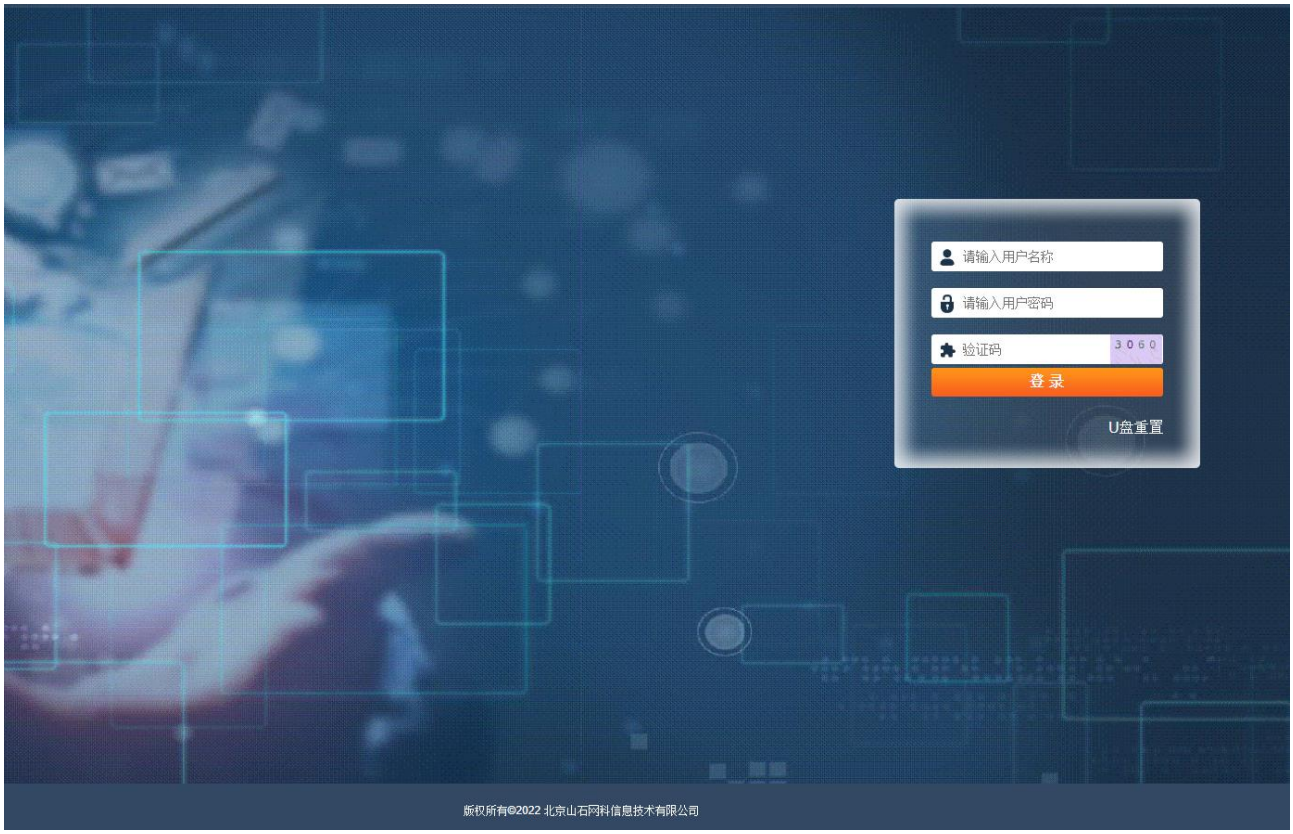
操作步骤：

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. 确保管理计算机的 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：

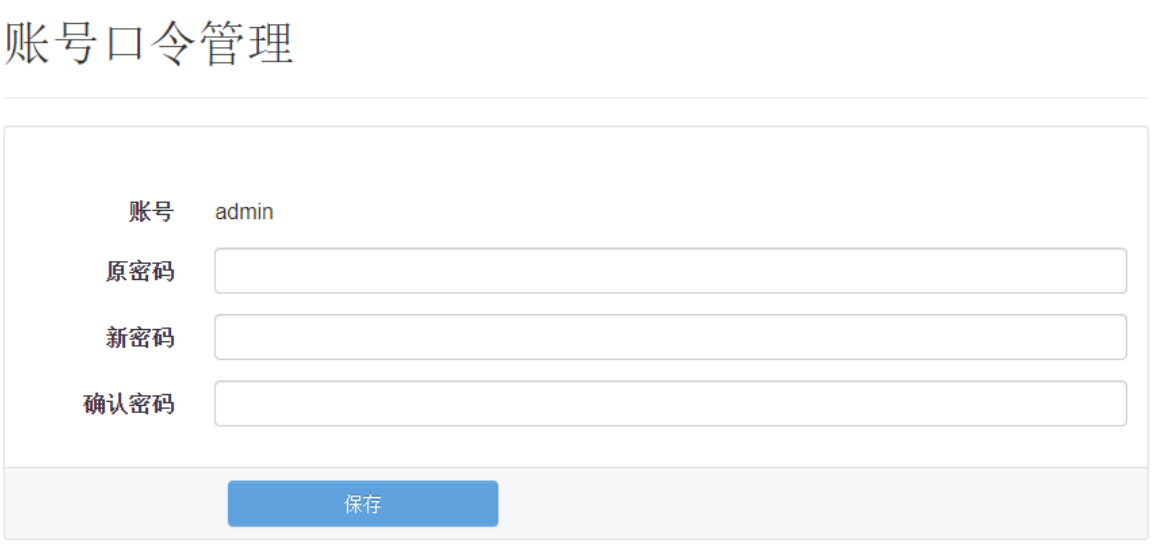
1. 用网线连接安装软件时设定 IP 的物理网口（假设安装时为服务器的第一块网卡设定 IP 地址为 192.168.1.1）。
2. 确保管理计算机的 IP 地址与服务器同网段，这里设置为 192.168.1.2，子网掩码为 255.255.255.0。
3. 在电脑上打开浏览器（建议使用 Chrome、Firefox 其中一种）。
4. 地址栏输入 https://192.168.1.1:8082。
5. 默认用户名/密码：admin/hillstone（首次登录需要修改密码）。

系统信息

展示产品硬件、版本等信息。

账号口令管理

修改管理控制平台用户密码。

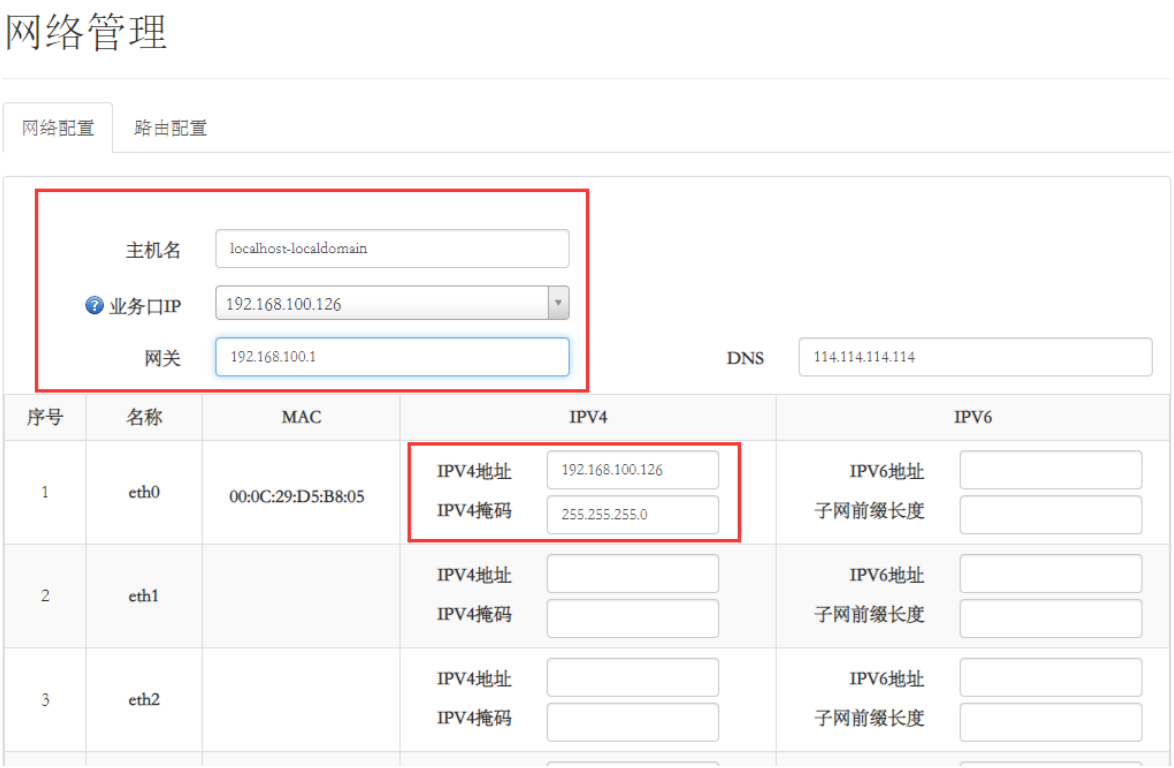


网络管理

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。



路由配置

配置系统路由信息。

系统工具

常用工具

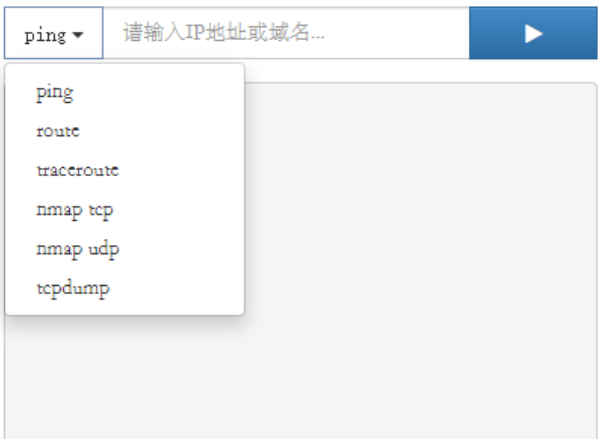
对目标地址进行 traceroute、ping、tcpdump 操作。

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

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



SSL 证书制作

原始日志下载

下载原始日志及通用日志。

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）。

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。

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）。

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）。

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