

山石网科安全审计平台

Virtual Hillstone Security Audit



随着网络建设的快速发展，互联网安全事件的不断增多，国家对网络监管的要求愈发严格，网络监管的范围日益广泛。山石网科安全管理平台虚拟化版（即 Virtual Hillstone Security Audit，简称：vHSA）为客户提供日志存储审计和行为监控溯源功能，配合山石网科全系列安全产品，能够有效记录用户环境中的网络日志和安全日志，可以帮助用户解决全网日志审计的困扰，并为用户提供了丰富便捷的日志查询功能，满足《网络安全法》和上级单位的监管要求。vHSA 可以在 VMware 和 KVM 等虚拟化环境部署，可以满足用户虚拟化安全建设等级保护要求和审计需求。

产品亮点

高性能日志处理，符合大流量应用场景

山石网科安全审计平台采用软硬件一体化设计，结合山石网科独有的日志格式，大幅度提升日志入库速度，日志入库速度最高可达270,000EPS（Event Per Second，每秒事件处理能力），可以满足运营商、高校、政府等大流量应用场景对日志审计的性能要求。同时山石网科安全审计平台的单台存储空间最大可达128T，在大流量应用场景下也可以满足网络安全法180天日志存储要求。

支持多种日志类型，满足不同场景要求

山石网科安全审计平台支持山石网科下一代防火墙发送的多种日志类型的接收和存储，包括 NAT、Session、URL、邮件、IM 上下线和威胁防护日志等，以满足运营商、高校、政府和企业等不同应用场景对日志审计的需求。同时，支持标准 Syslog 日志格式，可对第三方设备发送日志进行接收和存储。

实名制日志审计，轻松追溯查询

山石网科安全审计平台可以和山石网科防火墙配合，在使用认证计费系统的应用场景中，将从认证计费系统获得的用户名和IP对应关系同步给HSA，使HSA接收的日志直接关联用户名。由此，避免了日志溯源时需在安全审计平台上查找IP，再通过认证计费系统查找对应用户名的繁琐操作步骤，可直接从HSA中查询到用户信息的日志，更好的满足监管政策中的实名制审计要求。

丰富的日志查询，实现便捷检索

山石网科安全审计平台支持对海量日志信息进行多条件组合查询，采用独

特的海量数据查询技术，真正实现了即查即显。支持日志全文检索，对收集到的多台设备日志进行全局的统一查询。支持查询条件记忆功能，可以对常用的查询条件生成快捷查询标签，自动的记录最常使用的查询条件，实现便捷检索。在多台HSA部署的场景下，支持分布式查询，可以指定一台Master节点去查询其他分支节点HSA日志，实现集中检索。

可视化监控与报表，实时掌握统计信息

山石网科安全审计平台可实时监控自身设备状态与资源使用情况，图形化呈现日志存储状态及日志采集趋势图，使管理员对日志记录状况一目了然。内置多种报表模板，并为用户提供自定义报表统计功能，支持多种报表格式的导出。同时，还可对发送日志的网络设备进行基本信息的监控，掌握其日志发送的实时状态。

虚拟化安全审计，满足等级保护要求

vHSA是可以部署在VMware和KVM等虚拟化环境的安全审计产品，可以配合山石云·界和山石云·格等虚拟化安全产品，记录其上网行为和安安全日志，满足虚拟化安全建设等级保护要求和审计需求。

拥抱IPv6

山石网科安全审计平台同时支持山石网科下一代防火墙发送的 IPv4 和 IPv6 格式的会话日志、NAT 日志、PBR 日志、SLB 日志。逐步实现从 v4 到 v6 的平滑过渡。

功能规格

设备监控

- 支持设备自身关键信息监控
- 支持日志类型存储占比分析
- 支持设备和日志类型的趋势分析
- 支持对发送日志的设备进行监控
- 支持硬盘状态和 RAID 状态监控
- 支持自定义监控

日志管理

- 支持 NAT Session 等流量日志
- 支持 IPv6 NAT、Session、PBR、SLB 日志
- 支持 URL、邮件和 IM 上下线等数据安全日志
- 支持威胁防护日志
- 支持接入与解析第三方 Syslog 日志
- 支持 Windows 日志
- 支持多条件组合查询
- 支持日志聚合功能
- 支持日志加密传输

- 支持查询条件保存
- 支持后台查询任务
- 支持多设备分布式查询
- 支持日志的导入导出功能
- 支持日志的转发功能
- 满足《网络安全法》合规需求，支持 180 天的日志留存

报表管理

- 内置多种报表模板
- 支持自定义报表
- 支持 HTML、PDF 和 WORD 格式报表文件

系统管理

- 支持可信主机设置
- 支持分布式查询设置
- 支持三权分立管理
- 支持设置夏令时时区

参数		vHSA-2
日志处理速度 (EPS)		二进制NAT日志：30,000 EPS NAT444日志：3,000EPS URL日志：9,000EPS IM日志：6,000EPS WebPost：3,000EPS Session：15,000EPS 文本日志：4,000EPS
注：此处参数为默认配置下性能，具体性能参数视安装时服务器分配资源而定		
存储能力		1G链路下180天NAT日志存储
存储容量		2T
安装环境	处理器	64位处理器，安装和运行需要4个
	内存	安装和运行时要求4GB内存
	网络接口	可虚拟两个网络接口
	虚拟化环境	vMware workstations/EXSI、KVM

Copyright © 2020, Hillstone Networks 版权所有，保留所有权利。

Hillstone、Hillstone Networks 标识、山石网科、StoneOS、StoneManager、HillstonePnVPN 均为 Hillstone Networks 所属商标。

所有其他商标和注册商标均为其各自公司的财产。

本文所包含信息可能会有所修改，恕不另行通知，如需最新信息请浏览 Hillstone Networks 网站(www.hillstonenet.com.cn)。

股票代码：688030

文档编号：EX-08.08-HSA000-2.5.0-0819-Ch-03

www.hillstonenet.com.cn



官方微信



官方微博

中国·销售与服务热线：400-828-6655