H3C SecPath A2000-AK 系列 运维审计系统

产品概述

随着企业信息化建设的不断加强，各类业务系统承载的企业核心数据也越来越多，业务系统的稳定性和安全性变得愈发重要。除了来自于外部的安全威胁外，内部运维人员的操作行为将更为直接的影响业务系统能否正常运行。因此只有依靠严格的用户身份认证、精细化的访问权限控制、细粒度的操作行为审计等运维管理能力，才能降低企业内部运维操作风险，提高运维效率。同时在数字化转型浪潮下，新兴的信息化技术发展迅速，网络安全相关的法律法规也更加严格，对企业安全运维的管理能力提出了新的要求：

- 《网络安全法》、《信息系统等级保护》等法律法规纷纷对业务系统安全审计提出了明确要求。银保监办[2018]313 号便函“安全管理要求 8 条”等行业法规对运维用户的操作管控要求也在不算提升；
- 随着数据中心规模扩大，需要管理的设备数量急剧增加，资产的数据同步、可视化管理需求明显；
- 数据中心灾备建设模式增多，两地三中心、总分分布式、多活集群等部署方式成为常态；
- 虚拟化、云计算、IPv6 等新技术应用，企业 IT 基础设施规模和复杂度都急剧增加；

因此，新华三技术有限公司对 H3C SecPath A2000-AK 系列 运维审计系统进行了特性升级，以应对严苛的政策合规要求，日益复杂的运维环境变化，以及不断革新的技术挑战。

A2000-AK605　A2000-AK610　A2000-AK620　A2000-AK630

H3C SecPath A2000-AK 系列 运维审计系统外观图

产品特点

全面的运维兼容性

- 支持通过 IE、Firefox、Chrome、Safrai 等浏览器进行系统管理及资产访问，同时不依赖 JRE、Flash 环境
- 操作终端兼容 windows 及 Mac 操作系统，不改变用户原有使用环境
- 支持主流 IT 资产，包括主机、网络设备、安全设备、应用、中间件、数据库等

可视化的管理模式

- 支持按不同属性对资产进行多级分类并自动生成动态的树状结构视图，清晰的展示各资产的层级关系
- 借助数据状态标签，自动的统计敏感、异常的用户及资产数据，帮助管理员在海量用户及资产信息应用场景中洞察异常数据
- 通过权限自动化关联分析，直观的展示出用户/资产的权限划分情况，落实权限最小化管理

细粒度的权限控制

- 借助属性建模的方式创建动态的访问控制策略，与动态权限规则相匹配的用户、资产及系统账号会自动赋予相应的访问权限，以此简化权限管理复杂度
- 采用变更单模式实现权限的一键维护，变更单无需审批，但可以自动生成具有时效性的访问权限，使得权限管理变得更加灵活
- 领先的会话复核技术，在传统双人授权的模式上，提供深层次的会话管控手段，复核人可对用户的操作权限进行回收、下放及命令实时批复，进一步提升运维管控能力

可靠的密码管理

- 支持自动化密码管理功能，实现资产账号定期改密，同时具备密码自动拨测、多人分段保管、改密前后异地备份、改密触发校验等多种改密冗余机制确保密码变更的可靠性

- 提供密码动态管理模式，通过密码工单实现资产系统账号密码的动态申请、下放，工单具有时效性，过期后交由系统自动回收变更密码，降低密码管理风险
- 支持资产密码版本库，可同时记录资产系统账号的历史维护密码，并可根据用户需求进行密码备份及回退

全面的行为审计

- 完整记录各类运维操作行为，包括图形会话、字符会话、数据库会话及文件传输会话
- 独特的图形审计存储机制，采用协议分析记录、高压缩比、空闲操作审计记录无变化，减少审计日志的大小，提高空间利用率
- 精准的指令识别技术，确保各种非常规操作指令的准确识别，同时支持指令分层展示，敏感操作智能标记及命令分级播放功能

丰富的检索方式

- 采用三层存储架构，将配置信息、审计数据、审计索引分离存储，有效解决了在大数据应用场景下，数据响应慢的问题
- 基于专业的大数据检索引擎 ES，通过全量、全索引的检索模式，缩短 TB 级审计数据的检索时间，进一步提高审计检索效率
- 具备丰富的、多维度的检索方式，提升问题定位效率，包括会话热点排序、敏感会话统计局、多关键字检索、审计会话合并、图形切片等

高效的运维管理

- 具备运维账号自动化同步功能，可自动同步 AD/LADP 域认证服务器中账号的变更信息，降低管理复杂度
- 支持会话批量启动及基于网盘的文件批量分发功能，简化运维操作
- 通过脚本一键批量执行帮助管理员提高运维管理效率

领先的 IPv6 管理能力

- 全面兼容各类 IPv6 环境，满足数据中心的未来发展规划
- 支持基于 IPv6 环境的系统管理、集中认证、权限管控及行为审计，实现 IPv6 资产的全面集中管控
- 借助 IPv4/IPv6 双栈及隧道技术，帮助用户实现数据中心 IPv4 到 IPv6 的迁移过渡

可靠的部署模式

- 采用旁路部署模式，不需要调整用户网络架构，不需要在服务器上安装插件
- 支持双机 HA 热备，实现运维审计系统冗余化部署
- 支持自身多机集群部署，无需第三方负载均衡设备或共享存储，即可满足用户高并发、高可用的应用需求

产品规格

表1-1 H3C SecPath A2000-AK 系列 运维审计系统 产品规格

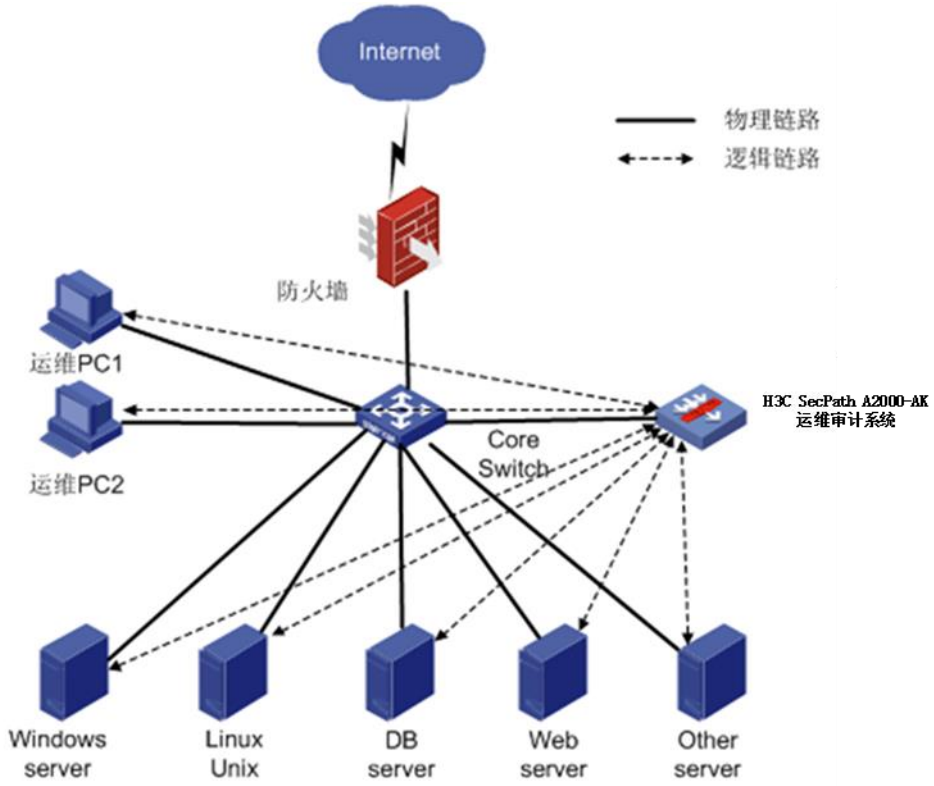
属性	A2000-AK605	A2000-AK610	A2000-AK620	A2000-AK630
兼容性	支持 IE、Firefox、Chrome、Safari 等多种浏览器			
	支持 Windows 及 Mac 操作终端			
	支持 IPv4 及 IPv6 应用环境			
部门管理	支持部门分级管理			
	支持部门分权管理，不同部门管理员仅能管理审计各自部门的用户及资产			
用户管理	支持通过内置的用户角色实现系统分权管理			
	支持自定义用户角色，并可依据角色灵活配置相应系统模块的管理访问权限			
	支持本地静态密码认证			
	支持与 AD、LDAP、RADIUS、短信平台等第三方认证平台对接			
	支持动态令牌、手机令牌、USBKEY 等双因素认证			

	支持用户组管理
	支持通过 EXCEL 表格批量导入、导出用户信息
	支持通过 LDAP 用户批量同步
	支持通过 WEB 页面批量修改用户属性
资产管理	支持主机资产管理，包括 Windows、Linux/Unix 等
	支持大型机资产管理，包括 IBM AS 400 等
	支持网络设备资产管理，包括 Cisco、Huawei、Juniper、H3C 等
	支持管理各种 C/S 和 B/S 应用
	支持数据库资产管理，包括 Oracle、MS SQL Server、MySQL、DB2 等
	支持中间件资产管理，包括 WebLOgic 等
	支持自定义资产类型
	支持按资产不同属性对资产进行多级分类，并以树状结构进行图形化展示
	支持资产组管理
	支持通过 EXCEL 批量导入、导出资产信息
	支持通过 WEB 页面批量修改、删除资产信息
密码管理	支持资产账号密码托管，实现资产单点登录功能
	支持系统账号密码触发式校验功能，对托管的口令进行验证
	支持基于资产、系统账号、改密时间等因素创建改密计划
	支持自定义密码规则，包括密码策略、是否分段保管、密码备份方式等
权限管理	支持配置基于用户（组）、资产（组）、系统账号、协议的静态访问权限
	支持按用户、资产和系统账号属性设定动态访问规则
	支持通过变更单导入方式动态管理用户访问权限
	支持工单授权审批管理，工单具有时效性，过期后自动回收
	支持自定义高危命令列表，并可灵活设置不同命令的响应策略（允许、拒绝、告警、复核等）及优先级
	支持会话审批模式，审批复核人可实时控制用户的操作权限，包括操作权限的下放、回收等
	支持以用户、资产维度统计相应访问权限
资产访问	支持 WEB、MSTSC、SSH Client 等多种访问方式
	支持会话批量启动功能
	支持会话共享功能
审计管理	支持 RDP、X11、VNC 等图形协议的行为审计
	针对图形会话支持键盘、剪切板、窗口标题等事件审计

	支持通过图形会话缩略图定位用户操作
	支持 TELNET、SSH 等字符协议的行为审计
	针对字符会话支持命令输入、输出分级展示
	支持指令级操作回放
	支持文件传输审计及附件留痕功能
	支持 ORACLE、MYSQL、MSSQL 等数据库的行为审计，包括图像及 SQL 语句审计
	支持在线会话实时管控
	支持多关键字、多条件的审计检索，支持多条审计结果合并查看
脚本任务	支持脚本任务功能，可将用户自定义的脚本文件批量下发至目标资产执行
统计报表	支持统计用户、资产、账号和会话的基本及变更信息
	支持以日、周、月、季度、年等周期自动生成相应报表数据
部署管理	支持 HA 部署管理
	支持集群部署管理

典型组网

H3C SecPath A2000-AK 系列 运维审计系统以物理旁路模式接入到用户网络中，采用操作网关方式实现对运维操作的集中管理，只需确保运维审计系统与被管理服务器、网络设备、应用等资产 IP 路由可达、远程协议互通即可。



H3C SecPath A2000-AK 系列运维审计系统应用组网图

订购信息

H3C SecPath A2000-AK 系列 运维审计系统是新华三技术有限公司自主研发的产品，用户可以根据实际需求按照型号进行选购。

1.1 选购一览表

（1）主机选购一览表

主机	描述	备注
NS-SecPath A2000-AK605+LIS	H3C SecPath A2000-AK605 运维审计系统	必配
NS-SecPath A2000-AK610+LIS	H3C SecPath A2000-AK610 运维审计系统	
NS-SecPath A2000-AK620+LIS	H3C SecPath A2000-AK620 运维审计系统	
NS-SecPath A2000-AK630+LIS	H3C SecPath A2000-AK630 运维审计系统	

（2）资产数扩展授权函选购一览表

资产数扩展类型	描述	备注
LIS-A2000-EXT-100	100 资产数量扩容授权函	选配
LIS-A2000-EXT-500	500 资产数量扩容授权函	
LIS-A2000-EXT-UL	无限资产数量扩容授权函	

（3）配件选购一览表

配件	描述	备注
NSQM1IPCGT4GP4A2	4 端口千兆以太网电接口+4 端口千兆以太网光接口模块	选配
NSQM1IPCGT8A2	8 端口千兆以太网电接口模块	
NSQM1IPCGP8A2	8 端口千兆以太网光接口模块	
NSQM1IPCTGS4A2	4 端口万兆以太网光接口模块	
R2A-AK-BV0350	H3C 350W 交流电源模块	
应用发布中心 RDS 授权函	应用发布中心 RDS 授权函	
双因素认证 动态口令卡	双因素认证 动态口令卡	
双因素认证 USBKey	双因素认证 USBKey	

新华三技术有限公司
北京总部
北京市朝阳区广顺南大街 8 号院 利星行中心 1 号楼
邮编：100102

杭州总部
杭州市滨江区长河路 466 号
邮编：310052
电话：0571-86760000
传真：0571-86760001

http://www.h3c.com

客户服务热线
400-810-0504