H3C SecPath D2000-V100 虚拟数据库审计系统

产品概述

随着信息化的发展，数据库成为客户核心数据的存储载体，数据库可以类比为所有业务系统的心脏，心脏的安全与稳定直接关系着前台业务的安全与稳定，数据库的安全直接关系着企业的命脉，其遭受的各种攻击，直接会导致用户敏感数据泄露，间接可能导致用户的破产，因此信息安全建设的中心由网络防护向数据防护转移，对于承载数据的容器——数据库，已然成为安全威胁的重点。

同时，越来越多的用户将传统的业务系统迁移至云环境中，而目前众多云平台关注的更多是基础实施的完善和业务的开展，对于安全层面的关注较少。云平台存在系统多、环境复杂的问题，安全问题尤其在云平台中更加突出，数据的泄露及篡改风险变的越发严峻，针对数据安全的防护以及事后审计追溯也变得越来越困难。对此，新华三技术有限公司提供了基于虚拟化的云数据库审计解决方案，H3C SecPath D2000-V100 虚拟数据库审计系统，是一款专业的虚拟数据库安全审计产品，适用于等级保护、企业内控、SOX、PCI、企业内控等信息安全规范，全面保障数据库的完整性、保密性和可用性。

H3C SecPath D2000-V100 虚拟数据库审计系统，广泛适用于“政府、公安、财政、教育、能源、工商、社保、医疗、国土、金融、运营商、企业”等所有涉及数据库应用的各个行业。

产品特点

云化环境，灵活部署

H3C SecPath 虚拟数据库审计系统适用虚拟云化环境，支持 SDN 引流审计、流量探针等多种灵活的部署方式，适用于公有云、私有云、混合云等多种类型云平台的数据库访问流量的审计，实现多种云架构下自建数据库、云数据库的全面审计，对数据库“零”影响。

授权池化，动态管理

H3C SecPath 虚拟数据库审计系统的授权采用授权资源池化的方式，提供虚拟化数据库审计模板和实例数的授权管理，可动态分配与回收模板授权、实例授权。

丰富的协议与版本支持

- 支持主流的关系型数据库议审计，准确分析出这些数据库协议，并支持对多种不同类型和不同版本的数据库的同时审计；
- 支持 VLAN、VXLAN 环境下数据库的审计，且支持指定源 IP 审计功能；
- 支持 WEB 中间件审计，不仅能审计中间件服务器对数据库的访问行为，还能对中间件前端的 WEB 访问行为进行审计，并能建立前后关联关系，回溯整个业务流程。

全面支持 IPV6 环境

H3C SecPath 虚拟数据库审计系统全面支持 IPV6 协议，不仅支持在 IPV6 环境下部署和管理，且支持在纯 IPV4

环境、纯 IPV6 环境及 IPV4 与 IPV6 混杂环境下对数据库进行审计。

细粒度审计

- 支持对数据库 SQL 操作语句的细粒度审计，可完整解析协议的所有字段；
- 支持正常请求信息的解析，同时支持对返回值行列结果全解析和全记录；
- 支持多元素符合逻辑的事件定义，包括操作时间域、操作方式、数据库用户名、数据库名、表名、应用程序名、执行时长、操作成功/失败、操作内容等；
- 支持超长 SQL 语句、注释内容、多嵌套语句、绑定变量、RPC 的审计；

数据库语句翻译

支持将复杂嵌套的数据库语句，转译为普通用户可直接阅读的中文。让更多不了解数据库的用户，能无障碍的使用该系统。系统支持标准的 SQL 语句和 NOSQL 语句。

基于业务行为的操作审计

与用户实际业务结合，关注关键操作流程和敏感数据表，是否存在资金归集、漏费、非法查询等等，一旦发现异常，立即将审计结果以用户业务视角加以展示告警。避免大量的数据库语言，让用户无从入手。

业务性能分析

系统以旁路方式接入用户网络，24 小时不间断的对核心数据进行采集分析，可为用户提供以下分析结果：

- 每日&每周的业务繁忙高峰，并提供具体峰值；
- 提供对业务性能消耗最大的操作内容，并提供日触发次数；
- 以力导向布局图和明细数据的方式实时监测当前连接会话，以便问题发生时定位故障点和责任人。

特权账号与风险操作监控

通过对系统特权限账号的监管和高危操作的监控（如赋权、数据库链、物化视图等），避免敏感数据的流失。

- 高性能海量数据挖掘及数据建模分析
- 完整记录对数据库的所有操作，以达到全审计的目的。以便用户在未知的风险事件发生后，定位问题的发生过程。系统可实现在以亿为单位的数据中，多条件查询数据，在数秒内返回结果，同时对海量数据实现压缩比 90%以上的高性能存储。
- 多维度海量审计数据对比分析工具，从不同的空间、时间对各个维度进行同比和环比分析。

产品规格

表1-1 H3C SecPath D2000-V100 虚拟数据库审计系统产品规格

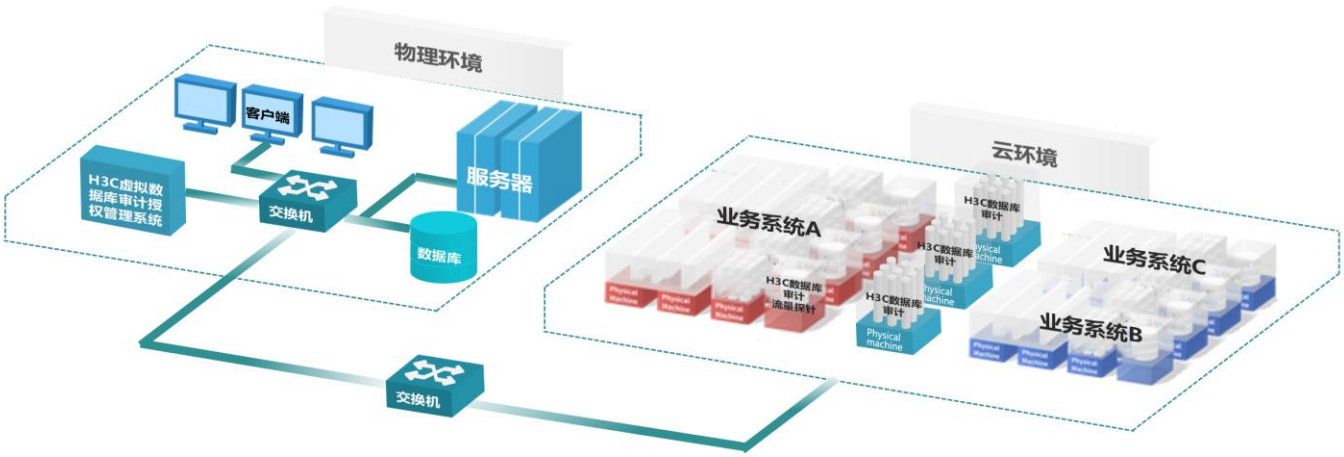
属性	说明
部署模式	旁路部署

属性	说明	
协议支持	数据库协议：Oracle，Microsoft SQL Server，DB2，Sybase, Informix、MySQL、人大金仓（Kingbase）、达梦(DM)、Cache、Teradata、MongoDB； WEB 协议：http 协议 虚拟化协议：VLAN、VXLAN 协议 其他协议：telnet、ftp、rdp、vnc、ssh	
网际协议	IPV4 协议； IPV6 协议； IPV4 与 IPV6 协议混杂；	
审计内容	数据库协议	审计日志包含数据库用户名、SQL 语句、表、字段、存储过程、应用程序名、IP、MAC、端口、数据库名、计算机名、起止时间、超长语句、注释内容、多嵌套语句、绑定变量、RPC 等；
	Web 协议	支持对http协议的审计 ； 支持对 http 协议返回内容的记录 ；
因子监测	对数据库中突发增加的因子提供独立展示页面。因子包括：IP 地址、应用程序名、计算机名、存储过程、数据库用户名、数据名、数据库主机；	
模型分析	支持可基于分类统计（源IP、目标IP、数据库用户名、数据名、应用程序名、协议类型、计算机名）、日期统计（按小时、日、周、月、年统计）、性能统计等维度对行为模型做钻取分析； 支持对查询结果的深度钻取，且不限制钻取次数；	
审计规则	支持全部审计策略及满足条件审计策略 ； 支持自定义业务审计及告警规则 ； 支持多元素符合逻辑的事件定义，包括操作时间域、操作方式、数据库用户名、数据库名、表名、应用程序名、执行时长、操作成功/失败、操作内容等； 支持规则导入、导出 ；	
告警通知	支持 syslog 告警通知方式； 支持 snmp 告警通知方式； 支持邮件告警通知方式； 支持短信告警通知方式； 支持 windows 消息告警通知方式；	
告警响应	支持屏幕录像； 支持网关联动；	
分析报表	内置多于多种不同类型的报表； 内置多种自动生成不同分析类型的报告； 支持自定义报表，可以根据客户需求自定义报表； 支持按照源源 IP、目标 IP、协议类型、客户端名、应用程序名、数据库名、数据库用户名、操作方式、操作对象、预警规则名、预警级别、执行时长等信息生成报表；	

属性	说明	
设备管理	监控管理	操作界面支持全中文； 通过 Console 口进行本地配置； 设备管理采用管理员与审计员三权分离； 支持将多个数据库 IP 绑定为一个业务系统； 支持系统自检功能且提供独立界面； 支持与物理设备面板一一对应的网卡模拟展示，可根据实际连线情况实时展示网卡当前状态； 支持设备自身运行状态查看：系统 cpu、内存、硬盘 I/O 等信息查看； 支持极简升级；
	系统管理	支持Web方式进行远程配置管理； 支持在IPV6环境下部署和管理； 支持一键清空数据和恢复出厂设置；

典型组网

H3C SecPath D2000-V100 虚拟数据库审计系统以旁路监听的方式接入云网络，可通过 SDN 引流或流量探针等方式，将访问数据库的流量引至虚拟数据库审计系统，使数据库审计系统能够监听到用户与数据库进行通讯的所有操作。同时，虚拟数据库审计授权管理系统部署在一台物理机上，为多台虚拟数据库审计系统提供授权服务。



H3C SecPath D2000-V100 虚拟数据库审计系统部署图

订购信息

H3C SecPath D2000-V100 虚拟数据库审计系统是新华三技术有限公司自主开发的产品，用户可以根据实际需求按照型号进行选购。

表1-2 选购一览表

对外型号	对外中文描述	备注
LIS-D2000-V100-SS-PERM	H3C SecPath D2000-V100 数据库审计系统软件功能永久授权函,含 1 个数据库实例	永久功能授权
LIS-D2000-V100-SS-1Y	H3C SecPath D2000-V100 数据库审计系统软件功能 1 年授权函,含 1 个数据库实例	1 年功能授权
LIS-D2000-V100-EXT-1	H3C SecPath D2000-V100 1 个数据库实例扩容授权函	审计实例扩展授权

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