HighGuard SDA

海加数据库安全审计分析系统

技术白皮书

上海海加网络科技有限公司

2015 年 12 月

目　录

1. 技术背景

随着企事业单位信息系统建设的不断深入，越来越多的资料被存放到数据库中。数据库系统的应用，不仅实现了无纸化办公，承载了单位中最有价值的无形资产，也成为攻击者最感兴趣的目标。

目前，绝大部分信息系统都采取了一定的安全防护措施来保护数据库的安全性，但仅仅只有安全防护是不够的。当攻击发生后，我们至少应该知道系统是怎样遭到攻击的，此外还要知道系统存在什么漏洞，如何能保证系统在受到攻击时有所察觉，如何获取攻击者留下的证据等。数据库安全审计技术就是在这样的需求下被提出的。

海加数据库安全审计分析系统（简称 SDA）能够对接收到的流量数据统一过滤，提取数据库操作相关的数据进行分析，达到实时监控数据库活动的目的。

SDA 主要由采集器及分析器两部分组成。采集器部署支持旁路模式、网关模式和代理模式。旁路模式利用网络侦听技术，只需要接入交换机的镜像端口即可工作，部署快速方便，且完全处于业务通道外，对现有系统影响最小。网关模式将采集器部署在各子网与数据库服务器中间，以串行方式接入，对各子网与数据库服务器透明，所有访问数据库服务的通讯将通过采集器。代理模式将采集器分布部署到各子网、数据库服务器上，以代理的形式将采集到的流量信息汇总到分析器。

分析器通过特征检测及审计规则匹配，对任何尝试的攻击或违反审计规则的操作，进行实时阻断或告警。

系统支持数据库有：

国产数据库：武汉达梦、人大金仓、南大通用、神州通用等；

国外数据库：Oracle、SQL Server、DB2、Informix 等；

开源数据库:MySQL、PostgreSQL、MongoDB、Hadoop(HBase)等。

系统对记入审计数据库中的数据 ,以多种维度、多种图表方式进行明细查询、统计分析。

2. 产品架构

系统架构在逻辑上可分为网元层、监控层、处理层和管理层。

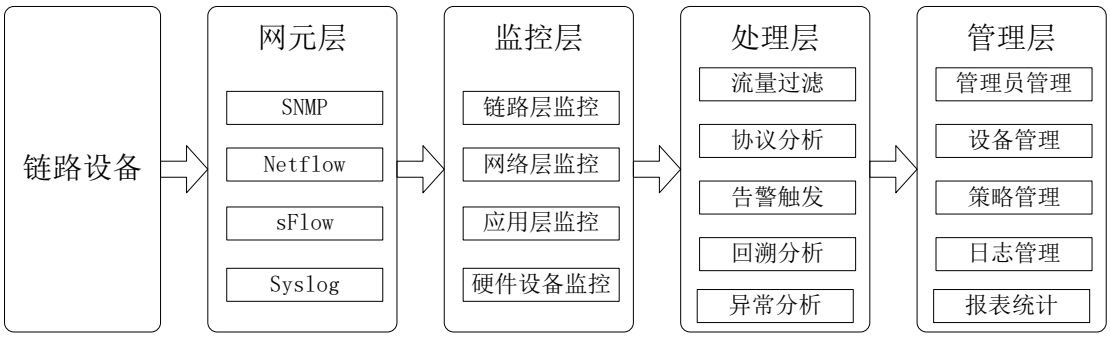

图 1 系统架构

网元层主要用来采集链路设备上的数据 ,支持采集 SNMP、Netflow、sFlow 和 syslog，将采集到的数据经过格式化处理后进行存储；

监控层主要对链路进行监控，可监控链路层和网络层的流量、应用层协议和链路上的硬件设备；

处理层主要对网元层采集到的数据进行过滤、分析，可以实现流量的初步过滤、数据库协议分析解析、满足安全审计规则后的相应触发动作、回溯分析和异常分析；

管理层主要为管理员提供系统管理功能和分析统计功能，支持管理员管理、设备管理、策略管理、日志管理和各种报表输出。

系统在硬件上由采集器和分析器组成。采集器工作在网元层和监控层，分析

器工作在处理层和管理层。

3. 部署方式

网络监听部署

通过对中心交换机配置，将交换机流量镜像到数据库审计设备上（需要中心交换机支持端口流量镜像功能）。

网络拓扑

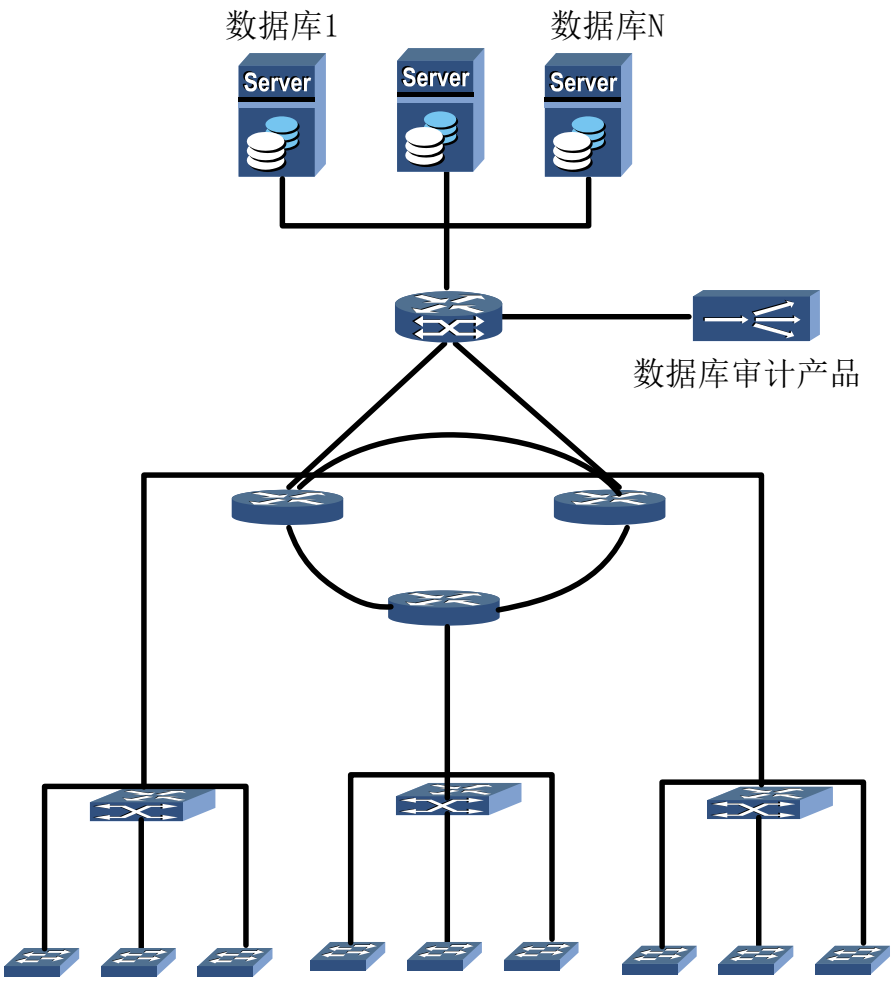

图 2 网络拓扑

可实现的功能

1) 具有全面丰富的数据库审计类型

支持对 Oracle、SQL Server、MySQL 等主流数据库。

2) 具有细粒度的数据库操作内容审计，能准确及时的对违规操作告警

基于内容关键字、IP 地址、用户、用户组、时间、数据库类型、数据库操作类型、数据库、字段名等多种组合策略，从而全面监测发现各种非法操作及合法用户的违规操作。

3) 数据库操作信息还原

实时审计用户对数据库系统所有操作（如：插入、删除、更新、用户自定义操作等），并完全还原 SQL 操作命令，实现安全事件准确全程跟踪定位，为事后追查取证提供有力支持。

4) 可以全面详细的审计信息，丰富可定制的报表分析系统

5) 自身的安全性高，不易遭受攻击

4. 技术优势

4.1 功能描述

系统功能模块可以分为网元层、监控层、处理层和管理层四个部分。

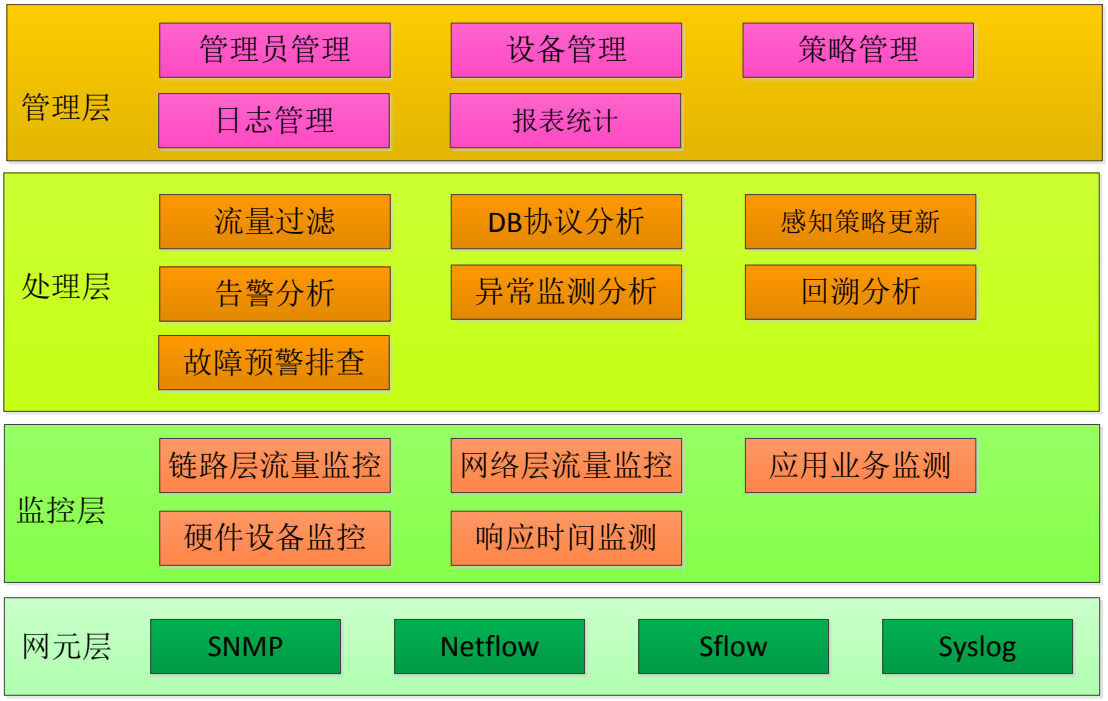

图 4 功能模块组成

4.2 功能模块

4.2.1 系统管理

系统配置

配置系统的参数，如操作员最大闲置时长、报表 TopN 取值、报表自动刷新间隔时长、网络日志保存时长、磁盘使用阈值等。采集器和分析器的端口配置。以及查询采集器和分析器的状态，如启动状态、内存的使用率、网络的使用率等。

用户管理

支持用户的新增、修改、删除功能。用户可自行调整定义不同角色的权限，也可增加角色。不同的用户拥有不用的权限。最高级别的系统管理员可以为其他人员配置密码和权限。设置的权限包含系统的配置、统计和分析、告警、报表等。

不同的管理员或者用户登陆系统后，看到的可能是完全不同的菜单内容，可以对系统的操作权限也是不相同的，这样可以做到权责分明，也可以增加系统运行的安全性和信息的保密性，使得系统管理更加规范化。

设备维护

对设备的配置进行备份、升级，或还原出厂配置。进行关机、重启等操作。

4.2.2 对象定义

数据库主机定义

系统可以自定义数据库主机，将数据库主机的业务名称、地址、端口定义为对象。可以根据这些对象去查询该服务器的安全事件，或对其配置策略，方便管理人员。

数据库客户端定义

对需要审计的访问数据库服务器的机器，进行定义。可以是安装有数据库客户端的 PC 机（开发、运维人员的电脑），或者是安装有 Tomcat 等的 WEB 服务器。

时间段定义

对需要审计的时间段进行定义，如工作日的 8:30-17:00，某个具体时间段，如 2015 年国庆节。

报警方式定义

对安全事件产生时，可以定义该事件使用哪一类的报警方式，此方式中如果采用邮件方式，则需要配置邮件模板；此方式中如果需要声音报警，持续的时间是多少秒。

4.2.3 策略定义

规则管理

对审计的规则进行定义：要审计哪些表，哪些字段。

对规则归类成规则集。

策略管理

对指定的数据库主机（或任意）、指定的数据库客户端（或任意），及指定的规则集，定义需要进行记录，或阻断操作。

4.2.4 日志审计

管理员操作日志查询

日志管理记录了系统的主要操作和事件。方便管理员进行系统的维护和故障的查询。日志管理员可以根据时间段、关键字等方式灵活的查询信息。

日志管理主要包括所有用户的操作、访问记录等各类信息。

5. 分析中心

TOP N 查询

显示最经常访问的数据库、表，审计事件中出现最多的 IP、用户等。

数据库审计日志综合查询

便于管理员多维度得对审计日志明细进行查询、导出，做出自主分析。

6. 报表中心

统计报表是一种事后的分析工具。统计报表按照其内容分为：

◆ 审计报表

◆ 告警报表

◆ 自定义报表

系统可提供日报、周报、月报、季报、年报等中、长期的审计报告。系统内置多个标准报表，同时支持用户自定义报表。

在生成报表之前，允许用户从界面上选择一些报表条件，如时间范围、统计周期、报表类型、报表模板等。在分析页面中可以选择特定监控对象和时间范围，然后把查询结果输出成 PDF、HTML、EXCEL、WORD 等格式的文档，也可以作为一种灵活定制的报表。

7. 产品型号说明

7.1 技术参数

产品型号	DBA-1000
系统管理	1.支持通过 HTTP 和 HTTPS 两种方式远程管理系统； 2.系统全中文操作界面，便于管理； 3.支持用户访问权限管理，可为不同级别管理员指定不同的权限； 4.支持对各类对象统一配置；
应用业务监测	1.支持将应用业务定义为分析对象，对其进行统计分析；

		2.支持对应用业务的响应时间进行监测。
回溯分析		1.支持对历史数据进行回溯分析，精细查找问题原因； 2.支持对历史数据进行各种自定义查询。
异常告警		1.能够及时发现违规操作并发出告警； 2.支持多种告警方式，包括页面、邮件、声音等，提供定制化接口； 3.支持通过 SNMP、Syslog 将告警信息发送到网管平台。
硬件设备实时监控		1.支持统一集中管理硬件设备； 2.自动生成当前网络拓扑图，对网络拓扑进行管理； 3.支持对各硬件设备告警日志统一集中管理； 4.支持对各硬件设备性能统一集中管理。
报表统计		1.系统内置多种标准报表，分为审计报表、告警报表、日志报表等； 2.支持用户自定义报表。
部署方式		支持旁路部署
硬件规格	**分析器**	1.规格：2U 机架式 8 个热插拔硬盘位 2.处理器：2*INTEL Xeon E5-2640 v2 8C 20M 2.6GHz 3.内存：4*16GB DDR3 RECC 1600 4.存储：8*3TB SATA 7200r 5.网卡：4*INTEL 千兆网口 6.电源：2U/500W 冗余电源
	采集器	1.规格：2U 机架式 8 个热插拔硬盘位

		2.处理器：2*INTEL Xeon E5-2620 v3 6C15M 2.4GHz 3.内存：2*16GB DDR3 RECC 1600 4.存储：2*300G SAS15000r 5.网卡：4*INTEL 千兆网口，1*万兆卡含 2 个 SPF+多模模块 6.电源：2U/500W 冗余电源
工作温度		工作环境：10℃～35℃ 运输/储存环境：-40℃～70℃
工作湿度		工作环境：8%-90%相对湿度 运输/储存环境：5%-95%相对湿度

7.2 安全性说明

安全性包括操作系统本身的安全性和应用系统的健壮性。海加数据库审计系统的采集器和分析器的操作系统均采用最新版的 Linux，且对内核进行了裁剪，去除了不相关的功能，最大程度地对操作系统进行优化，提高了系统的性能。除 443、80、22（用于远程管理）端口外，关闭操作系统其它端口。采用的 Web 容器、数据库、第三方开发库等均采用当前的最新版本。

8. 海加网络服务体系

海加网络凭借着先进的技术，秉承客户至上的服务理念，为客户提供最为完善的技术支持服务。

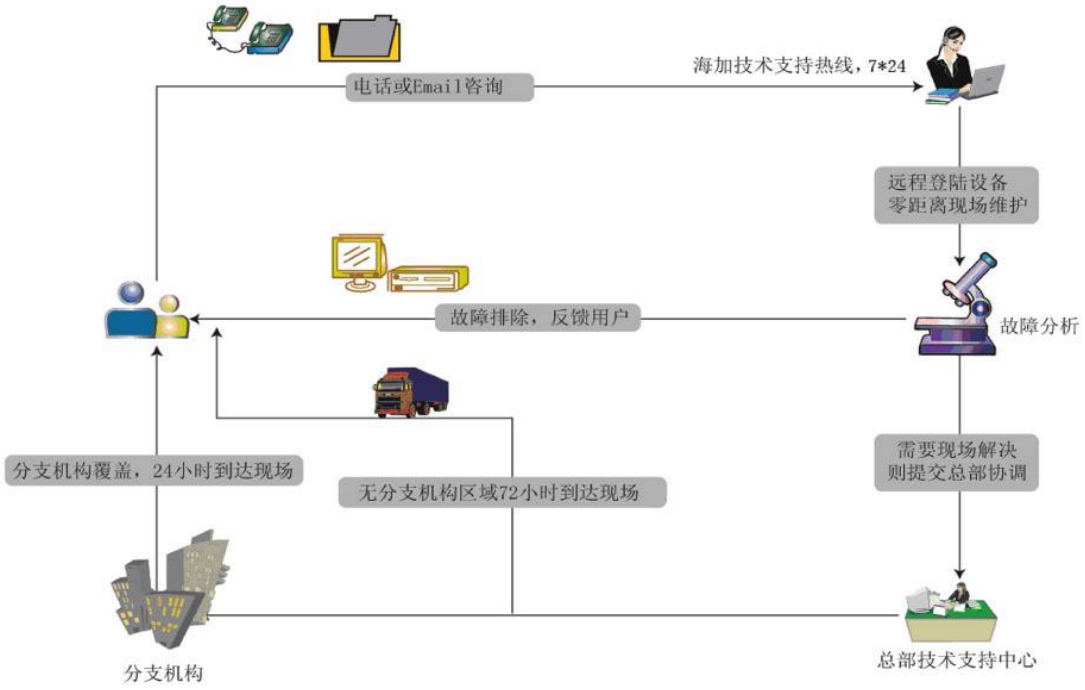

图 5 售后服务体系

- 远程支持服务

Email和电话技术支持服务

公司设有7 x 24小时的电话和Email支持服务，接收客户咨询、服务调度和投诉。

虚拟现场产品维护服务

公司技术人员通过在公司和客户间利用互联网建立SSL数据加密通道，远程登录公司设备，为用户提供零距离的虚拟现场产品维护。

- 现场服务

有办事机构覆盖区域将在24小时内到达现场为用户排除故障，无办事机构或需总部支持则公司总部技术人员可以在72小时内到达现场解决问题。

- 备机服务

基于用户业务运行的重要性及响应时间考虑，通过公司备件更换程序，可以先将好的备用设备供用户使用，直至故障设备修复。