东北师范大学信息化管理与规划办公室
日志审计系统测试报告

测试时间：2017 年 4-5 月

测试部门：系统运行部

一、前言

按照信息安全等级保护的要求，同时，为了加强整个学校信息系统的安全建设，及时发现系统异常事件，并通过事后分析和直观的报表呈现，方便高效地对信息系统进行有针对性的安全审计，我们调研了日志审计系统，并选择了三家产品进行测试，具体情况如下：

二、测试产品选择

通过对日志审计系统市场进行调研，我们选择了三家产品进行测试：□□□日志审计系统、□□□日志审计平台、□□□日志管理工具。

三、收集日志对象

	Windows 主机	Linux 主机	Web 应用防火墙	天融信防火墙
IP 地址	*.*.*.*	*.*.*.*	*.*.*.*	*.*.*.*

表 1.收集日志对象

四、功能指标对比

1.采集日志方式

信息化管理与规划办公室

日志接入主要分两种方式，一种是通过标准协议(例如 Syslog)，设备直接发送日志到日志审计系统，日志审计系统被动接收解析；另一种是安装采集代理（Agent）,通过 Agent 采集后发送日志到审计系统，下面是三家产品的对比：

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
Windows 主机	Agent	Agent	Agent
Linux 主机	Syslog	Syslog	Agent
Web 应用 防火墙	Syslog	Syslog	Syslog
天融信 防火墙	Syslog	Syslog	Syslog

表 2. 采集日志方式对比

通过对比发现，这三家产品的采集日志方式没有明显的差异。

2.日志规范化

日志审计系统根据不同厂商的日志格式，对日志进行解析展示，如果接入的日志不是日志审计系统支持的日志格式，则无法正常显示出日志的相关信息，就需要进行规范化处理，例如，图 1 和图 2 是□□□日志审计系统在对 WAF 日志进行范化之前和范化之后的图片，可以看到范化之前无法显示出设备类型、源地址、目标地址等

信息化管理与规划办公室

信息。

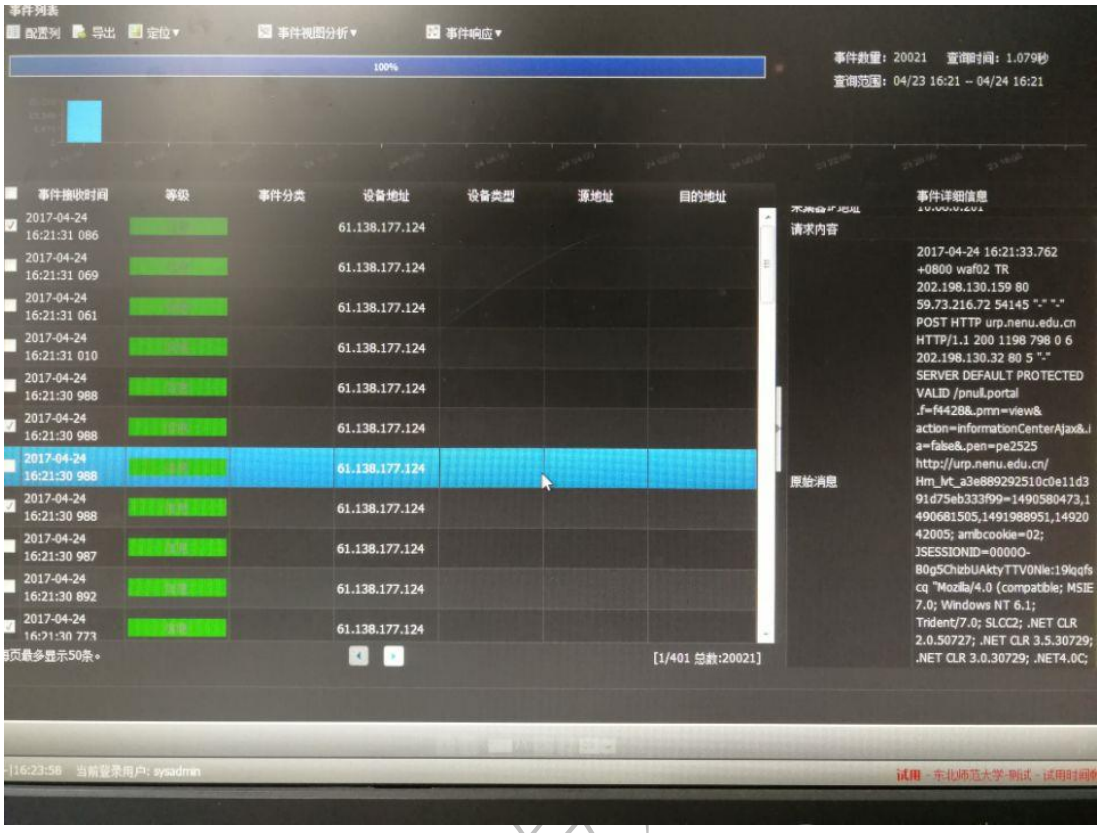

图 1. 范化前

图 2. 范化之后

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
Windows 主机	不需要范化	不需要范化	不需要范化
Linux 主机	需要范化	不需要范化	不需要范化
Web 应用 防火墙	需要范化	不需要范化	不需要范化
天融信 防火墙	需要范化	不需要范化	不需要范化

表 3.日志范化对比

通过对比发现，□□□日志审计平台和□□□日志管理工具不需要人工进行日志规范化操作，就可以直接读取并自动对其进行规范化，确保了日志的可读性。而□□□日志审计系统需要其工程师持续的介入，不利于日后工作的独立开展。

3.支持的日志编码

日志审计系统所支持的日志编码不同，一般 windows 系统日志都是 GBK 编码，linux 系统日志是 UTF-8 编码，对数据库执行更改的操作日志是二进制编码。

信息化管理与规划办公室

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
支持的 日志编码	ASCII、 GB2312、GBK、 ISO-8859-1、 Unicode、UTF-8	UTF-8、GBK 、 ISO-8859-1	UTF-8、GBK、 UTF-16、二进制

表 4.支持的日志编码对比

通过对比发现，除了三家产品共同支持的日志编码格式外，只有□□□日志管理工具支持二进制编码。

4.支持的日志协议

不同的日志审计系统所支持的日志协议不同，其中，HTTP 一般是针对公有云或者外网环境，日志发送端通过开放接口，日志审计系统定时或实时通过 HTTP 请求去获取日志；FTP：日志审计系统作为 FTP 服务器，日志发送端通过 ftp 定期把日志传输到日志审计系统上；Flume 是 Cloudera 提供的一个高可用的，高可靠的，分布式的海量日志采集、聚合和传输的系统，Flume 支持在日志系统中定制各类数据发送方，用于收集数据，同时，Flume 提供对数据进行简单处理，并写到各种数据接受方（可定制）的能力。

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
支持的 日志协议	Agent 抓取 /SYSLOG	Agent 抓取 /SYSLOG、	SYSLOG、AGENT 抓取、数据库

信息化管理与规划办公室

		SNMPTRAP、 HTTP、FTP	ODBC、HTTP 上 传、FLUME、API

表 5.支持的日志协议对比

通过对比发现，□□□日志管理工具支持的日志协议最多。

5.数据存储

由于大量的日志内容相似，所以需要对日志进行压缩和归档，节省日志存储空间，同时为了保证日志的安全，需要进行异地备份，并能恢复显示。

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
异地备份	支持	支持	支持
恢复	支持	支持	支持
压缩/归档	支持	支持	支持

表 6.数据存储对比

通过对比发现，三家产品的数据存储方式没有明显差异。

6.解析规则库

日志审计系统需要根据不同厂商产品的日志格式（解析规则库）对日志进行解析，使得日志更加通俗易懂。

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
解析规则库	233 条	5 万条	没有统计

表 7.解析规则库对比

信息化管理与规划办公室

通过对比发现，□□□日志审计平台的解析规则条数最多，表明其可识别目前市场上多数产品的日志格式并自动规范。

7. 日志可读性

日志审计系统能正确读取原始的日志信息，对日志字段进行提取，并准确的显示出来供管理员阅读。

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
日志可读性	不好	较好	一般

表 8. 日志可读性对比

例如，图 3 和图 4 分别是□□□日志审计平台和□□□日志审计系统显示的 WAF 日志，可以看到□□□日志审计系统显示的 WAF 日志有用信息较少，不利于管理员日后对问题进行定位分析；□□□日志审计平台显示的 WAF 日志信息更有价值，例如图 3 中的“事件描述”很准确，方便管理员对事件进行审计追溯。

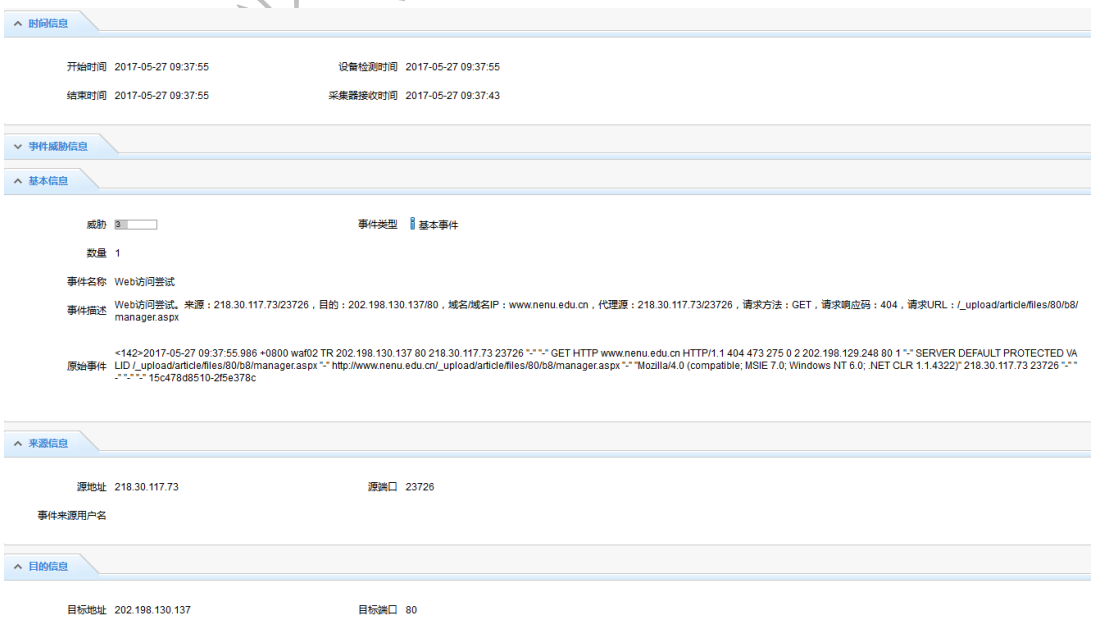

图 3. □□□日志审计平台显示的 WAF 日志

事件接收时间	2017-05-03 14:14:03 176
用户名称	
源地址	61.49.176.94
源端口	31946
操作	
目的地址	202.198.129.248
目的端口	80
对象	
结果	
持续时间	
响应	
发送流量	
接收流量	
归并数目	1
事件名称	访问日志
事件摘要	632
事件分类	/访问控制
采集类型	syslog
等级	轻微
原始等级	6
原始类型	
产生时间	2017-05-03 14:14:08 000
监控数值	
网络协议	hopopt
网络应用协议	www-http

图 4. □□□日志审计系统显示的 WAF 日志

8.日志搜索方式

日志的搜索也是日志审计系统的关键性能之一，其中有的日志审计系统支持二次搜索，即在检索结果基础上，可以通过某个字段纬度关联的多纬度事件进行检索，对日志的分析更深入，如下图。

图 5. 二次搜索

SPL（Search Processing Language)语句，类似 SQL 语法，不同的是，SPL 搜索的不是关系数据库，而是输入到日志审计系统中所有的日志数据。

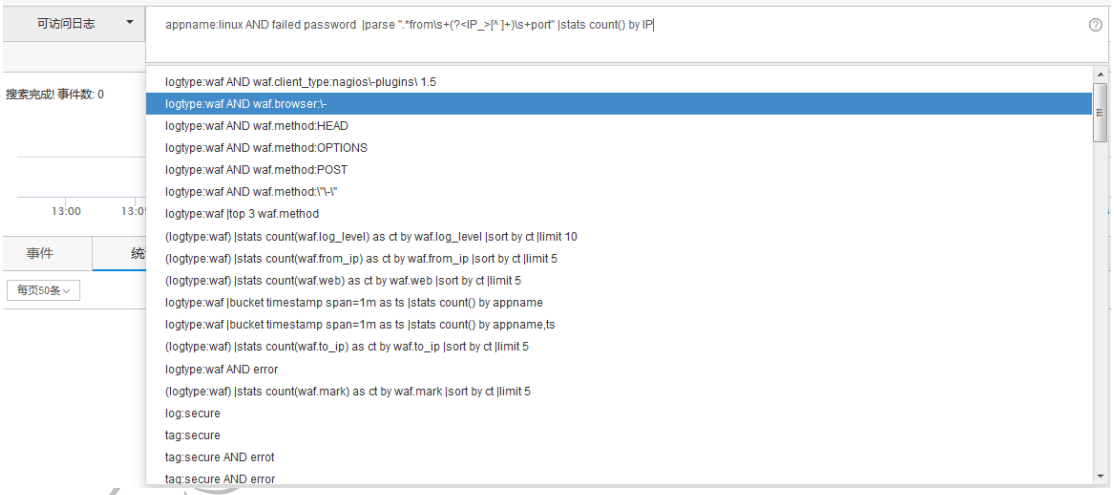

图 6. SPL 语句

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
基本搜索	选择已有字段/ 自定义	选择已有字段/ 自定义	SPL 语句

二次搜索	不支持	选择已有/ 自定义	SPL 语句

表 9. 日志搜索对比

通过对比发现，□□□日志审计系统和□□□日志审计平台都支持可视化的基本搜索，操作比较简单，□□□日志管理工具需要管理员编写 SPL 语句，来进行搜索，操作难度稍大，□□□日志审计平台支持的二次搜索方便日志的快速定位分析。

9. 性能监控

对服务器进行性能监控，并通过设置阈值，进行报警，如下图所示：

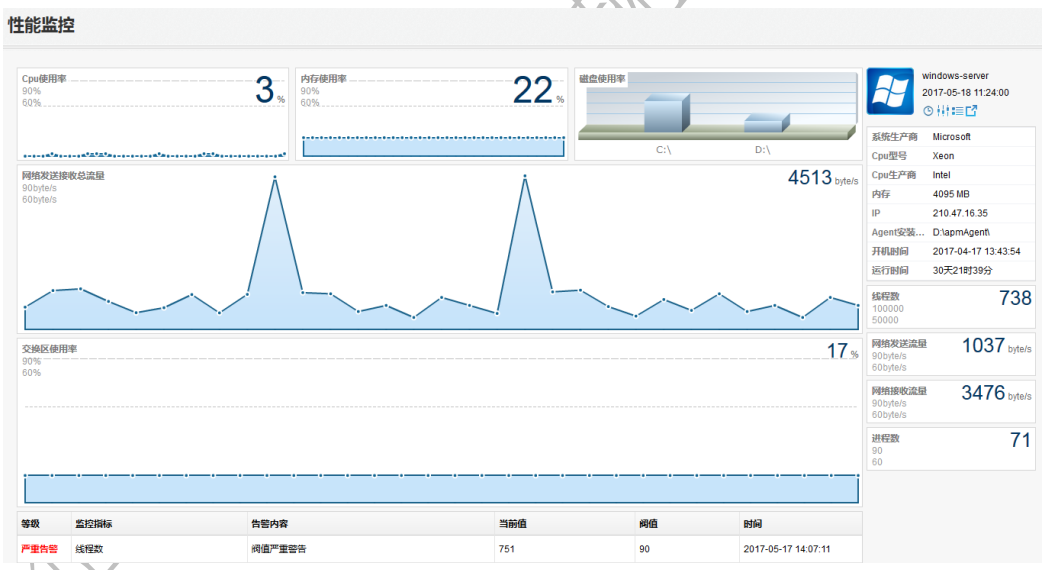

图 7. 性能监控

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
Windows 主机	不支持	支持	如果日志上有 性能相关内

			容，可以进行监控
Linux 主机	不支持	支持	如果日志上有性能相关内容，可以进行监控

表 10.性能监控对比

通过对比发现，只有□□□日志审计平台支持对服务器进行性能监控。

10.统计报表

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
统计报表	支持	支持	支持

表 11.统计报表对比

通过对比发现，三家产品统计报表没有明显差异。

11.告警方式

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
告警方式	邮件/短信	邮件/短信/微信	邮件/短信

表 12.告警方式对比

通过对比发现，除了三家产品共同支持的告警方式外，只有□□

信息化管理局规划办公室

□日志审计平台支持微信告警。

12.弱点管理

支持将漏洞扫描报告导入日志审计系统，如果有报告中漏洞相关的安全日志，则进行关联分析。

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
弱点管理	不支持	支持	不支持

表 13.弱点管理对比

通过对比发现，只有□□□日志审计平台支持弱点管理，可以将我校现有的绿盟漏洞扫描系统的报告导入其中进行分析。

13.数据库审计

即对数据库本身的日志以及事务操作日志进行记录。本次只是测试了对数据库本身的日志进行收集。

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
数据库审计	可以收集数据库本身的日志	可以收集数据库本身的日志	可以收集数据库本身的日志/事务日志以及操作日志

表 14.数据库审计对比

通过对比发现，除了三家产品共同支持的对数据库本身日志进行收集外，只有□□□日志管理工具支持对数据库的失误日志以及操

信息化管理与规划办公室

作日志进行收集。

五、事前发现异常自动提醒测试

测试场景：用绿盟漏洞扫描系统对*.*.*.*进行口令猜测，三个设备的表现如下：

	□□□ 日志审计系统	□□□ 日志审计平台	□□□ 日志管理工具
异常自动提醒	刚开始没有报警，修改规则后进行告警	显示“可能的扫描爆破尝试”	统计失败登录本机的 IP 地址和次数在上升

表 15. 发现异常自动提醒对比

图 8. □□□日志审计系统安全提醒

图 9. □□□日志审计平台安全提醒

通过对比发现，□□□日志审计系统没有对口令猜测做出报警提示，在工程师新建规则之后才可以显示告警，而□□□日志审计平台直接就显示告警。即，虽然□□□日志审计系统和□□□日志审

计平台都有一些攻击场景的报警规则，但是□□□日志审计平台的报警场景更合理，利于管理员快速发现攻击问题。

六、商业日志审计系统与免费 SYSLOG 系统的对比

	商业日志审计系统	免费 rsyslog 系统
日志呈现方式	根据不同厂商的日志格式，进行通俗解读	记录原始日志
关联规则	带有已经固化的关联规则，可以进行安全探查，报警	无
搜索方式	易用性强	易用性弱
收集日志方式	代理或者 syslog	syslog

表 16.商业日志审计 vs 免费 SYSLOG

通过以上对比，可以看出商业日志审计系统的主要优势为：1.不仅仅通过 syslog 协议，而是可以收集目前常用的服务器或者安全设备的日志；2.可以针对不同厂商的设备，进行不同的日志呈现，使得日志的可读性更强；3.可以对日志进行关联分析，对用户关注的场景进行报警；4.通过统计报表和图形来直观的展现日志统计。

对日志的收集、解析，以及通过对日志的关联分析

七、总结

通过对三家日志审计系统进行对比测试，结论为：□□□日志审计系统和□□□日志审计平台功能偏重于对日志进行解析和安全关联分析，得出有价值的报警信息。□□□日志管理工具功能偏重于

信息化管理与规划办公室

对日志进行人工分析，即，相当于购买日志分析服务，例如，对校园卡之类系统的业务情况进行分析，得出交易量变化等，但是这些特性不是本次调研的需求；□□□日志审计系统对日志的解析不好，需要进行人工范化处理才可以正确的显示日志，虽然经过人工干预，□□□日志审计系统的可读性依然不好，不利于管理员日常查看和问题定位、追溯；□□□日志审计系统和□□□日志审计平台有现成的攻击场景报警规则，可以对攻击场景进行警报，可是针对测试场景，□□□日志审计系统报警规则需要人工建立和调整，可见其报警规则并不合理。为了使□□□日志审计系统正常显示日志并对日志进行关联分析，需要大量人工参与；□□□日志管理工具没有已经制定好的配置在系统里面的关联规则，所有的安全审计告警规则都需要人工配置，日后使用难度较大；□□□日志审计平台具有更多可用的功能：性能监控和弱点管理，而且□□□日志审计平台的使用顺畅，不需要太多的人工干预即可有理想的表现。

信息化管理与规划办公室