日志管理解决方案的测试和评估

日志管理是所有企业都应该部署的技术，但却只有很少的企业部署了良好的日志管理。收集和分析计算机和设备日志在很多方面都发挥着重要作用，包括信息安全、操作管理、应用程序监控、系统故障排除和合规审计等，良好的日志管理解决方案能帮助加强企业安全。安全审计应该是很多企业调查日志管理工具的首要原因。Verizon 公司的“2008 年数据泄漏调查报告”(该报告正迅速成为计算机犯罪统计数据的最可靠资源)显示“82%的数据泄漏事故在实际事故发生前就能找到蛛丝马迹，不管具体使用的是何种类型的事件监控，结果都相同：关于数据泄漏攻击的信息并没有被通知或者采取行动”。

本文对七种不同的日志管理硬件和软件解决方案进行了分析，包括 ArcSight Logger 4.0、GFI EventsManager v.8.2、 LogLogic MX3020 v.4.9.1、 LogRhythm LR2000-XM v.5.0、 NitroSecurity NitroView ESM and ELM v.8.4、Splunk 4.1.2 和 Trustwave SIEM。此次产品评估和分析的目的在于让大家了解日志管理的特性和功能，包括什么功能可以区分不同解决方案。我们根据相同评估标准来为每个产品评分(1 到 10 分，10 分为最高分)，这些产品都是互不相同的，属于不同产品类别。

举例来说，ArcSight 的单设备 Logger 属于严格意义上的日志管理解决方案，因而缺少 NitroSecurity 的双设备 SIEM(安全信息和事件管理)解决方案的很多功能。本文的产品评估仅仅侧重于日志管理功能，并且产品评分表也只反映其日志管理功能。当然，从给定价格的角度来看，解决方案提供更多的功能绝对是好事。

本文评估的产品特性和功能与收集、存储和审查企业可能需要密切关注的各种类型事件日志有关。虽然你不需要了解日志管理完整的详尽的原理信息，但你需要记住日志管理生命

周期的几个阶段：政策定义、配置、收集、规范化、索引、存储、相关性、基线、警报和报告。

此次测试是在一个小型实验室进行的，包括 15 到 20 台计算机(包括物理和虚拟的)，模拟 Windows、Linux、BSD、路由器和无线客户端的小型企业网络。有些功能是当产品在大型真正的生产网络或者供应商传教的远程实验室运行时来测试的。

测试评分表					
	40%	20%	20%	20%	
ArcSight Logger 4.0	10	8	8	9	9.0 优秀
	40%	20%	20%	20%	
GFI EventsManager 8.2	7	8	8	8	7.6 良好
	40%	20%	20%	20%	
LogLogic MX3020 (版本 4.9.1)	8	9	8	8	8.2 很好
	40%	20%	20%	20%	
LogRhythm LR2000-XM (版本 5.0)	9	9	9	9	9.0 优秀
	40%	20%	20%	20%	
NitroSecurity NitroView ESM 5750 and ELM 2250	10	8	9	9	9.2 优秀
	40%	20%	20%	20%	
Splunk 4.1.2	8	8	8	9	8.2 很好

	40%	20%	20%	20%	
Trustwave SIEM	8	9	8	8	8.2 很好

在本文的测试中，并没有测试供应商性能或者压缩报告，这两者通常都被夸大。有些供应商感到很遗憾，因为他们所声称的最大竞争优势是迅速处理大量数据。我们建议在购买任何日志管理产品前，测试真实性能，我们看到过很多日志管理产品在处理几百台机器时游刃有余，而处理几千台机器时则慢如蜗牛。

所有这些测试的产品都很不错，能够有效部署在任何企业网络中。测试的产品中，没有一个产品不能提供值，当然有些产品能提供更多值。每个测试的产品都有无数有用的功能，并且完全可以胜任生产环境的日志管理工作。此次评估的最主要目的是为了突出每个产品独特的功能，这样大家可以决定选择哪款日志管理产品来帮助实现生产环境的有效日志管理。

日志管理评估指南

本节将讨论的是每个日志管理产品提供的各种功能，并提供评估其他任何日志管理解决方案的标准。

首先需要作出的决定就是是否选择使用“包罗万象”的设备或者软件产品。大多数日志管理产品都是以设备的形式，纯粹是因为设备通常在处理性能和存储要求方面能够比在通用操作系统运行的软件产品更简便。当然，管理员也能够配置和优化软件产品的主机操作系统让软件产品像设备产品一样有效，毕竟，设备也只是运行日志管理软件的操作系统主机而已。只不过设备产品已经完成了硬配置和优化工作。

设备的缺点就是，它们往往局限于现成的配置和磁盘能力，而基本操作系统(通常是 Linux 或者 Windows 系统)的补丁修复也是个问题。虽然本文测试的设备供应商都声称会将基本操作系统的漏洞修复和更新作为其正常产品升级(通常为自动化)的一部分，我们发现很

多产品仍然在运行旧版本的代码，例如 Apache 网络服务器，存在很多已知漏洞。如果你决定使用设备产品，询问供应商他们是否会及时更新基本操作系统的漏洞修复程序。如果根据使用条款允许的话，可以考虑在购买前测试产品的漏洞问题。

工作量分配

测试的产品中，大多数产品都提供一体化功能，也就是说他们的产品可以作为管理控制台、数据采集器、存储设备、索引(搜索查询结果和过滤器)、报告生成器。此外，大多数产品都可以配置为提供一个或者多个功能服务，而不需要执行所有功能。

如果你要从几百个客户端收集日志信息的话，工作量分配无疑是非常重要的。这并不是日志管理产品本身的瓶颈问题，对于设备产品来说，它通常会有四个或者四个以上千兆以太网接口，但是网络只能够维持这么多的额外流量才不会造成应用程序和操作性能问题。从 1000 台计算机发送日志信息到一个日志管理器会导致网络瘫痪。

与供应商合作来解决日志管理工作量分配问题，以最大限度提高系统环境的性能。本文中的每个产品都可以作为本身的存储和转发收集器，这意味着你有一个日志管理层可以在转发数据(通常是压缩)到中央日志管理层之前收集所有本地流量。很多产品都可以转发事件到其他产品，特别是那些支持 syslog 和 SNMP 的产品。而有几个产品(包括软件和设备产品)可以只作为收集器或者索引器，这两个也是占用 CPU 最多的操作。

向供应商提供你的网络数据(网络带宽、有效功率和需要监测的客户端数量)以及企业日志管理计划。然后让供应商提供他们推荐的工作量分配配置。对于设备产品来说，这往往意味着不同位置的不同硬件模型。

性能是非常重要的，不仅对于避免网络拥堵问题，也关系到实时或者历史数据分析、打印报告和进行更深入的分析。当你需要处理几千万到几十亿的事件信息时，你肯定不想为了

简单的查询回复而等待 10 分钟。如果你的解决方案涉及多个日志管理节点，请确保查询和报告可以在各个节点间允许哦那个，这意味着在管理控制台的一次点击能够执行所有产品的搜索和报告。这些测试的产品在工作量分配方面都相当灵活，而唯一例外就是 GFI EventsManager。

大部分供应商都会声称他们的产品适用于任何类型的环境，并且很多供应商还表示他们安装的解决方案每天都在处理数百亿的信息，而没有任何客户投诉。在花大笔钱购买日志管理产品前，务必要进行完全测试，并获取供应商关于性能方面的书面保证。

管理控制台仪表板

每个日志管理产品都有管理控制台仪表板，显示关于日志管理系统本身和所监测事件的关键实时和短时期总统计数据。大多数仪表板都会报告事件消息数、本地 CPU 性能以及关于任何重要事件的通知。

几乎所有供应商都允许仪表板自定义，让用户自己配置仪表板显示信息。在大多数情况下，仪表板显示是上下文相关的。你可以点击显示的图形来获取更详细的信息。少数产品(例如 NitroSecurity)允许大量修改，几乎所有数据、图形或者警报都可以显示。

用户角色是很重要的，大多数产品都允许管理员(拥有完全权限)来设置更多有限角色。例如，有些产品允许有限的管理员被定义，以防万一当需要管理员级别权限而仅涉及预定义客户端：所有 windows 计算机、所有思科路由器等。大多数产品都有一个只读角色，不能对任何配置设置作修改，但该角色用户可以运行报告和查看预定义图表和数据。大多数产品都只允许 2 至 4 个角色被定义，值允许管理员来定义显示什么屏幕。其他产品(包括 Splunk、NitroSecurity 和 LogLogix)允许更多的角色定义，屏幕上的每个属性和域都可以根据每个角色来定义。

日志收集

从各种被监测客户端收集日志信息是所有日志管理产品的主要功能，大多数产品既有无代理模式又有客户端代理模式来收集日志。没有代理意味着管理员不需要为每个客户端分配、安装和配置额外软件。但是，无代理日志收集仍然需要规划。大多数产品使用 syslog 转发、WMI 查询或者其他远程方法来收集日志(后两者通常需要客户端管理员密码)。如果涉及防火墙的话，这些方法都需要必要的规则修改。不管怎样，都不要认为无代理没有运行或者会发挥巨大作用。

客户端代理具有无代理收集方法不具备的优势。大多数代理都有多个配置选择，允许管理员对哪些事件被收集以及如何收集有更细粒度的控制。例如，不是发送每条日志信息到中央服务器，代理可以仅发送关键事件，并且如果需要的话，还可以本地存储事件信息以备以后的检索。客户端代理通常能够提供传输压缩，允许更多的时间在更多的时间使用更少的网络带宽来发送。

被监测的客户端可以一次添加一个(通常通过 IP 地址或者域名)，使用大量输入(一次添加多个设备)或者使用某种发起查询进程(通常通过 Active Directory 浏览或者 IP 地址扫描)。带部分产品允许“设备组”被创建，来收集一个或多个既定组名的受监测客户端，根据某种属性来分组，例如设备类型、IP 地址或者名称。设备组然后可以作为单一实体被监测，这样当试图监测某特定类型设备时更容易实现警报和报告。

客户端代理也可以用来存储事件，例如当集中日志管理工具离线时。最先进代理的最佳功能之一就是衡量网络和/或本地 CPU 使用率，并节流信息发送率直到网络不在拥堵。最后，很多代理都有“心跳”功能，让客户端没有在一定时间内传输信息就会发出警报，虽然这可

以被“零基准”警报模拟。毫不奇怪，长期的 SIEM 领跑者 ArcSight 比其它竞争对手拥有更多的客户端代理。

如上所述，日志管理产品拥有的解析数据越多，就能够更快更有效地从大量数据中筛选特定数据类型。一个产品最大的不同就是，该产品定义了多少解析器。例如 ArcSight 就捆绑了超过 100 个定义的数据收集器。在更低端领域，有些产品只有几十个解析器或者声称他们的通用解析器效率相同。但在一般情况下，解析器越能够模拟你的环境就越好(但这不是唯一的判断点)。有些日志管理产品允许管理员创建他们自己的解析器，这在很多环境都非常有用。

相关补充说明：大多数产品都声称拥有 windows 事件日志收集代理。然而，很多这些代理都是在微软最新 windows 版本推出前创建的，并不能对这些最新操作系统版本进行细致的分析。很多解析器和代理了解三种传统默认日志：应用程序、安全和系统，但是不能允许管理员从 Windows Vista、Windows7 和 Windows Server 2008 提供的 100-plus 内置审查中进行选择。

Splunk 是一款理解新 windows 日志格式的工具，不过，我们还没能找到一款工具能够与更新的 windows 内置事件转发技术结合(即使该产品承载在 windows 操作系统上并能够使用这项更新的技术)。Windows 自带的事件转发可以替代所有其他代理和无代理方法。如同大多数产品的通病，日志管理并没有更上最新客户端变化的步伐。

日志存储

存储数百万到数十亿信息需要占用大量磁盘空间。大多数设备在 RAID 配置中都有兆兆级磁盘存储。虽然软件和硬件产品都声称能够进行某种存储压缩，但是根据很多客户对传输

压缩的投诉，供应商所谓的存储压缩让我们将信将疑。他们的存储压缩统计数据通常都是基于最小的事件日志信息以及最高的压缩数值，这并不能反映真实世界的结果。

不过，大家需要找供应商弄清楚产品是软件还是合并？产品支持的最大磁盘空间(或者文件大小)以及配置？支持何种 RAID 阵列？不同 RAID 配置有不同的性能特点，也就是说，有些写入很快，有些读取更快，灵活度是一个考量因素。供应商是否支持对收集日志数据的数字签名以满足验证需求？

大多数产品都有最大日志尺寸，这与底层主机操作系统的限制有关。如果产品是设备产品，数据能被存储到外部驱动阵列吗？多少数据可以有效被检索和简便地恢复？每个产品都允许数据导出或者存档。导出数据通常是离线状态，必须一起输入以确保可搜索性。有几个解决方案能够灵活处理这个问题，例如 LogRhythm 允许管理员定义过滤器来导入需要的数据，而不是所有数据。

有些产品还有所谓的“存储组”，这是专门为某特定任务单独定义的逻辑分区，例如 PCI 合规，或者特定设备分组，如思科无线路由器。除了为报告目的组织某种类型数据外，存储组还可以用来确保特定应用程序有足够磁盘空间来满足特定政策要求，例如，保存数据两年。ArcSignt 在这方面很有实力，包括有效的尺寸参数和 CPU 优先。

最后，你还需要确定事件日志数据是否是以供应商的专有格式(原始的未过滤和非结构化格式)被存储或者检索？大多数产品都是以专有格式存储有效数据，但是却是以原始格式检索和导出数据。这意味着重新导入的数据将需要被再次解析和检索才能使用，但是如果原始数据(假设这些数据进行了数字签名)需要用于法律目的，这也更容易带来产销监管链问题。

实时审查

大多数产品都允许多传入数据的实时查看并显示一些主要趋势。如果你有一个中等规模的系统，每秒中都有数百条到数千条信息传入，快速实时查看所有数据就失去了吸引力。所有产品都允许实时数据被过滤以仅仅显示与特定任务相关的事件。通常这些过滤器可以保存为搜索历史数据和生成相关报告。

最好的实时查看器允许用户点击特定数据字段来查看事件。举例来说，也许你正在查看关于某特定工作站的输入数据，然后你看到一个可疑的 TCP 端口。在某些产品中，点击该端口值会将现有实时查看信息转变为显示所有使用该相同端口的所有工作站。其他产品只能对历史数据进行这种转变显示或者要求你将信息查看变为“调查员”模式。所有这些测试的产品都提供非常灵活的查看功能，其中 LogLogix 和 LogRhythm 在这方面是最强的。

搜索存储的数据

根据感兴趣类型和事件来搜索存储数据同样是日志管理重要的功能，这也使很多供应商试图将自身产品与其他竞争对手产品区别开来的领域。供应商往往会吹嘘他们的过滤搜索如何能够快速从非常大量数据(尽快这些说法在本文中没有进行验证)进行搜索工作。大多数供应商都是基于关键字、英语短语和布尔逻辑来进行搜索。有些供应商要求用户输入所有搜索表达式类型，而其他供应商则提供图形让用户选择使用，“建立查询”界面。根据点击建立查询在教育新管理员方面很有帮助，虽然有经验的管理员大多数都喜欢输入查询的快速和灵活性。

如果你的企业需要搜索大量原始、非结构化事件日志，询问供应商是否支持非规范化数据间的搜索过滤？如果他们能够提供这种搜索，具体是怎样进行搜索的？对非结构化数据的搜索与结构化数据的搜索有什么不同？很多供应商只允许对原始数据的关键字搜索，而其他供应商还允许布尔逻辑。

可以在同类产品间执行搜索吗？在所测试的产品中，只有 ArcSight、LogLogic、LogRhythm 和 Splunk 可以在不同节点间执行搜索。所有这些产品都允许搜索过滤被保存。不过更好的产品则会让搜索过滤转变为报告，并保存报告供日后使用，有些产品允许搜索过滤发送和共享，这在拥有很多日差查看器的非常大的系统环境尤其有帮助。

另外，拥有很多内置、预定义搜索过滤器也很不错。有些产品没有或者只有一小部分样品，而最好的产品应该有几十个预定义的有趣的查询，并且通常是与一个或者多个合规要求联系的。最常见的就是登陆失败，一些产品(包括 LogLogic)包括“近似文本”查询，显示你感兴趣的特定消息前面和后面的 10 个左右的事件。

警报

警报是日志管理非常重要的功能，对于 SIEM 也是至关重要的功能。供应商应该能够支持几种不同类型的警报方式。所有被测试的产品都有电子邮件警报，并且大部分都允许 SNMP 转发。出人意料的是，只有少数产品有短袖报警或者允许模拟调制解调器电话拨号(对于缺乏互联网接口拨号)。有些产品(包括 NitroSecurity)界面有帮助她软件(通常是 Remidy)或者有他们自己的“服务台”功能来帮助解决警报问题。大多数产品允许无限制的保健，但是有些产品，尤其是 ArcSight Logger，仅允许有限次数的有效警报，确切来说，Logger 允许五次有效警报。ArcSight 的 SIEM 产品没有这样的限制。

警报可以分为以下几种类型。从最基本的情况来看，当检测到特定日志事件时，警报允许发送通知，所有产品都允许根据特定时间内一定数量事件的警报。笔者最喜欢的警报类型是基本警报，也就是产品本身确定环境的“正常”事件类型，而管理员来确定偏差百分比来发送警报。NitroSecurity 支持每种信息类型的基本报警，而 LogLogic 基本报警限制于来自特定设备或者设备组的所有信息。

不管你选择的是哪种日志管理产品，请确保它有控制警报信息的功能。没有什么比半夜收到来自单个事件的一百条警报更糟糕的事情了。

报告

所有产品都有内置式报告，并允许报告进行自定义化或者创建。最好的产品拥有数以百计的内置报告(无论是免费的还是额外收费的)涉及特定安全或者合规需求：NERC、PCI、SOX、FISMA 等。报告通常能够以不同格式存储：CSV、HTML、XLS、TXT 和 PDF 等。拥有越多的内置报告越有帮助。

一定要测试结构化数据与非结构化数据有关的报告差异。大多数供应商不能够处理非结构化数据报告，或者不能够适用于结构化数据的总结和技术。有些供应商将非结构化数据纳入到报告中，仅通过涵盖完整的原始信息细节或份很小的数据汇总。

除了与特定合规要求相关的中高层管理报告外，寻求支持技术故障排除的详细报告。具有最佳报告功能的产品，包括 ArcSight、LogRhythm 和 NitroSecurity，这些产品符合以上要求。有些产品实在工作流进程运行，合规报告可以发送命令链，并由相关责任方签字。我们的建议就是找出哪些报告属于内置的，哪些报告是需要收取额外费用的，并审查这些报告是否能够符合你的合规要求。

结论

这七个被评估的产品包含数百个功能，并且具有极强的可配置型，每个产品都是值得考虑的日志管理产品。大家可以仔细阅读上述产品分析，以及产品的差异，以寻找最适合企业环境的产品。然后对所选择的产品进行详细的测试以衡量它是否合适以及性能问题。

如果你还没有使用全面的企业级日志管理解决方案，你有很多优秀的产品可以选择。最佳解决方案就是：仅发送你要求的警报类型，过滤掉不必要的信息，提供有用的仪表信息显示，有效的报告帮助你确定是否满足你的特定需求。日志管理部署得越好，就越能够满足企业的信息技术需求，包括安全、合规、操作管理和所有 IT 相关的其他领域。

日志管理解决方案评估

	平台和价格	**优点**	**缺点**
ArcSight Logger 4.0	拥有可选软件解决方案的设备 价格：20,000 美元起	连接器提供灵活性和大量选择 快速查询 丰富的报告选择	局限于五个有效警报，大量客户端代理
GFI EventsManager 8.2	适用于 Windows 系统使用的软件 价格：每台服务器 220 美元起 每个工作站 22 美元起	简单易用的图形用户界面 中小企业值得选择 大量预定义规则和报告	不能在全部事件范围内执行整体的关键字搜索 缺乏企业级功能，例如事件压缩、网络带宽限制、命令行界面和存储组 性能不能与企业级产品相提并论

LogLogic MX3020	设备和虚拟设备 价格：20000 美元起	整洁简单界面 确定进入设备流的功能 自适应基线警报	很多方面缺乏上下文相关图形 功能不像竞争对象一样丰富 有限的警报通知方式
LogRhythm LR2000-XM	拥有可选软件解决方案的设备 价格：35000 元起	很多数据查看和简单图表 能够查看和过滤实时数据 强大的 Active Directory 整合	初始安装需要改善 不能够捕捉 SNMP 陷阱
NitroSecurity NitroView ESM and ELM	设备 价格：39995 美元起	非常灵活的控制台查看和图形 很多功能和选择 自适应基线警报	自动发现比较薄弱 没有短信警报 图形用户解决有点复杂
Splunk 4.1.2	适用于 Windows、Linux、Unix、BSD、Mac 系统和其他系统的软件 价格：企业版本为 5000 元起 免费版本最高 500MB 每日事件	强大的非结构数据报告 Windows 日志选择 分配功能的能力 用户角色	一些自定义配置选择要求 XML 编码 默认 windows 应用程序中报告和搜索的有限数量 一些功能配置在管理控制台外，如客户端证书映射功能
Trustwave SIEM	拥有可选软件解决方案的设备 价格：27000 元起	结合了日志管理和 SIEM 动态流量地图 强大的技术支持	启动时间很长 嵌入式帮助系统薄弱 一些小的技术问题