BMST Session-Auditor FAQ

目 录

Q：什么是 Session Auditor

A：Session Auditor简称SA是北京比蒙科技公司的一款网络会话监控与回放产品,其主要功能是监控远程桌面、SSH、TELNET、RLOGIN以及数据库等各类远程维护操作，并且按照真实再现的方式进行回放。

Q：SA 与其他审计产品相比有什么优势

A：SA能对WINDOWS远程桌面（RDP）、VNC、SSH等协议进行记录与回放，这是在业界领先的技术水平。

Q：SA 产品需要在服务器上安装 AGENT 吗

A：SA是网络审计的工具，不需要在主机上安装各种AGENT

Q：SA 是怎么工作的

A：SA为三层架构，控制台(Console)-数据中心(Data Center)-传感器（Sensor)。一个控制台可以连接多个数据中心，一个数据中心可以连接多个传感器，一个传感器可以监控多个服务器。传感器采集数据发送到数据中心，数据中心提供数据的查询分析审计等各项功能，控制台进行搜索回放报表等多项展现。

Q：怎样部署 SA 产品

A：传感器串连在需要监控的网络中，传感器、数据中心、CONSOLE的管理端口需要在一个VLAN中。

Q：SA 产品能够以监听方式工作吗

A：不行，SA产品只提供串联的接入方式

Q：我已经有了 IDS，SNIFFER 等网络监听产品，还需要 SA 产品吗

A：是的，需要。IDS、SNIFFER仅仅只能对非加密协议进行监听，而SA除了非加密协议，还可以对加密协议进行记录、回放及控制。并且SA不仅仅是记录的入侵行为，而是对非法行为与合法行为忠实的全记录，内控与审计更多的是审计的合法行为。

Q：SA 支持 BYPASS 功能吗

A：是的，SA硬件支持BYPASS功能，当出现故障甚至关掉电源时，相当于网线直接的物理连通。

Q：SA 的性能如何

A：SA产品有多种型号，从较低端的400兆产品，到千兆产品都有覆盖。

Q：怎样保证审计记录全面性不丢包的

A：SA产品通过以下两个方面来保证记录全面性的

a. 并行的监听方式会因为各种原因，造成仅丢失一个数据包而导致整个会话数据不可用，SA产品是串行的PROXY方式，所有信息不可旁路也不会丢失。

b. SA产品的传感器只进行数据包的收集与转发，而在将复杂的协议分析和审计交给并行的数据中心进行协议的分析与处理，从而保证了网络性能。

Q：网络审计与主机审计相比有什么好处

A：网络审计的记录内容存在于网络上，不容易被篡改；网络审计不需要在主机上安装AGENT，减少不必要的对服务器的影响；网络审计部署简单，扩展性强，不会因为服务器的增减而改动

Q：通常能存储多长时间的数据

A：SA低端产品的数据中心有1TB的容量，对于100台机器的网段，通常的维护操作可以至少存储3个月以上，SA产品还支持转储，可以将数据导出至其他介质存储。

Q：是如何保证高性能的

A：SA产品采用的是三层架构，最底层传感器是单独的硬件，只进行数据包的收集与转发，因此对网络几乎不造成影响，传感器是桥方式工作在三层以下；中间层是数据中心进行大量的协议分析处理的，因为是旁挂的，因此不会对网络造成影响；顶层是控制台，实现图形回放等各类复杂工作。

Q：是否支持数据库

A：SA产品目前支持的数据库有ORACLE、SYBASE、MSSQL三种

Q：是否支持自定义报表

A：SA产品支持灵活的报表定制，并且有接口可以进行二次开发。

Q：管理端是 BS 方式还是 CS 方式

A：管理端是使用的CS方式（专用的管理客户端），不支持浏览器。

Q：为什么使用 CS 方式而不使用 BS 方式

A: BS方式通常是为了方便使用者从任何地方进行连接，而SA产品属于专用的安全产品，其记录与审计的内容都是机密的，因此使用专用的客户端方式。

Q：记录数据是怎么保证完整性的

A：SA产品数据中心使用的是RAID阵列进行数据记录。

Q：是否支持在线升级

A：是的，支持

Q：桥方式的传感器是否支持 VLAN-TRUNK

A：是的，支持

Q：是否支持关键字搜索

A：是的，支持关键字搜索，并且支持中文关键字的正则表达式搜索。

Q：管理员角色是否进行了分权

A：是的，管理员进行了备份、查看、管理等多种分权。

Q：LICENSE 授权方式是怎样的

A：LICENSE是按照SA产品型号进行授权的。

Q：是否可以定制策略,只记录感兴趣的会话

A：是的，可以自定义网络对象，对网络对象进行灵活的策略定制。

Q：除了监视,是否具有控制功能

A：是的，SA产品内置了防火墙的访问控制功能，能对会话按照安全策略进行方便的管理控制。

Q：SA 能透明支持 RDP 协议所有功能吗？

A：支持所有版本的RDP协议(Windows 2000/XP/2003/R2)，支持完全的RDP功能（包括音频、文件系统，剪切板、本地硬盘重定向等），支持全透明接入（不需要更改服务端或客户端的任何配置）。

Q：SA 透明支持 SSH 协议所有功能吗？

A：支持所有版本的SSH协议(SSH1/SSH2)，支持完全的SSH功能(包括sftp, scp, port forwarding, x11 forwarding)，支持压缩方式的SSH数据传输，支持全透明接入（不需要更改服务端或客户端的任何配置）。

关于比蒙科技

北京比蒙科技有限公司（以下简称“比蒙科技”）总部设在北京中关村科技园区，成立于2006年3月，是目前中国优秀的专注于网络安全产品和技术创新的高科技公司之一。创业团队成员拥有多年的电信运营商运营维护经验，以及多年的网络安全产品设计和研发经验，他们在国际国内领先的网络安全专业技术公司有令人自豪的职业经历。他们对安全运营和技术需求有着充分的理解和认识，对于安全产品的创新和开发拥有敏锐的观察和触觉。比蒙科技通过对市场的感知和对技术的深入研究，可以为各行业、各层次的客户群提供实时的、有效的网络安全解决方案和专业化的信息安全服务。