



BMST Session-Auditor FAQ

Content

Q: What is Session-Auditor?.....	2
Q: What is the advantage of Session-Auditor compared with other products?.....	2
Q: Do I have to install agents on the hosts?	2
Q: How does Session-Auditor work?.....	2
Q: How to deploy Session-Auditor?	2
Q: Does SA work in SPAN model?.....	2
Q: I have had IDS's, Sniffers in place, do I still need Session-Auditor?.....	2
Q: Does Session-Auditor have BYPASS feature?.....	2
Q: How about the performance of Session-Auditor?	2
Q: How to guarantee the completeness of audit records without any loss of packet?	2
Q: What's the advantage of network based audit against host based audit?	3
Q: Generally speaking, how long time of network traffic can SA's storage support?.....	3
Q: How to guarantee the high performance of SA?	3
Q: Does SA support any database?	3
Q: Does SA support user defined report?.....	3
Q: How does the management client work, B/S or C/S?	3
Q: Why choose C/S, not B/S?	3
Q: How to guarantee the integrity of recorded data?	3
Q: Does SA support online upgrade?	3
Q: Does SA's sensor support VLAN-TRUNK?	3
Q: Does SA support key word search?.....	4
Q: Does SA support privilege separation of administrator?.....	4
Q: How about the LICENSE model?	4
Q: Does SA support policy customization in order to record specific sessions only?	4
Q: Besides monitoring, does SA have any access control capabilities?.....	4
Q: Does SA support all functions of RDP protocol transparently?	4
Q: Does SA support all functions of SSH transparently?.....	4
About BMST	4

Confidentiality Notice

This document contains Proprietary Trade Secrets of BMST Co. LTD and its receipt or possession does not convey any right to reproduce, disclose its contents or to manufacture, use or sell anything that it may describe. Reproduction, disclosure or use without specific authorization from BMST is forbidden. BMST reserves the right to make changes, add, remove or change the schedule of any element of this document.

Q: What is Session-Auditor?

A: Session-Auditor (SA) is one security audit product by BMST to provide monitoring, recording, control, replay and search of network sessions. The protocols it support cover Windows Remote Desktop (RDP), SSH, TELNET, RLOGIN, Oracle, MS SQL, and other remote maintenance operations.

Q: What is the advantage of Session-Auditor compared with other products?

A: SA support transparent audit of those encrypted protocols, such as RDP and SSH, both recording and replay. That's the unique value of SA.

Q: Do I have to install agents on the hosts?

A: SA is a network based audit product, without necessity of installation of various agents on hosts. This helps lower the implementation and operation cost.

Q: How does Session-Auditor work?

A: SA has 3-tier architecture: SAC (console), SAD (datacenter) and SAS (sensor). One SAC can connect and control multiple SADs, while one SAD can connect multiple SAS's. One SAS can monitor and record sessions from multiple servers. Recorded data is transferred from SAS to SAD, where they can be searched and analyzed according to the commands from SAC. SAC is the command center for the whole audit system.

Q: How to deploy Session-Auditor?

A: SAS is in-line connected between servers and terminals, while management ports of SAS, SAD and SAC should be configured into one single VLAN.

Q: Does SA work in SPAN model?

A: No, SA supports in-line bridge mode only.

Q: I have had IDS's, Sniffers in place, do I still need Session-Auditor?

A: Yes, you do. IDS's and Sniffers only work for those non-encrypted protocols, while SA supports recording, replay and control of encrypted and non-encrypted protocols. At the same time, compared against IDS, SA records not only intrusion activities, but complete recording of legal and illegal activities. That's the right direction of internal control and audit systems.

Q: Does Session-Auditor have BYPASS feature?

A: Yes. SA supports BYPASS at the hardware level, i.e. whenever SAS encounters failure or other sort of outage, the two network interfaces will be connected directly to guarantee the continuity of business.

Q: How about the performance of Session-Auditor?

A: SA has multiple models, supporting network bandwidth from 400M to Giga Ethernet.

Q: How to guarantee the completeness of audit records without any loss of packet?

A: Completeness of recording data is guaranteed from the following two aspects in SA:

- a. SAS works in line as a transparent proxy and it's impossible for any packet to bypass SAS or to be dropped. For those sniffer-like products, loss of a single packet might lead to failure of

audit to whole session.

b. SAS is designed to collect and forward packets only. The complicated protocol analysis and audit are left to SAD which works off-line and won't impact the network performance at all.

Q: What's the advantage of network based audit against host based audit?

A: The recorded data are collected from network directly, with little potential to be tampered or modified purposely, compared against those host based audit systems which collect log files from the hosts that might be compromised. Additionally, with SA, it's not necessary to install agents on hosts so that the potential impact to hosts is minimized. Another obvious advantage of SA is its simple implementation and strong flexibility.

Q: Generally speaking, how long time of network traffic can SA's storage support?

A: Even the low end of SA series products have more than storage capacity of 1TB. For a subnet with about 100 servers, 1TB can accommodate operation data of up to 3 months. Additionally, SA supports data dumping, i.e. the stored data can be dump out to other storage media.

Q: How to guarantee the high performance of SA?

A: SA uses 3-tier architecture. The bottom tier – SAS is a dedicated hardware, for data packets collection and forwarding only. So it brings little impact to network performance. SAS works at layer 2. SAD is responsible for computing extensive protocol analyzing. But it works off-line. So it doesn't introduce impact to network performance either.

Q: Does SA support any database?

A: At this moment, SA supports ORACLE, SYBASE, MS SQL Server.

Q: Does SA support user defined report?

A: SA supports flexible report customization, with data interface to field development.

Q: How does the management client work, B/S or C/S?

A: The management console is C/S, i.e. special purpose GUI client. Browser is not supported.

Q: Why choose C/S, not B/S?

A: The advantage of B/S lies at the convenience provided to users: connection from anywhere with a common browser. However, SA is for very special purpose and administrators often have steady connection style. Meanwhile, most of the recorded audit data is confidential. So SA chooses dedicated GUI clients.

Q: How to guarantee the integrity of recorded data?

A: SAD uses RAID to store recorded data.

Q: Does SA support online upgrade?

A: Yes

Q: Does SA's sensor support VLAN-TRUNK?

A: Yes

Q: Does SA support key word search?

A: Yes, SA supports regular expression and key word search

Q: Does SA support privilege separation of administrator?

A: Yes. Administrators can be authorized to backup, view, manage privilege respectively.

Q: How about the LICENSE model?

A: SA is licensed based on product models.

Q: Does SA support policy customization in order to record specific sessions only?

A: Yes. Administrator can define network objects and flexible audit policy accordingly.

Q: Besides monitoring, does SA have any access control capabilities?

A: Yes. SA has a built-in firewall with access control capability so that administrators can manage and control sessions according to security policy without additional firewalls. This helps save money and lower network delay and latency.

Q: Does SA support all functions of RDP protocol transparently?

A: Yes. SA supports Remote Desktop Protocol for all OS version (Windows 2000/XP/2003/R2) and complete functions (including audio, file system, clipboard, redirect of local hard disk and etc.)

Q: Does SA support all functions of SSH transparently?

A: Yes. SA supports all version SSH protocol (SSH1/SSH2) and full SSH functions (including sftp, scp, port forwarding, x11 forwarding). SA supports SSH data transmission with compression mode.

About BMST

BMST Co. Ltd. is located at Zhong Guan Gun High-Tech District, Beijing, China. Founded at March 2006, BMST focus on technology innovation and development of network security products. The founders have many years of security experience and professional qualifications, especially on telecommunication operations and maintenance. They worked for a variety of world leading IT companies, with thorough understanding and perspective on security essentials and directions. They are pioneering at cutting-edge audit technologies with Session-Auditor series products.