

Session Auditor helps your compliance journey!

Session Auditor

Transparent Audit of RDP/SSH/ICA



June 2008

Contents

Why Audit?	3
What Kind of Audit System Do You Need?	3
What's Session Auditor?	4
System Architecture	4
What SA Can Do?	6
VCR-like Session Playback	6
Policy-based Auditing and Access Control	8
Script-based Intelligent Auditing: AuditScript	9
Search Session Records	10
Report System	10
System Status Monitoring	11
Online Upgrade and Time Synchronization	11
Data Dump and Load	12
Real time Notification on Events	12
Real Time Display of Sessions	12
Encrypted Communications among Components	12
Support of VLAN Trunk	13
Role Based Access to System Administration	13
Logging of System Operations	13
Configuration through Serial Ports	13
Deployments	13
Features and Advantages	14
About BMST	16

Why Audit?

Compliance and internal control are two key missions that security managers must pay attention to. They spend a lot of money in fighting against various threats of misuse and abuse from employees inside the enterprise perimeter, which is protected by those firewall boxes. After many sleepless days and nights, security managers might still be worrying about being challenged by external auditors just because they don't have enough operation records. Among those requirements from Sarbanes Oxley Act and BS7799/ISO27001, completeness and effectiveness of audit systems are the core functionalities that security managers can't overlook.

Typically, more than 75% of security incidents come from internal network, including abuse, misuse of privileges and fault operations. A recent survey to senior IT managers of a leading global mobile carrier shows that about 66% of them regard internal misuse and abuse, divulge of operation data and virus as top threats, while only 13% of them consider that hacking is the top threat.

Among all potential root causes of failure to control those threats, lack of trustworthy and complete audit system is the most common one. That is the reason why audit system has been emphasized by more and more regulations and industry best practices.

In ISO27001:2005, article A15.1.3 requires organizations to protect operation records and A15.2.1 requires information system managers shall ensure all security processes are conducted correctly, in compliance to security policy and standards.

The compliance of Sarbanes Oxley Act requires public list companies to build complete internal governance system, where security audit to information systems are one of the core requirements.

What Kind of Audit System Do You Need?

Generally speaking, there are two layers of "audit system" for information systems: management layer and technical layer. The former can be mapped to those auditing tools that based on best practices and standards, such as ISO 27001 (BS7799) and COBIT. As to the technical layer, there are also many tools and approaches. Log collection and analysis tools in the IDC's security product category of SIEM (Security Information and Event Management) may be the most typical ones. However, those logs are designed to record only the events, without the details of the activities and operations. In other words, if security managers and auditors want to do in-depth investigation and forensics, those logs can't help any more.

Collecting data from network switch's SPAN port may be a solution. Network traffic can be recorded completely, just like using sniffers. But it's difficult for such audit

products to go deep inside the sensitive data and applications and position users. Further, they cannot be used to audit applications with encrypted protocols.

In large enterprises and organizations, core application systems consist of a large amount of network devices, Unix/Linux servers, Windows servers, over which are complicated applications such as ERP, CRM, resource management, billing system, office automation, electronic operation and maintenance, knowledge management and other client/server and/or browser/server applications.

Generally, administrators and operators use Telnet/SSH to remotely manage Unix/Linux servers and network devices, and use Windows Remote Desktop Protocol (RDP) or Citrix ICA protocol to remotely manage Windows servers.

Security managers are facing a dilemma. On the one hand, to counteract the threats of network eavesdropping and hijacking, they urge and even require administrators to use encrypted protocols in remote management; on the other hand, due to the lack of audit ability, security auditors might prevent administrators to use those encrypted protocol so that they can collect and record the audit information. Which choice should security managers adopt: to use encrypted protocols to avoid threats, or not to use encrypted protocols in order to audit the operations?

ENCRPTED PROTOCOLS SHOULD AND CAN BE AUDITED IN THE SAME WAY AS THOSE UNENCRYPTED PROTOCOLS.

What's Session Auditor?

Session Auditor is a Network-based Human Behavior Auditing system. Unlike the traditional log management systems which record discrete events happening in computer systems, Session Auditor records the entire session of human-application interaction and the recorded sessions can be played back later. It records screen updates, mouse clicks and keyboard input, thus you can watch the entire session like you watch the operation of the user “over the shoulder”.

Session Auditor (SA) has unique capability to enhance audit systems by network based transparent RDP/SSH/ICA auditing, with build-in complete recording and playback. In some sense, RDP/SSH/ICA auditing is completely one bonus you can take, SA supports other general protocols just like other audit products. SA is the trustworthy “Black Box” and analyzer in your compliance flight journey.

System Architecture

Session Auditor has three components. Sensor (SAS) is responsible to identify the protocols and record them transparently, and the recorded data is reassembled in sessions and sent back to the second component – Datacenter (SAD), where the session data are stored, processed, indexed and searched. The third component is

the GUI Console (SAC) which is responsible for configuration and management of all components in the system.

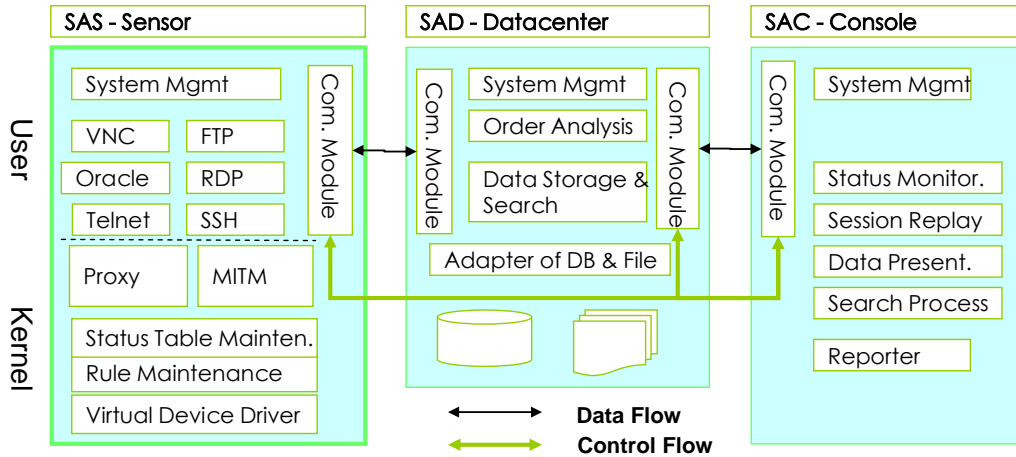


Fig.1. System architecture of Session Auditor

Sensor - SAS

- Independent kernel modules for an efficient and stable system
- User space modules to acquire data with flexible support of protocol expansion
- Built-in firewall module with flexible configuration interface
- Bridge-mode with support of VLAN TRUNK to ease deployment and transparent to clients and servers
- Transparent recording of Windows Remote Desktop, SSH, Citrix ICA
- Transparent recording of Oracle, Sybase, and etc.

Datacenter - SAD

- Central management and distributed deployment to increase flexibility and protect investment
- Dedicated appliance to ensure the security of the recorded data and to eliminate the performance impact on the Sensor
- Huge volume of RAID-5/50 storage in SAD to ensure continuity and completeness session data
- High performance built-in session database for efficient search

Console - SAC

- Central and role based access control management to SAD and SAS
- VCR-like session player
- Script-based intelligent auditing engine with many built-in scripts
- Real time acquisition and display of various kind of component events and audit events
- Real time acquisition and graphical display of control and statistical data
- Customizable reports

What SA Can Do?

Traditional log management solutions focus on recording low-level activities of the **software** (such as OS system calls, login/logout events, network connections, etc) and don't provide details about what **users** are doing. Session Auditor provides an alternative to log-based solutions by revealing what **users** are doing. This change of angle of vision brings several important advantages.

Session Auditor provides unparalleled user behavior reconstruction ability. By watching the playback of a recorded network session, inspector can easily understand the meanings of the chain of activities. In contrast, if you only have log-based solutions in hand, you may have to invest tremendous time and expertise to reconstruct the original user behavior from hundreds or even thousands of logs which come from various different sources, such as from network devices, OS or applications.

Session Auditor can transparently record, playback, search, correlate network sessions of most popular protocols used in the daily maintenance and operation of network and system, such as SSH, Remote Desktop(RDP), Citrix ICA, Telnet, FTP, HTTP, Rlogin, VNC, Oracle, Sybase, MS SQL and etc. The most brilliant point is its unprecedented audit capability to the two most popular encrypted protocols, i.e. SSH and RDP, making it unique in the competition against common sniffer-based audit products and forensics tools.

VCR-like Session Playback

Complete network session recording provides solid technical base for network forensics and audit. Based on that, playback of those recorded sessions is one of the most important analyzing method, which is the right shortage of nowadays security information management (SIM) or security operations center (SOC) products.

The diagrams below are the screenshots of playback of SSH, RDP and Oracle sessions respectively. You can control the playback speed, suspend the playback, and take a snapshot during the playback.

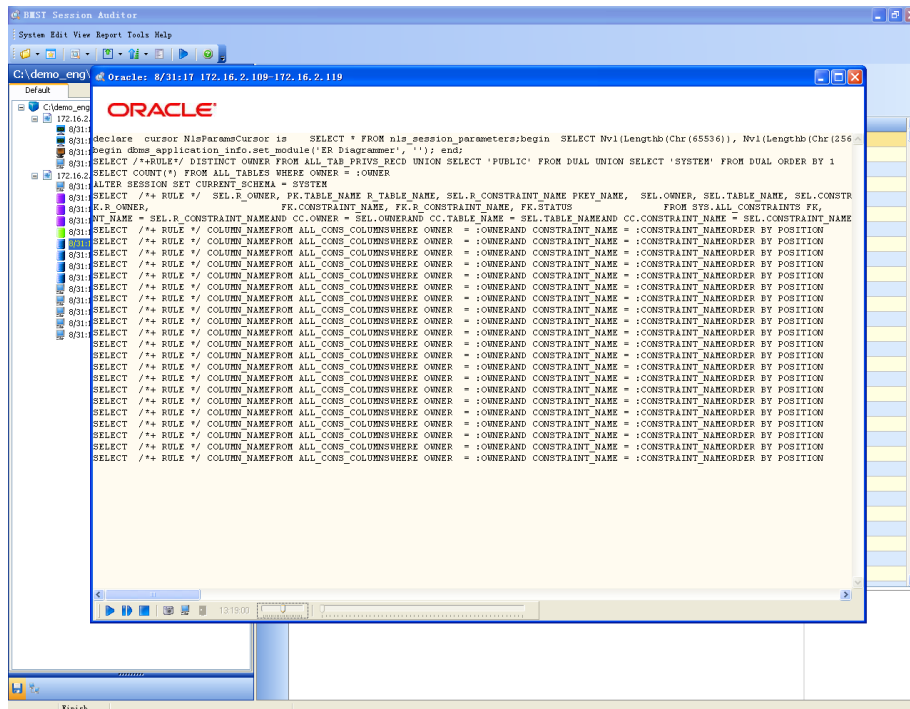


Fig.4. Playback of database sessions

Policy-based Auditing and Access Control

Enterprises can create a series of auditing and access control policies that will control the traffic flow from network to network by defining the kinds of traffic permitted to pass from specified sources to specified destinations and whether the sessions should be recorded for later playback.

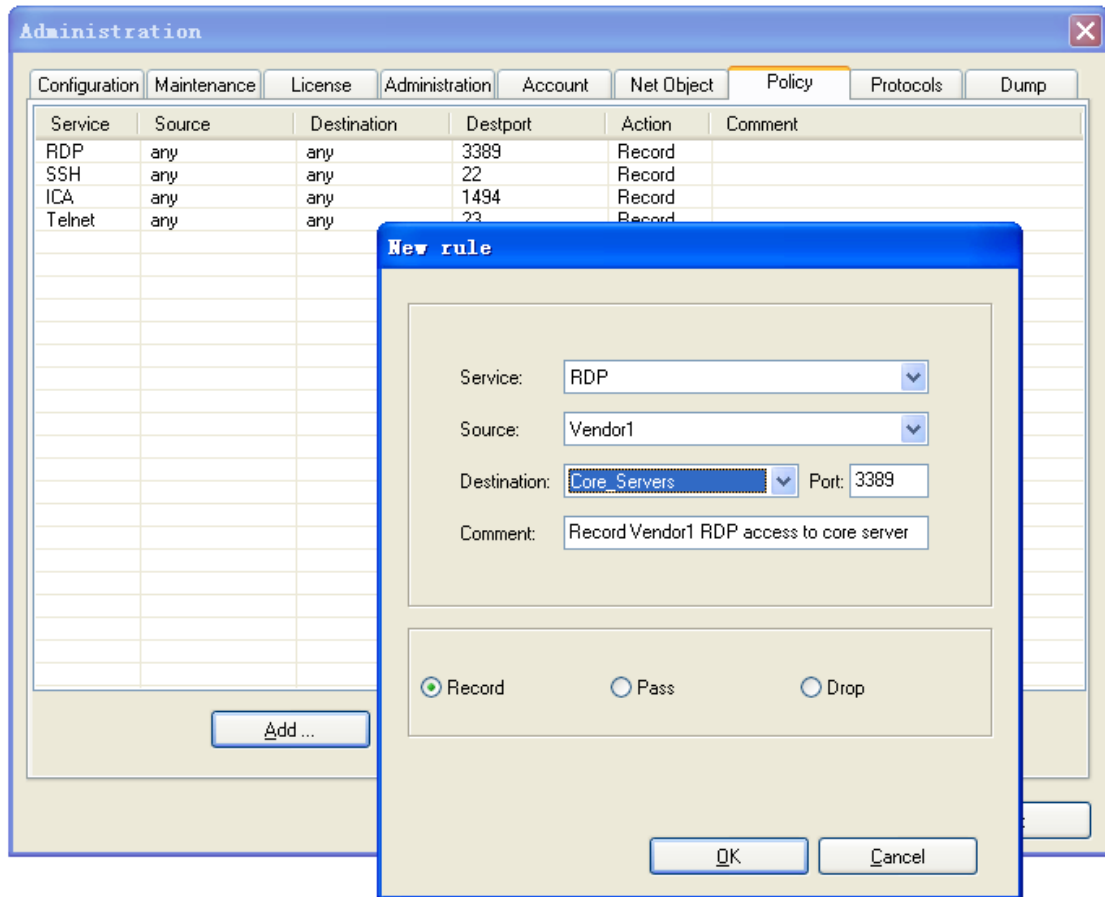


Fig.5. Policy-based Auditing and Access Control

Script-based Intelligent Auditing: AuditScript

AuditScript enables auditors and analyzers to fast locate specific activities within sessions. For example, you can use scripts to search and locate password guessing, file deleting, application launching in RDP, SSH and other sessions. The GUI Console has a built-in IDE for developing new scripts.

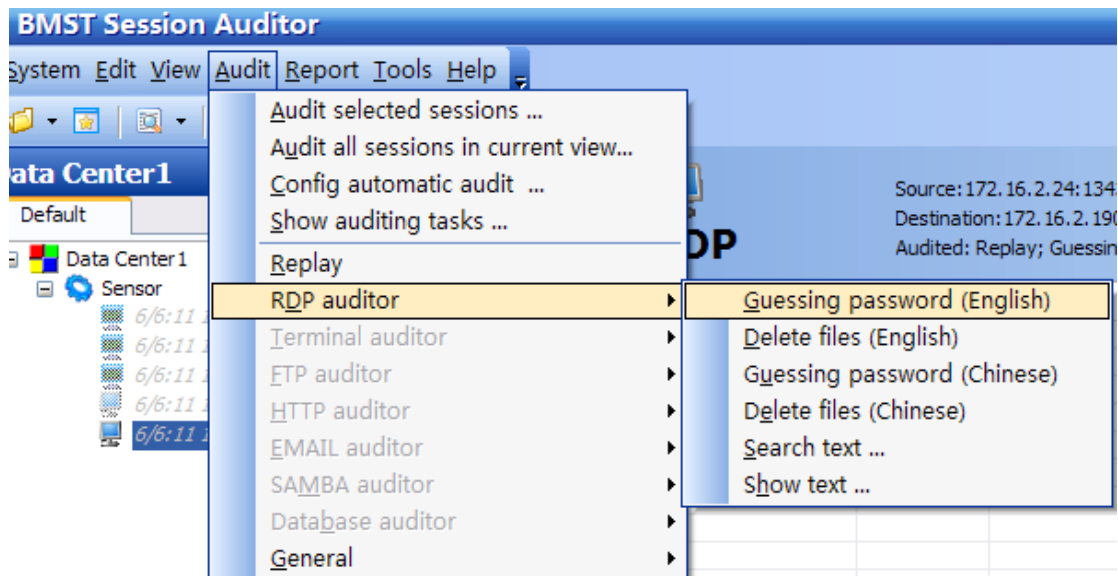


Fig.6. Script-based Intelligent Auditing

Search Session Records

Session Auditor provides the capability of compound search of recorded sessions. See the below diagram. Search conditions might be session start and end time, protocol, source and destination IP addresses and ports and etc. Reports can be generated directly based on the search results. Search conditions can be combined by AND, OR operations. As a plus, SA has the feature of keyword search with regular expression support.

The screenshot shows a 'Search' dialog box with the following fields and controls:

- Name: Search 1
- Search in: DataCenter2
- Predefined: [Dropdown]
- Protocol: RDP
- Source: 0 . 0 . 0 . 0
- Source mask: 255 .255 .255 .255
- Source Port: [Text Box]
- Destination: 0 . 0 . 0 . 0
- Destination mask: 255 .255 .255 .255
- Dest Port: [Text Box]
- Key words: [Text Box]
- Begin time: [Dropdown] (2006-10-17)
- Begin range: [Dropdown]
- End time: [Dropdown] (2006-10-17)
- End range: [Dropdown]
- Buttons: Add, Add, Search, Cancel, Save

Fig.7. Search of audit records

Report System

Session Auditor has a very flexible and powerful built-in report system, which enables administrators track down the whole system to get comprehensive summary and detailed data in a specific time period. The report can be based on the following variables:

- Specific date period, e.g. every day, week and month
- Specific time period in a day, e.g. working hour (8:30 am - 5:30 pm) everyday. It's configurable.
- Specific servers
- Specific clients
- Specific users

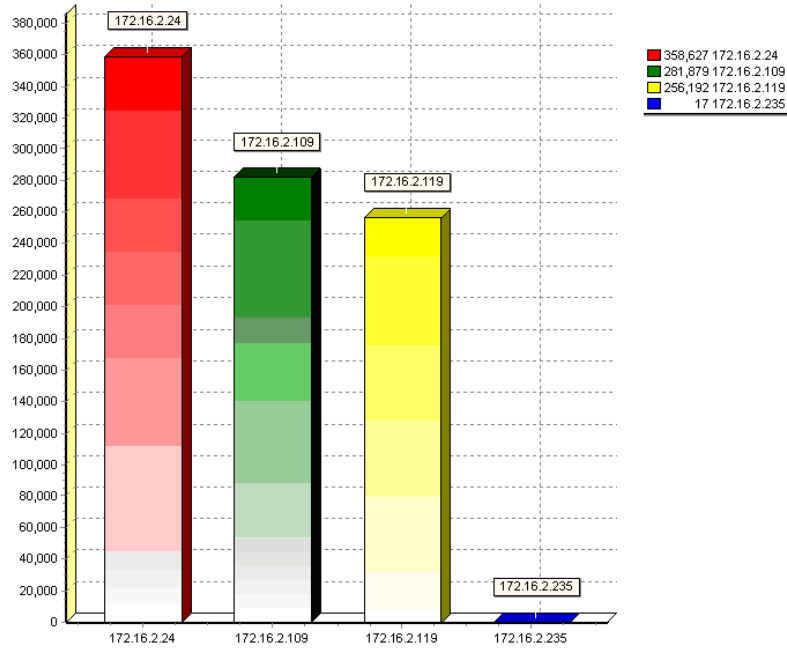


Fig.8. Report chart

System Status Monitoring

The console has a dashboard of system running status and audit output, covering all components (Fig.9). Alerting events can be generated according to the customizable conditions that administrators define.

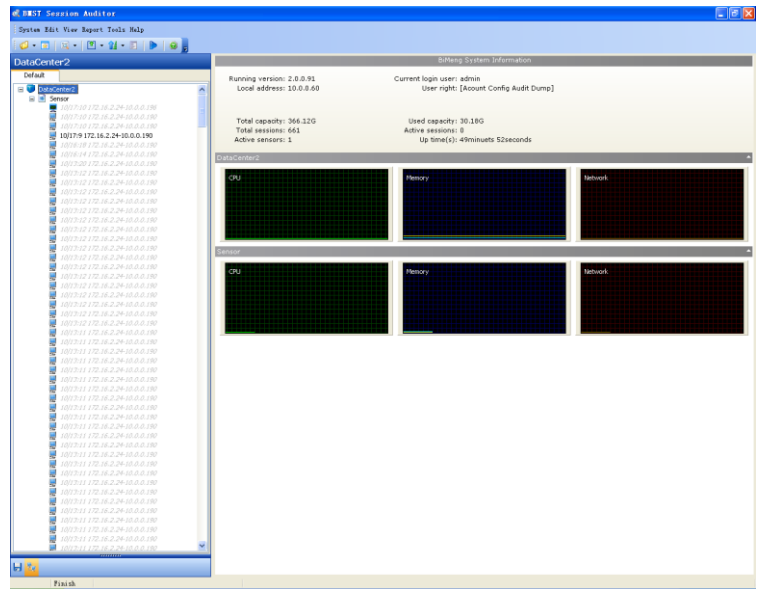


Fig.9. System status monitoring

Online Upgrade and Time Synchronization

Along with powerful recording and playback, Session Auditor has very efficient tools to

help administrators. The whole system can be upgraded online remotely through Console (Fig.10). Console can query and manage system versions and licenses in all Sensors and Datacenters remotely from a central point. Additionally, Console can synchronize the clock of all Sensors and Datacenters to ensure the integrity and trustworthy of recorded data.

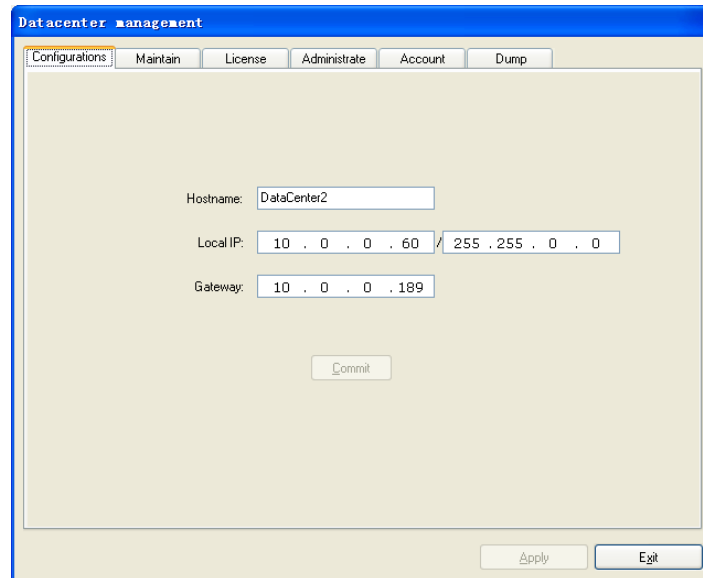


Fig.10. System maintenance and automatic upgrade

Data Dump and Load

Session data dump/load function is provided in Session Auditor. Administrators can dump specific recorded data to local storage. Administrators can also load session data that was dumped previously in order to search and playback.

Real time Notification on Events

Events from SAS and SAD are displayed at Console in real time. Events might be customized audit events and other activities that administrators should pay attention to. Real time notification enables administrators discover and position network or system incidents in order to remove them in time.

Real Time Display of Sessions

Starting and ending of sessions are displayed at the console almost in real time.

Encrypted Communications among Components

Strong encryption are used in communication among components, where 2048bit RSA algorithm and random-generated keys are used in challenge/response

authentication, and 128bit RC4 algorithm is used to encrypt network communications to get very good performance.

Support of VLAN Trunk

SAS can be deployed transparently in various network topologies with VLAN TRUNK. The deployment is very quick and straightforward.

Role Based Access to System Administration

Multiple administration accounts with different privileges can be created in Session Auditor, such as read/write of system configuration, dump/load of recorded data, create/edit/delete of system accounts and etc. (Fig.11).

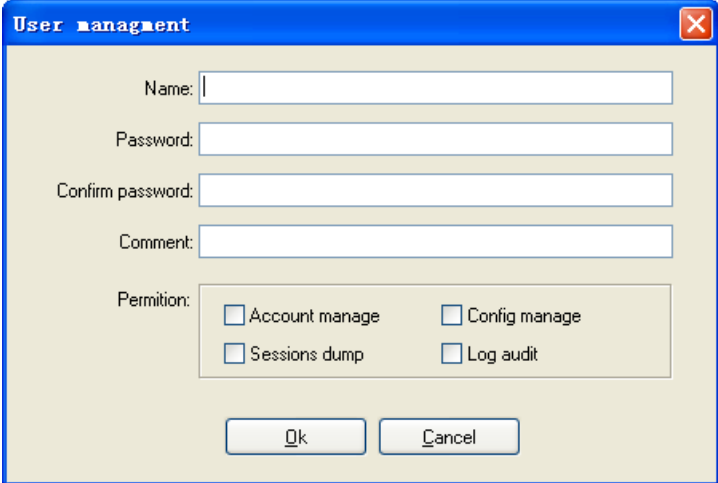


Fig.11. Accounts with different privileges

Logging of System Operations

Complete operation logging is a built-in function which covers all system level operations, such as changes of system accounts, configurations, searching and dumping operations, etc.

Configuration through Serial Ports

Configuration can be conducted through serial ports in SAS and SAD. It's very convenient for administrators to configure SAS/SAD quickly, including network addresses, password recovery, restoring default configurations.

Deployments

It's an easy job to deploy rack-mountable boxes of SAS and SAD. Fig.12 shows a

typical information system environment, where many mission critical servers are placed in server rooms at the right side and staff terminals are placed at operation rooms at the left side to manage, operate, maintain and develop. Switches are used to connect server rooms and operation rooms. SAS is hooked into this link transparently with third port to communicate with SAC and SAD.

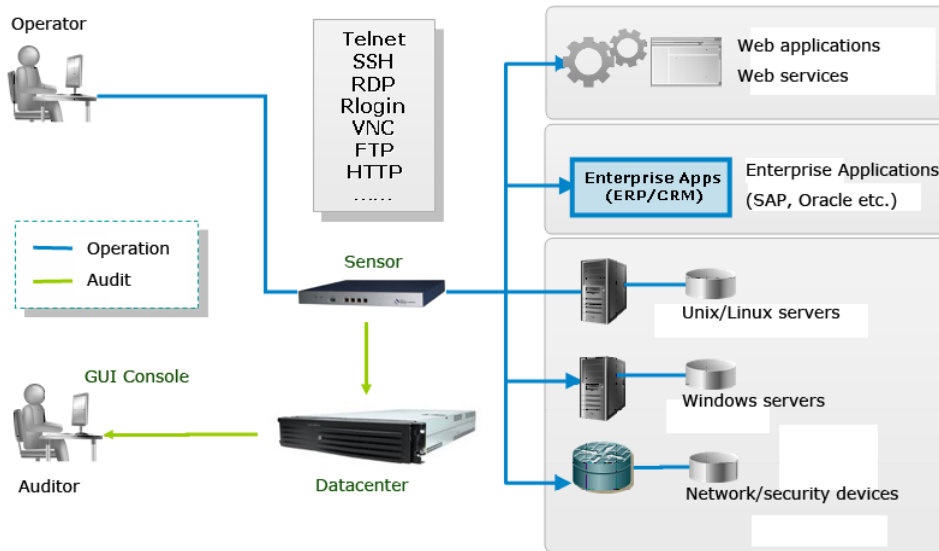


Fig.12. Deployment of Session Auditor

Both SAS and SAD support hierarchical deployment and management (Fig 13). It provides SA customer outstanding expandability and performance balance.

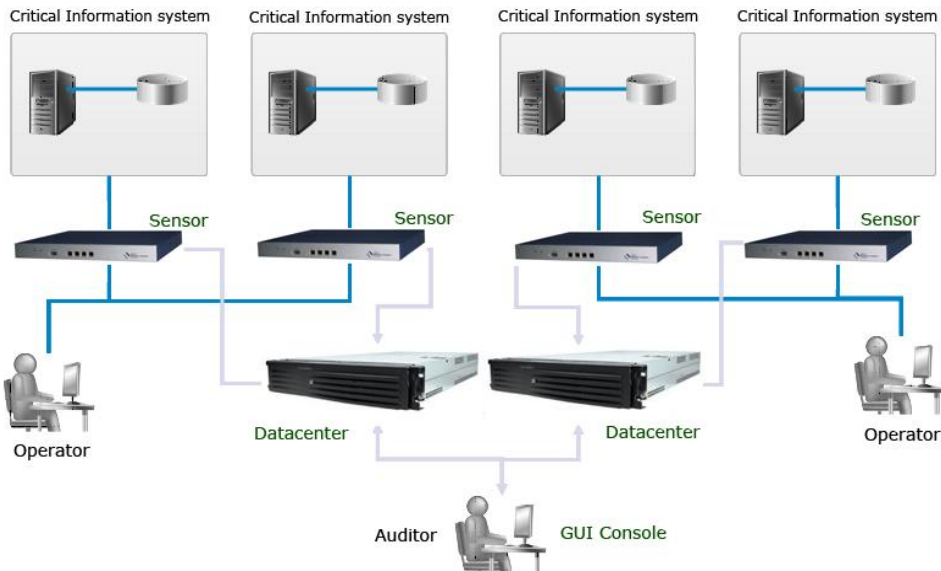


Fig.13. Hierarchical deployment

Features and Advantages

Session Auditor has unparalleled features and competitive advantages with its

ground-breaking transparent audit to encrypted protocols and expandability:

Audit of Encrypted Protocols

- Unique transparent audit of Windows Remote Desktop (**RDP**), Citrix ICA and VNC, including recording and playback to all windows based remote graphical interface operations.
- Unique transparent audit of **SSH** /Sftp /SCP /SSH Port Forwarding and etc., including recording and playback. Those protocols cover most of applications used in remote maintenance and operations to UNIX systems.
- Transparent audit of Telnet, FTP, SNMP, Rlogin, Oracle, Sybase, MS SQL, POP3, SMTP and etc.

Easy Deployment

- Transparent bridge-mode deployment, without any change to servers and therefore without any risk of compatibility among audit software to applications, drastically decreasing the cost of deployment and maintenance of audit systems.
- Support high availability and clustering
- Support **BYPASS**, i.e. remote maintenance and operations won't be interrupted due to power failure of Session Auditor.
- Built-in access control with flexible configurable security policy, i.e. intranet firewall is not necessary any more with Session Auditor in place.
- Hierarchical and distributed deployment to provide high flexibility and scalability
- Support VLAN/Trunk network environment

Strong Administration

- Role based access control mechanism, authentication and encryption to protect the audit information
- Data dump/backup and reload to ensure the integrity and availability of recorded data
- User and operating activity oriented presentation and report
- Convenient configuration through serial port
- Remote online system upgrade
- Synchronization among all components to make sure all audit data are trustworthy and reliable

About BMST

BMST Co. Ltd. is located at Zhong Guan Cun 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.