Microsoft Windows Event Data Collection

How SenSage provides agent-less event collection in Microsoft Windows environments for security, compliance and systems management.

Events in the Microsoft Windows Environment

As more production systems are deployed on Microsoft Windows, organizations are facing the requirement to collect event log data from Windows to support security, compliance and systems management initiatives. In the UNIX environment, transport facilities such as syslog have allowed logs to be centrally collected and stored for years. However, in the Windows environment, no standard tools are installed with the standard Windows operating system to collect and forward important log data.

Different Attempts to Solve the Problem

Microsoft and other third-party software vendors provide limited and largely unsupported open source tools to help security professionals collect events from Windows. A subset of the more common tools include:

- DumpEvt – a freeware utility that dumps all the different Windows event logs into CSV format suitable for importing into a database. DumpEvt generally runs as part of a batch job so it works better when real-time collection and analysis is not a requirement.
- Event Log API – a Microsoft application programming interface (API) that allows administrators to retrieve events, send events, and perform routine maintenance on the event logs (such as clearing events). The API requires homegrown programming in one of the supported programming languages (e.g., Perl, C++) to be utilized.
- WMI – Windows Management Instrumentation (WMI) is Microsoft's implementation of the Web-Based Enterprise Management (WBEM) whose goal was to provide a standard technology for accessing management information in an enterprise environment. This method also requires users to write their own programs to call the WMI APIs.
- Snare – developed by Intersect Alliance, and available in open source, is an agent that provides a syslog-like capability to retrieve and forward Windows event logs to a centralized server. Snare is the de facto standard for Windows event retrieval. The software is distributed as both source code and executable.
- Project Lasso -Project Lasso is Windows-based open source software designed to collect Windows event logs, including custom application logs, and provide central collection and transport of Windows log data via TCP syslog to any syslog-NG compatible log receivers. The software is distributed as both source code and executable.

Introducing the SenSage Agentless Windows Retriever

SenSage provides an alternative to open source and homegrown solutions with the SenSage AgentlessWindows Retriever. Unlike solutions deployed in open source, SenSage provides a supported and secure solution for collecting Windows events with an agentless deployment. Combined with the SenSage Windows Analytic Reports, SenSage provides customers with a secure, maintenance-free solution for collecting, analyzing and understanding their Windows environment.

Agentless Windows Retriever Features

- ✓ No agents to configure, distribute or update
- ✓ No Windows server required to collect event data
- ✓ No programming thereby reducing complexity and eliminating maintenance responsibilities
- ✓ Real-time data collection and full Windows event log support including:
  - ✓ Security, Application, System, DNS Server, File Replication Service, and Directory Service
- ✓ Ability to filter data by SubSystem and/or Event IDs
- ✓ Communicates over TCP protocol to ensure data delivery (not UDP)
- ✓ Automatic discovery and collection of new Windows Servers through LDAP queries
- ✓ Automated recovery for dropped connections
- ✓ Maintains the "state" of each log collection on each server so no data is missed or duplicated
- ✓ Centralized management of your Windows data collection
  - ✓ Check status, stop and start collection sessions
- ✓ Runs under a secure domain user's credentials (No Administrator rights needed)

How Does the SenSage Agentless Windows Retrieve Work?

The SenSage Agentless Windows Retriever is a Java application that resides on the SenSage Collector server. Every Windows server whose data is to be collected is defined in the Collector configuration file, including its IP address, authentication credentials, and the desired frequency of the data collection.

- The Retriever takes the IP address information and utilizes the Server Message Block (SMB) protocol to establish a connected "session" with each of the defined Windows servers.
- Each session is authenticated using a restricted domain User ID that allows access only to the event logs. The password that is used is stored and sent in an encrypted format. Administrator rights are not needed.
- Once the session is established, the Retriever uses the DCE/RPC (Distributed Computing Environment / Remote Procedure Calls) to start collecting the binary logs from the server. The DCE/RPC was designed specifically to allow software to work across multiple computers, as if it were all working on the same computer .
- The Retriever maintains a state for each log collected on each Windows server for which a session has been established. If a connection is lost, the Retriever will automatically try to re-establish the session every polling interval. Once successful, the Retriever uses its state information to resume its collection, ensuring that data is not missed or duplicated.
- Once collected onto the SenSage Collector, the application translates the binary data into ASCII format, where it is then loaded into SenSage's patented event data warehouse. By default, a backup copy is made and stored safely for data redundancy and failover requirements.

SenSage Provides Detailed Analysis

SenSage Agentless Windows Retriever allows organizations to track the most common security policy issues such as changes to domains, groups and access to filesystems where auditing is turned on. SenSage also provides filtering capabilities to help filter out "the noise" in Windows event logs.

SenSage also correlates Windows events. Some actions, such as file deletions require three different Windows events to be correlated to determine the file name and user. SenSage correlates Windows events across all sources, providing an authoritative view of all user access, file access, and other important events

GroupModificationSummary

author: administrator created: Dec 10, 2006 12:14

starting Dec 10, 2004 7:00:00 AM, ending Dec 10, 2006 6:59:59 AM GMT+00:00

View Query/Library | Filter

Table | Graph

Rows 1-100 of 1928

Time	Information System	Domain	Called By	Target Group	Event ID	Status
06-Oct-30 18:44:01	FINANCE_AD	FINANCE	Administrator	AUDITOR	653	Global distribution group created
06-Oct-30 19:20:19	HR_AD	HR	Administrator	STAFF	635	Local security group created
06-Oct-30 20:26:50	IT_AD	IT	Administrator	STAFF	657	Global distribution group deleted
06-Oct-30 20:40:57	MEDICAL_AD	MEDICAL	Administrator	STAFF	653	Global distribution group created
06-Oct-30 20:41:58	IT_AD	IT	Administrator	AUDITOR	631	Global security group created
06-Oct-30 21:02:07	FINANCE_AD	FINANCE	Administrator	AUDITOR	658	Universal security group created
06-Oct-30 22:18:44	MEDICAL_AD	MEDICAL	Administrator	STAFF	639	Local security group changed
06-Oct-30 22:19:44	FINANCE_AD	FINANCE	Administrator	USERS	635	Local security group created
06-Oct-30 22:58:02	FINANCE_AD	FINANCE	Administrator	STAFF	641	Global security group changed
06-Oct-30 23:07:07	IT_AD	IT	Administrator	STAFF	641	Global security group changed
06-Oct-30 23:28:17	FINANCE_AD	FINANCE	Administrator	STAFF	659	Universal security group changed
06-Oct-30 23:47:26	MEDICAL_AD	MEDICAL	Administrator	STAFF	664	Universal distribution group changed
06-Oct-30 23:48:26	MEDICAL_AD	MEDICAL	Administrator	AUDITOR	652	Local distribution group deleted
06-Oct-31 00:17:40	IT_AD	IT	Administrator	USERS	659	Universal security group changed
06-Oct-31 01:36:18	MEDICAL_AD	MEDICAL	Administrator	USERS	635	Local security group created
06-Oct-31 02:01:30	MEDICAL_AD	MEDICAL	Administrator	MANAGERS	641	Global security group changed
06-Oct-31 03:08:01	MEDICAL_AD	MEDICAL	Administrator	STAFF	652	Local distribution group deleted
06-Oct-31 03:17:06	FINANCE_AD	FINANCE	Administrator	STAFF	631	Global security group created

Summary report of Windows group modifications

A complete data analytics environment allows operational reporting as well as complex forensic investigations. Both scheduled and ad-hoc reports can be run, scanning 100s of billions of rows of data in minutes. SenSage provides pre-packaged analytics for SOX, HIPAA, PCI and a host of other regulatory mandates. Thorough investigative queries are available to support audit and root-cause analysis. Standards-based normalization of disparate sources through database views is provided, while maintaining source-data integrity.

Comprehensive Insight

With SenSage's patented datamart technologies, event data is treated as true structured information and can be analyzed by standard "relational" queries. The result is an ability to find information quickly, and perform complex data analysis, such as correlation, user defined aggregates (UDAs), user defined functions (UDFs), trending and other forms of data mining. SenSage turns events into actionable information.

About SenSage, Inc.

SenSage, Inc., www.sensage.com, offers the only patented event data warehousing solution for log management and compliance auditing applications. Over 300 customers have deployed SenSage solutions to reduce the risks associated with insider threats, system downtime and failed audits by providing faster, more granular analysis of privileged user behavior and analyzing anomalies across network, system and application activity. Based in San Francisco, the company markets its solutions directly and through partners, including Cerner, EMC, HP, HDS, IBM, Intec Billing Systems, Lockheed Martin, Network Appliance, Sendmail, Symantec and Tokyo Electron Device.

SenSage, Inc. - 415.808.5900 - www.sensage.com