

## Windows Event Data Collection

### How SenSage allows organizations the flexibility of using an agent-less collection technology in their Windows environment

---

#### Why is this an issue?

One of the biggest issues facing IT organizations today is the need to, and method of, collecting event log data from a distributed application network. 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, there's no such tool installed with the standard Windows operating system to collect and forward important log data.

#### Different Attempts to Solve the Problem

Third party software vendors, and even Microsoft itself, have attempted to address this task but with mixed results:

- **DumpEvt** – a freeware utility that dumps all the different Windows event logs into a format suitable for importing into a database. It 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). However, it requires homegrown programming in one of the supported programming languages (e.g., Perl, C++) to take advantage of it.
- **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 API's. It has also been shown to be resource intensive and not able to keep up with heavy loads.
- **Snare** – developed by Intersect Alliance, this freeware tool is an agent that, once installed, provides a syslog-like capability to retrieve and forward Windows event logs to a centralized server. It is field-tested and has been deployed by many organizations. SenSage has a number of customers who use Snare to collect and forward their Windows logs on to the SenSage product.

#### Any Other Choices?

**Yes!** While all of these approaches work, many organizations don't want to have to code and maintain their own systems management programs, or have to deploy another agent (i.e., Snare) to each of their Windows servers. For that reason, SenSage has developed the **Agentless Windows Retriever**, that together with the SenSage Windows Analytic Reports, provides customers with a secure, maintenance-free solution for collecting, analyzing and understanding their Windows environment

#### Agentless Windows Retriever Benefits Summary

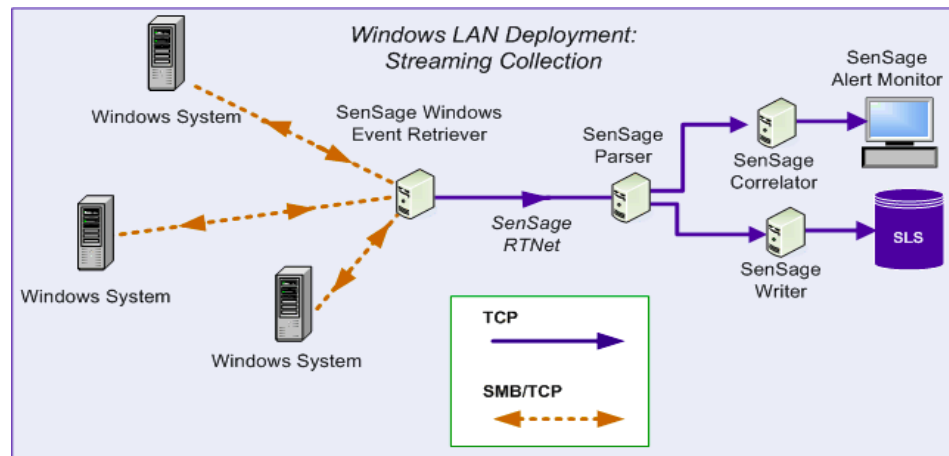
- No agents to configure, distribute or update
- No programming thereby reducing complexity and eliminating maintenance responsibilities
- Real-time data collection of all your Windows logs
  - Security, Application, System, DNS Server, File Replication Service, and Directory Service
  - Optional ability to filter data by SubSystem and/or Event IDs
- Communicates over TCP protocol to ensure data delivery
- 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
- Can run under a secure domain user's credentials (No Administrator rights needed)
  - Password is encrypted when stored and used in authentication activities



## How Does it 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 data repository. By default, a backup copy is made and stored safely for data redundancy and failover requirements.



Please note that all SenSage components listed here could run on the same server.

### SenSage Provides Detailed Analysis

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., the leading provider of event data management solutions, enables the collection, analysis, and retention of event data for security, compliance and systems management. The company offers unparalleled performance and a scalable means for organizations to centrally aggregate, efficiently analyze, dynamically monitor and cost-effectively store massive volumes of event data. Based in San Francisco, CA, SenSage currently works with Global 2000 customers in financial services, government, healthcare, retail, manufacturing, telecommunications and technology. For more information, visit [www.sensage.com](http://www.sensage.com).