



Integrating ASG-Sentry And CorreLog Server

mailto: info@correlog.com

<http://www.correlog.com>

This paper describes methods of easily integrating the ASG-Sentry Network Management System with the CorreLog Security Correlation Server, including techniques, features, and benefits.

ASG-Sentry is a web-based SNMP network management system that incorporates a variety of sophisticated polling functions. The ASG-Sentry manager continuously checks the network state by fetching and comparing SNMP MIB object values to user-defined thresholds. When a network value is found to be out-of-tolerance, ASG-Sentry logs this event to its internal event log.

The CorreLog Server is a web-based message aggregation program, with neural-network components. The program is classified as a Security Information and Event Management (SIEM) system. CorreLog receives, indexes, and correlates large amounts of real-time message data sent by diverse types of computer systems, including Windows, all flavors of UNIX and Linux, as well as network routers, firewalls, application programs, and mainframe computers.

Unlike the ASG-Sentry program, Correlog Server does not poll the network. Rather, the role of CorreLog is to listen for and log messages sent by applications and devices, and make sense from this data.

As discussed in this paper, these two software programs are highly complementary, providing access to data that has similar importance, but which is derived in completely different manners. This paper will be of special interest to existing ASG-Sentry sites, or customers looking for a comprehensive new system for implementing both SNMP and SIEM management.

Background

ASG-Sentry is an SNMP manager. It is mainly useful for determining network states and conditions. SNMP, while a useful management protocol, has numerous limitations; generally, SNMP cannot be used to determine the precise nature of an error condition or system state. For example, SNMP is capable of determining the number of active users on a particular system, but cannot tell who has actually logged on to the system, and when.

CorreLog corrects this limitation of SNMP by providing substantial and important visibility to data that is not normally available via SNMP. Specifically, while SNMP might be used to perform a superficial test of whether a device is experiencing errors, it cannot be used to determine the precise nature of the error. In contrast, CorreLog can log and correlate the exact error message, error source, nature of the error, severity of the error, and the precise time of the error.

This capability of CorreLog, to extract semantic information from a stream of events, is especially valuable for security monitoring, but also is quite useful for any type of performance monitoring where real-time actionable events are to be created from a stream of message data. CorreLog permits users to tap into a new universe of information that is readily available, but invisible to SNMP managers like ASG-Sentry.

Program Compatibilities

ASG-Sentry and CorreLog are quite compatible, sharing common concepts and attributes. The programs work well together, without any programming or extensive configuration required.

- **Device Oriented Views.** Both ASG-Sentry and CorreLog record messages by device, and have device oriented views of the data. CorreLog actually expands the number of devices that can be managed by ASG-Sentry, since CorreLog does not have to poll devices. (The total number of devices that can be managed by CorreLog is 10,000 devices, whereas the number of devices that can be managed by a single copy of ASG-Sentry is only 1000 devices.)
- **Standards Based Messaging Protocols.** ASG-Sentry is mainly SNMP trap-centric, but supports sending of syslog messages. CorreLog is mainly syslog-centric, but supports both sending and receiving SNMP traps. This allows users to employ both of these common and widely used standards in a highly complementary fashion, and relay information between the two programs.
- **Compatibility of Messages And Data.** Both ASG-Sentry and CorreLog employ exactly the same message severity levels (ranging from debug to emergency.) Messages can be sent between the program with no change to or loss of severity information. Additionally, the source of a message (typically the IP address of the device that sent the message) is preserved when exchanging messages, so that the two programs can reflect precisely the same message content.
- **Data Grouping.** ASG-Sentry employs a "device group" concept, which allows devices to be grouped arbitrarily together. In a similar fashion, CorreLog employs the concept of "message groups" (or "threads"), which

allow messages to be arbitrarily grouped together by semantic content. This provides two radically different perspectives of the same data, allowing operators to view information by type of device, as well as type and content of message.

- **Program Navigation.** Both ASG-Sentry and CorreLog are entirely web-based, and use "tabbed" navigation to access screens. Also, both ASG-Sentry and CorreLog implement "wizard" based procedures, assisting the user in configuring and maintaining the two systems. The operation of these programs is similar enough so that the time for an ASG-Sentry operator to learn CorreLog is short. Users can navigate between the two programs using a single browser window.
- **Extensibility.** Both ASG-Sentry and CorreLog are highly extensible. For sites that already have ASG-Sentry, CorreLog furnishes expansive additional functionality with regards to network adapters, event logs, streaming log data, POP3 monitoring, and other adapters that expand the view of IT operations. For example, CorreLog provides additional reporting capabilities that ASG-Sentry lacks, such as the ability to update multiple ODBC data sources and databases with event and state information, the ability to create Excel spreadsheets, and ability to distribute reports using standard RSS.

Integration Techniques And Applications

Both ASG-Sentry and CorreLog can function in a stand-alone mode of operation, requiring no other supporting software. However, when combined, these programs are highly synergistic. Working together, these programs increase the number of devices that can be managed and the diversity of data being monitored. This greatly improves the overall visibility of an enterprise.

Both ASG-Sentry and CorreLog are highly flexible components, and can be arranged in various ways to support both single and multi-tier management. Strategies include both centralized and distributed management architectures. Some of the more obvious types of applications are discussed here (although the list below comprise only a small set of possible integration strategies).

Strategy: ASG-Sentry Feeds Messages To CorreLog

This approach consists of ASG-Sentry feeding its event information to CorreLog, which logs, indexes, and archives the information, and combines this information with other data received from applications and event logs across the enterprise. CorreLog serves as a highly sophisticated "correlation engine" for ASG-Sentry, to combine SNMP type data with other types of data.

Using this technique, CorreLog can expand the view of the enterprise by correlating the SNMP specific data of ASG-Sentry with data from Windows

event logs, UNIX platforms, application programs, legacy devices, as well as mainframes.

When employing this strategy, ASG-Sentry serves as an important data source, but far from the only type of data source in the enterprise. CorreLog acts as a higher-level manager, accepting data from a much more diverse (and larger) set of devices, possibly including multiple copies of ASG-Sentry, or other network managers and applications.

Strategy: CorreLog Feeds Messages To ASG-Sentry

This approach consists of CorreLog sending its raw or correlated event information to ASG-Sentry via SNMP trap messages. The precise message severities and source devices used by CorreLog are reflected exactly in ASG-Sentry, so that messages appear to come directly from the managed device, and not from the CorreLog Server.

This approach is useful in extending the range of monitoring at an ASG-Sentry site, such as to include non-SNMP devices, as well as mainframes. Specifically, ASG-Sentry can use "Trap Alarms" to show CorreLog data on ASG-Sentry Maps and screens. CorreLog serves as an "adaptor / extender" to ASG-Sentry, acting as "middleware".

Specifically, CorreLog operates as a type of "SNMP Proxy Agent" for ASG-Sentry, especially useful in managing devices that do not necessarily have SNMP capability, such as serial devices, point of sale systems, and computer peripherals. This approach can greatly increase the number and types of managed devices.

Strategy: ASG-Sentry and CorreLog Feed Data To Third Party Software

This approach leverages the high degree of interoperability and standards-based operation of both programs to feed third party software, such as other network managers, reporting systems, incident management systems, and dashboards.

Both ASG-Sentry and CorreLog can update ODBC data sources with information, and can execute action programs to send e-mail, send SNMP traps, and send Syslog messages to third party software. Both ASG-Sentry and CorreLog can open tickets in popular incident management systems.

In particular, both ASG-Sentry and CorreLog support the ASG-CMDB dashboard system; ASG-Sentry updates ASG-CMDB dashboards with state information that describes the current state of the network. At the same time, CorreLog updates ASG-CMDB dashboards with historical information and trend data describing the number of logins, security violations, Windows Active Directory events, and other historical data.

Integration Benefits

For customers with planned or existing ASG-Sentry sites, CorreLog provides a number of benefits that increase the performance, capabilities, and security of ASG-Sentry. These benefits include the following, and more:

- **CorreLog increases the number of managed devices.** In a one-tier management strategy, ASG-Sentry can poll a maximum of 1000 different SNMP agents and devices. CorreLog, because it does not poll, expands the number of fully managed devices to be 10,000. This allows the user to monitor many more devices in a single console without resorting to a multi-tier strategy.
- **CorreLog increases SNMP trap reception rate.** ASG-Sentry is mainly designed to be an SNMP polling manager. As such, Sentry contains some of the best and most powerful polling functions available to industry. However, Sentry is not highly adept at receiving SNMP traps or handling events, and is capable of handling only five to ten events per second under normal conditions. In contrast, CorreLog can receive more than 2000 messages per second, with an upper limit approaching 10,000 messages per second. CorreLog adds true SIEM capability to an ASG-Sentry installation.
- **CorreLog furnishes unique new adapters.** CorreLog provides a number of new interfaces that enhance ASG-Sentry's visibility to enterprise software and data, including a z/OS Mainframe Agent for monitoring RACF LPARs, a high-speed asynchronous ICMP polling agent, a POP3 agent, an interface to McAfee ePO, an authenticating SMTP e-mail interface, and the ability to integrate to a much wider range of reporting and incident management systems.
- **CorreLog provides additional integration points to ASG-Sentry.** CorreLog provides multiple new integration points for ASG-Sentry, including a highly extensible dashboard, the ability to update multiple ODBC databases from a single location, and the ability to generate RSS feeds. The CorreLog "Sigma Framework" developer API, included in all copies of the program, allows a developer to easily add new screens and functions to the CorreLog system. These functions enhance the life cycle for both programs, and furnish an easy way to tailor these programs to the specific requirements of an organization.
- **CorreLog increases the security of ASG-Sentry implementations.** ASG-Sentry was never intended to be a particularly secure program. In particular, ASG-Sentry (in its unpatched form) contains multiple well-known hooks and exploits. CorreLog, in its role as a security management server and SIEM tool, can make ASG-Sentry fully secure. CorreLog uses

AES-256 encryption, secure TLS, File Integrity Monitoring and the various intrusion detection functions, which have distinguished CorreLog as a PCI/DSS and HIPAA compliance tool. CorreLog adds immediate security to your ASG-Sentry installation, as well as the entire organization.

Conclusions

While ASG-Sentry contains various clever event management functions, the primary focus of ASG-Sentry is SNMP polling. As such, Sentry represents a state-of-the-art polling system, but is unable to serve in any serious capacity as an enterprise-wide event management program or SIEM tool, since it is able to process only a few events per second.

In contrast, CorreLog focuses completely on event management and SIEM functions, incorporating unique and advanced correlation capabilities, as well as providing high-rate interoperability with all types of real-time message data.

Given the numerous integration points and similarities between these two programs, CorreLog provides enormous benefit to those enterprises and organizations seeking to collect data from non-SNMP devices, or implementing a security management system, or both. The two programs complement each other by specializing in two distinct but equally important IT management roles

Parties interested in testing CorreLog with their ASG-Sentry implementations are encouraged to contact either CorreLog, Inc., or ASG, Allen Systems Group. The CorreLog Server installs on Windows 2000, 2003, 2008, XP, Vista, and Windows 7 platforms within just a few minutes.

Evaluation copies of the CorreLog Server are available for immediate download from the CorreLog website: <http://www.correlog.com>. A 30-day evaluation license is automatically created upon program installation.

Contact CorreLog today for more information and immediate assistance.

CorreLog, Inc.

Contact: info@correlog.com

<http://www.correlog.com>