

Getting the Most Out of Centralized Logging and Event Management

Finding the needle in the haystack

There are very few IT administrators who enjoy poring through log files by hand to diagnose and fix a system or network problem, especially when it happens in the middle of the night and involves a potential breach of sensitive company information. It's about as close a scenario to finding a needle in the haystack as it gets. Luckily for administrators, there is an easy way to avoid this: by implementing centralized logging and event management.

Back in the day, logs were mostly a tool for troubleshooting problems. More recently, they have become important for network and system performance optimization, recording user actions, providing helpful data for investigating suspicious activity, and assisting with proactive monitoring of the environment. In many cases, having log data easily available can provide early warnings about problems before they spiral out of control.

Not just good practice

Centralized logging and event management is required or heavily implied by many security standards, making it one of the fastest growing segments of the industry. If your organization is subject to FISMA, GLBA, HIPAA, SOX, COBIT, or PCI DSS compliance, then this is something you should already be thinking about or have implemented. Although ISO 27002 compliance is not mandated for any organization, if you are striving to comply with it you'll also need to address this issue.

The challenges to success

Recognizing the need for guidance on how to implement sound computer security log management, the National Institute of Standards and Technology (NIST) has created Special Publication 800-92, which provides a comprehensive overview of and best practice recommendations on this topic. This publication discusses the biggest hurdles to successfully implementing centralized logging and event management, including the following:

- Log generation and storage. Most organizations generate many different types of logs on many hosts throughout the organization, requiring a need for log management to be handled organization-wide. In addition, log content is not generated in the same format, making it difficult to link events recorded by different sources. For example, if one log source identifies Telnet by name in one log, and by

port number (23) in another log, it will be much harder to associate those two events. Issues such as inaccurate timestamps and inconsistent log formats only compound the difficulty of meaningful log analysis.

- Log confidentiality, integrity, and availability. Because logs contain records of system and network security, they must be protected against breaches of confidentiality and integrity. The availability of logs must also be protected. Data retention requirements may necessitate keeping copies of logs for longer periods of time than the original sources are able to support, requiring them to be archived. And, the confidentiality and integrity of the archived logs must also be protected.
- Log analysis. Log analysis has always been considered one of the most dreaded, boring tasks for system and network administrators. It is often done only in a reactive manner, administrators are seldom trained on how to do it efficiently, and they often don't have tools that could help automate much of the analysis process. Without sound processes for analyzing logs, their value to an organization is dramatically reduced.

Overcoming the challenges

Although the list of log management challenges can seem daunting, the following key practices can set an organization on the right path to avoid and even solve many of these challenges.

- Properly prioritize the function of log management. First, define requirements and goals for log performance and monitoring based on applicable laws, regulations, and existing organizational policies. Then, prioritize goals based on balancing the need to reduce risk with the time and resources necessary to perform log management functions.
- Establish log management policies and procedures. Policies and procedures allow for a consistent approach through the organization, and ensure that laws and regulatory requirements are met. Conducting periodic audits is a great way to confirm that logging standards and guidelines are being followed throughout the organization.
- Create and maintain a secure log management infrastructure. Identify the needed components for your organization's log management infrastructure, and determine how they interact. Be sure to create an infrastructure that is robust enough to handle peak volumes during extreme situations as well as the expected volumes of log data. The three primary tiers of a log

management architecture include log generation, log analysis and storage, and log monitoring.

- Provide appropriate support for staff with log management responsibilities. All efforts to implement log management will be for naught if the staff members who are tasked with log management responsibilities do not receive adequate training or support to do their jobs effectively. Providing log management tools, documentation, and technical guidance are all critical for log management staff members to succeed at their jobs.

Tools to get the job done

Syslog, originally developed in the 1980s, is the standard logging solution for Linux- and Unix-based systems. Its simple framework allows for log entry generation, storage, and transfer, and it is supported by a wide variety of devices and receivers across multiple platforms. Because of this, syslog is a great tool for integrating log data from many different types of systems into a central repository.

Security information and event management software (SIEM) is the modern marketing name for centralized logging tools (see Table). These products have one or more log servers that perform log analysis, and one or more databases for storing the logs, and generally come in one of two types:

- Agentless products: The SIEM server receiving data from individual log hosts without needing to have any special software installed on the hosts. The primary disadvantage of this method is the inability to filter and aggregate logs at the individual host level, which can increase the amount of time it takes to filter and analyze logs. It can also be a problem if credentials are required to authenticate to the log hosts.

- Agent-based products: An agent program is installed on the log host to perform tasks such as event filtering, aggregation, and log normalization for a particular type of log, and then transmitting the normalized log to the SIEM server. This usually occurs on a real-time or near real-time basis for analysis and storage. The biggest disadvantage to this method is the amount of administrator time needed to install, configure, and maintain the agent on each individual logging host.

Here are a few other tools that may be part of your centralized log environment:

- Host-based intrusion detection systems (HIDS): Monitor the characteristics and events of a specific host for suspicious activity.
- Visualization tools: Present security event data in a graphical format. Can be part of a SIEM product, or a third-party tool.
- Log-rotation utilities: Can improve log management for log sources that do not offer sufficient, or any, log rotation capabilities on their own.
- Log-conversion utilities: Can help to incorporate data from less common log sources into a log management infrastructure, or when syslog is being used and one or more log generators cannot log directly to syslog.
- Event correlation utilities: Help with review and interpret log data in an automated way, possibly sending alerts to system administrators when concerning conditions arise.

Leaving the haystack behind

Centralized logging and event management is a critical part of any well-maintained IT infrastructure. It provides an invaluable

TOOL	DESCRIPTION	MORE INFORMATION
<i>Cyberoam iView</i>	Comprehensive centralized logging and reporting tool; also available in appliance form.	http://www.cyberoam-iview.org/
<i>OSSEC</i>	Host-based intrusion detection system; runs on most operating systems.	http://www.ossec.net/
<i>OSSIM (Open Source Security Information Management)</i>	A comprehensive compilation of tools to provide administrators with detailed views networks, hosts, etc.	http://www.alienvault.com/community.php?section=Home
<i>Rrdtool/ddraw</i>	Rrdtool is an industry standard, high-performance data logging and graphic system for time-series data; ddraw is a powerful diagram editor.	http://oss.oetiker.ch/rrdtool/ http://www.gnomefiles.org/app.php/DDraw
<i>SEC</i>	Platform independent event correlation tool designed to fill the gap between commercial event correlation systems and homegrown solutions.	http://simple-evcorr.sourceforge.net/
<i>Snare Agent for Windows</i>	Windows-compatible service that interacts with Windows Eventlog subsystem to enable remote, real-time event log information transfer.	http://www.intersectalliance.com/projects/SnareWindows/
<i>Splunk</i>	Software that uses data indexing to enable real-time event searching across an entire IT infrastructure.	http://www.splunk.com
<i>Syslog-ng</i>	Flexible, highly scalable system logging application that transfers log messages in a TLS-encrypted channel; compatible with many operating systems and platforms.	http://www.balabit.com/network-security/syslog-ng/

Table: Open source tools for centralized logging and event management

source of information that can be used in a number of business processes, and various laws also mandate that logs be maintained and reviewed. With implementation options to fit any size budget, no organization can afford to still be searching for the needle in a haystack. ■

This article was reprinted from the Q2 2010 issue of The Barking Seal, a publication of Applied Trust. You can subscribe to The Barking Seal online at <http://www.appliedtrust.com/barkingseal>. "Applied Trust" and the "Seal on a Rock" Applied Trust Engineering logo are registered service marks of Applied Trust. All other trademarks are registered to their respective owners.