



White paper
on
Centralized Log Management using SapphireIMS

by

Deepa Sathyajeeth
&
Swaminathan V



Centralized Log Management

Events and Log messages are considered as a critical information career. Managing the events in an effective manner and analyzing the data is critical to protect the IT environments from the potential failures. The vast amount of data being logged makes it impossible for the IT administrators to analyze each and every record manually. The manual process is prone to human-error as well. Mission critical applications use system based logging features to indicate critical failures or potential upcoming problems and it's important to have a good watch on the same.

Efficient log analysis and timely corrective action reduces:

- System downtime
- Increases Network/System/Application performance
- Tighten security policies

As business dependency over IT grows, organizations require a more structured approach towards log management. Organizations does require good log management tool to meet the host-based [security information and event management \(SIEM\)](#) objectives and adhere to the demands of regulatory security compliance requirements.

There are various types of logging methodology being followed based on the types of operating system/device. Windows based systems use 'Event Log', Unix based and Networking devices use 'Syslog' for the logging purpose.

Good log analyzer should have the capability to monitor standard log approaches. They are

- Event Log
- Syslog
- SNMP Trap
- INTEL AMT Event log
- Custom / Application Event log

Event Log: System administrators use event logs as a critical source to troubleshoot performance problems on hosts across the network. Event logs are a valuable source to monitor network security and performance that are often under-utilized due to their complexity and volume. Auditing security event logs is an important part of network security. Microsoft recommends auditing your event logs in its Security Operations Guide for Windows 2000 Server. However, this is easier said than done. Windows NT/2000 is good at collecting security data, but analyzing the data is complicated and has the following limitations:

- No real time monitoring and notification - Windows NT/2000/XP has no way to notify you of suspicious activity.
- Fragmented audit trail - Each computer on the network has its own security log. If you monitor the domain-controller security logs only, you can't get a complete picture of your network's security status. Windows NT/2000 logs



many of the most important security events only on workstations and member servers!

- No long-term archive - Regulatory agencies and public auditors assign a high value to the ability to follow audit trails back in time.
- Insecure log files - Windows NT/2000/XP auditing can be disabled.

Syslog: Syslog is typically used for computer system management and security auditing. Syslog is supported by a wide variety of devices and receivers across multiple platforms. Because of this, syslog can be used to integrate log data from many different types of systems into a central repository

SNMP Traps: SNMP traps are a powerful network management tool to alert network administrators to potential network security violations or disruptions such as authentication violations, network equipment failure, network configuration changes, equipment self-test results, and excessive error conditions

INTEL AMT Event Log: Intel Active Management Technology is relatively newer management technology in the Industry and provides an easy manner to manage the INTEL systems in a unified manner. It generates event logs and can be monitored as well for information about that system.

Custom Application Logs: Applications create their own log files without using Syslog or event log for logging purpose. Due to the critical dependency over these applications, businesses need to keep a watch on the log messages to avoid any potential problems.

Sapphire IMS allows you to manage the logs in a centralized manner through dynamic retrieval / collection, filtering and intuitive display of **EventLog**, **Syslog** and **SNMP traps** from hosts such as windows, routers, switches, Unix hosts and any other syslog enabled devices.

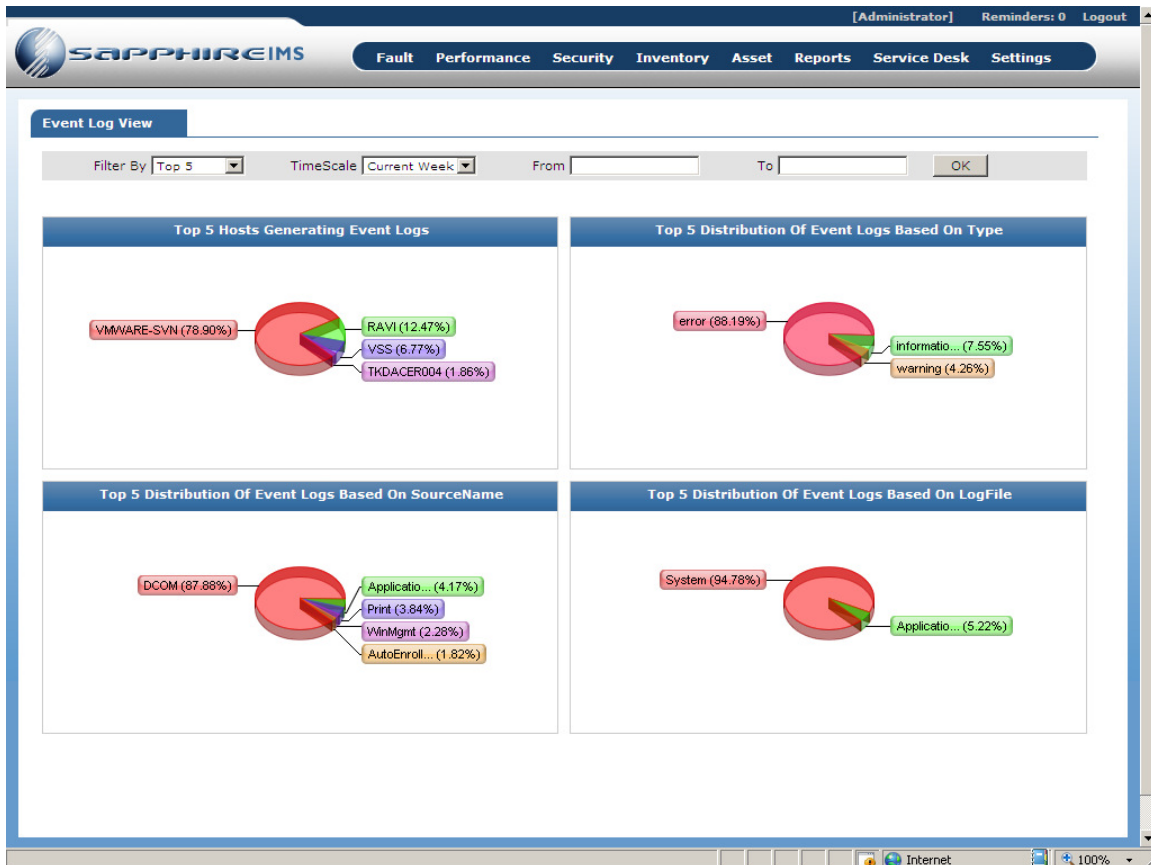
SapphireIMS provides scalable and cost effective centralized log management that can collect and log data from various sources. This provides the ability to identify security breaches, hacker, intrusion and virus activity that could potentially be crippling valuable corporate assets and helps network administrators analyze system problems, improve network security, and reduce downtime of servers, workstations, domain controllers, switches, and routers of enterprise networks.

SapphireIMS log monitoring has an agent-less architecture that uses built-in engine to retrieve the event logs & receive Syslog messages obtained from all the configured devices. SapphireIMS uses MySQL database for storage and archival all logs collected at periodic intervals. With advanced data filtering and log management, SapphireIMS helps administrators manage and report on event logs, syslog and SNMP Traps across the enterprise, in a simple and effective manner.

How can SapphireIMS help you?

- Identify applications and systems that may not be functioning optimally

- Identify unauthorized access attempts and other policy violations
- Understand security risks in the network



Features and Benefits

Scalable Solution – collects application, system, and security event data from enterprise-wide Windows systems, syslog and SNMP Traps from UNIX systems, Routers and Switches, and other Syslog devices. Automatically stores them all in a centralized log database.

Real-time Alarms & Automatic Notification – Alerting allows you to set the specific criteria on hosts for which you need to be notified.

Powerful Multi-level Filters -- SapphireIMS provides powerful event search and filtering engine. You can easily filter events in the list by any criteria like time, event type, severity etc.

Security Analysis – identify unauthorized and failed logins, and malicious user(s). Set alerts for suspicious hosts, and monitor events exclusively.

Built-in Database –integrated MySQL database is already configured to store all log data. No external database configurations are needed.

Event Log View

Severity: All | Log File: Application | From: 2008-11-24 00:00 | To: 2008-11-28 00:00 | OK

Site: All | System: All | Source: All

Host	Message	Source Name	Severity	Time
RAVI	Automatic certificate enrollment for local system failed to contact the active directory (0x8007054b). The specified domain either does not exist or could not be contacted. Enrollment will not be performed.	AutoEnrollment	❌	2008-11-27 19:32:23.0
TKDACER004	Automatic certificate enrollment for local system failed to contact the active directory (0x8007054b). The specified domain either does not exist or could not be contacted. Enrollment will not be performed.	AutoEnrollment	❌	2008-11-27 18:25:23.0
VSS	Automatic certificate enrollment for local system failed to contact the active directory (0x8007054b). The specified domain either does not exist or could not be contacted. Enrollment will not be performed.	AutoEnrollment	❌	2008-11-27 18:21:29.0
RAVI	Automatic certificate enrollment for local system failed to contact the active directory (0x8007054b). The specified domain either does not exist or could not be contacted. Enrollment will not be performed.	AutoEnrollment	❌	2008-11-27 18:21:29.0

Supported Operating Systems

SapphireIMS can collect and report on event from the following operating systems and devices:

- Windows NT/2000/2003/XP
- Linux
- UNIX platforms
- Switches and Routers
- And, Other Syslog devices

For more details about centralized Log management solutions, please contact sapphire@tecnodreams.com or visit <http://www.sapphireims.com>