How network admins can make connections with log & event manager
For a complete picture of what’s going on in your network, look beyond the network itself to correlate events in applications, databases, and middleware.

The larger and more compartmentalized an organization is, the less likely it is for network administrators to have direct responsibility for applications, databases, and network security (except to the extent that security “is everyone’s job”). Yet in implementing Security Information and Event Management (SIEM), security professionals have learned to use tools like SolarWinds® Log & Event Manager (LEM). This tool is not only essential for investigating security incidents, it is also powerful enough to be used for many more applications.

Network admins owe it to themselves to learn enough about SIEM to put it to work for both security and troubleshooting purposes.

What makes a good SIEM tool different from all the other management and monitoring tools you have is its breadth. LEM pulls together logs from network devices, identity management infrastructure such as Active Directory®, Web servers, application servers, and virtually every other system that records system events. Then LEM normalizes the data into a common taxonomy that allows you to browse events in real-time, spot correlations, and search the history of interactions across devices, networks, operating systems, and applications.
LEM could be the key to finding the answer faster the next time you’re wrestling with the question, “Is the problem with the network or the application?” LEM lets you start with one simple fact, such as discovering the IP address of a server that is not performing properly. It then helps you retrieve a set of correlated events. Rather than cycling through a list of specialized tools for network, application, and database monitoring, use LEM to get a snapshot of all of them together. You can then go back to those other tools as necessary.

For example, a search that starts by looking up an e-commerce application server by IP address and sorting through correlated events might show that the problem was neither the application nor a network failure. Instead, you discover several Duplex Mismatch errors pointing toward a misconfigured switch. If the problem was a misconfigured router, log analysis would provide clues to that issue, too.

SIEM lets you correlate between events recorded in different logs for related systems. This is significant because attackers often exploit multiple vulnerabilities on separate but connected systems. With today’s distributed applications, the challenge of troubleshooting more routine failures or slowdowns is not so different. The breakdown often lies in the connection between two systems, rather than in one or the other.
You can do this the hard way or the easy way.

LEM’s nDepth Explorer lets you search log data and discover correlations between events.

Many network administrators might dig into logs the hard way. They rely on grep, Perl scripts, and regular expressions, which may require writing scripts or programs to extract even the most basic information. Locating that information is challenging, especially if you don’t know what you are looking for, or where to look.

To find the data you need, use Log & Event Manager’s nDepth search. You can think of LEM’s nDepth data exploration tool as a search engine for system logs. LEM also includes a reporting engine for retrieving data you consult on a routine basis.
LEM provides a consolidated database of system and network events compressed into a tamper-proof database. It is normalized and optimized for search, and intelligent enough to help you identify meaningful correlations. For example, you can see the relationships between Web application server and database events recorded in separate logs, and the sequence in which they occurred.

LEM uses a variety of visualization and data discovery techniques, such as word clouds and parameterized searches to help you filter through the inherent noise found in log data. This makes it easier to identify the events that are most important.

Look at any single system event, and LEM lets you see what other events occurred immediately before and immediately after. This allows you to piece together the sequence of events related to a problem. Similarly, you can start your search with the IP address of the Web server front end of a malfunctioning application. LEM also displays log data from related systems, such as the database backend. So even if you were certain that the problem was on the Web server, you would be able to quickly see if the database server has been generating error messages, which would then help guide your search for clues.
Network administrators should become more familiar with LEM, given the role they play with network security. They are often the first to spot suspicious traffic patterns or other signs of a breach, even in organizations large enough to support a dedicated security specialist.

A SolarWinds product manager was demonstrating LEM for a client recently and stumbled across a pattern of traffic being directed through a DNS server outside the firewall. It turns out this was no mere misconfiguration, but a hack designed to misdirect proprietary information outside the organization.

While hacking occurs at every level, from the application to the hardware, attacks targeting the base network infrastructure are among the most insidious. The entire IT team must work together to prevent them, detect them, and shut them down. LEM is great for tracking unauthorized access that might not be “hacking” per se, but might include improper off-hours access by a contractor, or prohibited use of remote access tools such as GoToMyPC on an enterprise network. LEM also pays off in more network-related issues, or those that span networking and security concerns.

Managing virtual private networks: Proper VPN configuration is a security issue as well as a reliability and performance issue, particularly for remote or traveling employees who rely on VPN connections. The two most common network administration requirements are:

- **User monitoring:** Many organizations want routine tracking of logons and logon attempts, particularly for outside vendors with network access permissions. LEM can extract this information from firewall and VPN logs and flag inappropriate access in scheduled reports—or shut it down automatically.
- **VPN connection problems:** LEM can provide real-time alerts with details when a failure occurs at any phase of the VPN connection process.
Change management: If you have been tasked with applying an enterprise-wide change to firewalls and
VPNs, SolarWinds® Network Configuration Manager (NCM) can help you prepare the configurations and
perform a mass update.
Immediately after, you can use your SIEM console to monitor events recorded on these devices, and check
for:
  • Errors, warnings, or exceptions following the push.
  • Negative effects on traffic flow across the network.

You can filter real-time log views for specific ports, IP addresses, and log messages to verify that the change
was successful. Best of all, you can view all device activity in a single console, rather than accessing each
device individually.

Finally, NCM allows you to schedule a search or report following the change, which helps you review the
logs for further verification.

Pinpointing failures: Instead of pointing fingers, a network administrator should strive to pinpoint the real
cause of any problem as quickly as possible. LEM can help. For example, one user complained about how
Microsoft® Exchange server was performing poorly. However, SIEM analysis showed a pattern of constant
disconnects and reconnects on the server. This wasn’t a software problem at all, but a bad network
interface card. Another example involves a remote VoIP service that blamed voice quality problems on the
corporate firewall. The logs proved traffic was coming through
the firewall just fine, and that the problem was a timing issue
on the service provider network due to misconfigured server
ports.
Being able to investigate problems is good, but being able to prevent problems is better. LEM can be configured to detect important events, such as firewall rule changes or port scans, and alert you immediately.

With LEM Active Response, you can also define rules that dictate actions to be performed automatically. For example, Windows® agents can be programmed to restart applications that crash or freeze automatically. Other actions include blocking access from a specific IP address, shutting down a service, or deactivating a user account.

One customer reported saving at least five hours per week after automating the password reset process for its mail server. Instead of waiting for users to request a password reset after being locked out of their account, they configured LEM to detect the lockout condition and automatically initiate a password reset.
LEM ships with a library of suggested Active Response actions, and multiple actions can be applied to a single response. Most customers tend to build rules around sending an alert to a system administrator when an event occurs, but you can specify other actions that should be taken in addition to or instead of an alert, such as automatically restarting an application or suspending the account of a user. Possible actions vary depending on the system in question, but we give you a range of options.

Using Correlation Rules, you can go beyond detecting a single event to watching for patterns within common problems, such as configuration changes that result in network slowdowns. A Correlation Rule might also detect three failed attempts within a 30-second window to log on to a server that manages payroll. In this case, that user’s account could be deactivated, either across a domain or on that local machine.

LEM comes with more than 700 built-in event Correlation Rules, which you can clone and modify as needed.
Think of LEM as a tool to help teams of network, system, application, database, and security professionals act more like one big team. The key to achieving a high-performing, reliable system isn’t to expect perfection, but to improve prevention skills and work to resolve issues faster when things do go wrong.

Network administrators have limited visibility beyond their area of expertise. What we can do is work with them to pay attention to the borders between our specialties so that nothing falls through the cracks.

By correlating data across the entire IT department, we have the opportunity to not merely point fingers but discover the probable root cause of a problem. So instead of saying, “It’s not the network, it’s the application,” you can indicate to where your system administrator peer can start looking by pointing to a specific series of log entries correlated with an application failure.
Although we talk about log analysis, LEM does not rely on the actual text-based log files written to disk. This is partly because text-based log files are too easily altered or deleted. In most cases, LEM data collection agents intercept log data before it is written to disk. This is true of events captured from operating systems, Windows® Active Directory®, major database platforms, ERP, customer service systems, and many other sources, with more than 800 connectors available.

Connectors are designed for a very lean footprint, consuming no more than 2% of CPU in most cases. In the case of network devices, LEM records log messages sent via a syslog and SNMP without the need for an agent.

LEM compresses data by 95% to 98% compared with the original log files. At the same time, data is indexed for retrieval, and normalized to factor out superficial differences between the logs generated by different operating systems, applications, and network devices. This makes it possible to see correlations between events recorded by different, but related systems across your network. The original log data is retained, so you can always refer back to it after finding a significant event with LEM’s discovery tools.

LEM is implemented as a virtual appliance, a ready-made virtual machine image you can run on VMware® ESX® or Microsoft Windows Hyper-V®. A LEM instance includes a hardened operating system and a combination of PostgreSQL™ and the Apache® Lucene™ search engine for data storage and retrieval. Once recorded, data becomes read-only, making it a trustworthy source for audits and compliance review.
PUT LEM TO WORK FOR YOU

The best way to understand how LEM can save you time and aggravation is to try it. Download a free 30-day trial from www.solarwinds.com. Out of the box, you get an easy-to-install virtual appliance containing a database optimized for indexing log data, more than 800 connectors for collecting that data, and extensive libraries of reports and filters, as well as intelligent Correlation Rules. You can have it up and running in about an hour.

As a network administrator, you may be only one of the people evaluating the product while peers are looking at it through the lens of security or application administration. Still, take the time to run a few searches to see what you can learn through consolidated log and event analysis that would be hard to find out any other way. Try applying the tool to troubleshooting if something goes wrong. If nothing goes wrong during the 30-day evaluation period (how likely is that?), maybe you force the issue by simulating a network or application failure during a scheduled maintenance window so you can see how the glitch shows up in the logs.

We think you will find LEM’s value goes beyond security to solving problems of all sorts across the network and networked applications.
LEARN MORE ABOUT LOG & EVENT MANAGER

Or visit solarwinds.com/lem to learn more about the capabilities of Log & Event Manager