

whitepaper

# How to Use Log & Event Management For Fault Diagnosis and Prevention

---

**Greg Ferro**  
Author and Blogger

## How to Use Log & Event Management For Fault Diagnosis and Prevention

*What's the process of diagnosing a network fault? It's one of the toughest questions in IT Operations because there is no single or best way. Our IT infrastructures are multi-layered and integrate many different systems: Networks, Servers, and Applications act together to provide the solution and the underlying problem can change at any time.*

*Often referred to as Security Event Management (SEM), Security Information Management (SIM), or Security Information and Event Management (SIEM), log and event analysis can provide a strategy for fault diagnosis and prevention. This paper looks at satisfying these with what we will refer to as log and event management.*

### Fault Diagnosis

At a high level, the process of handling a fault breaks down into four steps:

1. Find it
2. Fix it
3. Diagnose the root cause.
4. Prevent the fault from happening again

A log & event manager can be either a hardware appliance or a software toolset that assists you with the collection, analysis, and diagnosis of log data from your network devices, applications, and systems. This log data can then be used to detect and troubleshoot network related issues. When customers and users are offline, there is tremendous pressure on IT staff to rapidly locate the source of and start fixing the problem. Log and event management can improve your reaction time by providing an answer to "Where do I start troubleshooting?"

Each system in your infrastructure logs information by default and those logs contain important clues to be used to reactively and proactively solve problems. Fault finding by manually moving from system-to-system to hunt and cross-reference log data is hard, inefficient and delivers poor outcomes. Log and event management products give you a chance to centralize all your log data into a single location, automatically analyze the data and spot trends that could result in issues.

### Find it

Log and event management helps you respond to security, operational, and policy-driven events immediately and minimize the impact to your users. As previously discussed, knowing where to start looking can be as difficult, if not more, than actually fixing the problem. The good news is that all parts of your infrastructure such as the operating system, network equipment, and even application software generates log files that can provide information that you can use to locate the problem.

Where solutions differ from each other is in their ability to correlate the log data with detected anomalies and issues in your infrastructure and then present them in an easy-to-understand format with clearly defined actions. Solutions that present simple search bars hardly satisfy this need. After all, if you knew what to look for, you wouldn't need a log and event management product.

## Fix It

Once you have identified the when and where of your infrastructure issues, you need to determine how best to fix it. More advanced log and event management solutions will provide immediate or automated corrective actions such as: quarantining infected machines; blocking IP addresses; disabling user accounts; killing unauthorized processes; restarting services; and more.

A good logging system also shows that the fault is fixed by not showing error messages.

## Diagnose the Root Cause

Your IT infrastructure can be large and complex with many interconnected elements so, once you have found and fixed the problem, you need to know that you have identified the root cause so it can be prevented in the future.

Deeper analysis of the log data through ad-hoc search will allow you to perform detailed forensic analysis on events. Search capability across different vendors varies from a basic search toolbar to advanced search that takes advantage of visual data representation.

## Prevent the Fault From Happening Again

Once you have resolved a problem for the first time, there is a good chance that either you or management will want to know that the problem won't occur again or that you will be better prepared next time it happens.

A log and event management system can assist in both fault prevention and fault handling by creating rules for common conditions and correlating those in real-time so you get immediate visibility into potential issues. Examples of correlation rules may include: verify that a firewall is working by measuring flows against a specific pattern; looking for SNMP polling alerts; or looking for application failure logs on your Windows server.

Alerts and automated responses provide a mechanism for immediate action, thereby reducing potential downtime. A log and event system should be able to monitor for specific log messages and then create alerts and take action based on a set of pre-determined rules. Examples of alerts and actions may include: send an alert to the help desk or system operations center with a custom message that helps with the cause of the problem; or to notify and then restart a service or application.

## How SolarWinds Can Help

### Virtual Appliance Means You're Up and Running Faster -

SolarWinds Log & Event Manager (LEM) delivers powerful log management capabilities in a highly affordable, easy-to-deploy, virtual appliance that eliminates the hassle of configuring databases, servers or operating systems ensuring that you can be up and running quickly. LEM provides you a set of 300 predefined templates for log monitoring and analysis so you can start to make sense of the logs quickly and easily. LEM provides automatic support for well-known log types including; Microsoft; Cisco; CheckPoint and many more. These templates, developed from customer reports and requests, are also a starting point for developing your own customized rules in a graphical web interface.



**Know Immediately When Issues Occur** - LEM includes a patented correlation engine that is real-time, in-memory, non-linear and multi-dimensional meaning that you will know immediately if there is an issue in your infrastructure. With LEM's correlation engine you can: send notifications and trigger actions based on event correlation; perform multiple event correlation; and set independent thresholds for activity per event or group of events. LEM comes with over 700 built-in event correlation rules so you can get started immediately.



**Visual Search For Quicker Troubleshooting** - LEM's advanced IT search functionality is built around a point-and-click graphical web interface that allows you to explore your data visually using word clouds, tree maps, bubble charts, and histograms. As you move through your log data, options for searching and sorting are exposed to you in the U/I and the responses to your queries are intuitively displayed. While a command line interface can be powerful; it requires significant effort and time to reach mastery and works best when you know what to look for. The graphical interface of LEM provides better opportunities to rapidly move into and out of interesting data in the log files, and to verify log files from different devices. It's far superior at problem solving the unknown by providing guidance on how to use the system and better feedback as you progress through narrowing the search.



**Take Automated Responses** - Using a library of built-in Active Responses, LEM executes automated responses needed to mitigate threats and respond to security, operational, and policy-driven events. LEM includes a library of actions including: quarantining infected machines; blocking IP addresses; disabling user accounts; killing unauthorized processes; restarting services; and more.



**Point-and-Click, Drag-and-Drop** - LEM's intuitive graphical user interface is the foundation for its' ease-of-use. Leveraging drag-and-drop, and point-and-click features, users can easily sort through all of their log data without having to learn complex query languages. Whether you need to build rules, create custom filters, or simply explore data to get to the bottom of a sticky problem, the visual nature of this interface will save you countless hours.

Download a fully functional, FREE, 30-day trial and see how SolarWinds LEM can be the foundation for your fault diagnosis and prevention.


## About the Author

Greg Ferro is a consulting network architect and senior engineer/designer. He has more than 25 years of experience in IT and more than 12 years of experience in networking. He is Cisco CCIE#6920. His current focus include data centers, security and application networking. He has worked for financial institutions, service providers, resellers and other verticals. Ferro also writes for Network Computing, blogs about networking at [etherealmind.com](http://etherealmind.com) and hosts the weekly "Packet Pushers Podcast" at [packetpushers.net](http://packetpushers.net).

## About SolarWinds

SolarWinds (NYSE: SWI) provides powerful and affordable IT management software to customers worldwide - from Fortune 500 enterprises to small businesses. The company works to put its users first and remove the obstacles that have become "status quo" in traditional enterprise software. SolarWinds products are downloadable, easy to use and maintain, and provide the power, scale, and flexibility needed to address users' management priorities. SolarWinds online user community, <http://thwack.com>, is a gathering-place where tens of thousands of IT pros solve problems, share technology, and participate in product development for all of the company's products. Learn more today at <http://solarwinds.com>.

*For additional information, please contact SolarWinds at 866.530.8100 or e-mail [sales@solarwinds.com](mailto:sales@solarwinds.com). To locate an international reseller near you, visit [http://www.solarwinds.com/partners/reseller\\_locator.aspx](http://www.solarwinds.com/partners/reseller_locator.aspx)*

Did you like this white paper? Tweet about it.  <http://www.twitter.com>