Sponsored by NetIQ

NetIQ Sentinel 7 Review

January 2012

A SANS Whitepaper

Written by: Jerry Shenk

Executive Summary

Over the past seven years, the SANS Institute has conducted a yearly log management survey that has tracked steady improvements in log collection and management. In the early days, respondents reported having difficulty collecting logs; today's challenge, however, is analyzing all the data organizations collect from an ever-growing variety of logs.

In the SANS 2011 Log Management Survey, the majority of companies reported that they were still having problems reporting and analyzing their log data (particularly data from Windows devices). They also indicated they would like more timely alerting capabilities.[1] Respondents further reported that they didn't have the time needed to allocate to log management.

This paper is a functional review of the latest NetIQ offering in the Security Information and Event Management (SEIM) space that effectively addresses these and other issues organizations are having with their logs. The product, NetIQ® Sentinel™ 7 (formerly Novell® Sentinel™ 7), is a culmination of more than a decade of Novell SIEM and log management experience that brings together log management and real-time SIEM in a single product and interface. NetIQ Sentinel correlates events against a variety of log sources with nominal latency and provides strong reporting, search and trend-analysis capabilities. The convergence of the product's log and security event management functionalities also provides the security intelligence that organizations need to act in near realtime against classified threats.

NetIQ also addresses problems arising from lack of IT resources by providing a 90-day free trial of its NetIQ Sentinel SIEM product, which organizations can have up and running quickly. This free trial removes much of the risk barrier associated with buying products and installing them before trying them out in the enterprise environment. Sentinel is simple to set up and make functional, yet it provides powerful features that can make even seasoned log analysts more effective and efficient. Perhaps best of all, it comes in an easily deployed virtual appliance that was collecting log events in about 12 minutes on our first setup attempt! This version of NetIQ Sentinel includes a number of default reports that are designed for a quick read, such as the Authentication Report, which includes a timed graph, a pie chart (located at the top of the report) and color-coding for quick visualization.

As is often the case with technology installations, the biggest problem with NetIQ Sentinel was the product's documentation. Its *Quick Start Guide* helped us get the system up and running quickly. However, getting some of the advanced features working took some research, and the product documentation was at times hard to follow. The large number of available options is partly responsible for this difficulty. Although information about the options was generally available, the details were sometimes dispersed over a few different files, requiring us to search through all of them. NetIQ is improving Sentinel documentation as a result of this feedback.

1 www.sans.org/reading_room/analysts_program/logmgt-survey-web.pdf

Fifteen Minute Set Up

NetIQ Sentinel 7 is a breeze to set up. Most users can begin collecting logs in less than 15 minutes. Maybe Sentinel is cheating a little because it is available as a virtual appliance. Then again, maybe it's not cheating, because ease of use and set up are key factors in reducing log- and event-management overhead.

NetIQ has provided a variety of packaging options for NetIQ Sentinel 7. The company offers virtual appliances for VMware, Hyper-V and XEN virtualization environments, a soft appliance you can install directly on dedicated hardware, and a more traditional software package. NetIQ delivers VMware and XEN virtual appliances as preconfigured virtual machines with an embedded Linux-based operating system (OS). The soft appliance is a DVD ISO (International Organization for Standardization) image that installs the combined software and OS directly on your organization's targeted hardware. Finally, NetIQ delivers an RPM-based software installer for installation on a customer-provided SUSE® Enterprise Linux or RedHat Enterprise Linux host. Although this review is based on the VMware virtual appliance, the installation process is very similar for other Sentinel options.

In this review, our NetIQ Sentinel 7 server was running as a VMware guest on a Windows 7 host machine. The Windows 2008 Server that hosted the Windows Event Collection service was also running as a guest OS. This Windows 2008 server was also an event source. Two other Windows event sources in our lab were running Windows XP. The remaining event sources were a Cisco 877 router, a Cisco PIX firewall, a Cisco 3600 router, and a Linux firewall running iptables.

You can download the NetIQ Sentinel virtual appliance for VMware from the NetIQ website.[2] Because NetIQ Sentinel was formerly branded under Novell, some of the filenames and documentation still reference Novell. The documentation, however, fully applies to the NetIQ products. The current VMware appliance is available as a gzip file named **sentinel_server_7.0.0.0.x86_64-0.623.0.vmx.tar.gz**. In our test, the VMware host ran the Windows operating system and the guest NetIQ Sentinel server ran SUSE Linux Enterprise Server. Default tools on the Windows computer could not extract the file. To install the file on a VMware host running on Windows, you'll need a utility such as 7-Zip[3] to unpack the file. The **.gz** (gzipped) file contains a file named **sentinel_server_7.0.0.0.x86_64-0.623.0.vmx.tar**. Files with the **.tar** extension are familiar to UNIX and Linux operators, but are less recognizable by Windows operators. The tar format provides a way to combine a number of files into one. Using 7-Zip, we double-clicked on the 1.6 GB **.tar** file and opened a directory or folder, which took a few minutes. We then copied the file to the directory or folder that stores other virtual machines, which created a folder named **sentinel_server_7.0.0.0-0.623.0**.

If you do this and double-click the file named **sentinel_server_7.0.0.0.x86_64-0.623.0.vmx**, the virtual machine should start the SUSE Linux server and the NetIQ Sentinel 7 processes. NetIQ has noted our experience and is planning an update in the near future that will streamline this process even more.

2 www.novell.com/products/sentinel

3 www.7-zip.org/download.html

After getting answers to a few basic configuration questions, the NetIQ Sentinel 7 server was ready to accept log data. During the initial boot, we saw a number of basic setup questions that were fairly standard with any setup: questions about the language, keyboard, license agreement, and so forth. In our case, there were two license agreements—one for the SUSE Linux Server and one for NetIQ Sentinel 7.0.

One default option to change before putting any log server into production is the Internet Protocol (IP) address. By default, this is set to use Dynamic Host Control Protocol (DHCP). For a log server, you'll want to use a static IP address.

The NetIQ Sentinel 7.0 *Quick Start Guide* is definitely worth reading during setup. Under the "Installing the Appliance" section, the guide mentions setting up Network Time Protocol (NTP). Having a good time source is important for a log server, so we installed NTP during setup. You can change the time source later if a good time source isn't available at initial setup time.

After picking an NTP server, we used the Configure option to change the Start NTP Daemon from Only Manual to Now and on Boot. After setting the time and a few passwords, the system finished the setup script and rebooted. When NetIQ Sentinel 7 came up, the console screen (named Novell Sentinel) displayed the URL needed to access the appliance: **https://[ip_address]:8443**. (If the web server doesn't respond right away, try again in a little bit. It may take a few minutes for background processes and the web server to finish after the login prompt appears.) When the web server responded, it presented a login page, and we logged in using the administrator account and password we'd defined a few minutes earlier. This brought up the main search window, shown in Figure 1.

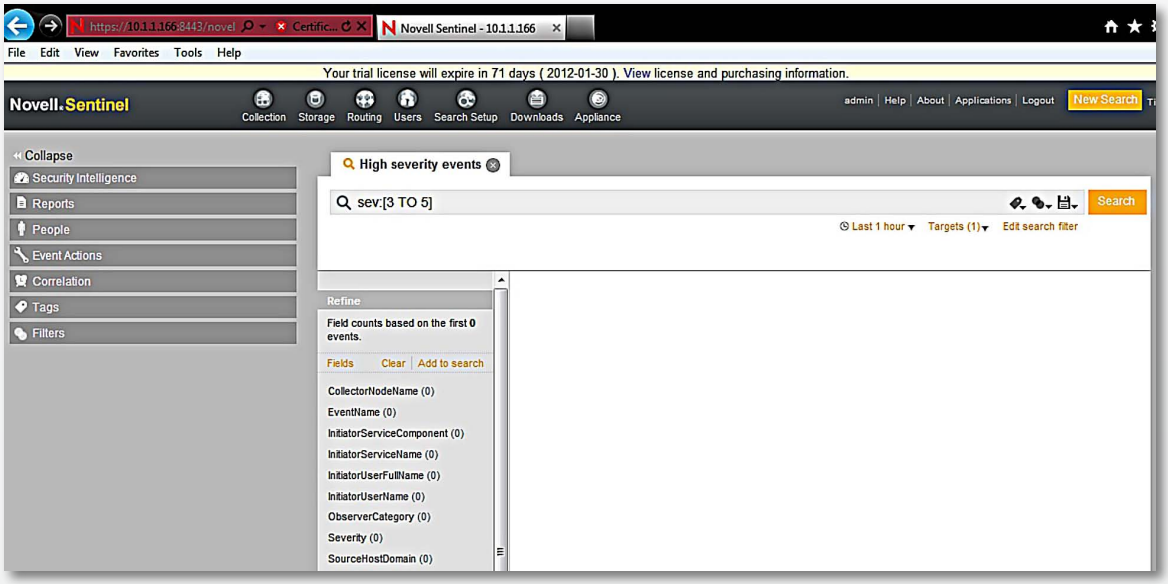


Figure 1. NetIQ Sentinel 7 Main Screen

The default search criteria, **sev:[3 TO 5]** (see Figure 1), enabled us to search for all events with a severity of 3 to 5. For our initial test, we changed the 3 to 0 so that we would see all events. We immediately saw events from the local NetIQ Sentinel server. This demonstrated that the NetIQ Sentinel server was collecting events and cataloging them.

To get something a little more interesting, we telneted to the Sentinel server on port 1468 (**telnet 10.1.1.166 1468**) of the test server, typed testing and pressed Enter. (Note: If the telnet command fails, then your machine is probably running Windows 7 or later, in which case telnet is not installed by default; install it using this command: [**pkgmgr /iu:"TelnetClient"**]. Include everything between the brackets, including the double-quotation marks, then try the telnet command again.)

We entered "**testing**" in the search string (note the double-quotation marks), and clicked the Search button. This pulled up the log entry that our telnet action had just created. When we clicked the More link, we got a window showing the message (testing), the IP address, the timestamp of the message and the retention time of this event (see Figure 2).

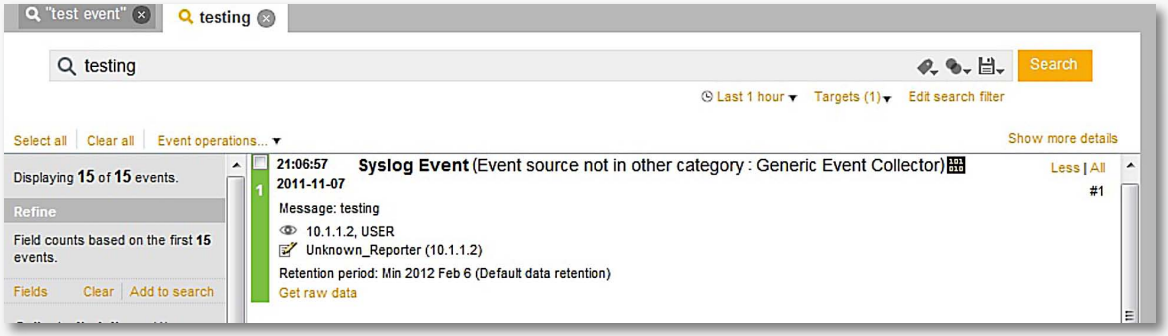


Figure 2. Detail of Logged Event

With this log detail, we verified that we had a working log server. Twelve minutes had passed from the time we double-clicked on **sentinel_server_7.0.0.0.x86_64-0.623.0.vmx** to the time we had an event logged from an outside connection. This included the time it took to read the quick-start documentation and methodically go through the entire step-by-step process.

Other means of connecting are also available in the Sentinel product. We used Transmission Control Protocol (TCP) port 1468 to send log data over TCP; but the most popular port for transporting log data is User Datagram Protocol (UDP) port 514—the old standard syslog port. If you have Netcat[4] or something else that can generate a UDP connection, you can try this port as well. You can also configure routers, firewalls, switches and servers to send syslog data to the Sentinel server's IP address.

4 www.downloadnetcat.com

Windows Log Data

According to the SANS 2011 Log Management Survey, handling Windows log events is a big challenge for a lot of IT administrators. In fact, over the past few years, respondents said they weren't too happy with their Windows log management capabilities. NetIQ Sentinel supports at least two ways of collecting Windows log data. One way is to put a collection service on a server, convert the Windows events to syslog events and send them to a log server over UDP port 514. Sentinel also includes a Windows Event Collection Service (WECS) that runs as a service on a Windows 2008 R2 64-bit system and defaults to forwarding security events to the log server.

The WECS server can reach out and pull events from event sources that include Windows Server 2003 SP2, Windows XP SP3 and more recent operating systems. When you configure WECS to pull events from the event sources, it then sends them to the Windows event connector process that would typically be running on the Sentinel server.

Windows Event Collection Service

During installation, the interaction between collectors, connectors, collection services and event sources was a little confusing. Once we got it, however, it wasn't too bad. Figure 3, which we took from the WECS section of the Sentinel documentation, shows the path from Windows event sources to the Sentinel log server.

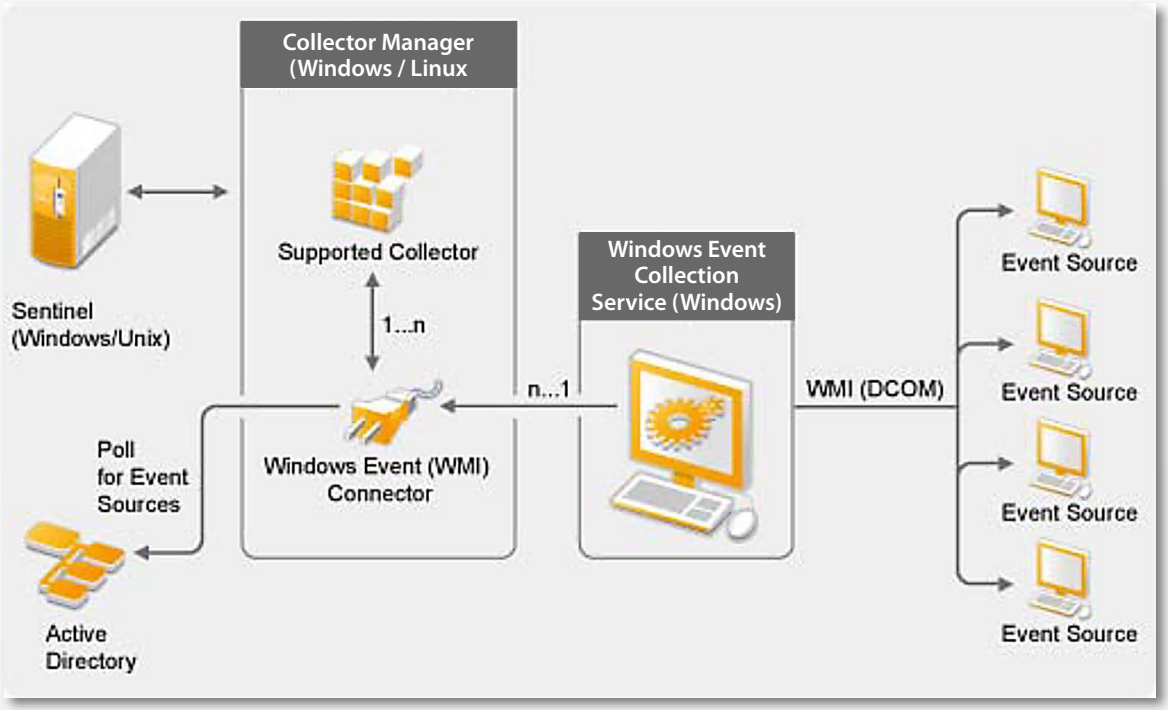


Figure 3. WECS Event Path

WECS is not installed by default, and installation requires downloading the plugin from NetIQ's website. Before proceeding, we grabbed another snapshot of our virtual machine, which came in handy during installation. The terminology to get WECS set up was a little confusing and caused a few starts and stops. The snapshot provided an easy way to roll back when we, ultimately, made installation mistakes. See the Appendix at the end of this review for details about these mistakes. The NetIQ Sentinel 7.0 *Quick Start Guide* step-by-step instructions for configuring WECS (also known as the Windows Management Instrumentation [WMI] connector). WECS uses the WMI infrastructure to authenticate to Windows event sources and pull down log data. Additional, more detailed documentation is included with the WECS plugin.

Windows Events with Syslog

Another option for collecting events from Windows computers is to use a syslog redirector. These software agents run on each Windows event source (that is, the Windows computers that generate the events). One popular option that Sentinel supports is the Snare Event Log Agent,[5] which forwards events to the syslog server over UDP port 514.

Windows Events Monitoring

Upon receiving the Windows events, Sentinel automatically detected the types of events that were recorded. With Sentinel log-event normalization, you can detect similar events on multiple platforms from a single report (rather than detecting them the old way, by weeding through multiple reports of the same instance).

For example, a report named Sentinel Core Password Changes is designed to make it easy to track password changes. We were able to run the report and collect password changes from the Windows 2003 server, XP workstations and a Windows 2008 server. Even though these events all happened on Windows devices, they were logged quite differently and had different Windows event ID numbers. A Snare agent running on an older server transported some events, and others came through the NetIQ WECS process. NetIQ Sentinel normalized and correlated the events.

5 www.intersectalliance.com/projects/BackLogNT

Event Correlation and Alerting

Log collection and management have progressed over the last ten years or so, moving from simple log collection with manual review, to automated review that looks for key pieces of information, to automated review with event correlation across multiple log sources. NetIQ Sentinel combines log management and SIEM functionality into one appliance, so event correlation can include multiple events and sequences of events as they occur over a period of time. You can program NetIQ Sentinel correlation rules to do much of the repetitive log analyses more efficiently and accurately than is possible with constant manual log review. Event correlation rules can associate with actions—such as sending Simple Network Management Protocol (SNMP) traps, sending e-mail messages, running scripts, or all three (or with any of the many other action options).

This ability to associate makes it possible to automate a high level of correlation and detection with the event correlation in NetIQ Sentinel 7. For example, the sample correlation rule shown in Figure 4 watches for a string of events that include a failed login followed by a successful login within five minutes.

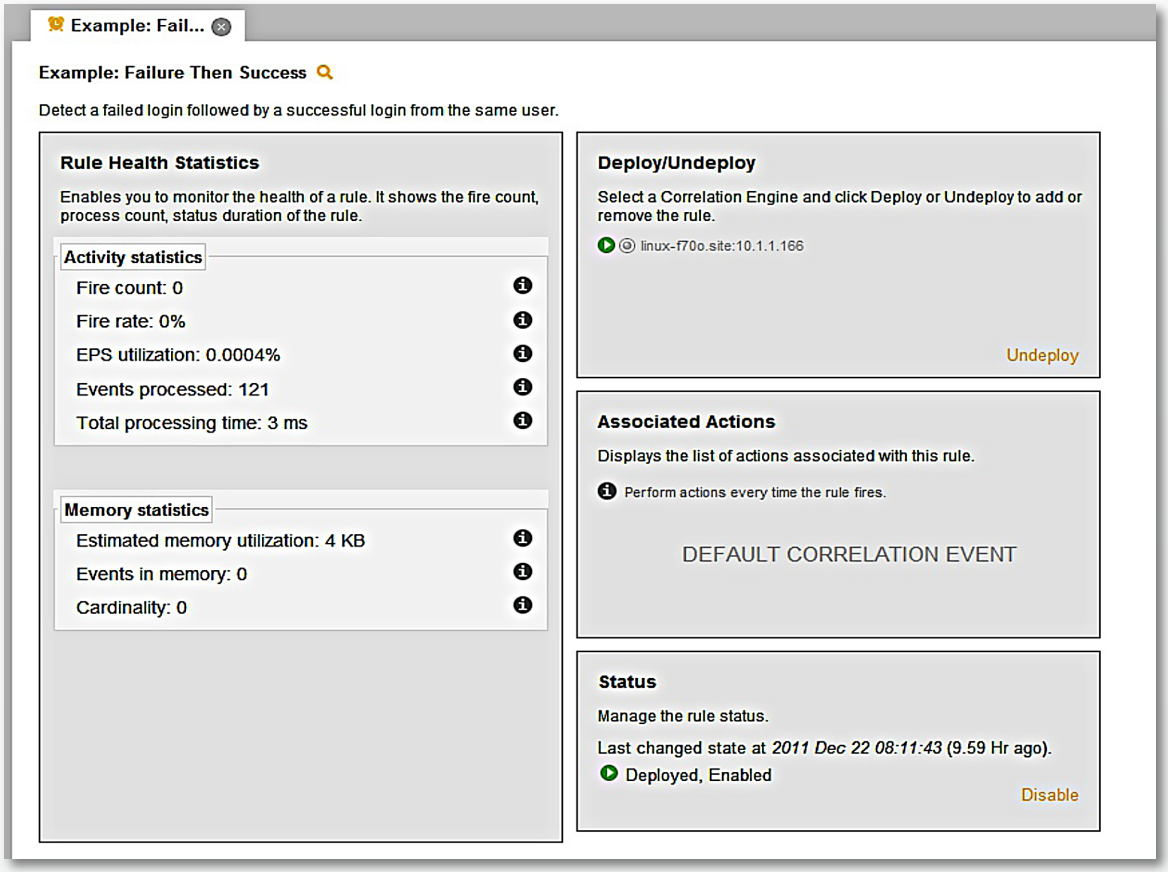


Figure 4. Success after Failure Rule

If a successful login happens within five minutes, the deny rule trips. In our review, an invalid login to our PIX firewall showed up as a deny event. But a failed login to a Windows server got logged as a failure yet didn't match the rule, so we wanted to modify the rule.

NetIQ Sentinel rules are easy to edit. All we had to do was change the first trigger to be either a failure or a deny event. This rule is handy, but people often make mistakes or "fat-finger" their keystrokes, so we raised the number of failures to five to eliminate many of the inevitable false positives. In fact, if somebody is trying to break into an account, he or she will often fail many more times than five, so an even higher number of failures may be acceptable in many environments.

We modified the rule to match after five failures in less than two minutes, followed by a single success within five minutes. If these events happened in order, it would generate an e-mail alert.

When the rule tripped, the e-mail alert contained enough details about what tripped the event that we could make an initial analysis on the event's severity simply by viewing the e-mail message. Figure 5 shows the modified rule.

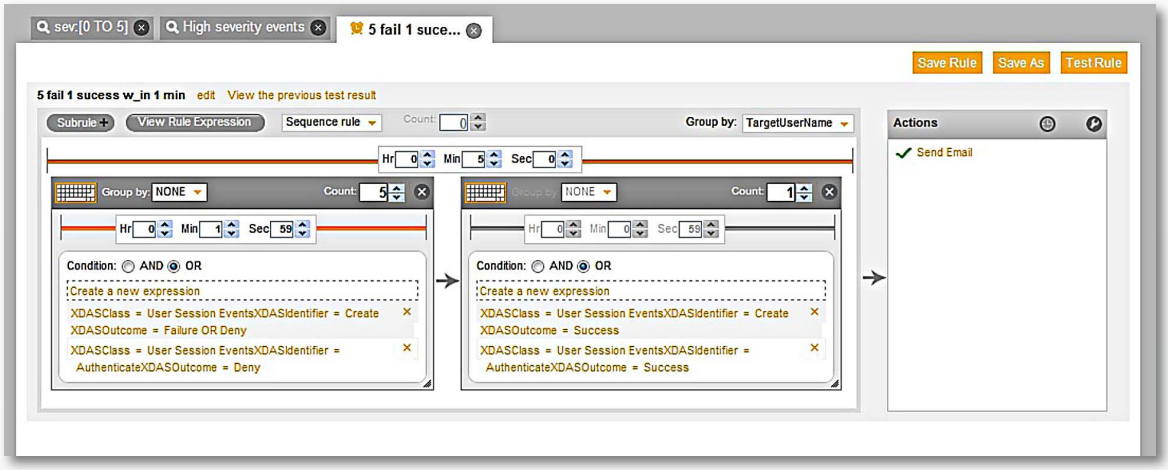
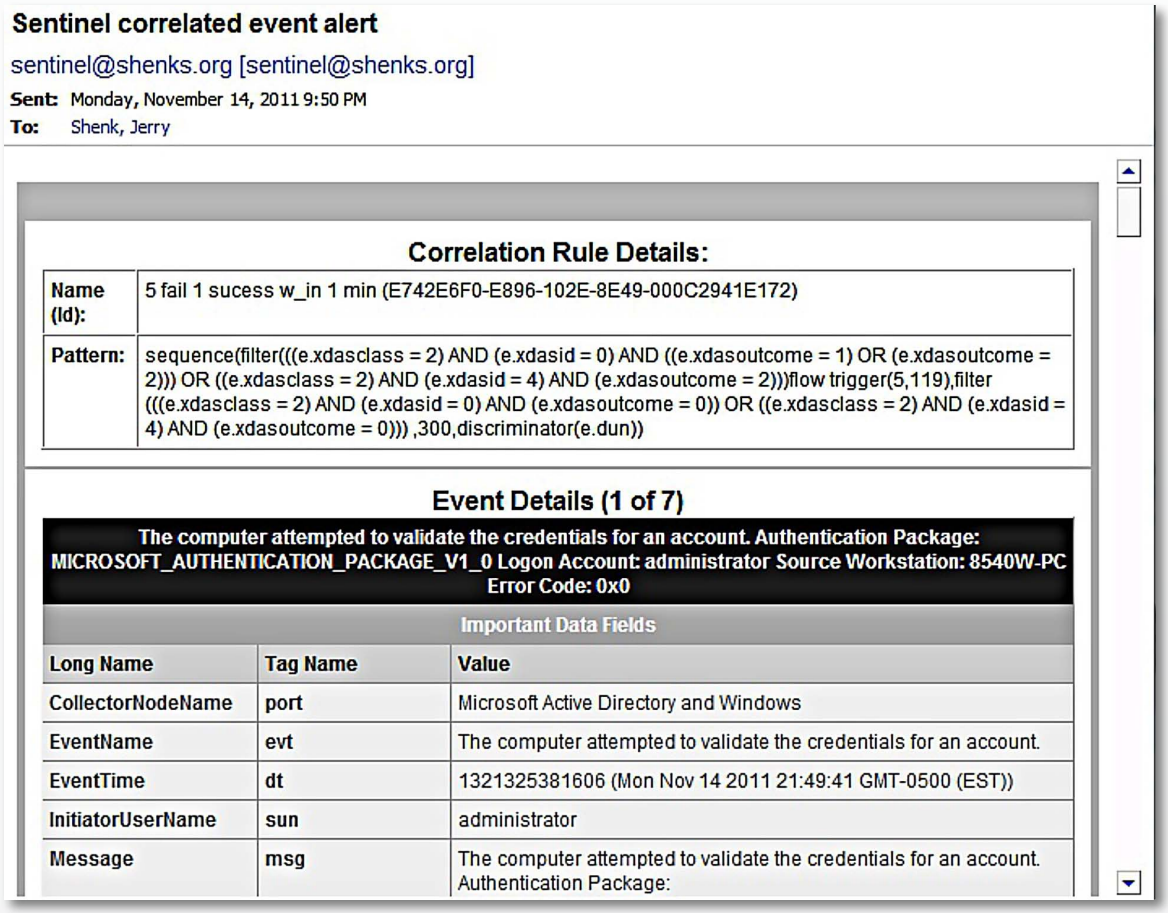


Figure 5. Rule Modification to Reduce False Positives

Figure 6 shows the message this rule generates, including all the details about why the rule tripped, so the recipient can review the message and determine if further research is needed.



Sentinel correlated event alert

sentinel@shenks.org [sentinel@shenks.org]

Sent: Monday, November 14, 2011 9:50 PM
To: Shenk, Jerry

Correlation Rule Details:

Name (Id):	5 fail 1 sucess w_in 1 min (E742E6F0-E896-102E-8E49-000C2941E172)
Pattern:	sequence(filter(((e.xdasclass = 2) AND (e.xdasid = 0) AND ((e.xdasoutcome = 1) OR (e.xdasoutcome = 2))) OR ((e.xdasclass = 2) AND (e.xdasid = 4) AND (e.xdasoutcome = 2)))flow trigger(5,119),filter (((e.xdasclass = 2) AND (e.xdasid = 0) AND (e.xdasoutcome = 0)) OR ((e.xdasclass = 2) AND (e.xdasid = 4) AND (e.xdasoutcome = 0))) ,300,discriminator(e.dun))

Event Details (1 of 7)

The computer attempted to validate the credentials for an account. Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 Logon Account: administrator Source Workstation: 8540W-PC Error Code: 0x0

Important Data Fields

Long Name	Tag Name	Value
CollectorNodeName	port	Microsoft Active Directory and Windows
EventName	evt	The computer attempted to validate the credentials for an account.
EventTime	dt	1321325381606 (Mon Nov 14 2011 21:49:41 GMT-0500 (EST))
InitiatorUserName	sun	administrator
Message	msg	The computer attempted to validate the credentials for an account. Authentication Package:

Figure 6. Sample Correlation Rule

Rule modification was intuitive, and the rule change we made demonstrates the power of correlation. In years past, many log administrators were able to get similar functionality only by using scripts and conducting hours of painstaking testing. NetIQ Sentinel correlation logic makes it easy to do something simple like this and also makes it possible to create very complicated correlation chains to do things that simply couldn't be done with scripts.

Security Intelligence and Trend Analysis

NetIQ Sentinel 7's event correlation includes a new trend analysis feature called *Security Intelligence*. One thing that sets Security Intelligence apart is that analysis continues even when you're not actively viewing the dashboard. An administrator could, then, configure multiple dashboards that will continue to process events even if they aren't being viewed.

For example, we created a custom dashboard that analyzed all events using **sev:[0 TO 5]** as the search criterion. In Figure 7, you can see peaks and valleys in overall event counts. On the right side, you can see trends for other categories.

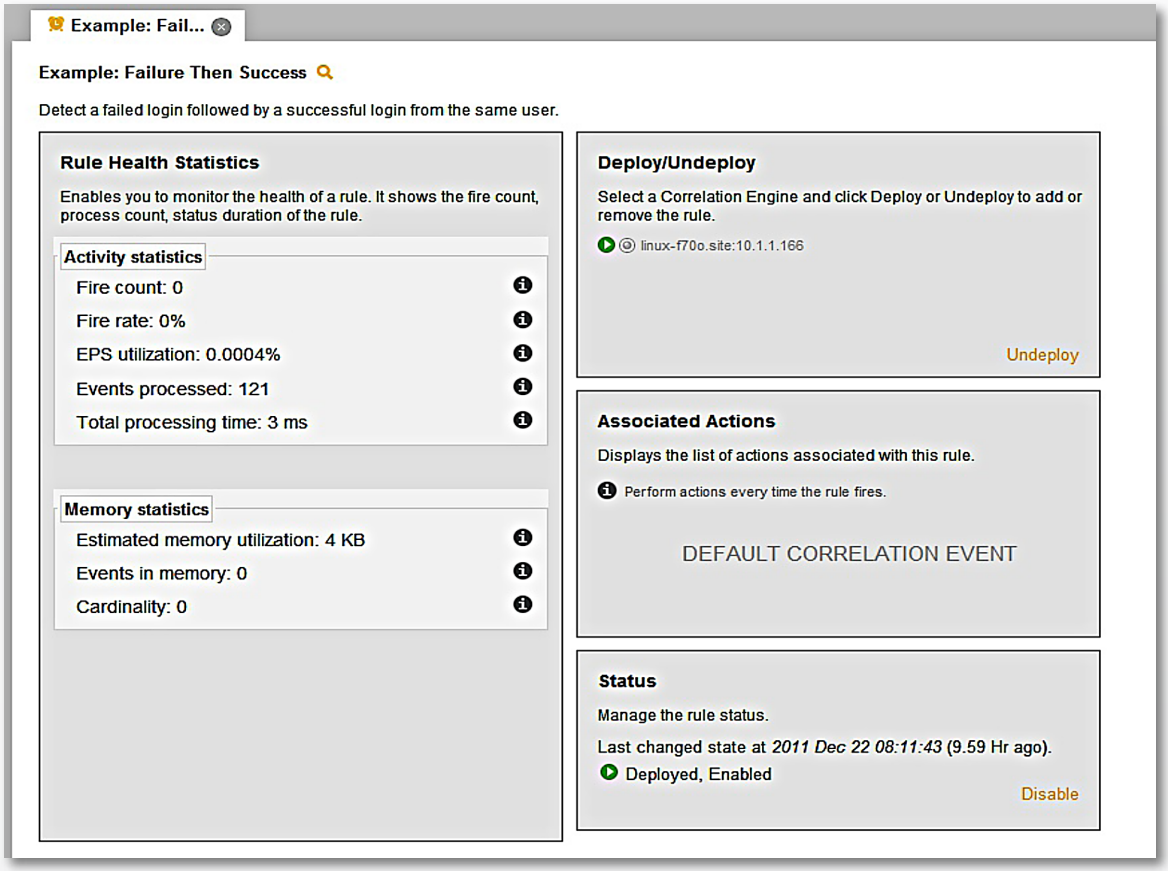
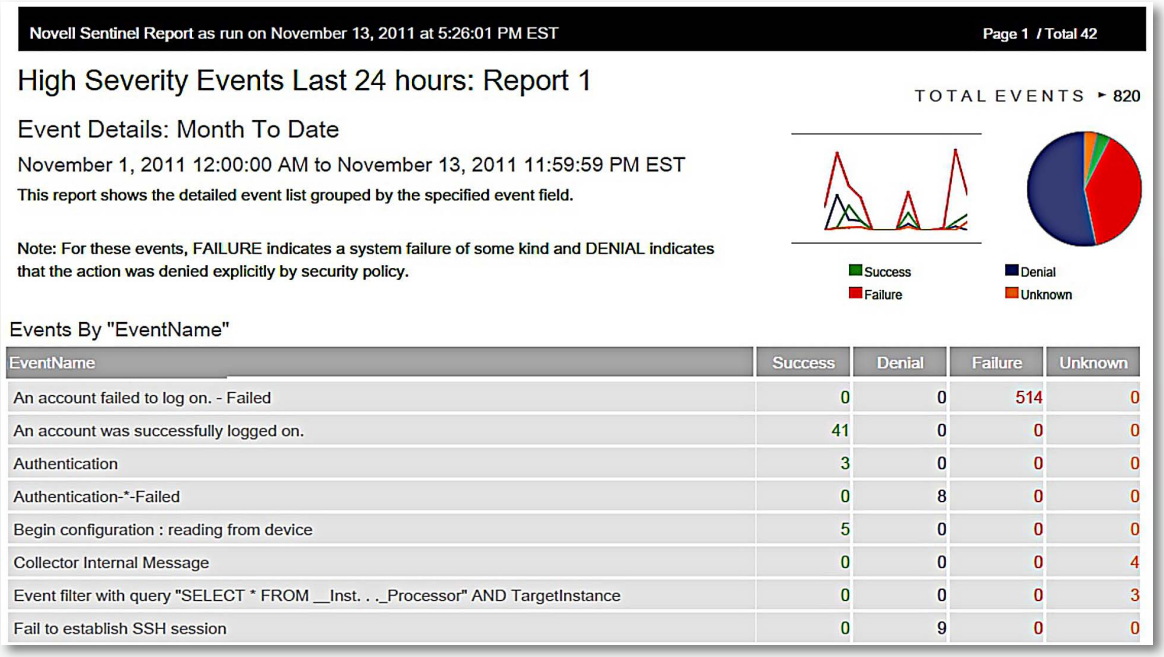


Figure 7: Dashboard View of Events for Trending and Other Purposes

Every SIEM or log analysis program should track overall event counts. If the number of events is excessively high, somebody should figure out why. Low event counts could be just as big an issue—or perhaps a bigger issue. We have checked on too many production systems only to find that they were disconnected, reconfigured or were, for some other reason, not working correctly. Our answer was to set up anomaly detection for our custom dashboard to send out an e-mail alert if the event count dropped to less than five events for any five-minute time interval. This rule allows a little time for reboots and event generators (to which we wanted to make adjustments during this review). We elected to use an overall event count, although we could have selected only specific event categories. We also could have set up a dashboard using criteria that would monitor only specific events, such as events from an IDS/IPS.

Reports

One of the key requirements for any log management or SIEM solution is the ability to get data out of the system and make it available throughout the organization in an understandable format. In addition to providing trending analysis, NetIQ Sentinel 7 comes with a number of reports that organizations need for compliance, network monitoring, error tracking and more. It is also possible to turn results from any search into a report by simply saving the search from the search window. You can run these reports, including the report shown in Figure 8 or any of the included sample reports, on a scheduled basis.



Novell Sentinel Report as run on November 13, 2011 at 5:26:01 PM EST — Page 1 / Total 42

High Severity Events Last 24 hours: Report 1

TOTAL EVENTS ▸ 820

Event Details: Month To Date

November 1, 2011 12:00:00 AM to November 13, 2011 11:59:59 PM EST

This report shows the detailed event list grouped by the specified event field.

Note: For these events, FAILURE indicates a system failure of some kind and DENIAL indicates that the action was denied explicitly by security policy.

Success
Failure
Denial
Unknown

Events By "EventName"

EventName	Success	Denial	Failure	Unknown
An account failed to log on. - Failed	0	0	514	0
An account was successfully logged on.	41	0	0	0
Authentication	3	0	0	0
Authentication-*-Failed	0	8	0	0
Begin configuration : reading from device	5	0	0	0
Collector Internal Message	0	0	0	4
Event filter with query "SELECT * FROM __Inst. . ._Processor" AND TargetInstance	0	0	0	3
Fail to establish SSH session	0	9	0	0

Figure 8. Details of Scheduled Reports by Events

The reports are laid out so you can scan them quickly to determine whether or not they look normal for your organization. In Figure 8, the red-line spikes indicate early morning and late evening periods during which the system experienced a high number of login failures—a clear and easy indicator that there's a problem that needs addressing.

The NetIQ Sentinel reports start with a graph. If the graph looks questionable, check out the next section, which offers single-line summaries that contain more detail. In the sample report in Figure 8, the summary is based on high-severity events—and login failures are the big news. The body of the report contains every event that matched correlation rules.

For example, in our failed-login scenario, the recipient of the report may need to see if there were more failed logins than normal and when the successful and failed logins occurred. They can scroll through the report and see how many logins were associated with each user. That knowledge would often enable them to determine if there was a process problem, an attack on a specific user or an attempt to guess passwords for many users.

Custom Searches

In the previous examples, we searched for well-supported information commonly found in logs (failed logins) on common platforms (Cisco firewalls and Windows computers). Yet nearly every environment includes critical elements that the default normalization of a log server or SIEM never supports, such as legacy or custom applications. This creates a need to scan through log data for ad-hoc information that is not normally reported or included in correlations. NetIQ Sentinel enables you do these custom searches and turn the searches into reports.

To review the customization features, we ran a script named *portsentry* on the Linux firewall to detect packets coming in to commonly scanned ports. In this case, the port being scanned was the port 22, commonly used by ssh. The firewall has an internal IP address of **10.1.1.2**. The following event was logged by portsentry:

> ***Nov 14 19:36:28 firewall portsentry[4852]: attackalert: SYN/Normal scan from host: 172.151.338.175/172.151.338.175 to TCP port: 22***

(The astute reader will recognize that the source address in the preceding character string, **172.151.338.175**, is not a valid IP address—we changed the address to protect the guilty.) To search for this data, we entered **(("attackalert" AND "scan") AND (obsip:"10.1.1.2"))** as the search criteria. This search will find the two words, **attackalert** and **scan**, coming from an observer IP (obsip) of **10.1.1.2**. In this case, the IP address of the host that observed the attack and the destination of the attack are the same. The event is shown in Figure 9.

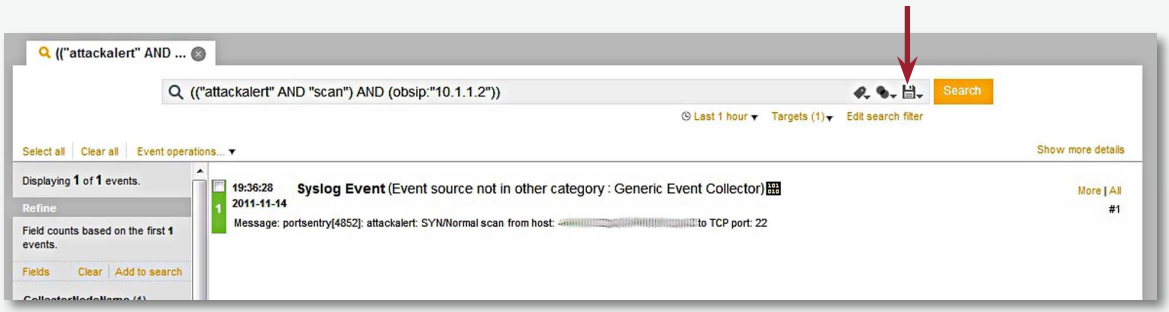
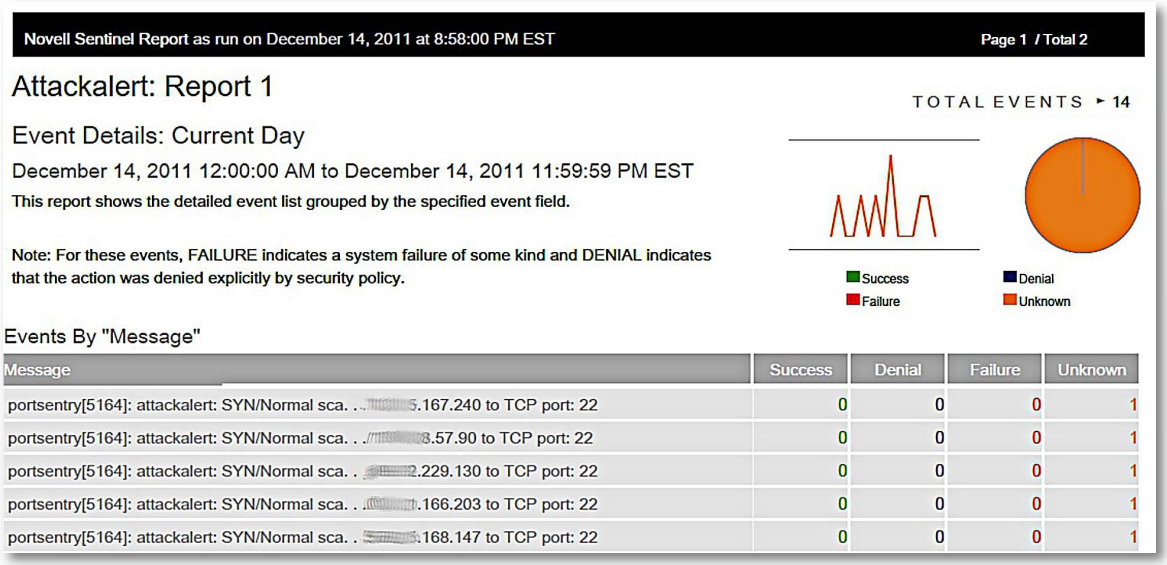


Figure 9. Results from Custom Search

Figure 9 represents a search for this specific information through the previous hour's log data. By clicking on the disk icon at the left of the Search button, we saved this as a report so we could go back and reuse it by highlighting the report, clicking Run and selecting the parameters for the report. We set up the report to be delivered to an operator by e-mail on a daily basis (see Figure 10).



Novell Sentinel Report as run on December 14, 2011 at 8:58:00 PM EST — Page 1 / Total 2

Attackalert: Report 1

Event Details: Current Day

December 14, 2011 12:00:00 AM to December 14, 2011 11:59:59 PM EST

This report shows the detailed event list grouped by the specified event field.

Note: For these events, FAILURE indicates a system failure of some kind and DENIAL indicates that the action was denied explicitly by security policy.

TOTAL EVENTS ▸ 14

Success
Failure
Denial
Unknown

Events By "Message"

Message	Success	Denial	Failure	Unknown
portsentry[5164]: attackalert: SYN/Normal sca. . . .5.167.240 to TCP port: 22	0	0	0	1
portsentry[5164]: attackalert: SYN/Normal sca. . ./.3.57.90 to TCP port: 22	0	0	0	1
portsentry[5164]: attackalert: SYN/Normal sca. . .2.229.130 to TCP port: 22	0	0	0	1
portsentry[5164]: attackalert: SYN/Normal sca. . .166.203 to TCP port: 22	0	0	0	1
portsentry[5164]: attackalert: SYN/Normal sca. . .168.147 to TCP port: 22	0	0	0	1

Figure 10. Scheduled Report Example

The ability to create reports as needed, and the ability to schedule reports containing information that you regularly review, saves time by automatically pushing out this information. You can also e-mail these reports to personnel, such as auditing staff, who would normally not have access to the log management system.

As shown from the reports captured here, the NetIQ Sentinel user interface is intuitive, and NetIQ Sentinel delivers data from multiple log sources in an easily digestible format.

Summary

Novell was in the log management business for over a decade before it was acquired by NetIQ. The new company's latest product—NetIQ Sentinel 7—does a good job of addressing issues expressed by respondents to the SANS Annual Log Management Survey, including providing more analysis from more log sources with reduced complexity and overhead. By combining the features of what were formerly Novell log management and SIEM products into one tool, NetIQ provides a solid product with combined intelligence and alerting, as well as solid searching and reporting features.

You can set up NetIQ Sentinel 7 and have it monitoring logs for a number of devices in well under an hour. For an experienced log analyst, the details needed for reports and analysis are accessible. For somebody new to log analysis, NetIQ has made Sentinel logs manageable with quick, easy set up; built-in reports; and the Security Intelligence dashboard—all included in an out-of-the-box installation.

A nice surprise in reviewing NetIQ Sentinel 7 was the speed at which it started functioning and collecting logs from the devices on our sample network. Our review experience is based on the NetIQ Sentinel 7 virtual appliance, which saves a lot of setup and management time—something respondents to the SANS Log Management Survey said they are short on.

Respondents' bigger issue was collecting data from a wide variety of devices that speak their own logging language. NetIQ Sentinel 7 includes normalization that allows for a single report to include similar events, which we demonstrated with various reports related to failed logins. It was able to normalize and report on these events from a variety of platforms—including Windows, even with all its inconsistencies in log-data formats.

NetIQ Sentinel 7's flexibility to correlate and actively respond to these events is nearly endless using standard methods, such as e-mail, SNMP traps, scripts and quite a few other techniques. NetIQ support staff also say they are constantly working to make NetIQ Sentinel normalization and correlation capabilities even more powerful by supporting and analyzing more types of events from more devices. If the capabilities of their latest offering—Sentinel 7—is any indicator, it looks as if NetIQ will deliver future versions with even more correlative and reporting capabilities to support the growing demands of security, compliance and operations staff.

Appendix: WECS Installation Workarounds

Opening Port 1024 on the Server's Firewall

To conduct this review, we needed to modify the firewall using YaST (Yet another Setup Tool) to open port 1024 for WECS communications. You can use YaST for many configuration tasks, including two that are critical for log servers: changing IP addresses and changing time settings.

According to NetIQ support, another option is to change the WECS process to use a port between 40000 and 41000, because these ports are open on the Sentinel server by default. NetIQ is aware of this setup issue and plans to update the NetIQ Sentinel documentation.

To allow incoming traffic from WECS, we took the following steps:

1. Login to the server as root , type **yast** and press Enter.
2. Access firewall configuration under Security and Users.
   a. Use the Arrow key to highlight Allowed Services, then press Enter.
   b. Press Tab to move to the Advanced option in the lower right corner of the window.
   c. Press Enter to select Advanced.
   d. Press Tab to get to the TCP Ports list.
   e. Add **1024** to the list, then press Tab until OK is highlighted. Press Enter.
   f. Press Tab until Next is highlighted, then press Enter to select Next.
   g. Press Enter to Finish.
3. Press the Tab key until Quit is highlighted, then press Enter to exit YaSt.

Although this description sounds complicated, it was really just a matter of selecting the right screen, adding **1024** and then backing out. NetIQ Sentinel also provides the option to make this change from the appliance's web interface.

Referencing the Username for WECS Authentication

The collector manager runs on the Sentinel server. If we set up additional event sources, they will use the user credentials that WECS uses on our Windows 2008 server. Had we known it earlier in the setup process, specifying the username preceded by a backslash (**\sentinel**) would have avoided authentication problems and saved us from going back and forth with tech support. In some cases, the backslash is not required, but including it doesn't seem to have a downside.

Syntax Needed for the eventManagement.config File

The *Quick Start Guide* does contain thorough step-by-step instructions for installing the collection service on Windows 2008 R2 Server. The only problem we encountered while setting up WECS was a comment we left in the **eventManagement.config** file. This particular comment was the example configuration (**example config**) line we used to set up the endpoint IP address and port (the location of the Sentinel server). Even though it is a standard XML-formatted file, we missed the comment and had to call tech support. We're noting this mistake here in hopes that it will save others from making the same mistake.

In our lab, the virtual server running NetIQ Sentinel 7 had an IP address of **10.1.1.169**. The WECS service was listening on TCP port 1024 (the default port—you can change this if necessary). The endpoint address configuration line was: **<endPoint address="tcp://10.1.1.169:1024" behaviorConfiguration="localhost" />**. The Windows event (WMI) connector service documentation file, **Windows-Event-(WMI)_2011.1r1.pdf**, which comes with the plugin, contains further details. Sections 5.2 and 5.3 are particularly helpful in this regard.

The WECS connector has some advantages over a syslog redirector: It collects historical data, it includes encryption, and you don't need to load additional software on the event source. The disadvantages are initial setup complexity and the difficulty of getting log events from other event-log files.

About the Author

Jerry Shenk currently serves as a senior analyst for the SANS Institute and is senior security analyst for Windstream Communications, working out of the company's Ephrata, Penn., location. Since 1984, he has consulted with companies and financial and educational institutions on issues of network design, security, forensic analysis and penetration testing. His experience spans networks of all sizes, from small home-office systems to global networks. Along with some vendor-specific certifications, Jerry holds six Global Information Assurance Certifications (GIACs), all completed with honors: GIAC Certified Intrusion Analyst (GCIA), GIAC Certified Incident Handler (GCIH), GIAC Certified Firewall Analyst (GCFW), GIAC Systems and Network Auditor (GSNA), GIAC Penetration Tester (GPEN) and GIAC Certified Forensic Analyst (GCFA). Five of his certifications are Gold certifications.

SANS would like to thank its sponsors: