McAfee Collector Plug-in

Gather Microsoft Windows logs without WMI

Whether you are tracking an insider threat or a compliance violation, logs from Microsoft Windows hosts can often provide crucial clues. Now you can leverage your current McAfee® ePolicy Orchestrator® (McAfee ePO™) software environment and the McAfee Enterprise Security Manager (SIEM) solution to securely gather logs from your Windows systems. With the SIEM collector plug-in, you gain visibility into host events, correlate these activities with other data, accelerate analysis and response, and improve overall log management.

How do you collect and interpret Windows logs from your Windows-based endpoints and servers today? Some organizations implement a separate agent-based log collection system, but the downside of that approach is the heavy operational burden of deploying and supporting another endpoint agent.

Windows Management Instrumentation (WMI) is another alternative, but it has too many technical and operational issues, as well as an inherent lack of assurance. One of the main concerns with WMI is that it runs on top of another of Microsoft's proprietary protocols, Distributed Component Object Model (DCOM). This dependency requires receiving systems to open all ports 1024 and above. This opens up a gaping hole in network firewalls, putting organizations at risk. In addition, many federal organizations cannot implement WMI because it does not comply with Federal information Processing Standards (FIPS).

Leverage McAfee ePO Software

Now, through a bidirectional integration between McAfee ePO software and McAfee Enterprise Security Manager, collecting Windows logs just got easier. You can use the same security management platform and the McAfee agent that already manages your endpoint security to deploy an SIEM plug-in. There's no need to open extra ports for another monitoring and collection system or add a new agent to your hosts.

Within minutes, the SIEM collector can start gathering event logs from your Windows-based systems and track any syslog data source files supported by McAfee Enterprise Security Manager. The plug-in transmits logs to the McAfee Enterprise Security Manager receiver for viewing within the McAfee Enterprise Security Manager console. You can even use Microsoft Active Directory to define a Windows logging policy and then use the McAfee ePO software agent to deliver the policy to the plug-in on the relevant clients.

Key Advantages

- Gain visibility into Windows events without installing an extra agent.
- Avoid the complexity, security issues, and limitations of WMI.
- Leverage your existing McAfee ePO software agent and policy infrastructure.
- Integrate Windows log events into your SIEM data set to expand situational awareness and speed analysis.

Once collected, you have all the speed, scale, and analytical power of McAfee Enterprise Security Manager to help correlate data and mine the logs for meaningful intelligence. McAfee Enterprise Security Manager's integrated, scalable, and high-performance log management system enables you to securely and reliably collect the logs you'll need to support incident response, evidentiary search, and compliance program requirements.

Near Real-Time Log Collection

Most government and industry regulations mandate log collection as a standard requirement. NIST SP800-53 states that, in addition to specific requirements to collect audit and fault logs, all logs should be collected as close to real time as possible. The SIEM collector gathers and sends logs without storing them on the client to help you meet this goal.

Scalable, Court-Ready Log Retention

McAfee Enterprise Security Manager uses a high-performance engine and a patented database technology to collect, index, and archive log data. With the optional McAfee Enterprise Log Manager, you can collect, sign, retain, and preserve any log type in its native, court-acceptable format for as long as you require for your specific compliance needs. Logs can be differentiated to facilitate access: easy and immediate local access for logs that may need to be parsed and analyzed for security or a managed storage area network (SAN) to store logs retained purely for compliance.

McAfee Enterprise Security Manager provides easily customized storage pools so you can ensure that your logs are stored correctly for the period of time dictated by regulations relevant to your organization. Payment Card Industry (PCI) regulations require log retention for one year, for example, while financial services and healthcare industry regulations may require up to seven years. PCI compliance is especially tricky. Some organizations don't realize that they should be collecting and retaining logs from hosts connected to servers that manage PCI-regulated data. Simply sharing the network makes these hosts subject to PCI controls, and McAfee Enterprise Solution Manager solution helps you achieve this compliance.

> **"Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs."**
>
> —NIST Special Publication 800-53, Revision 4

Rapid Visibility into Anomalous Events and Insider Threats

Once logs enter the SIEM realm, they increase in value. Logs can provide crucial analytics and event correlation data—and the sooner you see it, the faster you can act. This resource helps detect unexpected behaviors, such as escalation of administrative privileges, uninstallation of security applications, or introduction of hacking tools. Because this data comes into McAfee Enterprise Security Manager, any of these actions beyond an established normal baseline can trigger a corresponding SIEM alert for administrative intervention.

This visibility can also enable unobtrusive monitoring of behaviors and user events when you suspect an insider threat, such as data theft or sabotage. Your investigations are backed up by verifiably reliable log collection.

Correlation and Mining to Enhance Security Operations

Security analysts can use rules to normalize and correlate a broad assortment of data to understand events fully. Where WMI might provide a stream of data that you must interpret and act on manually, the McAfee Enterprise Security Manager integration helps translate log data into direct, often automated, actions. For example, by using McAfee ePO software with McAfee Enterprise Security Manager, you can combine host and network log data to detect anomalous events, such as worm propagation, using SIEM correlation rules and alarms. As you investigate, you have one-click access to the original log files and even the specific log records. You can then use the McAfee ePO software agent, tags, and tasks to quarantine and scan infected hosts.

Get Started

This solution, which integrates McAfee ePO software, the McAfee agent, and McAfee Enterprise Security Manager is a simpler and more secure way to perform log collection from Windows-based endpoints and servers. It helps you derive value from your existing McAfee ePO software deployment and enables you to use all the information you have available—in a timeframe and with the speed required to manage your risk and security posture proactively. Learn more about this solution configuration by downloading the SIEM collector and McAfee ePO software extension readme and release notes documentation.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60609ds_siem-log_1213B
DECEMBER 2013