White Paper

PCI Guidance: Microsoft Windows Logging

intel Security

This white paper was written by:
Cayce Beames, CISSP, QSA,
Technical Practice Director,
Strategic Services, Intel Security

Table of Contents

Introduction

Logging, sometimes referred to as system auditing, is an important mechanism to help administrators monitor and troubleshoot the systems on their network. Unfortunately, it is not unusual to see that logging is not being fully leveraged. Administrators often claim that system logging puts too much demand on their system and network resources.

Administrators face a myriad of challenges in operational assurance, regulatory compliance (HIPAA, SOX, FISMA, and others), and industry compliance (PCI). The compliance challenges can be daunting because there are few resources to guide administrators to get the job done.

In this paper, we will specifically discuss what is involved in establishing logging for Microsoft Windows systems, so that, if applied on your system, you will meet PCI requirements. These settings will also be useful in detecting system anomalies that could be indicative of system misuse or even a system breach. We have attempted to present this guidance in a straightforward manner and will discuss:

- Preparation for logging.
- PCI requirements for logging.
- Domain audit policy.
- Log repository.
- Alerts.
- References.

Preparation for Logging

Before any system auditing activities occur, it's important to have a baseline for the capacity and performance of your system. On a Microsoft Windows system, you should be concerned with:

- CPU utilization.
- Memory utilization.
- Network bandwidth utilization.
- Disk space availability for log files (both with the local system and remote log server).
- Disk I/O utilization.

To establish a baseline for the system, you'll need to set up monitoring of these items and track them over a period that covers your organization's busy and not-so-busy times. Depending on your business, this could be a weekly, monthly, quarterly, or yearly cycle. There are plenty of tools available to do this baselining. Microsoft Operations Manager, NetIQ, SolarWinds Orion, and What's Up Gold are all useful tools for measuring these performance and capacity management functions.

If you are unable to establish a baseline and understand your system headroom over multiple critical business cycles, you should be prepared to quickly turn off logging on your systems if service impacts occur. Logging can impact a system's CPU utilization, memory utilization, network utilization and, of course, disk space—which goes for both the system generating the log messages, as well as the centralized log server receiving those messages.

If baselining is not performed, and it is not a viable option for your organization to turn off logging, another method of applying system logging without a baseline is to establish monitoring processes using built-in tools, such as Resource Manager, and slowly begin applying system logging settings so that the impact can be monitored prior to the system having a service impacting event.

PCI Requirements for Logging

Below are PCI CSS requirements for logging (See PCI DSS v2.0: **https://www.pcisecuritystandards.org/security_standards/index.php**.):

- **10.2.1 All individual accesses to cardholder data**: Malicious individuals could obtain knowledge of a user account with access to systems in the cardholder data environment (CDE), or they could create a new, unauthorized account in order to access cardholder data. A record of all individual accesses to cardholder data can identify which accounts may have been compromised or misused.
- **10.2.2 All actions taken by any individual with root or administrative privileges**: Accounts with increased privileges, such as the "administrator" or "root" account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is unable to trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and individual.
- **10.2.3 Access to all audit trails**: Malicious users often attempt to alter audit logs to hide their actions, and a record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account,
- **10.2.4 Invalid logical access attempts**: Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an indication of an unauthorized user's attempts to "brute force" or guess a password.
- **10.2.5 Use of identification and authentication mechanisms**: Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may be used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account. Activities including, but not limited to, escalation of privilege or changes to access permissions, may indicate unauthorized use of a system's authentication mechanisms.
- **10.2.6 Initialization of the audit logs**: Turning the audit logs off prior to performing illicit activities is a common goal for malicious users wishing to avoid detection. Initialization of audit logs could indicate that the log function was disabled by a user to hide their actions.
- **10.2.7 Creation and deletion of system-level objects**: Malicious software, such as malware, often creates or replaces system level objects on the target system in order to control a particular function or operation on that system.

Domain Audit Policy

Since the PCI Security Standards Council describes the requirements in general that are applicable to most all system types, system administrators and security and compliance teams have to work together to figure out how to implement the requirements on the individual systems within the organization. Here's a suggested approach for the Windows Domain Audit Policy:

Audit Policy	Audit On	PCI Requirement
Audit account logon events	Success, Failure	10.2.4, 10.2.5
Audit account management	Success, Failure	10.2.2
Audit directory service access	Success, Failure	10.2.2
Audit logon events	Success, Failure	10.2.4
Audit object access	Success, Failure	10.2.1, 10.2.2, 10.2.3, 10.2.6, 10.2.7
Audit policy changes	Success, Failure	10.2.2
Audit privilege use	Success, Failure	10.2.2, 10.2.5
Audit process tracking	Success, Failure	10.2.2
Audit system events	Success, Failure	10.2.2, 10.2.7

Table 1. Suggested approach for Windows Domain Audit Policy.

With audit object access, you will also need to specify which objects to audit on an individual object basis. This should be done for objects like the system log files, properties files, encryption keys, and certificates. See **http://technet.microsoft.com/en-us/library/cc163121.aspx#EKH** for more information on Windows audit.

Also, be careful with how Group Policy Object (GPO) policy precedence is handled. See **http://technet.microsoft.com/en-us/library/ff182311(WS.10).aspx#BKMK_4** for more information on how GPO policy merging occurs. If you apply the audit policy at the top level of the domain, and a policy gets set at a lower level, the lower level policy will take precedence. Ensure that the policy is applied in the correct place and cannot be overwritten.

How to Configure Audit Object Access

As mentioned above, after configuring the auditing of success/failure of object access, you need to configure each object or object container (folder) to be audited. To do this, follow the general process below on your objects:

1. For any target directory to audit, right click on the directory and select Properties:

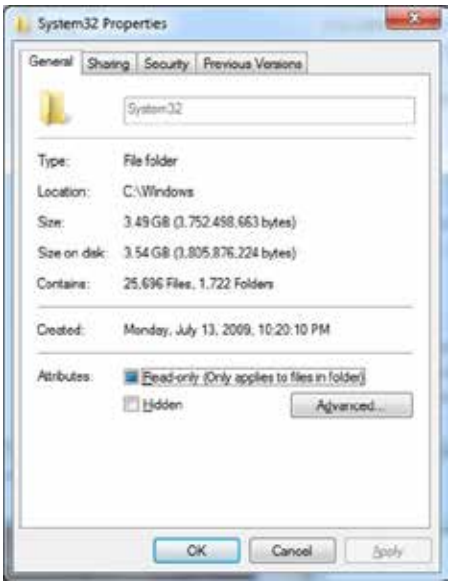

Figure 1. General properties for the System32 directory.

2. Then click the Security tab:

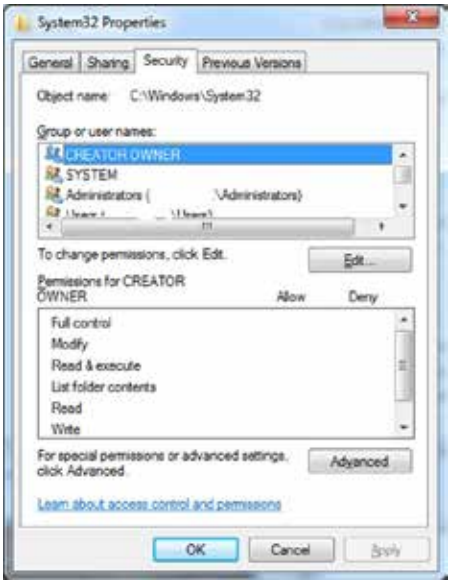

Figure 2. Security properties for the System32 directory.

3. On the Security tab, click the Advanced button to bring up the following window:

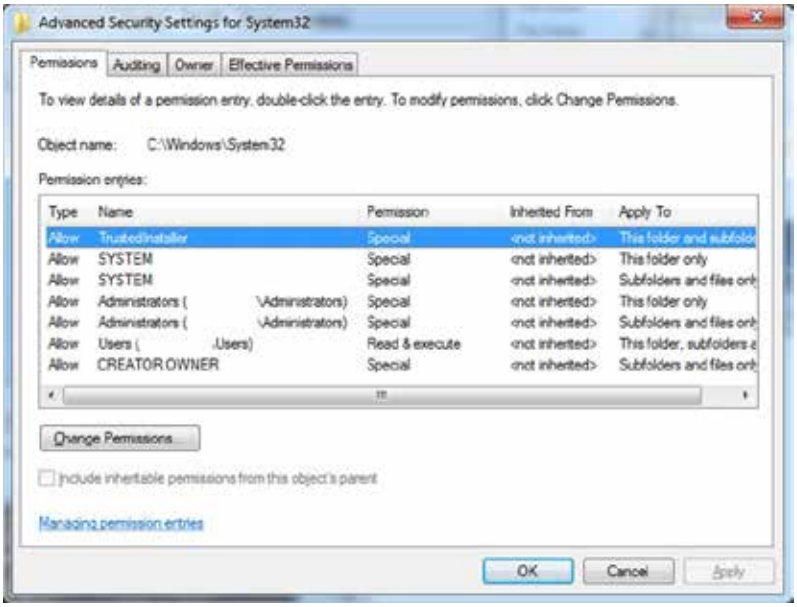

Figure 3. Advanced Security Settings for the System32 directory.

4. Next, select the Auditing tab:

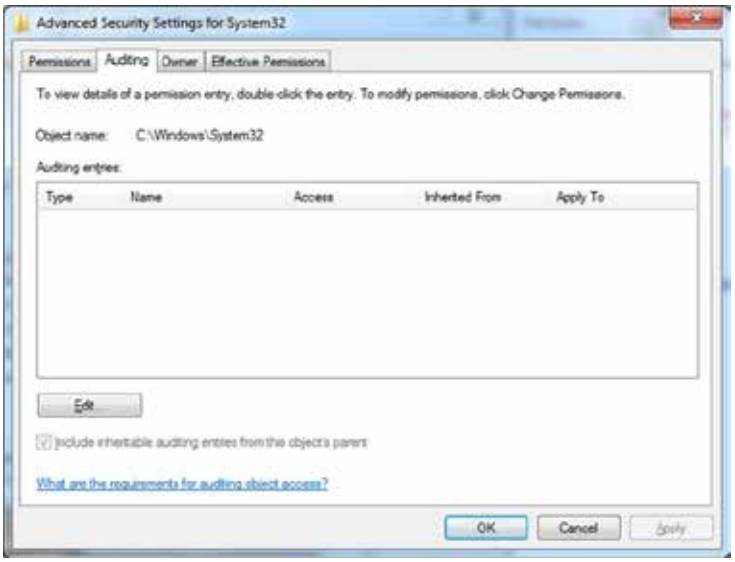

Figure 4. Auditing tab within the Advanced Security Settings for the System32 directory.

If nothing is listed here, and the audit object access Windows audit policy is configured to log on success and failure, no file activities will be logged on this directory.

5. To establish logging on this directory, click the Edit button on the Auditing tab to bring up the following window:

Figure 5. Editing the Auditing settings within the Advanced Security Settings for the System32 directory.

6. Next, click the Add button to bring up the following window:

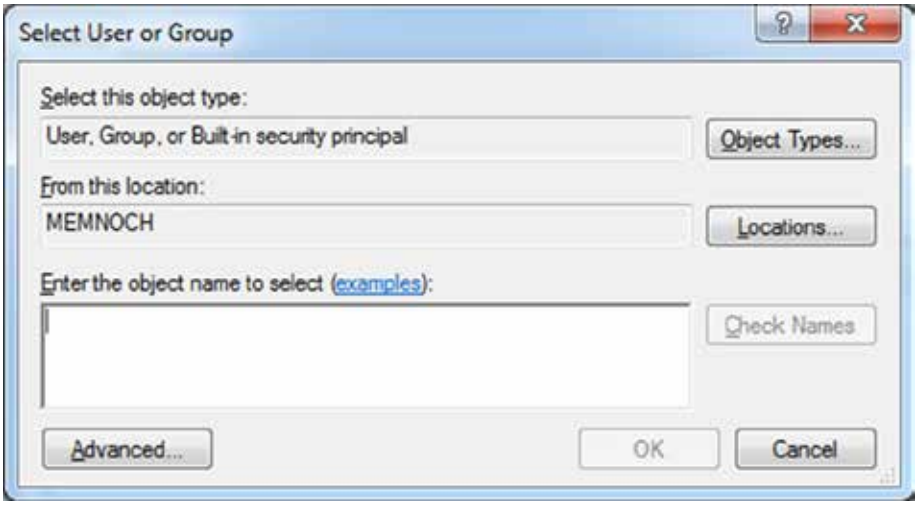

Figure 6. User and group selection dialog box for the System32 directory audit settings.

7. Click the Advanced button, and then click Find Now on the new window that opens:

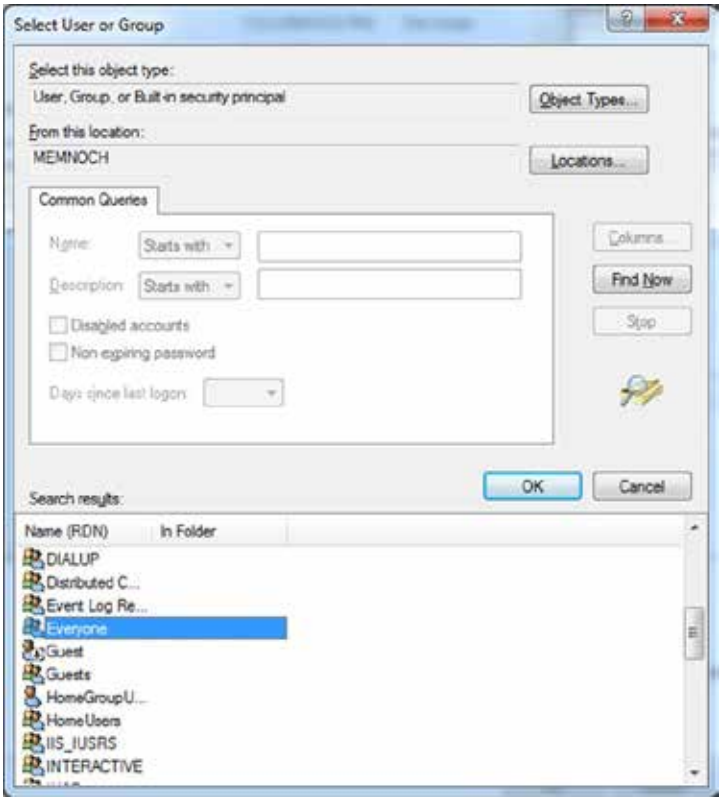

Figure 7. Finding users to add to the audit settings for the System32 directory.

8. Select Everyone, and click OK to close the window, and then click OK again on the Select User or Group window:

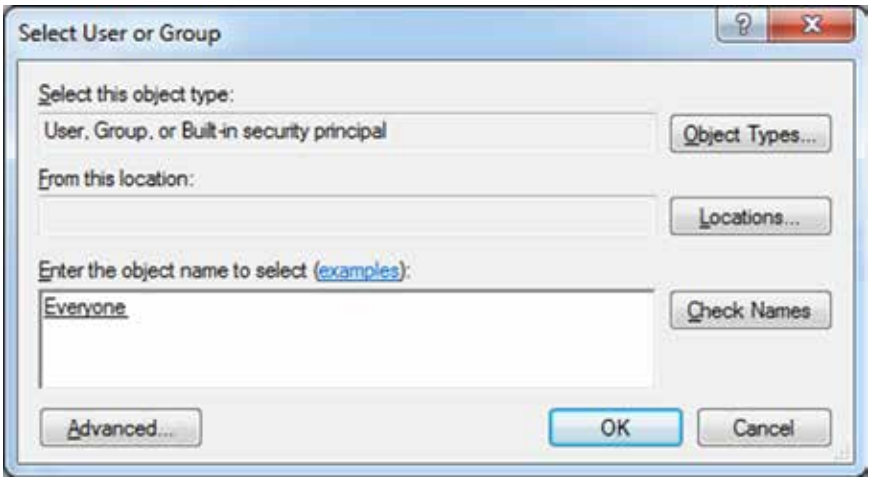

Figure 8. Everyone has been added to the Audit settings for the System32 directory.

9. You should then be presented with the following screen:

Figure 9. The current System32 directory Auditing permissions for the Everyone group.

10. As scary as it might seem, you want to log all activities in this directory and subdirectory from all users. Therefore, you would select the Full Control for Successful and Failure, as well as the checkbox at the bottom to Apply these auditing entries to objects and/or containers within this container only. Then click OK.

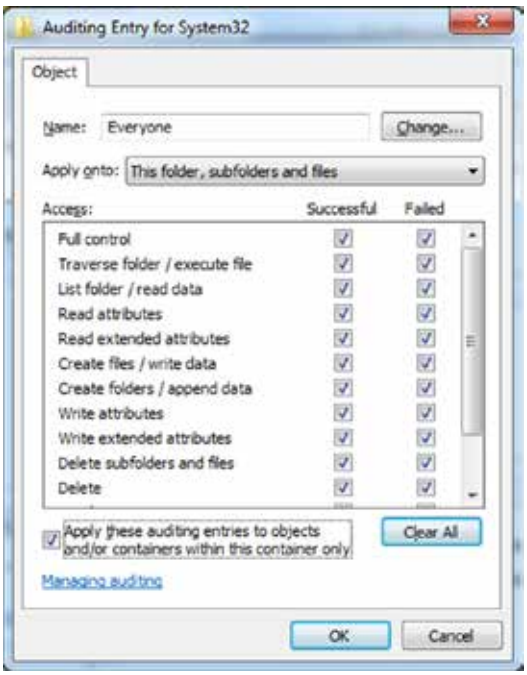

Figure 10. Modifying the System32 directory's Auditing permissions for the Everyone group.

11. If you check the bottom checkbox, “Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object,” you will replace all the auditing inheritability settings for the contents of this directory.

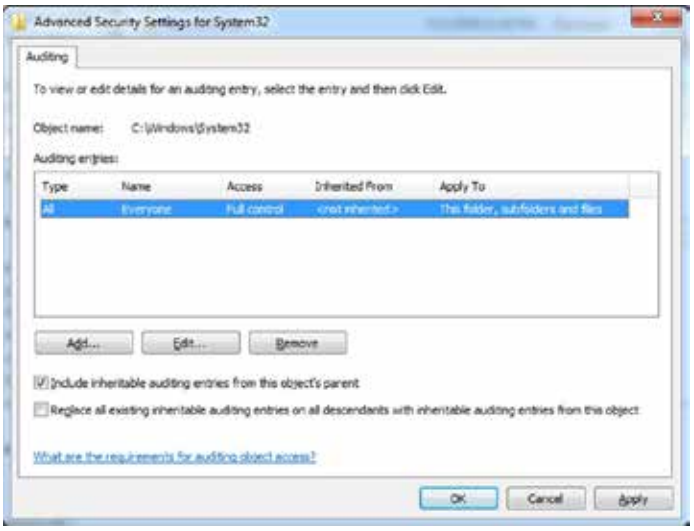

Figure 11. The resulting Advanced Security Settings dialog box for the System32 directory.

Note: Keep in mind that your log file size may need to be adjusted to accommodate the new logging. Also, be mindful of performance impacts to your system by enabling auditing.

Log Repository

All logs on your network should be sent to a central repository for safekeeping. If there is ever a system compromise or virus outbreak, this centralized log server contains all the forensic evidence. You should ensure that it is protected with limited access enforced by strong access controls and integrity monitoring to ensure that changes to log files don’t occur. For more information, see PCI requirement 10.5 and its sub-requirements.

Recent versions of Microsoft Windows and Windows Server (Windows 7, Server 2008, and others) have built-in capabilities to send logs to a designated system recipient. This event subscription capability is documented here: **http://technet.microsoft.com/en-us/library/cc749183.aspx**.

Alerts

Manually reviewing log data as recommended in requirement 10.6 is rather difficult. Requirement 10.6 asks that the merchant review logs, and, when suspicious events are found, report them. In breaking this high-level process down into its component parts, a log reviewer must:

- Have a complete set of logs.
- Have an idea of what suspicious events to look for.
- Have an idea of how a series of unrelated events might collectively become a suspicious event.
- Have a process to follow for expanding the investigation to other team members or logging an incident through the incident reporting process of the organization.

For a human to do this at any scale above five to 10 computers is an impossible task. Computers are much better at this type of work than humans, so we recommend that you use a computer to do a certain amount of your event log review for you. Keep in mind, though, computers don’t understand context. In this case, we’re asking for them to simply search and report on the presence or absence of certain strings of text found within the events.

Below is a list of events that can help identify suspicious events that should be taken into consideration when building an understanding of what is happening on the systems.

The primary source for this is **http://www.ultimatewindowssecurity.com/webinars/register.aspx?id=75**.

Event ID Server 2003	Event ID Server 2008	Category (which audit policy triggers this log)	Default Severity/ Type/Level (Here the message is found by default.)	Description	Rationale
512, 513	4608	Process Tracking	Success Audit	Windows is starting up or shutting down.	You should never restart a system unless it's being patched or you have a regular reboot time. This could indicate an attack of some type or potentially the insertion of a rootkit.
517	1102 (system, not security event)	Process Tracking	Success Audit	The audit log was cleared.	We want to know when it was cleared and by whom so that we know if it's normal or whether an attacker is trying to hide his tracks.
528, 540	4624	Logon/Logoff	Success Audit	A user successfully logged on to a computer or the network.	"Administrator" (or whatever "Administrator" was changed to as part of the system build) should never log in directly to any system unless it is under maintenance. Even then, there should be a verifiable approved change that this login is part of. Also, if your organization is using an envelope procedure, you should never have a direct administrative login.
529	4625	Logon/Logoff	Failure Audit	Logon failure—a logon attempt was made with an unknown user name or a known user name with a bad password.	Excessive failed logins for a system should not occur. Any server with more than six failed logins within a one-hour period should be in the alarm "on" state. This account should be locked after no more than six failed logins, per PCI requirements. But if your organization uses automatic account unlocks, you want to ensure that repeat lockouts are investigated.
539	4625	Logon/Logoff	Failure Audit	Account was locked out.	Repeating account lockouts of the same account should happen infrequently. Account lockouts on many different accounts could be indications of a brute-force attack underway or system configuration issue.
592	4688	Logon/Logoff	Success Audit	A new process was created.	Servers usually don't run new programs. The program name of a newly run program should not be something abnormal for the system.
601	4697	Logon/Logoff	Success Audit	A service was installed in the system.	This is the same as installing new software that runs in the background. This should only be done during an approved change. An event should always be investigated to validate an approved change request is present.

602	4698	Logon/Logoff	Success Audit	A scheduled job was created.	When a regular user creates an "at" job to run a program, that program runs as "SYSTEM," which has lots of power. No one should be doing this except an administrator as part of an approved change.
612	4719	Policy Change	Success Audit	Audit policy was changed.	An audit policy should typically not change. An attacker might want to turn something off so that no one notices what is going on.
624	4720	Account Management	Success Audit	A user account was created.	Of course, we're mostly interested in local accounts created, not necessarily domain accounts, as domain accounts are created all the time.
632	4728	Account Management	Success Audit	A member was added to a global group.	You would be interested in any addition to the domain administration group.
636	4732	Account Management	Success Audit	A member was added to a local group.	You'd want to know who gets added to "administrators." A local administrator has the capability to grab the SAM, crack all local passwords, and then mount an attack on the domain.
660	4756	Account Management	Success Audit	A member was added to a security-enabled universal group.	This is the primary group. No one should be added here.
	5025	System, Other System Events	Success Audit	The Windows Firewall Service has been stopped.	Under normal situations, this should not occur. You would want to know who initiated this.
852	4946, 4947, 4948	Policy Change, MPSSVC Rule-Level Policy Change	Success Audit	Changes have been detected in Windows Firewall rules.	There should not be any changes unless there's an approved change request.
	4649	Logon/Logoff, Other Logon/ Logoff Events	Success Audit	A replay attack was detected.	Someone is trying to reuse a Kerberos ticket. You'd want to find that person quickly. Kerberos tickets aren't meant to be used in this way, and this should never occur.
	4616	System Events	Success Audit	The system time was changed.	For time change events longer than five minutes between the previous time and the new time contained within the message, throw an alert. This could be indicative of an attempt to change system time, thus altering logs and thus altering the timeline of an attack.

Table 2. Windows events that may be associated with suspicious activity.

Configuring alerts on a Windows 7, Server 2003/2008 is relatively simple. Each event being monitored should be tested to generate an event that will show up in the security log.

For each event that appears in the security log, you can assign a task to the event to generate an alert to the screen, send an email, or run a program.

One of the simplest methods is to send an email. For this, you will need an SMTP server to send your message to.

Auditing tools such as McAfee® Enterprise Security Manager, ArcSight, NetIQ, and Splunk will be more feature-rich for performing the log correlation and alerting to different destinations.

References

Event IDs

- Windows Server 2003: **http://technet.microsoft.com/en-us/library/cc163121.aspx#EKH**
- Windows Server 2008: **http://support.microsoft.com/kb/947226**
- Primary source for what to look for to detect an attack/intruder: **http://www.ultimatewindowssecurity.com/webinars/register.aspx?id=75**

About the Author

Cayce Beames has more than 20 years of experience in information technology and has been an active information security practitioner since 1992. Beames has been consulting for more than 15 years. She has served as a system administrator, consultant, technology manager, regional risk manager for a Top Five banking institution, and consulting manager for a Forbes Global 200 telecommunications firm with project delivery, sales and operations responsibilities. Beames has designed, built, secured, managed, and evaluated a wide range of commercial and open source technology.

About McAfee Foundstone Professional Services

McAfee Foundstone® Professional Services, a division of McAfee, offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, McAfee Foundstone identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company's professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military.

About Intel Security

McAfee is now part of Intel Security. With its Security Connected strategy, innovative approach to hardware-enhanced security, and unique Global Threat Intelligence, Intel Security is intensely focused on developing proactive, proven security solutions and services that protect systems, networks, and mobile devices for business and personal use around the world. Intel Security is combining the experience and expertise of McAfee with the innovation and proven performance of Intel to make security an essential ingredient in every architecture and on every computing platform. Intel Security's mission is to give everyone the confidence to live and work safely and securely in the digital world. **www.intelsecurity.com**.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com