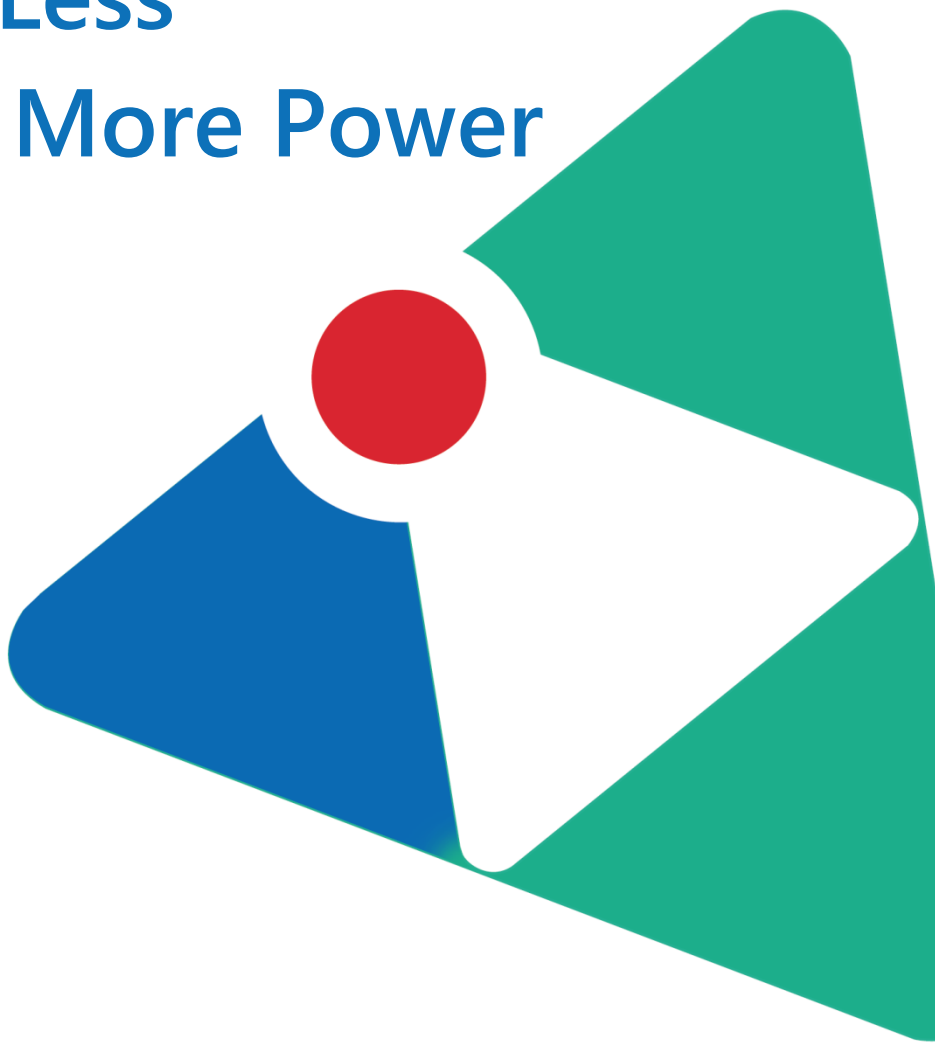
netwrix
#1 for change auditing

Better Active Directory Auditing…Less Overhead, More Power



www.netwrix.com | **Toll-free**: 888.638.9749

Table of Contents

Defining Your Auditing Needs

Today's organizations – faced with stricter internal security policies as well as stringent legislative and industry requirements – continue to struggle to make Windows Server auditing simpler, more reliable, and better able to meet their business requirements.

It's no wonder that organizations have such difficulties: Windows' native auditing and logging mechanisms were originally and primarily designed to support troubleshooting efforts, not to meet the security auditing needs of modern businesses.

The auditing problem in Windows starts with Active Directory. Active Directory sits at the center of your security strategy: It provides user authentication, and forms the basis upon which access authorization is based. Pretty much everything that happens in Active Directory needs to be audited.

But the auditing needs go beyond mere security: Active Directory is mission-critical, and downtime simply isn't acceptable. Auditing Active Directory for change control purposes, as well as for troubleshooting, is as paramount as capturing information purely related to security.

Organizations dealing with compliance regulations like HIPAA, PCI DSS, SOX, FISMA, GLBA, and more also have to audit how users use their authorizations. In other words, those organizations need to carefully audit access to selected files, Exchange Server mailboxes, SQL Server databases, and much more – as well as configuration and security changes to those products. Being "compliant" means more than just having the right security in place – it means being able to prove that the right security is in place and has been in place – something that can only be done with audit reports.

Windows Auditing Shortcomings

Native Windows auditing capabilities lack a few important features that are crucial to companies dealing with compliance and other stringent security requirements.

Chief amongst these shortcomings are:

- The native audit logs are not centralized. This essentially makes the logs useless as an enterprise-wide audit trail.
- The native logs are not tamper-proof or tamper-resistant; administrators are able to easily cover their tracks by clearing the logs, and the logs can even be cleared accidentally.
- The native event log viewer application provides only primitive filtering and searching capabilities that are nowhere near the level needed for security and audit reporting.
- If you're relying solely on the Windows event logs, you're missing tons of critical changes in your environment – you're flying blind.
- The native logs don't always contain information from the other products you run on Windows, such as SQL Server, VMware, and so forth.

- The native event logging system, to be frank, produces an abundance of information, yet it provides few ways to filter that information, to correlate related events, and so on. It's a glut of data that is extremely difficult to use when trying to create a report of "who did what," for example.

In newer versions of Windows, Microsoft has made some improvements to the logging infrastructure. For example, Windows Server 2008 introduced the ability to log changed attribute values for Active Directory changes, allowing administrators to see what settings were changed and what the new values were.

While this is helpful for both troubleshooting and security logging, the new capability doesn't extend fully across all of the events captured in the log, nor does it include the attribute values as they were before the change – meaning that you're still resorting to backup files to discover "how things were."

Another weakness of the native audit logs is that they simply don't provide everything. If you're relying on native event logs alone, then you're missing an incredible amount of information about the changes going on in your environment. You won't know what settings were changed within a Group Policy object, for example. You'll be missing details on Active Directory schema changes. You won't capture non-owner mailbox access in Exchange Server. You're flying blind – and there's no way you can expect to achieve and maintain compliance without being able to audit and report on the key changes and events.

If you're relying solely on the Windows event logs, you're missing tons of critical changes in your environment – you're flying blind.

Does your company use Exchange Server? If so, the native event logs are probably capturing very little of the auditing information you actually need, including system level configuration changes, Outlook Web Access settings in Internet information Services, and more. What changes are captured in the native event logs are typically full of cryptic, low-level data that is difficult to use for auditing purposes.

The unfortunate fact is that most experienced professionals agree that **the native Windows event logs, by themselves, are useless for modern security auditing requirements, and especially useless by themselves for any compliance scenario.**

Two Solutions to the Problem

Obviously, if native auditing alone doesn't meet your needs, you have to do something else, and there are two basic approaches.

The Intrusive Agent Approach

The first possible approach is to forgo the native auditing completely. This usually entails installing a software application – referred to as an agent – on every single one of your servers. That agent collects auditing data in its own way, bypassing the native logging systems, and forwards its audit events to a centralized server. That central server takes care of your reporting, event storage, and so on. Something to keep in mind is that the agent will

typically be task-specific, capable of auditing Active Directory or SQL Server or something else; if you have servers filling multiple roles, you may be deploying – and maintaining – multiple agents per server.

There are some downsides to the agent-based approach. First, you're taking on a much bigger long-term maintenance commitment, because agents are software, and software has to be patched and kept up-to-date. Agents can also reduce your infrastructure's stability, because agents are software and software can contain bugs.

Few businesses are excited about the possibility of having critical servers like domain controllers and Exchange Server computers unexpectedly crashing because of a buggy piece of management software.

Agents can decrease server stability and reliability, prolong maintenance activity, and delay the application of critical Microsoft patches.

Agents can also complicate overall server maintenance. When Microsoft "Patch Tuesday" rolls around, will every single patch be compatible with your agent software – or will installing a patch suddenly break everything? The unfortunate fact is that most agents work by "hacking" the operating system in some way, and the hacks needed for the agent to work can be changed at any time by a Microsoft patch, hotfix or service pack. By committing to the agent-based approach, you're committing to having to pilot test every single patch and update Microsoft issues – or waiting for the agents' software vendor to test each patch before you can deploy it. In the case of critical Microsoft patches, the necessary lag time created by having agents on your servers may not be practical.

All of these extra caveats are one reason that the agent-based approach is sometimes referred to as an invasive or intrusive approach – harsh words, but ones that can accurately describe the situation.

Another downside to the intrusive agent approach is that solutions built in this fashion typically ignore the native event logs, and may even encourage you to disable native event logging. That means you're losing valuable information, and you're only able to work with the information that the auditing solution provides. That's a shame, because although they're not perfect, the native event logs do provide a lot of valuable information.

The Agent-Free Approach

The second approach is to keep the native logging in place – and to simply enhance it. This can typically be accomplished without installing anything on your servers, meaning you can deploy a solution that uses this approach much more quickly, and with much less impact in your environment. The solution simply contacts each of your servers, retrieves their event log entries as they are created, and stores copies of them in a centralized database. Again, that central database is where the magic happens: It can offer event searching and filtering, reporting, and so on. Such a solution could also remotely – again, without the use of an agent – capture information above and beyond what Windows itself would normally log, providing extended auditing capabilities for security, troubleshooting, and even change control.

There are some distinct advantages of the second, agent-less approach:

- The native logs don't always contain information from the other products you run on Windows, such as SQL Server, VMware, and so forth.
- Operating without an agent also makes for easier long-term maintenance: When software updates come out for your auditing solution, you'll only have to update the central server – you won't be re-deploying updated agents to all of your servers.
- An agentless approach offers faster deployment, practically zero server impact, and all the auditing capabilities you need.
- Operating without an agent also eliminates the potential for third-party software instabilities, conflicts, and so on. Microsoft will never be able to "point the finger" at a third-party agent on your domain controllers when there isn't an agent, and your domain controllers will remain more "pure" and stable.
- By gathering all of the event information into a single location, the auditing solution could easily support a broad range of products, such as Exchange Server, SQL Server, and more – all without having to deploy additional agents to every server.
- You still get all of the valuable, technical information contained in the native event logs – you just get more information than the native event logs provide.

An agentless approach offers faster deployment, practically zero server impact, and all the auditing capabilities you need.

Again, the idea is to not simply abandon the native event logging system, because that system does capture a great deal of useful data – and does so in a way that is completely understood, and which is obviously supported by Microsoft. The idea, rather, is to extend that native logging system to shore up its weak points and provide the business capabilities you require.

A key component of the approach is the automated collection and centralization of event log information: By moving those events into a separate database, you can create a tamper-proof or tamper-evident store that is not subject to clearing by administrators trying to cover their tracks. This key element of a centralized auditing solution is what sets the stage for it to become a means of achieving security compliance.

Thinking Beyond Basic Security Auditing

In today's world, it is not enough to simply capture events that indicate someone was added to a security group, or events that log a user's access to a file. Those are merely starting points; what you really need is a robust auditing architecture that has modern capabilities, including:

- Full auditing of all Active Directory events and activity.
- Full auditing of Group Policy objects (GPOs), which provide a critical component of your overall security strategy. This auditing should include details on what settings have been changed inside a modified GPO, including "before and after" data on the changes that were made.
- Exchange Server auditing – including access to mailboxes by users other than the mailbox owner, system-level configuration changes, and more – all with plain-English information rather than technical gibberish.
- "Who, What, When, and Where" information for every configuration change made in the IT infrastructure – critical both for troubleshooting and change control as well as for security and compliance.

In addition, any auditing solution worth looking at must include pre-defined reports that help address the most common compliance needs, and should allow you to create custom reports to help support your own internal security policies and IT management processes. An ideal solution will build these reports in SQL Server Reporting Services, which offers Web-based reporting, subscription-based reports, and much more – making it easier to get information into the right hands.

But a good auditing solution should do much more than just capture events and produce reports. A good solution can also be a valuable change management and change recovery tool. For example, if your auditing solution can capture "before and after" information on Active Directory configuration changes, then you might expect it to offer the ability to undo, or roll back, selected changes – ideally without having to take a domain controller offline for an authoritative restore operation.

Enhanced Native Logging

There's little question that most companies will need to either supplement or replace the native Windows event logging capabilities; Windows simply doesn't support the feature set that companies need to meet modern security compliance requirements.

Replacing the native event logging system with an agent-based approach is a high impact, intrusive operation. You will solve most of the problems associated with the native auditing system, but at the cost of a lengthier, more complex deployment, higher ongoing maintenance overhead, and unknown impact on your servers' performance and stability.

In the end, many businesses will prefer auditing solutions that enhance and extend what's already in Windows. You're creating less impact on your servers and less intrusion into your environment; the auditing solution remains more standalone and compartmentalized. Long-term maintenance is easier, and you're working with Windows the way it was designed to work. You're still solving the problems of the native auditing system and gaining the capabilities you need to achieve and maintain compliance, but you're doing so with less overall risk and effort.

Netwrix Auditor: A Non-Intrusive Way to Enhance Windows' Native Auditing

Netwrix Auditor solutions are designed to work with Windows native event logging system, enhancing it to provide more powerful capabilities and to fill its gaps. The Netwrix Auditor platform uses an agent-free approach, offering non-intrusive, fast deployments that don't complicate your server installs or maintenance.

The Netwrix Auditor solutions include all the things the native event logs don't, such as Active Directory schema changes and setting-level GPO changes covered by Netwrix Auditor for Active Directory, non-owner mailbox access in Exchange Server covered by Netwrix Auditor for Exchange, and much more. The Netwrix Auditor product captures the **who**, **what**, **when**, and **where** for every change in your environment, and enables you to produce custom reports through SQL Server Reporting Services. It comes packed with pre-defined reports for compliance and management needs, and captures before-and-after information for your infrastructure's critical changes.

Netwrix Auditor doesn't propose that you "rip and replace" the native event logging system – it simply fills in the gaps in Windows' native event logs, capturing more and more detailed information and storing it in a secure database. Best of all, the product can be easily deployed by any experienced Windows administrator, without the need for expensive consulting services or lengthy deployments. The alternative Netwrix freeware tools can be used indefinitely and are suitable for small businesses with flexible auditing requirements.

And if you are looking for extended auditing for your entire IT infrastructure, Netwrix provides the integrated auditing solution that includes AD and other similar solutions for Windows Server, VMware vSphere, file storage appliances (such as NetApp and EMC), Microsoft SQL Server, and several other platforms. Gain more insight, achieve and maintain compliance, speed troubleshooting and problem resolution, and ensure the security of your IT infrastructure – easily and quickly, and without installing a single bit of code on your precious production servers. That's Netwrix Auditor.

Freeware Products

Tens of thousands of IT professionals use Netwrix freeware tools, including Netwrix Change Notifier for Active Directory and many more. All tools can be downloaded at no charge on the Netwrix website.

About Netwrix Corporation

Netwrix Corporation is the leading provider of change auditing software, offering the most simple, efficient and affordable IT infrastructure auditing solution with the broadest coverage of audited systems and applications available today. Founded in 2006, Netwrix has grown to have thousands of customers worldwide. The company is headquartered in Irvine, California, with regional offices in New Jersey, Ohio, Georgia and the UK.

Netwrix Corporation, 20 Pacifica, Suite 625, Irvine, CA 92618, US

Regional offices: New York, Atlanta, Columbus, London

netwrix.com/social

Toll-free: 888-638-9749 **Int'l:** +1 (949) 407-5125 **EMEA:** +44 (0) 203-318-0261