netwrix
#1 for change auditing

File Auditing in the Enterprise

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

netwrix
#1 for change auditing

Table of Contents

Why Is File Auditing Important?

A Real-World Example

The importance of comprehensive file auditing is best illustrated by a real-world example. Data housed in an organization's servers and storage devices contain massive amounts of information. Much of this information is sensitive and is not intended for all eyes. It is absolutely critical that at any point in time, records can show an audit trail of who has accessed or attempted access to files and folders or have attempted to modify permissions of files and folders including the date and time when the attempt or change was made and on what server the change occurred.

For organizations bound by regulations such as SOX, HIPAA, PCI, and FISMA, detailed file auditing showing **who** changed **what**, **when**, and **where** is a necessity. Without it, the organization risks non-compliance which may result in fines and sanctions. Consider all the information in any organization stored in various files: employee data, financial information, proprietary and trade information not meant for public or even selective internal access. One bad change can put that information and compliance at serious risk.

Imagine a user browsing the network who finds various shares visible to them. Upon further examination, they stumble upon a file created by a senior executive outlining an upcoming merger including monetary transactions, leadership changes, and employee consolidations. Once opened by the casual user, the confidentiality of this information is lost. If this information were distributed, it may have serious negative consequences for the organization such as legal action or non-compliance. File access violations such as this have great potential of becoming much worse if information in sensitive files has been modified or removed or if the file were deleted altogether.

Without an effective file auditing procedure in place, this organization has no way of providing an audit trail of who accessed what, when, and where this activity took place. With file access auditing, this information could have been quickly and easily discovered. The organization would then have been provided an opportunity to reduce the risks associated with this breach and improve their security.

File Auditing to Reduce Risk

Detailed file access auditing delivers accountability and proof of regulatory compliance. Automatic collection and reporting of file change and file access information provides organizations with a steady stream of feedback regarding file activity in the enterprise. Using this information can greatly reduce risks. A file permission change may allow a user or group to see or modify sensitive information. A user repeatedly reviewing information they would not normally read may reveal an employee who is providing a competitor with upcoming product details.

Important files deleted from a network share may explain why important reports were not submitted on time. File auditing is the vehicle by which access attempts and changes made to files, folders and permissions can be monitored to uncover security risks so they can be addressed. For file servers and storage appliances, auditing permissions helps to ensure rights to sensitive data are maintained properly.

Effectively managing every aspect of user and administrator interaction with the multitude of files within the environment reduces risk while granting the appropriate access users need to perform their duties. Change may sometimes bring unpredictable results, one of which is unintentionally creating conditions that disrupt or put the organization at risk.

File auditing provides actionable and historical forensic information to ensure risk factors are managed appropriately while delivering consistent service to the end users.

File Auditing to Improve Security

Internal threats pose a greater immediate danger to the organization than ever before. News headlines, such as the July 2011 breach of Shionogi, Inc. by a former employee frequently depict the disgruntled employee who has exploited their knowledge of internal systems for their own purposes. The primary reason these events are so prevalent is because of trust. Employees are given a level of trust and when that trust is abused, organizations quickly become victims.

File auditing provides organizations with the ability to establish a robust check-and-balance record for all file system activity thus greatly improving security. Security improvements through the use of traditional file auditing are most often reactionary. Security flaws and holes are often discovered after the fact and the reason for this is automatic file auditing and file audit reporting is not present.

Monitor file activity frequently to improve security in the enterprise. File auditing using only native tools can be cumbersome because of the volume of information recorded and while the majority of events are legitimate. One of the easiest ways to improve file security is to extract and review change information automatically on a regular basis.

File Auditing to Sustain Compliance

Regulations such as SOX, PCI, FISMA, and HIPAA each have their own detailed explanations of security standard practices including what exactly needs to be tracked and recorded in files and file systems. These regulations exist to establish (IT) change auditing standards to protect both businesses and consumers. At the end of the day, these regulations and their enforcement strive to confirm the organization is securing, recording and monitoring change events that permit access to sensitive information such as banking information, social security numbers, and health records.

Additionally, regulations exist to establish a minimum set of security standards as they apply to user access within the environment in which they operate. File and folder permissions are essential to segregating information so that only select groups and individuals can access it without having to locate the information on separate physical or virtual systems. Demonstrating compliance is an exercise in presenting this information to auditors upon request and to the level of detail as is interpreted by the law or standard and subject to the individual auditor's discretion.

Auditing files, folders and permission access attempts and changes provides the **who**, **what**, **when**, and **where** information most frequently requested by auditors and almost equally important is the need to store this information for sometimes up to 7 years or more to be considered compliant. For Windows file servers and storage appliances (such as NetApp Filer), this is extremely difficult and an entirely manual process with native functionality and thus gives rise to the demand for additional tools, especially in large environments with multiple levels of IT administration.

Required File Auditing Features

File auditing is the process of gathering file, folder and permission change and access attempt information, storing such information, and reporting on that information on a regular basis. It also includes analyzing the information, taking action and evaluating the results of those actions, to sustain compliance, secure information, and ensure consistent delivery of services to end users. Windows file servers and storage appliances natively possess the ability to record audit information, however this information is dispersed throughout the various file servers and storage appliances in the environment and is not centrally aggregated.

File reporting tools are also unavailable for audit data making the collection and reporting steps of change auditing for file, folder and permission access attempts and changes difficult and time-consuming. There is also a risk of losing audit data if event log settings are not set properly to handle the volume of information logged and running out of disk space on servers if too much information is being captured or overwritten. Once native information is analyzed by an administrator experienced with the various system events and messages, the interpretation then would need to result in a decision to act.

Combine these factors and the result is native file auditing is not feasible except for small to mid-sized environments that are adequately staffed to handle the workloads. The following information is a collection of must-have file auditing features. Additional deployment considerations are provided as well.

Automatic Data Collection

In order to efficiently audit file servers, the process must be automated through scripting or a third-party tool. Without it, collecting the information in a timely manner is not feasible. This is especially true as the size of the organization will have a great impact on the raw volume of information collected making it even more challenging to track and report file changes. Special steps must also be taken on servers and domain controllers throughout the environment to facilitate auditing of the information which is by default not enabled.

Additional scripting and/or a third-party file server monitoring tool may also be employed to pre-configure systems in preparation of collecting event data. Furthermore, if audit data is not collected regularly, there is a risk of losing this information due to event log automatic overwrites or disk space issues. This is an important required feature to change auditing because without it, timely auditing is nearly impossible.

Efficient and Centralized Data Storage

Automation of any kind typically requires additional resources and may negatively impact system performance which can lead to bigger problems. For this reason, it's important that the impact of the method employed to automatically collect data is minimal. Furthermore, storage of data must also be a consideration during implementation.

While it is possible to store event and audit data exclusively on the local system where the events are taking place, the preferred method will be to centralize this information in a data store that is both secure and readily available. This leads to numerous additional benefits over time as the need to analyze and report on this information becomes part of a daily routine for the IT administrator or group responsible for the overall health of the various file services.

Collection of information must also be reliable. Occasionally, each piece of the file auditing system should have a periodic check to ensure information is consistent when collected. The most advanced methods of reliably collecting this information will also have the ability to pre-screen data and filter for only essential information. During collection, preference should be given to methods that leverage the existing Windows Event Log and other native audit information as opposed to injected agents or modified core system code for event extraction. Doing so will eliminate any potential system stability issues or future incompatibility problems.

For Windows systems especially, relying solely on event log data may introduce problems because this information is frequently incomplete. To completely understand an event, information from all sources involved must be aggregated and analyzed as a whole. Securing this information for short and long-term storage is also an important consideration and thus best-practices for securing audit data should be included pre-deployment such that no single power-user has access to or the ability to delete or tamper with information. Access to this information should be heavily restricted and monitored.

Scalability

To audit file changes, access attempts and permission adjustments in the enterprise, the solution must be readily scalable to adjust to a constantly changing environment without the need for dramatic steps. Implementation and ongoing use of file auditing will be simplified when no additional software or extensive reconfigurations are required when adjusting to changes within the organization. File auditing should keep pace with all granular changes as the overall topology of the network, domain controllers and Active Directory changes to ensure consistent control to best serve end users and provide an invaluable audit trail for the IT staff.

Advanced Reporting Capabilities

Once data collection from various sources has been automated and stored securely, file auditing can assume a proactive role in sustaining compliance, securing information and improving overall stability. Advanced reporting is necessary to provide IT administrators, management and auditors with customizable summarized report output on every change and access attempt for any time period.

Without the ability to produce clear information on change history for day-to-day modifications to files and folders, such as, who changed shared folder permissions or who deleted an important accounting spreadsheet, sustaining compliance, stability and security will be impossible and many opportunities to improve these functions will be surrendered.

Using SQL to store data and leverage SQL Reporting Services proves obvious choices for storing and reporting on data in primarily Windows-based environments. SQL Server Express Edition with SQL Reporting Services can be downloaded for free from Microsoft and expertise with SQL is common and frequently available. Having the ability to customize ad-hoc and predefined third-party reports will accelerate file auditing efforts by saving time and providing configuration options to suit the majority of needs. Using reports on a daily basis ensures complete visibility over the entire file infrastructure providing opportunities to improve security and sustain compliance.

Additional reporting services such as email alerts and subscription capabilities will also add to the impact advanced reporting will have on overall file systems management effectiveness. Once established, advanced reporting will be the main driver behind a successful sustained file auditing and will become an important part of day-to-day management of the environment.

File Auditing for Storage Appliances

Windows systems are predominant in most environments, however popular appliances such as Dell Celerra and NetApp Filer are also used extensively and require consideration in a comprehensive file reporting solution. These and other similar systems behave in their own unique ways and must be accounted for. Any chosen solution must also place appropriate emphasis on providing automatic, detailed file, folder and permission auditing as well as file access attempt auditing.

Ignoring auditing of these popular storage appliances threatens security and compliance. For these reasons, any file auditing solution will need to include support for these and other platforms and must homogenize report output for administrators. This will save time, resources as well as the needs for additional software and/or vendors and having to learn additional software tools to facilitate file auditing across the enterprise.

File Integrity Monitoring

File Integrity Monitoring, or FIM, ensures the integrity of files by monitoring a hash representation of a file instead of the entire file itself. This approach allows for fast detection of file changes facilitating timely alerting when a change occurs on a file. FIM is also required for PCI compliance. Using file integrity monitoring in a file auditing solution is necessary to provide the highest level of security and change control over data.

Additional Considerations

Preferred solutions (and providers) should offer plug-in or add-on modules and software to help form a cohesive and comprehensive management suite to maximize the potential benefits of change auditing. Some additional types of systems may include firewalls, switches, database servers, SANs, storage appliances and other Microsoft

technologies such as SQL and SharePoint and especially Active Directory and Group Policies. Real-time alerting and object restore features will also add great value to any selected file auditing solution.

Netwrix Approach to File Auditing

The Netwrix approach incorporates all the necessary features for achieving effective file auditing in a software solution. Netwrix Auditor for File Servers helps to track changes made to files, folders, permissions and access attempts across the entire enterprise including many popular filer appliances. It generates audit reports that include the four W's: **who**, **what**, **when**, and **where** for every audited file change, permission change, or access attempt.

It also automatically provides before and new setting values for each file, folder or permission to improve security and change control efforts. The automatic collection and reporting on file changes not only surpasses native capabilities in Windows and storage appliances but expands upon them eliminating the time and effort spent collecting change audit information manually or through complex scripting thereby making this information both reliable and actionable. It has the ability to sustain compliance through historical reporting for up to 7 years and more. File integrity monitoring further extends the oversight on files through advanced change detection methods.

To learn more about Netwrix Auditor for File Servers, please read its overview or download a **free** 20-day trial.

In addition to the solution for file servers, Netwrix offers additional integrated solutions for Active Directory, Group Policy and more helping protect existing investments in current Netwrix product installations. See the full list of the Netwrix Auditor solutions.

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.

Additional Resources

Information security professionals and trends - http://www.infosecisland.com

Articles and commentary on a wide array of IT related topics - http://www.techrepublic.com

Innovative tool and active community of IT practitioners - http://www.spiceworks.com

Focused community on Windows security needs, trends, and information - http://www.windowssecurity.com

10 Immutable Laws of Security - http://technet.microsoft.com/en-us/library/cc722487.aspx

Netwrix Corporate Blog - http://blog.netwrix.com

Netwrix Corporation, 6160 Warren Parkway, Suite 100, Frisco, TX, US 75034

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