Successful File Server Auditing: Looking Beyond Native Auditing

WHITEPAPER

Lepide

1. Introduction

Regular file server auditing helps increase security, protect business critical data and ensure service availability with minimum downtime. File system administrators need to be fully aware of what's happening in their critical files and folders; including file access information, file system events and other activities. In-depth reports on changes to Files, Folders, Shares and Permissions help to maintain a safe and secure File system environment, eliminate security threats and sustain compliance.

File system auditing is no longer simply about the passive auditing of past events. Admins need a system that can generate real-time alerts for critical events, so that necessary actions can be taken to mitigate risks and potential damages. File System auditing solutions also help organizations meet compliance requirements through a centralized pool of File server audit data to help meet various standards such as SOX, HIPAA, and PCI.

2. The importance of File Server auditing

Any unauthorized access to file servers and changes made within them may expose sensitive data leading to potentially expensive losses. Administrators therefore need to monitor in real time who accesses what and when; including what changes were made to shares and permissions. Regular, pro-active auditing of the File Server should be undertaken for a number of reasons:

- To prevent unauthorized access to sensitive business data
- To analyze whether each user has appropriate access rights
- To keep file systems safe from intentional abuses of privilege
- To monitor the activities of privileged users
- To archive changes to enable forensic investigations of events occurring years ago
- To analyze the effective permissions on a shared file or folder by comparing NTFS and Share permissions
- To obtain event details in easy-to-read formats

Other external factors also combine to make File system auditing a necessity:

- Various industry specific compliances such as SOX, HIPAA, PCI etc. lay down a number of regulations that can be fulfilled only through comprehensive auditing
- Performing regular audits of the File systems can instill confidence in various stakeholders and help to increase the reputation of your organization.
- File system auditing can help present event logs in the required format for the purpose of litigation.

3. File Server auditing; what are the options?

3.1 Native Auditing

Native auditing can give you who, what, when and where information on File system changes but requires a disproportionate amount of manual effort – including sorting through a large number of inappropriate log files.

Native File system auditing suffers from a number of drawbacks, including:

- A single event such as copying a file from one location to another could generate multiple raw event logs. Piecing together the relevant information in a readable format can take a lot of time and effort.
- No built-in reports to meet compliance requirements. Admins need to manually go through raw event logs to find the required information.
- Absence of a centralized platform to look into the File system event logs means admins need to visit each file server in the network, set auditing rules and collect the required data manually.

3.2 File System Auditing: Third Party Solutions

There are numerous third-party solutions on the market that help to automate and simplify File Server auditing. Such solutions exist not only to aid organizations with external requirements, like compliance audits, but also to help maintain a secure environment and streamline systems management.

4. A practical approach for the real world

LepideAuditor Suite for File Server is a powerful solution that audits all file servers in the network and generates reports on them. As well as producing reports to satisfy compliance requirements; it ensures that critical business data stored on File systems is safe from the unauthorized access and modifications.

It offers a host of features that will help your organization increase security, simplify systems management and meet compliance. Here are a few of the features included:

- Provides who, what, when and where information for all access attempts and changes made to Files, Folders, Shares and Permissions on the File server.
- Performs the auditing of both Windows File Systems and NetApp Filers
- Reports on all access rights given to users and Files and Folders that they are accessing to give complete control to administrators.
- Consolidates event logs from all File servers in the network and reports and alerts on important event from a centralized platform.
- Archives event logs for a longer period thus helping in staying compliant and forensic investigations.
- Generates real-time alerts on critical events such as unauthorized access to folders containing sensitive data and deletion or modification to important files.
- Dedicated reports to satisfy the regulatory standards of compliances: HIPAA, FISMA, GLBA, PCI, SAS, and SOX
- Generate customized reports to monitor the specific files and folders
- Evaluate the effective permissions on shared files and folders with Current Permission Report
- Historical Permission Analysis to keep a check on the changes in permissions

5. LepideAuditor Suite versus Native File Server Auditing

Feature	LepideAuditor for File Server	Native Auditing
Track File server changes to give Who, What, When and Where information for each change.	Yes	Difficult to identify the changes as there could be multiple log entries for a single change.

Tracks Files and Folders access/share and permission changes.	Alerts and Built-in reports to track File and Folder access related changes.	Need to analyze logs manually to find out such changes.
Compliance support	Long-term archiving and customizable built-in reports help you to stay complaint to industry acts and standards.	Difficult to support long-term archiving and search required information from cryptic logs.
Real-time Alert	Allows you to set instant alerts for the changes that you think are important alerts for the	No
Consolidated Logs	Acts as a centralized platform to collect logs from all File servers in the network and report and alert on them.	No
Reporting on event logs	Offers a number of built-in reports to give detail information about each change.	No built-in reports. Need to get information through Windows event viewer.
Schedule Report feature	Automatic generation and delivery of reports at specified email address.	No
Schedule Report feature	Automatic generation and delivery of reports at specified email address.	No
Easy identification of changes	Highlights different types of changes in different color with old and new value.	No
Long term archiving	Archive event logs for years in secure and efficient storage of SQL server.	A complex process to archive the event logs in files, which may have drawbacks.

Feature	LepideAuditor for File Server	Native Auditing
Current Permission Report	Dedicated Report to evaluate the current effective permissions on the shared files and	No mechanism to compare the currently applied NTFS and Share Permissions on the
Historical Permission Analysis	Compare the permissions on the files and folders between two different intervals. Keep a	It is complex to keep a track of changes in permissions for each file and folder using Event

6. Get an edge over native auditing

LepideAuditor for File Server clearly offers more than native auditing alone. In a world where the majority of security breaches come from the inside, organizations must be vigilant when it comes to auditing their critical files and folders. LepideAuditor for File Server provides administrators with an easy way to track and alert on all aspects of file and folder activity – all without breaking the bank.