netwrix
#1 for change auditing

Tracking File Access for Auditing and Compliance

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

Table of Contents

Introduction

File servers can be among the most critical objects in the IT infrastructure of an enterprise. The importance of a particular server depends on the importance of the files kept there, and an organization generally has one or more file servers storing business-critical and confidential data. If that data is lost or compromised, this can disrupt operations or even jeopardize jobs at the company.

For valuable file servers, precautions against unauthorized access and hardware failure are taken accordingly. However, preventive and protective measures do not help to determine the cause of a contingency, if one does occur. For that purpose, file server operations and security configuration should be constantly audited, enabling you to investigate problems and minimize the effects of adverse changes.

In addition, IT staff has to deal with compliance regulations. SOX, HIPAA, GLBA, and FISMA compliance measures are not dictated by internal needs, but still have to be considered for the enterprise to function smoothly.

Change Auditing for Compliance

Audit data must be kept for a very long time – up to 7 years by some regulations. The scope of the stored data should be sufficient to satisfy any requests from the auditors and be as detailed as possible. Whether an auditor needs to know who opened a sensitive document at a specific point or view a complete history of changes to the permissions on the Projects folder for the past 3 years, the data should be readily available for analysis.

Importantly, the data should clearly indicate who initiated the recorded change. Otherwise, the responsibility for any harm caused by the changes rests with the CIO. The more complete the audit data, the more certainty there is that the actual guilty party will be held responsible for damaging actions.

Why Change Auditing Is Vital

Consider a well-administered file server or storage appliance, such as a NetApp filer or an EMC Celerra system, where file access activity is not audited. This is a common situation, but that does not make it acceptable. Lack of auditing means that any problems related to file access or hardware maintenance cannot be dealt with efficiently.

In fact, most of them are not even discovered. Major problems come to light indirectly and belatedly only when the company starts to feel their consequences – for example, leaked trade secrets, sabotaged accounting records or misplaced project data.

Auditing on its own cannot prevent problems, but it can help do the following:

- Detect problems early
- Find the causes and solve the problems
- Plan for prevention of such problems in the future

These aspects of file server auditing are described in detail below.

Detection

If a problem occurs, it should be discovered as soon as possible, before it can cause an outage or impede operations. The more important the data, the more closely it should be monitored. If a number of business-critical files are deleted accidentally or intentionally, this should be reported the same day. The lost files can then be promptly restored from backup, and the risk of disruptions days later can be eliminated.

Early detection is just as important for some actions that are not nearly as intrusive. Sneaky activity, such as copying large amounts of sensitive or confidential data to removable media, should not fall under the radar. The act of copying is indicated by the presence of a large number of reads, and it is easy to anticipate and track.

Solution

To solve problems that occur on a file server, it is important to have a comprehensive body of specialized audit data. Although the share of useful information found in audit trails is never big, there is no way of knowing in advance which parts will prove meaningful. Solutions often begin with investigations into the causes of problems so that the people responsible can be confronted with the evidence and correct the situation.

For example, an important file, such as a balance sheet or healthcare patient data, may be found to contain invalid or misleading information. To find out who invalidated the file and when it happened, you will need audit trails.

Sometimes, non-restrictive permissions can be set on confidential files so that everybody has access to them. Without an investigation, it may not be clear whether this was done on purpose or what the original permissions were. To look into the matter and restore the permissions, you need a detailed record of what happened.

It may also become necessary to find out where a particular file or folder has gone. To grant such a request, you need the audit data ordinarily considered unimportant.

Anticipation

Experience with problems can be converted to preventive measures. As you resolve file server issues, your security and hardware configuration can evolve.

For example, on a new file server, permissions may not be configured optimally, but after you gather and study file access statistics, you can confidently decide whom to grant access to which resources. On a different note, if the server periodically runs out of disk space because a lot of files are stored there, it may be a good time to increase the server's storage capacity.

Auditing Toolset for File Server Changes

The tools you use for change tracking must be able to cope with the enormous amount of audit data that needs to be sifted through. This section lists the main approaches used in production IT environments.

Native Tools

The Windows native file auditing system and tools such as Event Viewer are an entry-level solution. They have the advantage of requiring no customization or third-party software, but even in a mid-size IT infrastructure, they are not suitable for performing any meaningful change management.

The native object auditing system, which supports auditing of files, provides very low-level events. It creates numerous log records for even a single action, such as copying a file. This makes the manual examination and correlation process inefficient and painful.

Even with a well-designed change management strategy, native tools cannot significantly reduce the effects of adverse changes, due to the high latency between the change and its discovery, and lack of reporting capabilities. A change is not examined until after it has caused some negative results such as service failure or slowdown of operations.

The time between an unwarranted change and its undesirable effects can be very short, and change detection automation is very important to ensure a timely response. However, if the administrator is armed with only native tools, a change-induced problem might take a week or longer to solve.

Building versus Buying

The search for automation and analysis methods can lead a company to invest in in-house software. The range of technologies that can be employed is wide. PowerShell, the .NET framework, and many other programming and scripting languages have bindings for Active Directory and Windows APIs, which are extensively documented.

The following tasks are well-suited for automation:

- Subscribing to events – watching for the events you anticipate is very efficient as long as you know what kind of event you are looking for.
- Handling event logs – backing up, archiving, and clearing logs for compliance and auditing continuity.
- Querying for events – centralizing the search for events and making it more efficient.

This list continues, depending on the specific needs of an organization. In fact, it can grow quite long, due to the comprehensive scope of available functionality.

The effectiveness of in-house development is determined not so much by what is possible to do as by what can be done in the given time with the available resources. If the company does not specialize in change auditing

software – and most companies do not – then the time and resources are bound to be too scarce for comfort. Even if the in-house solution is good, its development is certain to face problems:

- Support – the software produced in house may have many authors, which increases support difficulty; in addition, such a solution may evolve organically and is not likely to be centralized.
- Testing – new software does not normally go into production use until it has undergone extensive tests, which require a lot of time and expertise.

In-house scripts and programs may be the optimal solution for some companies, but this is a rare case in large distributed environments that have to accommodate internal and remote clients, heterogeneous systems, and so on. Often, a more cost-effective and better-quality alternative is to purchase third-party software specifically designed for file server change auditing.

Third-Party Software

When it comes to choosing a third-party solution for file server change auditing, a great variety of available software seems to fit the bill. The final decision can be influenced by many factors, such as the following:

- Transparency of information about the product's capabilities
- Quality-price ratio
- Cost of ownership

When the choice is made, it is important to remember that the tools alone cannot solve complex file server change auditing, tracking, and management problems.

Success Recipe

To be effective at tracking file server changes, it is important to have a sensible strategy and software tools that are flexible enough to meet all your needs but do not get in the way of your strategy. Good change auditing tools, together with a sound audit policy, have the additional benefit of helping you improve the management of your file servers.

The Smart Choice: Netwrix Auditor for File Servers

Netwrix Auditor for File Servers incorporates knowledge and understanding of the needs of file server change auditing personnel. It is a cost-effective solution offering competitive functionality for a low price. Netwrix Auditor places change information directly at the administrator's fingertips, without the need to extract it by roundabout methods.

The advanced reports provided with the product are based on the SQL Server Reporting Services technology and are suitable for ensuring SOX, HIPAA, GLBA, and FISMA compliance. Another feature essential for compliance is a long-term archival of audit data.

There is also an alternative freeware tool which can be used indefinitely, and is suitable for small businesses with lenient auditing requirements. The fully functional solution is available as a **free** 20-day trial.

About Netwrix Corporation

Netwrix Corporation is the leading provider of change auditing software, offering the most simple, efficient and affordable IT infrastructure auditing solutions 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