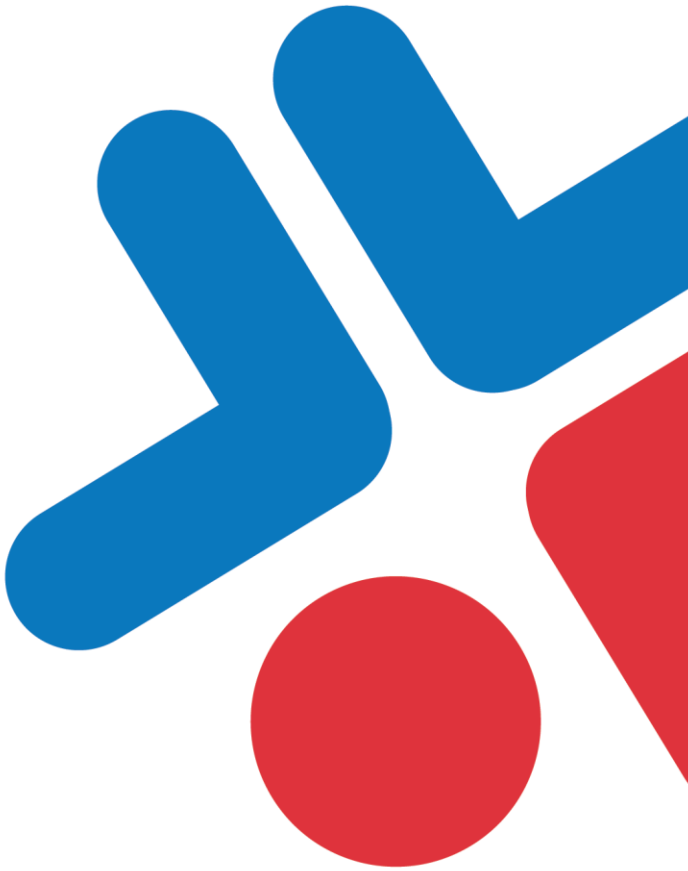
netwrix
#1 for change auditing

Auditing SQL Server for Change Tracking and Compliance



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

Table of Contents

Introduction

Databases and database servers can be among the most critical objects in the IT infrastructure of an enterprise. Their importance depends on the value of the stored data, which can be business-critical and confidential. If that data is lost or compromised, this can disrupt operations or even jeopardize jobs at the company.

For valuable database servers, precautions against unauthorized access and hardware failure are significant. However, preventive and protective measures don't help to find the cause of a contingency if it 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 so the enterprise can function smoothly.

This white paper describes approaches to change auditing for the most widespread database management technology used by businesses today: Microsoft SQL Server.

Change Auditing for Compliance

Audit data must be kept for a very long time, up to 7 years according to 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 gained access to a particular database at some point or view a complete history of security settings on a selection of databases for the past year, the requisite data should be readily available for analysis.

The diversity of the regulations makes it necessary to ensure that the audit data is copious and highly detailed. Otherwise, the organization runs the risk of noncompliance.

Why Change Auditing Is Vital

Consider an SQL Server that is not audited for administrative activity. This is a common situation, but that does not make it acceptable. If there is no auditing, any problem related to security, data loss, or maintenance cannot be dealt with efficiently. In fact, most of them are not even discovered. Only major problems come to light indirectly and belatedly when the company starts to feel their consequences—for example, leaked trade secrets, sabotaged personal data, or malfunctioning business applications.

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 SQL 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 hosted by a database server, the more closely it should be monitored. If database schema modifications occur (for example, new tables are added, columns are altered, views or indices are created), this can have undesirable consequences such as data leakages or privilege elevation. Such situations should be reported the same day they occur and promptly scrutinized before they can impact business.

Changes to server instance parameters are significant events that should be immediately examined because they can affect all databases residing on the server instance. Even such sneaky activity as creation of new database logins should not fall under the radar because this might be the first step to data leakage. Such actions are easy to anticipate and track.

Early detection is just as important for some actions that are not nearly as intrusive. For example, it is a good idea to monitor creation of databases to prevent production SQL servers from being cluttered with unnecessary databases. If the audit data is at hand, you can ask the DBA responsible for any new database about the purpose of that database.

Solution

To solve problems that occur with multiple SQL servers in an organization, especially if they are managed by multiple DBAs and operators, 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, a database or a table in a database can be deleted unexpectedly. To find out who did this and when it happened, you will need audit trails.

Sometimes, changes to stored procedures can render database applications unworkable and cause privilege elevations — for example, if the modifications concerned the logic that checks access rights based on some internal access controls managed by the database application. Without an investigation, it may not be clear whether this was done on purpose or what the original stored procedure did. To look into the matter and restore the configuration, you need a detailed record of what happened.

Application

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

For example, to ensure that SQL Server security conforms to the established enterprise policy, all changes to security roles should be tracked and analyzed. On a different note, studying the rate of database creation can help a person analyze trends and make plans for storage space increases.

System administrators of applications relying on databases (such as CRM systems and data analysis tools) should also keep track of changes made by database administrators to be aware of all changes that can potentially impact their applications. They need detailed change reports on databases using their applications.

Auditing Toolset for SQL 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 examined. This section lists the main approaches used in production IT environments that rely on the Microsoft SQL Server technology.

Bundled Tools

The auditing facilities bundled with SQL Server are an entry-level solution. The SQL Server C2 log is contained in a database, and you can work with it using SQL Query Analyzer. The other main audit trail, Error log, is text-based and lends itself to parsing.

These tools 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 because the manual examination and correlation process is inefficient and painful.

In addition, business applications relying on SQL Server databases (such as CRM and ERP systems) may offer their own high-level auditing facilities, which may be reliable and convenient. However, these tools cannot detect actions that specifically bypass them — for example, using SQL Query Analyzer to secretly modify roles and logins and gain unauthorized access to data in an ERP database. You still need low-level auditing to cover all activity.

Even with a well-designed change management strategy, bundled tools cannot significantly reduce the effects of adverse changes because of 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, but 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 other programming and scripting languages have bindings for the SQL Server.

The following tasks are well-suited for automation:

- Subscribing to events and SQL Server trace logs—watching for the events you anticipate is very efficient as long as you know what kind of event you are looking for.
- Handling text-based logs — parsing, 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 might be longer, depending on the specific needs of an organization. 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 it is possible to do but by what can be done in the given time with the given resources. If the company does not specialize in database server change auditing software — and most companies do not — the time and resources necessary 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 or 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. More often, a more cost-effective and better-quality alternative is to purchase third-party software specifically designed for SQL Server change management.

Third-Party Software

When it comes to choosing a third-party solution for SQL 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:

- 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 on their own cannot solve complex SQL Server change auditing, tracking, and management problems.

Success Recipe

To be effective at tracking SQL 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 SQL servers.

The Smart Choice: Netwrix Auditor for SQL Server

Netwrix Auditor for SQL Server incorporates knowledge and understanding of the needs of SQL Server change auditing personnel. It is a cost-effective solution offering competitive functionality for a low price. It places change information directly at the administrator's fingertips, so he or she does not need to extract it using roundabout methods.

For each captured change, all possible detail is shown: who made the change, when it happened, the "before" and "after" settings, and so on.

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

To learn more about Netwrix Auditor for SQL Server, please read its overview or download 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 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