Craig S. Mullins

Return to Home Page

Vol. 14, No. 3 (Winter 2007)

From IDUG Solutions Journal...

The Buffer Pool

Compliance Needs Drive Data Access Auditing Requirements

By Craig S. Mullins

In this day and age regulatory compliance has become a critical aspect of the IT landscape, and nowhere is it more crucial than within the realm of database management. More and more regulations are being passed that dictate increased effort be exerted to better secure and protect the accuracy and privacy of enterprise data. And because this data typically is housed within a database, DB2 database

administrators and technicians are being asked to comply with these regulations.

The Regulatory Environment

What regulations you ask? Well, there are many, so let's just talk about a couple of the high visibility regulations. Unless you have been living under a rock you've at least heard about the Sarbanes-Oxley Act (SOX). The goal of SOX is to regulate corporations in order to reduce fraud and conflicts of interest, to improve disclosure and financial reporting, and to strengthen confidence in public accounting. Section 404 of this act, the one giving IT shops fits, specifies that the CFO must do more than simply vow that the company's finances are accurate; he or she must guarantee the processes used to add up the numbers. Those processes are typically computer programs that access data in a database, and DBAs create and manage that data as well as many of those processes.

Consider also the Health Insurance Portability and Accountability Act, more commonly referred to simply as HIPAA. This legislation contains language specifying that health care providers must protect individual's health care information even going so far as to state that the provider must be able to document everyone who even so much as looked at their information. Think about that? Could you

produce a list of everyone who looked at a specific row or set of rows in any database under your control?

And then there is PCI DSS, which stands for Payment Card Industry (PCI) Data Security Standard (DSS). It was developed by the major credit card companies to help prevent credit card fraud, hacking and other security issues. A company processing, storing, or transmitting credit card numbers must be PCI DSS compliant or they risk losing the ability to process credit card payments. Given the availability and volume concerns of payment card transactions this information is typically stored in an enterprise database.

So DBAs have expanding requirements for assuring that databases are protected such that only properly authorized entities have access to only the specific data they need in order to do their jobs – and to be able to prove this.

Being able to track who did what to which piece of data and when is important because there are many threats to the security of your data. External agents trying to compromise your security and access your company data are rightly viewed as a threat to security. But industry studies have shown that the majority of security threats are internal – within your organization. Indeed, some studies have shown that internal threats comprise 60% to 80% of all security threats. The most typical security threat comes from a disgruntled or malevolent current or ex-employee that has

valid access to the DBMS. Auditing is crucial because you may need to find an unauthorized access emanating from an authorized user.

Tactics for Compliance

So how can organizations ensure they are in compliance with these regulations (and others)? Data access auditing, sometimes simply called database auditing, can be enabled to track the use of database resources and authority. When auditing is enabled, each audited database operation produces an audit trail of information. The audit trail will show which database objects were impacted, what the operation was, who performed the operation, and when it occurred. This comprehensive audit trail of database operations produced can be maintained over time to allow DBAs and auditors, as well as any authorized personnel to perform in-depth analysis of access and modification patterns against data in the DBMS.

Sounds good, you might say, let's turn it on! Well, don't be so quick there. As with any technology there are multiple considerations that you need to understand and deliberate upon before you move forward.

Of course, before you do anything, you will need to classify your data and match each data element against the regulations that apply to your organization. To be able to accomplish this feat requires input from subject matter

experts (business folks), legal experts (corporate counsel), and information technology (data architects and DBAs). And the output will differ for every organization because of the many variations in terms of technical database implementations and the different regulations that apply to each business.

After you have armed yourself with your compliance roadmap you will then need to determine what level of data access auditing is required. But it is not as simple as this. You will need to compile a list of the types of questions that you want your data access auditing solution to be able to answer. A good database access auditing solution should be able to provide answers to at least the following questions:

1. Who accessed the data?
2. At what date and time was the access?
3. What program or client software was used to access the data?
4. From what location was the request issued?
5. What SQL was issued to access the data?
6. Was the request successful; and if so, how many rows of data were retrieved?
7. If the request was a modification, what data was changed? (A before and after image of the change should be accessible)

Of course, there are numerous details behind each of these questions. A robust auditing solution should provide an independent mechanism for the long-term storage and access of audit details. The solution should offer the canned queries for the most common types of queries, but the audit information should be accessible using industry standard query tools to make it easier for auditors to customize queries as necessary.

Additionally, you will need to consider any additional type of database auditing you want to accomplish. A common need is to be able to track SYSADM accesses. As DB2 professionals know, users with SYSADM authority (usually DBAs) have carte blanche access to the DB2 subsystem and all of its data. Of course, DBAs are trusted agents and most will not abuse the overarching security access granted to them. But a data access auditing solution can verify that by tracking all SYSADM accesses, which will make both your DBAs and your internal auditors happy. The DBA gets to keep the SYSADM authority thereby allowing the DBA to perform his or her job – and the auditor gets to monitor the DBAs activities to ensure that the DBA is being above board.

Data Access Auditing Techniques

So far, so good, but let’s dive down to another level of detail and examine how data access auditing solutions produce detailed audit trails. There are several popular techniques

that can be deployed so we'll briefly discuss four techniques them and highlight their pros and cons.

The first technique is trace-based auditing. This technique is usually built directly into the native capabilities of the DBMS. Commands or parameters are set to turn on auditing and the DBMS begins to cut trace records when activity occurs against audited objects. Although each DBMS offers different auditing capabilities, some common items that can be audited by DBMS audit facilities include:

- login and logoff attempts (both successful and unsuccessful attempts)
- database server restarts
- commands issued by users with system administrator privileges
- attempted integrity violations (where changed or inserted data does not match a referential, unique, or check constraint)
- select, insert, update, and delete operations
- stored procedure executions
- unsuccessful attempts to access a database or a table (authorization failures)
- changes to system catalog tables
- row level operations

The problems with this technique include a high potential for performance degradation when audit tracing is enabled, the database schema will need to be modified to turn auditing on and insufficient granularity of audit control, especially for reads.

Another technique is to scan and parse the database transaction logs. Every DBMS uses transaction logs to capture every database modification for recovery purposes. Software exists that interprets these logs and identifies what data was changed and by which users. The drawbacks to this technique include the fact that reads are not captured on the logs, there are ways to disable logging that will cause modifications to be lost, performance issues scanning volumes and volumes of log files looking for only specific information to audit and the difficulty of retaining logs over long periods for auditing when they were designed for short-term retention for database recovery.

The third technique is to sniff packets for database requests as they cross the network. By capturing the SQL statements as they cross the network an audit trail of all database requests that go over the network can be produced. Of course, the problem here is that not every request goes across the network. For example, a DB2-CICS application where all of the work is mainframe-resident does not require TCP/IP and therefore this work will not be captured. Same

thing goes for SPUFI requests or for non-mainframe folks any DBA work done right on the server.

The fourth data access auditing technique is proactive monitoring of operations at the database server level. This technique captures **all** SQL requests as they are made. It is important that all SQL access is audited, not just network calls, because not every SQL request goes over the network. Proactive audit monitoring does not require transaction logs, does not require database schema modification, and will be highly granular in terms of specifying what to audit.

Synopsis

DBAs are being asked to more closely protect corporate data in their databases and to monitor who does what to which data when. Data access auditing solutions can help organizations to meet this growing compliance requirement.

From *IDUG Solutions Journal*, Winter 2007.

© 2008 Craig S. Mullins, All rights reserved.
Home.