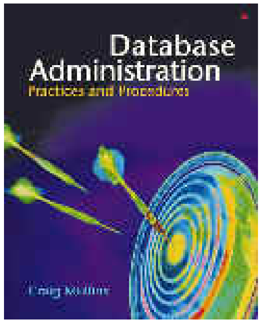
Craig S. Mullins

Return to Home Page

July 2005

DATABASE TRENDS AND APPLICATIONS



The DBA Corner

by Craig S. Mullins

Database Auditing

Auditing is a facility of the DBMS that enables DBAs to track the use of database resources and authority. When auditing is enabled the DBMS will produce an audit trail of database operations. Each audited database operation produces an audit trail of information including what database object was impacted, who performed the operation, and when. Depending on the level of auditing supported by the DBMS, an actual record of what data actually changed also may be recorded.

Tracking who does what to which piece of data 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 eminating from an authorized user.

But keep in mind that auditing tracks what a particular user has done once access has been allowed. Auditing occurs post-activity; it does not do anything to prohibit access. Audit trails help promote data integrity by enabling the detection of security breaches, also referred to as intrusion detection. An audited system can serve as a deterrent against users tampering with data because it helps to identify infiltrators.

There are many situations where an audit trail is useful. Your company's business practices and security policies may dictate a comprehensive ability to trace every data change back to the initiating user. Perhaps government regulations (such as the Sarbanes-Oxley Act) require your organization to analyze data access and produce regular reports. You may be required to produce detailed reports on an ongoing basis, or perhaps you just need the ability to identify the root cause of data integrity problems on a case-by-case basis. Auditing is beneficial for all of these purposes.

A typical auditing facility permits auditing at different levels within the DBMS, for example, at the database, database object level, and user levels. One of the biggest problems with DBMS audit facilities can be performance degradation. The audit trails that are produced must be detailed enough to capture before- and after-images of database changes. But capturing so much information, particularly in a busy system, can cause performance to suffer. Furthermore, this audit trail must be stored somewhere which is problematic when a massive number of changes occur. Therefore, most auditing facilities allow for the selective creation of audit records to minimize performance and storage problems.

Additionally, third party vendors offer products that scan the database logs to produce audit reports. The DBMS must create log files to assure recoverability. By scanning the log, which has to be produced anyway, the performance impact of capturing audit information can become a non-issue.

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

When the DBMS does not support the level or type of auditing required, log analysis tools from third party ISVs can be purchased to retrieve most types of information from the database transaction log.

Each DBMS provides different means to view the audited data. Formatted reports and graphical reporting tools that read and present the audit information in a reasonable manner make it easy to identify security problems from among many recorded database operations.

If you have turned on database auditing at your site, consider the following advice:

- Auditing can be a large consumer of system resources. When the audit queue is full, tasks that generate audit records will wait until the auditing task can resume. Consider using a larger audit queue if performance suffers. As a last resort, discontinue auditing when performance is unacceptable.
- Place the system catalog tables that store security-related information on a separate, inactive disk. This may enhance auditing performance by decreasing disk contention.
- Be careful to ensure that the data set or table used to store audit data does not fill up. When the audit data set is full, auditing will be disabled, records in the current audit queue will be lost, and any user task attempting to send data to the audit queue will be cancelled.

Database auditing can be a crucial component of database security and compliance with government regulations. Be sure to study the auditing capabilities of your DBMS and to augment these capabilities with third party tools to bolster the auditability of your databases.

From Database Trends and Applications, July 2005.

Home.