Database security

Law, Security

The need for the security of the database has evolved from the simple protection of the unauthorized retrieval or use of the data to the current detection of the possible database attacks from an enemy (Newman, appecinc. com). Since the database contains sensitive data of a firm, one way to provide security is to have auditing or monitoring software such as SQL Server. The following propositions will give simple instructions on using the SQL server for auditing. During installation, the user will be prompt to enter a destination to put the audit logs, the tabulated data showing vital information on monitoring.

After the installation has been done, there are several ways to enable auditing of the use of the database. One way is to use the native auditing system which is the traditional and the easiest form of auditing (Newman, appecinc. com). This is sometimes also referred to as login auditing since it only considers the login logout activity of those users that are connected or trying to connect to the information on the database. To enable this application, first, open the Enterprise Manager, select Properties and under the Security heading, you will be asked to select the security level you intended to apply.

This includes options such as “ NONE”, “ SUCCESS”, “ FAILED”, and “ ALL” that specifies the attempt to enter the database (Policht, databasejournal. com). Since this is the simplest, it has many limitations such as it does not record the user’s actions when it has successfully login. Also, it has a tendency to result to an information overload since it has no filter for the users ID. These and some other limitations have been the basis for the creation of the SQL Server. To audit other information or objects such as who

wants to login, which query did he execute and what actions did he invoke to utilize, the SQL Server should be put into use.

Note that if you will use the SQL Server, you must not enable the login auditing since it will only cause the system to write the same set of data to two different locations. To enable the SQL Server, open the CMD prompt and type The previous executable statement will only work if you are the database administrator (Howie, Microsoft Technet). If you intend to use an authorized account then, you must type After doing the above instruction the SQL Server is now activated, though there are some specifications to be done in order o make the auditing.

There are two options available for the user – either C2 auditing or the Server Side Traces. To make use of the C2 editing, just type the following executable statements Note that you can only type the ‘ reconfigure’ if there are no errors occurring after executing the first statement. If errors occur, then you must encode the following After reconfiguring has been executed you must restart the auditing, since it will monitor actions with new specifications defined in the reconfiguration (Polícht, databasejounal. com). After the activation, it is a must that the administrator must learn about log files.

The software will write the audit logs into the destination with the format of YYYYMMDDHHMMSS. trc that specifies the exact time of creation of the log files. A log file can hold as much as a volume of 200MB. After the said volume has been achieved, it will automatically create a new log file provided that there are free spaces in the disk where the log files are saved. In the case that the disk became full, the operation of auditing will be

stopped and will only be resumed if the administrator has solved the problem. To open the log files created, use the SQL Profiler and open the Trace file using the Open instruction on the File menu.

Note that you cannot open the log file that the server was currently writing. If you wish to or you need to, you must first stop the operation or wait until the desired volume has been achieved. The log file will show the administrator objects such as operations performed, who performed the operation and what time is has been executed (Howie, Microsoft Technet). This operation is really essential for monitoring but it may be the cause overflow or overload of information since it will audit all transaction, even those that do not poses any threat or are ordinary operations.

The administrator, then, has to look and read all lines of audit logs, even if it has no sense to dos so. This problem can be reduced by using the other option inherent in the SQL Server – the Server-Side Traces. The Server-Side Traces eliminates the audit logs that are not important in monitoring or auditing. Since not all data in a database are sensitive or top secret, the administrator can specify which transaction about the sensitive data has taken place, thus, improving efficiency. A sample code for the activation and configuration of this feature is given below.