An Auditing Facility for DB2/VSE

The SQL/Auditing Facility ("**SQL/AF")** records how users and programs access sensitive or vital corporate data in designated DB2/VSE tables.

SQL/AF performs its auditing functions in the database server. Therefore, it is capable of auditing all DB2/VSE clients, including those that connect using the DRDA protocol.

SQL/AF monitors access to the tables defined as auditing candidates in the SQL/AF **RULES** dataset. Both interactive and compiled program access is subject to auditing. Depending on the auditing rules defined, both read (SQL SELECT) and write (SQL DELETE, INSERT and UPDATE) access is monitored. By default, all table columns are audited so that SQL statements are recorded, whenever they access the table. Alternatively, one or more table-columns can be defined in the RULES. Auditing then occurs when an SQL statement refers to one of the specified columns.

Audit Log

For each access to an audited table or table-column, the Audit Processor writes a record in a file, called the **SQL/AF audit log**. An audit record contains the **context** of statement execution (date, time, program name, user name, terminal name) and the **text** of the SQL statement **as executed by DB2/VSE**. To achieve this, statement variables are replaced with their contents and additional transformations are carried out when needed (for example, when views are used to access audited tables).

Log Archiving

The SQL/AF **archiving** function transfers the audit log to tape, so that auditing results can be kept for a longer period of time. Archiving must be scheduled explicitly. An archive does not disrupt the auditing process.

Inspecting the Audit Log

A part of the SQL/AF user interface, the **Logscan** program interactively searches the audit log or an audit archive tape for specific audit events. To perform the log scan, the user formulates a number of search criteria.

Following search criteria can be supplied:

- One or more **audit record fields**. This provides for scan requests such as:

  Search all accesses made by a named user to a named table during a specified period.

- **Table column-names** used in the text of an audited SQL statement.
  This scan method selects statements that reference a named table-column, for example:

  Search all statements that selected the column CONFIDENTIAL in the customer table

- **Table column values** used in the text of an audited SQL statement.
  This scan method selects statements that reference a named table-column with a specified value. It can be used to trace all audit events for a given table "key", such as:

  Search all accesses made to the EMPLOYEE table for EMPNO = 100 during a specified period.

Audit request queueing

The *Audit Initiator* component executes in the database server, the *Audit Processor* executes in its partition. SQL/AF uses **dataspaces** as a physical support for the audit request queue. This will significantly improve performance.

Prerequisites

- VSE/ESA Version 2 Release 4 or later.
- DB2/VSE Version 3 Release 3 or later.
- The Monitoring Facility, a program product available from Software Product Research.
-