SQL/AUDITING FACILITY

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

SQL/AF performs its auditing functions in the virtual machine of the database server. Therefore, it is capable of auditing all DB2/VM 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 CMS 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/VM**. 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 may be scheduled explicitly. It may also occur implicitly when the audit log is full or when a defined number of audit requests have been stored. 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.

  Search all updates made by a named program to a named table on a specified date.

- **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.

TableName	**SQLDBA.EMPLOYEES**		
AuditDate	**1996-04-16**	**Time**	**14:42:55**
Database	**TSTDB2**	**SQL_User**	**TSTAST2**
VM_User	**TSTAST2**	**Terminal**	**T25TT261**
ProgCrea	**SQLDBA**	**ProgName**	**GD40A**
Section	**6**	**Commit**	**Y**
Commtype	**SELECT**	**Rows_Proc**	**1**
SQLCODE	**0**	**SQL_LUW**	**478875**

```
SELECT EMPNO, DEPTNO, EMPNAME, STATUS
FROM SQLDBA.EMPLOYEES WHERE EMPNO = 100
```

Logscan output screen

Section Authorities

When requested, SQL/AF will implement a new security concept, called **section authorities**, as an extension to the **table** and **package authorities** provided by DB2/VM.

In the DB2/VM authorization schemes, a user with the RUN privilege on a program is able to execute all SQL statements contained in that program. With SQL/AF section authorities defined, the user will also need DB2/VM **table authorities** to successfully execute a program section that accesses an audited table.

Using section authorities, operations on audited tables can be restricted more easily to one or more named users.

Audit request queueing

The *Audit Initiator* component executes in the database server, the *Audit Processor* executes in its own virtual machine. By default, the Initiator and the Processor exchange data using IBM's **IUCV** communications protocol. However, when the necessary hardware is available, SQL/AF will use **dataspaces** as a physical support for the audit request queue. This will significantly improve performance.

Data Compression

With VM/ESA Version 2 installed, SQL/AF may be requested to use data compression when writing to the audit log. With data compression, the disk space required for the log will be significantly reduced.

Customizing SQL/AF

An installation may provide an **audit user exit** to be invoked by the Audit Processor for every audit log record written. The exit is written as a REXX program.

Benefits

Centralized auditing as implemented by SQL/AF offers the following benefits:

- SQL/AF controls **all** table access. It monitors accesses from both compiled applications and dynamic query environments.

- Auditing is done for all clients of DB2/VM: VM/ESA, VSE/ESA, OS2/DB2 and other database platforms that can connect to DB2/VM. In environments that integrate mainframe and PC applications, the security aspect of PC access to DB2/VM tables can be controlled entirely using SQL/AF.

- The SQL/AF auditing rules are easy to implement, they can be modified at any time and they take immediate effect.

- The auditing rules provide for very granular auditing, up to the table column level.

- Auditing has no impact on application program coding.

- SQL/AF avoids the cost and the additional quality assurance of application implemented auditing procedures.

- SQL/AF stores its audit events in the form of SQL statements. Since the SQL/AF logs are regular CMS files or tapes, they can be exploited easily by user procedures. Moreover, the historical access information contained in the logs, may be valuable input for new or existing business applications.

Prerequisites

- VM/ESA Version 1 Release 1 or later.
- DB2/VM Version 3 Release 3 or later.
- The Command Capturing or the Monitoring Facility, both program products available from Software Product Research.