# RECORDING DATA ACCESS ON DB2 FOR z/OS

In today's distributed environments, protecting sensitive corporate data is of vital importance. While mainframe security software and DB2 privileges protect against unauthorized access to DB2 tables, they do little to comprehensively report all accesses to DB2 tables and what was done within those tables. In the wrong hands, confidential information can have a negative impact on a corporation and affect the privacy of customers and employees. Furthermore, in many countries, laws have been instituted to protect against unauthorized disclosure of such information.

- DB2 provides access controls to ensure that only authorized users access the data.
- The DB2 audit trace facility records how users access sensitive tables.
- DB2 log analysis shows the actual modifications to the data.

These DB2 facilities are not sufficient to fully record all access to sensitive data:

- Log Analysis will not show read (SELECT) access.
- The DB2 audit trace will record only the **first** read or write table access in a logical unit of work.
- The trace records do not provide the contents of the input variables submitted with the SQL statement. Without these data, access recording is not complete.
- DB2 auditing requires that auditing trace be enabled. If many tables are audited or intensively used, the operating cost of tracing may be excessive.

## DBARS

**DB2 Access Recording Services** is a product developed by Software Product Research.

- DBARS records all accesses to sensitive DB2 tables.
- DBARS records both read (SELECT) and write (DELETE, INSERT and UPDATE) access.
- DBARS records SQL statements with their associated input variables ("host variables").
- For each access to an audited table, DBARS inserts into its Recorder:
    - The text of the SQL statement
    - The context of statement execution:
        - the date and time of execution
        - the identification of the user submitting the statement
        - the z/OS job name
        - the name of the application program
        - the number of rows modified
        - the SQLCODE indicating successful or failing access
        - if distributed access: the names of the external server, application and workstation

### REPORTING FROM THE RECORDER

The DBARS Reporting functions search the Recorder for specific events, using the following criteria:

- Recorder columns
- Audited table column names used in the recorded SQL statement. This will show all SQL statements that reference the table column.
- Audited table column names and values, to show all SQL statements that reference the column with the specified value. This option may be used to report all recorded access for a given table "key".

### ARCHIVING THE RECORDER

The DBARS archiving function transfers the Recorder to tape, to a flat file or to a DB2 table, so that recorded information can be kept for a longer period of time. An archive operation will not disrupt the recording process. DBARS supplies functions to scan its archives for specific events.

## DBARS Alerting

The DBARS "RULES" dataset specifies the conditions for generating a DBARS alert. When an SQL statement meets these conditions, an entry is made into the DBARS Exception table. Alternatively, an installation may provide a user-written REXX program to handle the alert. In addition, DBARS may be requested to transmit the alert to a Windows Event Log, where it can be exploited by third-party software, such as big data systems

## DB2 Access Blocking

The DBARS "RULES" dataset specifies the conditions for blocking DB2 accesses. When an SQL statement meets one of these conditions, DBARS abnormally ends the application and records the statement into the Recorder. Blocking is based on user-name, table-name, program-name, job-name, IP-address, execution time, type of access or a combination of these parameters. Because the DBARS blocker executes in the DB2 address space, it is able to block any SQL statement, whatever its origin.

## Customizing DBARS

Data recorded by DBARS can be archived to a DB2 table, for subsequent processing by customer procedures. An installation may provide a REXX user exit to be invoked when an access is stored in the Recorder. The exit receives the Recorder data columns as its input arguments.

## Connecting DBARS to an ESM

When connected to an external security manager, DBARS will act as an auditing agent for DB2 on z/OS.

Connection with the ESM is achieved either by FTP-ing the DBARS data to the ESM or by direct TCP/IP communication between the DBARS Writer and the ESM.

## Benefits

- DBARS provides all functions needed for auditing access to sensitive data in DB2 tables.
- DBARS has its own proprietary interface to DB2 and does not depend on DB2 tracing. As a result, recording overhead will be extremely low.
- DBARS is able to block fraudulent access to DB2 data.
- In an ESM environment DBARS will act as an agent for DB2 on z/OS.
- Even when DBARS is not used in an auditing context, it still provides valuable recording services:
  - In development and QA environments, DBARS will show whether applications perform adequately and whether correct SQL is submitted.
  - In operational environments, DBARS will record all DB2 accesses for designated tables. Using the DBARS archiving facility, an organization may keep an historical track of these accesses for an unlimited period of time.