DB2 FOR z/OS

RECORDING ACCESS TO SENSITIVE DATA

In today's distributed IT environments, protecting sensitive and confidential corporate data is of vital importance. However, it is often difficult for system security personnel to determine how and where such data are accessed.

- DB2 provides access controls to ensure that only authorized users access the data.
- The DB2 audit trace facility will record how users access sensitive tables.
- DB2 log analysis will show 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 audit trace records only the first read or write SQL statement in a logical unit of work.
- The trace records do not provide the contents of the input variables submitted with the SQL statement. Without this information, full access recording is not possible.
- DB2 auditing requires that an 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 ("**DBARS**") is a product developed by Software Product Research.

- DBARS records all accesses to sensitive DB2 tables. Both read (SELECT) and write (DELETE, INSERT and UPDATE) access is recorded.
- DBARS records SQL statements with their associated input variables ("host variables").
- If requested, DBARS will mask data values in the recorded SQL statement text.
- DBARS is able to issue alerts on unusual DB2 accesses.
- Using installation specified rules, the DBARS blocking facility is capable of prohibiting DB2 access at the SQL statement level.
- DBARS provides a powerful Recorder scan function.

Because DBARS has its own interface to DB2 and does not depend on DB2 tracing, recording overhead is extremely low.

THE DBARS RECORDER

For each access to an audited table, DBARS inserts following data into the 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

During product installation, the DBARS Recorder is implemented as a DB2 table, a VSAM cluster or a sequential BSAM dataset.

Reporting from the Recorder

The Recorder Scan functions search the Recorder for specific access events. The user supplies one or more of the following search 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 a sequential dataset or to a DB2 table, so that recorded information can be kept for a longer period of time. An archive operation does not disrupt the recording process. The product supplies a utility to scan an archived Recorder using the search criteria, described above.

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 abends the application and writes the statement to the Recorder with a "blocked" indicator. Blocking may be based on username, tablename, programname, jobname, 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 access, whatever its origin.

Customizing DBARS

Data recorded by DBARS can be stored in a DB2 table, for subsequent processing by customer procedures. In addition, 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 External Security Manager

When connected to an external security manager (such as the Oracle Audit Vault and Database Firewall®), DBARS will act as an auditing agent for DB2_for_z/OS. The DBARS FTP task will transfer the auditing data intercepted by DBARS to the ESM for further processing. The DBARS reporting, alerting and archiving functions are then performed by the ESM.