# 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 however are not sufficient to fully record all accesses 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. If all accesses should be recorded, audit policies should be activated.
- To fully record an access, several Db2 trace points will be necessary, for example to record the contents of the host variables used by the SQL statement.
- The operating cost of Db2 audit tracing may be prohibitive, even when audit policies are in use.

## The DBARS Solution

"Db2 Access Recording Services" is a product developed by Software Product Research.

- DBARS records all accesses to sensitive Db2 tables, both read (SELECT), write (DELETE, INSERT and UPDATE) and all data definition statements (CREATE, ALTER etc.)
- DBARS records SQL statements with the contents of the associated input variables ("host variables").
- DBARS has a proprietary interface to Db2 and **does not depend on Db2 tracing** for its recording operations.
- For each access to an audited table, DBARS inserts into its Recorder:
    - The text of the SQL statement
    - The context of statement execution:
        - date and time
        - identification of the user
        - z/OS job name
        - name of the application program
        - number of rows modified
        - SQLCODE indicating successful or failing access
        - if distributed access, the names of the external server, application and workstation
- The DBARS Recorder is defined during installation as a VSAM cluster or a sequential dataset. The Recorder may be shared between multiple Db2 systems and DBARS instances.
- When DBARS is connected to external security software, these data are not written to the Recorder, but passed to the ESM.

## Reporting from the Recorder

DBARS Reporting searches the Recorder for specific events, based on:

- The contents of the Recorder columns
- The audited table column names used in the recorded SQL statement.
- The audited table column names with their values.

## SQL Reduction

The SQL Reduction option reduces to a single Recorder entry, all sequences of SQL statements that are structurally identical. Sequences of INSERTs for example, where only the data values inserted vary.

## Archiving the Recorder

The DBARS archiving function transfers the Recorder to tape, 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 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 Recorder and the DBARS Exception table. If the DBARSNAX facility is active, the alert is sent to defined email addresses.

## 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 and the DBARS Exception table. If the DBARSNAX facility is active, the blocking event is sent to defined email addresses.

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 Db2 access, whatever its origin.

## Customizing DBARS

An installation may provide a user exit to be invoked when an access is stored into 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. In such scenarios, the archiving, reporting and alerting functions are carried out by the ESM. However, DBARS will still perform Db2 access blocking.

The DBARS audit data are communicated to the ESM either by FTP or by TCP/IP communications between DBARS and the ESM.

## Benefits

- DBARS provides all functions needed for auditing access to sensitive data in Db2 tables.
- DBARS is a software-only solution: no hardware appliances are needed to intercept accesses from the network.
- DBARS has its own proprietary interface to Db2 and does not depend on Db2 tracing. As a result, recording overhead will be low.
- DBARS is able to signal and 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 may provide valuable recording services.

    - In operational environments, DBARS may record all accesses to designated Db2 tables.
    - In development and QA environments, DBARS may be used to verify the submitted SQL.
    - Using DBARS archiving, an organization may keep track of all Db2 accesses.

(c) Copyright 2014-2024 Software Product Research
www.sprdb2.com