Auditing DB2 on z/OS

Software Product Research

Information stored in DB2 databases is of enormous value to corporations. Misuse of this information can launch competitive and legal penalties.

In many countries, laws have been instituted to protect against unauthorized disclosure of such information.

Controlling Access

Only authorized persons should have access to sensitive data. DB2 privileges are used to achieve this.

Recording Access

Recording access to sensitive data is a necessary security measure. Ideally, access logs should be maintained, either by application programming or by system tools.

DB2 Log

Records updates only, not SELECT's.

Audit trace

DB2 records only the first table access within a logical unit of work.

To achieve comprehensive recording, many tracepoints must be enabled.

The operational cost of intensive tracing is high.

While mainframe security software and DB2 privileges protect against unauthorized access to DB2 tables, they do little to report all accesses to DB2 tables and what was done within those tables.

“DBARS”

DB2 Access Recording Services

A software tool developed by

Software Product Research

DBARS Facilities

Records all accesses to designated DB2 tables by recording the SQL statements that perform the access.

- Records DML access (SELECT, DELETE, INSERT, UPDATE)
- Records COMMIT and ROLLBACK
- Records DDL access (CREATE, ALTER, etc)
- Records DB2 bind, DB2 commands and DB2 utilities

Records the content of all input variables used by the SQL statements.

Intercepted DB2 accesses are stored into the DBARS Recorder.

The Recorder is created at product installation as a DB2 table, a VSAM cluster or a sequential dataset.

Audit Data Captured

Date and time of access
Creator and name of the accessed table
Name of DB2 subsystem accessed
DB2 userid performing the access
Z/OS userid performing the access
DB2 connection (Batch, TSO, DDF,CICS)
DB2 system sending the SQL statement
Application and workstation name if distributed access
Name of program performing the SQL statement
Result of statement execution (SQLCODE)
Number of rows modified
Text of the recorded SQL statement with host variables replaced by their contents.

SPR software product research

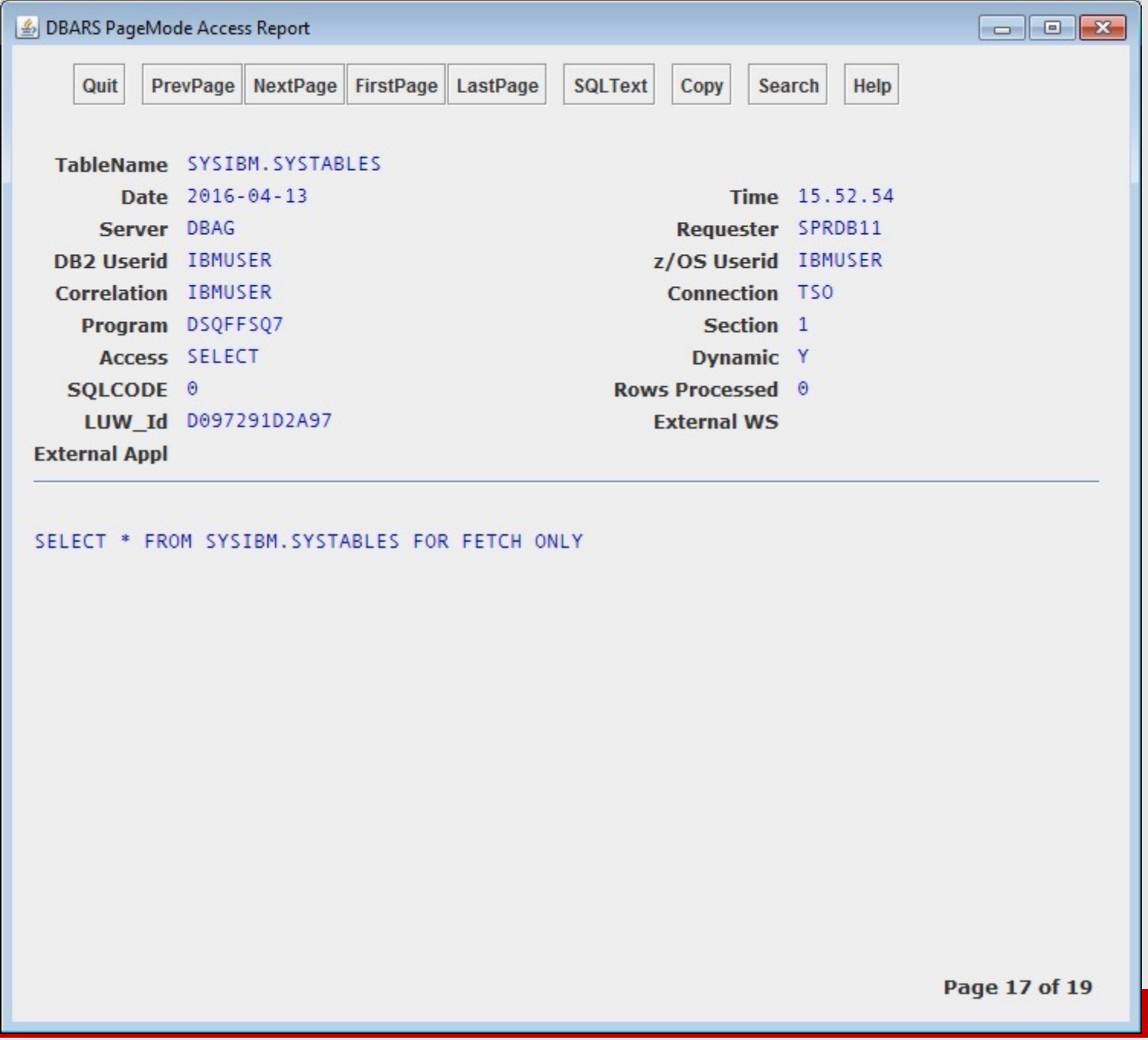
DBARS Additional Facilities

- A powerful Recorder Scan utility to report on audited access.

Scans of the Recorder and the Recorder Archive are invoked from batch, TSO or using a GUI interface provided by DBARS.

- Automated Recorder Archives, to keep recorded accesses for an unlimited period of time.

- User Exit for customization. An exit is written in REXX or as a compiled load module.


DBARS PageMode Access Report
Quit
PrevPage
NextPage
FirstPage
LastPage
SQLText
Copy
Search
Help
TableName SYSIBM.SYSTABLES
Date 2016-04-13
Time 15.52.54
Server DBAG
Requester SPRDB11
DB2 Userid IBMUSER
z/OS Userid IBMUSER
Correlation IBMUSER
Connection TSO
Program DSQFFSQ7
Section 1
Access SELECT
Dynamic Y
SQLCODE 0
Rows Processed 0
LUW_Id D097291D2A97
External WS
External Appl
SELECT * FROM SYSIBM.SYSTABLES FOR FETCH ONLY
Page 17 of 19

Alert & Block

- The DBARS “Rules” dataset defines the conditions for alerting or blocking a given DB2 access.
- When DBARS blocks an access, the entire unit of work is rolled back.
- When DBARS issues an alert for a given access:
- the SQL statement is stored in the “Exceptions” table
- a user alert exit is invoked, if provided
- the alert may be stored in a Windows event log

Following rule ensures that only users in the accounts receivable department can update the customer table:

```
Block when table acr.customer
and access not select
and user not acr
```

Integration with SIEM products

- Integration by FTP

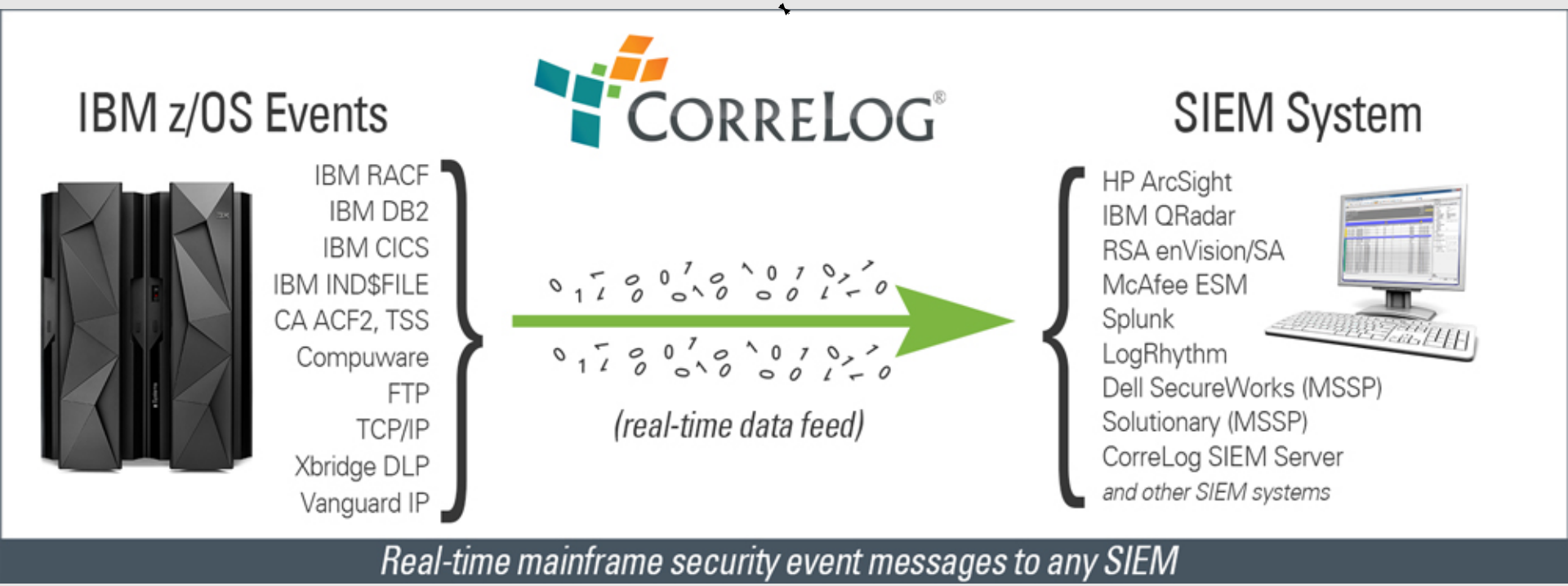
DBARS provides a program function that sends recorded accesses to an external server by FTP.

This method is used to communicate with Oracle's DBFW®.

- Integration by user exit

A compiled exit can be used to communicate with the SIEM.

Integration with Correlog SIEM Agent for z/OS



DBARS intercepts the DB2 accesses and passes them to the Correlog Agent.

A compiled DBARS exit is used as the communication method, to send all data extracted from DB2, including the SQL statement text.

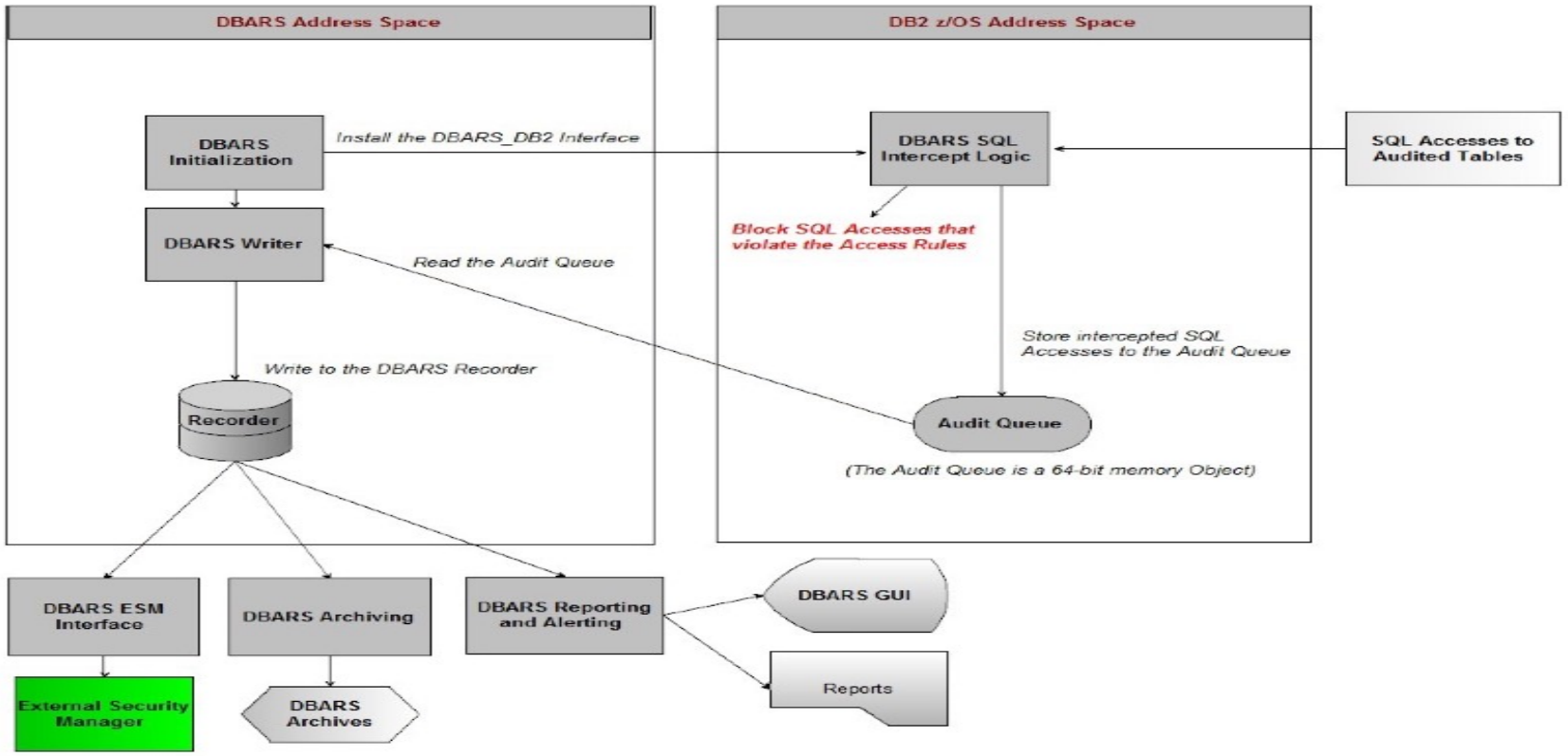
Operational Notes

- DBARS does not depend on DB2 log or DB2 audit tracing. The product interacts with DB2 using a proprietary interface.
- IFI facilities are used only to intercept DB2 utility execution.
- DBARS intercepts all accesses from all DB2 clients.
- Tables to be audited are named in the DBARS startup member.
- Dual logging to the Recorder is performed. Recording continues during Recorder archiving.

DBARS Components

- Initiator
  - Executes in the DB2 address space
  - Intercepts and queues all SQL statements executed into the Audit Queue
  - Blocks illegitimate DB2 access when requested by a policy rule
- Writer
  - Executes in the DBARS address space
  - Processes the Audit Queue entries
  - Writes the audit records to the DBARS Recorder
  - Issues alerts when requested by a policy rule
  - Invokes eventual user exits
- Audit Queue
  - Owned by the DBARS address space
  - A 64-bit object, residing above the 2 Gigabyte bar

DBARS Overview



Using DBARS as an Access Recorder

Even when DBARS is not used in an auditing context, it still can provide valuable recording services.

- In development and QA environments, DBARS can show whether applications perform adequately and whether correct SQL statements are submitted.

- In operational environments, DBARS will record all DB2 accesses for designated tables. Using the DBARS archiving facilities, these recordings can be kept for an unlimited period of time.

Performance

Background Information

- Performed in major bank facility
- Conducted over 24 hour period; 4 hour batch window
- DBARS ALLTABLES parameter turned on, resulting in over 16000 objects from the DB2 LPAR being monitored

Results

- Audited 220 million SQL transactions during batch window
- Audited 610 million SQL transactions during 24 hour test period
- CPU peak for batch window: 4.2%
- CPU over 24 hour period: less than 1%

More information on DBARS can be found on our website.

http://www.sprdb2.com/DBARS/summary.htm