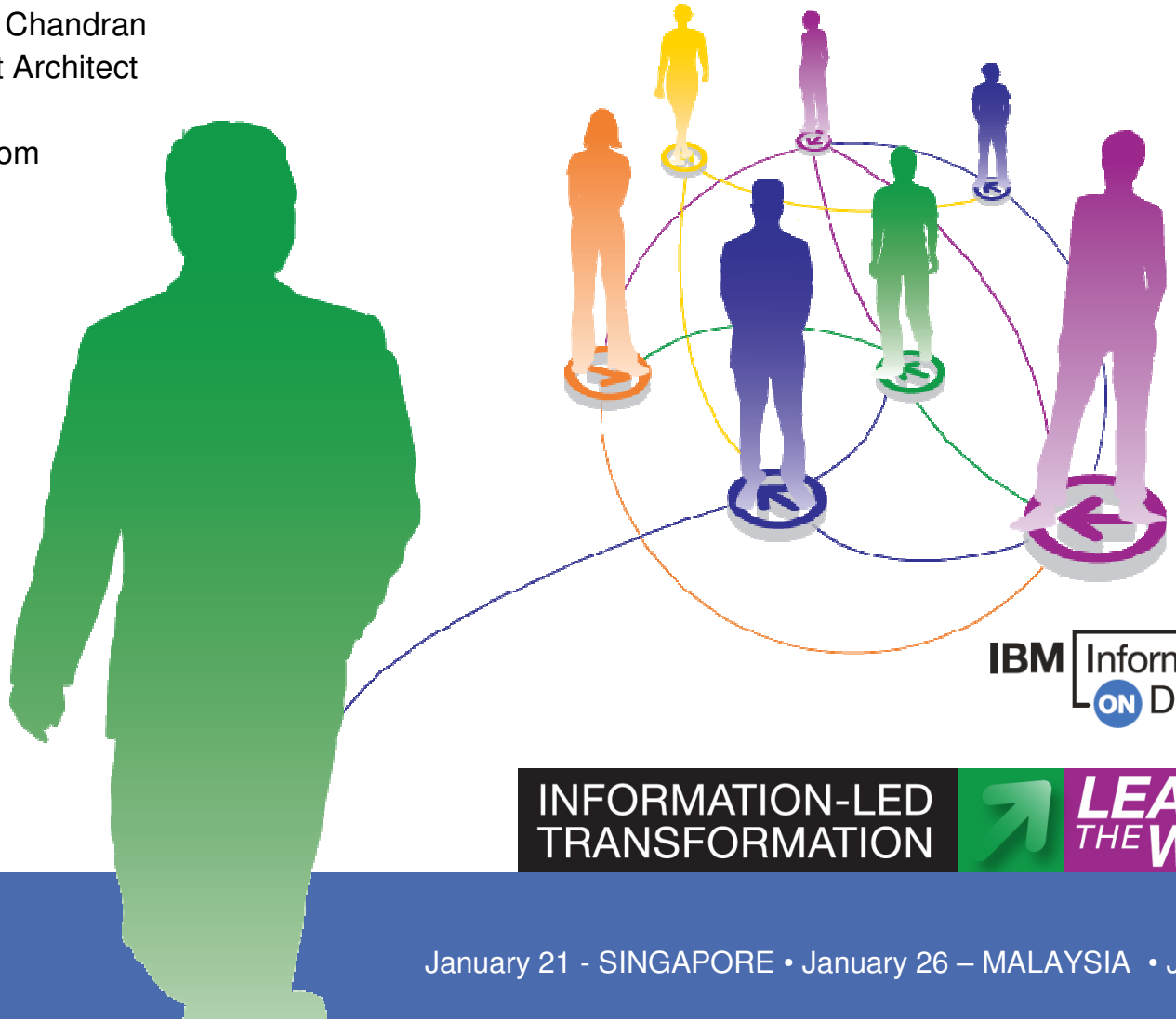
Addressing Audit and Compliance requirements in a DB2 z/OS environment

Presenter: Rajesh Chandran
Data Management Architect
IBM ASEAN
rajeshc@sg.ibm.com
Session: 003



IBM Information ON Demand 2010

INFORMATION-LED TRANSFORMATION LEAD THE WAY

Disclaimer

Landscape – Customer Challenges

- Tremendous regulatory compliance pressures to demonstrate adequate institutional controls including audit reporting.
- Current DB2 on z/OS environment typically has minimal auditing
- Manual effort requiring interaction by DBA's
- Reactive in nature with the implication that you only find information post event, or after the first breach
- Home grown process can provide some level of access reporting, however:
  - Application managed code you have to maintain
  - Exposure as a lack of robust application change controls can allow disabling of audit processing
- Overhead (perceived or actual) in many cases drive decision to not audit DB2 on z/OS data
- DB2 trace based processes are managed by DBA's
  - **The DBA's are responsible for generating audit data with which they are in turn audited, this constitutes a significant security risk and exposure.**

DB2 Audit Trace versus RACF

Why Audit when Production is Locked Down?

- Common arguments:
  - "We don't need to audit, we have controls surrounding who can access data"
  - "'We control who is connected to the DB2 SYSADM group and we know what those people are authorized to do"
- Counter arguments:
  - RACF does two things:
    - Prevents people from accessing a resource that is not essential or appropriate for their jobs
    - Allows people access to the necessary data to do their jobs
  - But RACF does NOT:
    - prevent a malicious update if the user has authority to the data.
    - prevent an authorized user from accessing sensitive data that is ***NOT*** within the scope of their job.
      - E.g. a bank teller looks up the CEOs bank balance or personal customer information
    - provide meaningful information about access to protected DB2 resources (authorized or not).

What to Audit – A busy slide

- **Closed Application Environment (*Probably not a candidate*)**
  - **Traditional Application controls well defined and comprehensive**
    - **CICS and IMS TM – Signon and Transaction Access secured via RACF**
    - **Production Batch – Controlled via program pathing / Job Scheduling**
- Data warehouse – no risk of update but access audit might be needed
- Adhoc execution environnent – QMF, SPUFI, etc. Constitutes exposure
  - SPUFI Plan can be restricted but ALL use should be audited
- Privleged ID's (DBA/Sysadmin) should be audited
- Data may not be as granular as you think
  - Depending on how you configured your connections into DB2 – CICS attach, SAP, or CICS users with unique id's, and distributed transactions. May get all audit data but may not be meaningful because of attach environments. Group versus AUTHID. SQLESETI implementation can help
- "Offline" Utilities and certain tools are used outside of DB2
  - RACF dataset access defined controls
  - "Trigger" based audit
  - Use of DSN1COPY should be restricted

Audit data sources

- DB2 catalog
  - SQL queries on catalog, other data
  - audit, accounting and performance traces
  - recovery log, current & historical data
  - RACF audit facility, other SMF data, ...
- Audit tools and techniques
  - tracing: audit, performance, accounting, monitor
  - formatting the traces: OMPE or PM, others
  - DB2 Audit Management Expert, others
  - DSN1SMFP, others
  - log formatting: tools, DSN1LOGP, Log Analyzer

What actions are needed to start the Audit trace?

- -DSN START TRACE (AUDIT) CLASS (1,2,4,5,8) DEST (SMF)
  - Requires one of the following privileges:
    - SYSOPER
    - SYSCTRL
    - SYSADM
    - TRACE
  - In addition, Class 4 and 5 events will only be collected for objects (tables) with the audit attribute turned on via ALTER:
    - AUDIT CHANGES – enables collection of changes in conjunction with CLASS (4)
    - AUDIT ALL – enables collection of changes and / or reads with CLASS 4 and/or 5 active
  - Note: When ALTER AUDIT is performed, plan and package invalidation occurs which requires a rebind to be performed

Audit class Events that are traced

1. Access attempts that DB2 denies because of inadequate authorization. This class is the default.
2. Explicit GRANT and REVOKE statements and their results. This class does not trace implicit grants and revokes.
3. CREATE, ALTER, and DROP statements that affect audited tables, and the results of these statements. This class traces the dropping of a table that is caused by DROP TABLESPACE or DROP DATABASE and the creation of a table with AUDIT CHANGES or AUDIT ALL. ALTER TABLE statements are audited only when they change the AUDIT option for the table.
4. Changes to audited tables. Only the first attempt to change a table, within a unit of recovery, is recorded. (If the agent or the transaction issues more than one COMMIT statement, the number of audit records increases accordingly.) The changed data is not recorded, only the attempt to make a change is recorded. If the change is not successful and is rolled back, the audit record remains; it is not deleted. This class includes access by the LOAD utility.

   Accesses to a dependent table that are caused by attempted deletions from a parent table are also audited. The audit record is written even if the delete rule is RESTRICT, which prevents the deletion from the parent table. The audit record is also written when the rule is CASCADE or SET NULL, which can result in deletions that cascade to the dependent table.
5. All read accesses to tables that are identified with the AUDIT ALL clause. As in class 4, only the first access within a DB2 unit of recovery is recorded. References to a parent table are also audited.
6. The bind of static and dynamic SQL statements of the following types:

   INSERT, UPDATE, DELETE, CREATE VIEW, and LOCK TABLE statements for audited tables. Except for the values of host variables, the audit record contains the entire SQL statement.

   SELECT statements on tables that are identified with the AUDIT ALL clause. Except for the values of host variables, the audit record contains the entire SQL statement.
7. Assignment or change of an authorization ID because of the following reasons:

   Changes through an exit routine (default or user-written)

   Changes through a SET CURRENT SQLID statement

   An outbound or inbound authorization ID translation

   An ID that is being mapped to a RACF ID from a Kerberos security ticket
8. The start of a utility job, and the end of each phase of the utility.

Audit Trace Overhead

- The performance impact of auditing is directly dependent on the amount of audit data produced. When the audit trace is active, the more tables that are audited and the more transactions that access them, the greater the performance impact. The overhead of audit trace is typically less than 5% but workload dependent.

- Consider the frequency of certain events. Eg. security violations are not as frequent as table accesses. The frequency of utility runs is likely to be measured in executions per day. Alternatively, authorization changes can be numerous in a transaction environment.

- Weigh auditing requirements against workload and anticipated impacts to application service levels and performance objectives carefully.

- Don't underestimate impact on SMF activity and associated overhead

DSN1SMFP offline utility

- The DSN1SMFP utility processes DB2 trace data into reports.
- DSN1SMFP accepts data that SMF collects in standard SMF format and produces from one to fifteen reports. DSN1SMFP accepts all SMF record types, but it processes only type 101 (DB2 Accounting) and 102 (DB2 Performance) records.
- DSN1SMFP checks each type 101 and 102 record for DB2 audit trace types of these DB2 IFCIDs:
  - 003: Accounting - DDF Data by Location (security-relevant fields only)
  - 004: Trace Start
  - 005: Trace Stop
  - 023: Utility Start
  - 024: Utility Change
  - 025: Utility End
  - 106: System Parameters (security-relevant fields only)
  - 140: Audit Authorization Failures
  - 141: Audit DDL Grant/Revoke
  - 142: Audit DDL Create/Alter/Drop
  - 143: Audit First Write
  - 144: Audit First Read
  - 145: Audit DML Statement
  - 350: SQL Statement

The OMPE “File” Report command is used to create DB2 Load compatible record formats

OMPE “File” report commands

```
MSG.ID.    DESCRIPTION
---------  ------------------------------------------------------------------
FPEC2001I  COMMAND INPUT FROM DDNAME SYSIN
           AUDIT
                       REPORT
                                LEVEL(DETAIL)
                                TYPE(DDL DML)
                                DDNAME(AUDITDD)
                       FILE
                                TYPE(DDL)
                                DDNAME(AUFILDD1)
                       FILE
                                TYPE(DML)
                                DDNAME(AUFILDD2)
                       FILE
                                TYPE(AUTHFAIL)
                                DDNAME(AUFILDD3)
           EXEC
```

OMPE Audit Detail Report

```
   LOCATION: NDCDB203                    OMEGAMON XE FOR DB2 PERFORMANCE EXPERT (V3)          PAGE: 1-1
      GROUP: N/P                              AUDIT REPORT - DETAIL                    REQUESTED FROM: NOT SPECIFIED
     MEMBER: N/P                                                                                 TO: NOT SPECIFIED
  SUBSYSTEM: DSNC                         ORDER: PRIMAUTH-PLANNAME                     ACTUAL FROM: 09/06/06 01:47:43.60
DB2 VERSION: V8                                SCOPE: MEMBER                                      TO: 09/06/06 01:49:38.83
PRIMAUTH CORRNAME CONNTYPE
ORIGAUTH CORRNMBR INSTANCE
PLANNAME CONNECT               TIMESTAMP   TYPE                              DETAIL
-------- -------- ------------ ----------- -------- ------------------------------------------------------------------------

SYS248   SYS248   DB2CALL      01:47:43.60 DML      TYPE    : 1ST READ
SYS248   'BLANK'  BF5CF720228D                     DATABASE: SYS248SA            TABLE OBID:      5
ETIPLAN1 DB2CALL                                   PAGESET : SYS248TS            LOG RBA    : X'000000000000'

SYS248   SYS248   DB2CALL      01:48:22.56 DML      TYPE    : 1ST WRITE
SYS248   'BLANK'  BF5CF7454387                     DATABASE: SYS248SA            TABLE OBID:      5
ETIPLAN1 DB2CALL                                   PAGESET : SYS248TS            LOG RBA    : X'00036FBEA220'

SYS248   SYS248   DB2CALL      01:48:22.56 DML      TYPE    : 1ST WRITE
SYS248   'BLANK'  BF5CF7454387                     DATABASE: SYS248SA            TABLE OBID:      5
ETIPLAN1 DB2CALL                                   PAGESET : SYS248TS            LOG RBA    : X'00036FBEA3DA'
```

A view of the audit data stored in the OMPE performance warehouse using DB2 Control Center

Log RBA can be used to locate details about other actions for the LUW

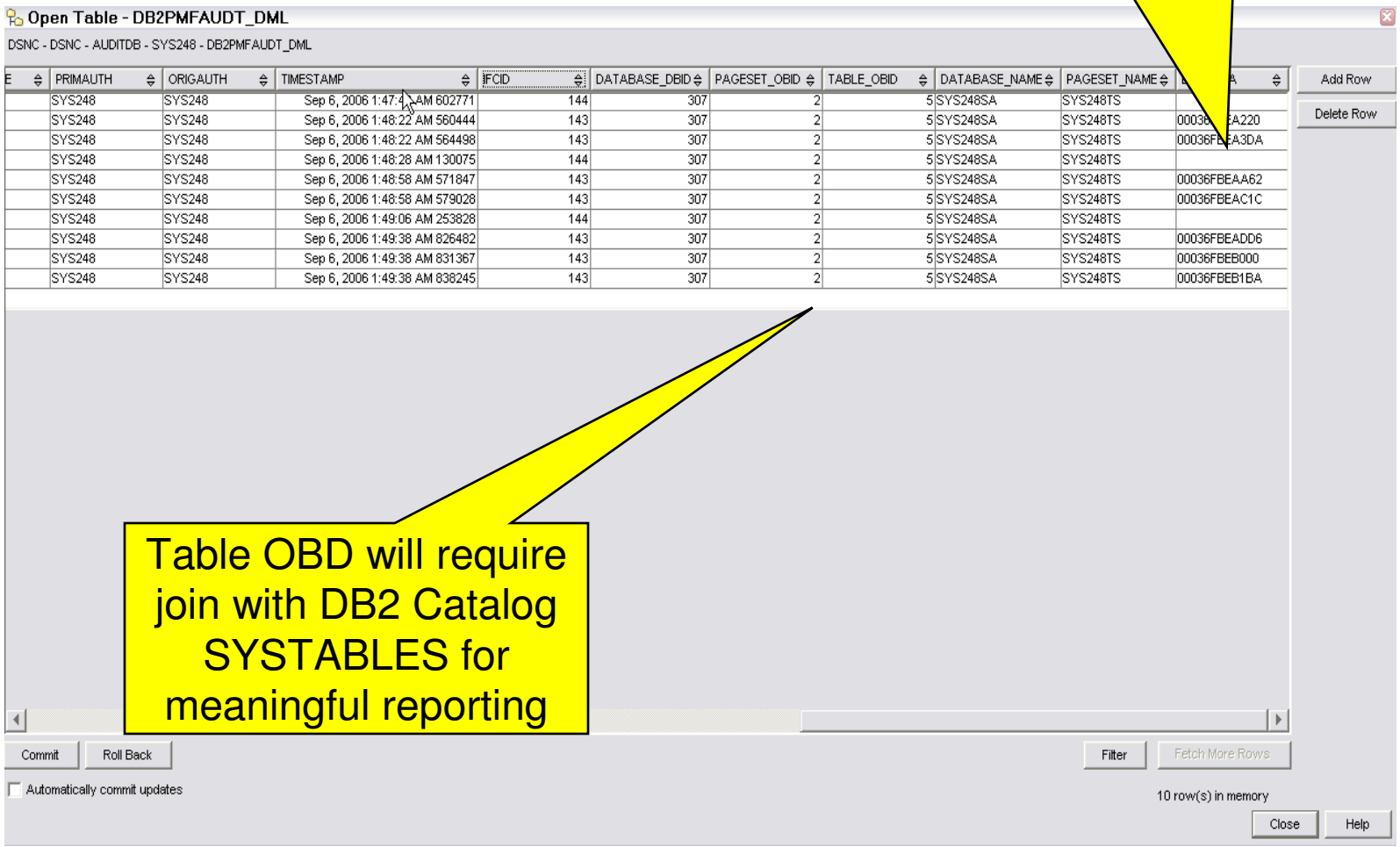


Table OBD will require join with DB2 Catalog SYSTABLES for meaningful reporting

Limitations of the audit trace

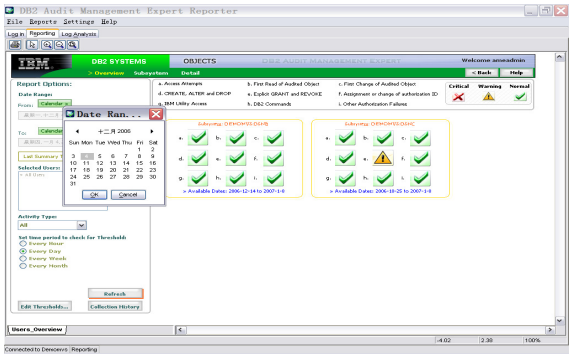
- Does not record everything
  - Only records when Audit Trace is ON
  - only the tables that you specifically choose to audit.
- Does NOT capture before/after change data
- Only records first access within a single unit of recovery
- The audit trace does not audit some utilities. eg COPY, RECOVER, REPAIR ,DSN1CHKR and DSN1PRNT.
- You cannot audit the catalog tables.
- Dynamic SQL host variable data not collected
- When you choose classes of events to audit, consider that you might ask for more data than you are willing to process.
- Depending on AUDIT classes active, and workload mix, significant increases in SMF activity might be experienced. One customer scenario, with CLASS (1-6) a 12% increase in SMF was observed.

Separation of Roles and Responsibilities

- DB2 trace based processes are managed by DBA's
  - The DBA's are responsible for generating audit data with which they are in turn audited, this constitutes a significant security risk and exposure
  - Trace data collection can be interfered with or turned off completely
    - DBA can issue –DSN Stop Trace
    - Use IFASMFDMP to selectively filter SMF data based on timestamp
    - Use DB2PM (Or Equivalent) filter such as DATE/TIME/EXCLUDE to filter selected records
  - Having the DBA involved in the collection of audit data is viewed as weak from a compliance and control perspective
- Security and Auditors with system privileges
  - Also viewed as problematic from a compliance perspective
  - Requires additional technical skills not within their core competencies
  - Misuse of privileges without coordination can result in performance and availability issues
    - Turning on traces without proper filtering to reduce overhead or quantity of trace data collected
    - Altering objects to AUDIT without ensuring that plan/package invalidation is not an issue

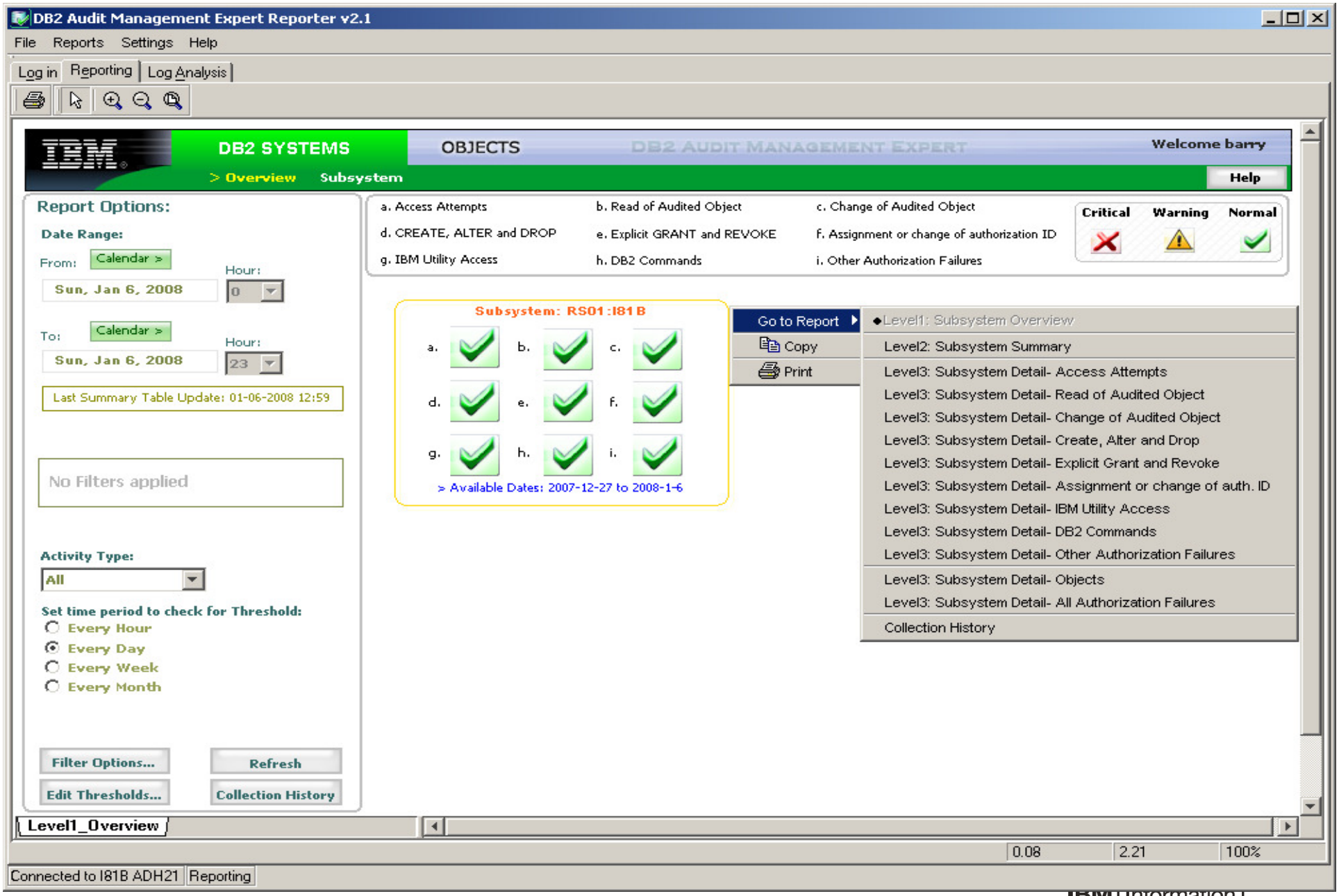
Audit Management Expert - Monitor and Audit

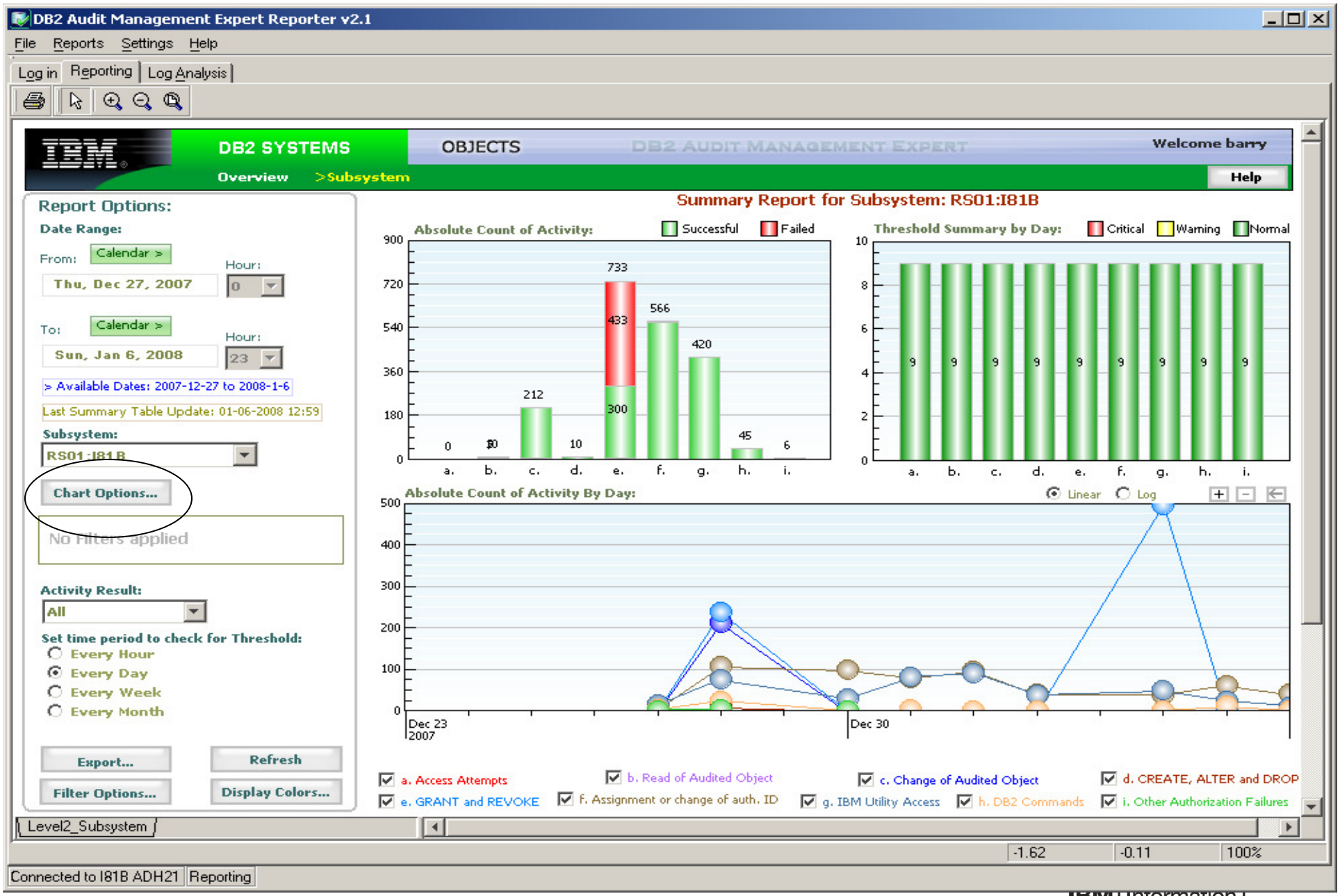
- **Helps auditors answer:**
  - Who, What, Where, Why, When, How
- **Centralizes the audit data**
  - Pulls together disparate data sources from all the systems into a central repository
- **Automates auditing process**
  - Eliminates all home grown processes
- **Creates segregation of duties**
  - Gives auditors the business activity collected without being reliant on the technical personnel they need to monitor
- **Flexible Reporting**
  - Drill down from overview to detail for forensic analysis



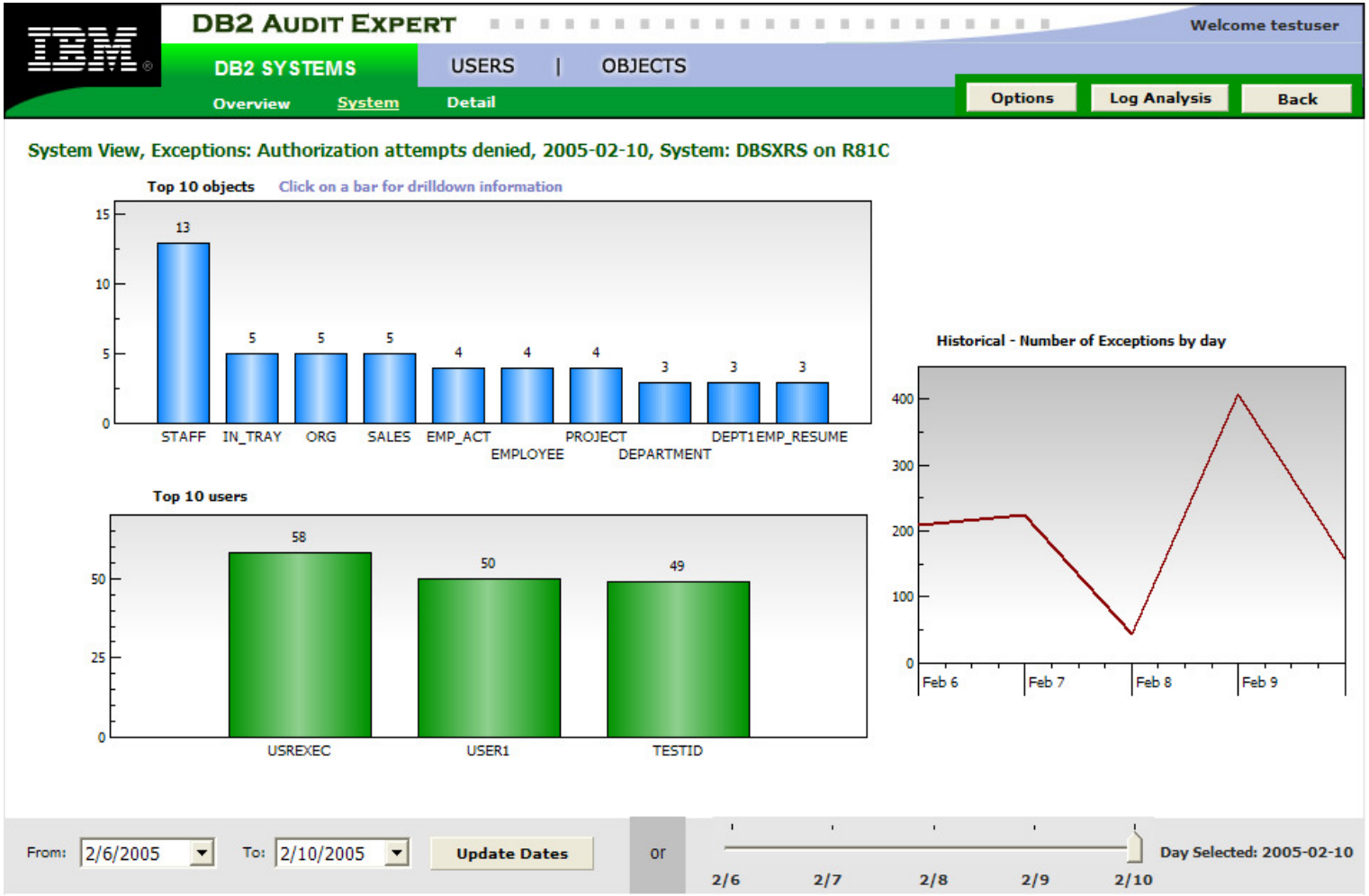
Audit Management Expert Overview

- Auditors will be able to Access:
  - SELECT, INSERT, UPDATE, and DELETE activity by user or by object
  - **SQL Text and Host Variable value for each statement**
    - **Row count that SQL statement affects**
  - CREATE, ALTER, and DROP operations against an audited object
  - Explicit GRANT and REVOKE operations
  - Utility access to an audited object
  - DB2 commands entered
  - Assignment or modification of an authorization ID
  - Authorization failures
- **Provides auditors with flexible options for examining the data in the audit repository**
  - Audit Trace Data, **Audit SQL Collector (ASC),** Log Analysis data
    - V2.1 no longer needs to alter objects to 'AUDIT ALL' for read/update
    - DB2 Catalog Objects can now be audited for SQL read/update

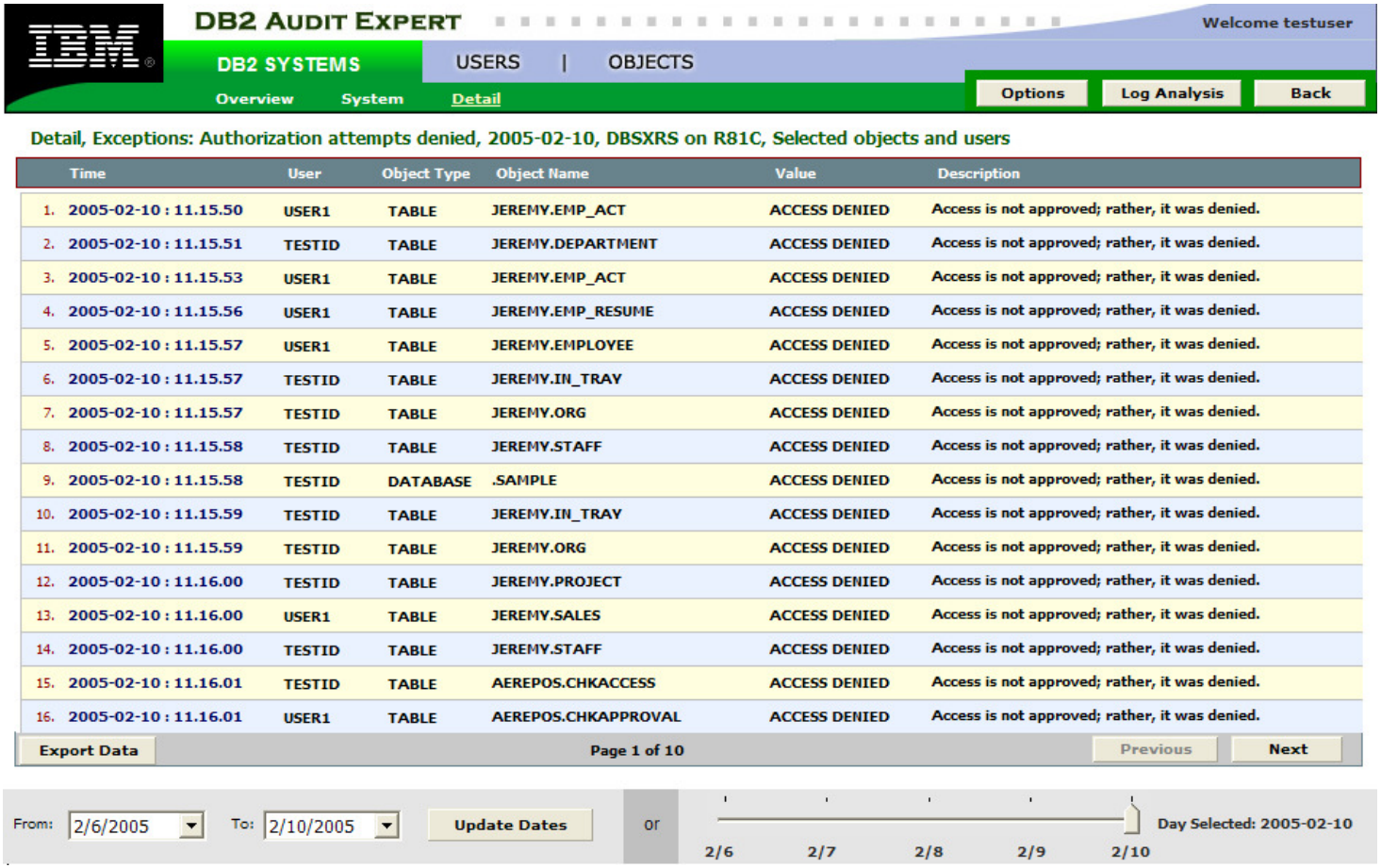

DB2 Audit Management Expert Reporter v2.1
File Reports Settings Help
Log in Reporting Log Analysis
DB2 SYSTEMS
OBJECTS
DB2 AUDIT MANAGEMENT EXPERT
Welcome barry
> Overview Subsystem
Help
Report Options:
Date Range:
From: Calendar > Hour:
Sun, Jan 6, 2008 0
To: Calendar > Hour:
Sun, Jan 6, 2008 23
Last Summary Table Update: 01-06-2008 12:59
No Filters applied
Activity Type:
All
Set time period to check for Threshold:
Every Hour
Every Day
Every Week
Every Month
Filter Options...
Refresh
Edit Thresholds...
Collection History
a. Access Attempts
b. Read of Audited Object
c. Change of Audited Object
d. CREATE, ALTER and DROP
e. Explicit GRANT and REVOKE
f. Assignment or change of authorization ID
g. IBM Utility Access
h. DB2 Commands
i. Other Authorization Failures
Critical
Warning
Normal
Subsystem: RS01:I81B
a. b. c.
d. e. f.
g. h. i.
> Available Dates: 2007-12-27 to 2008-1-6
Go to Report
Copy
Print
Level1: Subsystem Overview
Level2: Subsystem Summary
Level3: Subsystem Detail- Access Attempts
Level3: Subsystem Detail- Read of Audited Object
Level3: Subsystem Detail- Change of Audited Object
Level3: Subsystem Detail- Create, Alter and Drop
Level3: Subsystem Detail- Explicit Grant and Revoke
Level3: Subsystem Detail- Assignment or change of auth. ID
Level3: Subsystem Detail- IBM Utility Access
Level3: Subsystem Detail- DB2 Commands
Level3: Subsystem Detail- Other Authorization Failures
Level3: Subsystem Detail- Objects
Level3: Subsystem Detail- All Authorization Failures
Collection History
Level1_Overview
0.08 2.21 100%
Connected to I81B ADH21 Reporting

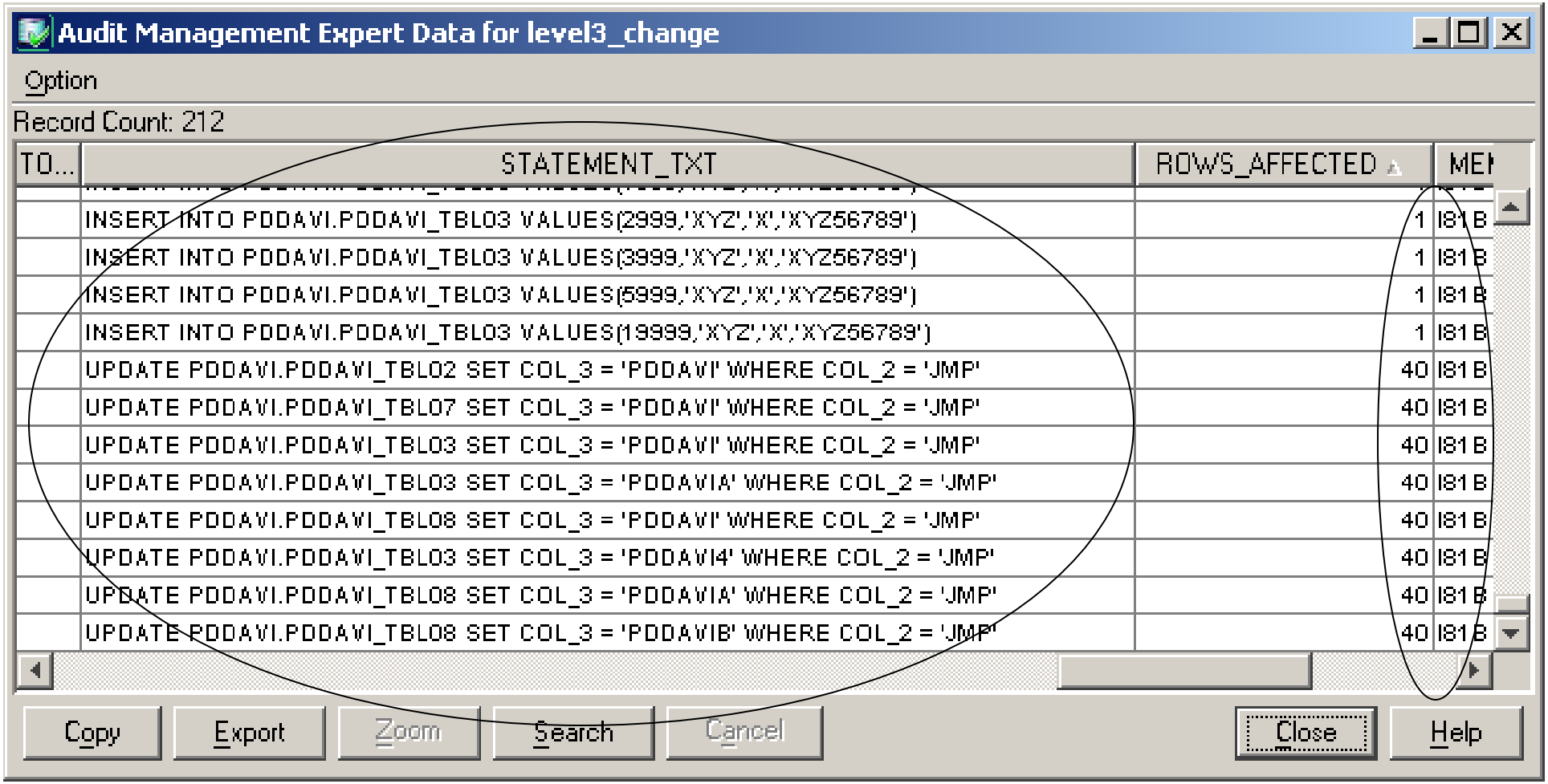

DB2 Audit Management Expert Reporter v2.1
File Reports Settings Help
Log in Reporting Log Analysis
DB2 SYSTEMS
OBJECTS
DB2 AUDIT MANAGEMENT EXPERT
Welcome barry
Overview >Subsystem
Help
Report Options:
Date Range:
From: Calendar > Hour:
Thu, Dec 27, 2007
0
To: Calendar > Hour:
Sun, Jan 6, 2008
23
> Available Dates: 2007-12-27 to 2008-1-6
Last Summary Table Update: 01-06-2008 12:59
Subsystem:
RS01:I81B
Chart Options...
No filters applied
Activity Result:
All
Set time period to check for Threshold:
Every Hour
Every Day
Every Week
Every Month
Export...
Refresh
Filter Options...
Display Colors...
Summary Report for Subsystem: RS01:I81B
Absolute Count of Activity:
Successful
Failed
Threshold Summary by Day:
Critical
Warning
Normal
Absolute Count of Activity By Day:
Linear
Log
Dec 23
2007
Dec 30
a. Access Attempts
b. Read of Audited Object
c. Change of Audited Object
d. CREATE, ALTER and DROP
e. GRANT and REVOKE
f. Assignment or change of auth. ID
g. IBM Utility Access
h. DB2 Commands
i. Other Authorization Failures
Level2_Subsystem
-1.62
-0.11
100%
Connected to I81B ADH21
Reporting

Audit Management Expert GUI Client



Audit Management Expert GUI Client




Audit Management Expert Data for level3_change
Option
Record Count: 212
TO...
STATEMENT_TXT
ROWS_AFFECTED
MEI
INSERT INTO PDDAVI.PDDAVI_TBL03 VALUES(2999,'XYZ','X','XYZ56789') 1 I81B
INSERT INTO PDDAVI.PDDAVI_TBL03 VALUES(3999,'XYZ','X','XYZ56789') 1 I81B
INSERT INTO PDDAVI.PDDAVI_TBL03 VALUES(5999,'XYZ','X','XYZ56789') 1 I81B
INSERT INTO PDDAVI.PDDAVI_TBL03 VALUES(19999,'XYZ','X','XYZ56789') 1 I81B
UPDATE PDDAVI.PDDAVI_TBL02 SET COL_3 = 'PDDAVI' WHERE COL_2 = 'JMP' 40 I81B
UPDATE PDDAVI.PDDAVI_TBL07 SET COL_3 = 'PDDAVI' WHERE COL_2 = 'JMP' 40 I81B
UPDATE PDDAVI.PDDAVI_TBL03 SET COL_3 = 'PDDAVI' WHERE COL_2 = 'JMP' 40 I81B
UPDATE PDDAVI.PDDAVI_TBL03 SET COL_3 = 'PDDAVIA' WHERE COL_2 = 'JMP' 40 I81B
UPDATE PDDAVI.PDDAVI_TBL08 SET COL_3 = 'PDDAVI' WHERE COL_2 = 'JMP' 40 I81B
UPDATE PDDAVI.PDDAVI_TBL03 SET COL_3 = 'PDDAVI4' WHERE COL_2 = 'JMP' 40 I81B
UPDATE PDDAVI.PDDAVI_TBL08 SET COL_3 = 'PDDAVIA' WHERE COL_2 = 'JMP' 40 I81B
UPDATE PDDAVI.PDDAVI_TBL08 SET COL_3 = 'PDDAVIB' WHERE COL_2 = 'JMP' 40 I81B
Copy
Export
Zoom
Search
Cancel
Close
Help

Log Analysis Reports

```
                    DB2 LOG ANALYSIS- SUMMARY REPORT: D8A
                   ******************************************

LOG RANGE
---------
START DATE     : 2006/03/13
START TIME     : 21:07:00
END DATE       : 2006/03/13
END TIME       : 21:17:00

FILTERS
-------
SHOW UPDATES   : Y
SHOW INSERTS   : Y
SHOW DELETES   : Y
SHOW ROLLBACKS : N
CATALOG DATA   : N
  INCLUDE-TABLE..... ADHSCH1.ADH1T1


*****************************
* COMMITTED ACTIVITY        *
*****************************

OBJECT TYPE/NAME                        UPDATES     INSERTS     DELETES     MD
--------------------------------------  ----------- ----------- ----------- --
TABLE..... ADHSCH1.ADH1T1               0           4           0
TABLESPACE. ADHTS1                      0           4           0
DATABASE... ADHDB1                      0           4           0


OBJECT TYPE/NAME (RI ACTIONS ONLY)      UPDATES     INSERTS     DELETES     MD
--------------------------------------  ----------- ----------- ----------- --

TOTAL SUMMARY REPORT
------------------------
TOTAL UPDATES: 0
TOTAL INSERTS: 4
TOTAL DELETES: 0
```

Log Analysis Detailed Reports

```
                    DB2 LOG ANALYSIS - DETAILS REPORT: D8A
                    **************************************

_____________________________________________________________________________

ACTION DATE       TIME     TABLE OWNER  TABLE NAME                URID
------ ---------- -------- ------------ ------------------------- ------------
INSERT 2006-03-13 21.15.38 ADHSCH1      ADH1T1                    00164DB5A558

DATABASE TABLESPACE DBID  PSID  OBID  AUTHID   PLAN     CONNTYPE LRSN
-------- ---------- ----- ----- ----- -------- -------- -------- ------------
ADHDB1   ADHTS1     00538 00002 00003 PDUSERA  DSNTEP2  BATCH    BE7FB51C73B2

MEMID CORRID       CONNID   LUW=NETID/LUNAME/UNIQUE/COMMIT      PAGE/RID
----- ------------ -------- ----------------------------------- -----------
00001 PDUSERT1     BATCH    ABCDNET1/D8ADB2  /BE7FB51B2EE6/0001 00000003/72

ROW STATUS  COL1       COL2
----------- ---------- --------------------
POST-CHANGE ADHS1      ADHSCHXXXXXX
PRE-CHANGE  -          -
```

Security and separation of roles

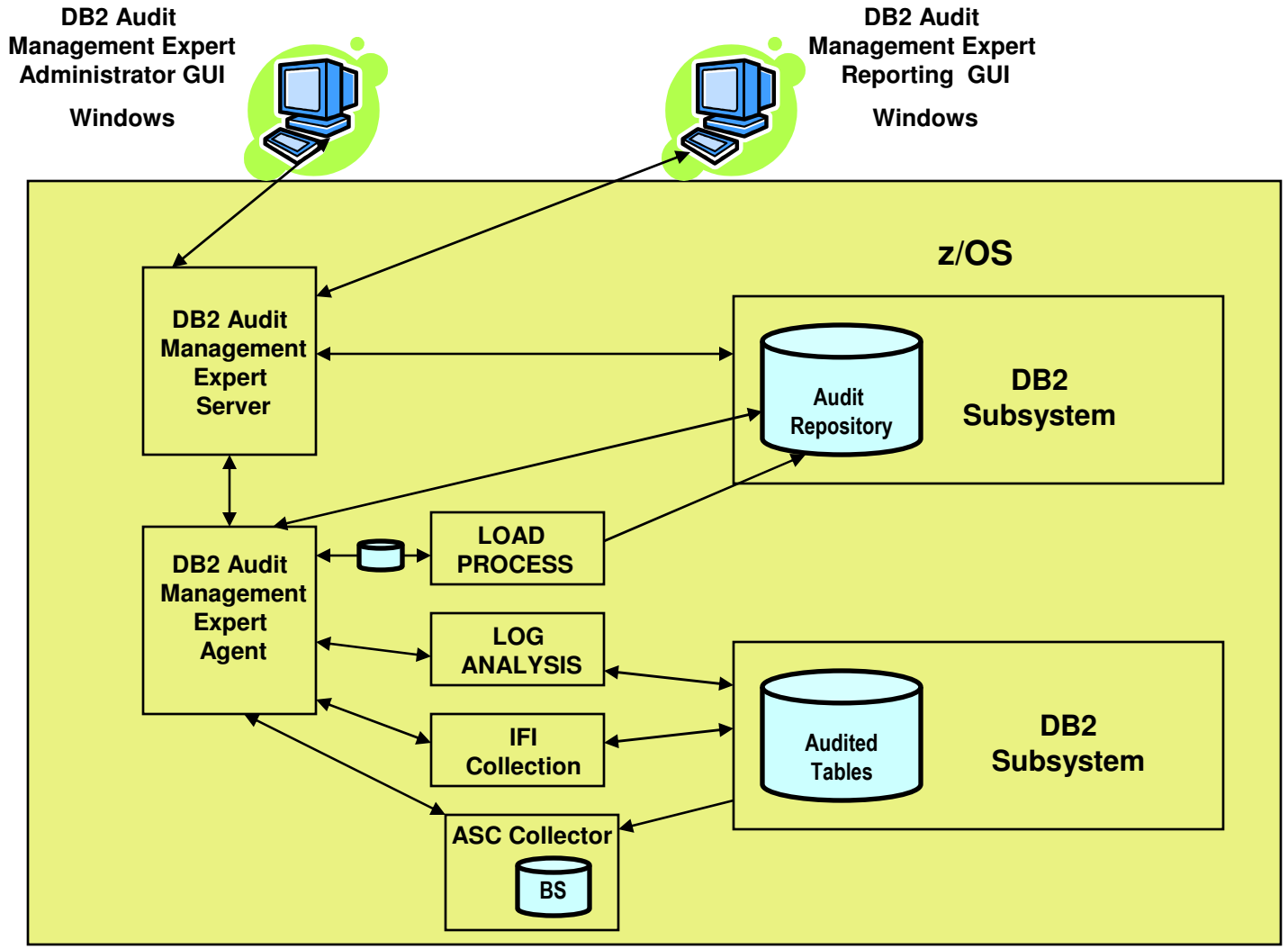
- Supporting internal and external auditors in collection and reporting of DB2 audit data
  - Does not require auditors to be DB2 defined users within the monitored DB2 system(s)
  - Does not require the auditors to log on to the operating system where the monitored system is running
    - Does not require extensive interaction between the auditor and the system support personnel (DBA/Sys admin)
- Auditor will not be able to directly manipulate any DB2 resources
- Provide complete visibility of all auditable objects to an administrator level user
- Provide controls for limiting visibility to auditors of auditable objects

- Removes DBA from audit data collection process. With V2.1 removes the "ALTER for AUDIT" requirement

Audit Trace only or Audit Trace and Audit SQL Collector (ASC)

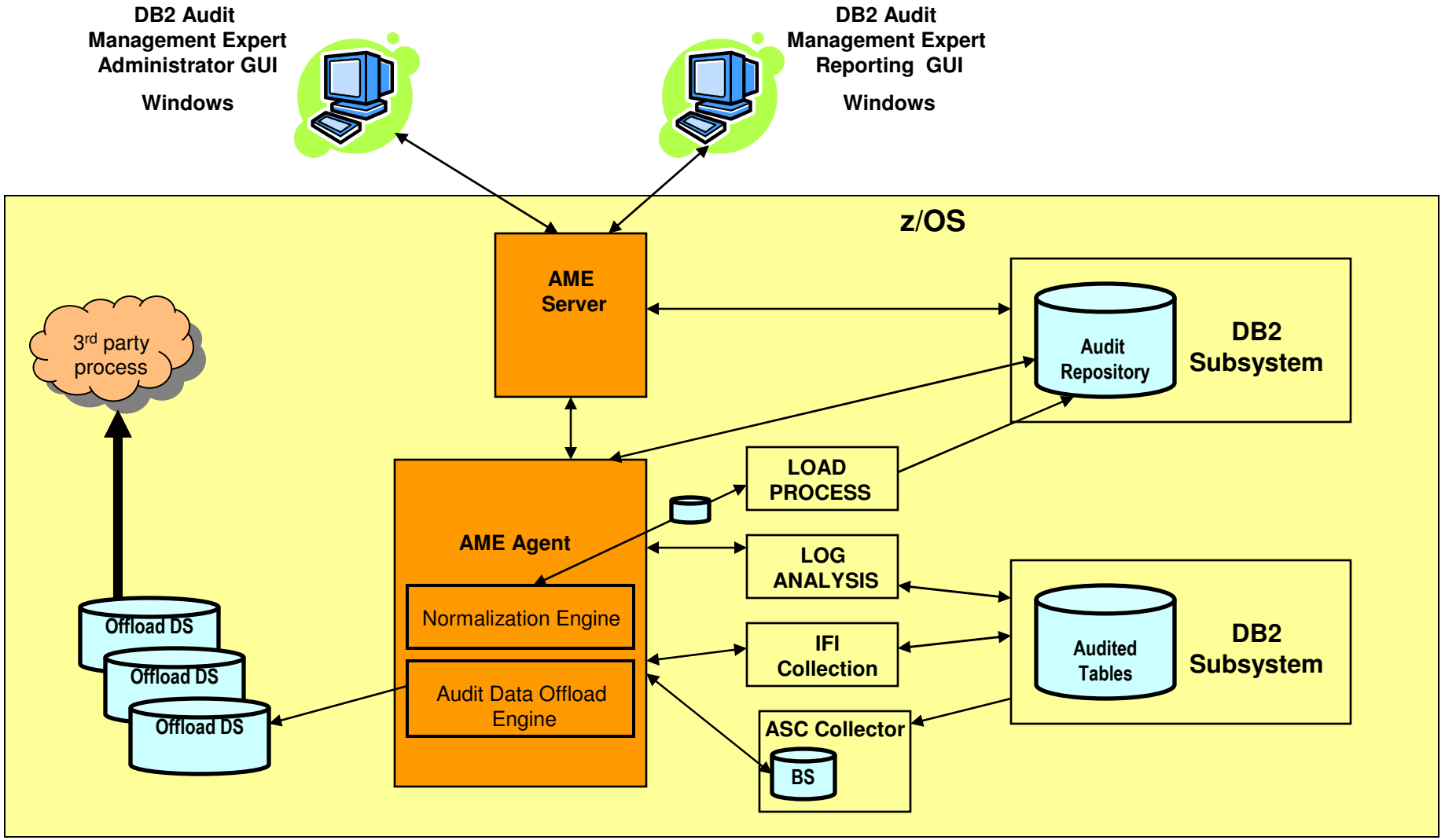
- AME can collects audit information by using Audit Trace Data, Audit SQL Collector data and Log Analysis data
- Audit Trace
  - Class 1,2,7 & 8 - little or no overhead
    - 1 Access attempts that DB2 denies,
    - 2 Explicit GRANT and REVOKE,
    - 7 Assignment or change of an authorization ID,
    - 8 start of a utility job
  - Class 3 create, alter, drop of **AUDIT ALL** Tables - little or no overhead
  - Class 4 & 5 (read, update) may show overhead of 15 -18%
    - 4 Changes to **AUDIT ALL** tables (Only the first attempt within a unit of recovery)
    - 5 Read accesses to **AUDIT ALL** tables (Only the first attempt within a unit of recovery)
  - IFCID 90 & 91 for DB2 COMMANDS – little or no overhead
- ASC:
  - Using the ASC Audit SQL Collector is an alternative to using Classes 4 & 5
  - Advantage of using the ASC
    - ASC sees every read or update
    - Collects SQL text, Host Variable value, affected row count
    - Tables do not require **AUDIT ALL** for read or update
  - AME Agent Started Task starts ASC started task and Audit trace as required
    - If valid collection profile defined for that DB2
    - Agent definition of collection method
    - Can change collection choice and/or collection profile without stopping Agent

DB2 Audit Management Expert Architecture

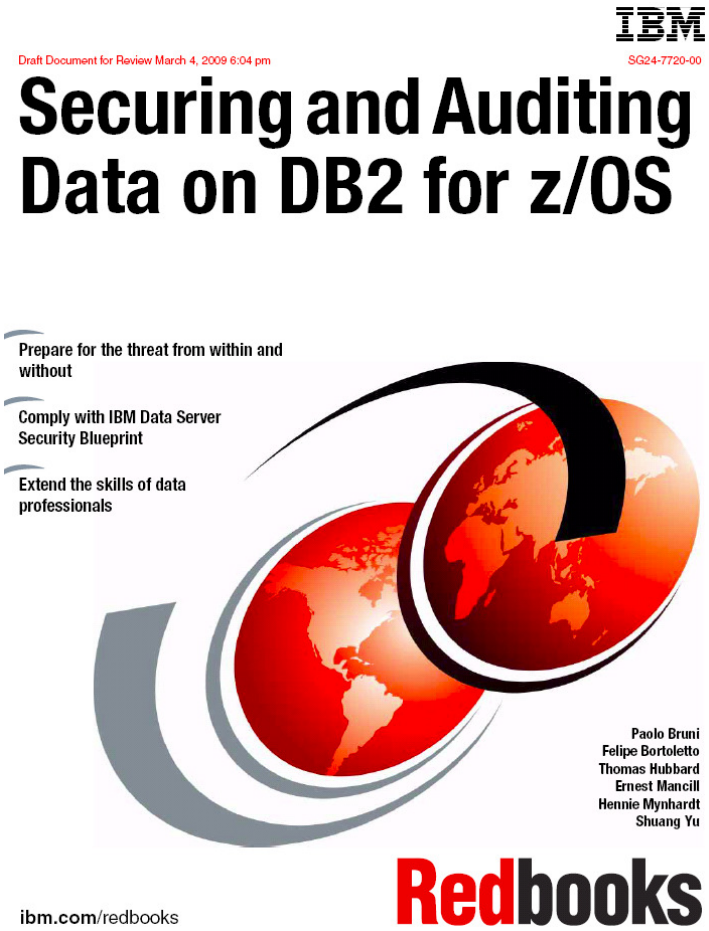


ASC- Audit SQL Collector

DB2 Audit Management Expert Architecture Dual Mode



Redbook on Audit and Encryption on DB2 for z/OS – SG24-7720




Thank
You