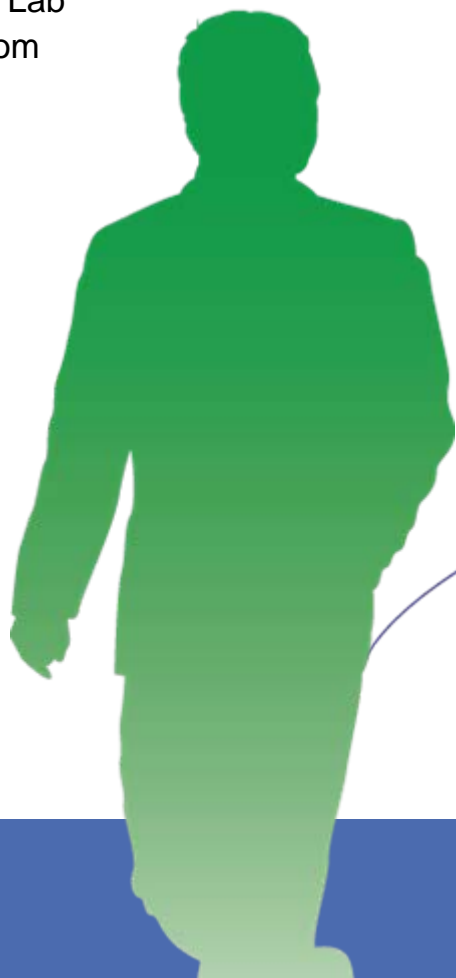


Addressing Audit and Compliance requirements in a DB2 z/OS environment

Presenter: Mike Biere
IBM WW Marketing Mgr.
IBM Silicon Valley Lab
mbiere@us.ibm.com
Session: 003



IBM Information
ON Demand 2010

INFORMATION-LED
TRANSFORMATION



LEAD
THE WAY



IBM

January 21 - SINGAPORE • January 26 – MALAYSIA • January 28 - THAILAND

Data Management Communities for DB2

- IDUG – the worldwide community of DB2 users
 - Membership is FREE – join today! www.idug.org

- Data Management Community – share and interact with peers around the world
 - www.ibm.com/software/data/management/community.html

- Information Champions – recognizes individuals who have made the most outstanding contributions to the Information Management community
 - www.ibm.com/software/data/champion

Disclaimer

© Copyright IBM Corporation [current year]. All rights reserved.
U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM’S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS AND/OR SOFTWARE.

IBM, the IBM logo, ibm.com, are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml

Other company, product, or service names may be trademarks or service marks of others.

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).

DB2 Audit Trace versus RACF

→ Key Points:

- RACF provides significant controls to protect access to resources, but does little in the way of meaningful access reporting
- DB2 Audit trace will do nothing to protect data, but provides data to help understand what type of access has occurred.
 - Auditing is about ensuring that the appropriate controls are in place to identify inappropriate access and use of production data
 - You need some form of audit facility to watch your privileged users who have RACF and/or DB2 authority and users that have access to sensitive data within the scope of their job
 - Understanding how trusted (privileged) users access sensitive information is essential to ensuring that data is indeed protected

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 environment – QMF, SPUFI, etc. Constitutes exposure
 - SPUFI Plan can be restricted but ALL use should be audited
- Privileged ID's (DBA/Sysadmin) should be audited
- Distributed Application Environment
 - Use of SQLESETI can provide granularity with credential population to IFI extensions
 - End User Workstation Name
 - End User Workstation Process
 - End User Workstation Userid
 - Implement RACF Enterprise Identify Mapping Feature
 - <http://www-03.ibm.com/servers/eserver/security/eim>
- 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
- TCIM, DB2 Audit Management Expert, others
- DSN1SMFP, others
- log formatting: tools, DSN1LOGP, Log Analyzer
- various recovery and cloning techniques
 - triggers
- REPORT RECOVERY
- RACF print, unload

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.

Suggested Audit traces on DB2 for z/OS DB2 Common Criteria

- IFCIDs for Audit
- Accounting
 - 0003 successful access
- Audit
 - 0140: Audit all authorization failures
 - 0141: Audit all grants & revokes
 - 0142: Audit DDL Create / Alter / Drop
 - 0143: Audit First Write
 - 0144: Audit First Read
 - 0145: Audit DML Statement
 - 0314: Authorization Exit Parameters
- Performance
 - 0004: Trace Start
 - 0005: Trace Stop
 - 0023: Utility Start
 - 0024: Utility Change
 - 0025: Utility End
 - 0106: System Parameters
 - 0247: input host variables
 - 0350: SQL Statement

Suggested Audit traces – The “Bare Bones Minimum”

→ DB2 security audit suggestions:

- Catalog table queries
- Audit class 1, 2, 3
 - 0140: audit all authorization failures
 - 0141: audit all grants & revokes
- DB2 9 audit class 10: audit trusted context
 - 0269: establish trusted connection and switch user
 - 0270: CREATE & ALTER TRUSTED CONTEXT statements
- Performance
 - 0004: Trace Start
 - 0005: Trace Stop
 - 0106: System Parameters

Auditing utilities which act outside of DB2

The audit gap

- When a 3rd party unload is executed against the DB2 VSAM data sets instead of through DB2, the IBM audit record has no knowledge of data access. However, the 3rd party utility “history” table will contain the date and time of the utility with the relevant utility id. The utility activity at run time is kept in another “in-flight” table. But the records are deleted upon completion of the utility.

Closing the Gap

- A DB2 trigger is deployed on the “in-flight” table that checks against the list of sensitive tablespaces. If it is one of our audited objects, the after trigger fires to insert this information into the DBA version of the in-flight table.

→ CREATE TRIGGER

→ xxxxx.trigger name

→ AFTER

→ INSERT

→ ON xxxxx.DBA_UTILITY_INFLIGHT

→ REFERENCING

→ NEW AS N

→ FOR EACH ROW

→ MODE DB2SQL

→ WHEN (N.NAME2 IN ('TS1', 'TS2', 'TS3', 'TS4','TS5')) BEGIN

→ ATOMIC INSERT INTO xxxxx. DBA_UTILITY_INFLIGHT (UTILID, NAME1, NAME2, KIND,

→ PARTITION, UTILNAME, SHRLEVEL, STATUS, XCOUNT, DDNAME,

→ BLOCKS, ORIG_STATUS, EXTRBA, STATE) VALUES (N.UTILID, N.NAME1,

→ N.NAME2, N.KIND, N.PARTITION, N.UTILNAME, N.SHRLEVEL,

→ N.STATUS, N.XCOUNT, N.DDNAME, N.BLOCKS, N.ORIG_STATUS, N.EXTRBA,

→ N.STATE) ; END

- In DBA_UTILITY_INFLIGHT, the record will not be deleted and so the audit trail is left in tact. A separate query of this table will yield all 3rd party unload activity.

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**.
- When estimating the performance impact of the audit trace, consider the frequency of certain events. For example, 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.
 - Following is the summary of results of the DB2 V8 Audit trace measurements :

The measurements were done with Audit trace class(*) on and all the tables in the workload were enabled for 'Audit All'.

For OLTP measurement with distributed IRWW SQL CLI workload with 9 Tables, 3 PI, 8 NPI and 7 transactions running at 493 transactions per second, the **DB2 Class 2 CPU increase was +7.2%**.

For Utility measurements with LOAD, Rebuild Index, Reorg Table, Reorg Index utilities using 1 Table, 10 partitions, 1 PI and 5 NPI, there was no measurable CPU increase.

- 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

V9 Trace Extensions – START TRACE

→ Qualifications by:

- LOC
 - Location-Name
 - LUName
 - IPAddress
- PLAN
- PACKAGE
 - PKGLOC
 - PKGCOL
 - PKGPROG
- Workstation Identifiers
 - USERID
 - APPLNAME
 - WRKSTN
- Miscellaneous
 - CORRID
 - CONNID
 - ROLE

→ Exclude by:

- LOC
 - XLOC
- PLAN
 - XPLAN
- PACKAGE
 - XPKGLOC
 - XPKGCOL
 - XPKGPROG
- Workstation Identifiers
 - XUSERID
 - XAPPLID
 - XWRKSTN
- Miscellaneous
 - XCORRID
 - XCONNID
 - XROLE

V9 Trace Extensions - Wildcards

→ Tracing threads using the * wildcard:

–You can use the wildcard suffix, “*” to filter threads. For example, if you specify “-START TRACE PLAN (A,B,C*)”, DB2 will trace, and then return A, B, CDE, CDEFG, CDEFGH, and so on. It will trace threads “A”, “B” and all threads starting with “C”.

→ Tracing threads using the positional, (_) wildcard:

–You can utilize the positional wildcard, which is represented by the, “_” character, to trace threads when you want the wildcard in the middle, or when you want to trace threads of a specific length. For example, if you specify “-START TRACE PLAN (A_C)”, all threads will be traced that are three characters that have “A” as the first character, and “C” as the third.

→ Tracing multiple threads at once using wildcards:

–You also have the option of tracing multiple threads based on multiple trace qualifications. For example, you can specify, “-START TRACE PLAN (A*, B*, C*)” to simultaneously trace ALL threads for plan that start with “A”, “B”, and “C”. The wildcard character, “*” will trace all threads.

–You have the ability to filter multiple threads at the same time, setting specific criteria for the trace: For example, you can specify “-START TRACE PLAN (A) USERID (B)”. This will trace the threads where the plan thread is A, and the user ID is B.

V9 Trace Extensions – Some Restrictions

- When tracing threads, you can only specify more than one thread criteria for one filter per “-START TRACE” command.
 - For example, you can specify “-START TRACE PLAN (A,B) USERID (B) WRKSTN (E),” but you cannot specify “-START TRACE PLAN (A, B) USERID (A, B) WRKSTN (E).
- If you use one or no values for PLAN, AUTHID, or LOCATION, the START TRACE command starts a single trace. If you use multiple values for PLAN, AUTHID, or LOCATION, the command starts a trace for each plan, authorization ID, or location. There can be a total of up to 32 traces going at one time (**all trace types**).
- You must use a privilege set of the process that includes one of the following privileges or authorities:
 - TRACE privilege
 - SYSOPR authority
 - SYSCTRL authority
 - SYSADM authority

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

DSN1SMFP – Sample Report Outputs

IFCID – 141 Audit Grant/Revoke Report

```
GRANTOR : SYSADM          REASON : SYSADM          RETURN: 0000000000
OBJECT  : STORAGE GROUP   OPTIONS: X'0400000000000000'
SQL STMT: GRANT USE OF STOGROUP DSN86810 TO PUBLIC
```

IFCID – 106 System Parameters Report

```
COMMON CRITERIA ENVIRON : NO
SYSADM ID 2              : SYSADM
ENABLE DB2 AUTHORIZATION: YES
PACK AUTH CACHE         : 0000032768
ONL SYSPARM CORID       :

MISCELLANEOUS INSTALLATION PARAMETERS
DDL REGISTRATION FLAG: X'30'
SITE TYPE             : LOCAL
CACHE DYNAMIC SQL    : NO
DBADM CREATE VIEW    : NO
ONL SYSPARM USER ID  :

INSTALL SYSADM : SYSADM
SYSOPER ID    : SYSOPR
AUTH. CACHE SIZE: 01024
EDM STMT CACHE : 0005120000
ONL SYSPARM TIME: 00:26:40

DEFAULT USERID : IBMUSER
SYSOPER ID 2   : SYSOPR
HOP SITE AUTHORIZ.: YES
ONL SYSPARM TYPE : N/A
```

OMEGAMON XE for DB2 Performance Monitor/Expert for z/OS

- Real-time monitoring
 - Threads and Statistics monitoring
 - DB2 Connect monitoring
 - Object Analysis
 - Data Sharing/Sysplex data (DB2Plex data)
- Near-term history
- Trace collection (**also as part of the PWH process support**)
- Reporting
 - Accounting, Statistics, SQL Activities, Locking, I/O Activity, Audit, Utilities, Record Trace
 - Executable as separate jobs or via PWH process engine
- Performance Warehouse with expert analysis support
- Buffer Pool Analysis, expert advice, and simulation (**only with the OMEGAMON XE for DB2 Performance Expert**)



DB2 OMEGAMON Performance Expert Audit Report Set

- Not strictly a performance report.
- Reports information about usage of auditable objects and authorization management.
 - Authorization changes
 - Authorization control (GRANTS and REVOKEs of privileges)
 - Authorization failures
 - DML statements against auditable DB2 tables at bind time
 - DDL operations against auditable DB2 tables
 - Read/write access against auditable DB2 tables
 - Utility executions against auditable DB2 tables
- Traces show individual events.
- Reports show audit information for an aggregation of DB2PE identifiers, e.g. primauth-planname-objects.

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

OMPE "File" report
commands

OMPE Audit
Detail Report

```

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
    
```

```

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                ORDER: PRIMAUTH-PLANNAME                                         TO: NOT SPECIFIED
SUBSYSTEM: DSNC           SCOPE: MEMBER                                           ACTUAL FROM: 09/06/06 01:47:43.60
DB2 VERSION: V8                                                   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'
    
```

Invoking the DB2 load utility to populate the DB2 Performance DB with Audit data.

Load Control sample statements located in RKO2SAMP

```

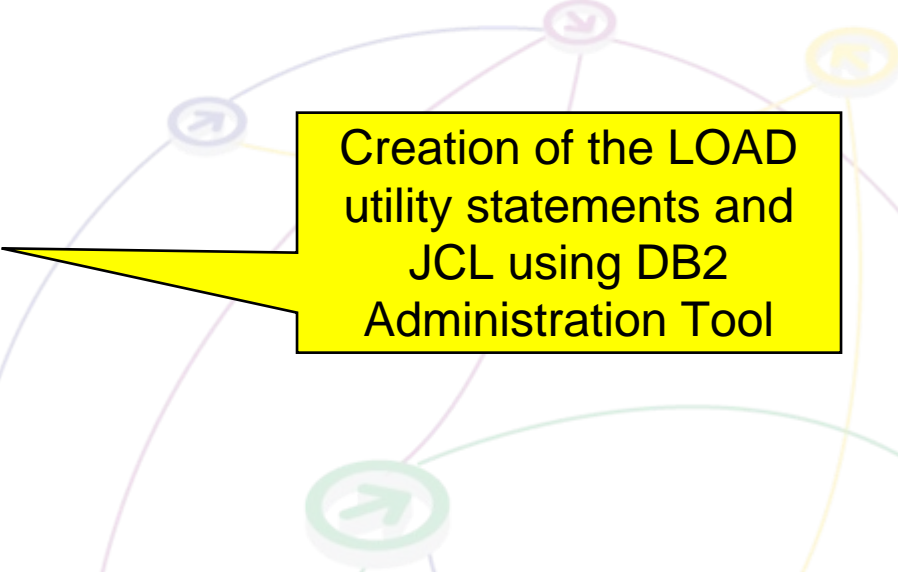
File Edit Edit Settings Menu Utilities Compilers Test Help
EDIT      SYS248.SPFTEMP2.CNTL      Columns 00001 00072
000052 LOAD INDDN SYSREC
000053 RESUME NO
000054 REPLACE
000055 INTO TABLE DB2PMFAUDT_DML
000056 WHEN (251:259) = 'DML N'
000057 (DB2PM_REL POSITION(3) SMALLINT,
000058 DB2_REL POSITION(9) CHAR(2),
000059 LOCAL_LOCATION POSITION(11) CHAR(16),
000060 GROUP_NAME POSITION(27) CHAR(8),
000061 SUBS_ID POSITION(35) CHAR(4),
000062 MEMBER_NAME POSITION(39) CHAR(8),
000063 NET_ID POSITION(47) CHAR(8),
000064 LUNAME POSITION(55) CHAR(8),
000065 INSTANCE_NBR POSITION(63) CHAR(12),
000066 LUW_SEQNO POSITION(75) SMALLINT,
000067 REQ_LOC_NAME POSITION(87) CHAR(16),
000068 ENDUSER POSITION(103) CHAR(16),
000069 USNAME POSITION(119) CHAR(18),
Command ==> Scroll ==> CSR
F1=Help F2=Split F3=Exit F5=Rfind F6=Rchange F7=Up
F8=Down F9=Swap F10=Left F11=Right F12=Cancel
    
```

```

DB2 Admin ----- DSNL Specify Utility Options - LOAD ----- 08:20
Option ==>
Top of data
Execute utility on table SYS248.DB2PMFAUDT_DML
using the following options:

Utility ID      ==> LOADAUD      More: +
                (Name identifying this utility to DB2)
Unloaded Data  ==> SYS248.OMPE.AUFIL2
                (Name of data set containing unloaded data)
Unloaded How?  ==> U          (U=Unload Utility, R=Reorg Utility)
Table/Col Info ==> CANDLET.XEGA.DEMOMVS.RKO2SAMP(DGOXLDML)
                (Name of data set containing table/column info)
RESUME         ==> NO        (Yes/No, load recs into non-empty table space)
SHRLEVEL      ==>          (None/Change, concurrent table space access)
REPLACE       ==> YES       (Yes/No, empty table space/index before load)
COPYDDN1      ==>          (DDname identifying primary copy data set)
COPYDDN2      ==>          (DDname identifying backup copy data set)
RECOVERYDDN1  ==>          (DDname identifying primary ds @ recovery site)
RECOVERYDDN2  ==>          (DDname identifying backup ds @ recovery site)

TABLE ALL     ==>          (Yes/No, info for all columns in table space)
F1=HELP      F2=SPLIT      F3=END      F4=RETURN   F5=RFIND    F6=RCHANGE
F7=UP        F8=DOWN       F9=SWAP     F10=LEFT    F11=RIGHT   F12=RETRIEVE
    
```



Creation of the LOAD utility statements and JCL using DB2 Administration Tool

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

Open Table - DB2PMFAUDT_DML

DSNC - DSNC - AUDITDB - SYS248 - DB2PMFAUDT_DML

E	PRIMAUTH	ORIGAUTH	TIMESTAMP	IFCID	DATABASE_DBID	PAGESET_OBID	TABLE_OBID	DATABASE_NAME	PAGESET_NAME
	SYS248	SYS248	Sep 6, 2006 1:47:41 AM 602771	144	307	2	5	SYS248SA	SYS248TS		
	SYS248	SYS248	Sep 6, 2006 1:48:22 AM 560444	143	307	2	5	SYS248SA	SYS248TS	00036FBEA220	...
	SYS248	SYS248	Sep 6, 2006 1:48:22 AM 564498	143	307	2	5	SYS248SA	SYS248TS	00036FBEA3DA	...
	SYS248	SYS248	Sep 6, 2006 1:48:28 AM 130075	144	307	2	5	SYS248SA	SYS248TS		...
	SYS248	SYS248	Sep 6, 2006 1:48:58 AM 571847	143	307	2	5	SYS248SA	SYS248TS	00036FBEEA62	...
	SYS248	SYS248	Sep 6, 2006 1:48:58 AM 579028	143	307	2	5	SYS248SA	SYS248TS	00036FBEEAC1C	...
	SYS248	SYS248	Sep 6, 2006 1:49:06 AM 253828	144	307	2	5	SYS248SA	SYS248TS		...
	SYS248	SYS248	Sep 6, 2006 1:49:38 AM 826482	143	307	2	5	SYS248SA	SYS248TS	00036FBEEADD6	...
	SYS248	SYS248	Sep 6, 2006 1:49:38 AM 831367	143	307	2	5	SYS248SA	SYS248TS	00036FBEEB000	...
	SYS248	SYS248	Sep 6, 2006 1:49:38 AM 838245	143	307	2	5	SYS248SA	SYS248TS	00036FBEEB1BA	...

Commit Roll Back Filter Fetch More Rows

Automatically commit updates 10 row(s) in memory Close Help

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

Limitations of the audit trace

- The audit trace does not record everything, as the following list of limitations indicates:
 - The auditing that is described in this information takes place only when the audit trace is on.
 - The trace audits only the tables that you specifically choose to audit.
- The trace does NOT capture before/after change data because the DB2 log records this information.
 - If an agent or transaction accesses a table more than once in a single unit of recovery, the audit trace records only the first access.
- The audit trace does not audit some utilities. The trace audits the first access of a table with the LOAD utility, but it does not audit access by the COPY, RECOVER, and REPAIR utilities. The audit trace does not audit access by stand-alone utilities, such as DSN1CHKR and DSN1PRNT.
- You cannot audit the catalog tables because you cannot create or alter catalog tables.
- 3rd Party DB2 utilities (run outside of DB2) will not be caught with the AUDIT CLASS 8
- Dynamic SQL host variable data not collected
- This auditing coverage is consistent with the goal of providing a moderate volume of audit data with a low impact on performance. However, 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 IFASMFDMF 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

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

DB2 Audit Management Expert Components

→ Audit server

- Started task or batch job
- central control point for an Audit Management Expert network
- single audit server can support data collection from multiple agents on multiple z/OS systems

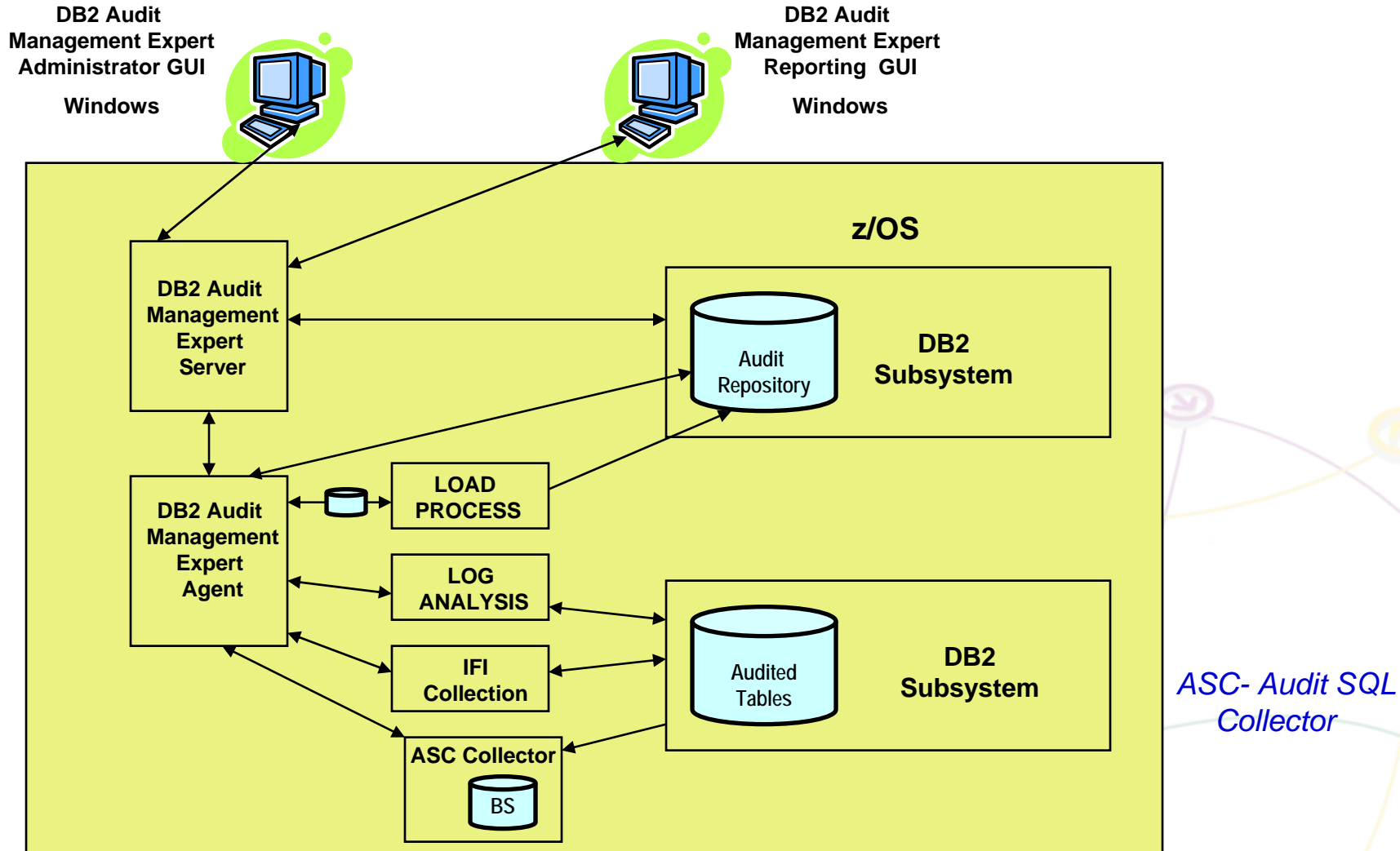
→ Agent

- Started Task or batch job
- responsible for communications in an Audit Management Expert environment
- acts as a "container" to run the various collectors
- One per DB2 to Audit

→ CLIENT User interfaces

- Audit Management Expert Reporter
- Audit Management Expert Administration
- Windows

DB2 Audit Management Expert Architecture



ASC- Audit SQL Collector

DB2 Audit Management Expert Profiles

→ Profiles are created/maintained via **Administration UI**

– Collection Profile

- records the details for what audit data is stored to the Audit Management Expert repository

– Agent Profile

- Select ASC collection method
- Configure General settings
 - Retention count, interval length
- DB2 Load utility parameters
- Define Job cards for load and log analysis

– User Profile

- contain information specific to an individual Audit Management Expert user such as: the user type, configurable privileges, and associated user groups

AME and Enterprise Wide Auditing - Challenges

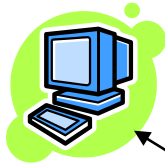
- Existing appliance technology based on data feeds from primarily 2 sources
 - Event log from DB2 trace events written to SMF (agent)
 - Network “Sniffer” implementation (appliance)
- Restrictions and challenges with DB2 Trace versus a superior low overhead data collection approach with AME’s ASC
- Network traffic based audit feeds challenged by
 - Encrypted Data Streams
 - Local Attachments (Batch, TSO, etc.)
 - Stored Procedures
 - Performance impact to network throughput due to indiscriminate examination of all network flows
- Strong requirement to view and manage Audit events across the enterprise from a single UI

AME Extract File Enhancement via maintenance stream (PTFs UK41519, UK41521, UK41523)

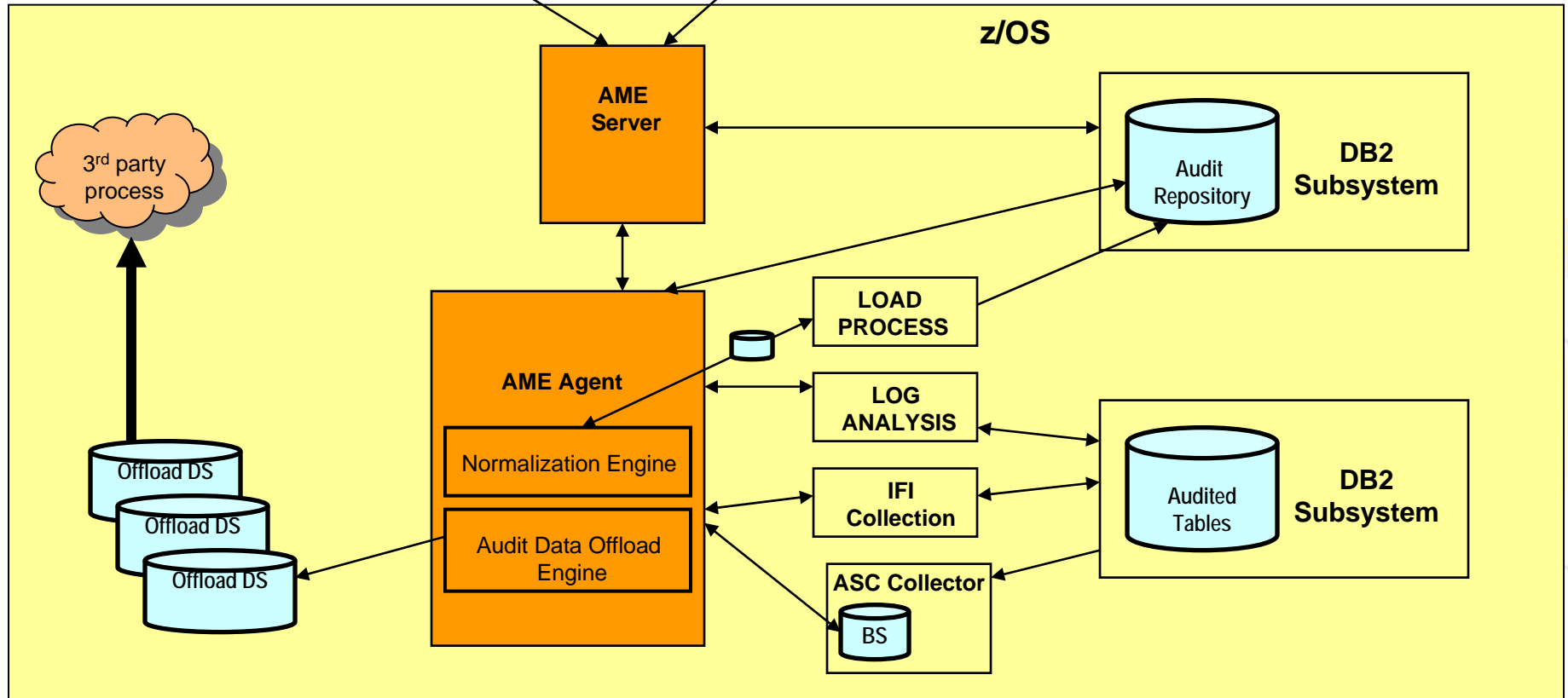
- AME will provide an option to generate audit log data sourced from either DB2 Trace or ASC (Audit SQL Collector) in an documented extract file format.
- Extract files will be standard physical sequential datasets.
- Exploiters will be responsible for transporting (via secure FTP for example) data to appliance server environment.
- Management of Extract files (archiving, deleting, etc.) will be the responsibility of exploiters
- Data will be not be aggregated (normalized), this is to reduce overhead of data collection.
- Static SQL statement collection will be optional, this is to avoid the overhead of accessing the catalog with static SQL statement number to extract SQL statement text.
- Exploiters to include
 - Tivoli Consul Insight Manager (coming Q1 2010)
 - Tizor - Mantra
 - Imperva - SecureSphere
 - Others anticipated at a future date

DB2 Audit Management Expert Architecture Dual Mode

DB2 Audit
Management Expert
Administrator GUI
Windows



DB2 Audit
Management Expert
Reporting GUI
Windows



Alerts

- Real-time alert monitoring
- Exceptions outside of expected business process
- Immediate triaging & response
- Easy integration with 3rd-party IT ecosystems: SYSLOG, SNMP, Email...

Alerts (filtered)

No.	Updated	#	Alert Description
2004	08:49:02	11	z/OS Security Po

Violations:

User	OS User	OS Host
ajcuser		

Event 6909825234996570923: Custom Rule Violation

Key	Value
Violation Description	z/OS Security Policy
Violated Item	Custom Violation

Event Details:

Event Time	Server Group	Service	Application
July 31, 2008 6:24:39 PM	DB2 Mainframe	DB2	Default DB2 Application

Connection	User	DB Application	OS User	OS Host
:0 → :0	ajcuser			

Affected Rows	Response Size	Response Time
0	0 Records	0 msec.

Error Code	Error Message

START TRACE (AUDIT)CLASS (3)RMD (*)DEST (OPX)PLAN (*)AUTHID (*)IFCID (*)BUFSIZE (16)TDAT A (CORRELATION DISTRIBUTED)

Alert 2004: z/OS Security Policy

Actions: None
Policy: z/OS Security Policy

Aggregated from 08:49:01 (0 hour(s), 2 minute(s)),

Alert aggregated by:

Distinct value for:	Value
Custom Rule	z/OS Security Policy
Server Group	DB2 Mainframe
Source IP	

Violations:

User	OS User
ajcuser	
ajcuser	
ajcuser	

Viewing the Audit Logs:

Provides all the details including: date and time , database user name and parsed query

Date/Time	Database Username	Parsed Query	Log Collector
7/21/08 3:45:57 PM	csliivi	display log	z/OS
7/21/08 3:45:58 PM	csliivi	display log	z/OS
7/21/08 3:46:01 PM	csliivi	display log	z/OS
7/21/08 3:46:02 PM	csliivi	display log	z/OS
7/31/08 5:12:09 PM	csliivi	display log	z/OS
7/21/08 3:32:55 PM	csliivi	display utility(*)	z/OS
7/21/08 3:37:41 PM	csliivi	display utility(*)	z/OS
7/21/08 3:38:14 PM	csliivi	display utility(*)	z/OS
7/21/08 3:45:57 PM	csliivi	display utility(*)	z/OS
7/21/08 3:45:58 PM	csliivi	display utility(*)	z/OS
7/21/08 3:46:01 PM	csliivi	display utility(*)	z/OS
7/21/08 3:46:02 PM	csliivi	display utility(*)	z/OS
7/31/08 5:12:09 PM	csliivi	display utility(*)	z/OS
7/31/08 5:15:51 PM	csliivi	delete from dsn8710.act where actno=?	z/OS
7/31/08 5:15:51 PM	csliivi	insert into dsn8710.act (actno,actkwd,actdesc) values(?,?,?)	z/OS
7/31/08 5:15:51 PM	csliivi	update dsn8710.act set actdesc=? where actno=?	z/OS
7/21/08 3:28:15 PM	ajcuser	start trace (audit)class (?)rmid (*)dest (opx)plan (*)authid (*)ifcid (*)bufsize (?)tdata (correlation distributed)	z/OS
7/21/08 3:42:23 PM	ajcuser	start trace (audit)class (?)rmid (*)dest (opx)plan (*)authid (*)ifcid (*)bufsize (?)tdata (correlation distributed)	z/OS
7/21/08 3:48:27 PM	ajcuser	start trace (audit)class (?)rmid (*)dest (opx)plan (*)authid (*)ifcid (*)bufsize (?)tdata (correlation distributed)	z/OS

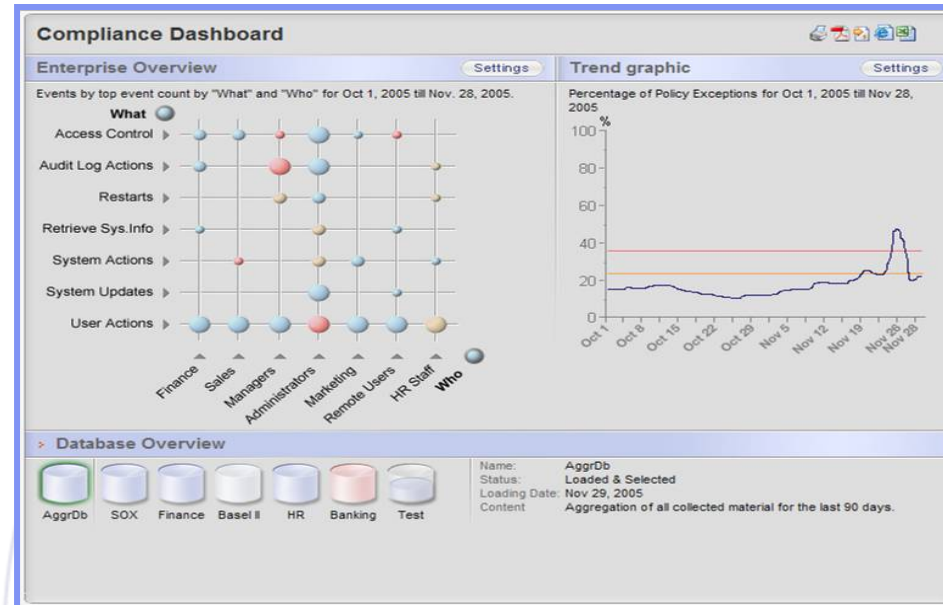
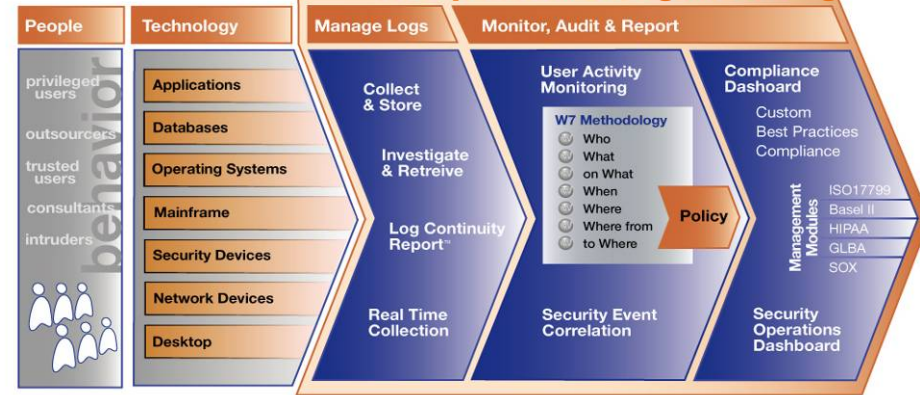
Tivoli Compliance Insight Manager

Tivoli Compliance Insight Manager

Tivoli Compliance Insight Manager provides an enterprise security compliance dashboard with in-depth privileged user **monitoring** capabilities, all powered by a comprehensive log and audit trail collection capability

Key Features

- ➔ Compliance management modules and regulation-specific reports
- ➔ Unique ability to monitor user behavior, including PUMA (Privileged User Monitoring and Audit) reporting
- ➔ Broadest, most complete log and audit trail capture capability
- ➔ W7 log normalization translates your logs into business terms
- ➔ Easy ability to compare behavior to regulatory and company policies – auditors no longer need RACF expertise to monitor activities
- ➔ Enabler event source integrates the OS and mainframe database events into TCIM's enterprise compliance dashboard



TCIM – Representative Screen

Platform History Event List on Platform Z180 (z/OS) - Database GEM on Server CIFDB - Microsoft Internet Explorer

Address: http://9.142.236.76/view/?expert=platformhistoryevents&GEMCatalog=GEM&plfdett=z%2FOS&plfdetnm=Z180&count=1573&plfdetix=3&EPRISECatalog=EPRISED&navig=Gem&navname=Gem.GemSummary&stid=1207083708203

IBM Business Transformation Homepage IBM Standard Software Installer IT Help Central Join World Community Grid Windows Marketplace

Information Management Lotus Rational Tivoli WebSphere

Dashboard Trends Reports Regulations Policy Groups Distribution Settings

CIFDB > GEM > Platform History Events

Platform History Event List on Platform Z180 (z/OS)

Database GEM on Server CIFDB

Setup:

Start time: Month: June, Day: 20, Year: 2007, Hour: 8, Min: 10
 End time: Month: March, Day: 31, Year: 2008, Hour: 13, Min: 0

Execute Reset

Time zone: Event time zone

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
10	Wed Jun 20 2007 06:10:36 GMT+00:00	1	Verify : Dbtablespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.DSN6S91E	Z180 (z/OS)
50	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Modify : Dbtablespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
50	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Modify : Dbtablespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP2	Z180 (z/OS)
50	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Change : Auditlog / Success	Z180 (z/OS)	System	Z180 (z/OS)	SYSTEM : Z180 / SMF	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Read : Dbtablespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Read : Dbtablespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Read : Dbtablespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Read : Dbtablespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Read : Dbtablespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Read : Dbtablespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Write : Dbtablespace / Success	Z180 (z/OS)	.SYSOPR	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Write : Dbject / Success	Z180 (z/OS)	.SYSOPR	Z180 (z/OS)	DBOBJECT : - / -	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Write : Dbtablespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)

Regulatory Resource Center

start

10:29:50 - AT&T Ne... Vacation Planner - 2... Session B - [24 x 80] Platform History Eve... IBM Lotus Sametime ... meadowsr@us.ibm.c... 100%

5:02 PM Tuesday 4/1/2008

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

IBM

Draft Document for Review March 4, 2009 6:04 pm

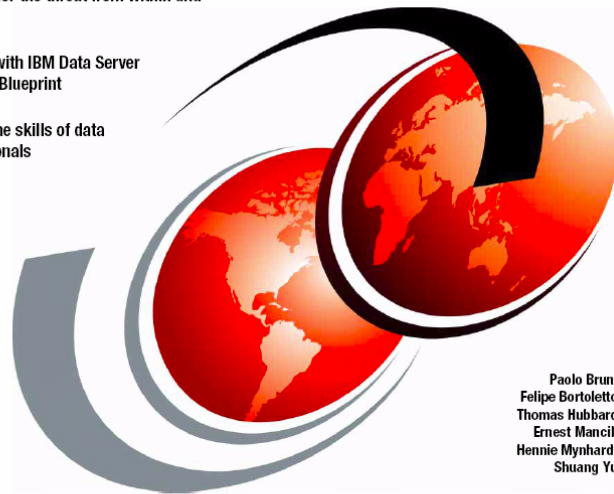
SG24-7720-00

Securing and Auditing Data on DB2 for z/OS

Prepare for the threat from within and
without

Comply with IBM Data Server
Security Blueprint

Extend the skills of data
professionals



Paolo Bruni
Felipe Bortoletto
Thomas Hubbard
Ernest Mancill
Hennie Mynhardt
Shuang Yu

Redbooks

ibm.com/redbooks



Data Management Communities for DB2

- IDUG – the worldwide community of DB2 users
 - Membership is FREE – join today! www.idug.org

- Data Management Community – share and interact with peers around the world
 - www.ibm.com/software/data/management/community.html

- Information Champions – recognizes individuals who have made the most outstanding contributions to the Information Management community
 - www.ibm.com/software/data/champion

Disclaimer

© Copyright IBM Corporation [current year]. All rights reserved.

U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM’S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS AND/OR SOFTWARE.

IBM, the IBM logo, ibm.com, are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at “Copyright and trademark information” at www.ibm.com/legal/copytrade.shtml

Other company, product, or service names may be trademarks or service marks of others.

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 CEO's bank balance or personal customer information
- provide meaningful information about access to protected DB2 resources (authorized or not).

DB2 Audit Trace versus RACF

→ Key Points:

- RACF provides significant controls to protect access to resources, but does little in the way of meaningful access reporting
- DB2 Audit trace will do nothing to protect data, but provides data to help understand what type of access has occurred.

- Auditing is about ensuring that the appropriate controls are in place to identify inappropriate access and use of production data
- You need some form of audit facility to watch your privileged users who have RACF and/or DB2 authority and users that have access to sensitive data within the scope of their job
- Understanding how trusted (privileged) users access sensitive information is essential to ensuring that data is indeed protected

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 environment – QMF, SPUFI, etc. Constitutes exposure
 - SPUFI Plan can be restricted but ALL use should be audited
- Privileged ID's (DBA/Sysadmin) should be audited
- Distributed Application Environment
 - Use of SQLESETI can provide granularity with credential population to IFI extensions
 - End User Workstation Name
 - End User Workstation Process
 - End User Workstation Userid
 - Implement RACF Enterprise Identify Mapping Feature
 - <http://www-03.ibm.com/servers/eserver/security/eim>
- 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
- TCIM, DB2 Audit Management Expert, others
- DSN1SMFP, others
- log formatting: tools, DSN1LOGP, Log Analyzer
- various recovery and cloning techniques
 - triggers
- REPORT RECOVERY
- RACF print, unload

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.

Suggested Audit traces on DB2 for z/OS DB2 Common Criteria

- IFCIDs for Audit
- Accounting
 - 0003 successful access
- Audit
 - 0140: Audit all authorization failures
 - 0141: Audit all grants & revokes
 - 0142: Audit DDL Create / Alter / Drop
 - 0143: Audit First Write
 - 0144: Audit First Read
 - 0145: Audit DML Statement
 - 0314: Authorization Exit Parameters
- Performance
 - 0004: Trace Start
 - 0005: Trace Stop
 - 0023: Utility Start
 - 0024: Utility Change
 - 0025: Utility End
 - 0106: System Parameters
 - 0247: input host variables
 - 0350: SQL Statement

Suggested Audit traces – The “Bare Bones Minimum”

→ DB2 security audit suggestions:

- Catalog table queries
- Audit class 1, 2, 3
 - 0140: audit all authorization failures
 - 0141: audit all grants & revokes
- DB2 9 audit class 10: audit trusted context
 - 0269: establish trusted connection and switch user
 - 0270: CREATE & ALTER TRUSTED CONTEXT statements
- Performance
 - 0004: Trace Start
 - 0005: Trace Stop
 - 0106: System Parameters

Auditing utilities which act outside of DB2

The audit gap

- When a 3rd party unload is executed against the DB2 VSAM data sets instead of through DB2, the IBM audit record has no knowledge of data access. However, the 3rd party utility “history” table will contain the date and time of the utility with the relevant utility id. The utility activity at run time is kept in another “in-flight” table. But the records are deleted upon completion of the utility.

Closing the Gap

- A DB2 trigger is deployed on the “in-flight” table that checks against the list of sensitive tablespaces. If it is one of our audited objects, the after trigger fires to insert this information into the DBA version of the in-flight table.

→ CREATE TRIGGER

→ xxxxx.trigger name

→ AFTER

→ INSERT

→ ON xxxxx.DBA_UTILITY_INFLIGHT

→ REFERENCING

→ NEW AS N

→ FOR EACH ROW

→ MODE DB2SQL

→ WHEN (N.NAME2 IN ('TS1', 'TS2', 'TS3', 'TS4','TS5')) BEGIN

→ ATOMIC INSERT INTO xxxxx. DBA_UTILITY_INFLIGHT (UTILID, NAME1, NAME2, KIND,

→ PARTITION, UTILNAME, SHRLEVEL, STATUS, XCOUNT, DDNAME,

→ BLOCKS, ORIG_STATUS, EXTRBA, STATE) VALUES (N.UTILID, N.NAME1,

→ N.NAME2, N.KIND, N.PARTITION, N.UTILNAME, N.SHRLEVEL,

→ N.STATUS, N.XCOUNT, N.DDNAME, N.BLOCKS, N.ORIG_STATUS, N.EXTRBA,

→ N.STATE) ; END

- In DBA_UTILITY_INFLIGHT, the record will not be deleted and so the audit trail is left in tact. A separate query of this table will yield all 3rd party unload activity.

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**.
- When estimating the performance impact of the audit trace, consider the frequency of certain events. For example, 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.
 - Following is the summary of results of the DB2 V8 Audit trace measurements :

The measurements were done with Audit trace class(*) on and all the tables in the workload were enabled for 'Audit All'.

For OLTP measurement with distributed IRWW SQL CLI workload with 9 Tables, 3 PI, 8 NPI and 7 transactions running at 493 transactions per second, the **DB2 Class 2 CPU increase was +7.2%**.

For Utility measurements with LOAD, Rebuild Index, Reorg Table, Reorg Index utilities using 1 Table, 10 partitions, 1 PI and 5 NPI, there was no measurable CPU increase.

- 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

V9 Trace Extensions – START TRACE

→ Qualifications by:

- LOC
 - Location-Name
 - LUName
 - IPAddress
- PLAN
- PACKAGE
 - PKGLOC
 - PKGCOL
 - PKGPROG
- Workstation Identifiers
 - USERID
 - APPLNAME
 - WRKSTN
- Miscellaneous
 - CORRID
 - CONNID
 - ROLE

→ Exclude by:

- LOC
 - XLOC
- PLAN
 - XPLAN
- PACKAGE
 - XPKGLOC
 - XPKGCOL
 - XPKGPROG
- Workstation Identifiers
 - XUSERID
 - XAPPLID
 - XWRKSTN
- Miscellaneous
 - XCORRID
 - XCONNID
 - XROLE

V9 Trace Extensions - Wildcards

→ Tracing threads using the * wildcard:

–You can use the wildcard suffix, “*” to filter threads. For example, if you specify “-START TRACE PLAN (A,B,C*)”, DB2 will trace, and then return A, B, CDE, CDEFG, CDEFGH, and so on. It will trace threads “A”, “B” and all threads starting with “C”.

→ Tracing threads using the positional, (_) wildcard:

–You can utilize the positional wildcard, which is represented by the, “_” character, to trace threads when you want the wildcard in the middle, or when you want to trace threads of a specific length. For example, if you specify “-START TRACE PLAN (A_C)”, all threads will be traced that are three characters that have “A” as the first character, and “C” as the third.

→ Tracing multiple threads at once using wildcards:

–You also have the option of tracing multiple threads based on multiple trace qualifications. For example, you can specify, “-START TRACE PLAN (A*, B*, C*)” to simultaneously trace ALL threads for plan that start with “A”, “B”, and “C”. The wildcard character, “*” will trace all threads.

–You have the ability to filter multiple threads at the same time, setting specific criteria for the trace: For example, you can specify “-START TRACE PLAN (A) USERID (B)”. This will trace the threads where the plan thread is A, and the user ID is B.

V9 Trace Extensions – Some Restrictions

- When tracing threads, you can only specify more than one thread criteria for one filter per “-START TRACE” command.
 - For example, you can specify “-START TRACE PLAN (A,B) USERID (B) WRKSTN (E),” but you cannot specify “-START TRACE PLAN (A, B) USERID (A, B) WRKSTN (E).
- If you use one or no values for PLAN, AUTHID, or LOCATION, the START TRACE command starts a single trace. If you use multiple values for PLAN, AUTHID, or LOCATION, the command starts a trace for each plan, authorization ID, or location. There can be a total of up to 32 traces going at one time (**all trace types**).
- You must use a privilege set of the process that includes one of the following privileges or authorities:
 - TRACE privilege
 - SYSOPR authority
 - SYSCTRL authority
 - SYSADM authority

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

DSN1SMFP – Sample Report Outputs

IFCID – 141 Audit Grant/Revoke Report

```
GRANTOR : SYSADM          REASON : SYSADM          RETURN: 0000000000
OBJECT  : STORAGE GROUP  OPTIONS: X'0400000000000000'
SQL STMT: GRANT USE OF STOGROUP DSN86810 TO PUBLIC
```

IFCID – 106 System Parameters Report

```
COMMON CRITERIA ENVIRON : NO
SYSADM ID 2              : SYSADM
ENABLE DB2 AUTHORIZATION: YES
PACK AUTH CACHE         : 0000032768
ONL SYSPARM CORID      :

MISCELLANEOUS INSTALLATION PARAMETERS
DDL REGISTRATION FLAG: X'30'
SITE TYPE             : LOCAL
CACHE DYNAMIC SQL    : NO
DBADM CREATE VIEW    : NO
ONL SYSPARM USER ID  :

INSTALL SYSADM : SYSADM
SYSOPER ID    : SYSOPR
AUTH. CACHE SIZE: 01024
EDM STMT CACHE : 0005120000
ONL SYSPARM TIME: 00:26:40

DEFAULT USERID : IBMUSER
SYSOPER ID 2   : SYSOPR
HOP SITE AUTHORIZ.: YES
ONL SYSPARM TYPE : N/A
```

OMEGAMON XE for DB2 Performance Monitor/Expert for z/OS

- Real-time monitoring
 - Threads and Statistics monitoring
 - DB2 Connect monitoring
 - Object Analysis
 - Data Sharing/Sysplex data (DB2Plex data)
- Near-term history
- Trace collection (**also as part of the PWH process support**)
- Reporting
 - Accounting, Statistics, SQL Activities, Locking, I/O Activity, Audit, Utilities, Record Trace
 - Executable as separate jobs or via PWH process engine
- Performance Warehouse with expert analysis support
- Buffer Pool Analysis, expert advice, and simulation (**only with the OMEGAMON XE for DB2 Performance Expert**)

DB2 OMEGAMON Performance Expert Audit Report Set

- Not strictly a performance report.
- Reports information about usage of auditable objects and authorization management.
 - Authorization changes
 - Authorization control (GRANTS and REVOKEs of privileges)
 - Authorization failures
 - DML statements against auditable DB2 tables at bind time
 - DDL operations against auditable DB2 tables
 - Read/write access against auditable DB2 tables
 - Utility executions against auditable DB2 tables
- Traces show individual events.
- Reports show audit information for an aggregation of DB2PE identifiers, e.g. primauth-planname-objects.

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

OMPE "File" report
commands

OMPE Audit
Detail Report

```

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
    
```

```

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                      ORDER: PRIMAUTH-PLANNAME                TO: NOT SPECIFIED
SUBSYSTEM: DSNC                 SCOPE: MEMBER                ACTUAL FROM: 09/06/06 01:47:43.60
DB2 VERSION: V8                 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'
    
```

Invoking the DB2 load utility to populate the DB2 Performance DB with Audit data.

Load Control sample statements located in RKO2SAMP

```

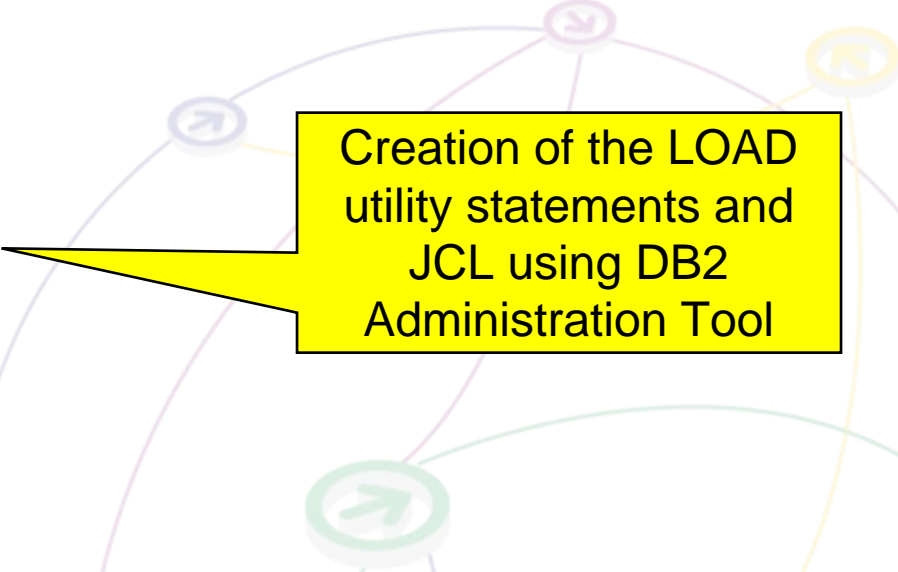
File Edit Edit Settings Menu Utilities Compilers Test Help
EDIT      SYS248.SPFTEMP2.CNTL      Columns 00001 00072
000052 LOAD INDDN SYSREC
000053 RESUME NO
000054 REPLACE
000055 INTO TABLE DB2PMFAUDT_DML
000056 WHEN (251;259) = 'DML N'
000057 (DB2PM_REL POSITION(3) SMALLINT,
000058 DB2_REL POSITION(9) CHAR(2),
000059 LOCAL_LOCATION POSITION(11) CHAR(16),
000060 GROUP_NAME POSITION(27) CHAR(8),
000061 SUBS_ID POSITION(35) CHAR(4),
000062 MEMBER_NAME POSITION(39) CHAR(8),
000063 NET_ID POSITION(47) CHAR(8),
000064 LUNAME POSITION(55) CHAR(8),
000065 INSTANCE_NBR POSITION(63) CHAR(12),
000066 LUW_SEQNO POSITION(75) SMALLINT,
000067 REQ_LOC_NAME POSITION(87) CHAR(16),
000068 ENDUSER POSITION(103) CHAR(16),
000069 WSNNAME POSITION(119) CHAR(18),
Command ==> Scroll ==> CSR_
F1=Help F2=Split F3=Exit F5=Rfind F6=Rchange F7=Up
F8=Down F9=Swap F10=Left F11=Right F12=Cancel
    
```

```

DB2 Admin ----- DSNB Specify Utility Options - LOAD ----- 08:20
Option ==>
Top of data
Execute utility on table SYS248.DB2PMFAUDT_DML
using the following options:

Utility ID ==> LOADAUD (Name identifying this utility to DB2)
Unloaded Data ==> SYS248.OMPE.AUFIL2 (Name of data set containing unloaded data)
Unloaded How? ==> U (U=Unload Utility, R=Reorg Utility)
Table/Col Info ==> CANDLET.XEGA.DEMOMVS.RKO2SAMP (DG0XLDML) (Name of data set containing table/column info)
RESUME ==> NO (Yes/No, load recs into non-empty tablespace)
SHRLEVEL ==> (None/Change, concurrent table space access)
REPLACE ==> YES (Yes/No, empty table space/index before load)
COPYDDN1 ==> (DDname identifying primary copy data set)
COPYDDN2 ==> (DDname identifying backup copy data set)
RECOVERYDDN1 ==> (DDname identifying primary ds @ recovery site)
RECOVERYDDN2 ==> (DDname identifying backup ds @ recovery site)

TABLE ALL ==> (Yes/No, info for all columns in table space)
F1=HELP F2=SPLIT F3=END F4=RETURN F5=RFIND F6=RCHANGE
F7=UP F8=DOWN F9=SWAP F10=LEFT F11=RIGHT F12=RETRIEVE
    
```



Creation of the LOAD utility statements and JCL using DB2 Administration Tool

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

Open Table - DB2PMFAUDT_DML

DSNC - DSNC - AUDITDB - SYS248 - DB2PMFAUDT_DML

E	PRIMAUTH	ORIGAUTH	TIMESTAMP	IFCID	DATABASE_DBID	PAGESET_OBID	TABLE_OBID	DATABASE_NAME	PAGESET_NAME	...
	SYS248	SYS248	Sep 6, 2006 1:47:41 AM 602771	144	307	2	5	SYS248SA	SYS248TS	...
	SYS248	SYS248	Sep 6, 2006 1:48:22 AM 560444	143	307	2	5	SYS248SA	SYS248TS	00036FBEA220
	SYS248	SYS248	Sep 6, 2006 1:48:22 AM 564498	143	307	2	5	SYS248SA	SYS248TS	00036FBEA3DA
	SYS248	SYS248	Sep 6, 2006 1:48:28 AM 130075	144	307	2	5	SYS248SA	SYS248TS	...
	SYS248	SYS248	Sep 6, 2006 1:48:58 AM 571847	143	307	2	5	SYS248SA	SYS248TS	00036FBEEA62
	SYS248	SYS248	Sep 6, 2006 1:48:58 AM 579028	143	307	2	5	SYS248SA	SYS248TS	00036FBEEAC1C
	SYS248	SYS248	Sep 6, 2006 1:49:06 AM 253828	144	307	2	5	SYS248SA	SYS248TS	...
	SYS248	SYS248	Sep 6, 2006 1:49:38 AM 826482	143	307	2	5	SYS248SA	SYS248TS	00036FBEEADD6
	SYS248	SYS248	Sep 6, 2006 1:49:38 AM 831367	143	307	2	5	SYS248SA	SYS248TS	00036FBEEB000
	SYS248	SYS248	Sep 6, 2006 1:49:38 AM 838245	143	307	2	5	SYS248SA	SYS248TS	00036FBEEB1BA

Commit Roll Back Filter Fetch More Rows

Automatically commit updates 10 row(s) in memory Close Help

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

Limitations of the audit trace

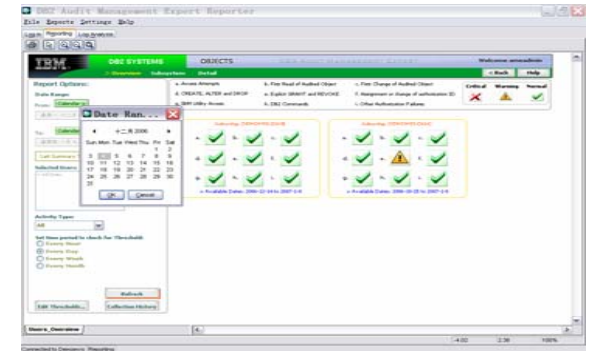
- The audit trace does not record everything, as the following list of limitations indicates:
 - The auditing that is described in this information takes place only when the audit trace is on.
 - The trace audits only the tables that you specifically choose to audit.
- The trace does NOT capture before/after change data because the DB2 log records this information.
 - If an agent or transaction accesses a table more than once in a single unit of recovery, the audit trace records only the first access.
- The audit trace does not audit some utilities. The trace audits the first access of a table with the LOAD utility, but it does not audit access by the COPY, RECOVER, and REPAIR utilities. The audit trace does not audit access by stand-alone utilities, such as DSN1CHKR and DSN1PRNT.
- You cannot audit the catalog tables because you cannot create or alter catalog tables.
- 3rd Party DB2 utilities (run outside of DB2) will not be caught with the AUDIT CLASS 8
- Dynamic SQL host variable data not collected
- This auditing coverage is consistent with the goal of providing a moderate volume of audit data with a low impact on performance. However, 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 IFASMFDM 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

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

DB2 Audit Management Expert Components

→ Audit server

- Started task or batch job
- central control point for an Audit Management Expert network
- single audit server can support data collection from multiple agents on multiple z/OS systems

→ Agent

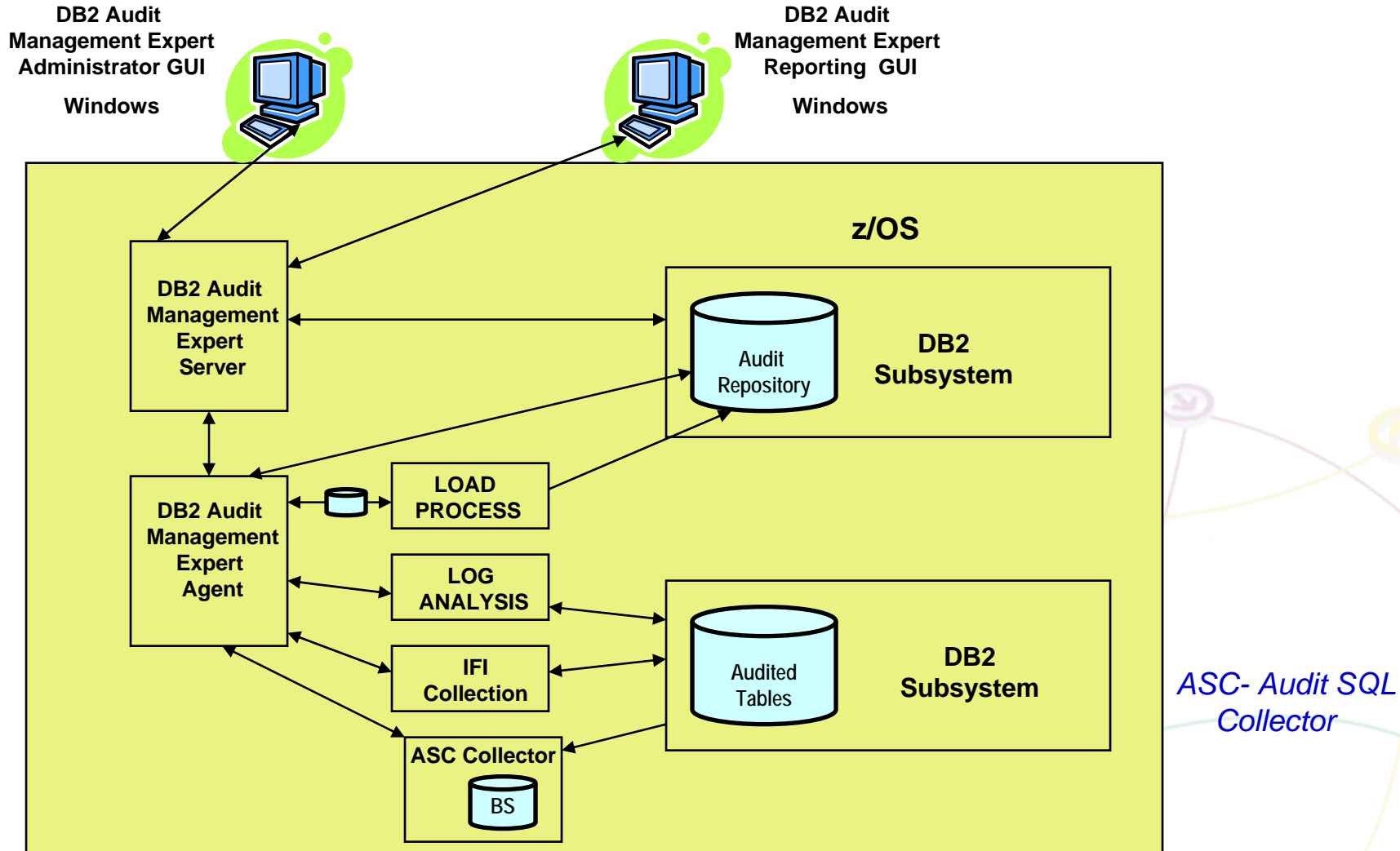
- Started Task or batch job
- responsible for communications in an Audit Management Expert environment
- acts as a "container" to run the various collectors
- One per DB2 to Audit

→ CLIENT User interfaces

- Audit Management Expert Reporter
- Audit Management Expert Administration
- Windows



DB2 Audit Management Expert Architecture



ASC- Audit SQL Collector

DB2 Audit Management Expert Profiles

→ Profiles are created/maintained via **Administration UI**

– Collection Profile

- records the details for what audit data is stored to the Audit Management Expert repository

– Agent Profile

- Select ASC collection method
- Configure General settings
 - Retention count, interval length
- DB2 Load utility parameters
- Define Job cards for load and log analysis

– User Profile

- contain information specific to an individual Audit Management Expert user such as: the user type, configurable privileges, and associated user groups

AME and Enterprise Wide Auditing - Challenges

- Existing appliance technology based on data feeds from primarily 2 sources
 - Event log from DB2 trace events written to SMF (agent)
 - Network “Sniffer” implementation (appliance)
- Restrictions and challenges with DB2 Trace versus a superior low overhead data collection approach with AME’s ASC
- Network traffic based audit feeds challenged by
 - Encrypted Data Streams
 - Local Attachments (Batch, TSO, etc.)
 - Stored Procedures
 - Performance impact to network throughput due to indiscriminate examination of all network flows
- Strong requirement to view and manage Audit events across the enterprise from a single UI

AME Extract File Enhancement via maintenance stream (PTFs UK41519, UK41521, UK41523)

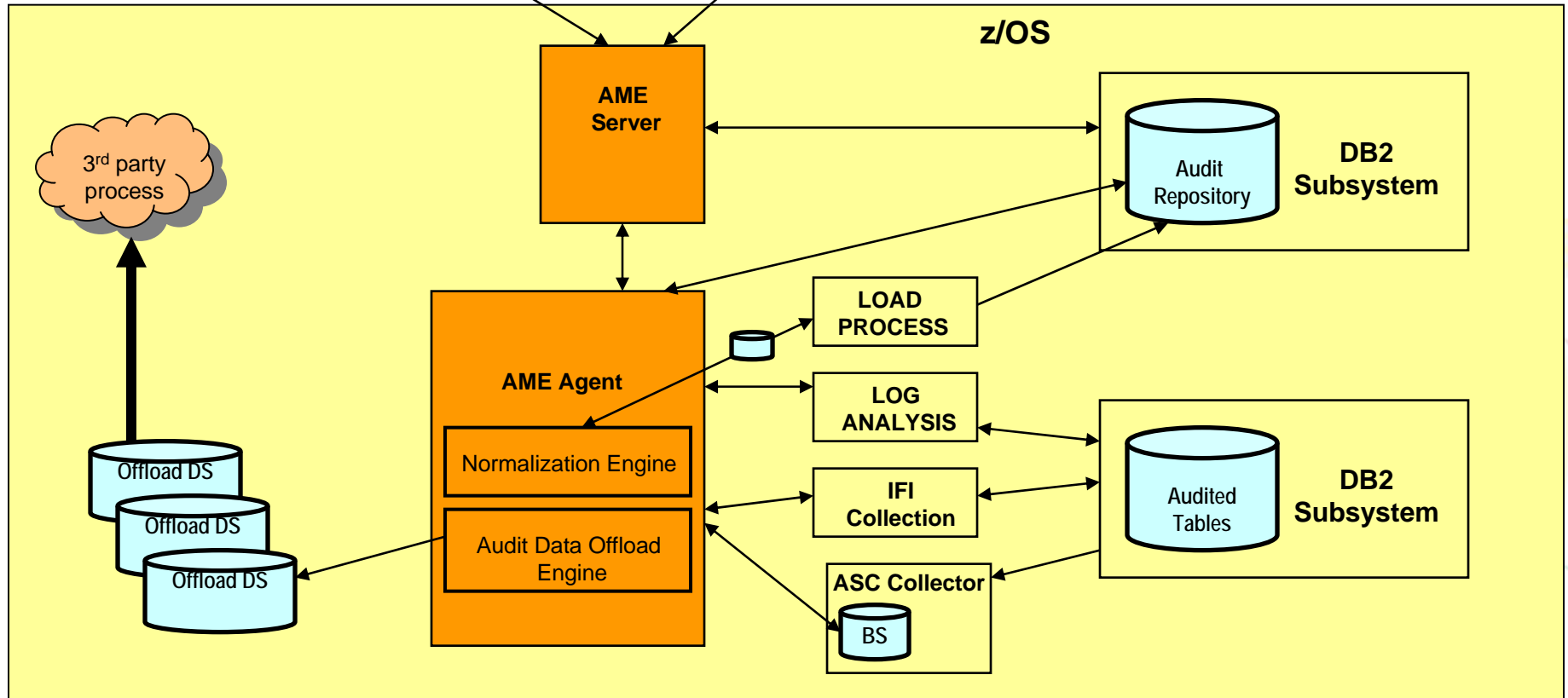
- AME will provide an option to generate audit log data sourced from either DB2 Trace or ASC (Audit SQL Collector) in an documented extract file format.
- Extract files will be standard physical sequential datasets.
- Exploiters will be responsible for transporting (via secure FTP for example) data to appliance server environment.
- Management of Extract files (archiving, deleting, etc.) will be the responsibility of exploiters
- Data will be not be aggregated (normalized), this is to reduce overhead of data collection.
- Static SQL statement collection will be optional, this is to avoid the overhead of accessing the catalog with static SQL statement number to extract SQL statement text.
- Exploiters to include
 - Tivoli Consul Insight Manager (coming Q1 2010)
 - Tizor - Mantra
 - Imperva - SecureSphere
 - Others anticipated at a future date

DB2 Audit Management Expert Architecture Dual Mode

DB2 Audit
Management Expert
Administrator GUI
Windows



DB2 Audit
Management Expert
Reporting GUI
Windows



Alerts

- Real-time alert monitoring
- Exceptions outside of expected business process
- Immediate triaging & response
- Easy integration with 3rd-party IT ecosystems: SYSLOG, SNMP, Email...

Alerts (filtered)

No.	Updated	#	Alert Description
2004	08:49:02	11	z/OS Security Po

Violations:

User	OS User	OS Host
ajcuser		

Event 6909825234996570923: Custom Rule Violation

Key	Value
Violation Description	z/OS Security Policy
Violated Item	Custom Violation

Event Details:

Event Time	Server Group	Service	Application
July 31, 2008 6:24:39 PM	DB2 Mainframe	DB2	Default DB2 Application

Connection	User	DB Application	OS User	OS Host
:0 → :0	ajcuser			

Affected Rows	Response Size	Response Time
0	0 Records	0 msec.

Error Code	Error Message

START TRACE (AUDIT)CLASS (3)RMD (*)DEST (OPX)PLAN (*)AUTHID (*)IFCID (*)BUFSIZE (16)TDAT A (CORRELATION DISTRIBUTED)

Alert 2004: z/OS Security Policy

Actions: None
Policy: z/OS Security Policy

Aggregated from 08:49:01 (0 hour(s), 2 minute(s)),

Alert aggregated by:

Distinct value for:	Value
Custom Rule	z/OS Security Policy
Server Group	DB2 Mainframe
Source IP	

Violations:

User	OS User
ajcuser	
ajcuser	
ajcuser	

Viewing the Audit Logs:

Provides all the details including: date and time , database user name and parsed query

Date/Time	Database Username	Parsed Query	Log Collector
7/21/08 3:45:57 PM	cslivi	display log	z/OS
7/21/08 3:45:58 PM	cslivi	display log	z/OS
7/21/08 3:46:01 PM	cslivi	display log	z/OS
7/21/08 3:46:02 PM	cslivi	display log	z/OS
7/31/08 5:12:09 PM	cslivi	display log	z/OS
7/21/08 3:32:55 PM	cslivi	display utility(*)	z/OS
7/21/08 3:37:41 PM	cslivi	display utility(*)	z/OS
7/21/08 3:38:14 PM	cslivi	display utility(*)	z/OS
7/21/08 3:45:57 PM	cslivi	display utility(*)	z/OS
7/21/08 3:45:58 PM	cslivi	display utility(*)	z/OS
7/21/08 3:46:01 PM	cslivi	display utility(*)	z/OS
7/21/08 3:46:02 PM	cslivi	display utility(*)	z/OS
7/31/08 5:12:09 PM	cslivi	display utility(*)	z/OS
7/31/08 5:15:51 PM	cslivi	delete from dsn8710.act where actno=?	z/OS
7/31/08 5:15:51 PM	cslivi	insert into dsn8710.act (actno,actkwd,actdesc) values(?,?,?)	z/OS
7/31/08 5:15:51 PM	cslivi	update dsn8710.act set actdesc=? where actno=?	z/OS
7/21/08 3:28:15 PM	ajcuser	start trace (audit)class (?)rmid (*)dest (opx)plan (*)authid (*)ifcid (*)bufsize (?)tdata (correlation distributed)	z/OS
7/21/08 3:42:23 PM	ajcuser	start trace (audit)class (?)rmid (*)dest (opx)plan (*)authid (*)ifcid (*)bufsize (?)tdata (correlation distributed)	z/OS
7/21/08 3:48:27 PM	ajcuser	start trace (audit)class (?)rmid (*)dest (opx)plan (*)authid (*)ifcid (*)bufsize (?)tdata (correlation distributed)	z/OS

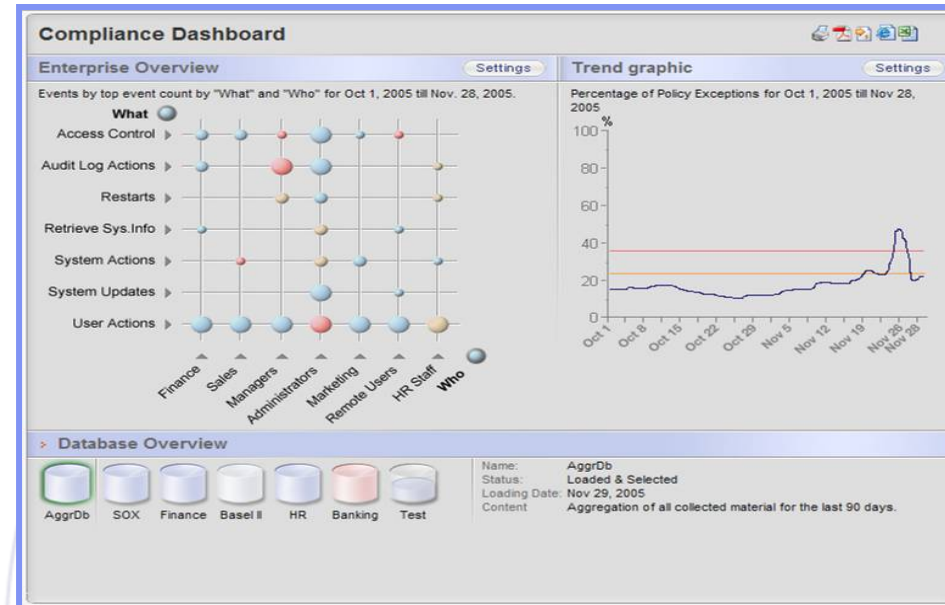
Tivoli Compliance Insight Manager

Tivoli Compliance Insight Manager provides an enterprise security compliance dashboard with in-depth privileged user **monitoring** capabilities, all powered by a comprehensive log and audit trail collection capability

Key Features

- ➔ Compliance management modules and regulation-specific reports
- ➔ Unique ability to monitor user behavior, including PUMA (Privileged User Monitoring and Audit) reporting
- ➔ Broadest, most complete log and audit trail capture capability
- ➔ W7 log normalization translates your logs into business terms
- ➔ Easy ability to compare behavior to regulatory and company policies – auditors no longer need RACF expertise to monitor activities
- ➔ Enabler event source integrates the OS and mainframe database events into TCIM's enterprise compliance dashboard

Tivoli Compliance Insight Manager



TCIM – Representative Screen

Platform History Event List on Platform Z180 (z/OS) - Database GEM on Server CIFDB - Microsoft Internet Explorer

Address: http://9.142.236.76/view/?expert=platformhistoryevents&GEMCatalog=GEM&plfdett=z%2FOS&plfdetnm=Z180&count=1573&plfdetix=3&EPRISECatalog=EPRISED&navig=Gem&navname=Gem.GemSummary&stid=1207083708203

IBM Business Transformation Homepage IBM Standard Software Installer IT Help Central Join World Community Grid Windows Marketplace

IBM Information Management Lotus Rational Tivoli WebSphere

Dashboard Trends Reports Regulations Policy Groups Distribution Settings

CIFDB > GEM > Platform History Events

Platform History Event List on Platform Z180 (z/OS)

Database GEM on Server CIFDB

Setup:

Start time: Month: June, Day: 20, Year: 2007, Hour: 8, Min: 10
 End time: Month: March, Day: 31, Year: 2008, Hour: 13, Min: 0

Execute Reset

Time zone: Event time zone

Severity	Date / Time	#	What (detail)	Where (detail)	Who (detail)	Where from (detail)	On what (detail)	Where to (detail)
10	Wed Jun 20 2007 06:10:36 GMT+00:00	1	Verify : Databasespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.DSN6S91E	Z180 (z/OS)
50	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Modify : Databasespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
50	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Modify : Databasespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP2	Z180 (z/OS)
50	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Change : Auditlog / Success	Z180 (z/OS)	System	Z180 (z/OS)	SYSTEM : Z180 / SMF	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Read : Databasespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Read : Databasespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Read : Databasespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Read : Databasespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Read : Databasespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Read : Databasespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Write : Databasespace / Success	Z180 (z/OS)	.SYSOPR	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Write : Dobject / Success	Z180 (z/OS)	.SYSOPR	Z180 (z/OS)	DBOBJECT : - / -	Z180 (z/OS)
10	Wed Jun 20 2007 06:10:28 GMT+00:00	1	Write : Databasespace / Success	Z180 (z/OS)	.CRMBFT1	Z180 (z/OS)	DBTABLESPACE : DB9G / DSN8D91A.XEMP1	Z180 (z/OS)

Regulatory Resource Center

start

10:29:50 - AT&T Ne... Vacation Planner - 2... Session B - [24 x 80] Platform History Eve... IBM Lotus Sametime ... meadowsr@us.ibm.c... 100%

5:02 PM Tuesday 4/1/2008

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

IBM

Draft Document for Review March 4, 2009 6:04 pm

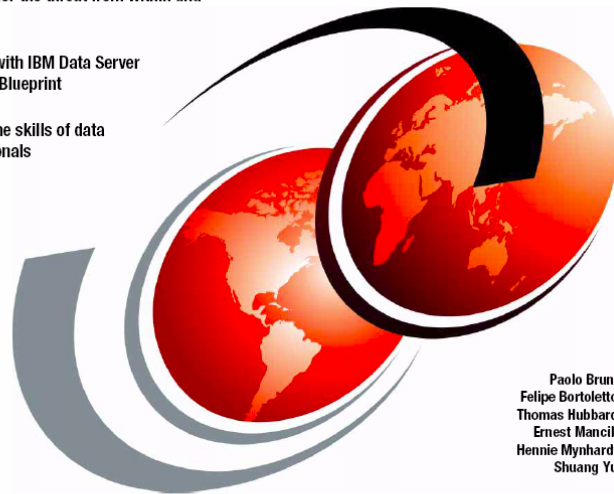
SG24-7720-00

Securing and Auditing Data on DB2 for z/OS

Prepare for the threat from within and without

Comply with IBM Data Server Security Blueprint

Extend the skills of data professionals



Paolo Bruni
Felipe Bortoletto
Thomas Hubbard
Ernest Mancill
Hennie Mynhardt
Shuang Yu

Redbooks

ibm.com/redbooks



Summary

→ Take Back Control with IBM Data Governance solutions :

- Transform your information from a Liability into your most strategic, valuable Asset
- Help manage business risk by enforcing security, audit, privacy and policy controls
- Lower operational costs by optimising data management, retention and archiving
- Increase profitability by enabling more accurate business intelligence
- Increase management's confidence in making more informed decisions based on quality and more complete data
- Increase customer satisfaction and retention through targeted advertising and up/cross selling

→ Software, Hardware and Expertise.

- Information Management - the most complete end-to-end Data Governance software solutions
- zSeries the ultimate platform to govern your enterprise data
- IBM Industry Data Models as a fast-start, best practice and help with industry compliance
- GBS - Expertise and skills from DG readiness assessments to solution implementation.

Thank YOU

Summary

→ Take Back Control with IBM Data Governance solutions :

- Transform your information from a Liability into your most strategic, valuable Asset
- Help manage business risk by enforcing security, audit, privacy and policy controls
- Lower operational costs by optimising data management, retention and archiving
- Increase profitability by enabling more accurate business intelligence
- Increase management's confidence in making more informed decisions based on quality and more complete data
- Increase customer satisfaction and retention through targeted advertising and up/cross selling

→ Software, Hardware and Expertise.

- Information Management - the most complete end-to-end Data Governance software solutions
- zSeries the ultimate platform to govern your enterprise data
- IBM Industry Data Models as a fast-start, best practice and help with industry compliance
- GBS - Expertise and skills from DG readiness assessments to solution implementation.

Thank YOU