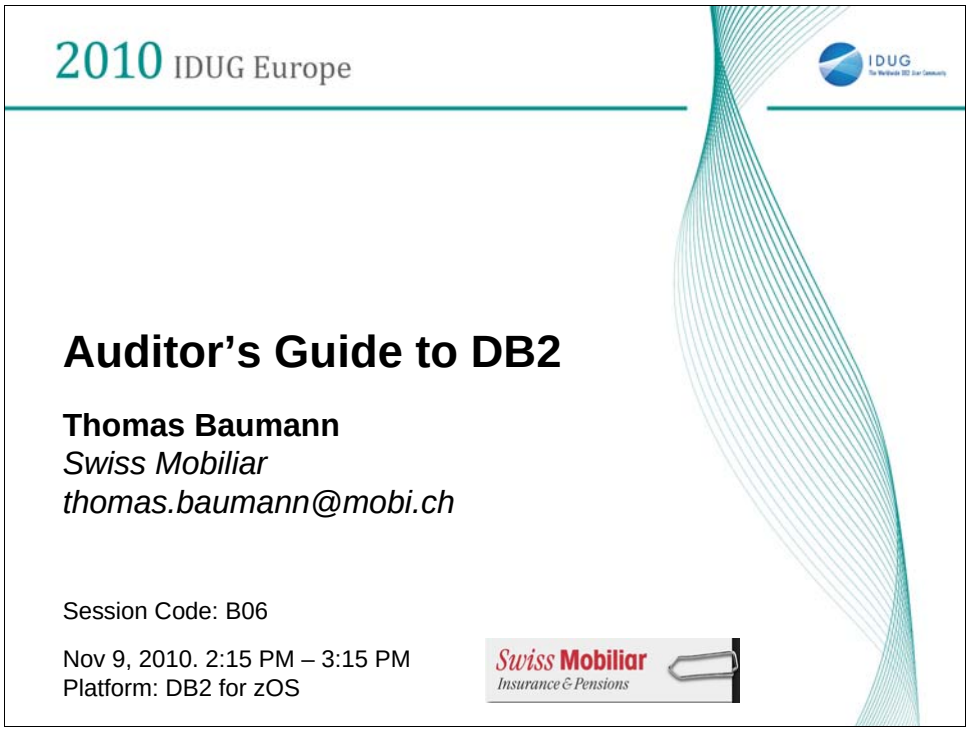


The goal of this presentation is to provide guidelines and procedures for auditors and DBAs to conduct database audits to DB2. Control practices based on risk analysis will be presented, and many test procedures will be discussed, ready to be implemented in any shop. These tests are performed by check scripts, catalog queries, log analysis, and queries to application's data; they produce valuable results to assure and enhance database availability, confidentiality, data integrity and efficiency. Some examples include estimation of recovery elapsed times, reports on unused indexes, triggered actions circumvented by utilities, anomalies detected in database structures, etc. The queries and scripts are developped and tested for DB2 z/OS, but can be adapted easily to other platforms and database management systems.

Objectives

- Differentiate DBA's and Auditor's Roles and Responsibilities
- Use presentation as guideline for
  - Risk Self Assessment if you are a DBA
  - Preparing and Performing DB audit if you are an auditor
- Become familiar with the reports and results presented
- Recognize DB2 objects from a different perspective
- NOT an Objective of this presentation:
  - All encompassing audit guideline
  - Ensuring strategical and organizational appropriateness of an organization's database department

It is not an objective to present an all encompassing guideline for all installations, and the scope of the audit approach presented focuses on operations, including but not limiting access to dats and systems. Audit objectives ensuring that IT strategies and policies are covering DB2, and ensuring that an appropriate organizational structure is in place are not covered within this presentation, and are assumed to be verified before performing an audit on the more detailed level presented in this presentation.

Agenda

- Database Risks and Vulnerabilities
  - DBA vs. Auditor Roles in Designing and Evaluating Controls
- Part I: Continuous Assessment of Risk Indicators
  - High-Level Audit Reports
- Part II:Detailed Audit Reports to Identify and Mitigate Risks
  - Confidentiality
  - Integrity
  - Availability
  - Efficiency (Performance)
- Summary

Swiss Mobiliar – Key Facts at a Glance

- Major insurer for all sectors.
- Leading property insurer.
- Leader in term insurance (private and occupational pensions).
- Reliable and expert partner.
- Mutual basis.
- Customers and employees share in our success.
- Continuity and a lasting relationship with policyholders.
- Committed to good corporate citizenship for the common good and the environment.

Disclaimer

- The Information contained in this presentation has not been submitted to any formal Swiss Mobiliar or other review and is distributed on an ‘as is‘ basis without any warranty either expressed or implied. The use of this information is the user‘s responsibility.
- The procedures, results and measurements presented in this paper were run in either the test and development environment or in the production environment at Swiss Mobiliar in Berne, Switzerland. There is no guarantee that the same or similar results will be obtained elsewhere. Users attempting to adapt these procedures and data to their own environments do so at their own risk. All procedures presented have been designed and developed for educational purposes only.

Just a standard disclaimer

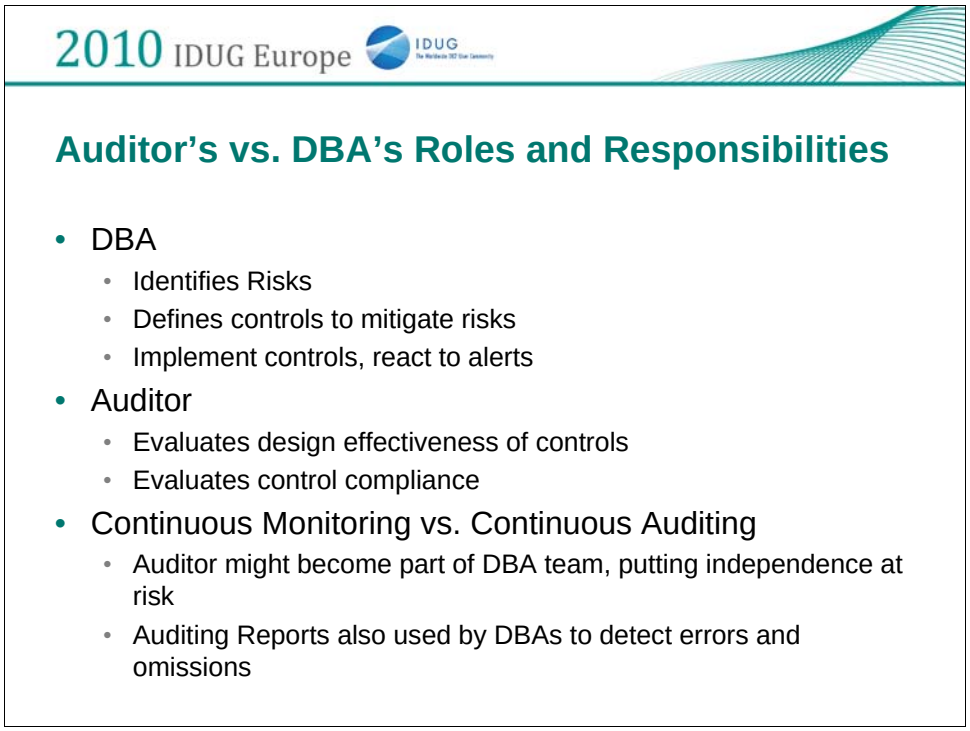
Database Risks and Vulnerabilities

- Intentional Risks
  - Often address Confidentiality only C
  - Traditional area of auditing
- Unintentional Risks
  - Integrity I
  - Availability A
  - Often neglected in database audits
- The other aspect of Risk: A Risk is also an Opportunity
  - Efficiency (Performance): What could we do more efficiently? E

Addressing Database Vulnerabilities

- Stay current on Maintenance
  - Both for intentional and unintentional threats
- Multiple Levels of Information Security
  - Regularly scan databases for vulnerabilities
    - Confidentiality, Integrity, Availability, Efficiency issues
  - Implement database activity monitoring
    - Including intrusion detection

where this presentation focuses

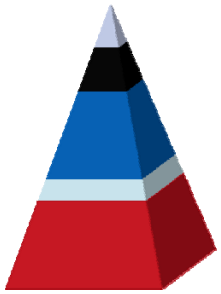


Automation of audit tasks is often involved in the practise of continuous auditing. While the employment of relevant technical auditing tools can improve the efficiency and accuracy of audit activities, the adoption of these tools embedded within respective systems has weakened the independence of the auditing function because the performance of ongoing management and application fo these tools by an auditor has undertaken a responsibility of the control function normally assigned to the database administration.

If the ongoing management of these tools is performed by the database administration, the question of the appropriateness and reliability of audit evidence arises.

Therefore, audit and database administration tasks, functions, reports and data sources must be separated.

2010 IDUG Europe



- Regulatory supervision
- External Audit
- Internal Audit
- Risk Management
- Internal Controls

Responsibilities	performed by
Evaluate Control compliance	IT Audit
Evaluate Control design effectiveness	IT Audit
Risk identification, assessment and evaluation	IT Audit/DBA
Risk response and monitoring	DBA/IT Audit
Control monitoring and maintenance	DBA
IS control design and implementation	DBA

This pyramid demonstrates the tasks and responsibilities performed by the different stakeholders in the IT control and risk environment.

Maintaining Audit Independence: High Level Reports vs. Detail Reports

- Continuous Assessment of Risk Indicators by Audit
  - High Level Reports to identify areas of risk
  - Confidentiality, Integrity, Availability, Efficiency Risk Indicators
  - Define, Compute and Evaluate Risk Indicators

- Continuous Monitoring by DBA
  - Detail Reports as part of continuous monitoring to alert to problems
  - Confidentiality, Integrity, Availability, Efficiency Key Numbers
  - Define, Compute and Monitor Key Numbers

- Incident and Problem Analysis by DBA
  - Detail Reports for problem investigation
  - Also useful for auditors when performing database audits

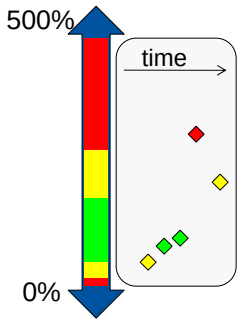
2010 IDUG Europe

Continuous Assessment of Risk Indicators: Area 1 (of 4): Confidentiality

C

- Risk indicator
  - No of direct database privileges
- Audit Objective
  - Determine if number of direct access privileges is appropriate
- Measurement (monthly)

$$100 \times \frac{\text{no of privileges granted}}{\text{total no of views}}$$



„Privileges should be granted according to roles, not directly to users“

Access privileges should be granted based on the user's roles through a security application such as RACF. However, there will always be exceptions, and privileges granted directly to DBAs, application developers, and end users. The number and types of those privileges are what we are interested in, and that is what the following query reports (naming conventions: userids of interest always begin with 'U'):

```
with temp
(GRANTEE,GRANTOR,DATUM,TCREATOR,TTNAME,UPDATE,DELETE,INSERT,AL
TER,DBADM,SYSADM) as (
Select GRANTEE , GRANTOR, DATE(GRANTEDTS),TCREATOR,TTNAME,
UPDATEAUTH,DELETEAUTH,INSERTAUTH,ALTERAUTH, ' ', ' '
from SYSIBM.SYSTABAUTH
WHERE GRANTEE LIKE 'U%'  AND GRANTEE <> GRANTOR   AND GRANTEE <>
TCREATOR  AND (UPDATEAUTH <> ' ' OR DELETEAUTH <> ' ' OR INSERTAUTH <>
' ' OR ALTERAUTH <> ' ')
UNION
Select GRANTEE, GRANTOR,DATE(GRANTEDTS),' ',NAME,' ',' ',' ',' ',DBADMAUTH,' '
from SYSIBM.SYSDBAUTH
WHERE GRANTEE LIKE 'U%'  AND GRANTEE <> GRANTOR AND NAME <> 'D'
!!GRANTEE
UNION
Select GRANTEE, GRANTOR,DATE(GRANTEDTS),' ',' ',' ',' ',' ',' ',' ',SYSADMAUTH
from SYSIBM.SYSUSERAUTH
WHERE GRANTEE LIKE 'U%'  AND SYSADMAUTH <> ' ' )
select  A.GRANTEE,  A.GRANTOR ,  A.DATUM, A.TCREATOR, A.TTNAME as Object,
A.UPDATE,A.DELETE,A.INSERT,A.ALTER,A.DBADM,A.SYSADM
from temp A order by 1,5,6
```

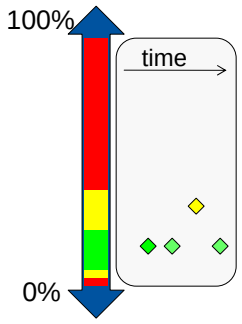
2010 IDUG Europe

Continuous Assessment of Risk Indicators: Area 2 (of 4): Integrity

I

- Risk indicator
  - No of utilities executed
- Audit Objective
  - Determine if number of executions of load / recover / reorg discard / check data utilities is appropriate
- Measurement (weekly)

$$100 \times \frac{\text{no of util executions}}{\text{no of tablespaces}}$$



„Logging and log analysis must be done for both queries and utilities“.

A very simpl query reports the ratio of (Load, Repair, Recover) utilities per tablespace:

```
select float(no_of_util) / float(no_of_tspces) from
(select count(*) as no_of_util from sysibm.syscopy
 where dbname like 'DP%'
   and ictype in ('P', 'R','S','V', 'Y','Z')
 and date(timestamp) >= current date - 7 days) a,
(select count(*) as no_of_tspces from sysibm.systablespace
 where dbname like 'DP%') b
```

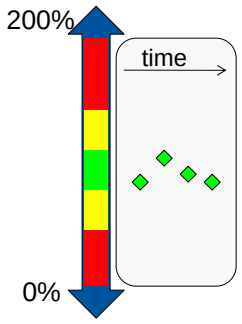
2010 IDUG Europe

Continuous Assessment of Risk Indicators: Area 3 (of 4): Availability

A

- Risk indicator
  - Elapsed time for recovery
- Audit Objective
  - Determine if estimation of elapsed time is within SLA requirements
- Measurement (daily)

$$100 \times \frac{\max(\text{tspce recovery time estimation})}{\text{SLA recovery time}}$$



„A predictable outage time is always better than an unpredictable, even if it lasts longer “

The estimation (calculation) of the recovery (or rebuild time respectively for indexes) consists of an estimation of image copy restore time, logapply time, etc. and is not a comprehensive and very accurate estimation. However, it is sufficiently accurate to provide an idea of recovery and rebuild times. As the query is too long to be reproduced here, please feel free to send me a mail and ask for the complete query (see mail address at last page).

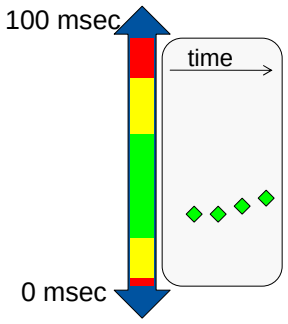
2010 IDUG Europe

Continuous Assessment of Risk Indicators: Area 4 (of 4): Efficiency (Performance)

E

- Risk indicator
  - Query CPU usage
- Audit Objective
  - Determine if ratio of *CPU usage per query execution* is within predefined limits and decreasing over time
- Measurement (daily) *)

$$\frac{\text{sum of CPU µsec used}}{\text{total no of queries}}$$



*) measured @Mobiliar by BMC Apptune 6.2.00

„Eventually, applications are always judged by their response times "

These numbers should be provided by your favourite performance monitoring tool. It is a suprisingly constant value, and therefore a good indicator of middle- and long-term increases or decreases in query performance.

2010 IDUG Europe

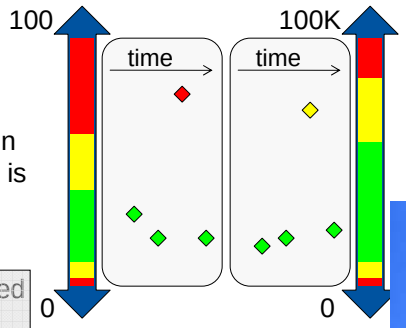
Continuous Assessment of Risk Indicators: Area 5 (of 4!): DSNMSTR inspection

C I A E

- Risk indicator
  - Severe error messages
- Audit Objective
  - Determine if number of selected message types in DSNMSTR adress space is appropriate
- Measurement (daily)

no of messages of selected types,

no of total rows written to DSNMSTR



At Swiss Mobiliar, we daily scan the DSNMSTR address space's output in order to

Count and report number of timeouts

Count and report number of deadlocks

Count and report number of specific RC00XXXXXX reason codes

E20003 (memory constraints)

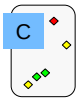
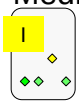
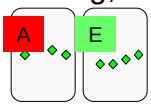
E20016 (memory constraints)

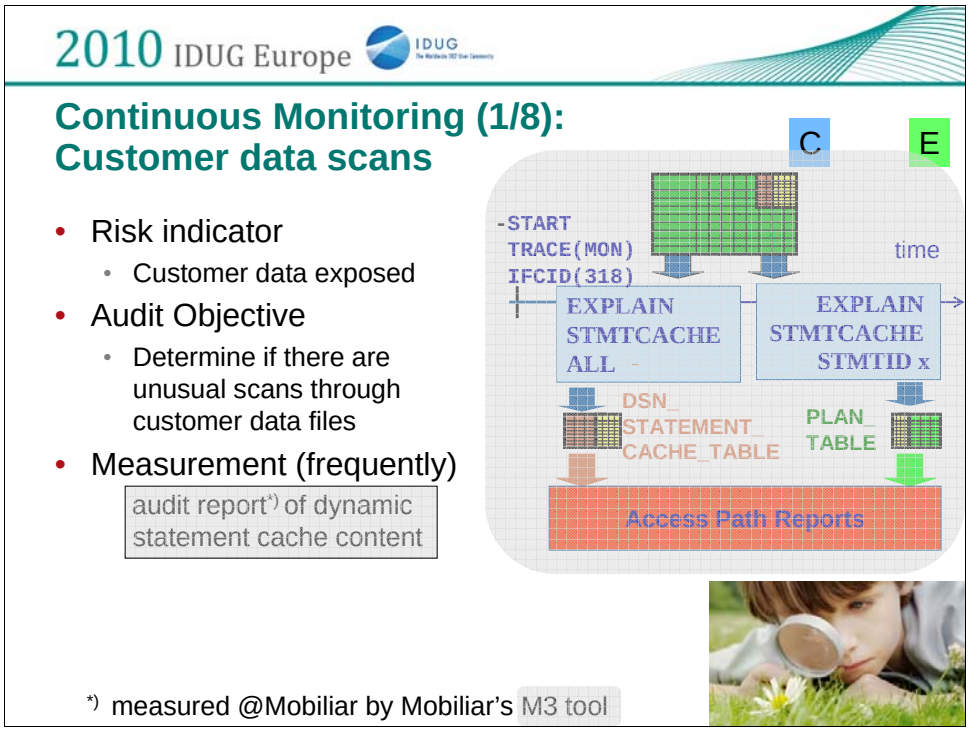
C90101 / C90102 (data inconsistencies)

Some of those values directly trigger alarms, others are considered for reporting uses only. From an auditor's perspective, error messages such as memory constraints or data inconsistencies should be tracked to their corresponding incident, problem, and eventually change requests.

Evaluation of Risk Indicators

Controls are considered

Weak, if 	value is red once within time period, or value is yellow in two or more consecutive weeks
Medium, if 	value is sometimes yellow, but only in single weeks
Strong, if 	value is always in green zone



Swiss Mobiliar's dynamic query performance monitoring tool "M3" was introduced at the 2008 North American IDUG conference (session title "Memory Management for Dynamic SQL" and further detailed at an IDUG one-day educational seminar ("Dynamic SQL Performance Diagnosis Class for DB2 z/OS") also in 2008.

The tool is available at no cost by sending me a mail, a workshop might be organized upon request.

The M3 tool guides the user through a comprehensive tuning methodology for evaluating the performance of a database. Key performance metrics are measured, and the users are given a comprehensive analysis of their dynamic SQL workload and a number of tuning ideas. 25+ reports offer a wide range of insight into dynamic query performance.

In order to detect scans through customer data, an additional report has been incorporated into the M3 tool described above.

PROGRAM_NAME	CURSQLID	TOTAL_ELAP	NO_OF_EXEC	SAMPLE_QUERY	APID
SYSSH200	$SAPISA	0.001676	10	SELECT benID FROM Benutzer WHERE benVorges..	0DB2PRODTPISBENR0NS
SYSSH200	$SAPISA	0.010007	7	SELECT benID, benTS, benNTID, benKurzzeichen, ..	0DB2PRODTPISBENR0NS30N
SYSLN300	CORTTOOL	0.039251	2	SELECT VISDBET1.C97278 as "code", VISDBET1...	0DB2PRODTINFBERR0NS30N
SYSLN300	CORTTOOL	0.463340	6	SELECT VPD07521.C95836_0 as "roleFromTo", VP..	0DB2PRODXPD07522I0YS1DB2
DSQLDB2	DB2PCOPY	0.043061	3	SELECT C97251, C54260, C54261, CHAR(C54262,I..	0DB2PRODTPARAUSR0NS
DSQLDB2	DB2PCOPY	0.024253	2	SELECT C99992, C97251, C99995, C97386, C9738..	0DB2PRODTPA9940R0NS
DSQLDB2	DB2PCOPY	0.020960	1	SELECT C95826, C95820, C94235, C94236, C9423..	0DB2PRODTPA9015R0NS
DSQLDB2	DB2PCOPY	0.000082	1	SELECT C95836_0, C95836_1, C95862_1, C97251..	0DB2PRODTOBPARR0NS
DSQLDB2	DB2PCOPY	0.015143	1	SELECT C95836, C95862, C99992, C99995, C9585..	0DB2PRODTEO_TPA0028R0NS
DSQLDB2	DB2PCOPY	0.079553	1	SELECT C95836, C95862, C94206, C94207, C9420..	0DB2PRODTEO_TPA9039R0NS
SYSLN300	EDOCTOOL	0.043223	4	SELECT VORPRGA2.C97132 as "code", VORPAR..	0DB2PRODTORPRGAR0NS4DE
SYSLN300	ORPTOOL	3.082992	7	SELECT DISTINCT CASE WHEN DB2PVIEW.VOR..	0DB2PRODTORPREPR0NS1DE
SYSLN300	ORPTOOL	0.081644	1	SELECT DISTINCT CASE WHEN DB2PVIEW.VOR..	0DB2PRODTORPREPR0NS1DE
SYSLN300	ORPTOOL	1.541790	4	SELECT DISTINCT CASE WHEN DB2PVIEW.VOR..	0DB2PRODTORPREPR0NS1DE
QPACBDB2	U100997	524.375549	1	SELECT C97227, C97229, C97147, C97148, C972..	0DB2PRODTGESGADR0NS30N
DSNUGSQL	U109746	1.616142	15	SELECT * FROM DB2P.DB2PVIEW.VEM00651 WH..	0DB2PRODXEM00651I0YS
DSNUGSQL	U109746	2.831516	15	SELECT * FROM DB2P.DB2PVIEW.VPA00652 WH..	0DB2PRODTPA0065R0NS

Example of a table scan by user U100997

2010 IDUG Europe

Continuous Monitoring (2/8): Detecting database commands

C I

- Risk indicator
  - Database integrity at risk due to –STA ACCESS(FORCE) commands
- Audit Objective
  - Determine if there are undocumented –STA DB(…) SP (…) ACCESS(FORCE) commands
- Measurement (frequently)
  - log analysis reports*)

*) measured @Mobiliar by DSN1LOGP

DSN1LOGP:
LRSNSTART(C57ABDE3B9A0)
LRSNEND(C57ABF01D3D0)
TYPE(10)

(SUBTYPE(82) report –sta access force commands, but without user details)

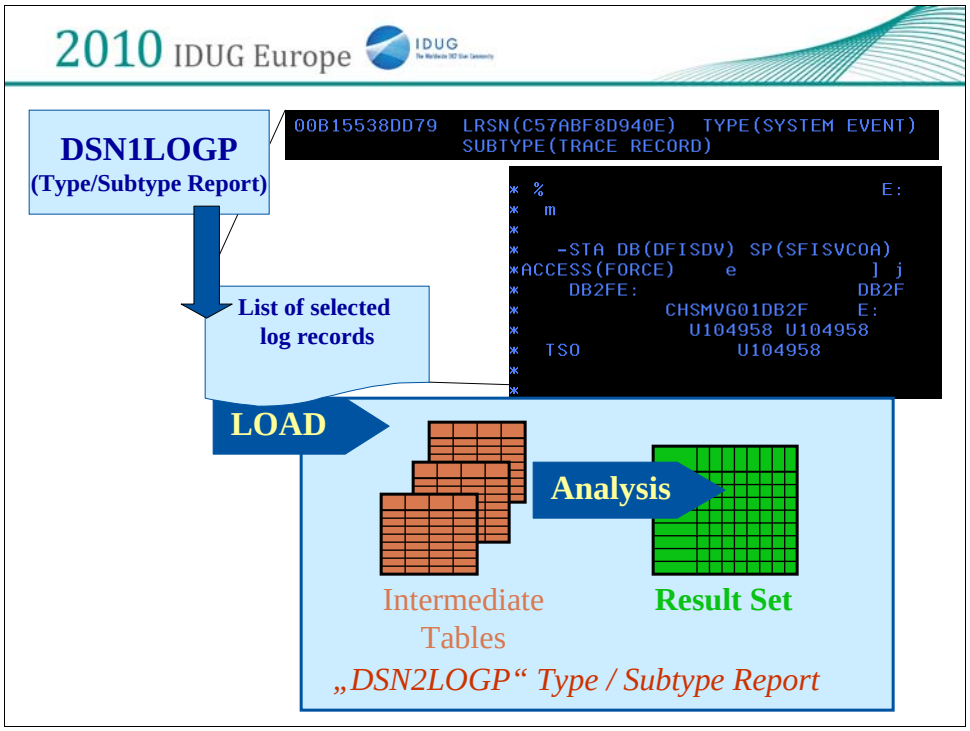
Please note that the LRSN-values can be used for DSN1LOGP, regardless of having DB2 data sharing enabled or not. Since the LRSN values are derived from the system clock value, they are much simpler to handle than RBA values.

```
//LOGP     EXEC PGM=DSN1LOGP
//GROUP    DD DSN=DB2S.DB2S.BSDS01,DISP=SHR
//SYSIN    DD *
 LRSNSTART(BAF7FB000000) LRSNEND(BAF7FCD117D0)
 TYPE(10)
```

An example of a LRSN → timestamp translation is the following simple query (translation of LRSN BAF7FCD117D0):

```
SELECT TIMESTAMP(X'BAF7FCD117D0'!!X'0000')
     + CURRENT TIMEZONE
FROM SYSIBM.SYSDUMMY1 ;

+----------------------------+
!                            !
+----------------------------+
! 2004-03-25-08.23.00.000000 !
+----------------------------+
```



A very useful source of information about DSN1LOGP is Ken McDonald‘s presentation (given at IGUD Europe 2006) ‚DSN1LOGP – It Could Save Your Job One Day‘. Therein, a brief discussion concerning the contents and information held within the DB2 log, details of the syntax and usage of DSN1LOGP are to be found, followed by examples of how to interpret DSN1LOGP output for auditing and recovery purposes.

At Swiss Mobiliar, we use the output of DSN1LOGP as input to some log-postprocessing which populates some intermediate tables, does some more analysis and inserts the calculations in an eventual result table. We called this process „DSN2LOGP“ .

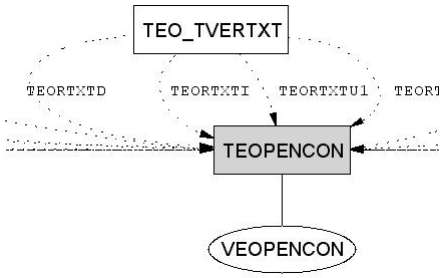
2010 IDUG Europe

Continuous Monitoring (3/8): Trigger-Rules overwritten by utilities

C I

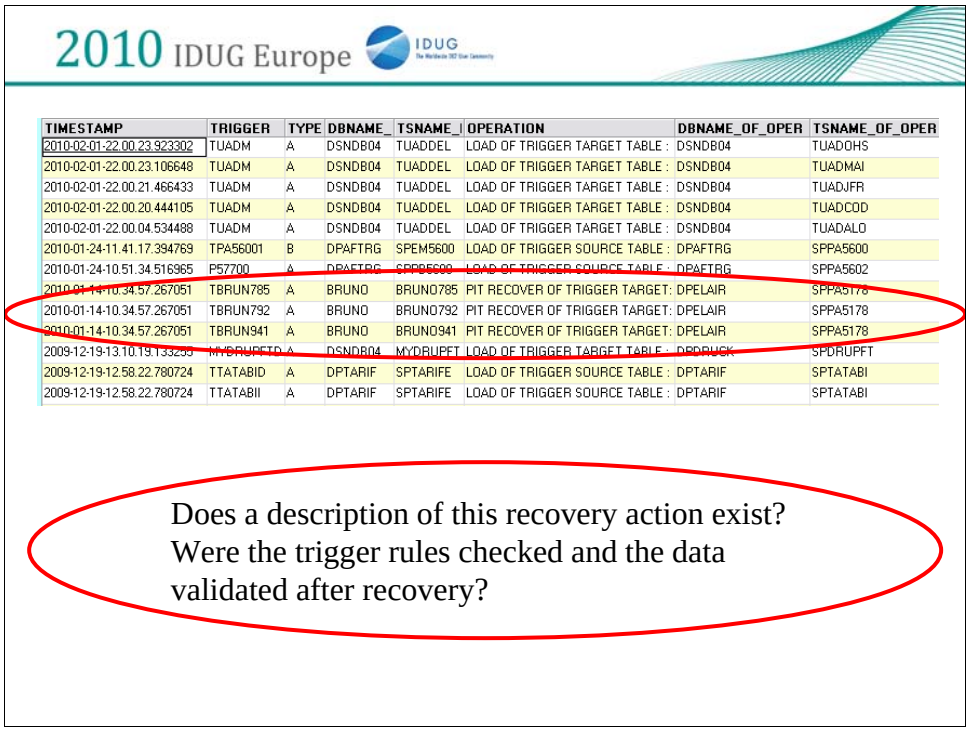
- Risk indicator
  - Trigger-based integrity constraints violated
- Audit Objective
  - Determine if there are utilities which could have invalidated trigger based constraints
- Measurement (daily)

  catalog query



The following sequence of statements reports utilities which might violate trigger-based constraints (continued on next pages):

```
DECLARE GLOBAL TEMPORARY TABLE SESSION.TRIGGER_FROM
( TRIGGER_SCHEMA CHAR(8)
 ,TRIGGER_NAME   CHAR(28)
 ,TRIGTIME       CHAR(1)
 ,DBNAME_FROM    CHAR(8), TSNAME_FROM CHAR(8)
 ) ON COMMIT PRESERVE ROWS;
COMMIT;
DECLARE GLOBAL TEMPORARY TABLE SESSION.TRIGGER_TO
( TRIGGER_SCHEMA CHAR(8)
 ,TRIGGER_NAME   CHAR(28)
 ,TRIGTIME       CHAR(1)
 ,DBNAME_TO      CHAR(8), TSNAME_TO   CHAR(8)
 ) ON COMMIT PRESERVE ROWS;
COMMIT;
INSERT INTO SESSION.TRIGGER_FROM
(TRIGGER_SCHEMA, TRIGGER_NAME, TRIGTIME, DBNAME_FROM,
TSNAME_FROM)
SELECT TR.SCHEMA, TR.NAME, TR.TRIGTIME, TAB.DBNAME, TAB.TSNAME
FROM SYSIBM.SYSTRIGGERS TR JOIN SYSIBM.SYSTABLES TAB
  ON TR.TBOWNER = TAB.CREATOR AND TR.TBNAME=TAB.NAME ;
COMMIT;
```




```
INSERT INTO SESSION.TRIGGER_TO
(TRIGGER_SCHEMA, TRIGGER_NAME, TRIGTIME, DBNAME_TO, TSNAME_TO)
SELECT TR.SCHEMA, TR.NAME, TR.TRIGTIME, BQUALIFIER, BNAME
FROM SYSIBM.SYSTRIGGERS TR JOIN SYSIBM.SYSPACKAGE P
ON TR.SCHEMA = P.COLLID AND TR.NAME=P.NAME
JOIN SYSIBM.SYSPACKDEP D ON P.NAME=D.DNAME AND P.COLLID=D.DCOLLID
WHERE D.BTYPE='R' ;
COMMIT;
SELECT DISTINCT C.TIMESTAMP,
            F.TRIGGER_NAME AS TRIGGER,
            F.TRIGTIME AS  TYPE,
            T.DBNAME_TO AS DBNAME_PEND,
            T.TSNAME_TO AS TSNAME_PEND,
            'PIT RECOVER OF TRIGGER SOURCE:' AS OPERATION,
            F.DBNAME_FROM AS DBNAME_OF_OPER,
            F.TSNAME_FROM AS TSNAME_OF_OPER
FROM SYSIBM.SYSCOPY C,
    SESSION.TRIGGER_FROM F, SESSION.TRIGGER_TO T
 WHERE C.ICTYPE='P'
  AND C.DBNAME=F.DBNAME_FROM
  AND C.TSNAME=F.TSNAME_FROM
  AND F.TRIGGER_SCHEMA=T.TRIGGER_SCHEMA
  AND F.TRIGGER_NAME  =T.TRIGGER_NAME
  AND C.TIMESTAMP = (SELECT MAX(C2.TIMESTAMP) FROM SYSIBM.SYSCOPY C2
                WHERE C2.ICTYPE IN ('R','S','Y','Z','P')
                  AND C.DBNAME=C2.DBNAME
 AND C.TSNAME=C2.TSNAME)
  AND NOT EXISTS (SELECT 1 FROM SYSIBM.SYSCOPY C3
                WHERE C3.ICTYPE='P'
                  AND C3.DBNAME=T.DBNAME_TO
                  AND C3.TSNAME=T.TSNAME_TO
                  AND C.PIT_RBA = C3.PIT_RBA)
UNION
```

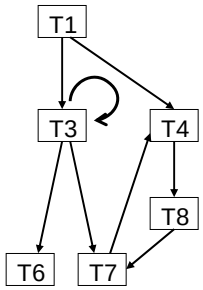
2010 IDUG Europe

Continuous Monitoring (4/8): Cyclic Referential Integrity Definitions

I

- Risk indicator
  - Data inconsistencies
- Audit Objective
  - Determine if there are circles in referential-integrity-structure definitions
- Measurement (monthly)
  - catalog query

SYSIBM.SYSRELS

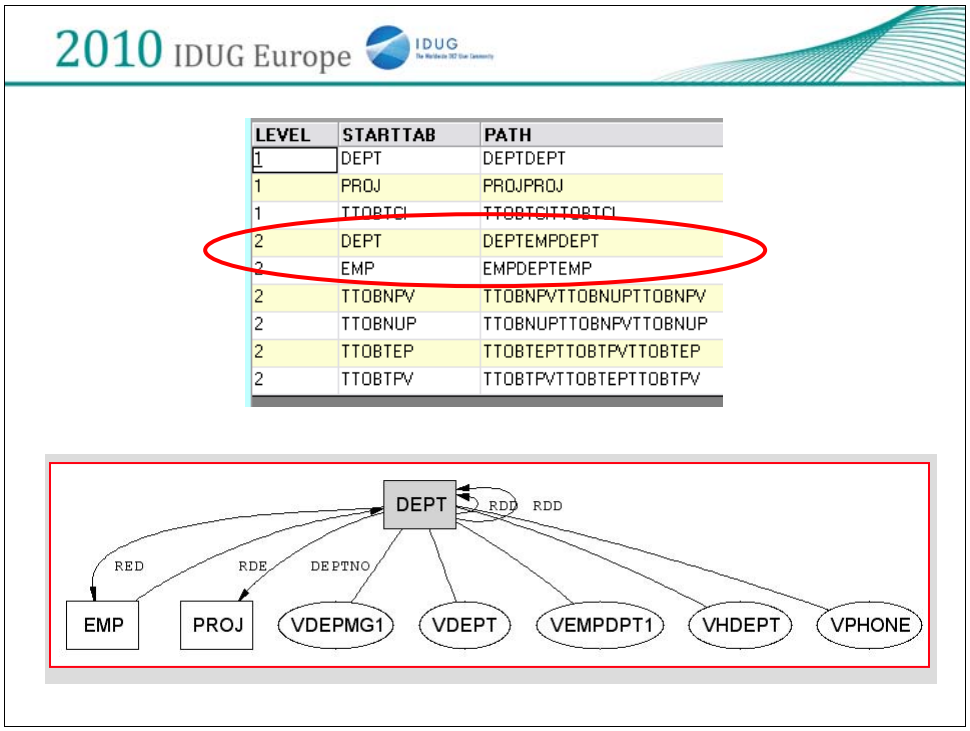


Cycles:
T3→T3
T4→T8→T7→T4
(and T8→T7→T4→T8 etc.)

See query details on notes page 26

(…) continued form last page:

```
SELECT DISTINCT C.TIMESTAMP,
            F.TRIGGER_NAME AS TRIGGER,
            F.TRIGTIME AS  TYPE,
            F.DBNAME_FROM AS DBNAME_PEND,
            F.TSNAME_FROM AS TSNAME_PEND,
            'PIT RECOVER OF TRIGGER TARGET:' AS OPERATION,
            T.DBNAME_TO AS DBNAME_OF_OPER,
            T.TSNAME_TO AS TSNAME_OF_OPER
FROM SYSIBM.SYSCOPY C,
    SESSION.TRIGGER_TO T, SESSION.TRIGGER_FROM F
 WHERE C.ICTYPE='P'
  AND C.DBNAME=T.DBNAME_TO
  AND C.TSNAME=T.TSNAME_TO
  AND F.TRIGGER_SCHEMA=T.TRIGGER_SCHEMA
  AND F.TRIGGER_NAME  =T.TRIGGER_NAME
  AND C.TIMESTAMP = (SELECT MAX(C2.TIMESTAMP) FROM SYSIBM.SYSCOPY C2
                WHERE C2.ICTYPE IN ('R','S','Y','Z','P')
                  AND C.DBNAME=C2.DBNAME
                  AND C.TSNAME=C2.TSNAME)
  AND NOT EXISTS (SELECT 1 FROM SYSIBM.SYSCOPY C3
                WHERE C3.ICTYPE='P'
                  AND C3.DBNAME=F.DBNAME_FROM
                  AND C3.TSNAME=F.TSNAME_FROM
                  AND C.PIT_RBA = C3.PIT_RBA)
UNION
```




```
SELECT DISTINCT C.TIMESTAMP,
            F.TRIGGER_NAME AS TRIGGER,
            F.TRIGTIME AS  TYPE,
            T.DBNAME_TO AS DBNAME,
            T.TSNAME_TO AS TSNAME,
            'LOAD OF TRIGGER SOURCE TABLE :' AS OPERATION,
            F.DBNAME_FROM AS DBNAME_OF_OPER,
            F.TSNAME_FROM AS TSNAME_OF_OPER
FROM SYSIBM.SYSCOPY C,
    SESSION.TRIGGER_FROM F, SESSION.TRIGGER_TO T
 WHERE C.ICTYPE IN ('R','S','Y','Z')
  AND C.DBNAME=F.DBNAME_FROM
  AND C.TSNAME=F.TSNAME_FROM
  AND F.TRIGGER_SCHEMA=T.TRIGGER_SCHEMA
  AND F.TRIGGER_NAME  =T.TRIGGER_NAME
  AND C.TIMESTAMP = (SELECT MAX(C2.TIMESTAMP) FROM SYSIBM.SYSCOPY C2
                WHERE C2.ICTYPE IN ('R','S','Y','Z','P')
                  AND C.DBNAME=C2.DBNAME
                  AND C.TSNAME=C2.TSNAME)
  AND NOT EXISTS (SELECT 1 FROM SYSIBM.SYSCOPY C3
                WHERE C3.ICTYPE IN ('R','S','Y','Z')
                  AND C3.DBNAME=T.DBNAME_TO
                  AND C3.TSNAME=T.TSNAME_TO
                  AND DAY(C.TIMESTAMP) = DAY(C3.TIMESTAMP))
UNION
```

2010 IDUG Europe

Continuous Monitoring (5/8): Tablespace/Index Recreation Time

A

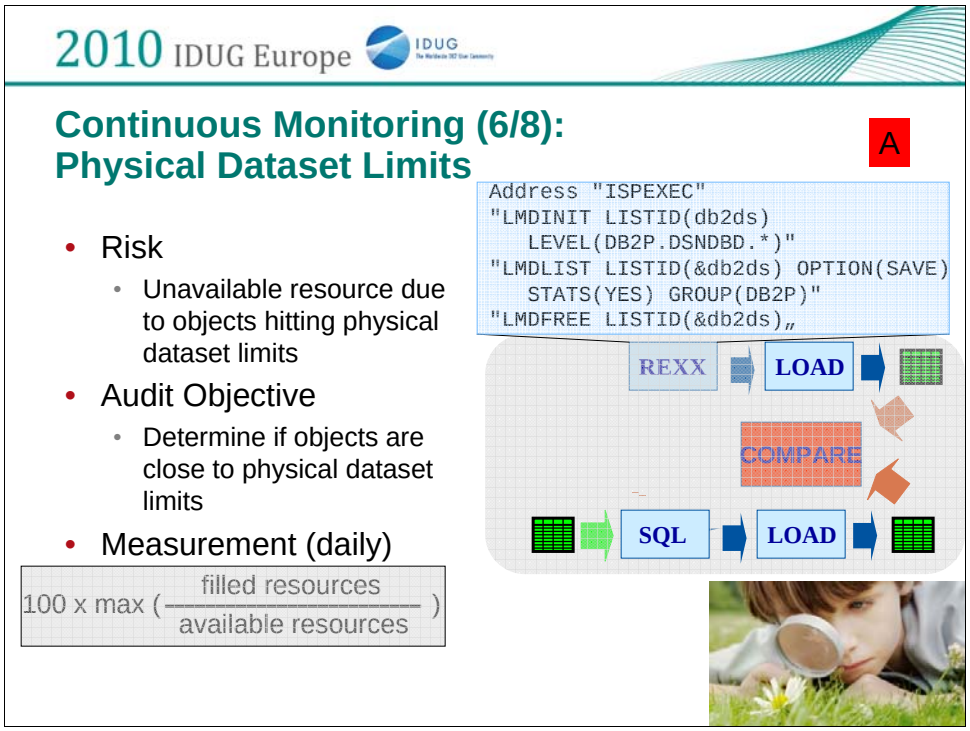
- Risk indicator
  - High outage time
- Audit Objective
  - Determine if estimation of elapsed time is within SLA requirements
- Measurement (twice per day)

  catalog query to estimate recovery time for all tablespaces, and rebuild/recover time for all indexes

```
SELECT DISTINCT C.TIMESTAMP,
            F.TRIGGER_NAME AS TRIGGER,
            F.TRIGTIME AS  TYPE,
            F.DBNAME_FROM AS DBNAME_PEND,
            F.TSNAME_FROM AS TSNAME_PEND,
            'LOAD OF TRIGGER TARGET TABLE :' AS OPERATION,
            T.DBNAME_TO AS DBNAME_OF_OPER,
            T.TSNAME_TO AS TSNAME_OF_OPER
FROM SYSIBM.SYSCOPY C,
    SESSION.TRIGGER_TO T, SESSION.TRIGGER_FROM F
 WHERE C.ICTYPE IN ('R','S','Y','Z')
  AND C.DBNAME=T.DBNAME_TO
  AND C.TSNAME=T.TSNAME_TO
  AND F.TRIGGER_SCHEMA=T.TRIGGER_SCHEMA
  AND F.TRIGGER_NAME  =T.TRIGGER_NAME
  AND C.TIMESTAMP = (SELECT MAX(C2.TIMESTAMP) FROM SYSIBM.SYSCOPY C2
                  WHERE C2.ICTYPE IN ('R','S','Y','Z','P')
                    AND C.DBNAME=C2.DBNAME
                    AND C.TSNAME=C2.TSNAME)
  AND NOT EXISTS (SELECT 1 FROM SYSIBM.SYSCOPY C3
                  WHERE C3.ICTYPE IN ('R','S','Y','Z')
                    AND C3.DBNAME=F.DBNAME_FROM
                    AND C3.TSNAME=F.TSNAME_FROM
                    AND DAY(C.TIMESTAMP) = DAY(C3.TIMESTAMP))
order by timestamp desc;
```

The following query reports cyclic referential integrity definitions, as presented in slides on pages 21 and 22:

```
WITH PUMP (LEVEL, STARTTAB, ENDTAB, PATH) AS
(SELECT 1, REFTBNAME, TBNAME ,
STRIP(REFTBNAME)!!STRIP(TBNAME)
 FROM SYSIBM.SYSRELS
UNION ALL
 SELECT PUMP.LEVEL+1, PUMP.STARTTAB, CHILD.TBNAME,
PUMP.PATH!!CHILD.TBNAME
 FROM PUMP, SYSIBM.SYSRELS CHILD
 WHERE PUMP.ENDTAB = CHILD.REFTBNAME
   AND CHILD.TBNAME  <> CHILD.REFTBNAME
   AND PUMP.STARTTAB <> PUMP.ENDTAB
   AND PUMP.LEVEL < 30)
SELECT DISTINCT LEVEL, STARTTAB, PATH
FROM PUMP
WHERE STARTTAB=ENDTAB
```



Limits include but are not limited to tablespace partition limits:

```
SELECT DBNAME, NAME,
CASE
  WHEN TYPE = 'P' AND DSSIZE > 0 THEN 41943040
  WHEN DSSIZE      > 0 THEN DSSIZE
  WHEN PARTITIONS BETWEEN  1 AND 16 THEN 4194304
  WHEN PARTITIONS BETWEEN 17 AND 32 THEN 2097152
  WHEN PARTITIONS BETWEEN 33 AND 64 THEN 1048576
  WHEN PARTITIONS >       64        THEN 4194304
END AS MAX_PART_SIZE,
CASE
  WHEN DSSIZE      >= 4194304 AND PARTITIONS  > 254 THEN 4096
  WHEN DSSIZE      >= 4194304 AND PARTITIONS <= 254 THEN  254
  WHEN DSSIZE       =       0 AND PARTITIONS  >  64 THEN  254
  ELSE                                       32
END AS MAX_NPI_DATASETS
FROM SYSIBM.SYSTABLESPACE
WHERE PARTITIONS > 0  ;
```

Other limits considered are index partition limits, limited number of pieces for PIECESIZEd inexes, and number of extents for individual pagesets.

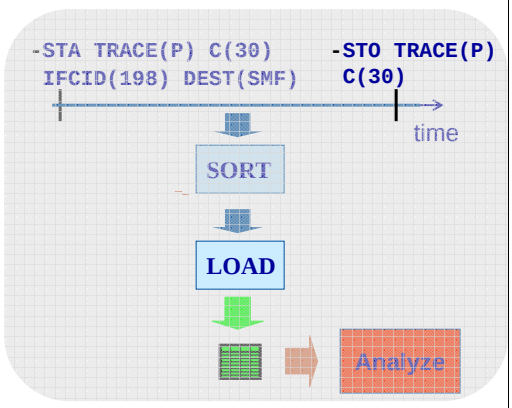
2010 IDUG Europe

Continuous Monitoring (7/8): Pageset I/O Activity

E

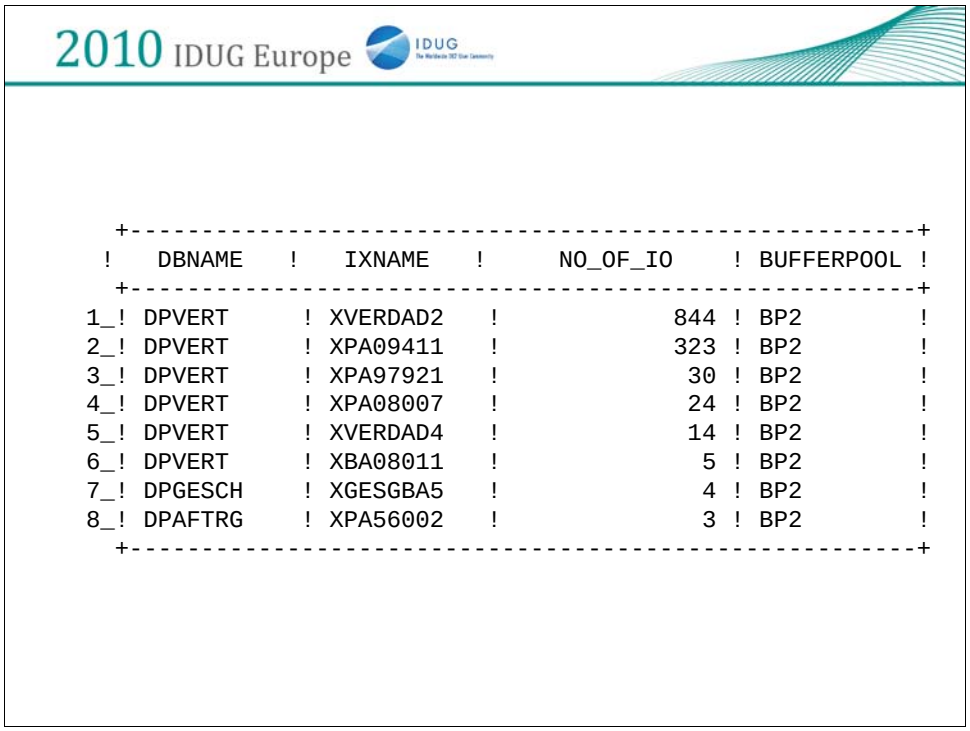
- Risk
  - Long or increasing query response times due to intensive I/O processing
- Audit Objective
  - Determine if I/O activity per pageset and/or application is increasing
- Measurement (daily)

IFCID(198) pfm trace analysis



SORT JCL (for Subsystem "DB2P"):

```
//SORTSMF  EXEC PGM=SORT
//SORTIN   DD DSN=MBS00.SMFDATA.V001.GV(0),DISP=SHR
//*-------------------------------------------------------------
//*   FOR A NEW DS
//*SORTOUT  DD DSN=MV020.BPASMF.DB2P.DATAV,
//*          DISP=(NEW,CATLG,DELETE),
//*          UNIT=SYSDA,SPACE=(CYL,(30,50),RLSE),
//*          LRECL=8188,BLKSIZE=8192,RECFM=VB,DSORG=PS
//*-------------------------------------------------------------
//SORTOUT  DD DSN=MV020.BPASMF.DB2P.DATAV,DISP=SHR
//SORTWK01 DD SPACE=(CYL,(9,10)),UNIT=SYSDA
//SYSPRINT DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//SYSIN    DD *
  SORT FIELDS=(45,2,BI,A,47,2,BI,A)
  INCLUDE
COND=(19,4,CH,EQ,C'DB2P',AND,06,1,CH,EQ,X'66',AND,74,1,CH,EQ,*
  X'C6')
  OPTION VLSHRT
/*
```



	DBNAME	IXNAME	NO_OF_IO	BUFFERPOOL
1_	DPVERT	XVERDAD2	844	BP2
2_	DPVERT	XPA09411	323	BP2
3_	DPVERT	XPA97921	30	BP2
4_	DPVERT	XPA08007	24	BP2
5_	DPVERT	XVERDAD4	14	BP2
6_	DPVERT	XBA08011	5	BP2
7_	DPGESCH	XGESGBA5	4	BP2
8_	DPAFTRG	XPA56002	3	BP2

LOAD control card:

```
LOAD DATA REPLACE
 INDDN SYSREC00
INTO TABLE DB2PROD.TPBPASMF
 (  QW0198BP  POSITION(00045:00045) CHAR
 ,  "DBID "   POSITION(00041:00042) SMALLINT
 ,  "OBID "   POSITION(00043:00044) SMALLINT
 ,  QW0198FC  POSITION(00046:00046) CHAR
 ,  QW0198PS  POSITION(00047:00047) CHAR
 ,  QW0198AT  POSITION(00048:00048) CHAR
 ,  QW0198PN  POSITION(00049:00052) CHAR
 ,  QW0198PR  POSITION(00057:00057) CHAR
 ,  USERID    POSITION(00151:00158) CHAR
 ,  PLANNAME  POSITION(00179:00186) CHAR )
```

2010 IDUG Europe

Continuous Monitoring (8/8): Query/Job progress information

A E

- Risk
  - Currently active queries/jobs run longer than expected
- Audit Objective
  - Determine if there exist exact predictions for query/job processing
- Measurement (ad hoc)

$$100 \times \frac{\text{predicted / estimated remaining run time}}{\text{measured remaining run time}}$$

Analyze Index Pageset actitiy report for report 7 (part 1 of 2):

```
DECLARE GLOBAL TEMPORARY TABLE OBJECTIOS
(DBID INTEGER, OBID INTEGER, ANZ_IO INTEGER, BP CHAR(06)) ;
INSERT INTO SESSION.OBJECTIOS
SELECT  A.DBID, A.OBID, COUNT(*) AS ANZ_IO,
  CASE   WHEN A.QW0198BP =    X'00' THEN 'BP0'
       WHEN A.QW0198BP =    X'01' THEN 'BP1'
       WHEN A.QW0198BP =    X'02' THEN 'BP2'
       WHEN A.QW0198BP =    X'03' THEN 'BP3'
       WHEN A.QW0198BP =    X'04' THEN 'BP4'
       WHEN A.QW0198BP =    X'05' THEN 'BP5'
       WHEN A.QW0198BP =    X'06' THEN 'BP6'
       WHEN A.QW0198BP =    X'07' THEN 'BP7'
       WHEN A.QW0198BP =    X'50' THEN 'BP32K0'
       WHEN A.QW0198BP =    X'64' THEN 'BP8K0'
       WHEN A.QW0198BP =    X'78' THEN 'BP16K0'
  END AS BUFFERPOOL
FROM DB2PROD.TPBPASMF A
WHERE QW0198PS = 'M'    -- I/OS ONLY, BP HITS NOT REPORTED
AND   QW0198AT = 'R'    -- RANDOM ACCESS ONLY, NO PREFETCH
AND PLANNAME = 'P51200' -- ONLY FOR A SPECIFIC PLAN
GROUP BY A.DBID, A.OBID, A.QW0198BP
;
```

Continuous Monitoring: Other reports

- Access matrix C
  - Detailed information of granted privileges to users
- Detailed performance reports E
  - Detail reports of dynamic statement cache contents
- List of unused indexes E
  - Reports indexes not used for query processing (w/o unique or clustering indexes)
- Detect lost optimizer hints A E
  - Optimizer hints lost because of (re)binds
- List of users with zparm update privileges C
  - To detect changes of INSTALL SYSADM

Summary From the Auditor's Perspective

- Continuously assess risk indicators
  - For example, use procedures presented in part I
- Check effectiveness of internal controls (part II reports)
  - If ok, verify if reports are current and available
    - Analyze result summary over longer period of time
  - If not, apply procedures yourself
    - If results are satisfactory, look for compensating controls
    - If results are not satisfactory, report risks and vulnerabilities

Summary From the DBA's Perspective

- Offer and publish risk indicators
  - For example, use procedures presented in part I
- Continuously self-assess the risks to your data by applying procedures such as those presented in part II

- If appropriate, use exception management tool
- Analyze number of exceptions per type over time

Summary: 5 tips

- Audit Independence
  - Auditors and DBAs must not use the same reports
- More Audit Independence
  - Auditors and DBAs must not rely on the same data sources
- Use continuous risk assessment on both the audit and the DBA level
- Stay patched!
- Expand audit scope to all aspects of information security
  - Confidentiality, Integrity, Availability, but also
  - Efficiency (Performance)

Thank you!

References

- IDUG NA and European Conference 2008 Proceedings
  - Session B01 (IDUG Europe): Memory Management for Dynamic SQL
- Dansk IT-Sikkerhedsforum
  - Audit Guideline for DB2, Copenhagen, October 2002
- Implementing Database Security and Auditing
  - Ron Ben Natan, Elsevier Digital Press, ISBN 1-55558-334-2
- Security, Audit and Control Features
  - Oracle Database 3rd Edition, ISACA, ISBN 978-1-60420-118-5
- ISACA Journal, Vol.6, 2009
  - Achieving Continuous IT Auditing, pp.37-41

2010 IDUG Europe

Session Code: B06

Thomas Baumann

thomas.baumann@mobi.ch

Since 1992, Thomas Baumann has been focusing on understanding how the DB2 database engine works. He has a master degree of computer sciences from ETH Zurich, Switzerland, and is currently working as head of data management at Swiss Mobiliar Insurance in Berne, Switzerland. If he is not in his office trying how to get the most out of DB2, he is somewhere lecturing on DB2 optimization, or performing a database audit. Thomas is a certified information systems auditor (CISA), and a member of the IDUG speaker hall of fame.