DB2 RUG Sandviken 2007

- DB2 Log Extract Tool for audit
- Diverse DB2 v8

Author: Michael Ärlebrandt
Dept: 8062
Date: 2007-01-17

Varför

- Sarbanes-Oxley Act commonly called **SOX** or **Sarbox**
- Vi vill kunna logga aktiviteter som DBA har gjort i DB2 systemen
- Vi har inga verktyg typ Log Analyzer
- Med DB2 leveraras DSN1LOGP

Overview

Collect

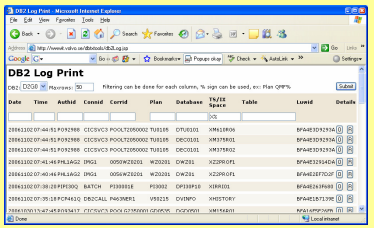
Batch run once a day

- **LISTBSDS (IBM utility)**
- **READBSDS (Rexx)**
- **DSN1LOGP (IBM utility)**
- **READLOG (Rexx)**
- **LOAD (IBM utility)**

LOG_DATA
LOG_RECORD
LOG_OBJECT

Report

Web gui



Daily Batch

Collect
Batch run once a day

- **LISTBSDS (IBM utility)**
- **READBSDS (Rexx)**
- **DSN1LOGP (IBM utility)**
- **READLOG (Rexx)**
- **LOAD (IBM utility)**

- LISTBSDS - DSNJU004 (print log map) – IBM Utility
  - List active and arcive log record sequence numbers (LRSN/RBA)
  - List checkpoint record sequence numbers
- READBSDS – Rexx – Volvo Utility
  - Parse the LISTBSDS output for LRSN/RBA for a given date/time
- DSN1LOGP – Log Print - IBM Utility
  - Formats the contents of the recovery log for display.
  - Summary report
- READLOG - Rexx – Volvo Utility
  - Parse the output from DSN1LOGP and build load file

DSN1LOGP

- Parameters used for batch running in Rollup mode:

  STARTLRSN(BFA413BB785A) (saved from previous run)
  ENDLRSN(FFFFFFFFFFFF) (to end of log)
  SUMMARY(ONLY) FILTER (We only want summary)
  DATAONLY(YES) (only Data Changes)

- Example of other parameters available

  DBID/OBID - Database/Object ID
  PAGE – RID (rowid) – Limit to specific page or row
  URID - Unit of recovery
  LUWID – Logical Unit of Work
  TYPE/SUBTYPE – Type of records

DSN1LOGP Summary Output

DSN1151I DSN1LPRT **MEMBER=D2G1** UR **CONNID=CICSVC3 CORRID=POOLT2050002 AUTHID=PO92988 PLAN=TU0105**

START DATE=06.306 TIME=07:44:51 DISP=COMMITTED INFO=COMPLETE
STARTRBA=05D3F74E5000 ENDRBA=05D3F74E74BD STARTLRSN=BFA4E3D95767 ENDLRSN=BFA4E3D99EAA
NID=* **LUWID**=VCCSNI01.D2D2G101.**BFA4E3D9293A**.0001
COORDINATOR=* PARTICIPANTS=*

DATA MODIFIED:
DATABASE=017A=DTU0101 PAGE SET=0152=XM610R06
DATABASE=017A=DTU0101 PAGE SET=0004=SM610
DATABASE=016D=DEC0101 PAGE SET=008F=SM375
DATABASE=016D=DEC0101 PAGE SET=0092=XM375R01
DATABASE=016D=DEC0101 PAGE SET=0094=XM375R02

* LUWID – Logical Unit of Work ID
3 parts: LU network name, an LUW instance number, and a commit sequence number – We use the LUW instance number as key

DSN1LOGP Detail Output

- Can be used if needed to investigate
- Warning: Can produce a lot of data
- Hex format of data – hard to decode
- Subject of change – new row format in V9

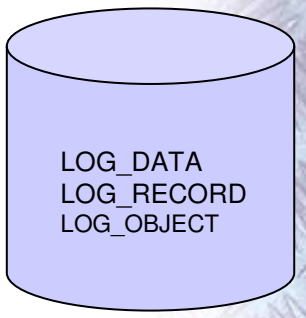
```
05D3F74E550A  MEMBER(D2G1    )  URID(05D3F74E5000)
              LRSN(BFA4E3D96371)  DBID(017A)  OBID(0004)
              PAGE(0000104B)  TYPE( UNDO  REDO )
              SUBTYPE(UPDATE IN-PLACE IN A DATA PAGE)  CLR(NO)
              PROCNAME(DSNILREP)
     *LRH* 044A003D 06000001 0E8005D3 F74E5000 05D3F74E 54CD0526 05D3F74E 54CDBFA4  * §         L7+&  L7+     L7+   u
           E3D96371 0001                                                          *TR
     *LG** 08017A00 04000010 4B00009A A9765B7C 2B00                               *  :     .   z ÅÖ
     0000  04120103 002B0900 000FF440 F000F010 F002D2D6 D7D7D3C9 D5C7E2D3 5BC4C140  *          4 0 0 0 KOPPLINGSLÅDA
     0020  40404040 40404040 40404040 40404040 F00000F0 000000D5 40404040 40404040  *                0  0   N
     0040  4040D5F0 01404040 40404040 40404040 40404040 40F00000 00004040 40404040  *  N0                 0
     0060  40404040 40404040 40404040 40404040 40404040 40404040 D5F0F0F0 F6D54040  *                       N0006N
     0080  40404040 40404040 40404040 40404040 40404040 40404040 40404040 40404040  *
     00A0  40404040 40404040 40404040 40404040 40404040 40404040 4040D540 F7F6F2F6  *                           N 7626
     00C0  40404040 40404040 40404040 40F00000 0000F000 00000040 4040F000 000000F0  *             0    0       0    0
     00E0  00F0F1F1 F97CC140 40F02006 1102F0F1 F1F97CC1 4040F019 851129F0 00000000  * 0119ÖA  0    0119ÖA  0 e  0
     0100  40404040 40404040 40404040 40F00000 007435F0 2005F000 00000000 D5F00000  *             0     0  0     N0
     0120  0000F000 00F00000 0000F000 00004040 40404040 40404040 40404040 40404040  *  0  0    0
     0140  40404040 40404040 40404040 20061102 07445137 2870F000 00000000 F0000000  *                        0     0
     0160  00F00040 40404040 40404040 40404040 40404040 40404040 40404040 40404040  * 0
     0180  40404040 40404040 40404040 40404040 40404040 40404040 40404040 40404040  *
     01A0  40404040 40404040 40404040 40404040 40404040 40404040 40404040 40404040  *
     01C0  40404040 40404040 40404040 40404040 40404040 40404040 40404040 40404040  *
     01E0  40404040 40404040 40404040 40404040 40404040 40404040 40404040 40404040  *
     0200  D5404040 40404040 40404040 40F0F3D5 F000F010 F002D2D6 D7D7D3C9 D5C7E2D3  *N            03N0 0 0 KOPPLINGSL
     0220  5BC4C140 40404040 40404040 40404040 40404040 F00000F0 000000D5 40404040  *ÅDA                 0  0   N
     0240  40404040 4040D5F0 01404040 40404040 40404040 40404040 40F00000 00004040  *      N0                0
```

Parameter input for batch

- Mode='ROLLUP' - Read logs since last run.
  To be run daily
- Mode='DATE' - Specify date and time
  stadate=200610181400 start
  stodate=200610181500 stop
- Mode='RECORD - Specify LRSN/RBA
- Userids='V0xxxxx,V0yyyyy' - List of userids to include
- ExclUserids='PC0DB21' - List of userids to exclude
- Incldb and Excldb - Databases to include
- Datasharing='YES' - support for datasharing
- List of Database/Indexspace in catalog corresponding to which table

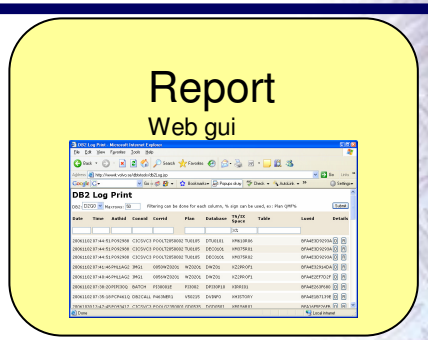
```
:PRM db2=D2G0                                    /* name of db2             */
:PRM datasharing='YES'                           /* datasharing of not      */
:PRM mode='ROLLUP'                               /* DATE, RECORD, ROLLUP    */
:PRM stadate=200610181400                        /* start date (and time)   */
:PRM stodate=200610181500                        /* stop  date (and time)   */
:PRM starec ='BF937587A9C4'                      /* start rba/lrsn          */
:PRM storec ='BF9382F232CB'                      /* start rba/lrsn          */
:PRM gmtoffset=1                                 /* gmt offset              */
:PRM listbsds='YES'                              /* run LISTBSDS            */
:PRM readbsds='YES'                              /* run READBSDS            */
:PRM logp='YES'                                  /* run DSN1LOGP            */
:PRM report='YES'                                /* print report            */
:PRM load='YES'                                  /* load into db2 tables    */
:PRM userids=''                                  /* special userids to log  */
:PRM excluserids=''                              /* special userids to excl */
:PRM excluserids='SYSOPR V00DB21 V00DB20'        /* special userids to excl */
:PRM excldb=''                                   /* exclude of db           */
:PRM incldb=''                                   /* specific db             */
:PRM debug=0                                     /* debug or not            */
*
* List of Database/Indexspace in catalog corresponding to which table
*    DB       SP        Table
:OBJ DSNDB06 DSNDOB02 SYSIBM.SYSOBDS
:OBJ DSNDB06 DSNDOB01 SYSIBM.SYSOBDS
:OBJ DSNDB06 DSNUCX01 SYSIBM.SYSCOPY
:OBJ DSNDB06 DSNUCH01 SYSIBM.SYSCOPY
:OBJ DSNDB06 DSNACX01 SYSIBM.SYSCOLAUTH
```

Data saved in DB2 tables

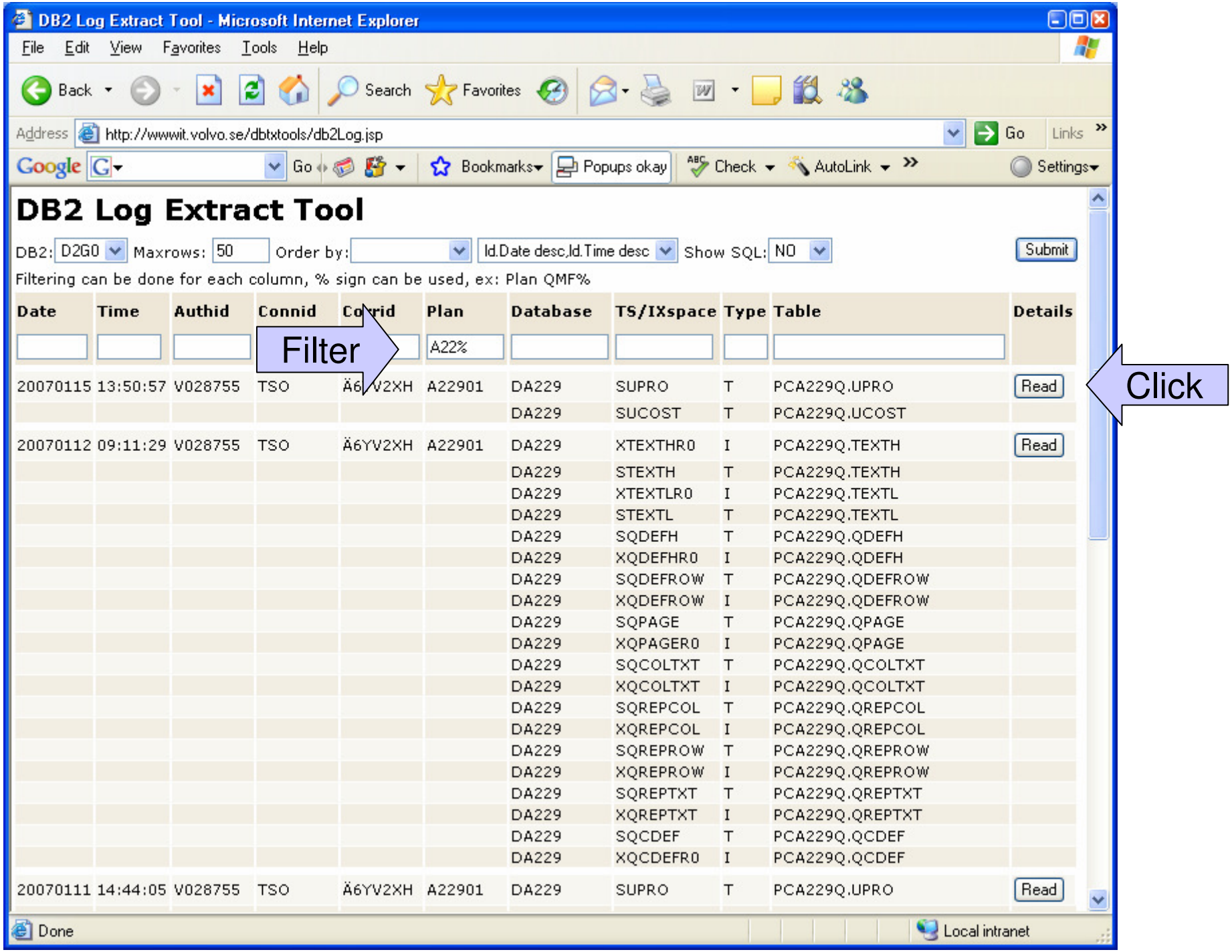


- Saved in 3 tables
  - partioned by date range to provide growth and to be able to rollout outaged partions
- LOG_DATE
  - One summary record per LUW (Logical Unit of Work)
- LOG_RECORD
  - Record information for each record – LRSN/RBA
- LOG_OBJECT
  - Database and Tablespace/Indexspace info

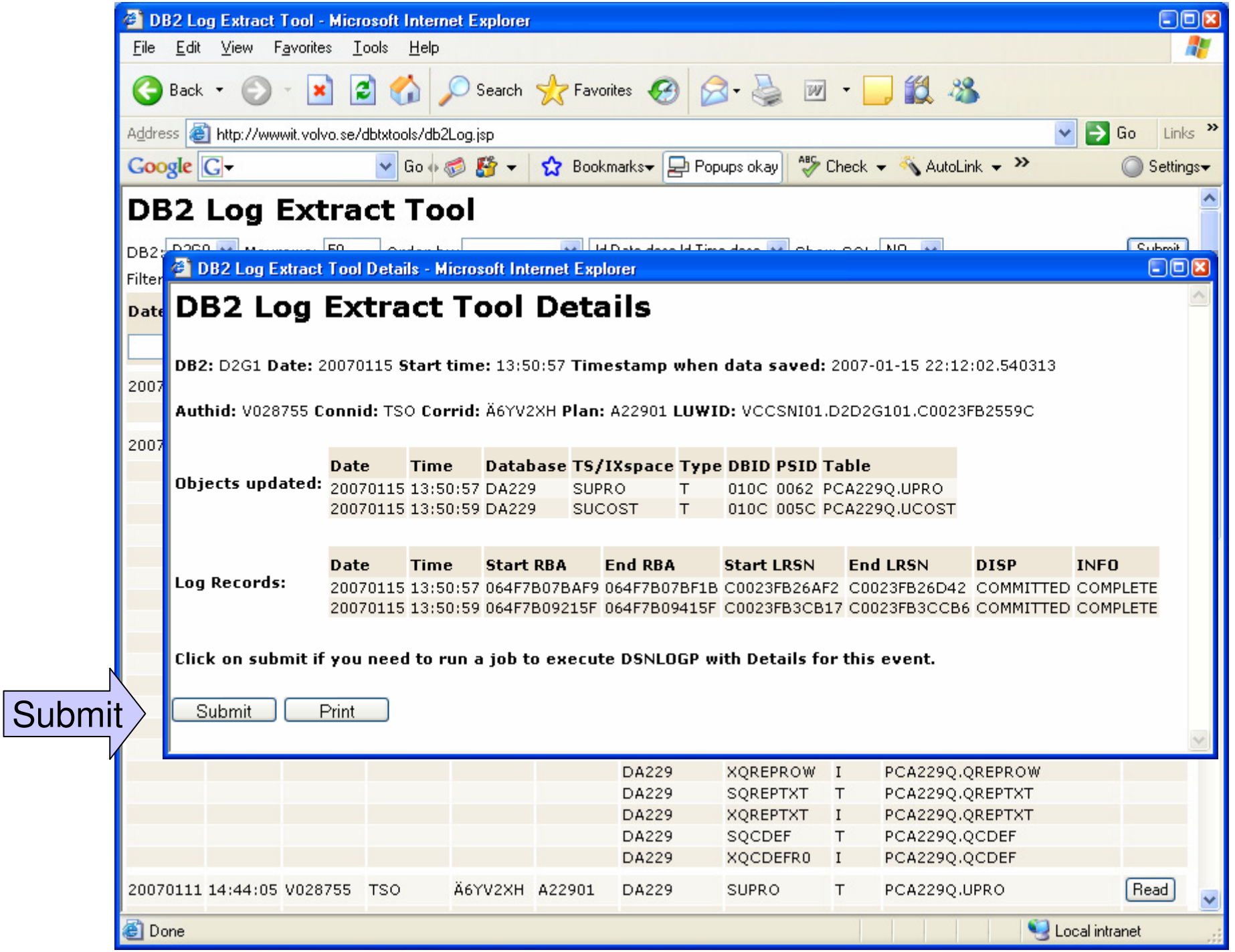
Report



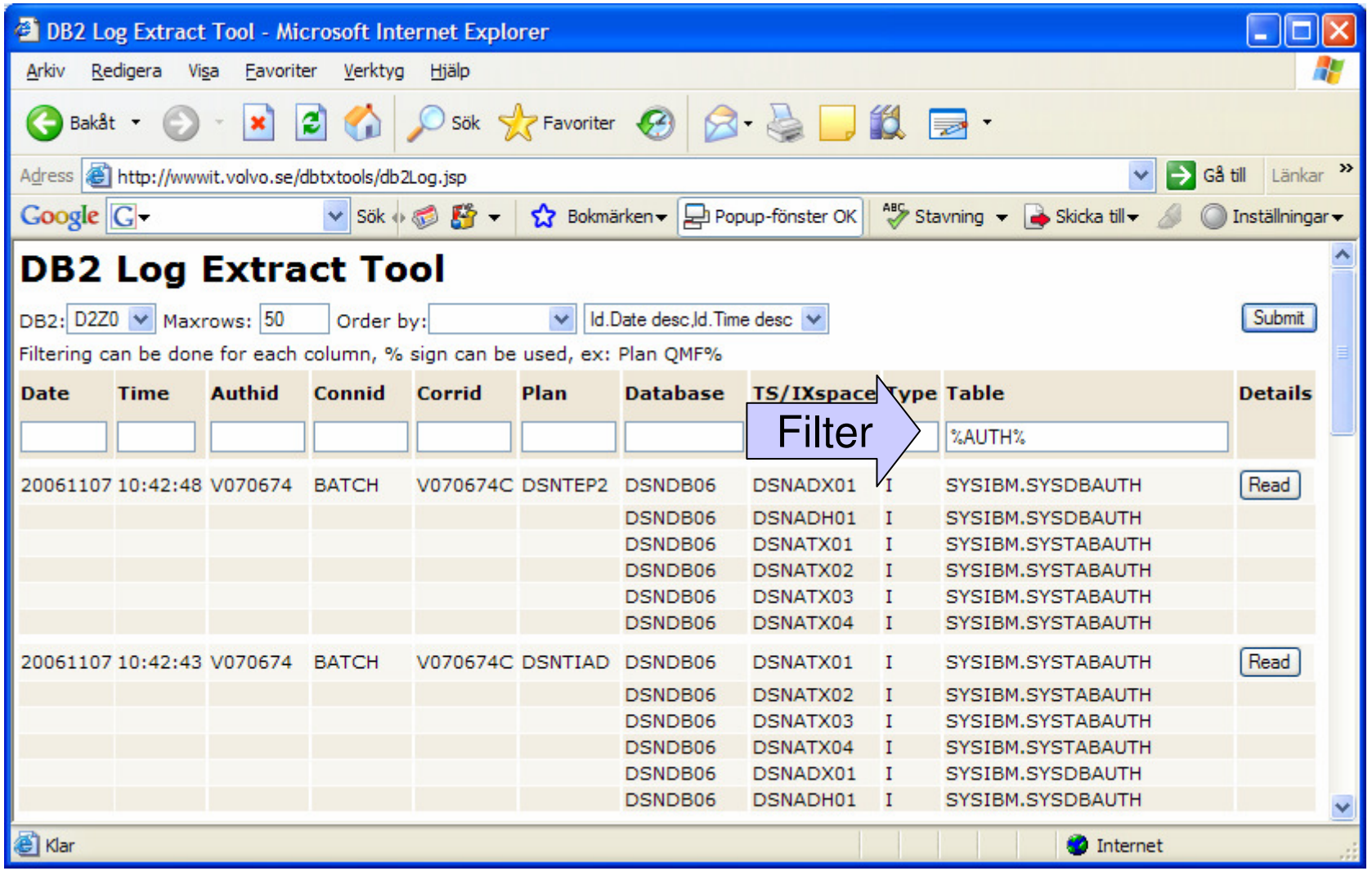
- Sample JSP application written to show what kind of info that can be read from the DB2 log tables
- Filtering on
  - Date and time
  - Authid
  - Connid – Batch, IMS, CICS, TSO, DB2CALL, SERVER
  - Corrid – Ex batch job name
  - Plan - Ex QMF%, DSNESPCS (Spufi)
  - Database
  - TS/IX Space
  - Table - If indexspace or tablespace with only 1 table
- Detail records for records and objects can be selected



Date	Time	Authid	Connid	Corrid	Plan	Database	TS/IXspace	Type	Table	Details
					A22%					
20070115	13:50:57	V028755	TSO	Ä6YV2XH	A22901	DA229	SUPRO	T	PCA229Q.UPRO	Read
						DA229	SUCOST	T	PCA229Q.UCOST	
20070112	09:11:29	V028755	TSO	Ä6YV2XH	A22901	DA229	XTEXTHR0	I	PCA229Q.TEXTH	Read
						DA229	STEXTH	T	PCA229Q.TEXTH	
						DA229	XTEXTLR0	I	PCA229Q.TEXTL	
						DA229	STEXTL	T	PCA229Q.TEXTL	
						DA229	SQDEFH	T	PCA229Q.QDEFH	
						DA229	XQDEFHR0	I	PCA229Q.QDEFH	
						DA229	SQDEFROW	T	PCA229Q.QDEFROW	
						DA229	XQDEFROW	I	PCA229Q.QDEFROW	
						DA229	SQPAGE	T	PCA229Q.QPAGE	
						DA229	XQPAGER0	I	PCA229Q.QPAGE	
						DA229	SQCOLTXT	T	PCA229Q.QCOLTXT	
						DA229	XQCOLTXT	I	PCA229Q.QCOLTXT	
						DA229	SQREPCOL	T	PCA229Q.QREPCOL	
						DA229	XQREPCOL	I	PCA229Q.QREPCOL	
						DA229	SQREPROW	T	PCA229Q.QREPROW	
						DA229	XQREPROW	I	PCA229Q.QREPROW	
						DA229	SQREPTXT	T	PCA229Q.QREPTXT	
						DA229	XQREPTXT	I	PCA229Q.QREPTXT	
						DA229	SQCDEF	T	PCA229Q.QCDEF	
						DA229	XQCDEFR0	I	PCA229Q.QCDEF	
20070111	14:44:05	V028755	TSO	Ä6YV2XH	A22901	DA229	SUPRO	T	PCA229Q.UPRO	Read


DB2 Log Extract Tool - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://wwwit.volvo.se/dbtxtools/db2Log.jsp
Go Links
Google Go Bookmarks Popups okay Check AutoLink Settings
DB2 Log Extract Tool
DB2 Log Extract Tool Details - Microsoft Internet Explorer
DB2 Log Extract Tool Details
DB2: D2G1 Date: 20070115 Start time: 13:50:57 Timestamp when data saved: 2007-01-15 22:12:02.540313
Authid: V028755 Connid: TSO Corrid: Ä6YV2XH Plan: A22901 LUWID: VCCSNI01.D2D2G101.C0023FB2559C
Objects updated:
Date Time Database TS/IXspace Type DBID PSID Table
20070115 13:50:57 DA229 SUPRO T 010C 0062 PCA229Q.UPRO
20070115 13:50:59 DA229 SUCOST T 010C 005C PCA229Q.UCOST
Log Records:
Date Time Start RBA End RBA Start LRSN End LRSN DISP INFO
20070115 13:50:57 064F7B07BAF9 064F7B07BF1B C0023FB26AF2 C0023FB26D42 COMMITTED COMPLETE
20070115 13:50:59 064F7B09215F 064F7B09415F C0023FB3CB17 C0023FB3CCB6 COMMITTED COMPLETE
Click on submit if you need to run a job to execute DSNLOGP with Details for this event.
Submit
Print
Submit
DA229 XQREPROW I PCA229Q.QREPROW
DA229 SQREPTXT T PCA229Q.QREPTXT
DA229 XQREPTXT I PCA229Q.QREPTXT
DA229 SQCDEF T PCA229Q.QCDEF
DA229 XQCDEFR0 I PCA229Q.QCDEF
20070111 14:44:05 V028755 TSO Ä6YV2XH A22901 DA229 SUPRO T PCA229Q.UPRO Read
Done
Local intranet

Track of Authority table updates



Load test i D2G1 1 Dygn

Kördes i D2G1 den 10/10 2006 22:00

Logggar i D2G1 för ett dygn lästes
Inget urval vad gäller userid eller DB

Jobbet tog 35 min
CPU USAGE: 7266.488 PU-NIGHT
TOTAL JOB COST: 1453.30 SEK

600 000 rader i tabell logdata	**2295 tracks**	**2160K**
2 000 000 rader i tabell logobject	**4500 tracks**	**4320K**
2 113 userid found		

Just nu

- Kör vi den dagligen i ett Prod system för utvärdering
- Endast för 18 utvalda userid – DBA och Sysprog
- 1 gång per dag i rollup mode
- Antal arkivloggar varierar mellan 2-3 st upp till 30 a 800 cyl.
- 1 månads data - 15Dec till 15Jan – 44000 record , om man bortser från några systemid som används för batchar så blir det 144 rekords

- ➔ men vi fångar ju knappast bovarna …

Tex .AUTH i CA batch processor

F1PT00.PROD.LOADLIB(BPLSEC)
och APF authorized

.CONNECT D2Z0
RETCODE = 0
.AUTH V00DB21
RETCODE = 0

- Och voilaa – full behörighet och allt loggas på V00DB21 istället för mitt eget id !!!

.AUTH V00DB21
You are not allowed to use .AUTH command, please contact dept 8062 for info
BPA0013I: COMMAND CANCELLED BY USER SECURITY EXIT: EXIT01.
RETCODE = 8

Diverse DB2 v8

DSNTEP4 Multirow fetch

```
//RUNTEP2 EXEC PGM=IKJEFT01,DYNAMNBR=20
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SYSTSIN DD *
  DSN SYSTEM(DSN)
  RUN PROGRAM(DSNTEP4) PLAN(DSNTEP4)
//SYSIN DD *
-- default 100
--#SET MULT_FETCH 250
SELECT * FROM DSN8810.EMP;
```

Dynamic Statement Cache Statistics

- START TRACE(MON) IFCID(318) DEST(OP30)
  IFCID318= Dynamic statement cache statistics
- När man stoppar och startar tracen för IFCID318 så nollställs även alla räknare för IFCID318
- Gör EXPLAIN STMTCACHE ALL eller använd Visual Explain för att plocka ut datat **innan** man stoppar tracen. Allt nollställs vid STOP TRACE.
- Notera att med Visual Explain så töms DSN_STMT_CACHE_TABLE statistiken varje gång man tar ut rapporten
- Exempel på rapport sparad i Excel

Java and streaming of LOB data

- Efter förra RUG så kollade jag upp på Volvo
  Vi körde **INTE** med streaming av LOB i våra Java app mot DB2
- Men nu gör vi det, fr.o.m 22/11 i prod
  Detta för att inte åka på OutOfMemoryError vid stora LOB:ar
- **fullyMaterializeLobData=false**
  LOB data is retrieved with locators when you request a stream on the LOB column
- Vi kör med XA-driver för att vi använder 2 Phase Commit
- JCC drivers **DB2 v8 fixpack 13**
- Lite problem på vägen
  - Med fixpack 13 fick vi SQL kod -423 med lobdata.length(), fungerade med befintlig nivå fixpack 7