BROADCOM®
MAINFRAME SOFTWARE

Who's Knocking At the Door? Best Practices for Auditing Access to Db2 for z/OS

Denis Tronin | Product Manager
denis.tronin@broacom.com

March 2025

Agenda

- **Overview**
- Leveraging Db2 Catalog Tables
- Audit Traces (overview, classes and audit policies)
- Audit details in Db2 Log
- How about External Security?
- Other audit data sources
- Summary and Q&A

Information Technology Audit

Information Technology Audit is an examination of the management controls within an IT infrastructure and business applications. The evaluation of evidence obtained determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organization's goals or objectives

https://en.wikipedia.org/wiki/Information_technology_audit

Auditing Access to Db2

- Who is privileged to access the data?
- Who has actually accessed the data?
- What attempts are made to gain unauthorized access
- What has been done to the data?
- What can be done to mitigate the impact?

Db2 Authorization Control Basis

- Authorization ID (both primary and secondary IDs)
- Role ID (within a trusted context)
- Object ownership
- Multi-level security (row-level labels)

- Via Db2 or External security (RACF, TSS, ACF2) means

Db2 Authorization Control Basis: Db2 Privileges

- **Explicit** – established with GRANT statement
  - Collections, database, distinct type and JAR, UDF and procedure, global variable, package, plan, routine, schema, sequence, systems, table and view, usage, use
- **Implicit** – established with object creation
- **Administrative Authorities**
  - A named group of privileges
  - ACCESSCTRL, DATAACCESS, DBADM, DBCTRL, DBMAINT, Installation SYSADM, Installation SYSOPR, PACKADM, SECADM, SQLADM, SYSADM, SYSCTRL, SYSOPR, System DBADM
  - Hierarchy applies (e.g. DBCTRL includes DBMAINT)

Leveraging Db2 Catalog Tables

Leveraging Db2 Catalog Tables

- Db2 catalog contains Db2 authorization and authentication details – audit data “**at rest**”
  - Privilege type
  - Object name
  - IDs receiving the privilege
  - IDs granting the privilege
  - Grant timestamp
- Serves as primary audit trail for the Db2 subsystem
- Can be simply queried by issuing a SELECT

Catalog “AUTH” Tables (1 of 4)

- SYS**DB**AUTH
  - Privileges held by users over **databases** (CREATETAB, STARTDB, DROP, etc.)
- SYS**TAB**AUTH
  - Privileges held by users on **tables**, **views**, and **triggers** (SELECT, ALTER, INSERT, UPDATE, etc.)
- SYS**COL**AUTH
  - UPDATE privileges held by users on **individual columns** of a table or view (UPDATE (COL1, COL2..)
- SYS**SCHEMA**AUTH
  - Privileges held by users on a **schema** (CREATEIN, ALTERIN, DROPIN)

Catalog “AUTH” Tables $^{(2 \text{ of } 4)}$

- SYS**ROUTINE**AUTH
  - Privileges held by users on **routines** (EXECUTE ON FUNCTION, etc.)
- SYS**VARIABLE**AUTH
  - Privileges held by users on **global variables** (READ, WRITE,)
- SYS**SEQUENCE**AUTH
  - Privileges held by users on **sequences** (ALTER, USAGE)

Catalog “AUTH” Tables (3 of 4)

- SYS**PLAN**AUTH
  - Privileges held by users on application **plans** (BIND, EXECUTE)
- SYS**PACK**AUTH
  - Privileges held by users on **packages** (BIND, COPY, EXECUTE, etc.)
- SYS**RES**AUTH
  - Privileges held by users on **resources** like buffer pools, storage groups, table spaces, and collections (USE OF, CREATE ON)

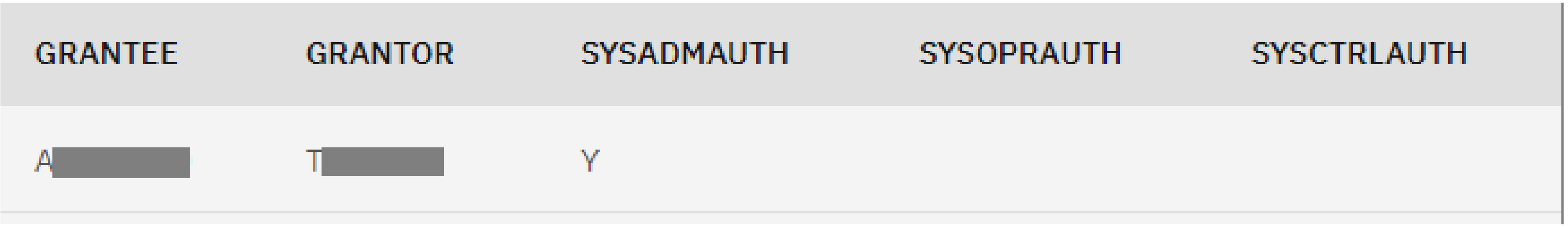
Catalog “AUTH” Tables (4 of 4)

- SYS**CONTEXT**AUTHIDS
  - Auth IDs under which a **trusted context** can be used
- SYS**USER**AUTH
  - System privileges that are held by users (including administrative authorities ACCESSCTRL, DBADM, SECADM, SQLADM, SYSADM, etc.)

A couple sample queries to Db2 Catalog

- Users with high privileges

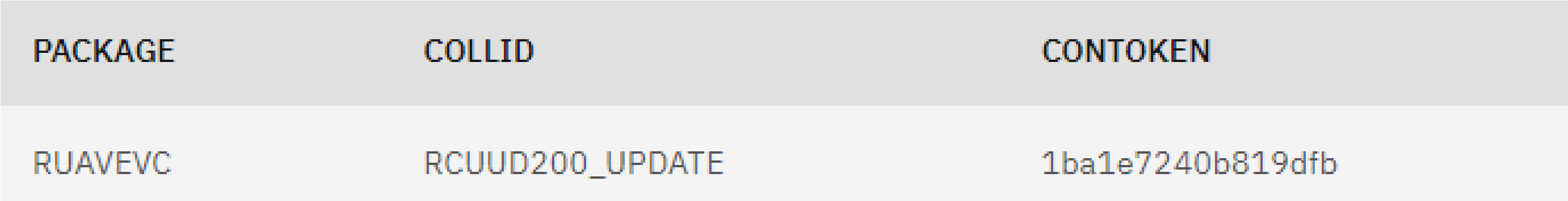
```
SELECT GRANTEE, GRANTOR, SYSADMAUTH, SYSOPRAUTH, SYSCTRLAUTH
  FROM SYSIBM.SYSUSERAUTH
```



GRANTEE	GRANTOR	SYSADMAUTH	SYSOPRAUTH	SYSCTRLAUTH
A[redacted]	T[redacted]	Y		

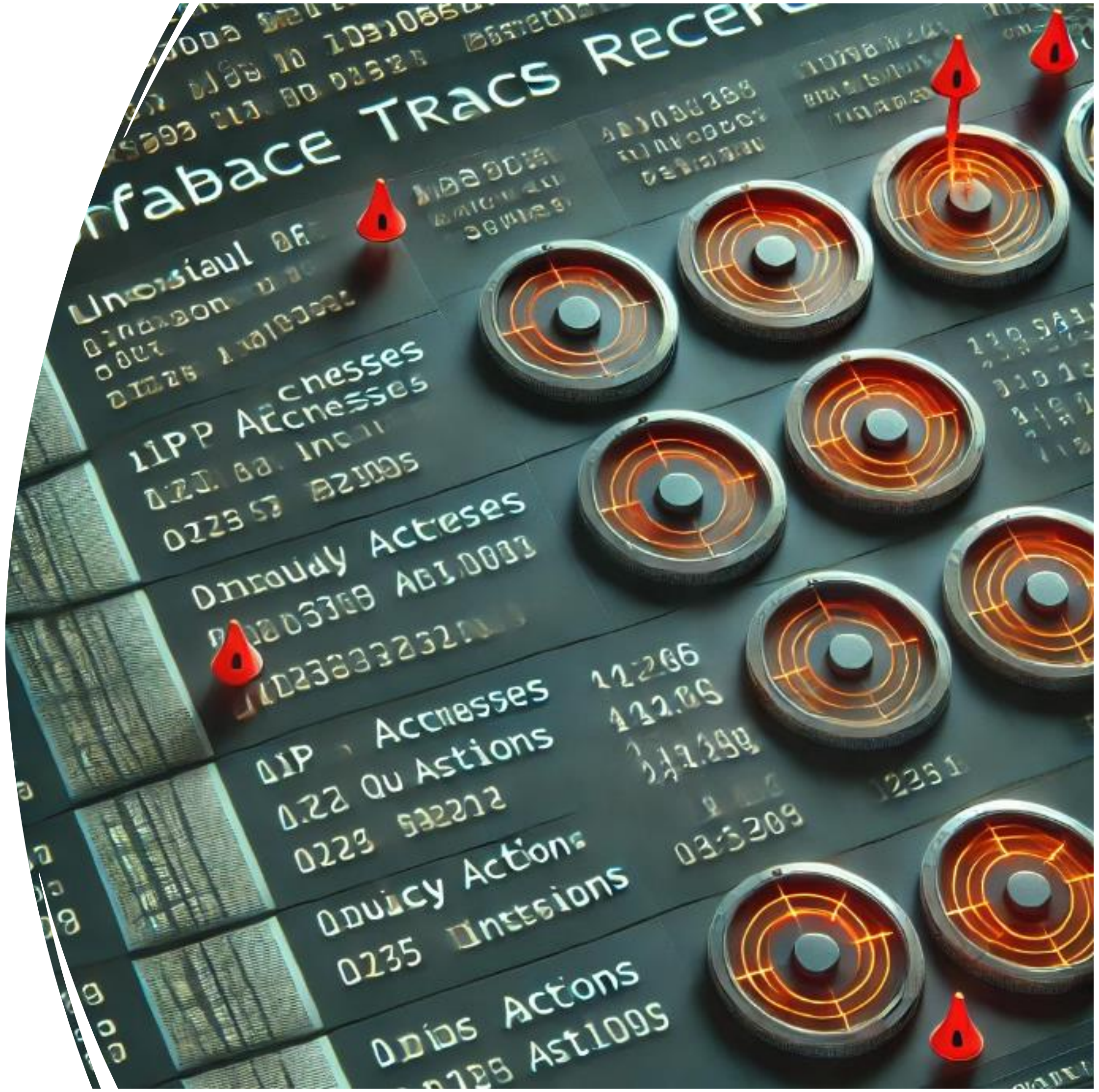
- Packages with granted privileges to a table (e.g. SYSIBM.SYSTABLES)

```
SELECT GRANTEE AS PACKAGE, COLLID, CONTOKEN  FROM SYSIBM.SYSTABAUTH
 WHERE GRANTEETYPE='P' AND COLLID IS NOT NULL
   AND TCREATOR='SYSIBM' AND TTNAME='SYSTABLES'
```



PACKAGE	COLLID	CONTOKEN
RUAVEVC	RCUUD200_UPDATE	1ba1e7240b819dfb

Audit Traces and Policies



Audit TRACEs

- Serve for monitoring and tracking security and data access events – audit data “**at motion**”:
- Traces are enabled via command, zParm or started AUDIT policy
- Traces mainly apply to audited tables (defined with **`AUDIT ALL`**)
  - Audit policies help to overcome this
- Collection of trace records can be enabled and disabled – thus should be properly controlled
- Traces are stored and processed outside of Db2
  - Using reporting tools, Db2 performance monitors (e.g. SYSVIEW for Db2)..
  - Storing in form raw SMFs type 102, printed reports, in tables, etc.

TRACE Command

- –START TRACE command tells Db2 WHAT events to capture and WHERE to write out the related trace records
- –START TRACE(PERFM/ACCTG/STAT/**AUDIT**/MONITOR) DEST(GTF/**SMF**/SRV/OPn/OPX) **CLASS**(n) SCOPE(LOCAL/GROUP) PLAN(xx) AUTHID(xx) IFCID(nn)...
- Required access:
  - TRACE privilege or authorities: System DBADM, SYSOPR, SYSCTRL, SYSADM or SECADM
- Management commands:
  - –DISPLAY TRACE, –MODIFY TRACE, –STOP TRACE
- Audit trace overhead is typically < 5%

Audit Trace Classes

- There are 11 audit trace classes
  - `–START TRACE(AU) D(SMF) C(*)` to start all audit classes
  - `–START TRACE(AU) D(SMF) C(1,3)` to start a list of audit classes
- Each class activates collection of specific audit trace records
- Db2 zParm AUDITST defines what audit classes are started at the start of Db2 (default is NO, YES = 1)
  - Alternatively, you can start manually or have your performance monitor to do it
- –START TRACE command allows including additional IFCIDs to be enabled along with those included into a CLASS

Audit Policies

- Alternative and preferable way to manage Audit Traces
  - As they offer more flexibility and easier management
- Policies group audit traces to 8 categories (vs. 11 audit classes)
- Policies are defined using SQL and stored in the catalog table SYSIBM.SYSAUDITPOLICIES
- Policies can be started
  - Manually with -START TRACE(AUDIT) **AUDTPLCY**(*policy-id*) command
    - Cannot be combined with CLASS or IFCID parameters
  - Automatically at Db2 startup if defined with **DB2START=Y/S/T**

SYSIBM.SYSAUDITPOLICIES Layout

- “Policy name” in AUDITPOLICYNAME column
- “Category” to enable:
  - CHECKING, VALIDATE, OBJMAINT, EXECUTE, CONTEXT, SECMAINTSYSADMIN, DBADMIN
- “Object names” to audit:
  - OBJECTSCHEMA, OBJECTNAME, OBJECTTYPE for categories OBJMAINT and EXECUTE
    - SQL Like syntax for the name
  - DBNAME for category DBADMIN (authorities DBADM, DBCTRL, and DBMAINT)
  - COLLID for category DBADMIN (authority PACKADM)
- “Start up” in DB2START column
  - “Y” to start, “S” to start and stop with SECADM only, “T” – tamper-proof, “N” – No

Define and start an Audit Policy

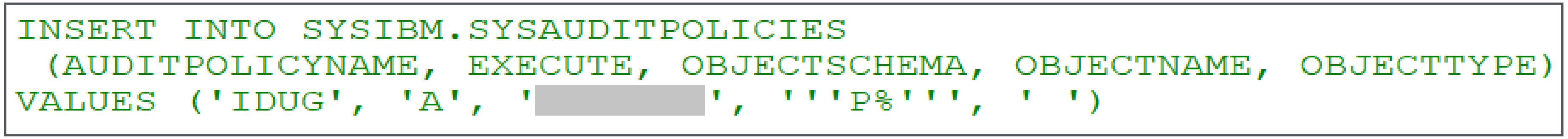
INSERT into SYSIBM.SYSAUDITPOLICIES

- Requires SECADM authority
- Specify a name for the policy (e.g. “IDUG”)
- Specify audit categories
- Specify list of audit objects with SQL LIKE predicate syntax (optional)

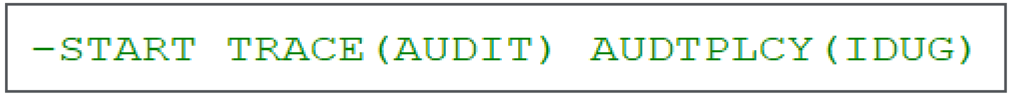
```
-START TRACE(AUDIT) AUDTPLCY(IDUG)
```

- Multiple policies can be specified
  - Generates IFCID 362
- Details include policy details, activated policies, matching audit tables, etc.

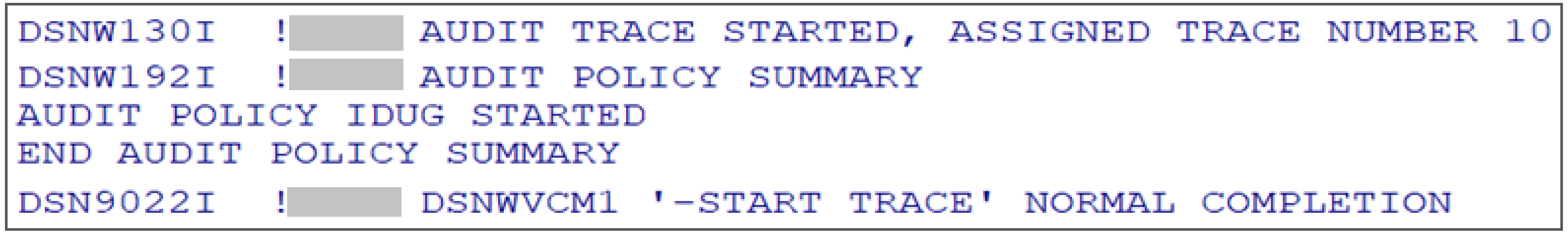
Define and start an Audit Policy



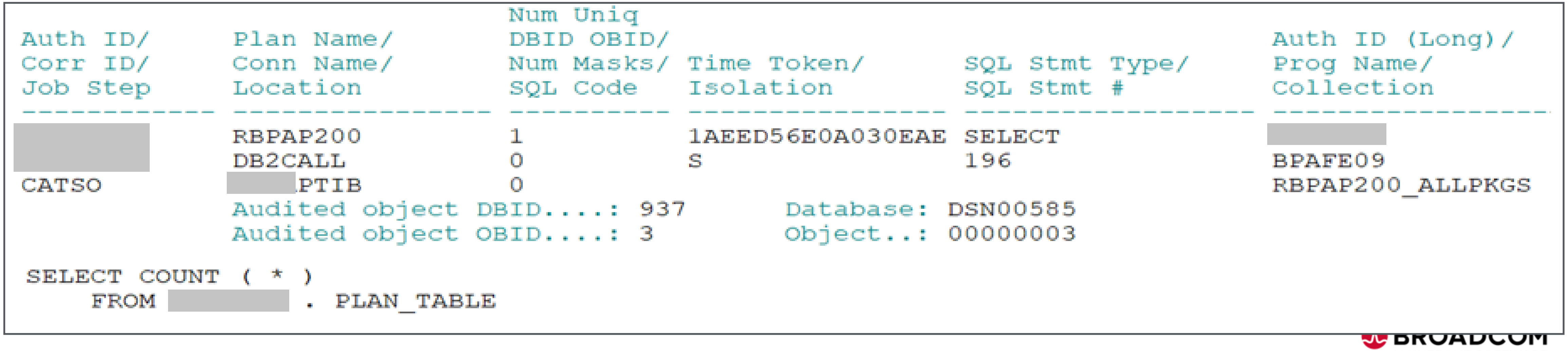
```
INSERT INTO SYSIBM.SYSAUDITPOLICIES
 (AUDITPOLICYNAME, EXECUTE, OBJECTSCHEMA, OBJECTNAME, OBJECTTYPE)
VALUES ('IDUG', 'A', '[redacted]', '''P%''', ' ')
```



```
-START TRACE(AUDIT) AUDTPLCY(IDUG)
```



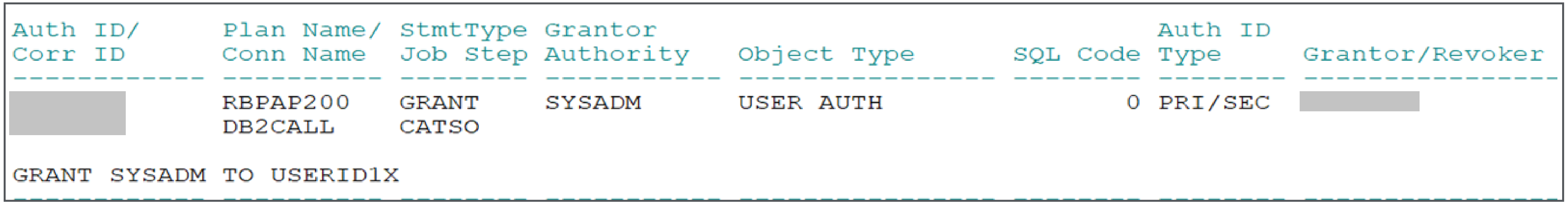
```
DSNW130I  ![redacted] AUDIT TRACE STARTED, ASSIGNED TRACE NUMBER 10
DSNW192I  ![redacted] AUDIT POLICY SUMMARY
AUDIT POLICY IDUG STARTED
END AUDIT POLICY SUMMARY
DSN9022I  ![redacted] DSNWVCM1 '-START TRACE' NORMAL COMPLETION
```



```
                                 Num Uniq
Auth ID/     Plan Name/          DBID OBID/                                        Auth ID (Long)/
Corr ID/     Conn Name/          Num Masks/ Time Token/        SQL Stmt Type/      Prog Name/
Job Step     Location            SQL Code   Isolation          SQL Stmt #          Collection
------------ ------------------- ---------- ------------------ ------------------- ------------------
[redacted]   RBPAP200            1          1AEED56E0A030EAE   SELECT              [redacted]
             DB2CALL             0          S                  196                 BPAFE09
CATSO        [redacted]PTIB      0                                                 RBPAP200_ALLPKGS
             Audited object DBID....: 937        Database: DSN00585
             Audited object OBID....: 3          Object..: 00000003

 SELECT COUNT ( * )
     FROM [redacted] . PLAN_TABLE
```

Traced Audit Events $^{(1 – 6)}$

- **Authorization failures** (IFCID 140) – attempts denied due to inadequate authorization (CLASS 1, CHECKING='A')
  - connection credentials, privilege, object name and type, authid type, auth check return code, SQL text, etc.
- **GRANT and REVOKE** (IFCID 141) – execution of each GRANT and REVOKE SQL statements (CLASS 2, SECMAINT='A')
  - connection credentials, grantor and revoker auth ids, access type, object type, authid type, SQL return code, SQL text, etc.

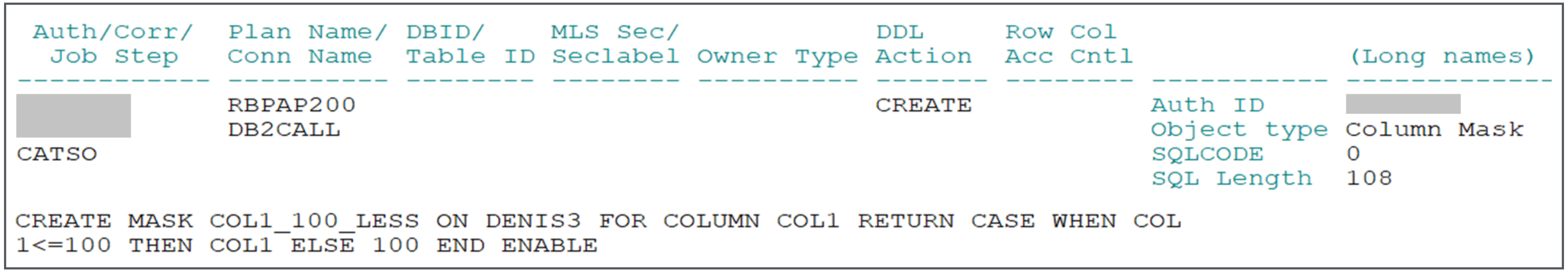


```
Auth ID/      Plan Name/ StmtType Grantor                                   Auth ID
Corr ID       Conn Name  Job Step Authority   Object Type       SQL Code  Type      Grantor/Revoker
------------  ---------- -------- ----------- ----------------- --------  --------  ---------------
[redacted]    RBPAP200   GRANT    SYSADM      USER AUTH                0  PRI/SEC   [redacted]
              DB2CALL    CATSO

GRANT SYSADM TO USERID1X
```

Traced Audit Events (2 – 6)

- **CREATE, ALTER, or DROP** (IFCID 142) – DDL statements against an audited table or table with row/column security (CLASS 3, OBJMAINT='A')
  - connection credentials, object details, statement type, access type, object type, table owner type, SQL return code, SQL text, etc.

- **Row/Column security management** (IFCID 271) – CREATE, ALTER, DROP of a row permission or a column mask (CLASS 11, SECMAINT='A')
  - connection credentials, package and collection names, SQL type/number/text, SQL code, object details, etc.

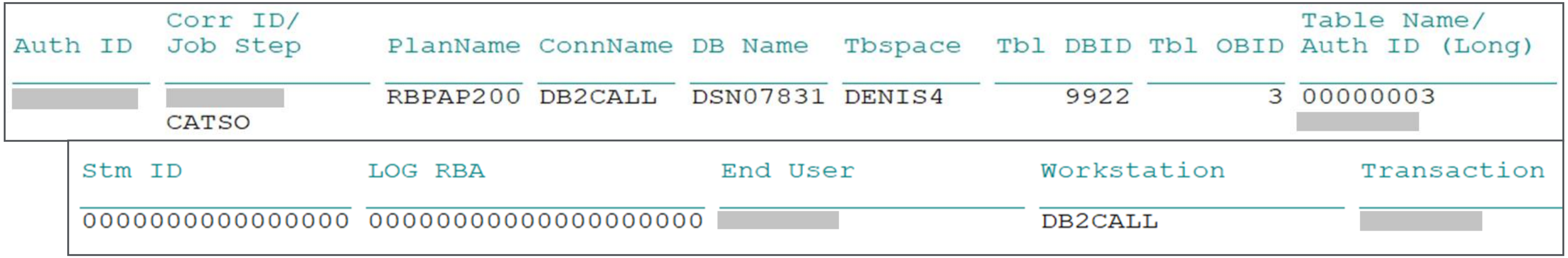


```
 Auth/Corr/   Plan Name/ DBID/    MLS Sec/                   DDL     Row Col
  Job Step    Conn Name  Table ID Seclabel Owner Type Action  Acc Cntl              (Long names)
------------ ---------- -------- -------- ---------- ------- -------- ----------- -------------
[redacted]    RBPAP200                                CREATE           Auth ID     [redacted]
              DB2CALL                                                  Object type Column Mask
CATSO                                                                  SQLCODE     0
                                                                       SQL Length  108

CREATE MASK COL1_100_LESS ON DENIS3 FOR COLUMN COL1 RETURN CASE WHEN COL
1<=100 THEN COL1 ELSE 100 END ENABLE
```

Traced Audit Events (3 – 6)

- ***First* table change** (IFCID 143) – change (write) of an audited table by a unique statement ID (CLASS 4, EXECUTE='A'/'C')
  - connection credentials, object details, statement ID (or zeroes), unit of recovery

- ***First* table read** (IFCID 144) – read access of an audited table by a unique statement ID (CLASS 5, EXECUTE='A'/'C')
  - connection credentials, object details, statement ID (or zeroes), unit of recovery (or zeroes)

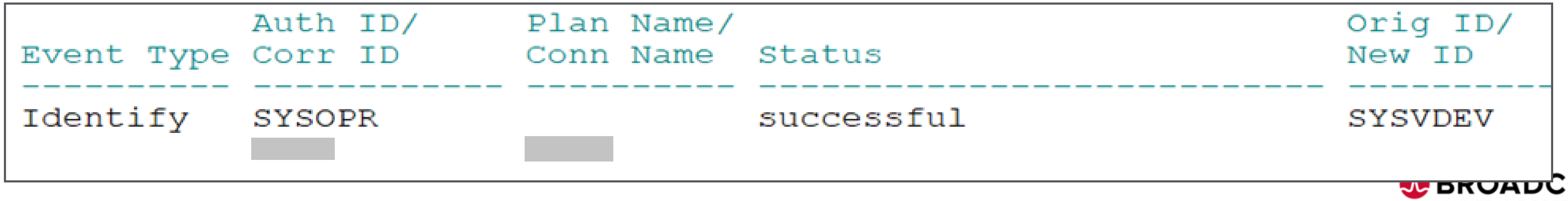


```
           Corr ID/                                                                   Table Name/
Auth ID    Job Step        PlanName  ConnName  DB Name   Tbspace   Tbl DBID Tbl OBID  Auth ID (Long)
________   ____________    ________  ________  ________  ________  ________ ________  ______________
[redacted] [redacted]      RBPAP200  DB2CALL   DSN07831  DENIS4        9922        3  00000003
           CATSO                                                                      [redacted]

    Stm ID            LOG RBA                 End User         Workstation      Transaction
    ________________  ____________________    ______________   ______________   ____________
    0000000000000000  00000000000000000000    [redacted]       DB2CALL          [redacted]
```

Traced Audit Events $^{(4 – 6)}$

- **SQL Bind time information** (IFCID 145) – audit log records for a prepared SQL statement against an audited table (CLASS 6, EXECUTE='A'/'C')
  - connection credentials, package and collection names, SQL type/number/text, SQL code, object details, etc.

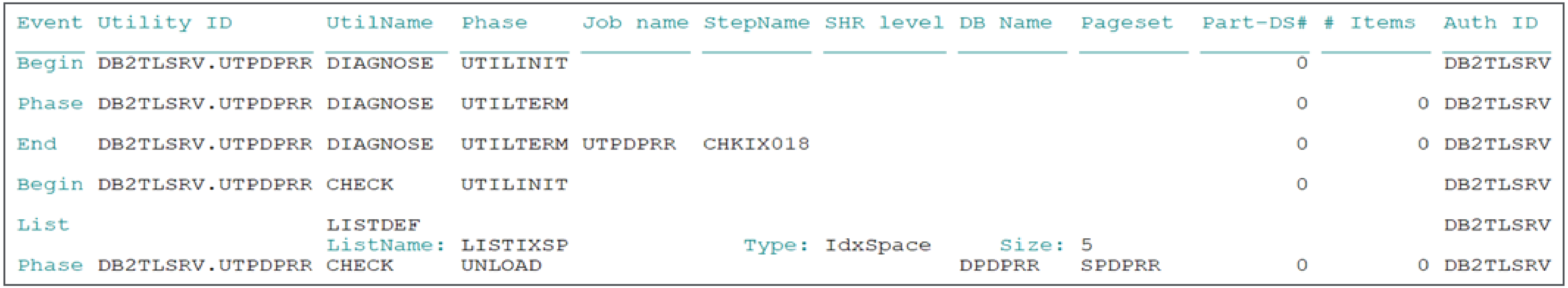
- **Assignment or change of authorization ID** (CLASS 7, VALIDATE='A')
  - IFCID 55 – SET CURRENT SQLID statements
  - IFCID 83 – End of an INDENTIFY request
  - IFCID 87 – SIGNON might have changed auth ID
  - IFCID 169 – Distributed auth ID translation
  - IFCID 319 – Remote user ID conversion to a local Db2 auth ID



```
           Auth ID/      Plan Name/                                    Orig ID/
Event Type Corr ID       Conn Name   Status                            New ID
---------- ------------  ----------  --------------------------------  ----------
Identify   SYSOPR                    successful                        SYSVDEV
           [redacted]    [redacted]
```

Traced Audit Events (5 – 6)

- **Db2 utility execution** (CLASS 8, CONTEXT='A')
  - IFCIDs 23-25 – Start/Phase/End of utility
  - IFCID 219 – LISTDEF usage (not in CONTEXT)
  - IFCID 220 – Dataset usage (not in CONTEXT)

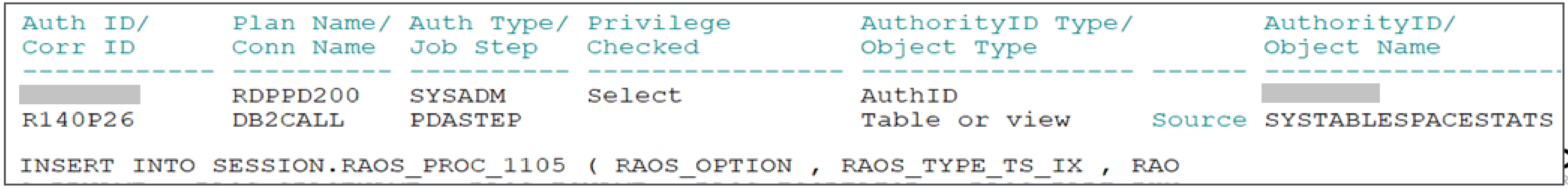


```
Event Utility ID       UtilName  Phase    Job name StepName SHR level DB Name  Pageset  Part-DS# # Items  Auth ID
----- ---------------- --------- -------- -------- -------- --------- -------- -------- -------- -------- --------
Begin DB2TLSRV.UTPDPRR DIAGNOSE  UTILINIT                                                      0          DB2TLSRV
Phase DB2TLSRV.UTPDPRR DIAGNOSE  UTILTERM                                                      0        0 DB2TLSRV
End   DB2TLSRV.UTPDPRR DIAGNOSE  UTILTERM UTPDPRR  CHKIX018                                    0        0 DB2TLSRV
Begin DB2TLSRV.UTPDPRR CHECK     UTILINIT                                                      0          DB2TLSRV
List                   LISTDEF                                                                            DB2TLSRV
                       ListName: LISTIXSP             Type: IdxSpace     Size: 5
Phase DB2TLSRV.UTPDPRR CHECK     UNLOAD                               DPDPRR   SPDPRR          0        0 DB2TLSRV
```

- **Trusted context monitoring** (CLASS 10, VALIDATE='A', SECMAINT='A')
  - IFCID 269 – Trusted connection is established or reused (VALIDATE)
  - IFCID 270 – Trusted connection is CREATEd or ALTERed (SECMAINT)

Traced Audit Events $^{(6 – 6)}$

- **Administrative authorities** (IFCID 361) – audit successful use of Db2 administrative authorities (CLASS 11, SYSADM and DBADMIN policies)
  - Authority type, authorization type, checked privilege, object details, SQL statement, etc.
  - When started with CLASS 11 – every access is recorded
  - When started with a policy – only access with SYSADM or DBADMIN authorities
    - SYSADM: '*'=all, 'I'=Install-SYSADM, 'R'=Install-SYSOPR, 'S'=SYSADM, 'L'=SYSCTRL, 'O'=SYSOPR
    - DBADMIN: '*'=all, 'E'=SECADM, 'B'=System-DBADM, 'C'=DBCTRL, 'D'=DBADM, 'G'=ACCESSCTRL, 'K'=SQLADM, 'M'=DBMAINT, 'P'=PACKADM, 'T'=DATAACCESS
      - Specific database name can be provided for DBADM, DBCTRL and DBMAINT
      - Specific collection ID can be provided for PACKADM
  - In case of external security (active Access Control Authorization Exit) only Install-SYSADM, Install-SYSOPR and SECADM are audited

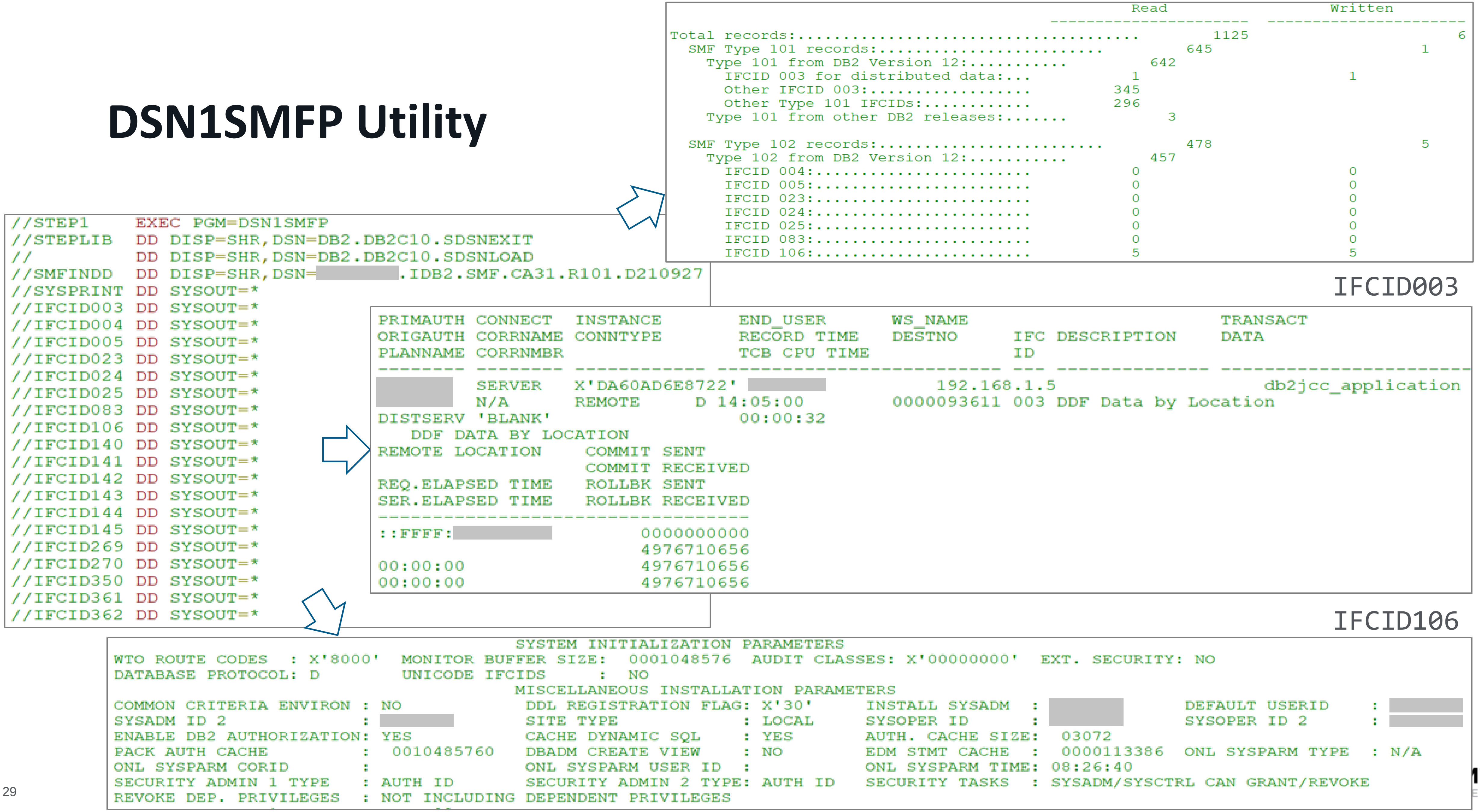


```
Auth ID/      Plan Name/ Auth Type/ Privilege         AuthorityID Type/         AuthorityID/
Corr ID       Conn Name  Job Step   Checked           Object Type               Object Name
------------- ---------- ---------- ----------------- ----------------- ------- -------------------
[redacted]    RDPPD200   SYSADM     Select            AuthID                    [redacted]
R140P26       DB2CALL    PDASTEP                      Table or view     Source  SYSTABLESPACESTATS

INSERT INTO SESSION.RAOS_PROC_1105 ( RAOS_OPTION , RAOS_TYPE_TS_IX , RAO
```

TRACE Reporting Tools

- DSN1SMFP
  - Db2 batch utility to report on most of audit IFCIDs:
    3, 4-5, 23-25, 83, 106, 140-145, 269-270, 350, 361-362
  - Takes SMF records 101 and 102 as input
- Vendor tools
  - Provide various batch and online reports on all IFCIDs (e.g. SYSVIEW for Db2)
  - Support storing audit data to Db2 tables (performance DB)

DSN1SMFP Utility



```
//STEP1     EXEC PGM=DSN1SMFP
//STEPLIB   DD DISP=SHR,DSN=DB2.DB2C10.SDSNEXIT
//          DD DISP=SHR,DSN=DB2.DB2C10.SDSNLOAD
//SMFINDD   DD DISP=SHR,DSN=[redacted].IDB2.SMF.CA31.R101.D210927
//SYSPRINT DD SYSOUT=*
//IFCID003 DD SYSOUT=*
//IFCID004 DD SYSOUT=*
//IFCID005 DD SYSOUT=*
//IFCID023 DD SYSOUT=*
//IFCID024 DD SYSOUT=*
//IFCID025 DD SYSOUT=*
//IFCID083 DD SYSOUT=*
//IFCID106 DD SYSOUT=*
//IFCID140 DD SYSOUT=*
//IFCID141 DD SYSOUT=*
//IFCID142 DD SYSOUT=*
//IFCID143 DD SYSOUT=*
//IFCID144 DD SYSOUT=*
//IFCID145 DD SYSOUT=*
//IFCID269 DD SYSOUT=*
//IFCID270 DD SYSOUT=*
//IFCID350 DD SYSOUT=*
//IFCID361 DD SYSOUT=*
//IFCID362 DD SYSOUT=*
```

SYSPRINT

```
                                                      Read                         Written
                                          -----------------------      -----------------------
Total records:....................................           1125                            6
  SMF Type 101 records:........................          645                           1
    Type 101 from DB2 Version 12:..........          642
      IFCID 003 for distributed data:...          1                         1
      Other IFCID 003:..................        345
      Other Type 101 IFCIDs:............        296
    Type 101 from other DB2 releases:.......            3

  SMF Type 102 records:........................          478                           5
    Type 102 from DB2 Version 12:..........          457
      IFCID 004:........................          0                         0
      IFCID 005:........................          0                         0
      IFCID 023:........................          0                         0
      IFCID 024:........................          0                         0
      IFCID 025:........................          0                         0
      IFCID 083:........................          0                         0
      IFCID 106:........................          5                         5
```

IFCID003

```
PRIMAUTH CONNECT  INSTANCE       END_USER     WS_NAME                        TRANSACT
ORIGAUTH CORRNAME CONNTYPE       RECORD TIME  DESTNO      IFC DESCRIPTION    DATA
PLANNAME CORRNMBR                TCB CPU TIME             ID
-------- -------- ------------ -------------------------- --- -------------- ------------------------
[redacted] SERVER   X'DA60AD6E8722' [redacted]       192.168.1.5                      db2jcc_application
         N/A      REMOTE       D 14:05:00     0000093611 003 DDF Data by Location
DISTSERV 'BLANK'                 00:00:32
   DDF DATA BY LOCATION
REMOTE LOCATION    COMMIT SENT
                   COMMIT RECEIVED
REQ.ELAPSED TIME   ROLLBK SENT
SER.ELAPSED TIME   ROLLBK RECEIVED
-----------------------------------
::FFFF:[redacted]        0000000000
                         4976710656
00:00:00                 4976710656
00:00:00                 4976710656
```

IFCID106

```
                                   SYSTEM INITIALIZATION PARAMETERS
WTO ROUTE CODES   : X'8000'  MONITOR BUFFER SIZE:  0001048576  AUDIT CLASSES: X'00000000'  EXT. SECURITY: NO
DATABASE PROTOCOL: D         UNICODE IFCIDS     :  NO
                                   MISCELLANEOUS INSTALLATION PARAMETERS
COMMON CRITERIA ENVIRON : NO          DDL REGISTRATION FLAG: X'30'       INSTALL SYSADM    : [redacted]     DEFAULT USERID    : [redacted]
SYSADM ID 2             : [redacted]  SITE TYPE            : LOCAL       SYSOPER ID        :                SYSOPER ID 2      : [redacted]
ENABLE DB2 AUTHORIZATION: YES         CACHE DYNAMIC SQL    : YES         AUTH. CACHE SIZE:  03072
PACK AUTH CACHE         :  0010485760 DBADM CREATE VIEW    : NO          EDM STMT CACHE    :  0000113386   ONL SYSPARM TYPE  : N/A
ONL SYSPARM CORID       :             ONL SYSPARM USER ID  :             ONL SYSPARM TIME: 08:26:40
SECURITY ADMIN 1 TYPE   : AUTH ID     SECURITY ADMIN 2 TYPE: AUTH ID     SECURITY TASKS    : SYSADM/SYSCTRL CAN GRANT/REVOKE
REVOKE DEP. PRIVILEGES  : NOT INCLUDING DEPENDENT PRIVILEGES
```

TRACE Limits

- Can be turned on and can be turned off (*)
- Records the after event/data
- Records first data access/change only
- Apply to audit tables only (*)
- Auxiliary tables can’t be audited

(*) Limitation are lifted with Audit Policies

Tamper-Proof Audit Policy – Db2 12 FL509

- Can be created by inserting into SYSIBM.SYSAUDITPOLICIES with **DB2START='T'**
- Started automatically during Db2 startup
- UPDATE or DELETE statements or STOP TRACE on such a policy require additional ESM authorization
  - RACF profile: DSNAUDIT.policy-name

Audit details in Db2 Log

Db2 Log

- Contains information required for recovery of program execution results and contents of a database
- Log consists of 3 main log record types:
  - “Unit of recovery” records that describe changes to Db2 objects
  - “Page set control” records that register allocation, opening, and closing of page sets
  - “System event” records that include Db2 command, begin/end of Db2 checkpoint, various summary information (UOR, pageset, pageset exception..), etc.
- Log datasets include Active logs, Archive logs and BSDS

Unit-Of-Recovery Log Records

- UR credentials
  - RBA/LRSN, connection name, correlation, auth ID, plan name, LUWID
- Redo/Undo details
  - DBID, PSID, RID, page number
  - Before and after row/column data
- Changed data
  - INSERT, DELETE – complete row
  - UPDATE – complete row only if DATA CAPTURE(CHANGES)

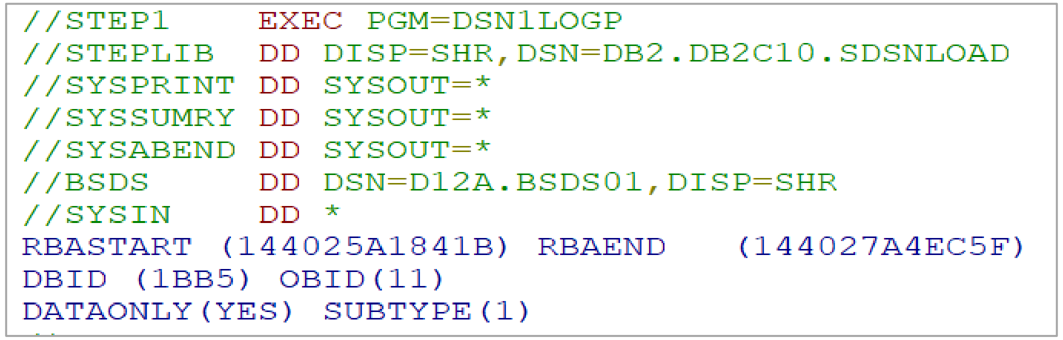
Db2 Log Auditing

- Db2 Catalog changes to identify DCL and DDL change events
  - CREATE / ALTER / DROP
  - GRANT / REVOKE
- Data changes
  - Who: connection name, correlation, auth ID, plan name, LUWID
  - When: timestamp and event sequence
  - What: undo/redo contents
- Db2 Commands

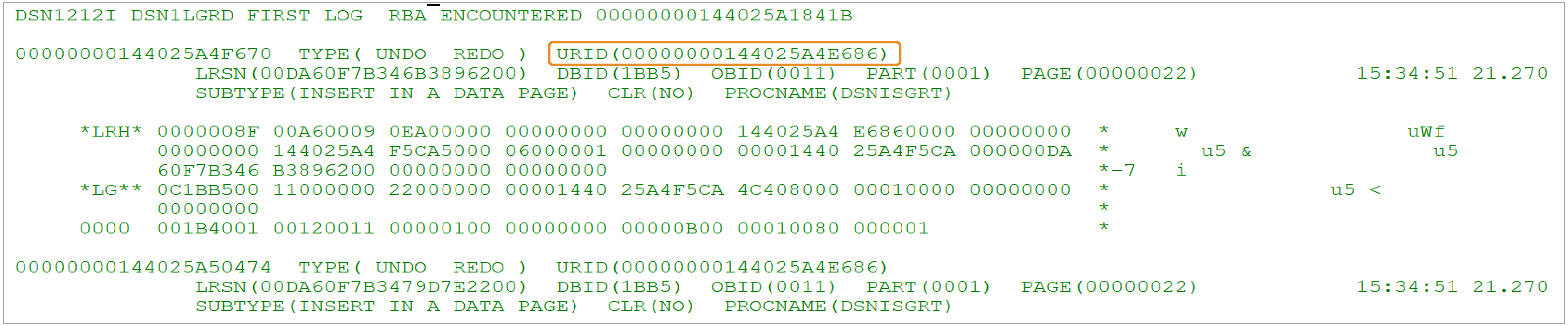
Log Reporting Tools: DSN1LOGP Utility

- Stand-alone utility to print out recovery log contents as
  - Detail report (individual log records)
  - Summary report
- Options:
  - Begin/end RBA, begin/end LRSN
  - DBID, OBID, Page number, RID, URID, LUWID
  - Record type/subtype
  - Etc.

Tooling : DSN1LOGP Utility – Detail report

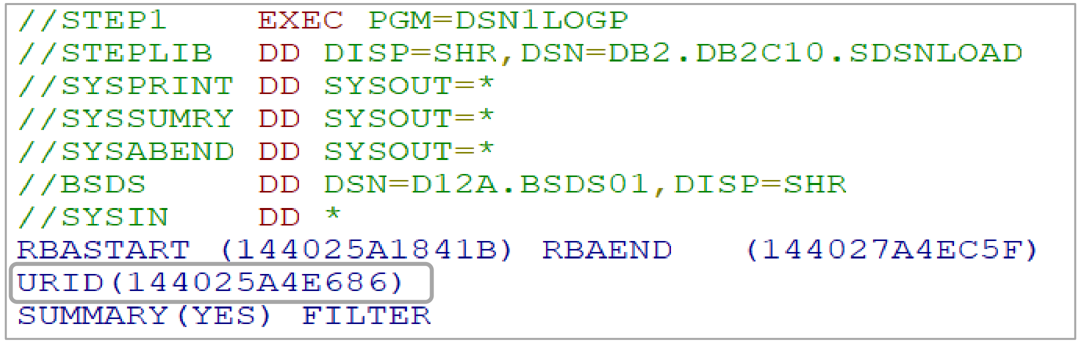


```
//STEP1     EXEC PGM=DSN1LOGP
//STEPLIB   DD DISP=SHR,DSN=DB2.DB2C10.SDSNLOAD
//SYSPRINT DD SYSOUT=*
//SYSSUMRY DD SYSOUT=*
//SYSABEND DD SYSOUT=*
//BSDS      DD DSN=D12A.BSDS01,DISP=SHR
//SYSIN     DD *
RBASTART (144025A1841B) RBAEND   (144027A4EC5F)
DBID (1BB5) OBID(11)
DATAONLY(YES) SUBTYPE(1)
```

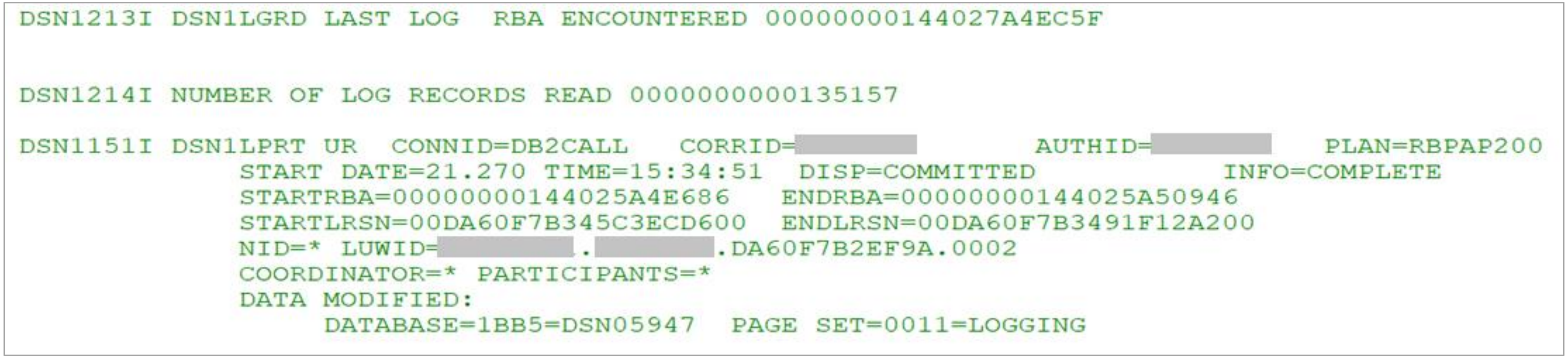


```
DSN1212I DSN1LGRD FIRST LOG   RBA ENCOUNTERED 00000000144025A1841B

00000000144025A4F670  TYPE( UNDO  REDO )  URID(00000000144025A4E686)
              LRSN(00DA60F7B346B3896200)  DBID(1BB5)  OBID(0011)  PART(0001)  PAGE(00000022)            15:34:51 21.270
              SUBTYPE(INSERT IN A DATA PAGE)  CLR(NO)  PROCNAME(DSNISGRT)

     *LRH* 0000008F 00A60009 0EA00000 00000000 00000000 144025A4 E6860000 00000000  *    w                 uWf
           00000000 144025A4 F5CA5000 06000001 00000000 00001440 25A4F5CA 000000DA  *      u5 &              u5
           60F7B346 B3896200 00000000 00000000                                       *-7  i
     *LG** 0C1BB500 11000000 22000000 00001440 25A4F5CA 4C408000 00010000 00000000  *                u5 <
           00000000                                                                  *
     0000  001B4001 00120011 00000100 00000000 00000B00 00010080 000001              *

00000000144025A50474  TYPE( UNDO  REDO )  URID(00000000144025A4E686)
              LRSN(00DA60F7B3479D7E2200)  DBID(1BB5)  OBID(0011)  PART(0001)  PAGE(00000022)            15:34:51 21.270
              SUBTYPE(INSERT IN A DATA PAGE)  CLR(NO)  PROCNAME(DSNISGRT)
```

Tooling : DSN1LOGP Utility – Summary report

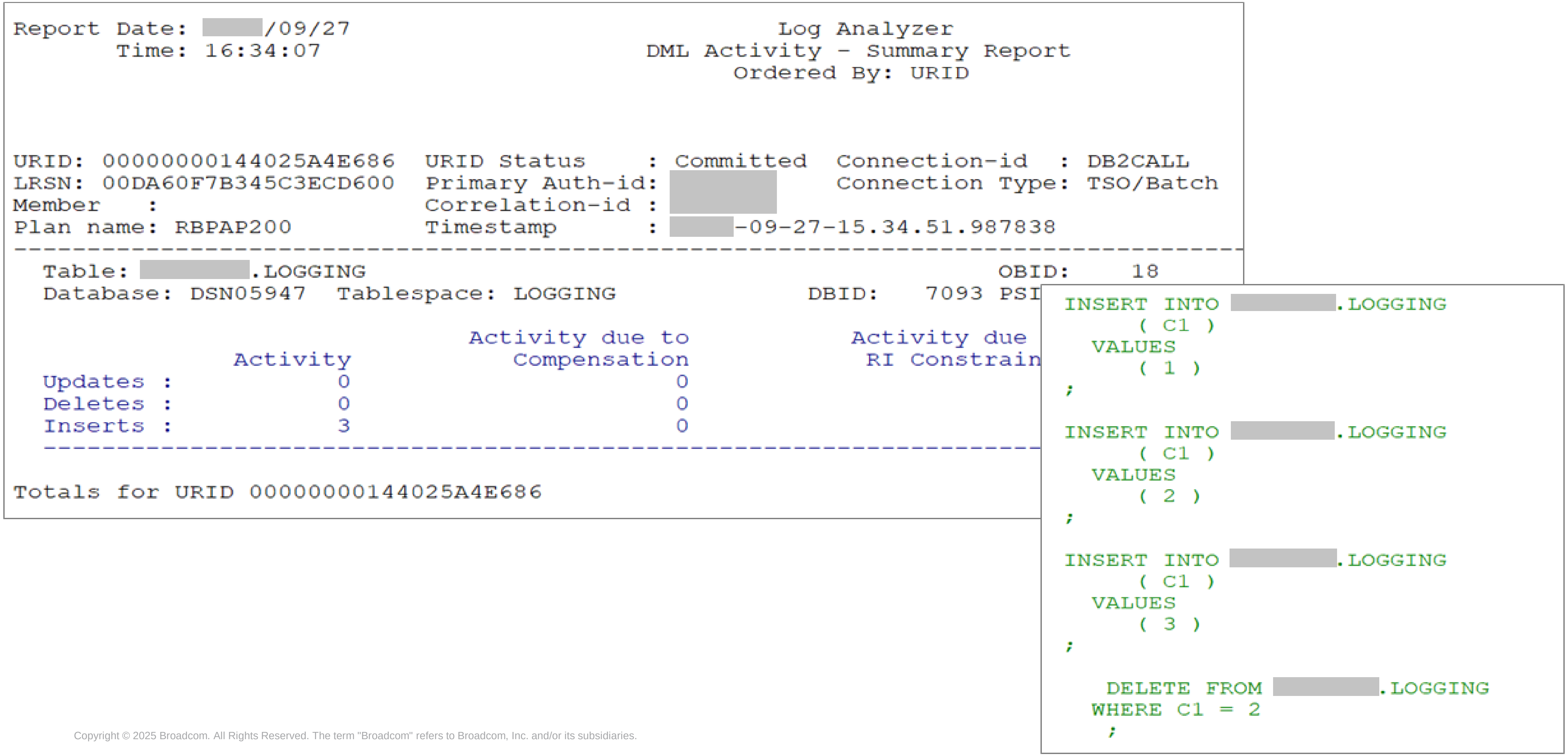


```
//STEP1      EXEC  PGM=DSN1LOGP
//STEPLIB    DD  DISP=SHR,DSN=DB2.DB2C10.SDSNLOAD
//SYSPRINT   DD  SYSOUT=*
//SYSSUMRY   DD  SYSOUT=*
//SYSABEND   DD  SYSOUT=*
//BSDS       DD  DSN=D12A.BSDS01,DISP=SHR
//SYSIN      DD  *
RBASTART  (144025A1841B)  RBAEND    (144027A4EC5F)
URID(144025A4E686)
SUMMARY(YES)  FILTER
```



```
DSN1213I DSN1LGRD LAST LOG  RBA ENCOUNTERED 00000000144027A4EC5F


DSN1214I NUMBER OF LOG RECORDS READ 0000000000135157

DSN1151I DSN1LPRT UR  CONNID=DB2CALL   CORRID=[redacted]        AUTHID=[redacted]     PLAN=RBPAP200
              START DATE=21.270 TIME=15:34:51  DISP=COMMITTED            INFO=COMPLETE
              STARTRBA=00000000144025A4E686   ENDRBA=00000000144025A50946
              STARTLRSN=00DA60F7B345C3ECD600  ENDLRSN=00DA60F7B3491F12A200
              NID=* LUWID=[redacted].[redacted].DA60F7B2EF9A.0002
              COORDINATOR=* PARTICIPANTS=*
              DATA MODIFIED:
                   DATABASE=1BB5=DSN05947  PAGE SET=0011=LOGGING
```

Tooling : Vendor Products (e.g. Log Analyzer)



```
Report Date: [redacted]/09/27                                    Log Analyzer
       Time: 16:34:07                                 DML Activity - Summary Report
                                                            Ordered By: URID



URID: 00000000144025A4E686  URID Status     : Committed  Connection-id   : DB2CALL
LRSN: 00DA60F7B345C3ECD600  Primary Auth-id: [redacted]   Connection Type: TSO/Batch
Member    :                 Correlation-id :
Plan name: RBPAP200         Timestamp      : [redacted]-09-27-15.34.51.987838
----------------------------------------------------------------------------------
  Table: [redacted].LOGGING                                         OBID:    18
  Database: DSN05947  Tablespace: LOGGING                   DBID:   7093 PSI

                                      Activity due to             Activity due
                      Activity         Compensation             RI Constrain
  Updates :                  0                       0
  Deletes :                  0                       0
  Inserts :                  3                       0
  ----------------------------------------------------------------------------

Totals for URID 00000000144025A4E686
```

```
INSERT INTO [redacted].LOGGING
     ( C1 )
  VALUES
     ( 1 )
;

INSERT INTO [redacted].LOGGING
     ( C1 )
  VALUES
     ( 2 )
;

INSERT INTO [redacted].LOGGING
     ( C1 )
  VALUES
     ( 3 )
;

   DELETE FROM [redacted].LOGGING
  WHERE C1 = 2
   ;
```

How about External Security?

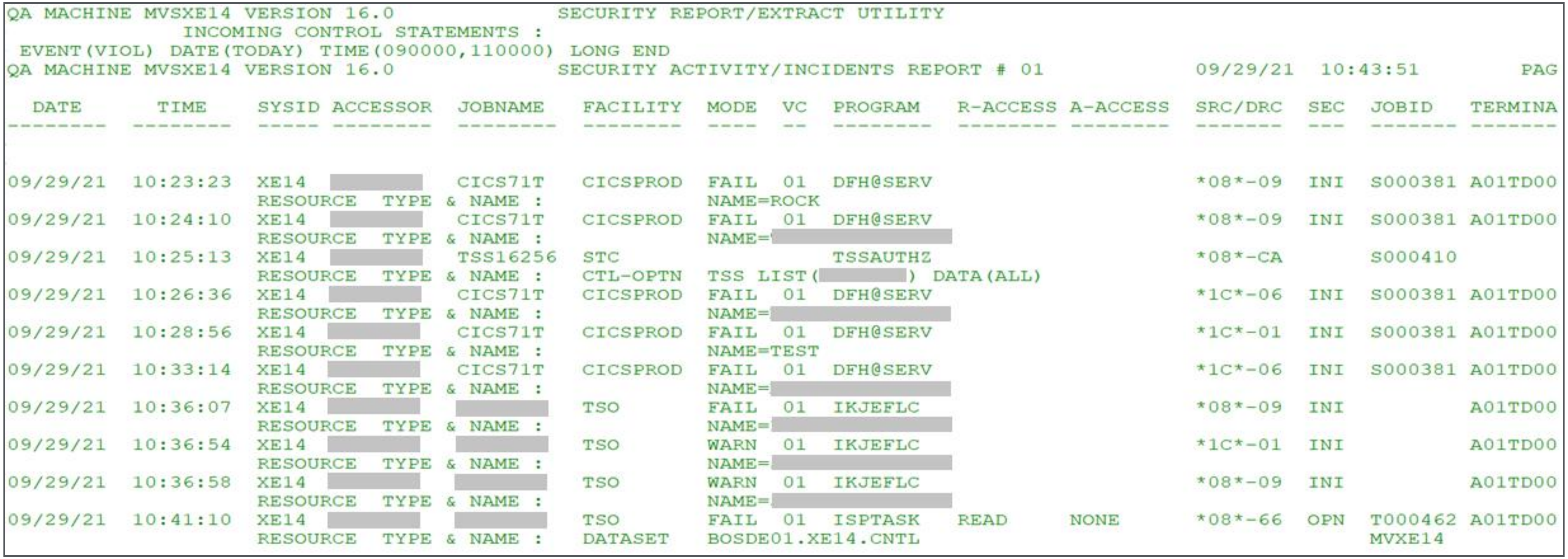
External Security

- Internal Db2 security can be replaced with an **External Security Manager** (ESM) control:
  - RACF, Top Secret, ACF2
- Mainframe **Security Administrators** grant security rights vs. Database Administrators
- Db2 access is handled through Db2 exit routines
- Audit is provided by the appropriate ESM solution
  - E.g. ACFRPTRV – ACF2’s resource event log and TSS’s TSSUTIL security-related activity report

Db2 External Security

- Assigning primary IDs, secondary IDs, and SQL IDs
  - **RACF** and **Top Secret** use 2 exit routines
    - **DSN3@ATH** – for connections (TSO, batch jobs, IMS control region, CICS recovery coordination task, RRSAF, DRDA, SNA..)
    - **DSN3@SGN** – for sign-ons (IMS requests, CICS transactions, SNA, etc.)
  - **ACF2** ships with own similar exit routines (**ACF3@ATH** and **ACF3SGN**)
- Authorizing access to Db2 resources
  - Each Db2 resource should be defined to ESM
  - **RACF** uses **DSNX@XAC** authorization exit routine (code in DSNXRXAC)
  - **TSS/ACF2** use their own intercept in Db2
    - CADB2XAC module for the DSNX@XAC exit is provided to prevent access to Db2 if the intercept is not installed
  - Not invoked for Installation SYSOPR or Installation SYSADM authority

Top Secret – TSSUTIL sample



```
QA MACHINE MVSXE14 VERSION 16.0             SECURITY REPORT/EXTRACT UTILITY
              INCOMING CONTROL STATEMENTS :
 EVENT(VIOL) DATE(TODAY) TIME(090000,110000) LONG END
QA MACHINE MVSXE14 VERSION 16.0             SECURITY ACTIVITY/INCIDENTS REPORT # 01            09/29/21  10:43:51         PAG

  DATE       TIME      SYSID ACCESSOR  JOBNAME    FACILITY  MODE  VC  PROGRAM   R-ACCESS A-ACCESS  SRC/DRC  SEC  JOBID   TERMINA
--------   --------    ----- --------  ---------  --------- ----  --  --------  -------- --------  -------  ---  ------- -------


09/29/21   10:23:23    XE14  [redacted] CICS71T   CICSPROD  FAIL  01  DFH@SERV                     *08*-09  INI  S000381 A01TD00
                       RESOURCE  TYPE & NAME :              NAME=ROCK
09/29/21   10:24:10    XE14  [redacted] CICS71T   CICSPROD  FAIL  01  DFH@SERV                     *08*-09  INI  S000381 A01TD00
                       RESOURCE  TYPE & NAME :              NAME=[redacted]
09/29/21   10:25:13    XE14  [redacted] TSS16256  STC                 TSSAUTHZ                     *08*-CA       S000410
                       RESOURCE  TYPE & NAME :    CTL-OPTN  TSS LIST([redacted]) DATA(ALL)
09/29/21   10:26:36    XE14  [redacted] CICS71T   CICSPROD  FAIL  01  DFH@SERV                     *1C*-06  INI  S000381 A01TD00
                       RESOURCE  TYPE & NAME :              NAME=[redacted]
09/29/21   10:28:56    XE14  [redacted] CICS71T   CICSPROD  FAIL  01  DFH@SERV                     *1C*-01  INI  S000381 A01TD00
                       RESOURCE  TYPE & NAME :              NAME=TEST
09/29/21   10:33:14    XE14  [redacted] CICS71T   CICSPROD  FAIL  01  DFH@SERV                     *1C*-06  INI  S000381 A01TD00
                       RESOURCE  TYPE & NAME :              NAME=[redacted]
09/29/21   10:36:07    XE14  [redacted] [redacted] TSO      FAIL  01  IKJEFLC                      *08*-09  INI          A01TD00
                       RESOURCE  TYPE & NAME :              NAME=[redacted]
09/29/21   10:36:54    XE14  [redacted] [redacted] TSO      WARN  01  IKJEFLC                      *1C*-01  INI          A01TD00
                       RESOURCE  TYPE & NAME :              NAME=[redacted]
09/29/21   10:36:58    XE14  [redacted] [redacted] TSO      WARN  01  IKJEFLC                      *08*-09  INI          A01TD00
                       RESOURCE  TYPE & NAME :              NAME=[redacted]
09/29/21   10:41:10    XE14  [redacted] [redacted] TSO      FAIL  01  ISPTASK   READ     NONE      *08*-66  OPN  T000462 A01TD00
                       RESOURCE  TYPE & NAME :    DATASET   BOSDE01.XE14.CNTL                                    MVXE14
```

BROADCOM
MAINFRAME SOFTWARE

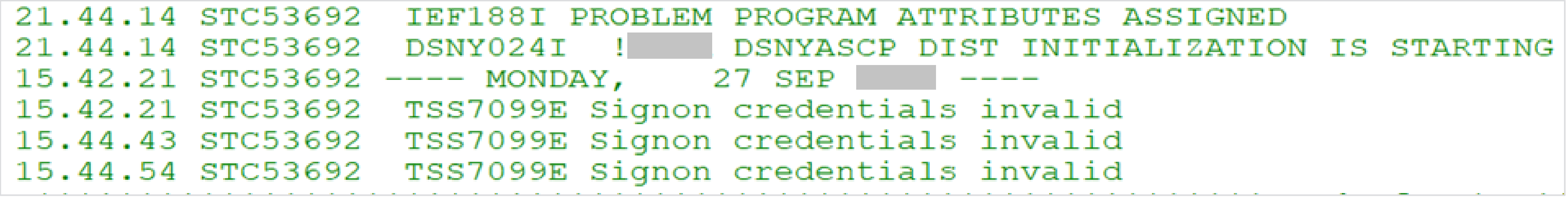
Other Audit Data Sources

More TRACEs

- SQL execution details
  - IFCID 62 – DDL execution
  - IFCID 58 – SQL execution complete
  - IFCID 247 – Input HOST variables
- Db2 commands
  - IFCID 90/91
- System parameters
  - IFCID 106
- Trace start/stop
  - IFCID 4 & 5 – TRACE command text

JES Messages

- MSTR address space
  - Db2 system parameters, commands and messages
- DBM1 address space
  - Db2 dataset messages
- DIST address space
  - Remote connection failures and access denials



```
21.44.14 STC53692  IEF188I PROBLEM PROGRAM ATTRIBUTES ASSIGNED
21.44.14 STC53692  DSNY024I  ![redacted] DSNYASCP DIST INITIALIZATION IS STARTING
15.42.21 STC53692 ---- MONDAY,     27 SEP [redacted] ----
15.42.21 STC53692  TSS7099E Signon credentials invalid
15.44.43 STC53692  TSS7099E Signon credentials invalid
15.44.54 STC53692  TSS7099E Signon credentials invalid
```

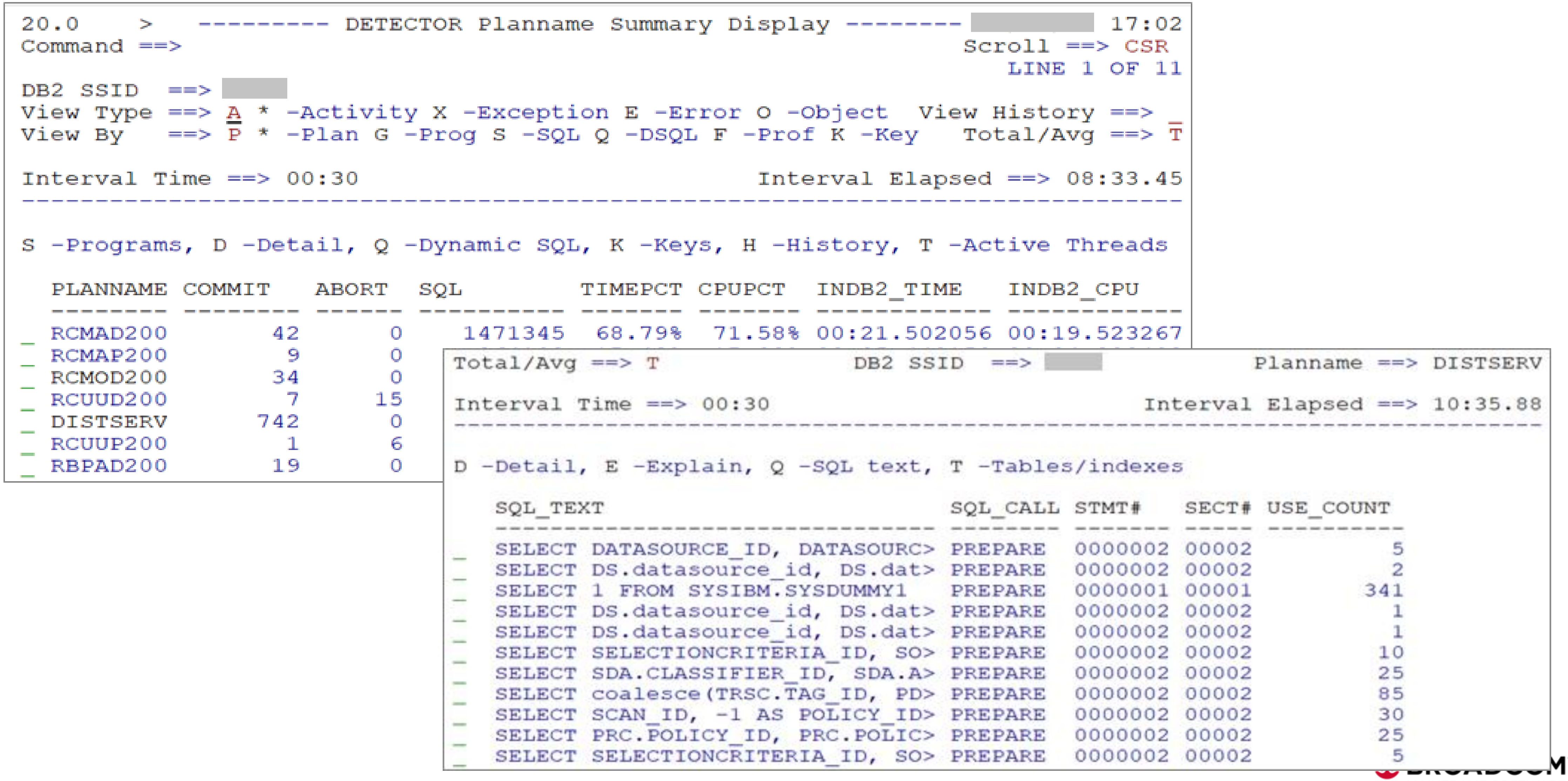
Db2 Commands

- DISPLAY THREAD
  - Provides details for active threads and users
- DISPLAY LOCATION
  - Provides details of remote locations
- DISPLAY DATABASE
  - Lists Db2 objects and their states
- DISPLAY TRACE
  - Lists activated Db2 traces
- DISPLAY UTILITY
  - Provides details of Db2 utility jobs

SQL and I/O Monitors

- Monitor and collect SQL execution details:
  - Plan name, program name, auth ID, etc.
  - SQL text, number, ID, etc.
  - Performance statistics
- Intercept every SQL statement and/or a Getpage
- Allow offloading collected details into Db2 performance warehouse database
- Vendor products
  - Detector, Subsystem Analyzer, Query Monitor, Apptune, etc.

Detector for Db2 for z/OS



```
20.0     >   --------- DETECTOR Planname Summary Display --------- [redacted] 17:02
Command ==>                                                        Scroll ==> CSR
                                                                     LINE 1 OF 11
DB2 SSID  ==> [redacted]
View Type ==> A * -Activity X -Exception E -Error O -Object  View History ==> _
View By   ==> P * -Plan G -Prog S -SQL Q -DSQL F -Prof K -Key   Total/Avg ==> T

Interval Time ==> 00:30                               Interval Elapsed ==> 08:33.45
-------------------------------------------------------------------------------

S -Programs, D -Detail, Q -Dynamic SQL, K -Keys, H -History, T -Active Threads

  PLANNAME COMMIT   ABORT  SQL        TIMEPCT CPUPCT  INDB2_TIME   INDB2_CPU
  -------- -------- ------ ---------- ------- ------- ------------ -----------
_ RCMAD200       42      0    1471345  68.79%  71.58% 00:21.502056 00:19.523267
_ RCMAP200        9      0
_ RCMOD200       34      0
_ RCUUD200        7     15
_ DISTSERV      742      0
_ RCUUP200        1      6
_ RBPAD200       19      0
```

```
Total/Avg ==> T                DB2 SSID   ==> [redacted]          Planname ==> DISTSERV

Interval Time ==> 00:30                                    Interval Elapsed ==> 10:35.88
-----------------------------------------------------------------------------------------

D -Detail, E -Explain, Q -SQL text, T -Tables/indexes

   SQL_TEXT                         SQL_CALL STMT#   SECT# USE_COUNT
   -------------------------------- -------- ------- ----- ---------
_  SELECT DATASOURCE_ID, DATASOURC> PREPARE  0000002 00002         5
_  SELECT DS.datasource_id, DS.dat> PREPARE  0000002 00002         2
_  SELECT 1 FROM SYSIBM.SYSDUMMY1   PREPARE  0000001 00001       341
_  SELECT DS.datasource_id, DS.dat> PREPARE  0000002 00002         1
_  SELECT DS.datasource_id, DS.dat> PREPARE  0000002 00002         1
_  SELECT SELECTIONCRITERIA_ID, SO> PREPARE  0000002 00002        10
_  SELECT SDA.CLASSIFIER_ID, SDA.A> PREPARE  0000002 00002        25
_  SELECT coalesce(TRSC.TAG_ID, PD> PREPARE  0000002 00002        85
_  SELECT SCAN_ID, -1 AS POLICY_ID> PREPARE  0000002 00002        30
_  SELECT PRC.POLICY_ID, PRC.POLIC> PREPARE  0000002 00002        25
_  SELECT SELECTIONCRITERIA_ID, SO> PREPARE  0000002 00002         5
```

“Special” Db2 Tables

- Db2 table history can be preserved with Temporal and Archive tables
- Temporal Tables
  - Record the period of time when a row is valid
  - Types: System-period and Application-period
  - In case of system-period, previous row versions (after update/delete) are stored in a history table
- Archive Tables
  - Contains row deleted from the base table
- Db2 13 FL505 introduced support for most of security-related Db2 catalog tables (system-period)

Summary and Q&A

Highlights

- Db2 Catalog provides audit information “at rest”
  - Run queries against the catalog tables to report on who has access to what. Consider enabling the temporal history tables
- IFCID traces provide audit information “at motion”
  - Collect and report on security events – who did what and when
- Audit policies give a better way to handle IFCID traces
- Db2 Log complements audit data and contains every update
- In case of external security, rely on ESM reports
  - But use IFCID 361 audit Installation SYSADM/SYSOPR
- More audit data is available

References

- Db2 for z/OS: Managing Security
  - https://www.ibm.com/support/knowledgecenter/SSEPEK_12.0.0/pdf/db2z_12_secabook.pdf
- Db2 for z/OS: Auditing Access
  - https://www.ibm.com/docs/en/db2-for-zos/12?topic=facilities-auditing-access-db2
- CA Top Secret Option for Db2
  - https://techdocs.broadcom.com/us/en/ca-mainframe-software/security/ca-top-secret-option-for-db2/1-3.html

BROADCOM®
MAINFRAME SOFTWARE

Thank you

Denis Tronin | Product Manager
denis.tronin@broacom.com