IDUG

2024 NA Db2 Tech Conference

Considerations for Migrating Db2 Security to RACF

Ray Overby roverby@rocketsoftware.com

Jørn Thyssen jthyssen@rocketsoftware.com

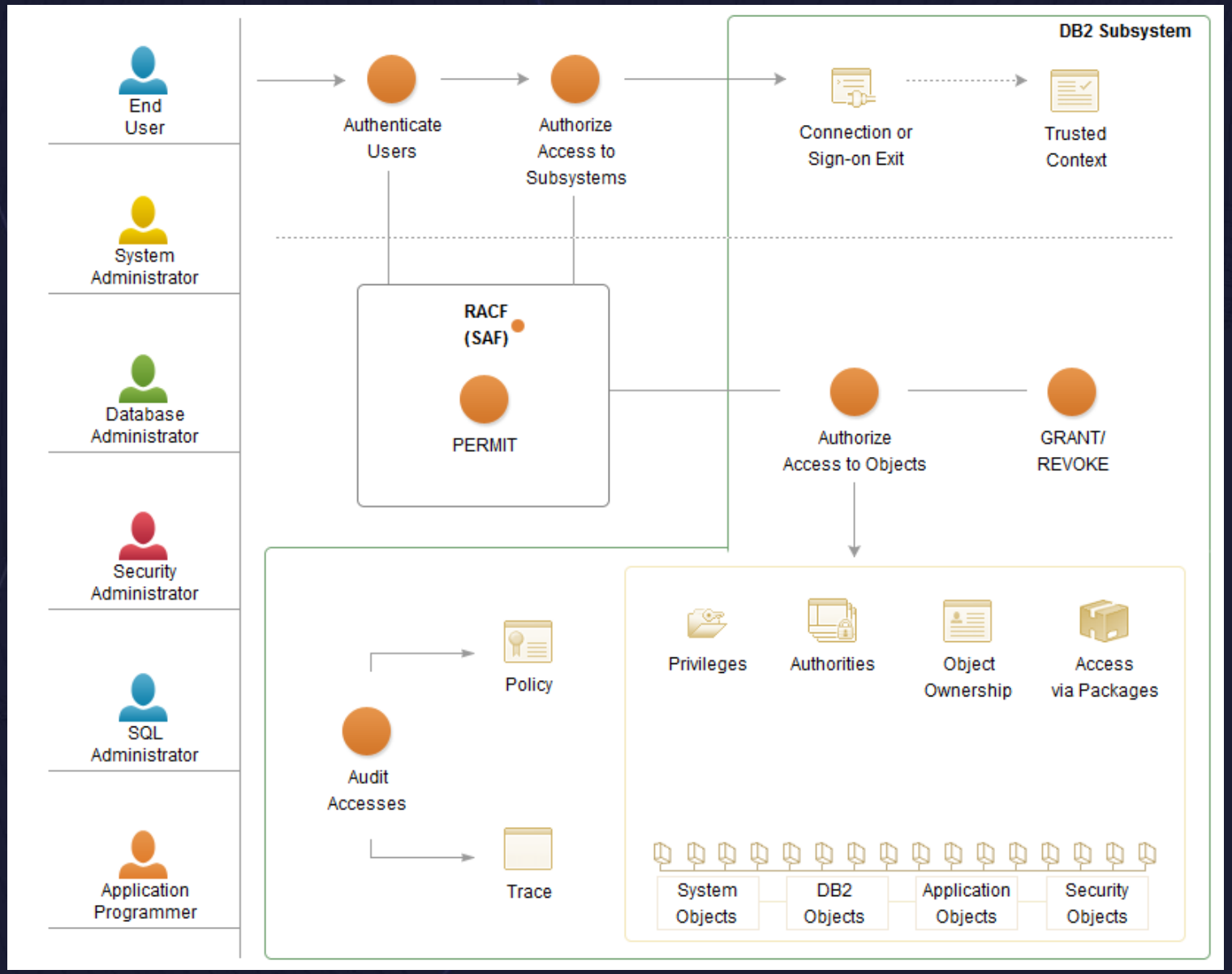
Rocket Software

Session Code: SEC2 | Platform: z/OS

Agenda

- Native Db2 Security
- Why use RACF for Db2 security
- Migration process to convert to RACF security
- Best practices for your Db2 security
- Helpful tools to use when using RACF security

Db2 security



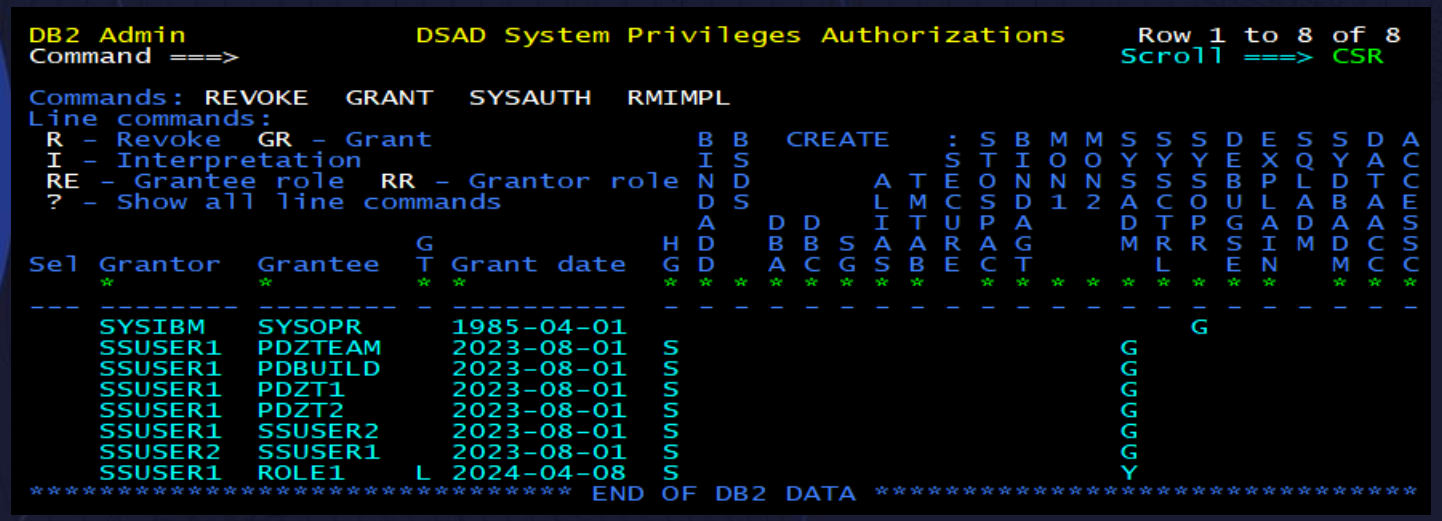
https://www.ibm.com/docs/en/db2-for-zos/13?topic=securing-db2

Db2 native security

- Original implementation
  - In effect if DSNZPARM SECURE=YES
- Managed through GRANTs and REVOKEs
- Stored in 13 SYSIBM.SYSxxxxAUTH tables
  - System level privileges, object level privileges, column privileges, …
  - https://www.ibm.com/docs/en/db2-for-zos/12?topic=catalog-tables-privilege-records
- Security managed by SYSADM, SYSCTRL, ACCESSCTRL, install SECADM
  - or users with WITH GRANT option or ownership of object or …
- Db2 z/OS V10 introduced SEPARATE_SECURITY
  - Prevents SYSADM and SYSCTRL from issuing GRANT/REVOKE

Db2 native security

- Db2 Vendor tools all support native security



Db2 native security

- A couple of vendors have built capabilities to do RACF-like administration of native Db2 security
  - Set-up desired auth through users, roles, objects, applications with wildcard support & optional expiry
  - GRANT/REVOKE auth in Db2 based on desired auths

```
ADB2ZGPP  ------------- DD1A GM - Manage Pending Privileges   Row 1 to 13 of 29
Command ===>                                                   Scroll ===> PAGE
                                                                      More: >
Commands: CLEANUP  DELETE  RUN  DISFAILED
Line commands:
 C - Cleanup  D - Delete  G - Group  GP - Group privilege  I - Interpret
 P - Privilege  R - Run  S - SSID  ? - Show all line commands

Sel AUTHID    R Group Name        Privilege Name     P Statement
    *         * *                 *                  * *
--- -------> - ---------------> ---------------> - ------------------------->
    TS5500      APP01             READTAB            N GRANT SELECT,UNLOAD ON TABLE
    TS5500      APP01             READTAB            N GRANT SELECT,UNLOAD ON TABLE
    TS5500      APP01             READTAB            N GRANT SELECT,UNLOAD ON TABLE
    TS5500      APP01             READTAB            N GRANT SELECT,UNLOAD ON TABLE
    TS5100      APP01             UPDATETAB          Y GRANT DELETE,INSERT,UPDATE O
    TS5100      APP01             UPDATETAB          Y REVOKE DELETE,INSERT,UPDATE
    TS5100      APP01             UPDATETAB          Y GRANT DELETE,INSERT,UPDATE O
    TS5100      APP01             UPDATETAB          Y REVOKE DELETE,INSERT,UPDATE
    TS5100      APP01             UPDATETAB          Y GRANT DELETE,INSERT,UPDATE O
    TS5100      APP01             UPDATETAB          Y REVOKE DELETE,INSERT,UPDATE
    TS5100      APP01             UPDATETAB          Y GRANT DELETE,INSERT,UPDATE O
    TS5100      APP01             UPDATETAB          Y REVOKE DELETE,INSERT,UPDATE
    TS5770      APP01             EXECPRIV           N GRANT EXECUTE ON FUNCTION AD
```

Why use RACF for Db2 security – Organizational benefits

- Who is performing Db2 security now?
  - Db2 systems programmers or DBAs
  - Security is not their primary function
- Support for ESM based security was added to Db2 V6 as an alternative to Db2 native security

Why use RACF for Db2 security – Organizational benefits

- Moving Db2 security from where it is today to mainframe security
  - Primary responsibility is Security and Compliance
  - Adherence to security principles
    - Individual accountability
    - Auditability
    - Separation of function
    - Least privilege
- May satisfy an audit requirement
- Align Db2 security with all other mainframe resources

Why use RACF for Db2 security – Technical advantages

- There are several technical advantages
- But: Db2 for z/OS engine and vendor tooling have delivered features and enhancements to reduce this

Why use RACF for Db2 security – Technical advantages

- Security rules are defined outside Db2 in a single system (RACF)
  - Multiple Db2 subsystems can be protected by the same RACF
  - Db2 subsystem does not need to be started to query auth
- Rules can be defined before object exist
  - Also possible with tools that add RACF-like administration of Db2 native security
- Rules persist when an object is dropped
  - Db2 vendor tools supports recreating native authorizations, e.g.,
    - for complex Db2 changes that require drop/recreate
    - Recovery of dropped objects

Why use RACF for Db2 security – Technical advantages

- Eliminates revoke of dependent privileges when a privilege is revoked from a Db2 user
  - Db2 now has ZPARM REVOKE_DEP_PRIV=YES|NO|SQLSTMT
  - for REVOKE_DEP_PRIV=SQLSTMT:
    - REVOKE … NOT INCLUDING DEPENDENT PRIVILEGES
- A single rule can cover multiple objects
  - RACF Generics (wildcards)
  - RACFVARS
  - Grouping class profiles

Differences between RACF and native Db2 security – some highlights

- Long list of differences and considerations https://www.ibm.com/docs/en/db2-for-zos/13?topic=module-special-considerations
- Implicit databases
  - RACF only checks for access against DSNDB04
- Updatable views
- Ownership privileges still apply
- Grants are still possible
- Db2 object names with special characters, blanks, or mixed case
  - Default RACF classes do not allow mixed case
- Db2 objects with long names
- … review the doc to see if any of these apply to you

Conversion to RACF security

- Step 1 – optional, but recommend: Review and cleanup
- Step 2 – prepare and customize Db2 RACF exit
- Step 3 – Loop: Define, protect, activate, and test
  - Step 3A – define RACF classes
  - Step 3B – define RACF resources to protect Db2 objects and privileges
  - Step 3C – activate and refresh classes
  - Step 3D – restart Db2
  - Step 3E – test & debug
- Step 4 – revoke grants

Review and cleanup

- Optional, but highly recommend
  - Can reduce conversion work significantly
- Review local modifications to Db2 sign-on exit
- Review who have install SYSADM, SYSOPR, SECADM, or high-level database management privileges
- Grants “WITH GRANT OPTION” – won’t translate properly to RACF
  - … and you probably don’t want to translate them
    - Partially defeats the purpose of migrating to RACF security

Review and cleanup, cont’ed

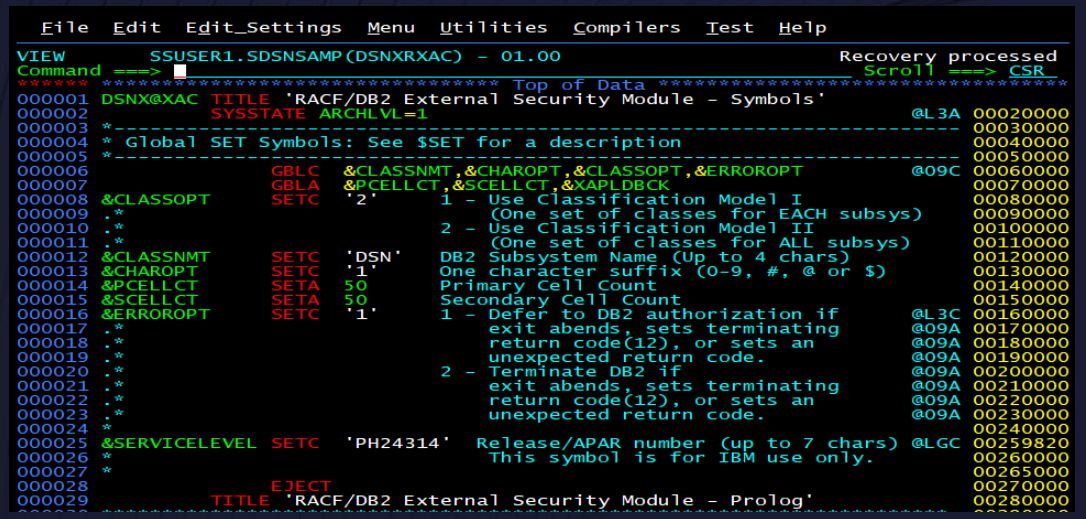
- Grants to PUBLIC
  - will translate to RACF UACC(READ)
  - Auditors don’t like UACC >= READ
- Look for orphaned grants where GRANTEE does not exist in RACF
  - REVOKE
- Look for orphaned objects where owner does not exist in RACF
  - TRANSFER OWNERSHIP

Prepare and customize Db2 RACF exit

- RACF exit source code: DSNXRXAC in hlq.SDSNSAMP
- Assemble and link: Step 3 (JEX0003) in DSNTIJEX
  - Creates load module DSNX@XAC
- Have a copy of both versions of DSNX@XAC so you can switch between native and RACF security easily

- Have processes in place to review and deploy updates to DSNXRXAC delivered through Db2 maintenance or new Db2 versions

Db2 RACF exit options



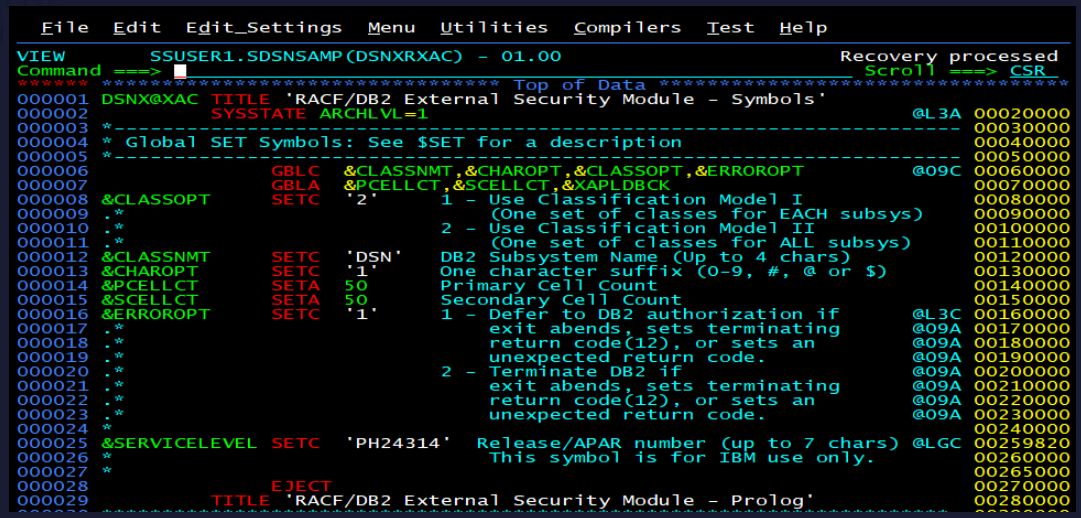
- &CLASSOPT - scope
  - 1 – single-subsystem scope
    - The class names identify with the SSID, e.g., class name M<ssid>TB1
  - 2 – multiple-subsystem scope
    - Same class is used for all Db2s; resource name includes the SSID
      - Example: class name MDSNTB, resource name <ssid>.*<something>*

- Considerations:
  - Centralized security team
  - Number of classes
  - POSITs
  - Class sizes
  - Class options, e.g., ASIS
  - Class refresh disruptiveness

For DSGs the group attach name is used

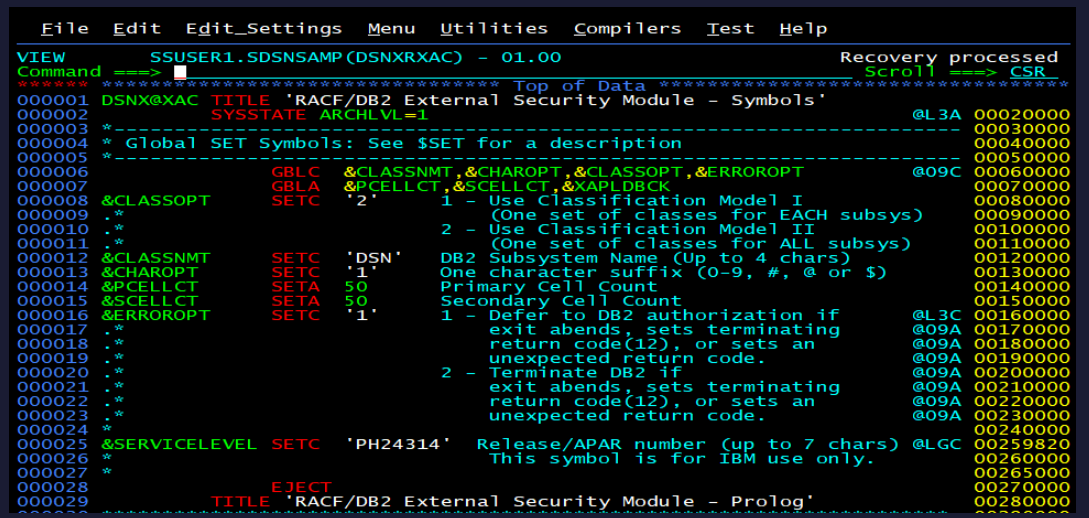
Db2 RACF exit options, cont'ed

- &CLASSNMT (for &CLASSOPT=2 only) – class name root
  - Default is DSN, e.g., M**DSN**TB
- &CHAROPT (ignored for &CLASSMNT=DSN) – class name suffix
  - Default is 1: M<ssid>TB1



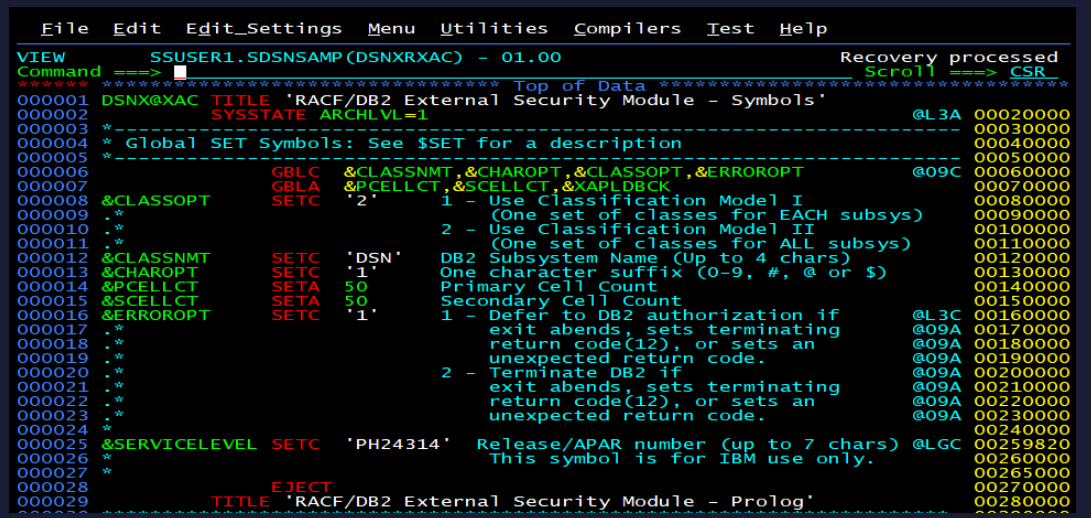
Db2 RACF exit options, cont’ed

- &ERROROPT – error option
  - What to do if exit initialization fails, unexpected return codes during authorization checking, or if # abends exceed “AUTH EXIT LIMIT”
  - 1 – fallback to Db2 native auth
  - 2 – stop Db2
- &PCELLCT, &SCELLCT – work cells



Db2 RACF exit modifications?

- Is possible, but we recommend against it
- Use cases:
  - Create new Db2 authorizations tailored to organization
    - Example: R/O access to all tables



Relevant Db2 DSNZPARMs

- AUTHEXIT_CHECK
  - ”DB2” – use package owner for autobind, BIND, and REBIND instead of primary auth id
  - ”PRIMARY” (default)
- AUTHEXIT_CACHEREFRESH
  - ”ALL” – Db2 refreshes the internal plan and package auth cache, routine auth cache, and DSC when user profile or resource access is changed in RACF
    - Listens to type 62, 71 and 79 ENF signals from RACF
    - Does not support RACFVARS
  - ”NONE” (default)
    - Can lead to incorrect access to objects
- AEXITLIM
  - Number of abends before security exit shuts down
  - Default is 10

Big bang or piecemeal?

- Db2 supports RACF and native security concurrently
  - Actually, you can't turn off native security …
  - Declined: https://ibm-data-and-ai.ideas.ibm.com/ideas/DB24ZOS-I-443
- If the RACF exit is active, but a class is not active, or the class is active, but the resource is not defined
  - Fallback to Db2 native security
  - Also: auth exit failures
- Allows both big bang and piecemeal conversion

Big bang or piecemeal?

- Example: start with administrative privileges DSNADM and MDSNSM; then move on to object specific classes
- Example
  - Piecemeal for lower environments while gaining experience
  - Big bang for higher environments to reduce conversion time

Define RACF classes

- Classes predefined in RACF for &CLASSOPT=2 + &CLASSMNT=DSN but need to be activated

Admin	Grouping classes		Member classes	
DSNADM	GDSNBP	GDSNSG	MDSNBP	MDSNSG
	GDSNCL	GDSNSM	MDSNCL	MDSNSM
	GDSNDB	GDSNSP	MDSNDB	MDSNSP
	GDSNJR	GDSNSQ	MDSNJR	MDSNSQ
	GDSNPK	GDSNTB	MDSNPK	MDSNTB
	GDSNPN	GDSNTS	MDSNPN	MDSNTS
	GDSNSC	GDSNUF	MDSNSC	MDSNUF
		GDSNUT		MDSNUT

DSNR checking not affected by conversion

Defining resources

- Mapping all objects to resources 1:1 will be very inefficient
  - will lead to definition of 100k or even millions of resources
  - Will negatively impact RACF performance
  - SETROPTS … REFRESH will be too disruptive
  - Will negatively impact managing security
  - Add multiple member profiles to grouping class profile
  - Use generic profiles if all grants map to a single level of access
  - Create RACF groups for multiple users with same access level and permit group instead of users

Back-stop profiles & warning

- <ssid>.** or ** with UACC(NONE)
  - Will prevent Db2 from falling back to Db2 security if a resource is undefined
- You can define profiles with RDEFINE … WARNING on sandbox
  - This will allow access, but issue ICH408I

Audit considerations

- Define administrative resources in classes DSNADM and MDSNSM with AUDIT(ALL)
- Define other resources with AUDIT(FAILURES)
- Consider audit record volumes if you use AUDIT(ALL) for other objects
  - You can restrict AUDIT(ALL) to resources for I/U/D or DDL activity

Activate and refresh classes

- Activate the class in RACF
  - Class must be RACLIST’ed
- Refresh class

Start Db2 with RACF exit

- Stop Db2
- Copy the RACF exit to your SDSNEXIT library
- Restart Db2
- Look for IRR9xx on SYSLOG

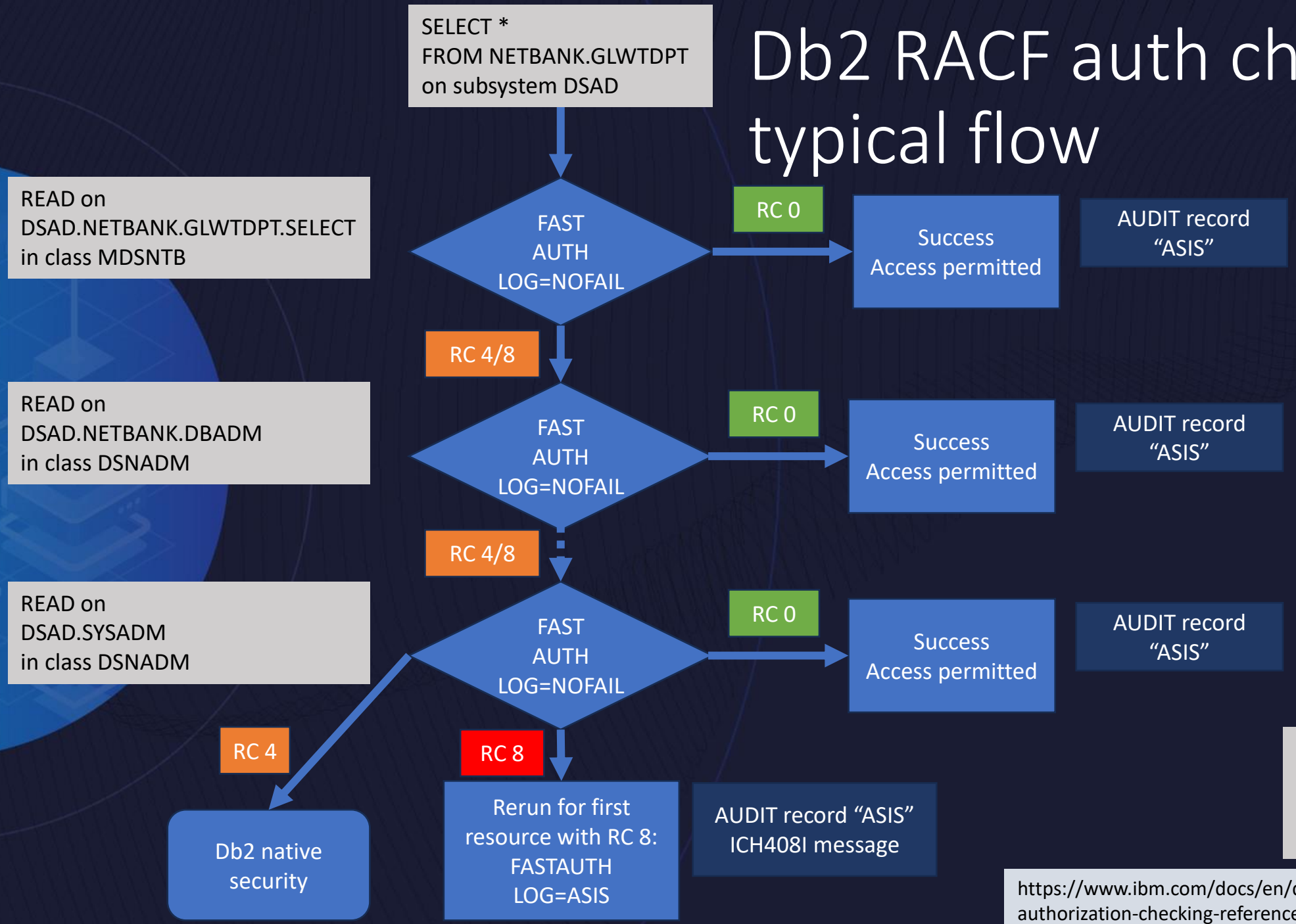
```
IRR908I RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2 SUBSYSTEM DSAD HAS
        A MODULE VERSION OF PH24314  AND A MODULE LENGTH OF 00007EA0.
IRR909I RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2 SUBSYSTEM DSAD
        IS USING OPTIONS: &CLASSOPT=2
                          &CLASSNMT=DSN
                          &CHAROPT=1
                          &ERROROPT=1
                          &PCELLCT=50
                          &SCELLCT=50
```

https://www.ibm.com/docs/en/db2-for-zos/13?topic=module-db2-racf-access-control-messages

```
IRR910I RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2
SUBSYSTEM DSAD
        INITIATED RACLIST FOR CLASSES:
         MDSNDB   MDSNPK   MDSNPN   MDSNBP   MDSNCL
         MDSNTS   MDSNSG   MDSNTB   MDSNSM   MDSNSC
         MDSNUT   MDSNUF   MDSNSP   MDSNJR   MDSNSQ
         MDSNGV   DSNADM
```

```
IRR911I RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2
SUBSYSTEM DSAD
        SUCCESSFULLY RACLISTED CLASSES:
         MDSNDB   MDSNPK   MDSNPN   MDSNBP   MDSNCL
         MDSNTS   MDSNSG   MDSNTB   MDSNSM   MDSNSC
         MDSNUT   MDSNUF   MDSNSP   MDSNJR   MDSNSQ
         MDSNGV   DSNADM
IRR916I RACF/DB2 EXTERNAL SECURITY MODULE WAS ASSEMBLED
WITH AN HRF7730 OR LATER MACRO LIBRARY.
ROLES AS RACF CRITERIA ARE SUPPORTED.
```

Db2 RACF auth checking – typical flow



https://www.ibm.com/docs/en/db2-for-zos/13?topic=module-racf-authorization-checking-reference

Debugging

- Db2 trace IFCID 314 – Authorization Exit Parameters
  - -START TRACE(PERF) CLASS(22)
  - If you turn on IFCID 410 a record is only cut for RC 04
  - You get one record per access attempt
- Db2 trace IFCID 140 – Audit Auth Failures
  - -START TRACE(AUDIT) CLASS(1)
- RACF SMF80 records
- IBM SAF trace (GTF) or equivalent vendor tooling
- Modify exit

Debugging – IFCID 314 Auth exit parameters

- User SSUSER6 attempt to run SQL: SELECT * FROM NETBANK.GLWDPT

```
EXIT RETURN CODE:                    8
EXIT REASON CODE:                    0
```

```
AUTH ID                          : SSUSER6
UNQUALIFIED OBJECT NAME: GLWTDPT
OBJECT OWNER                     : NETBANK
RELATED INFO 1                   :   NETBANK   NETBANK
RELATED INFO 2                   : NETBANK
```

```
SSUSER6  TSO
SSUSER6  SSUSER6                                                    AME:  DSADDB2   LUWSEQ:    6
ADB      'BLANK'          N/P                EXIT PARM
|-------------------------------------------------------------------------------------------------
|ADDRESS EXPL     : X'7E96CAD8'   EXIT RETURN CODE:        8   STO CLOCK BEFORE EXIT CALL: 05/03/24 08:50:10.207630
|ADDRESS WORK AREA: X'7EA38000'   EXIT REASON COD
|AUTH ID                : SSUSER6
|UNQUALIFIED OBJECT NAME: GLWTDPT
|OBJECT OWNER           : NETBANK
|RELATED INFO 1         :   NETBANK   NETBANK
|RELATED INFO 2         : NETBANK
|LENGTH WORK AREA :       4096
|ACEE UTOKEN      : &     {
|PARAMETER LIST   :
|0000  216A0100  E7C1D7D3  E5F1F3D9  F1D4F540  D
|0020  008FB770  E2E2E4E2  C5D9F640  0002C4E2  C
|0040  7E96DC92  7E96DD14  00000000  7E96CC20  O
|0060  00000000  00000000  00000000  00000000  00000000  000000E5  F1F3D9F1  D4F5F0F3  |.....V13R1M503
|0080  40000000  00000000  00000000  00000000  00000000  00000000  00000000  00000000  |
|00A0  00404000  00000000  00000000  00004010  08080004  04040000  04040000  04040000  |
|00C0  00000000  00000000  00000000  00000000  00000000  00000000  00000000  00000000  |
|00E0  00000000  00000000  00000000  00000000  00000000  00000000  00000000  00000000  |
|.....
|-------------------------------------------------------------------------------------------------
```

```
.¦..XAPLV13R1M5  ..j..8V.....
...nSSUSER6 ..DSAD    .....T}=o..
=o.k=o.....=o.....=o.o.....
.....V13R1M503
```

Debugging – IFCID 140 Audit Auth failures

- User SSUSER6 attempt to run SQL: SELECT * FROM NETBANK.GLWDPT

```
   LOCATION: SSO1DSAD                    IBM OMEGAMON FOR DB2 PERFORMANCE EXPERT (V5R5M0)          PAGE: 1-2
      GROUP: N/A                              RECORD TRACE - SHORT                    REQUESTED FROM: NOT SPECIFIED
     MEMBER: N/A                                                                              TO: NOT SPECIFIED
  SUBSYSTEM: DSAD                                                                    ACTUAL FROM: 05/03/24 08:49:53.18
DB2 VERSION: V13                                                                       PAGE DATE: 05/03/24
PRIMAUTH CONNECT    INSTANCE      END_USER       WS_NAME                          TRANSACT
ORIGAUTH CORRNAME   CONNTYPE      RECORD TIME    DESTNO ACE IFC  DESCRIPTION      DATA
PLANNAME CORRNMBR                 TCB CPU TIME             ID
-------- -------- ---------- ---------------- ------ --- --- -------------- ----------------------------------------
SSUSER6  TSO      DF0990F37DF9 SSUSER6          TSO                          SSUSER6
SSUSER6  SSUSER6  TSO          08:50:10.20843146      8   2 140 AUDIT AUTH     NETWORKID:  ROCKNET1  LUNAME:  DSADDB2   LUWSEQ:     6
ADB      'BLANK'               N/P                                FAILURES
         |-------------------------------------------------------------------------------------------------------------
         |*** Long name section:
         |AUTH CHECKED  : SSUSER6
         |SOURCE OBJECT : GLWTDPT
         |SOURCE OWNER  : NETBANK
         |TARGET OBJECT : 'BLANK'
         |TARGET OWNER  : 'BLANK'
         |*** End of long names
         |
         |REASON        :          0                STATMNT LENGTH:          48          RETCOD       :          8
         |PRIV CHECKED  : SELECT                      OBJECT         : TABLE OR VIEW
         |OPTIONS       : X'0400000000000000'         RID OF ROW     : N/P                SECLABEL ROW  : N/P
         |AUTH ID TYPE  : PRIMARY OR SECONDARY AUTH ID
         |
         |SQL STATEMENT :
         |SELECT * FROM "NETBANK"."GLWTDPT" FOR FETCH ONLY
         |
         |ACEE UTOKEN (STRING):  &     {                                    SO1TCP42        SSUSER6 PDUSER
         |
         |ACEE UTOKEN (IN HEX):
         |500120060001C000000000000000000000000000000000000000000000000000000000000000000000000000000000E2F0F1E3C3D7F4F200000000
         |00000000E2E2E4E2C5D9F640D7C4E4E2C5D94040
         |-------------------------------------------------------------------------------------------------------------
```

Debugging – ICH408I message

- User SSUSER6 attempt to run SQL: SELECT * FROM NETBANK.GLWDPT

```
ICH408I USER(SSUSER6 ) GROUP(PDUSER   ) NAME(SELF SERVICE USER 6 )
  DSAD.NETBANK.GLWTDPT.SELECT CL(MDSNTB   )
  INSUFFICIENT ACCESS AUTHORITY
  FROM DSAD.** (G)
  ACCESS INTENT(READ    )  ACCESS ALLOWED(NONE    )
```

Debugging – SMF 80

- User SSUSER6 attempt to run SQL: SELECT * FROM NETBANK.GLWDPT

```
Command ===>          SMF record RACF processing and audit records

  Description
  SSUSER6 RACF ACCESS violation: (READ,NONE) on MDSNTB DSAD.NETBANK.GLWTEMP.SELECT

  Record identification
_ Jobname + id:  SSUSER6
_ SMF date/time: Fri  3 May 2024 12:18:28.28
  SMF system:    SS01        record type:   80   record no: CKR4SM01 698

  Event identification
  RACF event description          Resource access (Failure:Insufficient authority)
  RACF event qualifier            1
  RACF descriptor for event       Violation
  RACF reason for logging         Resource
  SAF authority used              Normal
  Access intent                   READ
  Access allowed                  NONE
  Unix Audit Function Code
  Unix Access Intent
  Unix Access Allowed
  Unix Access Used
  RACF command
  Audit/message logstring         ∩.5∩.GG⌄ SSUSER6  DSAD T Y Y N Y N N     GLWTEMP
  Audit/message logstring         050   MDSNTB   DSAD.NETBANK.GLWTEMP.SELECT

  Object identification
  SAF resource class              MDSNTB
  SAF profile key                 DSAD.**
  SAF resource name               DSAD.NETBANK.GLWTEMP.SELECT
  Volume serial
  Resource token
  Pathname
  Failing job name

  Object ownership
_ Profile owner id                SSUSER1  SELF SERVICE USER 1
  Installation data

  Subject identification
_ User:  SSUSER6      Group: PDUSER       Terminal: SO1TCP47   Appl:
  Name:  SELF SERVICE USER 6              Security label:
  SERVAUTH POE:
  Token: User:SSUSER6; Group:PDUSER; Flags:(Pre 1.9); Session:TSO; Port:TERMINAL(SO1TCP47)
```

Cleanup grants – backup first

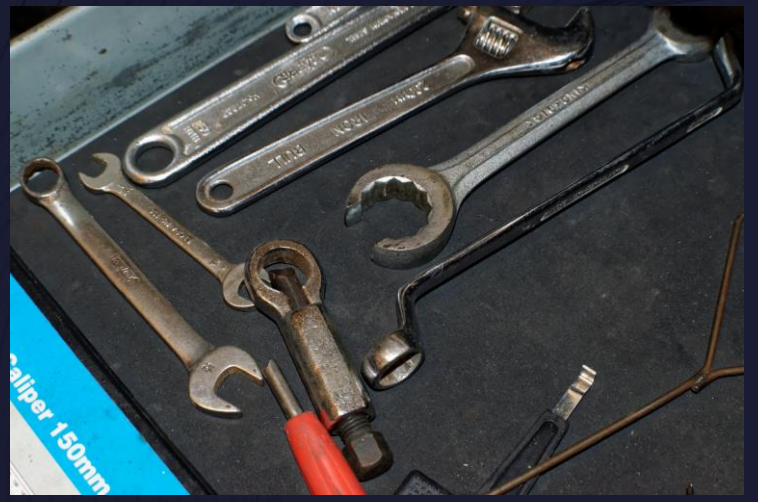
- Make a backup copy of grants
- Options:
  1. Db2 UNLOAD of relevant SYSIBM.SYSxxxAUTH tables
     - Difficult to query
  2. Copy all SYSIBM.SYSxxxAUTH tables to new schema
     - Vendor tooling that allow “catalog copy”
  3. Db2 V13 FL505: enable temporal history on SYSIBM.SYSxxxAUTH
     - Vendor tooling that exploit FL505: “show authorizations as of June 1, 2024”
  4. Vendor tooling that can generate GRANTs from catalog

NEW

Cleanup grants - revoke

- Revoke the authorizations that are no longer used
  - Strongly recommended for security reasons
  - Db2 can fallback
    - All classes not implemented
    - No backstop profiles
    - Db2 auth exit failures
    - Processing GRANTs
- Vendor tooling typically support mass revokes
- You cannot revoke implicit privileges
  - Ownership
  - Package

Conversion tools & support



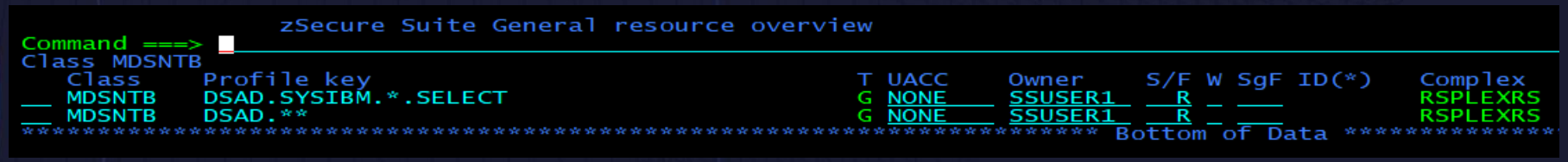
- RACFDB2
  - 2002 edition is still available: https://public.dhe.ibm.com/eserver/zseries/zos/racf/racfdb2/
  - No compression of profiles
  - Updates/improvements discussed on IDUG-L in 2020: https://community.idug.org/discussion/6581994178556524276/migrating-from-db2-internal-security-to-db2-external-security-racf
- Build your own tools
- Consultants
  - E.g., Rocket Software ☺

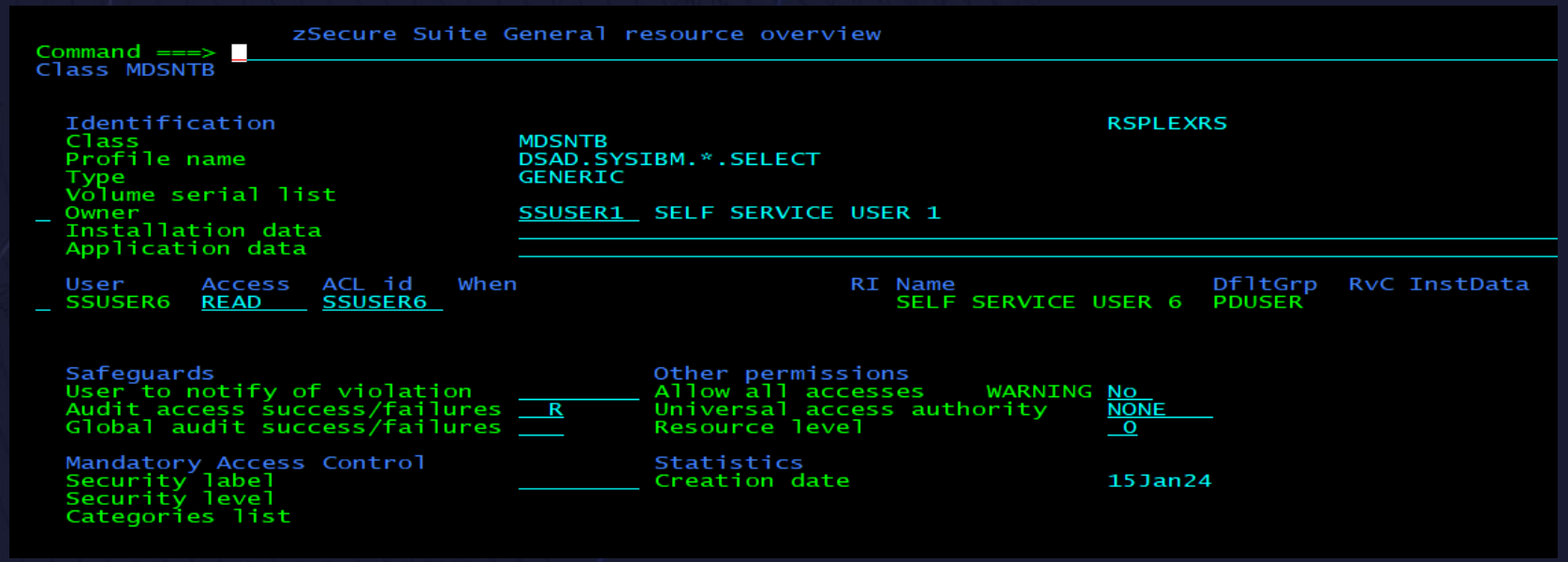
Helpful tools for DBAs when using RACF security

- Before: the security admin had to learn a new tool to manage Db2 native security
- Now: the DBA must learn a new tool to answer questions like:
  - Why do I get a sqlcode -551?
  - What profile provides UPDATE access to this object?
  - What access does this user have?
- Options:
  1. RACF commands (see appendix for samples)
  2. Vendor tools for RACF administration
  3. Db2 vendor tools with RACF support

Helpful tools for DBAs when using RACF security

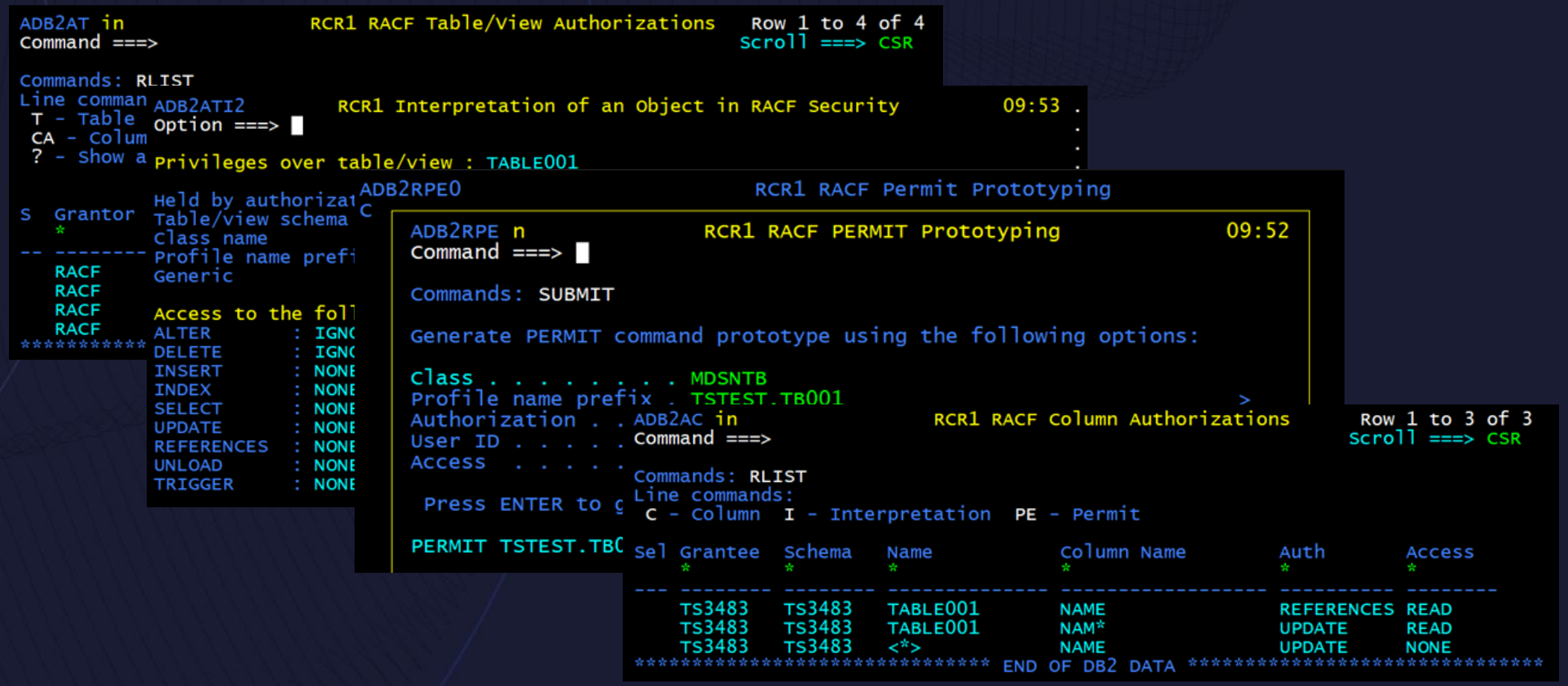
- Vendor tooling – generic RACF administration tools
  - Example: IBM zSecure Administration





Helpful tools for DBAs when using RACF security

- Vendor tooling – Db2 specific



IDUG

IDUG

2024 NA Db2 Tech Conference

Considerations for Migrating Db2 Security to RACF

Ray Overby

roverby@rocketsoftware.com

Jørn Thyssen

jthyssen@rocketsoftware.com

Session Code SEC2

Please fill out your session evaluation!

@IDUGDb2
#IDUG_NA24

Appendix: helpful RACF commands

- Activate & raclist class
  - SETROPTS CLASSACT(MDSNTB) RACLIST(MDSNTB)
- Refresh class after changes
  - SETROPTS RACLIST(MDSNTB) REFRESH
- Define profile
  - RDEFINE MDSNTB DSAD.SYSIBM.*.SELECT UACC(NONE) OWNER(<owner>) AUDIT(FAILURES(READ))
  - Requires refresh to take effect
- Delete profile
  - RDELETE MDSNTB DSAD.SYSIBM.*.SELECT
  - Requires refresh to take effect

Appendix: helpful RACF commands, cont’ed

- Search
  - Search for all profiles:
    - SEARCH ALL CLASS(MDSNTB)
  - Search for all profiles for subsystem DSAD
    - SEARCH ALL CLASS(MDSNTB) MASK(DSAD)
    - SEARCH ALL CLASS(MDSNTB) FILTER(DSAD.**)
  - Search for all profiles for tables in schema SYSIBM for any subsystem
    - SEARCH ALL CLASS(MDSNTB) FILTER(*.SYSIBM.**)

Appendix: helpful RACF commands, cont’ed

- List profile
  - List all information about profile
    - RLIST MDSNTB DSAD.** ALL
- List user
  - LU <userid>
- List group
  - LG <group>

Appendix: helpful RACF commands, cont’ed

- Permit access
  - PERMIT AC(READ) CL(MDSNTB) DSAD.SYSIBM.*.SELECT ID(JORN)
  - Requires refresh to take effect
- Revoke access
  - PERMIT CL(MDSNTB) DSAD.SYSIBM.*.SELECT ID(JORN) DELETE
  - Requires refresh to take effect