RACF for DB2 Control – Beyond the Basics

Doug Behrends
Vanguard Professional Services
Trademarks

The following are trademarks or registered trademarks of the International Business Machines Corporation:

<table>
<thead>
<tr>
<th>CICS</th>
<th>IMS</th>
<th>S/390</th>
<th>z9</th>
</tr>
</thead>
<tbody>
<tr>
<td>CICSPlex</td>
<td>MQSeries</td>
<td>System z</td>
<td>z10</td>
</tr>
<tr>
<td>DB2</td>
<td>MVS</td>
<td>System z9</td>
<td>z13</td>
</tr>
<tr>
<td>eServer</td>
<td>NetView</td>
<td>System z10</td>
<td>z14</td>
</tr>
<tr>
<td>IBM</td>
<td>OS/390</td>
<td>System/390</td>
<td>z/Architecture</td>
</tr>
<tr>
<td>IBM z</td>
<td>Parallel Sysplex</td>
<td>VTAM</td>
<td>z/OS</td>
</tr>
<tr>
<td>IBM z Systems</td>
<td>RACF</td>
<td>WebSphere</td>
<td>z/VM</td>
</tr>
<tr>
<td>IBM z14</td>
<td>RMF</td>
<td>z Systems</td>
<td>zEnterprise</td>
</tr>
</tbody>
</table>

Java and all Java-based trademarks are trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

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

• RACF® Security for DB2® Objects
• RACF Access Control Module
• RACF Profiles for DB2 Objects
• Controlling Access to DB2 Objects
• Migrating from DB2 Security to RACF Security
RACF Security for DB2 Objects
Group DB2AB needs execute privilege to the ACT01234 plan

GRANT EXECUTE ON PLAN ACT01234 TO DB2AB
RACF Security for DB2 Objects

Group DB2AB needs execute privilege to the ACT01234 plan in the DB2P subsystem.

RACF Admin

RDEFINE
RALTER
PERMIT

RDEF MDSNPN DB2P.ACT01234.EXECUTE OW(DB2ADM) UA(NONE)
PE DB2P.ACT01234.EXECUTE CLASS(MDSNPN) ID(DB2AB) AC(READ)
### RACF Classes For DB2 Objects

<table>
<thead>
<tr>
<th>DB2 Object Type</th>
<th>Member</th>
<th>Grouping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bufferpool</td>
<td>MDSNBP</td>
<td>GDSNBP</td>
</tr>
<tr>
<td>Collection</td>
<td>MDSNCL</td>
<td>GDSNCL</td>
</tr>
<tr>
<td>Database</td>
<td>MDSNDB</td>
<td>GDSNDB</td>
</tr>
<tr>
<td>Global Variables</td>
<td>MDSNGV</td>
<td>GDSNGV</td>
</tr>
<tr>
<td>JAR - Java Archive File</td>
<td>MDSNJR</td>
<td>GDSNJR</td>
</tr>
<tr>
<td>Package</td>
<td>MDSNPK</td>
<td>GDSNPK</td>
</tr>
<tr>
<td>Plan</td>
<td>MDSNPN</td>
<td>GDSNPN</td>
</tr>
<tr>
<td>Schema</td>
<td>MDSNSC</td>
<td>GDSNSC</td>
</tr>
<tr>
<td>Sequence</td>
<td>MDSNSQ</td>
<td>GDSNSQ</td>
</tr>
<tr>
<td>Storage Group</td>
<td>MDSNSG</td>
<td>GDSNSG</td>
</tr>
<tr>
<td>Stored Procedure</td>
<td>MDSNSP</td>
<td>GDSNSP</td>
</tr>
<tr>
<td>System</td>
<td>MDSNSM</td>
<td>GDSNSM</td>
</tr>
<tr>
<td>Table / Index / View</td>
<td>MDSNTB</td>
<td>GDSNTB</td>
</tr>
<tr>
<td>Table Space</td>
<td>MDSNTS</td>
<td>GDSNTS</td>
</tr>
<tr>
<td>User Defined Distinct Type</td>
<td>MDSNUT</td>
<td>GDSNUT</td>
</tr>
<tr>
<td>User Defined Function</td>
<td>MDSNUF</td>
<td>GDSNUF</td>
</tr>
</tbody>
</table>
RACF Access Control Module
DB2 Authorization Exit

DB2 Subsystem
- DB2 Start up
- Access to DB2 Objects
- DB2 Shutdown

Authorization Exit
- Initialization
- Authorization Checking
- Termination

RACF
- Data Space
- Database

DSNX@XAC
Steps To Implement DSNX@XAC Exit

1. Obtain the RACF Access Control Module
   • From prefix.SDSNSAMP(DSNXRXAC) – starting with DB2 V8

2. Copy to a private library with name of DSNX@XAC

3. Specify the exit options (optional)
   • &CLASSOPT
   • &CLASSNMT
   • &CHAROPT
   • &ERROROPT

4. Define DB2 classes in CDT (if exit modified)

5. Define RACF profiles - RDEFINE, RALTER, PERMIT

6. Activate the DB2 classes

7. Assemble and link edit the sample exit
   • Modify JEX0003 step of DB2 install job
   • Run JEX0003 job

8. Start DB2
Single or Multi-Subsystem Scope?

• Multi-Subsystem Scope Classes
  • Default
  • First qualifier is DB2 subsystem name
  • No changes to CDT

• Single Subsystem Scope Classes
  • Optional
  • DB2 subsystem name not in profile
  • Add classes to CDT
Customizing the DSNX@XAC Exit

I need to know:
Class scope
Pattern of DB2 class names
Format of RACF profile names

Security Administrator

System Programmer

Edit source code

&CLASSOPT
&CLASSNMT
&CHAROPT
&ERROROPT
Customization Options for DSNX@XAC

**&CLASSOPT** Class Scope

- 1 = Single-subsystem scope
- 2 = Multi-subsystem scope

**&CLASSNMT** Class Name Root

- 1 to 4 characters
- ‘DSN’ is the default
- Only for &CLASSOPT=2
- Example: MDB2PTB

**&CHAROPT** Class Name Suffix

- Last character of classname
- 0 - 9, #, @, $
- Default is ‘1’
- Example: MDB2PTB#
Customization Options for DSNX@XAC

&ERROROPT

1 = Defer to DB2 when an unexpected error occurs
2 = Instruct DB2 to terminate when an unexpected error occurs

An unexpected error is:
• DSNX@XAC abends
• DSNX@XAC returns an unexpected return code
• DSNX@XAC instructs DB2 to not call it again
Multi-Subsystem Scope Options

Example of using the default settings:

Exit options

&CLASSOPT = 2
&CLASSNMT = DSN

Classes for DB2 Objects

MDSNTB
GDSNTB
MDSNPN
GDSNPN
Etc.

Class for DB2 Authorities

DSNADM

Profile names must be prefixed with DB2 subsystem name
Multi-Subsystem Scope (Default)

- **DB2P**
  - TABLE U01.TAB123
  - SELECT

- **DB2T**
  - TABLE U49.TABXYZ
  - ALTER

- **RACF Database**
  - MDSNTB Class
  - DB2P.U01.TAB123.SELECT
  - DB2T.U49.TABXYZ.ALTER

- **RACF CDT (No Change)**
Single-Subsystem Scope Options

Example of installation-defined classes

Exit options

&CLASSOPT = 1
&CLASSNMT = Not Applicable
&CHAROPT = #

Classes for DB2 Objects

MDB2PTB#    MDB2TTB#
GDB2PTB#    GDB2TTB#
MDB2PPN#    MDB2TPN#
GDB2PPN#    GDB2TPN#
Etc.        Etc.

Class for DB2 Authorities

DB2PADM#    DB2TADM#

Profile names are not prefixed with DB2 subsystem name
Class names must contain DB2 subsystem name
Dynamic CDT

RDEFINE CDT MDB2PTB#
CDTINFO(DEFAULTUACC(NONE)
FIRST(ANY) OTHER(ANY)
MAXLNTH(100)
GROUP(GDB2PTB#)
OPER(N0)
DEFAULTRC(4)
POSIT(526)
SIGNAL(YES)
RACLIST(REQUIRED))

RDEFINE CDT GDB2PTB#
CDTINFO(DEFAULTUACC(NONE)
FIRST(ANY) OTHER(ANY)
MAXLNTH(100)
MEMBER(MDB2PTB#)
OPER(N0)
DEFAULTRC(4)
POSIT(526)
SIGNAL(YES)
RACLIST(REQUIRED))
Single-Subsystem Scope

DB2P
- TABLE
  - U01.TAB123
  - MDB2PTB# Class
  - MDB2PTB
  - GDB2PTB#

DB2T
- TABLE
  - U49.TABXYZ
  - MDB2TTB# Class
  - MDB2TTB
  - GDB2TTB#

RACF Database
- MDB2PTB# Class
  - U01.TAB123.SELECT
- MDB2TTB# Class
  - U49.TABXYZ.ALTER
RACF Profiles for DB2 Objects
RACF Profile Syntax - Single-Subsystem Scope
RACF Profile Syntax - Multi-Subsystem Scope

Privilege: SELECT
Object: U01.TAB123

Privilege: EXECUTE
Object: PLN987

Subsystem: DB2P
Class: MDSNTB
Object: DB2P.U01.TAB123.SELECT

Subsystem: DB2P
Class: MDSNPN
Object: DB2P.PLN987.EXECUTE

RACF Database
Profiles for Databases

DB2-subsystem.database-name.privilege

Privilege
- CREATETAB
- CREATETS
- DISPLAYDB
- DROP
- IMAGCOPY
- LOAD
- RECOVERDB
- REORG
- REPAIR
- STARTDB
- STATS
- STOPDB

DB2P Subsystem
- CREATE
- DATABASE
- DROP
- IMPORT
- RECOVER
- REORG
- REPAIR
- START
- STATS
- STOP

RACF Database
- MDSNDB Class
  - DB2P.PAYDB.*
  - DB2P.PAYDB.REORG
Profiles for Database Authority

DB2-subsystem.Database-name.authority

Database Authority
- DBADM
- DBCTRL
- DBMAINT

DB2P Subsystem
PAYDB Database

RACF Database
- DSNADM Class
  - DB2P.PAYDB.DBADM
  - DB2P.PAYDB.DBCNTL
  - DB2P.PAYDB.DBMAINT
Profiles for Tables

Valid privileges for table columns are REFERENCES and UPDATE.
Profiles for Views

```
DB2-subsystem.view-qualifier.view.SELECT
DB2-subsystem.table-qualifier.table-name.view-qualifier.view.privilege
```

- Privilege
  - SELECT
  - DELETE
  - INSERT
  - UPDATE

DB2P Subsystem

RACF Database

MDSNTB Class

- DB2P.U01.VIEW789.SELECT
- DB2P.U01.TAB123.U01.VIEW789.INSERT
- U01.VIEW789
- U01.TAB123
Profiles for System Privileges

Privilege
- ARCHIVE
- BINDADD
- BINDAGENT
- BSDS
- CREATEALIAS
- CREATEDBA
- CREATEDBC
- CREATESG
- CREATETMTAB
- DISPLAY
- EXPLAIN
- MONITOR1
- MONITOR2
- RECOVER
- STOPALL
- STOPSPACE
- SQLADM
- TRACE

DB2-subsystem.privilege
DB2-subsystem.package-owner.BINDAGENT

DB2P Subsystem

System Privileges

RACF Database

MDSNSM Class
- DB2P.CREATEDBA
- DB2P.SQLADM
- DB2P.*
Profiles for System Authorities

System Authority

accesscontrol
dataaccess
secadm
sysadm
sysctrl
sysdbadm
sysopr

DB2P Subsystem

System Authorities

DB2-subsystem.authority

RACF Database

DSNADM Class

DB2P.ACCESSCTRL
DB2P.SYSDBADM
DB2P.SYSADM
Controlling Access to DB2 Objects
Access Control With RACF

• To access a DB2 object requires:

- Ownership
- Privilege to Object
- Administrative Authority

- or -
- or -
Does the user **ARTH** have **INSERT** privilege to the table **PAYID.EMPL** in the **PAYDB** database?

**DB2P Subsystem**

- **Allow**
  - **RC = 8**
  - **DB2 Security**

- **Deny**
  - **RC = 8**
  - **DB2 Security**

**Access Control Module**

- **Owner?**
  - **ARTH ≠ PAYID**
    - **No**
      - **Check Privilege**
        - **RC = 0**
          - **Deny**
            - **RC = 8**
            - **Set RC 8**

- **RC = 8**
  - **DB2 Security**

**RACF**

- **Data Space**
  - **MDSNTB Class**
    - **DB2P.PAYID.EMPL.INSERT**
      - **UA(NONE) PHILE(READ)**
      - **RC = 8**
      - **DSNADM Class**
        - **DB2P.PAYDB.DBADM**
          - **UA(NONE) JOHNH(READ)**
          - **RC = 8**
          - **DSNADM Class**
            - **DB2P.DATAACCESS**
              - **UA(NONE) JIMM(READ)**
              - **RC = 8**
              - **DSNADM Class**
                - **DB2P.SYSADM**
                  - **UA(NONE) JULIE(READ)**
                  - **RC = 8**
## DSNX@XAC Exit Return Codes

<table>
<thead>
<tr>
<th>Return Codes from RACF</th>
<th>Return Code passed to DB2</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Object Profile</strong></td>
<td><strong>DSNADM Profile</strong></td>
</tr>
<tr>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>4</td>
<td>8</td>
</tr>
<tr>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>8</td>
</tr>
</tbody>
</table>
Implicit Privileges for Table Ownership

Access Request

RC = 0

Set RACF RC

Set RC

Check RACF Profiles

RACF

Is user ID of accessor equal to owner of table?

Yes

No

Is Current SQL ID equal to owner of table?

Yes

No

DSNX@XAC
Access Allowed By Ownership

**DB2P Subsystem**

Does PAYID have **INSERT** privilege to the table **PAYID.EMPL** in the **PAYDB** database?

- **Allow**
  - **RC = 0**
  - DB2 Security

- **Deny**
  - **RC = 8**

**Access Control Module**

- **Owner?**
  - PAYID = PAYID
  - Check Privilege

- **DBADM Authority?**
  - **RC = 0**

- **DATAACCESS Authority?**
  - **RC = 4**

- **SYSADM Authority?**

**RACF**

**Data Space**

- **MDSNTB Class**
  - DB2P.PAYID.EMPL.INSERT
  - UA(NONE) PHILE(READ)

- **DSNADM Class**
  - DB2P.PAYDB.DBADM
  - UA(NONE) JOHNN(READ)

  - DB2P.DATAACCESS
  - UA(NONE) JIMM(READ)

  - DB2P.SYSADM
  - UA(NONE) JULIE(READ)

**DB2 Security**

- **RC = 0**
Access Allowed By Object Profile

Does the user PHILE have INSERT privilege to the table PAYDB.EMPL in the PAYDB database?

Owner? PHILE = PAYID

Check Privilege

Set RC 0

RC = 0

DBADM Authority?

DATAACCES Authority?

SYSADM Authority?

DB2 Security

DB2P Subsystem

Access Control Module

RC = 0

Deny

RC = 8

Allow

RC = 0

Data Space

RACF

MDSNTB Class

DB2P.PAYDB.DBADM
UA(NONE) JOHNH(READ)

DSNADM Class

DB2P.DATAACCESS
UA(NONE) JIMM(READ)

DSNADM Class

DB2P.SYSDM
UA(NONE) JULIE(READ)
Access Allowed By SYSADM Profile

DB2P Subsystem

Does the user JULIE have INSERT privilege to the table PAYID.EMPL in the PAYDB database?

Owner? JULIE = PAYID

Check Privilege

RC=0

No

DBADM Authority?

RC=0

No

DATAACCES Authority?

RC=0

No

SYSADM Authority?

Set RC 0

Deny

RC=8

Allow

RC=0

RC=4

DB2 Security

Access Control Module

RACF

Data Space

MDSNTB Class

DB2P.PAYID.EMPL.INSERT
UA(NONE) PHILE(READ)

RC=8

DSNADM Class

DB2P.PAYDB.DBADM
UA(NONE) JOHNH(READ)

RC=8

DSNADM Class

DB2P.DATAACCESS
UA(NONE) JIMM(READ)

RC=8

DSNADM Class

DB2P.SYSADM
UA(NONE) JULIE(READ)

RC=0
Access Allowed By DBADDM Profile

DB2P Subsystem

Does the user JOHNH have INSERT privilege to the table PAYID.EMPL in the PAYDB database?

- Allow: RC = 0
- Deny: RC = 8

Access Control Module

Owner?
JOHNH = PAYID

No

Check Privilege
RC = 0
No

DBADDM Authority?

Set RC 0

DATAACCESS Authority?

SYSADM Authority?

RACF

Data Space

MDSNTB Class
DB2P.PAYID.EMPL.INSERT
UA(NONE) PHILE(READ)

RC = 8

DSNADM Class
DB2P.PAYDB.DBADM
UA(NONE) JOHNH(READ)

RC = 0

DSNADM Class
DB2P.DATAACCESS
UA(NONE) JIMM(READ)

DSNADM Class
DB2P.SYSADM
UA(NONE) JULIE(READ)
Unprotected Object - Defer To DB2

DB2P Subsystem

Does the user JOEM have SELECT privilege to the table PAYID.REG in the PAYDB database?

DB2 Security

RC = 4

Access Control Module

Owner?
JOEM = PAYID
No

Check Privilege
RC=0
No

DBADM Authority?
RC=0
No

DATAACCESS Authority?
RC=0
No

SYSADM Authority?
Set RC 4

RACF

Data Space

MDSNTB Class
NO PROFILE FOUND

DSNADM Class
DB2P.PAYDB.DBADM
UA(NONE) JOHNH(READ)

DB2P.DATAACCESS
UA(NONE) JIMM(READ)

DB2P.SYSADM
UA(NONE) JULIE(READ)
DB2 Access Events Logged to SMF

**Violations**

- RACF has checked all object profiles
- RACF has checked all authority profiles
- The final resulting return code is 8
- AUDIT(FAILURES) in object profile

**Successes**

- A RACF profile has allowed access (RC=0)
- AUDIT(SUCCESS) in profile
Migrating from DB2 Security to RACF Security
Migrating from DB2 to RACF Security

How can I convert from DB2 security to RACF security?

Let’s use the DB2 to RACF Migration Utility!
DB2 to RACF Migration Tool

**DB2 Subsystem**

**DB2 Authorization Tables**
- SYSIBM.SYSCOLAUTH
- SYSIBM.SYSDBAUTH
- SYSIBM.SYSPACKAUTH
- SYSIBM.SYSPLANAUTH
- SYSIBM.SYSRESAUTH
- SYSIBM.SYSTABAUTH
- SYSIBM.SYSUSERAUTH

**RACF Database**
- DSNADM Class
- MDSNTB Class
- MDSNPN Class

**RCF.RACFDB2.CONVCLST**
- RDEF ...
- RALT ...
- PERMIT ...
- RDEF ...
- PERMIT ...
- RDEF ...
- ...

**RACFDB2 Utility**
- JCL
- EXEC
- Documentation

[Diagram showing the flow from DB2 Subsystem to RACF Database through RACFDB2 Utility to the output file RCF.RACFDB2.CONVCLST.]
Running the RACFDB2 Utility

• Download the RACF to DB2 utility via WWW or FTP

• Specify values for
  • DB2 subsystem name
  • Owner of profiles
  • Class name root
  • Single subsystem or multi-subsystem
  • Last character of classname

• User who runs tool must have SELECT privilege on the SYSIBM.SYSxxxAUTH tables
Migration to RACF Security

• RACF commands are generated for only 9 of the 16 DB2 Object types, and DB2 Authorities
• Not all DB2 Object types are handled:
  • Global Variables
  • Java Archive files (JARs)
  • Schemas
  • Sequences
  • Stored Procedures
  • User Defined Distinct Types
  • User Defined Functions
  • Trusted Context
• Privileges higher than SELECT to a VIEW not processed correctly
Profiles Generated by RACFDB2 Utility

- Builds RDEFINE commands for all objects, privileges and authorities
- AUDIT(ALL(READ)) is set for DB2 administrative authorities
- UACC is set to READ if granted to PUBLIC
- PERMIT with ACCESS(READ) if authorized without GRANT
- PERMIT with ACCESS(ALTER) if authorized with GRANT
- All profiles are defined in member classes
Executing the Commands Generated

• Consider replacing many discrete profiles!
  • Use generic profiles?
  • Use some grouping profiles?
  • Use RACFVARS variable?

• Execute the generated RACF commands
• Customize the DSNX@XAC exit
• Activate the DB2 general resource classes
• Activate the DSNX@XAC exit
• Administer DB2 security with RACF
Considerations

• Any tools that use the security tables in DB2 catalog?
• There are some differences between DB2 and RACF security
  • See *DB2 UDB RACF Access Control Module Guide*
  • BINDAGENT (see next slide)
  • “Any table” privilege
  • WITH GRANT OPTION
BINDAGENT

• Beginning in DB2 V11 BINDAGENT has been fixed
• You must use a new DSNZPARM
  • AUTHEXIT_CHECK=DB2 (the default is AUTHEXIT_CHECK=PRIMARY)
  • Specifies that Db2 provides the ACEE of the package or plan owner to perform authorization checking when processing the autobind, BIND and REBIND commands
• Assume JIMTEST will BIND Plans on behalf of JIMM
  • Create [ssid].JIMM.BINDAGENT in the MDSNSM class (or user defined class)
  • Permit JIMTEST read access to the profile
  • JIMTEST does a BIND specifying OWNER(JIMM)
  • The OWNER may be a GROUP
Questions

How to Contact Us
Vanguard Integrity Professionals
6625 South Eastern Ave., Suite 100
Las Vegas, NV 89119-3930

Direct/International: (702) 794-0014
Toll Free: (877) 794-0014
info@go2vanguard.com