Migrating DB2® Security to RACF®

Presented by Vanguard Integrity Professionals
Legal Notice

Copyright

©2014 Vanguard Integrity Professionals - Nevada. All Rights Reserved. You have a limited license to view these materials for your organization’s internal purposes. Any unauthorized reproduction, distribution, exhibition or use of these copyrighted materials is expressly prohibited.

Trademarks

IBM, RACF, DB2, CICS, OS/390 and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.
Session Topics

• Benefits of Using RACF for DB2 Security
• Migrating from DB2 Security to RACF Security
  – Migration Planning – Implementation Options
  – Converting DB2 Grants to RACF profiles
  – DB2 External Security Module for RACF
• Migration Considerations
Organizational Benefits of RACF for DB2

• Fundamental Security Principals
  – Accountability
  – Auditability
  – Separation of duties
  – Least privilege
Organizational Benefits of RACF for DB2

- RACF is administered by staff focused on security.
- Database access is just one of the security areas on which they are focused.
- Using RACF encourages separation of duties between security administration and DB2 DBA role.
- RACF Security staff is aware of compliance considerations.
- Compliance reports from one source.
Technical Benefits Of RACF for DB2

• One or several sets of general resource classes
• A single profile can protect multiple objects via generics, RACFVARS, group class profiles
• Phased implementation by DB2 subsystem, object type, and object
• Support for IBM® z/OS® RACF constructs introduced in z/OS V1R10 and later releases, e.g. distributed identities
• Conversion utility available to assist RACF implementation
• Further Enhancements are likely
Traditional DB2 Security

User BOBS needs execute privilege to the ACT01234 plan

DB2 Administrator

GRANT EXECUTE ON PLAN ACT01234 TO BOBS
RACF Security For DB2 Objects

User BOBS needs execute privilege to the ACT01234 plan in the DB2P subsystem

RACF Admin

RDEFINE

RALTER

PERMIT

RACF Database

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

## DB2 Object Type

- Bufferpool
- Collection
- Database
- JAR - Java Archive File
- Package
- Plan
- Schema
- Sequence
- Storage Group
- Stored Procedure
- System
- Table / Index / View
- Table Space
- User Defined Distinct Type
- User Defined Function

## Member

- MDSNBP
- MDSNCL
- MDSNDB
- MDSNJR
- MDSNPK
- MDSNPN
- MDSNSC
- MDSNSQ
- MDSNSG
- MDSNSP
- MDSNSM
- MDSNTB
- MDSNTS
- MDSNUT
- MDSNUF

## Grouping

- GDSNBP
- GDSNCL
- GDSNDB
- GDSNJR
- GDSNPK
- GDSNPN
- GDSNSC
- GDSNSQ
- GDSNSG
- GDSNSP
- GDSNSM
- GDSNTB
- GDSNTS
- GDSNUT
- GDSNUF
RACF Profile Syntax For DB2 Objects

- **SELECT**
  - DB2P U01.TAB123

- **EXECUTE**
  - PLN987

---

**RACF Database**

- **MDSNTB Class**
  - DB2P.U01.TAB123 SELECT

- **MDSNPN Class**
  - DB2P.PLN987 EXECUTE

---

**DB2P Subsystem**

- **TABLE**
  - U01.TAB123

- **PLAN**
  - PLN987

---

Privilege -> Object -> Subsystem Object Privilege
RACF Profiles for Tables

DB2-subsystem-name.owner.table-name.privilege
DB2-subsystem-name.owner.table-name.column-name.privilege

Privilege
- ALTER
- DELETE
- INDEX
- INSERT
- SELECT
- REFERENCES
- UPDATE
- TRIGGER

DB2P Subsystem

RACF Database

MDSNTB Class
- DB2P.U01.TAB123.SELECT
- DB2P.U01.TAB123.INSERT
- DB2P.U01.TAB123.DEPTNO.*
Profiles for Views

DB2-subsystem.owner.view.SELECT
DB2-subsystem.table-owner.table-name.view-owner.view-name.privilege

New Format introduced in DB2 V9 via PTF UK50217

Privilege
- SELECT
- DELETE
- INSERT
- UPDATE

DB2P Subsystem
- U01.VIEW789
- U01.TAB123

RACF Database
- MDSNTB Class
  - DB2P.U01.VIEW789.SELECT
  - DB2P.U01.TAB123.U01.VIEW789.INSERT
Migrating from DB2 to RACF Security

How can I convert from DB2 security to RACF security?

Let’s use the DB2 to RACF Migration Tool!

RACFDB2 Migration Tool
DB2 to RACF Migration Planning

• Is the current “internal” DB2 security in “good enough shape” to consider converting to RACF?

• Where can I find a conversion tool?
  IBM website – RACF Downloads Page
  – Tool developed for DB2 V6 (1999) for OS/390® & V7 for z/OS (2001)

• What structure in RACF should be my target?
  – Multi-Subsystem Scope Classes vs. Single Subsystem Scope Classes?
Single or Multi-subsystem Scope?

- **Multi-Subsystem Scope Classes - Default**
  - First profile qualifier is DB2 subsystem name
  - Resource Classes are predefined
  - Delegation of administrative authority by DB2 subsystem requires CLAUTH and Genericowner

- **Single Subsystem Scope Classes - Optional**
  - DB2 subsystem name not in profile
  - DB2 subsystem name is part of the class name
  - Requires definitions to be added to CDT class
  - Delegation of administrative authority by DB2 subsystem requires only CLAUTH
Multi-Subsystem Scope (Default)

DB2P
- TABLE: U01.TAB123

DB2T
- TABLE: U49.TABXYZ

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

RACF CDT (No Change)
DB2 to RACF Migration Tool

**DB2 Subsystem**

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

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

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

**Output**
- RDEF ..........
- RALT ..........
- PERMIT ......
- RDEF ..........
- PERMIT ......
- RDEF ..........
- ..................
DSNX@XAC DB2 Authorization Exit

DB2 Subsystem

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

DB2 Authorization Exit - DSNX@XAC

- Initialization
- Authorization Checking
- Termination

RACF

Data Space

- RACF
- RAelist
- FASTAUTH

RACF Database

©2014 Vanguard Integrity Professionals, Inc.
To access a DB2 Object requires:
Ownership
or
Privilege to Object
or
DB2 Administrative Authority
Access Allowed By Ownership

DB2P Subsystem

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

Allow

Deny

RC = 0

RC = 8

RC = 4

DB2 Security

Authorization Exit Module

Owner?
PAYID = PAYID

Check Privilege

DBADM Authority?

SYSDBADM Authority?

SYSADM Authority?

RACF

Data Space

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

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

DSNADM Class
DB2P.SYSDBADM
UA(NONE) BOBS(READ)

DSNADM Class
DB2P.SYSADM
UA(NONE) JULIE(READ)
Access Allowed By Object Profile

DB2P Subsystem

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

<table>
<thead>
<tr>
<th>Allow</th>
<th>Deny</th>
</tr>
</thead>
<tbody>
<tr>
<td>RC = 0</td>
<td>RC = 8</td>
</tr>
</tbody>
</table>

RC = 0

DB2 Security

Authorization Exit Module

Owner? PHILE = PAYID

No

Check Privilege

Set RC 0

Yes

DBADM Authority?

SYSDBADM Authority?

SYSADM Authority?

RACF

Data Space

MDSNTB Class

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

DSNADM Class

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

DSNADM Class

DB2P.SYSDBADM
UA(NONE) BOBS(READ)

DSNADM Class

DB2P.SYSADM
UA(NONE) JULIE(READ)
Access Allowed By Admin Authority

DB2P Subsystem

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

- Allow
  - RC = 0
  - RC=8

- Deny
  - RC = 0
  - RC=4

DB2 Security

Authorization Exit Module

Owner? JOHNH = PAYID

- No
  - Check Privilege
    - RC=0
    - No
    - DBADM Authority?
      - Yes
      - RC=0
      - Set RC 0
      - SYSDBADM Authority?
      - SYSADM Authority?
    - No
      - RC=4

- RC=0

RACF

Data Space

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

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

DSNADM Class
- DB2P.SYSDBADM
  - UA(NONE) BOBS(READ)

DSNADM Class
- DB2P.SYSADM
  - UA(NONE) JULIE(READ)
Does the user JULIE have INSERT privilege to the table PAYID.EMPL in the PAYDB database?

- **Owner?** JULIE = PAYID
  - **No**
  - **Check Privilege**
    - **RC=0**
    - **No**
    - **DBADM Authority?**
      - **RC=0**
      - **No**
      - **SYSDBADM Authority?**
        - **RC=0**
        - **No**
        - **SYSADM Authority?**
          - **Set RC 0**

**RACF**

- Data Space
  - MDSNTB Class
    - DB2P.PAYID.EMPL.INSERT
      - UA(NONE) PHILE(READ)
  - DSNADM Class
    - DB2P.PAYDB.DBADM
      - UA(NONE) JOHNH(READ)
  - DSNADM Class
    - DB2P.SYSDBADM
      - UA(NONE) BOBS(READ)
  - DSNADM Class
    - DB2P.SYSADM
      - UA(NONE) JULIE(READ)
Does the user JOEM have SELECT privilege to the table PAYID.REG in the PAYDB database?

Check Privilege

DBADM Authority?

SYSDBADM Authority?

Set RC 4

Owner?

JOEM = PAYID

RC = 4

Allow

Deny

RC = 0

RC = 8

RC = 4

DB2 Security

RACF

Data Space

MDSNTB Class

NO PROFILE FOUND

DSNADM Class

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

DSNADM Class

DB2P.SYSDADM
UA(NONE) BOBS(READ)

DSNADM Class

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

Violations

- After RACF has checked all object profiles
- After 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
Customizing the DSNX@XAC Exit

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

DSNX@XAC Exit

Security Administrator

DB2 System Programmer

Edit source code

&CLASSOPT
&CLASSNMT
&CHAROPT
&ERROROPT

©2014 Vanguard Integrity Professionals, Inc.
Customization Options for DSNX@XAC

<table>
<thead>
<tr>
<th><strong>&amp;CLASSOPT</strong></th>
<th>Class Scope</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = Single-subsystem scope</td>
<td></td>
</tr>
<tr>
<td>2 = Multi-subsystem scope</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>&amp;CLASSNMT</strong></th>
<th>Class Name Root</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only applicable for &amp;CLASSOPT=2</td>
<td></td>
</tr>
<tr>
<td>Default is ‘DSN’ to use predefined classes</td>
<td></td>
</tr>
<tr>
<td>1 to 4 characters</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>&amp;CHAROPT</strong></th>
<th>Class Name Suffix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last character of classname: 0 - 9, #, @, $</td>
<td></td>
</tr>
<tr>
<td>Default is ‘1’</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>&amp;ERROROPT</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = Defer to DB2 when an unexpected error occurs</td>
<td></td>
</tr>
<tr>
<td>2 = Instruct DB2 to terminate when an unexpected error occurs</td>
<td></td>
</tr>
</tbody>
</table>

Unexpected errors: DSNX@XAC Abends, unexpected return codes
Example of using the default settings:

**Exit options**

```plaintext
&CLASSOPT = 2
&CLASSNMT = DSN
&CHAROPT = ""
```

**Classes for DB2 Objects**

- MDSNTB
- GDSNTB
- MDSNPN
- GDSNPN
- Etc.

**Class for DB2 Authorities**

- DSNADM

Profile names *must* be prefixed with DB2 subsystem name.
Example of installation-defined classes

Exit options

\&CLASSOPT = 1
\&CLASSNMT = Not Applicable (DB2 subsys name is used)
\&CHAROPT = #

Classes for DB2 Objects

- MDB2PTB#
- GDB2PTB#
- MDB2PPN#
- GDB2PPN#
- Etc.

Class for DB2 Authorities

- DB2PADM#
- DB2TADM#
- Etc.

Profile names are *not* prefixed with DB2 subsystem name
Steps To Implement DSNX@XAC Exit

1. Obtain sample RACF Access Control Module
   – From prefix. SDSNSAMP(DSNXRXAC)
2. Copy to a private library with name of DSNX@XAC
3. Specify the exit options (optional)
   – &CLASSOPT
   – &CLASSNMT
   – &CHAROPT
   – &ERROROPT
4. Define & activate DB2 classes in CDT class (optional)
5. Assemble and link edit the sample exit
6. Run DSNTIJEX install job
   – Replaces dummy DSNX@XAC
7. Start DB2
Running the RACFDB2 Utility

- Download the RACF to DB2 utility via WWW or FTP
- User running the tool must have SELECT privilege on the SYSIBM.SYSxxxxAUTH tables
- Specify values for
  - Owner for profiles
  - DB2 subsystem name
  - Class name root
  - Single subsystem or multi-subsystem
  - Last character of class name
RACFDB2 Generated Commands

- Discrete profile RDEFINE commands for all objects, privileges and authorities
- UACC is set to READ for objects granted to PUBLIC
- AUDIT(ALL(READ)) is set for DB2 administrative authorities
- PERMIT DELETE command generated for each profile
- PERMIT with ACCESS(ALTER) if authorized ‘WITH GRANT’ option
- PERMIT with ACCESS(READ) if authorized without GRANT option
- PERMIT commands are generated for all GRANT statements, including users with SYSADM
- PERMIT commands are generated for all GRANT statements on tables for the table owner
- All RDEFINE commands are for profiles in the member classes
• Edit the generated commands
  – Remove or modify unnecessary commands

• Consider replacing many of the discrete profiles!
  – Use generic profiles?
  – Use some grouping profiles?
  – Use RACFVARS variables for privilege qualifiers?

• Define RACF classes for DB2 if using Single-Subsystem Scope

• Enable Generic profiles for the RACF classes to be used for DB2

• Activate the DB2 general resource classes

• Execute the generated RACF commands
Migration Considerations

- Differences between (internal) DB2 and RACF security
  (See DB2 for z/OS RACF Access Control Module Guide, Chapter 10. Special Considerations)
  - Materialized query tables
  - PUBLIC* (DB2 V9)
  - Authorization for implicitly created databases
  - Authorization checking for operations on views
  - Implicit privileges of ownership
  - Matching schema names
  - ALTER and DROP Index
  - CREATETMTAB, CREATE VIEW, & CREATE ALIAS privileges
  - “Any table” and “any schema” privileges
  - GRANT statements
  - ...
Migration Considerations

- Software, applications, tools that use the security tables in DB2 catalog?
Migration GOTCHAs

• The IBM tool only converts 9 of the object types.

• It does not convert:
  – Sequences
  – JARS
  – Stored Procedures
  – User Defined Distinct Types
  – User Defined Functions
  – Schemas

Note: Vanguard’s DB2 Migration Tool creates the required profiles for these additional object types.
Migration GOTCHAs

- The IBM tool does not handle the new format for View authorities for INSERT, UPDATE and DELETE.
- DYNAMIC tables and Views.
- Create ** profile in all DB2 classes with UACC(NONE) and no access list.
- CICS® Connection Entries (next slide)

Note: Vanguard’s DB2 Migration Tool correctly creates the new VIEW profile formats.
Migration GOTCHAs

Note: AUTHTYPE(SIGN), when SIGNID(CICS_region_user id) passes CICS region ACEE AUTHID(string) does not pass an ACEE To the Security Exit.
Key Migration Benefits

1. Seperation of Duties
   Migration to RACF ensures security is managed by RACF administrators versus Database Administrators to ensure separation of duty.

2. Risk Reduction
   Migration to RACF reduces operational risk as security is managed within RACF and reduces cost as no additional tools are needed to manage security within DB2.

3. Compliance
   Migration to RACF streamlines and improves your audit and compliance processes as you will be able to leverage your Vanguard tools investment.

4. Security
   Migration to RACF improves your overall security posture as you now have visibility through your existing Vanguard tools into the security of DB2.
DB2 Release Considerations

• On August 3, 2010, IBM announced the End of Service (EOS) for DB2 8 for z/OS. The effective EOS date is April 30, 2012.

• On February 7, 2012, IBM announced the End of Service (EOS) for DB2 9 for z/OS. The effective EOS date is June 27, 2014.

• On October 19, 2010, IBM announced General Availability for DB2 10 for z/OS as of October 22, 2010.

• On October 3, 2012, IBM announced an Early Support Program for DB2 11 for z/OS.
Planned Enhancements beyond DB2 V10

• Further External Security (DSNX@XAC) consistency with DB2 (internal) security
  – Allow owner to be checked on BIND and REBIND
  – Support Dynamic SQL authorization using DYNAMICRULES behavior
  – Allow automatic REBIND

• Refresh authorization related caches and invalidate dependent packages when external security permissions change
Bibliography for DB2 Version 9

- DB2 V9R1 for z/OS RACF Access Control Module Guide, SC18-9852-06
- DB2 V9R1 for z/OS Managing Security, SC19-3495-03
- DB2 V9R1 for z/OS Administration Guide, SC18-9840-15
- DB2 V9R1 for z/OS SQL Reference, SC18-9854-15
- DB2 V9R1 for z/OS Command Reference, SC18-9844-09
- DB2 V9R1 for z/OS Utility Guide and Reference, SC18-9855-14
Bibliography for DB2 Version 10

- DB2 V10R1 for z/OS RACF Access Control Module Guide, SC19-2982-06
- DB2 V10R1 for z/OS Managing Security, SC19-3496-03
- Security Functions of IBM DB2 V10 for z/OS, SG24-7959-00
- DB2 V10R1 for z/OS Administration Guide, SC19-2968-08
- DB2 V10R1 for z/OS SQL Reference, SC19-2983-09
- DB2 V10R1 for z/OS Command Reference, SC19-2972-05
- DB2 V10R1 for z/OS Utility Guide and Reference, SC19-2984-08
Thank You!

For more information, please visit:
http://www.go2vanguard.com or
e-mail: sales@go2vanguard.com