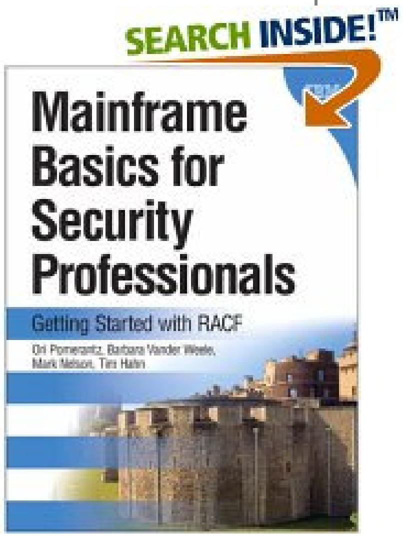
RACF® and DB2®: Teamed for Security

RACF Users Group of New England (RUG-ONE)
June 2015

Mark Nelson, CISSP®, CSSLP®
z/OS® Security Server (RACF) Design and Development
IBM Poughkeepsie
markan@us.ibm.com

Gayathiri Chandran
DB2® for z/OS Security Development
IBM San Jose
gchandran@us.ibm.com


SEARCH INSIDE!™
Mainframe Basics for Security Professionals
Getting Started with RACF
Ori Pomerantz, Barbara Vander Weele, Mark Nelson, Tim Hahn

Disclaimer

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Trademarks

Agenda

- **A RACF View of DB2**
  - Tables and the DB2 catalog
  - Privileges and authorities
  - Ownership
  - How is RACF always used with DB2
- **Using RACF to Control Access to DB2 Objects**
  - Privileges and administrative authorities
  - Mapping DB2 authorization requests to RACF resource names
  - Auditing
  - Considerations
  - Migration

RACF and DB2: Teamed for Security (G)

A RACF View of DB2

A RACF View of DB2

- **Everything in DB2 is a table**
- **The *DB2 catalog* is a set of tables (sometimes called the catalog tables) which contain information about the data that DB2 is managing**
  - Table names, column names, database names, data types
  - DB2-managed authorization information is in the DB2 catalog
- ***TABLES*** reside in ***DATABASES*** which reside in ***TABLE SPACES*** (which map to one or more VSAM data sets) that use ***BUFFERPOOLS*** (for performance) and can be allocated in ***STORAGE GROUPS***. ***VIEWS*** and ***INDEXES*** can be created on ***TABLES***.

A RACF View of DB2…

- There are many other DB2 objects that support DB2 tables.
  - Other DB2 objects include: ***PLANS, PACKAGES, USER DEFINED TYPES, USER DEFINED FUNCTIONS, STORED PROCEDURES, SCHEMAS, JARS, and SEQUENCES***.

A RACF View of DB2…

- **Privilege**
  - Allows a specific function, sometimes on a specific object
- **Explicit privilege**
  - Has a name and is held as a result of an SQL GRANT statement
- **Administrative Authority**
  - Set of privileges, often covering a related set of objects. Authorities often include privileges that are not explicit, have no name, and cannot be specifically granted; For example, the ability to terminate any utility job is included in the SYSOPR authority

A RACF View of DB2…

- **Each DB2 object type (e.g. table, plan, view) has a set of privileges**
- **Example: For tables the privileges are:**
  - **SELECT**: retrieve data from a table
  - **INSERT**: insert rows into a table
  - **ALTER**: change the table definition
  - **UPDATE***: change the contents of a specific column
  - **DELETE**: delete rows
  - **INDEX**: to create an index
  - **REFERECES***: to add or remove a referential constraint
  - **TRIGGER**: to define a trigger

  A "*" indicates that the privilege may be granted on a specific column

- ***Note: Privileges are not hierarchical***

A RACF View of DB2…

- **DB2 has a set of DB2 system authorities**
  - **SYSADM**, which has all DB2 privileges
  - **SYSCTRL**, which has all DB2 privileges, except those which read or modify user data
  - **SYSOPR**, which is allowed to issue most DB2 commands and to end utilities
- **DB2 has a set of database authorities**
  - **DBADM**, which has the DB2 privileges required to control a data base; Allowed to manipulate any table within the database
  - **DBCTRL**, which has the DB2 privileges required to control a data base and run utilities against the data base
  - **DBMAINT**, which is allowed to work with certain objects and run certain utilities on a data base

A RACF View of DB2…

- **"Ownership" of an object within DB2 carries with it a set of implicit privileges:**
  - **Tables**
    - Alter/drop the table or any index, lock, comment, label, create an index or view, select or update any column, insert or delete any row, use the LOAD utility, define referential constraints, create a trigger
  - **Database**
    - DBCTRL or DBADM, depending on how the database was created
- **DB2 has its own protection mechanisms for controlling access to DB2 objects**
  - `GRANT SELECT  ON TABLE SYSIBM.SYSTABAUTH  TO MARKN;`

A RACF View of DB2…

- **How is RACF Always Used with DB2?**
  - Identities
    - The DB2 primary authorization ID is a RACF identity
    - Secondary auth IDs are often derived by exit from the RACF-generated list of groups
  - DB2's underlying VSAM data sets can and should be protected by RACF
  - When multilevel security (MLS) is enabled, RACF is the evaluator of SECLABEL checks

A RACF View of DB2…

- **The ability of a user to connect to DB2 is controlled through checks in the DSNR class**
  - Separate controls for batch/TSO, IMS, CICS, distributed data facility (DDF), and Recoverable Resource Manager Services Attachment Facility (RRSAF)

- **With RACF's plug-in for DSNX@XAC, RACF can be used to control access to DB2 objects**

RACF and DB2: Teamed for Security (M)

Using RACF to Control Access to DB2 Objects

Requirements

- **Provide the ability to control DB2 resources from RACF**
- **Provide a mechanism to:**
  - Validate auth IDs before granting DB2 authorities
  - Define security rules before object is created
  - Preserve security rules for dropped objects
  - Control and audit resources for multiple DB2 subsystems from single point
  - Administer DB2 security with a minimum of DB2 skill
  - Eliminate DB2 cascading revoke
- **Provide an exit point which can control access to DB2 resources**

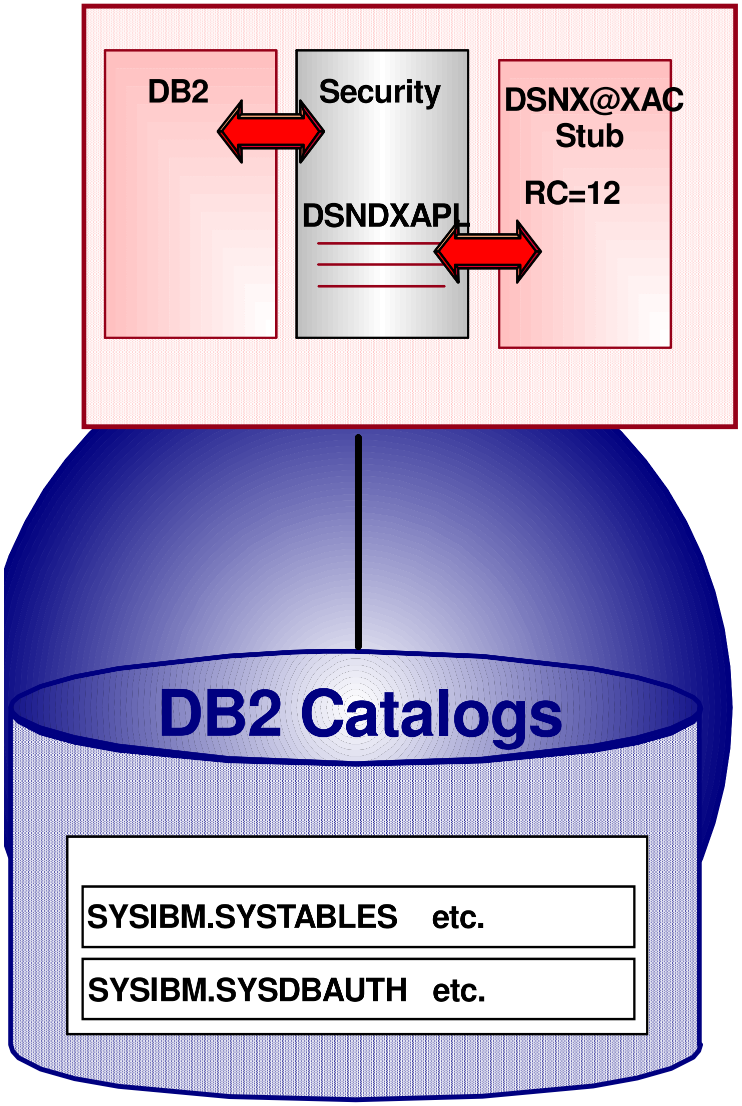
RACF and DB2 Solution

- **DB2 - Access Control Authorization Exit Point**
  - An exit point documented by DB2
  - Exit point is driven:
    - Once at DB2 subsystem startup
    - For each DB2 authorization request
    - Once at DB2 subsystem Termination
  - Exit CSECT Name - DSNX@XAC
  - Exit parameter list - DSNDXAPL
  - DB2 provides dummy DSNX@XAC routine
  - DB2 provides sample LKED JCL for DSNX@XAC
    - Install job DSNTIJEX in SDSNSAMP

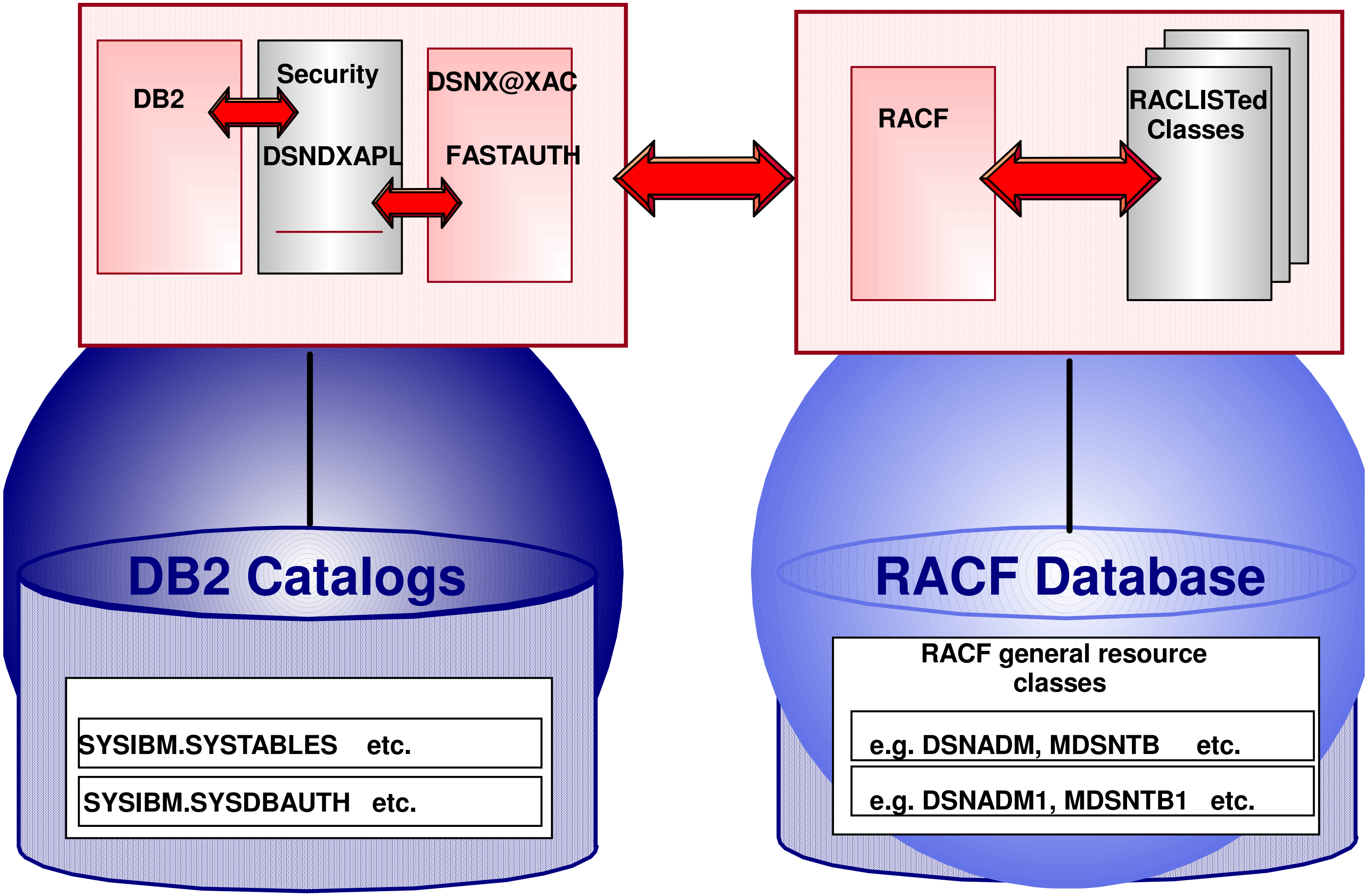
RACF and DB2 Solution…

- **RACF - The RACF/DB2 External Security Module**
  - Fully supported exit module designed to receive control from the DB2 Access Control Authorization Exit Point
    - Shipped in ‘SYS1.SDSNSAM(DSNXRXAC)’
  - New classes in RACF CDT (Class Descriptor Table)

Native DB2 Security



DB2 with RACF



RACF External Security Module Functions

- **Initialization Function**
  - Loads profiles for RACF/DB2 authorization checking function
  - Profiles loaded into data spaces
  - Classes targeted for use must be active
  - If unsuccessful or if no classes are active, exit point will not be driven again
- **Authorization Checking Function**
  - Check user's authority to specified DB2 resource
- **Termination Function**
  - Clean-up profiles loaded into data spaces

Mapping DB2 Authorization Checks

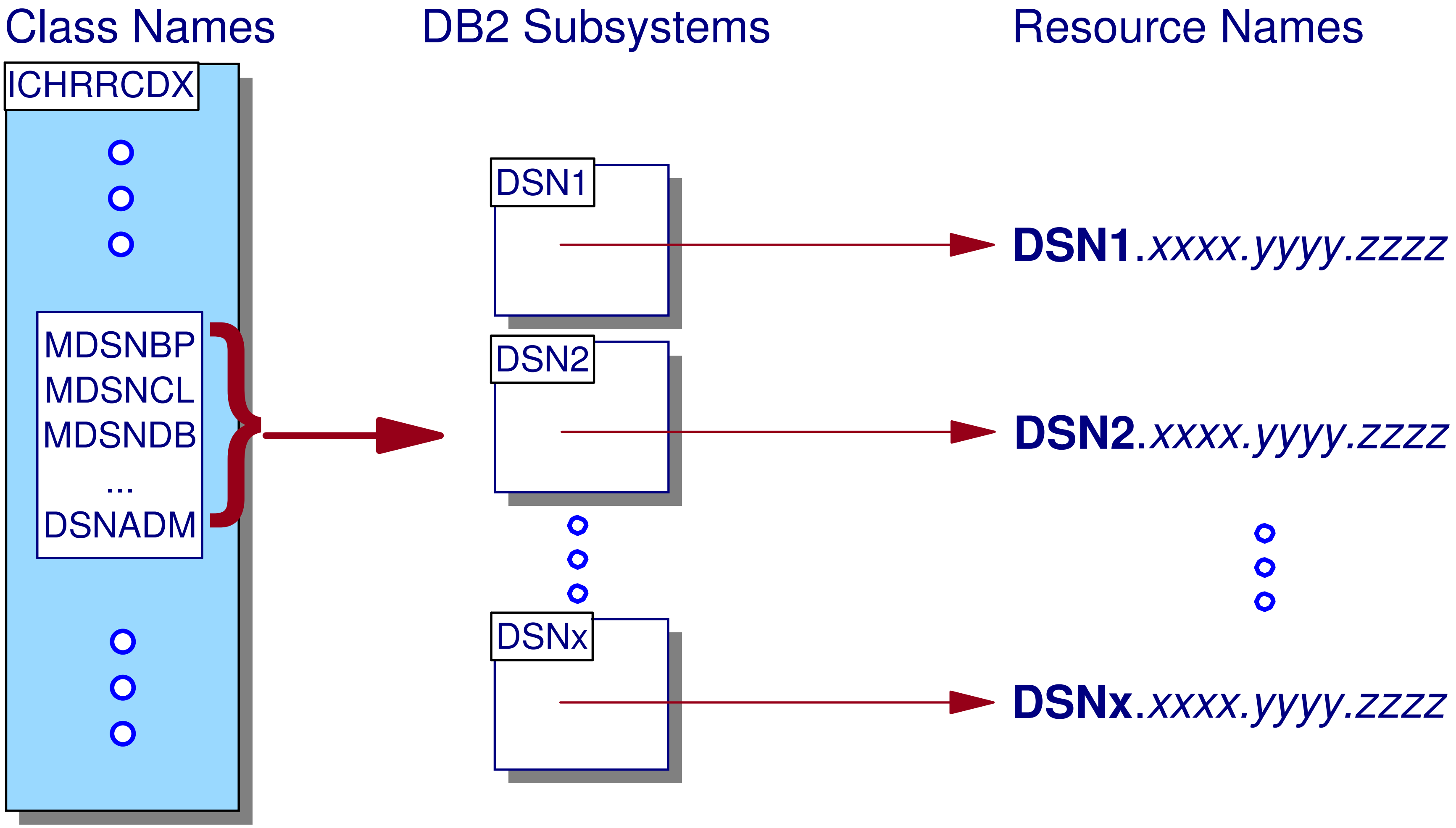
- **How are DB2 authorization checks mapped to RACF?**
  - DB2 objects (table, database, view, user defined function, etc.) correspond to RACF general resource classes
  - DB2 privileges are a part of RACF profile names
  - DB2 administrative authorities are profiles within RACF general resource classes

Scope of RACF Classes

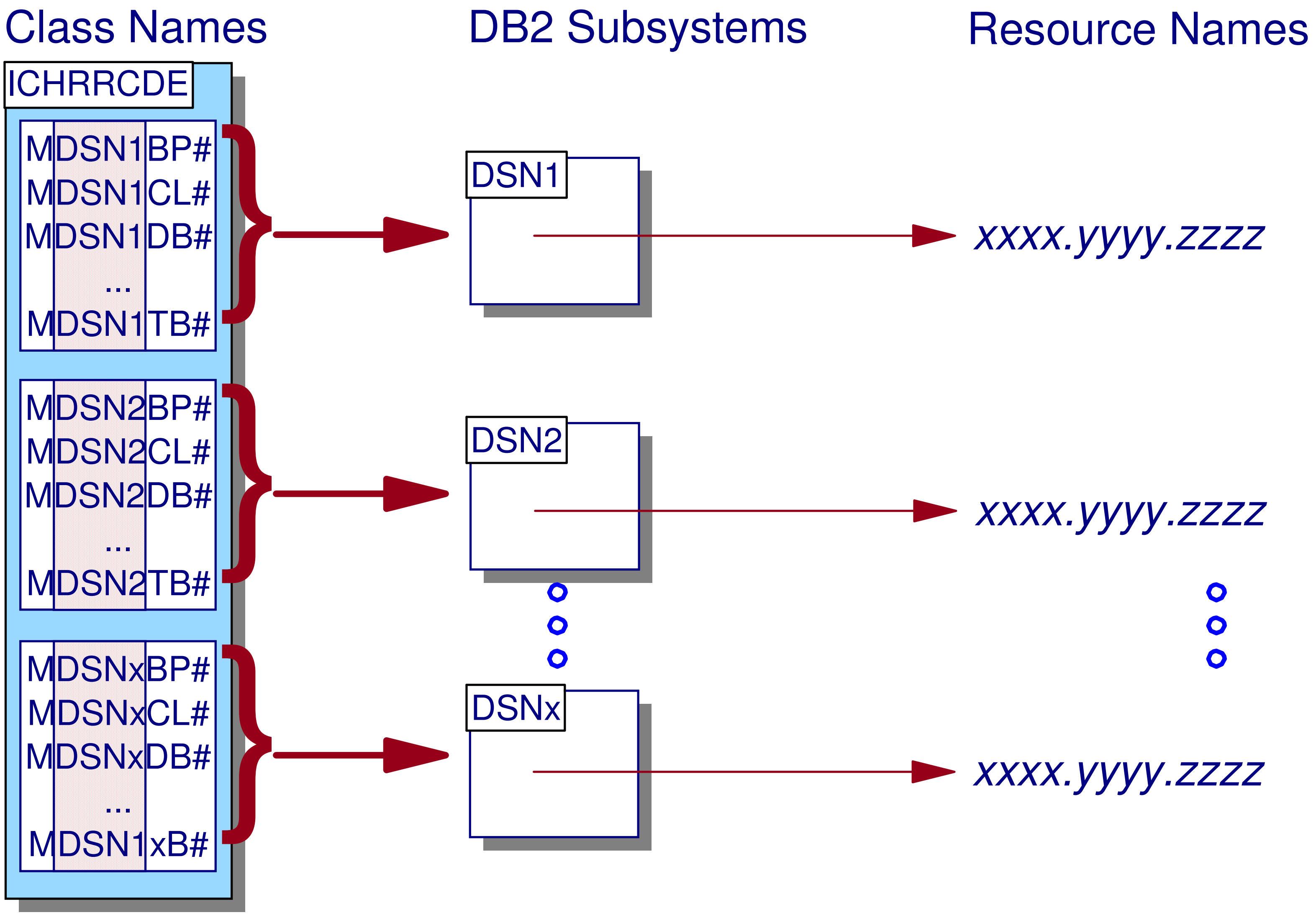
1. **Multi-Subsystem Scope (default)**
   - One set of general resources classes that protect multiple subsystems
   - General resource names are prefixed with DB2 subsystem name
   - Classes provided in the IBM supplied CDT are multi-system scope
   - Protect multiple subsystems with single set of resource profiles
   - Fewer classes overall

2. **Single Subsystem Scope (an option)**
   - One set of general resources classes dedicated to one subsystem
   - General resource names are not prefixed with DB2 subsystem name
   - Classes must be defined by the installation
   - Segregates resources by subsystem
   - Fewer profiles per class

Multi-Subsystem Scope Classes



Single-Subsystem Scope Classes



Class Names

DB2 Subsystems

Resource Names

ICHRRCDE

MDSN1BP#
MDSN1CL#
MDSN1DB#
...
MDSN1TB#

MDSN2BP#
MDSN2CL#
MDSN2DB#
...
MDSN2TB#

MDSNxBP#
MDSNxCL#
MDSNxDB#
...
MDSN1xB#

DSN1

DSN2

DSNx

xxxx.yyyy.zzzz

xxxx.yyyy.zzzz

xxxx.yyyy.zzzz

DB2 Objects and their RACF Classes

DB2 Object Type	RACF Class Name
Bufferpool	MDSNBP
Collection	MDSNCL
Database	MDSNDB
Package	MDSNPK
Plan	MDSNPN
Storage Group	MDSNSG
System	MDSNSM
Table/Index/View	MDSNTB
Table Space	MDSNTS
User Defined Type	MDSNUT
User Defined Function	MDSNUF
Stored Procedure	MDSNSP
Schema	MDSNSC
Jar	MDSNJR
Global Variable	MDSNGV
Sequence	MDSNSQ

DB2 Privileges

- **A *privilege* allows a specific function to be performed, often on a specific object.**

- **Not all DB2 privileges are explicitly GRANTable**

- **Table**
  - ALTER, DELETE, INDEX, INSERT, SELECT, TRIGGER, REFERENCES, UPDATE
- **Database**
  - CREATETAB, CREATETS,DISPLAYDB,DROP, IMAGCOPY, RECOVERDB, REORG, REPAIR, STARTDB,STATS,STOPDB,LOAD
- **System**
  - ARCHIVE, BINDADD, BINDAGENT, BSDS, CREATEALIAS, CREATEDBA, CREATEDBC, CREATESG, DISPLAY, MONITOR1, MONITOR2, STOPALL, STOSPACE, TRACE, RECOVER, CREATETMTAB
- **Table space, buffer pool, storage group**
  - USE

DB2 Privileges…

- **Collection**
  - CREATEIN
- **Plan**
  - BIND, EXECUTE
- **Plan**
  - BIND, COPY, EXECUTE
- **Started procedure, user defined function**
  - EXECUTE, DISPLAY, START(**), STOP(**)
- **User defined distinct type**
  - USAGE
- **Schema**
  - ALTER, COMMENT ON(**), CREATEIN, DROP, CHANGE QUALIFIER(**)
- **Global Variable**
  - READ, WRITE

(**): Cannot be explicitly GRANTED

RACF Access Checks for DB2 Objects

- **When a DB2 object is accessed, the RACF-supplied DSNX@XAC module performs a one or more RACF authorization checks to see if the user is allowed to access the resource.**
- **For example, when a table is accessed, RACF generates a resource access check of the form:**
  - *db2-subsystem.table-owner.table-qualifier.privilege* in the MDSNTB class
    - Privilege names are: ALTER, DELETE, INDEX, INSERT, SELECT, TRIGGER, REFERENCES, UPDATE
  - If the privilege name is either UPDATE or REFERENCES, then if the check above fails, a check is driven against the resource *DB2-subsystem.table-qualifier.table-name.column-name.privilege* in the MDSNTB class
  - If the MDSNTB check does not allow access, other DB2 privilege checks (such as DBADM and SYSADM) are performed.

Termination Options

- **You can tell DB2 what to do in the event of an "unexpected error" with the &ERROROPT setting**
  - An "unexpected error“ is an:
    - abend in the external security module
    - unexpected return and reason code returned by the external security module
- **Your choices are**
  - &ERROROPT='1' causes DB2 to continue processing (documented as the default value)
  - ERROROPT='2' causes the DB2 subsystem to terminate
- **If an error occurs during initialization**
  - RACF issues diagnostic messages and message IRR912I ("Native DB2 Authorization is used")
- **If an unexpected error is encountered**
  - DB2 issues message DSNX210I ("ACCESS CONTROL AUTHORIZATION EXIT (DSNX@XAC) HAS INDICATED THAT IT SHOULD NOT BE CALLED, HAS ABENDED, OR HAS RETURNED AN INVALID RETURN CODE ")

Initialization Messages

- **IRR9xxI initialization messages (issued in the xxxDBM1 address space) list information about the external security module**

```
IRR908I RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2 SUBSYSTEM DSND HAS
        A MODULE VERSION OF OA05967  AND A MODULE LENGTH OF 00005254.

IRR909I RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2 SUBSYSTEM DSND
        IS USING OPTIONS: &CLASSOPT=2
                          &CLASSNMT=DSN
                          &CHAROPT=1
                          &ERROROPT=1
                          &PCELLCT=50
                          &SCELLCT=50

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

IRR911I RACF/DB2 EXTERNAL SECURITY MODULE FOR DB2 SUBSYSTEM DSND
        SUCCESSFULLY RACLISTED CLASSES:
         MDSNDB   MDSNPK   MDSNPN   MDSNBP   MDSNCL
         MDSNTS   MDSNSG   MDSNTB   MDSNSM   MDSNUT
         MDSNSP   MDSNJR   DSNADM
```

DB2 Administrative Authorities

- **Database**
  - Authorities: DBADM, DBCTRL, DBMAINT
  - Checks are performed against the DSNADM class
  - Resource name is *subsystem.database-name.privilege*

- **System**
  - Authorities: SYSADM, SYSCTRL, SYSOPR
  - Checks are performed against the DSNADM class
  - Resource name is *subsystem.privilege*

Notes on Access Control

- **Each DB2 SQL statement, Command, Utility, etc. requires a set of sufficient privileges and/or authorities**
- **The RACF/DB2 External Security Module will check the RACF profiles corresponding to that set of privileges and/or authorities**
- **Implicit privileges of ownership will only be checked for tables**

The RACF Access Control Module Guide documents the profiles required to access DB2 resources

Example: Selecting from a Table

- **SELECT**

  - The SQL Reference indicates that the authorization ID must have at least one of the following:

    - Ownership of the table
    - SELECT privilege on the table
    - DBADM authority for the database
    - SYSCTRL authority (catalog tables only)
    - SYSADM authority

Example: Selecting from a Table…

- **SELECT**
  - The access is allowed only if one of the following is true:
    - Ownership of the table or view (DB2 owner compared to requester ID)
    - Read authority to one of these resources:

Class	**Profile**	**Access**
MDSNTB	*subsystem.owner.table*.SELECT	READ
DSNADM	*subsystem.database-name*.DBADM	READ
DSNADM	*subsystem*.SYSCTRL (catalog table only)	READ
DSNADM	*subsystem*.SYSADM	READ

Auditing

- **Failure SMF records are cut only after entire list of profiles is exhausted**

- **SMF records for a single invocation of the exit will be "linked" using LOGSTR data which contains:**
  - Time Stamp
  - Subset of exit input parameters
  - For the first profile in list
    - Class Name
    - Profile Name

- **New DB2 trace record IFCID 314**
  - DB2 trace record and RACF SMF records will also be "linked"

Example: SELECTing a Row (Not Authorized)

- **Selecting a row without authority**

```
SELECT * FROM SYSIBM.SYSTABAUTH
```

- **The RACF Result**

```
ICH408I  USER(DBUSER) GROUP(SYS1)
         NAME(###################)  CL(MDSNTB)
         DSN.SYSIBM.SYSTABAUTH.SELECT INSUFFICIENT ACCESS
         AUTHORITY FROM ** (G)
         ACCESS     INTENT(READ)  ACCESS ALLOWED(NONE )
```

- **The DB2 Result**

```
DSNT408I SQLCODE = -551, ERROR:  DBUSER DOES NOT HAVE THE
         PRIVILEGE TO PERFORM  OPERATION SELECT ON OBJECT
         SYSIBM.SYSTABAUTH
```

Installation (M)

- **Installation process**:
  - Verify installation options and change if necessary
  - Assemble and link-edit the module into a library which is on your DB2 subsystems searched libraries (e.g. STEPLIB)
  - Start or restart your DB2 subsystem

Migration

- **Can be implemented one DB2 Object at a time**
  - If the RACF/DB2 External Security Module detects that an object class is not active or an object profile is not defined (and no administrative profile allows access) it will defer to DB2 authority checking
  - When additional classes have been setup and activated, restart DB2

DB2 to RACF Migration Tool

- **RACFDB2 utility**
  - DB2 to RACF migration tool
    - Converts contents of SYSIBM.SYSxxxAUTH tables to RACF profiles
  - Internally developed, not officially supported
  - Limitations:
    - One RACF profile per DB2 object
    - No support for user defined types, user defined functions, schemas, sequences, or jars
  - Available from the “downloads” section of the RACF web page at http://www.ibm.com/servers/eserver/zseries/zos/racf/

Considerations

- **The exit returns a return code 4 ("defer to DB2") if an ACEE is not passed to it. This occurs when:**
  - The DB2 request originated from an IMS transaction (fixed with PM27835)

- **DB2 object names are mapped to upper case, with blanks replaced with a "_" (underscore, X'6D')**

- **DB2 object names which contain parenthesis, commas, or semicolons must be protected by RACF profiles with generic characters that will match these RACF-unsupported characters.**

- **Be sure to RACLIST REFRESH general resource classes after defining, changing, or deleting a resource profile**

Considerations…

- **Ownership of a view is not sufficient to grant access**
- **DB2 does not call RACF for any requests made by the INSTALLSYSADM and INSTALLSYSOPR user IDs**
- **BINDAGENT is supported in DB2 11.**
  - DB2 9 and 10 require the use of TRUSTED CONTEXTs, ROLEs, and the RACF WHEN(CRITERIA(SQLROLE(…))) support
- **The DB2 application plan can be invalidated when a security change is made to a RACF-protected resource in DB2 11.**

References

- ***DB2 11 for z/OS RACF Access Control Module Guide*** (SC19-4065)

- ***RACF Security Administrator's Guide*** (SA23-2289)

- ***DB2 11 for z/OS Managing Security*** (SC19-4061)

- ***Security Functions of IBM DB2 10 for z/OS*** (SG24-7959-00), available at http://www.redbooks.ibm.com

- ***RACF System Programmer's Guide*** (SA23-2287)

- ***OS/390 Security Server Enhancements*** (SG24-5158), available at http://www.redbooks.ibm.com

- ***Using RACF to Control Access to DB2 Objects***, Adrian Lobo, Randy Love, Mark Nelson, zJournal, December 2003/January 2004, available at http://enterprisesystemsmedia.com/article/using-racf-to-control-access-to-db2-objects#sr=g&m=o&cp=or&ct=-tmc&st=%28opu%20qspwjefe%29&ts=1425646312

- ***RACF and DB2: Teamed for Security***, Michael Jordan, Roger Miller, Mark Nelson, Technical Support Magazine, October, 1997.

- ***DB2 for z/OS Information Center***
  - http://www-01.ibm.com/support/knowledgecenter/SSEPEK/db2z_prodhome.html

Summary

- **Controlling Access to DB2 Objects Using RACF**
  - Single point of control for administration and auditing
  - Ability to define security rules before a DB2 object is created
  - Allows security rules to persist when a DB2 object is dropped
  - Ability to protect multiple DB2 objects with a single security rule using generic profiles and/or member/grouping profiles
  - Eliminates DB2 cascading revoke
  - Preserves DB2 privileges and administrative authorities
  - Flexibility for multiple DB2 Subsystems
    - One set of RACF classes for multiple DB2 subsystems
    - One set of RACF classes for each DB2 subsystem
  - Selectable on an object-by-object basis