IBM eServer™

RACF® and DB2®: Teamed for Security

New York RACF Users Group
April 2006

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

Trademarks

- **These terms are trademarks of the IBM Corporation in the United States, other countries, or both:**
  - **DB2**
  - **IBM**
  - **MVS**
  - **OS/390**
  - **RACF**
  - **z/OS**

Agenda

- **A Quick DB2 Overview**
  - What is a relational data base management system?
  - DB2 catalog
  - Privileges and authorities
  - Ownership
  - How is RACF always used with DB2
- **Using RACF to Control Access to DB2 Objects**
  - Requirements
  - Privileges and administrative authorities
  - Mapping DB2 authorization requests to RACF resource names
  - Auditing
  - Considerations
  - Migration
  - Customization
  - DB2 Universal Database (UDB) Release 8 for z/OS

RACF and DB2: Teamed for Security

An Overview of DB2

DB2 Overview

- **The key concept in DB2 is the concept of the table**
  - A table consists of rows and columns
  - At the intersection of the row and a column is a value

Serial Number	Last Name	First Name	Dept	Job Category
134487	Jones	Jack	ZNTP	Senior Engineer
357356	Palmer	Mile	ZACE	Manager
403668	Doe	Jane	ZNTP	Senior Engineer
083405	Shine	Susan	ZNTO	Senior Programmer

The DB2 Catalog

- 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

DB2 Privileges and Administrative Authorities

- **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

DB2 Privileges

- **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***

DB2 Authorities

- **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

Implicit Privileges of Ownership

- **"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
- **Ownership is set at object creation time**

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**

How is RACF Always Used with 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

Using RACF to Control Access to DB2 Objects

Security within DB2

- **DB2 has always used RACF to**
  - assign identities
  - control connections to the DB2 subsystem
  - protect the underlying DB2 data store
- **DB2 has its own protection mechanisms for controlling access to DB2 objects**
  - `GRANT SELECT  ON TABLE SYSIBM.SYSTABAUTH  TO MARKN;`

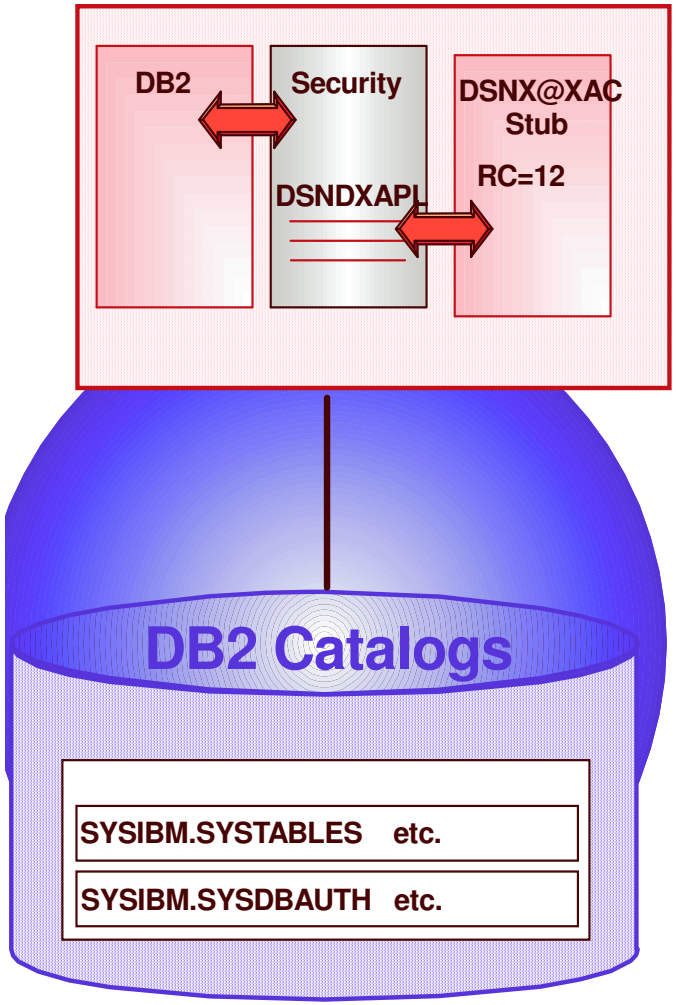
Requirements

- **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**

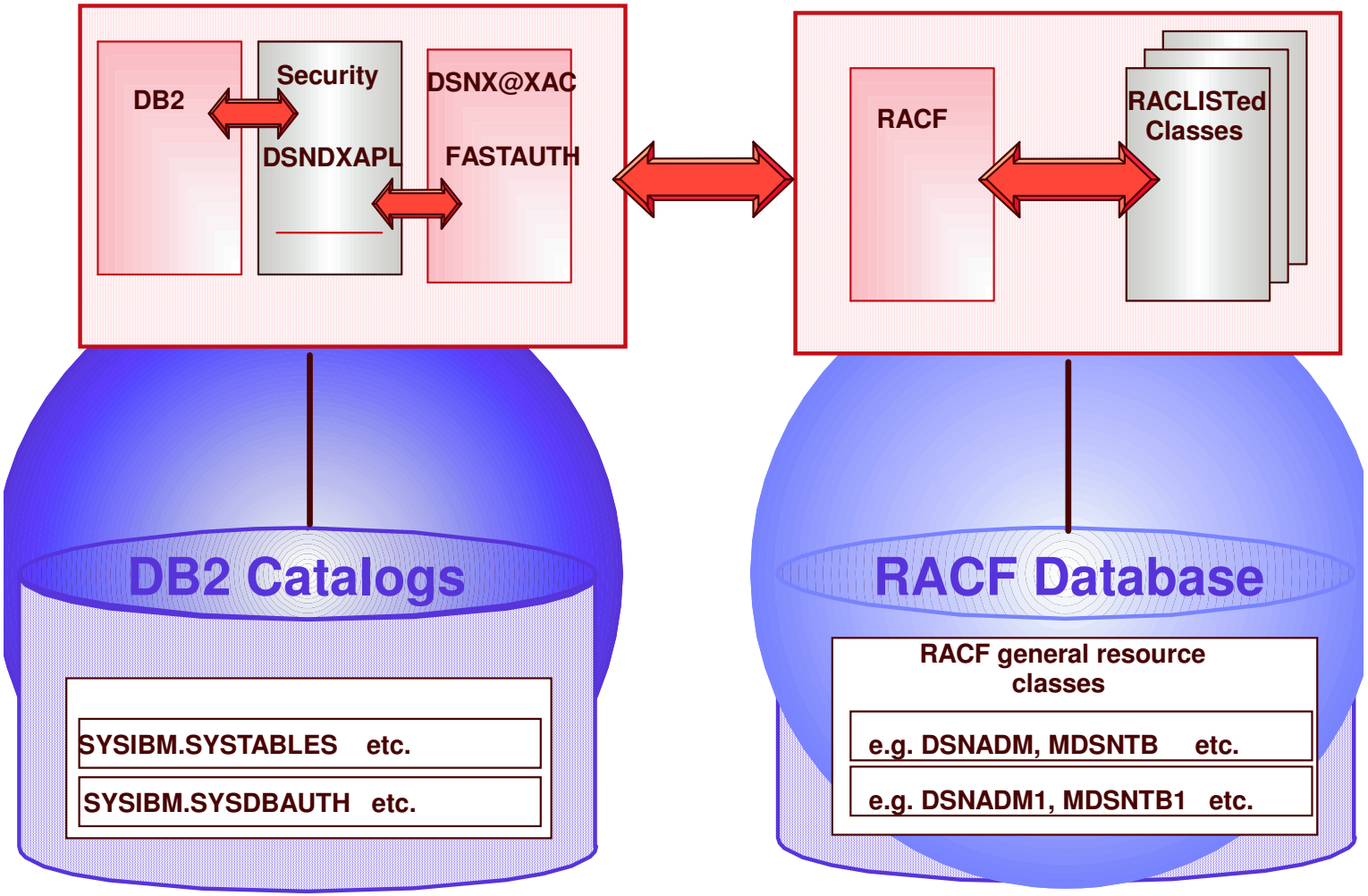
RACF and DB2 Solution

- **DB2 - Access Control Authorization Exit Point**
  - A new 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

Native DB2 Security



DB2 with RACF



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
  - New classes in RACF CDT (Class Descriptor Table)

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

- **DB2 security mechanisms consist of several constructs:**
  - Objects, such as tables, table spaces, data bases, user defined functions, etc.
  - Privileges, such as insert, update, select, etc.
  - Administrative authorities, such as DBADM, SYSADM, etc.

Mapping DB2 Authorization Checks…

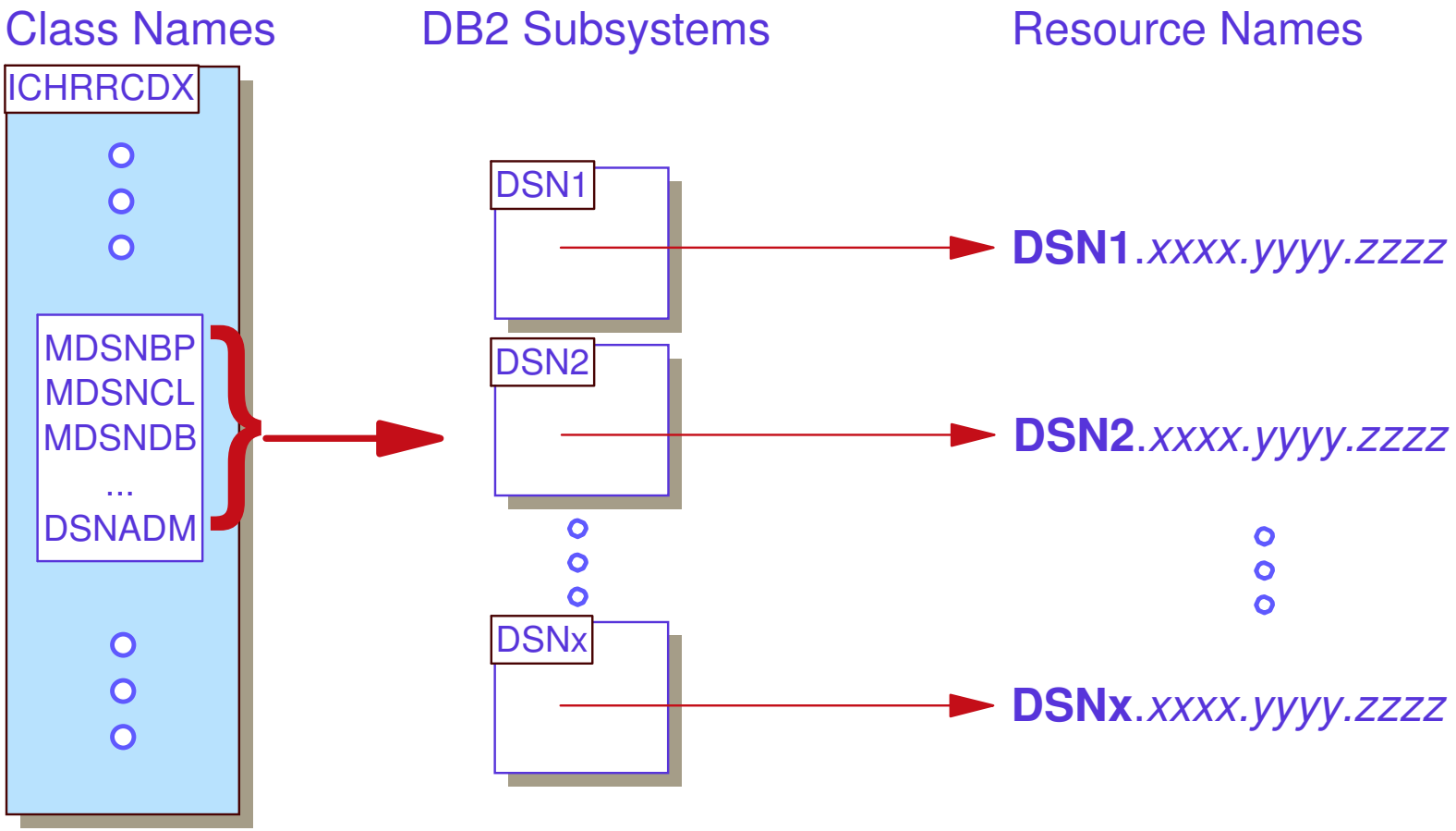
- **How are DB2 authorization checks mapped to RACF?**
  - DB2 objects (table, database, view, user defined function, etc.) correspond to RACF general resource classes
  - DB2 privileges are a part of RACF profile names
  - DB2 administrative authorities are profiles within RACF general resource classes

Scope of RACF Classes

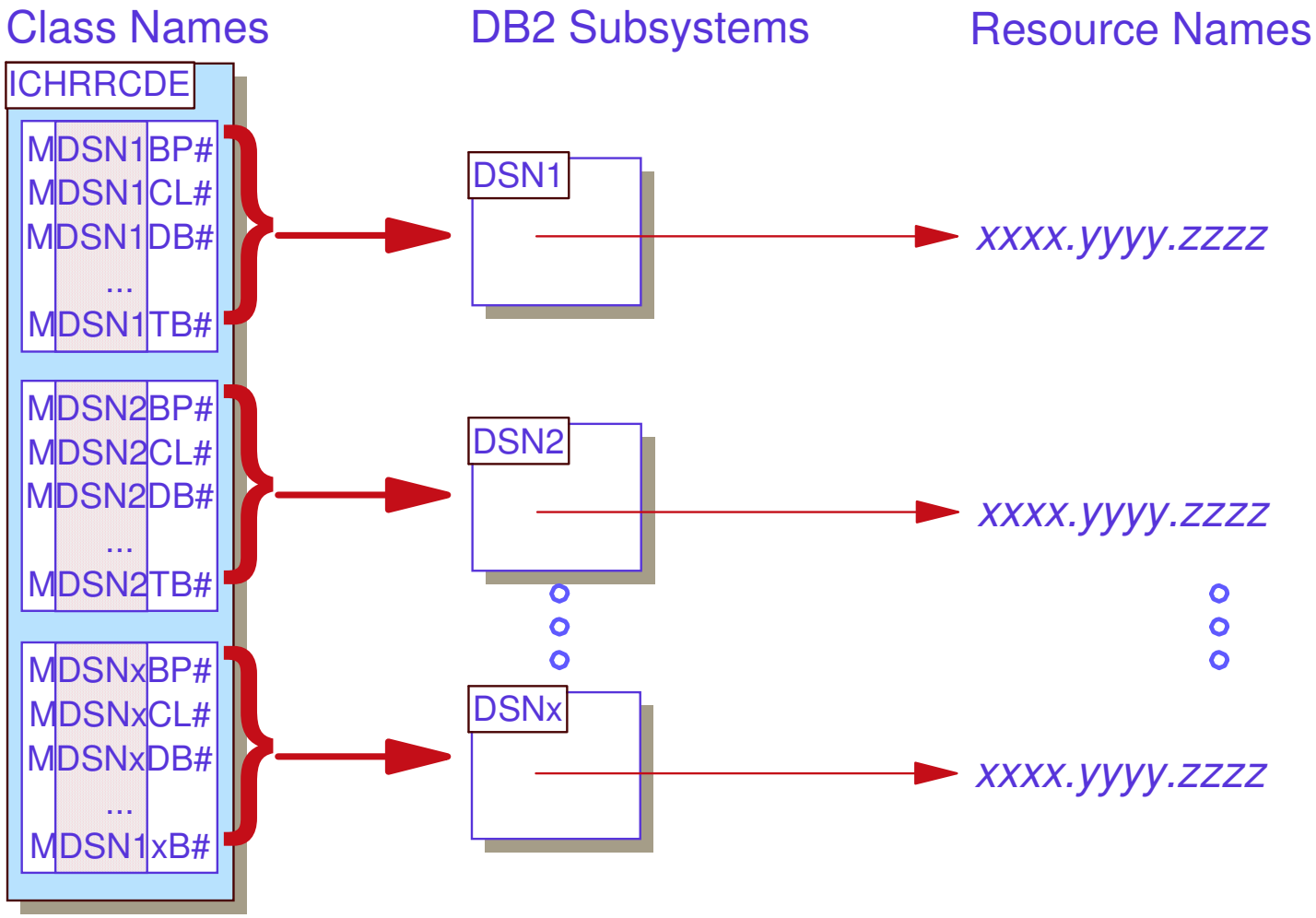
1. **Multi-Subsystem Scope (default)**
   - One set of general resources classes that protect multiple subsystems
   - General resource names are prefixed with DB2 subsystem name
   - Classes provided in the IBM supplied CDT are multi-system scope
   - Protect multiple subsystems with single set of resource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



DB2 Objects and the 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
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(**)

(*): Can be controlled by RACF starting with DB2 V8, prior releases defer to DB2

(**): 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-name.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-owner.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**.

DB2 V7

- **Enhanced Create View Support**
  - allow DBADM to create views for others
  - option set by DB2
- **Customization option to support new DB2 reason code: &ERROROPT**
  - Controls DB2 processing after "unexpected error"
    - &ERROROPT='1' causes DB2 to continue processing (documented as the default value)
    - &ERROROPT='2' causes the DB2 subsystem to terminate
    - Check your default setting! APAR OA05967 corrects the default to '1‘

DB2 V7…

- **Two new messages**
  - IRR912I NATIVE DB2 AUTHORIZATION IS USED.
  - IRR913I DB2 SUBSYSTEM TERMINATION REQUESTED.
- **IRR909I initialization message updated**
  - now includes &ERROROPT setting
- **Terminating messages changed to use IRR912I or IRR913I as appropriate:**
  - IRR900A
  - IRR901A
  - IRR902A
  - IRR903A

DB2 V7…

- **DB2 V7 introduces a new message and a new SQL return code in support of &ERROROPT=2:**
  - a message:
    - DSNX210I csect-name - ACCESS CONTROL AUTHORIZATION EXIT (DSNX@XAC) HAS INDICATED THAT IT SHOULD NOT BE CALLED, HAS ABENDED, OR HAS RETURNED AN INVALID RETURN CODE DURING function-code. RETURN CODE=return-code, REASON CODE=reason-code
  - a SQL return code
    - x'00E70015': DB2 was abnormally terminated because the Access Control Authorization Exit has indicated that it is unable to process authorization requests and that DB2 should be terminated.

DB2 Administrative Authorities

- **An *administrative authority* is a set of privileges, often covering a related set of objects.**
  - Often include privileges that are not explicit, have no name and can not be specifically granted.
- **Administrative authorities for a given object type are hierarchical. (For example, DBADM authority includes all DBCTRL privileges.)**
- **The class name for the administrative authorities is DSNADM.**
- **Can not be used to deny access to explicitly GRANTable privileges**

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**

RACF 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 or view
    - SELECT privilege on the table or view
    - 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:
    - The The SQL Reference indicates that the authorization ID must have at least one of the following:
      - 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*	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"

DB2 Version 8

- **DB2 Universal Database (UDB) Version 8 for z/OS "breaks the barriers of information management“**
  - Multilevel security
  - 64-bit enablement
  - Maximum number of partitions increased to 4096 (was 254)
  - SQL statements may now be 2M (was 32K)
  - Index keys may now be 2,000 characters (was 255)
  - Number of tables in a join may now be 255 (was 15)
  - Table, view, and alias names may now be 128 characters (was 18)
  - Column names may now be 30 characters (was 18)

DB2 Version 8…

- **The RACF-developed authorization control exit has been modified to support DB2 V8**
  - Longer names
  - START, STOP, DISPLAY privileges
  - Multilevel Security
    - Row level multilevel security can be implemented with native DB2 security
- **The exit is shipped with DB2 V8**
  - Shipped under DB2 FMID DHRE810
  - Located in member DSNXRXAC of SDSNSAMP
  - Support for DB2 V6 and DB2 V7 continues to be shipped with RACF in member IRR@XACS of 'SYS1.SAMPLIB.

Installation

- **Source code for DB2 V6 and DB2 V7 provided in:**
  - SYS1.SAMPLIB(IRR@XACS)
  - APAR OA05967
- **Source code for DB2 V8 provided in:**
  - DB2 Sample library SDSNSAMP(DSNXRXAC)
- **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, or sequences
    - Internally developed, not officially supported
  - See README file for details
  - Three versions:
    - RACFDB2/RXSQL - Requires RXSQL
    - RACFDB2/BatchPipes - Requires BatchPipes or MVS Pipes product.
    - RACFDB2 for V5/V6 - Requires DB2 V6 or refreshed DB2 V5.1
  - 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:**
  - A DB2 "-" command is issued (DB2 V7 and earlier)
  - The DB2 request originated from an IMS transaction
- **Be sure to RACLIST REFRESH general resource classes after defining, changing, or deleting a resource profile**
- **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.**

Considerations…

- **The DB2 application plan is *not* invalidated when a security change is made to a RACF-protected resource**
- **Note that after the application of OW52799/PQ68177, 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**

Example: SELECTing a Row

- **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
```

Example: Successful Initiation

```
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
```

References

- ***RACF Access Control Module Guide*** (SC18-7433), available on the web at http://www.ibm.com/software/data/db2/zos/v8books.html
- ***RACF Security Administrator's Guide*** (SC28-1915), available on the web at http://www.ibm.com/servers/eserver/zseries/zos/bkserv/r7pdf/secserv.html
- ***DB2 UDB for z/OS and OS/390 Administration*** (SC26-9931), available on the web at http://www.ibm.com/software/data/db2/os390/v7books.html
- ***RACF System Programmer's Guide*** (SC28-1913), available at http://www.ibm.com/servers/eserver/zseries/zos/bkserv/r4pdf/secserv.html
- ***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://www.zjournal.com/PDF/nelson%20love%20lobo.pdf
- ***RACF and DB2: Teamed for Security***, Michael Jordan, Roger Miller, Mark Nelson, Technical Support Magazine, October, 1997, available at http://www.naspa.com/PDF/98/06-pdf/T9806001.pdf

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

Disclaimer

The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.