RACF and DB2
Teamed for Security

Jun Ogata / Poughkeepsie, NY
ogata@us.ibm.com
Phone #: (845) 435-7680

Trademarks

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

- IBM
- BatchPipes
- DB2
- OS/390
- RACF

Sun Microsystems, Inc:

- Java

Agenda

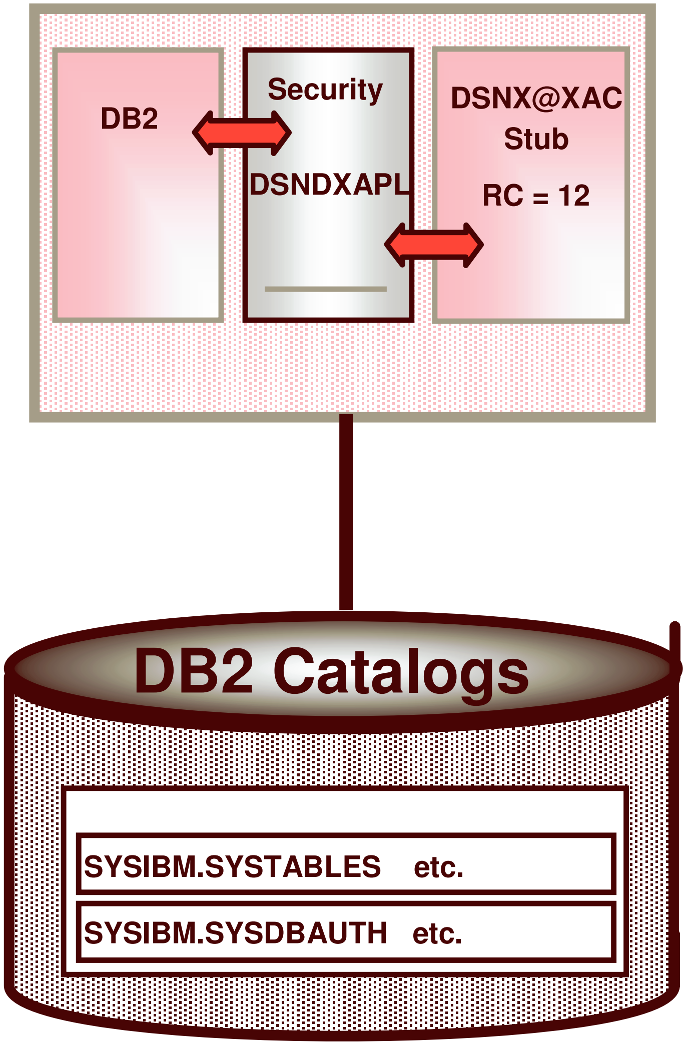
- Overview
- RACF Access Control Module
- Authorization processing
- Mapping DB2 Authorization Checks
- Scope of RACF classes
- Installation
- Migration
- New with DB2 V8
  - Long Name Support
  - Multilevel Security

Overview

- **Prior to DB2 Version 5 and OS/390 Release 4, only DB2's 'native' security mechanisms (GRANT and REVOKE) could be used to control access to DB2 objects such as tables, views, and databases.**

- **DB2 Version 5 defined an exit point (DSNX@XAC) which is called whenever access control decisions need to be made.**

Native DB2 Security



Overview…

- **Problems**
  - DB2 has its own security mechanisms and set of security administrators.
  - Cascading revoke.

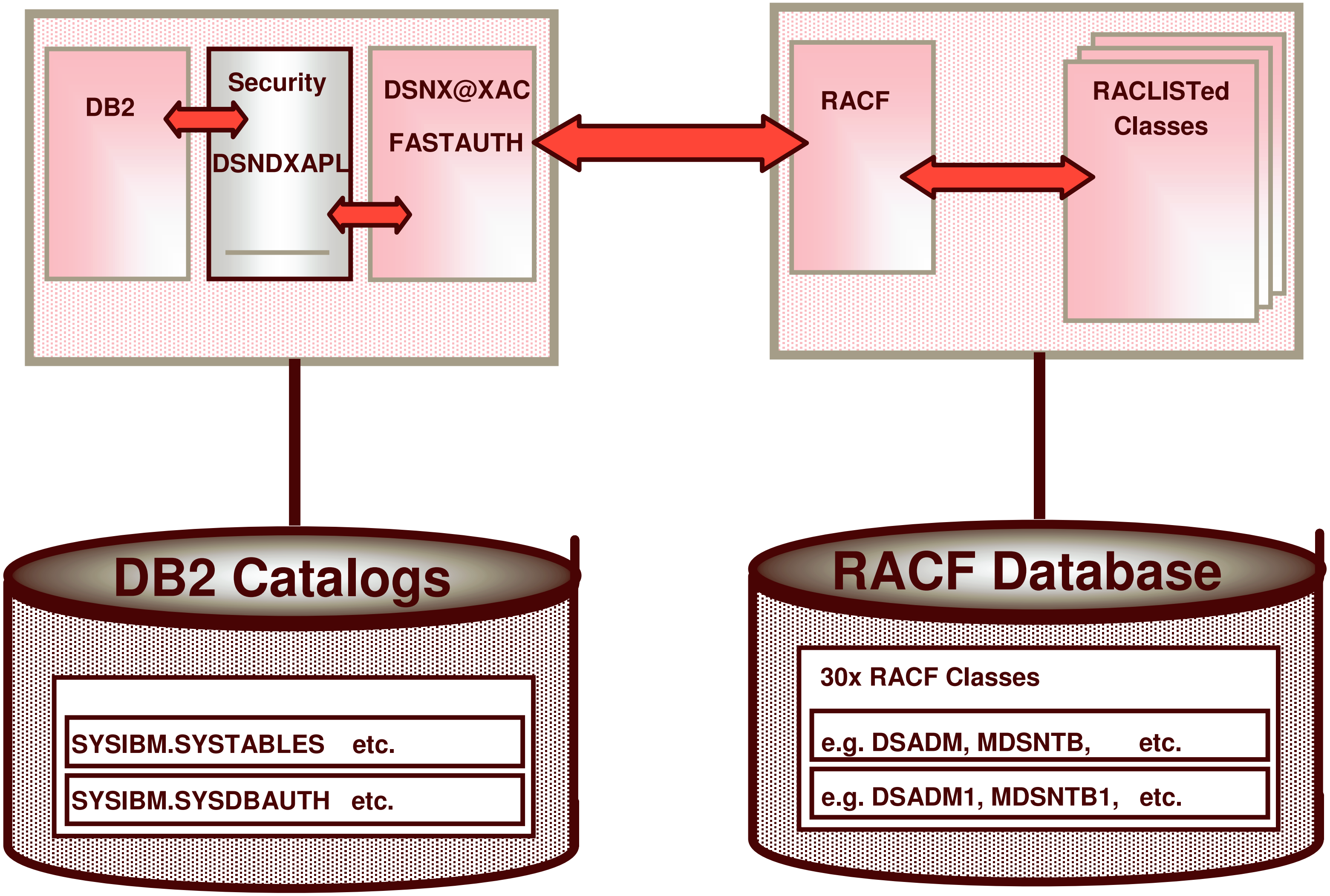
- **Solution**
  - RACF Access Control Module.

- **Customer Value**
  - Allows consolidation of security administration.
  - Integrates DB2 processing with RACF security.

Overview…

- **Since OS/390 R4, RACF has shipped a "plug-in" (also known as the RACF Access Control Module) to be used at the DB2 exit point (DSNX@XAC) that allows RACF to be used to control access to DB2 resources.**
  - For DB2 V5, V6, & V7, the RACF Access Control Module is shipped as part of RACF in 'SYS1.SAMPLIB(IRR@XACS)'.
  - For DB2 V8, the RACF Access Control Module is shipped as part of DB2 in '*prefix*.SDSNSAMP(DSNXRXAC)'.

DB2 Security w/ RACF Access Control Module



Other advantages

- **Centralized Security.**
- **Take advantage of other RACF features such as:**
  - Generics
  - Grouping classes
  - RACFVARS
  - Etc.
- **Eliminate DB2 cascading revoke.**
- **Define security rules before object is created.**
- **Preserve security rules for dropped objects.**
- **Control and audit resources for multiple DB2 subsystems from a single point.**

RACF Access Control Module

- **Support consists of two parts.**
  - Fully supported exit module (also known as the RACF Access Control Module).
  - New classes in the RACF CDT (Class Descriptor Table).

- **RACF Access Control Modules uses the exit point (DSNX@XAC) as documented by DB2.**
  - Exit parameter list - DSNDXAPL

- **DB2 provides a dummy DSNX@XAC routine.**

- **DB2 provides sample LKED JCL for DSNX@XAC.**

RACF Access Control Module …

- **Initialization**
  - RACLISTs profiles for RACF/DB2 authorization checking.
  - If unsuccessful or if no classes are active, exit point will not be driven again.

- **Authorization checking**
  - Check user’s authority to specified DB2 resource.

- **Termination**
  - Clean-up links to profiles loaded into data spaces.

Authorization Processing

- **Authorization checking is what happens most of the time, so lets take an basic overview of how the authorization checking works.**
  - – DB2 exit point is called.
  - – Mapping is found for request.
    - Ownership and/or Match checks (if required)
    - Object Authorities checks (if required)
    - Administrative Authorities checks
  - – Failure reporting / Auditing

- **Upon the first successful check, the RACF Access Control Module returns control back to DB2 with an return code of 0.**

Authorization Processing ...

- **When DB2 has an authorization request, DB2 will call the DSNX@XAC exit point with a parameter list, defined by DSNDXAPL.**

- **The DSNDXAPL provided information for the exit, such as:**
  - The privilege that is being requested.
  - The object type of the privilege.
  - Owner and/or schema name of the object.
  - Object information to help determine security.

Authorization Processing ...

- **DB2 security mechanisms consist of several sets of privileges which can be broken up into two different categories:**
  - Objects
    - Tables, Database, etc.
    - Each DB2 object corresponds to a RACF general resource class.
    - The specific DB2 privilege is then part of the RACF profile name that will be searched for.
  - Administrative authorities
    - DB2 administrative authorities are defined in profiles in the RACF general resource class DSNADM.

Authorization Processing ...

- **Based on the privilege and object type, a mapping can be found to determine what kind of checks need to be done.**
  - Ownership and/or Match check(s) (if required).
    - Basic string compare is done, so there is no call to RACF.
  - Object Authorities check(s) (if required)
    - Profile is built using the object information in DSNDXAPL.
    - FASTAUTH call is then made to RACF.
  - Administrative Authorities check(s)
    - Profile is built using the object information in DSNDXAPL.
    - FASTAUTH call is then made to RACF.

- **Only READ authority is needed for the check to pass.**

Authorization Processing ...

- **Upon the first successful check, the RACF Access Control Module passes back a return code of 0.**
  - **This will overrides all return codes that follow.**
- If all the object checks result in a return code 4, the RACF Access Control Module passes back a return code of 4.
- If at least one object check results in a return code 8, the RACF Access Control Module passes back a return code 8.
- If no object checks are done, and all the admin. checks results in a return code 8, the RACF Access Control Modules passes back a return code 8.
- If no object check are done, and one of the admin. check results in a return code 4, the RACF Access Control Modules passes back a return code 4.

Authorization Processing ...

- **The RACF Access Control Module will not generate a failure until after checking the entire list of profiles.**

- If the RACF Access Control Module passes back a return code 8, a SMF record and ICH408I error message will be produced for the first profile in the list of profiles.

- If the RACF Access Control Module passes back a return code 0 or 4, the RACF Access Control Module will not produce an SMF record.

Mapping DB2 Authorization Checks

- **RACF Access Control Module maps the required DB2 authorization into RACF profiles.**
  - For example let’s look at the **CREATE TABLE** statement.

  - DB2 authorization:
    - The CREATETAB privilege for the database.
    - DBADM, DBCTRL, or DBMAINT authority for the database.
    - SYSADM or SYSCTRL authority.

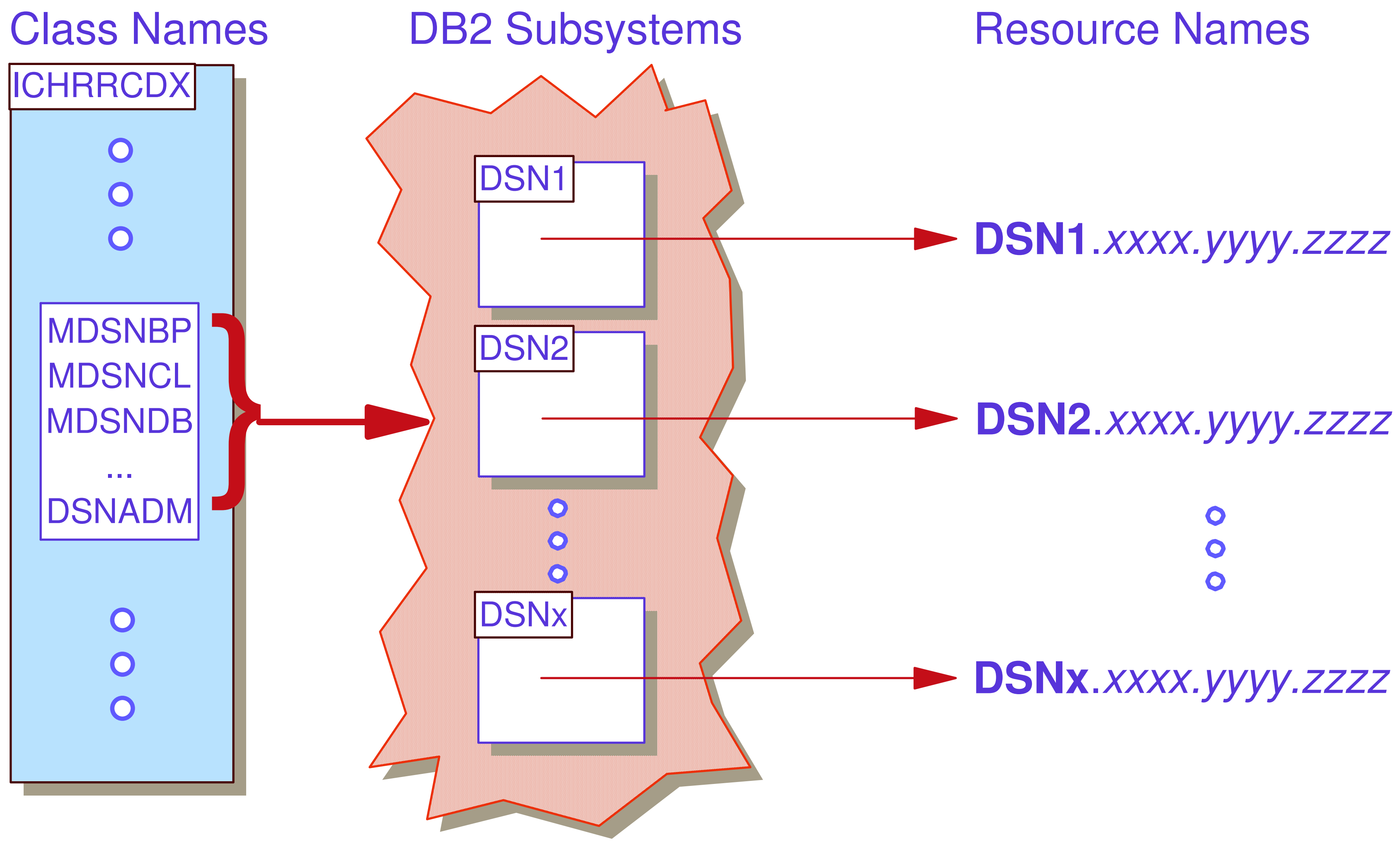
  - RACF authorization:

• *DB-subystem.DB-name*.CREATETAB	MDSNDB
• *DB-subystem.DB-name*.DBMAINT	DSNADM
• *DB-subystem.DB-name*.DBCTRL	DSNADM
• *DB-subystem.DB-name*.DBADM	DSNADM
• *DB-subystem*.SYSCTRL	DSNADM
• *DB-subystem*.SYSADM	DSNADM

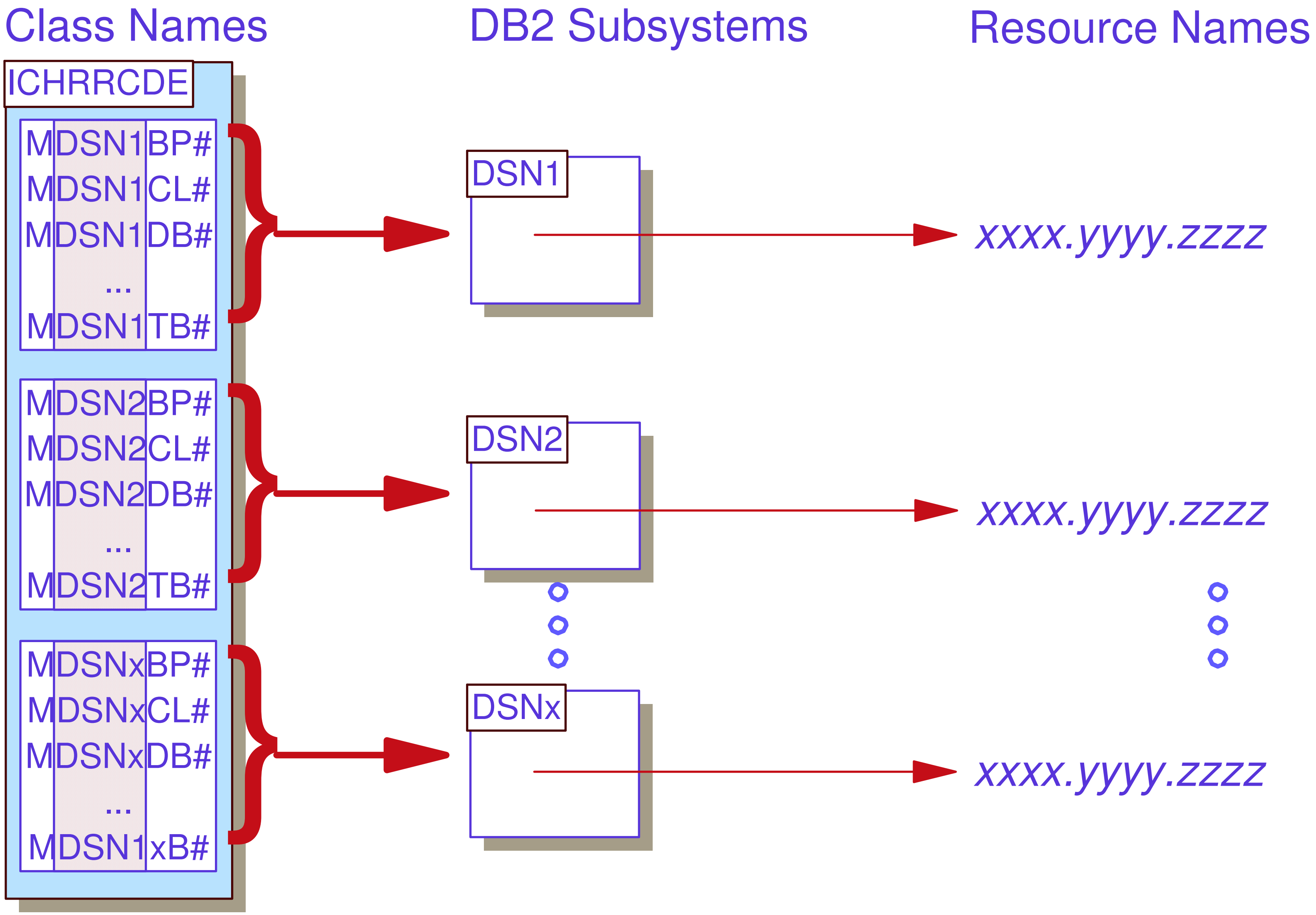
Scope of RACF classes

1. **Multi-Subsystem Scope** *(default)*
   - One set of general resource classes can protect multiple subsystem.
   - Profile names are prefixed with DB2 subsystem name.
   - Classes provided in the IBM supplied CDT are multi-system scope.
2. **Single Subsystem Scope** *(an option)*
   - One set of general resource classes dedicated to one subsystem.
   - Profile names are not prefixed with DB2 subsystem name.
   - Classes must be defined by the installation.

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

IBM Provided DB2 Classes

Administrative	DSNADM
Buffer Pool	MDSNBP
Collection	MDSNCL
Database	MDSNDB
Index	MDSNTB
Java^{tm} archive (JAR)	MDSNJR
Package	MDSNPK
Plan	MDSNPN
Schema	MDSNSC
Sequence^{+}	MDSNSQ
Storage Group	MDSNSG
Stored Procedure	MDSNSP
System	MDSNSM
Table	MDSNTB
Table Space	MDSNTS
User-defined distinct type	MDSNUT
User-defined function	MDNSUF
View	MDSNTB

$^{+}$ Class new for DB2 V8.

Installation

There are several steps to install the RACF Access Control Module.

1. **Locate the RACF Access Control Module is either in:**
   - ‘SYS1.SAMPLIB(IRR@XACS)’ for DB2 V5, V6, & V7.
   - ‘*prefix*.SDSNSAMP(DSNXRXAC)’ for DB2 V8.
2. **Set any option desired to customize the RACF Access Control Module to your installation's needs.**
3. **Assemble and link-edit the RACF Access Control Module into the APF-authorized DB2 exit load library** ‘*prefix*.SDSNEXIT’
   - A sample installation job DSNTIJEX exists to help.

Installation …

Here are the options that can be set in the RACF Access Control Module before it is assembled.

- **&CLASSOPT**
  - Specifies the class scope option.
  - Default = Multi-Subsystem Scope.
- **&CLASSNMT**
  - Specifies the class name *root,* which is character 2-5 of the class name when &CLASSOPT = 2 specified.
  - Default = **DSN**

Installation …

- **&CHAROPT**
  - – Specifies the class name *suffix*, which is the last character of the class name for installation-defined classes.
  - – Default = 1
- **&ERROROPT**
  - – Specifies the action to take in the event of certain errors the RACF Access Control Module encounters
  - – Default = Native DB2 authorization is used.
- **&PCELLCT & &SCELLCT**
  - – Work area to contain local variables.
  - – Default = 50

Migration

- **There is a DB2 to RACF migration tool that was internally developed, but <u>not officially supported.</u>**
  - This can be found at:
    - http://www.ibm.com/servers/eserver/zseries/zos/racf/racfdb2.html

- **Three versions of this migration tool:**
  - RACFDB2/RXSQL – Requires RXSQL
  - RACFDB2/BatchPipes – Requires BatchPipes or MVS Pipes product.
  - RACFDB2 for V5/V6 – Requires DB2 V6 or refreshed DB2 V5.1

Migration …

- **The migration tools basically converts contents of SYSIBM.SYSxxxAUTH tables to RACF profiles.**
  - See **README** file for more details.

- **Utility is also documented in the ITSO Red book: OS/390 Security Server Enhancements (SG24-5158)**
  - http://www.redbooks.ibm.com/redbooks/pdfs/sg245158.pdf

Other DB2 V8 features

- **What new V8 features have we talked about.**
  - New shipping mechanism for IRR@XACS.
  - **SEQUENCE** objects (in the new class MDSNSQ).

- **What other things are new in V8?**
  - Availability of accessor environment element (ACEE) with DB2 "-" commands.
  - WARNING mode support.
  - **REFRESH** privilege on materialized query tables.
  - Allow DBADM to create **VIEWs** for others.

and….

Long Name Support

- **DB2 has extended the lengths that may be specified for many of its constructs.**
- **These longer DB2 names result in longer RACF resource names**
- **Several RACF general resource classes have been updated to support these longer names:**
  - The RACF general resource classes MDSNTB, DSNADM, MDSNCL, MDSNSG, MDSNUT, MDSNUF, MDSNSC, MDSNSP, and MDSNJR now have a maximum profile length of 246 characters.
- **SCHEMA names are truncated at 100 characters when building a RACF resource name**

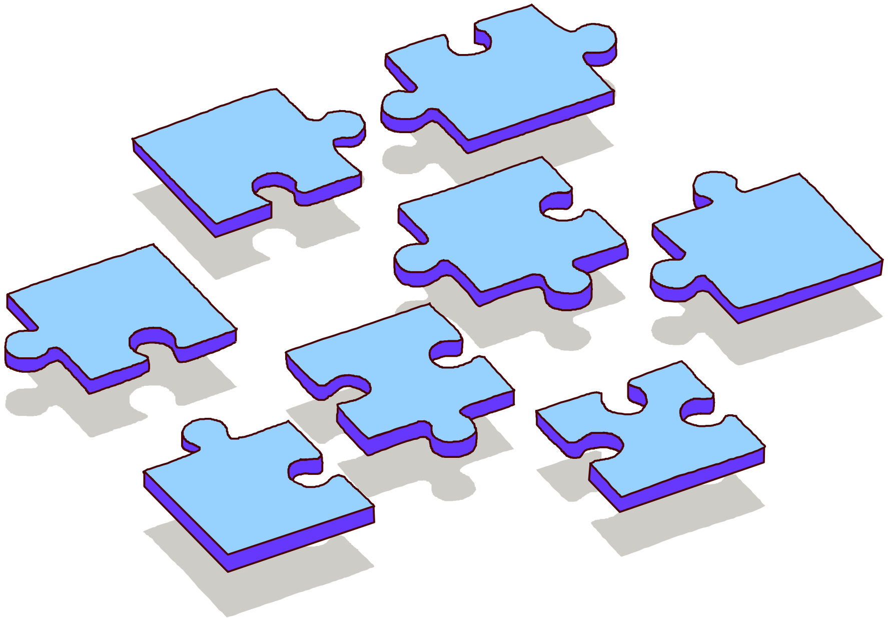
Multilevel Security

The RACF Access Control Module does support multilevel security for DB2.

- Profiles in the DB2 classes can have security label associated with it.
  - Only in a multilevel security check might the user need UPDATE authority to the DB2 profile.
- Some of the DB2 classes require a security label for **ALL** the profiles in that class, **if and only if**, MLACTIVE is on.
- DB2 rows in a table can also have their own security label as well.
  - **NOTE:** There is no need to install the RACF Access Control Module if you **ONLY** want to do row-level multi-level security support.

Q & A

- **Any final questions?**



Reference

- **RACF Security Administrator's Guide**
  - http://publibz.boulder.ibm.com/epubs/pdf/ichza751.pdf
  - Chapter 13 – Controlling Access to DB2 Objects
  - Appendix D – RACF External Security Module …

- **ITSO Red book: OS/390 Security Server Enhancements (SG24-5158)**
  - http://www.redbooks.ibm.com/redbooks/pdfs/sg245158.pdf
- **ITSO Red book: Multilevel Security and DB2 Row-Level Security Revealed (SG24-6480)**
  - http://www.redbooks.ibm.com/redpieces/pdfs/sg246480.pdf

Reference

- **DB2 Universal Database for z/OS: RACF External Security Module Guide and Reference (SC18-7433)**
  - http://publib.boulder.ibm.com/epubs/pdf/dsnraj11.pdf
- **DB2 Universal Database for z/OS: Administration Guide (SC18-7413)**
  - http://publib.boulder.ibm.com/epubs/pdf/dsnagj11.pdf
- **DB2 Universal Database for z/OS: SQL Reference (SC18-7426)**
  - **http://publib.boulder.ibm.com/epubs/pdf/dsnsqj11.pdf**
- **RACF and DB2: Teamed for Security; Michael Jordan, Roger Miller, Mark Nelson, Technical Support Magazine, October, 1997**
  - **http://www.naspa.com/PDF/98/06-pdf/T9806001.pdf**