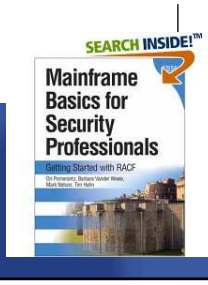
RACF® z/OS® V1.13 Update

NY RACF Users Group

March 2011

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



Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

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

RACF Access Control Module for DB2 for z/OS Version 10

DB2 V10: New DB2 System Authorities

- **DB2 for z/OS Version 10 introduces new system authorities that allow for a finer granularity of control:**
  - **SECADM:** Manage all of the security-related objects in DB2 and control access to all DB2 resources in native DB2 security
  - **System DBADM:** Manage most objects in a DB2 subsystem, without having the ability to access data or control access to data
  - **DATAACCESS:** Access data in all user tables, materialized query tables, and views and execute plans, packages functions and procedures in a DB2 subsystem.
  - **ACCESSCNTL:** Grant all authorities and privileges except, DBADM, DATAACCESS, ACCESSCTRL and privileges on security-related objects.
  - **SQLADM:** Monitor and tune DB2 without have any other privilege

DB2 V10: New DB2 System Authorities…

- **If you are using the RACF Access Control Module for DB2 (DSNXRXAC) you can grant these authorities by giving a user READ authority to these resource names in the indicated class:**

DB2 Authority	RACF General Resource Class	Resource Name
ACCESSCTRL	DSNADM	*db2-subsystem*.ACCESCTRL
DATAACCESS	DSNADM	*db2-subsystem*.DATAACCESS
EXPLAIN	DSNADM	*db2-subsystem*.EXPLAIN
SECADM	DSNADM	*db2-subsystem*.SECADM
SQLADM	MDSNSM	*db2-subsystem*.SQLADM
System DBADM	DSNADM	*db2-subsystem*.SYSDBADM

DB2 V10: Other New Security Functions

- **Separation of Duties**
  - You can configure DB2 to prevent users with SYSADM authority from altering authorizations, thus restricting security-related work to SECADM users.
  - This is done by setting the “SEPARATE SECURITY” ZPARM to ‘YES’
  - When SEPARATE_SECURITY is set to ‘YES’, then the SYSADM and SYSCTRL authorities cannot be used to affect the security characteristics of the system. Specifically:
    - The SYSADM authority does not allow the management of security objects, such as roles and trusted contexts.
    - The SYSCTRL authority does not allow the management of roles.
    - The SYSADM and SYSCTRL authorities cannot perform grants and cannot revoke privileges granted by others.
- **Row and Column Access**
  - DB2 allows you to restrict access to the contents of a table by row by and column

z/OS V1.13 Preview Announcement for RACF

z/OS V1.13 Preview Announcment (RACF)

- **RACF Remote Sharing Facility (RRSF)** will be designed to **support the use of TCP/IP connections**, in addition to the current support for SNA Advanced Peer-to-Peer Communications(APPC). When used with TCP/IP, **RRSF will be designed to use Application-Transparent Transport Layer Security (AT-TS) to authenticate peer RRSF nodes and encrypt replication traffic.** AT-TLS provides encryption algorithms **thought to be stronger than those available using APPC**. A sample rule that specifies the strongest available encryption method is planned to be provided. The use of TCP/IP is intended to help improve usability, simplify network configuration, and improve the security of RACF data shared between RACF nodes in the RRSF network.

z/OS V1.13 Preview Announcement (RACF)…

- **What this means is that you can:**
  - Manage your RRSF network using the same skills as the rest of your TCP/IP network
  - Ensure that the same network security policy (IDS, IPS, etc.) is in place for your RRSF network as in place for the rest of your z/OS TCP/IP network
  - Utilize the encryption and peer-node authentication of AT-TLS
  - Keep up with improvements in z/OS Communications Server Security

z/OS V1.13 Preview Announcement (RACF)…

- **RACF is planned to support hardware-generated Elliptic Curve Cryptography (ECC) secure keys**, giving you the ability to issue and use certificates hardware-protected ECC keys**.**

- **RACF support is planned for generating Elliptic Curve Cryptography (ECC) secure keys using the Crypto Express3 Cryptographic Coprocessors (CEX3C) available for zEnterprise servers.** New keywords on the RACDCERT command are designed to allow **you to specify that an ECC key be stored in the ICSF public key data set (PKDS). Corresponding hardware ECC key support is planned for PKI Services.** This new support is intended to allow you to expand your use of certificates with ECC keys protected by hardware.

z/OS V1.13 Preview Announcement (PKI)…

- **For z/OS V1.13, z/OS PKI Services** is planned to **add support for DB2 9 for z/OS or later as its back-end key store**, enabling enterprise-class scale and resilient certificate management.
- **What this means to you:**
  - Leveraging DB2's capabilities for storage and retrieval of large numbers of digital certificates
  - Remove the 32K limit on Certificate Revocation Lists (CRLs)

z/OS V1.13 Statement of Direction (RACF)

- **z/OS V1.13 is planned to be the last release to support BPX.DEFAULT.USER. IBM** recommends that you **either use the BPX.UNIQUE.USER support that was introduced in z/OS V1.11, or assign unique UIDs to users who need them and assign GIDs for their groups.**

z/OS V1.13 Statements of Direction (RACF)…

- **Background: Assigning UID and GIDs**
  - **RACF 2.1 (1994):** Introduced OMVS segments for USERs and GROUPs.
    - Users with an OMVS segment could now use “Open MVS” (now z/OS UNIX System Services)
  - **OS/390 R2.4 (1997**): Introduced BPX.DEFAULT.USER FACILITY class profile
    - Allows assigning UIDs and GIDs to users and groups who do not have OMVS segments; ***One UID and one GID for all default users***

z/OS V1.13 Statements of Direction (RACF)…

- **Background: Assigning UID and GIDs…**
  - **z/OS V1.4 (2002):** Introduced AUTOUID/AUTOGID keyword on ADDUSER, ALTUSER, ADDGROUP, ALTGROUP
    - RACF could now find the next available UID or GID using the BPX.NEXT.USER profile in the FACILITY class
    - Required enabling RACF Alternate Index Mapping (“AIM”) to stage 2
      - Limitation of 129 eight-character users sharing one UID
      - Required running migration utility (“IRRIRA00”)
  - **z/OS V1.11 (2009):** Automatic generation of OMVS segment for USERs and groups
    - Built upon AUTOUID/AUTOGID
    - Requires AIM stage 3
    - Uses the BPX.UNIQUE.PROFILE in the FACILITY class

z/OS V1.13 Statements of Direction (RACF)…

- **What this means to you:**
  1. If you are using BPX.UNIQUE.USER then:
     - You are not using BPX.DEFAULT.USER (even if it is defined)
     - This SoD has no impact to you.
  2. If you are already assigning UIDs and GIDs to all users using z/OS UNIX System Services by assigning OMVS segments to all necessary users and groups, then:
     - You must continue to assign all new users and groups OMVS segments
  3. If you are already assigning UIDs and GIDS to all users user z/OS UNIX Sstem Services by defining OMVS segments using AUTOUID/AUTOGID (which uses BPX.NEXT.USER) then:
     - You are already using AIM at a minimum of stage 2
     - You must continue to assign all new users and groups OMVS segments
  4. If you are using only BPX.DEFAULT.USER
     - You must either move to the automatic generation of OMVS user and group segments or assign OMVS user and group segments to all necessary users and groups