RACF® z/OS® V1R12 RAS Enhancements

RACF Users Group
Fall 2010

Scott Woolley, CISSP®
z/OS® Security Server (RACF) Design and Development
IBM Poughkeepsie
swoolley@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.

Agenda

RAS Enhancements for RACF z/OS V1R12

- SAF TRACE filtering by user ID or class
- “Ghost” generic profile avoidance

SAF TRACE Filtering

- **The SAF TRACE facility, allows an in-depth analysis of the calls made from resource managers to RACF**
  - Can trace at the RACROUTE, callable service, or ICHEINTY (database) level
  - Can select events based on jobname and address space ID
  - Trace records are written to GTF and formatted with IPCS
  - Intended for use under the direction of RACF's service team
  - Example syntax:

```
SET TRACE (RACROUTE(ALL)
           ASID(*)
           JOBNAME(APP321))
```

SAF TRACE Filtering by Class

- **With V1R12, you can select trace events for RACROUTE and database (ICHEINTY) access by class.**

```
SET TRACE(… CLASS(class … |*)      |
            IFCLASS(class …|*)     |
            NEVERCLASS(class …|*) |
            NOCLASS)
```

- **CLASS is an inclusive setting**
  - Trace events which match CLASS may be recorded.
  - Trace events which do not match CLASS() *may* be recorded if they match another setting, like ASID or JOBNAME.
- **IFCLASS is an exclusive setting**
  - Trace events which do not match IFCLASS are not recorded, even if they match another trace setting, like ASID or JOBNAME.
- **NEVERCLASS**
  - Trace events which match are NOT recorded, regardless of other settings

SAF TRACE Filtering by User ID

- **With V1R12, you can also select trace events for RACROUTE by user ID:**

```
SET TRACE(… USERID(userid … |*) |
          IFUSERID(userid … |*) |
          NEVERUSERID(userid … |*) |
          NOUSERID)
```

- **USERID is an inclusive setting:**
  - Trace events which match the user ID are recorded
  - Trace events which do not match USERID *may* be recorded if they match another setting, like CLASS or JOBNAME
- **IFUSERID is an exclusive setting:**
  - Trace events which do not match IFUSERID are not recorded, even if they match another trace setting, like CLASS or JOBNAME
- **NEVERUSERID**
  - Trace events which match are NOT recorded, regardless of other settings

“Ghost” Generics

- **RACF requires that SETROPTS GENERIC is in effect for a class before generic profiles are defined in the class**
  - If not, the profile is created as a discrete profile, even if it contains generic characters such as “*” or “%”
  - Profiles such as these are:
    - Not involved in access control decisions
    - Not what you intended
    - Not displayed by RLIST, except for “RLIST *”
    - Displayed by SEARCH without the “(G)” after the name
    - Annoyances to security administrators, systems programmers, and auditors
    - To fix, require that you turn GENERIC and GENCMD off for the class, delete the profile, SETROPTS GENERIC the class (which also turns GENCMD on), and redefine the profile.

“Ghost” Generics…

- **With V1R12, RACF now issues a warning message when creating a profile which contains generic characters in a non-generic class**

```
ICH10321I The profile name profile_name contains generic
characters, but generics are not enabled for class
class_name.  A discrete profile has been created.
```

“Ghost” Generics…

- **In V1R12 both RLIST and SEARCH commands will now label ghost generic profiles as '(UNUSABLE)' in their output**

```
RLIST FACILITY T*

CLASS NAME
----- ----
FACILITY T* (UNUSABLE)  <--- ghost generic indicator
...
CLASS NAME
----- ----
FACILITY T* (G)  <-- Standard generic indicator
...
```

“Ghost” Generics…

- **NOGENERIC keyword added to the RDELETE command to facilitate the deletion of ghost generic**

```
RDELETE FACILITY T* NOGENERIC
```

- **Specifies that you want RACF to delete the discrete profile**
  - If a generic profile with the same name exists, it will be unaffected.
- **SAF callable service R_admin also updated such that the delete function supports a GENERIC=N flag**
- **RACF panels also support NOGENERIC processing**

Questions?