RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 5
Issue 1

January
2011

IGGCSI00 and Catalog Access

During a project to reduce catalog ALTER access permissions (for the reasons cited in our July 2008 newsletter article "Auditors: Review ALTER Access to the Catalogs"), we noticed that the number of catalog ALTERs by certain users matched their executions of the catalog search interface program IGGCSI00. This led to our discovery that when a user who is permitted ALTER access to a catalog opens it using IGGCSI00, the program requests ALTER access even though only read operations are to be performed. If the user is permitted less than ALTER, the program only requests READ. We have since been successful in removing ALTER permissions from all such users without incident.

Prevent Connection Mishaps

Many people think RACF's only use is to provide security, but it can also prevent potentially costly connection errors within your system. For instance, profiles in the DSNR class can stop production CICS regions from inadvertently connecting to test DB2 subsystems. VTAMAPPL profiles can prevent non-APF-authorized processes from opening the VTAM ACBs of production systems. DFHAPPL-prefixed profiles in the FACILITY class can block test CICS regions from binding to production regions.

WHEN(CONSOLE(SDSF))

When implementing OPERCMDS profiles as part of an SDSF protection project, you will discover users need access to resources such as *jesname*.CANCEL.BAT. If you permit access using the standard access list, users will have authority to cancel any job. If your intent is to allow users to cancel or otherwise manage only those jobs they can access within the confines of SDSF, grant them conditional access to OPERCMDS profiles using PERMIT parameter WHEN(CONSOLE(SDSF)).

To use this conditional permission, you need to activate the CONSOLE class and create a profile covering resource SDSF. Since CONSOLE is a default return code 8 class (no profile = no access), start by activating GENERIC for CONSOLE and defining profile ** with UACC READ before activating the class.

Websphere Library Change

This tip applies if (a) you have a PROGRAM class profile of * or ** defined to maintain a clean program environment for your z/OS Unix daemons, and (b) you have Websphere Application Server (WAS). The version of WAS determines what libraries are to be included in this PROGRAM profile. For versions prior to V7, include libraries *hlq*.SBBOLOAD, *hlq*.SBBOLPA, and *hlq*.SBBOLD2. Once at V7, you can remove these libraries because the programs have been moved into z/OS Unix directories.

When upgrading to V7, you may encounter problems if you do not assign the programs the program-controlled extended attribute 'p'. For more information, search the IBM website for "ICH420I and BPXP014I messages when logging into the Form Based Web Application."

Performance: CA-Endevor LAT

If you have implemented Endevor’s External Security Interface (ESI), you can use the security Look Aside Table (LAT) to improve performance. You activate it using the LATSIZE parameter located in the ESIDFLTS section of Endevor's BC1TNEQU security table.

Endevor uses the LAT to cache the results of RACROUTE resource access authorization requests sent to the z/OS Security Authorization Facility (SAF) interface. Before calling SAF, Endevor checks the LAT for a prior authorization result for the same resource and will reuse a prior result rather than calling SAF again.

LATSIZE specifies the number of 4K pages to be used for the LAT and is set to an integer from 0 to 524287. Each 4K page holds about 35 access request results. Note that a LATSIZE of 0 disables the LAT, and 0 is the default value.

For maximum benefit be sure the LAT is large enough to hold the results of all access requests an individual user is likely to encounter during a typical Endevor session. This is influenced by the number of resource names created by format statements in the NAMEQU section of the security table. Once the LAT is full, Endevor will make repeated SAF calls for resources whose results could not be cached.

The Endevor Security Guide recommends a LATSIZE value between 2 and 10 (70 - 350 results). We recommend an initial setting of 10. Ask your Endevor Administrator to turn on the ESI trace facility periodically to look for repeated SAF calls for the same resource by the same user. This indicates the LAT is too small. Increase the LATSIZE value to address this condition and also provide for expansion.

Note that a LAT is created for each individual user when the user begins an Endevor session and is discarded when the user exits Endevor. If a user is denied access to a resource and is subsequently permitted the required access, the user will need to exit and reenter Endevor for the permission to take effect. Otherwise the cached access denial will continue to prohibit access.

Auditors: Check Password History Option

RACF can be configured to remember up to 32 of each user's most recent prior passwords. To guard against reuse of passwords within two years, verify that the number of passwords saved multiplied by the change interval exceeds 730. SETROPTS LIST displays both options.

```
PASSWORD PROCESSING OPTIONS
    PASSWORD CHANGE INTERVAL IS   45 DAYS.
    …
    17 GENERATIONS OF PREVIOUS PASSWORDS
           BEING MAINTAINED.
```

Correction: SMP/E Protection

Our October 2010 newsletter listed SMP/E FACILITY resources as CIM.CMD.*command* and CIM.PGM.*program*. They are actually GIM.CMD.*command* and GIM.PGM.*program*.

RSH News

We are so often faced with determining why particular profiles were created ages ago and whether they are still effective that we now jokingly call ourselves **RACF Archeologists**. In the process though, we have become experts at evaluating ancient profiles and finding the adjustments necessary to provide the protection and performance required by today's systems. If you need help understanding and modernizing your profiles, call us.

Receive top-notch RACF training without leaving home or incurring travel costs. Check out our **remote, web-enabled, instructor-led training**.

Upcoming ***RSH RACF Training***:

- RACF - Audit for Results
  April 12-14, 2011 - Boston, MA
- RACF - Intro and Basic Administration
  January 24-28, 2011 - WebEx
  May 10-12, 2011 - Boston, MA
- RACF and z/OS Unix
  February 8-10, 2011 - WebEx

See our website for details and registration form.