RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 4
Issue 4

October
2010

SMP/E Protection

Beginning in z/OS 1.12 or earlier with APAR IO11698, System Modification Program / Extended (SMP/E) checks FACILITY resources to determine if a user is authorized to perform certain maintenance functions. The resource names have the format GIM.CMD.*command* and GIM.PGM.*program*. Users must be permitted READ access to perform the function.

***WARNING*:** If the above APAR is applied to your system before you define profiles, your SMP/E technicians will be unable to back out problem changes or apply further maintenance. RSH recommends you define profiles immediately in case the APAR is applied without forewarning.

For more details, see IBM's SMP/E V3R5.0 for z/OS V1R12.0 User's Guide.

Performance: GENERICANCHOR

When a user attempts to access a dataset or a non-RACLISTed/GENLISTed general resource that is not protected by a discrete profile, RACF searches for a list of related generic profiles in the user's address space in order to identify the protecting profile. For datasets, the list includes all profiles with the same High Level Qualifier (HLQ). For general resources, it usually includes all profiles in the class. These lists are known as Generic Anchor Table Entries or GATEs.

If no GATE is found, RACF retrieves a list of generic profiles from its database and builds one. RACF will reuse this GATE for subsequent access requests. RACF also individually fetches, saves, and reuses copies of the related generic profiles as needed for authorization checking.

For releases of z/OS prior to 1.12, RACF keeps 4 GATEs for each address space. When all the GATEs are filled and a different dataset HLQ or general resource is accessed, RACF drops the least recently referenced GATE and replaces it with one for the newest resource. An address space that randomly accesses many different HLQs and resources may experience thrashing, a condition where GATEs are continuously dropped and created. This can nullify the performance benefits gained by keeping reusable lists and profiles in memory, especially when the lists of profiles are long.

In z/OS 1.12, the number of GATEs can be increased from 4 to 99 for the system as a whole and for individual jobs or tasks using the SET command with the new GENERICANCHOR operand. SET commands are executed by the RACF subsystem during initialization via its parameter library and afterwards via the console. The optimum number of GATEs varies by installation depending on factors such as available memory and projected reduction in I/O.

For more details, see IBM's z/OS V1R12.0 Security Server RACF Systems Programmer's Guide and Command Language Reference.

Correction: FILEPROCMAX

Early edition copies of our July 2010 newsletter have an error in the article "DB2 DDF and MAXFILEPROC". To increase the number of sockets a task may open, use the command operand FILEPROCMAX, not MAXFILEPROC. (The PARMLIB parameter is MAXFILEPROC.)

FASTAUTH Now Honors TRUSTED and PRIVILEGED

In z/OS 1.11, RACROUTE REQUEST= FASTAUTH began honoring Started Task TRUSTED and PRIVILEGED authority and granting such tasks unrestricted access to all resources. If you previously permitted Started Tasks access to resources only checked by FASTAUTH, you can remove those permissions.

***NOTE*:** You can no longer rely on FASTAUTH to restrict access by TRUSTED and PRIVILEGED Started Tasks. To restrict their access, you will need to remove these privileges and instead use ordinary permissions for all their access needs.

Auditors: Check User Password Change Intervals

The frequency with which a user's password must be changed is determined by the lesser of the interval set for the user's ID or the password interval set by SETROPTS, which defines the upper limit for all users. Execute SETROPTS LIST to display the system-wide limit.

```
PASSWORD PROCESSING OPTIONS
  PASSWORD CHANGE INTERVAL IS   45 DAYS.
```

To see the limit for a user, execute LISTUSER.

```
USER=JSMITH1  NAME=JOHN SMITH …
 …  PASSDATE=10.256 PASS-INTERVAL= 30 …
```

Every ID has its own password interval setting. It is initially set to the SETROPTS value in effect at the time the ID is created. The PASSWORD command can be used to change the interval to a value equal to or less than the SETROPTS value. Ensure the SETROPTS limit adheres to organizational security standards.

If the SETROPTS limit is lowered after an ID is created, the ID retains its higher setting, but the lower SETROPTS limit is used to enforce changes. LISTUSER displays the lesser value. User records in an IRRDBU00 utility unload of the RACF database show the actual intervals.

The PASSWORD command can also assign NOINTERVAL to an ID, which exempts it from having to make periodic password changes. For IDs with NOINTERVAL, LISTUSER displays N/A instead of a number for PASS-INTERVAL.

The assignment of NOINTERVAL should be scrutinized. It is typically assigned only to IDs used by processes on other platforms to access the mainframe. Examples are IDs used for Remote Job Entry (RJE) batch jobs and by distributed servers for FTP or web applications. Review procedures for password change in the event of compromise or staff changes.

At one time, NOINTERVAL was appropriate for Started Tasks and non-RJE batch IDs. No more. These IDs should now be made PROTECTED.

IPv4 Terminal IDs

The terminal ID of a user who connects to the mainframe via TCP/IP is an IP address. IPv4 addresses are comprised of four sets of digits of from 0 to 255 each (e.g., 192.44.18.11). SMF records show the address as a hexadecimal value comprised of four pairs of hexadecimal characters (e.g., C02C120B). Each pair equates to a set of digits (e.g., C0 = 192).

To find the decimal equivalent of each hexadecimal pair, open MS-Windows' Calculator and select View - Scientific. Select the Hex button, enter the hex value, and then select the Dec button to display the decimal value.

RSH News

Want ***a RACF expert at the ready*** to answer questions, provide advice, or tackle complex tasks? Call us about our ***Retainer Service***.

Upcoming ***RSH RACF Training*:**

- RACF - Audit for Results
  October 26-28, 2010 - Boston, MA
  April 12-14, 2011 - Boston, MA
- RACF - Intro and Basic Administration
  October 5-7, 2010 - Boston, MA
  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.

RSH CONSULTING, INC.
RACF Specialists
www.rshconsulting.com ■ 617-969-9050
29 Caroline Park, Newton, Massachusetts 02468