RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 5
Issue 2

April
2011

Trust SMS

The MVS Initialization and Tuning Reference for z/OS 1.12 added SMS to the list of Started Tasks that should be given TRUSTED authority. The manual also replaced OMVSKERN with OMVS in the list of optional TRUSTED tasks.

Proper RACF Database Backup

RACF does not handle I/O to its databases as one might expect. Rather, it opens its databases during IPL, closes them shortly thereafter, and subsequently accesses the databases via direct disk address even though they are not open.

When a typical process is working with a dataset, the dataset remains open until the process completes. This alerts other processes that the dataset is in use. Since RACF does not keep the databases open, other processes may be unaware that the databases are in use.

This behavior can compromise backups of your RACF databases. If you backup the databases with a utility such as DFSMSdfp's ADRDSSU or FDR, the utility may copy the database at the same instant RACF is updating it. The resulting backup might be corrupted and unusable.

To create viable backups of your RACF databases, use the IRRUT200 utility. It suspends updates while creating the backup.

A quarter of the RACF installations we have reviewed have not been using IRRUT200 to back up their databases. Contact your Storage Administrators and ask what method they use.

Demise of BPX.DEFAULT.USER

z/OS 1.13 will be the last release to support FACILITY class profile BPX.DEFAULT.USER. Thereafter, users will require an OMVS segment with a uid in order to access Unix and TCP/IP socket applications such as FTP. Groups used for logon (e.g., user default groups) will need OMVS segments with gids.

To help replace BPX.DEFAULT.USER, z/OS 1.11 introduced the FACILITY class profile BPX.UNIQUE.USER. Defining this newer profile causes RACF to automatically add OMVS segments and assign ids to users and groups that do not already have segments. RACF creates the segments when the user first accesses Unix (i.e., dubs). BPX.UNIQUE.USER works in combination with FACILITY class profile BPX.NEXT.USER, which defines the uid and gid number ranges to be used for automatic id assignment. Use of these profiles requires your databases to be in the Application Identity Mapping (AIM) structure.

In analyzing and planning the replacement of BPX.DEFAULT.USER, we have found it helpful to review reports listing every user dubbing with either the default uid or the default gid. We use ICETOOL to select INITOEDP records from SMF Unload data and generate the reports.

MVS.DISPLAY.TCPIP

RSH discovered MVS.DISPLAY.TCPIP is missing from the OPERCMDS resources listed in the z/OS MVS System Commands manual. READ access is required to execute DISPLAY TCPIP. We reported the omission to IBM.

RACF Administrator's DFLTGRP

If a RACF Administrator neglects to code the DFLTGRP(*group*) operand on an ADDUSER command, the Administrator's current connect group (most likely the Administrator's own default group) becomes the new user's default group. During several RACF reviews, we found

inappropriate users mistakenly connected to the Administrator's group due to this error. Thus we recommend the RACF Administrator's default group not be permitted access to prevent the unintentional granting of access to such users.

RACF Protect TCP/IP Ports

The TCP/IP configuration statements PORT and PORTRANGE can be used to reserve ports for processes executing with specific job names. These statements are found in the dataset referenced by the PROFILE DD statement in the TCPIP Started Task PROC. The following example reserves use of port 80 for a job named HTTPSTC when using the TCP protocol.

PORT 80 TCP HTTPSTC

Note the reservation is by job name, not the USERID on the job. Conceivably, any user who could submit a job named HTTPSTC could open this port and masquerade as the HTTP server.

JESJOBS class profiles could be used to indirectly restrict use of a port by limiting who can submit jobs with the specified name. This would not, however, restrict Started Tasks. We feel a better approach is to use SERVAUTH class profiles and control access by USERID.

To use SERVAUTH, add the keyword SAF to a PORT or PORTRANGE statement as shown below. (The * matches any job name.)

PORT 80 TCP * SAF HTTPSERV

The SAF keyword directs TCPIP to check the user's access to SERVAUTH resource EZB.PORTACCESS.*sysname.tcpname.safname*, where *sysname* is the MVS system name, *tcpname* is the TCPIP task name, and *safname* is the name following the SAF keyword, which in this case is HTTPSERV. The resulting resource name might look like this:

EZB.PORTACCESS.PRD1.TCPIP.HTTPSERV

To enable job HTTPSTC to bind to port 80, permit its USERID read access to the profile protecting this resource.

Auditors: Review Password Minimum Change Interval

RACF can be configured to stop users from changing passwords repeatedly within a short time period. This inhibits reuse of old passwords sooner than allowed by policy. The minimum interval can be set from 1 day up to the required password change interval value. The default is 0 days, which allows unlimited password changes in a single day. Use the SETROPTS LIST command to display this option.

```
PASSWORD PROCESSING OPTIONS
 PASSWORD MINIMUM CHANGE INTERVAL IS 3 DAYS.
```

RSH News

Be sure to attend our **RACF - Audit for Results** course before your next RACF audit or review. You will learn about common weaknesses and best practices, and we will examine and discuss your current RACF controls. By the end of class, your audit will be almost done, and you will have a long list of findings and recommendations. Register for a course today.

Upcoming ***RSH RACF Training*:**

- RACF - Audit for Results
  April 12-14, 2011 - Boston, MA
  October 25-27, 2011 - Boston, MA
- RACF - Intro and Basic Administration
  May 10-12, 2011 - Boston, MA
  October 11-13, 2011 - Boston, MA
- RACF and z/OS Unix
  July 19-21, 2011 - WebEx

See our website for details and registration form.