RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 4
Issue 3

July
2010

Goodbye VSAMDSET and SYSCTLG

Groups VSAMDSET and SYSCTLG have been fixtures in the RACF database for more than two decades. Even though they have not served a security purpose for some time, the IRRMIN00 utility would always define them to a new RACF database, and RACF would automatically restore them at IPL if they were missing. All this changed as of z/OS R1.9. These groups are no longer required and can now be deleted.

DB2 DDF and FILEPROCMAX

Started tasks created for DB2's Distributed Data Facility (DDF), typically having names with the suffix DIST, are often assigned UID 0 (root authority). This enables these tasks to invoke callable service 'setrlimit' to raise the maximum number of TCP/IP sockets they can open above the limit established for the system by parameter MAXFILEPROC (specified in PARMLIB member BPXPRMxx).

To avoid assigning these tasks UID 0, simply add FILEPROCMAX to their OMVS segments and set it to the minimally required value. For DB2 V8, this value is 65535. For V9, the value was increased to 131702. (If you previously set FILEPROCMAX for your DB2 DDF tasks to the v8 value, you can change them to the v9 value now in preparation for future upgrades.)

Deleting an Invalid Profile Containing Character '('

We have encountered several cases where a general resource profile was somehow added to RACF with an open left parenthesis character embedded in the name. Getting rid of the profile is problematic because RDELETE assumes an open parenthesis is accompanied by a closing right one and the command fails. A workaround is to code the RDELETE command to delete two profiles, the first being the invalid one and the second a bogus profile name. Enclose both in parentheses. Here is an example.

```
RDEL class (BAD.PROF.WITH(N  XXXXX)
```

OPERCMDS Profile Prefixes

An increasing number of system software products are using the OPERCMDS class to govern use of their commands. Here are prefixes for the ones we know of so far. (Please tell us of any others.)

MVS	z/OS operator commands
jes	JES commands for subsystem *jes*
RACF	RACF commands entered via a console
IMS	IMS Operations Manager commands
vtcs	StorageTek VTCS subsystem *vtcs*

Auditors: Check for Weak Password Rules

RACF password rules are defined using the SETROPTS command. Each rule can specify the minimum and maximum length of the password and its composition with respect to the type of characters allowed. Up to 8 rules can be specified. SETROPTS LIST displays them.

```
PASSWORD PROCESSING OPTIONS
  …
  INSTALLATION PASSWORD SYNTAX RULES:
    RULE 1  LENGTH(6:8)   LLLLLLLL
    RULE 2  LENGTH(5:8)   ********
   LEGEND:
    A-ALPHA C-CONSONANT L-ALPHANUMERIC
      N-NUMERIC V-VOWEL W-NOVOWEL *-ANYTHING
    c-MIXED CONSONANT m-MIXED NUMERIC
      v-MIXED VOWEL $-NATIONAL
```

These rules are checked when a user tries to change the password for his or her own ID or

when a RACF Administrator resets a user's password using the ALTUSER command with the NOEXPIRE operand. To be accepted, the new password must conform to any one of the rules. The rules are not used in combination. Using the example above, a 5 character, all alphabetic password would be acceptable since it matches RULE 2 even though it would be rejected by RULE 1. We regularly find weaker rules that are undermining stronger rules in our security reviews.

Performance: CICS USRDELAY

When a CICS user initiates a transaction that is routed for execution on a remote region which has ATTACHSEC=IDENTIFY specified on its CONNECTION definition, the remote region performs an automatic logon of the user's ID and uses the resulting ACEE for authorization checking. To improve system performance, this ACEE can optionally be retained for reuse with subsequent routed transactions. The length of time an ACEE is retained is determined by the CICS System Initialization Table (SIT) parameter USRDELAY. USRDELAY specifies the number of minutes an ACEE will be retained since its last use. The default is 30 minutes.

The ACEE in the remote region contains a list of the user's groups for authorization checking. If a RACF Administrator connects a user to another group to grant new access *after* the remote ACEE has been created, the change is *not* reflected in the remote ACEE, and the user will not be able to use the new access until the existing ACEE has been purged so that a new, updated one can be created. To accomplish this, the user's only recourse has been to cease executing transactions until the USRDELAY waiting period has lapsed.

This has changed with the introduction of CICS TS 4.1 and z/OS 1.11. CICS will now be notified when the user's profile has changed and will immediately purge the existing ACEE, thereby allowing a new one to be created.

Avoid setting USRDELAY to 0. This causes a logon for every transaction executed and can severely hamper system performance.

SEARCH LEVEL(nn)

Our article "Practical Uses for LEVEL" in the January 2008 edition of RSH RACF Tips introduced you to LEVEL, a two-digit number you can assign to dataset and general resource profiles. If you are now using this feature, you can also use the SEARCH command to find all the profiles with a specific LEVEL number.

```
SR NOMASK CLASS(class) LEVEL(nn)
```

RSH News

We describe our RACF reviews as "***stripping RACF down to bare metal***." We do not simply execute a program that identifies the obvious configuration errors. Rather, we examine and question nearly every profile and search for what may be missing, such as profiles which should exist to protect sensitive functions. We even go beyond RACF to examine system software security parameters like those in CICS and Innovation's FDR. We provide more than 200 recommendations in a typical assessment, and our recommendations for adding staff have often led to the creation of new positions. If you want a ***thorough review*** of your RACF, call us.

Upcoming ***RSH RACF Training***:

- RACF and z/OS Unix **!!! NEW !!!**
  July 13-15, 2010 - WebEx
- RACF - Audit for Results
  October 26-28, 2010 - Boston, MA
- RACF - Intro and Basic Administration
  October 5-7, 2010 - Boston, MA

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