RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 1
Issue 2

July
2007

Entering RACF Commands at the Console

If your installation starts the RACF subsystem, you can execute RACF commands via the console. This capability can be invaluable in helping you recover from a RACF authorization problem that prevents TSO user logons.

To enter RACF commands at the console, it is first necessary to logon. To do so, simply enter the console command LOGON, whereupon the following prompt will be displayed:

```
LOGON          PASSWORD
GROUP          SECLABEL
```

After entering your ID and password, you can enter RACF commands as you would normally from TSO except that you must append the appropriate console command prefix like this:

```
#SETROPTS LIST
```

This prefix is assigned with the INITPARM operand on the RACF subsystem definition in PARMLIB member IEFSSNxx. For example:

```
SUBSYS SUBNAME(RACF)
  INITRTN(IRRSSI00) INITPARM('#')
```

Most installations set the prefix to # in keeping with examples in the RACF manuals. If no INITPARM is specified, the prefix by default becomes the name of the RACF subsystem. If your prefix is the subsystem name, you must include a space between it and the command:

```
RACF SETROPTS LIST
```

To successfully logon and enter commands, you will need the following:

- READ permission to the CONSOLE class profile for the console you are logging onto

- RACF administrative authority sufficient to execute the command (e.g., SPECIAL)

- READ permission to the OPERCMDS class profile for the RACF command, which has the format *racf-subsystem-name.command*:

  ```
  RACF.ALTUSER
  ```

- UPDATE permission to the OPERCMDS class profile for SETROPTS, which has the format *racf-subsystem-name.*SETROPTS (SETROPTS LIST only requires READ)

We strongly urge you to periodically test logon and entry of RACF commands at the console, especially after major system maintenance or the implementation of any new subsystems. Other subsystems may interfere with the entry of RACF commands, and you will want to discover this before you have an emergency.

For details, see IBM's z/OS MVS Initialization and Tuning Reference, Security Server RACF Systems Programmer's Guide, and Security Server RACF Security Administrator's Guide.

Performance: NOYOURACC

When you list a profile using either LISTDSD or RLIST, one of the items displayed is YOUR ACCESS. For a dataset profile or a general resource profile in a class with no companion grouping class, RACF merely checks the UACC and access list of the profile you are listing to determine your level of authority.

With general resources protected by profiles in member/grouping class pairs however, UACCs and permissions in multiple profiles could affect the outcome. To find your access, RACF must retrieve and RACLIST all the profiles in the class pair and then perform an authorization check to get the answer. All this takes place within your own user address space. For member/grouping class pairs with thousands of profiles, a single RLIST will cause significant I/O to the RACF database to fetch the profiles and consume large amounts of CPU time to process them.

RACF provides a means of skipping the process of finding out your access in order to avoid this overhead. All you need do is enter the parameter NOYOURACC with your RLIST command. This parameter is only available to SPECIAL users. When the results of the RLIST are displayed, you will see N/A for YOUR ACCESS. It can be abbreviated NOY as shown:

```
RLIST TCICSTRN CEMT NOY
```

Use of parameters ALL and RESGROUP to list a member class resource will also result in all profiles being retrieved and inspected to identify every grouping profile covering the resource.

Auditors: Review DITTO and FILE Manager DISK.FULLPACK

IBM utilities DITTO and File Manager provide a variety of data management functions. Certain functions, available if the product's program executes APF-authorized, allow a user to manipulate data by physical disk track address and bypass normal dataset access controls. Their use is controlled by FACILITY resource *product*.DISK.FULLPACK, where *product* is either <u>DITTO</u> or <u>FILEM</u>. DASDVOL profiles also play a role in controlling these functions.

Users with ALTER access to FULLPACK can read and update any track on any volume.

Users with UPDATE access to FULLPACK can read any track on any volume. They can update tracks on a specific volume if they have ALTER access to the volume's DASDVOL profile.

Users with READ access to FULLPACK can read or update tracks on a specific volume if they have READ or ALTER access, respectively, to the volume's DASDVOL profile.

If the DASDVOL class is active but no profile is defined for the volume, no access to the volume is allowed. If, however, the DASDVOL class is <u>not</u> active, users permitted READ or greater access to FULLPACK are treated the same as if they have ALTER access.

Here are sample commands to list and display the FACILITY and DASDVOL profiles:

```
RLIST FACILITY DITTO.DISK.FULLPACK ALL
RLIST FACILITY FILEM.DISK.FULLPACK ALL
RLIST DASDVOL volume ALL
SEARCH CLASS(DASDVOL)
RLIST DASDVOL profile AUTH
SEARCH CLASS(GDASDVOL)
RLIST GDASDVOL profile AUTH
```

If either product is installed, confirm the discrete FACILITY profile *product*.DISK.FULLPACK is defined. If any users are permitted READ or UPDATE access, ensure the DASDVOL class is active and appropriate profiles are defined.

All relevant profiles should have UACC NONE, NOWARNING, and a very restricted access list. Ideally, any access to FULLPACK, especially UPDATE or ALTER, should be permitted only on a temporary, as needed basis for problem resolution.

To learn more about protecting related functions, read our magazine article titled <u>RACF Self-Assessment: 3 Critical Areas to Examine</u>, in the April/May 2007 issue of zJournal.

RSH News

On July 1st, RSH Consulting, Inc. celebrated its ***15th Anniversary*.** To our many past and present clients, thank you for helping us grow and sustain our business.

Are you contending with misguided audit findings such as having to delete IBMUSER? Hand your auditors a copy of the latest version of our white paper ***RACF Audit Guidance***. This document provides information to help auditors avoid issuing invalid findings. For best results, pass it to them at the start of the audit along with the RACF reports they request. Visit our website to obtain a copy.