

## 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 products DITTO and File Manager are utilities providing a number of data management and manipulation functions. If your installation has either of these products and the product is APF-authorized, review the access list of the FACILITY class profile protecting resource *product.DISK.FULLPACK*, where *product* is either DITTO or FILEM. Here is a sample command to list the DITTO profile.

```
RLIST FACILITY DITTO.DISK.FULLPACK ALL
```

Users with ALTER access to this profile can perform any of its functions on all disk datasets. All normal dataset access permissions are bypassed.

Users with UPDATE access can perform read functions on all datasets. To perform update functions, users also need ALTER access to the DASDVOL profile protecting the disk volume where the dataset resides.

Users with READ access can perform read or update functions only if they also have READ or ALTER access respectively to the DASDVOL profile protecting the disk volume where the dataset resides.

If the DASDVOL class is not active or there is no DASDVOL profile guarding a particular disk volume, all users are treated as if they have ALTER access to the volume. To list and display DASDVOL profiles, here are sample commands:

```
SEARCH CLASS(DASDVOL)
SEARCH CLASS(GDASDVOL)
RL DASDVOL profile-or-volume AUTH
RL GDASDVOL profile AUTH
```

The profile guarding *product.DISK.FULLPACK* and all DASDVOL profiles should have a UACC of NONE, not be in WARN mode, and have a very restricted access list. Some installations may consider it too risky to give anyone access to *product.DISK.FULLPACK*, especially ALTER.

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

## **RSH News**

On July 1<sup>st</sup>, RSH Consulting, Inc. celebrated its **15<sup>th</sup> 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.

### **Upcoming RACF Training:**

- RACF - Introduction & Basic Administration  
September 25-27, 2007 - Boston, MA
- RACF - Audit for Results  
November 6-8, 2007 - Charlotte, NC

See our website for details and registration form.

## **RSH CONSULTING, INC.**

RACF & ENDEVOR Specialists

www.rshconsulting.com ■ 617-969-9050

29 Caroline Park, Newton, Massachusetts 02468

**SECURITY  
SUPPORT  
SOLUTIONS**