RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 2
Issue 1

January
2008

Practical Uses for LEVEL

Next time you list a profile, look closely at the first few lines of the display. You will see the profile's LEVEL displayed as follows:

```
LEVEL  OWNER    UNIVERSAL ACCESS …
-----  -------- ---------------- …
 00    RASST           READ      …
```

LEVEL is simply a 2-digit integer stored in the profile. It is not used in access authorization. The default value is 0. You set or change it by specifying LEVEL(*n*) with an ADDSD, ALTDSD, RDEFINE, or RALTER command, where '*n*' is an integer from 0 to 99.

LEVEL is included in the 0400 and 0500 RACF database unload records. LEVEL is also included in any SMF Type 80 RACF Processing record generated as a result of access granted by the profile; although, you will often not see it in a DEFINE record. For both the database and SMF unload records, the LEVEL field is a 3-digit integer. LEVEL can be specified as a selection option on the RACFRW EVENT subcommand.

LEVEL can be quite useful for documentation and record selection. For instance, you could assign LEVEL(1) to all the profiles guarding APF authorized libraries. This LEVEL might serve as a flag to RACF administrators that special approvals are required before granting access. Using the database unload, you could write a REXX EXEC to select and generate access list reports on these profiles for review. You could also use REXX or DFSORT ICETOOL to create monitoring reports on all events associated with this LEVEL from SMF unload data.

Another use of LEVEL is documenting resource owners. Assign a number to each owner and set the LEVEL in each of the owner's profiles to this number. This will enable you to create access administration and monitoring reports by owner.

LEVEL can be handy in database cleanup tasks. Assign a unique LEVEL number along with AUDIT(ALL) to profiles you suspect are obsolete. Periodically generate and review monitoring reports to determine if any of the profiles are still being used to grant access. If you see activity for a particular profile, set its LEVEL back to the previous value. At the end of your monitoring period, delete any remaining profiles with the LEVEL you originally assigned. Be careful using this technique. Some profiles are used in ways that do not result in logging, and RACLIST processing for grouping profiles may not retain the LEVEL.

CSA Storage Protection

In z/OS 1.8, IBM introduced a new PARMLIB option to prevent the allocation of storage in Common Storage Area (CSA) with user key 8. Unlike storage with a system key, user key storage is accessible by all address spaces and is considered to be an integrity exposure. The new option is ALLOWUSERKEYCSA(YES|NO) and is specified in PARMLIB member DIAGxx. The default value in z/OS 1.8 is YES (allow user key) and NO in z/OS 1.9. We believe NO is the proper setting. Beware! A NO value breaks *lots* of 3rd party software products. A Google search will identify many of these issues. For details on this new PARMLIB option, see IBM's z/OS MVS Initialization and Tuning Reference.

Auditors: Verify FDR's RACF Interface is Active

Many installations use the Fast Dump Restore (FDR) product from Innovation Data Processing to backup data. FDR is typically executed from an APF authorized library, enabling it to use privileged instructions to access data directly without going through normal dataset open routines. This allows it to run much more quickly, but it also bypasses data access authorization checking. FDR programs could be misused to read or overlay data the user is not authorized to access. For instance, a malicious user could

backup a dataset to which the user does not have read access and restore it with another name to which the user does have access.

FDR provides security options ALLCALL, NOABSTRK, and NONEW that can be set to guard against misuse. None of their default settings provide security.

ALLCALL, when set to YES, directs FDR to perform volume and dataset authorization checking before allowing access. Volume checking is implemented using profiles and permissions in the DASDVOL class. Use of DASDVOL authority can improve FDR's performance. Individual dataset access checking is skipped if the user has access to the entire volume. Innovation recommends ALLCALL be set to YES and DASDVOL profiles be created to protect all DASD volumes.

NOABSTRK, when set to NO, disallows the use of absolute track operations which access data without checking dataset access. If ALLCALL is set to YES, volume level checking is still performed. When volume level protection has been properly implemented, it is reasonably safe to set NOABSTRK to YES.

NONEW, when set to NO, prevents restore or copy operations which change the name of the dataset. Setting NONEW to NO prevents the type of misuse previously described, but it also restricts the use of a potentially valuable feature. If ALLCALL is set to YES, FDR will check the user's authority to read the original dataset before restoring it to a new name, thereby preventing this form of misuse. Provided that ALLCALL is set to YES, it is reasonably safe to set NONEW to YES.

There are compensating controls to consider as alternatives to setting ALLCALL to YES. You could restrict access to the FDR program library or to the FDR programs themselves. In our opinion, these methods are not as robust as setting ALLCALL to YES. You could also install it without APF authorization, but this will greatly reduce its efficiency. Ultimately, each installation must decide for itself what option settings are appropriate.

To check the status of all FDR options, run the FDRZAPOP utility. Sample JCL is provided below. You will need read access to the FDR program library to execute this program.

```
//jobname  JOB (account),'username'
//STEP0001 EXEC PGM=FDRZAPOP
//SYSLIB   DD DSN=fdr.library.dsname,
//            DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
  PRINT
```

P.S. Make sure the backup datasets created using FDR are protected with UACC(NONE)!

For details, see Innovation's FDR User Manual.

See the July 2007 issue of RSH RACF Tips for guidance on reviewing DASDVOL profiles.

RSH News

Did you know RSH's consulting services are ***eco-friendly***? We deliver most of our services remotely to spare clients the financial and ecological costs of travel. We even offer discounts for off-site work. With our efficient and effective use of email, telephone, VPN, and secure document sharing via the web, clients find they receive more value for their consulting dollar when we provide off-site services. To save money and the environment while receiving superior RACF consulting assistance, call RSH.

Upcoming ***RSH RACF Training***:

- RACF - Intro and Basic Administration
  April 29 - May 1, 2008 - Boston, MA
- RACF - Audit for Results
  May 20-22, 2008 - Boston, MA

See our website for details and registration form.

Our FACILITY class presentation was recently added to the agenda for the upcoming joint **NYRUG & TRUG** (Tampa) meeting. Come hear this valuable presentation on February 12th.