RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 10
Issue 3

July
2016

RACF SMF Tidbits

SETROPTS AUDIT(DATASET) and other audit settings will cause RACF to create SMF records when a dataset is created, deleted, renamed, expanded, or condensed. The corresponding SMF unload record event types are DEFINE, DELRES, RENAMEDS, ADDVOL, and DELVOL, respectively. The last two are created only when a dataset spans volumes. These record types provide the dataset name but not the associated profile. The "Access Intent" in these records is ALTER except for ADDVOL, where it is UPDATE. ACCESS event records are often created as well, and these do show the associated profile.

When a tape dataset is created, no ACCESS event record for intent ALTER will accompany the DEFINE, and when a tape dataset is deleted, no DELRES is generated.

ACCESS records indicate when OPERATIONS authority was used. The others very rarely do.

When remediating OPERATIONS authority, do not limit your analysis to only those records showing OPERATIONS use. Review these other records to identify all instances where ALTER access is required, especially to tape datasets.

"Hidden" Profiles

If you delete a class from the Class Descriptor Table without first deleting all associated profiles, those profiles will remain in the database indefinitely. They cannot be listed with RACF commands and will not appear in an IRRDBU00 database unload. An IRRUT200 database copy report, however, will list the class along with a profile count. Confirm that all classes listed by IRRUT200 are defined to RACF. To delete such orphaned profiles, you must temporarily redefine the class to RACF and activate it for GENCMD.

If you define generic profiles to a general resource class and subsequently deactivate SETROPTS GENCMD for that class, you will not be able to list the profiles with RLIST or SEARCH. They will, however, appear in an IRRDBU00 unload. Confirm all generic profiles listed by IRRDBU00 are associated with classes where GENCMD is active. To list or administer these profiles, you must activate GENCMD for the class.

Broken DFLTGRP Connect

A user's group connection is considered broken if the corresponding group profile either no longer exists or, for a non-UNIVERSAL group, does not have a connect entry for the user. A LISTUSER shows AUTH=? for such a connection. Most broken connects can be fixed with CONNECT and REMOVE commands. However, if the broken connection involves the user's default group, you must change the user's default group to another group before the connection can be fixed.

Accurate IRRDBU00 Unloads

Your choice of z/OS system when executing IRRDBU00 is important. IRRDBU00 unloads profiles only from classes defined to the Class Descriptor Table (CDT) on the system where it executes. It uses the Enhanced Generic Naming (EGN) SETROPTS setting on the system where it executes to determine how to display dataset profiles. The types and contents of the records generated can vary depending upon the level of the templates in the database and the version of IRRDBU00 on the z/OS system.

To get an accurate unload, we suggest you execute IRRDBU00 on one of the systems that uses the database to be unloaded. Choose a system that has the latest release of z/OS with the most recent IBM-supplied ICHRRCDX table. Ensure all systems sharing the database have the same installation-defined classes either by ensuring they all have identical ICHRRCDE installation-defined tables, or better still, replacing all ICHRRCDE classes with CDT class profiles. If any new CDT class profiles have been defined since the last IPL, ensure the CDT class has been RACLIST REFRESHed on the system where IRRDBU00 is to be executed. Finally, ensure the database has the most current templates.

RSH submitted a Request for Enhancement to have IRRDBU00 unload all profiles without regard to the classes defined on the system where it executes. Let IBM know if you support this RFE.

Auditors: Review JES2 PROCLIB Protections - Part 1

JES2 PROCLIBs (Procedure Libraries) are partitioned datasets (PDSs) with members that contain JCL procedures (PROCs) for Started Tasks, TSO logons, system jobs, and application jobs. PROCs define the programs and datasets each task or job will use. PROCLIBs are critical datasets and require strict update access control.

PROCLIBs can be defined to JES2 either by specifying their dataset names in PROC*xx* DD statements in the JES2 PROC ('Static'), or by specifying them in PROCLIB statements in JES2 initialization parameters in the HASPPARM DD datasets ('Dynamic'). Here is a sample.

```
//JES2     PROC
//IEFPROC  EXEC PGM=HASJES20
//PROC00   DD  DSN=SYS1.PROCLIB,DISP=SHR
//         DD  DSN=TECHSPT.PROCLIB,DISP=SHR
//PROC01   DD  DSN=USER1.PROCLIB,DISP=SHR
//         DD  DSN=PAY.PROCLIB,DISP=SHR
//HASPPARM DD  DSN=SYS1.PARMLIB(JES2PARM),
               DISP=SHR

SYS1.PARMLIB member JES2PARM
PROCLIB(PROC02) DD(1)=(DSN=TEST.USER.PROCLIB),
                DD(2)=(DSN=TEST.APPL.PROCLIB)
```

Dynamic PROCLIBs can be added, changed, and deleted after JES2 startup using the $T PROCLIB operator command. Static PROCLIBs cannot be changed, but they can be replaced by Dynamic entries. If a Dynamic entry replacing a Static entry is deleted, the Static entry again becomes active.

To identify the Dynamic PROCLIBs currently in use by JES2, execute this operator command:

$D PROCLIB

To run the command, you need READ access to the OPERCMDS profile protecting the resource *jesname*.DISPLAY.PROCLIB.

To identify Static PROCLIBs, prior to z/OS 2.1 it was necessary to either examine the JES2 PROC or look at JES2 startup messages in the System Log. As of z/OS 2.1, the $D command above now displays both Static and Dynamic PROCLIBs.

After identifying all PROCLIBs, review their RACF profiles and permissions. Only a limited set of users, generally Systems Programmers or change management processes, should have UPDATE or greater access to PROCLIBs, especially those with Started Tasks, TSO logon PROCs, and system batch jobs.

SDSF SECURITY TRACE

Introduced in z/OS 2.1, SDSF Security Trace is a valuable tool for implementing RACF protection for SDSF and troubleshooting access problems. The trace shows each access authorization check made by SDSF and the corresponding decision made by SAF or ISFPARMS. SDSF command SET SECTRACE ON activates the trace and no permissions are required to use it. Results may be viewed using the ULOG command provided you have READ access to the SDSF resource ISFCMD.ODSP.ULOG.*jesname* or ISFPARMS authority AUTH(ULOG).

RSH News

Some SOC2 auditors now use sophisticated RACF assessment tools. If your security might not measure up to enhanced scrutiny and needs remediation before the auditors show up, call us.

Travel time and expenses can easily double the cost of training. Save time and money by attending our on-line, instructor-led, WebEx-based training. We offer entry-level, intermediate, and advanced training for RACF administration and auditing. Our half-day format lets attendees keep up with day-to-day work and avoids information overload. Visit our website for details.

Support for z/OS 1.13 ends this September. Still need to replace the Unix Default User? Call us.

Many thanks to all who participate in our surveys!