RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 12
Issue 1
January
2018

Proper RACF Database Allocation

A RACF database dataset must be allocated in a single extent with fixed length, unblocked 4096-byte records (RECFM=F, LRECL=4096, and BLKSIZE=4096). It should also be both non-SMS managed and allocated as Physical Sequential Unmovable (DSORG=PSU) to prevent relocation of the dataset, which could result in catastrophic database I/O errors. To confirm all RACF database datasets are properly allocated, list them using ISPF option 3.2 and check the attributes highlighted in the sample display below.

```
----------- Left Hand Column -----------

General Data
 Management class . . : **None**
 Storage class  . . . : **None**
  Volume serial . . . : RAC001
  Device type . . . . : 3390
 Data class . . . . . : **None**
  Organization  . . . : PSU
  Record format . . . : F
  Record length . . . : 4096
  Block size  . . . . : 4096
  1st extent cylinders: 3
  Secondary cylinders : 0
  Data set name type  :

SMS Compressible  . : NO

---------- Right Hand Column -----------

Current Allocation
Allocated cylinders : 3
Allocated extents . : 1

Current Utilization
Used cylinders  . . : 3
Used extents  . . . : 1

Dates
Creation date . . . : 2017/06/20
Referenced date . . : 2017/12/03
Expiration date . . : ***None***
```

Unix - UID Displayed, not USERID

The File Security Packet (FSP) for a Unix file or directory contains the UID of the Owner, not the USERID. The same is true for Extended Access Control List (ACL) user permission entries.

If you list the FSP using Unix commands 'ls -l' or 'getfacl', the commands will try to find and display the USERID assigned the Owner or ACL UID. If multiple USERIDs share a UID, only one will be displayed. When no USERID has been assigned a UID, the command will display the UID itself.

If a UID is assigned to a USERID whose Default Group does ***not*** have a GID, the aforementioned commands will display the UID, not the USERID. Similarly, the HFS Unload utility IRRHFSU will show USERID fields as blank, and command 'find *path* -nouser' will include files and directories with these Owner UIDs in its output. These results can mislead you into thinking a UID is unassigned.

When remediating Unix File System security to eliminate orphaned Owner and ACL UIDs, verify the UIDs are unassigned before replacing them.

Limiting Scope for FIELD Authority

Heretofore, permissions to FIELD class profiles enabled a user to view or update segment fields for all profiles. As of z/OS 2.3, a user can be restricted to viewing and updating segments for only those profiles within the scope of their administrative authority (e.g., Group-SPECIAL scope-of-groups, profile owner). To implement this restriction, simply define the following profile.

```
RDEF FIELD FLAC.SKIP.BASECHECK UACC(NONE)
```

To allow certain users to view or update segments for all users as before, permit them READ access to this profile.

Permissions to &RACUID that allow users to view or update fields in their own segments will continue to work as before.

Pervasive Encryption & DFP Segment Administration

The label of the CKDS key to be used to encrypt the contents of new datasets using pervasive encryption can be specified in the DATAKEY field of the DFP segment of the DATASET profile protecting the datasets. If a new profile is defined

that is more specific than an existing profile with a DFP segment, the key label in the existing profile segment will need to be added to the new profile. There is no command for copying the segment.

Recent SDSF RACF Changes

In V2.1, SDSF introduced task SDSFAUX, which uses RACROUTE REQUEST= FASTAUTH to check access to newly added SDSF resources. To support SDSFAUX, the SDSF class had to be RACLISTED and in V2.3 RACLIST is REQUIRED. If the class is not RACLISTed, authorization checks will receive a Return Code (RC) of 4. Once the class is RACLISTed, an RC=4 will only be issued if no covering profile is found.

The AUXSAF parameter setting found in the ISFPARMS CONNECT statement determines how SDSF will react to an RC=4 for newer functions. If the default setting of FAILRC4 is used, SDSF will deny access to the function. When AUXSAF(NOFAILRC4) is specified, ISFPARMS will govern access. In either case, ISFPARMS will continue to govern access when RC=4 is returned for older functions.

New Operator Display (ODSP) functions have been added to SDSF. Use of many of these functions requires READ access to both a function resource ISFCMD.ODSP.*function.system* and a target system resource ISF.CONNECT.*sysname.* To display information on jobs not running under JES, access to new ISFJOB resources is needed.

In V2.1 through V2.3, SDSF added other new resources whose names are prefixed with ISFAPF, ISFCFC, ISFCFS, ISFDEV, ISFDISP, ISFDYNX, ISFENQ, ISFFS, ISFGT, ISFJDD, ISFLNK, ISFNETACT, ISFPAG, ISFPARM, ISFSMSVOL, ISFSTORGRP, ISFSUBSYS, ISFSYM, and ISFSYS. Also new are ISFCMD.DSP.JGROUP.*jesx* and several ISFATTR resources.

We advise you to RACLIST the SDSF class if not already RACLISTed and to update your profiles to appropriately protect the newest resources.

z/OSMF ZMFAPLA Tips

z/OSMF checks access to resources in the ZMFAPLA class using RACROUTE REQUEST= FASTAUTH. ZMFAPLA must be RACLISTed in order for z/OSMF to use its profiles.

z/OSMF denies access if a ZMFAPLA resource is not protected and issues a CWWKS2911E message naming the resource. These messages are only displayed in the z/OSMF's server's STDERR DD SYSOUT.

FASTAUTH - No Audit, No ICH408I

If a RACROUTE REQUEST=FASTAUTH call determines an access attempt is a violation, an ICH408I message will only be displayed if audit settings specify that an SMF record is to be generated. If no SMF record is to be generated, no ICH408I message will be displayed.

SMF record generation for a FASTAUTH check is governed by profile AUDIT and GLOBALAUDIT settings and by user UAUDIT. FASTAUTH ignores SETROPTS LOGOPTIONS settings.

An ICH408I message will always be displayed for a warning or a REQUEST=AUTH violation even if no log record is to be generated.

To get ICH408I messages and SMF records for all violations and warnings, ensure auditing options for every profile include FAILURES(READ).

Caveat: If the RACROUTE call specifies LOG=NONE, no message or SMF record will be generated regardless of any audit setting. Note that LOG=NONE is the default for FASTAUTH.

RSH News

Make 2018 the year you have RSH perform a top-to-bottom review of your RACF implementation to find the holes in your defenses and get advice on how to plug them. Call us today.