RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 7
Issue 4
October
2013

Deleting UNIVERSAL Groups

RACF will prevent you from deleting a group if the group profile shows there are users connected to it. But with a UNIVERSAL group, no connect entry is recorded in the group profile when a user is connected with AUTHORITY(USE). The connect information is stored only in the user profile. If all the users connected to a UNIVERSAL group have only USE authority, the group will appear to be empty and LISTGRP will display NO USERS. RACF allows deletion of the group even though there may be thousands of connected users.

If you delete a UNIVERSAL group and then list one of the connected users, you will see an entry like this in the LISTUSER display. Note AUTH=?.

```
ICH30001I UNABLE TO LOCATE GROUP ENTRY USRID1
  GROUP=FINUSERS  AUTH=?      CONNECT-OWNER=…
  CONNECTS=    00  UACC=NONE   LAST-CONNECT=…
  CONNECT ATTRIBUTES=NONE
  REVOKE DATE=NONE   RESUME DATE=NONE
```

Unlike a connection to a traditional group, an orphaned connection like the one above can be removed simply by issuing a REMOVE command.

To avoid orphaning connections, always use IRRRID00 to build commands to delete a group. This is a best practice even if the group is not UNIVERSAL. IRRRID00 will generate REMOVE commands for all connected users. It will also build PERMIT DELETE commands to remove the group from access lists as well as ALT-type commands to replace it as a profile owner.

TFS FSP

A z/OS Unix Temporary File System (TFS) is a memory-resident file system that exists only for the life of the system and is most commonly used for the /tmp directory. At the time a TFS is mounted, its associated mount-point directory is given a File Security Packet (FSP). By default, this FSP has an OWNER of UID 0 (a.k.a., Superuser), a GROUP of GID 0, and mode 0777, which displays as 'rwxrwxrwx'.

You can override the FSP default settings by specifying options in the PARM parameter of the MOUNT statement for the TFS. Options are:

-u *uid* Numeric OWNER UID value (e.g., 99)
-g *gid* Numeric GROUP GID value
-p *mode* Octal permissions (e.g., 1777)

You can also change the mount-point directory FSP after the TFS is mounted. For instance, with the /tmp directory, most installations activate the directory sticky bit. This is usually done by adding either one of the following chmod commands to the file /etc/rc which is executed during z/OS Unix initialization soon after the TFS is mounted.

chmod 1777 /tmp
chmod +t /tmp

For the full details on Unix security, attend RSH's RACF - Securing z/OS Unix course.

Auditors: Ensure OPERATIONS is Controlled, Part 1

OPERATIONS is a powerful attribute. It enables a user to access datasets and resources at ALTER level and to create datasets and dataset profiles for any group. OPERATIONS can be assigned to a user's ID, in which case it applies to all datasets and resources, or to a group connection, where it only applies to datasets and resources within the scope of the connect group.

OPERATIONS only grants access to resources in those classes where OPERATIONS authority is enabled. To identify these classes, review the RACF Class Descriptor Table report generated by DSMON. (DSMON, or Data Security Monitor, is a RACF utility. Its program name is ICHDSM00.) Look for a YES under the rightmost column which is labeled OPERATIONS ALLOWED.

The Class Descriptor Table (CDT) that IBM provides with RACF has certain classes already enabled for OPERATIONS. They are:

DATASET	DASDVOL & GDASDVOL	
DIRECTORY	FILE	NETCMDS
NETSPAN	PSFMPL	RODMMGR
TAPEVOL	VMBATCH	VMCMD
VMMDISK	VMNODE	VMRDR

Any other class you find with OPERATIONS enabled is most likely a locally defined, non-IBM class. It is not unusual to find such classes. Prior to the introduction of the CDT class, which allows new classes to be added to RACF dynamically, local classes had to be defined by the ICHRRCDE module created using ICHERCDE macros. This macro activates OPERATIONS by default if parameter OPER=NO is omitted. 3rd party product vendors often neglected to include OPER=NO in their instructions for adding new classes, so older classes are more likely to have OPERATIONS enabled. (Fortunately, classes added via the new CDT class default to OPERATIONS(NO).)

RSH has yet to find a non-IBM class where OPERATIONS is necessary. Best practice is not to have any non-IBM class with OPERATIONS. If you find any local classes with OPERATIONS enabled, recommend OPERATIONS be disabled.

In future articles, we will examine how to identify OPERATIONS users, place restrictions on this authority, and monitor its use.

For more on auditing RACF, attend RSH's RACF - Audit & Compliance Roadmap course.

CA ENDEVOR Resource Class

ENDEVOR allows you to specify the resource class it will use for authorization checking by using the CLASS parameter in NAMEQU statements in the Security Table BC1TNEQU. The default is DATASET, but we recommend using a locally defined class named something like $ENDEVOR. Here are the advantages in doing so.

- You can have longer resources names, up to 246 characters, rather than the 44 for datasets.
- It allows creation and deletion of discrete profiles without having to specify NOSET to circumvent the RACF indicator bit processing associated with dataset profiles.
- If properly configured, the class can be RACLISTed to improve performance.
- Profile refreshes are less disruptive and do not affect all dataset profile users.
- OPERATIONS authority does not grant access (unless you mistakenly activate it).

Replacing an Access List

If you want to replace the access list of one profile with that of another, simply execute the following. Include CLASS and FCLASS as needed.

PERMIT *target-profile* RESET FROM(*source-profile*)

RSH News

To those of you who have been missing out on hearing our RACF User Group presentations because you do not have a local RUG, we bring good news. RSH will soon begin offering our presentations via webcast. To request notification of these invitation-only webcasts, send your email address to info@rshconsulting.com.

Planning to conduct your own audit or review of RACF but need some expert guidance? Call to ask about our audit assistance services. A few hours of our time may be all that is needed.

Upcoming ***RSH RACF Training*:**

- RACF - Audit & Compliance Roadmap
  November 5-8, 2013 - Boston, MA
- RACF - Intro and Basic Administration
  October 21-25, 2013 - WebEx
  February 3-7, 2014 - WebEx
- RACF - Securing z/OS Unix
  December 3-6, 2013 - WebEx
  March 4-7, 2014 - WebEx