RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 2
Issue 4

October
2008

Authority to Administer Unix Directory & File Permissions

Increasingly, RACF administrators are being asked to administer the permission bits and extended Access Control Lists (ACLs) on files and directories in the z/OS Unix Hierarchical File System (HFS). Many are using Unix Superuser (a.k.a. root) to obtain the necessary authority to administer security. Superuser authority is like a cross between SPECIAL and OPERATIONS. It grants far more power than is required just to manage security, including the ability to change and delete files.

Two UNIXPRIV resources offer an alternative to Superuser for Unix security administration. One is SUPERUSER.FILESYS.CHOWN. READ access lets an administrator change a file or directory owner and group using the Unix commands chown and chgrp, respectively.

SUPERUSER.FILESYS.CHANGEPERMS is the other resource. READ access lets an administrator change access bits and extended ACLs using the commands chmod and setfacl.

Note there are other UNIXPRIV resources with the same SUPERUSER.FILESYS prefix as the two discussed above. In designing profiles to grant access to CHOWN and CHANGEPERMS, take care not to give access to any of the others.

To learn more about Unix file protection, visit the **RACF Center** *on our website for a copy of our presentation zOS Unix - File System Security.*

Performance: Avoid SETROPTS GENERIC(DATASET) REFRESH

When a user attempts to access a dataset protected by a generic profile, RACF retrieves the profile from its database and checks the access list to see if the user is authorized for access. RACF then retains a copy of the profile in memory within the user's address space for further reference. If the user accesses another dataset protected by the same profile, RACF uses the stored copy for authorization checking, thereby enhancing performance by avoiding repeated I/O to the database to fetch the same profile. RACF will keep profiles for up to four different dataset High Level Qualifiers (HLQs) in memory for each user.

If a user does not have sufficient authority to access a dataset and a RACF administrator permits higher access to the associated profile while the user is logged on, the user may still not be able to access the dataset. RACF continues to use the prior copy of the profile in memory and not the updated profile on the database. To acquire the new permission, the copy of the profile in memory must be refreshed.

One way to refresh the profile is to execute SETROPTS GENERIC(DATASET) REFRESH. This command causes RACF to discard all saved dataset profiles for every user. RACF then has to retrieve all the profiles again. We have encountered several sites where RACF administrators routinely issued this command every time they executed ADDSD or ALTDSD and have since ceased doing so on our advice.

For TSO users, there are two techniques for refreshing a profile without affecting the entire system. One is to logoff and log back on again. Doing so refreshes all of the user's profiles.

The second technique avoids logging off. The user merely needs to execute a LISTDSD to list any generic profile with the same HLQ as the dataset to be accessed. This causes a discard of the stored generic profiles for just the one HLQ. The command need not even specify an existing profile or dataset name. Entering a command like the one below will do.

```
LISTDSD 'hlq.REFRESH' GEN
```

As a general rule, use SETROPTS REFRESH only when the user needing new permissions is a started task or process that cannot be stopped and restarted to acquire updated profiles.

To learn more about how to improve RACF performance, visit the ***RACF Center*** *on our website for a copy of our presentation* *RACF Performance Tuning.*

Auditors: Find and Investigate Profiles in WARNING

WARNING is a dataset and general resource profile option intended for use in temporarily testing a profile to confirm all required access permissions have been properly granted. If a user attempts to access a resource protected by a profile in WARNING and does not have sufficient permission, a violation warning message is issued and an SMF log record is generated. The access, however, is allowed at whatever level the user requested. RACF does not prohibit unauthorized access when the profile is in WARNING; it merely reports it.

To find all the dataset profiles in WARNING, execute the following RACF TSO command.

```
SEARCH NOMASK WARNING
```

To find all the general resource profiles in WARNING, execute the following command for every active resource class.

```
SEARCH CLASS(class-name) WARNING
```

Note that WARNING has no effect on profiles in the PROGRAM and NODES classes.

If you have access to a RACF database unload file and are familiar with programming tools such as REXX or DFSORT ICETOOL, you can create software routines to produce reports on all profiles in WARNING. Most 3rd party RACF administration tools will do so as well.

The use of WARNING should be thoroughly investigated. RACF administration should have documentation on each profile in WARNING as to why WARNING is being used, when it was first applied, and when it will be removed. They should also be generating monitoring reports on a regular basis showing any access granted by WARNING and have a process for reviewing these reports and taking appropriate action.

Profiles protecting the use of high-powered authorities should never be put in WARNING because it would enable anyone to use them. An example is any FACILITY class profile guarding a resource with a name having the prefix STGADMIN.ADR.STGADMIN (our audits have found this on several occasions).

To learn more about auditing RACF, attend our **RACF - Audit for Results** *course.*

RSH News

Have you recently ***converted*** from CA-ACF2 or CA-Top Secret to RACF? We typically find that post-conversion implementations of RACF are designed merely to mimic the functionality of the prior software and do not take full advantage of RACF's capabilities. Much of our recent remediation work has focused on significantly improving the efficiency and effectiveness of RACF implementations following a conversion. To find out what improvements you might need to make, attend our ***RACF - Audit for Results*** course.

Upcoming ***RSH RACF Training***:

- RACF - Audit for Results
  October 28-30, 2008 - Boston, MA

See our website for details and registration form.

RSH offers ***in-house RACF training***. Our training can be tailored to your precise requirements and unique configuration. If you have four or more students, this may be a cost-effective alternative to a public seminar.

For those of you in New England or the Ohio, Indiana, and Kentucky tri-state area, be sure to attend the upcoming ***RUGONE*** or ***KOIRUG*** meeting. See our website for meeting details.