RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 13
Issue 2

April
2019

Password Phrases and z/OS FTP

FTP supports the use of password phrases if the FTP.DATA configuration option PASSPHRASE is set to TRUE, which is the default setting.

In testing and implementing the use of phrases, we found FTP does not handle phrases with embedded blanks. This is not documented.

If you have servers logging onto z/OS FTP with RACF IDs used only for this purpose and their FTP client is capable of supporting longer passwords, start using phrases for these IDs. All you need to do is assign the IDs a phrase like so:

ALTUSER *userid* PHRASE('*phrase*') NOEXPIRE

Once you have confirmed the phrase is working properly, remove the ID's password so that only the phrase can be used for authentication.

ALTUSER *userid* NOPASSWORD

CDT - 1,024 Limit on Classes

The maximum number of classes that can be defined to RACF's Class Descriptor Table (CDT) is 1,024. This includes classes defined by IBM in the ICHRRCDX table and those defined by an installation in the ICHRRCDE table and with CDT class profiles. An installation class defined by both an ICHRRCDE entry and a CDT profile is only counted once. Keep this limit in mind when adding classes, especially for DB2 subsystems, or when merging RACF databases. Also, be mindful of the limit when implementing new z/OS releases as IBM may have added classes.

Tips on setgid

If the setgid bit is turned on for an executable file (program or script), the file will execute with the authority of the file's group GID even if the user executing the file is not a member of the group.

The Owner of a z/OS Unix file system object (directory or file) can only turn its setgid bit on if the Owner's ID is connected to the group specified in the object's File Security Packet (FSP).

If profile FILE.GROUPOWNER.SETGID is defined in the UNIXPRIV class, the FSP for a new object will inherit its group from the effective group in the creator's User Security Packet (USP) unless the object is being created under a directory that has its setgid bit set on, in which case the FSP for a new object will inherit its group from the directory's FSP, the same as it would if the UNIXPRIV profile were not defined.

For more, attend "RACF - Securing z/OS Unix".

Printing RACF Healthchecks II

Our January 2019 Tips showed you how to print RACF Healthchecks using SDSF in batch. You can also print them using Healthchecker's HZSPRNT utility. Here is sample JCL.

```
//jobname JOB job-card-parameters
//RACFCKS EXEC PGM=HZSPRNT,
      PARM='CHECK(IBMRACF,*)'
//SYSOUT DD SYSOUT=*,DCB=LRECL=256
```

For each Healthcheck, the output has a "Start: *check-name*" comment block followed by the report and then an "End: *check-name*" comment block. If a check is not active, the report for that particular check will display "No messages exist".

Thank you Mark Nelson of IBM for this tip.

Auditors: RACF 'AUDIT'

The term "audit" generally refers to activities related to reviewing controls. In RACF, "AUDIT" refers to options related to logging user activity. User profile option UAUDIT logs every access a user makes. Dataset and General Resource profile options AUDIT and GLOBALAUDIT govern resource access auditing. SETROPTS options for logging include SAUDIT, OPERAUDIT, AUDIT, CMDVIOL, LOGOPTIONS, and APPLAUDIT.

Attend our course "RACF - Audit and Compliance Roadmap" for details on AUDIT options.

Catalog Alias Administration

A catalog alias is an entry in a master catalog consisting of a dataset name prefix and the identity of the user catalog where datasets with this prefix are to be cataloged. Generally, the provisioning of a new TSO user requires creation of an alias for the user's ID, and the elimination of a TSO ID requires deletion of the ID's alias after disposal of the user's cataloged datasets.

Although management of aliases is usually performed by the Technical Support staff responsible for catalog administration, some installations delegate the maintenance of TSO user aliases to the RACF Administration staff.

For those that choose to delegate, it becomes a question as to what RACF authority should be granted to perform this task. Here are options.

1) Permit UPDATE access to the Master Catalog. This allows the creation of aliases. It also allows cataloging a dataset in the Master Catalog, but only if permitted ALTER access to the dataset.

2) Permit ALTER access to the Master Catalog. This allows the creation and deletion of aliases. It also allows the cataloging and uncataloging of datasets in the Master Catalog as well as deletion of VSAM and SMS-managed datasets cataloged in the Master Catalog, all without ALTER access to the datasets themselves.

3) Permit READ access to the FACILITY class profile STGADMIN.IGG.DEFDEL.UALIAS. This allows the creation and deletion of any alias, not just those for TSO users, and regardless of whether there are any cataloged datasets.

RSH recommends the first option above, which restricts RACF staff to the creation of aliases and leaves deletions to the Technical Support staff.

SU in ISPF 3.17 (UDLIST)

A user with READ access to FACILITY resource BPX.SUPERUSER can switch to Superuser UID(0) authority by entering command SU on the ISPF 3.17 panel's command line. Entering SU again switches the user back to their assigned UID. This can also be done by selecting item 4 under the panel's pull-down Options menu.

A user with READ access to SURROGAT resource BPX.SRV.*userid* can switch to the UID assigned to *userid* by entering SU *uid* (e.g., SU 12). Entering SU switches the user back.

The ISPF manual states that a user with READ access to FACILITY resource BPX.DAEMON can switch to the UID assigned to any user. RSH testing found otherwise. The manual makes no mention of SURROGAT authority. RSH has notified IBM of the discrepancy in the manual.

When a user changes their UID, the change is retained until the user either changes it back to their original UID or exits ISPF. Users switching to Superuser authority should take care to remember to switch back to their own UID once the task requiring Superuser authority is complete.

Monitor IRRUT100

Utility IRRUT100 allows a user to discover the extent of his or her own RACF authority. It is so rarely used that any use of it is suspect and may indicate a user is probing security as part of a penetration attempt. Execute the following command to define a profile for IRRUT100. Monitor and investigate its use.

```
RDEF PROGRAM IRRUT100 AUDIT(ALL)
ADDMEM('SYS1.LINKLIB'//NOPADCHK)
```

RSH News

Robert Hansel earned a "Best Conference Session" award from SHARE for his RACF Performance Tuning presentation at the Summer 2018 conference in St. Louis.

Our RACF training is more popular than ever. Sign up today to reserve a seat.

Be sure to attend our upcoming presentations at RUGONE, KOIRUG, NYRUG, CHIRUG, and IBM TechU in Atlanta.