RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 13
Issue 1

January
2019

Protect Confidential RACF Data

Information stored in Installation Data, User Data, and Custom Field CSDATA segments will appear in IRRDBU00 database unloads and in SMF records for commands that populate these fields. If any of this information is confidential, ensure unloads and SMF data are strictly protected.

SETROPTS RACLIST(DIGT-class) REFRESH Delegation

If digital certificate administration has been delegated via FACILITY class IRR.DIGTCERT-prefixed profile permissions to individuals who do not have SPECIAL authority, and any of the DIGT-prefixed classes are RACLISTed, these same individuals can be given the ability to perform SETR RACLIST(DIGT-class) REFRESH by assigning CLAUTH(DIGT-class) to their IDs.

Thank you Mike Bushard of MIB for this tip.

Intrusion Detection in z/OS

z/OS Communication Server has host-based Intrusion Detection Services (IDS) that operates much like a network-based IDS to detect and correlate scan and attack events and to log these events in the Unix syslogd daemon. z/OS IDS is configured via the Policy Agent (PAGENT) and uses the Traffic Regulation Management Daemon (TRMD) for reporting and to enforce connection limit policy.

Multiple Console Logons

A RACF ID can only be logged onto one console at a time. To remove this limitation, define discrete profile MVS.MULTIPLE.LOGON.CHECK in the OPERCMDS class. This profile acts as a switch to activate the option. No permissions are needed.

Batch Print RACF Healthchecks

In addition to viewing RACF Healthchecks on-line, they can be printed via a batch job.

```
//jobname JOB job-card-parameters
//SDSF    EXEC PGM=SDSF
//ISFOUT  DD DUMMY
//RACFOUT DD DSN=dsname,DISP=(,CATLG),
//        UNIT=SYSALLDA,LRECL=251,
//        RECFM=FB,BLKSIZE=0,DSORG=PS,
//        SPACE=(TRK,(2,1),RLSE)
//ISFIN   DD *
PRINT FILE RACFOUT
CK
FILTER CHECKOWNER EQ IBMRACF
SNAP
PRINT
RESET
CK
FIND RACF_AIM_STAGE
++S
PRINT
RESET
CK
FIND RACF_AUDIT_CONTROLS
++S
PRINT
RESET
(repeat CK through RESET for each check)
PRINT CLOSE
/*
```

The first item printed is a list of the RACF checks and their status. If a check is inactive, no output for the check itself is displayed.

The user executing this job will need permissions to use the SDSF CK command and to print the RACF Healthchecks.

For more on RACF Healthchecks and SDSF protection, attend our RACF training.

Auditors: SPECIAL Auditing

RACF commands executed by IDs with SPECIAL (RACF administration) authority will be logged if SETROPTS option SAUDIT is active. This option appears in the first line of output displayed by a SETROPTS LIST command provided that the command was executed by a user with AUDITOR or ROAUDIT authority. SAUDIT also logs access to unprotected datasets using SPECIAL authority. RSH recommends the option be active.

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

Tips When Batching Commands

When executing RACF commands via batch jobs, remember Murphy's Law. Before submitting a job, carefully consider how the failure of a command could result in unintended outcomes from commands later in the batch stream.

When creating replacement profiles using the FROM option to copy permissions from profiles being replaced and deleted, do not put both the profile define and delete commands in the same batch job. If the define commands fail and the delete commands succeed, resources may be improperly protected, and you will not be able to correct and rerun the define commands using FROM because the original profiles will have been deleted. Execute the define commands first, verify they were successful, and then execute the deletes separately.

If executing commands to modify profiles in a RACLISTed class, do not include the RACLIST REFRESH command at the end of the batch stream. Execute the commands, verify they were successful, and then execute the REFRESH.

If permitting access to a profile in preparation for removing WARNING, execute the PERMIT commands first, verify they were successful, and then execute the command to remove WARNING.

A Return Code of 0 on a batch job does not indicate all commands executed successfully. Never assume all your commands were coded correctly. Always check the job SYSOUT to verify every command worked exactly as intended.

CONNECT and REMOVE commands perform up to three separate updates to the RACF database. RACF locks out other users when making these updates. Do not execute large batches of these commands during peak work periods, especially at times when many users are logging on for the first time that day.

SEARCH CLIST Line Numbers

Commands generated by SEARCH CLIST have line numbers to their left. To remove these line numbers, enter **NUM OFF** in the Command line and then use ISPF's shift left line command '**(**' or '**((**', where the former is for a single line and the latter is for a block of lines. Enter the number 8 with the command to shift left 8 positions, thus eliminating the numbers. Here is an example.

```
((8010 00000010CONTROL ASIS
000030 00000030ALD 'RSH.TEST.**' …
000040 00000040ALD 'RSH.**' …
((0050 00000050ALD 'RSHTEST.*.**' …
```

As a shortcut, enter **X ALL** in the Command line to exclude all lines, **(8** to the left of the line of dashes, and then **RESET** in the Command line.

Monitoring Password Changes

If SETROPTS AUDIT(USER) is in effect, SMF Type 80 log records are generated whenever users change their passwords. The SMF80REA flag in these records is set to indicate logging was because of SETROPTS AUDIT. The passwords themselves are not included in these records.

The SMF record for a password change made during logon will have Event Code 01. The corresponding SMF unload record will have event JOBINIT and YES in field INIT_LOG_CLASS.

The SMF record for a password change made with the rarely used PASSWORD command will have Event Code 18. The SMF unload record will have event PASSWORD and YES in field PWD_LOG_CLASS.

RSH News

RSH added a half day to the RACF Level I class to allow more time for exercises and instruction. To encourage educating the next generation of RACF Administrators, we did not raise the fee.