RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 3
Issue 2

April
2009

TEMPDSN and CA-Endevor

If you plan to activate the TEMPDSN class to restrict access to temporary datasets and you have CA-Endevor Software Change Manager installed, you will need to wait until you have upgraded to Endevor release 12 before doing so. In prior releases, Endevor processors create temporary datasets while momentarily operating under the identity of the Alternate ID and attempt to delete these datasets after switching back to the ID of the invoking user. TEMPDSN interferes with their deletion. Endevor R12 has a new option - RACF_TEMPDSN_OPTION - for addressing this issue. If set to ON, temporary datasets will be allocated as ordinary files to be deleted when the processor completes.

JESINPUT

Profiles in the JESINPUT class determine whether a batch job entering the system from a particular input source (a.k.a., Port of Entry or POE) will be allowed to execute. The execution ID - the USERID associated with the job (not necessarily the submitter) - must be permitted READ access to the profile guarding the POE.

JES input sources and their associated RACF resource names are listed below. The 'nnnn' is a number coinciding with the device definition in the JES configuration parameters.

INTRDR	Internal Reader
TSUINRDR	TSO User Logon Reader
STCINRDR	Started Task Reader
RDRnnn	Physical Card Reader
OFFn.JR	Spool Offload Job Reload
OFFn.SR	Spool Offload SYSOUT Reload
Nnnnnn	Adjacent NJE node
Rnnn.RDn	RJE Workstation Reader (JES2)

JESINPUT issues a **default return code of 8**. If no profile covers a POE, no access is allowed. (Exception: authorization is never checked for TSUINRDR or STCINRDR.) Activate GENERICs for JESINPUT and define a profile of ** with UACC of READ before activating the class.

UACC of READ is generally acceptable for all JESINPUT profiles except those protecting NJE nodes and RJE workstations, which may involve connections to outside organizations. Strictly control access to these POEs.

RJE readers can be numbered 1 to 32767. The maximum length of a JESINPUT profile is 8 characters. If an RJE reader is numbered 1 to 999, the resource name is Rnnn.RDn. If 1000 to 9999, it is RnnnnRDn. If 10000 or greater, the resource name is RnnnnnRn. (Honorable mention for the first person who can show us where this is documented in an IBM manual.)

Glad to be of Help

"*I owe you a debt of gratitude. I'd migrated 4 of our 10 lpars successfully to z/os 1.9, w/o any problems, when, last night, doing the 5th one, I started encountering all sorts of OEM 3rd party product b04-5c and b78-5c CSA abends. I recalled what you'd said about that in the January 2008 edition of your "RSH RACF Tips" newsletter* [article: CSA Storage Protection], *and was consequently able to immediately fix the problem. Saved me hours and hours of time. Thanks a lot, man.*" Tuco Bonno, South Carolina Budget & Control Board

Performance: Database Reorg

Over time, RACF administrative actions cause the following negative effects on performance:

- Profile expansions fill database blocks to overflowing requiring I/O for block splits
- Profile and segment deletions empty all but a small percentage of a block, wasting both database and buffer space

- Newly added profile segments get stored in different blocks than the related profile requiring more I/O to fetch during logon

To address these issues, periodically (annually at least) reorganize your RACF database using the IRRUT400 utility. IRRUT400 realigns index and profile blocks into consecutive order, places a profile's segments in the same block with the related profile, fills in blocks, adds free space for subsequent growth, compresses the index, and corrects upper level index errors.

When reorganizing the database, use an offline copy created using IRRUT200 as input to avoid locking the active database. After creating the newly reorganized database, use RVARY commands to bring the database online. Perform this task during a system maintenance period to minimize disruption.

Auditors: PRIVILEGED and TRUSTED Started Tasks

Started Tasks (a.k.a. Started Procedures) are independent processes, often long running service routines that are initiated by the z/OS console operator START command. Examples are JES2, CATALOG, CICS, TCPIP, and VTAM.

Started Tasks are assigned a USERID via either a STARTED class profile or an entry in the ICHRIN03 table. They may also be given PRIVILEGED or TRUSTED authority via the same profile or entry. To identify which Started Tasks are assigned these authorities, review the Data Security Monitor (DSMON) RACF Started Procedures Table Report.

PRIVILEGED and TRUSTED are extremely powerful. Both give unlimited access to all datasets and most resources, allow a task to submit a batch job with any USERID without a password, and grant unix uid(0) root authority. The only difference between the two is that the activity of a TRUSTED task can be logged. Because these authorities can be used to bypass access controls, their assignment should be avoided except where vendor documentation specifically indicates they are required and the vendor has satisfactorily justified their use.

While it may be tempting to insist that no Started Tasks be given these authorities, consider the following. When IBM tests new releases and fixes to z/OS, it does so with certain Started Tasks running as TRUSTED because they are considered critical to the operation of the system. Beginning with z/OS 1.10, these tasks are explicitly identified in the MVS Initialization and Tuning Reference manual. If you choose to run these Started Tasks without TRUSTED, you are using a configuration IBM has not tested. You might therefore encounter unanticipated access authorization failures that could result in a system outage. Furthermore, IBM might have difficulty helping you troubleshoot the cause of the problem since they will not have tested the configuration themselves.

We have never encountered a situation where a task should be made PRIVILEGED instead of TRUSTED. PRIVILEGED tasks should be changed to TRUSTED to enable monitoring.

RSH News

Upcoming ***RSH RACF Training***:

- RACF - Intro and Basic Administration
  April 28-30, 2009 - Boston, MA
  September 22-24, 2009 - Boston, MA
- RACF - Audit for Results
  May 19-21, 2009 - Boston, MA
  November 3-5, 2009 - Boston, MA

See our website for details and registration form.

Attend one of our upcoming presentations at the following ***RACF User Group meetings***:

CRUG	RACF & Storage Admin	4/9
NYRUG	RACF Command Tips	4/21
RUGONE	z/OS Unix File Security	4/23
KOIRUG	Circumventing RACF	5/7