RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 7
Issue 1

January
2013

Protect Shutdown Commands

Execution of certain operator commands can severely disrupt the operation of the system. RSH recommends you protect such commands with OPERCMDS profiles and permit no access to them except at a secure system console. The commands and their corresponding resource names are as follows:

$P	JESx.STOP.SYS
$P JES2	JESx.STOP.SYS
HALT EOD	MVS.HALT.EOD
HALT NET	MVS.HALT.NET
QUIESCE	MVS.QUIESCE

If your consoles are defined with AUTOLOGON, you will need to either permit access to Console IDs or allow operators conditional access using WHEN(CONSOLE) permissions.

Custom Field Names

CFIELD profiles end with the name of the locally defined field, e.g., USER.CSDATA.HOME. Do not choose field names where one is the prefix of another, such as HOME and HOMEADDR or LOC and LOCPHONE. When RACF tries to parse a command to process a CFIELD field name like HOME, it currently cannot determine whether "HOME" refers to the field HOME or to an abbreviation for HOMEADDR. The command will fail with an IRR52119I message. APAR OA38517 indicates this issue will be addressed in a future RACF release.

RRSF & Batches of Commands

Executing commands in an RRSF environment requires additional processing to route the commands to other RRSF nodes for execution and to handle the returning results. Executing extremely large sets of commands can degrade performance, especially when there are many nodes. To improve performance in such situations, construct identical sets of commands, one set for each node with an ONLYAT(node) keyword on each command, and then execute each set only on its corresponding node.

UNIX sudo & sudoedit

UNIX commands sudo and sudoedit enable a user to execute a specific command or edit a particular file with Superuser authority. They can even allow a user to perform functions with the authority of another user. These commands are useful in delegating limited Superuser authority when UNIXPRIV is not sufficiently granular.

These commands are not standard components of z/OS UNIX, but IBM has recently made them available for optional implementation. See IBM's Ported Tools for z/OS - Supplementary Toolkit.

The configuration file /etc/sudoers contains the rules defining what functions users may perform. For example, the rule …

bob ALL = /bin/ls

… allows user bob to execute the following sudo command to perform an ls on any directory.

sudo ls /*target-directory*

If your organization chooses to implement sudo, review the sudoers file thoroughly because improperly coded rules can allow unintended access with Superuser authority. Also, strictly control and monitor write access to this file.

Auditors: Confirm Started Task and Batch IDs are PROTECTED

Started Tasks are independent processes, often long running service routines, initiated by a z/OS START command. Examples are JES2, CICS, TCPIP, and VTAM. RACF IDs are assigned to

Started Tasks either by STARTED class profiles or by entries in RACF's ICHRIN03 table. No password is used to initiate a Started Task.

Batch IDs are process IDs that are assigned to batch jobs typically submitted by Started Tasks such as a job scheduler. SURROGAT class profiles allow jobs with these IDs to be submitted without requiring a password.

We strongly recommend Started Task and Batch IDs be used solely for their intended purposes as described above and that they not be given passwords. Assigning passwords exposes these IDs to misuse. This is a major concern because these IDs are often given extensive permissions to system and production data. These IDs should instead be made PROTECTED.

PROTECTED is an attribute that prevents use of the ID for logons where a password is required such as at a terminal or with FTP. It also prevents disruption of production processing because the ID cannot be accidentally or maliciously revoked by logon attempts using invalid passwords. Help Desk staff whose authority is limited to password resets are blocked from assigning passwords to these IDs. Only a user with System or Group SPECIAL authority can remove PROTECTED from an ID.

Use the LISTUSER command to inspect an ID's attributes and confirm it is PROTECTED.

```
USER=PAYBAT01 NAME=PAYROLL SYSTEM…
 DEFAULT-GROUP=BATCHIDS  PASSDATE…
 ATTRIBUTES=PROTECTED
```

SURROGAT Contest

SURROGAT class resources enable a user to perform certain types of work under the identity and authority of another user. Resource names are comprised of a USERID (under whose authority work will be performed) and a specific suffix or prefix. RSH is aware of eight prefixes and suffixes. Correctly name at least seven of them to be entered in a drawing for a $25 gift certificate from amazon.com. To enter, email your list to racftips@rshconsulting.com. Include your contact information. Only one entry per person is allowed, and only those individuals on our newsletter mailing list are eligible to enter. Entries must be received by January 31, 2013. The next newsletter will announce the winner and publish a list of all the prefixes and suffixes.

FIELD Permits to &RACUID

FIELD class profiles delegate authority to view and administer fields in profile segments to users who do not have SPECIAL authority. You can enable all users to view or update the contents of specific fields in their own user segments by permitting access to ID(&RACUID).

RSH News

Do not trust your critical RACF projects to anyone other than a bona fide RACF expert. To ensure your project is staffed with one of our RACF specialists, call RSH **before** you send a staffing requisition to HR.

See our latest RACF articles in Enterprise Tech Journal -- ***"The Demise of the Unix Default User"*** (August/September 2012) and ***"Ten More Ways to Improve RACF Performance"*** (October/November 2012). Links are on our website.

Faced with the daunting task of having to replace the Unix Default User? Attend our **RACF and z/OS Unix** class to get essential knowledge and tools for successfully completing this effort. The class is taught in half-day sessions over 3 days via WebEx (*no travel costs*). The next class is scheduled for January 15-17, 2013. See our website for details. ***Register today!***

Do you have a tip to share? Send it to us at racftips@rshconsulting.com. If we include it in our newsletter, we will gladly give you credit.