RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 8
Issue 4

October
2014

OPERCMDS Resource Prefixes

To the list of OPERCMDS resource name prefixes published in our July 2010 newsletter, add:

CEX	IMS Connect Extension
JESMON	JES2 Monitor
mimgr	CA-MIM (set by SAFPREX statement)

Started Tasks & REVOKE

To ensure system availability, z/OS allows a task to start even though its RACF ID is revoked. This guards against denial of service should someone intentionally or accidentally revoke a Started Task ID by entering invalid passwords. This exception only applies when the ID itself is revoked and not if the ID's connection to its logon group is revoked. Note that any batch jobs submitted by a Started Task running with a revoked ID will fail. You can avoid this issue altogether by making your Started Task IDs PROTECTED.

PROTECTED & INACTIVE

A PROTECTED ID is exempt from revocation due to inactivity. The SETROPTS INACTIVE setting is ignored. This is yet another reason to make Started Task and Batch IDs PROTECTED.

For more on PROTECTED, see our January 2013 newsletter.

Outsource Risk

Today, if your organization manages its own z/OS systems, you likely have a relatively small set of technicians (e.g., system programmers, storage administrators) who are highly privileged users with full control of your systems and access to all your data. By outsourcing management of your systems, you may gain the services of a much larger pool of technicians with more specialized skills. However, along with this, you are likely to experience a dramatic increase in the number of highly privileged users with access to your systems. *These individuals will not be your employees.* This has come as a nasty aftershock to firms who did not anticipate this situation. Make sure that all your auditors and your compliance team are aware of this and accept the risk before finalizing the outsourcing deal.

Call RSH for assistance with architecting and overseeing RACF in an outsourced situation.

z/OS Unix Command History

When you use the OMVS command, Unix keeps a history of your recent Unix commands in a file for reference and recall. The file name is set by the environment variable HISTFILE, and it defaults to $HOME/.sh_history. ($HOME is a variable set by HOME in your OMVS segment, and it defaults to the / directory.) The number of commands to be retained is set by HISTSIZE, which defaults to 128. To see if the HIST variables have been set to non-default values, look for them in the list of variables displayed by the Unix command **set**.

To display and recall commands, you can use the **history** and **r** commands, respectively. To list your 16 most recent commands, simply enter **history**. Note that each command has a sequence number. To list earlier commands, enter **history #**, where # is a starting sequence number. To list commands in a range, enter **history #1 #2**, where the #s are starting and ending numbers.

To recall and execute a prior command, enter **r #**, where # is its sequence number. The recalled command is executed as is. To edit a prior command before execution, it is easiest to display and then copy/paste the desired command to the command line where it can be modified.

In addition to the history file, Unix saves the most recent commands entered during your current session in memory. You can recall these commands and navigate within the list using PF12

(Retrieve) and PF11 (Forward Retrieve). Each will display a prior command in the command line where you can edit it before execution.

OMVS automatically tries to access the history file when executed. If the user is not authorized to access the file, access is denied and an ICH408I message is displayed. This usually occurs for ordinary users (non-Superuser) who have not been assigned a HOME. In these cases, OMVS tries to access file .sh_history in the root / directory, to which the user (hopefully) does not have write access. The violation is harmless, and the user's use of OMVS is unaffected but no history file is available.

Note as well the default history file name starts with a period '.', which makes it a hidden file. To list such files, you need to specify the **-a** operand with the **ls** command.

For the full details on Unix security, attend RSH's RACF - Securing z/OS Unix course.

WARNING Contest

RACF ignores the WARNING option on profiles in certain resource classes. Correctly name at least two such classes 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 name and 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 October 31, 2014. The January 2015 newsletter will announce the winner and list the classes.

Auditors: Ensure SETROPTS JES(BATCHALLRACF) is active

One of the primary tenets of security is to ensure all users are identified. There are ways batch jobs can enter a z/OS system without a user identity. RJE (Remote Job Entry) is one of them. A job running with an undefined user can access a resource if allowed by its associated profile's UACC (Universal Access).

To ensure all batch jobs have IDs authenticated by RACF, require the SETROPTS option JES(BATCHALLRACF) be activated.

SETROPTS has two other JES related settings. JES(XBMALLRACF) requires all Execution Batch Monitor (XBM) jobs have IDs. XBMs are unheard of these days. JES(EARLYVERIFY) is obsolete. Both can be ignored.

For more on auditing RACF, attend RSH's RACF - Audit and Compliance Roadmap course.

Invalid RACF Activation Code

As tweeted by @RSH_RACF on 9/11/14, "PARMLIB(IFAPRDxx) product enabling ID in z/OS 2.1 #RACF System Programmer's Guide is incorrect. See APAR OA45982 for details."

For the latest RACF news, follow @RSH_RACF.

RSH News

Which of these **RACF reviews** would be more helpful? One generated by software that issues a finding of risk simply because the number of users permitted access to a profile exceeds an arbitrary threshold – *or* – an RSH review that examines every permission and identifies those that are inappropriate. **Call RSH for your next review.**

Upcoming ***RSH RACF Training***:

- RACF - Audit & Compliance Roadmap
  October 27-30, 2014 - Boston, MA
- RACF - Intro and Basic Administration
  December 8-12, 2014 - WebEx
  March 23-27, 2015 - WebEx
- RACF - Securing z/OS Unix
  February 3-6, 2015 - WebEx