RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 10
Issue 2

April
2016

DSMON - LINECOUNT 0

To have DSMON print report headers only once at the beginning of each report, add the following instruction to your SYSIN input:

LINECOUNT 0

Unix Protection Loophole

Back when *User*, *Group*, and *Other* permission bits alone were used to grant access to Unix objects, a common protection scheme was to block access at the parent directory and permit *Other* access to objects beneath it. For example:

```
drwxr-x--- JOHN PAYDIR /pay
drwxrwxr-x DEB  PAYTEC /pay/data
-rwxrwxr-- SAM  PAYTEC /pay/data/file
```

Only JOHN and PAYDIR members could enter directory /pay to access underlying objects. This allowed *Other* permissions to be less strict for objects under this directory. The limitations of permission bits made this practice necessary.

This protection scheme is no longer appropriate today. Alternate authorities allow users to enter /pay and access underlying objects. They are:

USER AUDITOR or ROAUDIT
UNIXPRIV SUPERUSER.FILESYS
UNIXPRIV SUPERUSER.FILESYS.DIRSRCH

FSACCESS profiles can be used to block access granted by the UNIXPRIV authorities but not that of AUDITOR or ROAUDIT.

Nowadays, Extended Access Control Lists (ACLs) can be used in place of *Other* access permissions to provide better granularity of control.

Auditors: Review DITTO and FILE Manager DISK.FULLPACK

We revised our July 2007 RACF Tips newsletter article on this topic. An updated copy is available on our website.

SECLEVELAUDIT 64 Error

The first record in the RACF database is known as the Inventory Control Block (ICB). This is where all the SETROPTS options are defined. In the 1980s, there was an error in the ICB field definitions resulting in an overlap in the fields for PREFIX and SECLEVELAUDIT. Defining an eight character PREFIX caused SECLEVELAUDIT to be erroneously set to the value 64. If SETROPTS LIST shows SECLEVELAUDIT is set to 64 and SECLEVELs are not in use, it is safe to execute SETR NOSECLEVELAUDIT.

PROGRAM Class Anomalies

The PROGRAM class differs from all other resource classes in many ways, such as …

- It is activated by SETR WHEN(PROGRAM), not SETR CLASSACT(PROGRAM).
- Activating the class automatically loads the profiles into memory; however, they are stored in z/OS's Extended Common Storage Area (ECSA), not a RACLIST dataspace.
- To update the profiles stored in ECSA, you enter SETR WHEN(PROGRAM) REFRESH.
- SETR CLASSACT, GENCMD, GENERIC, GLOBAL, GENCMD, RACLIST, and LOGOPTIONS have no effect.
- All profiles are discrete, but profiles with an * or a ** are treated as generic.
- Profiles may not contain generic character % or a RACFVARS variable.
- Profiles are processed in reverse order. A profile like ABCD* is checked before ABCD, and ** is checked before *.
- When attempting to find the protecting profile, RACF first matches the program module name to the profile and then checks if the program was fetched from one of the libraries listed in the profile. If there is no library match, RACF continues checking other profiles.
- WARNING has no effect.

- PROGRAM resources can be used in conditional access permissions, but only with DATASET and SERVAUTH class profiles.
- The only conditional access permission that can be used in PROGRAM profiles is WHEN(SMF(*smf-id*)), and WHEN(SMF(*smf-id*)) can only be used with PROGRAM profiles.
- Although it is treated like a Member class, PROGRAM is actually a special type of Grouping class whose associated Member class is PMBR. PMBR is never used.

Finding RACF Exit Modules

DSMON does not give complete information on dynamic exits nor does it list SAF or Callable Services exits. To obtain information about them, execute the following operator commands.

```
DISPLAY PROG,EXIT,EXITNAME=IRREVX01
DISPLAY PROG,EXIT,EXITNAME=IRRVAF01
DISPLAY PROG,EXIT,EXITNAME=ICHRTX00
DISPLAY PROG,EXIT,EXITNAME=ICHRTX01
DISPLAY PROG,EXIT,EXITNAME=IRRSXT00
```

Catch-all / Backstop Profile

The term 'catch-all' or 'backstop' profile refers to an * or ** profile that protects all resources not covered by a more specific profile.

We recommend you define a catch-all profile in any class that allows generic profiles and is not a Default Return Code 8 class to ensure all related resources are protected. Catch-all profiles are not, however, recommended for classes FACILITY, UNIXPRIV, or XFACILIT.

Depending on the class, you may wish to set the catch-all profile's UACC to NONE to prevent access unless permitted or to READ with AUDIT(ALL) to allow but log all access.

We prefer use of ** for the catch-all profile. This enables you to list just the catch-all profile with an RLIST *class* ** command. If you use profile * instead, to list the profile you must code an RLIST *class* * command, which causes all profiles in the class to be listed with profile * being shown last.

If you define both an * and ** profile, the * profile will be checked first and used as the catch-all, except with the PROGRAM class.

TSO PASSWORDPREPROMPT

Normal TSO processing prompts a user for an ID at logon and then displays the TSO logon panel filled in with the contents of the ID's TSO segment or SYS1.UADS entry. If the ID has no segment or entry, TSO displays the message "IKJ56420I Userid *userid* not authorized to use TSO", and the logon panel fields are blank. This behavior can be exploited to discover valid TSO IDs.

This concern is addressed in z/OS 2.2 and in 1.13 and 2.1 with APAR OA44855. The LOGON statement in TSO's PARMLIB member IKJTSOxx has a new parameter PASSWORDPREPROMPT. If set to ON (the default is OFF), users must enter a valid RACF ID and password before any TSO logon information is displayed. Moreover, IDs defined in SYS1.UADS but not RACF will not be allowed to logon to TSO unless RACF is inactive.

Prevent Anonymous FTP Job Submissions

To prevent anonymous FTP users from submitting batch jobs, set ANONYMOUSLEVEL to 3 and ANONYMOUSFILETYPEJES to FALSE in your FTP configuration parameters. (APAR OA49668)

RSH News

RSH has redesigned its RACF training curriculum and now offers basic, intermediate, and advanced classes via WebEx. Visit our website for details.