RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 11
Issue 4
October
2017

RACF 2.3 SETROPTS ENHANCEDGENERICOWNER

SETROPTS GENERICOWNER has long existed as a control option that prevents users with Class Authorization (CLAUTH) from creating more specific profiles that undercut an existing profile unless the user has authority over that existing profile. This option does not, however, prevent such users from circumventing this restraint by creating more specific members in grouping class profiles. The new ENHANCEDGENERICOWNER option in RACF 2.3 closes this loophole.

For more on RACF authorities, attend our "RACF Level II Administration" course.

SMF Logging for Logons

At logon, in addition to authenticating the user, RACF may also verify the user's access authority to one or more general resources in classes such as SURROGAT, JESINPUT, JESJOBS, and APPL. If successful, an SMF Type 30 or 80 record may be created for the logon, and based on audit settings, RACF may also create SMF Type 80 Event Code 02 (ACCESS) records to log access to the aforementioned general resources.

However, when a logon fails because of insufficient access to one of these resources, no SMF Type 80 ACCESS record is created to log the resource access violation. Only an SMF Type 80 Event Code 01 (JOBINIT) record is produced. The Event Code Qualifier for this record indicates the reason for the logon failure, which will identify the associated resource class for the violation. For example, Event Code Qualifier 17 (Submitter not authorized by user) is a SURROGAT violation.

Neither the general resource name nor its protecting profile are specifically identified in the JOBINIT record created for such a logon failure, but the record does contain sufficient information to determine the resource name. The RLIST command can then be used to identify the profile.

Refer to the RACF Macros and Interfaces manual for a list of these Event Code Qualifiers.

Grouping Profile Member Sequence

The method used to add members to a grouping class profile determines the sequence in which the members are stored in the profile.

Members specified in the ADDMEM keyword of an RDEFINE command are added to the new profile in the sequence that they appear in the command. ADDMEM(A B) would result in the profile having a member list of A B.

Conversely, members specified in the ADDMEM keyword of an RALTER command are added to the front of the existing member list in the reverse sequence that they appear in the command. ADDMEM(X Y) would result in the profile above having a member list of Y X A B.

Member sequence matters when processing variable string values in RACFVARS profiles, especially when a shorter string is the prefix of a longer one. It matters, too, if multiple translation IDs are mistakenly added to a NODES profile because RACF only uses the first value found.

RLIST displays profile members in alphanumeric sequence. IRRDBU00 database unload 0503 records, however, show the members in the sequence they are stored in the profile.

For more on Grouping Profiles and RACFVARS, attend our "RACF Level II Administration" course.

Auditors: Understanding SMF

System Management Facilities (SMF) is z/OS's centralized event log collection and recording service. A wide variety of system components, RACF included, send event information to SMF for collection. Each uses unique numbers to identify its events. RACF uses 80, 81, and 83.

SMF first writes event records to buffers in memory and from there to either an SMF dataset or a log stream. SMF datasets only store records for a single z/OS system; whereas, a log stream can store data from multiple systems. Usually two or more SMF datasets are allocated, and when the active one fills, SMF automatically switches to an empty one. Typically, records in the dataset that just filled are archived and the dataset is cleared for reuse.

The configuration of SMF is defined in PARMLIB members prefixed SMFPRM. These members are specified at IPL and may be changed dynamically.

To review the options currently in effect on a z/OS system, execute operator command "DISPLAY SMF,O". Here is an abbreviated output sample. The source of each parameter is shown after '--'.

```
IEE967I 13.45.12 SMF PARAMETERS 838
        MEMBER = SMFPRM91
        BUFUSEWARN(25) -- DEFAULT
        BUFSIZMAX(0128M) -- DEFAULT
        SUBSYS(STC,NOTYPE(16)) -- SYS
        SUBSYS(STC,EXITS(IEFUSO)) -- PARMLIB
        SUBSYS(STC,EXITS(IEFUJP)) -- PARMLIB
        SYS(EXITS(IEFUAV)) -- PARMLIB
        SYS(EXITS(IEFU29)) -- PARMLIB
        SYS(NOTYPE(16)) -- PARMLIB
        NOBUFFS(MSG) -- PARMLIB
        LASTDS(MSG) -- PARMLIB
        SID(SYSN) -- PARMLIB
        JWT(2400) -- PARMLIB
        NOPROMPT -- PARMLIB
        DSNAME(SYS1.SYSN.MAN2) -- PARMLIB
        DSNAME(SYS1.SYSN.MAN1) -- PARMLIB
        ACTIVE -- PARMLIB
```

Parameter SID assigns a system identifier, and this identifier is included in every SMF record.

SMF can be configured to save or exclude events by number (subparameters TYPE or NOTYPE) and to activate SMF exits. These options can be set for the entire system and for specific subsystems (parameters SYS and SUBSYS).

SMF exits can monitor, copy, modify, or suppress records. Most Security Incident Event Monitoring (SIEM) products provide SMF exits to capture event data in real time. Note that these SIEM exits will not see excluded events.

In your audit, request output from the above command for every z/OS system. Confirm that RACF and other critical record types are retained.

LDAP & SUPERUSER.FILESYS

The RACF commands generated by LDAP's dsconfig utility permit the server's ID CONTROL access to profile SUPERUSER.FILESYS in the UNIXPRIV class. This access is not necessary. Instead, the LDAP server's ID can be permitted appropriate access to its Unix files and directories using chmod, chown, or setfacl commands.

For more on protecting Unix, attend our "RACF - Securing z/OS Unix" course.

JESSPOOL SYSLOG Resource

In the JES2 Guide, the name of the JESSPOOL resource for SYSLOG is: ('*lnode*' is local node)

lnode.+MASTER+.SYSLOG.*jobid.dsidentifier.?*

The SDSF Guide, however, gives the name as:

lnode.+MASTER+.SYSLOG.SYSTEM.*sysname*

The JES2 Guide is correct.

RACF 2.3 WORKATTR WAEMAIL

You can now associate a RACF user with an email address using the new WAEMAIL field in the WORKATTR segment. This 246-byte field was added in RACF 2.3 and is available in 2.2 with APAR OA50735. The RACF database has to be at Application Identity Mapping (AIM) structure stage 3 to use it. Each email address must be unique - it cannot be assigned to multiple users.

RSH News

If you are unable to find qualified candidates to staff your RACF administration team, call RSH about our outsourcing and ad hoc services.

Familiarize your managers with RACF by giving them a copy of RACF - An Overview, available via our website's "RACF Center" webpage.

Receive a 5% discount on the admission fee for any RSH RACF training seminar if you attended one of our seminars in the past 12 months.

Not a member of RACF-L? Join today. See our website for instructions.