RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 11
Issue 1

January
2017

PPT NOPASS Change

After applying APAR OA50215, the Program Properties Table (PPT) parameter NOPASS will enable a program to bypass RACF dataset protection only when it is executed as a Started Task. If the program is executed in batch, NOPASS is ignored and message IEF188I is issued. New parameter NOPASS_ALLOWBATCH can be specified to allow a program to bypass protection in batch. Use of this new parameter may open integrity issues and is best avoided.

Neither NOPASS nor NOPASS_ALLOWBATCH allow bypass of RACF protection for the STEPLIB or JOBLIB library from which the program is fetched. The ID associated with the process must be permitted access to the library.

For more on the PPT, see "Auditors: Check the PPT" in the April 2013 issue of this newsletter and attend our "RACF Level II Administration" course.

NOREVOKE = RESUME

Setting REVOKE(*date*) on a user profile will prevent the user from logging onto the system on or after the specified date. LISTUSER will show such an ID as REVOKED once its revoke date is reached. However, the ID is not truly REVOKED because the REVOKED flag in the user profile is not set to ON. Nor is this flag set to ON if the user attempts to logon and is denied access because of the REVOKE(*date*). Therefore, if you execute ALTUSER NOREVOKE to remove the date, this effectively resumes the ID. To keep the ID REVOKED after removing REVOKE(*date*), you must execute ALTUSER REVOKE.

WARNING SMF Records

Access allowed by WARNING always generates an ICH408I message, but a corresponding SMF record will not be generated unless auditing options are set correctly. To ensure an SMF record is created, either SUCCESS or FAILURES in either AUDIT or GLOBALAUDIT must be set to log the intended level of access associated with the WARNING event. For example, if FAILURES is set to UPDATE, but the WARNING access intent was READ, no record will be generated. The same is true if AUDIT is set to NONE.

Regardless of the profile settings, WARNING events will always be logged if the user has UAUDIT or if SETROPTS LOGOPTIONS for the class is set to either SUCCESSES or ALWAYS.

To log all WARNING events, ensure all profiles have at least AUDIT(FAILURES(READ)).

AUDITORS: Review the Global Access Table (GAT)

The GAT is a RACF performance enhancement feature. It is intended to grant instant access to system resources that all users may need.

The GAT is constructed from profiles defined to the GLOBAL class. The names of these profiles correspond to the names of other resource classes (e.g., DATASET). Within each profile is a list of entries that look much like normal resource profiles, including the use of generic masking characters (e.g., CATALOG.**). Associated with each entry is an access level (e.g., READ) which is the highest level of access the GAT grants to all users. After creating a GLOBAL profile for a resource class, it must be activated with the command SETROPTS GLOBAL(*classname*).

Variables &RACUID and &RACGPID can be used in constructing GAT entries. &RACUID substitutes for the user's own logon ID. It is useful in coding entries when the user is considered to be the owner of the resource or the user's ID is part of the resource name. DATASET entry &RACUID.** with ALTER access is often coded to give TSO users instant access to their own datasets. &RACGPID substitutes for the user's current connect group (i.e., the group the user logged on with), typically the user's Default Group.

The GAT check occurs very early in the RACF access authorization decision process and before resource profiles are checked. When a user attempts to access a resource whose name matches a GAT entry, RACF grants access immediately if the requested level of access is equal to or less than the level specified in the entry. No further checking is done, and the access is not logged.

The GAT only grants access. It does not deny access. If access is not granted by the GAT, profile access checking is done. A GAT entry with a permission of NONE merely causes RACF to ignore the GAT and check the protecting profile.

GAT entries can undermine security by granting access that normal resource profiles would deny or by omitting logging specified in these profiles.

To review the GAT, start by obtaining a DSMON report created with option FUNCTION ALL or FUNCTION RACGAC to list all GAT entries by class. Then compare entries in the GAT with the corresponding resource profiles to see if any entries allow unintended access or omit intended logging. This analysis is complicated because GAT entries are rarely aligned with the underlying profiles. You are most apt to find problems with GAT entries having very broad generics like SYS1.**. Some entries may have no underlying profiles, and the GAT alone grants access.

GAT permissions act much like Universal Access (UACC) permissions by granting access to all users, including those executing without a RACF ID (a.k.a. undefined users). GAT entries undercut use of UACC(NONE) and ID(*) permissions that otherwise restrict access to RACF defined IDs.

For more on auditing RACF, attend our "RACF Audit and Compliance Roadmap" course.

RACFRW Limitations

The SMF reporting utility RACF Report Writer (RACFRW) was "functionally stabilized" in 1992, and has not been enhanced since. It can only be used to report information documented as being recorded in SMF Type 80 records prior to its stabilization. RACFRW cannot report on events or command operands added to RACF thereafter. Such exclusions include z/OS Unix events, newly added SETROPTS options, and newly added command operands such as ALTUSER's NOEXPIRE. For those still using RACFRW, we highly recommend you switch to using the SMF unload for reporting.

Visit RSH's website for instructions and samples for processing the SMF and IRRDUB00 database unloads using REXX and DFSORT_ICETOOL.

Logging FTP JES Activity

To find out who may be submitting batch jobs or fetching SYSOUT via FTP, add the following parameter to your FTP configuration to generate SMF 119 records for these events.

```
SMFJES TYPE119
```

For more on this topic, see "FTP and JES" in the April 2010 issue of this newsletter.

CIM and SURROGAT

The Common Information Model (CIM) server Started Task, often named CFZSRV, needs READ access to the profile protecting the SURROGAT resource associated with its own ID BPX.SRV.*cimtaskid*. See APAR OA16911.

RSH News

2016 is another year of significant milestones. It is RACF's 40th anniversary. For our founder Robert S. Hansel, it is his 40th year in IT, 35th year in IT security, and 30th year working with RACF.

Has your organization lost or is it about to lose its RACF SME? We can provide RACF experts to fill in on a temporary or part-time basis. Call us.

RSH's website has recently been praised as a source for highly valuable RACF information in the Cheryl Watson's Tuning Letter. Ms. Watson is a world-renowned z/OS performance tuning expert. Visit her website at http://watsonwalker.com/.