RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 7
Issue 2
April
2013

Improved RACF Googling

How often does your Google search on a RACF topic return page after page of irrelevant links? Would you like to tell Google to search only those sites where you expect to find answers to your RACF questions? You can simply by appending:

site:ibm.com OR site:rshconsulting.com

SURROGAT Contest Winner

Mike Booher of Secura was the winner of our SURROGAT resource naming contest. Here is a list of the resources and their related products.

userid.DFHINSTL	CICS
userid.DFHSTART	CICS
userid.DFHEXCI	CICS
userid.DSITSOSV	Tivoli NetView
userid.SUBMIT	JES
ATBALLC.*userid*	MVS/APPC
BBO.SYNC.*userid*	WebSphere
BPX.SRV.*userid*	z/OS Unix
LOGONBY.*userid*	z/VM.
SYSREXX.*userid*	System REXX

IRRUT200 ACTIVATE Hang

When you specify PARM=ACTIVATE with IRRUT200, it copies the Primary database to the Backup and then activates the Backup. IRRUT200 has been using the RACF subsystem to execute an RVARY to activate the Backup. If the RVARY is placed in the RACF subsystem queue behind other work needing serialization, IRRUT200 will hang. APAR OA35325 has a fix for this problem.

DEFINE RECATALOG Check

There is now a FACILITY class resource check for IDCAMS command DEFINE RECATALOG. The check was introduced via APAR OA33013 and has since been incorporated into z/OS 1.13 . The resource is STGADMIN.IGG.DEFINE.RECAT. READ access allows DEFINE RECATALOG for a dataset without having access to the dataset. The original implementation of this check actually granted too much authority and required a corrective fix. See APAR OA38273 for details.

Thank you Joel Tilton of Publix for this tip.

Protecting Program EDGINERS

It is standard practice to protect the z/OS tape initialization program IEHINITT with a profile in the PROGRAM class and to limit access to tape librarians and others responsible for initializing and erasing tapes. But should you do the same for EDGINERS, IEHINITT's equivalent provided with DFSMS's Removal Media Manager (RMM)?

Use of EDGINERS can be controlled by a profile in the FACILITY class that guards resource STGADMIN.EDG.OPERATOR. UPDATE is needed to use it, but if no guarding profile is defined, anyone can use EDGINERS. Just to be safe, protect it with a PROGRAM profile as well.

Auditors: Check the PPT

The Program Properties Table (PPT) is a z/OS configuration feature used to assign certain high level privileges to specific programs. z/OS comes with a PPT preloaded with entries for IBM programs. They are documented in the MVS Initialization and Tuning Reference manual.

An installation can define its own PPT entries via PARMLIB member SCHEDxx. These entries require close scrutiny, especially if they are assigned privileges KEY(n) or NOPASS.

KEY can be used to assign a Storage Protection Key to a program in the range of 0 to 7. Keys in this range are considered to be 'SYSTEM' keys

and allow the program to execute privileged Supervisor Calls (SVCs) that it could use to elevate its authority and circumvent security.

NOPASS originally meant Bypass Password Protection and harks back to when datasets were protected by MVS passwords. It also bypasses RACF. Programs with NOPASS will not be subject to authorization checks when accessing datasets.

DSMON's Program Properties Table Report lists all PPT entries and indicates if they have been assigned KEY(0-7) or NOPASS. Require clear and convincing justification as to why either of these privileges has been assigned to any installation-defined entry. One to watch for is the CICS program DFHSIP which is often needlessly and inappropriately assigned NOPASS. Review the code of any PPT program that was written in-house to confirm it does not compromise security.

It requires more than just a matching name for a program to acquire PPT privileges. The program must also be executed from an Authorized Program Facility (APF) library. Ensure update access to all your APF libraries is very restricted.

The IBM-supplied PPT will always contain a few entries that are not applicable to a particular system. A system's Job Entry Subsystem will be either JES2 or JES3, so either the HASJES20 or IATINTK entry will be extraneous. There is no harm in leaving such entries intact and nothing to be gained by having them removed or altered.

RACF FMID Reference

Ever come across a reference to RACF by its 4-digit Function Modification Identifier (FMID) code and wondered what release of RACF it meant? The RACF FMIDs are listed in the chapter on SMF records in the RACF Macros and Interfaces manual. See the description for the type-80 record field SMF80VRM. Here are three RACF FMIDs.

7760	z/OS Security Server (RACF) V1 R11
7770	z/OS Security Server (RACF) V1 R12
7780	z/OS Security Server (RACF) V1 R13

RACF Health Checker Issues

The RACF_SENSITIVE_RESOURCES check flags a dataset with a high-severity exception 'V' for not being found on its designated volume when, in fact, it actually does exist but is under exclusive control of some other address space. No fix is yet available. See APAR OA41458.

RSH discovered that OPERCMDS resources MVS.SET.PROG and MVS.SETPROG are flagged with a high-severity exception 'E' if they are protected by a profile with UACC of READ. These resources, however, require a minimum of UPDATE permission to use them. IBM has been notified and will eventually fix this error.

Group GID VLF Cache Problem

If you happen to connect a user to a group with a GID at the same instant the user is dubbing into Unix for the first time, the VLF cache entry for the user's User Security Packet (USP) may not pick up the additional group GID. The only way to correct this is to recycle VLF, which requires recycling LLA. See APAR OA41056 for details.

RSH News

Many thanks to all who have responded to our queries seeking to confirm you are receiving the newsletter and helping us update the mailing list.

Upcoming ***RSH RACF Training*:**

- RACF - Audit & Compliance Roadmap
  April 23-25, 2013 - Boston, MA
- RACF - Intro and Basic Administration
  May 21-23, 2013 - Boston, MA
- RACF and z/OS Unix
  July 23-25, 2013 - WebEx