RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 7
Issue 3

July
2013

IRRHFSU Enhancements

IRRHFSU is a free, unsupported IBM utility that creates a text file unload of Unix File System file and directory File Security Packets (FSPs) much like IRRDBU00 does for the RACF database.

RSH has been using IRRHFSU extensively with efforts to replace BPX.DEFAULT.USER and recommended enhancements that the utility's author, Bruce Wells, helpfully implemented. (*Many thanks, Bruce!*) IRRHFSU now provides the name of the file system dataset where the Unix file or directory resides, the contents of symbolic and external links, and a new record 0904 with the characteristics of each mounted file system. The newest version is dated October 19, 2012.

IRRHFSU is available for download via the RACF homepage on the IBM website, which you reach by entering URL http://www.ibm.com/racf. Go to Resources tab and then the Download link.

For tips on using IRRHFSU, visit our website to see our presentation on this utility.

z/OS 1.13 TRUSTED Tasks

As indicated in the MVS Initialization and Tuning Reference, z/OS 1.13 added these two Started Tasks to the list of those to be made TRUSTED.

Common Event Adaptor (CEA)
Hardware Instrumentation Services (HIS)

Group GID(0)

Unlike UID(0), GID(0) does not grant any special privileges. However, when a Temporary File System (TFS) is created and mounted, GID(0) is automatically defined as the GROUP in its File Security Packet (FSP) with full 'rwx' permissions. RSH recommends creating a group with GID(0) as a placeholder for the TFS GROUP.

Also, to install the Supplementary Toolkit for IBM Ported Tools for z/OS, which contains the sudo command (discussed in the January 2013 issue of our newsletter), a GID(0) group is required and will be made the FSP GROUP on the sudoers file.

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

RACDCERT LIST Clarification

The output of the RACDCERT LIST changed in z/OS 1.13 with respect to a certificate's PRIVATE key. See APAR OA41863 for clarification as to how RACDCERT ADD and GENCERT parameters affect the LIST output.

Group GID VLF Problem Update

Our previous newsletter alerted you to a problem whereby the VLF cache entry for the user's User Security Packet (USP) may not pick up the GID of a newly connected group. APAR OA41056 has since been updated and now recommends that to correct this condition, you remove and reconnect the user to the group on the system where the user is experiencing the problem.

FIELD Authority to Add an Empty Segment or Delete a Segment

FIELD class profiles allow non-System SPECIAL users to view and administer profile segments. For instance, if a user has UPDATE access to resource USER.CICS.OPIDENT and executes command "ALU *userid* CICS(OPIDENT(ABC))", a CICS segment will be added to the USERID if it does not already have one and the OPIDENT field will be filled in with the value ABC. The user can execute subsequent ALU commands to either change the value (e.g., CICS(OPIDENT(XYZ))) or delete the value (e.g., CICS(NOOPIDENT)). Deleting all the individual field values in a segment does not delete the segment itself.

To add a segment without specifying any fields or to delete a segment, the user needs UPDATE access to the resource *profile.segment.* (e.g., USER.CICS.). Note the trailing period (.) on the resource name. Absent a discrete profile, a generic profile with a prefix of *profile.segment* that ends with .* or .** (e.g., USER.CICS.*) would cover such a resource. Note that UPDATE access to *profile.segment.* alone permits the user to delete the segment even when the user has no authority to administer any of the segment fields.

Auditors: Ensure Effective Use of RESTRICTED

The typical z/OS environment is likely to have many resources accessible to all users. This access may be granted by the Universal Access (UACC) setting on a profile, by access permitted to ID(*), or by entries in the Global Access Table (GAT). Such permissions may allow access to information that should only be shared internally.

Certain IDs should have very limited authority and should not be able to access generally available resources. Examples are NJE and RJE IDs assigned to external organizations (e.g., business partners) and FTP IDs used by non-mainframe processes. These IDs usually have a very specific purpose, such as to upload a particular dataset, and do not need anything else. Such IDs typically have fixed passwords known to several system administrators, making accountability for their use difficult. Ideally, IDs of this nature should be assigned the RESTRICTED attribute.

An ID with the RESTRICTED attribute can only access those resources to which it has been explicitly permitted access, either directly to the ID itself or to one of its groups. RESTRICTED users cannot gain access via UACC, ID(*), or GAT.

Request and review a listing of IDs assigned to users and processes belonging to external organizations and any internal IDs used by processes on other platforms for file transfers and the like to see if they are RESTRICTED. If not, recommend they be made RESTRICTED if their access needs are fixed and limited in scope and it is reasonably practical to do so.

Also see article RESTRICTED & UNIX Access *in July 2009 issue for guidance on ensuring RESTRICTED is applied to Unix file access.*

Class SYSAUTO

IBM is introducing a new product called IBM Automation Control for z/OS. This product will use a new general resource class - SYSAUTO. APAR OA41282 adds the new class to RACF.

RSH News

Our RACF - Audit & Compliance Roadmap and RACF - Securing z/OS Unix classes have both been expanded by half a day to cover additional material. We have kept the admission fee the same - *for now*. Register soon to lock in the current price.

We have scheduled additional RACF - Securing z/OS Unix classes this year to better assist users address their BPX.DEFAULT.USER migrations.

Upcoming ***RSH RACF Training***:

- RACF - Audit & Compliance Roadmap
  November 5-8, 2013 - Boston, MA
- RACF - Intro and Basic Administration
  October 21-25, 2013 - WebEx
- RACF - Securing z/OS Unix
  July 23-26, 2013 - WebEx
  September 17-20, 2013 - WebEx
  December 3-6, 2013 - WebEx

Be sure to attend our presentations at SHARE this August in Boston. And check out the updated presentations and newest surveys on our website.