RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 5
Issue 3

July 2011

z/OS Security & Integrity APARs

IBM occasionally issues APARs to fix security and system integrity problems for System z. Though the PTFs are shipped as usual via the RSU process to z/OS customers, IBM does not make information about these APARs publically available or provide details about the vulnerabilities they might address. Providing details could put systems at risk. These APARs are not marked HIPER but should be regarded as equally, if not more, important. Ensure your z/OS Systems Programmers are aware of and applying these security fixes. IBM only grants access to limited information about these APARs to individuals who request it and have a verified need to know. For more information, go to http://www.vm.ibm.com/security/aparinfo.html.

Thank you Mark Nelson of IBM for this tip.

Performance Tip: IRRDBU00

To minimize interfering with production work, do not run an IRRDBU00 unload using a live RACF database. Always make an IRRUT200 copy first and create the unload from the copy. Follow this same process when creating database extracts for RACF administration products.

Monitoring Using JESJOBS

JESJOBS profiles can restrict who can submit jobs with certain job names and IDs. These profiles have the format shown below. (Note *userid* is the USER= ID on the JOB card.)

SUBMIT.*nodename.jobname.userid*

To discover who is submitting jobs using the password of a batch or Started Task ID that is not PROTECTED, create a profile such as the following and review the resulting SMF records.

SUBMIT.*.*.BAT01 UACC(READ) AUDIT(ALL)

This same profile can be used to identify jobs submitted using SURROGAT authority. Auditing a SURROGAT profile only produces records showing that SURROGAT authority was used for a particular ID, but it does not identify the jobs. JESJOBS can provide job information.

Be advised JESJOBS issues a **default return code of 8**. If no profile covers a job, submission is blocked. Activate GENERICs and define a profile of ** with UACC of READ before activating JESJOBS.

IRRHFSU & UAUDIT

IRRHFSU is a free IBM utility that creates a text file unload of HFS file and directory File Security Packets (FSPs) much like IRRDBU00 does for the RACF database. Do **not** execute this utility with an ID that has UAUDIT; otherwise you could inundate SMF with log records for every directory search and read.

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

Auditors: Review SETROPTS AUDIT(classes)

SPECIAL is just one of a number of different authorities for creating and changing RACF profiles. Others include profile owner and Class Authorization (CLAUTH). SETROPTS option SAUDIT only records profile changes made using SPECIAL authority.

To record changes to profiles in a particular class using an authority other than SPECIAL, activate SETROPTS AUDIT(*class*). This option will cause all profile changes to be logged regardless of what authority is used.

SETROPTS AUDIT is widely misunderstood and many believe it causes all access to be logged. In general, though, only profile changes will generate SMF records. For certain classes, it will result in logging of other events. They are:

DATASET	Create / Delete dataset
FSOBJ	Create / Delete Unix file/directory
IPCOBJ	Create / Delete Unix objects
PROCESS	Dub / Undub Unix process
USER	Password change during logon

To maintain a comprehensive audit trail of profile changes, we recommend AUDIT be activated for all classes. Execute the following command now and after each system upgrade.

SETROPTS AUDIT(*)

Your Unix Default User May Own Files & Directories

If you have a Unix Default User assigned via FACILITY BPX.DEFAULT.USER, executing Unix command 'chown *userid directory/file*' specifying a USERID that does not have an OMVS segment will result in the uid of the Unix Default User being assigned as the Owner of the target directory or file. IRRHFSU can be helpful in finding such directories and files.

More FACILITY Resources

The latest version of our FACILITY class presentation, available on our website, includes these recently discovered resources.

BPX.EXECMVSAPF.*program-name*
HWI.APPLNAME.HWISERV
HWI.CAPREX.*netid.nau.caprec*
HWI.TARGET.*netid.nau*[.*imagename*]
HWS.*ims-connect-name*
IMPLEX.*stack-name*
ISG.QSCANSERVICES.AUTHORIZATION
NEZ.NSEPARM.*subsystem-name*
nimispf-prefix.service[.*option*]
SDW[.*command*]
SELCOPYI.*resource-name*
SSZ.MOUNT
TDP*id.dbc-user-name*
userid_nvas-external-group

Thank you Joel Tilton of Publix, David Freedman of William Data Systems, and Jerry Seefeldt of NewEra Software for your contributions.

Grouping Profile Name Length

Grouping class profile names can be thought of simply as labels for sets of member resources. The profile names themselves are not used for access authorization decisions, and the length of their name does not matter. To give yourself the greatest flexibility in creating meaningful profile names, set MAXLENGTH and MAXLENX to 246 when creating grouping classes.

RSH News

Robert S. Hansel was named the Vanguard Security Conference 2011 ***"Top Gun"*** Instructor for having received the highest student ratings at the prior year's conference.

2011 is a year of significant milestones. It marks the 100th anniversary for IBM as well as the 35th anniversary for RACF. For our founder ***Robert S. Hansel***, it is his 35th year in IT, 30th year in IT security, and ***25th year working with RACF***.

Upcoming ***RSH RACF Training*:**

- RACF - Intro and Basic Administration
  October 11-13, 2011 - Boston, MA
- RACF - Audit for Results
  October 25-27, 2011 - Boston, MA
- RACF - Securing z/OS Unix
  January 24-26, 2012 - WebEx