RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 8
Issue 1

January
2014

CHOWN.UNRESTRICTED

Prior to z/OS 2.1, if discrete UNIXPRIV profile CHOWN.UNRESTRICTED was defined, any user owning a Unix file or directory could change its OWNER or GROUP to any other user or group.

Beginning with z/OS 2.1, users need READ access to this profile to make such changes. To set the OWNER to UID(0), UPDATE is required.

Sites with CHOWN.UNRESTRICTED already defined should adjust this profile in advance of the upgrade by adding either UACC(UPDATE) or WARNING to avoid a loss of functionality. The permissions can be tightened after the upgrade.

Security APAR OA41364 rolls this change back to z/OS 1.12 and 1.13. See DOC APAR OA41466.

@RSH_RACF on Twitter

RSH set up Twitter account RSH_RACF to tweet RACF tips and news. Here are recent tweets.

- IRRDBU00, #RACF Database Unload, only lists profiles in classes defined to the system "where executed" and may not list all profiles.
- Make an error entering a #RACF command and it annoyingly prompts you for a correction. To avoid this, enter TSO command PROFILE NOPROMPT.
- By default, the FSP for a z/OS Unix TFS is given GID 0 for its GROUP. Be sure to define a #RACF group with this GID to reserve it.

You do not need a Twitter account to see our tweets. Just visit https://twitter.com/RSH_RACF.

To avoid having to repeatedly check Twitter's website, sign up for a Twitter account and then have our tweets sent to your mobile device via text message. The RACF Center webpage on our website has instructions on activating this feature.

Sign up for Twitter today at www.twitter.com and follow us. Be sure to read all our past tweets.

BPX Profiles & Superuser

A Unix Superuser (effective UID of 0) can perform the functions controlled by the following FACILITY class resources even if not permitted access.

BPX.CONSOLE
BPX.EXECMVSAPF.*program*
BPX.JOBNAME
BPX.UNLIMITED.OUTPUT

A Superuser can perform the functions controlled by the following resources if they are not defined to RACF. Once a corresponding profile is defined, Superusers must be permitted access to continue to use the related functions. Implement profiles with care so as not to cut off needed access.

BPX.JOBNAME
BPX.MAP
BPX.POE
BPX.SHUTDOWN
BPX.STOR.SWAP
BPX.UNLIMITED.OUTPUT
BPX.WLMSERVER

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

Auditors: Ensure OPERATIONS is Controlled, Part 2

In Part 1 of this series (RACF Tips Newsletter of October 2013), we introduced you to the powerful OPERATIONS authority attribute. This article discusses how you identify OPERATIONS users.

The simplest means of finding users with OPERATIONS authority is to review the Selected User Attribute Report generated by the RACF utility DSMON. Look for users who have SYSTEM or GROUP under the OPERATIONS column. SYSTEM means OPERATIONS is assigned to the user's ID. GROUP means it is assigned to one or more of the user's group connections. A user with SYSTEM OPERATIONS might also have GROUP OPERATIONS, which, even though superfluous, is not flagged by DSMON. DSMON also does not name the group(s) where the user has group level OPERATIONS. For this, you will need to issue RACF's LISTUSER command and then look for OPERATIONS in the connect attributes for each group as shown below. (Lines are truncated.)

```
USER=RJONES   NAME=RODGER JONES   …
  GROUP=DASDMGT  AUTH=USE  CONNECT…
    CONNECTS=    00  UACC=NONE    …
    CONNECT ATTRIBUTES=OPERATIONS …
    REVOKE DATE=NONE   RESUME DATE…
```

Be aware there may be users who do not have OPERATIONS themselves but who can gain the use of this authority. See article Auditors: Review SURROGAT Batch Submit Authority in the April 2007 issue of our RSH RACF Tips newsletter.

In future articles, we will examine how to place restrictions on this authority and monitor its use.

For more on auditing RACF, attend RSH's RACF - Audit & Compliance Roadmap course.

CA-1 CDT Entries

The CA-1 Tape Management Programming Guide provides instructions for defining resource classes CA@APE and CA@MD to RACF's Class Descriptor Table (CDT) using either ICHERCDE macros or CDT class profiles. The ICHERCDE example results in the classes being defined with the default OPER=YES, which enables the use of OPERATIONS authority. The CDT profile example, however, results in their being defined with the default OPERATIONS(NO), which does not enable OPERATIONS use. RSH strongly discourages the use of OPERATIONS. If you defined them originally using ICHERCDE per CA's instructions, redefine them using CDT profiles without specifying OPERATIONS(YES).

If you set CA-1's option FUNC to EXT (Extended), it will append VOLSER and Unit Control Block (UCB) device information to some CA@APE resource names. For example, BLPRES expands to become BLPRES.V*volser*.UCB*nnnn*. Both of CA's CDT samples let the maximum resource name length default to 8. Before changing FUNC to EXT, increase the resource name length in the CDT entry for class CA@APE to at least 26 and allow the use of special characters (.) in the name.

```
RALT CDT CA@APE CDTINFO(MAXLENGTH(26)) +
   OTHER(ALPHA NUMERIC NATIONAL SPECIAL)
```

IRRHFSU Utility Update

We have found that in a few cases the IRRHFSU 0900 record does not show the USERID associated with the UID that owns the file or directory. We have not found this to be true for ACLs records, but our sample size is smaller. Let us know if you have encountered this as well.

One of IRRHFSU's most recent enhancements was the addition of 0904 Mounted File System records. This past July, RSH discovered the last 0904 record was being dropped and assisted IBM with troubleshooting the problem and testing the fix. A new version is available on IBM's website.

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

RSH News

Are your z/OS systems reasonably secure? If you are the least bit uncertain, call RSH for an assessment. If you know they are not, call RSH for remediation assistance. ***Call today!***

Upcoming ***RSH RACF Training***:

- RACF - Audit & Compliance Roadmap
  April 22-25, 2014 - Boston, MA
- RACF - Intro and Basic Administration
  February 3-7, 2014 - WebEx
  June 9-13, 2014 - WebEx
- RACF - Securing z/OS Unix
  March 4-7, 2014 - WebEx

In his evaluation of our Unix class, Dean Caldwell of FIS wrote "The whole presentation was motivational. I place a lot of value on the training."