RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 3
Issue 1

January
2009

Specifying a Replacement ID with IRRRID00

To generate commands to delete an ID and all references to it, use RACF's IRRRID00 utility. You simply enter the ID in the SYSIN DD statement of the IRRRID00 job like so:

```
//SYSIN DD *
USERX
```

If USERX is the owner of a profile or connect, IRRRID00 generates commands like:

```
CONNECT RDSADM GROUP(RACFSTC) OWNER(?USERX)
```

In these cases, you need to change ?USERX to a valid replacement ID. This can be done manually or with ISPF EDIT CHANGE.

Alternatively, you can tell IRRRID00 which replacement ID to use when it builds the commands. If, for instance, you want to replace every occurrence of USERX with USERJ, enter the following in the SYSIN DD:

```
//SYSIN DD *
USERX USERJ
```

IRRRID00 will then build commands like:

```
CONNECT RDSADM GROUP(RACFSTC) OWNER(USERJ)
```

Recent APARs of Interest

OA27225: Provides a fix to prevent users with access to FACILITY class resources prefixed IRR.PWRESET or IRR.PASSWORD.RESET from issuing RESUME for a PROTECTED ID.

OA26781: Provides a fix to cause RACROUTE FASTAUTH to process ID(*) with NONE and UACC with READ the same as AUTH.

OA24208: Introduces a new SMF 92 subtype 15 record created when Unix command **chattr** is used to change a file's attributes for Program Control, APF Authorized, and Shared Library.

Temporary Access with CONNECT REVOKE(date)

You may occasionally need to permit a user temporary access to a resource. One way to do so is to grant a group access to the resource and connect the user to that group with a revoke date. The command to set the connect revoke date would look something like this:

```
CONNECT USERA GROUP(TEMPACC) REVOKE(1/20/09)
```

On the date specified with the revoke, RACF will no longer allow the user to have the access permitted to the group. If you want to remove the revoke date but leave the connect intact, enter:

```
CONNECT USERA GROUP(TEMPACC) NOREVOKE
```

A banking client of ours used this capability to govern access to APF-authorized libraries. Access was only permitted on a temporary basis when maintenance was required.

Auditors: How to Examine z/OS Unix Directory and File Security

Auditors who are accustomed to reviewing unix systems will feel right at home on the mainframe when examining z/OS Unix. You will find the familiar **ls** command works much as it does on other unix systems.

To examine z/OS Unix directory and file permissions, you will first need to log onto TSO. Depending on your site's configuration, you will either be at the READY prompt or at the ISPF main menu. If in ISPF, enter option 6 for 'Command', which will take you to a screen that is essentially the same as being at READY.

From here, you enter z/OS Unix by executing either the ISHELL or OMVS command. ISHELL offers an ISPF-like interface with drop-down menus and text box displays. OMVS puts you into a command shell much like opening a command box in X-windows where you can enter unix line commands. This article only examines the use of OMVS and **ls**.

To enter z/OS Unix, your USERID will need to be assigned a unix uid. If you find you are not authorized to use OMVS, contact your RACF administrator to request an OMVS segment with a uid be added to your USERID. A RACF group gid may also be needed, and the administrator can provide this as well.

Once in the OMVS shell, you can navigate just as you would in a typical unix environment. For instance, use command **cd** to change directory.

To examine the standard unix permission bits on a directory or file, enter the **ls** command.

```
ls -options [path/file-name]
```

The options we find to be most useful are:

a	List all entries
l	Display permissions, owner, group
E	Display extended attributes
W	Display audit bits

ls -alEW /etc/ yields output like (line wrapped):

```
-rw-r--r--+ fff--- --s-  1 WEBADM   IMWEB
       4189 May  2  2000   socks.conf.exp
```

Notice the plus '+' sign following the owner, group, and other permission bits. This indicates the file has an Extended Access Control List (ACL). You will need to use the **getfacl** command to display it.

Note that the owner (WEBADM) and group (IMWEB) are RACF identities assigned the underlying uid and gid associated with the file or directory. If multiple users or groups share uids or gids respectively, the first RACF identifier found is displayed. This can be confusing especially when the owner is root - uid 0 - as many IDs may be assigned this uid.

Once you have completed your examination of unix permissions, enter **exit** to leave OMVS.

Historical Note: z/OS Unix was originally called OpenEdition/MVS (a.k.a. OMVS), a play on the term 'Open Systems' that was an emerging buzzword at the time when it was first introduced circa 1992. Although its name has changed over the years, the OMVS acronym persists.

To learn more about Unix file protection, visit the **RACF Center** *on our website for a copy of our presentation zOS Unix - File System Security.*

Limit on DB2 Secondary AUTHIDs Raised

The number of RACF groups DB2 will use as Secondary AUTHIDs for granting access to DB2 objects has been increased. With DB2 v8, the first 1024 connect groups for a user will now be used. Prior to v8, the limit was 300.

RSH News

RSH welcomes ***Ray Withrow*** as the newest member of our professional services staff. Ray has been a RACF/Security Technician, ITIL Change Manager, IT Auditor, and MVS Systems Programmer. He implemented RACF and Tivoli Identity Manager (TIM) at Ohio Casualty. Ray is based in the Cincinnati, Ohio area.

Upcoming ***RSH RACF Training*:**

- RACF - Intro and Basic Administration
  April 28-30, 2009 - Boston, MA
- RACF - Audit for Results
  May 19-21, 2009 - Boston, MA

See our website for details and registration form.