RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 4
Issue 1

January
2010

Custom Field List Titles

When you define a custom field in the CFIELD class, you can optionally specify a 40-character title to be displayed when this field is listed for a user or group profile. If you specify …

```
RDEF CFIELD USER.CSDATA.EMPNO +
   LISTHEAD('EMPLOYEE NUMBER') …
```

… and then enter the commands …

```
ALU USERA CSDATA(EMPNO(1234))
LU  USERA CSDATA
```

… the following will be displayed.

```
CSDATA INFORMATION
------------------
EMPLOYEE NUMBER 0000001234
```

Note that the LU display does not associate the 'EMPLOYEE NUMBER' title with custom field EMPNO. This can be confusing when you want to change the value. We have found it helpful to include the field name in the title as below.

```
LISTHEAD('EMPNO - EMPLOYEE NUMBER')
```

Safely Implement PROTECTED

Ideally, all your dedicated batch and Started Task IDs should be made PROTECTED. This prohibits their use as logon IDs and, more importantly, prevents them from being revoked due to bad password attempts. As an additional safeguard, their passwords cannot be reset with FACILITY IRR.PASSWORD.RESET or IRR.PWRESET.*qualifier* authority.

Use caution when making an ID PROTECTED because its current password hash will be erased, and there is no RACF command to restore it. After making an ID PROTECTED you may discover that a critical process has been logging on with the ID and its former password (e.g., a program on another platform with an embedded logon script). In order for this process to execute, you may have to reset the password to its prior value. If Murphy's Law is in effect, you will find no one knows the password and the program cannot be changed because its source code has been lost.

Before making an ID PROTECTED, take the following safety measures. Install the current version of IBM's PWDCOPY (Password Copy), available from the Downloads webpage link on the RACF Home webpage. Use PWDCOPY to capture a copy of the ID's current password hash prior to making it PROTECTED. If you later discover the ID was being used for logon, use PWDCOPY to restore the former password.

Auditors: Verify LOGOPTIONS are set to log z/OS Unix events

Several RACF and z/OS Unix options govern which access events in Unix are logged. This article addresses LOGOPTIONS in SETROPTS. They set the minimum audit level for each class.

Audit bits on each file and directory specify whether authorized access and/or violations are logged for read, write, and execute or search actions. By default, the bits are set to log all violations. If the audit bits are not set properly, some violations will not be recorded. To ensure violations are always logged regardless of the bit settings, require LOGOPTIONS FAILURES be activated for these general resource classes.

DIRSRCH	Directory searches
DIRACC	Directory read/write access
FSOBJ	HFS object (e.g., file) access

Preferably, all changes to file and directory security permissions and audit bits should be logged. Therefore, require LOGOPTIONS ALWAYS be activated for the following class.

FSSEC	File system security changes

Logging for certain events is governed solely by LOGOPTIONS, and violations will only be logged when it is set to FAILURES or ALWAYS. Require that LOGOPTIONS be set to at least FAILURES for the following classes.

PROCESS	Process uid or gid changes and privileged operations
PROCACT	Functions affecting other processes
IPCOBJ	Object access, uid or gid changes

If you were given System-AUDITOR authority to perform your audit, you can change SETROPTS LOGOPTIONS on your own. We advise you never to do so without first consulting RACF Administration and z/OS Technical Support. Changing LOGOPTIONS could cause a sudden surge in audit records or console messages that might disrupt system operations. We have seen activation of LOGOPTIONS FAILURES for the PROCACT class result in the system console being flooded with ICH408I violation messages when a Unix process repeatedly issued GETPSENT requests for which it was not authorized. (We were subsequently able to grant the authority with a permit of READ to the SUPERUSER.PROCESS.GETPSENT resource in the UNIXPRIV class.) As a precaution, activate LOGOPTION changes only during a non-prime shift period, preferably during a system maintenance period, and be certain to notify change management beforehand.

ISPF 3.17 Udlist - List Unix Files & Directories

Our article "Auditors: How to Examine z/OS Unix Directory and File Security" in the January 2009 edition of RSH RACF Tips provided instructions for listing Unix files and directories using the 'ls' command. ISPF menu option 3.17 - Udlist - offers an easy way to get the same information and also provides a means of navigating within the directory tree.

When you first enter panel 3.17, you will be prompted for a starting pathname (directory). Once you provide the pathname and hit Enter, you will be shown a list of all the files and subdirectories within the specified directory along with their security, audit, and extended attribute bits. (If you do not provide a pathname, the root directory will be displayed.) Note that the names are truncated to 15 characters.

Commands to process individual files and directories can be entered in the Command column. Here are a few you will find useful.

B	Browse a file
I	Display file attributes
L	Change to and list a directory

Hint: The dot-dot .. directory on any display represents the parent directory. Unless you are in the root directory, entering command L on this directory takes you up a level in the hierarchy.

RSH News

The RSH team is almost fully booked for 2010. If you have any projects in mind for us this year, please call us now before our schedule is full.

RSH now provides instructor-led training via WebEx. You can obtain in-house training for your staff without incurring travel costs!

Upcoming ***RSH RACF Training***:

- RACF - Audit for Results
  May 4-6, 2010 - Boston, MA
- RACF - Intro and Basic Administration
  May 25-27, 2010 - Boston, MA
- RACF and z/OS Unix **!!! *NEW* !!!**
  July 13-15, 2010 - WebEx

See our website for details and registration form.

Be sure to visit our exhibit and attend our RACF presentations this coming April at the 2010 Vanguard conference.