RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 6
Issue 1

January
2012

RSH RACF Surveys

RSH now conducts brief monthly surveys on RACF topics via the Internet. New surveys are announced on RACF-L. The results are posted on our website. Responses are anonymous. The more responses collected, the more meaningful the results. Please take a moment to participate.

CICS TS 4.2 & RACF

CICS Transaction Server 4.2 has new signon transaction CESL that will accept the entry of password phrases as well as passwords.

This release also introduces the following new system programmer commands whose access is checked in the RACF class specified by the SIT parameter XCMD. Permit READ for INQURE and UPDATE for SET.

CAPDATAPRED	INQUIRE
CAPINFOSRCE	INQUIRE
CAPOPTPRED	INQUIRE
CAPTURESPEC	INQUIRE
EPADAPTER	INQUIRE | SET
OSGIBUNDLE	INQUIRE
OSGISERVICE	INQUIRE
TEMPSTORAGE	INQUIRE | SET

For details and other changes, see IBM's CICS TS for z/OS 4.2: RACF Security Guide and Systems Programming Reference.

RACF-L Internet Discussion List

Have a question about RACF or need a quick solution to a problem? Want ideas and advice from world-renowned experts? All you need do is send your questions via email to RACF-L.

RACF-L is a discussion list dedicated to RACF. Membership is free and open to anyone. There are thousands of members. Anyone can post a message or respond to anyone else's postings.

Instructions for joining and using RACF-L can be found on the RACF Center page on our website.

Auditors: Review PROGRAM Protection

The use of programs can be controlled by profiles in the PROGRAM class. When a user attempts to execute a program, z/OS searches for a profile matching the program name and verifies the user is permitted to execute it.

Confirm programs are being protected. Look for WHEN(PROGRAM -- *mode*) in the first line of SETROPTS LIST output. Programs are not protected if NOWHEN(PROGRAM) is displayed.

List all PROGRAM profiles by executing the command SEARCH CLASS(PROGRAM).

Expect to see an all-inclusive profile of either * or ** with UACC of READ. This profile is needed to establish a program-controlled environment for z/OS Unix tasks. It is required when profile BPX.DAEMON is defined in the FACILITY class.

Discrete or generic profiles should be defined to protect the following programs. Use the RLIST command to list and inspect each profile to verify access is strictly limited.

ICHDSM00	RACF DSMON
IRRDPI00	RACF Dynamic Parse Table Load
IEHINITT	Initialize (Erase) Tapes
DGTxxxxx	ISMF Storage Administration

Profiles for other programs may be listed if the installation deems it necessary to protect them. Most programs do not need protection.

A program may have alternate names, a.k.a. aliases. Confirm that profiles are defined to protect the aliases of all protected programs.

It is no longer essential to protect 'SuperZap' program AMASPZAP and its alias IMASPZAP. The reasons are given in the White Paper RACF Audit Guidance available on our website.

Users are permitted READ access to use a program. EXECUTE permission may be used in rare instances for highly proprietary programs.

Ensure the program library datasets listed in each profile are up to date. See our April 2010 issue for further guidance on this.

Beware Making the Unix Default User a File or Directory Owner

When chown is used to change the owner of a file or directory, if the new owner does not have an OMVS segment, the owner will be set to the uid of the Unix Default User specified in the FACILITY BPX.DEFAULT.USER profile. (Note: BPX.DEFAULT.USER is being phased out.)

ISPF 3.17 MA Line Command

Our January 2010 issue described how to examine Unix files and directories via ISPF panel 3.17. z/OS 1.13 added line command MA (Modify Access) to administer permissions.

Protect TCP/IP Low Ports

Our April 2011 issue described how to use TCP/IP PORT and PORTRANGE configuration parameters in combination with SERVAUTH profiles to reserve and control access to ports.

To prevent unauthorized jobs from binding or listening to unreserved TCP/IP ports numbered 1 to 1023 (a.k.a. "low" or "non-ephemeral" ports), add the following statements to the TCP/IP task's PROFILE DD statement configuration parameters.

```
TCPCONFIG RESTRICTLOWPORTS
UDPCONFIG RESTRICTLOWPORTS
```

When these are specified, a job can only open a low port if it is either (a) APF-authorized, (b) has Superuser UID(0) authority, or (c) is permitted access via a PORT or PORTRANGE statement.

TSO User Data Sharing

TSO users occasionally need to share non-sensitive data with other users. To facilitate sharing without altering profiles, create the following entry in the Global Access Table and tell users they can share data by making the second qualifier of the dataset name PUBLIC. Users need to understand that such datasets can be read by all non-RESTRICTED users.

```
RALTER GLOBAL DATASET +
  ADDMEM('*.PUBLIC.**'/READ)
```

Thank you Alex Monaco of Liberty Mutual for this tip.

RSH News

We hope our newsletters, presentations, and surveys are beneficial to the RACF community at large. If you found them helpful, let us know.

Upcoming ***RSH RACF Training*:**

- RACF - Audit for Results
  April 24-26, 2012 - Boston, MA
- RACF - Intro and Basic Administration
  February 6-10, 2012 - WebEx
  May 8-10, 2012 - Boston, MA
- RACF and z/OS Unix
  January 24-26, 2012 - WebEx

See our website for details and registration form.