RSH RACF TIPS

For Administrators, Auditors, and Analysts

Volume 6
Issue 3

July
2012

To All Our Clients - Thank You!

RSH Consulting was established July 1, 1992. In celebrating our ***20th anniversary***, we offer you, our clients, past and present, a most sincere thank you for using our professional services and training to enhance your security. We look forward to serving you again in the future.

REQUEST=VERIFY & GLOBAL

During logon validation processing initiated by a RACROUTE REQUEST=VERIFY, RACF may check access permissions to resources in the APPL, TERMINAL, JESINPUT, CONSOLE, APPCPORT, or SERVAUTH classes. Note that VERIFY does not use the Global Access Table.

FACILITY BPX.SAFFASTPATH

Ordinarily, whenever a user attempts to access a Unix object such as a directory, z/OS Unix calls RACF for an access authorization decision. You can eliminate some of these calls and improve performance by defining discrete profile BPX.SAFFASTPATH in the FACILITY class. Once you define and activate this profile, z/OS Unix will grant access to an object if it can determine, on its own, that the user is permitted access (e.g., the user's UID is the OWNER of a file and OWNER permission bits allow access).

There are a few situations where it may not be desirable to bypass RACF. Do not activate this feature if you (a) use SAF's Callable Services exit IRRSXT00 to control access, (b) assign SECLABELs to Unix objects, or (c) need to log authorized access using file object auditing bits.

The last item is important if you are replacing BPX.DEFAULT.USER. If you need to log user activity to uncover Default User use, you might miss crucial events if BPX.SAFFASTPATH is defined. Consider delaying implementation or temporarily removing BPX.SAFFASTPATH until you have eliminated BPX.DEFAULT.USER.

Defining or deleting BPX.SAFFASTPATH alone is not sufficient to activate or deactivate this feature. It also requires execution of a SET OMVS operator command. See IBM's *z/OS UNIX System Services Planning* for details.

SMF Type 30 Records

When RACF's SMF Unload creates JOBINIT records for TSO, batch, and Started Task logon and logoff events, it uses information from SMF type 30 records (Common Address Space Work) to complete the unload records. However, it only uses subtypes 1 (Initiation) and 5 (Termination). If you maintain a separate archive or extract of RACF-only SMF records, you can reduce the amount of data you need to store and process by only selecting these two subtypes in your IFASMFDP SMF dump job. In SYSIN, code:

OUTDD(*ddname*,TYPE(30(1,5),80,81,83)

RACFRW uses type 20 records for job initiation information. You can zap the INITREC field of RACFRW's options module ICHRSMFI to cause it to use 30 records instead. See IBM's *RACF Systems Programmer's Guide* for details.

Auditors: Confirm PROTECTALL is Active

When a user attempts to access a dataset, z/OS asks RACF to verify the user has the necessary authority before allowing access. If there is no DATASET class profile that matches the name of the dataset, RACF by default issues a Return Code (RC) 4. An RC 4 tells z/OS the dataset is unprotected, and the system will allow unrestricted access to it.

RACF terminology tidbit - unprotected datasets are often described as being "undefined" or as "not defined to RACF".

SETROPTS option PROTECTALL can be activated to protect undefined datasets. The option can be set to WARNING or FAILURES. If a user attempts to access an unprotected dataset when PROTECTALL is set to WARNING, RACF still issues an RC 4, but it also generates an SMF log record to report the access. If the option is set to FAILURES, RACF instead issues an RC 8, which tells z/OS not to allow access. FAILURES is the preferred setting. WARNING is typically used on a temporary basis during initial implementation to identifying and address unprotected datasets. Output from SETROPTS LIST shows its status.

Note that PROTECTALL only requires that a dataset have a matching profile. It does not ensure the data is properly safeguarded. A matching profile with a UACC of ALTER satisfies the requirements of PROTECTALL even though it gives everyone full access.

More on Replacing BPX.DEFAULT.USER

Article "*Replacing BPX.DEFAULT.USER*" in the April 2012 edition of this newsletter offered tips on addressing the replacement of this profile. Based on our continuing work helping clients with this effort, here are a few more tasks you may need to complete.

- Before commencing widespread assignment of UIDs and GIDs, ensure the RACF database has sufficient free space for all the new OMVS segments. Each segment will require at least one 256-byte allocation to store the data.
- If the Default User is the OWNER of any files or directories, audit access to them to determine who is using them. It might be one user, or it could be many. Reset the OWNER when you assign UIDs to these users.
- We have been finding it necessary to replace Default User OWNER permissions with Access Control List (ACL) permissions in instances where multiple users are accessing the same object using the shared authority of the Default User. We recommend you activate class FSSEC now to enable the use of ACLs.

For additional tips, visit our website to obtain a copy of our recently-posted presentation on replacing BPX.DEFAULT.USER

Listing CA-1 Security Options

Articles in recent issues of RSH RACF Tips mention CA-1 configuration options governing tape security. These options are initially set in the TMOOPT*xx* member of *hlq*.CTAPOPTN. To list the options currently in effect on a specific system, execute the following job.

```
//jobname  JOB job-card-parameters
//STEP0001 EXEC PGM=TMSSTATS,PARM=OPT
//STEPLIB  DD DSN=ca1.software.lib,DISP=SHR
//TMSRPT   DD SYSOUT=*
```

RSH News

Our experience, proven methodologies, and powerful software tools enable RSH to maximize efficiency and effectiveness in delivering RACF services. Our goal is to offer you the best value.

Upcoming ***RSH RACF Training*:**

- RACF and z/OS Unix
  July 31-August 2, 2012 - WebEx
  January 15-17, 2013 - WebEx
- RACF - Audit for Results
  October 30-November 1, 2012 - Boston, MA
- RACF - Intro and Basic Administration
  October 15-19, 2012 - WebEx
  February 4-8, 2013 - WebEx

See our website for details and registration form.

RSH CONSULTING, INC.
RACF Specialists
www.rshconsulting.com ■ 617-969-9050
29 Caroline Park, Newton, Massachusetts 02468