RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 9
Issue 1
January
2015

RACF Password Enhancements

APARs OA43998 and OA43999 significantly enhance RACF password security. You may now:

- Encrypt passwords using algorithm Key Derivation Function with AES (KDFAES)
- Allow use of special characters .<+|&!*-%_>?:=
- Require a special character in new passwords
- Assign a password phase without a password
- Expire a user's password without a reset
- Remove old passwords when reducing password history (this replaces CUTPWHIS)

These enhancements modify SETROPTS options, user profile commands, utilities, macros, callable services, exit parameters, IRRDBU00 records, and SMF records. For details, see document "APAR OA43999 - RACF password security enhancements", which is available at this URL:

ftp://public.dhe.ibm.com/eserver/zseries/zos/racf/pdf/oa43999.pdf

BPX.SAFFASTPATH Addendum

Our July 2012 newsletter describes FACILITY profile BPX.SAFFASTPATH. We have since learned this only applies to file systems allocated with the older HFS format. Most file systems are now allocated in the newer zFS format, limiting any benefits it might otherwise have provided.

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

WebSphere MQ RACLIST

MQ uses RACROUTE REQUEST=LIST, GLOBAL=YES to RACLIST MQ-related classes with companion grouping classes, namely MQADMIN, MQCHAN, MQNLIST, MQPROC, MQQUEUE, and their MX-prefixed equivalents. MQ does not GLOBAL RACLIST standalone classes MQCMDS and MQCONN. These classes are defined RACLIST(ALLOWED), and we recommend you SETROPTS RACLIST them.

Unknown Operator Commands

When a subsystem receives a console command it does not recognize, the subsystem performs an authorization check for OPERCMDS resource *subsystem-name*.UNKNOWN. The RACF Security Administrator's Guide recommends creating the profiles below with the UACCs shown. We recommend adding AUDIT(ALL). The ACC_LOGSTR field of the ACCESS SMF unload record usually contains the unknown command.

MVS.UNKNOWN	READ
JES*n*.UNKNOWN	NONE
racf.UNKNOWN	NONE

CA Common Services & MAXTHREADS

If either CA Common Services (formerly CA-90s) Started Task CCITCP or CCITCPGW finds it has a maximum threads limit of less than 2000, it will invoke callable service BPX1STL to request an increase to 2000. If the requested value of 2000 exceeds the MAXTHREADS value set in z/OS PARMLIB member BPXPRMxx, the task will experience a PROCESS class violation with the ICH408I description INSUFFICIENT AUTHORITY TO THLMT. To resolve the issue, CA suggests setting MAXTHREADS to 2000, which increases the limit for all tasks. As an alternative, we suggest specifying THREADSMAX(2000) in the OMVS segments of the Started Tasks' IDs.

Finding Undefined User Logons

To find TSO, Batch, or Started Task logons by undefined users using SMF unload JOBINIT

records, ignore the INIT_USER_NDFIND and INIT_UTK_UNKNUSR fields and instead look for an asterisk (*) in the INIT_EVT_USER_ID field.

WARNING Contest Winner

Al Buschmann of FIS was the winner of our contest to identify resource classes where RACF ignores the profile WARNING option. The two classes are PROGRAM and NODES.

AUDIT NONE Becomes READ

When a resource is defined in multiple grouping class profiles, the RACLIST process combines the AUDIT settings from the different profiles. If any of the settings for SUCCESS is NONE, RACF erroneously processes this as READ, resulting in a merged setting of SUCCESS(READ) for the resource. This may generate a large volume of unwanted SMF records. To circumvent this, add SUCCESS(ALTER) to the AUDIT setting on all profiles with shared members. Do the same for the GLOBALAUDIT setting. See APAR OA46331.

Auditors: Find Responsible Party

Management often accepts a RACF related audit finding and mistakenly expects the RACF security staff alone to take corrective action. The RACF staff, however, is rarely empowered to implement changes unilaterally. Most controls are set as directed by IT management or resource owners, and their approval is required to make changes.

A common finding, for example, is excessive assignment of the powerful OPERATIONS authority. The staffs who hold this authority may insist it is required despite the availability of viable alternatives and prevent its removal by the RACF staff who is tasked with remediation. This puts the RACF staff in a very difficult position.

If you want to ensure a control deficiency is fully addressed, determine who is responsible for the deficiency and hold that party accountable for its remediation in your finding. Here is a sample: "Storage Management should fully implement storage administration authorities using FACILITY class STGADMIN profiles and remove OPERATIONS authority from their IDs."

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

REVOKED & BPX.UNIQUE.USER

If an attempt is made to logon to a TCP/IP application using a REVOKED ID that does not have an OMVS segment, FACILITY class profile BPX.UNIQUE.USER will nonetheless cause RACF to auto-assign the ID an OMVS segment with a UID. Likewise, if the ID's default group does not have an OMVS segment, one will be auto-assigned with a GID. If you want to prevent this from occurring, give the ID and/or the default group an empty OMVS segment.

RSH News

Do you have important RACF tasks you cannot find time to complete but do not require a full time consultant? ***Call RSH.*** We can provide you with professional services on an ad hoc basis, perhaps just a few hours a week, to help you finally finish these tasks. We are also available to offer advice, provide training, and help troubleshoot problems.

Upcoming ***RSH RACF Training*:**

- RACF - Securing z/OS Unix
  February 3-6, 2015 - WebEx
- RACF - Intro and Basic Administration
  March 23-27, 2015 - WebEx
- RACF - Audit & Compliance Roadmap
  April 21-24, 2015 - Boston, MA

All of us at RSH wish you a prosperous 2015.