RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 11
Issue 2

April
2017

CICS & KDFAES

With APAR AO43999, November 2014, RACF enabled the encryption of passwords using the algorithm KDFAES (Key Derivation Function with Advanced Encryption Standard). Most system software products let RACF handle password encryption and validation and need not be aware of which encryption method is being used.

A few products, however, perform their own password encryption and validation and need modifications to process KDFAES-encrypted passwords. One such product is CICS.

IBM enhanced CICS to enable it to validate passwords using KDFAES, but only for CICS Transaction Server releases 4.2 and later. If you have CICS regions with earlier releases, you will not be able to implement KDFAES until you have upgraded these regions to a newer CICS release.

For more information on other limitations to implementing KDFAES, see APAR II14765.

SMF Unload Errors Due To Record Format Changes

New z/OS releases and subsequent APARs occasionally change the format of RACF SMF records and make corresponding modifications to the SMF unload programs to handle these changes. An example is the Multi-Factor Authentication (MFA) APAR OA48359 which added a new relocate section to the type 80 JOBINIT record. This new relocate section, positioned at what is now the end of the record, only appears in SMF records generated on a system where the APAR has been applied.

If you process SMF records created on a system where such an APAR has been applied using the SMF unload programs from a system without it, the 'downlevel' SMF unload programs will not recognize the new format. When SMF unload encounters such records, it posts error messages IRR67581, IRR67582, and IRR67583 to DD ADUPRINT. These messages provide details about the error and identify the SYSID where the records were created. An SMF unload record will still be created, but it will not have complete information. This is a non-fatal error, and SMF unload completes with a Return Code of 0. You will not be aware of a problem unless you review ADUPRINT output.

As you should also do with the IRRDBU00 unload, always execute the SMF unload utility on one of your systems having the latest release of z/OS and latest maintenance.

ICB & RCVT

RACF stores options managed by SETROPTS in the first block in the RACF database, known as the Inventory Control Block (ICB). It got this name because the original designers envisioned RACF maintaining an inventory of all system resources including controls for their access. During system operation, these options are kept in memory in the RACF Communications Vector Table (RCVT).

POSIT

Each general resource class is assigned a numeric POSIT value ranging from 0 to 1023. POSIT values 0-18, 57-127, and 528-1023 are reserved for IBM's use. Values 19-56 and 128-527 are available for installation use.

Classes sharing a POSIT value are administered as a set. Both classes in a Member and Grouping pair typically share a POSIT. IBM's CICS classes all have a POSIT of 5. SETROPTS command operands like GENERIC that are directed at a specific class affect all classes with the same POSIT. Therefore, before taking any action against a particular class, especially deactivation, first determine what other classes will be affected.

For each class option (e.g. AUDIT), there is a corresponding 1024 bit mask in the ICB and RCVT. When you activate a class with a POSIT of 20, RACF turns on bit 20 in the CLASSACT bit mask. Hence, when you activate a class, you are actually activating the POSIT, resulting in activation of all classes that share the POSIT.

Changing a class' POSIT value does not alter the ICB-RCVT bit mask settings. If CLASSACT bit 20 is on but 21 is not, changing a class' POSIT from 20 to 21 will cause the class to become inactive.

Visit our website to obtain a list of all the IBM classes and their associated POSIT values.

CLAUTH

Class Authorization (CLAUTH) is a RACF administrative authority assigned to individual users. CLAUTH allows a user who does not have SPECIAL authority to create profiles in a specific class. It can be used to delegate administration for specific sets of resources to the individuals who are responsible for their management.

When CLAUTH is assigned for class USER, it allows creation of USER profiles, but only if the CLAUTH user also has either Group-SPECIAL, JOIN authority, or ownership of a group.

When a user is assigned CLAUTH for a general resource class, this authority extends to all other classes having the same POSIT. However, LISTUSER commands and IRRDBU00 unload 0202 records only list those classes explicitly named in the ADDUSER or ALTUSER command used to assign CLAUTH. Other classes that share their POSITs are not shown. To ensure these other classes are also listed, specify all the classes having the same POSIT in the command assigning CLAUTH authority.

For more on CLAUTH, attend our "RACF Level II Administration" course. Also visit our website to see the results of our October 2016 survey on CLAUTH.

&RACGPID & DFLTGRP

&RACGPID is a variable used in Global Access Table entries. During access authorization checking, RACF substitutes the user's current connect group, which is the group the user logged on with (usually their default group), for this variable to determine whether the entry matches the resource name. If you have any entries with &RACGPID, evaluate them carefully whenever you are contemplating changing a user's default group to determine how such a change would affect the user's access authority.

z/OS 2.3 Preview - UID(0) Display

Dozens of Unix daemons must, by necessity, be assigned a RACF ID with UID(0). However, when the Unix 'ls -l' command is used to list a file or directory owned by UID(0), just one of these IDs will be displayed as the OWNER. Which one depends on what IDs are cached in VLF at the time. To address the confusion this often causes, RSH Consulting submitted an RFE in 2009 recommending a consistent value always be displayed to represent a UID(0) OWNER.

Our RFE may finally be implemented. In z/OS 2.3, when RACF is invoked to map UID(0) to a USERID, it will return the value defined in the SUPERUSER(*userid*) keyword of PARMLIB member BPXPRMxx. The default is BPXROOT. This affects output from IRRHFSU as well as 'ls'.

To learn how to lock down your z/OS Unix, attend our "RACF - Securing z/OS Unix" course.

RSH News

We hope you find this 10th anniversary issue as informative as the prior ones. Please let us know if they have been helpful. With your permission, we will post your comments on our website.

RSH is at the forefront of training the next generation of RACF Administrators and Auditors. Our RACF course series offers you the ideal pathway for improving your skills. Training is conducted via WebEx to save you time and money. Our format of 4 hours of training per day lets you keep up with day-to-day work and avoid information overload. Admission is limited. To get the early registration discount, sign up today!