RSH CONSULTING

RSH RACF TIPS

For Administrators, Auditors, and Technicians

Volume 11
Issue 3

July
2017

RSH Consulting 25th Anniversary

RSH Consulting was established July 1, 1992. To those of you who have been our clients over these past 25 years, we sincerely thank you for using our professional services and training to help you enhance your RACF and z/OS security.

PROGRAM Protection & LPA

PROGRAM class profiles cannot control access to programs residing in the z/OS Link Pack Area (LPA). If you previously restricted use of the FTP program using a PROGRAM profile and then Tech Support moved the program into LPA as recommended by the IP Configuration Guide, the FTP program will no longer be controlled. (To control FTP, use an APPL class profile instead.)

For more on protecting programs, attend our "RACF Level III Administration" course.

JESJOBS GROUPREG Resources

JES2 for z/OS 2.2 introduced new JCL statements to support a concept called "Job Group". The new JOBGROUP and GJOB statements provide execution directions for a set of related jobs.

A JOBGROUP statement is like a JOB statement. It specifies a *jobgroupname* and OWNER, similar to the *jobname* and USER on a JOB statement. To submit a JOBGROUP, the submitter requires READ access to the JESJOBS resource:

SUBMIT.*localnode.jobgroupname.ownerid*

The submitter is assigned as the OWNER unless a different owner is specified via the optional JOBGROUP OWNER=*userid* parameter. To submit a JOBGROUP with a different ID as the OWNER, the submitter requires READ access to the SURROGAT resource *ownerid.*SUBMIT.

When a job is submitted that is intended to be governed by a Job Group, it must "register" with the Job Group using the new SCHEDULE JCL statement. If the job's USER is different from the Job Group's OWNER, the job's USER requires READ access to the JESJOBS resource:

GROUPREG.*localnode.jobgroupname.ownerid*

For more on protecting JES and SDSF, attend our "RACF Level III Administration" course.

z/OS 2.2 IRRDBU00 Database Unload

Fields related to password and phrase encryption algorithms and the new ROAUDIT attribute were added to the end of the 0200 User record.

The following are new records. All are related to Multi-Factor Authentication (MFA). The asterisk (*) flags records added by recent enhancements to MFA made subsequent to the initial release of 2.2.

020A	User MFA Factor Data
020B	User MFA Policies *
1210	User MFA Factor Tags Data
05H0	General Resource MFA Definition
05I0	General Resource MFPOLICY Definition *
05I1	General Resource MFA Policy Factors *

"List of Groups" Checking & UNIX

When a user dubs into Unix, a User Security Packet (USP) is built for the user, and the GID associated with the user's current connect group is set as both the "Real" and "Effective" GID in the USP. The Effective GID is used for file and directory access authorization checking. (Note: during execution of a Unix program that has the set-gid bit, a user's Effective GID will be temporarily changed to the GID of the program.)

If option "List of Groups" is active, RACF will use the GIDs assigned to the user's other groups in addition to the user's Effective GID for access authorization. These other GIDs are known as "Supplemental" GIDs, and a list of these GIDs is found in the USP. This list is limited to 300 entries.

The initUSP Callable Service builds the USP's Supplemental GID list from the list of groups in the user's ACEE field ACEEFCGP, which is in alphanumeric sequence. (The RACF Callable Services manual incorrectly states the list is built from the list of groups in the user's profile, which is in CONNECT sequence.) If a user is connected to 300 or more groups with GIDs, further group connects or removes will most likely change the alphanumeric sequence of the group list and may result in a different USP Supplemental GID list being created the next time the user logs on.

Thank you Bruce Wells of IBM for your input to this article. For more on protecting Unix, attend our "RACF - Securing z/OS Unix" course.

z/OS 2.2 ADDUSER NOPASSWORD

In z/OS 2.2, if you do not assign a password or a phrase when creating an ID using an ADDUSER command, the ID will be made PROTECTED.

Users who reset passwords using only the authority of the following FACILITY resources cannot assign passwords to PROTECTED IDs.

IRR.PASSWORD.RESET
IRR.PWRESET.OWNER.*owner*
IRR.PWRESET.TREE.*group*

To enable users with these authorities to reset passwords for newly created IDs, your existing ID creation processes may need to be modified to assign an initial password to new IDs.

RACF SMF Factoid - TRUSTED

Certain audit settings result in SMF 80 ACCESS event records being generated for access by a TRUSTED Started Task. When access is granted by TRUSTED authority, a bit in the header section of the SMF record is set ON, and the field ACC_AUTH_TRUSTED in the corresponding SMF Unload record contains YES. This bit is not set ON for DEFINE, ADDVOL, DELVOL, RENAMEDS, or DELRES events. However, the SMF 80 record for all these events has a UTOKEN relocate section, and this section has a bit which is set ON if the user had TRUSTED authority. If the bit is ON, the field *event*_UTK_TRUSTED in the corresponding SMF Unload record contains YES. This field is cryptically documented in the RACF Macros and Interfaces manual as "Is this user a part of the trusted computing base (TCB)?" It can be used to determine if any of these events were allowed because of TRUSTED authority.

Auditors: Check for Stronger Password Encryption

RACF user passwords can now be encrypted using the Key Derivation Function with Advanced Encryption Algorithm (KDFAES). This feature was added by APAR OA43999 and is included in z/OS 2.2. KDFAES encrypted passwords are vastly more difficult to crack than ones encrypted using the existing DES algorithm and provide far better protection in the event an assailant obtains a copy of your RACF database. (See Logica hack.)

The following line under "Password Processing Options" in a SETROPTS LIST report shows the algorithm in use. If the line is not displayed, the APAR has not been applied. If "LEGACY" is shown instead of "KDFAES", DES is being used.

```
THE ACTIVE PASSWORD ENCRYPTION ALGORITHM
 IS KDFAES
```

For more on auditing RACF, attend our "RACF Audit and Compliance Roadmap" course.

RSH News

Robert S. Hansel will be speaking at SHARE in Providence this coming August. To learn how to set RACF audit options to effectively monitor security events and maximize your SIEM ROI, attend his presentation on Thursday, August 10.

RSH's RACF experts are available on an ad hoc retainer basis to answer questions, provide advice, or resolve issues. You can select the service offering which best fits your needs and budget. You can even pay by credit card. Call us.