RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 92):

This Issue's Themes:

- Take advantage of free training available
- Prep now to make z/OS 2.3 upgrade easier

Free Webinars: Wednesday, October 18 at 12 pm EDT (9 am PDT)
Planning for Your Next Release of z/OS Presenter - Glennon Bagsby - NewEra Software

Thursday, October 19 at 12 pm EDT (9 am PDT)
Migrating to z/OS V2R3
Presenter: Marna Walle - IBM

To register:
www.newera-info.com/Month.html

If you miss these, you can get recordings and copies of handouts at
www.newera-info.com/Presenters.html

NY Metro NASPA (National Association of System Programmers) Meets Wednesday, 25 October, 2017, **Room 1219, IBM Building, 590 Madison Avenue, NYC**. For free registration email Mark Nelson ("markan@us.ibm.com") with the subject "***2017 October NASPA***"

NEW YORK RUG Meeting Date

November 14, 2017 from 10AM to near 4PM *at IBM in Tampa and NYC.*

THIS IS A LOT OF TRAINING AVAILABLE IN ONE DAY. **You will not be allowed to attend without pre-registering (it's free).** See inside for details. (The meeting after that will be **a Spring date to be determined in 2018**)

If you want reminders of upcoming RUG meetings, please click RUG Reminders to receive one email reminder before each meeting (two per year).

Please Note the New Website for the NYRUG and TBRUG: To simplify all the references, we have consolidated all info for the NYRUG and the Tampa Bay RUG at www.nyrug.stuhenderson.com

---

Today's Quotation

" *Passwords are no longer a reliable means of proving someone's identity."*

Vanguard Conference

Vanguard Security & Compliance 2017 takes place Monday, October 16 through Thursday October 19 at the DFW Airport Marriott South Hotel in Dallas/Ft. Worth, Texas. Visit www.go2vsc.com for more details. Earn up to 21 CPEs.

For more information, please contact glory.wade@go2vanguard.com .

To subscribe to this newsletter, or for back issues:

http://www.stuhenderson.com/Newsletters-Archive.html

RACF for z/OS 2.3 Arrives

This includes new features such as:

- Persistent Encryption for disk data, that is, you can specify which disk datasets are to be encrypted (and how) by specifying on the DD card or in SMS or in the RACF dataset profile. This can apply to MVS datasets, USS files in zFS file systems, and in the Coupling Facility of sysplexes.
- The ability to change the RACF dataset names table and the RACF range table dynamically by means of a parmlib member. This means you don't have to re-assemble them or re-IPL
- Eight character TSO ids
- The addition of the email address to the WORKATTR segment
- A new callable service which lets you do RACF administration based on an XML document

More and more, new RACF releases seem to be polishing a finished product as opposed to making corrections or performance improvements in an product still under development.

So How Do I Implement Persistent Encryption of Disk Datasets?

Start by reading the article below about organization changes needed for effective encryption. Then learn about how ICSF is implemented in your shop.

ICSF is a started task that serves as a router for requests to encrypt or decrypt data. It stores the encryption keys in special datasets, which you need to protect with dataset rules. Define its userid in the started task table and make its userid be protected (no password and no password phrase). Since ICSF calls RACF in the CSFKEYS and CSFSERV resource classes, start using those classes. See the articles below on SMS and organization changes.

If you want to use RACF dataset profiles to implement encryption, include the parameter **DATAKEY(CKDS xxx)** where **xxx** is the label of the key as defined in ICSF.

What Should RACF Admins Be Doing to Make The Upgrade to 2.3 Easier?

Test and implement anything new that can be implemented before 2.3, so the upgrade has less new stuff. This includes:

- Upgrade the record layouts in the RACF dataset by working with your sysprog to run the IRRMIN00 utility. But don't use any of the new features that use the new record layouts until all the CPUs and LPARs sharing the RACF database have been upgraded.
- Get your sysprog to make sure you are upgraded to AIM level 3 in the format of your RACF database
- Activate and start using the CSFKEYS and CSFSERV resource classes for encryption (see article below)

What's New with Passwords?

If you haven't addressed these changes, knowing about them in advance will make your life easier.

- KDFAES is a new encryption algorithm for passwords in the RACF database. Expect auditors soon to know to review SETR LIST to see if it's active
- Special characters are now allowed in passwords if you set the option. This may not be essential, but you should know about it.
- Now if you add a new user profile without specifying the password, it defaults to no password. (It used to default to the value of the default group, making it too easy to guess.)
- You can now have a userid with a password phrase but without a password.
- You will want to start preparing for MFA (Multi-Factor Authentication) if you don't have it already. The idea is that users signing on must prove their identity in more than one way. Passwords alone are no longer considered reliable evidence of who you are.

How Do I Know Which Resource Classes Are Essential?

One way is to see which resource classes IBM checks in the RACF_classname_ACTIVE health checks. These are: UNIXPRIV, FACILITY, TAPEVOL, TEMPDSN, TSOAUTH, OPERCMDS, CSFKEYS, CSFSERV, JESJOBS, and JESSPOOL.

The IBM manuals states that "*An effective RACF implementation requires that the baseline group of RACF general resource classes listed above be active*."

What About the Resource Classes CSFKEYS and CSFSERV?

These two resource classes are used for encryption and decryption control. CSFKEYS is used to control who can access specific encryption keys. CSFSERV is used to control who can request various functions of encryption and decryption. Calls to RACF for these classes are made by the ICSF software.

You need to find the system programmer who maintains ICSF and get him to tell you the names of the encryption keys and what userids should be permitted to them. If you have to, consider defining resource rules named ** with AUDIT(ALL) and UACC(ALTER) to collect information on what keys are in use now. Be sure to tighten these up to have a UACC(NONE) before long.

What Does My Organization Need to Do for Encryption?

If you're the RACF admin, then by default you are considered responsible for mainframe security. This is despite the fact that your company never paid for you to go to law school to learn how to research what regulations apply to your organization's datasets.

This is despite the fact that you have no authority over UNIX and Windows administrators, nor over MVS system programmers, who may have implemented encryption for some datasets without documenting the fact anywhere.

But if you allow the default to apply, if there are changes in technology (like the replacement of DES with AES), or in regulations (like the new ones from New York State for financial institutions and the other new ones coming from the European Union), or if digital certificates (in the RACF database or in USS) expire, everyone will assume that the problem belongs in your lap.

To help your CIO sleep at night, you want to encourage her to make sure that someone with suitable authority has the responsibility to manage all encryption. This "Encryption Czar" will need the authority to require that staff document all datasets that are encrypted. He will also need to get input from the Legal and Compliance departments to determine what datasets need to be encrypted. Company policy should make it clear that you do not decide what datasets get encrypted or how. Your job as RACF administrator is to receive this information from the designated Czar and issue RACF commands to implement whatever is decided.

An Easy Way to Protect Voting Machines From Hackers

See the article at http://www.stuhenderson.com/ProtectVote.pdf

RACF HealthChecks You Want to Consider

Here's an easy way to cause confusion to the auditors: point them at the RACF healthchecks you've implemented. These can also help you to know that your RACF options are properly set:

- **RACF_ENCRYPTION_ALGORITHM** raises an exception if KDFAES is not active
- **RACF_RRSF_RESOURCES**, checks how your RRSF data sets are protected
- **RACF_SENSITIVE_RESOURCES** (which now checks the protection of your ICSF datasets as well as other key datasets)
- **RACF_PASSWORD_CONTROLS** checks to examine your setting for password history, mixed case passwords, and the maximum number of days that a password or password phrase is valid
- **RACF_ENCRYPTION_ALGORITHM** checks return codes from your ICHDEX01 exit for encryption of passwords and password phrases
- **RACF_AIM_STAGE** tells you whether you are at AIM stage 3
- **RACF_classname_ACTIVE** tells you whether certain resource classes are active
- **RACF_BATCHALLRACF** tells you whether BATCHALLRACF is set
- **RACF_CERTIFICATE_EXPIRATION** tells you about certificates nearing their expiration

And more. Why don't you see much about them in the RACF manuals? Because there's an IBM manual dedicated to healthchecks in general, including RACF ones. It's called "***IBM Health Checker for z/OS User's Guide***" and belongs on your bookshelf.

How Do I Decide the UACC for System Datasets?

See IBM's recommendations in Appendix D of the RACF Security Administrator's Guide.

What is SMS (System Managed Storage) and Why Should a RACF Admin Care?

SMS is software that automatically manages disk datasets. For example, you can use it to specify JCL parameters for a dataset or to specify which group of disk drives a new dataset is to be allocated on. And you can use it to specify what sort of encryption a disk dataset is to have. You do this by means of the DFP segments in the RACF user, group, and dataset records. (In order to cause confusion, IBM has named the SMS-related segments of RACF profiles the DFP or Data Facility Product segments.)

SMS allows the DASD storage administrator to define several SMS classes for disk datasets

- **DATAAPPL** identifies the applicaiton such as Payroll or Sales
- **DATACLAS** specifies predefined JCL values
- **MGMTCLAS** specifies backup frequency and related values
- **STORCLAS** specifies I/O service levels for the dataset

Your SMS administrator defines the classes and writes routines to assign them to datasets. You can use RACF DFP segments on user and group profiles to specify the starting point for this assignment. Since the DFP segments can now be used for encryption, you'll want to find the system programmer who administers SMS and take him out to lunch (on your expense account of course).

Free Sources of Useful Guidance for InfoSec

- IBM manuals for z/OS and RACF 2.3 at https://www-304.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R3Library?OpenDocument
- The NIST STIGs (Security Technical Information Guides) for various types of computer, including mainframes https://web.nvd.nist.gov/view/ncp/repository
- Useful guidelines for knowing that your InfoSec is comprehensive (Note especially Publication 800-53): http://csrc.nist.gov/publications/PubsSPs.html#800-53
- Handouts from previous meetings of the NYRUG: http://www.nyrug.stuhenderson.com/handouts.HTM
- NewEra hosts free webinars on a variety of mainframe topics. You can see the schedule, and get handouts from previous sessions, at: http://www.newera-info.com/zwebs.html
- Articles from http://www.stuhenderson.com/Articles-Archive.html
- White papers from http://www.stuhenderson.com/XARTSTXT.HTM
- Newsletters from http://www.stuhenderson.com/Newsletters-Archive.html

NYRUG (New York RACF Users Group) and Tampa, FL RUG Meet November 14, 2017 from 10AM to 4PM:

Our next meetings are at IBM offices in NYC and in Tampa, a joint meeting by teleconference with the NY and Tampa FL RUGs.

Attendees **must present a government issued photo ID** to enter the IBM building. Admission is free, but even if you have registered for previous meetings, you must pre-register by emailing NO LATER THAN NOON the day before.
For Complete Directions, agenda, copies of handouts and to register, please visit the Website for the NYRUG and TBRUG: at www.nyrug.stuhenderson.

HG RACF Training Schedule:

The Henderson Group offers its RACF and information security/audit seminars around the country and on-site too. See the details below or call (301) 229-7187 for more information. For detailed class descriptions or to see what students say about these classes, please go to www.stuhenderson.com/XSECTTXT.HTM. (See info on Mainframe Audit classes below.) You can save money by holding a class session in-house, or by hosting a public session. Contact Stu for more info.

1) HG04 **Effective RACF Administration** (**$2195**)
December 5-8, 2017 in Bethesda, MD

2) HG05 **Advanced RACF Administration ($2050)**
Dec. 11-14, 2017 in Bethesda, MD

3) HG06 **UNIX (USS) for RACF Administrators** (**$550**)
Nov. 9, 2017 in Bethesda, MD

HG Mainframe Audit Training Schedule:

The Henderson Group now offers its series of "How to Audit.." seminars for IS auditors. These describe clearly how the associated software works, where the control points are, how to collect and interpret data, and how to conduct the audit. The workbooks include complete audit programs. More information is available at our website: www.stuhenderson.com/XAUDTTXT.HTM. (If you have a class topic you would like to have added to this series, please let us know.) (See info on "RACF Training" classes above.) You can save money by holding a class session in-house, or by hosting a public session. Contact Stu for more info

A) HG64 **How to Audit z/OS with MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (**$2300**)
Feb. 27-March 2, 2018 in Clearwater, Fl

B) HG65 **How to Audit z/OS with USS, TCP/IP, FTP, and the Internet**
(This class is a logical follow on to HG64.) ($1590)
Nov. 15-17, 2017 in Bethesda, MD

C) HG76 **How to Audit UNIX and Windows Security ($2200)**
October 24-27, 2017 in Bethesda, MD

Permanently Interesting Products Column

This column has been permanently moved from this newsletter to Stu's website. You can find it at: www.stuhenderson.com/XINFOTXT.HTM.

RACF User Services (Newsletter Subscriptions / Key Phone Numbers / Addresses)

Technical support hotline, Meetings, Seminar Catalogs:
Stu Henderson - (301) 229-7187
5702 Newington Rd, Bethesda, MD 20816

For Back Issues of this Newsletter, Subscriptions and Links to Several Useful Web Sites

check the Henderson Group website at:
http://www.stuhenderson.com/Newsletters-Archive.html

RACF List Server on the Internet

To join, send E-mail to the administrator for the server. (Don't send it to the server itself or your request will be routed to every subscriber.) For example, if your name is John Smith and you want to subscribe, then send this E-mail:

subscribe racf-l john smith

to the address: **listserv@listserv.uga.edu**

The reply will include directions on how to get info such as a list of all subscribers, an index to previous comments, and a command summary. You will want to set up a filter for incoming emails to direct mail from the list server to a dedicated folder or directory.

Free Email Newsletter for Mainframe Auditors

To see back issues or to subscribe to the Mainframe Audit News (MA News), check Stu's website at
http://www.stuhenderson.com/Newsletters-Archive.html

To Get a Free Subscription to the RACF User News Or to see back issues: check Stu's website at
http://www.stuhenderson.com/Newsletters-Archive.html

The RACF User News is published two times a year to share information about RACF. All information in it is offered on an "as is" basis, and should be used at your own risk, and with your own testing.

Another Source of Free, Practical Info:
Here are links to lots of useful info, including: a mainframe glossary, vendor integrity statements, z/OS configuration information, audit guides, and more.

www.stuhenderson.com/XINFOTXT.HTM

Other Internet places:

- Nigel Pentland's security page is www.nigelpentland.co.uk
- IBM RACF home page: www.ibm.com/servers/eserver/zseries/racf/
- RACF goodies site: www.ibm.com/servers/eserver/zseries/zos/racf/goodies.html
- RACF Presentations Page with lots of presentations from SHARE and GSE. Check out http://www.ibm.com/systems/z/os/zos/features/racf/presentations.html
- IBM Redbooks site: www.ibm.com/redbooks
- IBM z/OS Manuals: www.ibm.com/servers/eserver/zseries/zos/bkserv/
- Net-Q Enterprise Extender Security case studies and examples at www.net-q.com.
- (Other vendors contact info listed in the "Permanently Interesting Products" column which is now moved to Stu's website at:**www.stuhenderson.com/XINFOTXT.HTM**
- the Henderson Group: **www.stuhenderson.com**

21 Things RACF Auditors Should Know:
This PDF file lists 21 things for auditors, including a reference on why you don't need to protect the program AMASPZAP with RACF. The article is available at:
www.stuhenderson.com/XARTSTXT.HTM

More Info on Tape Security and RACF
is available at
www.stuhenderson.com/TAPESEC1.PDF

"Why RACF, ACF2, and TopSecret aren't sufficient for effective tape file security" describes how to get full security for tape datasets by using both security s oftware and tape management software