RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 96):

- **New z15 Computer**
- **Kubernetes**
- **NY RACF User Group Now Connects with Dallas, Raleigh and Tampa**

This Issue's Themes:

- Expand your career path
- Controlling all paths into your system

Free Webinars: NewEra sponsors great webinars each month on topics like:

- Protecting Your Critical UNIX Files on z/OS
- The ABC's of z/OS Integrity
- Preparing for Your Next Upgrade of z/OS
- Monitoring z/OS TCP/IP Network Defenses

See the schedule at: 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

----

Where to Get IBM z/OS Manuals

Here's a link that works:

https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zosInternetLibrary?OpenDocument

Where to get info on new stuff

(From the RUG handouts page, after October 23)

http://www.nyrug.stuhenderson.com/handouts.HTM

NEW YORK RUG Meeting Dates, Now Expanded to Dallas, Raleigh, as well as Tampa, October 23, 2019 from 10AM to near 4PM *at IBM in Dallas, Raleigh, 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).** To pre-register, please visit www.nyrug.stuhenderson.com See inside for details. (The meeting after that will be **in the Spring of 2020**)

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 and Raleigh and Dallas RUGs: To simplify all the references, we have consolidated all info for the NYRUG and the Tampa Bay RUG and Raleigh and Dallas RUGs at www.nyrug.stuhenderson.com

----

Today's Quotation

"*[Brunetti] was accustomed to swimming in the swirling froth of information and misinformation that flowed through so much of daily life;*"

— Donna Leon in "Unto Us a Son Is Given"

Vanguard Conference

The Vanguard Security Conference is in Charlotte, NC September 30-October 3, 2019. Visit www.go2vsc.com for more details.

To subscribe to this newsletter, or for back issues:

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

RACF (part of z/OS Security Server) is a trademark of IBM. This newsletter is not affiliated with IBM in any way.

==

New z/15 Computer

IBM recently announced the new z15 mainframe computer, with 25% better performance than the z14, and lots of new security features. The announcement tells us also that IBM z mainframes support 87% of all credit card transactions, as well as 29 billion ATM transactions a year. I guess the mainframe isn't dying after all.

What does this mean for RACF admins? The new z15 has lots more crypto capability. One executive commenting on the number of data breaches notes "The best thing you can do is encrypt 100% of your data, then when they get in, they can't make any sense of it." We will be seeing pressure to encrypt all data on the mainframe, both in flight (over the network) and data at rest (on disk and tape). And the hardware encryption built into disk and tape drives doesn't give much protection unless the volume is taken out of the data center.

So RACF admins will be needing to get familiar with the ICSF started task (the router for encryption/decryption requests). It uses new resource classes in RACF: **CSFKEYS** and **CSFSERV** and **CRYPTOZ** and **XCSFKEY**. We'll need to know about **Pervasive Encryption** and how it uses RACF to encrypt disk datasets. We'll need to know about **Policy Agent**, the mainframe firewall that provides the preferred method to enforce encryption over TCP/IP.

Perhaps most of all, we'll need to identify the system programmers and others who can provide us the input we need to make the RACF part of this all work.

All of these (**ICSF, CSFKEYS, CSFSERV, Pervasive Encryption, Policy Agent**) are available now with the z14 computer. This is a good time to start getting familiar with them all.

And to use them well you'll want to be on top of these RACF resource classes (and what they control)::

- **CRYPTOZ** (*access to PKCS #11 tokens)
- **CSFKEYS** and its group version **GCSFKEYS** (access to ICSF cryptographic keys)
- **CSFSERV** (access to ICSF cryptographic services)
- **XCSFKEY** and its group version **GXCSFKEY** (exportation of ICSF cryptographic keys)

Now is a good time to find the system programmer who manages ICSF and buy her lunch.

Mainframes and the Cloud

The new z15 also makes it easier to include the mainframe as part of a hybrid cloud. It gives us the capability to do cloud-native application development, using a feature called OpenShift.

We may be dealing soon with LINUX security on the mainframe, and with secure containers. Take this as an opportunity to expand your career path. Find who in your shop is starting to get into these topics and offer to work with them. The technology world is changing, and mainframe staffs are too thin already.

This is an opportunity to grow your job definition from RACF administrator to member of the enterprise-wide info security team. Volunteers will be welcomed in most if not all installations.

IBM's Cloud Strategy, What It Means for Us, Secure Containers

Imagine that your shop has the Accounts Payable application stored in a cloud provided by Microsoft. And your Order Entry application is stored in an Amazon AWS cloud server. And your CIO has just decided to put General Ledger on a cloud provided by LINUX on your mainframe, or even USS.

Your mainframe can already be a cloud server. IBM believes that most shops will not want to move critical applications and data outside of their control. The cloud server on your mainframe (your "private cloud") is where you can keep your sensitive applications and data under your own control.

IBM has stated that this is the opportunity for a **hybrid cloud**, linking applications on all these different cloud services. The idea of a hybrid cloud is the basis for IBM's strategy to catch up with Microsoft and Amazon in the cloud services marketplace. If you are part of the mainframe staff, you will be needed to help with your installation's private cloud.

So how do you share information among these applications? Securely? IBM's solution is a protocol called **Kubernetes**, which uses encryption to support a concept called **secure containers**. We'll be providing more info in future issues, but don't wait to find other opportunities to learn about these new, key disciplines. Volunteers are needed to put out the effort to learn this stuff.

What Are GENERICOWNER and ENHANCEDGENERICOWNER? (Hint: Delegation of Authority)

GENERICOWNER is a RACF option you set with the SETR command. To understand it, we introduce two types of authority in RACF:

Type 1 authority is the authority to create new profiles (user, group, dataset, resource)

Type 2 authority is the authority to alter or delete existing profiles

In general, if you have system SPECIAL, you have type 1 authority for all four types of profile (user, group,...).

If you have relevant group-SPECIAL, or if your userid is the owner of an existing profile, you have type 2 authority over it. You can issue commands to alter it and to delete it.

Now suppose you want to give someone type 1 authority just for one resource class. For example, you might want to give the CICS system programmer the ability to create new profiles in the **TCICSTRN** resource class. You do this by using the CLAUTH privilege (CLass AUTHorization):

ALU CICSUSER CLAUTH(TCICSTRN)

But what if you want to limit what that system programmer can do? Use GENERICOWNER or ENHANCEDGENERICOWNER.

GENERICOWNER This toggle switch controls the ability to undercut general resource rules (but NOT dataset rules). Imagine that for example in the resource class TCICSTRN, the following transaction rules have been defined: I*, IN%%, and INQ7.

You want to prevent unauthorized persons from creating a new rule for INQ%, since this would undercut I* and IN%%. (Remember that RACHECK and FRACHECK select the most specifically matching rule and use it for all their logic.) You would set GENERICOWNER, which specifies that only the owner or users with SPECIAL can alter existing (or create more specific new) general resource profiles. The effect of this is to prevent someone with CLAUTH(TCICSTRN) from creating a more specific profile, unless his userid is the owner of the less specific profile..

Of course, you need to be sure that this doesn't upset delegation of RACF authority in other resource classes.

Enhanced GENERICOWNER As of RACF 2.3, you can modify the extent of the effect of GENERICOWNER. Without this modification, GENERICOWNER applies only to individual profiles (such as TCICSTRN), but not to members specified in grouping profiles (such as GCICSTRN). With the enhanced version, grouping profiles are covered as well.

Protecting Every Path Into Your System

To have good security, you want to know (and be able to demonstrate) that every path into your system is controlled by RACF. For batch jobs, you can turn on **BATCHALLRACF** and **XBMALLRACF** with the SETR command. For started tasks, you can include a catchall entry in the **STARTED** resource class to ensure that every started task has a userid associated with it.

Which leaves all the network connections. Here's how to think about them: All of the network connections into your z/OS mainframe use of of three protocols: **SNA** (System Network Architecture), **TCP/IP** (Transmission Control Protocol / Internet Protocol), and **UDP** (User Datagram Protocol).

SNA You might hear that SNA is dead or not on your system. It is alive and well, on your system and needs to be protected.

TCP/IP supports sending of messages, with error checking and with confirmation that messages have been received. You use this for FTP, email, remote logons, browsers like Internet Explorer and Firefox, much of your Internet connections, and your refrigerator.

UDP supports sending of messages, just sending them quickly. It has no confirmation that the message was received, but the low overhead makes it fast. You use this over the Internet, and over your internal network, to send messages when error checking and confirmation of receipt are less important.

Originally, mainframes supported just SNA. Software like TSO and CICS were designed with SNA in mind. When the Internet and TCP/IP were added to z/OS, people needed to talk to TSO and CICS using TCP/IP. So what happens very often is that a program called a terminal emulator runs on your Windows computer. This program lets your Windows computer pretend to be an SNA-style terminal. This program wraps SNA packets inside a TCP/IP message, which is sent over the Internet to your mainframe. When it arrives, your mainframe extracts the SNA packet from the TCP/IP message and hands it to TSO, or CICS or whatever application your terminal is connected to.

To protect your SNA connections, you will want to have a policy requiring every **applid** (program that can connect to a terminal) to use RACF to verify the user's identity.

To protect your TCP and UDP connections, you can use statements like PORT UNRSV TCP * DENY and PORT UNRSV UDP * DENY in the TCP/IP configuration file. Or you could use the free firewall software that comes as part of z/OS named Policy Agent. You might discuss this with your TCP/IP administrator.

Note: You may think that this is not your job since you are responsible for RACF. But the TCP/IP administrator may think it's not his job, since you're the one responsible for mainframe security. Grow your career path and start the conversation.

(Cont'd)

If your shop uses **Enterprise Extender** or **APPN** (ask your VTAM system programmer), then you are using SNA there too (actually SNA in a UDP wrapper). This raises risks specific to APPN, which is often used for example when a financial institution connects its SNA network to that of a credit card processor like American Express or Visa. You can learn more about these risks and how to protect against them from this article:

http://www.stuhenderson.com/appnsec1.pdf

NYRUG (New York RACF Users Group) Now Extended to Dallas, TX and Raleigh, NC as well as Tampa, FL RUG

October 23, 2019 from 10AM to 4PM:

Our next meetings are at IBM offices in NYC and in Tampa and Raleigh and Dallas , a joint meeting by teleconference with all these RUGs.

The meeting after that will be in the Spring of 2020.

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 Effective RACF Administration Training and Mainframe Audit 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 RACF administration 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.

HG04 **Effective RACF Administration** (**$2195**)
November 4-7, 2019 in Bethesda, MD

For mainframe audit training, please see: www.stuhenderson.com/XAUDTTXT.HTM.

HG64 **How to Audit z/OS with MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (**$2300**)
November 18-21, 2019 in Bethesda, MD

Interesting Products We have not formally evaluated these products, but think you will find them interesting.

ETF/R - The EKC Firecall Tool for RACF allows controlled usage of special "high access" capabilities during an emergency situation, providing pre-defined "on demand" access capability when needed - eliminating the need for unnecessary full-time high level privileges. All requests to use Firecall and any access granted because of this facility are journalled to SMF and can then be reported using ETF/R report programs, meeting auditor requirements for PAM (Privileged Access Management).

E-SRF – EKC's Security Reporting Facility is a comprehensive security analysis and reporting tool designed to provide critical RACF security information in an easy-to-read format. E-SRF provides a full spectrum of reports to fully understand both potential and actual access.

Contact Information: Sales@ekcinc.com www.ekcinc.com Phone: 847.296.8010

---

eventACTION is a comprehensive change management solution designed specifically for mainframe technical support areas requiring 24/7 availability. It is no longer possible for all system changes to be introduced via IPL.

Management must be able to ensure that systems continue to operate properly in the face of dynamic changes and demonstrate to auditors that proper controls are in place. It is necessary to be able to identify all changes that have been made, and to provide the appropriate controls to assure that no unauthorized changes have been introduced to the system.

The typical application programmer's change management tool is unable to successfully track and manage the broad spectrum of tools that a systems programmer must use. Provisions have to be made so that changes can be made dynamically to the production Today's systems programmers must ensure maximum reliability and availability for environment. It is important that technical people can make these changes when required and equally important that these changes are tracked and/or controlled actively.

eventACTION provides complete and thorough solution and makes for an easy implementation without changing the way people work.

Action Software International's z/OS MVS and z/OS UNIX change management tools are deployed in over 250 of Global 2000 institutions.

For a copy of our position paper "Keys to effective systems change management", or further information please contact:

Action Software International
20 Valleywood Drive
Markham, ON L3R 6G1 Canada (800) 821-4551
www.actionsoftware.com sales@actionsoftware.com

RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

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
stu@stuhenderson.com

For Back Issues of this Newsletter, Subscriptionsand 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 iswww.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**

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 software and tape management software

To protect voting machines fromhackers,

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

RACF (part of z/OS Security Server) is a trademark of IBM. This newsletter is not affiliated with IBM in any way.