RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 93):

This Issue's Themes:

- Simpler security administration
- Better security
- Demonstrable to auditors

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

- The ABC's of z/OS Integrity
- Preparing for Your Next Upgrade of z/OS
- Guidelines for Managing z/OS Vulnerabilities
- A Guided Tour of Policy-Based Data Set Encryption

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

Special Info Source for Documents on RACF from NaSPA (Network and Systems Professionals Association http://naspa.com/) and others at:

http://ibm.biz/RACF_PDFs

The next NY Metro NaSPA Chapter meeting will be Wednesday, 17 October, 2018 at the IBM Building at 590 Madison Avenue in NYC

(Thanks to Mark Nelson)

NEW YORK RUG Meeting Dates, Now Expanded to Raleigh, NC, as well as Tampa, FL

May 9, 2018 from 10AM to near 4PM *at IBM in 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).** See inside for details. (The meeting after that will be **October 4, 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 and Raleigh site: To simplify all the references, we have consolidated all info for the NYRUG and the Tampa Bay RUG and Raleigh site at www.nyrug.stuhenderson.com

---

Today's Quotation

" *Dance like no one is watching, encrypt like everyone is."*

— Elardus Engelbrecht

Vanguard Conference

Vanguard Security & Compliance 2018 takes place September 10-13 at DFW Airport Marriott South in Ft. Worth, TX. 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.

First Way to Save Your CIO Money

Many software products charge fees based on the number of CPUs they execute on. If you have many CPUs in a sysplex, you can save money by using such products only on one CPU, avoiding the extra fees if used on every CPU or LPAR. You can use RACF to restrict this, using the PROGRAM class. Here's how, as shared on the RACF-L by Guus Bonnes and Elardus Engelbrecht:

"***Due to product licensing and do some penny pinching we would like to restrict usage of a particular product in a particular LPAR. I thought I could use RACF PROGRAM class to deny access to product Library / Module from that particular LPAR but not sure if it CAN WORK with SHARED RACF DABASE.***

Yes of course. Do what Guus said. Use PROGRAM <name of module> with WHEN(SYSID) plus your datasetname. All in all with a SysPlex shared RACF DB.

For example, COBOL is licensed on some LPARs, so I have this:

PROGRAM IGY*

DATA SET NAME VOLSER PADS CHECKING
---------- ------ ----------
IGY.SIGYCOMP NO

... and ...

WHEN(SYSID) giving Read Access on some LPARs for ids(*).

The COBOL programmers need to remember to use /*JOBPARM SYSAFF=<LPAR> otherwise they will get a very nice ICH408* message."

Thanks to Guus and Elardus for sharing.

If you don't subscribe to the free RACF-L on the Internet, here's how:

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.

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

Second Way to Save Your CIO Money

Many installations have UNIX or Windows servers connected to the Internet to let customers buy products and to let other users share information. And the large volumes of critical data such as the customer master file are stored on the mainframe. This happens often because the applications originally ran on the mainframe, before the Internet was invented. So now the applications running on the Windows and UNIX servers access the data stored on the mainframe over your internal network.

After this was all set up, IBM added UNIX to the mainframe and added TCP/IP on top of it. And added all the standard TCP/IP programs like FTP, email, and the http daemon. And IBM added JAVA to the mainframe. (Great way to win bar bets: ask a distributed person whether he thinks the mainframe supports JAVA.)

Since then, there isn't much that runs on Windows or UNIX that you can't easily port to the mainframe. By the way, the mainframe has better: security, reliability, scalability, and response time than distributed boxes.

What do you think it costs to support those UNIX and Windows servers? How many of them do you have? (In some shops, they number in the hundreds.) If anyone in your shop calculates the potential savings from porting all those applications to the mainframe, the numbers can be surprsingly large. Those servers have costs for hardware, software, office space, and administrative staff.

There are other factors to consider beyond just cost, but it's hard to dismiss the idea of porting all those applications to the mainframe if you don't know what the potential savings are.

Why the SEARCH Command Is the Coolest Command in All RACF:

1. It lets you search for the names of userids, groups, dataset rules, and resource rules that match two-part search terms. For example, to list the names of all the dataset rules whose names begin PROD and which have PAYROLL anywhere else in their name:

SEARCH CLASS(DATASET) MASK(PROD PAYROLL)

2. It lets you build a CLIST of commands to execute on the names it lists. For example, to create a CLIST of commands to revoke every userid that hasn't been used in 100 days:

SEARCH CLASS(USER) AGE(100) CLIST('ALU ' ' REVOKE')

(Note the spaces around ALU and REVOKE. Be sure to review the CLIST before you execute it.)

3. It tells you all the permissions a given user has to all rules in a given resource class. To list every FACILITY class resource rule to which USER17 has access:

SEARCH CLASS(FACILITY) USER(USER17) NOMASK

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

Why RACF is Better Than DB2 Internal Security

If your DB2 installation still relies on DB2 internal security, here are some reasons you might want to replace it with RACF. First, some description of how DB2 internal security works:

DB2 internal security uses the concept of “authid”, which is like a userid, but specific to DB2. You use the GRANT command to permit an authid to access data in a table. Originally, any user using DB2 was identified by a single authid. There was no method to group users. So if you wanted to grant 500 users to update data in a table, you would issue 500 GRANT commands.

DB2 internal security also has no way to use wild card characters in the names of tables. So if you have ten tables named STU.TABLE01, STU.TABLE02, etc, there was no way to grant access using a name like STU.TABLE*.

To grant those 500 users access to those ten tables would require 5,000 (500 times 10) GRANT commands. No wonder DBAs would identify users not by their RACF userid, but by the name of the CICS transaction they were using.

Then IBM made it possible for us to identify a user with several authids at once: a primary authid (which was a copy of the RACF userid) and one or more secondary authids (which were often the RACF groups that userid belonged to). There were still no wild card characters, but at least you could group users, defining a RACF group that would serve as a secondary authid.

But finally, IBM let us replace DB2 internal security with calls to RACF. This lets us group users in RACF groups, and use wild card characters in the names of the tables. And then all security administration is centralized using a single tool, with a single set of administrators. It’s a major project to convert to this, but shops that make the effort are glad they did, and they have better security, security which is easier to demonstrate to auditors, too.

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

What Is Air-Gapping?

See if these are true for your shop:

1. We agree that passwords are not a reliable way to prove someone's identity because, among other reasons, too often some user will fall for an email phishing attack and give away his userid and password.

2. Our email servers are connected to the Internet by means of our internal TCP/IP network, so we can email outside our organization.

3. Our customer facing e-commerce servers are also connected to the Internet by means of our internal TCP/IP network, so they can process customer requests to buy our products and services.

4. Our customer-facing e-commerce servers are also connected to our mainframe by means of our internal TCP/IP network, because they need to access the customer master file and similar essential data is stored there.

5. No one has an accurate, up-to-date map of our internal TCP/IP network, but someone informs us that there are lots of firewalls protecting us. Each of these firewalls is essentially a UNIX computer that can filter and block messages over our network, depending on the rules someone specified for them. No one has an accurate, up-to-date list of the rules, but there are literally hundreds of thouands of them.

6. We understand that hackers don't infiltrate systems in one fell swoop. Instead they collect information, find a way to break into one computer on the outside edge of the network, use this to find a way to get elevated privileges or to break into the next computer on the network, and so on,

7. We know that at least one mainframe computer has been hacked over the Internet, as described in http://www.stuhenderson.com/Mainframe%20Audit%20News/MANEWS22.pdf

8. The mainframe comes with a free firewall program that lets us protect the mainframe from attacks over TCP/IP. This tool is free, effective, centrally administered, and not used. (It is called **Policy Agent**.)

9. Because all the sub-nets in our internal TCP/IP network are physically connected together, anyone who can succeed in breaking into the UNIX computers that constitute our distributed firewalls may be able to move from one sub-net to the next.

10. Air-gapping is the breaking of subnets apart physically, so even if someone breaks into one sub-net, she can't cross over to the others. We isolate our production mainframe LPAR by air-gapping it from the rest of the network, or by having a single, tightly controlled, highly monitored, physical pathway between it and the rest of our internal network.

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

Easy Completeness

Our jobs as RACF administrators are made easier by options that force all items to be covered by RACF. Think of the **PROTECTALL** and **BATCHALLRACF** settings. Before we had these, you couldn't be sure that every dataset was protected by RACF, and that no batch job could execute without having a RACF userid.

Simpler administration. Better security. Easier to demonstrate to auditors.

And for many resource classes, we can ensure that every resource is protected by defining a "backstopping" rule (named **) which matches every resource name. So if the system programmer creates a new resource and forgets to tell the RACF administrator, the resource will be protected by the backstopping rule. (Be sure not to use backstopping rules with the FACILITY resource class, nor for any other class for which programs rely on whether a rule exists.)

And to ensure that every started task is defined to RACF, we can define a backstopping rule in the STARTED resource class.

And for network security, we can define policies in a central place to provide comprehensive protection. (It's called **Policy Agent** and should be administered by a security conscious TCP/IP administrator.)

And for security of disk datasets, we can also define polices in a central place to provide comprehensive protection. It's called **persistent encryption** with the latest release of z/OS.)

Simpler administration. Better security. Easier to demonstrate to auditors.

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

May 9, 2018 from 10AM to 4PM:

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

The meeting after that will be October 4, 2018.

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.

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

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

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.

HG04 **Effective RACF Administration** (**$2195**)
November 27-30, 2018 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

HG64 **How to Audit z/OS with MVS, RACF, ACF2, TopSecret, CICS, DB2, and MQ Series Security** (**$2300**)
November 5-8, 2018 in Bethesda, MD

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

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
stu@stuhenderson.com

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

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.