RACF USERS' NEWS

An Info-Sharing Newsletter for Users of RACF Security Software

IN THIS ISSUE (No. 94):

This Issue's Themes:

- MVS Security
- RACF Administration in the Organization
- Resource Class Self Check

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
- Let's Build a z Environment

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

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.

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

October 4, 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 **in the Spring of 2019**)

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

"*There are only two ways to live your life. One is as though nothing is a miracle. The other is as though everything is a miracle.*"

— Albert Einstein

To subscribe to this newsletter, or for back issues:

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

What is SIEM, Share Success Stories

SIEM (Security Information Event Management) is the collection and analysis of security information from a variety of sources, often for a variety of platforms, for automated comparison against specified norms or standards.

For mainframes, SMF data is a prime input to any SIEM effort. It might make sense to use a SIEM tool to combine SMF data, other mainframe log data (such as USS and TCP logs) with log data from connected Windows and UNIX computers. The volume and variety of information this makes available can be daunting, which is why we have software products to do a lot of the legwork for us.

We would love to hear success stories about SIEM: what the analysis discovered, what security exposures were fixed as a result, what unusual behavior was identified, and what it turned out to be. We can all benefit from good success stories. You don't have to share the SIEM product used or the organization using it (although you are welcome to), but we'd all like to hear good success stories. Please send yours to stu@stuhenderson.com. Thanks.

How RACF Provides MVS Security

MVS security relies on RACF security,since certain MVS system datasets are used to set options for MVS, including security options. Any user who can write to these **key system datasets** can then bypass all the security on the system (including RACF). Of course RACF controls who can write to these datasets.

So, to address MVS security, draw up a list of the key system datasets. This will include: the parmlibs, the proclibs, the APF libs, the LPA libs, and others specified by your system programmer. Make sure that the RACF dataset rules protecting them allow update access only to a small number of authorized users, and only with logging activated so that all updates will be logged to SMF.

A second set of datasets are called the **sensitive system datasets**, and include datasets that might contain sensitive information, including: the RACF database, the JES spool and checkpoint files, the page datasets, and others specified by your system programmer. Make sure that the RACF dataset rules protecting these datasets do not allow read access, except by the appropriate system software and a very small number of other users. The dataset rules should permit access only with logging activated so that all accesses will be logged to SMF.

It will then be useful to have a program read the SMF data and note any update accesses to key datasets and any read access to any sensitive system datasets. Someone should be responsible for reviewing this report, perhaps comparing accesses to change tickets or other indicatators of approved access.

RACF Administration and the Organization: From the Top, From Inside, Upwards

From the Top: A common complaint identified in surveys of employees is that supervisors do not provide clear explanation of a department's mission and of what each employee is expected to do. You can see that when this is the case, the whole organization is less effective, and employees are less happy.

Ask yourself if you provide clear direction to those who report to you. Then ask them their opinion.

Ask yourself I your supervisor gives you clear direction of what she expects from you and from the department. If you are not happy with the answer, have a courteous conversation with her to see what improvement is possible.

From Inside: We can view our role as RACF administrators as "Give access and reset passwords for anyone who gives you a form".

Or: "Working with others, find effective ways to improve mainframe security and implement them safely."

Which way makes you happier? They say that each of us creates his own universe by choosing what to think about, and what to think about it.

Upwards: We sometimes forget to ask ourselves what we think of the reporting we give to our management on what we have been spending time on. Possible reporting could include:

"This month, we successfully reset 2,300 passwords and reviewed the violations report thirty-one times. We proactively checked 100 percent of the compliance items prescribed by the auditors." Or

"We reviewed the access permissions for twenty-one applications with the application owners to ensure that the actual rules match their approvals. We implemented five new automated security healthchecks to increase our automatic security protection. We analyzed the report of password violations and developed a training program that reduced the time spent on addressing them by thirty percent. We documented the approved security software settings to create a baseline document. This will permit us to detect and correct any improper changes to the settings. We investigated possible software tools to improve our analysis of log files, both to improve security and to increase efficiency. In addition, we responded to over 4,000 requests for changes to rules and passwords." Or:

"This month we accomplished nothing other than respond to requests for information from auditors."

The way we report our progress and accomplishments will shape the way the rest of the organization views us.

RACF Protection of Tapes

There are three ways to tell RACF to protect tape datasets the same way it protects disk dataset, that is by means of the dataset rules. (Note that RACF treats datasets on virtual tapes exactly the same as on real tapes.)

The first and standard way is to use SETR TAPEDSN. This is sometimes not the best solution if you receive tapes from other organizations. If you have PROTECTALL turned on, and if their dataset naming standards don't match yours, the opening the dataset will fail.

The second way is to set options in your tape management software telling it to call RACF for tape datasets, but to accept the access request if RACF has no matching rule and the tape volume serial number is not one that belongs to your organization. You can sort this out with whoever administers your tape management software.

The third method is to use a member in the MVS parmlibs named DEVSUPxx which can specify these tape security options:

The way to provide better protection involves four values in parmlib member DEVSUPxx. They are:

- TAPEAUTHDSN (= YES or NO, defaults to NO)
- TAPEAUTHF1 (= YES or NO, defaults to NO)
- TAPEAUTHRC4 (= ALLOW or FAIL, defaults to FAIL)
- TAPEAUTHRC8 (= FAIL or WARN, defaults to FAIL)

The latter two only apply to SAF calls caused by the first two.

TAPEAUTHDSN tells the system whether to call RACF for tape datasets (similar to SETR TAPEDSN, but doesn't use TAPEVOL records).

TAPEAUTHF1 can be used to tell your Tape Management Software to call SAF for every dataset on a cartridge instead of just the dataset you are reading. This gives extra protection against someone authorized to one dataset on a tape using that authorization to access other datasets on the same tape.

TAPEAUTHRC4 tells the system what to do if SAF is called by either TAPEAUTHDSN or TAPEAUTHF1 and SAF indicates "no dataset rule matches this dsname." This is a way to bypass PROTECTALL just for tapes

TAPEAUTHRC8 tells the system what to do if SAF is called either by TAPEAUTHDSN or TAPEAUTHF1 and SAF says to fail the request. This is like a warning mode, but just for tape datasets.

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

October 4, 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 in the Spring of 2019.

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.

Our Latest Self Check for Resource Classes

Below is a selected list of resource classes we believe should be used in almost every RACF z/OS installation. We include for each class a description of what it is used for and why we consider it important. You can rate your own installation be comparing your active classes from the DSMON report or SETR LIST against the list below.

(Note that the list below leaves out grouping classes, and classes for: CICS, IMS, VM MQ, and APPC. You will have your own opinion and we would be glad to hear from you changes you would recommend for this list.

APPL controls access to CICS and IMS regions, to TSO, to USS, and to other paths into the system

CDT defines new resource classes dynamically

CONSOLE controls use of consoles, including MCS consoles

DASDVOL controls use of programs to take full-pack dumps and restores, use of AMASPZAP sensitive functions, and allows operators to erase certain disk datasets without letting them read the data

DEVICES controls allocation of certain devices

DIGTCERT and **DIGTRING** store digital certificates and keyrings

FACILITY catch-all class, covers USS privileges, use of BLP with tapes, allows storage management staff to do their jobs without OPERATIONS, and more

GLOBAL essential for performance

JESJOBS prevents spoofing of FTP by means of a batch job with the job name of the FTP daemon

JESSPOOL protects printouts waiting to be printed

NODES controls access through NJE

OPERCMDS controls use of operator commands

PROGRAM controls who can execute powerful programs

PROPCNTL prevents propagation of userids from CICS regions

RACFHC essential for healtchecks

RACFVARS defines symbolic variables, defines which nodes are local.

SDSF . controls use of SDSF functions

SERVAUTH protects TCP/IP

STARTED defines started tasks to RACF dynamically

SURROGAT controls submission of batch jobs for specified userids without passwords,

TEMPDSN protects temporary datasets if the system crashes

VTAMAPPL prevents rogue programmer from writing program that pretends to be for example production CICS region, in order to harvest passwords

WRITER controls access to writers, such as those writing pre-signed checks

CSFKEYS controls access to encryption keys for ICSF

CSFSERV controls access to encryption functions for ICSF

TSOAUTH controls privileges in TSO

UNIXPRIV controls privileges in USS

Free Sources of Useful Guidance for InfoSec

- 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
February 26 - March 1, 2019 in Clearwater, FL

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