Advanced Configuration and Auditing with RACF on z/VM

Date: March 3, 2011
Session ID: 8481

Bruce Hayden
IBM Advanced Technical Skills
Endicott, NY

Agenda

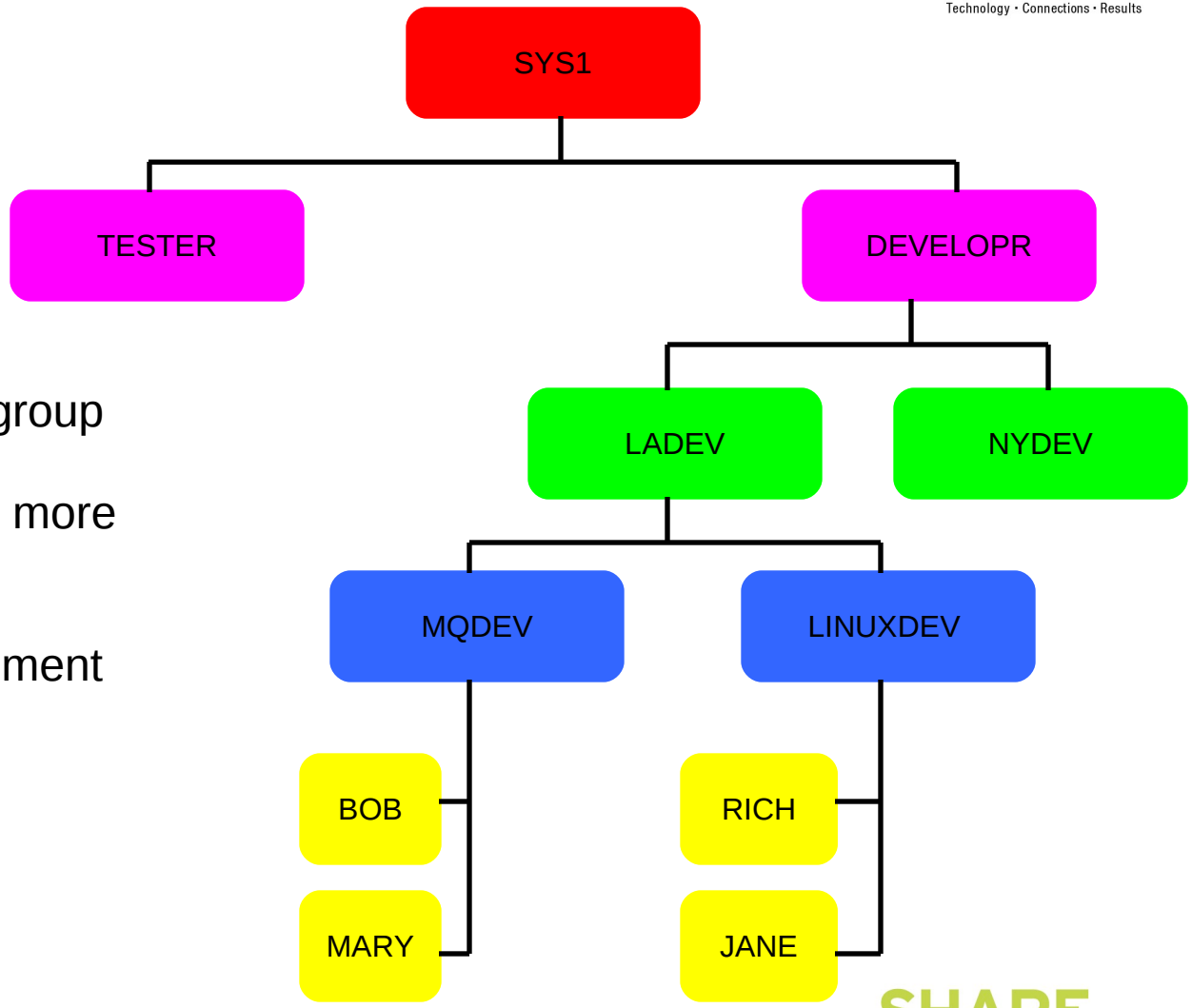
- Using Groups
- Shared user ids
- Directory Passwords
- DIRMAINT
- Customizing
- Error Recovery
- Auditing
- Reporting

RACF Groups

Using Groups

- Easier administration - group userids that have common uses
- Naming groups
  - Same “naming space” as users – hard to tell them apart!
  - Use a naming convention for groups
    - i.e., start with $, G, end with $, etc.
- Just connect new user ids to groups, and you're done!
  - Example:
    - System programmers to the $SYSPROG group
    - Linux guests to $LINUX group
- Be sure to enable RACF option GRPLIST
  - Enables checking all groups the user is connected to for authority
    - Otherwise, only the user's current connect group is checked
  - RAC SETROPTS GRPLIST

Group Structure



- Give access rights to a group
- Connect users to one or more groups
- Delegate group management

Using Groups – Examples

- Creating a Group for Linux servers
  - ADDGROUP $LINUX OWNER(LNXADM) SUPGROUP(SYS1)
- Give the LNXADM id authority to connect Linux servers
  - CONNECT LNXADM GROUP($LINUX) OWNER(LNXADM) AUTHORITY(CONNECT)
- Connecting a new Linux server to the group
  - CONNECT LINUX01 GROUP($LINUX) OWNER(LINUX01) AUTHORITY(USE)
- Granting permission to a resource for all Linux servers
  - PERMIT LNXADM.291 CLASS(VMMDISK) ID($LINUX) ACCESS(READ)
- Removing a user
  - REMOVE LINUX01 GROUP($LINUX)
- Deleting a group
  - Remove all users first
  - DELGROUP $LINUX

Shared User ids

Shared User ids

- Some user ids may need to be shared by multiple users
  - MAINT, OPERATOR, TCPMAINT
- However, sharing a common password is bad!
  - Frequently not allowed by security policy
  - No accountability
- CP has native LOGON BY support
  - Allows logon “by” (or using) an unshared id and its password
    - LOGON MAINT BY BRUCE
  - But, limited to only 8 unshared ids per shared id
- RACF has full support
  - No limit on number of sharing users
  - Part of the audit trail
  - Very handy when coupled with group support

Shared User ids – Examples of defining

- Activate the SURROGAT class
  - SETROPTS CLASSACT(SURROGAT)
- Define a resource for each user id that is shared
  - RDEFINE SURROGAT LOGONBY.OPERATOR UACC(NONE)
  - RDEFINE SURROGAT LOGONBY.MAINT UACC(NONE)
  - RDEFINE SURROGAT LOGONBY.TCPMAINT UACC(NONE)
- Give permission to any id allowed to logon
  - PERMIT LOGONBY.MAINT CLASS(SURROGAT) ID(BRUCE) ACCESS(READ)
- Using groups makes a lot of sense here
  - PERMIT LOGONBY.OPERATOR CL(SURROGAT) ID(**$SYSPROG**) AC(READ)
  - PERMIT LOGONBY.OPERATOR CL(SURROGAT) ID(**$OPERGRP**) AC(READ)
  - PERMIT LOGONBY.MAINT CL(SURROGAT) ID(**$SYSPROG**) AC(READ)
  - PERMIT LOGONBY.TCPMAINT CL(SURROGAT) ID(**$SYSPROG**) AC(READ)

Shared User ids – Using

- Logging on a shared id
  - LOGON MAINT BY BRUCE
  - Operator console shows:
    - `GRAF vdev LOGON AS MAINT USERS = nnn` **`BY BRUCE`**
  - Query who is logged on to MAINT
    - QUERY BYUSER MAINT
    - **`The BYUSER for MAINT is BRUCE`**
  - The “byuser” is retained when you disconnect, updated on reconnect
- Direct logon is no longer allowed when SURROGAT resource is defined for a user
  - LOGON MAINT
    RPIMGR066A User ID MAINT is defined as a shared user ID that may not be logged onto directly
    LOGOFF AT 16:24:31 EDT THURSDAY 03/25/10 BY SYSTEM
  - Allowed if you permit the shared user id read access to its own profile
    - PERMIT LOGONBY.MAINT CLASS(SURROGAT) ID(MAINT) ACCESS(READ)

Directory and DIRMAINT

Special Directory Passwords

- Some directory passwords have special meanings to CP
  - **NOLOG** Act like the userid doesn't exist (no logon or spooling)
  - **NOPASS** Allow logon without a password
  - **AUTOONLY** Do not allow direct logon, only XAUTOLOG
  - **LBYONLY** Only allow LOGON BY, or XAUTOLOG
- With RACF active, things change a little
  - **NOLOG**
    - Works as before
  - **NOPASS**
    - Allows logon without password if user is not revoked
  - **AUTOONLY**
    - Works as before – direct logon is not allowed
    - The password or pass phrase should be removed from the user in RACF
  - **LBYONLY**
    - Ignored, now controlled by a profile in the SURROGAT class

DIRMAINT with RACF

- Adding a new user
  - Defines user to RACF (ADDUSER)
  - Defines resources (RDEFINE)
  - RACF command arguments are customizable
- Changes to users
  - Same change is reflected to RACF – even password changes
- Setting it up
  - Configuration file supplied with DIRMAINT: CONFIGRC SAMPDVH
  - Rename and use it as supplied or customize it as needed.
    - DIRMAINT reads all CONFIG* DATADVH files that it finds
  - DIRMAINT will require:
    - Read access to resource DIAG088 in the VMCMD class
    - RACF SPECIAL authority
  - APAR note: VM64640 fixes handling of special directory passwords

Customizing RACF

Customizing the RACF – CP interface

- 6 “stub” CP modules used for the ESM interface
  - HCPRPD, HCPRPF, HCPRPG, HCPRPI, HCPRPW, and HCPRWA
  - ESM replaces these with its own code
- HCPRWA has the most common customization
  - High Level Assembler is required to make changes
  - If this is a problem – call the support center
  - This requirement should be relaxed in a later release
- 4 customizable macros in HCPRWA
  - RACSERV
  - GLBLDISK
  - SYSSEC
  - ICHNGMAX

Customizing HCPRWA

- RACSERV macro
  - Defines the name of a RACF service machine
  - Maximum of 10 can be defined
  - Default defines user ids RACFVM and RACMAINT
  - Specialized RACF servers could be created
    - Such as servicing SFS requests only and not used for CP
- GLBLDISK macro
  - Defines a table of public read only minidisks
    - No auditing or authorization checking done for read only access
  - Avoids a call from CP to RACF
  - Performance benefit for frequently linked public disks
- ICHNGMAX macro
  - Defines the maximum number of GIDs for POSIX
  - Only matters if you use OpenExtensions with RACF

Customizing HCPRWA, continued

- SYSSEC macro
  - Defines the relationship between RACF's response to an access request and the final disposition of that request by z/VM.
  - Choices:
    - Allow – Tell CP to allow the access
    - Defer – Process the request as if RACF was not active ("Defer to CP")
    - Fail – Tell CP to not allow access
  - Only classes VMMDISK, VMRDR, VMNODE, VMCMD, and VMLAN
    - No choices on the response for other classes

RACF Response to z/VM	**Choices** (default is underlined)
Authorized (PERMIT)	Allow or Defer
Access not authorized (FAIL)	Defer or Fail
Not authorized, WARNING	Defer or Fail
Resource not defined to RACF	Allow, Defer, or Fail

The SYSSEC macro

- Using the WARNING response with Defer to CP
  - Helps the transition to RACF
    - things work as they did before, but you also get messages
  - Controlled by the resource profile
    - WARNING option on the RDEFINE or RALTER command
    - Remove setting with RALTER ... NOWARNING
  - Access attempt is always written to the audit log
  - Also use NOTIFY to collect failed access attempts
- Response for resources undefined to RACF
  - In other words – no RDEFINE has been done
  - Defer to CP is necessary when setting up RACF
  - Not a good idea on a fully secured system
    - Requests for something undefined should fail!

Changing HCPRWA and SYSSEC

- Create a more secure system – what about this setup?

RACF Response to z/VM	Setting
Authorized (PERMIT)	Allow
Access not authorized (FAIL)	Fail
Not authorized, WARNING	Fail
Resource not defined to RACF	Fail

- IBM supplies a pre-built optional HCPRWA with these settings
  - Part of the recommended configuration defined in the *z/VM Secure Configuration Guide*
  - Called HCPRWAC
  - See Appendix C of the Guide for how to build your system with it
  - Do not change to this until RACF is configured!

RACF messages

- This is an additional setting on the SYSSEC macro
- Defines if a RACF message shows for an authorization failure
  - Along with the normal messages from CP
- Example

```
CP LINK MAINT 191 291 RR
RPIMGR032E YOU ARE NOT AUTHORIZED TO LINK TO MAINT.191
HCPLNM298E MAINT 0191 not linked; request denied
```

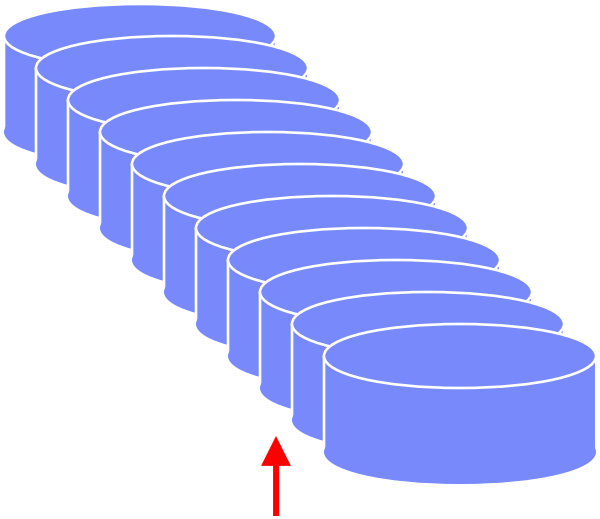
  - If DISKM=NO is specified, the RPI message is not displayed
- Can only be specified for certain RACF classes
  - VMMDISK, VMRDR, VMNODE, VMCMD, and VMLAN
- Default setting is Yes for all classes

Problems?

Error Recovery

- Built-in redundancy
  - 2 database disks
  - 2 sets of code disks
  - 2 servers (RACFVM for production, RACMAINT for test)
- 2 database disks (primary and backup)
  - Updated in parallel
  - Use the RVARY command to switch to the backup
    - Then you must repair the primary
- Please note!
  - The default location of both database disks is the same volume!
  - I suggest you move one of them to another system volume.
- There is also a utility to back up the database

RACF for z/VM Layout



6VMRAC10

Owns RACF/VM Installation and Service Disks

490
CMS/CST RACF Disk

305
Server Code

RACFVM

RACF Server Controls resource allocation

- Owns RACF databases
- Owns SMF records

200
Primary Database

300
Backup Database

301
Primary SMF Recording Disk

302
Secondary SMF Recording Disk

RACFSMF

Archives SMF records

192
SMF Archive Disk

RACMAINT user

- RACMAINT exists to test updated (serviced) RACF code
  - SERVICE process loads updated code to alternate disks (“test” disks)
    - Code to 6VMRAC10 505 instead of RACFVM 305
    - Common code to 6VMRAC10 29E instead of MAINT 19E
    - CST to 6VMRAC10 590 instead of RACFVM 490
  - RACMAINT always uses the alternate disks
  - RACF test procedure (as stated in the program directory):
    - IPL CP using parameter disk 2
    - Specify the NOAUTOLOG start option
    - XAUTOLOG RACMAINT
    - RACMAINT will start AUTOLOG2

RACMAINT in the service process

- After testing - put the serviced RACF code into production
  - Done by PUT2PROD, like all other z/VM components
    - RACFVM must be down and RACMAINT running for this process
    - If you did not reIPL your system, then on OPERATOR:
      - FORCE RACFVM
      - XAUTOLOG RACMAINT
  - After PUT2PROD – the same code is on both sets of disks
    - So, RACMAINT can be used if RACFVM has problems
- Perform a normal IPL of your system after PUT2PROD

Error Recovery – RACF abend

- What happens if RACFVM dies?
- Only the active system operator can XAUTOLOG RACFVM or RACMAINT
  - Any other use of XAUTOLOG is denied
  - The active system operator can be discovered with CP QUERY SYSOPER
- Only an operator, RACFVM, and RACMAINT can log on
  - ***Using the password in the CP directory!!!***
  - Make sure you know these and that they are not trivial!
  - An “operator” is the primary system operator or an alternate operator id, as defined in SYSTEM CONFIG
  - To start RACF if you logon directly to the RACFVM id:
    - CP IPL 490
    - RACSTART

Auditing

Auditing in RACF

- Many different things can be audited
  - Access to resources
  - RACF commands
  - CP commands and z/VM events
  - Actions performed by security administrators
  - Changes to profiles
  - Attempt to use unauthorized commands
  - and more..
- Separation of duties
  - All auditing settings and functions have separate controls
  - User must have attribute AUDITOR to change settings
- Audit log
  - RACF audit data are called SMF records
    - **S**ystem **M**anagement **F**acility

What should you Audit?

- Look at your company security policy
  - Find out what records must be kept and how long to keep them
  - What data will you need if a security problem occurs?
- Settings to audit the actions of privileged users
  - **SAUDIT** Log all commands issued by SPECIAL users
  - **OPERAUDIT** Log any accesses made by OPERATIONS users
  - **CMDVIOL** Log all command violations (unauthorized usage)
- Settings to audit access attempts by class
  - Keywords ALWAYS, NEVER, SUCCESSES, FAILURES
  - Example: SETROPTS LOGOPTIONS(ALWAYS(SURROGAT))
    - Always log all attempts to use shared user ids
- Audit changes to profiles in a class
  - Example: SETROPTS AUDIT(VMMDISK)

Auditing specific users

- Enable UAUDIT in the user's profile (NOUAUDIT to turn off)
  - ALTUSER BRUCE UAUDIT
- The following events are logged:
  - All RACF commands issued by the user
  - All additions, changes, or deletions that the user makes to RACF profiles
  - All attempts that the user makes to access RACF protected resources
- Useful for special situations and users
  - Security sensitive user or application
  - Suspect user (system misuse or exceeding authority)

Auditing CP commands and VM events

- A system event profile defines what to audit.
  - The profile is defined in the VMXEVENT class
- Many things you can choose to audit or not:
  - All CP commands
    - By privilege level if the command has multiple privileges
      - *Example: PURGE has Class A, B, C, D, E, and G versions*
    - Also all SET and QUERY subcommands
  - All Diagnose instructions
  - 17 other special events
    - Communication (IUCV and APPC)
    - Spool files (create, open, delete, print)
    - Maintenance CCWs, Restricted segments, VLAN sniffer mode
    - Commands in the directory
- No VM commands or events are audited by default

Auditing CP commands and VM events

- An event profile also defines RACF control of CP events
  - e.g. CP commands such as LINK, diagnoses, and others
- An AUDITOR can only change the audit controls
- A SPECIAL user cannot change audit controls
  - The SPECIAL user creates the profile and creates the CP controls
  - Gives ALTER permission for the profile to the auditor
  - The auditor creates the audit controls.
- Event profiles can have any name
  - More than one can exist
  - Only one can be active for the system
  - It must be “refreshed” if it is changed

Setup auditing – example

- Example – changing an existing profile named EVENTS1

```
RACF
RALTER VMXEVENT EVENTS1 ADDMEM(DIAG03C/AUDIT DIAG084/AUDIT)
RALTER VMXEVENT EVENTS1 ADDMEM(DISPLAY.C/AUDIT STORE.C/AUDIT)
RALTER VMXEVENT EVENTS1 ADDMEM(SEND.C/AUDIT SET.PASSWORD/AUDIT)
RALTER VMXEVENT EVENTS1 ADDMEM(SET.SECUSER.C/AUDIT)
RALTER VMXEVENT EVENTS1 ADDMEM(SET.SYSOPER/AUDIT LINK/AUDIT)
SETEVENT REFRESH EVENTS1
END
```

To list the settings

- RAC SETEVENT LIST
- RAC RLIST VMXEVENT EVENTS1

Auditing specific users (the sequel)

- Create an event profile that applies only to one user
  - Named USERSEL.*userid*, in the VMXEVENT class
  - Completely overrides system profile for that user
    - So – don't just specify the difference, specify everything
    - CP control settings and audit settings
- You can audit more or less things than the system profile
- Examples
  - Don't audit frequently used functions in trusted machines
  - Do more auditing for an untrusted machine
  - Test changes to proposed system wide audit settings
    - Use SETEVENT REFRESH to enable
    - Use SETEVENT RESET to disable

The RACFSMF user id

- Purpose is to archive the audit data (SMF records)
  - RACFVM actually writes the audit log, not RACFSMF
  - RACFSMF is normally logged off
- How often should you archive the data?
  - Option 1: On a regular schedule
    - Select daily or either weekly or monthly on a certain day
      - *Defined in the PROFILE EXEC on RACFSMF 191*
    - Use automation software to xautolog RACFSMF daily
    - It requests RACFVM to switch log disks
    - Then, it archives the data on the (now) inactive log disk
  - Option 2: Automatically when one log disk is full
    - RACFVM automatically switches to the other disk
    - RACFSMF is started by RACFVM
    - It archives the data on the (now) inactive log disk

Which log option to choose?

- I recommend a regular schedule (option 1)
- RACFSMF started daily
  - Processes log daily, weekly, or monthly
    - Depending on your choice in PROFILE EXEC
    - Sample code is SMFPROF EXEC on RACFVM 305
  - No surprises due to errors or revoked id
  - You must pass the RACF server id as console input data
    - CP XAUTOLOG RACFSMF #RACFVM
- RACFSMF sends messages to the operator
  - Both informational and error messages
- Ensures the inactive log disk is empty
  - Available for RACFVM if active log disk fills up

Managing the audit log disks

- File SMF CONTROL on RACFVM 191
  - Lists the primary and backup audit disks, and which is current
  - RACFVM updates the file when it switches audit disks
  - RACFSMF also reads it so that only the inactive disk is archived
- Note: Be careful if you make changes to this file
  - It is Fixed 100 format – not all of it is visible on an 80 character wide screen
  - Data is dependent on the columns
    - Do not insert or delete any characters – overtype only

Fields in SMF CONTROL

- Fields in SMF CONTROL you can modify
  - CLOSE nnn
    - The number of audit records buffered before they are written to the SMF file.
    - You can specify 000-999; the default value is 001.
    - Increase this if you create a lot of audit records.
  - SEVER NO|YES
    - Default setting is NO
      - do not stop RACFVM even if both SMF log disks are full
    - SEVER YES ensures that no auditable events occur that could not be logged
      - i.e. it there will be no “gaps” in your security log
    - Make sure your automatic log processing is in place before making this YES!

Archived audit data (SMF records)

- Managed by the RACFSMF user id
- Most current archive on RACFSMF 191 as SMF DATA
- Latest and older archived logs on RACFSMF 192
  - Location could be changed in PROFILE EXEC
  - Named SMFnnnnn DATA, where “nnnnn” is the Julian date
    - The filetype could be DATA0001, DATA0002, etc.
- 192 disk free space checked by RACFSMF
  - Can be tailored in PROFILE EXEC
  - Message issued if disk is too full (80% full is the default)
  - Your responsibility to process logs and clean up this disk

Forcing RACF to switch log disks

- What if you want to process current audit data?
- Tell RACFVM to switch to the other log disk
  - CP SMSG RACFVM SMF SWITCH
    - Must be an authorized id in the CSTCONS table
      - See *RACF Security Server System Programmer's Guide*
    - By default, only OPERATOR and RACFSMF allowed
    - The new log disk must be empty or the switch is not performed
  - RACF autologs RACFSMF after the switch
- RACFSMF will find logs on both disks
  - It will automatically archive the inactive one
- You may now process the archived audit data

RACMAINT and SMF logs

- Remember, RACMAINT uses the same disks as RACFVM
  - Same primary and backup database disks
  - Same primary and alternate SMF log disks
  - However – RACMAINT has its own 191 disk
    - Which means a different SMF CONTROL file
- What if RACMAINT is running and not RACFVM?
  - Hopefully this only occurs for short periods
  - Automatic procedures that start RACFSMF would need to specify RACMAINT as the RACF server
    - Otherwise, log switching cannot occur

RACMAINT and RACFSMF

- SMF CONTROL on the RACMAINT 191 disk
  - It may specify a different current log disk than RACFVM!
  - This can create log files on both log disks
- What if RACFSMF runs and finds logs on both disks?
  - RACFSMF archives the inactive one without a log switch

- Better solution:
  - Copy SMF CONTROL from RACFVM 191 to RACMAINT 191
  - Then switch to RACMAINT
  - This could be automated in the PROFILE EXEC on RACMAINT

Reports

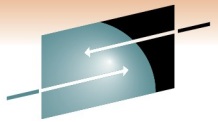
The Data Security Monitor (DSMON)

- A way to verify that the security mechanisms actually in effect are the ones intended
- DSMON reports on the status of your security environment
  - Runs while RACF is active
  - Must be run by the auditor
- Selecting reports in a control file
  - SYSTEM — System report (processor id, RACF level)
  - RACGRP — Group hierarchy report
  - RACCDT — Class descriptor table
  - RACEXT — RACF exits
  - RACGAC — RACF global access table
  - RACUSR — User attributes and user summary
  - RACDST — Data sets report (RACF database)

Running DSMON

- Runs using CST like RACFVM
  - Must link to RACFVM 490 and IPL 490 first
  - Other requirements – see the documentation
    - Chapter 4 of *RACF Security Server Auditor's Guide*
- RACDSMON EXEC invokes the DSMON program
  - Requires Read access to the RACF database
  - The EXEC prompts for all input it needs
  - Uses temporary disk space for its processing
- Create Report selection file
  - Named ICHDSM00 SYSIN
  - Uses an existing one if it exists
- Output is sent to your virtual printer
  - Each report selection is part of the output file

DSMON output



SHARE
Technology · Connections · Results

```
RACF DATA SECURITY MONITOR                                    DATE: 04/01/10  TIME: 14:26:21  PAGE:          2
                                S E L E C T E D    U S E R    A T T R I B U T E    R E P O R T
USERID            ----------------  ATTRIBUTE TYPE  ---------------
                  SPECIAL        OPERATIONS     AUDITOR        REVOKE
-------------------------------------------------------------------------------------------------------------
BLDSEG                           SYSTEM
DIRMAINT          SYSTEM
IBMUSER                                                         SYSTEM
MAINT             SYSTEM         SYSTEM         SYSTEM
RACAUDIT                                        SYSTEM
RACFADM           SYSTEM
```

```
RACF DATA SECURITY MONITOR                                    DATE: 04/01/10  TIME: 14:26:21  PAGE:          4
                              R A C F    C L A S S    D E S C R I P T O R    T A B L E    R E P O R T
CLASS                                                           DEFAULT        OPERATIONS
NAME           STATUS        AUDITING        STATISTICS        UACC           ALLOWED
-------------------------------------------------------------------------------------------------------------
RVARSMBR       INACTIVE        NO               NO             NONE             NO
RACFVARS       INACTIVE        NO               NO             NONE             NO
SECLABEL       INACTIVE        NO               NO             NONE             NO
VMMDISK        ACTIVE          YES              NO             NONE             YES
VMRDR          ACTIVE          NO               NO             NONE             YES
VMCMD          ACTIVE          YES              NO             NONE             YES
VMNODE         INACTIVE        NO               NO             NONE             YES
VMBATCH        ACTIVE          NO               NO             NONE             YES
```

```
RACF DATA SECURITY MONITOR                                    DATE: 04/01/10  TIME: 14:26:21  PAGE:         10
                                    R A C F    G R O U P    T R E E    R E P O R T
LEVEL   GROUP      (OWNER)
-------------------------------------------------------------------------------------------------------------

    1   SYS1       (RACFADM )
        |
    2   | $LINUX
```

Database Unload Utility

- Creates a sequential file from the RACF database
  - It has a side effect of validating profile data in the database
- Not really a “report”, but can input to other processes
  - Upload to a database
  - Write your own utilities
    - Records are labeled with a number
    - Group profiles are 01xx, User profiles are 02xx, Resource profiles are 05xx, etc.
- Unloads all profiles in the database
  - But does not unload every field of every profile
- RACFDBU EXEC runs the IRRDBU00 utility on z/VM
  - Requires a specific setup
  - Read the documentation!
    - Chapter 18 of *RACF Security Server Security Administrator’s Guide*
  - Runs using CST, not CMS

Processing archived SMF data

- RACF SMF Data Unload Utility (RACFADU)
  - Creates a sequential file from the audit data
  - 2 output formats
    - XML format
    - Table (SQL/DS database input format)
- Merge with z/OS data
  - Use the SMFCONV utility to reformat to the z/OS format
  - Send the output file to z/OS

The RACF Report Writer

- Lists information contained in the SMF records
  - Data about successful accesses and warnings
  - Find out attempts to access critical resources
  - Details of user and group activity
  - Summaries of system and resource usage
- It is supported on z/VM
  - Ignore the warning in the documentation that it is not the IBM recommended method
- Output is sent to your virtual printer
- Requires disk space for sort/work area
  - Either your A disk or a temporary disk

Using the Report Writer

- Report options go in RACFRW CONTROL file
  - Example: Produce a listing of all unsuccessful logons and all successful SETROPTS commands

```
RACFRW
SELECT VIOLATIONS
EVENT LOGON
SELECT SUCCESSES
EVENT SETROPTS
LIST
END
```

- Use SELECT and EVENT subcommands to select records
- There are 2 output selections
  - LIST – List all selected records
  - SUMMARY – Output a summary of the selected records

Running the Report Writer

- Access the disk with the SMF DATA file to process
  - Otherwise RACRPORT attempts to access the inactive SMF log disk
    -- which is probably empty
  - The most current SMF archive is on RACFSMF 191
    - VMLINK is the easy way to link it:
    - EXEC VMLINK RACFSMF 191 <* C-X> (NONAMES
    - Disk modes A, B, and Z are used by RACRPORT
- Invoke RACRPORT
  - It will ask you about space for a work file
  - The A disk or a temporary disk can be used
- The output print file is sent to your reader

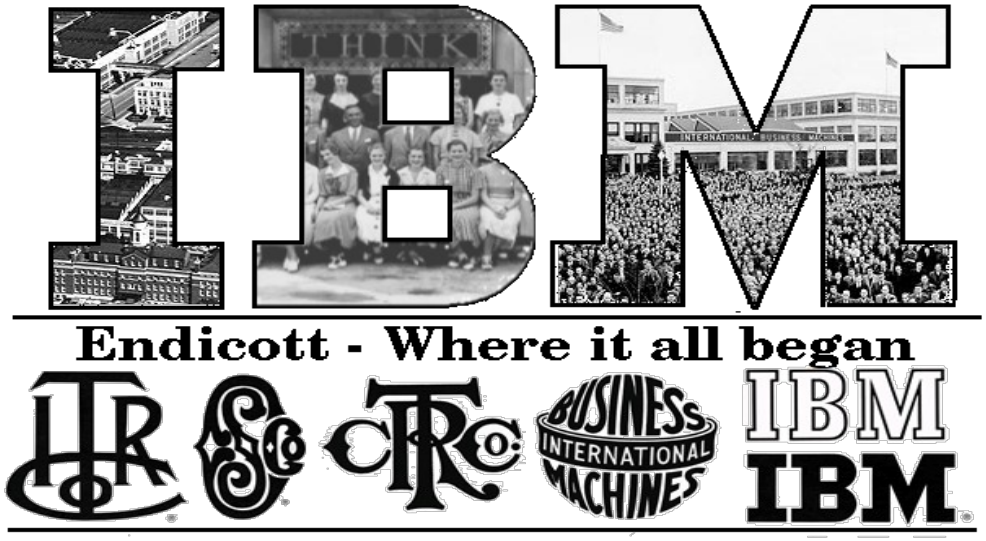
Running the Report Writer

```
vmlink racfsmf 191 <* c-x> (nonames
DMSVML2060I RACFSMF 191 linked as 0121 file mode C
Ready;
racrport
DMSACP723I B (305) R/O
The RACF Report Writer requires Disk Space for a Sort work file.
You may wish to use Tdisk for this function.

Note: If Tdisk is not used, the Sort work file will be written on the A disk.

Do you wish to use Tdisk for the Sort work file?

Please enter YES or NO
no
ENTER RACFRW COMMAND, OR "END"
RACFRW
SELECT VIOLATIONS
EVENT LOGON
SELECT SUCCESSES
EVENT SETROPTS
LIST
END
ICH64003I LISTING REPORT COMPLETE.
RDR FILE xxxx SENT FROM xxxxxxxx PRT
ENTER RACFRW COMMAND, OR "END"
END
Ready;
```

The End

- **Thank you for listening!**
- Session 8481
- **Contact information**

Bruce Hayden
bjhayden@us.ibm.com



References

- **VM home page**
  - http://www.vm.ibm.com
- **z/VM Security and Integrity Resources**
  - http://www.vm.ibm.com/security
- **z/VM Statement of Integrity**
  - http://www.vm.ibm.com/security/zvminteg.html
- **VM documentation center**
  - http://publib.boulder.ibm.com/infocenter/zvm/v6r1/index.jsp

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.
Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.