

Installing RACF for the First Time

For z/VM 5.4 and 6.1

Bruce Hayden

IBM Advanced Technical Skills

August 2, 2010

Session 7733



SHARE in Boston

Introduction to RACF Security Server for z/VM



- A priced, optional, pre-installed feature of z/VM
 - For all current releases - 5.3, 5.4, and 6.1
- Licensed under International Program License Agreement (IPLA) terms and conditions
- Pricing is based on engine-based Value Units and is available for both IFL and standard processor configurations.
- RACF releases are specific to the release of z/VM
 - The level of RACF and CP must be the same

Configuration guidelines

- What RACF options do you enable?
- What needs to be controlled and audited in z/VM?
- Who decides this? You?
- Answer: Not you.

Your company security policy

- It is the overall guideline for IT security in your company
- You decide how RACF is configured based on its requirements
- In other words – you are not the policy maker
 - You implement the policy

Installation

- No need – it is pre-installed!
- But, it is disabled by default
 - You enable it if you have a license
- The program directory is the main guide
 - Please read it!
 - Please follow it!
 - This presentation does not cover all topics
 - More background about configuration in the RACF documentation
 - See *z/VM: RACF Security Server Security Administrator's Guide*
- This presentation is mainly for first time installers
 - But – if you have it already installed, don't leave!
 - There are some choices I make that you may want to do on your system

User ids defined for RACF/VM

These are predefined on your z/VM system

- **RACFVM**
 - The main production service machine
- **RACMAINT**
 - Test the installation of RACF
 - Test applied service
- **5VMRAC40 or 6VMRAC10**
 - Name is derived from the z/VM version and release
 - Used for service and customization of RACF
 - Owns all the minidisks that hold RACF code
 - In this presentation, any reference to 6VMRAC10 can be replaced with 5VMRAC40 for z/VM 5.4 systems
- **RACFSMF**
 - Management of the RACF audit log files

User ids defined for RACF/VM

- **IBMUSER**
 - Used for the initial setup of RACF
- **SYSADMIN**
 - Security administration user
- **MAINT**
 - Maintenance of all z/VM components
- **BLDRACF**
 - Used to rebuild CST, the special version of CMS used by RACF

Overview



- If you will also activate DIRMAINT:
 - I prefer to activate and configure RACF first
- Prepare your system for RACF
 - Use RACF utilities to migrate definitions from the CP directory
- Enable RACF
 - This will create a new CP Nucleus with RACF enabled
- Shutdown and IPL z/VM from parm disk 2
- Start RACF in maintenance mode and initialize
- Configure RACF
- Start RACF in production mode

Prepare your VM directory

- Check your VM directory. Look for:
 - Duplicate user ids, if you have more than one VM system
 - In case you share the RACF database
 - The same user id must be owned by the same person
 - Unacceptable characters in user ids
 - No dash (-), plus (+), colon (:), or underscore (_).
 - Group names on POSIXGROUP statements
 - RACF does not support mixed case group names
 - The RACF utility automatically handles the VM default names
 - ACIGROUP statements
 - If you have these, read the RACF program directory

Prepare your VM directory, continued



- Update user 6VMRAC10
 - Add OPTION LNKNOPAS
 - This will make it easier to activate RACF
- If DIRMAINT will be activated later
 - Change password of NOLOG to a real password
 - Userids: DIRMAINT, DATAMOVE, DIRMSAT
- Consider adding user ids for security roles
 - For example, SYSAUDIT for the system auditor
- Run DIRECTXA to put these changes online

Migrate CP directory data to RACF using RPIDIRCT



- Logon to the 6VMRAC10 user id
 - Access your source CP directory:
 - **VMLINK MAINT 2CC**
 - Access the RACF utilities
 - **ACC 505 E**
- Run RPIDIRCT EXEC to scan the source directory
 - **RPIDIRCT USER DIRECT**
 - Accept the default group ID of “SYS1”
 - Scans CP directory source file, creates RACF commands
- Output file is RPIDIRCT SYSUT1
 - No database changes are made by RPIDIRCT
 - We will examine and edit this file

Editing RPIDIRCT SYSUT1

- You can make alterations to this file
 - Add permissions that are missing
 - Remove permissions that you don't want
 - Alter initial passwords
- RACF commands found in this file
 - ADDUSER - Defines a user to RACF
 - RDEFINE - Defines a resource
 - PERMIT - Allows a user access to a resource
- Resources defined by this file
 - VMMDISK - VM Minidisks
 - VMBATCH - Alternate userid
 - VMRDR - Ability to SPOOL TO the user

Handling of passwords from your user directory



- RPIDIRECT SYSUT1 defines your users to RACF
- User's initial password is the one in their directory entry
 - The passwords are temporary and must be changed at the first logon
 - No special password handling
 - NOLOG users have an initial password of "NOLOG"!
 - However – z/VM prevents logon and spooling to NOLOG users
- Special password processing for directory password of "UNLOG"
 - Defined with password of "UNLOG" and the user is REVOKED
 - A revoked user cannot logon to the system
- Potential problem: What if "NOLOG" is removed from a user's CP directory entry?
 - Anyone could log in using password of NOLOG!
 - We will fix this on a later step... after a small detour

Introduction to Generic resources

- Resources defined by the RPIDIRCT file are specific
 - Owned by a single userid
 - For minidisks – a specific virtual address
 - In RACF terms – a “discrete profile”
- RACF also supports generic resources
 - A lot like wildcard matching of file names
 - Permissions to discrete profiles have priority, however
- Example
 - Define a generic resource which is “all of MAINT's minidisks”
 - `RAC RDEFINE VMMDISK MAINT.* OWNER(MAINT) UACC(NONE)`
 - Give a user read/write access to all of MAINT's disks
 - `RAC PERMIT MAINT.* CL(VMMDISK) ID(MAINT2) AC(CONTROL)`

Generic resources

- Enabled via RACF options (SETROPTS command)
 - GENCMD(*classes*)
 - Allows generic profiles to be specified in commands
 - You can create generic profiles before making them active
 - GENERIC(*classes*)
 - Activates generic profile checking for specified classes
- Not enabled on any classes by default
 - Due to extra searching, and not part of old RACF systems
- This can make managing your system easier!
 - Fewer resources to define and manage
 - Some resources only need controls for the exceptions

Candidates for Generic Resources



- VMRDR (spooling)
 - To send a file to another user, you must be permitted in RACF to “update” their reader
 - i.e. SPOOL PUN TO *user*, SPOOL PRT TO *user*, TRANSFER TO *user*, CLOSE TO *user*
 - Without permission, the command fails
 - A security policy may not require this control for most users
 - Use a generic resource instead of definitions for each user
 - Create specific resources if there are exceptions
 - Example: Service machine that accepts commands via reader files
 - *Deny generic access to everyone by default*
 - *Create specific permissions as needed*

Resources, continued



- VMBATCH (secondary user)
 - These days, mostly used by FTPSERVE, the ftp server
 - Allows FTPSERVE to access your resources on your behalf – e.g. when you “log in” via FTP
 - Instead of giving FTPSERVE explicit permission to your resources
 - FTPSERVE uses Diag D4 to ask CP to set its secondary user to your user id
 - If FTPSERVE has permission from RACF to your VMBATCH resource, it is allowed
 - Maybe a generic resource is a good idea here?
 - Exceptions for critical users such as MAINT can be defined

Now back to RPIDIRCT SYSUT1 !!

- References to VMBATCH and VMRDR in file
 - Use generic resources instead
The actual resources will be defined later
 - Remove the lines that reference VMBATCH and VMRDR from the file
- References to users with a password of NOLOG
 - The utility sets the RACF password to “NOLOG”
 - It is better to not set a password at all
 - Change setting of PASSWORD(NOLOG) to NOPASSWORD
- We will make these changes to the file
 - Now is the best time to do it!
 - If you have AUTOONLY or LBYONLY users – make the same change to NOPASSWORD

Edit RPIDIRCT SYSUT1

- Use XEDIT to make these changes
 - **xedit RPIDIRCT SYSUT1**
 - **case upper ignore**
 - **change /password(nolog)/nopassword/* ***
 - Remove references to vmbatch
 - *top*
 - *all /rdefine vmbatch/*
 - *delete **
 - *top*
 - *all /class(vmbatch)/*
 - *delete **
 - Repeat these commands using **vmrdr** instead of **vmbatch**
 - **file**

Enable the RACFSMF user id

- This id performs SMF processing and archiving
 - SMF is not discussed in this presentation!
 - However, it is easy to set up the id right now, so we will
- A sample PROFILE EXEC is supplied
 - It can be customized for your own needs, or use the default:
 - LINK RACFSMF 191 291 M
 - ACCESS 291 M
 - COPY SMFPROF EXEC E PROFILE EXEC M (REPLACE OLDDATE
 - RELEASE M (DET
- We are done with 6VMRAC10
 - You may now log off

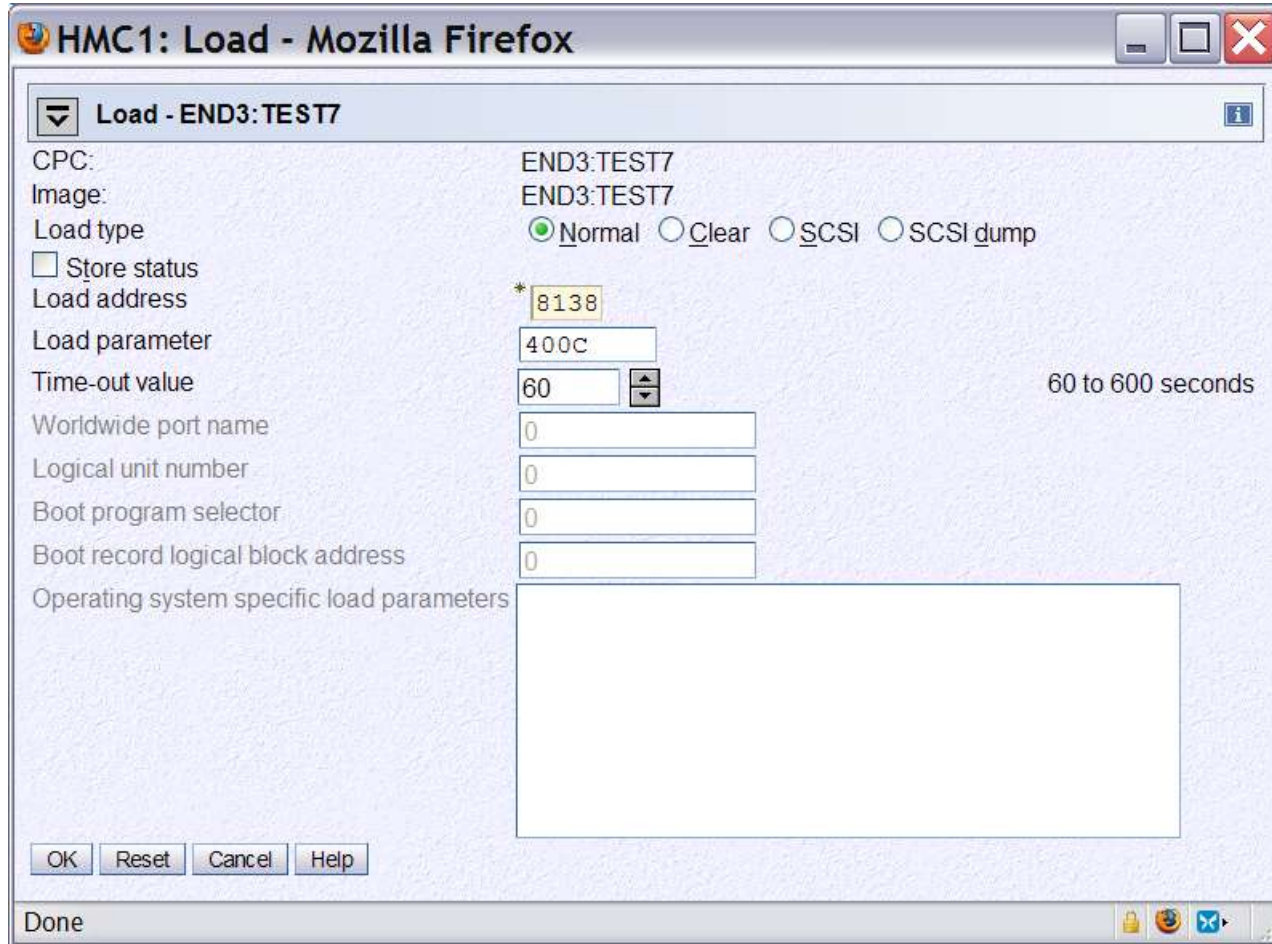
Enable the RACF/VM product

- The RACF product must be enabled
 - Updates to the SYSTEM CONFIG file
- CP must be rebuilt with the RACF modules included
- The SERVICE EXEC does all this for you
 - Log on to MAINT
 - Enter **SERVICE RACF ENABLE**
 - Check for errors with **VMFVIEW SERVICE**
- The rebuilt CP nucleus is ready for testing
 - Placed on the secondary parm disk (MAINT CF2)
 - SYSTEM CONFIG updated to enable RACF/VM on all parm disks

RelPL your system

- IPL using parameter disk 2
 - Shutdown your system
 - Bring up the Load screen on the HMC
 - Specify the address of the IPL volume
 - Specify a console address to show the stand alone loader
 - *This is the Load Parm*
 - *Use SYSG to use the integrated 3270 HMC console*
 - When the Standalone Loader screen appears
 - Change the “Extent” to 2
 - Specify a load parm of PROMPT
 - Optionally specify a console address
 - Press PF10 to load

Sample Load screen



The screenshot shows a web browser window titled "HMC1: Load - Mozilla Firefox". The main content area is titled "Load - END3:TEST7" and contains the following configuration options:

CPC:	END3:TEST7
Image:	END3:TEST7
Load type	<input checked="" type="radio"/> Normal <input type="radio"/> Clear <input type="radio"/> SCSI <input type="radio"/> SCSI_dump
<input type="checkbox"/> Store status	
Load address	* 8138
Load parameter	400C
Time-out value	60 <input type="button" value="▲"/> <input type="button" value="▼"/> 60 to 600 seconds
Worldwide port name	0
Logical unit number	0
Boot program selector	0
Boot record logical block address	0
Operating system specific load parameters	

At the bottom of the form are buttons for "OK", "Reset", "Cancel", and "Help". The status bar at the very bottom of the browser window displays "Done" and several system icons.

Sample Standalone Loader screen

```
z/VM [24 x 80]
STAND ALONE PROGRAM LOADER: z/VM VERSION 6 RELEASE 1.0

DEVICE NUMBER:  8138      MINIDISK OFFSET:  00000000  EXTENT:  2
MODULE NAME:    CLOAD     LOAD ORIGIN:    2000

-----IPL PARAMETERS-----
prompt_

-----COMMENTS-----

9= FILELIST  10= LOAD  11= TOGGLE EXTENT/OFFSET

MR h 08/007
```

Sample VM startup

```
z/VM [24 x 80]
10:41:22 z/VM V6 R1.0 SERVICE LEVEL 0901 (64-BIT)
10:41:23 SYSTEM NUCLEUS CREATED ON 2010-02-22 AT 10:05:47, LOADED FROM 610RES
10:41:23
10:41:23 *****
10:41:23 * LICENSED MATERIALS - PROPERTY OF IBM* *
10:41:23 * *
10:41:23 * 5741-A07 (C) COPYRIGHT IBM CORP. 1983, 2009. ALL RIGHTS *
10:41:23 * RESERVED. US GOVERNMENT USERS RESTRICTED RIGHTS - USE, *
10:41:23 * DUPLICATION OR DISCLOSURE RESTRICTED BY GSA ADP SCHEDULE *
10:41:23 * CONTRACT WITH IBM CORP. *
10:41:23 * *
10:41:23 * * TRADEMARK OF INTERNATIONAL BUSINESS MACHINES. *
10:41:23 *****
10:41:23
10:41:23 HCPZC06718I Using parm disk 2 on volume 610RES (device 8138).
10:41:23 HCPZC06718I Parm disk resides on cylinders 159 through 278.
10:41:23 Start ((Warm|Force|COLD|CLEAN) (DRain) (DISable) (NODIRect)
10:41:23 (NOAUTolog)) or (SHUTDOWN)

warm noautolog_

CP READ ZVMV6R10
MA h 23/015
```


Sample VM startup - continued

```
z/VM [24 x 80]
10:42:07 WARM NOAUTOLOG
10:42:07 NOW 10:42:07 EST MONDAY 2010-02-22
10:42:07 Change TOD clock (Yes|No)
10:42:08 NO
10:42:08 The directory on volume 610RES at address 8138 has been brought online.
10:42:10 HCPWRS2513I
10:42:10 HCPWRS2513I Spool files available          44
10:42:11 HCPWRS2512I Spooling initialization is complete.
10:42:11 DASD 8139 dump unit CP IPL pages 21220
10:42:11 HCPAAU2700I System gateway ZVMV6R10 identified.
10:42:13 z/VM Version 6 Release 1.0, Service Level 0901 (64-bit),
10:42:13 built on IBM Virtualization Technology
10:42:13 There is no logmsg data
10:42:13 FILES:   NO RDR, 0004 PRT,   NO PUN
10:42:13 LOGON AT 10:42:13 EST MONDAY 02/22/10
10:42:13 GRAF 400C LOGON AS OPERATOR USERS = 1
10:42:13 HCPIOP952I 3G system storage
10:42:13 FILES: 0000011 RDR, 0000005 PRT,   NO PUN
10:42:13 HCPCRC8082I Accounting records are accumulating for userid DISKACNT.
10:42:13 HCPCRC8082I EREP records are accumulating for userid EREP.

xautolog racmaint_

RUNNING  ZVMV6R10
MA h 23/018
```

Start up VM

- At the startup prompt, enter:
 - **WARM NOAUTOLOG**
 - This prevents any other guests from starting
- Once the system is up, enter:
 - **XAUTOLOG RACMAINT**
- RACF is now started with its initial database
 - A small set of basic profiles
- Disconnect from the Operator
 - **DISC**

Initialize the RACF database

- Only user IBMUSER is defined
 - User has full RACF authority
 - Links to 6VMRAC10 191, to read RPIDIRECT SYSUT1
 - We use this to build the database
- Logon to IBMUSER
 - Password is SYS1 and expired, you will have to change it
 - Enter *newpass/newpass* when prompted
 - Ignore any error messages from RACF

Load the initial RACF Database

- Access the RACF code disks
 - **ACCESS 305 C**
 - This is 6VMRAC10 505 – Test code for server
 - **ACCESS 192 B**
 - This is 6VMRAC10 191 – Contains RPIDIRCT SYSUT1
 - **ACCESS 29E D**
 - This is 6VMRAC10 29E – Test code for general users
- Run RPIBLDDS
 - This reads RPIDIRCT SYSUT1 B
 - Enter: **RPIBLDDS RPIDIRCT**
 - Clear the screen several times
- Your database is initialized!

Define the security administrator and auditor



- Best practice is to separate these duties
 - Administrator: SYSADMIN
 - Included in the initial z/VM directory for this role
 - Auditor: SYSAUDIT, RACAUDIT, or AUDITOR
 - Note:
AUDITOR exists in the initial z/VM directory, but is intended to run the AUDITOR monitoring code. One of the others would have to be added.
- This can easily be changed later on
- The role of MAINT is to maintain the RACF/VM code
 - And of course, the other components of z/VM

IBMUSER, again

- Define the roles to RACF
 - Note: Using a RACF command session started with the RACF command
- RACF
 - ALTUSER SYSADMIN SPECIAL
 - ALTUSER SYSAUDIT AUDITOR
 - ALTUSER MAINT OPERATIONS
 - ALTUSER BLDSEG OPERATIONS
- END
 - User BLDSEG is part of the service process
- We are now done with IBMUSER
 - LOGOFF from this id

Revoke access to IBMUSER

- IBMUSER has no further purpose
 - But this id cannot be deleted from the RACF database
- Log on to your security administrator id
 - **LOGON SYSADMIN**
 - You will have to set a new password during logon
 - **LINK 6VMRAC10 29E 29E RR**
 - **ACCESS 29E D**
 - The RACF code is not on the production Y disk yet
- Make IBMUSER unusable
 - Note: Using the RAC command to enter a single RACF command
 - **RAC ALTUSER IBMUSER REVOKE**
 - **RAC ALTUSER IBMUSER NOOPERATIONS NOSPECIAL**

Setting RACF options

- The SETROPTS command sets RACF options
 - There are a lot of options!
- Most resource classes are inactive until activated
 - The CLASSACT subcommand of SETROPTS activates classes
 - RAC SETROPTS CLASSACT(class)
- Some classes are always active
 - USER (allows LOGON and XAUTOLOG commands)
 - TERMINAL (allows you to login via a terminal)
- The next chart lists some of the classes
 - The complete list is in Appendix B of the Language Reference

Most common classes

VMBATCH	Allows use of DIAG D4 (alternate userid)
VMCMD	Certain CP commands and other requests
VMLAN	Permission to connect to VSWITCH and Guest LANs
VMMDISK	Minidisks
VMNODE	Allows you to target other VM nodes via RSCS
VMRDR	Allows you to target other users via spooling commands
VMSEGMT	Allows access to restricted saved segments
VMXEVENT	Event profiles for commands and auditing
FACILITY	Allows a virtual machine to use the RACROUTE interface.

Activating classes

- The classes I need active on my system are:
VMMDISK, VMLAN, VMCMD, VMRDR, VMBATCH
 - `RAC SETROPTS CLASSACT(VMMDISK VMLAN VMCMD VMRDR VMBATCH)`
 - I will activate VMXEVENT and FACILITY also later on
- VMCMD, VMRDR and VMBATCH are discussed later
- VMMDISK resources were created via the RPIDIRECT file
- VMLAN resources control connections to a vswitch
 - A resource must be created for each one and permissions granted
 - Examples:
 - `RDEFINE VMLAN SYSTEM.VSWITCH1 UACC(NONE)`
 - `PERMIT SYSTEM.VSWITCH1 CL(VMLAN) ID(TCPIP) AC(UPDATE)`
 - `PERMIT SYSTEM.VSWITCH1 CL(VMLAN) ID(LINUX1) AC(UPDATE)`
 - Note that VMLAN resources also apply to restricted guest lans

VMCMD class

Resources protected by the VMCMD class



VMCMD Profile Name	What It Protects
STORE.C	STORE HOST command
TRSOURCE	TRSOURCE command
DIAG0E4	Diagnose code X'E4' (Minidisk query and define)
XAUTOLOG. <i>userid</i>	XAUTOLOG command by a class G user
DIAG088	Diagnose code X'88' (all subcodes) (DMSPASS)
DIAG0A0.HRTSTORE	Diagnose code X'A0' Subcode X'34' (security labels)
DIAG0A0.QUERYSEC	Diagnose code X'A0' Subcode X'30' (query label)
DIAG0A0.VALIDATE	Diagnose code X'A0' Subcodes X'04' and X'3C' (Validate userid and password or pass phrase)
RAC	RAC command processor
RACF	RACF command session

VMCMD examples

- No VMCMD resources are defined by default
 - Exception: RAC and RACF commands are UACC(READ)
 - Anyone is allowed to use them
 - The default settings defer permission checking to CP
 - CP uses directory entries or privilege classes for permission
- To protect a command, define its resource and then give permission
 - Example: protecting STORE HOST
 - *RDEFINE VMCMD STORE.C UACC(NONE)*
 - Allow MAINT to use this command
 - *PERMIT STORE.C CLASS(VMCMD) ID(MAINT) ACCESS(READ)*
 - Example: allow a general user to use XAUTOLOG
 - *RDEFINE VMCMD XAUTOLOG.LINUX UACC(NONE)*
 - *PERMIT XAUTOLOG.LINUX CLASS(VMCMD) ID(BRUCE) AC(READ)*

Using RACF to allow DIAG 88 for TCPIP servers



- Create DIAG088 resource in VMCMD class
 - `RAC RDEFINE VMCMD DIAG088 UACC(NONE)`
- Give servers permission to perform password validation using the CMS facility DMSPASS
 - `RAC PERMIT DIAG088 CLASS(VMCMD) ID(FTPSEVE IMAP VMNFS REXECD) ACCESS(READ)`
- Allow servers to use RACROUTE
Permission to use RACROUTE is resource name ICHCONN in class FACILITY
 - `RAC SETROPTS CLASSACT(FACILITY)`
 - `RAC RDEFINE FACILITY ICHCONN UACC(NONE)`
 - `RAC PERMIT ICHCONN CLASS(FACILITY) ID(FTPSEVE VMNFS REXECD) ACCESS(UPDATE)`
- You must also read:
Appendix A of “TCP/IP Planning and Customization”

Defining Generic resources for some classes

- Use for VMRDR and VMBATCH
 - RACF
 - SETROPTS CLASSACT(VMRDR VMBATCH)
 - SETROPTS GENCMD(VMRDR VMBATCH)
 - SETROPTS GENERIC(VMRDR VMBATCH)
 - END
- VMRDR – permit access to all virtual readers
 - RAC RDEFINE VMRDR * UACC(UPDATE)
 - *Makes default permission “update”, which allows access*
- VMBATCH – allow some servers to act for others
 - RAC RDEFINE VMBATCH * UACC(NONE)
 - *Default permission defined as no access*
 - RAC PERMIT * CLASS(VMBATCH) ID(FTPSEIVE VMNFS REXECD) ACCESS (CONTROL)
 - *Allow FTPSEIVE, VMNFS, and REXECD to act on behalf of any user*

Defining exceptions to generic resources (examples)



Remember that a discrete profile overrides a generic one

- Restrict reader access to a service machine
 - Define the resource with no default access allowed
 - `RAC RDEFINE VMRDR OPERATOR UACC(NONE)`
 - Allow an authorized user to send files
 - `RAC PERMIT OPERATOR CL(VMRDR) ID(PERFSVM) AC(UPDATE)`
- Restrict FTP server's access to MAINT's resources
 - A discrete permission (permit) overrides a generic permission or universal access (UACC)
 - An access permission of NONE overrides any higher permission
 - `RAC RDEFINE VMBATCH MAINT UACC(NONE)`
 - `RAC PERMIT MAINT CLASS(VMBATCH) ID(FTPSEVE) ACCESS(NONE)`

Define your password rules

- SETROPTS PASSWORD(*options*)
 - Many options to chose from
 - Reuse of old passwords (HISTORY)
 - Maximum time before change (INTERVAL)
 - Mixed case allowed (MIXEDCASE)
 - Number of guesses (REVOKE)
 - Expiration warning messages (WARNING)
 - Password syntax rules (RULE)
 - Example: 90 day interval, 4 attempts, no repeat on last 4 passwords

RAC SETROPTS

PASSWORD(INTERVAL(90) HISTORY(4) REVOKE(4) NORULES)

Creating event profiles



- To change the VM events checked by RACF, you must create an event profile
- The profiles have a dual purpose
 - Access checking
 - Auditing (not discussed here)
- Create a resource profile in the VMXEVENT class
 - The name can be anything you choose
 - More than 1 system profile can exist, but only 1 is active
 - Members are added to stop control of selected events
 - By default, all events are controlled

Authorization Checking for z/VM Events



- VM may call RACF for authorization checking of certain z/VM events
- You may not require checking of some of these
 - It depends on your company security policy!
- Event profiles define the authorization checks
 - Profile for the entire system
 - Profiles for individual users (overrides system profile)
- By default, RACF checks all of these events
 - Listed on the next 2 charts

List of controlled events

COUPLE.G	Couple to restricted guest lan or VSWITCH
FOR.C	FOR command, IBMclass C
FOR.G	FOR command, IBMclass G
LINK	LINK command or directory statement
MDISK	Directory statement or LINK to own minidisk
STORE.C	STORE host memory command, IBMclass C
TAG	TAG command, for RSCS processing
TRANSFER.D	TRANSFER and CHANGE, IBMclass D
TRANSFER.G	IBMclass G spooling commands
TRSOURCE	TRSOURCE command

List of controlled events, continued

APPCWVL	Used to verify passwords on APPC connect
DIAG088	Use of Diag 88 (Check auth and link minidisk)
DIAG0A0	Use of Diag A0 (Obtain ACI Groupname)
DIAG0D4	Use of Diag D4 (Set Alternate User ID)
DIAG0E4	Use of Diag E4 (Define Full-Pack Overlay)
DIAG280	Use of Diag 280 (Set POSIX security values)
RSTDSEG	Access to restricted saved segments

Resource profile for my system



- An example based on my needs for a lab system
 - Note: Not based on IBM security policy!
- I want RACF control of everything, except:
 - FOR command
 - Controlled by the SURROGAT profile. I only want to use SURROGAT for logon to shared user ids
 - TAG command
 - I have no restrictions on RSCS file transfers, no need to control TAG
 - Restricted segments
 - I will use the NAMESAVE authorization in the directory, not RACF
 - User's own minidisks (in directory or via link command)
 - If it is yours, then no need for RACF to check your own access

RACF commands for my profile

- Create profile EVENTS1 in VMXEVENT

RACF

```
RDEFINE VMXEVENT EVENTS1
```

```
RALTER VMXEVENT EVENTS1 ADDMEM(FOR.C/NOCTL)
```

```
RALTER VMXEVENT EVENTS1 ADDMEM(FOR.G/NOCTL)
```

```
RALTER VMXEVENT EVENTS1 ADDMEM(TAG/NOCTL)
```

```
RALTER VMXEVENT EVENTS1 ADDMEM(RSTDSEG/NOCTL)
```

```
RALTER VMXEVENT EVENTS1 ADDMEM(MDISK/NOCTL)
```

```
SETROPTS CLASSACT(VMXEVENT)
```

```
SETEVENT REFRESH EVENTS1
```

END

Output from creating an event profile

- When profile is activated, default members are made active

```
SETEVENT REFRESH EVENTS1
RPISET113W TURNING CONTROL ON AUTOMATICALLY FOR: COUPLE
RPISET113W TURNING CONTROL ON AUTOMATICALLY FOR: LINK
RPISET113W TURNING CONTROL ON AUTOMATICALLY FOR: STORE.C
RPISET113W TURNING CONTROL ON AUTOMATICALLY FOR: TRANSFER.D
RPISET113W TURNING CONTROL ON AUTOMATICALLY FOR: TRANSFER.G
RPISET113W TURNING CONTROL ON AUTOMATICALLY FOR: TRSOURCE
RPISET113W TURNING CONTROL ON AUTOMATICALLY FOR: DIAG088
RPISET113W TURNING CONTROL ON AUTOMATICALLY FOR: DIAG0A0
RPISET113W TURNING CONTROL ON AUTOMATICALLY FOR: DIAG0D4
RPISET113W TURNING CONTROL ON AUTOMATICALLY FOR: DIAG0E4
RPISET113W TURNING CONTROL ON AUTOMATICALLY FOR: DIAG280
RPISET113W TURNING CONTROL ON AUTOMATICALLY FOR: DIAG290
RPISET113W TURNING CONTROL ON AUTOMATICALLY FOR: APPCPWVL
RPISET126I SETEVENT COMPLETED SUCCESSFULLY.
```

- You can explicitly define these members in the profile for completeness

```
RALTER VMXEVENT EVENTS1 ADDMEM(COUPLE.G/CTL LINK/CTL)
```

Event profiles for specific users

- Profiles can be created to override the system profile for specific users
 - They are named `USERSEL.userid` in the VMXEVENT class
- If a user profile exists, none of the system profile is used for that user
 - Make sure you create a complete user profile
- They are created just like the system profile
 - `RAC RDEFINE VMXEVENT USERSEL.DATAMOVE`
 - `RAC RALTER VMXEVENT USERSEL.DATAMOVE
ADDMEM(LINK/NOCTL TAG/NOCTL MDISK/NOCTL)`
 - `RAC SETEVENT REFRESH USERSEL.DATAMOVE`
 - etc.

Copy RACF files to production

- The initial configuration of RACF/VM is complete
 - Now we will put the code on the production disks
- Logon to MAINT
- Run **PUT2PROD**
 - Copies RACF code to production disks
 - This includes code to MAINT 19E for the user interface
 - *Also known as the “Y disk”*
 - Updates CP Parm disk 1 (MAINT CF1) from CP Parm disk 2
 - Copies the RACF enabled CLOAD MODULE from parm disk 2
 - Check for errors when it completes
 - **VMFVIEW PUT2PROD**
- **LOGOFF** of MAINT

Initialize RACFVM

- Reconnect to OPERATOR
 - This task must be done from the OPERATOR user id
- Stop all RACF maintenance ids
 - Probably only RACMAINT is running, but just to be sure:
 - FORCE 6VMRAC10
 - FORCE MAINT
 - FORCE RACMAINT
- Start up the production RACF server
 - XAUTOLOG RACFVM
 - This will also XAUTOLOG AUTOLOG2 (see next page)
- Disconnect from OPERATOR

Set up AUTOLOG1 and 2 user ids

- AUTOLOG1 is started as part of the z/VM IPL sequence
 - This is the z/VM default configuration
 - The PROFILE EXEC is used to execute CP commands
 - Perform any system wide CP settings here (Class A commands)
 - We need RACFVM started before any other users
 - *CP XAUTOLOG RACFVM*
 - *CP LOGOFF*
- RACFVM initializes and connects to CP
 - When it is running, it executes XAUTOLOG AUTOLOG2
- AUTOLOG2 will XAUTOLOG all other SVMs
 - Basically, the SVM start ups previously done by AUTOLOG1
- Copy PROFILE EXEC from AUTOLOG1 to AUTOLOG2
- Change AUTOLOG1 to only start RACFVM

RACF/VM is now operational

- You may start service machines for testing
 - To start all of them, just XAUTOLOG AUTOLOG2
 - Determine if any need access to additional resources
- Your last IPL was from the second parm disk
 - The PUT2PROD process has now updated parm disk 1
 - CPLOAD MODULE and SYSTEM CONFIG
 - It would be a good idea to test a normal system IPL using parameter disk 1
 - On OPERATOR:
 - SHUTDOWN REIPL EXTENT 1

Other tasks

- How to define a new user
 - `ADDUSER userid NAME('A. User') PASSWORD(password)`
 - Password is expired, must be changed during logon
- How to reset a user's password:
 - `RAC ALTUSER BRUCE PASSWORD(TEMP4YOU)`
 - Password is expired, must be changed during the next logon
- How to delete various things:
 - Users: `DELUSER userid`
 - This does not delete resources owned by the user!
 - Resources: `RDELETE resourcename`
 - Any permissions to the resource are deleted also
 - Permissions: `PERMIT DELETE`
- Changing resources
 - Use the `RALTER` command

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>

The End

- Thank you for listening!
- Contact information

Bruce Hayden
bjhayden@us.ibm.com



IBM System z Advanced Technical Skills
Washington Systems Center
Endicott, NY



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®, System z10®, 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.

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.

Pricing subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.