RACF for VM Overview

SHARE 2008 Orlando
Session 5524

Bruce Wells
IBM Security Server Design and Development
brwells@us.ibm.com

Disclaimer

The information contained in this document is distributed on as "as is" basis, without any warranty either express or implied. The customer is responsible for use of this information and/or implementation of any techniques mentioned. IBM has reviewed the information for accuracy, but there is no guarantee that a customer using the information or techniques will obtain the same or similar results in its own operational environment.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used. Functionally equivalent programs that do not infringe IBM's intellectual property rights may be used instead. Any performance data contained in this document was determined in a controlled environment and therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environment.

It is possible that this material may contain references to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM Products, programming or services in your country.

IBM retains the title to the copyright in this paper as well as title to the copyright in all underlying works. IBM retains the right to make derivative works and to republish and distribute this paper to whomever it chooses.

Trademarks

- The following are trademarks or registered trademarks of the International Business Machines Corporation:
  - IBM
  - RACF
  - z/OS
  - z/VM
  - zSeries
- UNIX is a registered trademark in the United States and other countries licensed exclusively through The Open Group.
- LINUX is a registered trademark of Linus Torvalds.
- All other products may be trademarks or registered trademarks of their respective companies

Agenda

- z/VM system integrity
- z/VM native security
- RACF for z/VM history and overview
- Survey of features and functions
- New in z/VM 5.3

z/VM system integrity

- The ability of the Control Program (CP) to operate without interference or harm, intentional or not, from the guest virtual machines
- The inability of a virtual machine to circumvent system security features and access controls
- The ability of CP to protect virtual machines from each other
- z/VM is the only virtualization technology on the market that provides not one, but **two** levels of hardware support for virtualization.
  - LPAR, and interpretive execution facility (SIE instruction)

Interpretive Execution Facility

- Start Interpretive Execution (SIE) instruction describes a virtual machine
  - Registers, PSWs, memory
  - Interception conditions (a.k.a. "SIE break")
    - Time slice expires
    - Unassisted I/O
    - Instructions that require CP's help
      - e.g. Set Clock
  - Certain program interrupts
- SIE runs until interception condition raised
- Basis for LPAR and virtual machines

IBM Commitment

- Continued investment
  - Built on almost 40 years of previous investment
- Prompt response to incidents reported to the IBM Support Center
- No public disclosure of IBM System z vulnerabilities
  - May disclose to individuals or groups that have demonstrated to IBM a legitimate need to know
  - ResourceLink provides access to more information
- Commitment published in z/VM General Information manual

What is z/VM System Security

- Authentication: Knowing who is accessing the system or its resources
- Authorization: Ensuring that a user has access only to system resources specifically permitted
- Audit: Knowing who has actually accessed (or failed to access) what resources
- Security is only meaningful in the presence of system integrity!
  - Integrity prevents bypass of security controls
  - Audit trail confirms conformance

Authentication

- Based on three basic forms
  - **What you know: password**
  - **What you have: security gadget, private key**
  - **Who you are: biometrics**
- VM uses “What you know” to establish your identity
- Others often used at network or access point boundaries so as to create combinations which provide more security

Authorization

- Authorization is based on
  - Who you are: your VM user ID
    - Unix UID/GID
    - privilege class
    - directory authorizations
    - ESM access control list
  - What you know: a password
    - If minidisks not protected by ESM

Audit

- CP “journal” records are part of the CP accounting record stream
  - Can audit LOGON, AUTOLOG, XAUTOLOG and LINK
  - Real-time alerts and user/terminal lockout
- Not really very useful as an audit trail
  - No other commands
  - No diagnose instructions

The CP Directory

- z/VM’s native user registry
- Contains user account information
  - Password, Minidisk definitions, privilege class, devices, authorities, virtual machine size, etc
- Must exist even when ESM is installed
  - Some ESM decisions override directory authorization mechanisms
  - z/VM system management APIs make updates in both the CP directory and in the ESM
- RPIDIRCT EXEC can prime RACF with definitions from the CP directory

The CP Directory – sample entry

```
USER RACFU01  MYPWD 100M   100M      G
  INCLUDE  TESTUSER
  OPTION DIAG88
  NAMESAVE GCS
  IUCV     ANY
  OPTION LNKSTABL LNKEXCLU
  OPTION DEVMAINT DEVINFO
  POSIXINFO UID 32 GID 1
  POSIXINFO FSROOT '/../VMBFS:RESEARCH:BFSTEST/'
  POSIXINFO IWDIR /u/RACFU01
  POSIXINFO IUPGM /bin/sh
  CONSOLE  009 3215 T IBMUSER
  LINK     MAINT    19C    19C    RR
  MDISK 191  3380   1000   50     U01DSK MR READ WRITE MULTI
```

*Stuff in bold can be overridden by RACF

CP Privilege Class

- CP commands and functions classified according to general scope
  - A - System operator
  - B - Real device management
  - C - System programmer
  - D - Spooling operator
  - E - Systems analyst
  - F - Service representative (CE)
  - G - General user
  - H - Reserved for IBM
  - Any
- Customer can use I-Z and 1-6

CP Privilege Class …

- Each user is assigned one or more privilege classes
  - usually give everyone class G
  - plus others only as needed
  - system operator usually has class A, B, and D
- User with class A, B, or C has the ability to bypass system integrity and security controls
- Customer can alter CP command privilege classes
- External Security Manager can audit all privileged commands and limit use to specific individuals

External Security Manager

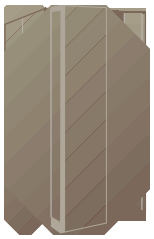
- Enhances auditing, authentication, and access controls
- Encrypt user passwords, or password substitutes
- Use Access Control List for minidisks instead of minidisk password
- Well-defined programming interfaces
  - RACROUTE macro
  - CSL routines
- RACF is a feature of z/VM

Elements of RACF for z/VM

Users
User identification and authentication

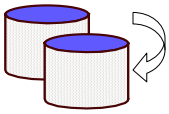
Resources

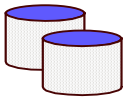
Resource and System access controls

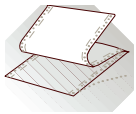


Security administration

Audit trail







Audit and Integrity reports

RACF database
- Primary and secondary
- Local sharing

Security console
- Violation reporting
- OPERATOR

History

- **September 1984** RACF/VM PRPQ
  - Based on RACF 1.6
- **December, 1985** RACF/VM PRPQ based on RACF/MVS 1.7
- **December, 1986** Version 1 Release 7.1
  - Improved installability
  - Documentation re-write
- **March, 1988** Version 1 Release 8
  - DSMON for VM
  - Dual registration
- **December, 1988** Version 1 Release 8.2
  - Enhanced VM event auditing
  - Limited function RACROUTE
  - Placed on the EPL by the NCSC at a C2 level of trust

History …

- **September, 1990** Version 1 Release 9
  - Support for mandatory access control policies
  - Full function RACROUTE
  - Tailorable command interface
  - RACF DB Unload (June, 1992)
- **September, 1992** Version 1 Release 9.2
  - Security label support
  - Multiple RACF service machines
  - Enhanced auditing
  - Expanded number of general resource classes
  - Enhanced DIAG X'A0' privilege checking and auditing
- **1993** – APAR VM56690: Secure Signon SPE (PassTickets)
- **1993** – APAR VM57305: LOGON BY SPE

History …

- **April 1996** Version 1 Release 10 for VM
  - OpenExtensions support
  - Shared file system (SFS) support
  - Use VMSES/E for simplified product installation and service
  - SMF data unload
- **July, 2004** – APAR VM63452: Guest LAN support
- **October, 2005** – APAR VM63750: Guest LAN sniffer support
- **June, 2007** - **z/VM RACF Security Server feature FL530!!!!**
  - RACF 1.10 was withdrawn from marketing in March '07, but remains in service until April '09 for z/VM 5.2 only.

Functions common between RACF for z/VM and z/OS

- **USER, GROUP, general resource profiles**
- **Familiar set of commands and ISPF panels**
- **Protected system access**
- **Access control based user identification and resource access definition**
- **Real-time violation notification**
- **RACF database and reporting utilities. E.G.**
  - **Unloaded image of RACF data base for analysis and reporting**
  - **Unloaded image of SMF (audit) records for analysis and reporting**
  - **Data security and integrity monitor (DSMON)**
- **Class Descriptor Table with ability to define installation resource classes**
- **RACROUTE application interface**

RACF Administrative Commands

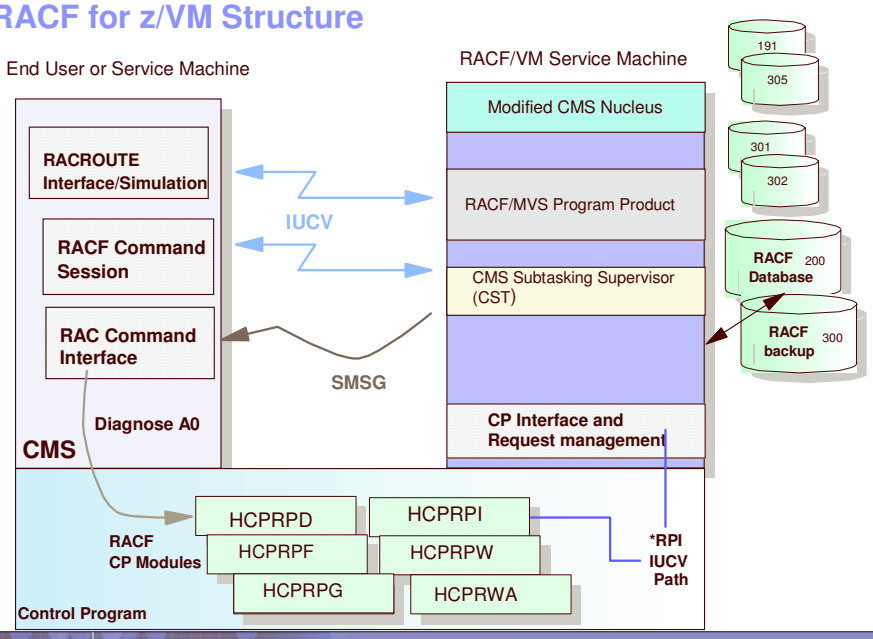
Function	User	Group	Resource
Create	ADDUSER	ADDGROUP	RDEFINE
Change	ALTUSER	ALTGROUP	RALTER
Delete	DELUSER	DELGROUP	RDELETE
Display	LISTUSER	LISTGROUP	RLIST

- PASSWORD
  - Change password or change interval
- PERMIT
  - Modify resource ACL
- SEARCH
  - Scan RACF database
- CONNECT
  - Associate user with a group
- REMOVE
  - Undo Connect
- SETROPTS
  - Control RACF processing
- SETEVENT
  - Modify VM events that are to be audited or controlled
- SETRACF
  - Turn RACF on or off
- SMF
  - Switch disks, or restart auditing
- RVARY
  - Deactivate RACF database

Issuing RACF Commands on z/VM using RAC

- Prefix RACF command with “RAC”
  - RAC LISTUSER BRUCE
- Output of command displayed, and also written to RACF DATA file on 191 disk
- Can modify some behavior of RAC using global variables
- Can support alternative command syntax, and output format using REXX execs
- Exit point in RACF service machine to code user restrictions

RACF for z/VM Structure



RACF control of z/VM Commands and Diagnoses

- Controlled by the SETEVENT command, and profiles in the VMXEVENT class
- The member list of a VMXEVENT profile specifies which CP functions are audited, and which are controlled
  - All CP command and diagnoses are auditable. None are audited by default
  - A subset of CP functions are controllable, as defined by z/VM. All are controlled by default. If a function is not controlled, authorization is determined by CP directory
  - Separation of duties: SPECIAL defines control policy, AUDITOR defines auditing policy
- SETEVENT REFRESH is used to alter the settings in CP
- SETEVENT LIST shows which functions are being audited and controlled
- VMXEVENT profiles can be defined at an individual user level to override system-wide settings (e.g. turn off control for high-volume events initiated by a trusted service machine)

Control of z/VM Commands and Diagnoses…

- When a function is controlled using VMXEVENT, CP calls RACF to authorize a request when that function is used
- At this point, RACF protection is handled by:
  - Defining RACF profiles which provide the security definition of the protected resource
  - Activating the appropriate RACF class
  - Using the same commands as is done on z/OS
- When a function is audited using VMXEVENT, CP calls RACF to write an SMF Type 80 record in the SMF DATA file

SETEVENT LIST sample output

```
PRE-LOGON COMMANDS

COMMAND              CONFIGURED IN
-------              -------------
DIAL                        YES
MESSAGE.ANY                 YES
UNDIAL                      YES


CONTROLLABLE VM EVENTS

VM EVENT                     STATUS     VM EVENT                     STATUS
--------                     ------     --------                     ------
COUPLE.G                     CONTROL    FOR.C                        CONTROL
FOR.G                        CONTROL    LINK                         CONTROL
STORE.C                      CONTROL    TAG                          CONTROL
TRANSFER.D                   CONTROL    TRANSFER.G                   CONTROL
TRSOURCE                     CONTROL    DIAG088                      CONTROL
DIAG0A0                      CONTROL    DIAG0D4                      CONTROL
DIAG0E4                      CONTROL    DIAG280                      CONTROL
DIAG290                      CONTROL    APPCPWVL                     CONTROL
MDISK                        CONTROL    RSTDSEG                      CONTROL


AUDITABLE VM EVENTS

VM EVENT                     STATUS     VM EVENT                     STATUS
--------                     ------     --------                     ------
ACNT                         NO_AUDIT   ACTIVATE                     NO_AUDIT
ADJUNCT                      NO_AUDIT   ADSTOP                       NO_AUDIT
ASSOCIATE                    NO_AUDIT   ATTACH                       NO_AUDIT
. . .                        . . .      ...                          ...
RPISET126I SETEVENT COMPLETED SUCCESSFULLY.
```


Example – protecting a minidisk

- **RDEFINE VMMDISK BRUCE.191 UACC(NONE)**
- **PERMIT BRUCE.191 CLASS(VMMDISK) ID(JOHN) ACCESS(READ)**
- **SETROPTS CLASSACT(VMMDISK)**
- **RALTER VMXEVENT MYEVENTS DELMEM(LINK/NOCTL)**
- **SETEVENT REFRESH MYEVENTS**

- Note:
  - Access modes specified on LINK command are mapped to the appropriate RACF profile access level (e.g. WR mode requires UPDATE access)

RACF classes which control CP events

VMMDISK	Minidisk access via LINK command
VMRDR	Ability to send files to unit record devices of a user via TRANSFER, SPOOL, etc commands
VMNODE	Ability to send files to RSCS nodes using the TAG command
VMBATCH	Ability to work on behalf of another user using Diagnose 0xD4. Used by FTP and NFS servers.
VMSEGMT	Use of a restricted named saved segment (NSS) or discontiguous saved segment (DCSS)
VMCMD	Various CP commands: STORE, XAUTOLOG, TRSOURCE, etc
VMLAN	Authorization to couple to a Guest LAN or Virtual Switch, plus VLAN id authorization

RACF classes which control CP events …

VMXEVENT	CP events that can be controlled or audited
VMMAC	Enables Mandatory Access Checking for CP events
SECLABEL	Information sensitivity and partitioning (MLS)
VMPOSIX	OpenExtensions mapping, and identity switching
OE audit classes	PROCESS, FSOBJ, DIRACC, DIRSRCH, and FSSEC used for auditing, as on z/OS
FILE	Shared File System file protection
DIRECTRY	Shared File System directory protection
SFSCMD	Shared File System server operator commands
SURROGAT	LOGON BY authority

RACF classes that control CP events …

TERMINAL	Local, SNA, or telnet terminals
FACILITY	Use of RACROUTE macro. Needed by FTP and NFS servers.
TAPEVOL	Tapes (if supported by tape management system)

LOGON Controls

- RACF is called whenever a user enters the system via LOGON, AUTOLOG, or XAUTOLOG
  - This is unconditional – cannot disable in the VMXEVENT profile
- Undefined users cannot logon
  - RACF does not defer to the CP directory for LOGON authority
- Time of day, day of week LOGON restrictions
- Can control which terminals a user can log on to using the TERMINAL class
  - IP addresses can be mapped into terminal names
    - e.g. 9.12.248.3 = 090CF803

Password Controls

- Common with z/OS
  - SETROPTS PASSWORD options (except minimum change int.)
  - New password and password phrase exits
  - NOEXPIRED option of ALTUSER
- Unique to z/VM:
  - No password assigned by default (set to DFLTGRP on z/OS)
  - Users can have a password, a password phrase, both, or neither.
    - Password can be removed with ALTUSER BRUCE NOPASSWORD
      - 'PROTECTED lite' – cannot be revoked for invalid password attempts
  - CP LOGON support for password phrases in z/VM 5.3
  - Multiple APIs with which to validate user passwords/phrases
    - RACROUTE, DMSPASS, RPIVAL, DIAGNOSE X'A0', DIAGNOSE X'88' , LDAP bind

Support for Shared User IDs (LOGON BY)

- Define **`LOGONBY.<userid>`** in **`SURROGAT`** class and permit surrogate users with READ access
- Users specify LOGON <shared> BY <surrogate>, specifying their own password
- Audit trail identifies shared and surrogate user IDs for subsequent authorizations
- Shared users cannot be logged onto directly by default.
  - Can be allowed by permitting user to its own SURROGAT class profile

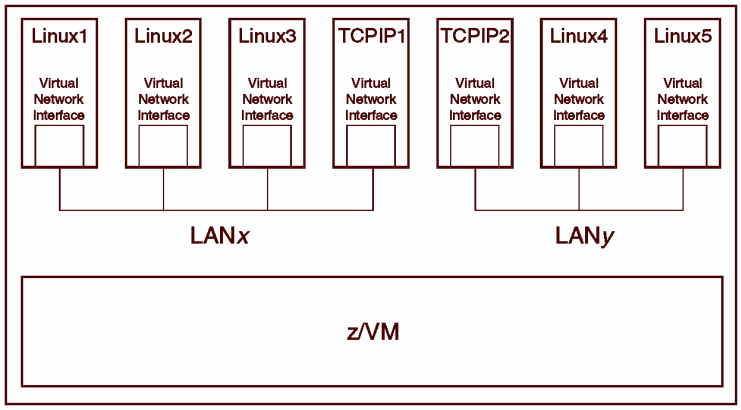
Support for OpenExtensions (UNIX)

- OVM segment of USER profile contains
  - UNIX UID
  - Initial working directory
  - path name of shell program (similar to z/OS use of OMVS segment for Unix System Services)
- OVM segment of GROUP profile contains GID
- Protection and auditing of files and directories in the Byte File System
- Protection of ability to execute set-UID and set-GID files with profiles in the VMPOSIX class. Extends granularity to an individual's ability to switch effective identity to a specific UID or GID.
  - Execution of set-UID and set-GID files is prevented by default

Support for Shared File System (SFS)

- Protection and auditing of SFS files with profiles in the FILE class
  - ADDFILE, ALTFILE, etc commands provided to manipulate resources using SFS file syntax
  - Improve usability with the ability to use SFS file syntax (vs. RDEFINE, RALTER, etc)
- Protection and auditing of SFS directories with profiles in the DIRECTRY class
  - ADDDIR, ALTDIR, etc commands provided (similar to file commands)
- Protection and auditing of SFS operator and administrator commands with profiles in the SFSCMD class

z/VM Guest LANs and Virtual Switches

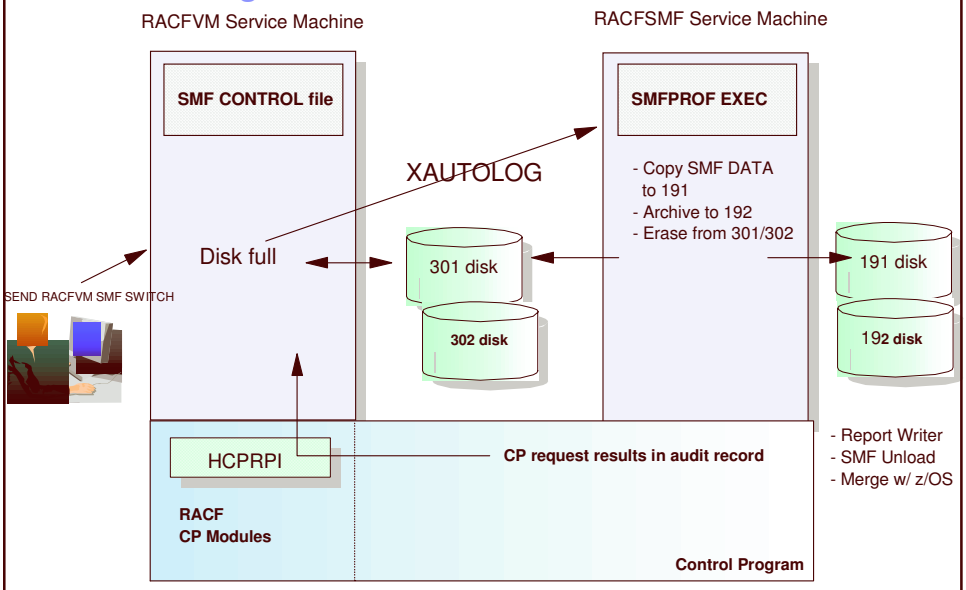


"network in a box"

Protection of Guest LANs via the VMLAN class

- UPDATE access to *USERID.LANNAME* required to COUPLE
- Virtual switches – specialized Guest LAN which can connect directly to external network, and understand IEEE VLANs
  - UPDATE access to SYSTEM.SWITCHNAME.VLANID in order to use that VLAN ID
- Example:
  - RDEFINE VMLAN SYSTEM.SWITCH01 UACC(NONE)
  - PERMIT SYSTEM.SWITCH01 CLASS(VMLAN) ID(NETGRP1) ACCESS(UPDATE)
  - RDEFINE VMLAN SYSTEM.SWITCH01.0001 UACC(NONE)
  - PERMIT SYSTEM.SWITCH01.0001 CLASS(VMLAN) ID(LARRY CURLY MOE) ACCESS(UPDATE)

SMF Auditing on z/VM

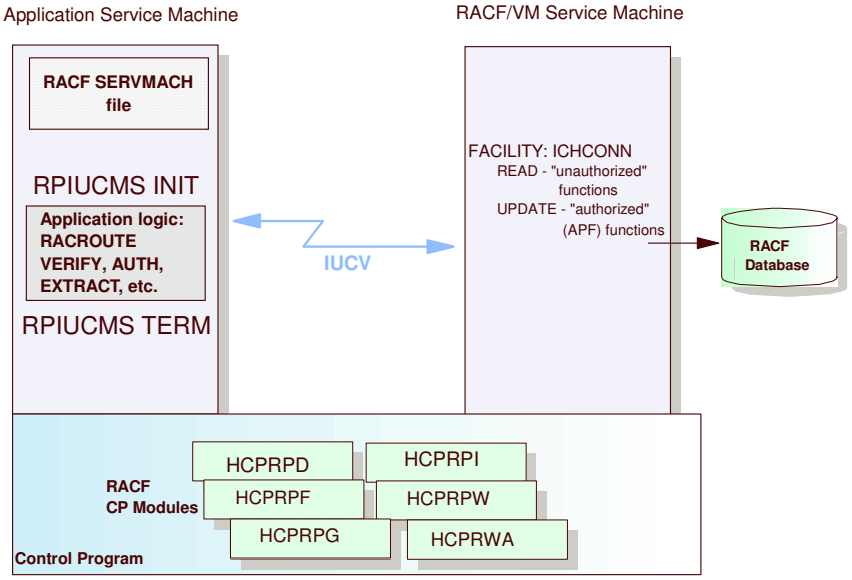


RACF Monitoring

Objective: Immediate notification of abnormal security events

- **Security console**
  - VM operator console or z/OS Operator console
  - Defined via the CSTCONS table on z/VM, Route code = 9 (z/OS)
  - Optionally sent to the resource owner
- **Dynamic messages to security console**
  - Unauthorized attempt to access system
  - Unauthorized attempt to access resource
  - Invalid RACF operations
- **Message information:**
  - Who user or job is
  - What user/job attempted to do

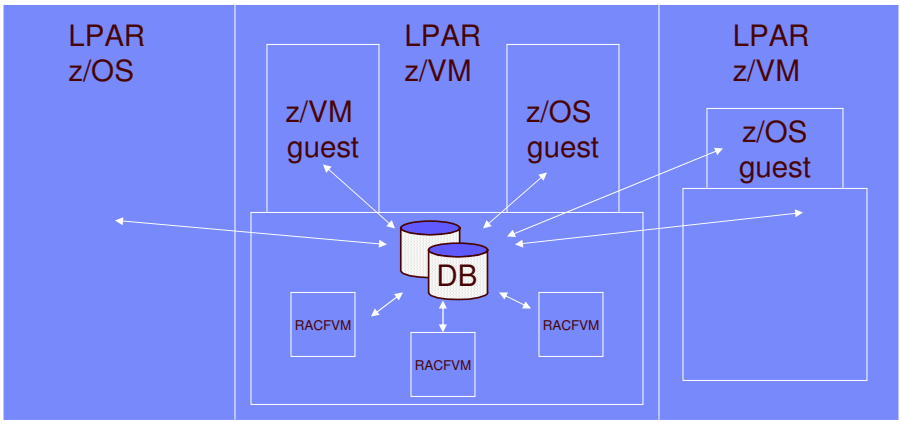
RACROUTE API for Application Security



Multiple RACF Service Machines

- Can configure several servers running concurrently to increase throughput of CP requests
- All servers share a common RACF database
- Individual servers can be “dedicated” to specific application servers
  - SFS, BFS (OpenExtensions file system)
  - Or other application server

RACF Database Sharing – Possible configurations

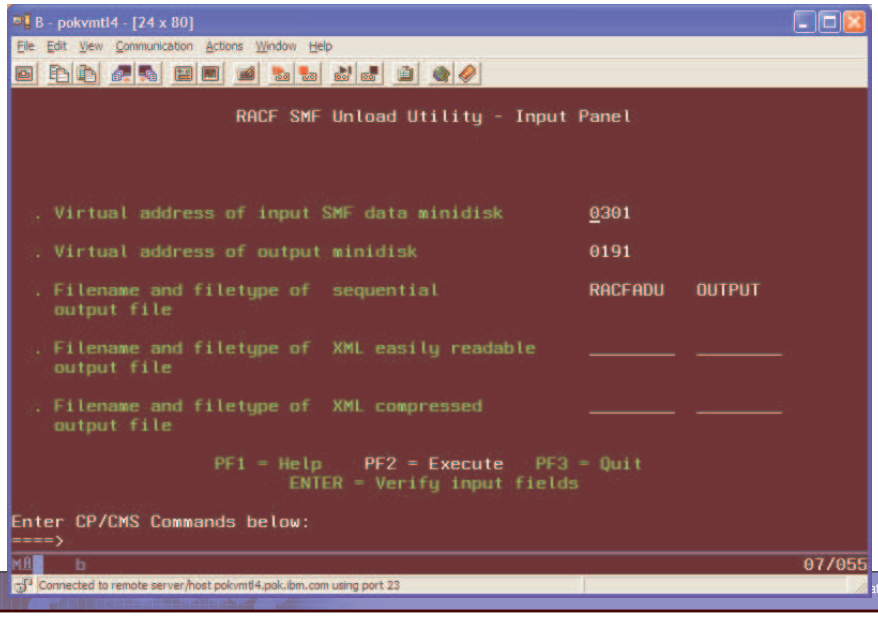


See APAR VM64383

RACF Utilities

- Familiar set from z/OS
  - SMF Unload, Database Unload, IRRMIN00, IRRUT100/200/400, DSMON
- Wrapped in EXECs for a z/VM look and feel
  - Interactive or command-line interface

RACF Utilities – Example: RACFADU EXEC



z/VM RACF Security Server feature FL530

- **Optional mixed-case 8-character passwords**
- **Mixed-case password phrases up to 100 characters, including blanks**
- **Passwords and phrases can be removed entirely**
- **Audit trail can be unloaded in XML format**
- **LDAP backend support**
- **Remote authentication and audit via new LDAP server and utilities**
- **Protection for the CP FOR command, and for DIAGNOSE X'88'**
- **Removal of z/OS-specific information from library**
- **Misc: NOPASSWORD, NOEXPIRED, auditing of password changes, increased number of POSIT values in Class Descriptor Table**

LDAP Server and Utilities

- Enables remote hosts or applications to securely authenticate users against the RACF database on z/VM
  - E.g. Linux PAM
- Enables central management of z/VM passwords
- RACF user and group interface (SDBM backend)
- Auditing of LDAP server events
- Remote audit and authorization via LDAP extended operation
- CMS client utilities
  - ldapadd, ldapsrch, ldapmdfy, ldapmrdn, ldapdlet

*This is a component of TCP/IP, not part of RACF

Common Criteria

- Common Criteria ensures
  - A set of meaningful security functions
    - Access control
    - Audit
  - Extensive testing of those functions
  - Effective processes
  - Good documentation
- Assurance levels 1 through 7
  - Evaluation by accredited firms
  - Certification by government agencies
  - CommonCriteriaPortal.org

Common Criteria …

- z/VM Version 5.1 completed evaluation
  - October 2005
  - Includes CP, TCP/IP stack with telnet, and RACF/VM
- Labeled Security Protection Profile (LSPP)
  - Mandatory access controls
  - Security clearances and compartmentalization enforced
- Controlled Access Protection Profile (CAPP)
  - Discretionary access controls
  - User- or administrator-controlled access
- Evaluation Assurance Level (EAL) 3+

Common Criteria …

- z/VM Version 5.3
  - Statement of Direction for CAPP/LSPP EAL4
  - Currently under evaluation
- z/VM Version 5.2
  - Will not be certified
  - Statement of Direction modified by z/VM V5.3 announcement
- z/VM Version 5.1
  - Withdrawn from service September 2007

Summary

- RACF for z/VM enhances security for z/VM by:
  - Providing fine-grained access controls of VM resources used by users and guests
    - Permits the sharing of VM UserIDs with accountability
  - Auditing capability of "VM events" – CP commands, diagnoses, access of resources, and authentication
  - Separates the disciplines of security Administrator, Auditor and operations staff
  - Passwords stored one-way encrypted
- Utilities which enable the unload of audit data and security database rules for reporting and data mining
- Built upon the time proven RACF for z/OS product – adapted to the z/VM environment
- Depends upon the base system integrity provided by both the z/VM operating system and the zSeries hardware

Resources and References

- RACF for VM publication library
  - Especially the Security Administrator's Guide
    http://publibz.boulder.ibm.com/cgi-bin/bookmgr_OS390/Shelves/HCSH2A91
- z/VM Security and Integrity
  http://www.vm.ibm.com/security/
- Security Evaluations for IBM Products
  http://www-3.ibm.com/security/standards/st_evaluations.shtml
- IBM Security Solutions
  http://www.ibm.com/security

Resources and References …

- z/VM publication library - http://www.vm.ibm.com/library/
  - z/VM Connectivity – for Guest LAN and virtual switch info
  - z/VM CP Commands and Utilities Reference – See commands that can be audited and protected
  - z/VM CP Programming Services – See diagnose codes which can be audited and protected, and see description of ESM interface
  - z/VM CP Planning and Administration – For description of CP directory statements
- IBM ITSO Redbooks for z/VM
  http://www.vm.ibm.com/pubs/redbooks/
- racf-l internet listserv- RACF/VM questions are fair game!