Tightening the z/VM Environment after initial installation

Sam Cohen
Levi, Ray & Shoup, Inc.
Email: sam.cohen@lrs.com

Agenda

- z/VM Background
- z/VM Security
- Issues with z/VM-supplied security settings
- “Tightening” the security environment
- Preparing for an external security manager

z/VM Background

z/VM Background

- z/VM’s CP (Control Program) provides for management of real resources and definition of virtual machines with (only) virtual resources
- CP can define virtual hardware where there is no equivalent in the real hardware
- More granular/flexible than Logical Partitioning (LPAR)

z/VM Background

- z/VM's CP (Control Program) provides for management of real resources and definition of virtual machines with (only) virtual resources
- CP can define virtual hardware where there is no equivalent in the real hardware
- More granular/flexible than Logical Partitions (LPAR)

System Startup

- Load from device containing CP nucleus (&SYSRES)
- CP reads file on System Parameter device (&SYSPARM) to determine resources and environment (default file: SYSTEM CONFIG)
- CP reads previously-compiled directory of virtual machines (allocated as DRCT space on &SYSRES)
- CP automatically starts virtual machines specified in SYSTEM CONFIG

z/VM Security

z/VM Security

Authentication

- Userid/Password combination
- Minidisk passwords

z/VM Security

Authentication

- Userid/Password combination
- Minidisk passwords

Authorization

- Resources (Real and Virtual)
- CP Commands

z/VM Security

Authentication

- Userid/Password combination
- Minidisk passwords

Authorization

- Resources (Real and Virtual)
- CP Commands

Auditing and Logging

Authentication

Controlled by z/VM Directory

- Each virtual machine is defined by a USER or IDENTITY statement
- Contains name of virtual machine (userid) and logon password
- Contains passwords for accessing minidisks
  - Positional entries on MDISK statement
    - Read password
    - Write password
    - Multiuser password
    - Value of “ALL” means unrestricted access

Authorization

Real Resources

- Access controlled by:
  - I/O Configuration Dataset (IOCDS)
    - Defined by HCD/HCM or compiled IOCP source
  - z/VM Directory
    - Minidisk definitions
    - Link to other users' minidisks (mdisk passwords not required)
    - Shared Filesystem (SFS) grants (file-level or directory-level)
    - Byte Filesystem (BFS) owner/group/world permissions

Authorization

Virtual Resources

- Access controlled by:
  - SYSTEM CONFIG file
    - Restricted vs. Unrestricted virtual devices (example: Guest LANs)
  - z/VM Directory
    - Virtual machine memory sizes
    - Inter-user communication
    - Virtual devices
  - Dynamically-defined virtual devices
    - Virtual terminals
    - Virtual NICs
    - Virtual CTCs
    - Virtual disks in memory
    - Are deleted when virtual machine is logged off

Auditing and Logging

- VM Event Records
- Operator Messages
- Secondary Console Interface (SCIF) Messages
- Virtual Machine Console Logs

Auditing and Logging

- VM Event Records
- Operator Messages
- Secondary Console Interface (SCIF) Messages
- Virtual Machine Console Logs

- IBM-provided Programmable Operator (PROP) can record Operator and SCIF messages
- User-written Execs (in REXX) can capture virtual machine console logs
- SYSTEM CONFIG options allow journaling of improper duplicate logon attempts

Issues with z/VM-supplied security settings

Issues with z/VM-supplied security settings

Initial Authorization and Authentication:

- SYSTEM CONFIG file
  - Activates all sensed devices visible to the LPAR (by I/O Subsystem via IOCDS)
  - Prompts for spool startup mode and TOD change
    - Note: There is no “TOD Enable” button on current hardware
  - Ability to enter visible passwords (on command-line logon, link statements)
  - No notification of multiple logon attempts with invalid passwords
- VM Directory
  - Userids have known passwords
    - Passwords documented in z/VM Installation Manual
    - Limited use of special passwords to restrict access (more later)
  - All minidisk definitions have common or easily guessed passwords
    - READ/WRITE/MULTIPLE
    - Ruserid/Wuserid/Muserid

Initial Auditing and Logging:

- CP messages go to the userid defined to CP as the “System Operator”
  - Default ID = OPERATOR
- No logging of directory changes
- No logging of system changes made by a superuser

“Tightening” the Security Environment

SYSTEM CONFIG file

- Remove the system operator from startup decisions during normal operations
  - Enable the following features,
    - AUTO_IPL
    - AUTO_IPL_AFTER_RESTART
    - AUTO_IPL_AFTER_SHUTDOWN_REIPL
  - If set to FORCE, the operator is only prompted if spool file destruction may occur
- Turn off PASSWORDS_ON_CMDs
- Define Virtual LANs/Switches here instead of AUTOLOG1
- Create new CP command classes allow subsets of IBM-supplied command classes.
  - Examples: FORCE, SET SECUSER, SIGNAL SHUTDOWN, XAUTOLOG
- Enable Journaling to track invalid logon attempts
- Use IMBED files for frequently changed sections
- Use –system–, &SYSRES and &SYSPARM variables to reduce complexity

Example of modified SYSTEM CONFIG

```
/**********************************************************************/
/*                Checkpoint and Warmstart Information                */
/**********************************************************************/

  System_Residence,
   Checkpoint  Volid &SYSRES  From CYL 21  For 9 ,
   Warmstart   Volid &SYSRES  From CYL 30  For 9

/**********************************************************************/
/* System-unique Volumes                                              */
/**********************************************************************/

  IMBED -system- VOLSERS

/**********************************************************************/
/* Journaling                                                         */
/**********************************************************************/

  Journal Facility ON Set_and_Query ON ,
    Logon Lockout After 3 Attempts for 5 Minutes ,
          VM_LOGO After 3 Attempts

/**********************************************************************/
/*                         Features Statement                         */
/**********************************************************************/

 Features ,
   Auto_IPL Force Drain ,          /* Startup options                */
   Auto_IPL_After_Restart Force Drain ,
   Auto_IPL_After_Shutdown_Reipl Force Drain ,
   Enable  ,                       /* Enable  the following features */
     STP_TZ ,
     New_Devices_Initialized_When_Added,  /* Make new devices online */
   Disable ,                       /* Disable the following features */
     Dynamic_IO ,
     Set_Dynamic_IO ,
     Set_Privclass ,               /* Disallow SET PRIVCLASS command */
     Clear_TDisk   ,               /* Don't clear TDisks at IPL time */
     Validate_Shutdown ,           /* Don't require system name      */
   Retrieve ,                      /* Retrieve options               */
     Default  20 ,                 /* Default.... default is 20      */
     Maximum  255 ,                /* Maximum.... default is 255     */
   MaxUsers noLimit ,              /* No limit on number of users    */
   Passwords_on_Cmds ,             /* What commands allow passwords? */
     Autolog  no  ,                /* ... AUTOLOG does               */
     Link     no  ,                /* ... LINK does                  */
     Logon    no  ,                /* ... and LOGON does, too        */
   Vdisk Userlim 144000 blocks,    /* Maximum vdisk allowed per user */
   Disconnect_Timeout 15           /* Can be OFF, default is 15 min  */
```

Contents of *system-1* VOLSERS:

```
User_Volume_List  VM1WK1
User_Volume_Include VM1*
User_Volume_Exclude VM2*
```

Contents of *system-2* VOLSERS:

```
User_Volume_List  VM2WK1
User_Volume_Include VM2*
User_Volume_Exclude VM1*
```

VM Directory

VM Directory

Know and use “reserved” passwords

VM Directory

Know and use “reserved” passwords

- NOPASS

VM Directory

Know and use “reserved” passwords

- NOPASS No password required for logon

VM Directory

Know and use “reserved” passwords

- NOPASS No password required for logon
- AUTOONLY

VM Directory

Know and use “reserved” passwords

NOPASS	No password required for logon
AUTOONLY	Similar to started task/process

VM Directory

Know and use “reserved” passwords

- NOPASS   No password required for logon
- AUTOONLY   Similar to started task/process
- NOLOG

VM Directory

Know and use “reserved” passwords

NOPASS	No password required for logon
AUTOONLY	Similar to started task/process
NOLOG	Logon not permitted

VM Directory

Know and use “reserved” passwords

NOPASS	No password required for logon
AUTOONLY	Similar to started task/process
NOLOG	Logon not permitted
LBYONLY	

VM Directory

Know and use “reserved” passwords

• NOPASS	No password required for logon
• AUTOONLY	Similar to started task/process
• NOLOG	Logon not permitted
• LBYONLY	Use Surrogate Userid for logon

VM Directory

Authentication Techniques

- Set all IBM-provided IDs that you don’t use to NOLOG
  - Don’t delete these definitions, otherwise system upgrades will be impacted
- Define “real” administrative users and LOGONBY to superuser virtual machines
  - Caution: These admin users should be subject to password management policies…but keep a “break-glass” password to MAINT in case all LOGONBY users get locked out.
- Set used IBM-provided service virtual machines to AUTOONLY
- Remove obsolete virtual machines after a version upgrade
  - For example, OSA/SF is gone from z/VM V7, but not deleted via the upgrade installation method, you should manually remove the virtual machines defined for OSA/SF
- Delete **all** Minidisk passwords, except for certain limited disks needing the universal read password of ALL:
  - MAINT190/193/19D/19E/402
  - TCPMAINT 592
- Carefully consider impact of IUCV ANY
- Don’t ‘overauthorize’ CP commands to a virtual machine
  - Define new command classes to avoid full CP CLASS authority when not needed

VM Directory

Additional Directory Cleanup

- Use Directory Profiles
  - Use profile IBMDFLT for the entries that don’t use any profile
  - Only use in-line values that differ from the profile entry
- Eliminate duplication within the IBM-supplied directory:
  - Use GLOBALOPTS MACHINE ESA and remove individual MACHINE ESA specifications
  - Move common TCPMAINT LINKS in individual TCP/IP entries to profiles TCPCMSU and TCPGCSU
  - Move non-version-specific LINK entries in SUBCONFIG clauses to the related USER or IDENTITY clauses
    - Keep version-specific links in SUBCONFIGs, since new versions are installed one LPAR at a time
- Cleanup like this speeds up DIRECTXA processing and reduces the size of the directory stored in DRCT space

Example of Directory Cleanup

```
 IDENTITY SYSMON   WD5JU8QP   32M   32M DG
 BUILD ON DEMOVM1 USING SUBCONFIG SYSMON-1
 BUILD ON DEMOVM2 USING SUBCONFIG SYSMON-2
* BUILD ON @@member3name USING SUBCONFIG SYSMON-3
* BUILD ON @@member4name USING SUBCONFIG SYSMON-4
 ACCOUNT 1 SYSMON
 MACHINE ESA
 IPL CMS PARM AUTOCR
 CONSOLE 01F 3215
 SPOOL 00C 2540 READER A
 SPOOL 00D 2540 PUNCH A
 SPOOL 00E 1403 A
SUBCONFIG SYSMON-1
 LINK MAINT 190 190 RR
 LINK MAINT 19D 19D RR
 LINK MAINT 193 193 RR
 MDISK 191 3390 03030 005 VM1RES MR RSYSMON  WSYSMON  MSYSMON
SUBCONFIG SYSMON-2
 LINK MAINT 190 190 RR
 LINK MAINT 19D 19D RR
 LINK MAINT 193 193 RR
 MDISK 191 3390 03030 005 VM2RES MR RSYSMON  WSYSMON  MSYSMON
*SUBCONFIG SYSMON-3
* LINK MAINT 190 190 RR
* LINK MAINT 19D 19D RR
* LINK MAINT 193 193 RR
*SUBCONFIG SYSMON-4
* LINK MAINT 190 190 RR
* LINK MAINT 19D 19D RR
* LINK MAINT 193 193 RR
```

```
IDENTITY SYSMON   WD5JU8QP   32M   32M DG
 INCLUDE IBMDFLT
 BUILD ON DEMOVM1 USING SUBCONFIG SYSMON-1
 BUILD ON DEMOVM2 USING SUBCONFIG SYSMON-2
* BUILD ON @@member3name USING SUBCONFIG SYSMON-3
* BUILD ON @@member4name USING SUBCONFIG SYSMON-4
 ACCOUNT 1 SYSMON
 IPL CMS PARM AUTOCR
LINK MAINT 193 193 RR
SUBCONFIG SYSMON-1
 MDISK 191 3390 03030 005 VM1RES MR
SUBCONFIG SYSMON-2
 MDISK 191 3390 03030 005 VM2RES MR
*SUBCONFIG SYSMON-3
*SUBCONFIG SYSMON-4
```

Auditing/Logging

- Use IBM Directory Maintenance Tool or similar
  - Logs all directory transactions
  - User password management (simple)
    - Limited policy enforcement
      - Number of characters
      - Password history
      - Expiration notices via reader notes
      - Userid is NOLOG'd upon expiration, administrator must reenable
  - IBM-provided exits synchronize directory changes with Security Server (RACF)
- Use CP Operator Message capturing tool
  - Programmable Operator (PROP)
  - Performance Toolkit
- Use virtual machine VMUTIL for time-based activities
  - Send daily virtual machine console logs to a collector
- Operations Manager for z/VM can also perform these non-directory functions

Preparing for an external security manager

Why consider an external security manager?

- Limitations of z/VM Directory
  - 8 LOGONBY userids per virtual machine
  - Up to 8-character passwords
  - No passphrases
  - Passwords stored on disk in clear text (EBCDIC)
  - Need more granular access to resources for superusers
- Limitations of DirMaint
  - Limited password validation
  - Crude password change mechanism
- Single collection point for access logs
- Single point of authorization for CMS users

Note that an external security manager does <u>not</u> control security inside a “bare metal” operating system running in a virtual machine

Preparing for an external security manager

Determine what resources you need to protect

- Do you really need to protect access to spool files?
- Do you really need to protect access to minidisks if there are no passwords associated with minidisks?
- Do you really need to protect resources for batch execution (under CMS)?
- Do you really need to protect CP commands if you have created custom command classes?

Prepare the z/VM Directory for loading the security database

- Use ACIGROUP directory statements to define virtual machines with a similar purpose
  - The ACIGROUP will be used to define the virtual machine's default group
  - Put the ACIGROUP statement in the PROFILE; override only on virtual machines that need to be in a different group

Run the IBM-supplied utility to build the initial RACF commands

- Remove the resource definitions that won't be tracked
- Remove the class activations for resources that won't be tracked

Update RACF exits to minimize security database access

- Primarily access the VM directory for most authorizations
- Don't bother authorizing minidisks with universal READ access (ALL in the minidisk read password position)

Select DirMaint exits to send RACF updates only for resources that are being protected by RACF

- If you are only protecting userids/passwords with RACF, don't send directory updates for minidisks, spool, etc.

References

- CP Planning and Administration (SC24-6175)
- CMS Planning and Administration (SC24-6171)
- Directory Maintenance Facility Tailoring and Administration (SC24-6190)
- Performance Toolkit Guide (SC24-6209)