Basic z/VM Security

Tony Noto

November 5, 2026

Agenda

- Introduction
- References
- Network
- Passwords
- Minidisks / SFS
- CMS Files
- CP privilege classes
- Resource limitations
- Backups
- Weakest link
- External Security Managers

Introduction

In this session we will discuss the on-board features of the z/VM system that can/should be used to secure the z/VM and CMS environment. Also discusses some simplistic approaches to securing maintenance virtual machines, access to data, virtual machine privileges, resource consumptions limits, backup and recovery strategies. We will also touch very briefly on the use and importance of utilizing an External Security Manager (ESM).

References

The following list of IBM reference manuals will be greatly helpful with questions that you may have regarding the content of this presentation:

- CP Planning and Administration - SC24-6271
- CMS Planning and Administration - SC24-6264
- CP Commands and Utilities Reference - SC24-6268
- CMS Commands and Utilities Reference - SC24-6260

Other documentation that may be helpful:

- External Security Manager, if present
- Directory Manager, if present

Note: Most, if not all, of the CP and CMS commands have “HELP” available, along with messages associated with the command responses.

While not specific to the z/VM environment ..

Securing the network is the first line of defense

- Implement firewalls
- Use internal networks and VPNs
- Implement the use of SSL/TLS for TN3270, web access, and FTP usage

Logon passwords w/o an ESM

- Are 1 to 8 characters in length
- Can contain characters, numbers and certain special characters
- Not case sensitive
- Should have basic rules implemented
- Should use AUTOONLY for “trusted servers”
- Should use LBYONLY for “maintenance servers”

Logon passwords w/ an ESM

- May contain more than 8 characters if passphrases are implemented
- Can contain characters, numbers and certain special characters
- May be case sensitive
- AUTOONLY can be controlled dynamically by the ESM
- LOGONBY can be controlled dynamically by the ESM
- Can set password/passphrase expirations and access time slots
- May be able to implement credentials via a “smart card”

Minidisk passwords w/o an ESM

- Can be omitted
- Can be defined as “ALL”
- Are 1 to 8 characters in length
- Can contain characters, numbers and certain special characters
- Not case sensitive
- Should have basic rules implemented

Password types

- READ - Read access
- WRITE - Write access (includes MR)
- MULTI - Multi-write access

Minidisk passwords w/ an ESM

Linking to a virtual machine's minidisk is generally under control of the ESM rules. However, depending on how the ESM is configured, LINKs may defer to CP for access resolution.

Minidisks / SFS

Defining minidisks must be a well thought out process. Choose the ideal location and associated link modes for minidisks:

- On which volume, or volume group, should the minidisk reside
- Should the minidisk be available to different member LPARs in an SSI cluster
- Ensure the minidisk does not overlap another minidisk (can use DISKMAP or DIRMAP style utility)
- Establish initial LINK mode and associated passwords and/or ESM rules
- V-DISKs are emulated in memory. Can be limited by VDISK SYSLIM/USERLIM statement in the SYSTEM CONFIG file
- T-DISKs are temporary, should have ENABLE CLEAR_TDISK in the SYSTEM CONFIG file

Minidisk link modes define the default

- R - Read-only access for a single virtual machine.
- RR - Read-only access by multiple virtual machines
- W - Write access if not linked by another virtual machine (default).
- WR - Write access if not linked by another virtual machine, otherwise read-mode.
- M - Write access if not linked in W mode by another virtual machine.
- MR - Write access if not linked in W mode by another virtual machine , otherwise read-mode..
- **MW - Multiple-write access**

Minidisk vs. SFS

- Granularity
- Multi-write access to directories
- Access authority
- Expansion

File mode numbers

- Number 0 - For the minidisk environment, file mode number 0 is used to make files private. For the SFS environment, file mode number 0 means the same as file mode number 1.
- Number 1 - File mode number 1 is used for reading and writing files. It is the default file mode number.
- Number 2 - File mode number 2 is the same as file mode 1.
- Number 3 - File mode number 3 means that files are erased after they are read. You can use file mode number 3 if you do not want to maintain copies on your minidisks or in your SFS directories.
- Number 4 - File mode number 4 means files are in OS simulated data set format. These files are created by OS macros in programs running in CMS.
- Number 5 - File mode number 5 is the same as file mode number 1.
- Number 6 - For EDF files, file mode number 6 indicates that the update-in-place attribute of a CMS file is in effect. This means that the existing records of a file are written back to their previous location on the minidisk, rather than in a new slot.

CP command privilege classes

Privileges

- Defined in the CP user directory for each virtual machine
- IBM CP command default classes ABCDEFG
- Can be extended to include H-Z, 1-6 using MODIFY directory statement or defined in the SYSTEM CONFIG file
- Virtual machines can have up to 32 classes
- Are specific to commands, and in some cases command operands, and are not inclusive of “lessor” privilege class commands
- Can be dynamically modified if enabled in the SYSTEM CONFIG file
- Impact of privilege class A

Resource limitations

SYSTEM CONFIG

- MAXUSERS
- VDISK SYSLIM/USERLIM
- CLEAR_TDISK
- PASSWORDS_ON_CMDS
- PRIV_CLASSES
- DISCONNECT_TIMEOUT

Resource limitations

USER DIRECTORY

- Logon NOPASS / AUTOONLY
- Privilege classes
- Memory limitations
- SHARE values
- LOGONBY lists
- OPTION LNKNOPAS
- VMRELOCATE (for SSI environments)

Resource limitations

In-house “concerns”

- Maximum idle-time
- Logged-on time frames
- Spool file purge

Backups

Having a backup plan in place is critical for successful recovery from a catastrophic situation:

- Hardware failures are rare but not unheard of
- Backup critical resources such as system DASD/disks, spool files, NSSes, product/utility development files, SFS filepools and/or filespaces
- Test restore/recovery processes

Weakest link

The weakest link in any environment is the people.

- Have a mechanism in place to audit events and identify peculiarities
- Have an understudy/secondary for those individuals responsible for maintaining the integrity of your environment
- Document critical procedures thoroughly
- Educate

External Security Managers

An ESM can …

- Offer Passive Security
- Extend on-board protections
- Make changing protection rules more flexible and dynamic
- Group virtual machines so that rules can apply to groups as opposed to individual virtual machines
- In some cases, can coordinate with an installed directory manager
- Produce reports of protocol attempts and/or violations
- Can establish logon windows
- Can force password change timeframes
- Can expire virtual machine access
- Can revoke access privileges based on access violations



Questions