


z/VM 7.3 Security News and How To's – 2023

Brian W. Hugenbruch, CISSP

IBM LinuxONE Resiliency Lead &&
IBM Z Security for Virtualization and Cloud

bwhugen@us.ibm.com

 @Bwhugen

 @the_lettersea



Agenda

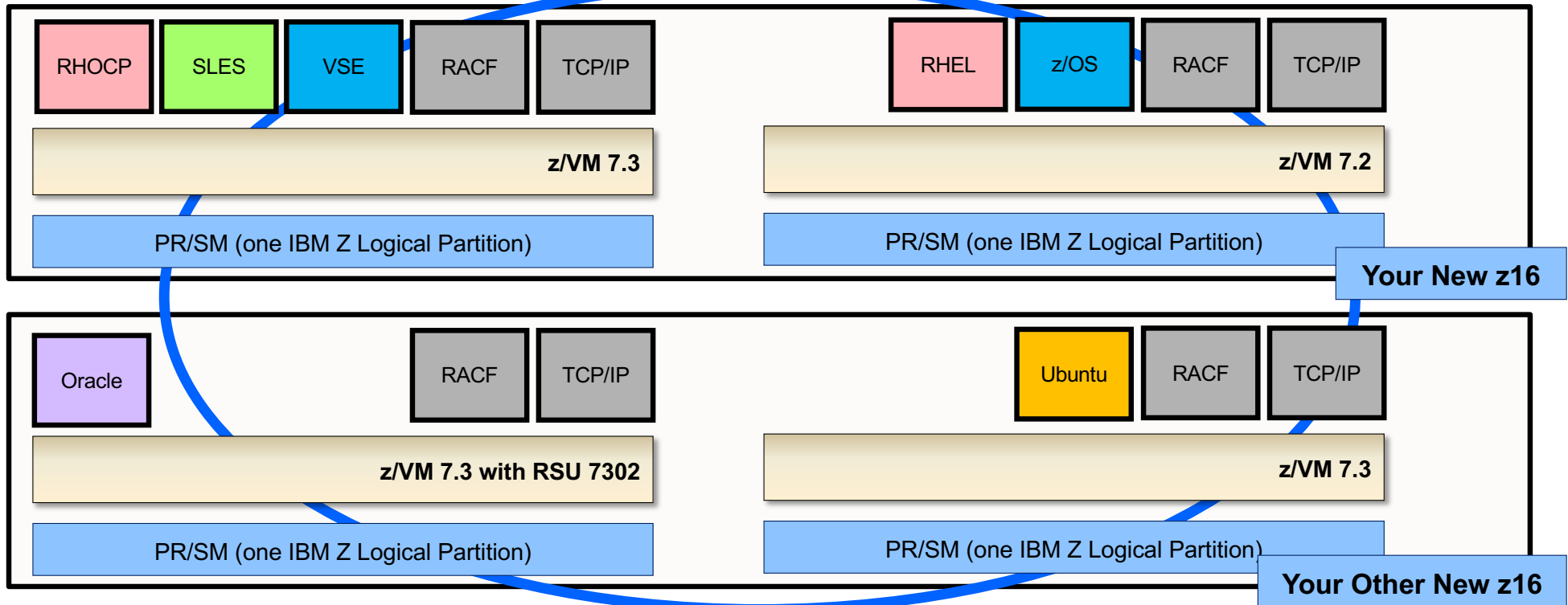
Why secure virtualization?

Short Topics in z/VM Security

A Deeper Dive: KEYVAULT, Compliance, and Guest Secure IPL

Looking Ahead

The z/VM Platform



- Shareable, multi-tenant overcommitment of IBM Z and LinuxONE hardware at scale, with a commitment to architectural fidelity and the highest levels of security, backed by the IBM Z Security & Integrity Statement.
- *(Four-member SSI shown; z/VM V7.3 can support up to eight systems in a cluster)*

Why secure z/VM?

**(PCI DSS v3.1 Supplement - Virtualization Guidance v2.1)*

1. Vulnerabilities in the Physical Environment Apply in a Virtual Environment
2. Hypervisor Creates a New Attack Surface
3. Increased Complexity of Virtualized Systems and Networks
4. More than One Function per Physical System
5. Mixing VMs of Different Trust Levels
6. Lack of Separation of Duties
7. Dormant Virtual Machines
8. VM Images and Snapshots
9. Immaturity of Monitoring Solutions
10. Information Leakage between Virtual Network Segments
11. Information Leakage between Virtual Components



Recommendations for Virtual Environments	Explanation or Examples
Evaluate risks associated with virtual technologies	<i>Draw diagrams of how sensitive data flows in your virtual environment; understand the capabilities granted to someone entering via the virtualization layer to see (or not) guest data; recognize badly configured virtualization as a threat vector.</i>
Understand impact of Virtualization to scope of CDE	
Restrict physical access	<i>Badge access to SE and CPC; locks on doors; 2FA for laptops.</i>
Implement defense in depth	<i>Add in an ESM. Turn on TLS. Don't trust that no one will find your LOGO screen.</i>
Isolate security functions	<i>Maybe don't combine MAINT and RACF SPECIAL?</i>
Enforce least privilege and separation of duties	<i>Be careful with / create your own privilege classes. Also applies to DirMaint and RACF.</i>
Evaluate hypervisor technologies	<i>Don't test in prod. C'mon, y'all, you know better than that.</i>
Harden the hypervisor	<i>Configure your ESM; change your defaults. Exercise LOGONBY-ONLY / SURROGAT.</i>
Harden virtual machines and other components	<i>Remove non-essential authorities from Linux guests</i>
Define appropriate use of management tools	<i>Who can use Operations Manager / ICIC when?</i>
Recognize the dynamic nature of virtual machines	<i>What happens to a VM's authorities when you upgrade to z/VM Next?</i>
Evaluate virtualized network security features	<i>Configure and control Vswitch and IVL; enable port isolation or VEPA mode as appropriate</i>
Clearly define all hosted virtual services	<i>What does virtual machine LNX01A5D do? Also, isolate *your* clients from one another.</i>
Understand the technology	<i>Listen to this presentation. :-) Attend MVMUA! Tip your host or hostess.</i>

*(PCI DSS v3.1 Supplement - Virtualization Guidance v2.1)

Is z/VM certified?

z/VM Level	Common Criteria		FIPS 140-2
7.3	Not evaluated ("designed to conform to standards")		
7.2	BSI OSPP (with Virt and Labeled Security extensions) at EAL 4+	NIAP VPP with Server Virtualization Extended Package	Level 1 Validated
7.1	Not evaluated ("designed to conform to standards")		
6.4	OSPP with Labeled Security and Virtualization at EAL 4+ --		Level 1 Validated

z/VM releases not listed are "designed to conform to the standards of each security evaluation."

Common Criteria: BSI Operating System Protection Profile with Virtualization and Labeled Security extensions at an assurance level of EAL 4+

All of z/VM V7.2



Common Criteria: NIAP Virtualization Protection Profile with Server Virtualization Extended Package

All of z/VM V7.2

Added to NIAP Approved Products List

Federal Information Processing Standard (FIPS) 140-2 Level 1 for z/VM V7.2 System SSL and ICSFLIB

* Revalidated and reapproved by NIAP in 2023



TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments.

Short Topics in z/VM Security

z/VM 7.3

- GA 3Q22
 - Preview announce April 5, 2022
 - See <https://www.vm.ibm.com/zvm730/> for more details
- New Architecture Level Set of z14 and LinuxONE II or newer processor families
- Includes all new function service shipped for z/VM 7.2 including:
 - 4 TB Real Memory, Dynamic Memory Downgrade, Improved LGR for Shared Crypto, z/Architecture Extended Configuration (z/XC) support, Direct to Host Service Download
- Additionally, includes
 - Eight-Member SSI support
 - NVMe EDEVICE support

z/VM 7.3 – System Default Changes

- **Set Default Password for User Directory**

- provides the ability to select a default password when installing or upgrading a z/VM system.

- **User Directory TODENABLE**

- Some capabilities that previously required OPTION TODENABLE will be standard for all users in z/VM 7.3.

NOTE: TODENABLE is still required for the FROMUSER and MSGPROC options of SET VTOD

- **TCP/IP Configuration Statement Changes**

- ASSORTEDPARMS option NOUDPQUEUELIMIT replaced by UDPQUEUELIMIT
 - Default of 20 datagrams queued on UDP port. Previously no limit.
- FOREIGNIPCONLIMIT default changed to 256

- **TLS 1.2 enabled by default (not TLS 1.1)**

External Security Manager (ESM) Control of Define MDISK Command

Sept 2022

- **DEFINE MDISK** is a command sometimes used in z/VM disaster recovery scenarios
 - E.g. when IPL'ing NODIRECT during a system restore
 - Similar functionality was controlled (Diagnose x'E4')
- Support has been updated to allow for control of this command by External Security Managers
 - Included in the base of z/VM V7.3
 - Audit remains through DEFINE.A in RACF/VM

z/VM 7.3: RACF and 8-Member SSI

Sept 2022

- RACF and its associated virtual machines are IDENT / SUBCONFIG
 - You'll need new ones for the new systems in your 8-way
 - Along with access to the RACFVM database
 - Remember to update your RACFSMF profile and audit controls, MFA controls, and system definitions in the IBM Z MFA server

- Beyond that, no major changes
 - RACF is capable of sharing its database (ECKD) with dozens of stand-alone systems
 - RACF is meant to be forward/backwards compatible
 - SSI will check for appropriate ESM enablement during cluster joining

zSecure for RACF/VM

June 2022

If you have zSecure for RACF/VM 2.5.1 (GA on 17 June 2022!), you now have:

- **SIEM integration** (for streaming SMF records to Qradar or similar);
- an **SMF cache server** (for collecting all SMF records in an SSI together);
- **support for MFA** (because you have MFA, I hope);
- and support for RACF databases residing (non-shared) **on SCSI volumes**.

(Along with a host of other improvements!)

https://www.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/5/877/ENUSZP22-0045/index.html&request_locale=en

Removal of RACF for z/VM support for RACF database sharing between z/VM and z/OS

April 14, 2020 Announcement

FULFILLED

Removal of RACF for z/VM support for RACF database sharing between z/VM and z/OS

z/VM V7.2 is intended to be the last z/VM release to support sharing RACF databases between z/VM and z/OS systems. While databases may remain compatible, sharing between operating systems is discouraged due to the distinct security and administration requirements of different platforms. A future z/VM release will be updated to detect whether a database is flagged as a z/OS database and reject its use if so marked. Sharing of databases between z/VM systems, whether in a Single System Image cluster or in stand-alone z/VM systems, is not affected by this statement.

- *Yes, the databases will remain compatible.*
- *Yes, the tools will still work against either.*
- *Yes, z/OS has turned off their side as well.*

A discussion on RACF/VM recovery

Best Practices for system recovery:

- Always ensure you have a SPECIAL user that is not revoked
 - If the problem is RACF repair, this is the VM you need
 - May require some “break glass in case of emergency” security procedures and documentation
- Always have a non-RACF enabled CPLOAD MODULE available (of your current release)
 - If RACF is the problem, this is the nuclear option
 - But sometimes a step back is required before you can step forward
- Always have the current USER DIRECT stored off system
- Have OPERATOR logged on through the HMC if possible
 - OPERATOR will run even if RACF is in a SBND situation
 - Can XAUTOLOG..ON the SPECIAL user at a specific device or terminal

Problem Avoidance with the RACF Database: <https://www.vm.ibm.com/devpages/hugenbru/RACDBREP.PDF>

- Make regular backups of your primary and secondary RACF databases
- Perform healthchecks of your backups
- Check database level (RACFCONV)
- RACUT200 (the Database Verification Utility) is your friend – use it regularly

IBM z16

May 2022

- Support availability May 31st, 2022 with z/VM 7.1 and z/VM 7.2. Support also included in the base of z/VM 7.3.
 - See <https://www.vm.ibm.com/service/vmreqz16.html> for details
- z/VM 7.1 and 7.2 PTFs include support for:
 - Imbedded AI Acceleration
 - [CPACF Counter Support](#)
 - Breaking Event Address Register Enhancements
 - Enhanced Vector Packed Decimal 2
 - Reset DAT Protection Facility
 - [Consolidated Boot Loader](#) (Allows guest IPL from a SCSI LUN)
 - RoCE Express3 Adapter
 - [Crypto Express8S Adapter and Cryptographic Enhancements](#)



FAQ: Have you made CEX easier to manage under z/VM? (Please?)

- Yes! We've introduced the following new enhancements in the service stream:
 - Dynamic Vary of Crypto Devices
PTF for APAR VM66266, z/VM V7.1 onward
 - Mixed-APVIRT LGR
PTF for APAR VM66496, z/VM V7.2 only
 - Host Support for Crypto Thin Interrupts
PTF for APAR VM66534, z/VM V7.2 only
 - IBM z16 Support
(as discussed)
 - *Crypto Stateless Command Filtering*
PTF for APAR VM66423, z/VM V7.3 only

- We've covered **Dynamic Vary Crypto** in this forum at length already.
- (If you need a refresher, *I'll pull out my Wheel of Fortune slides during the Q&A.*)

- Mixed-APVIRT LGR allows relocation of guests using shared crypto (clear-key only) when using a mix of CEX types
- So, you can relocate from a z15 to a z16 now.

-
- Thin Interrupts will provide a bit of a performance boost by ensuring we move away from polling ops to an interrupt-driven flow.
 - This is the default setting in z/VM V7.3. On earlier releases, use

SET CRYPTO APVIRT POLLING OFF

to enable this feature.

A Deeper Dive Into Recent z/VM Security Enhancements

KEYVAULT Utility and Enhancements for Centralized Service Management (CSM)

- **New CMS-based utility to be used to encrypt key/value pairs**
 - Associates system, userid, and password and encrypts using CPACF
 - **PBKDF2** for protecting secrets
 - Allows for storage of encrypted data in CMS for persistent use
 - Wrapped protected key is unique to a given virtual machine
 - Protected keys may not be shared between userids within an LPAR
 - Data stored on local minidisk, on a **per-userid basis**
- **Designed for at-keyboard use**
 - Replacement for NETRC.DATA file for FTP
 - Eliminates the need for passwords stored in clear-text
- **Updates to FTP Server and CSM for safer automation of multi-system management**
 - Clue off of NETRC's configured info for system/userid
 - Recover password automatically and insert everything into FTP dialogue
 - Automate past continual logon prompts during maintenance application

KEYVAULT Utility and Enhancements for Centralized Service Management (CSM)

June 2023

- **There shall be no passwords stored in clear-text**
 - Local flat file on CSM userid (or consumer userid) will hold encrypted values per system
 - NETRC DATA will no longer contain any passwords at all
 - Decrypted passwords will be stored in local variables, used for FTPS, and then erased

- **Use of the TLS Server (your existing one) is still highly recommended**
 - Transmitting decrypted passwords over a clear channel makes this whole exercise useless
 - No requirement to build a second network

KEYVAULT Usage Notes

June 2023

- **The ‘encrypting token’ is used for local password encryption**
 - The system administrator must remember this token
 - A hash of the encrypted token is temporarily maintained in memory
 - Never written to disk
 - Input for each time the admin logs onto the virtual machine
 - Treated with same delicacy as potential password input from CP LOGON
 - Shall not appear in console logs, shall not appear in the clear
 - Erased at the end of CSM processing or at virtual machine logoff
 - LOGON, IPL, or SYSTEM CLEAR creates new entry for protected keys
 - A protected key cannot be reused even in the same VM

- **A KEYVEXIT.EXEC is provided for password validation purposes**
 - To assure that an encrypting token of “12345” (for example) is not set
 - Define based upon your site’s security policies

KEYVAULT Usage Examples (1/2)

June 2023

- To create a new KEYVAULT database and add a new entry:

```
> KEYVAULT CREATEDB bwhugen
```

```
> (when prompted, enter and then re-enter a database encryption token)
```

```
DMSKEY2395I Database state is open; Database file is: bwhugen
```

```
> KEYVAULT ADDKEY myvmssys.ibm.com bwhugen
```

```
> (when prompted, supply the password for bwhugen at the target system)
```

```
DMSKEY2405I KEYVAULT stored values:
```

```
DMSKEY2405I Label: myvmssys.ibm.com UserID: bwhugen (default user)
```

```
DMSKEY2408I Request completed successfully.
```

```
> KEYVAULT CLOSEDB
```

KEYVAULT Usage Examples (2/2)

June 2023

- To query the contents of an open keyvault database:

```
> keyvault query *
```

```
DMSKEY2405I KEYVAULT stored values:
```

```
DMSKEY2405I Label: sample.host.com UserID: CSMWORK (default user)
```

```
DMSKEY2405I Label: another.system.com UserID: UserXYZ (default user)
```

```
DMSKEY2405I Label: host.somehwere.com UserID: AdminUser (default user)
```

```
DMSKEY2405I Label: host.somehwere.com UserID: UserABC
```

```
DMSKEY2408I Request completed successfully
```

KEYVAULT Utility and Enhancements for Centralized Service Management (CSM)

June 2023

- Available for z/VM V7.3
 - <https://www.vm.ibm.com/newfunction/#keyvault>

Component	APAR	PTF	RSU
CMS	VM66453	UM90280	-
SES	VM66457	UM90289	-
TCPIP	PH51239	UI91775	-

z/VM Systems Security and Compliance Utility

June 2023

- **Problem: measuring security and compliance is difficult**
 - Security data for z/VM is hard to find and harder to collect
 - Auditors don't know for what to ask
 - Known client pain-point

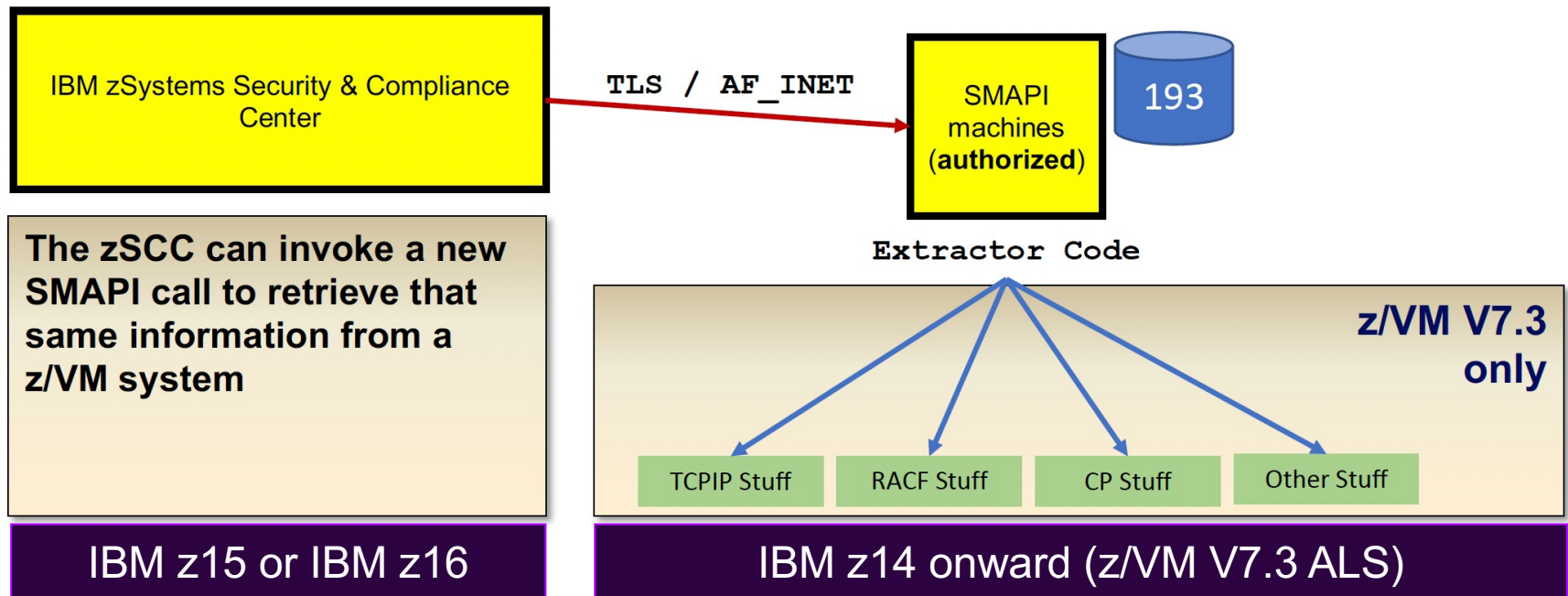
- **Deliverable: new CMS-based utility for gathering system data**
 - Centralize security-relevant data collection via one interface
 - **Gathers** security-relevant system data; **does not make security determinations**
 - Future integration with the IBM Z Security & Compliance Center product
 - **Plug-in for future vendor support or local add-ons**

- **Execute on a per-need basis (not a continuously running task)**
 - Data provided useful in measuring compliance drift or misconfiguration
 - Output provided either to console, to file (default <sysname>.<date>.A), or to calling program via API

Where does it run? (in a privileged virtual machine)

June 2023

Auditor



Who can run it?

June 2023

- A SMAPI worker machine, or
- A privileged virtual machine of your choosing

- If you're creating a new virtual machine, or using an existing one, assure that the following authorities are available:
 - **Classes A, B, D, E, G** *// a list of CP commands required is available in CMS Commands & Utilities*
 - **OPTION DEVMAINT**
 - TCP/IP connection authority
 - **PERMIT statement**, or ASSORTEDPARMS option PERMITTEDUSERONLY
 - **Admin_ID_List** authority in DTCPARMS for the TLS Server
 - Certain RACF authorities
 - **VMCMD** profile access (UPDATE) for commands protected by this class
 - **VMCMD** profile access (READ) for certain diagnose instructions, if these are protected
 - UPDATE access to an ICHCONN profile in the **FACILITY** class

- COMPEXTR will check all authorities prior to gathering information for your system, and will indicate whether or not something was missed in your configuration

z/VM Systems Security and Compliance Utility

June 2023

PCI DSS Requirement		z/VM Specific Data Required
3	Protect stored card holder data	Clear_TDISK, Passwords_on_Cmds, Set_Privclass, Disc_Operator Enabled/Disabled? Encrypted Paging TLS enabled (TLS 1.2) REQUIRED settings for Secure Telnet, FTPS, SMTP, RSCS VLAN configuration for Vswitch Is an ESM enabled Yes/No
7	Need To Know restrictions	How many machines are > Class G? Are they LBYONLY? Are there machines in the user directory with privileged options? Are they LBYONLY? Who's on the TCPIP OBEY List / SSL_Admin_List? RACF SPECIAL / OPERATIONS / AUDITOR / ROAUDIT users?
10	Track and monitor all access to network resources and cardholder data	Is anyone using anonymous FTP? Is the ESM controlling FTP? ESM control of VLAN settings (RACF VMLAN class)? Can a Class G guest create a transient Guest LAN? Are any guests in the PROFILE TCPIP running without TLS/SSL? (PORT/AUTOLOG statements)
2	Do not use vendor supplied defaults for system password and other security parameters	Scan z/VM User Directory for presence of default user password value ...And default minidisk password values RACF SYSSEC settings around DEFER RACF Audit SEVER=YES
8	Identify and authenticate access to system components	RACF: password/phrase intervals (min/max) RACF: password/phrase expiry RACF password history settings RACF password encryption – KDFAES? RACF: are the password exits enabled? Is MFA enabled? Is anyone enabled for PWFALLBACK? Are any users in the z/VM user directory not configured for LBYONLY / AUTOONLY?
6	Develop and maintain secure systems and applications (the “is it up on its service” question)	QUERY CPSERVICE QUERY CPLEVEL QUERY CMSLEVEL NETSTAT TCP/IP level output CP Environment variable output (if applicable)

Data Discussion

- Two formats – one YAML (indented, machine readable, meant for API), one “flat” (collapsed namespace)
 - Print to file or spool to console, your choice
 - Distinctions mostly fit-for-purpose
 - YAML for ZSCC consumption
 - Flat name-space for ease of lookup and comparative purposes
 - Will not introduce timestamps or variable output into content

```

zVM:
  Identity:
    Systemname: "ZVM710"
    SSI:
      SSI_name: "n/a"
      SSI_mode: "n/a"
  Version:
    CP_level: "z/VM Version 7 Release 3.0, service level 0000 (64-bit)"
    CP_service_APAR_PTF:
    CP_service_local_modifications:
    CMS_level: "z/CMS Level 31, Service Level 0000"
  CP:
    Features:
      - Feature: "Clear_TDisk"
        Enabled: "No"
      - Feature: "Not_Disconnect_Operator"
        Enabled: "No"
      - Feature: "Password_On_Command"
        LINK:
          Enabled: "No"
        LOGON:
          Enabled: "No"
        AUTOLOG:
          Enabled: "No"
      - Feature: "Set_Privclass"
        Enabled: "Yes"

```

```

zVM/Identity/Systemname: "ZVM710"
zVM/Identity/SSI/SSI_name: "n/a"
zVM/Identity/SSI/SSI_mode: "n/a"
zVM/Version/CP_level: "z/VM Version 7 Release 3.0, service level 0000 (64-bit)"
zVM/Version/CMS_level: "z/CMS Level 31, Service Level 0000"
zVM/CP/Features/Feature$Clear_TDisk/Enabled: "No"
zVM/CP/Features/Feature$Not_Disconnect_Operator/Enabled: "No"
zVM/CP/Features/Feature$Password_On_Command/LINK/Enabled: "No"
zVM/CP/Features/Feature$Password_On_Command/LOGON/Enabled: "No"
zVM/CP/Features/Feature$Password_On_Command/AUTOLOG/Enabled: "No"
zVM/CP/Features/Feature$Set_Privclass/Enabled: "Yes"

```

How does it run? (COMPEXTR)

June 2023

```

.-- SHOW ---.    .-- YAML --.
>>- COMPEXTR ---- ( ----+-----+-----+-----+----->
                        '-- QUIET --'    '-- FLAT --'

>-.-----).-- ) --><
|      .- ( - sysname date A -- ) -----.    (1).-QUIET-. |
'- FILE -+-----+-----+-----+-----+-----'-'-'
      |      .- date - A ---.    |
      '- ( - fn -+-----+-----+----- ) -'
          |      .- A -. |
          '- ft -+-----+-----'
              '- fm-'

```

(1) The FILE option implicitly suppresses console output unless SHOW is specified

z/VM Systems Security and Compliance Utility

June 2023

- **A new utility and Systems Management API for pulling security-relevant settings**
 - Extensible for both vendor and local add-on variables
 - Future exploit by zSCC in the works
 - README file in Markdown format included to explain key-value pairs and how to corroborate
 - Will be updated as IBM introduces more compliance-pertinent data to its lists
- **Available for z/VM V7.3**
 - <https://www.vm.ibm.com/newfunction/#qsec>

Component	APAR	PTF	RSU
CMS	VM66646	UM90295	-

Secure IPL for z/VM Guests

June 2023

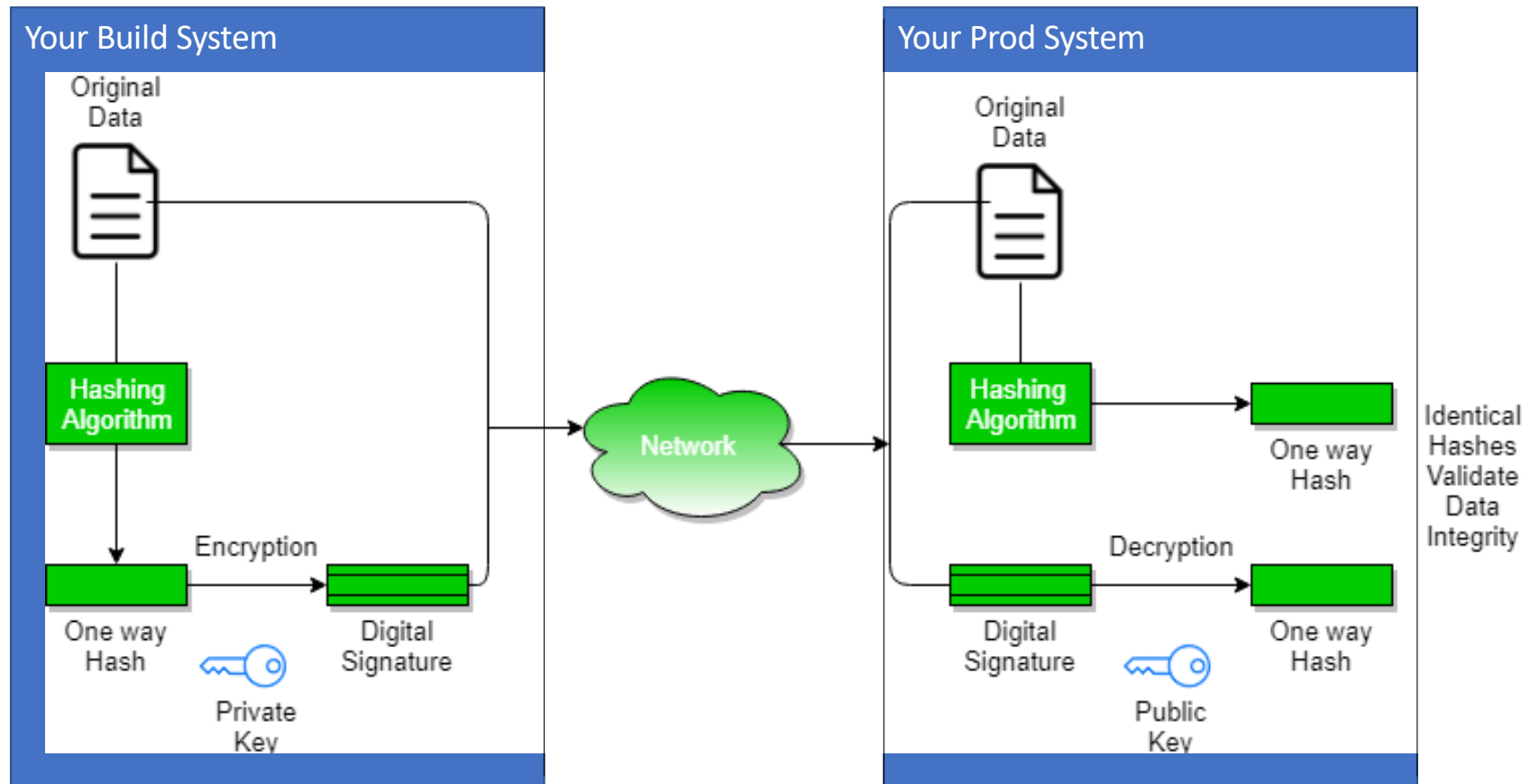
- **Assures that the content an administrator boots is unmodified from time of install**
- **New supply-chain requirement for a lot of industry regulations**
- **z/VM provides support for secure boot of guest operating systems**
 - Support added when IPL'ing from ECKD or from SCSI storage (DASD)
 - A guest must IPL LOADDEV, not IPL vdev
 - A securely IPL'd guest will behave the same way as a guest booted in its own partition

What is a digital signature?

- **A mathematical algorithm used to validate both authenticity and integrity of content**
 - Assure it hasn't been modified
 - Assure it's from a source you trust

- **Based on standard cryptographic algorithms used in the industry today**
 - A hash component for integrity (SHA-256 as most common)
 - An encryption of that hash with a private key (provides authenticity)
 - Verified by decrypting the hash with a public key, and then comparing that to a locally present hash

What is a digital signature (picture version)



How digital signatures help

- **Hashing (a cryptographic checksum) provides integrity validation**

- One way function with no collisions
- If you hash a piece of code twice, the result is always the same
- If code is modified by even one bit, result is different

- **Public-private key encryption provides authenticity**

- If you encrypt code with a private key, anyone with the public key knows for certain it came from you
- If you encrypt code with a public key, only the person with the private key can read it

What **don't** digital signatures do?

(In the context of Secure Boot and Measured Launch)

- **Prevent tampering after boot**
 - Your local access policies prevent this
 - Digital signature verification will prevent tampered code from booting, though

- **Prevent access to images**
 - Your local access policies prevent this

- **Prevent authorized changes**
 - But you have to re-sign content after you update!
 - **Because you need a private key to do this**, best to do this on a very secure system (in a clean room, if necessary)

Secure IPL for z/VM Guests

June 2023

How to use Secure IPL

- Upgrade machine firmware on your IBM z16 or IBM LinuxONE Emperor 4
 - Driver D51C bundle 19
- Install the levels of software required for support
 - z/VM PTFs as specified
 - z/OS PTFs as specified
 - Linux updates -- more support required than what was previously available for secure boot in an LPAR
- Import necessary certificate(s) with **public** key(s) into the HMC certificate store
 - Public key (**.p7b format**) must match signing private key
 - Check with your vendor(s) for more details
- Assign them to the LPARs where the guest will run
 - Any guest capable of, and attempting to, secure boot will use these certificates
- Use **SET LOADDEV** command to set load parameters
- **IPL LOADDEV** to boot your secure guest

SE/HMC Certificate Management – Certificate View

IBM Hardware Management Console

SEARCH FAVORITES acsadmin

Home

Secure Boot Certificate ...

Secure boot certificate management

Manage secure boot certificates by importing them to systems and assigning them to partitions.

Filter

System

All systems

Partitions

All partitions

Certificates

Search certificates

Assign

Import

<input type="checkbox"/>	Name	Description	Systems	Partitions	Assigned
<input type="checkbox"/>	RedHat 8 certificate	Secure boot certificate for RHEL 8	1	0	—
<input type="checkbox"/>	zLinux certificate	Certificate for Linux on Z secure boot	1	6	✓
<input type="checkbox"/>	zOS validated boot certificate	Certificate for secure boot with new z/OS	1	8	✓

Items per page: 5

1–3 of 3 items

1 of 1 page

SE/HMC Certificate Management - Import

The image displays two sequential screenshots of the IBM Hardware Management Console (HMC) interface, specifically the 'Import certificate to systems' workflow.

Left Screenshot: Select certificate

- Import certificate to systems** (Title)
- Select systems** (Selected)
- Select certificate** (Selected)
- Certificate details** (Unselected)
- Summary** (Unselected)
- Select import method**
 - ☐ USB
 - ☒ FTP server
- Hostname** (Text field)
- User name** (Text field)
- Password** (Text field with eye icon)
- File path** (Text field)
- Protocol** (Dropdown menu, currently set to FTP)
- Buttons:** Cancel, Previous, Next

Right Screenshot: Certificate details

- Import certificate to systems** (Title)
- Select systems** (Selected)
- Select certificate** (Selected)
- Certificate details** (Selected)
- Summary** (Unselected)
- Certificate name** (Text field, value: RedHat 8 certificate)
- Certificate description** (Text field, value: Secure boot certificate for RHEL 8)
- Certificate type** (Text field, value: Self-signed root certificate)
- Expires** (Text field, value: 12/31/2031, 11:59:59 PM)
- Subject name** (Text field, value: IBM Corp)
- Issuer name** (Text field, value: IBM Corp)
- SHA-256 fingerprint** (Text field, value: 78 3F 4D 25 35 A5 98 58 52 A2 07 5E 58 97 BC A0 A5 1E 26 27 3E DD C1 7B 0E 58 38 CB CE F5 CE CC)
- Buttons:** Cancel, Previous, Next

SE/HMC Certificate Management - Assign

IBM Hardware Management Console

Home Secure Boot Certificate ...

Assign certificate to partitions

Select certificate

Select the certificate you would like to assign.

Search certificates

Name	System	Description
<input checked="" type="radio"/> RedHat 8 certificate	HJVS2EKN	Secure boot certificate for RHEL 8
<input type="radio"/> zLinux certificate	HJVS2EKN	Certificate for Linux on Z secure boot

Items per page: 5 1-2 of 2 items 1 of 1 page

Cancel Previous Next

IBM Hardware Management Console

Home Secure Boot Certificate ...

Assign certificate to partitions

Select partitions

Select one or more partitions to assign the certificate to.

Search partitions

Name	System
<input checked="" type="checkbox"/> BLUEC1	HJVS2EKN
<input checked="" type="checkbox"/> BLUEC2	HJVS2EKN
<input type="checkbox"/> BLUEC3	HJVS2EKN
<input type="checkbox"/> BLUEC4	HJVS2EKN
<input type="checkbox"/> CF01	HJVS2EKN

Items per page: 5 1-5 of 93 items 1 of 19 pages

Cancel Previous Next

SET LOADDEV SCSI (Class G)

June 2023

```
>>-Set--LOADDEV+---CLEAR-----+--><
      |               +-SCSI--+      |
      +-+-----+---+-----+ | SCSI Operands |---+
      ' -CLEAR-' '              '              '
      ' --ECKD--- | ECKD Operands |--'
```

SCSI operands

```
.-----+-----+-----+-----+-----+-----+-----+-----+-----+
V                                             |
|-----+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
| -+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|   +-PORTname--hhhhhhhh hhhhhhhh-----+
|   +-LUN--hhhhhhhh hhhhhhhh-----+
|   +-BOOTprog--+---bootprog_number--+---+
|   |               '--AUTOMATIC-----' |
|   |               |                     |
|   +-BR_LBA--hhhhhhhh hhhhhhhh-----+
|   +-+---NOSECURE--+-----+
|   | '-SECURE---' |
|   |               .-APPend-. |
|   '-SCPdata--+-----+---+---+---+---+---+---+---+---+---+---+---+
|               +-NEW---+   '-HEX-'   '-text---'
|               '-offset-'
```

- SECURE valid only when DEVICE operand is used
- LOADDEV directory statement updated accordingly
- DUMPDEV has similar enhancements
- Associated DIRMAINT support added (VM66424)

SET LOADDEV ECKD (Class G)

June 2023

```
>>-Set--LOADDEV+--CLEAR-----+--><
      |               +-SCSI--+      |
      +-+-----+--+-----+ | SCSI Operands |--+--+
      ' -CLEAR- ' '              '
      ' --ECKD--- | ECKD Operands | --'
```

ECKD operands

```
.-----+-----+-----+-----+-----+-----+-----+-----+-----+
V                                             |
|-----+-----+-----+-----+-----+-----+-----+-----+-----+
| -+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+---+
|      |      |      |      |      |      |      |      |      |      |
| +-BOOTprog--+bootprog_number--+-----+
|      |      |      |      |      |      |      |      |      |      |
|      |      |      |      |      |      |      |      |      |      |
| +-BOOTREC--+cyl head rec--+-----+
|      |      |      |      |      |      |      |      |      |      |
|      |      |      |      |      |      |      |      |      |      |
| +-+---NOSECURE+-----+
| | -SECURE---'
| |      .-APPend-.
| | -SCPdata--+-----+---+---+---+---+---+---+---+---+---+---+---+---+
| |      +-NEW---+ | -HEX- ' | -text--- '
| |      '-offset-'
```

- SECURE valid only when DEVICE operand is used
- LOADDEV directory statement updated accordingly
- DUMPDEV has similar enhancements
- Associated DIRMAINT support added (VM66424)

June 2023

```
|-----+-----+-----+-----+-----+-----+-----+-----|
|'-LOADParm--load parm-'  '-STOP-'    '-ATTN-'
```

- LOADDEV / DUMPDEV point to parms set with SET LOADDEV or DUMPDEV
- IPL directory statement contains new LOADDEV option
- OPTION directory statement can enforce use with SECUREIPLREQ

Secure IPL for z/VM Guests

June 2023

▪ Available for z/VM V7.3

- <https://www.vm.ibm.com/newfunction/#gsipl>
- Requires Driver D51C Bundle 19 for IBM z16 or IBM LinuxONE Emperor 4
- Refer to Machine Field Alert for required Linux OS services levels
 - <https://www-40.ibm.com/servers/resourcelink/lib03020.nsf/pagesByDocid/272B3DD994A65B538525899F005FA0E6?OpenDocument>

- z/OS will only run in audit-mode, due to a requirement for Virtual Flash Memory
 - Use SET LOADDEV...NOSECURE when IPL'ing z/OS guests under z/VM

Component	APAR	PTF	RSU
CP	VM66434	UM90281	-
DirMaint	VM66424	UV99435	-
SMAPI	VM66650	UM90300	-

Looking Ahead

z/VM Continuous Delivery Page

- Gives an overview of new function that is under consideration. Allows clients to:
 - Express interest in being a sponsor user for an item.
 - Plan for new support coming out in the future.
 - Understand the value, benefit, and impact of new enhancements.
- <https://www.vm.ibm.com/newfunction/>
- Subscribe for updates via “Notify me” link on left navigation bar.

z/VM

- News
- About z/VM
- Events calendar
- Products and features
- Downloads
- Technical resources
- Library
- How to buy
- Install
- Service
- Support
- Education
- Site map
- Site search
- Printer-friendly
- Notify me**

z/VM Continuous Delivery News

News on upcoming and available new function for z/VM

Last Updated: 8 October 2020

Change Summary

- October 8: Added Environment variable name field. See [Characteristics of a New Function APAR](#) for more information. Various content edits.
- September 25: Added IPv6 Layer 2 Query VSwitch Support and various content edits.

Introduction

Not all enhancements to z/VM are part of a new release or even a formal IBM announcement letter. This page is a resource to learn about enhancements going out through continuous delivery for z/VM. It's also different from formal announcements as it shows work in progress. Think of it as a living preview announcement for z/VM. As significant changes take place, this page will be updated. Check back often or [subscribe](#). Note: The z/VM Web site subscription service is intended to provide email alerts when specific z/VM pages are updated. If you are interested in receiving APAR updates, click the link for the individual APAR and subscribe to updates on that page.

You may notice that some new functions are actively seeking sponsor users. If you are interested in becoming a sponsor user for a particular function, visit the [z/VM Sponsor User](#) page for more details. Also important, these and other ideas from customers and vendors are frequently discussed at the z/VM Council. For more information and details on how to join, please see the [z/VM Council web page](#). For a complete history of updates, please see the [z/VM Continuous Delivery spreadsheet](#).

+ Characteristics of a New Function APAR

New Function APARs

New function in progress	Target date	Last updated
Active Drain for PAGE Volumes *	TBD	October 14, 2019
AP Crypto Interruption Support *	2Q 2021	September 4, 2020
Automatic STANDBY Memory for Guests	1H 2021	July 29, 2020
CP New Feature Interrogation API *	October 2020	October 8, 2020
CP Query Devices	December 2020	October 8, 2020

Security on the z/VM Continuous Delivery Page

▪ System SSL 2.5 Uplift

- Upgrade of z/VM V7.3 crypto library from z/OS 2.3 to z/OS 2.5 levels
 - Includes foundation for TLS 1.3 and RSA-SSAPSS support
 - Includes foundation for FIPS 140-3 support
- Future PTFs required to enable these items
- V7.3 only; no support for z/VM V7.2.

▪ Enhanced Authorization Controls for Crypto Domains

- Updates to allow for more granular control of crypto resource virtualization
 - CONTROL and/or USAGE domain support
 - **CONTROL**: “Can I manage the keys?”
 - **USAGE**: “Can I use this crypto resource?”
 - As assigned at the HMC/SE
- Allows for a TKE catcher utility to run in a Linux on z/VM guest... without requiring domains be reassigned
 - Ease of use: key material management for a z/VM partition
 - Some updates to USER DIRECT syntax and terminology
 - Education will be delivered concurrently. :-)

Security **not** on the z/VM Continuous Delivery Page

*This slide intentionally left blank.
(Insert joke about observability of quantum state here.)*

Questions?

Thank you!

- **z/VM New Function Page and Sponsor User Program:**
<https://www.vm.ibm.com/newfunction>



Disclaimer

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. Target dates shared here are not formal commitments, but meant to assist in your planning purposes. Because of the likelihood of changes, we highly recommend [subscribing to the notifications](#) for this page.

- **z/VM Security Page:**
<https://www.vm.ibm.com/security>

Contact Information:

Brian W. Hugenbruch
IBM Z Security for Virtualization & Cloud
bwhugen@us.ibm.com

@Bwhugen

@the_lettersea

CISSP®

IBM Products & Solutions Services & Consulting Learn & Support Explore more

z/VM News About z/VM Events calendar Products and features Downloads Technical resources Library How to buy Install Service Support Education Site map Site search

Last Updated: 16 June 2021

Security Home News Service Pubs Best Practices

z/VM Security and Integrity Resources

- [Recent z/VM Security News](#)
- [Service Information for RACF for z/VM \(and related topics\)](#)
- [Publications, Papers, and Books](#)
- [z/VM Security Best Practices](#)

The z/VM virtualization platform has been addressing information security requirements for hosted workloads for decades. IBM first issued its System Integrity Statement for z/VM in 1973, and continues to affirm it in each new release. The statement reads, in part:

IBM has implemented specific design and coding guidelines for maintaining system integrity in the development of z/VM. Procedures have also been established to make the application of these design and coding guidelines a formal part of the design and development process. However, because it is not possible to certify that any system has perfect integrity, IBM will accept APARs [problem reports] that describe exposures to the system integrity of z/VM or that describe problems encountered when a program running in a virtual machine not authorized by a mechanism under the customer's control introduces an exposure to the system integrity of z/VM [...] IBM will continue its efforts to enhance the integrity of z/VM and to respond promptly when exposures are identified.

For more information on z/VM Security, whether it relates to service, certifications, configuration, best practices, or something else, please consult the links at the top of this page. If you have any questions or suggestions, please reach out to Brian Hugenbruch (z/VM Security Development Champion) at bwhugen@us.ibm.com.