

# z/VM 7.3 Security News and How To's – 2024

**Brian W. Hugenbruch, CISSP**

IBM LinuxONE Resiliency Lead &&

IBM z/VM Security and Cryptography Product Owner

[bwhugen@us.ibm.com](mailto:bwhugen@us.ibm.com)

 @Bwhugen

 @the\_lettersea



## Agenda

Why secure virtualization?

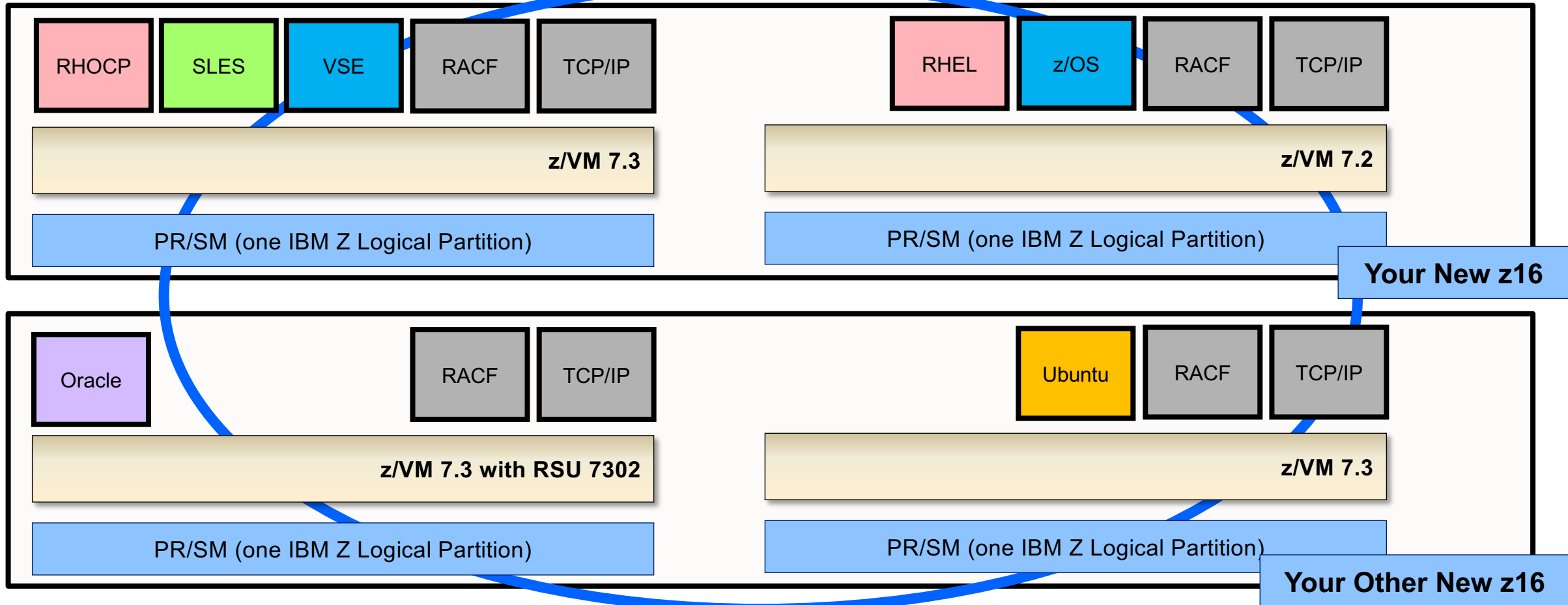
The IBM Z Security Portal

Short Topics in z/VM V7.3 Security

A Deeper Dive on KEYVAULT and Compliance

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

# Is z/VM certified?

| z/VM Level | Common Criteria   |   | FIPS 140-2               |
|------------|---|---|--------------------------|
| 7.4        | TBD   | TBD   | TBD                      |
| 7.3        | Not evaluated ("designed to conform to standards")                    |   |                          |
| 7.2        | <b>BSI OSPP (with Virt and Labeled Security extensions) at EAL 4+</b> | <b>NIAP VPP with Server Virtualization Extended Package</b> | <b>Level 1 Validated</b> |
| 7.1        | Not evaluated ("designed to conform to standards")                    |   |                          |
| 6.4        | OSPP with Labeled Security and Virtualization at EAL 4+ --            |   | <b>Level 1 Validated</b> |

*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.

# IBM's Commitment to Security & Integrity



The graphic features a black header with the text "IBM z/OS® System Integrity Statement" on the left and the IBM logo on the right. Below the header is a collage of images: a man in a suit, a stethoscope, a group of people, a padlock, a woman, and server racks. At the bottom of the graphic, there is a reflection of the padlock image.

**First issued in 1973 & Reaffirmed in 2007**

***IBM's long-term commitment to System Integrity is unique in the industry, and forms the basis of z/OS & z/VM industry leadership in system security***

“System Integrity” is defined as the inability of any program not authorized by a mechanism under the installation’s control to circumvent or disable z/OS or z/VM Security Controls

In the event that an IBM System Integrity problem is reported, IBM will always take action to resolve it.

IBM’s commitment extends to design, development and test practices. Including the creation of the *IBM Z Center for Secure Engineering* to provide additional security focused testing and scrutiny.

The IBM Z Security Portal informs clients about the latest security and system integrity service to help keep their enterprise up to date



“Is z/VM vulnerable to That Thing I  
Heard About On The Internet?”

“It  
depends.”





# "Is z/VM vulnerable to \_\_\_\_\_?"

IBM Z Security policy [prohibits general disclosure of vulnerability analyses \(negative or positive\)](#)

- Policy of responsible disclosure
- Mindful of client patch policies and speeds

To stay current, **your company** can register with the IBM Z Security Portal

- Manually vetted and verified process for enrollment
- Separation of access and notifications by products licensed
- Receive up to date lists regarding APAR/PTF information and CVSS scoring for SEC/INT service as it becomes available.
- Security Bulletins regarding high-profile security issues, notifications and possible warnings

## IBM Z Security Portal >> What Is It?

- Only available to IBM Z clients
- Clients must **register** to gain access
- Recommend clients **subscribe** for email notification
- Contains APAR/PTF numbers for all applicable exposures
  - Customers are considered exposed if they run affected product/component
  - No other details that could be used to potentially exploit are provided
- Industry standard scoring for risk assessment (**CVSS**)
- APAR/PTF fix information posted when fix is available
  - z/OS → SMP/E SECINT ++HOLDDATA and ++ASSIGN statements
  - z/VM → **APAR/PTF/COMPID**
- Security Notices for higher visibility vulnerabilities or issues
  - Including non-SMP/E products and general security communications

## IBM Z Security Portal >> Security Notices

- **Security Notices** are text (bulletin-like) documents provided on the Security Portal to communicate [information for highly publicized vulnerabilities](#) that may generate many inquiries.
  - Introduced in 2014
  - Updated as investigation progresses and whenever new information is available
  - May include mitigations if pertinent
  
- Concerns with responding to vulnerability requests in a PMR:
  - investigation may still be in progress; may make responses **incomplete or inaccurate**
  - information may be **updated** several times through the investigation.  
[Portal subscribers are notified each time there is an update.](#)
  - confirming an exposure with **no mitigation** puts all clients at risk
  - there are **many security fixes** identified on the Security Portal and reacting only to the highly publicized vulnerabilities is not a good/complete security process

# IBM Z Security Portal >> Sample z/VM CVSS Data

\* \* IBM Confidential \* \*

(Well, not in this example. This is made up.)

| YrDay | COMPID    | APAR    | Rel  | PTF     | CVSS Base/Temporal/Vector   |
|-------|-----------|---------|------|---------|---|
| ...   |           |         |      |         |   |
| 00000 | 568411201 | VM12345 | R710 | UM54321 | 4.3/3.7/ (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H/RL:O/RC:C) |
| 00000 | 5735FAL00 | PI23456 | R710 | UI65432 | 6.4/5.6/ (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L/RL:O/RC:C) |
| 00000 | 5735FAL00 | PI34567 | R710 | UI76543 | 7.5/6.5/ (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L/RL:O/RC:C) |
| 00000 | 5735FAL00 | PI45678 | R710 | UI87654 | 2.6/2.3/ (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H/RL:O/RC:C) |
| ...   |           |         |      |         |   |

Dates removed

APAR numbers changed

PTF numbers changed

Fake scores / vectors

# IBM Z Security Portal

**Portal Login:** <https://www.ibm.com/support/resourcelink/security-portal/resources>

**Request Access Here:** <https://www-50.ibm.com/systems/campaignmail/z/capabilities/system-integrity/register-zsecurity-portal>

# 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](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:

- If using Multi-factor Authentication, make sure you have one userid with PWFALLBACK
- 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 CLOAD 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 (“Failsoft” passwords)
- 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 31<sup>st</sup>, 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*

**“Getting Started with IBM Z Crypto”  
Thursday, 1pm, Room 2201**

- 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.

# 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)

- 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 myvm.sys.ibm.com bwhugen
```

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

```
DMSKEY2405I KEYVAULT stored values:
```

```
DMSKEY2405I Label: myvm.sys.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 | 2301RSU |
| SES       | VM66457 | UM90289 | 2401RSU |
| TCPIP     | PH51239 | UI91775 | 2401RSU |



# z/VM Systems Security and Compliance Utility

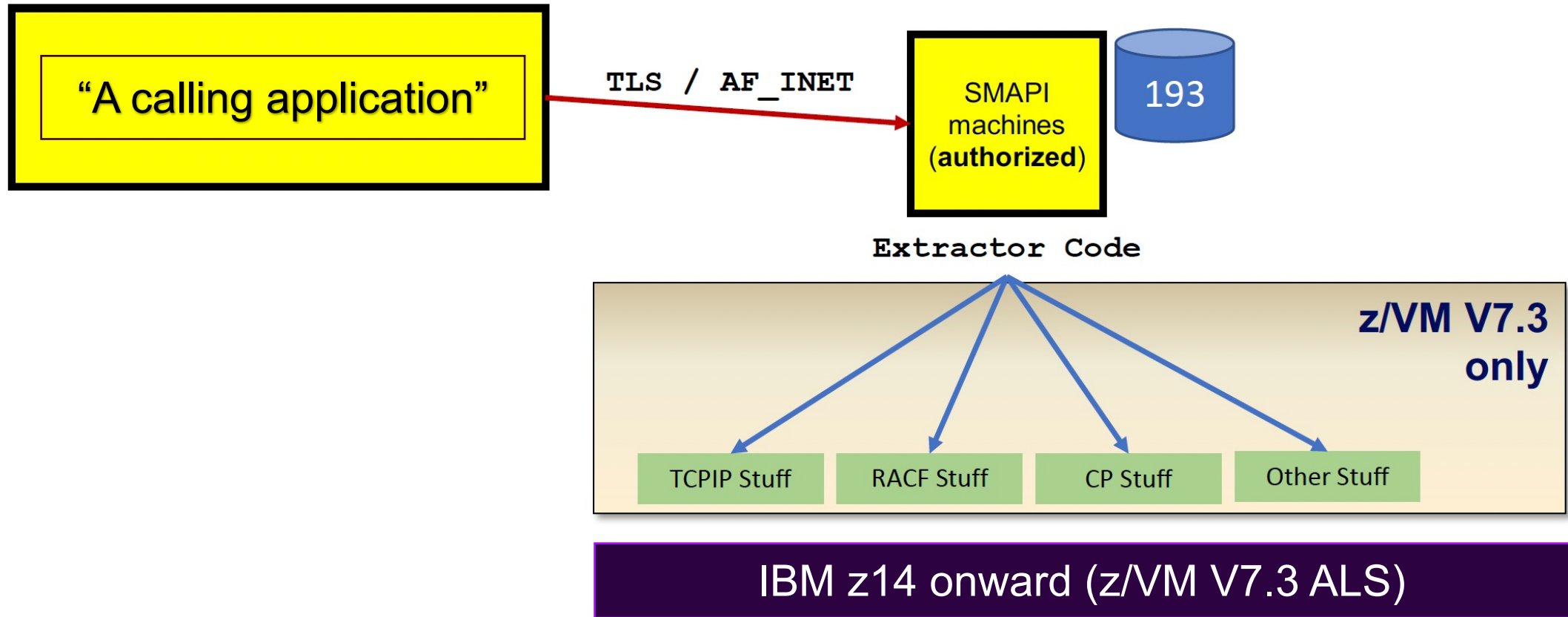
June 2023

- **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?

- 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?<br>Encrypted Paging<br>TLS enabled (TLS 1.2)<br>REQUIRED settings for Secure Telnet, FTPS, SMTP, RSCS<br>VLAN configuration for Vswitch<br>Is an ESM enabled Yes/No  |
| 7                   | Need To Know restrictions   | How many machines are > Class G?    Are they LBYONLY?<br>Are there machines in the user directory with privileged options?    Are they LBYONLY?<br>Who's on the TCPIP OBEY List / SSL_Admin_List?<br>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?<br>ESM control of VLAN settings (RACF VMLAN class)?<br>Can a Class G guest create a transient Guest LAN?<br>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<br>...And default minidisk password values<br>RACF SYSSEC settings around DEFER<br>RACF Audit SEVER=YES  |
| 8                   | Identify and authenticate access to system components   | RACF: password/phrase intervals (min/max)<br>RACF: password/phrase expiry<br>RACF password history settings<br>RACF password encryption – KDFAES?<br>RACF: are the password exits enabled?<br>Is MFA enabled?<br>Is anyone enabled for PWFALLBACK?<br>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<br>QUERY CPLEVEL<br>QUERY CMSLEVEL<br>NETSTAT TCP/IP level output<br>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

# What can be done with this output?

## ▪ Config verification

- Confirms upgrade completion and success
- Points out where certain virtual machines were missed (e.g. RACMAINT)
- Finds areas where old crypto algorithms are in use
- VLAN mapping

## ▪ Foundational delta

- Output should not change day to day
- This means change is detectable by hash verification
  - While there's no official IBM utility to do this, that's easy to automate via Pipelines
  - If there's a change in hash, the system settings have been modified
  - Combined with hashes of System Configuration, User Directory, and RACF database, you have the beginnings of Type 1 Resiliency mapping

## ▪ Local analysis

- Machine-readable format can validate config to local standards
- Actual compliance metrics will require some engineering...

# 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
  - 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 | 2401RSU |



# 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.

The screenshot shows the 'z/VM Continuous Delivery News' page. The left navigation bar includes links for 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, and Notify me. The main content area features a 'Change Summary' box with updates from October 8 and September 25. Below this is an 'Introduction' section explaining the continuous delivery process. A section titled '+ Characteristics of a New Function APAR' is followed by a table of '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 future TLS 1.3 and RSA-SSAPSS support
  - Includes foundation for future FIPS 140-3 support
- Future PTFs will be required to enable those 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-only domain support
  - In-line with the Support Element's controls for crypto resources assigned to an LPAR
- 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

***“Trusting Your Code”  
Friday, 1pm, Room 1201***

**Questions?**

# For more information



Brian W. Hugenbruch

IBM LinuxONE Resiliency Lead &&

IBM z/VM Security and Cryptography Lead

## IBM webpage:

<https://www.vm.ibm.com/devpages/hugenbru/>


## z/VM Security Page:


<https://www.vm.ibm.com/security>

Technical Blog: <https://bwhugen.github.io/>

## Social Media:

 <https://www.linkedin.com/in/bwhugen/>

 @the\_lettersea

 @apictureofaman@infosec.exchange

# THANK YOU

