z/VM Security News and How To's

Introducing z/VM V7.3 and recent security features

Brian W. Hugenbruch, CISSP
z/VM Security Nerd
bwhugen@us.ibm.com @Bwhugen

Agenda

- Why protect virtualization?
- Introducing z/VM V7.3
- RACF for z/VM
- Virtualized Crypto Management
- TLS and Network Security

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

z/VM 7.3

- Planned 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 Security Certifications

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

z/VM Level	Common Criteria	
z/VM 7.3 (coming soon)	*Not evaluated ("designed to conform to standards")*	
z/VM V7.2	***BSI OSPP (with Virt and Labeled Security extensions) at EAL 4+ -- Completed!***	***NIAP VPP with Server Virt. Extended Package***
z/VM 7.1	*Not evaluated ("designed to conform to standards")*	
z/VM 6.4	OSPP with Labeled Security and Virtualization at EAL 4+ -- ***COMPLETED!*** *http://www.ocsi.isticom.it/index.php/elenchi-certificazioni/in-corso-di-valutazione*	

z/VM Level	FIPS 140-2
z/VM 7.3 (coming soon)	*Not evaluated ("designed to conform to standards")*
z/VM V7.2	***FIPS 140-2 L1 for z/VM System SSL and ICSFLIB – Completed!***
z/VM 7.1	*Not evaluated ("designed to conform to standards")*
z/VM 6.4	FIPS 140-2 L1 -- ***COMPLETED!*** *https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3374*

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

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)**

z/VM 7.2 – System Default Changes

- **TDISK clearing**
  - The default has changed to Enabled.
- The SRM unparking model
  - The default unparking model has changed from HIGH to MEDIUM.
- System Recovery Boost
  - SRB has been enabled by default
  - Still requires z15 or newer and appropriate configuration.
- **z/VM Directory Maintenance (DirMaint)**
  - NEEDPASS - the default value has changed to No
  - DVHWAIT BATCH and CLUSTER INTERVAL values have been updated to improve DirMaint's overall processing time in response to directory change requests.
- **Telnet Server Certificate Check**
  - Changed from CLIENTCERTCHECK NONE to **CLIENTCERTCHECK PREFERRED**
  - Change made to z/VM 7.1 with APAR PH18435

SHARE
EDUCATE ‣ NETWORK ‣ INFLUENCE

RACF for z/VM

z/VM 7.3: RACF and 8-Member SSI

- 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

If you have zSecure for RACF/VM 2.5.1 (GA on 17 June 2022!), you now have **SIEM integration**, an **SMF cache server**, **support for MFA**, 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

SHARE
EDUCATE ‣ NETWORK ‣ INFLUENCE

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 issued a corresponding Statement of Direction for z/OS Next.*

z/VM 7.3: ESM Control of DEFINE MDISK

https://www.vm.ibm.com/newfunction/#esm-define-mdisk

- DEFINE MDISK is a command sometimes used in z/VM DR 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
  - Base of z/VM V7.3 (no plans to backport)
  - Audit remains through DEFINE.A in RACF/VM
  - Broadcom will be introducing support as well (watch for updates)

Multifactor Authentication for z/VM

SHARE
EDUCATE ‣ NETWORK ‣ INFLUENCE

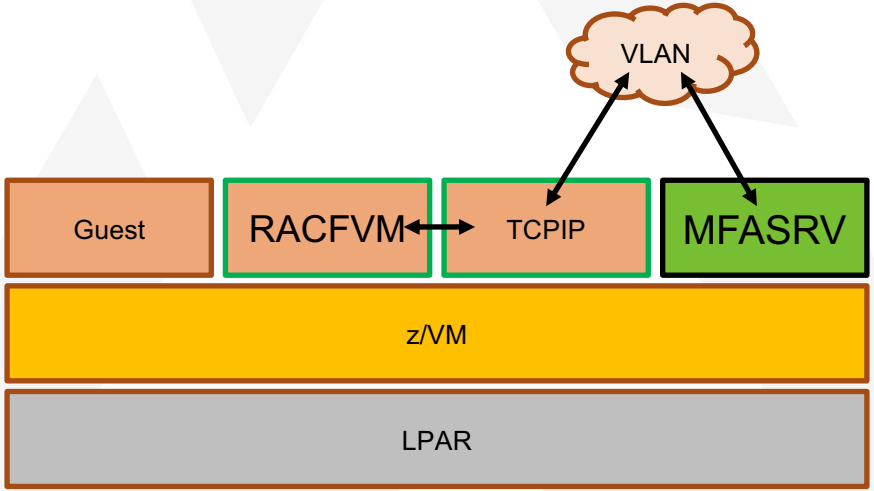
- **Multifactor Authentication support** enables a system administrator to logon to the hypervisor with one or several authentication credentials without requiring a traditional password or password phrase

- **Combination of:**
- A newer product (IBM Z Multifactor Authentication) running in a Linux on IBM Z guest
- z/VM with an External Security Manager updates
- TCP/IP communication from ESM to MFA (may require TLS server configuration)
- CP updates (apply the PTF for APAR VM66324)
- https://www.vm.ibm.com/newfunction/#mfa

Component	APAR	PTF	RSU
RACF	VM66338	z/VM 7.1 UV99363	TBD

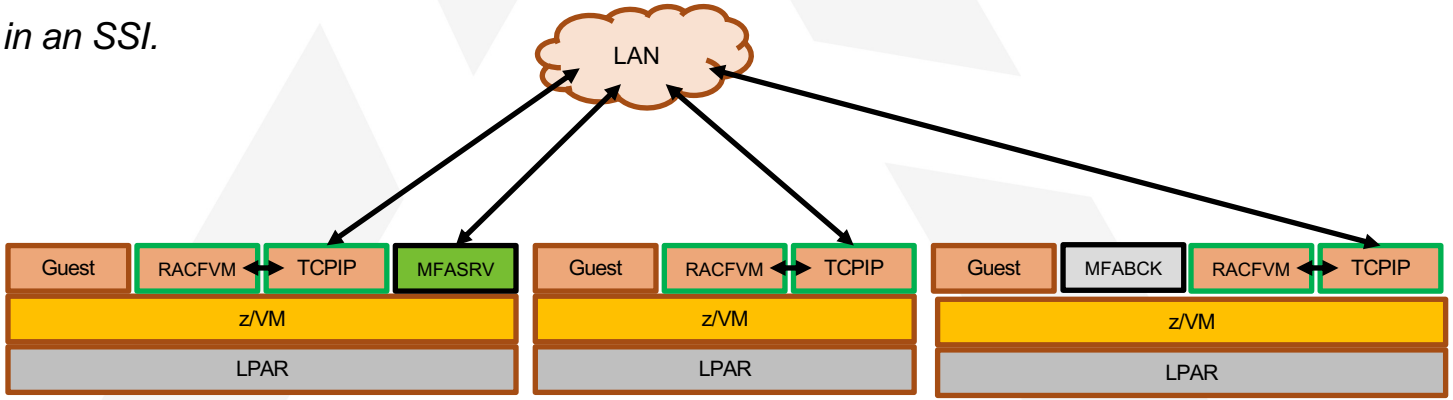
Where do I set up IBM Z MFA v2.2

- The constraint is ”one ESM database to one MFA server.”
- So you could do a single system…



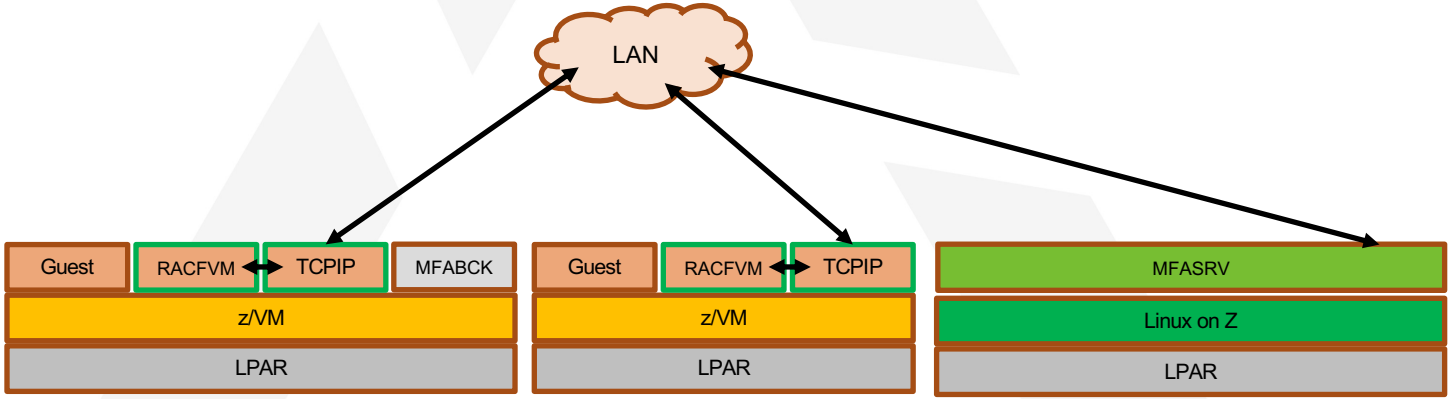
Where do I set up IBM Z MFA v2.2

- …or many systems*. Since it runs as a Linux on IBM Z guest, you could put the primary and back-up on different LPARs or CECs.
- **Be careful in an SSI.*



Where do I set up IBM Z MFA v2.2

- …since the requirement is Linux on Z, and communication is TCP/IP, you could even put the Linux guest in its own partition. Your ESM only cares about an IP address.



For more info…

https://www.vm.ibm.com/newfunction/#mfa

SHARE
EDUCATE • NETWORK • INFLUENCE

- IBM Z Multi-factor Authentication V2.2
  - Order through ShopZ
  - Yes, it'll say z/OS – don't panic. The Linux .iso will be available for download
- For more information:
  - **"Preparing for Multi-Factor Authentication on z/VM" presentation (recorded live at the VM Workshop):** https://www.youtube.com/watch?v=AFkOtgEZxAc
- Note: Apply VM66528: RACF FIXPACK for MFA ISSUES (PTFs for z/VM 7.1 or z/VM 7.2)

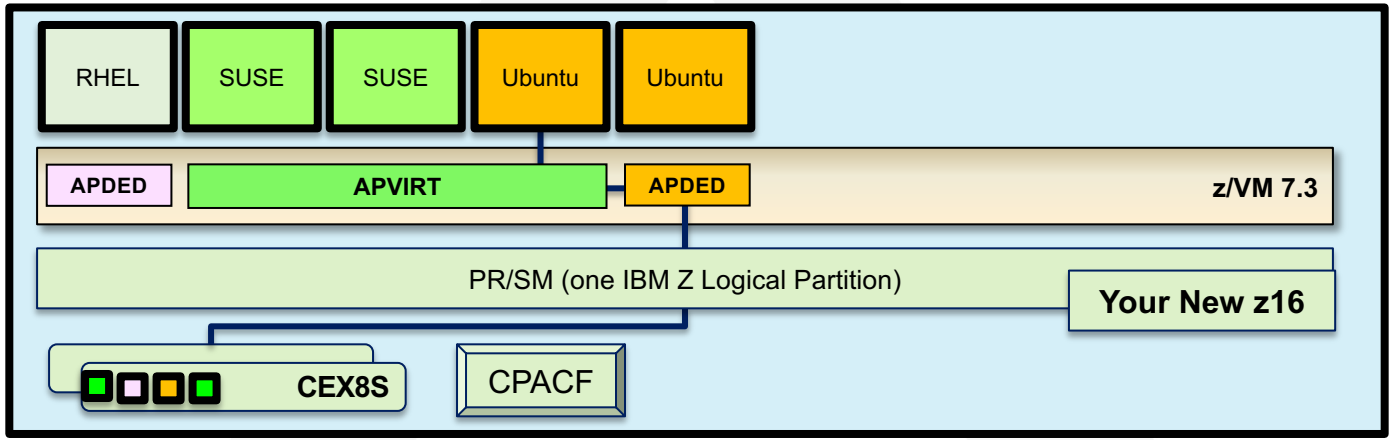
Component	APAR	PTF	RSU
CP	VM66324	UM35569	7.1 2101
RACF	VM66338	UV99363	7.1 2101
CA VM:Secure	**CA VM:Secure 3.2** with the following required PTFs: • SO11972 - CA VM:Secure 3.2 - RSU-2001 - Recommended Service • SO12552 - ENH: Multifactor Authentication (MFA) support		

SHARE
EDUCATE ‣ NETWORK ‣ INFLUENCE

Virtualizing IBM zSystems Hardware Cryptography

z/VM Virtualization of Hardware Cryptography

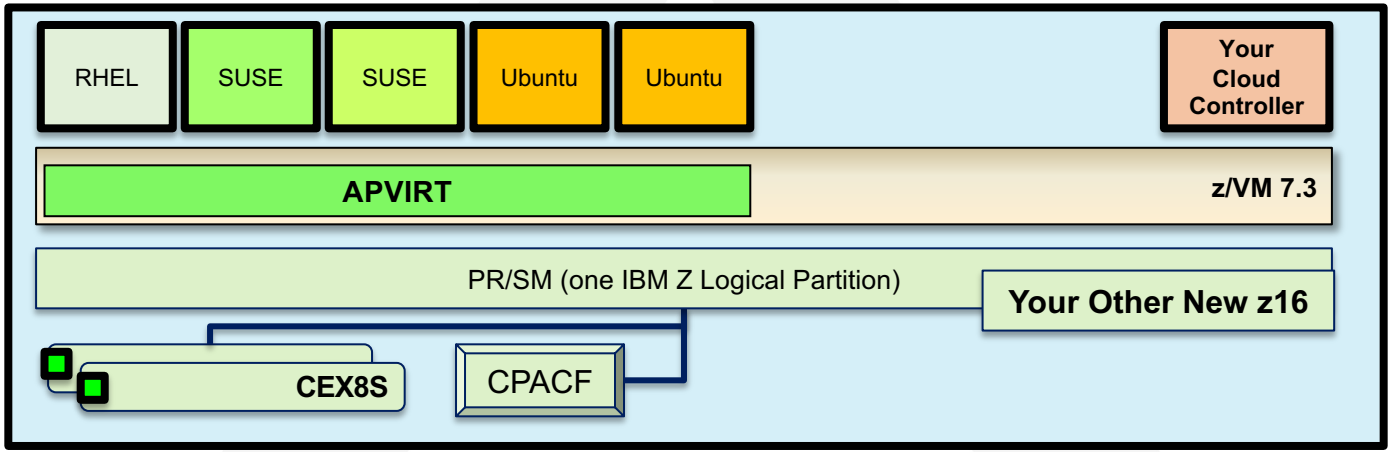
- Crypto Express features associated with your z/VM partition are **virtualized for the benefit of your guests**:



- **`APDED`** (“Dedicated”)
  Connects a particular AP domain (or set of domains) directly to a virtual machine – no hypervisor interference
  All card functions are available to the guest

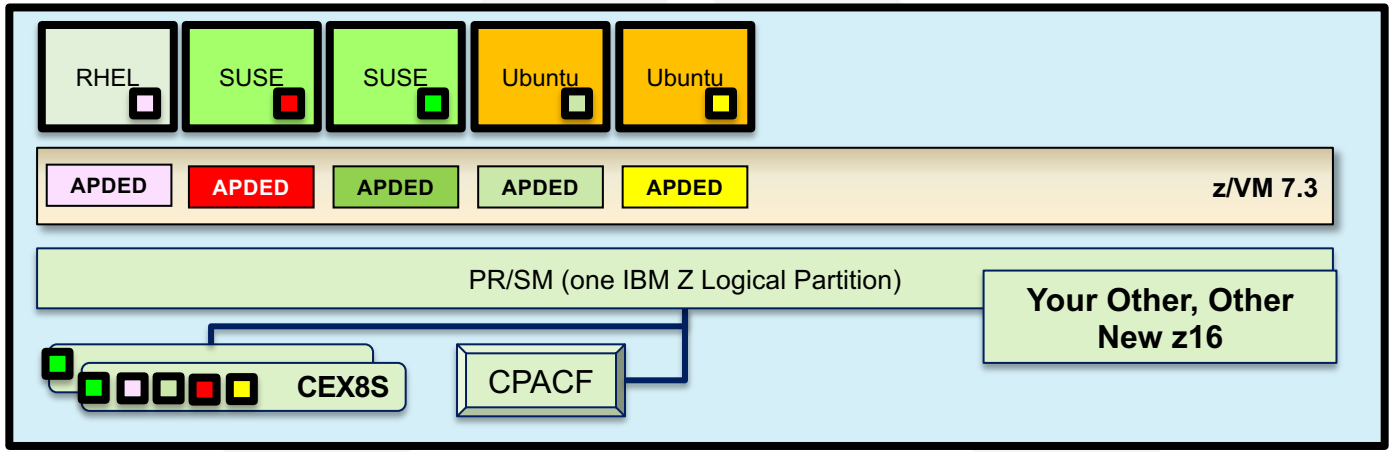
- **`APVIRT`** (“Shared”)
  Virtual machine can access a collection of domains controlled by the hypervisor layer
  Meant for **clear-key operations only** – sharing crypto material might otherwise break security policy.

Sample of Crypto Virtualization: LinuxONE Developer Cloud



- **Crypto operations**: SSH (RSA, SHA-2, AES), and *whatever data handled inside the guests*
- **Environmental Requirements**: Relocatable (it's a cloud)
- **Recommended Hardware**:
  - CPACF
  - Crypto Express CCA Accelerator in shared configuration (“APVIRT”)
    - Assign 1 domain from 2-3 different features (hardware failover, performance)

Sample of Crypto Virtualization: Hyperledger Fabric on Linux on IBM Z



- **Crypto operations**: A lot. It's a Blockchain
- **Environmental Requirements**: Protection of key material. (It's a Blockchain.)
- **Recommended Hardware**:
  - CPACF (required for secure and protected key ops on the crypto adapters)
  - Crypto Express CCA Coprocessors or EP11-mode Coprocessors, as appropriate
    - One domain per guest participating in the Hyperledger fabric

z/VM Support for IBM z16

z/VM 7.1, 7.2
PTF for APAR VM66532

EDUCATE ▸ NETWORK ▸ INFLUENCE

- With the PTF for APAR VM66532, z/VM® 7.1 and 7.2 provide support to enable guests to exploit function on IBM z16®. The following support is included:
- Breaking-event-address register (BEAR) enhancement facility, which facilitates the debug of wild branches.
- Reset DAT protection facility, which provides a more efficient way to disable DAT protection, such as during copy-on-write or page-change tracking operations.
- RoCE Express3 adapter, which allows guests to exploit Routable RoCE, Zero Touch RoCE, and SMC-R V2 support.
- The Crypto Express8S (CEX8S) adapter, supported as a dedicated or shared resource. Dedicated guests are able to take advantage of all functions available with the CEX8S adapters, including assorted new enhancements and use of Quantum-Safe APIs.

All crypto adapters that are configured in EP11 mode are reported with the 'P' suffix instead of the 'S' suffix (e.g., CEX8P).

A note on Quantum-Safe Crypto

SHARE
EDUCATE ▸ NETWORK ▸ INFLUENCE

This slide may or may not exist when you're not observing it.

Host Exploitation of Crypto Interruptions

- With the PTF for APAR VM66534, z/VM V7.2 supports host crypto-interruption exploitation for APVIRT cryptographic resources in the shared pool. The host is not required to poll cryptographic resources for replies that are ready to be delivered to the guest.
- Some performance benefit may be derived from enabling this capability

- Enabled by setting APVIRT POLLING to OFF
  - Not enabled by default via z/VM V7.2 PTF (default state is “polling is on”)

Commands impacted:

- **SET CRYPTO APVIRT POLLING** – change setting for entire APVIRT pool
- **QUERY CRYPTO POLLING** – query POLLING state [ON/OFF]

```
QUERY CRYPTO POLLING
```

```
Shared-crypto polling is OFF
Ready;
```

Dynamic Crypto Support for z/VM

https://www.vm.ibm.com/newfunction/#dynamic_crypto

z/VM 7.1
PTF for APAR VM66266

EDUCATE • NETWORK • INFLUENCE

Dynamic Crypto support enables changes to the z/VM crypto environment without requiring an IPL of z/VM or its guests (e.g. Linux on Z).

This allows:

- Less disruptive addition or removal of Crypto Express hardware to/from a z/VM system and its guests
- Less disruptive maintenance and repair of Crypto Express hardware attached and in-use by a z/VM system
- Reassignment and allocation of crypto resources without requiring a system IPL or user logoff/logon
- Greater flexibility to change crypto resources between shared and dedicated use.

Additionally, there are RAS benefits for shared-use crypto resources:

- Better detection of Crypto Express adapter errors with "silent" retrying of shared pool requests to alternative resources
- Ability to recover failed Crypto Express adapters
- Improved internal diagnostics for IBM service
- Improved logoff and live guest relocation latency for users of shared crypto.

z/VM Dynamic Crypto – Commands

z/VM 7.1
PTF for APAR VM66266

VARY ONLINE CRYPTO (B)

- Bring a Crypto Express adapter online

VARY OFFLINE CRYPTO (B)

- Take a Crypto Express adapter offline (device associations remain in place)

ATTACH CRYPTO (B)

- Add crypto resource(s) to your z/VM guest (or APVIRT)

DETACH CRYPTO (B or G)

- Remove dedicated crypto resources from a guest
- Remove crypto resources from the shared crypto pool
- Remove guest access to the shared crypto pool

DEFINE CRYPTO APVirtual (G)

- assign or reassign shared crypto resource access to a z/VM guest

QUERY CRYPTO DOMAINS (which is just what it sounds like)

z/VM Dynamic Crypto: Usage Notes

- Attachments persist even when a device is taken offline
- Resource assignment (dedicated/shared) does not change when an adapter is varied on/off

FORCE option is…..

- Not required when DETACHing crypto resources
- Required when VARYing OFF an adapter with crypto resources in use
- Either way, exercise caution when using

The Importance of Cryptographic Hygiene

SHARE
EDUCATE ‣ NETWORK ‣ INFLUENCE

- Dynamic Crypto gives you a lot of power to modify the environment
  - This is a good thing and a bad thing
  - **“With great power comes great responsibility.”**

- z/VM does not zeroize domains before reassigning to a guest (or to APVIRT)
  - We don’t want to make that assumption (traditionally, this is HMC territory)
  - **This might lead to “residual crypto” (Ewww)**

- Basic guidelines:
  - Zeroize (at HMC) when changing adapter modes or changing security zones
  - Changes between unused and APVIRT: safe (no key material involved)
  - Changes involving clear-key APDED: consider zeroizing
  - Changes involving secure-key APDED: definitely zeroize

- New chapter from z/VM Development now available via web / publications

Mixed-APVIRT
Live Guest Relocation

z/VM 7.2
PTF for APAR VM66496

EDUCATE ‣ NETWORK ‣ INFLUENCE

Mixed-APVIRT LGR allows flexible crypto configurations so guests using APVIRT can relocate with fewer hardware restrictions.

Removes restrictions on guest relocation in a z/VM Single System Image:

- *Then*: needed common type and mode (e.g., CEX7A) on source and target system
  - including firmware levels
- *Now*: guests in a relocation domain see lowest type of a common mode
  - E.g., a combination of CEX7A and CEX5A is seen as a CEX5A by all guests in that domain
  - Guests without a need to relocate, or in specialized domains, can see higher levels
  - Still requires common adapter “mode” (Accelerator or Coprocessor; EP11 cannot be relocated)

New Function APAR for z/VM V7.2 only

z/VM 7.2
PTF for APAR VM66496

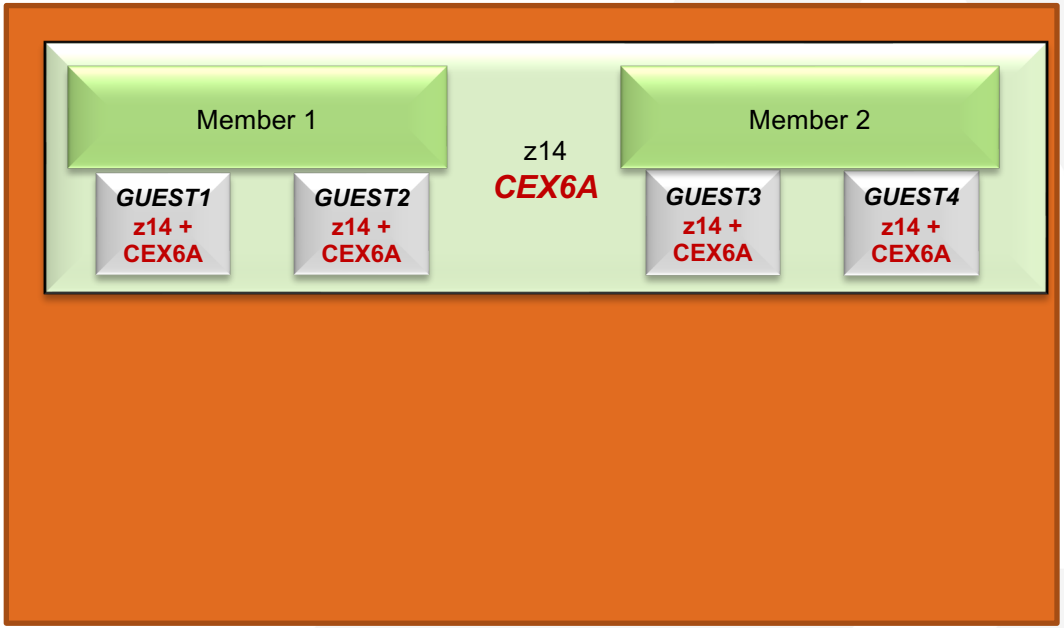
Shared Crypto Resources in Relocation Domains

- APVIRT crypto guests will see the lowest type of Crypto Express (CEX) adapter that is available in the shared pools of all systems in a relocation domain.
  - This is the level of functionality that enables guests to relocate between systems in the relocation domain without using the **FORCE ARCHITECTURE** option.

- **QUERY VIRTUAL CRYPTO**
  - Shows the lowest type of CEX adapter available in a guest's relocation domain
  - Only displays CEX adapters in the guest's relocation domain that have the same shared crypto mode as the current system
    - Shared pools can have adapters with either Accelerator (A) or CCA coprocessor (C) mode

Upgrading APVIRT Guests to a New Server

SSI Relocation Domain (default)

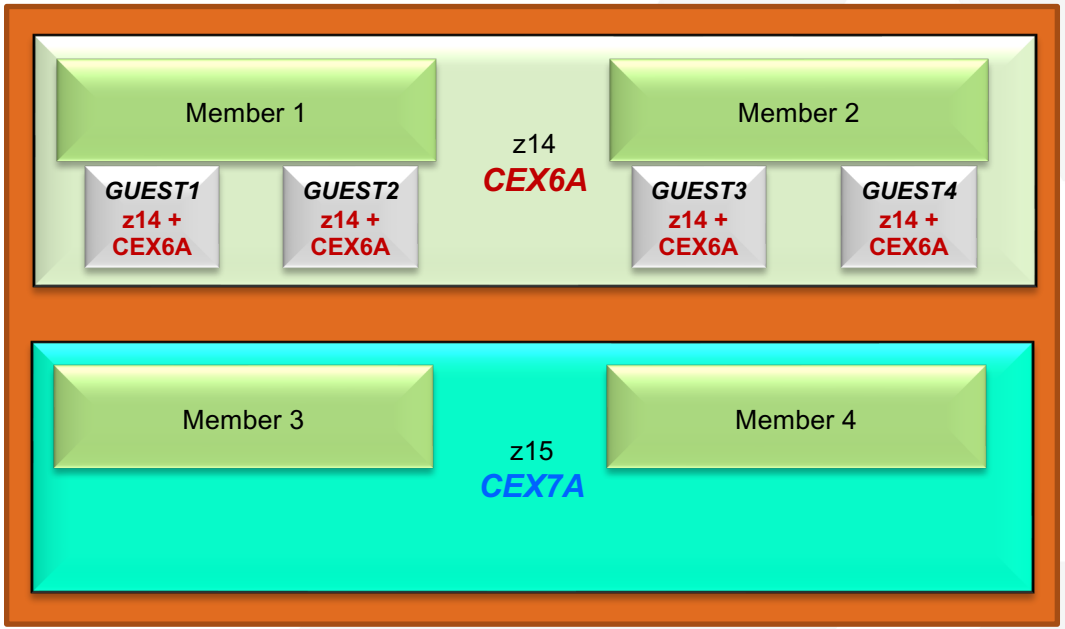


- 2 member SSI cluster
  - Both members on **z14** with **CEX6A** Crypto Express adapters
- SSI relocation domain
  - Includes all members of the cluster
- Crypto Express adapter level for APVIRT guests is **CEX6A**

** All systems have Improved LGR for Mixed-level Crypto function installed*

Upgrading APVIRT Guests to a New Server…

SSI Relocation Domain (default domain)

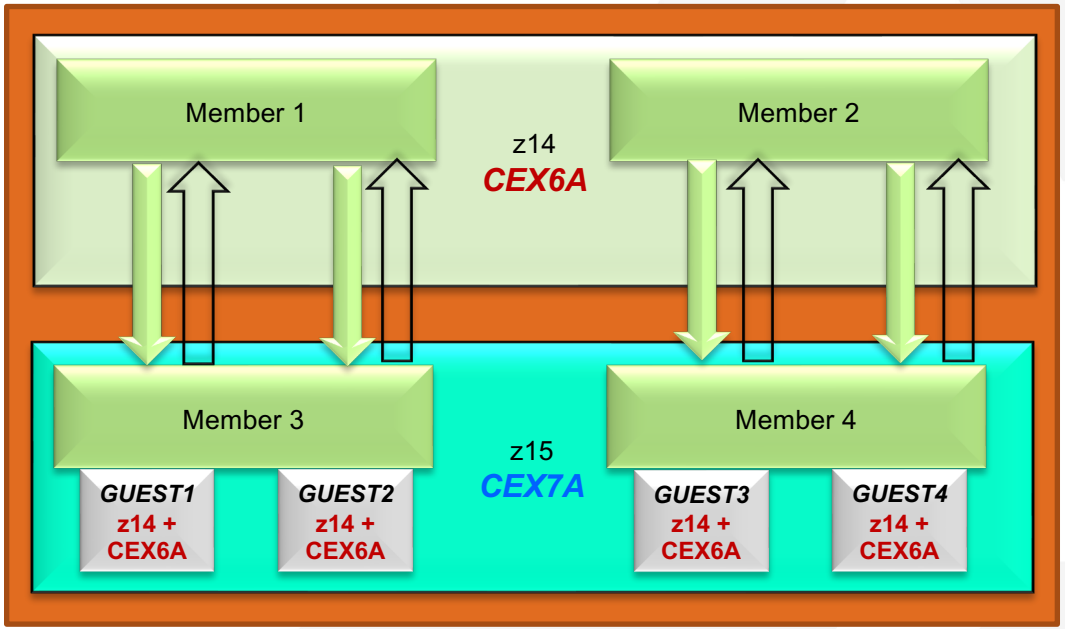


- Add members 3 and 4
  - On **z15** with **CEX7A** adapters
- All members are in SSI relocation domain

** All systems have Improved LGR for Mixed-level Crypto function installed*

Upgrading APVIRT Guests to a New Server…

SSI Relocation Domain (default domain)

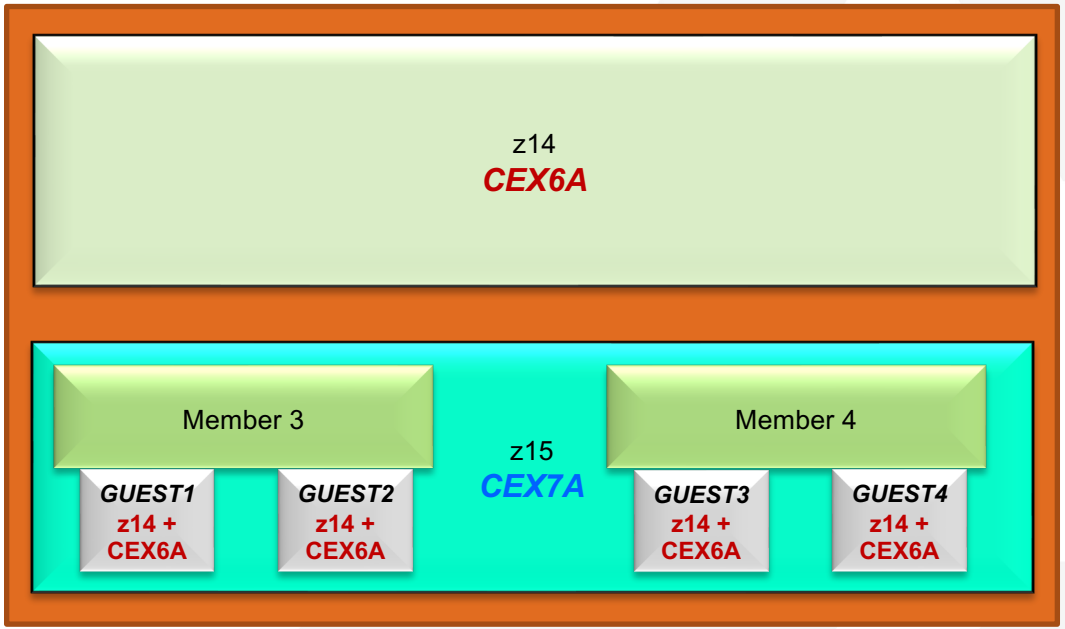


** All systems have Improved LGR for Mixed-level Crypto function installed*

- Functional level for guests on all members is still
  - **z14**
  - **CEX6A** for APVIRT guests
- This allows relocation of guests among all members without **FORCE ARCHITECTURE**

Upgrading APVIRT Guests to a New Server…

SSI Relocation Domain (default domain)

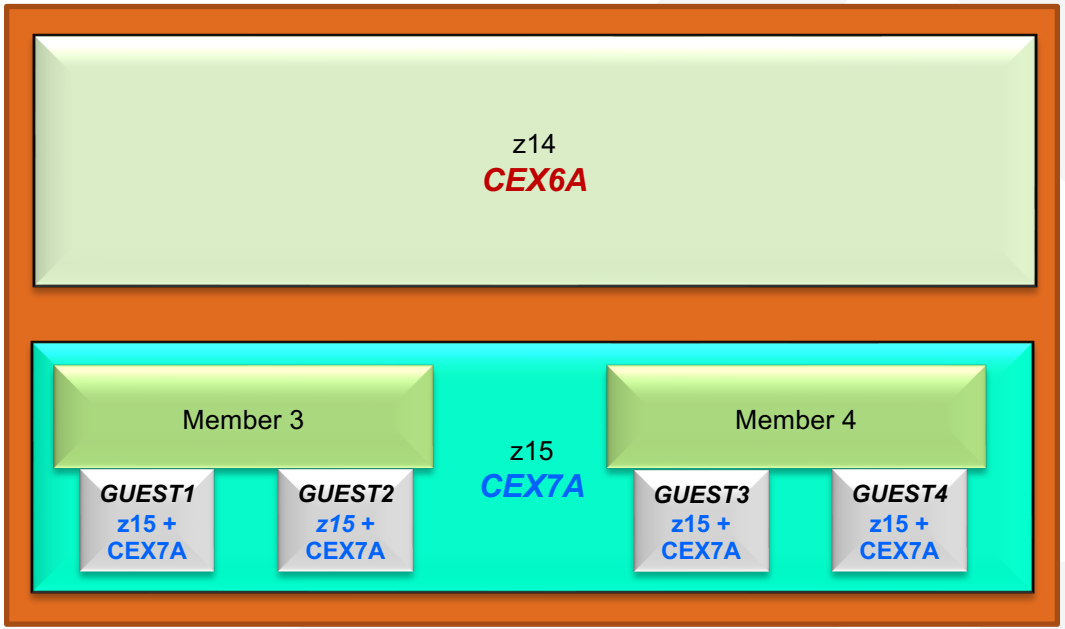


* *All systems have Improved LGR for Mixed-level Crypto function installed*

- Shutdown Member 1 and Member 2
- Remove them from SSI cluster configuration
  - **SET SSI SLOT 1 AVAILABLE**
  - **SET SSI SLOT 2 AVAILABLE**
- Update SSI statement in system config

Upgrading APVIRT Guests to a New Server…

SSI Relocation Domain (default domain)



- Functional level for guests changes to
  - **z15**
  - **CEX7A** adapter level for APVIRT guests

** All systems have Improved LGR for Mixed-level Crypto function installed*

Improved LGR for Mixed-Level Crypto

- New Function Page
  - https://www.vm.ibm.com/newfunction/#lgr-apvirt
- CP Function Environment Variable
  - **CP.FUNCTION.CRYPTO.MIXED_APVIRT** = 1

- Updated *z/VM: CP Planning and Administration*
  - Chapter 5: Crypto Planning and Management

Component	APAR	PTF	Available	RSU
CP	VM66496	z/VM 7.2 UM35893	August 6, 2021	TBD

z/VM 7.3 and Crypto

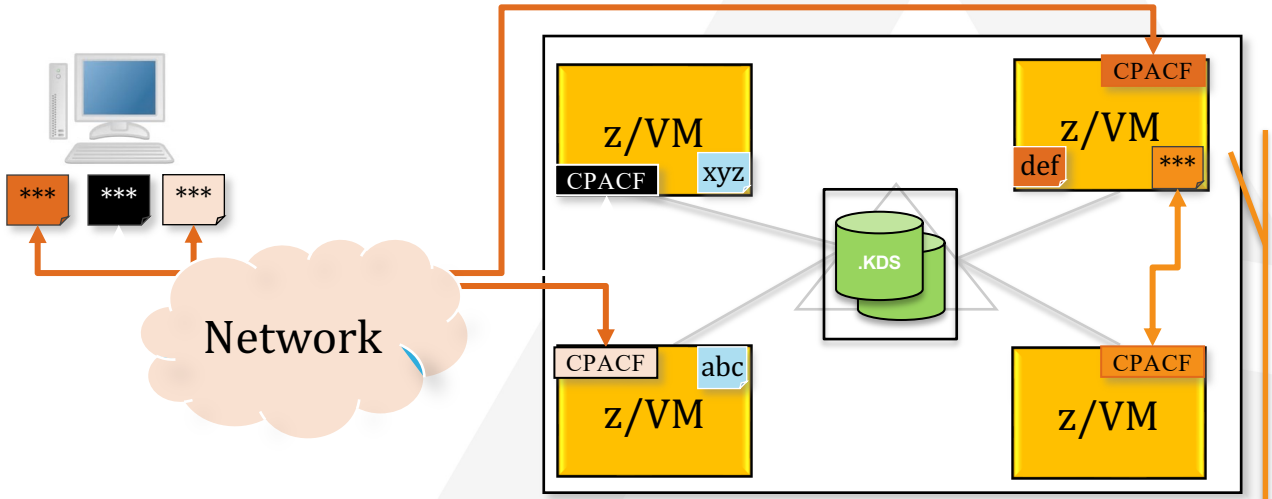
- Because of the Architecture Level Set, 730 will only support CEX6S and higher
- Because domains are assigned on a per-partition level, there's mostly no change to how SSI views the world
- No known performance issues regarding APVIRT in an 8-way cluster
- If using an 8-Member SSI, keep track of crypto usage across your hardware setup(s)
  - You were doing this anyway
  - But now it's more complicated

SHARE
EDUCATE ‣ NETWORK ‣ INFLUENCE

z/VM Network Security and TLS

z/VM Network Security

Protection of data in-flight



Client Value Proposition:

Not all organizations use host-based network encryption today … reduced cost of encryption enables broad use of network encryption

z/VM Secure Communications

- **Threat**: disclosure of sensitive data in flight to the hypervisor layer
- **Solution**: encrypt traffic in flight.

Notes:

- Automatic use of CPACF for symmetric algorithms
- Automatic use of Crypto Express features (**if available**) for acceleration of asymmetric algorithms
- Built on System SSL and ICSFLIB for z/VM

z/VM V7.3 and TLS

- TLS 1.2 will be the only version enabled by default
  - We don’t change your configuration, but we do change our underlying settings
  - Check your DTCPARMS files accordingly

- For 8-member SSI, consider how you’ll handle TCP/IP for your new nodes
  - This means encryption
  - You can copy or share your .kdb files between systems, but:
  - will you need to update or acquire certificates for new hostnames or IP addresses?

Certificate Verification

- **Client Certificate Authentication -** Allows a server to verify a client by ensuring that the client certificate
  - has been signed by a certificate authority that the server trusts
  - has not expired
  - Default Telnet certificate check change to CLIENTCERTCHECK PREFERRED
- **Host Name Validation -** Allows a client to verify the identity of a server using either
  - Host Name
  - Domain Name
  - Host IP Address
- **New APIs** to allow fields to be extracted from a client or server certificate

Component	APAR	PTF	RSU
TCP/IP	PH18435	z/VM 7.1 UI69975	7.1 2101
CMS	VM66348	z/VM 7.1 UM35651	7.1 2101
LE	VM66349	z/VM 7.1 UM35650	7.1 2001

Client Certificate Authentication

- Allows a server to verify a client by ensuring that the client certificate
  - has been signed by a certificate authority that the server trusts
  - has not expired
- Expands previous support for dynamically secured Telnet connections to the z/VM FTP and SMTP servers
- New or enhanced **CLIENTCERTCHECK** statement/option
  - **FTP server**
    - Statement in FTP configuration file (SRVRFTP CONFIG)
    - *SMSG server_id SECURE* command
    - CERTFULLCHECK and CERTNOCHECK removed from *FTP* command
  - **SMTP server**
    - *TLS* statement in SMTP CONFIG file
    - *SMSG server_id TLS* command
  - **Telnet server**
    - *INTERNALCLIENTPARMS* statement
  - **TCPIP CONFIG**
    - *PORT* statement
      - for verification of statically secured connections

Host Name Validation

- **Allows a client to verify the identity of a server using either**
  - Host Name
  - Domain Name
  - Host IP Address
- **SIOCSECCLIENT** call has been enhanced to accept a new version of the SecureDetailType structure which includes an extension for specifying the above validation string(s)

- New options on ***TELNET*** command
  HVCONTINUE
  – **SECURE HVNONE**
  HVREQUIRED

- New **HOSTVERIFICATION** statement in TCPIP DATA
  – Defines default client host verification setting when no **HV…** option is specified on *TELNET SECURE* command

Online Certificate Status Protocol

SHARE
EDUCATE • NETWORK • INFLUENCE

- **Online Certificate Status Protocol –** allows general peer certificate cross-checking against an external server
  - Via OCSP or via Certificate Revocation List (CRL) Distribution Points (CDP)
  - In support of RFCs 6960 and 5280
  - New configuration options in DTCPARMS of your TCP/IP stack

Enhances security by validating client certificate during handshake process; centralizes client certificate management to single external server

- **Will require a restart of the TLS servers to enable**

Component	APAR	PTF	RSU
TCP/IP	PH28216	z/VM 7.2 UI72963	TBD

Query GSKKYMAN Certificates

SHARE
EDUCATE ‣ NETWORK ‣ INFLUENCE

Introduces a CERTMGR command to the GSKADMIN and TCPMAINT virtual machines

- Address usability pain points around managing certificates in the gskkyman application
- CERTMGR QUERY allows administrators to list certificate labels and display attributes
- Useful for determining certificate chains, certificate expiry, and certificate TLSLABELs

Part of a larger Streamlined SSL Configuration project to improve the z/VM-TLS experience

Component	APAR	PTF	RSU
TCP/IP	PH40080	z/VM 7.2 UI78359	TBD
CMS	VM66561	z/VM V7.2 UI35911	TBD
VMSES	VM66581	z/VM V7.2 UM35914	TBD

CMS Pipelines – SSL Support

SHARE
EDUCATE ‣ NETWORK ‣ INFLUENCE

- **Enhance existing CMS applications** to use secure TCP/IP connections
  - Using z/VM System SSL to inherit the settings defined
  - Continue to use existing applications and comply with company security policy
- Integrate CMS applications and CMS-based data with **cloud-based services**
  - Interface with enterprise applications when replaced by web services
  - Exploit new web services for use in CMS applications
- **Implicit SSL** – application transparent secure “tunnel”
  - Suitable for HTTPS client (including RESTful services)
  - Trivial change to make a pipeline-based client application use SSL
- **Explicit SSL** – application protocol determined SSL (aka STARTTLS) *
  - Suitable for FTP and LDAP with secure connections
- **New built-in stage** to exchange data through FTP with secure connection *
  - Read file from FTP server into the pipeline for further processing
  - Write the data from the pipeline into a file on an FTP server

* Extra deliverables because of sponsor user feedback

CMS Pipelines – SSL Support

SHARE
EDUCATE ‣ NETWORK ‣ INFLUENCE

- Upward compatible enhancements to
  - `tcpclient` stage
  - `tcpdata` stage

- Possible Use Cases
  - store CMS data in cloud databases
  - post messages in a Slack channel
  - manage CMS files with GitHub
  - get data from Internet to use in CMS

Component	APAR	PTF	RSU
CMS	VM66365	z/VM 7.1 UM35658	7.1 2101RSU

Direct-to-Host Service Download

- Allows a mechanism for transfer of service directly from ShopZ to your z/VM system
  - Initiates a web interface inside CMS guest
  - Web browser allows you to download directly from ShopZ, or to your workstation if preferred
  - Data downloaded from ShopZ is verified and unpacked during transfer to the z/VM host system

- CMS program runs using the MAINT7n0 userid
- Requires use of the TLS server to connect to IBM ShopZ
- For more information, visit https://www.vm.ibm.com/service/getshopz.html

Component	APAR	PTF	RSU
CMS	VM66540	z/VM 7.2 UM35899	TBD

Coming Soon

You can get involved!! https://www.vm.ibm.com/newfunction/

KEYVAULT Utility

- A new CMS password/key management utility -- KEYVAULT -- is planned to allow applications to securely store and retrieve user ID keys (logon passwords) that are needed for data transfers (such as using FTP/FTPS) or automated login procedures.Transmit RACF audit records as they're written to an external service
- https://www.vm.ibm.com/newfunction/#keyvault

Query z/VM System Security Settings

- This item will provide a centralized 'collector' program which gathers security-relevant configuration information from various z/VM components (CP, TCP/IP, DirMaint, RACF) and provides them to a system programmer or security administrator via a single pane of glass. This item will also provide an API (via SMAPI) by which z/VM management programs, or compliance programs, can collect this data if authorized.
- https://www.vm.ibm.com/newfunction/#qsec

Bringing it all together —securely

SHARE
EDUCATE ‣ NETWORK ‣ INFLUENCE

z/VM Security: Development Principles

1

Meet and maintain **compliance** to industry security standards.

2

Remove obstacles to adopting a secure virtual infrastructure by making security "**easy to use**."

3

Expand capabilities of the IBM Z stack to **secure modern workloads**.