IBM WW Z Security Conference

October 6-9, 2020

z/VM Security: Introducing V7.2

(and Multi-factor Authentication for z/VM)

Brian W. Hugenbruch, CISSP

IBM Z Security for Virtualization and Cloud

bwhugen@us.ibm.com @Bwhugen

IBM

2020.10.09.3c

Introducing z/VM 7.2

GA September 18, 2020

- Preview announce April 14, 2020
- GA Announce August 4, 2020

New Architecture Level Set of z13 and LinuxONE or newer processor families

Includes new function service shipped for z/VM 7.1 including:

- 80 Logical Processor support, Dynamic Crypto, VSwitch Priority Queuing, etc.

Additionally, includes:

- Centralize Service Management
- Multiple Subchannel Set Multi-Target Peer-To-Peer Remote Copy support for the GDPS environment
- Adjunct virtual machine support
- Foundational support for future new function APARs

Summary of z/VM Releases

Release	ProdId	GA	EOM	EOS	Notes
z/VM 7.2	5741-A09	Sept 18, 2020	TBD	TBD	
z/VM 7.1	5741-A09	Sept 21, 2018	TBD	TBD	Start of 2 Year Cadence[1]
z/VM 6.4	5741-A07	Nov 11, 2016	Mar 9, 2020	Mar 31, 2021	
z/VM 6.3	5741-A07	July 26, 2013	Nov 11, 2016	Dec 31, 2017	

Release[3]	z15 & LinuxONE III	z14 & LinuxONE II	z13 & LinuxONE Emperor	z13s & LinuxONE Rockhopper	zEC12	zBC12	z196	z114	z10 EC	z10 BC
z/VM 7.2	Yes	Yes	Yes	Yes						
z/VM 7.1	Yes	Yes	Yes	Yes	Yes	Yes				
z/VM 6.4	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes		
z/VM 6.3[2]		Some[4]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

1. z/VM GA every 2 years with in service for ~4.5 years.
2. z/VM 6.3 no longer supported but referenced what machines were supported when it was.
3. Service may be required for support of various servers.
4. There was support for the enterprise class z14 and Emperor, but not for ZR1 and LR1 (Rockhopper).

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 Security Certifications

V7.2 Statements of Direction -- *April 14, 2020*

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

z/VM Level	Common Criteria	
z/VM V7.2 SoD	***BSI OSPP (with Virt and Labeled Security extensions) at EAL 4+***	***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 6.3 (Out of Service)	OSPP with Labeled Security and Virtualization at EAL 4+ -- ***COMPLETED!*** • was valid through March 2020	

z/VM Level	FIPS 140-2
z/VM V7.2 SoD	***FIPS 140-2 L1 for z/VM System SSL and ICSFLIB***
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*
z/VM 6.3 (Out of service)	FIPS 140-2 L1 **-- *COMPLETED!***

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

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

z/VM 7.2 includes all the new function from z/VM 7.1

Systems Management

- ESM control/audit of SMAPI calls
- CMS SSL Pipelines

TCPIP

- Elliptic Curve for the TLS Server
- Protocol identification on active connections
- TLS client certificate verification
- TLS server hostname validation settings

CP

- Support and virtualization of IBM z15 and LinuxONE III CPACF and Crypto Express features
- Dynamic crypto support

RACF

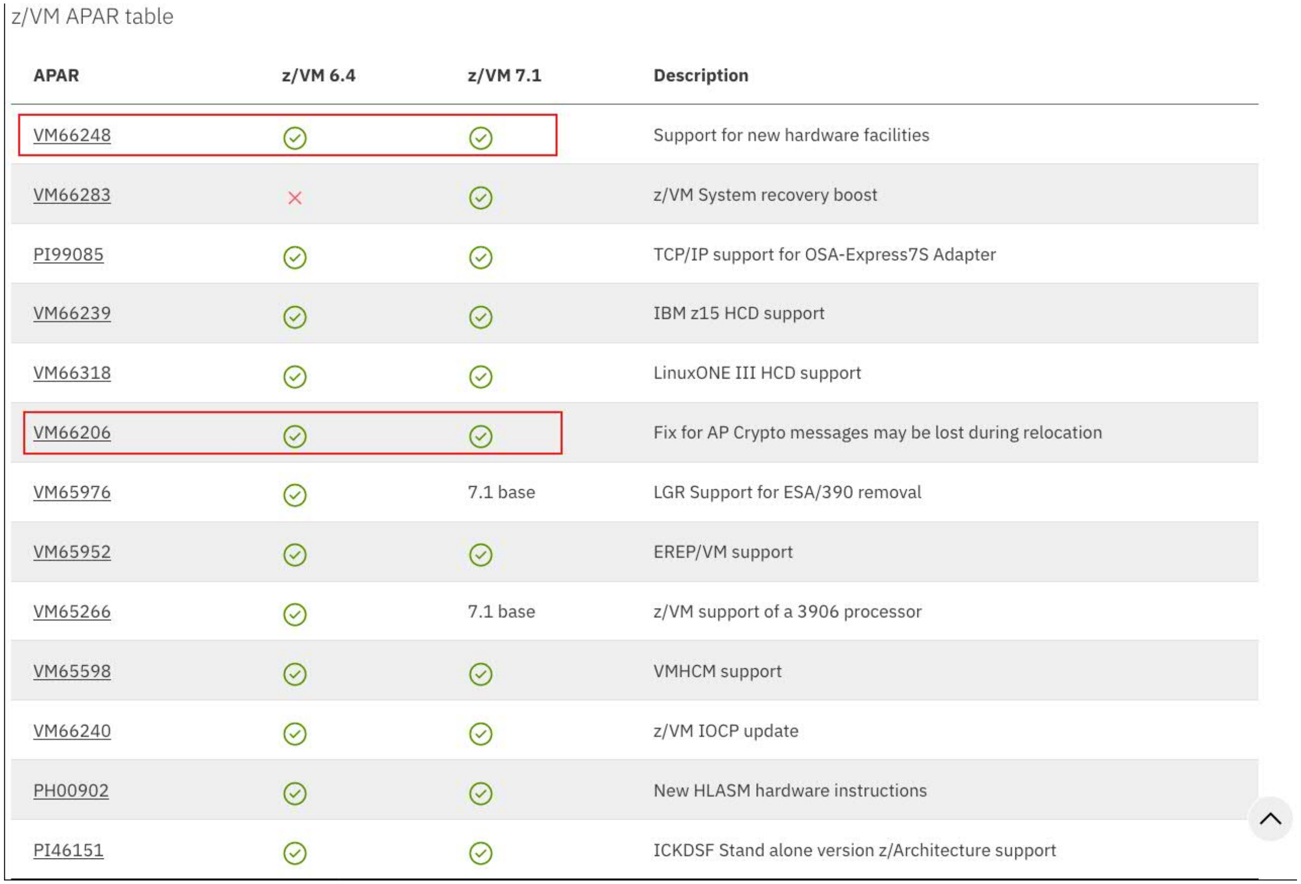
- RACF FixPack 2019 (includes query for the database template level)
- Multifactor Authentication (requires an ESM; also requires IBM Z Multi-factor Authentication V2.1)

z/VM Support of z15 Cryptographic Hardware

PTF for APAR VM66248 -- refer to [**http://www.vm.ibm.com/service/vmreqz15.html**](http://www.vm.ibm.com/service/vmreqz15.html)

New CPACF facilities and Crypto Express7S orderable features

Service implications when operating in an SSI with multiple z/VM release levels and/or hardware levels

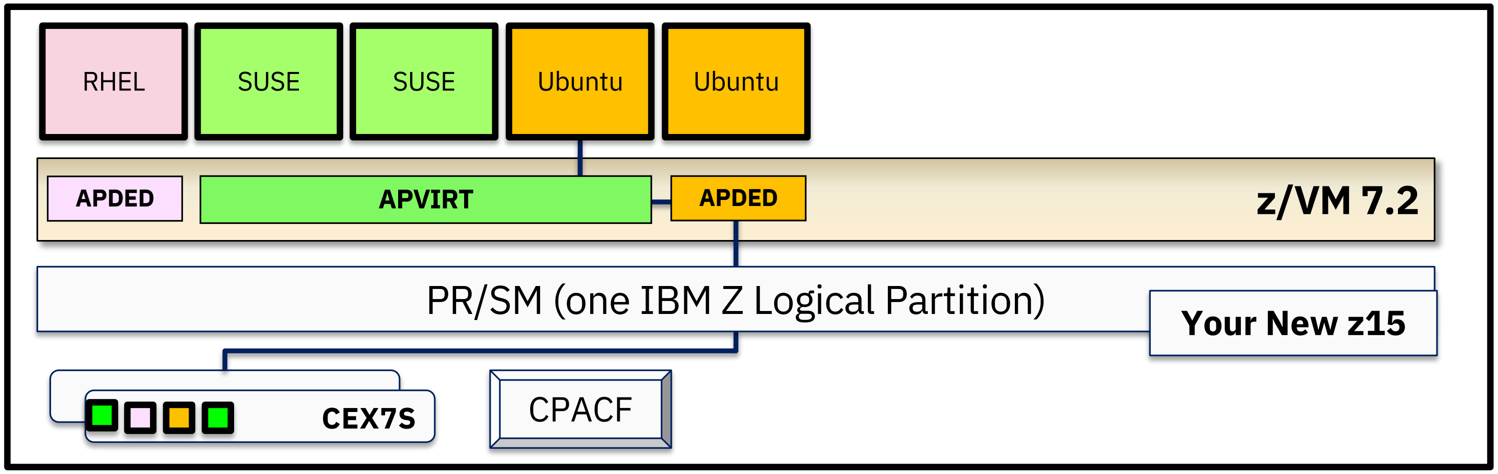


z/VM APAR table

APAR	z/VM 6.4	z/VM 7.1	Description
VM66248	✓	✓	Support for new hardware facilities
VM66283	✗	✓	z/VM System recovery boost
PI99085	✓	✓	TCP/IP support for OSA-Express7S Adapter
VM66239	✓	✓	IBM z15 HCD support
VM66318	✓	✓	LinuxONE III HCD support
VM66206	✓	✓	Fix for AP Crypto messages may be lost during relocation
VM65976	✓	7.1 base	LGR Support for ESA/390 removal
VM65952	✓	✓	EREP/VM support
VM65266	✓	7.1 base	z/VM support of a 3906 processor
VM65598	✓	✓	VMHCM support
VM66240	✓	✓	z/VM IOCP update
PH00902	✓	✓	New HLASM hardware instructions
PI46151	✓	✓	ICKDSF Stand alone version z/Architecture support

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

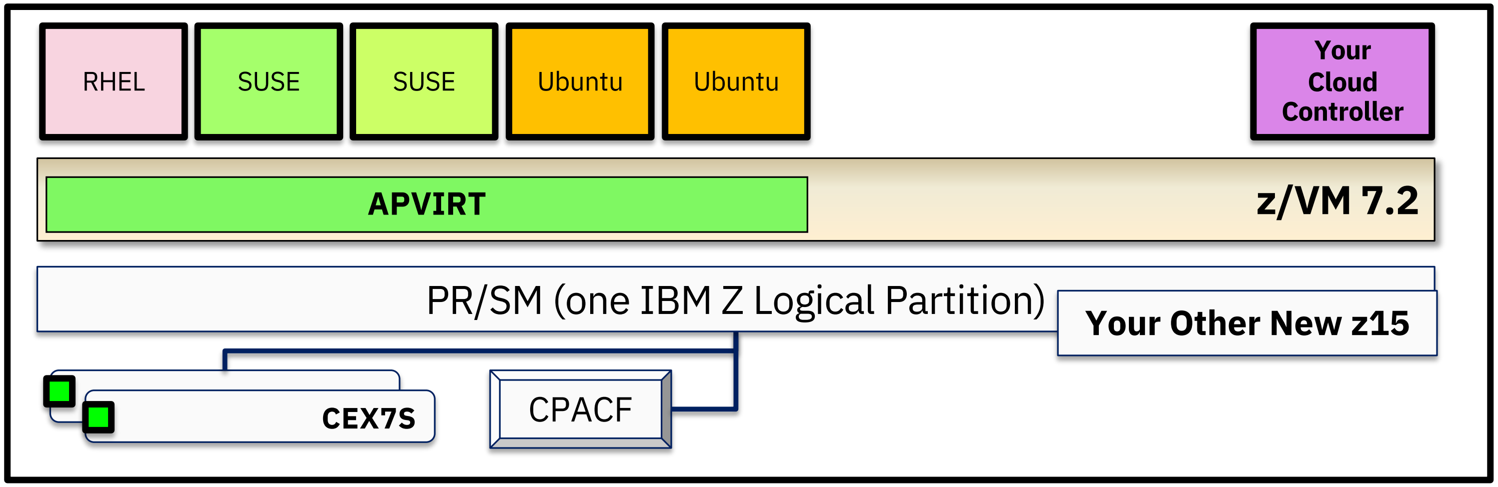
All card functions are available to the guest

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



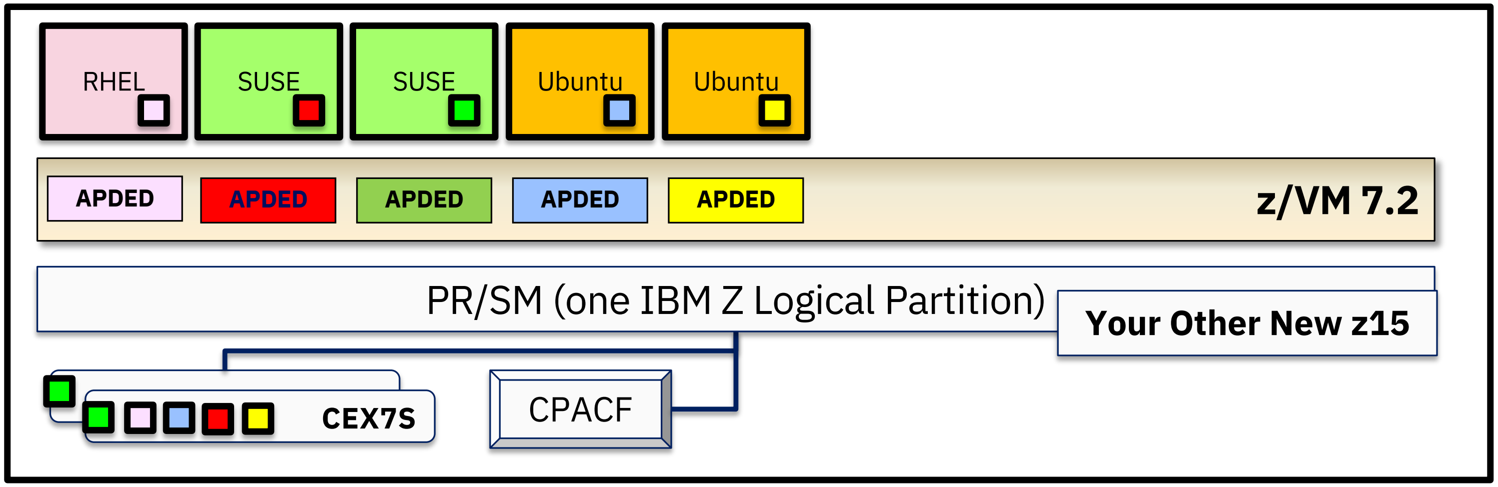
Crypto operations: SSH (RSA, SHA-2, AES), and *whatever data handled inside the guests*

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: Linux on IBM Z Blockchain (*not* HSBN)



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

Dynamic Crypto Support for z/VM

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

z/VM 7.1
PTF for APAR VM66266

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:

- 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

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

z/VM Dynamic Crypto – Summary

z/VM 7.1
PTF for APAR VM66266

Now available via PTF for APAR VM66266 for z/VM 7.1 only

- ***Prereq VM66206 for z/VM 6.4 and z/VM 7.1 (installed on all SSI members before dynamic crypto is applied.)***

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).

Sponsor users were engaged heavily in the process

- Design playbacks and to-be scenarios
- Usability iterations
- Demos and hands-on-code early testing

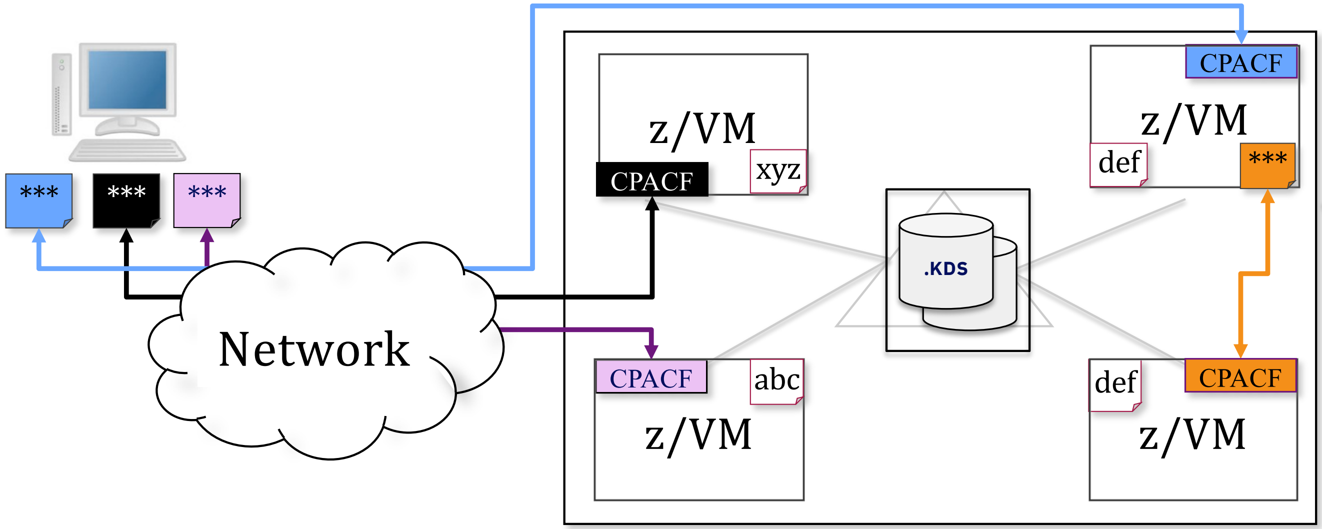
Data Protection // z/VM Network Security

Protection of data in-flight

Legend:

*** - encrypted data

abc - unencrypted data



z/VM Single System Image cluster

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

Client Value Proposition:

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

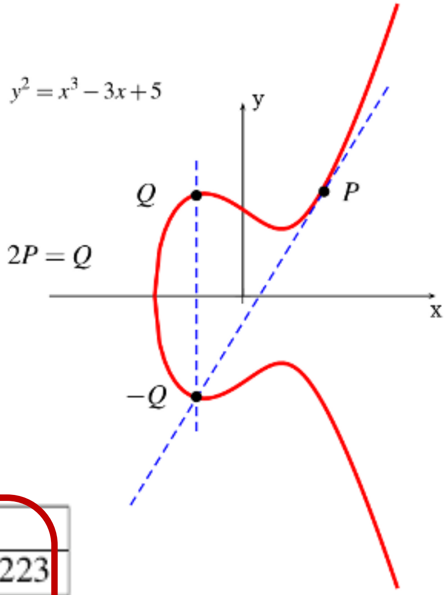
Elliptic Curve and the TLS Server

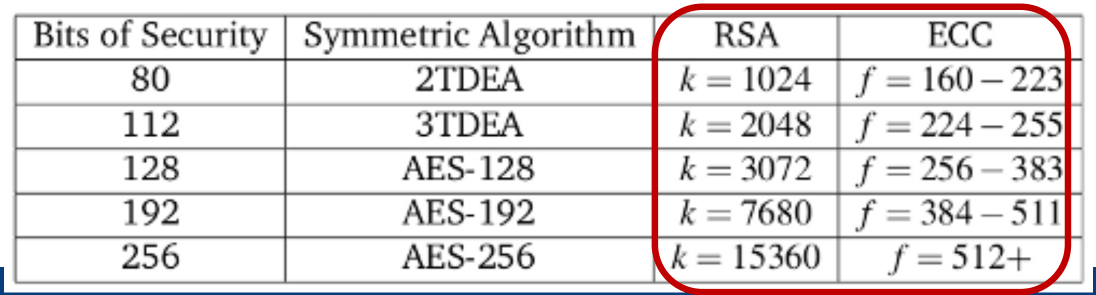
PTF for APAR PI99184

- Elliptic Curve variants of many major ciphers now available for the TLS Server
  - Enabled by default
  - Currently lacks hardware acceleration
  - Still faster/stronger than asymmetric algorithms based on on prime factorization

- Elliptic Curve operations available for certain asymmetric operations as well as key exchange algorithms

- Important update for future growth (TLS 1.3 will be made exclusively of Elliptic Curve ciphers)





Bits of Security	Symmetric Algorithm	RSA	ECC
80	2TDEA	$k = 1024$	$f = 160 - 223$
112	3TDEA	$k = 2048$	$f = 224 - 255$
128	AES-128	$k = 3072$	$f = 256 - 383$
192	AES-192	$k = 7680$	$f = 384 - 511$
256	AES-256	$k = 15360$	$f = 512+$

TLS Server – Sponsor User Feedback: Protocol Tracking

PTF for APAR PI99184

TLS protocol level now appears on output related to secure connections (**SSLADMIN QUERY SESSIONS** and **NETSTAT IDENTIFY SSL**)

- Easy way to determine **which active connections** may be using an older protocol level

```
ssladmin query sessions (ssl all
DTCSSL2404I Sending command to server(s): TCPIP01
DTCSSL2430I Session information:
Server   Local Socket      Remote Socket      Type  Label    Cipher Details
-------- ----------------- ------------------ ----  -------  ---------------------------------
SSL00001 9.60.60.3..23     9.60.60.4..1031    I     TESTCERT TLS1.2_ECDHE_ECDSA_AES_128_SHA256
SSL00002 9.60.60.3..23     9.60.60.7..1036    I     TESTCERT TLS1.2_ECDHE_ECDSA_AES_128_SHA256
SSL00003 9.60.60.3..23     9.60.60.12..1045   I     TESTCERT TLS1.2_ECDHE_ECDSA_AES_128_SHA256
SSL00005 <*No Sessions*>
SSL00004 <*No Sessions*>
```

z/VM TLS/SSL Certificate Verification

June 2020

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	TBD
CMS	VM66348	z/VM 7.1 UM35651	TBD
LE	VM66349	z/VM 7.1 UM35650	TBD

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

z/VM 7.1 ESM Controls for Systems Management

PTF for APAR VM66167

z/VM Systems Management APIs provide a fast-path to privileged function

- Used by various products for virtual infrastructure management
- Used by cloud products and plug-ins for Infrastructure-as-a-Service configurations

SMAPI will be upgraded to call an ESM to check authorizations for APIs

- Per system, per API, per calling userid
- FACILITY class profiles (e.g. **`SMAPI.<target>.<api>.<requestor>.<system_name>`**
- ESM auditing records (SMF) included in main security logs

Important for cloud-centric environments, like those managed by:

- IBM Wave for z/VM
- IBM Cloud Infrastructure Center
- OpenShift Control Program

CMS Pipelines – SSL Support

June 2020

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

May 2020

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	TBD

RACF for z/VM 7.1 FixPack 1 – Usability Enhancements

PTF for APAR VM66278

#	Description of the functional enhancement
1	Query RACF Database Template Level So sysprog or security admin can determine if a forthcoming APAR will require a database update or RACFCONV.
2	Halt RACFVM initialization when server detects a down-level database More immediate presentation of problem details, to enable sysprog to fix with minimum fuss
3	Remove contradictory information from RACFPERM Correction to bring help text in line with functional behavior.
4	Improve error messages when A-disk can't be written by RAC EXEC Check A-disk accessibility before executing RACF commands, so an environment error isn't mistaken for a security problem.
5	Improve consistency of SETROPTS error messages Addition of warning messages around invalid parameter use.
6	Enable RACFVM to accept SMSG from the current system operator Eliminate assumptions that OPERATOR is always the current OPERATOR
7	Message fixes for ROAUDIT Correction to bring certain RACF messages in-line with functional behavior.

Multifactor Authentication for z/VM

May 2020

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 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

Multifactor Authentication for z/VM

Linux-based server which runs the MFA application (Linux on Z)

- SLES and RHEL supported; some crypto library requirements
- Web-based UI for administering users, factors, and policies

Out-of-band authentication factors supported

- Present all credentials to a web browser interface
- Receive a ”derived credential” (CTC) which is valid for **nn** minutes/hours for **mm** use(s)
- Type in credential on CP LOGON where you would have used a password/phrase
- In-band authentication factors (e.g. RACF passwords) not supported

Can run as a guest of z/VM, on KVM, or in its own LPAR

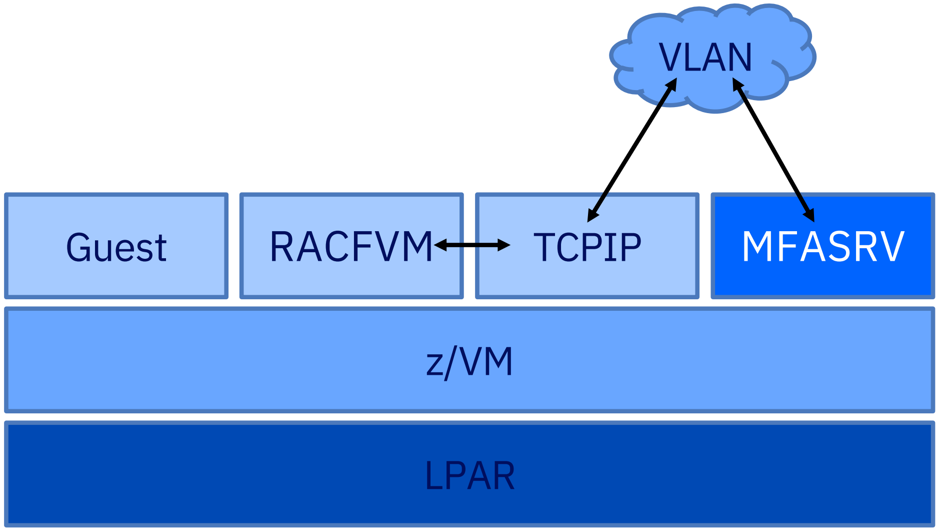
- Communicates over secure TCP/IP to your ESM

Policies are meant for human users

- Automated virtual machines don’t necessarily need passwords

Where do I set up IBM Z MFA V2.1 on under z/VM?

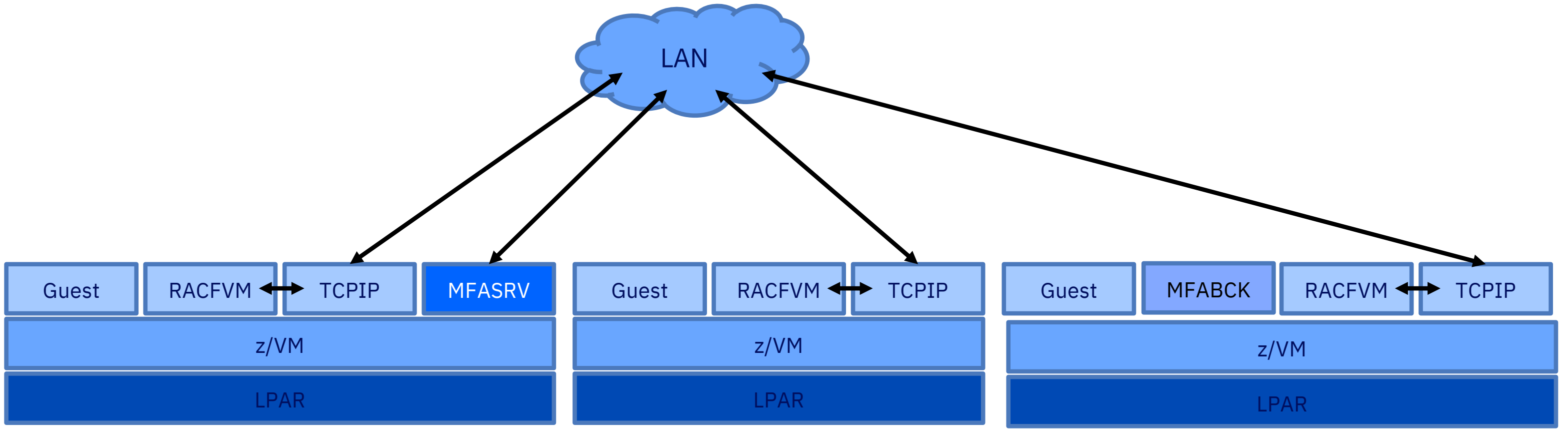
The constraint is ”one ESM database to one MFA server.”
So you could do a single system…



Where do I set up IBM Z MFA V2.1 on under z/VM?

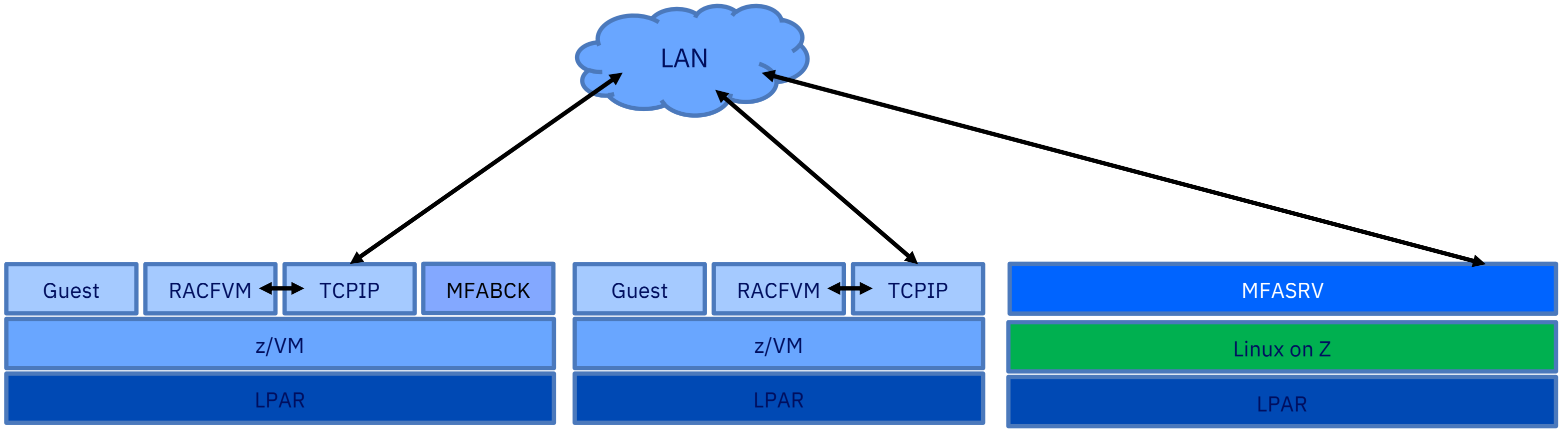
…or many systems*. Since it runs as a Linux on Z guest, you could put the primary and back-up on different LPARs or CECs.

**Be careful in an SSI.*

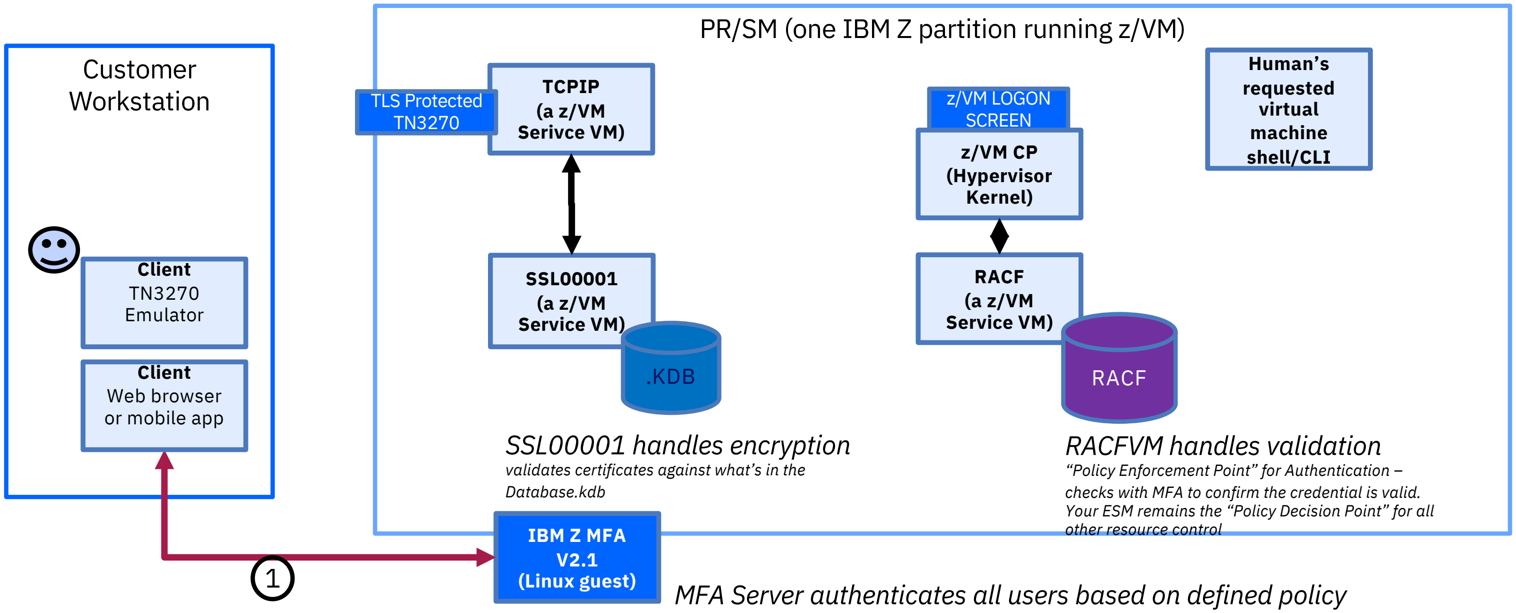


Where do I set up IBM Z MFA V2.1 on under z/VM?

…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.



Authentication Flow: z/VM with Multi-factor Authentication (1/2)



Customer Workstation

Client
TN3270 Emulator

Client
Web browser or mobile app

1

PR/SM (one IBM Z partition running z/VM)

TLS Protected TN3270

TCPIP (a z/VM Serivce VM)

SSL00001 (a z/VM Service VM)

.KDB

SSL00001 handles encryption
validates certificates against what's in the Database.kdb

z/VM LOGON SCREEN

z/VM CP (Hypervisor Kernel)

RACF (a z/VM Service VM)

RACF

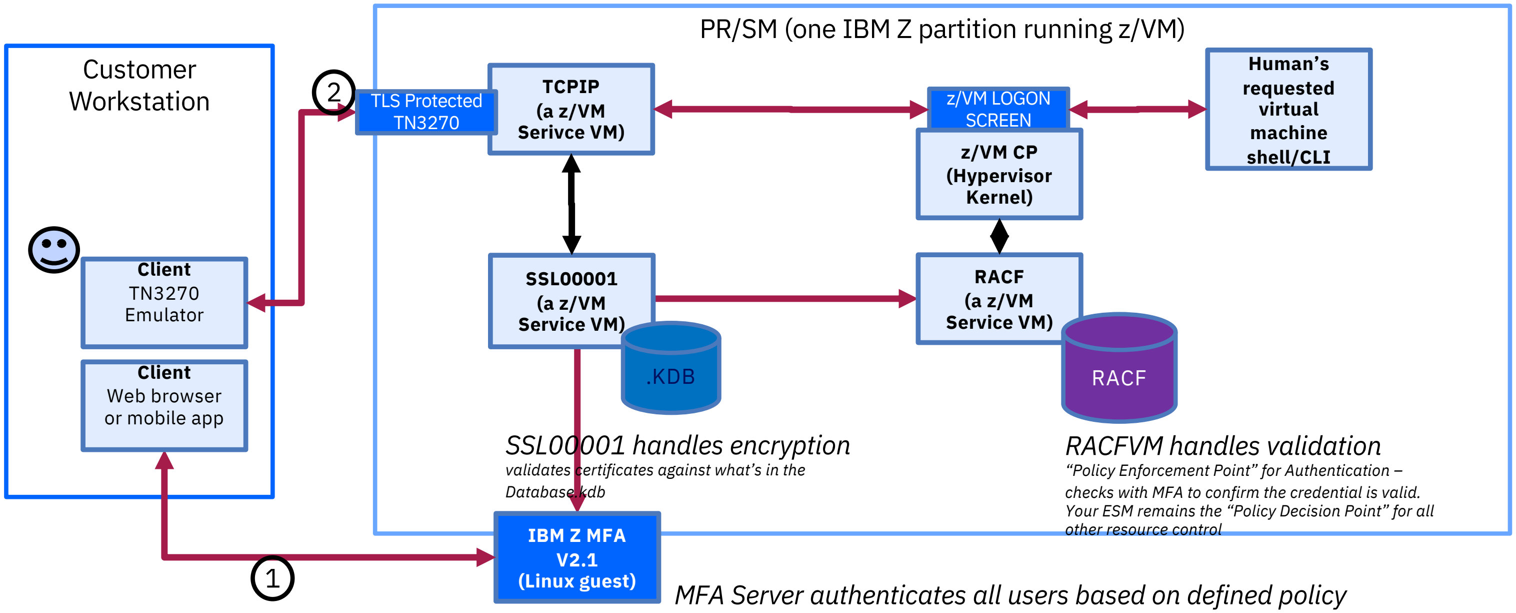
Human's requested virtual machine shell/CLI

RACFVM handles validation
"Policy Enforcement Point" for Authentication – checks with MFA to confirm the credential is valid. Your ESM remains the "Policy Decision Point" for all other resource control

IBM Z MFA V2.1 (Linux guest)

MFA Server authenticates all users based on defined policy
Returns a derived credential

Authentication Flow: z/VM with Multi-factor Authentication (2/2)



SSL00001 handles encryption

validates certificates against what's in the Database.kdb

RACFVM handles validation

"Policy Enforcement Point" for Authentication – checks with MFA to confirm the credential is valid. Your ESM remains the "Policy Decision Point" for all other resource control

MFA Server authenticates all users based on defined policy

Returns a derived credential

IBM Z Multi-factor Authentication – Available 22 May 2020

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

IBM Z Multi-factor Authentication V2.1 – a new priced product

- 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

Component	APAR	PTF	RSU
CP	VM66324	UM35569	TBD
RACF	VM66338	UV99363	TBD
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		

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

April 14, 2020 Announcement

> **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.

Bringing it all together—securely

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.**

z/VM Security – What's Next?

Continuous Delivery: Projects as announced, with more to follow
– *You can get involved!* https://www.vm.ibm.com/newfunction/
– We'll continue to find ways to deliver meaningful function to you

We're currently working on:
– SMF Realtime Audit and SIEM support (with zSecure)
– Online Certificate Status Protocol (OCSP)
– Streamlined SSL Configuration
– Mixed APVIRT for LGR
– Finishing Common Criteria and FIPS validations

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.

The VM Council has a workgroup exploring security and cryptography pain points
– Is something missing? Is something more difficult than it needs to be?
– How can we help get your security work sorted faster

For More Information…

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

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

- **IBM Z Multi-factor Authentication for z/VM Manual** (SC27-4938-40)**:**
  https://www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/zMFAv210sc274938/$file/azfv100_v2r1.pdf

- **“Preparing for Multi-Factor Authentication on z/VM” presentation (recorded live at the VM Workshop):**
  https://www.youtube.com/watch?v=AFkOtgEZxAc

Contact Information:

CISSP®

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