z/VM 6.4 Security News and Pervasive Encryption

News and How To's for Protecting Your Hypervisor

Brian W. Hugenbruch, CISSP
IBM Z Security for Virtualization & Cloud
z/VM Development: Endicott, NY, US
@Bwhugen

IBM’s Commitment to Security & Integrity

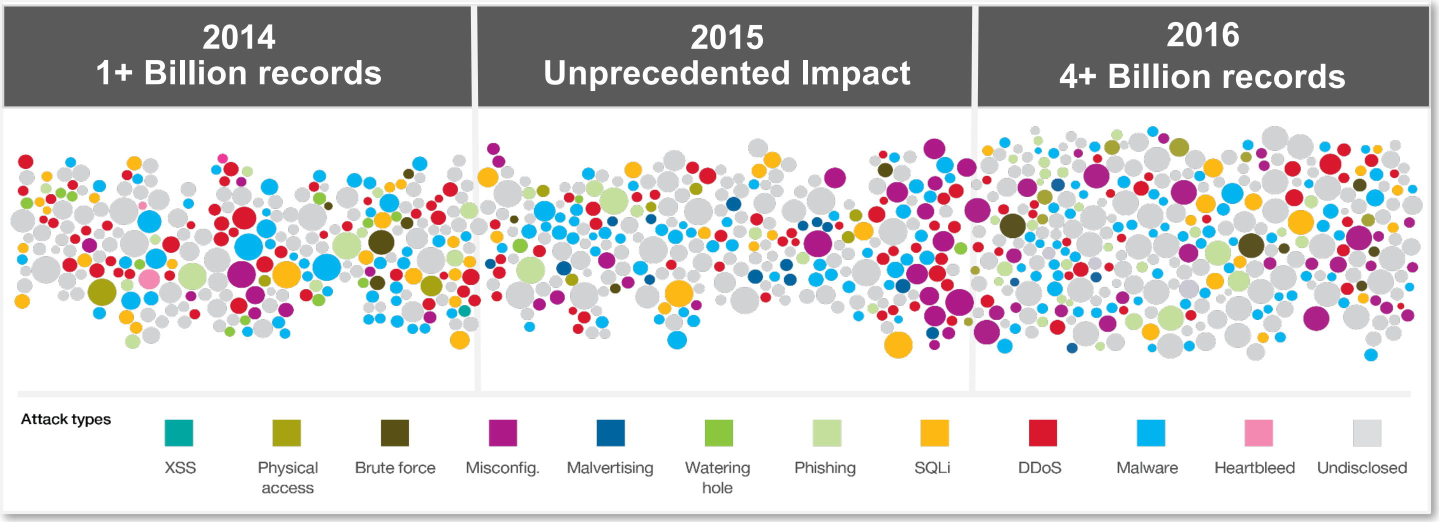
First issued in 1973 & Reaffirmed in 2007

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 *z Systems Center for Secure Engineering* to provide additional security focused testing and scrutiny.
- The z Systems Security Portal informs clients about the latest security and system integrity service to help keep their enterprise up to date

http://www-03.ibm.com/systems/z/os/zos/features/racf/zos_integrity_statement.html
http://www.vm.ibm.com/security/zvminteg.html

Today’s threats continue to rise in number and scale



average time to identify data breach

201 days

average cost of a U.S. data breach

$7M

Source: *IBM X-Force Threat Intelligence Index - 2017*

Example* risks to sensitive data in virtual environments

(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 Development Strategy

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.

Agenda

- **Security Certifications** for z/VM

- **Pervasive Encryption** for z/VM
  - Hardware Crypto Virtualization
  - The TLS/SSL Server
  - Encrypted Paging for z/VM (coming 4Q2017)

- **z/VM 6.4 Security (and 2017 PTFs)**
  - Control Program Updates
  - RACF Updates
  - DirMaint and Networking Updates

- **Questions**

z/VM Security Certifications

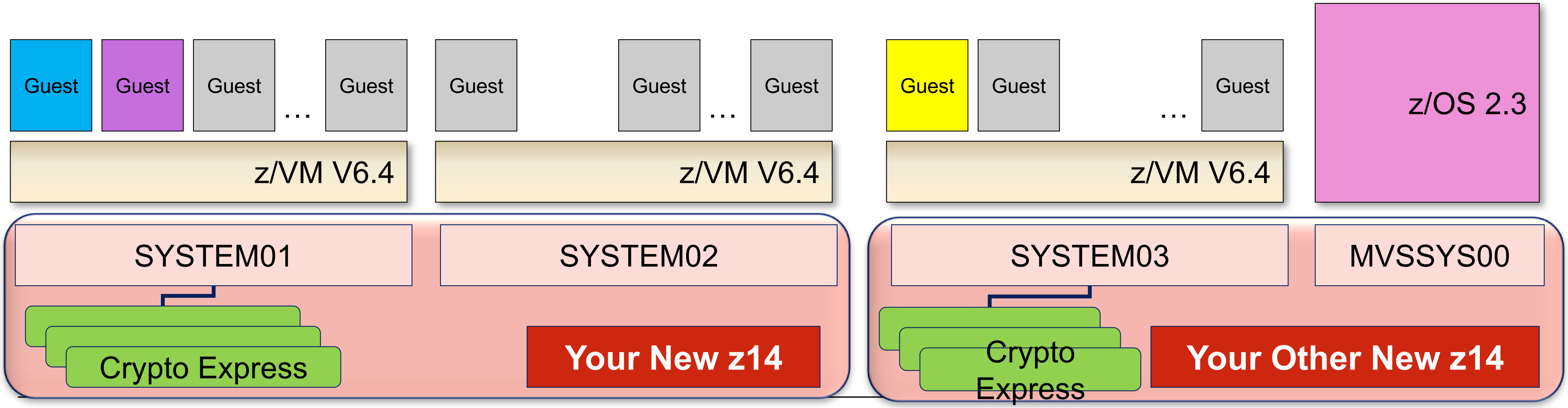
V6.4 Statements of Direction: 25 October 2016

z/VM Level	Common Criteria	FIPS 140-2
z/VM 6.4	***Formally Started*** *http://www.ocsi.isticom.it/index.php/elenchi-certificazioni/in-corso-di-valutazione*	***Formally Started*** *https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Modules-In-Process/IUT-List*
z/VM 6.3 **(EOS YE17)**	OSPP with Labeled Security and Virtualization at EAL 4+ • BSI-DSZ-CC-0903 • Valid through March 2020.	FIPS 140-2 L1
z/VM 6.1 **(Out of service)**	OSPP with Labeled Security and Virtualization at EAL 4+ • BSI-DSZ-CC-0752	FIPS 140-2 L1
z/VM 5.3 **(Out of service)**	CAPP/LSPP at EAL 4+	n/a

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

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

It's 22:00h. Do you know where your data is?



Guest Guest Guest … Guest

z/VM V6.4

Guest Guest … Guest

z/VM V6.4

Guest Guest … Guest

z/VM V6.4

z/OS 2.3

SYSTEM01

SYSTEM02

Crypto Express

Your New z14

SYSTEM03

MVSSYS00

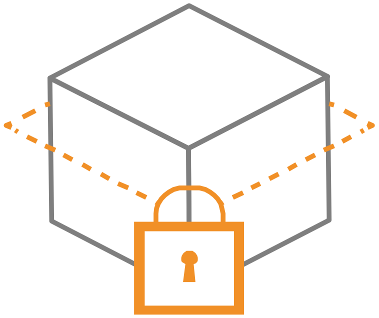
Crypto Express

Your Other New z14

The IBM Z Pervasive Encryption Strategy

- Extensive use of encryption is one of the most impactful ways to help reduce the risks and financial losses of a data breach and help meet complex compliance mandates.

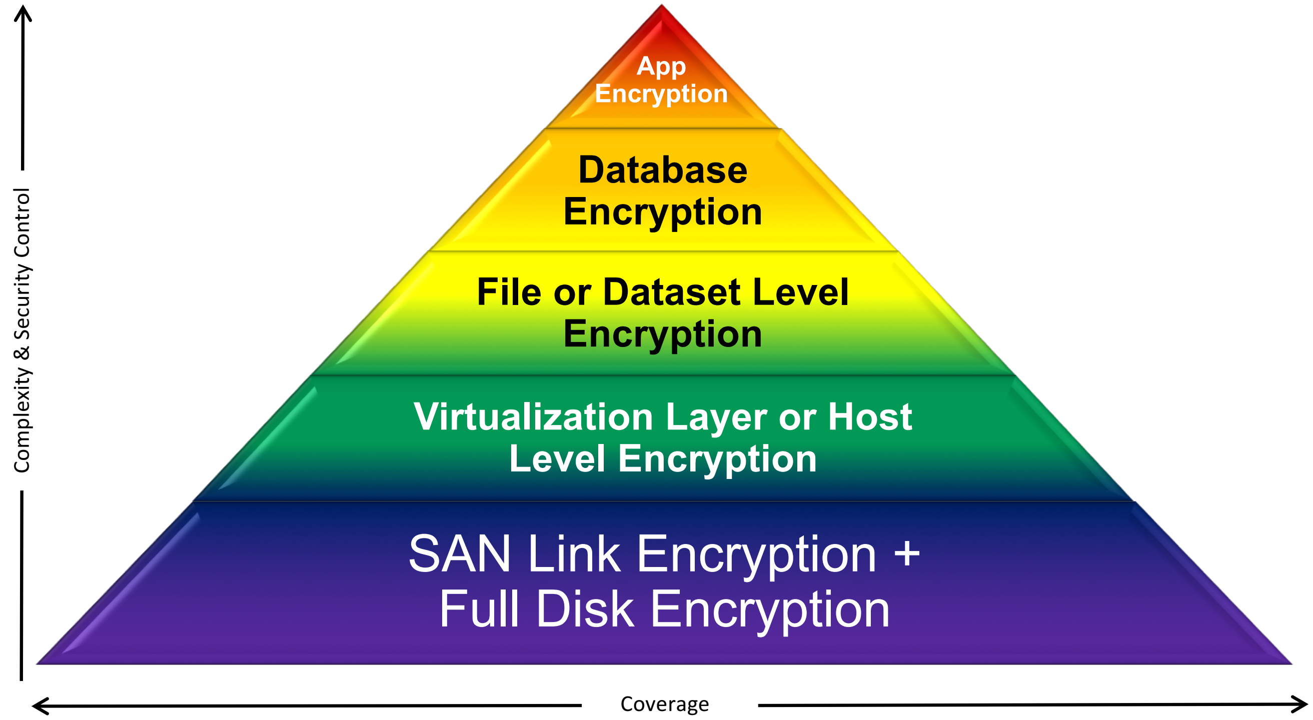
- However, implementing encryption can be a complex process …
  1. What data should be encrypted?
  2. Where should encryption occur?
  3. Who is responsible for encryption?



Transparent and consumable approach to enable extensive encryption of data in-flight and at-rest to substantially simplify & reduce the costs associated with protecting data & achieving compliance mandates

IBM Z Pervasive Encryption

From a Virtualization Point of View


App Encryption
Database Encryption
File or Dataset Level Encryption
Virtualization Layer or Host Level Encryption
SAN Link Encryption + Full Disk Encryption
Complexity & Security Control
Coverage

Pervasive Encryption and z/VM

Bringing Pervasive Encryption to z/VM involves the following:

Encryption Policy
In-Flight
Integrated Cryptographic Hardware
At-Rest

1. Ease of use needs to be mandatory
   - Client interviews and feedback a must

2. Enablement of **hardware facilities for guest usage**
   - If we're not first and foremost a virtualization platform, we're off-mission
   - Exploitation of crypto hardware for guests needs to happen Day 1

3. Encryption of security-pertinent hypervisor components
   - Question of **security policy** vs. **performance** vs. **risk**

IBM Z Pervasive Encryption for z/VM and Linux on z

z14 – Designed for Pervasive Encryption

- **CPACF** – Dramatic advance in bulk symmetric encryption performance
- **Crypto Express6S** – Doubling of asymmetric encryption performance for TLS handshakes

z/VM – Virtualizing Encryption for Linux

- **Virtualization** of IBM Z Crypto Hardware (**updated August 2017**)
- Crypto Express **acceleration** for encrypted data in flight (**available March 2017**)
- **Encrypted Paging** for z/VM (**coming 4Q2017**)

Linux on z – Full Power of Linux Ecosystem plus z14 Capabilities

- **LUKS dm-crypt** – Transparent file & volume encryption using industry unique CPACF protected-keys
- **Network Security** – Enterprise scale encryption and handshakes using zNext CPACF and SIMD
- **Secure Service Containers** – Automatic protection of data and code for virtual appliance

z/VM Support of z14 Cryptographic Hardware

PTF for APAR VM65942

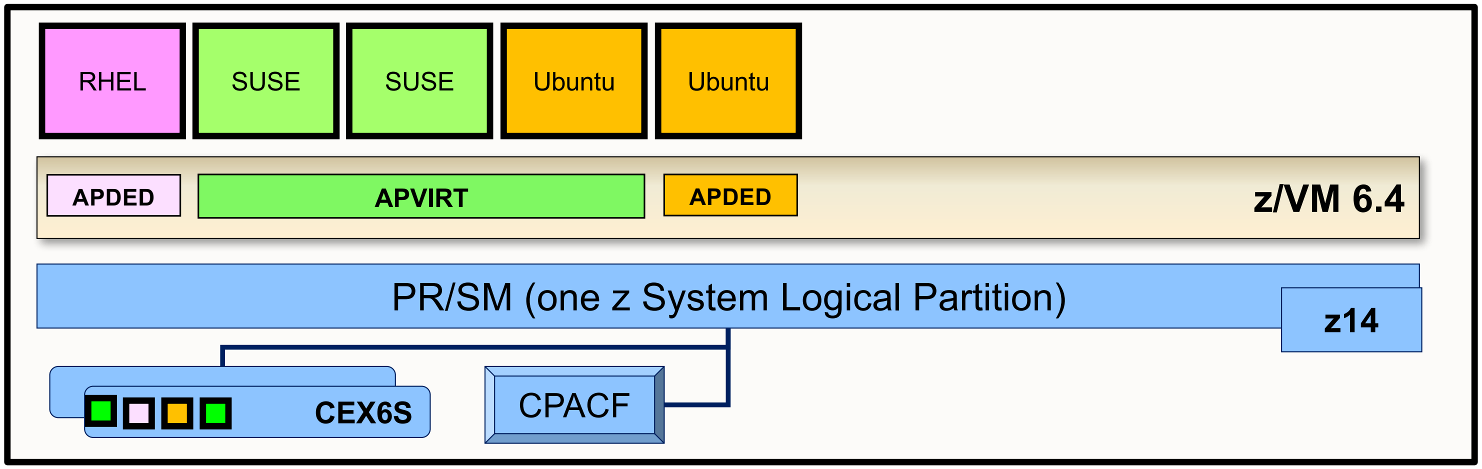
- New CPACF facilities and Crypto Express6S orderable features
  - CPACF now includes TRNG and AES GCM
  - Some fantastic performance benefits over previous hardware

- Elliptic Curve Cryptography for Shared Crypto Domains ("APVIRT")
  - All domains assigned to the CP-managed queues must be CCA coprocessors
  - No change to dedicated crypto domains – those function as before
  - Accelerates use of elliptic curve crypto for Linux or z/OS guests

–For more information, see the z14 Announce Letter at: https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=AN&subtype=CA&htmlfid=897/ENUS117-044&appname=USN

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

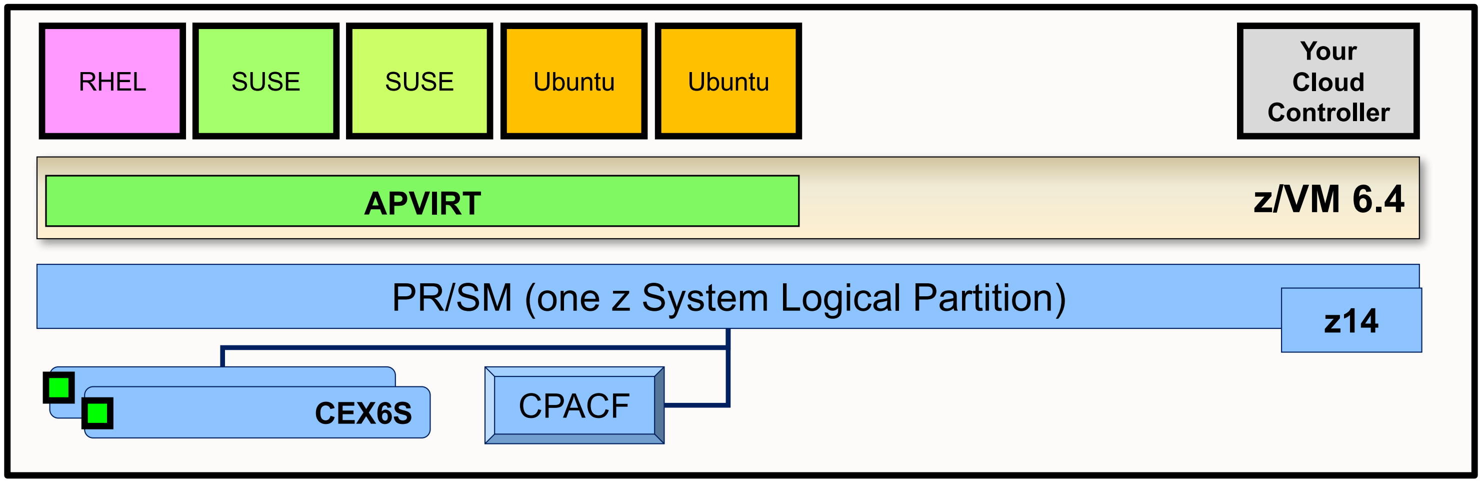
All card functions are available to the guest

APVIRT (“Shared”)

Virtual machine can access a collection of domains controlled by the hypervisor layer

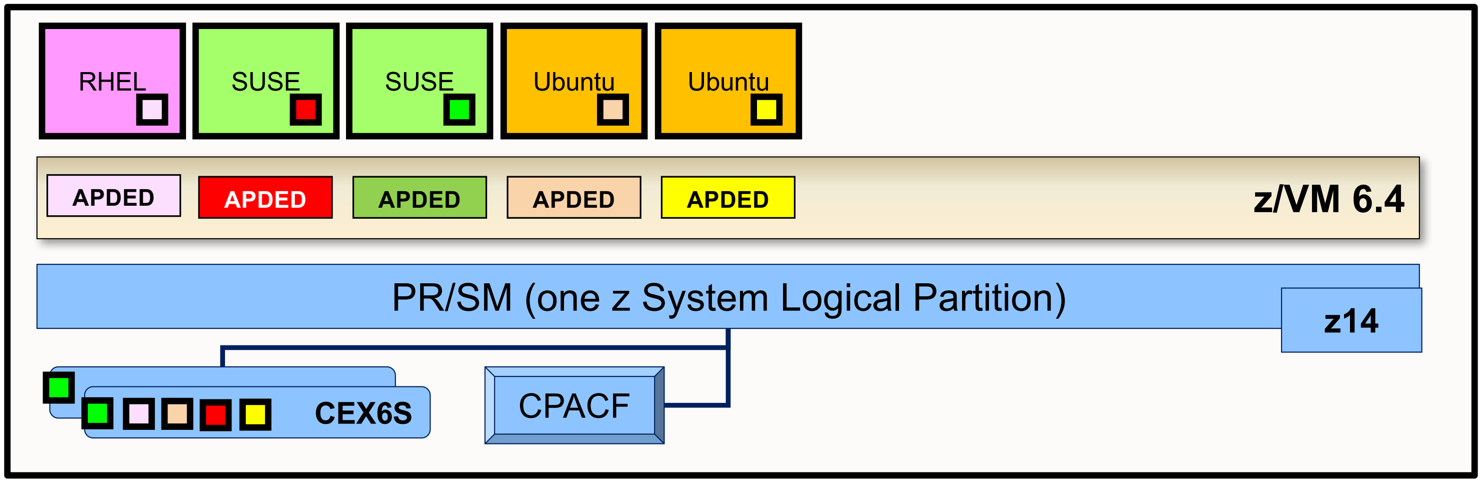
Meant for **clear-key operations only** – sharing crypto material might otherwise break security policy.

Sample of 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 Virtualization: Linux on z Blockchain (*not* HSBN)

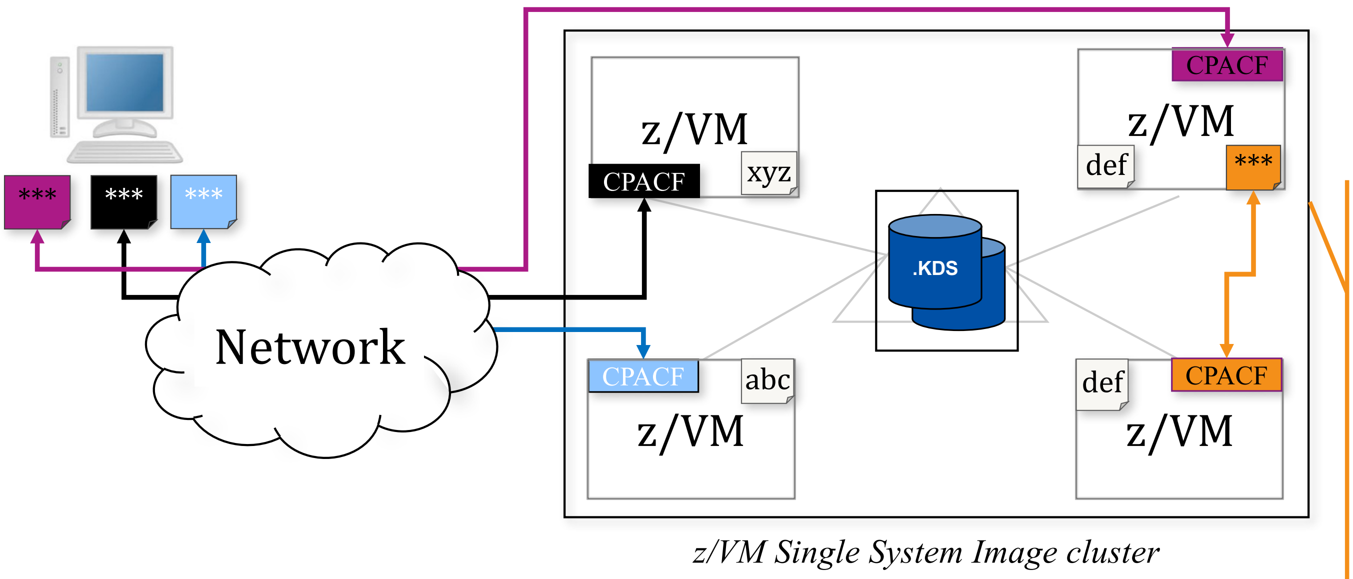


- **Crypto operations**: A lot. It's a Blockchain
- **Environmental Requirements**: Protection of key material. (It's a Blockchain.)
- **Recommended Hardware**:
  - –CPACF (required for secure and protected key ops on the crypto adapters)
  - –Crypto Express CCA Coprocessors
    - One domain per guest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

Data Protection // z/VM Network Security

Protection of data in-flight

z/VM 6.4
PTF for APAR VM65993



z/VM Single System Image cluster

Legend:

- *** - encrypted data
- abc - unencrypted data

z/VM Secure Communications

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

Notes:

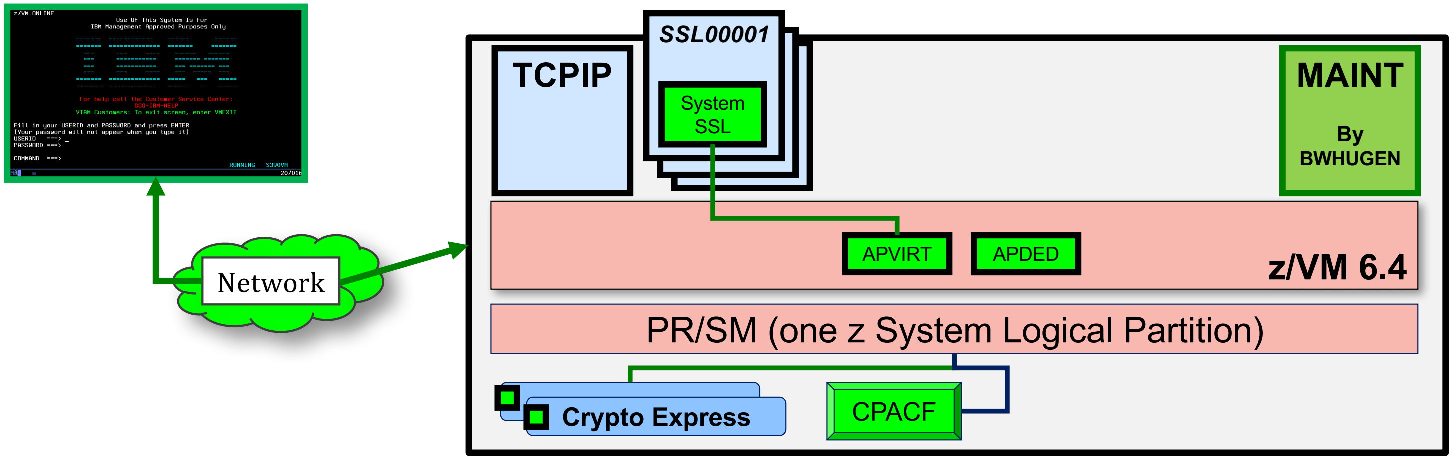
- Automatic use of CPACF for symmetric algorithms
- One-line change to enable automatic use of Crypto Express features for acceleration of asymmetric algorithms
- Built on System SSL and ICSFLIB for z/VM

Client Value Proposition:

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

Crypto APVIRT for the z/VM TLS/SSL Server

PTFs for APAR PI72106



```
z/VM ONLINE
                         Use Of This System Is For
                     IBM Management Approved Purposes Only

                   =======  ============    ======      ======
                   =======  ==============  =======    =======
                     ===      ===    ====     ======  ======
                     ===      ===========     ======= =======
                     ===      ===========     === ======= ===
                     ===      ===    ====     ===  =====  ===
                   =======  ==============  =====   ===   =====
                   =======  ============    =====    =    =====

                   For help call the Customer Service Center:
                                888-IBM-HELP
                   VTAM Customers: To exit screen, enter VMEXIT

Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ===> _
PASSWORD ===>

COMMAND  ===>
                                                      RUNNING   S390VM
MA    a                                                          20/016
```

- If Crypto Express domains are defined for sharing, then TLS/SSL Server will use them
  - **Clear-key RSA operations** are the primary beneficiary
    - Handshaking, rather than data transfer – **benefit will come from a lot of connections**
    - Will still use CPACF when pertinent
  - Meant as a performance enabler, not to replace key storage (still need .kdb or .p12 in BFS)
- ~30% savings in CPU time per transaction -- http://www.vm.ibm.com/perf/reports/zvm/html/640cip.html

Crypto APVIRT for the z/VM TLS/SSL Server

PTFs for APAR PI72106

```
PROFILE TCPSSL10
  CRYPTO APVIRTUAL
  IPL CMS PARM FILEPOOL VMSYS
  IUCV ALLOW
  LOGONBY GSKADMIN TCPMNT10
  NAMESAVE TCPIP10
  OPTION ACCT MAXCONN 1024 QUICKDSP
  POSIXINFO UID 7 GNAME security
  CONSOLE 0009 3215 T
  [...]
```

- Add `CRYPTO APVIRT` to your SSL server's PROFILE entry
  - **TCPSSLU** (the default PROFILE entry for the TLS/SSL Server)
  - APDED not allowed for a POOL of userids
- Insert directly into VM definition for:
  - **LDAPSRV** - uses its own System SSL build
  - **GSKADMIN** - for certificate creation / management
  - A **stand-alone TLS/SSL server** (non-POOL), if you have an old VM from z/VM 5.4 defined.

z/VM 6.4 TLS/SSL Server

- **TLS 1.2 is now the default encryption protocol for z/VM SSL**
  - Based on z/OS 2.2 System SSL and appropriate service

- **Also included are all the changes made in the service stream**
  - TLS and SSL PROTOCOL selection now available
  - AES Galois/Counter Mode (AES_GCM) – automatic with TLS 1.2
  - Larger DSA certificate support (2048)
  - 'Mode' Operand for auto-configuration to standards (`FIPS-140-2, NIST-800-131a`)
  - PKCS #12 Support (use a .p12 file instead of a key database)
    - `KEYFILE /etc/gskadm/bwhugen.p12`
  - ENABLE Operand to turn on any of the cipher suites now disabled by default
    - *NOTE: ciphers were disabled for security reasons. Turning these back on is for legacy support only. Exercise all caution when using weak crypto!*

Why does this matter to you?

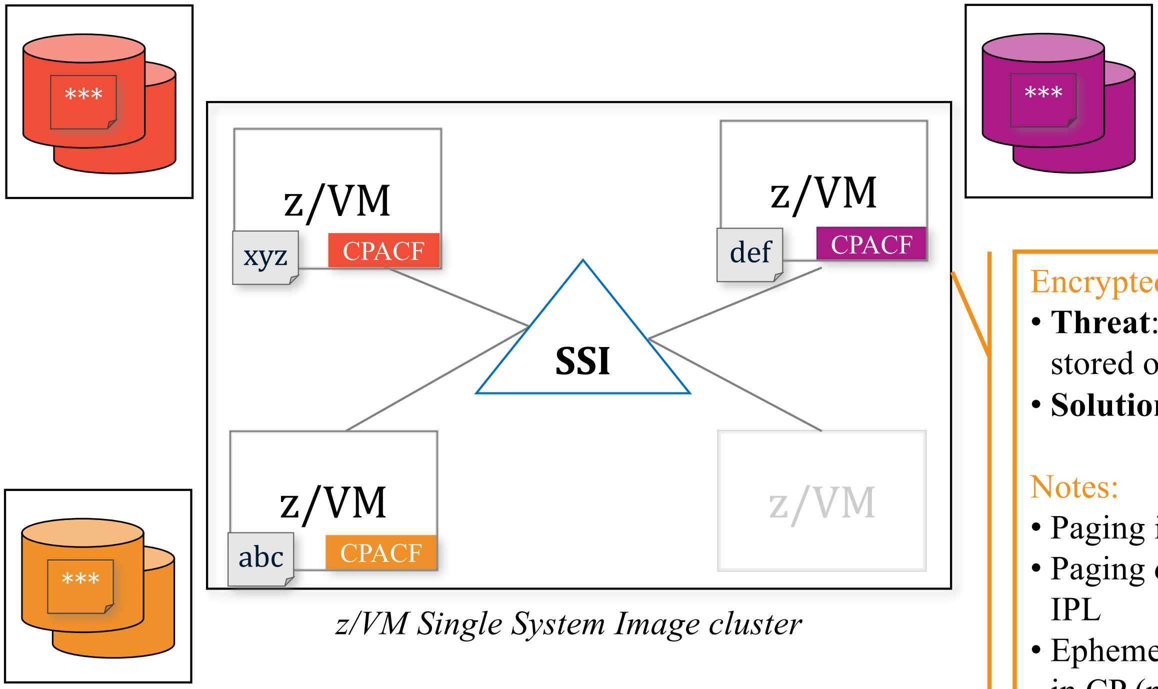
- **Standards compliance** (corporate, industry, government)
  - Corporate policy says "encrypt all traffic to hypervisor layer"
  - Usually not "unless it's only one person connecting"
  - We don't want a z/VM LPAR in the clear on the open internet

- **Encryption everywhere** for data in flight, inside the hypervisor as well
  - Secure Telnet, FTPS, SMTP
  - SMAPI worker machines
  - RSCS TCPNJE inside and between z/VM LPARs
    - RSCS + TCP/IP + SSL + DirMaint + SSI == Encrypted Spool File Transfer in a Cluster

Data Protection // z/VM Encrypted Paging

Protection of data at-rest

z/VM 6.4
PTF for APAR VM65993



z/VM Single System Image cluster

Legend:

*** - encrypted data

abc - unencrypted data

Encrypted Paging

- **Threat**: access to sensitive data when stored on CP owned disk
- **Solution**: encrypt guest data on page-out.

Notes:

- Paging is not SSI-relevant
- Paging data does not need to survive an IPL
- Ephemeral CPACF protected-key stored in CP (not on disk somewhere)
- AES encryption
- Very low overhead via CPACF

Client Value Proposition:

Protect guest paging data from administrators and/or users with access to volumes

Getting Started with Encrypted Paging

How Do I Get Value?

<u>**z/VM Encrypted Paging**</u>

1. Starting point: z/VM partition on a z14 with CPACF enabled

2. Select configuration in System Configuration file (can modify it dynamically later, if you change your mind)

3. Generate an ephemeral *n*-bit AES encryption key during IPL process

4. If ENCRYPT PAGING is ON, then pages are encrypted as they move to/from paging volumes.

5. Use monitor records to determine performance impact for workloads

Relevant Hills: SUB-HILLS 1 & 3
Relevant Sponsor User Roles: Data Owner, Security Admin, Auditor
Security Admin Products: z/VM

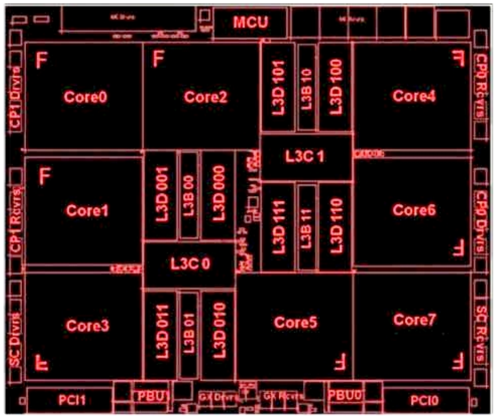
CP-Assisted Cryptographic Facility (CPACF)

CPACF Support (No-Charge Licensed Feature 3863)

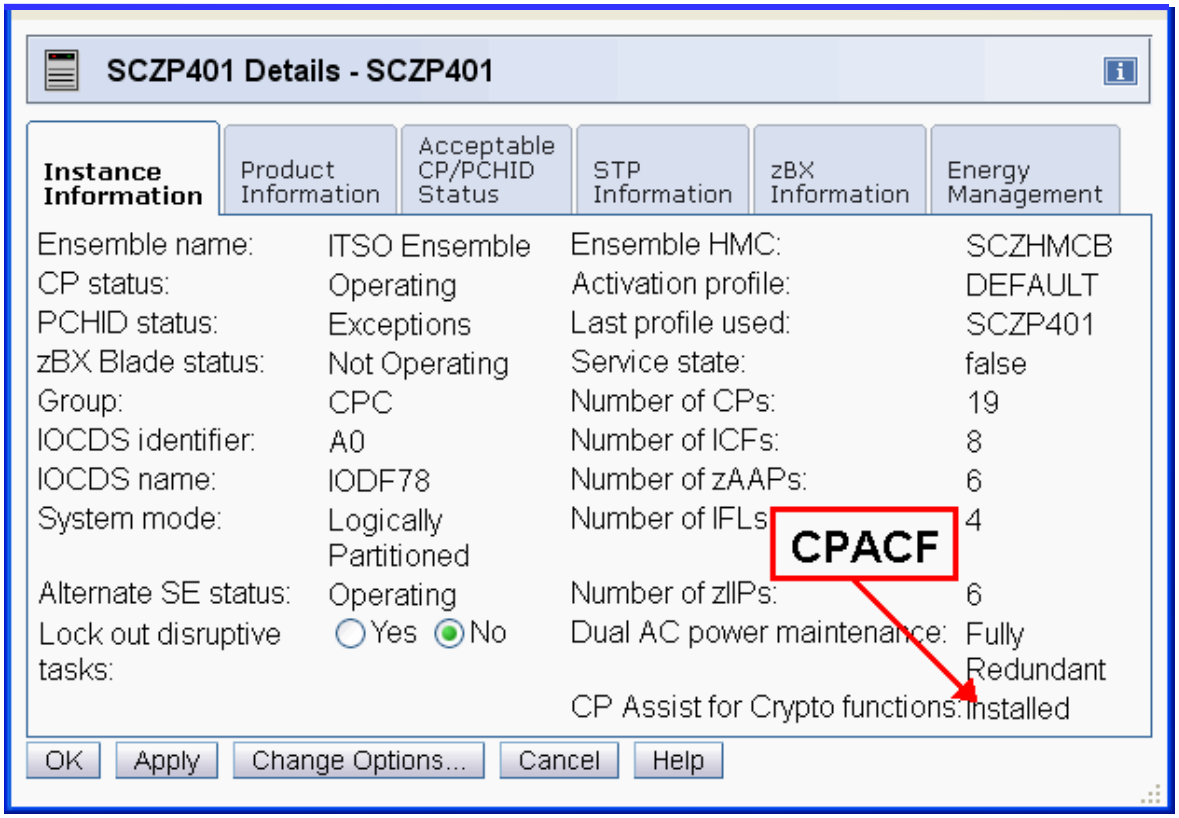
- Available on all modern IBM Z hardware but it must be explicitly ordered and enabled
- Provides on-CPU cryptographic processing ***at a higher throughput***
- Supports the following algorithms:
  - DES
  - TDES
  - AES-128
  - AES-256 (z10 onward)

  - SHA-1
  - SHA-224 and SHA-256
  - SHA-384 and SHA-512 (z10 onward)

  - Single-length key MAC
  - Double-length key MAC



CP-Assisted Cryptographic Facility (CPACF)



SCZP401 Details - SCZP401

Ensemble name:	ITSO Ensemble	Ensemble HMC:	SCZHMCB
CP status:	Operating	Activation profile:	DEFAULT
PCHID status:	Exceptions	Last profile used:	SCZP401
zBX Blade status:	Not Operating	Service state:	false
Group:	CPC	Number of CPs:	19
IOCDS identifier:	A0	Number of ICFs:	8
IOCDS name:	IODF78	Number of zAAPs:	6
System mode:	Logically Partitioned	Number of IFLs:	4
Alternate SE status:	Operating	Number of zIIPs:	6
Lock out disruptive tasks:	○ Yes ● No	Dual AC power maintenance:	Fully Redundant
		CP Assist for Crypto functions:	Installed

CPACF

Using Encrypted Paging for z/VM (1/2)

- ***new*** ENCRYPT Statement in System Configuration file
  - `ENCRYPT PAGING ON ALGORITHM AES256`

- ***new*** QUERY/SET ENCRYPT
  - `SET ENCRYPT PAGING {OFF | ON | REQUIRED}`
  - ALGORITHM selection when first enabled (AES 128, 192, 256)

- **Note**: REQUIRED may cause complications with DR sites
  - System will not IPL on earlier hardware, or if missing CPACF
  - Recommendation: keep a backup System Configuration file for SALIPL emergencies
  - Recommendation: use sysname keywords in System Config to specify ENCRYPT by system or node
  - Recommendation: IPL your system with `ENCRYPT PAGING ON <algorithm>`
    - `SET ENCRYPT PAGING REQUIRED` via AUTOLOG1 or via a COMMAND Statement
    - Audit trail demonstrates encryption was never “off.”

Using Encrypted Paging for z/VM (2/2)

- Auditing with MONITOR Records
  - D1R4 – System Configuration and current status thereof
  - D3R2 – Change record for status (SET ENCRYPT), with userid
  - ***new*** D1R34 – Pages encrypted/decrypted, CPU utilization for encryption

- If moving from ON to OFF, pages will still be decrypted when read into guest memory

- Only way to ensure 100% compliance is to IPL your z/VM system with
  - `ENCRYPT PAGING ON ALGORITHM AES256`

- Auditing with SMF Records
  - Auditing in RACF automatically covers new CP commands, per above
  - Just enable tracking in your VMXEVENT profile

D3R2CRP.EXEC

- Tool from z/VM Performance Team to track encrypted paging monitor values
- Will be available on z/VM Performance website when the PTF ships
- Performance Toolkit updates to follow at a later date

```
D3R2 Encrypted paging report for file: A05Y9152 MONDATA

Interval           <------- Rate of Pages --------> <------ Percent CPU busy ------>
__Ended_ Type LPU_ _Enc+Dec__ Encrypted_ Decrypted_ _Enc+Dec__ __Encrypt_ __Decrypt_

>>Mean>> IFL  0      19451.25   11662.78    7788.47    2.45044    1.71205    0.73840
>>Mean>> IFL  1      19036.57    9766.84    9269.73    2.31351    1.43584    0.87766
>>Mean>> IFL  2      19153.36    9761.35    9392.01    2.32062    1.43352    0.88710
>>Mean>> IFL  3      19010.73    9657.54    9353.18    2.32729    1.43122    0.89607
>>Mean>> IFL  4      19131.78    9685.10    9446.68    2.33772    1.43319    0.90453
>>Mean>> IFL  5      21139.60    9656.43   11483.17    2.50907    1.42566    1.08341
>>Mean>> IFL  6      21351.01    9744.53   11606.48    2.53488    1.44154    1.09333
>>Mean>> IFL  7      21167.82    9827.81   11340.01    2.52316    1.45072    1.07244
>>Total> .... 8     159442.12   79762.38   79679.73   19.31669   11.76374    7.55294

15:27:27 IFL  0      14500.07    9057.13    5442.94    1.83363    1.33507    0.49856
15:27:27 IFL  1      15452.78    8950.06    6502.72    1.91393    1.31984    0.59409
15:27:27 IFL  2      15215.59    8310.86    6904.73    1.85513    1.22522    0.62991
15:27:27 IFL  3      14394.43    7823.19    6571.24    1.78056    1.17005    0.61051
15:27:27 IFL  4      14700.28    8225.17    6475.11    1.82524    1.22422    0.60102
15:27:27 IFL  5      18332.57    8317.30   10015.27    2.14883    1.23835    0.91048
15:27:27 IFL  6      18304.86    8439.71    9865.15    2.15040    1.25402    0.89638
15:27:27 IFL  7      18117.23    8296.26    9820.97    2.12680    1.23287    0.89393
>>Total> .... 8     129017.81   67419.68   61598.13   15.63452    9.99964    5.63488

15:27:57 IFL  0      20984.71   11808.29    9176.42    2.58744    1.71926    0.86818
15:27:57 IFL  1      20038.51    8859.42   11179.09    2.34774    1.29137    1.05637
15:27:57 IFL  2      20170.38    9001.16   11169.22    2.36140    1.30838    1.05302
15:27:57 IFL  3      19741.21    8430.19   11311.02    2.31781    1.23350    1.08431
15:27:57 IFL  4      19681.81    8459.56   11222.25    2.30965    1.23409    1.07556
15:27:57 IFL  5      22587.21    8467.49   14119.72    2.56253    1.23307    1.32946
15:27:57 IFL  6      22904.38    8472.96   14431.42    2.59338    1.23633    1.35705
15:27:57 IFL  7      23478.97    9439.22   14039.75    2.70212    1.37671    1.32541
>>Total> .... 8     169587.18   72938.29   96648.89   19.78207   10.63271    9.14936
```

Best Practices with z/VM Encrypted Paging

- System Configuration: Use ON and <u>not</u> REQUIRED
  - –Safer for DR scenarios
  - –Prevents accidental lockout
  - –Switch to REQUIRED in AUTOLOG1 (before RACF is IPL'd)

- Test your workloads vs. ephemeral key size
  - –Find the encryption strength which works best for you
  - –Watch for Performance Guidance from IBM z/VM
  - –Consider your security needs when enabling encryption at one level vs. another

- Audit your Encryption
  - –Monitor records – watch for updates to Performance Toolkit etc.
  - –SMF records – mind your security at all times

Encrypted Paging: Frequently Asked Questions (1/2)

- Can I turn it on and/or off after IPL?
  - *Yes! But bear in mind that we won't automatically decrypt previously encrypted pages until it's time to page them out.*

- Why does Encrypted Paging require z14?
  - *In order to generate ephemeral keys, z/VM needs the TRNG now available on z14 CPACF. Keys generated with PRNG would not have been reasonably secure.*

- What do I do if I lock myself out?
  - *We recommend you keep a back-up system configuration file available and specify that on your SALIPL screen in case of emergencies.*

Encrypted Paging: Frequently Asked Questions (2/2)

- How much does it cost?
  - *Early performance measurements look good -- 4% increase in CPU utilization on a z14*
  - *Better performance encrypted than the z13 unencrypted*
  - *Official performance reports and tooling will follow PTF availability*

- What about Single System Images and Live Guest Relocation?
  - *One ephemeral key per member system where enabled*
  - *Guest relocation will need to decrypt pages before relocating them to target system*
  - *Relocation domains based on security rather than architecture*
  - *No, we're not encrypting CTCs – they're closed physical channels.*

- Why paging? Why not minidisks?
  - *"Minimum Viable Product."* (See Brian for more details on this part.)

IBM z/VM 6.4 Security Enhancements

- z/VM Control Program
  - –Logon Security
  - –CMS Pipelines
  - –Encrypted Paging (coming soon)
- Networking and TCP/IP
  - –Updates to default protocols and settings
  - –Default VLAN Security (with ESM)
  - –Update of crypto library and ported products
  - –CRYPTO APVIRT for TLS/SSL Server (03/2017)
  - –Directory Network Authorization (08/2017)
- Updates to RACFVM
  - –NoAddCreator
  - –DirMaint-RACF Connector
  - –Ease of Use Enhancements (03/2017)
- Cloud Security Updates (January 2017)

z/VM 6.4: LOGON Security

- **Problem**: phishing at CP LOGON to probe for valid virtual machines without authenticating e.g.

```
LOGON NOTHERE
HCPLGA053E NOTHERE not in CP directory

LOGON TCPMAINT
ENTER PASSWORD  (IT WILL NOT APPEAR WHEN TYPED):

HCPLGA050E LOGON unsuccessful--incorrect password
```

In z/VM 6.4: Change logon flow to accept both userid and password; if either invalid, issue a common message, e.g.

```
HCPLGA050E LOGON unsuccessful--incorrect userid
and/or password
```

- **Note**: unlike `TSO LOGON PREPROMPT`, this change is *non-configurable*

z/VM 6.4 CMS Pipelines – the *digest* stage

- Computes “digest” or “hash” over pipeline records
  - Verifies that data has not been modified
  - Similar to existing **crc** stage (16 or 32 bit checksum)

- New digest types create longer checksum
  - Supports popular cryptographic hash standards
  - Some use hardware support (if available)
  - Long checksum attractive for use in CMS as well

```
pipe < pipeline news | digest md5 | spec 1-* c2x 1 | cons
661913BF6328DD9A5B29C3A93CA60B70

pipe < pipeline news | digest sha512 | spec 1-* c2x 1 | cons
42FEF021EDB48AEBD1DB42071198E8241224A9F1E23DC15AC4958C837AF8FC62...
```

z/VM 6.4: Networking and TCP/IP

▪TLS Encryption of RSCS and TCPNJE

- –Shipped as an SPE to z/VM 6.3 (*APAR PI56474 and associated service*)
- –Allows RSCS to encrypt traffic to other TCPNJE nodes using the TLS/SSL Server
- –**Best Practices Whitepaper**:
  - http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=ZSW03288USEN&attachment=ZSW03288USEN.PDF

▪Default VLAN access with an ESM

- –Guests may only access VLANs to which they have been granted access
  - Whether it's the Default VLAN or not, your ESM needs to know about it
  - If you're using a Default VLAN today, you may need to update your ESM before migrating to 6.4.
- –True no matter which ESM you're using.

z/VM 6.4: Networking and TCP/IP

- **TLS Encryption of RSCS and TCPNJE**
  - –Shipped as an SPE to z/VM 6.3 (*APAR PI56474 and associated service*)
  - –Allows RSCS to encrypt traffic to other TCPNJE nodes using the TLS/SSL Server
    - Uses existing key databases or .P12 files
    - Uses CPACF automatically if enabled
  - –**`TLSLABEL`** parameter for specifying certificate label
  - –TLS tag on **`SMSG RSCS QUERY LINK`** to note which connections are encrypted
  - –In z/VM 6.4:
    - C and Assembler APIs that made this possible open for system programmer use
  - –**Best Practices Whitepaper**:
    - http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&htmlfid=ZSW03288USEN&attachment=ZSW03288USEN.PDF

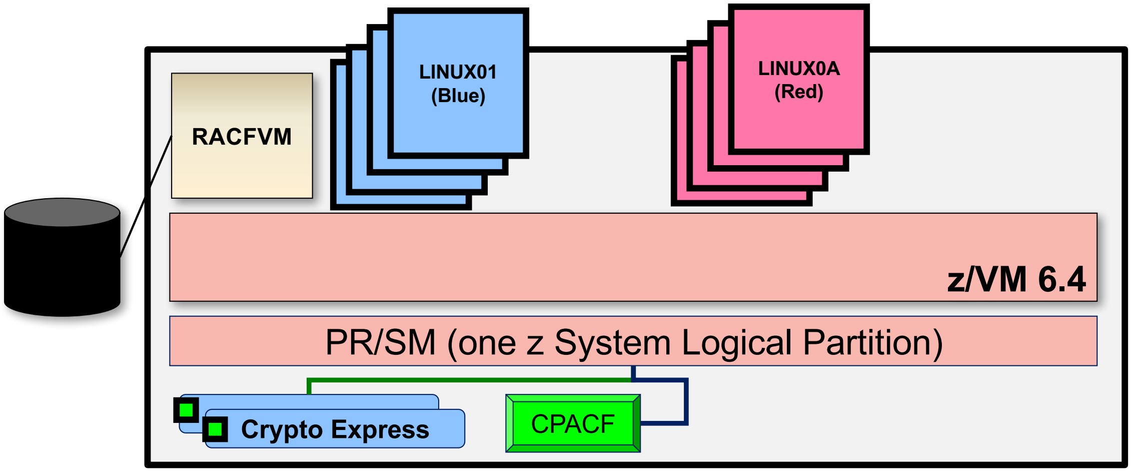
z/VM 6.4: Networking and TCP/IP

- **Default VLAN access with an ESM**
  - –Guests may only access VLANs to which they have been granted access
    - Whether it's the Default VLAN or not, your ESM needs to know about it
    - If you're using a Default VLAN today, you may need to update your ESM before migrating to 6.4.
  - –True no matter which ESM you're using.

- SMTP FORWARDMAIL NO is now default behavior for SMTP Server
  - –Already a best practice, now assumed
  - –No change if your config file already had alternate value

- LDAP has been updated to the z/OS ITDS v2.2 level
  - –Support for TLS 1.2
  - –Password hashing and salted hashing

z/VM 6.4 Security and RACFVM

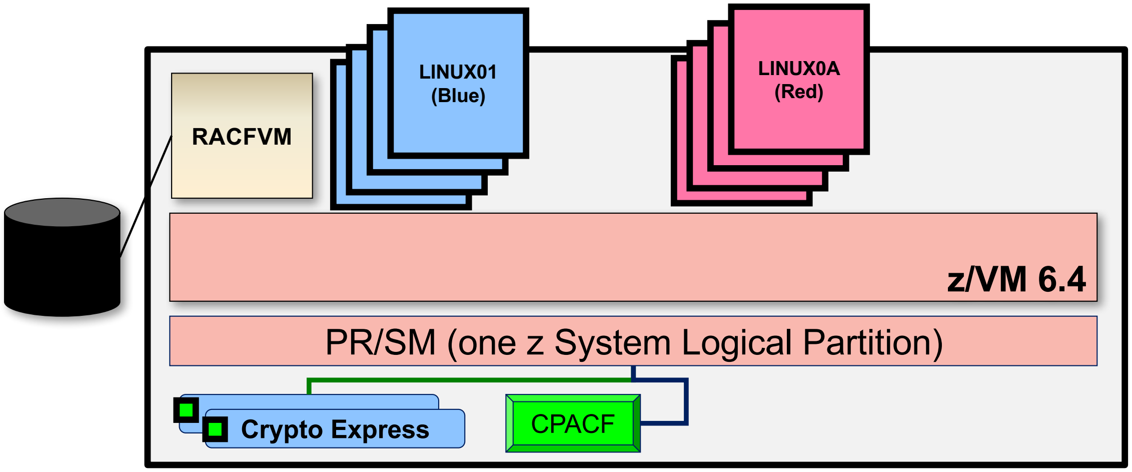


- A **requirement** for meeting today's enterprise security requirements

- RACF enhances z/VM by providing:
  - –Extensive auditing of system events
  - –Strong Encryption of passwords and password phrases
  - –Control of privileged system commands, password policies, access rights …
  - –Security Labeling and Zoning for multi-tenancy within a single LPAR (or across a cluster)

- RACF for z/VM is an **integral component** of z/VM's *Common Criteria evaluations*

z/VM 6.4 Security and RACFVM – What's New?



- RACF NoAddCreator
- Bundling of the z/VM 6.3 RACFVM Updates (KDFAES and associated)
- Exit ICHRCX02 is disabled by default
- **March 2017:** RACFVM Ease-of-Use Enhancements

z/VM 6.4: RACF NoAddCreator

- By default, the issuer of an **RDEFINE** command was added to the access control list for that particular resource
  - –Not a fair assumption to make for advanced-security systems
    - *We don't want BWHUGEN owning everything, after all.*
  - –Not really convenient for cloud-enabled z/VM systems
    - *We also don't want DIRMAINT owning everything, for the same reason*

- RACF for z/VM 6.4 ports the NOADDCREATOR option from z/OS
  - –`RAC SETROPTS ADDCREATOR|NOADDCREATOR`
  - –Default setting for new RACF databases
    - For older databases, template-dependent

- Eliminates need for work-arounds or extra configuration

z/VM 6.4: RACF and ICHRCX02

- ICHRCX02 is a RACF exit related to alternate userid checking

- For years, secure configuration guidance and best-practices have been telling you, "We recommend you just recompile without this. It's safer, especially when you're controlling FTP with RACF."

- In z/VM 6.4, ICHRCX02 is (finally) disabled by default.

RACF Password Encryption Upgrade

(APAR VM65719 and associated service for z/VM 6.3)

- Enables stronger encryption mechanism of passwords | passphrases in a RACF database
  - *Strengthen RACF database against offline attacks*
  - Mitigate compliance issues of older encryption algorithms

The Fine Print

1. Password Encryption Upgrade is for z/VM 6.3 and z/VM 6.4 only. It is not available for earlier releases.
2. KDFAES requires **CPACF**. Feature 3863 must be enabled, or RACFVM will not start if KDFAES is enabled.
3. KDFAES is for an entire database. Note that this may cause a lot of problems if sharing the RACF database (e.g., mixed-level Single System Image clusters, with other levels of z/VM, or even with z/OS).
4. Apply the PTF for APAR VM65688 before using special character support.
5. The RACF template has, understandably, changed. Be advised.

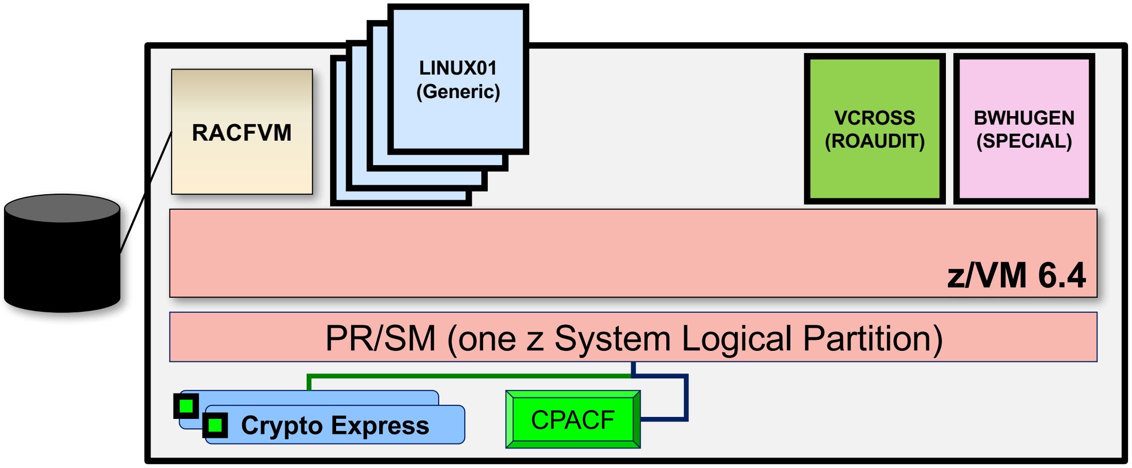
Recent RACF Security Policy Enhancements

(APAR VM65719 and associated service for z/VM 6.3)

Function	Command(s) or Classes
Password Algorithm Select	`SETROPTS PASSWORD(ALGORITHM(KDFAES))`
Password History Cleanup	`ALTUSER userid PWCLEAN`
Password History Conversion	`ALTUSER userid PWCONVERT`
Special Character Support	`SETROPTS PASSWORD(SPECIALCHARS)` ! % & \ _ + | : ? > < . - =
Helpdesk Support	`IRR.PASSWORD.RESET` `IRR.PWRESET.nn`
Password Min-Change Intervals	`SETROPTS PASSWORD(MINCHANGE(value))`
Password Expiry	`ALTUSER userid EXPIRED`
ALTUSER Updates	`NOREVOKE / NORESUME`
CONNECT Updates	`NOREVOKE / NORESUME`
RACUT200	Reserve/Release of RACF Database runs in CST
Passticket Generation (VM65759)	Create passtickets in z/VM via Diagnose x'A0'

z/VM 6.4 Security and RACFVM Ease-of-Use

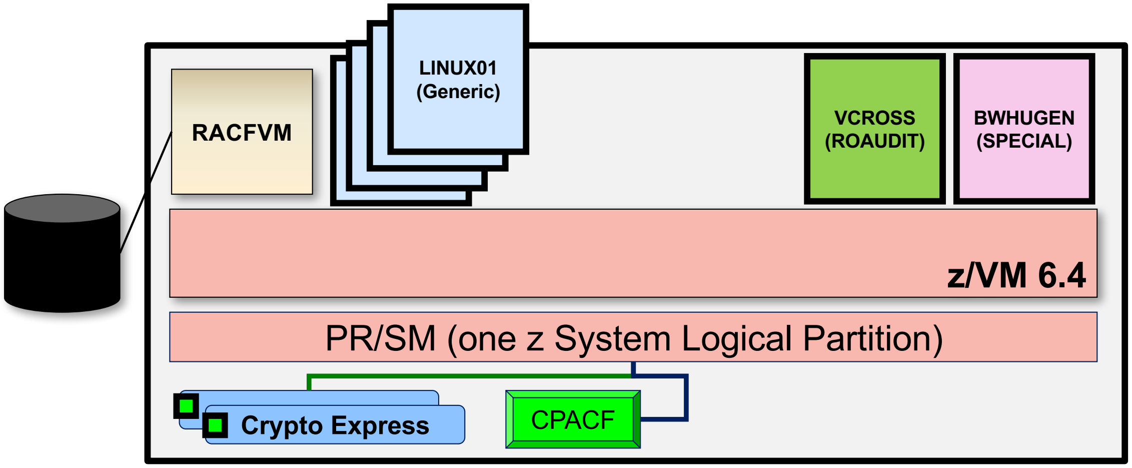
PTF for APAR VM65930



- Read-Only Auditor (ROAUDIT)
- Query VMXEVENT profile(s) – `RAC SET VMEVENT LIST`
- RACF now disallows XAUTOLOG..ON by default when PTF is installed
  - –Special option to consider – make an informed security decision

z/VM 6.4 Security and RACFVM Ease-of-Use

PTF for APAR VM65930



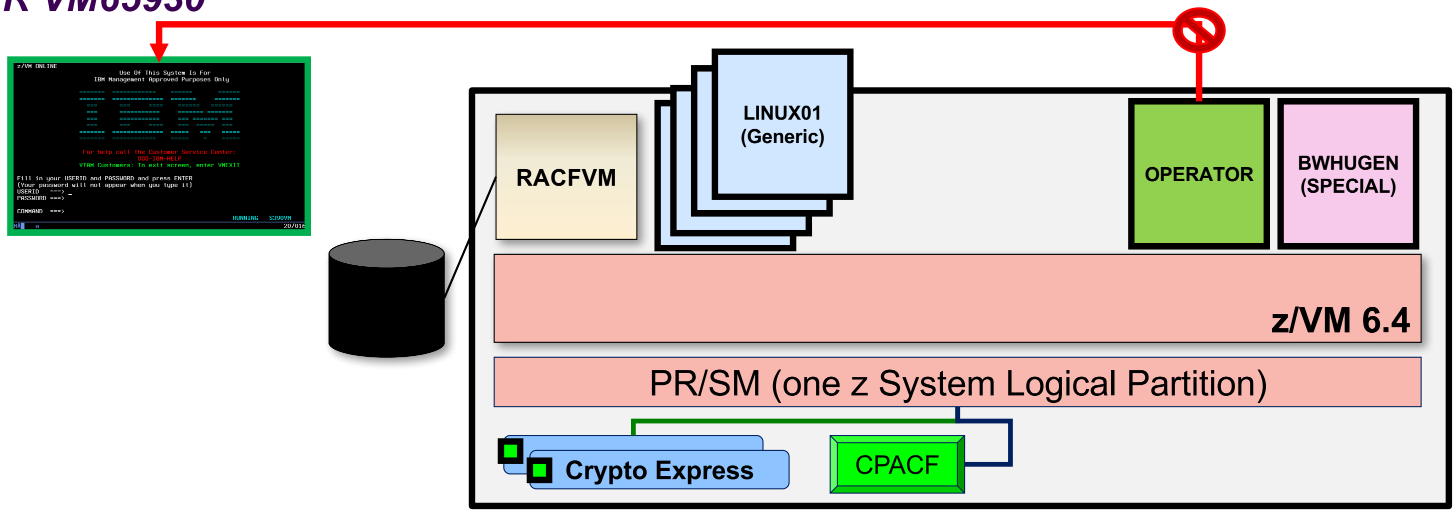
- Read-Only Auditor (ROAUDIT)
  - –Port z/OS feature of the same name – role associated with a RACF USER.
    - Similar to SPECIAL, OPERATIONS, or AUDITOR
  - –Access to SMF logs without the ability to write or tamper
  - –Meet compliance goals without privilege escalation. Also nice for external auditors.

- Use `RAC SET VMEVENT LIST` to query the current VMXEVENT profile(s)

[more…]

z/VM 6.4 Security and RACFVM Ease-of-Use

PTF for APAR VM65930



```
z/VM ONLINE
                              Use Of This System Is For
                          IBM Management Approved Purposes Only

                       =======  ============   ======      ======
                       =======  ==============  =======    =======
                         ===      ===    ====    ======  ======
                         ===      ===========    ======= =======
                         ===      ===========    === ======= ===
                         ===      ===    ====    ===  =====  ===
                       =======  ==============  =====  ===  =====
                       =======  ============    =====   =   =====

                       For help call the Customer Service Center:
                                     888-IBM-HELP
                       VTAM Customers: To exit screen, enter VMEXIT

Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ===> _
PASSWORD ===>

COMMAND  ===>
                                                            RUNNING   S390VM
MA    a                                                                20/016
```

- RACF now disallows XAUTOLOG..ON by default, the moment the PTF is installed
  - "XAUTOLOG Over There" autologs any virtual machine to a VDEV
  - A "break glass in case of emergency" operand (Class A/B) with no authentication required
  - Generic RAC profile can restore original behavior: `RAC RDEFINE VMCMD XAUTOLOG.ON.** UACC(READ)`
  - Specific access can be granted on a per-user / per-system basis
- We want you to make a security decision for your system – do what's right for your shop

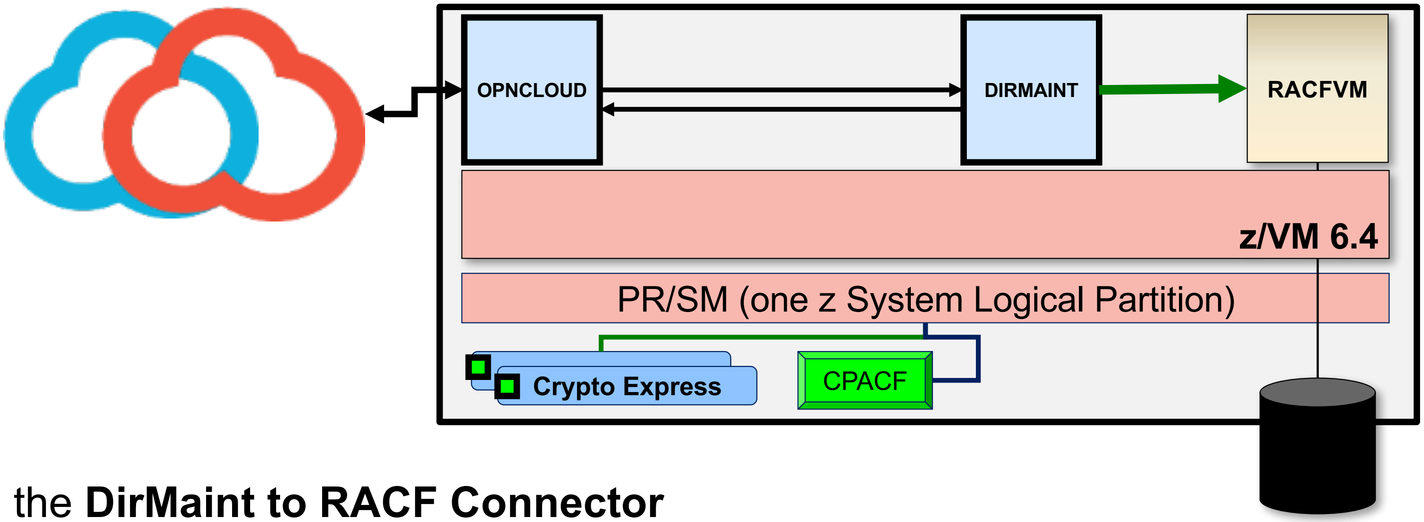
Why does this matter to you?

- Passwords and password phrases should only map to human users …
  - Linux guests and other workloads should be AUTOONLY or LBYONLY
  - Map administrator access to RACF SURROGAT class
  - Control and audit access by administrators to guest workload

- But even 1 password is applicable to by a corporate security policy
  - Or industry standards
  - Or government policy

- These changes enable greater control of the password lifecycle and protection of those credentials against offline attack

z/VM 6.4: DirMaint-RACF Connector Upgrade



- Upgrades to the **DirMaint to RACF Connector**
  - –Modernizes the Connector with a collection of functional enhancements
  - –Brings processing in line with modern z/VM practices
  - –Allows better passing of directory information to RACF
  - –Facilitates proper security policy in environment managed by IBM Wave for z/VM or OpenStack frameworks

z/VM 6.4: DirMaint-RACF Connector (Enabling)

1. Install an External Security Manager (RACF)
2. Update **CONFIGRC DATADVH** in DirMaint
   - Send the sample configuration file to your reader:
     ```
     DIRM SEND CONFIGRC SAMPVH
     ```
   - Rename file to CONFIGRC DATADVH and make changes
   - Update file on DIRMAINT production disk by issuing:
     ```
     DIRM FILE CONFIGRC DATADVH
     ```
   - Place new file into production
     ```
     DIRM RLDDATA
     ```
3. Adjustments based upon resource creation and modification
4. Password policy checks in DirMaint exits
5. Further refinements

z/VM 6.4: DirMaint-RACF Connector (How To)

Enable the exit for every supported RACF function …

```
USE_RACF= YES ALL
```

… Or enable on a per-function basis

```
/*!--------------------------------------------------------------------*/
/*! Command handler for LINK Change related commands.                  */
/*!--------------------------------------------------------------------*/
/USE_RACF= YES DVHRLN   EXEC
/USE_RACF= NO  DVHRLN   EXEC
/*!--------------------------------------------------------------------*/
/*! Command handler for NICDEF Change related commands.                */
/*!--------------------------------------------------------------------*/
/USE_RACF= YES DVHRVN   EXEC
/USE_RACF= NO  DVHRVN   EXEC
```

z/VM 6.4: DirMaint-RACF Connector (Details)

```
USE_RACF= YES|NO ALL|dirm_file_name|exit_name
RACF_ADDUSER_DEFAULTS= UACC(NONE
RACF_RDEFINE_VMMDISK_DEFAULTS= UACC(NONE) AUDIT(FAILURES(READ))
RACF_DISK_OWNER_ACCESS= ACC(ALTER)
RACF_RDEFINE_VMPOSIX_POSIXOPT.QUERYDB= UACC(READ)
RACF_RDEFINE_VMPOSIX_POSIXOPT.SETIDS= UACC(NONE)
RACF_RDEFINE_SURROGAT_DEFAULTS= UACC(NONE) AUDIT(FAILURES(READ))
RACF_RDEFINE_VMBATCH_DEFAULTS= UACC(NONE) AUDIT(FAILURES(READ))
RACF_RDEFINE_VMRDR_DEFAULTS= UACC(NONE) AUDIT(FAILURES(READ))
RACF RDEFINE_VMLAN_DEFAULTS= UACC(NONE) AUDIT(FAILURES(READ))
RACF_VMBATCH_DEFAULT_MACHINES= BATCH1 BATCH2
TREAT_RAC_RC.4= 0|4
ESM_PASSWORD_AUTHENTICATION_EXIT= DVHXPA EXEC
```

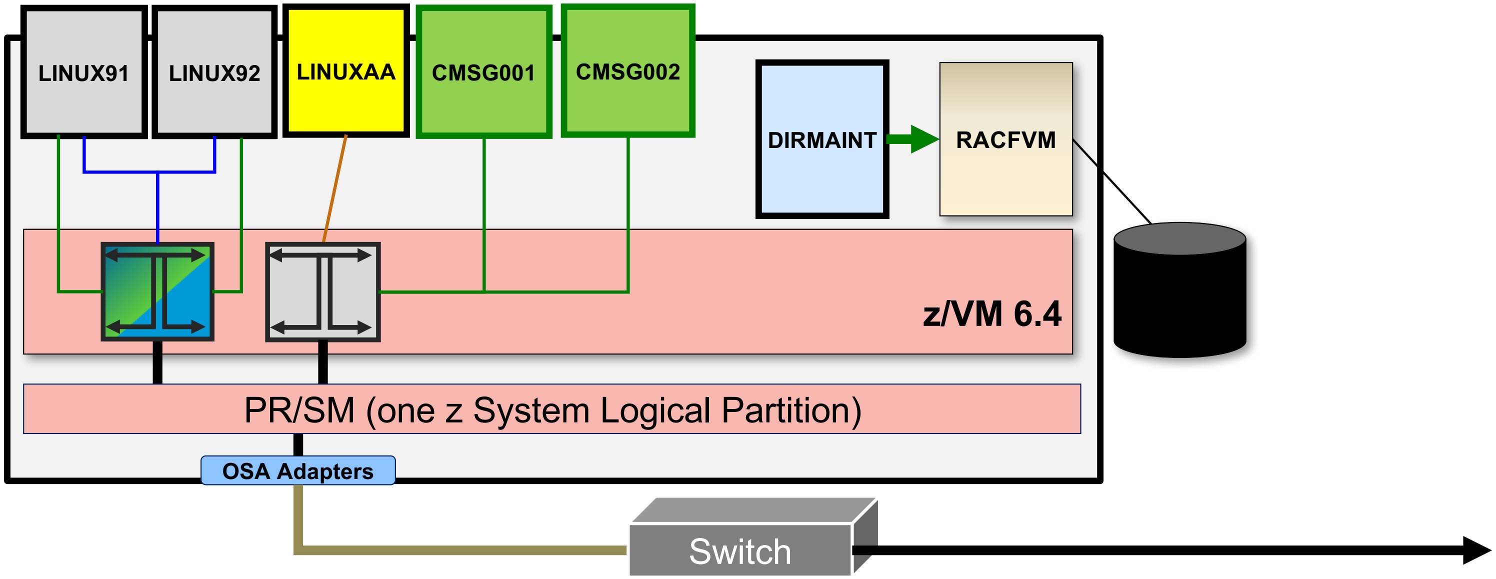
z/VM 6.4: DirMaint-RACF Connector (Updates!)

- **Connector: LINK statement handling**
  - –For changes made through DirMaint, VMMDISK permissions granted
  - –Configure UACC, Owner, etc.
  - –Removes 10 pages of extra steps for RACF+SMAPI configuration

- **Connector: NICDEF statement handling**
  - –VMLAN permissions granted for changes made in DirMaint
  - –Works for network connections of all types (Guest LAN, VSwitch …)
  - –Note that it's meant for access for guests to Switches, not for VSwitch management itself
  - –**With Directory Network Authorization, now handles User- and Port-based Switches**

Directory Network Authorization for z/VM 6.4 Virtual Switch

Available August 2017 – *PTFs for APARs VM65925, VM65926, VM65931*



- **Streamlining Network Security**
  - "Directory Network Authorization" (DNA)
  - Port-Based and User-Based access to virtual switch on CP NICDEF statement
  - Updates to DirMaint NICDEF command and DirMaint-RACF Connector –transfer to RACF
  - RPIDIRCT updated to translate new statement into security policy

What do I do to use DNA?

- Step 1: Apply PTFs for CP, DirMaint and RACF. *(C'mon, that was the easy part.)*
  - System Configuration: **VMLAN … DNA ENABLE** (default)
  - z/VM DIRECTXA processes the new directory statement changes
  - NICDEF statement defines properties of virtual NIC
  - NICDEF also now supports network attributes defined by CP SET VSWITCH

- Then, secure it. Recommend change access be restricted for:
  - LAN, MACID, PORTNUMBER, VLAN, PROMISCUOUS
  - Impacts security policy, should be administrator-only
  - DirMaint will have these changes when you apply that PTF (DIRM NICDEF no longer a general-user command)

```
NICDEF vdev [TYPE HIPERS | QDIO]
                [DEVices devs]
                [LAN owner name]
                [CHPID xx]
                [MACID xxyyzz]
                [PORTNUMber nnnn]
                [PORType ACCESS|TRUNK]
                [VLAN vidset]
                [PROmiscuous|NOPROmiscuous]
```

DNA: What About VMRELOCATE?

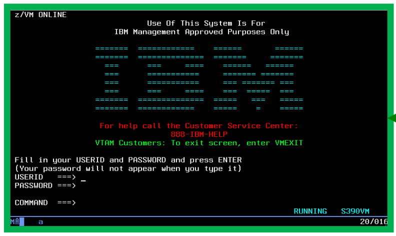
- VMRELOCATE is not directly affected, but be advised:
  - Systems without this PTF will not recognize new NICDEF features
  - Common User Directory interpreted differently on each member
  - Be cautious

If you have a …	on a …	Then be warned that …
System-assigned port	Port-based VSwitch	No relocation to a pre-DNA system. Ports > 2048 unsupported
User-defined port	User-based Vswitch	It may not have the same port if relocated to a pre-DNA system
User-defined port	User-based Vswitch	Relocation my fail if the port belongs to a different user on target system

Summary

OPEN STACK
LINUX
RSCS
RACF
XCAT
DUMP VIEW FACIL
XEDIT
PERF KIT
DIR MAINT
LGR
VM SSI
IUCV
APPC
AVS
GCS
OPEN EXTNS
CMS
REXX
HCD
HCM
LANGUAGE
TSAF
OSA
TCP /IP
OPEN VM
VM SES/E
HIPER DISPATCH
CP

z/VM and Pervasive Encryption

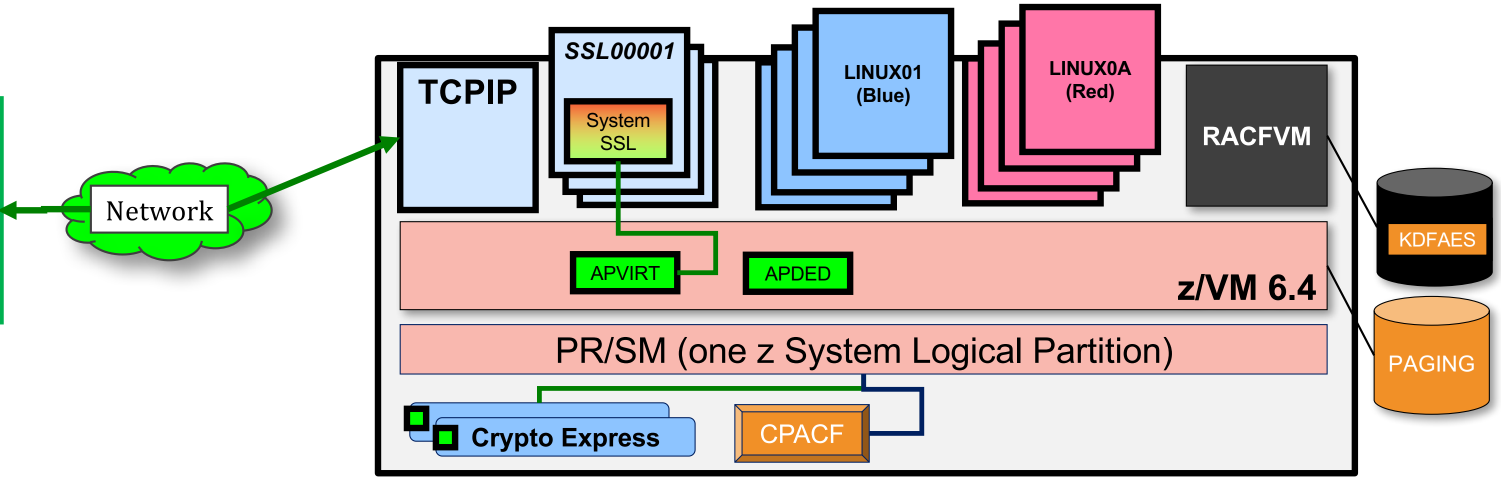


```
z/VM ONLINE
                    Use Of This System Is For
                IBM Management Approved Purposes Only

          For help call the Customer Service Center:
                         888-IBM-HELP
          VTAM Customers: To exit screen, enter VMEXIT

Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ===> _
PASSWORD ===>

COMMAND  ===>
                                             RUNNING   S390VM
MA   a                                                  20/016
```



- Protection for guest operating systems
  - Encryption needs to exist in virtual environments, too!
- Protection of data in flight
  - Modernized software crypto library
  - Crypto Express acceleration for hypervisor traffic

- Protection for data at rest
  - Encrypted Paging as the first step (12/2017)
  - More to follow …
- Simplification and ease of use
  - Security and cryptography should not be an impediment to business

z/VM 6.4 Security – What's Next?

- **Per Statements of Direction**: Security Certifications (in progress)
- **Per z14 RFA**: Encrypted Paging for z/VM

- We'll continue to work with Design Thinking and Sponsor Users
  - Finding out what's most meaningful to you
  - Delivering quick but meaningful function

Do you want more z/VM Security enhancements?

Submit one!

https://www.ibm.com/developerworks/rfe/

For More Information …

- **IBM z14 Technical Guide:** http://www.redbooks.ibm.com/redpieces/abstracts/sg248451.html?Open
- **IBM Z Crypto Education Community**: https://www.ibm.com/developerworks/community/groups/community/crypto
- **Linux on z Security:** https://www.ibm.com/support/knowledgecenter/linuxonibm/liaaf/security.html
- **z Systems Security Portal (IBM ResourceLink) :** http://www-03.ibm.com/systems/z/solutions/security_subintegrity.html
- **IBM Z Hardware Crypto Synopsis:** https://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100810
- **z/VM Security:** http://www.vm.ibm.com/security
- **1Q17 Security Enhancements – APAR Information**
  - http://www-01.ibm.com/support/docview.wss?uid=isg1VM65930
  - http://www-01.ibm.com/support/docview.wss?uid=isg1PI72106
  - http://www-01.ibm.com/support/docview.wss?uid=isg1VM65942

Contact Information:

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