


Security in z/VM 6.4:

News and How-To's (2017 Edition)

Brian W. Hugenbruch, CISSP  *@Bwhugen*
IBM z Systems Virtualization and Cloud Security
z/VM Development Lab: Endicott, NY



Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

BladeCenter*	FICON*	OMEGAMON*	RACF*	System z9*	zSecure
DB2*	GDPS*	Performance Toolkit for VM	Storwize*	System z10*	z/VM*
DS6000*	HiperSockets	Power*	System Storage*	Tivoli*	z Systems*
DS8000*	HyperSwap	PowerVM	System x*	zEnterprise*	
ECKD	IBM z13*	PR/SM	System z*	z/OS*	

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
 Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
 Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
 IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.
 ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
 Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
 Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and
 Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
 Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
 OpenStack is a trademark of OpenStack LLC. The OpenStack trademark policy is available on the [OpenStack website](#).
 TEALEAF is a registered trademark of Tealeaf, an IBM Company.
 Windows Server and the Windows logo are trademarks of the Microsoft group of countries.
 Worklight is a trademark or registered trademark of Worklight, an IBM Company.
 UNIX is a registered trademark of The Open Group in the United States and other countries.

* Other product and service names might be trademarks of IBM or other companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g., zIIPs, zAAPs, and IFLs) ("SEs"). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the "Authorized Use Table for IBM Machines" provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html ("AUT"). No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

Disclaimer

The information contained in this document has not been submitted to any formal IBM test and is distributed on an "AS IS" basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

In this document, any references made to an IBM licensed program are not intended to state or imply that only IBM's licensed program may be used; any functionally equivalent program may be used instead.

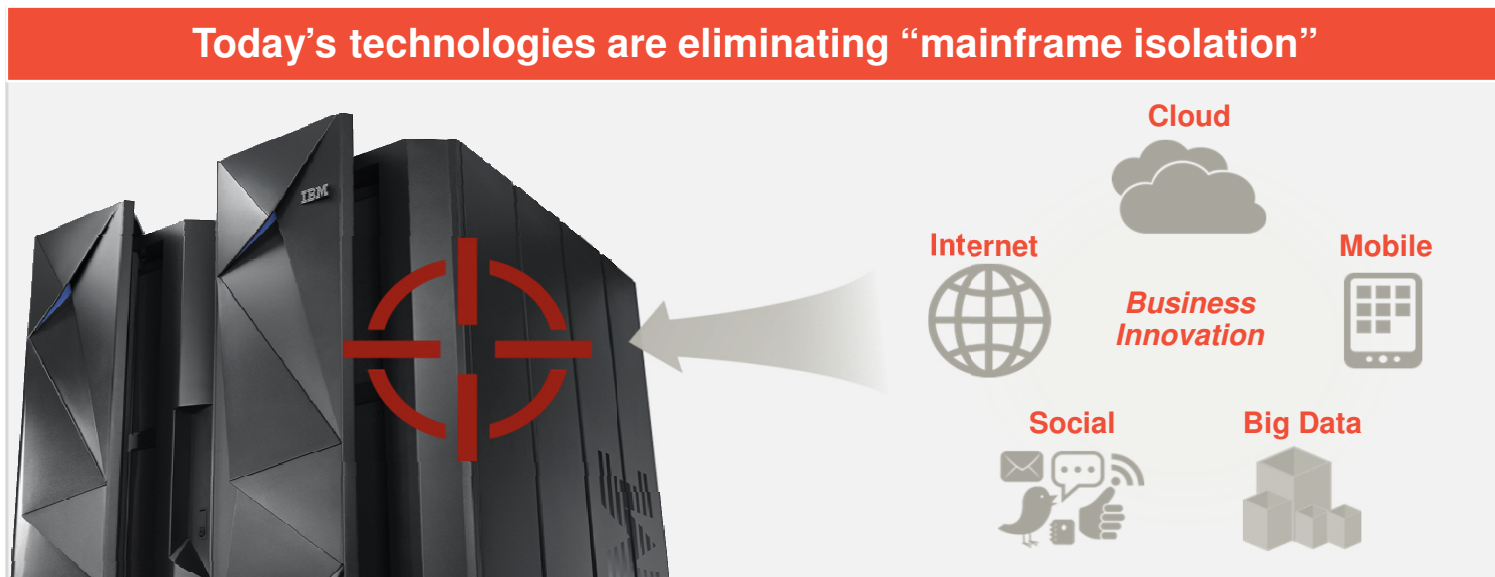
Any performance data contained in this document was determined in a controlled environment and, therefore, the results which may be obtained in other operating environments may vary significantly. Users of this document should verify the applicable data for their specific environments.

It is possible that this material may contain reference to, or information about, IBM products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that IBM intends to announce such IBM products, programming or services in your country.

The increasingly desirable target of the mainframe

80 %
of all active code
runs on the mainframe

80 %
of enterprise data is
housed on the mainframe



Source: 2013 IBM zEnterprise Technology Summit

Agenda

- **z/VM Security Certifications**

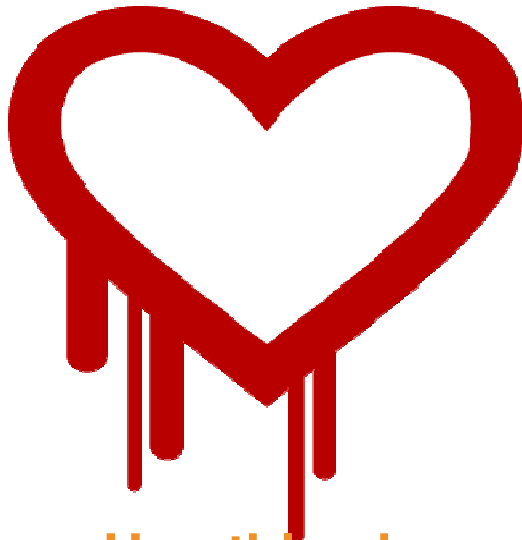
- **z/VM 6.4 – Ease-of-use in managing z/VM security**
 - z/VM 6.3 SPEs
 - z/VM 6.4 Base Security Content
 - *new*** *z/VM 6.4 1Q17 Security Enhancements!*

- **Discussion / Questions**

**But first, an advertisement:
z Systems Security Portal**



IBM Security formally labeled 2014 as "insane" ...



Heartbleed



Bar Mitzvah

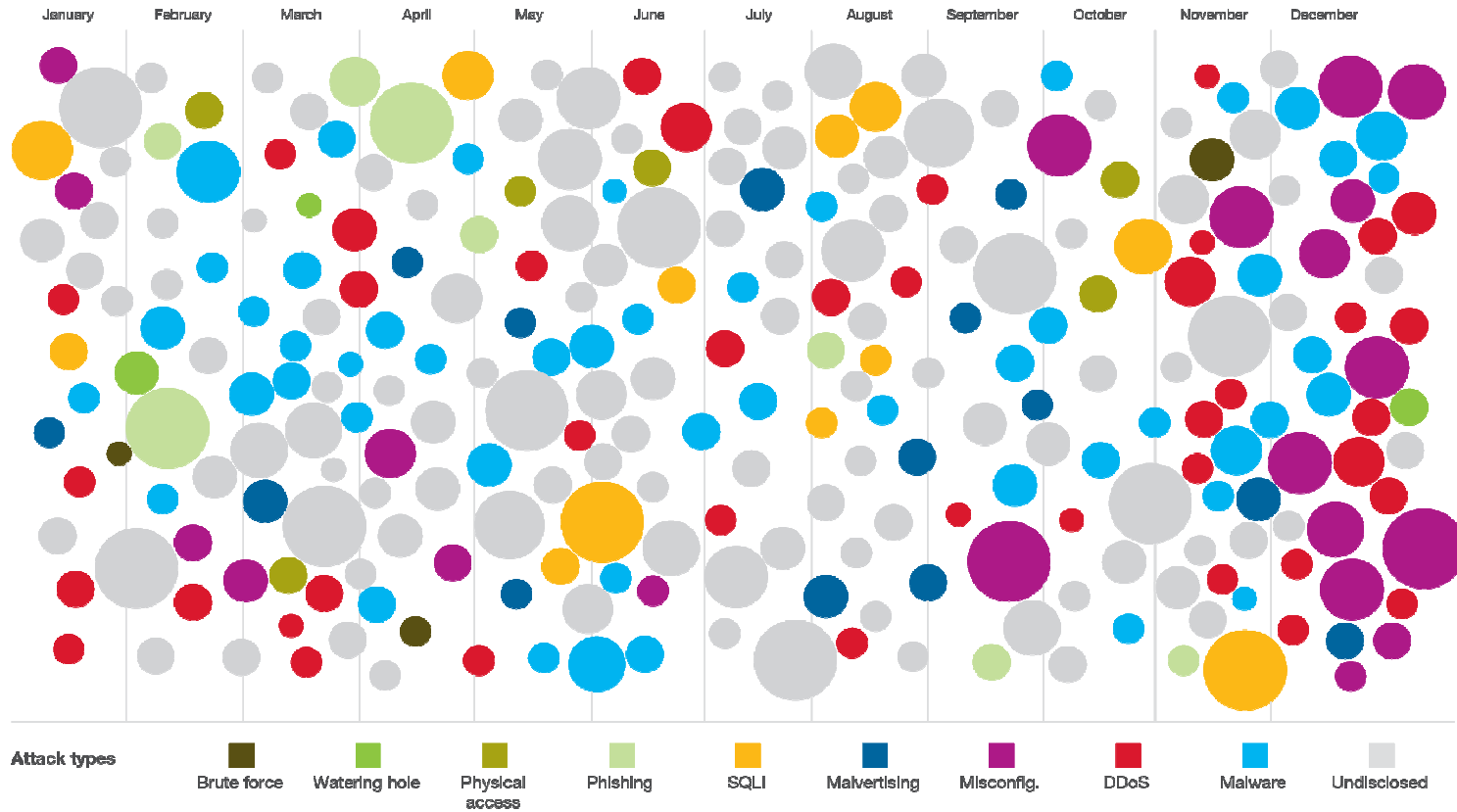


VENOM
CVE-2015-3456



... and the situation has not improved.

Sampling of 2015 security incidents by attack type, time and impact



\$18M average organizational cost of a data breach in the U.S.

\$606 average organizational cost per compromised record in the U.S.

"Is z/VM vulnerable to that thing I heard on Twitter?"



Advertisement: z Systems Security Portal

- IBM z Systems Security policy prohibits the general disclosure of vulnerability analyses (negative or positive).
- z/VM provides a CVSS Score and Vector for Security-related z/VM APARs (“**ResourceLink**” information) for subscribed customers
 - “In addition, Security Notices will be published through this website in order to address high-profile security issues, notifications and possible warnings.”
- **Customer access** to the portal can be obtained at the following website:
http://www-03.ibm.com/systems/z/solutions/security_subintegrity.html

z/VM Security Certifications (2017 News)



z/VM Security Certifications

z/VM Level	Common Criteria	FIPS 140-2
z/VM 6.4	<i>pending</i>	<i>pending</i>
z/VM 6.3	OSPP with Labeled Security and Virtualization at EAL 4+ <ul style="list-style-type: none"> • 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+ <ul style="list-style-type: none"> • 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.

Common Criteria Evaluation of z/VM V6.4

October 25, 2016 Announcement

IBM intends to evaluate z/VM V6.4 with the RACF Security Server feature, including labeled security, for conformance to the **Operating System Protection Profile (OSPP)** of the Common Criteria standard for IT security, ISO/IEC 15408, at **Evaluation Assurance Level 4 (EAL4+)**.

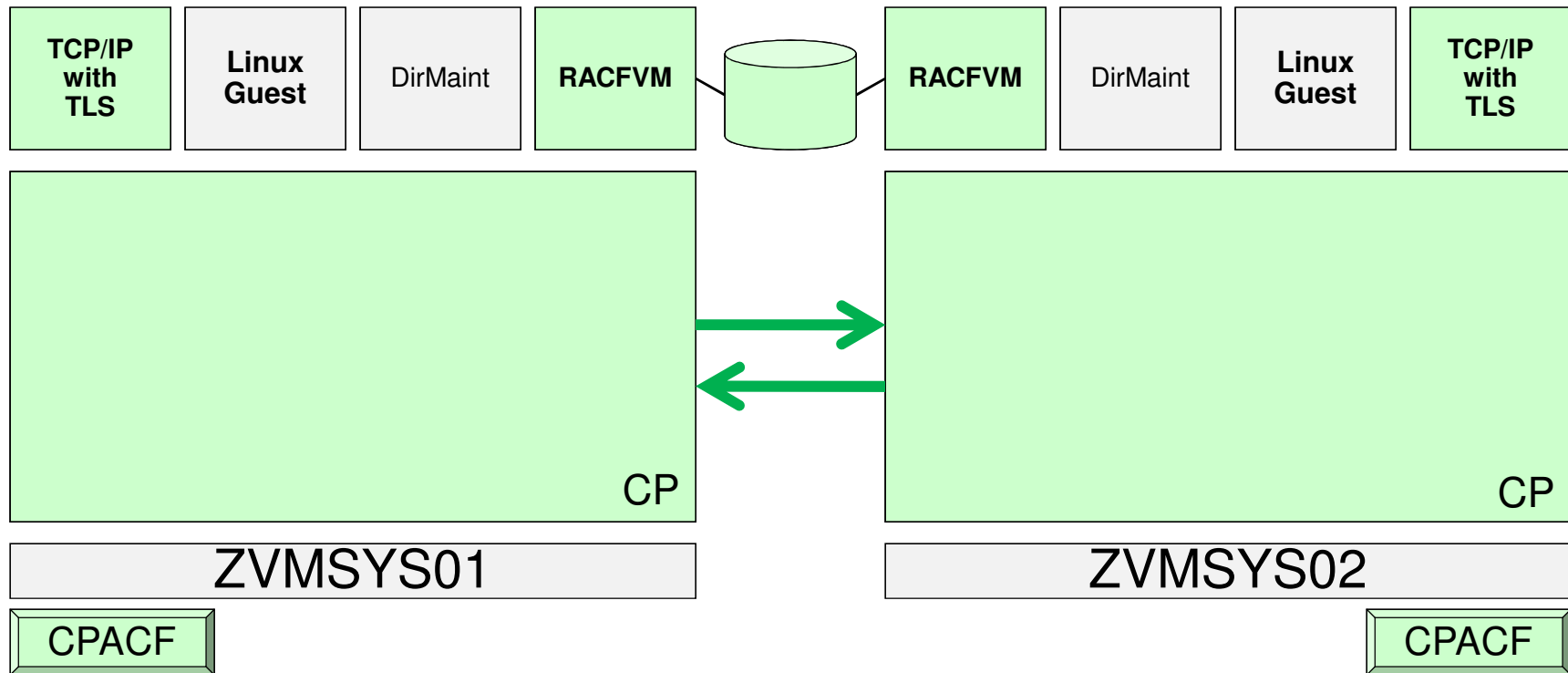
FIPS Certification of z/VM V6.4

October 25, 2016 Announcement

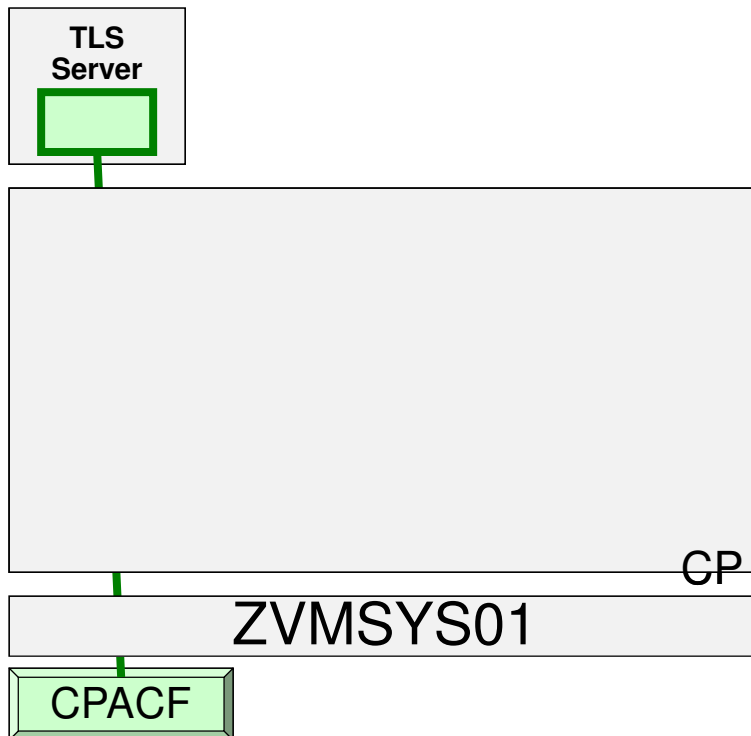
IBM intends to pursue an evaluation of the Federal Information Processing Standard (FIPS) 140-2 using National Institute of Standards and Technology's (NIST) Cryptographic Module Validation Program (CMVP) for the System SSL implementation utilized by z/VM V6.4.

z/VM 6.3 Common Criteria Target of Evaluation

(Operating System Protection Profile with Labeled Security and Virtualization extensions)



z/VM 6.3 FIPS 140-2 Cryptographic Boundary



- **z/VM System SSL**
 - Instantiated on a per-VM basis
 - No access to CryptoExpress
 - Does access CPACF
 - No direct CP involvement
- **The FIPS evaluation:**
 - Validates algorithms
 - Validates key sizes
 - Validates integrity checking
 - Power-On Self Testing
 - "FIPS-mode" certificate database



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

z/VM 6.4: Securing the Road to Virtualization



IBM z/VM 6.4

- A release born from customer feedback
 - z Systems Business Leaders Council (zBLC)
 - SHARE dialogues
 - IBM internal T3s (Teach the Teacher)

- Prioritizations set by customers and adjusted by IBM resources and skills

- Two major areas:
 - Technical enhancements that continue to improve TCO and bring direct value
 - Improved quality of life for z/VM system programmers

- New Architecture Level Set (ALS)
 - z196 and z114 or newer
 - Drops z10 EC and BC support



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 z Systems stack to secure modern workloads.

IBM z/VM 6.4 Security Enhancements

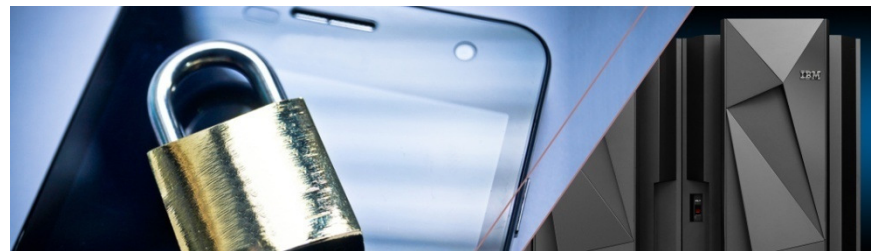
- z/VM Control Program
 - Logon Security
 - CMS Pipelines

- Networking and TCP/IP
 - Updates to default protocols and settings
 - Default VLAN Security (with ESM)
 - Update of crypto library and ported products

- Updates to RACFVM
 - NoAddCreator
 - DirMaint-RACF Connector

- Roll-up of z/VM 6.3 Security SPEs

- Cloud Security Updates



z/VM 6.4: LOGON Security

- **Problem:** someone can connect to CP LOGON and probe for valid virtual machine names 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

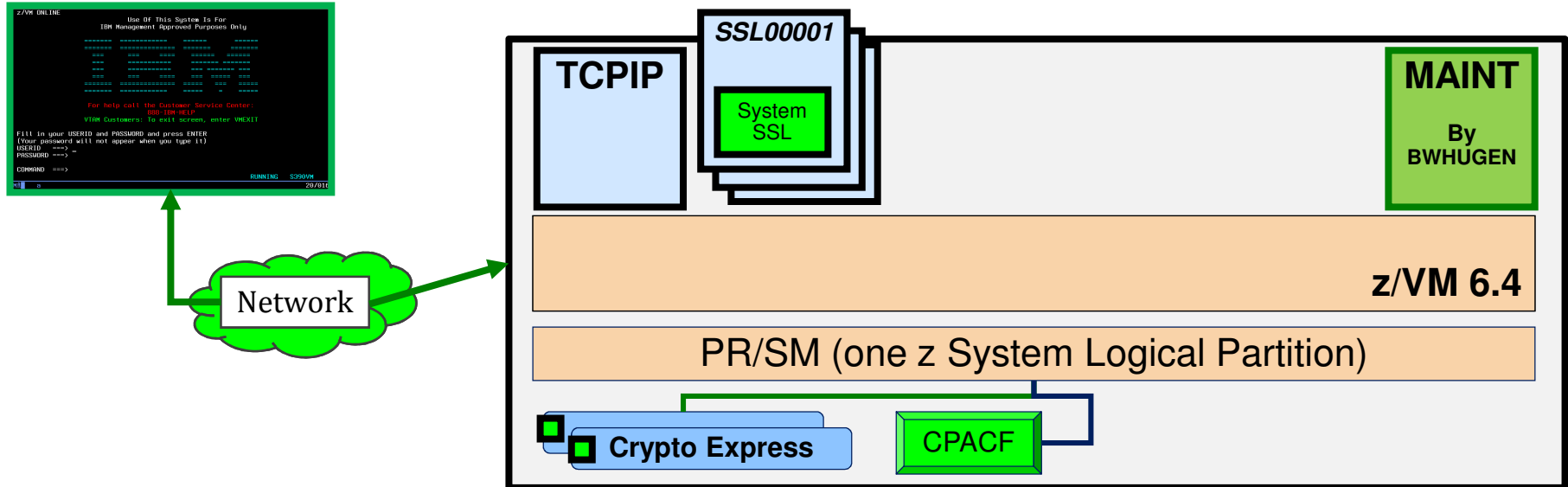
- Computes “digest” or “hash” over pipeline records
 - Verifies that data has not been modified
 - Similar to existing **crc** stage (16 or 32 bit checksum)

- New digest types create longer checksum
 - Supports popular cryptographic hash standards
 - SHA224, SHA256, SHA384 and SHA512 (FIPS 180)
 - SHA1 (160 bit, RFC 3174)
 - MD5 (128 bit, RFC 1321)
 - 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 TLS/SSL Server



- **The TLS/SSL Server has been updated ... a lot.**
 - TLS 1.2 and TLS 1.1 now the default TLS protocols (no SSL)
 - New set of default cipher suites (weak ones disabled by default)
 - System SSL v2.2 support
 - z/VM 6.3 debuted with v1.13, was updated to v2.1 in 2015
 - SHA2 family of hashes (SHA256, SHA512 ...)

z/VM 6.4 TLS/SSL Server

- **Also included are all the changes made in the service stream**
 - TLS and SSL **PROTOCOL selection** now available
 - **PROTOCOL +TLSV1_1**
 - **PROTOCOL -SSLV3**

 - AES Galois/Counter Mode (**AES_GCM**) – automatic with TLS 1.2
 - Larger **DSA certificate** support (2048)
 - 'Mode' Operand for auto-configuration to standards
 - **MODE FIPS-140-2**
 - **MODE 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!*

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
 - CPACF if enabled

- **TLSLABEL** parameter for specifying certificate label

- TLS tag on **MSG 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

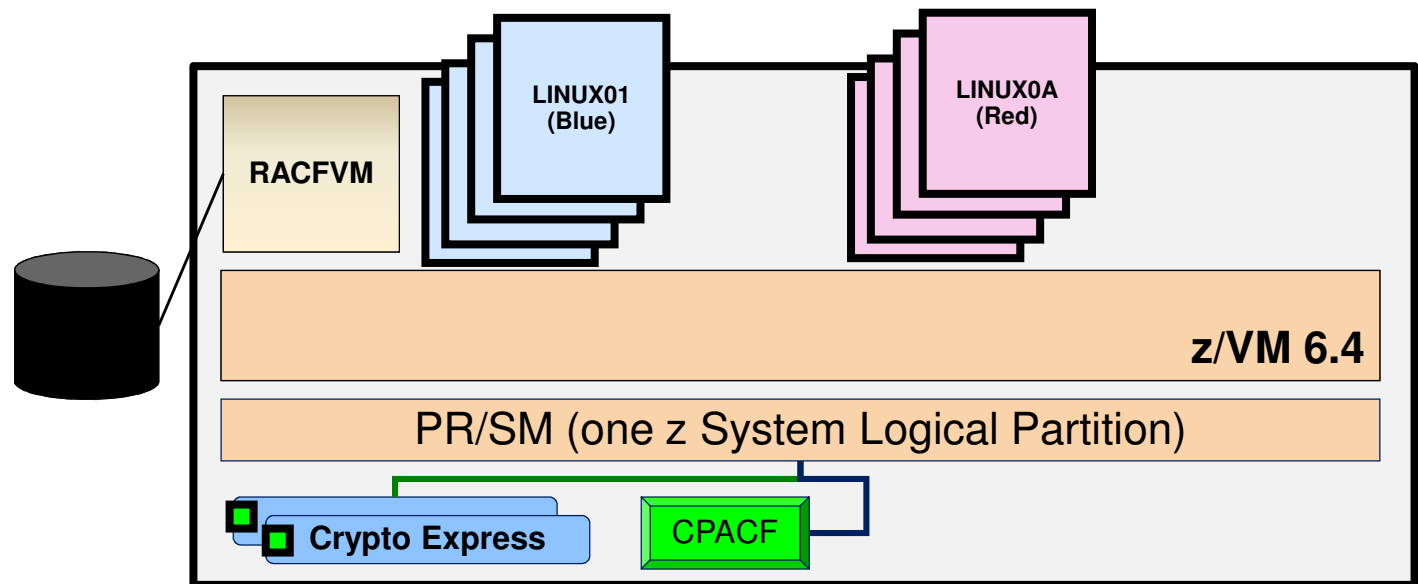
Why does this matter to you?

- 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

- Ability to encrypt TCP/IP traffic inside the hypervisor as well
 - 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

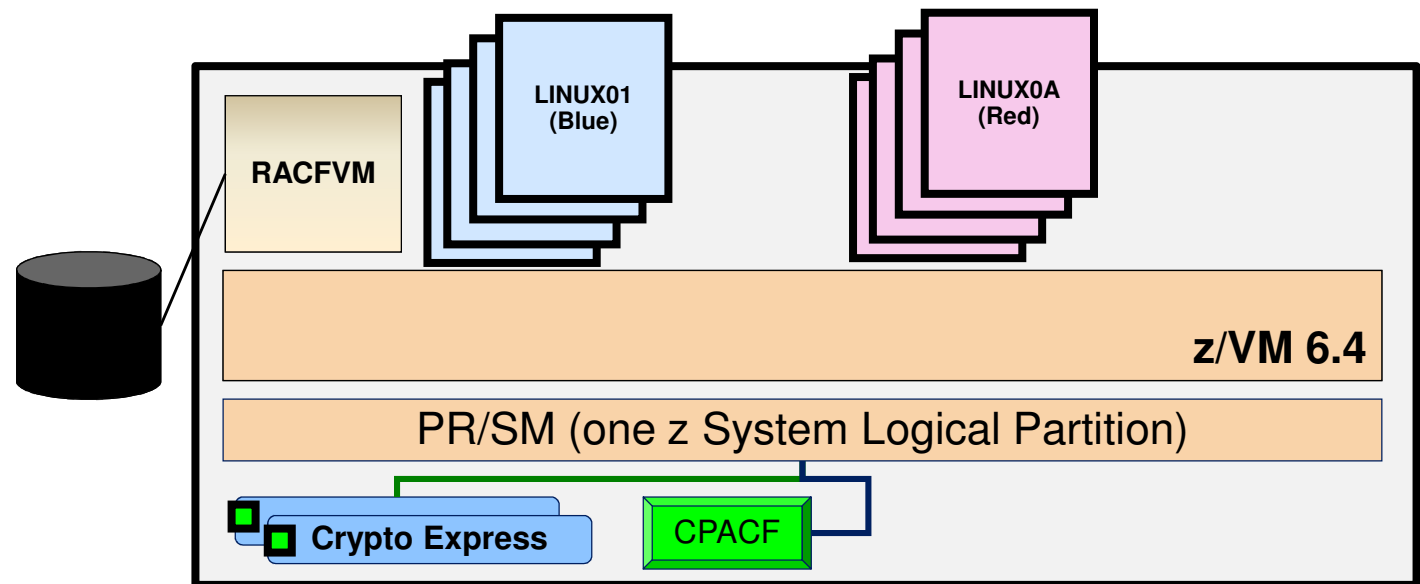
- Future expansion

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
 - Controls on password policies, access rights, and security management
 - 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 RACFVMM – What's New?



- RACF NoAddCreator
- Bundling of the z/VM 6.3 RACFVMM Updates (KDFAES and associated)
- ICHRCX02

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*

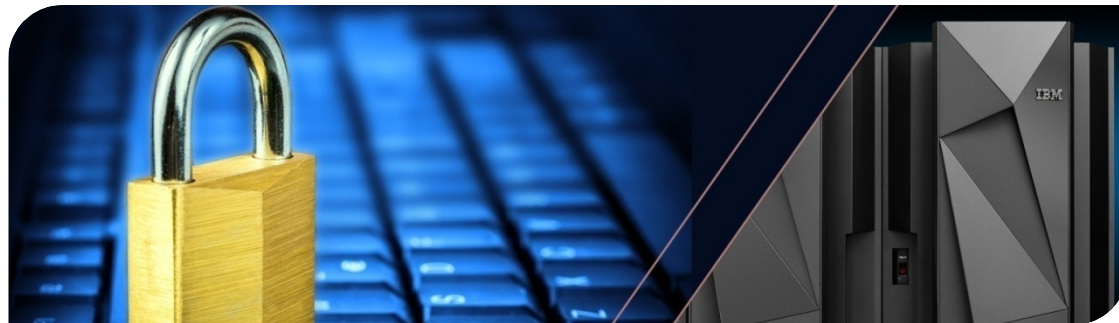
- RACF for z/VM 6.4 ports the NOADDCREATOR option from z/OS
 - **RAC SETROPTS ADDCREATOR | NOADDCREATOR**
 - Default setting for new RACF databases
 - For older databases, template-dependent

- Eliminates need for work-arounds or extra configuration

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
Passticket Generation (VM65759)	Create passtickets in z/VM; returned by x'A0'

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.

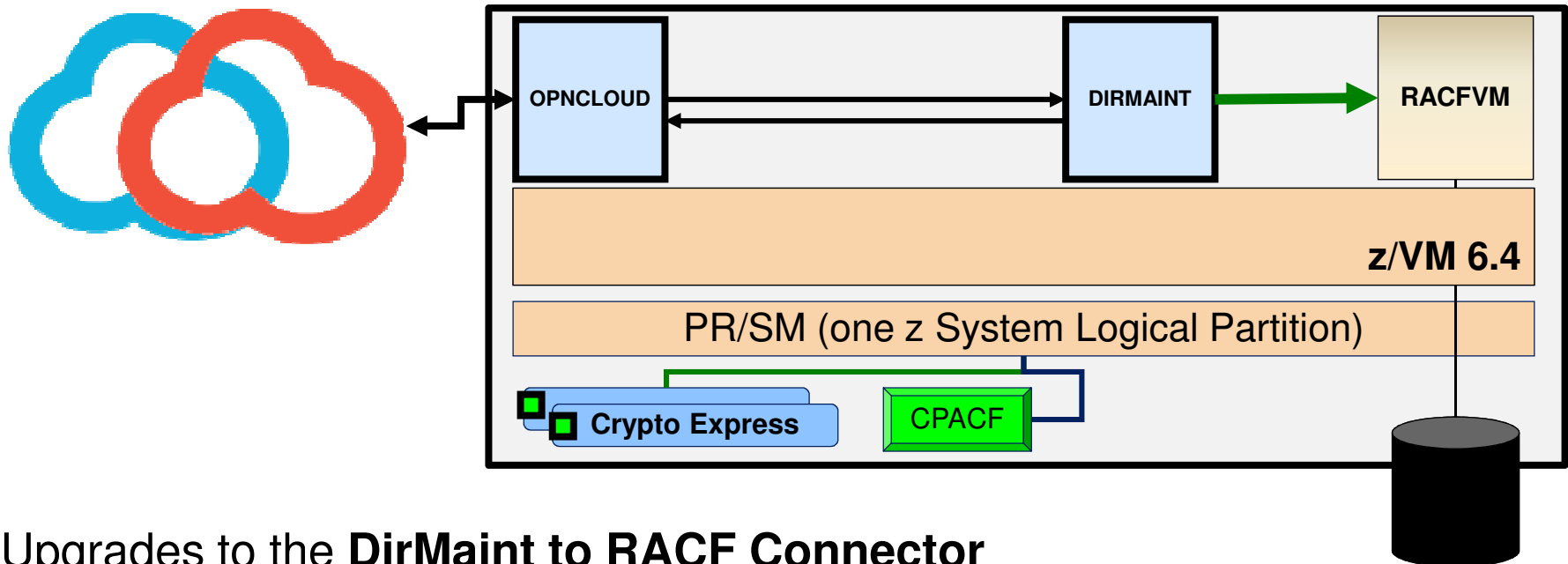
Why does this matter to you?

- 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 (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
 - **User-Based Virtual Switches** to start (limitation of NICDEF statement)

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
```

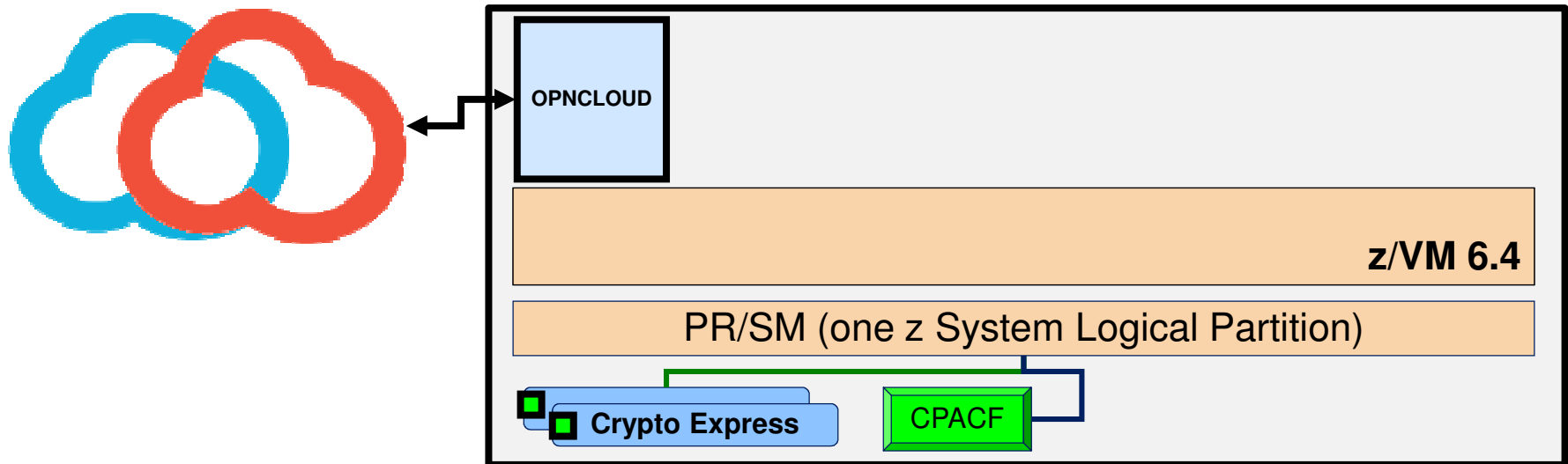
z/VM 6.4 Security in 2017: Security Policy Ease-of-Use Enhancements



z/VM Security in 2017

- OpenStack Newton support << **January, 2017**
- RACF Ease-of-Use Enhancements << **March 15, 2017**
- Crypto Express APVIRT for z/VM TLS/SSL << **March 31, 2017**

z/VM 6.4 Security and the Cloud Management Appliance ('Newton') Available now!



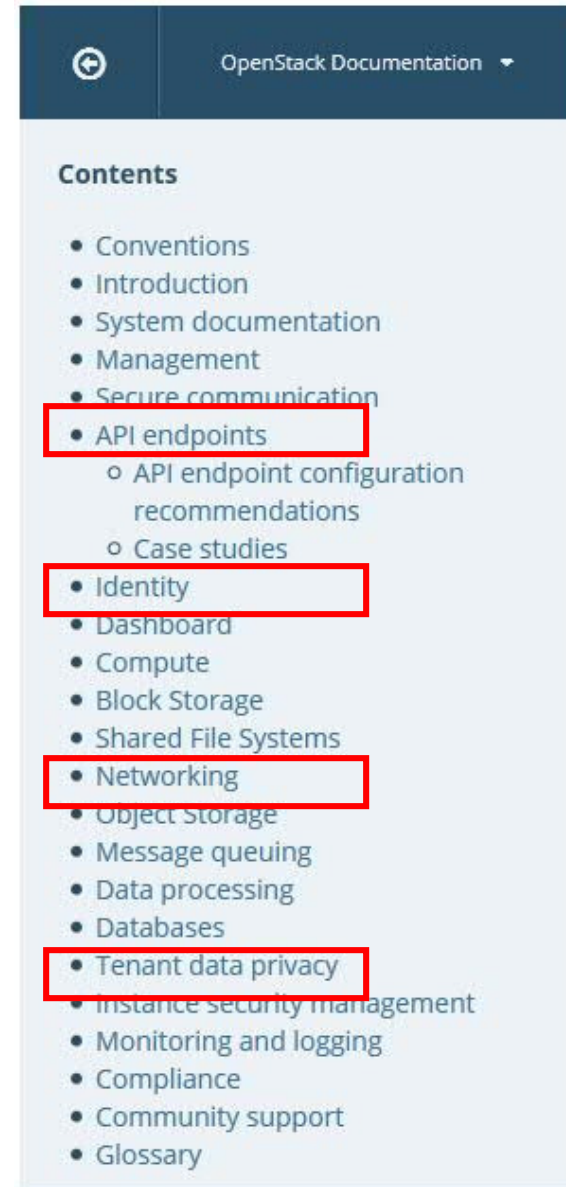
- Hardening of the OPNCLOUD virtual machine
 - NIST compliant crypto
 - API Endpoint Security (HTTPS for OpenStack Services)
 - Security service bundled up
- IUCV replaces SSH for compute-to-guest communication in an LPAR (less key sprawl)
- IBM Secure Engineering Framework guidelines
 - Source code and API scanning of both z/VM and its appliances
 - **New:** integration of **OpenStack Bandit** into testing procedures (Python code scanning)

OpenStack Security

- OpenStack community has its own Security Group
 - Security Advisories, Code Scanning tools
 - OpenStack Security Guide
 - Recommendations
 - Examples
 - Covers common cloud threats

– <http://docs.openstack.org/sec/>

- **Note:** OpenStack community guidance is KVM for x86-centric, so it is not a substitute for z Systems security analysis and planning. (But it is a good reference point.)

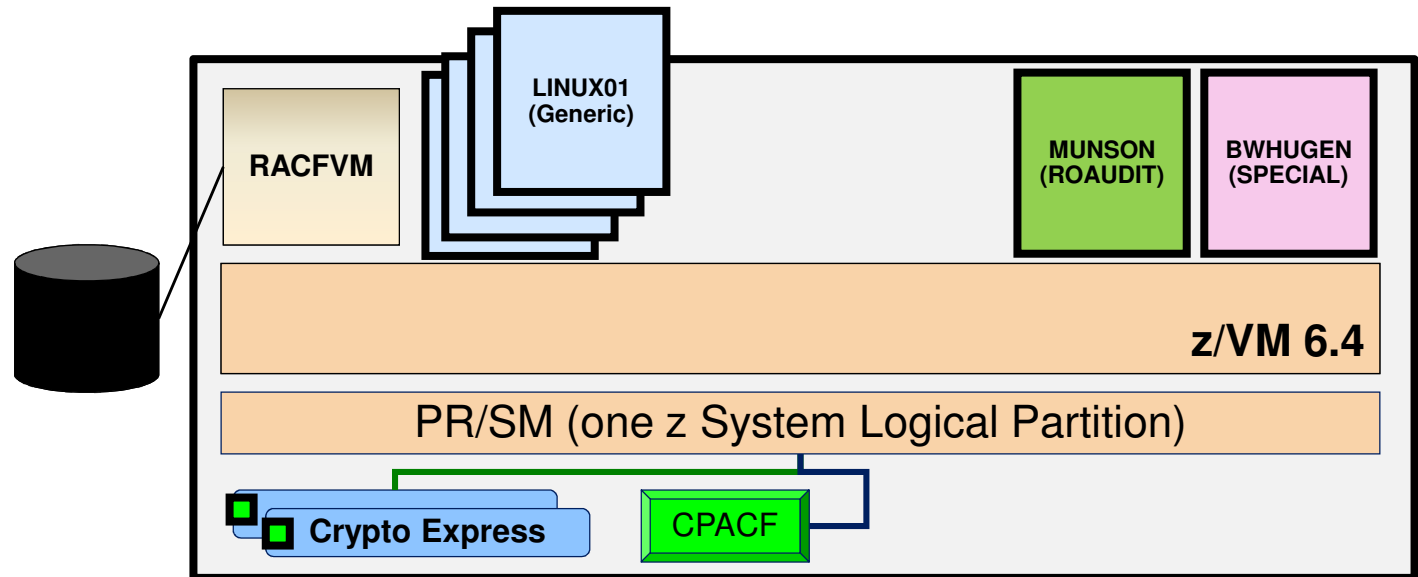


The screenshot shows the 'OpenStack Documentation' page with a 'Contents' section. The following items are highlighted with red boxes:

- API endpoints
 - API endpoint configuration recommendations
 - Case studies
- Identity
- Networking
- Tenant data privacy

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

PTF for APAR VM65930

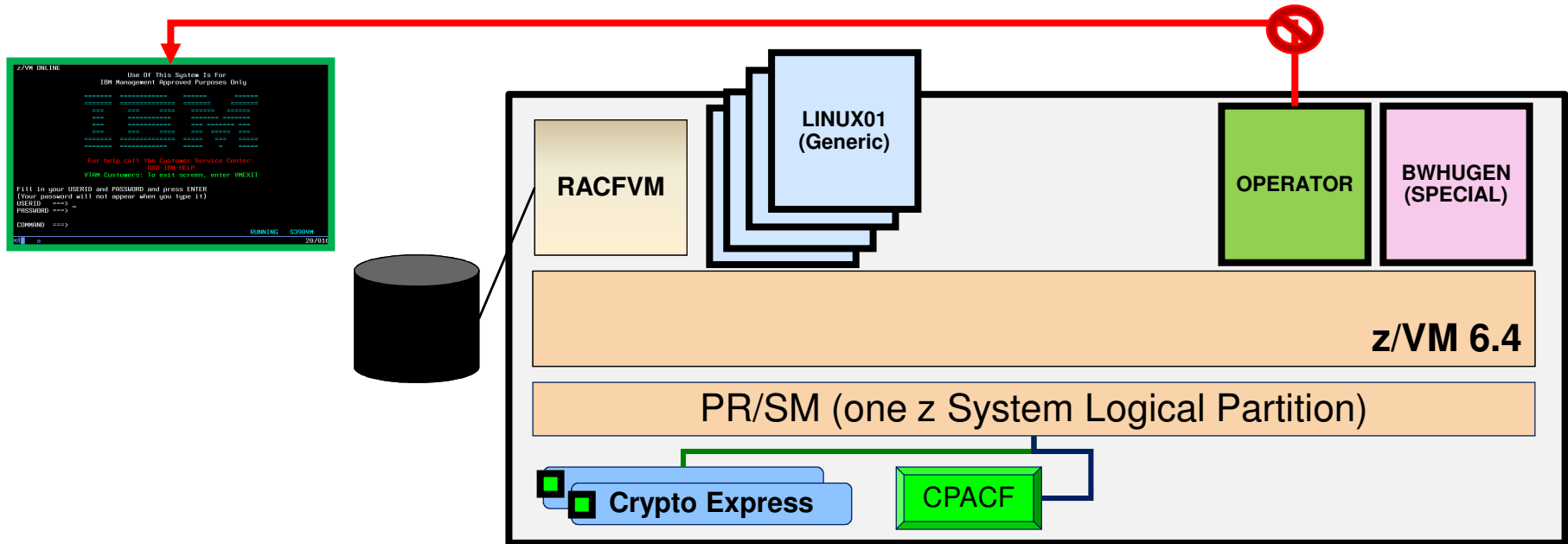


- Read-Only Auditor (**ROAUDIT**)
 - Port z/OS feature of the same name – role associated with a RACF USER.
 - Similar to SPECIAL, OPERATIONS, or AUDITOR
 - Access to SMF logs without the ability to write or tamper
 - Meet compliance goals without privilege escalation. Also nice for external auditors.

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

[more...]

z/VM 6.4 Security and RACFVMM Ease-of-Use PTF for APAR VM65930



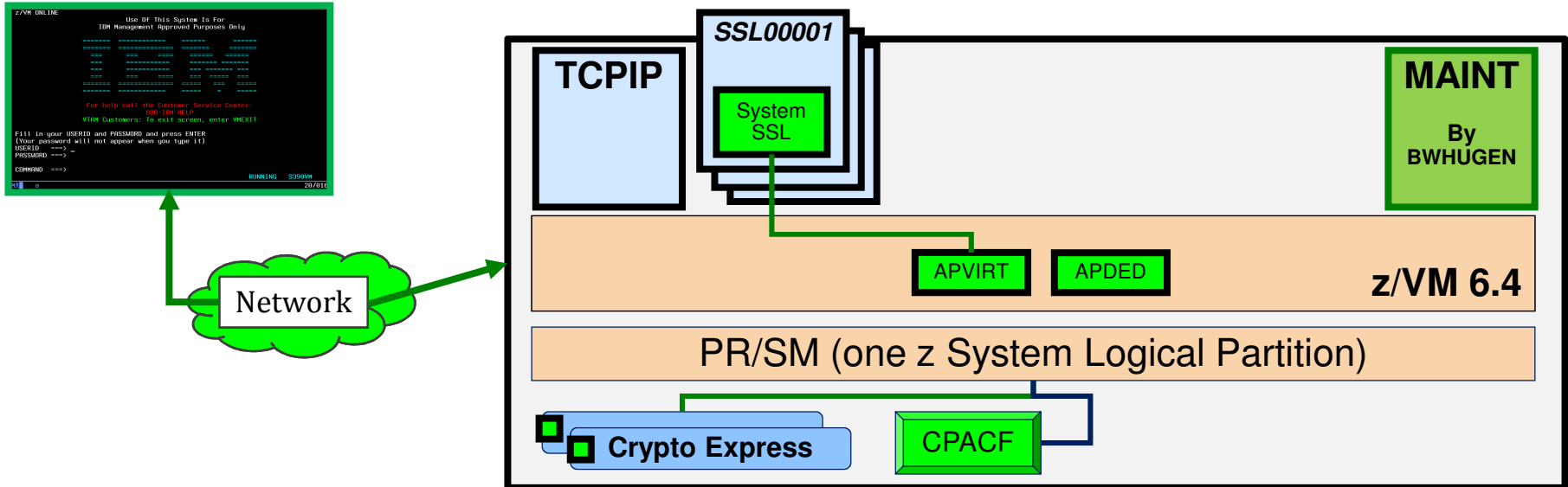
- RACF now **disallows XAUTOLOG..ON by default**, the moment the PTF is installed
 - "XAUTOLOG Over There" autologs any virtual machine to a VDEV
 - A "break glass in case of emergency" operand (Class A/B) with no authentication required
 - Generic RAC profile can restore original behavior:

RAC RDEFINE VMCMD XAUTOLOG.ON. UACC(READ)**

- Specific access can be granted on a per-user / per-system basis
- But we want you to make a security decision for your system – do what's right for your shop

Crypto APVIRT for the z/VM TLS/SSL Server

PTFs for APAR PI72106



- 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)
- Also works for your LDAP/VM Server!

Crypto APVIRT for the z/VM TLS/SSL Server

PTFs for APAR PI72106

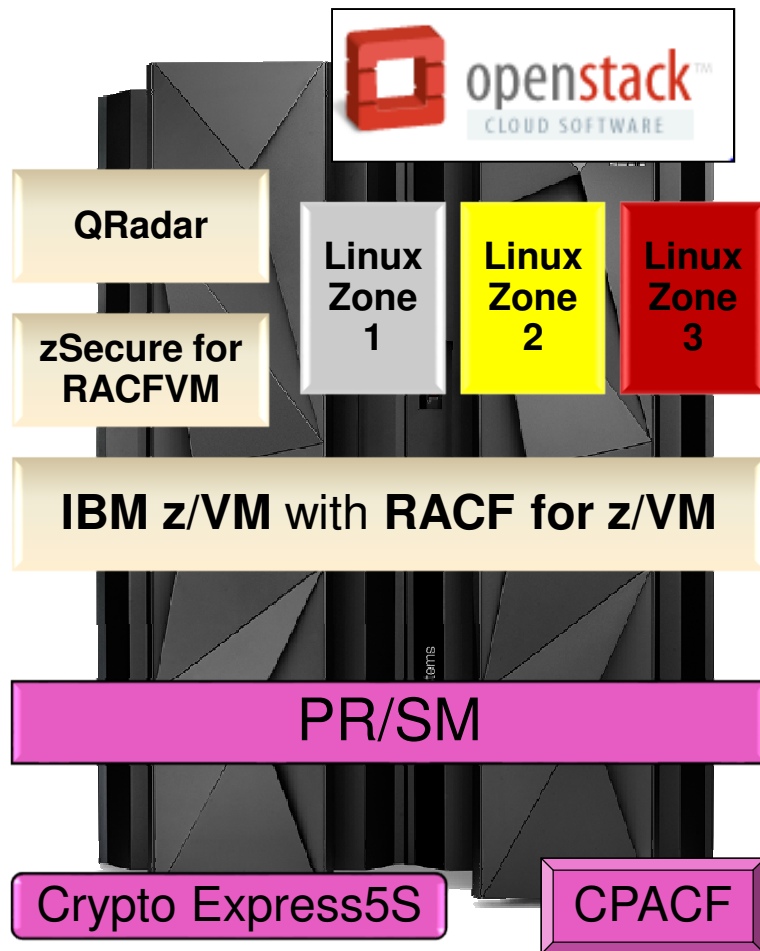
```
PROFILE TCPSSL10
  CRYPTO APVIRTUAL
  IPL CMS PARM FILEPOOL VMSYS
  IUCV ALLOW
  LOGONBY GSKADMIN TCPMNT10 BWHUGEN
  NAMESAVE TCPIP10
  OPTION ACCT MAXCONN 1024 QUICKDSP
  POSIXINFO UID 7 GNAME security
  SHARE RELATIVE 3000
  CONSOLE 0009 3215 T
  [...]
```

- 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 calls
 - **GSKADMIN** - for certificate creation / management
 - A **stand-alone TLS/SSL server** (non-POOL)

Summary



Summary



IaaS on z Systems for Linux
 OpenStack for compatibility and open standards
 Keystone for Identity Management and Integration

Linux Security (SELinux, AppArmor, cgroups)
 OpenSSH for secure guest connectivity
 Centralized Audit with PAM and ITDS

Architecture-layer guest isolation
 TLS 1.2 connectivity & VLAN-aware Virtual Switch
 OSPP EAL 4+ with Labeled Security (Multitenancy)

Architecture-layer isolation of workload
 Ultimate partition isolation (CC EAL 5)
 Hipersockets for secured internal traffic

Hardware acceleration of cryptographic ops
 PKCS #11 and CCA support
 FIPS 140-2 Level 4 HSM (Secure Key)

Advertisement: Submitting Requirements (RFE)

**Do you want more z/VM Security
enhancements?**

Submit one!

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

For More Information (z/VM 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>
- z/VM Security
 - <http://www.vm.ibm.com/security/>
- z Systems Security Portal (IBM ResourceLink) – Register at:
http://www-03.ibm.com/systems/z/solutions/security_subintegrity.html

Contact Information:

[Brian W. Hugenbruch](#), CISSP
IBM z Systems Virtualization Security
[bwhugen at us dot ibm dot com](mailto:bwhugen@us.ibm.com)

 [@Bwhugen](#)

Dank u

Dutch

Merci

French

Спасибо

Russian

Gracias

Spanish

شكراً

Arabic

감사합니다

Korean

Tack så mycket

Swedish

धन्यवाद

Hindi

תודה רבה

Hebrew

Obrigado

Brazilian
Portuguese

谢谢

Chinese

Dankon

Esperanto

Thank You

ありがとうございます

Japanese

Trugarez

Breton

Danke

German

Tak

Danish

Grazie

Italian

நன்றி

Tamil

děkuji

Czech

ขอบคุณ

Thai

go raibh maith agat

Gaelic