Fundamentals of z/VM Security and Cyber Resiliency

Brian Hugenbruch, CISSP
IBM LinuxONE Resiliency Lead &&
IBM z/VM Security and Cryptography Champion
bwhugen@us.ibm.com

Agenda

- Who am I?
- How does one secure z/VM?
- Suggested Practices
- Questions

Who am I?

- “Sir Brian, Wielder of the Security Hammer”
- 24 years as a z/VM Developer
  - CP, TCPIP, TLS, RACF coding
  - CP, Virtual Networking, RACF testing
- 15 years as the z/VM Security Champion
  - Roadmap for z/VM security development (not just for RACF)
  - Five Common Criteria certifications completed
  - Four FIPS 140-2 evaluations completed
  - Sponsor user discussions and research around security, ease of use, …
- 4 years as LinuxONE Resiliency Lead
  - Four lights, eight nines
  - All my work merges together into the fun of Cyber Resiliency

- Most common question I receive?

“How do I secure z/VM?”

- Fantastic question!
- Brian answers this question with another question:
  - “What are you doing with it?”
- Is this system…
  - A production LPAR hosting traditional Linux guests, with three system programmers?
  - A development LPAR with 491 human users, each with their own CMS guest?
  - A test LPAR for measuring Cloud Service scalability?

“How do I secure z/VM?” – “Well, that’s just RACF, isn’t it?”

**(PCI DSS v3.1 Supplement - Virtualization Guidance v2.1)*

1. Vulnerabilities in the Physical Environment Apply in a Virtual Environment
2. Hypervisor Creates a New Attack Surface
3. Increased Complexity of Virtualized Systems and Networks
4. More than One Function per Physical System
5. Mixing VMs of Different Trust Levels
6. Lack of Separation of Duties
7. Dormant Virtual Machines
8. VM Images and Snapshots
9. Immaturity of Monitoring Solutions
10. Information Leakage between Virtual Network Segments
11. Information Leakage between Virtual Components

Recommendations For Virtual Environments

(An example list from the PCI DSS v2 standard)

- 4.1.1 – Evaluate risks associated with virtual technologies
- 4.1.2 – Understand impact of Virtualization to scope of the CDE
- 4.1.3 – Restrict physical access
- **4.1.4 – Implement defense in depth**
- **4.1.5 – Isolate security functions**
- **4.1.6 – Enforce least privilege and separation of duties**
- *4.1.7 – Evaluate hypervisor technologies*
- **4.1.8 – Harden the hypervisor**
- **4.1.9 – Harden virtual machines and other components**
- **4.1.10 – Define appropriate use of management tools**
- **4.1.11 – Recognize the dynamic nature of virtual machines**
- **4.1.12 – Evaluate virtualized network security features**
- 4.1.13 – Clearly define all hosted virtual services
- *4.1.14 – Understand the technology*

So. Where do we start?

(Answer: “The beginning.”)

1. Know your rules

It might sound obvious, but especially in a large enterprise, **the number of rules** to which you must adhere is non-trivial

- *Just because no one's told you about the rules does not mean they're not there.*

In an ideal world, you start with the rules and then build the system

When inheriting architecture, this isn't always possible

Step 1: know your system

Step 2: know the technology

Step 3: know your requirements

8

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

z/VM Security Certifications

z/VM Level	Common Criteria	
z/VM 7.4	*Announced – coming in ~3Q2024*	
z/VM 7.3	*Not evaluated ("designed to conform to standards")*	
z/VM 7.2	***BSI OSPP (with Virt and Labeled Security extensions) at EAL 4+ – Completed!***	***NIAP VPP with Server Virt. Extended Package – Completed!***
z/VM 7.1	*Not evaluated ("designed to conform to standards")*	
z/VM 6.4	OSPP with Labeled Security and Virtualization at EAL 4+ -- ***COMPLETED!*** http://www.ocsi.isticom.it/index.php/elenchi-certificazioni/in-corso-di-valutazione	

z/VM Level	FIPS 140-n
z/VM 7.4	*Announced – coming in 3Q2024*
z/VM 7.3	*Not evaluated ("designed to conform to standards")*
z/VM 7.2	***FIPS 140-2 L1 for z/VM System SSL and ICSFLIB – Completed!***
z/VM 7.1	*Not evaluated ("designed to conform to standards")*
z/VM 6.4	FIPS 140-2 L1 – ***COMPLETED!*** https://csrc.nist.gov/projects/cryptographic-module-validation-program/Certificate/3374

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

Quickly… EAL what?

- EAL5 – better than an air gap when it comes to data confidentiality and compute management
  - Isolation of a logical partition at the architectural level (more on this in a moment)
  - Controls on direct access to devices
  - **Elimination** of covert channels
  - Role-based access controls to a partition (or partitions), or hardware

- With a few added bonuses:
  - Controlled in-memory communication paths (**HiperSockets**)

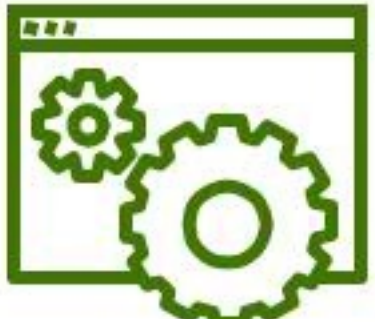
…and how does this compare to z/VM?

- z/VM is meant for “secure and scalable sharing”
  - z/VM, z/OS, and PR/SM all evaluate to different checklists – different rules apply
  - Multitenancy (“Coke and Pepsi”) rather than ultimate isolation

- Common Criteria takes the lowest number of a software stack
  - z/VM running in PR/SM has an EAL 4+ aggregate
  - Your business operations will almost certainly require co
    performance)
  - Again, this isn’t bad! You just need to make **informed decisions** about your workloads

… but certifications aren't "enough."

- z/VM Development does its best to give you the capabilities you need to defend your installation
- z/VM Development does not know every regulation or law to which you need to adhere
- All certifications for information security will <u>require a particular configuration</u>.
  - This includes z/VM Common Criteria evaluations (BSI OSPP at EAL 4+; NIAP VPP)
  - … and z/VM's FIPS 140-n validations (for secure connectivity)
- **Your needs may vary**, based upon your security policy
  - Based on the needs of a government, industry, or company
  - Additional software (e.g. DirMaint) needs to be considered
  - The Common Criteria configuration is **a good starting point**.
  - "Knowing the path" vs. "walking the path."

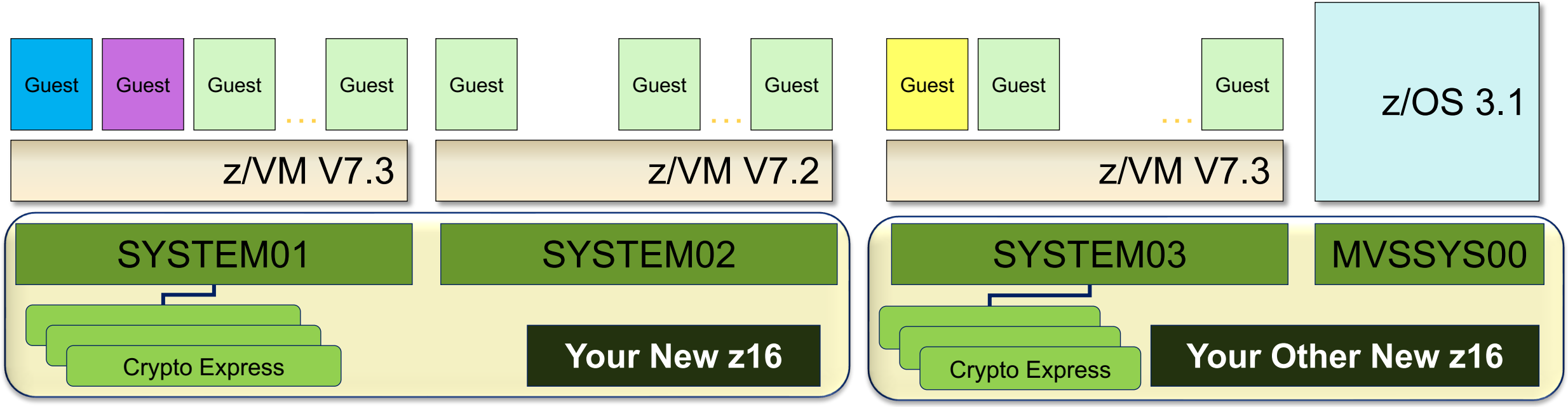


2. Knowing your data

- Rules change depending upon the classification of the data in use in your z/VM partition
  - Prod is more restrictive than test
    - Prod has live client data
    - Test better not have live client data!
    - Prod has different resiliency and up-time requirements than test…
    - Security is no different
  - Dev is a strange, strange place
    - Not necessarily client data, but ‘secret sauce’ work which may have distinct requirements

- Pro Tip: the PCI DSS v3 asks you to draw diagrams of where Cardholder Information (CHI) flows
  - Reminder: that’s not cut-and-dried in a virtualized environment…

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



3. Change your defaults

- Shrink-wrap attacks
- IBM z/VM Development does not change its defaults as fast as this speaker would like
  - *And if you have an old System Configuration file, it may not matter what we change!*
- Go through the System Configuration file, User Directory, and feature defaults to toggle things like:
  - Default privilege classes for basic workload
  - OPERATOR Privclass and ALTERNATE_OPERATOR
  - TDISK Clearing (**enabled by default in z/VM V7.2**)
  - Default passwords in the z/VM user directory (also applies to minidisks)
  - Virtual machine existence
    - Not using SMAPI? NOLOG it
- A useful evaluation both for new installs and existing infrastructure – challenge your own assumptions

15

4. Only humans need passwords

- By default, a lot of virtual machines have their own distinct passwords in the CP User Directory
  - They shouldn't. They're not on the payroll; they can't be fired if there's a breach.
  - And you're certainly not sharing passwords for OPERATOR amongst administrators!
    - Passwords should be socially distanced
    - And not just by putting the Post-It Note six feet away

- IBM is making progress on the default user directory, but that doesn't impact existing systems
  - And there's more work to do here…
  - Which means that you should investigate your own systems
  - Convert anything that isn't already LBYONLY or AUTOONLY
  - Give passwords only to human users
    - And revoke <u>the humans</u> when pertinent

16

5. Least Privilege

- **Class G is defined for CMS General Users created in 1984**
  - There are 60 Class G commands today, not including QUERY and SET
  - Linux requires ~15 of them to IPL

- **Don’t give out an entire privilege class for one command**
  - Class C contains the FOR and SEND commands.
  - But it also contains STORE HOST
  - See also: COMMAND statement in the User Directory

- **IBM z/VM Development does not change its defaults as fast as this speaker would like**

- Any time IBM creates a new CP command, they go into the existing privilege classes
- Having user-defined content allows you to restrict guest access (either for Linux servers or human administrators) in accordance with policy, e.g.
  - L for Linux guests
  - P for Programmers
  - S exclusively for the SHUTDOWN command

17

5. Least Privilege

So what options are available?

1. **Local modification** – SET PRIVCLASS (Class ANY and Class C)
   - Remove class authority from inside a virtual machine.
     - `SET PRIVCLASS * -AC`
   - But be careful; the Class C version can exceed directory-granted privilege!

2. **Global modification** – `MODIFY CMD` and `MODIFY DIAGNOSE` (Class A)
   - Dynamically redefine a command into a different privilege class.
     - `MODIFY COMMAND SHUTDOWN PRIVCLASS S`
     - `MODIFY COM XAUTOLOG IBMCLASS A PRIVCLASS OUX`
     - `MODIFY CMD QUERY SUBCMD NAMES IBMCLASS G PRIVCLASS Z`
     - `MODIFY COMMAND XAUTOLOG RESET`
     - `MODIFY DIAG 94 PRIVCLASS V`
       - No IBMCLASS functionality for MODIFY DIAGNOSE

18

6. Enable TLS for z/VM

- z/VM does not enable TLS by default. (It should, but it doesn't.)
- If your Rules (**see #1**) mandate that administrative access to systems must be encrypted, then TLS must be enabled.
  - The hypervisor is a point of entry
  - Linux has its own TCP/IP stack and encryption, but that doesn't help your CP LOGON screen
- If they don't… it's still a good idea, honestly
  - Data transferred in the clear can be observed (**see #2**)
  - Humans reuse passwords
  - And new technology (**Direct-to-host Service Transfer**) requires it
- TLS for z/VM has been FIPS 140-2 validated (through z/VM V7.2)
  - Cryptographic policy is configurable based on your needs
  - We're working on making certificate management easier (see: CERTMGR, available in 12/2021)
  - FIPS 140-3 validation is coming soon for z/VM V7.4

7. Install and Enable an External Security Manager

- Yes, really.
  - Yes, “if needed.”
  - But back that up with your rules. (**See #1**)

- I’m going to say ‘RACF’ a lot over the next few slides.
  - But, honestly, if you have one of the other ESM’s, I’m cool with it.
  - All I care about is that you’re computing safely.

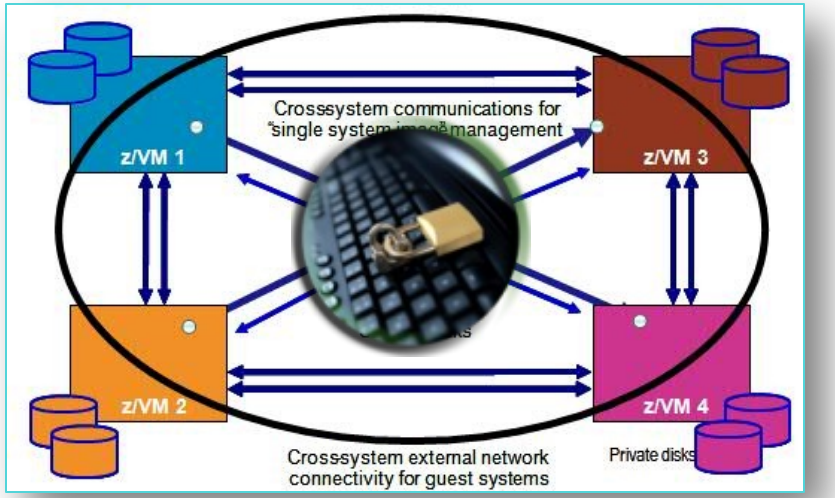
- We reached Slide 20 before the RACF discussion began

- If you have **no ESM**, though, your system cannot meet the industry standards and regulations through which all modern IT is built.
  - Where by “modern” I mean 2003.

20

7. Install and Enable an External Security Manager

- RACF Security Server is a priced feature of z/VM
- 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
  - Extensibility in z/VM environments clustered through Single System Image
  - 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 (OSPP-LS at EAL 4+)*

21

7. Install and Enable an External Security Manager

- **"It's the same as z/OS, right?"**

- **Common code base rehosted into a z/VM CMS environment**
  - Port features and fixes from z/OS on an as-needed basis
  - Runs as a Service Virtual Machine, rather than as a system-level process
  - RACFVM should be autologged before any other service (so security is "always on")

- **Missing some larger-ticket items**
  - RACDCERT
  - RRSF
  - Tooling is better on z/OS than on z/VM, honestly

- **Slightly different set of security concerns**
  - Do enable VMCMD, VMDEV, VMLAN classes (commands, real devices, network)
  - A lot of the others may not be pertinent to a z/VM system

22

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 had issued a corresponding Statement of Direction for z/OS 3.1*

7. Install and Enable an External Security Manager

- **"But we only have one administrator!"**
  - Did the Rules (**see #1**) have an "Except for Joel, we know he's cool" clause?
  - If Mark's been bribed in dollars or dogecoins, what tracks the damage he might do to the system?

- **"Do you have RACF installed?" "…yes?"**

- **"We already have a control policy" (Three Stooges story)**
  - Consider auditing
  - Consider collusion
  - Consider your choices again (and **see #1**)

- **"It's too complicated!"**
  - There are ways IBM can help with that (see: Lab-Based Services)
  - There are ways programs can help with that (see: zSecure for RACFVM or similar)
  - There are ways **you can help us** with that (see: VM Council)
    - *We can't fix the problems we're not seeing*

24

zSecure for RACF/VM

If you have zSecure for RACF/VM 2.5.1 (GA on 17 June 2022!), you now have **SIEM integration**, an **SMF cache server**, **support for MFA**, and support for RACF databases residing (non-shared) **on SCSI volumes**. (Along with a host of other improvements!)

https://www.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/5/877/ENUSZP22-0045/index.html&request_locale=en

8. Deploy Multifactor Authentication

- **If needed.**
  - Again, **see #1**
  - This is where a closer understanding of the Rules will help.

- That said, passwords are understood to be a technology that can be compromised
  - Humans don't generate strong ones willingly
  - Humans will rotate them or reuse them

- Use of a second authentication factor ("something you have" or "something you are") can strengthen your system against compromise of a single password

- On z/VM, this requires the IBM Z Multi-factor Authentication product…. as well as an ESM.
  - ***Honestly, we figured if you didn't have an ESM, you didn't care about security***
  - ***So, no, we're not enabling MFA for an ESM-less system.***

26

IBM Z Multi-factor Authentication

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

- IBM Z Multi-factor Authentication V2.x – a new priced product
  - Order through ShopZ
  - Yes, it'll say z/OS – don't panic. The Linux .iso will be available for download
  - The most recent version, V2.3, introduces a lot of stability enhancements for the MFA Server

- 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		

27

9. Encrypt Sensitive Data

- **See #2**: know your data
- Encrypt it when it moves from place to place (**see: #4, #10**)
- Encrypt it when it's resident in memory, where you can
  - **dm-crypt** in Linux
  - **Dataset encryption** in z/OS
  - **RACF database for passwords and passphrases**
  - **Encrypted Paging** (when running on a z14 or later)
- Encrypt it when it's out on your storage volumes (**DS8880** and similar storage units)

28

10. Treat your virtual networks with care

- **You should be using the z/VM Virtual Switch for Layer 2 routing between guests on a single z/VM partition**
  - With guests using TLS to encrypt data leaving the virtual machine
  - With separation of traffic enforced as pertinent, from basic separation through VEPA
  - With ESM control of guest access to Virtual LANs
  - With a security decision being made (read: firewall) when data crosses network segments
    - Firewalls on a physical switch are fine
    - No need to waste the MIPS by putting this on z/VM itself

- Have you double-checked your defaults? Can your guests add themselves to networks, or create transient Guest LANs?
  - **See #3**
- How are your IUCV settings? How prevalent is IUCV ANY? **See #3**
- Are there controls around Hipersockets access?
- *Are there geographic regulations on relocation of guests onto another CPC?*

- Do you still have that diagram for where your data is flowing?

29

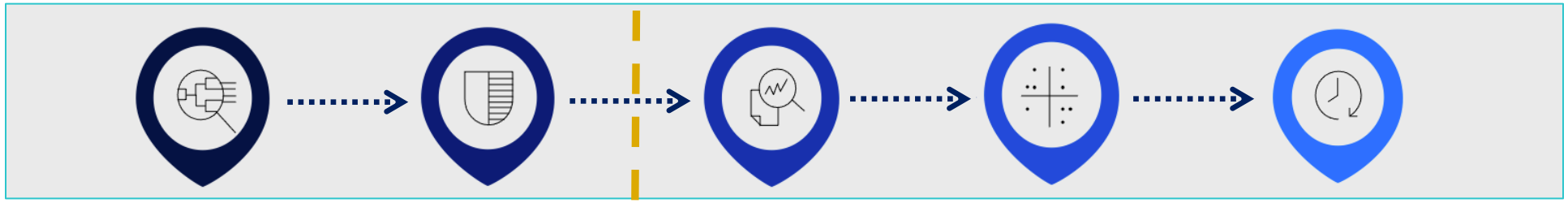
10. Treat your virtual networks with care

- Your inter-VM traffic can be as “separate” as your rules require (**see #1**)
- Basic Vswitch connectivity, no virtual lans
- Vswitch access with multiple lans
- Vswitch access with Port Isolation, to force traffic to consider the OSA ports
- Vswitch access with VEPA mode, to force traffic out to a physical switch before a “security decision” is made (read: there’s a firewall)
- Use Directory Network Authorization (DNA) if you’re not already
  - Simplify management
- Your VLANs, if you need them, should be backed by your ESM
  - If not for the controls, then for the auditing

30

11. Do you have a recovery plan?

- Security is defined as a combination of data confidentiality, system integrity, and service availability
- If your system ceases to be available (via hardware error, programmer error, intern pulled the wrong plug, meteor…)
  - How long will it take to recover your system?
- Are you making data backups (of sensitive data or otherwise)? Are those backups protected?

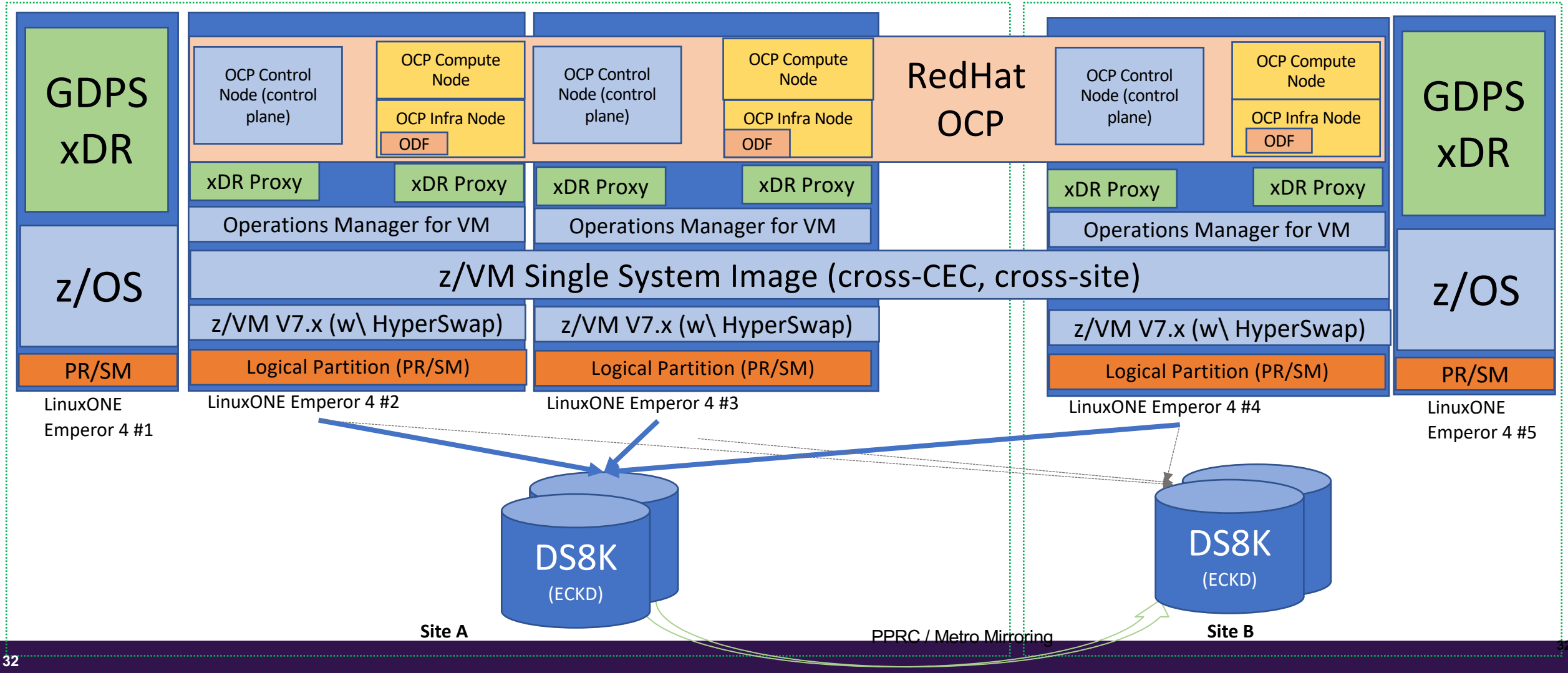


IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
Risks and vulnerabilities	Your critical applications and data	Data corruption and configuration anomalies	To changes in configuration and data	Access to critical applications and data

31

IBM LinuxONE Framework for 99.999999% availability

(Redbook draft now available: https://www.redbooks.ibm.com/redpieces/abstracts/sg248544.html)



12. Gather Proof

- If a security event isn't audited, did it ever really happen?

- Is your system configured for compliance to [insert standard here]?
  - Was it yesterday?
  - Will it be tomorrow?

- When a z/VM security person says "audit," they mean RACF
  - SMF records for security-relevant events and RACF-specific tracking
  - SIEM streaming support with zSecure
  - No, the VM "Journaling" option doesn't count
  - Performance monitoring (e.g. 'DATAPUMP') may be a useful supplement

33

z/VM Compliance Utility (COMPEXTR)

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

- Delivery of PTF for APAR VM66646 for z/VM V7.3, which introduces the Compliance utility (COMPEXTR) for z/VM **available now**
- Two formats for content display (YAML or flattened)
  - Print to console, spool to file, or pass via new API
  - 210 key-value pairs enumerated, covering almost everything we could think of to track
  - Need more? We take requests

- Does not itself calculate z/VM compliance posture – just give you the data (and the capacity to diff a baseline)
- We’re working with the zSCC team to enable their product to determine what makes z/VM compliant…

34

z/VM Systems Security and Compliance Utility

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

PCI DSS Requirement		z/VM Specific Data Required
3	Protect stored card holder data	Clear_TDISK, Passwords_on_Cmds, Set_Privclass, Disc_Operator Enabled/Disabled? Encrypted Paging TLS enabled (TLS 1.2) REQUIRED settings for Secure Telnet, FTPS, SMTP, RSCS VLAN configuration for Vswitch Is an ESM enabled Yes/No
7	Need To Know restrictions	How many machines are > Class G? || Are they LBYONLY? Are there machines in the user directory with privileged options? || Are they LBYONLY? Who's on the TCPIP OBEY List / SSL_Admin_List? RACF SPECIAL / OPERATIONS / AUDITOR / ROAUDIT users?
10	Track and monitor all access to network resources and cardholder data	Is anyone using anonymous FTP? Is the ESM controlling FTP? ESM control of VLAN settings (RACF VMLAN class)? Can a Class G guest create a transient Guest LAN? Are any guests in the PROFILE TCPIP running without TLS/SSL? (PORT/AUTOLOG statements)
2	Do not use vendor supplied defaults for system password and other security parameters	Scan z/VM User Directory for presence of default user password value …And default minidisk password values RACF SYSSEC settings around DEFER RACF Audit SEVER=YES
8	Identify and authenticate access to system components	RACF: password/phrase intervals (min/max) RACF: password/phrase expiry RACF password history settings RACF password encryption – KDFAES? RACF: are the password exits enabled? Is MFA enabled? Is anyone enabled for PWFALLBACK? Are any users in the z/VM user directory not configured for LBYONLY / AUTOONLY?
6	Develop and maintain secure systems and applications (the "is it up on its service" question)	QUERY CPSERVICE QUERY CPLEVEL QUERY CMSLEVEL NETSTAT TCP/IP level output CP Environment variable output (if applicable)

35

13. Now, set a timer.

- This may be Rule-dependent (#1)
- But however long it's for, when it pops… revisit these decisions
- The security landscape is changing continuously, and changing quickly
- Yesterday's "secure enough" is tomorrow's "broken"
  - That might move more slowly on IBM Z or IBM LinuxONE….
  - But it's still true

36

Suggested Practices

Suggested Practice – Identity Management

- **Humans** need to prove who they say they are when authenticating to an information system. Only humans should be prompted for passwords (or other authentication tokens).
- Managing access—general authentication, levels of authorization—is vital to ensuring that your system is not modified improperly.
- Being able to prove it? Even more important.
- **Brian recommends**: a z/VM External Security Manager; IBM Z MFA; LDAP if pertinent across the enterprise; use of LOGONBY and SURROGAT for access to privileged virtual machines; a robust auditing policy

38

Suggested Practice – Authorization and Least-Privilege

- **Any virtual machine** (and by extension, the humans logging into them) should only have enough privilege to do their jobs—no more, no less

- z/VM comes “pre-packaged” with seven default privilege classes.
  More can be defined.

- An External Security Manager allows for granular access to all system resources and security-relevant commands

- **Brian recommends**: user-defined privilege classes for (a) Linux workloads / applications, and (b) administrators; ESM-defined privileges for access to specific resources—especially in cases where human jobs (e.g. network admin, storage admin) require separation of authorization between admins

39

Suggested Practice—Encrypt Sensitive Data

- Confidentiality is ensuring that only authorized personnel can see the data you want them to see
- Encryption is key to enforcing that separation
- Your regulations (internal/external/geo/industry/gov) may have specific requirements, both for data-in-flight and data-at-rest
- **Brian recommends**: z/VM TLS Server (data in flight), z/VM Encrypted Paging, Dynamic Vary Crypto for hardware-to-guest support, ***openssl*** and ***dm-crypt***, DS8880 (for encryption of storage), Encrypted Tape…

40

Suggested Practice – Trust But Verify

- **Use GETSHOPZ for service**
  - Validates digital signatures on IBM packages during download process
  - Avoids multiple hops in moving fixes from source to target
  - Web interface that functions even without external connectivity

- **Validate your guests**
  - List-directed IPL (“Secure Boot / Validated Boot”) for Linux or z/OS guests

- **Diff your compliance data (COMPEXTR)**
  - Assure no changes have been made and escaped notice
  - Also worth hashing files like the User Directory and System Configuration

41

Suggested Practice – Have a Backup Plan

- **Take backups of your data**
  - And test restore procedures – no, seriously. Get a stopwatch.
  - Technologies like SCP and GDPS LCP can help protect your backups
  - Cyber Vault (a “lifestyle choice,” rather than a product) to help with DFIR and recovery

- **Have redundant storage**
  - And test your HyperSwap configuration

- **Have (and test!) a DR plan**
  - What happens if you have to live at your DR site for a while?

42

Suggested Practice—Audit, Audit, Audit

- If you can't prove it happened, did it happen?
- If you can't prove who did it, who's responsible?
- Auditing may seem like busy-work (sort of like commenting code); but it can be what allows for problem determination and incident response to happen in a smooth and meaningful fashion
- **Brian recommends**: monitor records, ESM audit logs, and analysis of same; streaming to SIEM in accordance with your local policies; and doing delta comparisons of Compliance Utility output to determine if unauthorized changes have been made

43

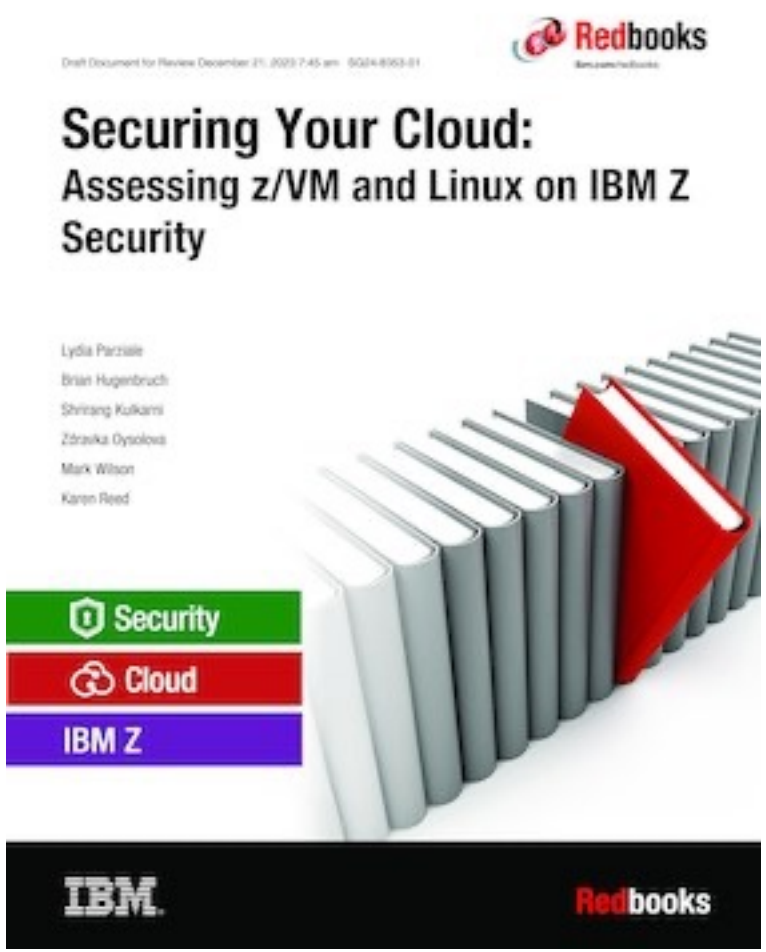
Questions? Comments?
(Time for a nap?)

Summary

- z/VM has a lot of features to offer to help the security-conscious programmer
- “We can only show you the door. You’re the one who must walk through it.”
- Measure twice, cut once
  - Know your rules
  - Know the technology, and know where the data is going
  - Know how to “prove it” and meet audit requirements
  - Know how to recover in an emergency
  - Know when it’s time to change security posture

45

For More Information…



- If you'd like a hands-on guide to following these guidelines, we can help!
- Updated December 2023
  - https://www.redbooks.ibm.com/redpieces/abstracts/sg248353.html

46

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:

Brian W. Hugenbruch
IBM LinuxONE Resiliency Lead &&
IBM z/VM Security and Cryptography Lead
https://www.linkedin.com/in/bwhugen/
bwhugen@us.ibm.com **@the-lettersea**

47