

Leveraging the Newest Capability in z/VM 7.1

v7.1.g

For the most current version of this presentation, please see
<http://www.vm.ibm.com/library/presentations/>

John Franciscovich
z/VM Design and Development
francisj@us.ibm.com

February 2020



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

Db2*	FlashCopy*	IBM (logo)*	OMEGAMON*	z13*	z/Architecture*	zSeries*
DirMaint	FlashSystem	IBM Z*	PR/SM	z13s	zEnterprise*	z/VM*
DS8000*	GDPS*	LinuxONE*	RACF*	z14	z/OS*	z Systems*
ECKD	ibm.com	LinuxONE Emperor	System z10*	z15	zSecure	
FICON*	IBM eServer	LinuxONE Rockhopper	XIV*	z10 BC		
				z10EC		

* Registered trademarks of IBM Corporation

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. IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.

ITIL is a Registered Trade Mark of AXELOS Limited.

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 other countries.

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.

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.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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.

UNIX is a registered trademark of The Open Group in the United States and other countries.

VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.

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.

Abstract

With z/VM's continuous delivery strategy, most new function is now being delivered as New Function APARs. The "z/VM Platform Update" covered the business value of the newest enhancements to z/VM; in this session we'll cover technical information that you need to take advantage of the newest enhancements that are available in z/VM 7.1.

Agenda

- z/VM 7.1 Notes
- Continuous delivery enhancements – recent New Function APARs
- Keeping up with releases, service, and new function updates

z/VM 7.1

z/VM 7.1

<http://www.vm.ibm.com/zvm710/index.html>

- GA September 21, 2018

- Single System Image and Live Guest Relocation included in the base
 - In z/VM 6.4 it was the VMSSI priced feature

- Architecture Level Set of zEC12, zBC12, or newer processor families

- Includes SPEs shipped for z/VM 6.4
 - Virtual Switch Enhanced Load Balancing, EAV Minidisks, Encrypted Paging, etc.

- Additionally, includes:
 - Dump scalability improvements
 - Foundation work for future New Function APARs

Initial Dump Scalability Improvements in z/VM 6.4

- Larger systems mean larger dumps
- Performance enhancement for hard abend and snap dumps to 3390 DASD
 - More intelligent channel programs
 - Decreases **dump time** significantly
 - 30 to 40% improvement in lab testing
- Create **smaller** snap dumps by not dumping guest PGMBKs (page tables)
 - Optionally can select to include them
- Available May 31, 2017

Component	APAR	PTF	RSU
CP	VM65989	UM35132	1702

z/VM 7.1 Dump Scalability Improvements

- Reduce size of both snap dumps and hard abend dumps
- Reduce time to create and process dumps
- No longer dump the Frame Table and Page Tables by default
 - Unless it is an abend code where they are helpful for problem determination
 - Dump size reduction varies
 - Lab testing showed often 20% of the size of former dumps
- New options to override defaults on what data is dumped
 - **SET DUMP** and **SNAPDUMP** commands
- We still calculate the maximum size needed when reserving space in spool for dumps
- No longer support dumping to tape devices

z/VM 7.1 Additional Dump Scalability Improvements

- Reduce CPU required for snap dump and hard abend dump processing
 - Further improves performance of dump processing from a processor requirement perspective.

- Available September 21, 2018

Component	APAR	PTF	RSU
CP	VM66176	UM35352	1901

Single System Image (SSI) *Function*

- SSI (including Live Guest Relocation) is included in the base of z/VM 7.1

- A **PRODUCT** statement for the VMSSI feature is no longer necessary in the z/VM 7.1 system config file
 - If specified, it will be displayed by the **QUERY PRODUCT** command
 - If your software audit people use **QUERY PRODUCT** to determine the software that you purchased, be ready to explain to them that it is free or remove from the system config file.

- If an **SSI** statement is included in the system config file, the following will be displayed during IPL:

```
*****  
* IBM z/VM Single System Image Function is active.  
*****
```

z/VM 7.1 Memory Management Changes

- Some changes were introduced in z/VM 7.1 for upcoming New Function APARs

- Minimum memory size for a second level z/VM is now 128MB (previously 32MB)
 - First level z/VM minimum is unchanged (256MB)

- **SET STORAGE** command changes
 - New **PERMANENT** keyword
 - Remove **AS** keyword
 - No more rounding up to the increment boundary

z/VM 7.1 User Directory Modifications

- Changes to IBM supplied directory to make more consistent with recommended security policies
 - IBM-provided virtual machines changed to be either:
 - Autolog Only (AUTOONLY)
 - Logon By (LBYONLY)

- Changes to other IBM-provided virtual machines
 - Deleted those that are no longer used
 - New virtual machines
 - Some as infrastructure/placeholders for upcoming new function
 - Release-specific userids renamed
 - e.g. MAINT640 -> MAINT710
 - Specifications changed for some

- See *z/VM Enhancements Guide*
 - Chapter 2, section [V7.1] *User Directory Modifications*

z/VM 7.1 Security Modes

- z/VM 6.4
 - January 8, 2018 APAR VM65396 (PTF UM34851) introduced the **CP SET SPECEX** command
 - March 23, 2018 APAR VM65414 (PTF UM34853) introduced the **CP SET CPPROTECT** command
 - **CP SET SPECEX** still recognized but recommended adopting syntax used with **CP SET CPPROTECT**
- z/VM 7.1 Base
 - **CP SET SPECEX** is no longer supported or recognized
 - **CP SET CPPROTECT** is supported with same defaults and syntax as previously supported
- If you're using **SET SPECEX**, please convert to **SET CPPROTECT** prior to going to z/VM 7.1

Other z/VM 7.1 Changes

- No longer install to 3390-3 Volumes
 - z/VM does support 3390-3, just not for install
 - Install can be done on
 - 3390 with minimum size of 10016 cylinders
 - SCSI volumes with minimum size of 6 GB

- Kanji is no longer supported as a system default language

- OSA/SF is no longer shipped with z/VM

- No longer support dedicating logical processors to individual virtual machines.

z/VM 7.1 New Function APARs

New Function APAR:
Fast Minidisk Erase

Fast Minidisk Erase - Overview

- Efficiently erase data on ECKD minidisks
- New operands on CPFMTXA
 - ERASE**

```
cpfmtxa 1234 erase
```

```
ERASE WILL DESTROY THE CONTENTS OF DISK 1234 ON MDISK JAF1      1234  
DO YOU WANT TO CONTINUE? (YES | NO)  
yes
```

```
Erasing 1234 with      2000 cylinders at 11:40:32  
Erased      1360 cylinders at: 11:40:33  
Erased      2000 cylinders at: 11:40:34
```

–**NOMSG**

- Suppress ICKDSF cylinder progress messages
 - Starting and ending cylinder message will be displayed

Fast Minidisk Erase – DirMaint

- **CPFMTXA ERASE** is used by DirMaint when
 - Deleting a minidisk (**DIRM DMDISK**)
 - When *DISK_CLEANUP = YES (default)*
 - Removing a directory entry (**DIRM PURGE**)
 - When *PURGE_COMMAND_PROCESSING = FULL (default)*
- The **CLEAN/NOCLEAN** operands can be used on the above commands to override the defaults

How to get Fast Minidisk Erase

- Available December 5, 2019
–z/VM 7.1

Component	APAR	PTF	RSU
CP (CPFMTXA)	VM66288	UM35563	2001
DirMaint	VM65784	UM99356	2001
ICKDSF	PH14249	IU64239	

New Function APAR:
Dynamic Crypto

Dynamic Crypto Support - Overview

- **Enables** changes to the z/VM crypto environment **without requiring an IPL of z/VM or its guests**

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

- **Additionally, there are RAS benefits for shared-use crypto resources**
 - Better detection of Crypto Express hardware errors with "silent" retrying of shared pool requests to alternative resources
 - Ability to recover failed Crypto Express adapters
 - Improved internal diagnostics for IBM service
 - Improved logoff and live guest relocation latency for shared crypto users.

Dynamic Crypto – New Commands

- **VARY ONLINE/OFFLINE CRYPTO**
 - Bring a Crypto Express adapter online and make it available
 - Take a Crypto Express adapter offline and make it unavailable

- **ATTACH CRYPTO**
 - Connect crypto resource(s) to
 - A guest for dedicated use (APDED)
 - The system for shared use (APVIRT)

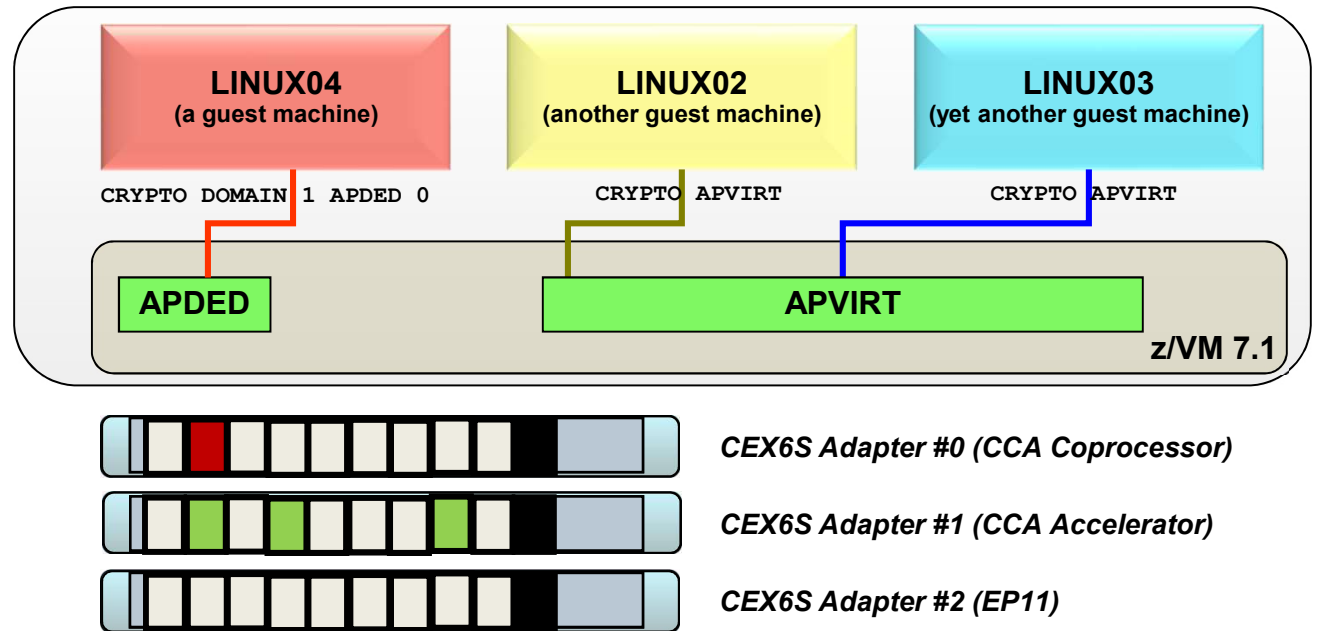
- **DETACH CRYPTO**
 - Remove
 - Dedicated crypto resource(s) from a guest
 - Crypto resources from the shared crypto pool
 - Guest access to the shared crypto pool

- **DEFINE CRYPTO APVIRTUAL**
 - Assign (or re-assign) a shared crypto resource to a guest
 - Guest must be enabled for access in their directory entry

- **QUERY CRYPTO and QUERY VIRTUAL CRYPTO**
 - Enhanced to report online/offline status of crypto resources

How To: Make a new adapter available to z/VM

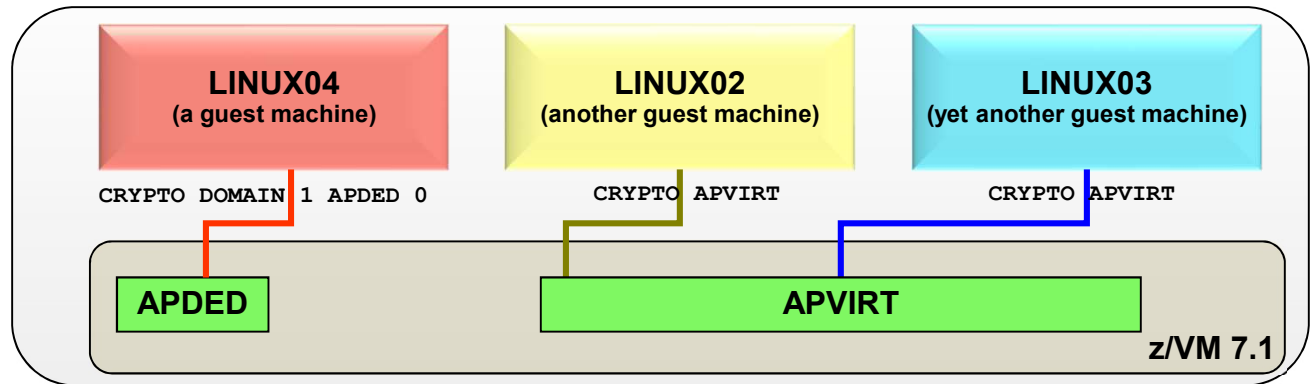
VARY CRYPTO ON 2



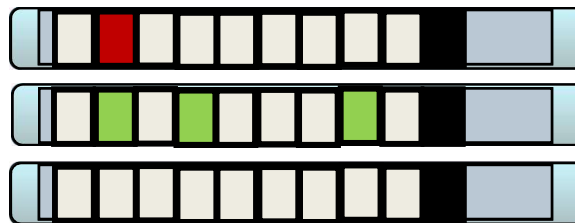
How To: Assign a crypto resource to a user

ATTACH CRYPTO AP 2 DOMAIN 1 to LINUX04

Warning: does not change your z/VM User Directory... so static configuration does not update automatically.



Don't forget to update your defaults!



CEX6S Adapter #0 (CCA Coprocessor)

CEX6S Adapter #1 (CCA Accelerator)

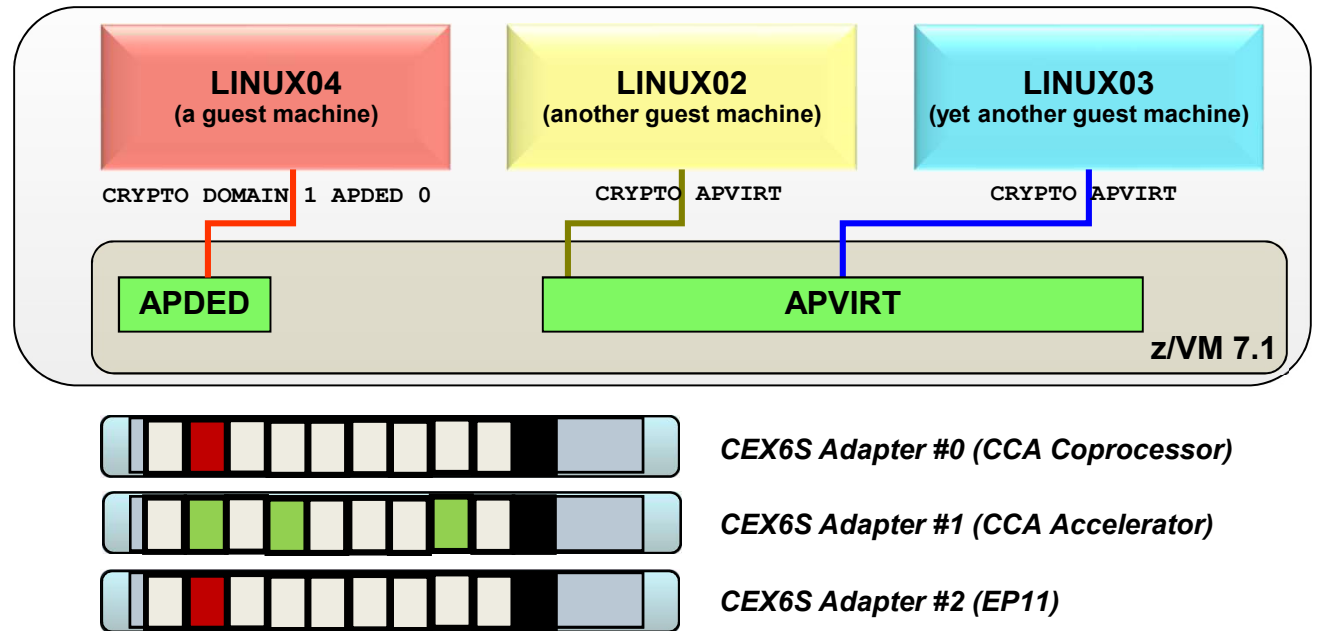
CEX6S Adapter #2 (EP11)

How To: Remove crypto resources from the shared pool

DETACH CRYPTO AP 1 DOMAINS 1 3 7 from SYSTEM (FORCE

Change does not remove APVIRT access from the guests.

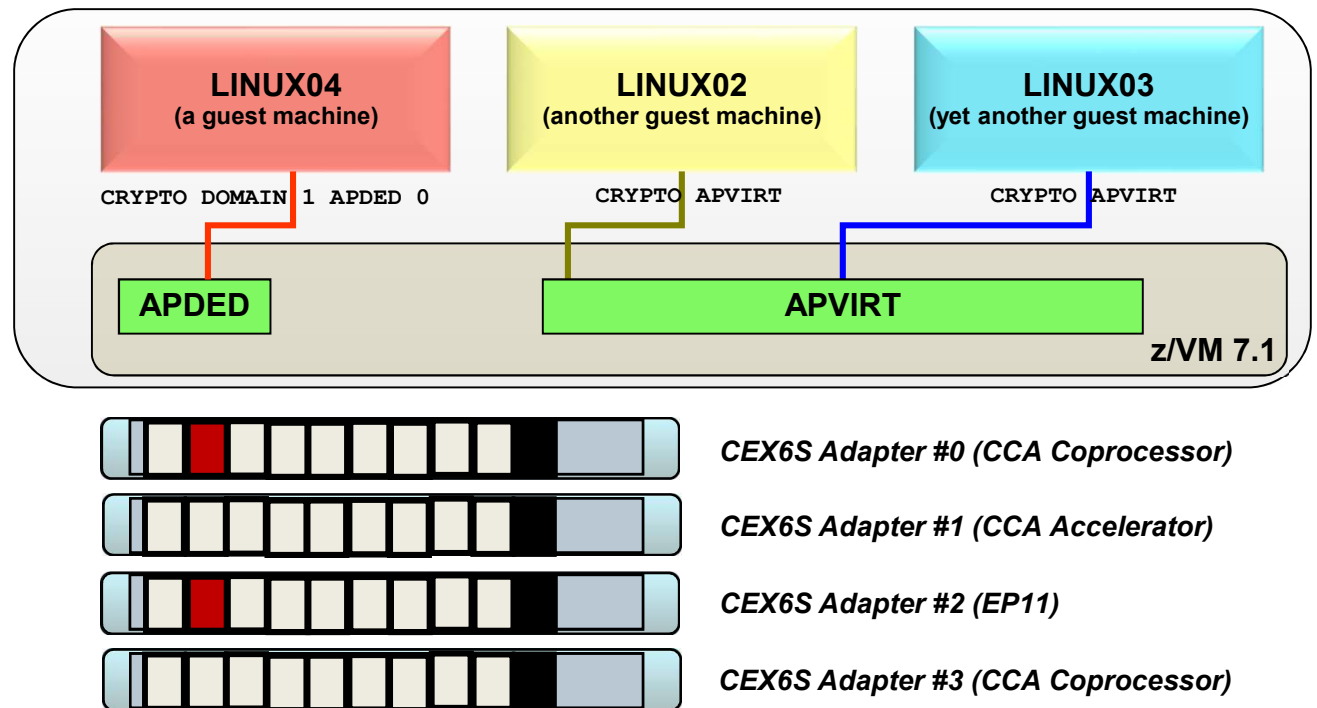
Note: this is an extreme example, you may not want to remove these all at once.



How To: Assign new crypto resources for sharing

VARY CRYPTO ON 3

ATTACH CRYPTO AP 0 3 DOMAIN 6 7 to SYSTEM



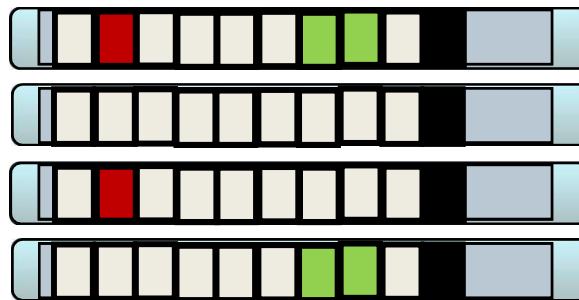
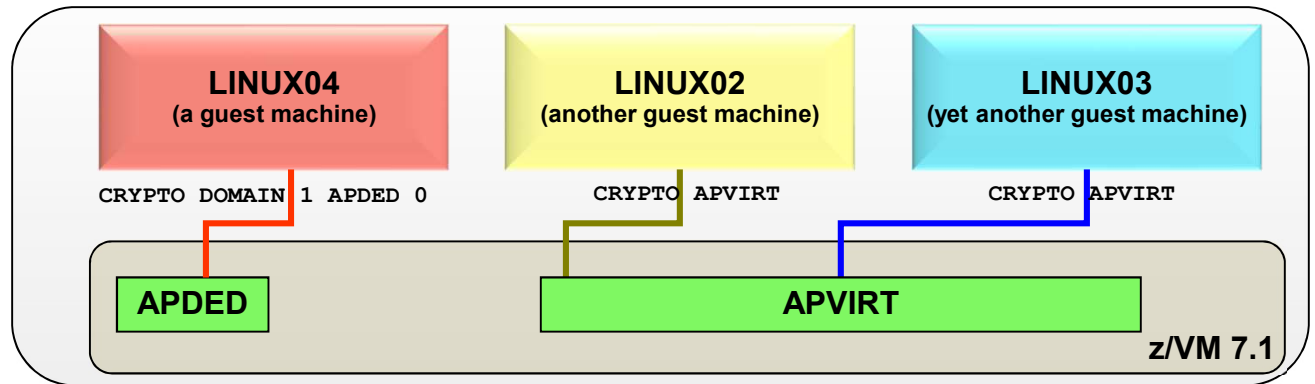
How To: Take an adapter offline

VARY CRYPTO OFF 1

Adapter will be listed as offline and will not available for use

VARY ON the adapter to bring it back to active configuration...

...no IPL required.



- CEX6S Adapter #0 (CCA Coprocessor)
- CEX6S Adapter #1 (CCA Accelerator)
- CEX6S Adapter #2 (EP11)
- CEX6S Adapter #3 (CCA Coprocessor)

How to get Dynamic Crypto Support

- Available September 2019
–z/VM 7.1

	APAR	PTF	RSU
CP	VM66266 (pre-req VM66206)	UM35531 (pre-req UM35449)	TBD

- Pre-req VM66206 is also available on z/VM 6.4 (PTF UM35448)
 - In an SSI cluster, must be applied to all members (z/VM 6.4 *and* 7.1) before applying Dynamic Crypto PTF to any member

New Function APAR:
80 Logical Processor Support

80 Logical Processor Support

- Increases the number of logical processors that z/VM supports to from 64 to 80

- Processor requirements
 - z14 and newer processor families for greater than 64 logical processors
 - z13 and newer processor families for greater than 32 logical processors
 - Is your Disaster Recovery system the same?

- Maximum of 40 cores with both SMT-1 and SMT-2
 - (80 logical processors = 80 threads = 40 cores * 2 threads)

- Share settings are a percentage of the system, so increasing the number of processors, typically increases the share entitlement

- Performance Toolkit enhanced to display processor ids in hex
 - OMEGAMON XE for z/VM and Linux 4.3.0 support in Fixpack 5
 - If you install either the Perfkit or OMEGAMON update, you must also install the other

How to Get 80 Logical Processor Support

- Available August 6, 2019 for z/VM 7.1

Component	APAR	PTF	RSU
CP	VM66265 (pre-req VM66301) ¹	UM35474 (pre-req UM35496) ¹	2001
Stand Alone Dump	VM66296	UM35499	TBD
Perfkit	VM66292	UM35501	2001

- If you apply OMEGAMON XE Fixpack 5 on z/VM 6.4
 - Perfkit APAR VM65863 (UM35472) must also be applied
 - Toleration only, does not support increased number of logical processors

¹VM66301 was found in error, PE fix is VM66319 (PTF UM35530) affects those using: EDEVs for paging or spool, EDEVs for guest MAPMDISK, or PAGING63 IPL parameter

More Information

- z/VM Performance Report article
– <http://www.vm.ibm.com/perf/reports/zvm/html/2q9r2.html>
- z/VM Spotlight: <http://www.vm.ibm.com/news/spotlight/80pro.html>



IBM z/VM Spotlight

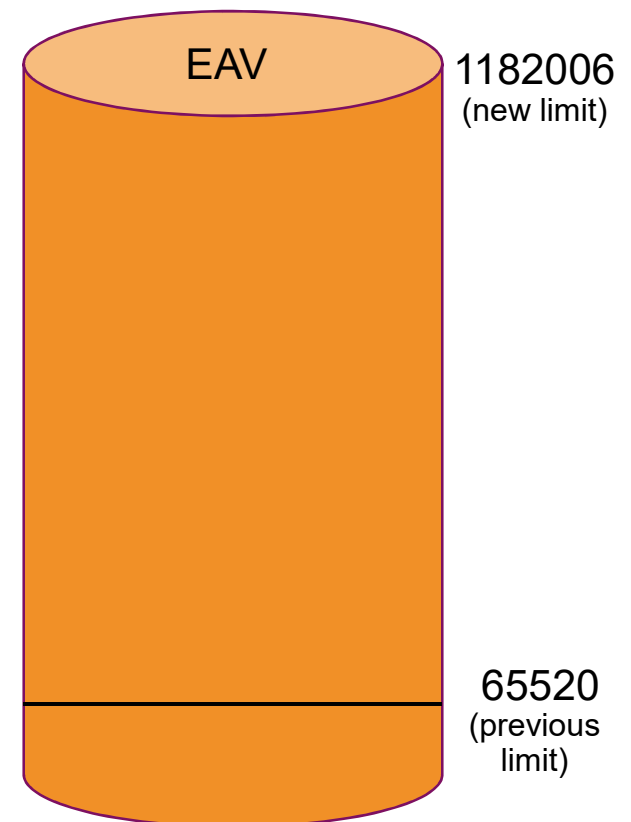
80 Logical Processor Support

We in z/VM know the demand for processing resources continues to increase; and we know that many of our clients benefit from the economies of scale provided by z/VM. With that in mind, we have advanced the scaling capability again, increasing the limit of 64 logical processors to 80 logical processors. When combined with Single System Image (SSI) clusters, this can provide a 320 logical processor environment with the four SSI-members. Clients looking for increased processing capability should look at this latest enhancement.

New Function APAR:
EAV Paging

EAV Paging: Overview

- Allows use of ECKD paging volumes larger than 65520 cylinders (~45 GB)
 - Up to 1,182,006 cylinders
- Benefits:
 - Can use fewer volumes to meet the page space requirements
 - Increases the total page space possible when using ECKD paging space
 - Will be helpful when increasing the amount of virtual memory used in conjunction with future increases in real memory supported
- **CPFMTXA** is enhanced to allow paging space to be allocated on cylinders 65520 and above
 - For an EAV the range is 0-1,182,005



EAV Paging

- Maximum ECKD paging volume sizes

	Number of Cylinders	Usable Space (approx.)
Before EAV paging	65520	45 GB
With EAV paging	1,182,006	812 GB

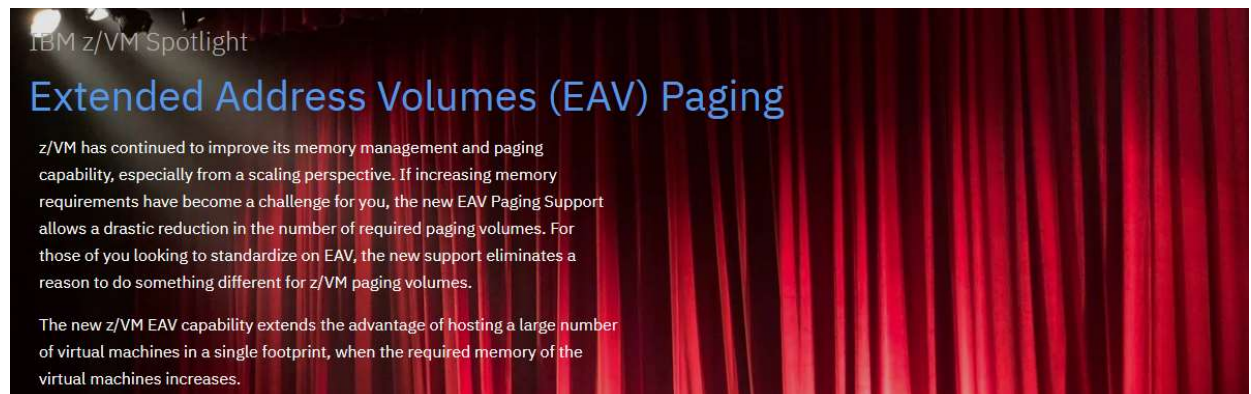
- Example: 2 TB real memory with 3:1 overcommit
 - Before EAV paging, requires 100 paging volumes
 - With EAV paging, requires 7 paging volumes
- Consider enabling HyperPAV and High Performance FICON (HPF) to increase paging I/O rates if you are paging to EAVs.

How to Get EAV Paging Support

- Available June 20, 2019 for z/VM 7.1

Component	APAR	PTF	RSU
CP	VM66263	UM35475	1902
CMS	VM66297	UM35483	1902
Perfkit	VM66293	UM35484	1902

- z/VM Spotlight: <http://www.vm.ibm.com/news/spotlight/eavp.html>



IBM z/VM Spotlight

Extended Address Volumes (EAV) Paging

z/VM has continued to improve its memory management and paging capability, especially from a scaling perspective. If increasing memory requirements have become a challenge for you, the new EAV Paging Support allows a drastic reduction in the number of required paging volumes. For those of you looking to standardize on EAV, the new support eliminates a reason to do something different for z/VM paging volumes.

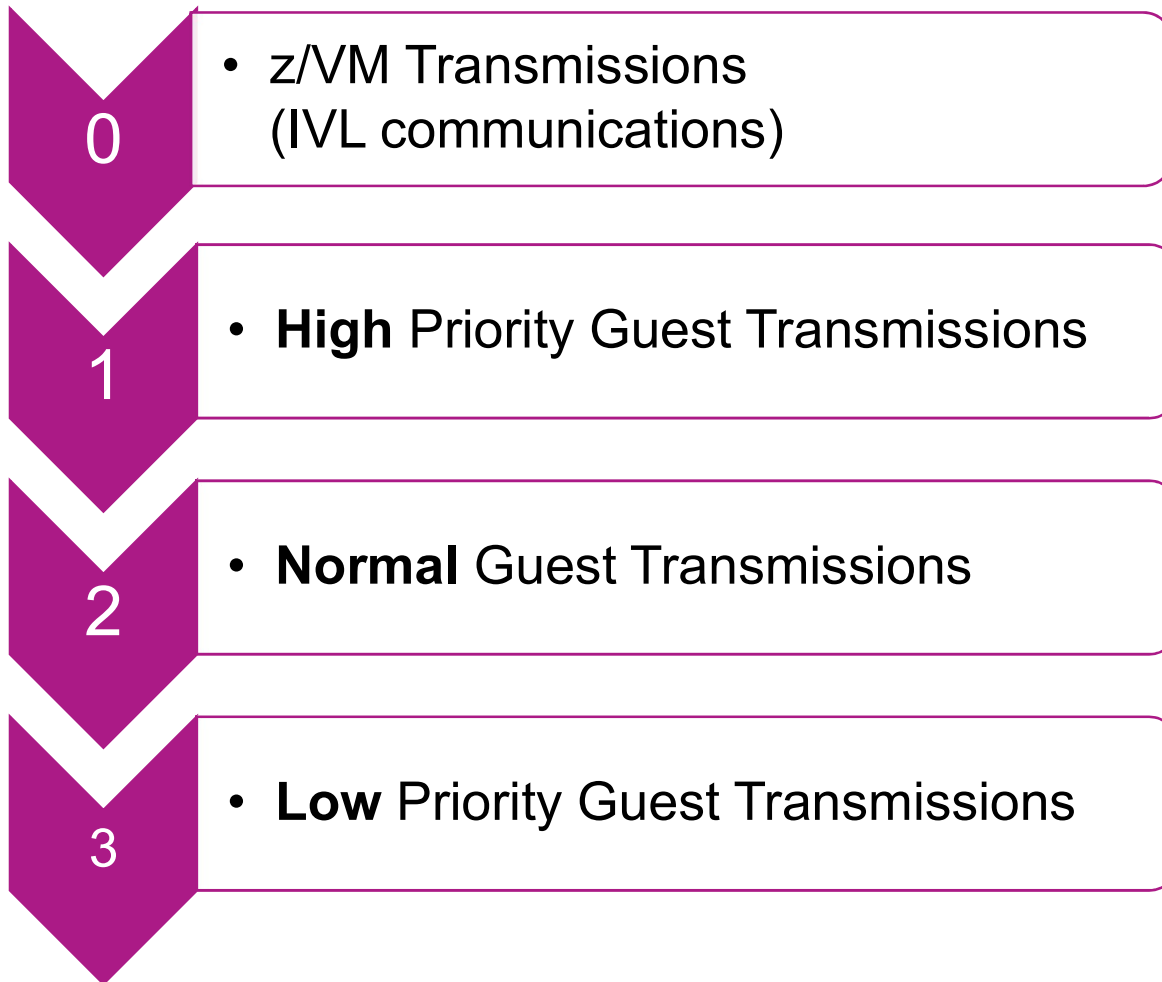
The new z/VM EAV capability extends the advantage of hosting a large number of virtual machines in a single footprint, when the required memory of the virtual machines increases.

New Function APAR: Virtual Switch Priority Queuing

Virtual Switch Priority Queuing

- Allows multiple priority levels for transmissions on a Virtual Switch
- Allows VSwitch management communication (IVL) to operate at highest priority to ensure better management
- Three optional user priority levels allow:
 - Different SLAs for different groups of guests
 - Combining different priority workloads onto fewer, or a single, VSwitch
 - Eliminating need for separate heartbeat network in some clustering solutions

Virtual Switch Priority Assignments



Enabling VSwitch Priority Queuing

- Priority Queuing is enabled in OSA-Express hardware by default
 - IOCP or dynamic I/O change is required to disable

- IVL VSwitches always exploit priority queuing if not disabled

- Exploitation must be enabled for non-IVL VSwitches
 - DEFINE VSWITCH** command/config statement

- Set guest priority (default is NORMAL)
 - NICDEF** directory statement
 - Can be changed dynamically with **MODIFY VSWITCH** command

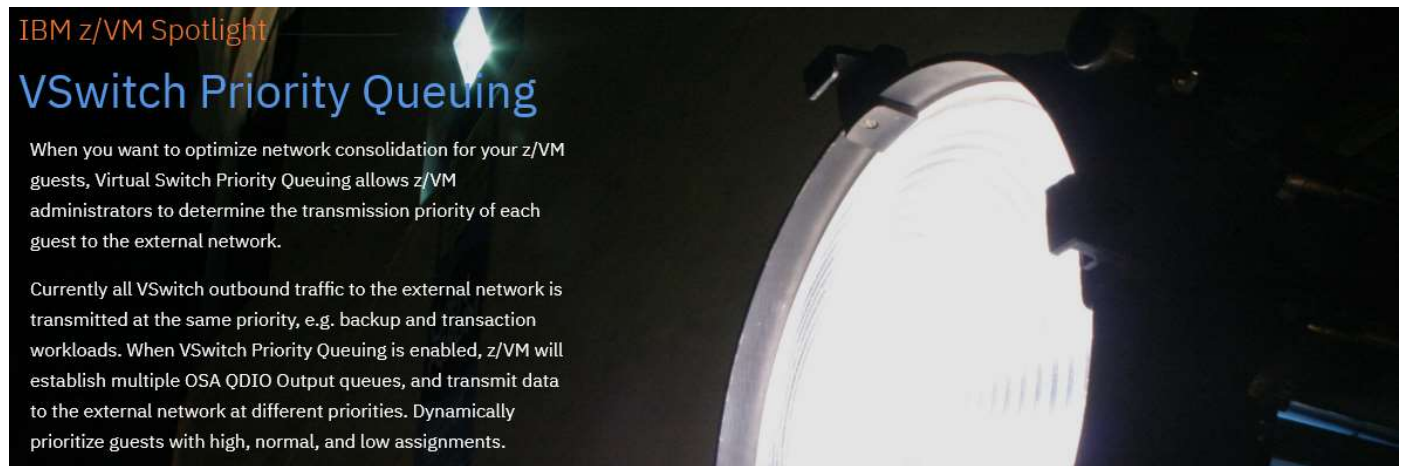
- If you want to relocate a guest that is using priority other than NORMAL, then the VSwitch on the target system must also be enabled for priority queuing
 - Or set guest priority to NORMAL before relocating guest

How to get VSwitch Priority Queuing

- Available May 22, 2019 for z/VM 7.1

Component	APAR	PTF	RSU
CP	VM66219	UM35465	1902
TCP/IP	PH04703	UI62768	1902
DirMaint	VM66223	UV99352	1902

- z/VM Spotlight: <http://www.vm.ibm.com/news/spotlight/vspq.html>



IBM z/VM Spotlight

VSwitch Priority Queuing

When you want to optimize network consolidation for your z/VM guests, Virtual Switch Priority Queuing allows z/VM administrators to determine the transmission priority of each guest to the external network.

Currently all VSwitch outbound traffic to the external network is transmitted at the same priority, e.g. backup and transaction workloads. When VSwitch Priority Queuing is enabled, z/VM will establish multiple OSA QDIO Output queues, and transmit data to the external network at different priorities. Dynamically prioritize guests with high, normal, and low assignments.

New Function APAR:
DEFINE HYPERPAVALIAS and PAVALIAS Enhancements

DEFINE HYPERPAVALIAS/PAVALIAS Enhancements

- A range of virtual alias devices may now be defined with a single command
 - DEFINE HYPERPAVALIAS**
 - DEFINE PAVALIAS**
- Especially useful if the **COMMAND** directory statement is used to define aliases
 - Fewer statements are now needed to define the same number of aliases
 - Helps avoid limits on **COMMAND** statements for each guest
- Available February 8, 2019 for z/VM 7.1

Component	APAR	PTF	RSU
CP	VM66249	UM35427	TBD

New Function APAR:
Elliptic Curve Cryptography

Elliptic Curve Cryptography Support

- z/VM TLS/SSL Server enhanced with enablement of Elliptic Curve Cryptography (ECC) cipher suites

- ECC ciphers provide a more secure mechanism for asymmetric encryption than standard RSA or DSS algorithms.
 - Smaller key sizes for same levels of encryption

- Specific cipher suites can be enabled or disabled by name
 - :parms** tag in DTCPARMS

- Output from the following commands shows information about the new cipher suites and TLS version:
 - SSLADMIN QUERY SESSIONS**
 - SSLADMIN QUERY STATUS DETAILS**
 - NETSTAT IDENTIFY SSL**

Elliptic Curve Cryptography Support

- New Cipher Suites have been added to Table 39 in *z/VM TCP/IP Planning and Customization*
 - Includes strength and symmetric key length
- z/VM Performance Report
<http://www.vm.ibm.com/perf/reports/zvm/html/4q8qk.html>
- Available December 6, 2018 for TCP/IP 7.1

Component	APAR	PTF	RSU
TCP/IP	PI99184	UI60128	1901

New Function APAR:
New RSCS Query Command

New RSCS QUERY Command

- New command option that shows the service level for each of the RSCS parts
 - Highest level PTF that is applied to each part
- **QUERY SYSTEM SERVICE**
 - "BASE" is displayed if no APARs are applied
 - User updates may be displayed in place of the above

```
14:11:11 * MSG FROM RSCS : RSCS Service Level
14:11:11 * MSG FROM RSCS : ---- - - - - - - - - - -
. . .
14:11:11 * MSG FROM RSCS : SLVL DMTCMX BASE
14:11:11 * MSG FROM RSCS : SLVL DMTCMY BASE
14:11:11 * MSG FROM RSCS : SLVL DMTCMZ VM66174
14:11:11 * MSG FROM RSCS : SLVL DMTCMA BASE
14:11:11 * MSG FROM RSCS : SLVL DMTCMB BASE
14:11:11 * MSG FROM RSCS : SLVL DMTCMQ INTEST1
14:11:11 * MSG FROM RSCS : SLVL DMTCQX BASE
14:11:11 * MSG FROM RSCS : SLVL DMTCQY BASE
. . .
```


QUERY SYSTEM SERVICE Command

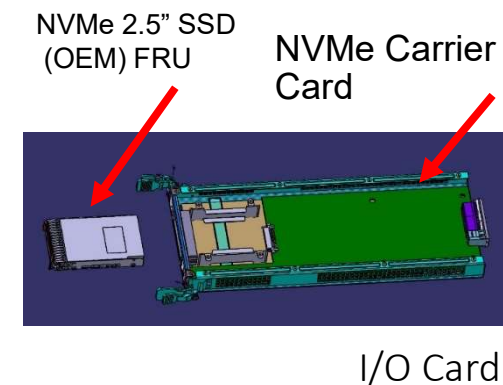
- Available November 29, 2018 for RSCS 7.1

Component	APAR	PTF	RSU
RSCS	VM66174	UV99342	1901

***New Function APAR:
IBM Adapter for NVMe***

IBM Adapter for NVMe

- Support for NVMe (non-volatile memory express) drives
- Available on LinuxONE Emperor II and Rockhopper II with driver D36
 - Client must procure the SSD device
- SSD device directly connected through an IBM PCIe adapter
 - Ability to have embedded storage for some applications
- High I/O throughput can help with various workloads
 - Memory intensive
 - Real-time analytics
 - Fast storage workloads
 - Relational databases



Using the IBM Adapter for NVMe on z/VM

- Requires system configuration file changes and a system IPL
 - Enable PCI support
 - **FEATURES ENABLE PCI**
 - Configure memory for PCIe functions
 - **STORAGE IOAT**
 - See *z/VM CP Planning and Administration*, Chapter 16: "Using PCIe Functions for z/VM Guests"

- Guest enablement
 - Create PCI function dynamically and attach to guest
 - **DEFINE PCIFUNCTION / ATTACH** commands

 - Ensure setting on **SET IO_OPT UID** allows for guest to define options
 - **QUERY IO_OPT**

IBM Adapter for NVMe – z/VM Support

- Available October 31, 2018 for z/VM 6.4 and 7.1

Component	APAR	PTF	RSU
CP	VM66180	UM35381 (6.4) UM35382 (7.1)	1901 1901

***New Function APAR Coming Soon:
TLS/SSL Certificate Verification***

TLS/SSL Certificate Verification - Overview

▪ **Client Certificate Authentication**

- Allows a server to verify a client by ensuring that the client certificate
 - has been signed by a certificate authority that the server trusts
 - has not expired

▪ **Host Name Validation**

- Allows a client to verify the identity of a server using either
 - Host Name
 - Domain Name
 - Host IP Address

▪ **New APIs** to allow fields to be extracted from a client or server certificate

Client Certificate Authentication

- Allows a server to verify a client by ensuring that the client certificate
 - has been signed by a certificate authority that the server trusts
 - has not expired

- Expands previous support for dynamically secured Telnet connections to the z/VM FTP and SMTP servers

- New or enhanced **CLIENTCERTCHECK** statement/option
 - FTP server
 - Statement in FTP configuration file (SRVRFTP CONFIG)
 - *SMSG server_id SECURE* command
 - CERTFULLCHECK and CERTNOCHECK removed from *FTP* command

 - SMTP server
 - *TLS* statement in SMTP CONFIG file
 - *SMSG server_id TLS* command

 - Telnet server
 - *INTERNALCLIENTPARMS* statement

 - TCPIP CONFIG
 - *PORT* statement
 - for verification of statically secured connections

Host Name Validation

- Allows a client to verify the identity of a server using either
 - Host Name
 - Domain Name
 - Host IP Address

- **SIOCSECCLIENT** call has been enhanced to accept a new version of the SecureDetailType structure which includes an extension for specifying the above validation string(s)

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

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

New APIs

- Pascal
 - **TCPSCERTDATA**
 - Request a specific field from the local or partner certificate

- IUCV/C
 - **SIOCGCERTDATA** ioctl command
 - Request a specific field from the local or peer certificate

How to get TLS/SSL Certificate Verification

- Planned availability: June 2020
 - z/VM 7.1
 - See <http://www.vm.ibm.com/newfunction/#ssl-cert-ver> for the latest information

Component	APAR	PTF	RSU
TCP/IP	PH18435	TBD	TBD
CMS	VM66348	TBD	TBD
LE	VM66349	TBD	TBD

- The LE update changes the definition of the SecureDetail structure
 - May need to modify programs using SecureDetail

How to get TLS/SSL Certificate Verification (cont.)

- Requires new versions of CMS and LE for SSL servers

- Requires new modules for
 - TCPIP
 - SSLSERV
 - NETSTAT
 - SRVRFTP
 - SMTP
 - FTP
 - TELNET

- All of the above need to be restarted with the new support

- No restart of z/VM is required

Keeping Up with Releases, Service, and New Function Updates

z/VM Releases

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

Release ³	z15 & LinuxONE III	z14 & LinuxONE II	z13 & LinuxONE Emperor	z13s & LinuxONE Rockhopper	ZEC12	ZBC12	z196	z114	z10 EC	z10 BC
z/VM 7.1	Yes	Yes	Yes	Yes	Yes	Yes				
z/VM 6.4	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes		
z/VM 6.3 ²		Some ⁴	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

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

Upgrade Installation

- Easier upgrade to a new z/VM release from existing systems
 - Avoids a full and fresh install
 - Especially helpful in a Single-System-Image (SSI) environment
 - All members of your SSI cluster must be on the same release

- Supports upgrades to z/VM 7.1 from z/VM 6.4

- Requires appropriate service on the old z/VM release

- Support for vendor products, local mods, and backing out if necessary

- See the *z/VM Installation Guide* for details

Verify That You Have Required Service for z15, z14, etc.

▪ z15, LinuxONE III

- <http://www.vm.ibm.com/service/vmreqz15.html>
- If running SSI, make sure VM66206 is applied to all members **before** IPLing any member on a z15
 - z/VM 6.4 *and* 7.1

- **New:** VM66332 is required to run Stand-alone Dump from SCSI Dasd
 - z/VM 6.4 *and* 7.1

▪ z14, LinuxONE Emperor II, z14 Model ZR1, LinuxONE Rockhopper II

- <http://www.vm.ibm.com/service/vmreqz14.html>
- If running SSI, make sure VM65976 is applied to all z/VM 6.4 members **before** IPLing any member on a z14

▪ Pages above have service lists which can be downloaded to verify you have correct service, e.g.

- Get file `VM710D36 SERVICE`
- Issue: `SERVICE ALL STATUS LIST VM710D36 SERVICE`

Migrating z/VM from z13 or earlier to an IBM z15 or z14/etc.

- The Stand Alone Program Loader (SAPL) **must** be rewritten with the z/VM 6.4 or 7.1 SALIPL utility
 - Otherwise you will not be able to IPL
 - Look for current release number in upper right corner of SAPL
- Upgrade installation does **not** rewrite SAPL
 - Must be done manually
- See red alert <http://www.vm.ibm.com/service/redalert/index.html#SAPLZ14>

```
STAND ALONE PROGRAM LOADER: z/VM VERSION 6 RELEASE 4.0  
DEVICE NUMBER: 018B MINIDISK OFFSET: 35 EXTENT: -  
MODULE NAME: CPLOAD LOAD ORIGIN: 2000
```

- Other stand alone utilities also need to be updated in order to IPL on z14
 - Standalone Dump, DDR, etc.

Stay Informed about Future New Function

- New web page to subscribe to:
 - <http://www.vm.ibm.com/newfunction/>

- Lists enhancements IBM is pursuing and gives:
 - Tentative dates for planning purposes
 - A high level view of impact and compatibility
 - Interaction with ISV products, Linux, and hardware

- Allows clients to
 - Express interest in being a sponsor user for the item
 - Plan for upcoming new support
 - Avoid surprises

Stay Informed about New-Function PTFs

- Off z/VM service page <http://www.vm.ibm.com/service/> is new page for new-function APARs
 - <http://www.vm.ibm.com/service/vmnfapar.html>

- Applies to z/VM operating system and related products:
 - Operations Manager for z/VM
 - Backup and Restore Manager for z/VM
 - OMEGAMON XE on z/VM and Linux
 - Etc.

- Subscribe to receive notifications automatically when new-function APARs become available

- Obtain lists of previously shipped new-function APARs

z/VM RSU News

- **z/VM 6.4 RSU 1901** - June 28, 2019
 - Includes APAR VM65930 (PTF UV61335)
 - **Introduces a RACF/VM template change**
 - APAR and associated template change is included in RACF/VM 7.1 base

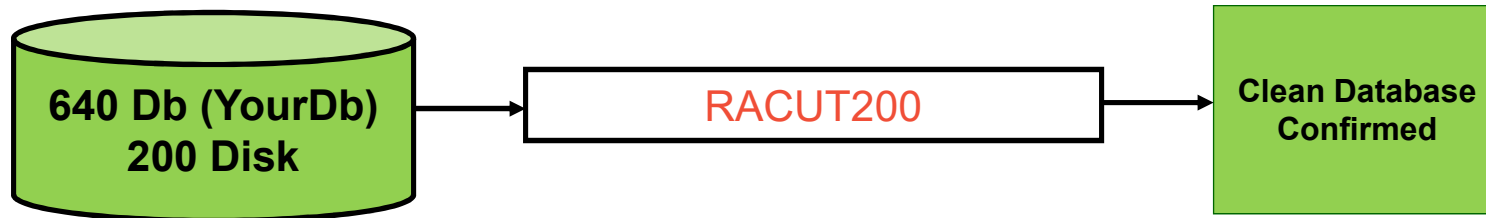
 - The RACF database must be upgraded when either
 - Applying the above APAR/RSU on RACF/VM 6.4
 - Installing RACF/VM 7.1 if the APAR/RSU was not previously applied on RACF/VM 6.4

 - When sharing a RACF database among multiple systems, **RACFVM must be forced off all of the systems** before the database is upgraded
 - Multi-member SSI clusters
 - Multiple LPARs that are not in an SSI cluster

 - See Chapter 17 of the *z/VM Installation Guide* for details

RACF Database Validation

- **Remember to validate your RACF database prior to and after applying a new template**
 - RACUT200 utility checks database integrity



- **Database best practices**
 - Have a procedure for database backups
 - Integrity-check your back-up databases
 - Automate around RACF initialization
- White paper on validating and repairing the database is available:
<https://www.ibm.com/downloads/cas/LVOL5P8Q>

Summary

Summary

- z/VM 7.1 is the newest release of z/VM
 - Enhancements for dump scalability and infrastructure for future enhancements
 - Includes all New Function APARs shipped for z/VM 6.4

- New Function APARs are continuing to be delivered on z/VM 7.1
 - Heavy dependence on the sponsor user program
 - Plans for new function will be published on the z/VM website

- Subscribe to or follow the websites referenced throughout this presentation for the latest news on new function, required service, and more