z/VM I/O Update: EAV Minidisk & Secure Paging Support

Steve Wilkins
IBM z/VM Development

wilkinss@us.ibm.com

IBM Systems Technical Events
ibm.com/training/events

MVMUA

January 25, 2018

Please note

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.

The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including 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 results similar to those stated here.

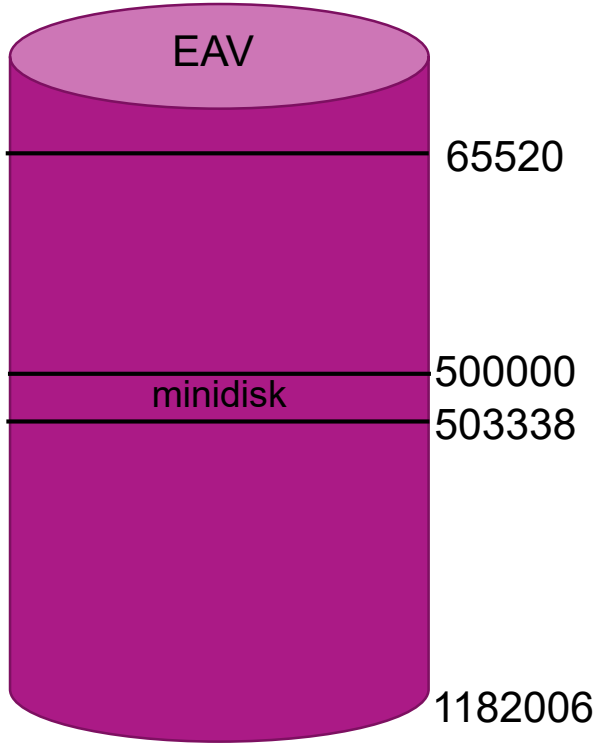
Abstract

- While z/VM has had support for Extended Address Volumes (EAV) for years, the associated minidisk support was restricted in many ways. A lot of those restrictions have been lifted by service to z/VM 6.4 and this session will describe those changes. Additionally, IBM has provided the ability to encrypt z/VM paging volumes with service to z/VM 6.4. This session will walk through the details of that support as well.

Extended Address Volumes (EAV) – Updates for non-FP Minis

Agenda

- Overview
- Required Service
- What is Really Supported Now
  - more than one might think
- What Remains Restricted
- API updates
  - and what they mean to you



Overview

- IBM has delivered service that has greatly enhanced VM Minidisk support for EAV volumes
- Definition: An Extended Address Volume (EAV) is a 3390 Model A (Sense ID x0E) that is greater than 65,520 cylinders
- Before: VM supported only 0 to END FP minis on EAVs, or non-FP minis defined **below** real cylinder 65520
- After: VM now supports non-FP minis defined anywhere on an EAV.
  - This includes EAVs up to 1TB (1,182,006 cylinders); the current hardware max.
  - Some other nusance restrictions where lifted

Required Service

- Service available on August 25, 2017 for z/VM 6.4
- CP APAR VM65943 (PTF UM35187)
- CMS APAR VM65945 (PTF UM35204)
- ICKDSF R17 APAR PI85943 (PTF UI49579)
  - MUST HAVE bug fix (IF REQ of CP APAR)

What is Really Supported Now

- Minidisks anywhere on an EAV:
  - Directory Statement: MDISK 700 3390 100000 50 SGW230 MR
  - Command: DEFINE MDISK 700 100000 50 SGW230
- Temporary disks of any size on an EAV (up to size of real volume TDSK allocation)
  - Directory Statement: MDISK 700 3390 T-DISK 100000
  - Command: DEFINE T3390 700 100000
  - TDSK Allocation can exist anywhere on real EAV
  - CLEAR_TDISK function is supported no matter where TDSK allocation resides
- PARM Allocation can exist anywhere on real EAV (but is limited to 65520 cylinders)
  - CPACCESS command fully supports this *sliding* location
  - SAPL utility fully supports this *sliding* location
- DDR Utility fully supports EAV fullpack and non-fullpack virtual DASD located (anywhere) on real EAV
- Ditto for CP FLASHCOPY command functions; eg. Fully supported.

What Remains Restricted

- DRCT, PAGE, SPOL extents must remain **below** real cylinder 65520
- Checkpoint & Warmstart areas can start no higher than cylinder 65511 (since they can be 1-9 cylinders in size)
- CMS minidisks are restricted to 65520 cylinders or less in size
- There is no minidisk cache support for any minidisk defined on an EAV
  - However, if the real 3390-A is 65,520 cylinders (or less) MDC is supported as on other volumes with APAR VM65741 (PTF UM34922)
- MAPMDISK mapping service is restricted to minidisks that are entirely **below** real cylinder 65520.
- XLINK only supports the **first** 65520 cylinders (0-65519) on an EAV
- DFSMS/VM only supports minidisks up to 65520 cylinders in size

API Updates

- No Diagnose x'18' (Standard DASD I/O) support for virtual DASD on real EAVs
  - This is an older interface with no known exploiters
  - Diagnose x'A4' has been enhanced & should be used instead
- DIAG X'20' (370 Synchronous I/O) is restricted to virtual DASD 65520 cylinders (or less) in size but supports locations anywhere on a real EAV
  - RACF uses this Diagnose restricting RACF to virtual DASD 65520 cylinders (or less) in size, but in-line with CMS volume size restriction.
- DIAG X'A4' (Synchronous Block I/O) & *BLOCKIO System Service limited to minidisks of 65520 cylinders (anywhere on real volume), regardless of formatted block size.
  - In-line with CMS volume size restriction and most applications built on CMS (e.g., SFS, DB2)
- DIAG X'A8' (Synchronous I/O) fully supports virtual DASD of any size on real EAVs
  - Application must indicate support via input flag (but no known use outside CMS)
- DIAG X'250' (Synchronous & Asynchronous Block I/O) fully supports virtual DASD of any size, and any formatted block size, on real EAVs.
- DIAG X'E4 (Process minidisk real device information) & DIAG X'210' (Retrieve Device Information) fully support virtual DASD of any size on real EAVs

Misc. Notes

- CMS APAR VM65945 exists to allow SFS to handle the non-zero return code gracefully in the case an attempt is made to map a dataspace on an EAV.
  - Occurs if DIRCONTROL directories are defined on a minidisk spanning (or above) real cylinder 65519.
  - DIRCONTROL uses MAPMDISK & hits the MAPMDISK mapping restriction in this case.
- Live Guest Relocation (LGR) will fail if target system does not have VM65943 applied, the source system has VM65943 applied, and the guest has non-fullpack minidisks defined above real cylinder 65519.

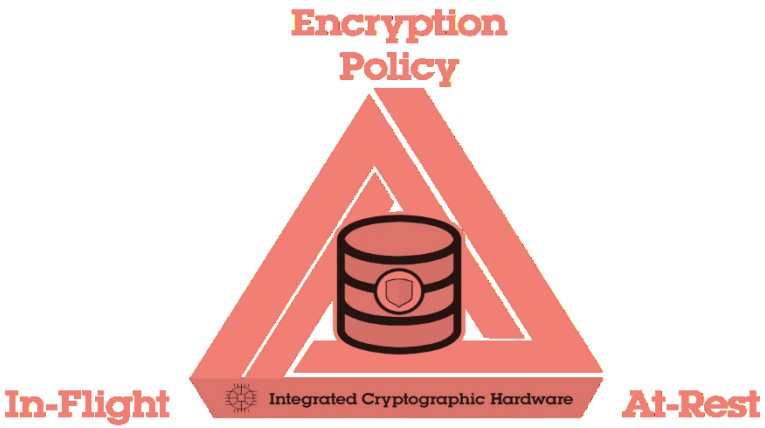
Encrypted Paging

Agenda

- Pervasive Encryption
- Intro to z/VM Encrypted Paging
  - How to Get Started
  - What's CPACF?
- How to Use Encrypted Paging
  - System Configuration File
  - QUERY ENCRYPT
  - SET ENCRYPT
  - Auditing and Monitor Records
- Sample Performance Data
- Best Practices

IBM Z Pervasive Encryption

- Pervasive Encryption is an important IBM Z strategic theme
- The VM Encrypted Paging project falls in-line with this theme
- *Transparent and consumable approach to enable extensive encryption of data in-flight and at-rest to substantially simplify & reduce the costs associated with protecting data & achieving compliance mandates*



Required Service

- Service available on December 11, 2017 for z/VM 6.4
- CP APAR VM65993 (PTF UM35257)

Getting Started with Encrypted Paging

- Starting point: z/VM partition on **a z14** with CPACF enabled
- Set up in System Configuration file (can modify it dynamically later, if you change your mind)
- Generates an ephemeral *n*-bit AES encryption key during IPL process
- If ENCRYPT PAGING is ON, then pages are encrypted as they move to/from paging volumes.
- Use monitor records to determine performance impact for workloads
- **Relevant User Roles: Data Owner, Security Admin, Auditor**

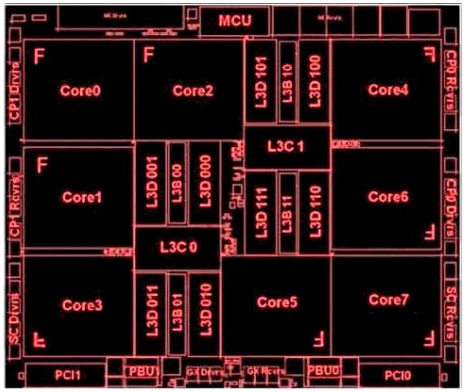
CP-Assisted Cryptographic Facility (CPACF)

CPACF Support (No-Charge Licensed Feature 3863)

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

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

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



Getting Started with Encrypted Paging: What's Encrypted?

- This function encrypts data moved from active memory to a paging volume owned by CP
  - ECKD or SCSI

- Encryption is limited to guest pages and VDisk pages written by the CP paging subsystem

- The following types of pages will **not** be encrypted:
  - Spool files
  - Directory pages
  - Minidisk data to a mapped minidisk pool
  - Minidisk cache pages
  - CP page tables (PGMBKs)

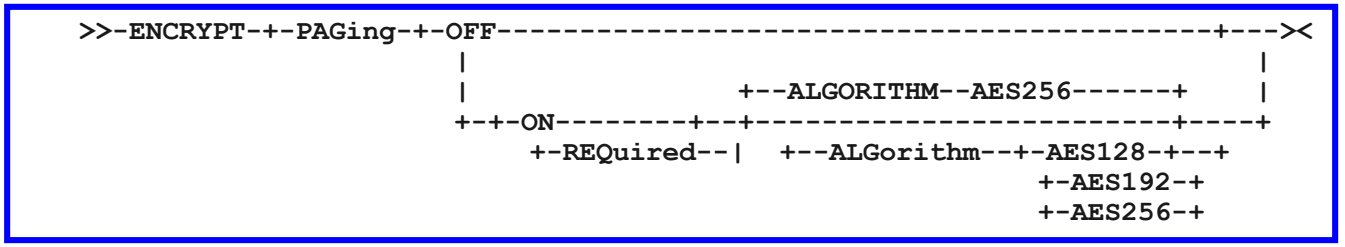
System Config Statement: ENCRYPT

- If OFF, no change – no problem. (This is the default behavior, even after PTF is applied.)
- If ON and (missing or low-level CPACF) then

```
HCP1390E Encrypt Paging Not Available due to missing hardware
support
(IPL processing continues)
```

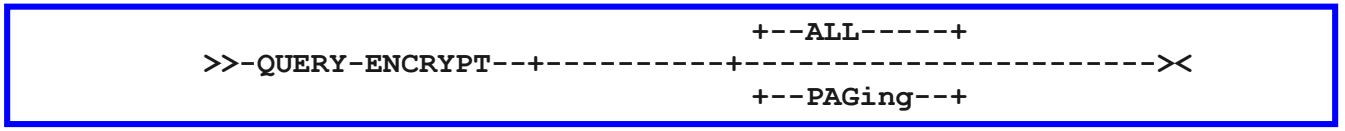
- If REQUIRED and (missing or low-level CPACF) then

```
HCP1393W Encrypt Paging Not Available due to missing hardware
support, specified as Required
wait state
```



QUERY ENCRYPT (IBMCLASS A, C, or E)

- QUERY ENCRYPT displays settings for host level encryption on the hypervisor. (Right now, this is 'PAGING' only)
- **Note**: QUERY ENCRYPT does not notify the user whether hardware support is available on this CEC.




```
Encrypt Paging settings:
      Currently: Required AES256
      At IPL: Off

Ready;
```

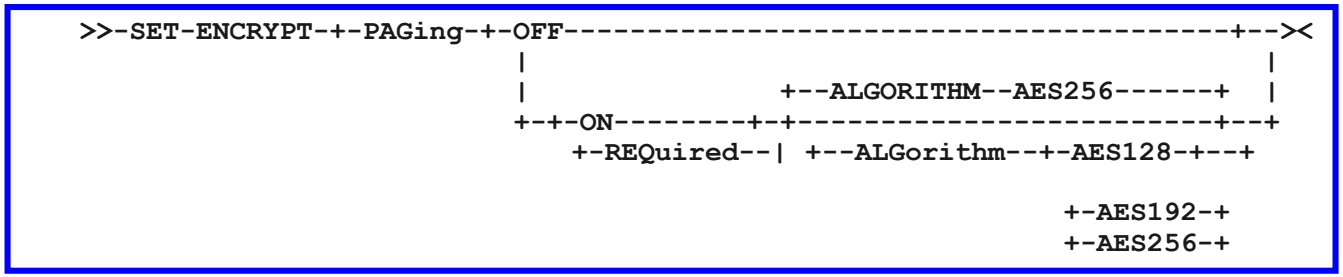
SET ENCRYPT (IBMCLASS A) (1/2)

- *Using SET ENCRYPT:*
  - When specifying ON or REQUIRED, the default ALGORITHM is always AES256.
  - The algorithm value may only be selected when Encrypted Paging is enabled for the first time. This may be via SET or in the System Configuration file.

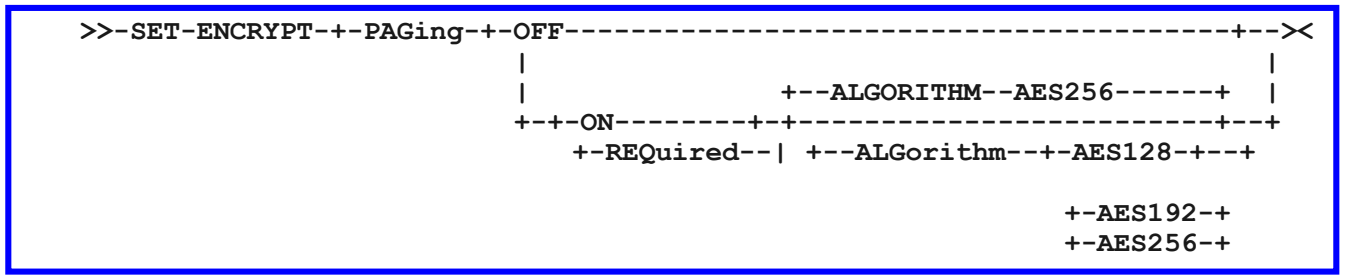
    Algorithm value cannot be changed without a re-IPL:

    HCP1391E: Encryption algorithm previously set to ALGORITHM; no change made
  - The System Operator is notified of changes to primary setting, e.g.

    HCPENC1394I Encryption of paging changed from OFF to ON, with algorithm AES256, by user WILKINSS



SET ENCRYPT (IBMCLASS A) (2/2)



- *Using SET ENCRYPT:*
  - SET ENCRYPT cannot be used when missing hardware support:
    HCPENC1390E Encrypt Paging cannot be enabled due to missing hardware support
  - If set to REQUIRED, changes cannot be made without a System IPL.
    HCPENC1390E Encrypt Paging is required; no change made

Notes on 'REQUIRED' option

- Please note that REQUIRED means REQUIRED.
  - Cannot be changed, cannot be broken
  - Meant to assure 100% compliance for the customers who need it

- If you have configured REQUIRED on a system which does not support the feature, your system will not IPL
  - Double-check system labels in an SSI cluster – exclude back-level systems
  - CPACF not enabled on new CEC – turn on CPACF
  - z13 and earlier hardware – not supported
  - May be a problem for DR sites

- IBM recommends:
  1. Test Encrypted Paging with ON before switching to REQUIRED
  2. **Consider switching from ON to REQUIRED in AUTOLOG1 (during System IPL process)**
     or put SET ENCRYPT PAGING REQUIRED on a COMMAND statement for OPERATOR
  3. Having a back-up System Configuration file (ON) for emergency purposes
  4. Double-checking DR plans for hardware availability of z/VM systems

Details on Encrypted Paging – How To Use

1. Make sure CPACF is enabled on your z14 system.
   – Support requires CPACF (no-charge Feature 3863) to be enabled on z14 hardware or later
2. Set **ENCRYPT PAGING ON** in System Configuration or use **CP SET ENCRYPT PAGING**
3. Protected ephemeral key (of selected algorithm) generated by CP for system lifetime, for all guests
   – No key rotation mechanism in this function
4. Support comes in **OFF** (default), **ON**, and **REQUIRED** modes
   – Per sponsor user feedback, changing algorithm in this deliverable will require an IPL
5. To prevent against timing attacks, TRSOURCE not permitted in keygen section of the IPL process
6. One key per z/VM partition – no SSI dependencies
   – Performance considerations for guest relocation: re-enciphering paging data
7. A mandate for 100% encryption should use 'ENCRYPT PAGING REQUIRED' at IPL
   – ENCRYPT PAGING ON gives function but can be dynamically toggled
   – Dynamic support can enable compliance, but **proving it** is difficult (draining volumes)

Auditing your Encrypted Paging

- Auditing with MONITOR Records
  - D1R4 – System Configuration and current status thereof
  - D3R2 – Pages encrypted/decrypted, CPU utilization for encryption
  - ***new*** D1R34 – Event record for status (SET ENCRYPT), with userid
- If moving from ON to OFF, pages will still be decrypted when read into guest memory
- Only way to ensure 100% compliance is to IPL your z/VM system with
  - `ENCRYPT PAGING ON ALGORITHM AES256`
- Auditing with SMF Records
  - Auditing in RACF automatically covers new CP commands, per above
  - Just enable tracking in your VMXEVENT profile

New Monitor Record (D1R34): MRMTRENC (Encrypted Service Event)

- Track changes to Encrypt Paging settings
- Notes who made changes, timestamps, requested algorithms, etc.

Dec	Hex	Type	Len	Name	Description
000	000	Structure	28	MTRDDR	Start of monitor record
000	000	Character	0	MTRDDR_MRHDR	Record header. See MRRECHDR for details.
000	000	Character	20	MRHDR	
000	000	Unsigned	2	MRHDRLEN	Record length in bytes
002	002	Unsigned	2	MRHDRZER	Field of zeros
004	004	Unsigned	1	MRHDRDM	Domain identifier
005	005	Unsigned	1	*	Reserved for IBM use
006	006	Unsigned	2	MRHDRRC	Record identifier
008	008	Character	8	MRHDRTOD	Time at which this record was built. In time-of-day (TOD) clock format. See IBM System 370 XA Principle of Operation for explanation of format.
016	010	Character	4	*	Reserved for IBM use
020	014	Character	0	MRHDR_END	End of header
020	014	Character	8	MTRENC_ENCSERV	CP service to cipher
028	01C	Bitstring	1	MTRENC_ENCPREV	Previous configuration
		1...		MTRENC_ENCREQP	ENCRYPT Required
		.1..		MTRENC_ENCONP	ENCRYPT On
		..1.		MTRENC_ENCOFFP	ENCRYPT Off
		...1		MTRENC_ENC128P	Algorithm AES128
		.... 1...		MTRENC_ENC192P	Algorithm AES192
		.... .1..		MTRENC_ENC256P	Algorithm AES256
		.... ..1.		*	Reserved for IBM use
		1		*	Reserved for IBM use
029	01D	Bitstring	1	MTRENC_ENCCUR	Changed configuration
		1...		MTRENC_ENCREQC	ENCRYPT Required
		.1..		MTRENC_ENCONC	ENCRYPT On
		..1.		MTRENC_ENCOFFC	ENCRYPT Off
		...1		MTRENC_ENC128C	Algorithm AES128
		.... 1...		MTRENC_ENC192C	Algorithm AES192
		.... .1..		MTRENC_ENC256C	Algorithm AES256
		.... ..1.		*	Reserved for IBM use
		1		*	Reserved for IBM use
030	01E	Bitstring	2	*	Reserved for IBM use
032	020	Character	8	MTRENC_ENCUSRID	z/VM userid that issued the SET ENCRYPT command
040	028	Character	0	MTRENC_END	End of record

Updated Monitor Records

- **Domain 1 Record 4 MRMTRSYS (System Configuration)** – Logs Encrypted Paging settings and algorithm at time of IPL. Will also indicate failure reason (e.g., CPACF not available)
- **Domain 3 Record 2 MRSTORSP (Real Storage Activity per Processor)**

Offsets					
Dec	Hex	Type	Len	Name	Description
720	2D0	Unsigned	4	STORSP_PLSENCRYPTPAGES	Cummulative number of pages encrypted by the paging subsystem
724	2D4	Unsigned	4	STORSP_PLSDECRYPTPAGES	Cummulative number of pages decrypted by the paging subsystem
728	2D8	Unsigned	8	STORSP_PLSENCPTCPUTIME	Cummulative raw CPU time spent doing page encryption for the paging subsystem
736	2E0	Unsigned	8	STORSP_PLSDECPTCPUTIME	Cummulative raw CPU time spent doing page decryption for the paging subsystem
744	2E8	Character	0	STORSP_END	

D3R2EC.EXEC

- Tool from z/VM Performance Team to track encrypted paging monitor values
- Available on z/VM Performance website
- Performance Toolkit updates to follow at a later date

D3R2 Encrypted paging report for file: A05Y9152 MONDATA

Interval			<------- Rate of Pages -------->			<------ Percent CPU busy ------>		
__Ended_	Type	LPU_	_Enc+Dec__	Encrypted_	Decrypted_	_Enc+Dec__	__Encrypt_	__Decrypt_
>>Mean>>	IFL	0	19451.25	11662.78	7788.47	2.45044	1.71205	0.73840
>>Mean>>	IFL	1	19036.57	9766.84	9269.73	2.31351	1.43584	0.87766
>>Mean>>	IFL	2	19153.36	9761.35	9392.01	2.32062	1.43352	0.88710
>>Mean>>	IFL	3	19010.73	9657.54	9353.18	2.32729	1.43122	0.89607
>>Mean>>	IFL	4	19131.78	9685.10	9446.68	2.33772	1.43319	0.90453
>>Mean>>	IFL	5	21139.60	9656.43	11483.17	2.50907	1.42566	1.08341
>>Mean>>	IFL	6	21351.01	9744.53	11606.48	2.53488	1.44154	1.09333
>>Mean>>	IFL	7	21167.82	9827.81	11340.01	2.52316	1.45072	1.07244
>>Total>	....	8	159442.12	79762.38	79679.73	19.31669	11.76374	7.55294
15:27:27	IFL	0	14500.07	9057.13	5442.94	1.83363	1.33507	0.49856
15:27:27	IFL	1	15452.78	8950.06	6502.72	1.91393	1.31984	0.59409
15:27:27	IFL	2	15215.59	8310.86	6904.73	1.85513	1.22522	0.62991
15:27:27	IFL	3	14394.43	7823.19	6571.24	1.78056	1.17005	0.61051
15:27:27	IFL	4	14700.28	8225.17	6475.11	1.82524	1.22422	0.60102
15:27:27	IFL	5	18332.57	8317.30	10015.27	2.14883	1.23835	0.91048
15:27:27	IFL	6	18304.86	8439.71	9865.15	2.15040	1.25402	0.89638
15:27:27	IFL	7	18117.23	8296.26	9820.97	2.12680	1.23287	0.89393
>>Total>	....	8	129017.81	67419.68	61598.13	15.63452	9.99964	5.63488
15:27:57	IFL	0	20984.71	11808.29	9176.42	2.58744	1.71926	0.86818
15:27:57	IFL	1	20038.51	8859.42	11179.09	2.34774	1.29137	1.05637
15:27:57	IFL	2	20170.38	9001.16	11169.22	2.36140	1.30838	1.05302
15:27:57	IFL	3	19741.21	8430.19	11311.02	2.31781	1.23350	1.08431
15:27:57	IFL	4	19681.81	8459.56	11222.25	2.30965	1.23409	1.07556
15:27:57	IFL	5	22587.21	8467.49	14119.72	2.56253	1.23307	1.32946
15:27:57	IFL	6	22904.38	8472.96	14431.42	2.59338	1.23633	1.35705
15:27:57	IFL	7	23478.97	9439.22	14039.75	2.70212	1.37671	1.32541
>>Total>	....	8	169587.18	72938.29	96648.89	19.78207	10.63271	9.14936

Sample Performance Data

- High Paging workload with scaling of logical processors & memory
- MT disabled with default algorithm AES256
- Workloads paged between 150K to 163K pages / sec (considered high)
- Stats taken from D3 R2 monitor records
- Used between **18% to 20%** of one processor
- The percent CPU used to do encryption was more costly than to do decryption
- Total CPU/tx did not exceed **5%** when encryption was enabled

Logical Processors/ Memory (GB)	En+Decrypted paging Rate (D3R2)	En+Decrypted CPU Bsy (D3R2)
08 / 512	159997.55	19.57
16 / 1024	163467.08	19.57
24 / 1536	150619.01	17.96
32 / 2048	155924.89	18.88

Best Practices with z/VM Encrypted Paging

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

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

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

More Information

For More Security Related Information …

- **IBM z14 Technical Guide:**
  http://www.redbooks.ibm.com/redpieces/abstracts/sg248451.html?Open
- **IBM Z Hardware Crypto Synopsis:**
  https://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP100810
- **IBM Z Crypto Education Community**:
  https://www.ibm.com/developerworks/community/groups/community/crypto
- **z/VM Security:**
  http://www.vm.ibm.com/security
- **Linux on z Security:**
  https://www.ibm.com/support/knowledgecenter/linuxonibm/liaaf/security.html

Security Contact:

CISSP

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

Encrypted Paging: Frequently Asked Questions (1/2)

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

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

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

Encrypted Paging: Frequently Asked Questions (2/2)

- How much does it cost?
  - *Performance measurements look good – no more than 5% increase in CPU utilization on a z14*
  - *Better performance encrypted than the z13 unencrypted*
  - *As paging rate increases, the total amount of CPU used will also increase*

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

- Why paging? Why not minidisks?
  - *"Minimum Viable Product" for now*

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

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

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

- **Note**: REQUIRED may cause complications with DR sites
  - System will not IPL on earlier hardware
  - Recommend you IPL with `ENCRYPT PAGING ON <algorithm>`
    - `SET ENCRYPT PAGING REQUIRED` via AUTOLOG1 or via a COMMAND Statement

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

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

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

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

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

Continue growing your IBM skills

ibm.com/training

provides a comprehensive portfolio of skills and career accelerators that are designed to meet all your training needs.

If you can't find the **training that is right for you** with our Global Training Providers, we can help.

Contact IBM Training at dpmc@us.ibm.com

Notice and disclaimers

Notice and disclaimers cont.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of 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. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products**. IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a particular, purpose.**

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

IBM, the IBM logo, ibm.com, AIX, BigInsights, Bluemix, CICS, Easy Tier, FlashCopy, FlashSystem, GDPS, GPFS, Guardium, HyperSwap, IBM Cloud Managed Services, IBM Elastic Storage, IBM FlashCore, IBM FlashSystem, IBM MobileFirst, IBM Power Systems, IBM PureSystems, IBM Spectrum, IBM Spectrum Accelerate, IBM Spectrum Archive, IBM Spectrum Control, IBM Spectrum Protect, IBM Spectrum Scale, IBM Spectrum Storage, IBM Spectrum Virtualize, IBM Watson, IBM Z, IBM z Systems, IBM z13, IMS, InfoSphere, Linear Tape File System, OMEGAMON, OpenPower, Parallel Sysplex, Power, POWER, POWER4, POWER7, POWER8, Power Series, Power Systems, Power Systems Software, PowerHA, PowerLinux, PowerVM, PureApplica- tion, RACF, Real-time Compression, Redbooks, RMF, SPSS, Storwize, Symphony, SystemMirror, System Storage, Tivoli, WebSphere, XIV, z Systems, z/OS, z/VM, z/VSE, zEnterprise and zSecure are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.