KIOXIA

White Paper

Encrypt Data Faster with PCIe® 4.0 NVMe® SSDs versus Software Solutions:

Comparing Encryption Protection: KIOXIA CM6 Series SSDs and Software RAID

A common IT practice for many years has involved protecting user and business data from being used maliciously by unauthorized parties and hackers. This practice applies to both data that is being transferred from one location to another across a network (data-in-transit) and data that is not actively moving across a network but is being stored on a storage device (data-at-rest). However, these practices are more challenging today versus in years past as significantly more data has been generated from sources such as PCs, smartphones, tablets and IoT edge devices and is a trend that is expected to continue.

Additionally, malicious parties are becoming more adept at accessing exposed and unprotected data as they can bypass implemented security measures such as firewalls and other network access controls. With an abundance of sensitive and business-critical data captured, it is as important as ever to protect data-in-transit and data-at-rest for short-term and future use. Fortunately, there are SSD encryption methods available that can help to protect data from unauthorized parties or hackers. With more data coming from more sources that must be encrypted, this white paper focuses on SSD encryption methods and their impact on system/storage performance and CPU utilization when compared to software encryption.

Hardware Encryption vs. Software Encryption

Data encryption enables digital content, such as databases, documents, emails, images, videos, etc., to be translated into unreadable characters that only users with a security key or password can access. In the past, data-at-rest encryption had not been used as frequently as data-in-transit encryption due to the amount of time and additional system CPU cycles that were required to encrypt and decrypt data, while running intended applications and workloads. When improperly deployed, data-at-rest encryption can negatively impact system and application performance, as well as the user experience.

To address these performance limitations and offload the CPU cycles required for data-at-rest encryption on a system, storage manufacturers developed Self Encrypting Drives[1] (SEDs). These drives typically include on-board crypto-processers that use AES[2]-256-compliant encryption algorithms to encrypt plaintext data. With this level of data-at-rest encryption at the hardware layer, unauthorized user access can be prevented. The best SEDs for meeting this objective will not negatively impact performance when encryption within the drive is turned on.

Complementary to SEDs are hardware RAID solutions that can be used to encrypt drives and locally manage the security keys. However, these RAID card solutions can create bottlenecks in the storage stack that limit the paths through which data travels, impacting SSD data throughput and overall system performance. With the popularity and increased deployment of NVMe SSDs within data center systems, maximum performance can only be achieved by connecting the SSD directly to the host. This eliminates the possibility for a RAID card and utilizes the PCIe lanes directly from the CPU.

IT personnel may use software RAID to avoid potential bottlenecks associated with NVMe hardware RAID solutions. When software-based (or file system based) RAID encryption is used, a substantial amount of system CPU resources are required which can result in storage performance degradation that can drastically decrease a system's ability to perform storage operations. This white paper showcases the impact that hardware encryption and software encryption have on system/storage performance. It also presents whether hardware encryption or software encryption taxes CPU resources more versus when encryption is disabled.

System and Application Test Scenario

To determine the impact that hardware encryption and software encryption have on performance and CPU resources in a PCIe 4.0 NVMe based system, KIOXIA conducted throughput, input/output operations per second (IOPS) and CPU utilization tests in a lab environment with hardware encryption and software encryption enabled, as well as when encryption was disabled. The test system configuration included a Dell® EMC® PowerEdge™ R7525 server with dual AMD EPYC™ 7552 CPUs and four (4) KIOXIA CM6 Series SSDs that support TCG-Opal and Ruby[3] Security Subsystem Classes[4] (SSCs) and utilize security modules designed to comply with FIPS 140-2 Level 2 and FIPS 140-3 Level 2[5]. The security modules utilized by the CM6 Series SSDs were validated for FIPS 140-2 Level 2 requirements.

The workload tests were run through Flexible I/O (FIO) software[6] - a tool that provides the ability to create a broad spectrum of workload tests with results that deliver the actual raw performance of the drive itself. There were 4 performance tests conducted that included sequential read and write throughput tests, and random read and write IOPS tests. For each of the four performance tests conducted, CPU utilization was measured concurrently to record how many additional CPU cycles and extra processing were required for encryption while performing a given workload. Each of the tests is described below:

- **Sequential Read and Write Operations:** *These operations read and write data of a specific size which is ordered one after the other from a logical block address (LBA) perspective. Sequential read and write performance is regarded as data throughput and specified in megabytes per second (MB/s).*
- **Random Read and Write Operations:** *These random operations read and write data of a specific size that is ordered randomly from an LBA perspective. Random read and write performance is specified in IOPS.*
- **CPU Utilization:** *CPU utilization represents a percentage of the total amount of available CPU cycles being used for a given workload. Encryption requires CPU cycles to encrypt and decrypt data on the storage media itself which can negatively impact system performance as a whole. CPU utilization was recorded concurrently with the four performance test workloads.*

A description of the test configuration, set-up, execution procedures, results and analysis are presented below. The test results demonstrate the probable effects that encryption has on four-corner performance when running raw FIO workloads with CM6 Series SSDs.

Test Configuration:

The hardware and software equipment used for the four-corner and CPU utilization tests included:

- **Dell EMC PowerEdge R7525 Server:** One (1) dual socket server with two (2) AMD EPYC™ 7552 processors, featuring 48 processing cores, 2.2 GHz frequency, and 256 gigabytes[7] (GB) of DDR4 RAM
- **Operating System:** Ubuntu® v21.10 (Kernel 5.13.0-30-generic)
- **Test Software:** Four-corner synthetic tests run through FIO v2.29-108 test software
- **Storage Devices (Table 1):** Four (4) KIOXIA CM6 Series SSDs with 1.6 terabyte[7] (TB) capacities and following specs:

Specifications	CM6 Series
Interface	PCIe 4.0
Protocol	NVMe 1.4
Capacity	1.6 TB
Form Factor	2.5-inch[8] (15mm)
NAND Flash Type	BiCS FLASH™ 3D flash memory
NAND Flash Layers	96
Drive Writes per Day[9] (DWPD)	3 (5 years)
Power	16W typical

Table 1: KIOXIA CM6 Series SSD specifications

Set-up & Test Procedures

The test system was configured using the hardware and software equipment outlined above. A Dell EMC PowerEdge R7525 rack server was configured with an Ubuntu operating system, FIO test software and four KIOXIA CM6 Series SSDs. The four CM6 Series SSDs were then configured with a MDADM[10] RAID 0 array with default settings as follows:

- ***For the software-based encryption tests**, LUKS[11] was utilized to encrypt the created software volume on the 4-drive RAID set.*
- ***For the hardware-based encryption tests**, SEDutil[12] was utilized to activate hardware-level encryption on each of the individual drives in the 4-drive RAID set.*

The FIO software performed 4-corner workload tests of the KIOXIA CM6 Series SSDs, obtaining the throughput, IOPS and CPU utilization results in a hardware-encrypted, software-encrypted and unencrypted configuration. The throughput and IOPS results were recorded and the CPU utilization was also monitored and recorded as the performance tests were being run. The four workload tests included:

Workload A: 100% Sequential Read

Designed to simulate a stream of data similar to an object store or media streaming application.

Test Order	Test Metric	Test Type	Block Size	Queue Depth	# of Threads
Workload A	Throughput	100% Sequential Read	128 kilobyte[7] (KB)	4,096	4

Workload B: 100% Sequential Write

Designed to mimic database logging or other log file workloads.

Test Order	Test Metric	Test Type	Block Size	Queue Depth	# of Threads
Workload B	Throughput	100% Sequential Write	128KB	4,096	4

Workload C: 100% Random Read

Simulates a multi-user environment with many random read operations.

Test Order	Test Metric	Test Type	Block Size	Queue Depth	# of Threads
Workload C	IOPS	100% Random Read	4KB	8,192	128

Workload D: 100% Random Write

Represents normal server write workloads from many applications.

Test Order	Test Metric	Test Type	Block Size	Queue Depth	# of Threads
Workload D	IOPS	100% Random Write	4KB	8,192	128

NOTE: For each of the four workload tests, CPU utilization was also measured concurrently.

The MDADM utility was used to create a RAID 0 set for the four CM6 Series SSDs (configured with a default chunk size of 512K). Hardware encryption and software encryption were not enabled. The 4-corner tests were run using FIO test software and the results were recorded in conjunction with the system CPU utilization tests (see Test Results section).

For software encryption, the MDADM created RAID set was then removed and recreated. Once completed, the software RAID set was then configured with LUKS software-based encryption. The 4-corner workload tests were performed again in an identical manner on the software encrypted volume, and the results and system CPU utilization were recorded for comparison against the unencrypted RAID set (see Test Results section).

When the software encrypted tests were completed, software-based encryption was removed via LUKS and the software RAID 0 set was also removed. Hardware encryption was then turned on for each CM6 Series drive through the SEDutil, and then the software RAID set was recreated. The 4-corner workload tests were performed again in an identical manner on the hardware based encryption RAID set. The results and system CPU utilization were recorded concurrently for comparison against software encryption and unencrypted RAID sets (see Test Results section).

Test Results

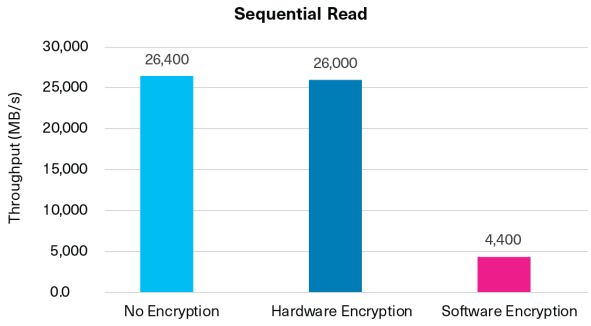
The four workload tests were run using FIO software with the throughput, IOPS and CPU utilization results recorded for hardware encryption, software encryption and no encryption at all. The following is a snapshot of the test results:

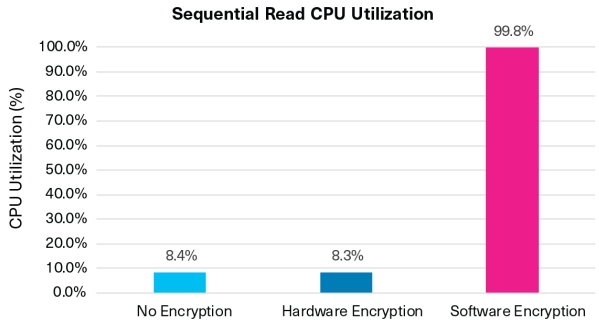
	No Encryption		HW Encryption		SW Encryption	
4-Corner Performance + CPU Utilization Tests	**Test Results**	**CPU Utilization**	**Test Results**	**CPU Utilization**	**Test Results**	**CPU Utilization**
Workload A: 100% SR	26,400 MB/s	8.4%	26,000 MB/s	8.3%	4,400 MB/s	99.8%
Workload B: 100% SW	11,200 MB/s	1.5%	11,000 MB/s	1.7%	3,600 MB/s	77.1%
Workload C: 100% RR	3,517K IOPS	87%	3,595K IOPS	88%	882K IOPS	99.8%
Workload D: 100% RW	320K IOPS	21%	319K IOPS	21%	141K IOPS	99.8%

	No Encryption	HW Encryption		SW Encryption	
CPU Utilization Comparison	**CPU Utilization**	**CPU Utilization**	**HW Encryption Difference**	**CPU Utilization**	**HW Encryption Difference**
Workload A: 100% SR	8.4%	8.3%	-0.1%	99.8%	-91.5%
Workload B: 100% SW	1.5%	1.7%	+0.2%	77.1%	-75.4%
Workload C: 100% RR	87%	88%	+1%	99.8%	-11.8%
Workload D: 100% RW	21%	21%	0%	99.8%	-78.8%

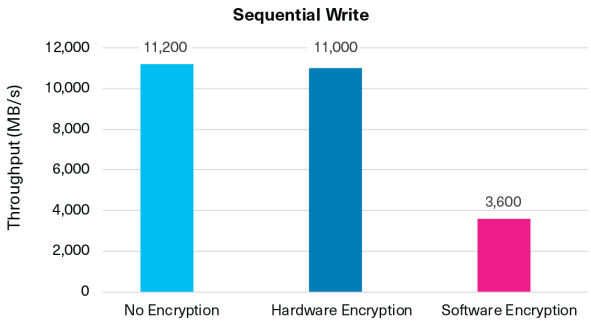
The results for each of the four workload tests:

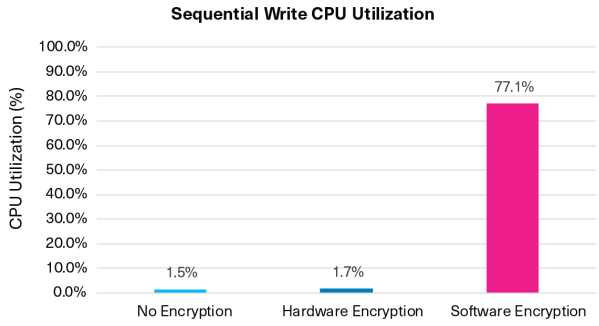
Workload A: 100% Sequential Read



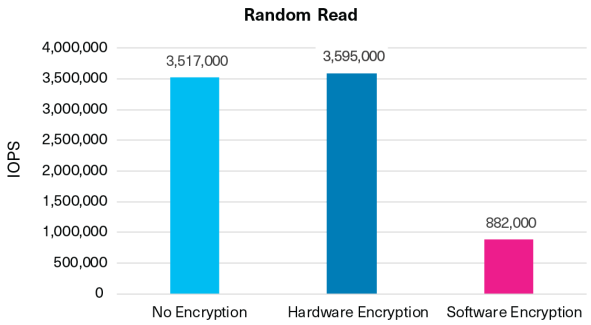


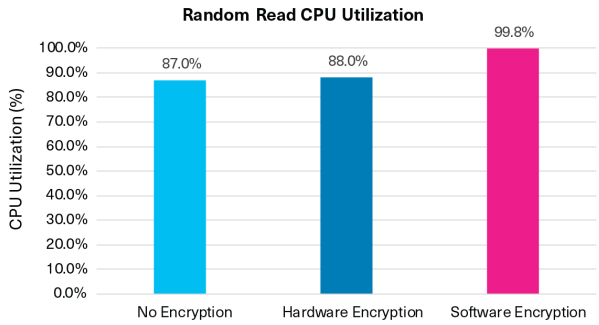
Workload B: 100% Sequential Write



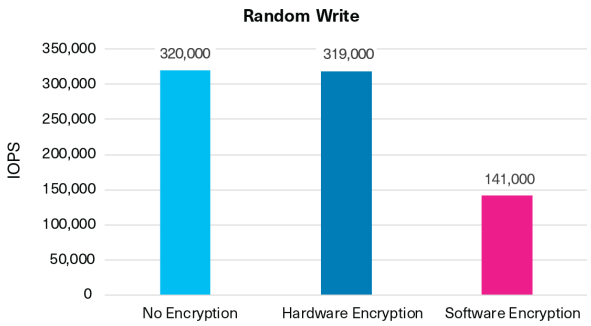


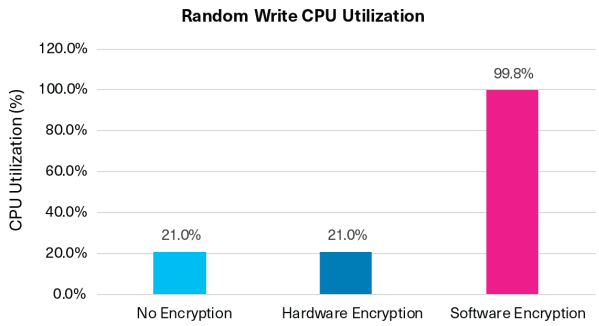
Workload C: 100% Random Read





Workload D: 100% Random Write





Test Analysis

The test results validate that a server using software encryption has significant performance degradation. In comparison to PCIe 4.0 NVMe SSDs with SEDutil and drive level encryption enabled, there was relatively insignificant performance impact. In fact, the test results indicate very little variation in performance or CPU utilization when the CM6 Series SSDs operated with hardware encryption enabled and disabled.

When CPU utilization was tested concurrently on the CM6 Series SSDs with no encryption enabled or when CPU cycles were offloaded to the SED drives, there was virtually no impact on system CPU utilization. However, when software encryption was used, all workloads were impacted due to the extra CPU cycles that are required to process encryption tasks concurrent in addition to processing each workload.

The following is an analysis of each workload test result:

Workload A: 100% Sequential Read

When 100% sequential read operations were tested, the CM6 Series SSDs with hardware encryption enabled delivered 26,000 MB/s. In comparison to software encryption at 4,400 MB/s, hardware encryption had a 490% improvement in sequential read operations. There was only a 1.5% difference in sequential read performance between hardware encryption and no encryption.

100% SEQUENTIAL READ
HW Encryption vs SW Encryption = +490%
HW Encryption vs No Encryption = -1.5%

For CPU utilization, hardware encryption enabled and no encryption delivered comparable results, 8.3% and 8.4% respectively, demonstrating no practical difference in CPU utilization whether hardware encryption was enabled or disabled. However, with software encryption enabled, CPU utilization increased dramatically to 99.8%. The result represented 91.5% less CPU cycles required for hardware encryption.

100% SEQUENTIAL READ CPU UTILIZATION
HW Encryption vs SW Encryption = -91.5%
HW Encryption vs No Encryption = -0.1%

Workload B: 100% Sequential Write

When 100% sequential write operations were tested, the CM6 Series SSDs with hardware encryption enabled delivered 11,000 MB/s. In comparison to software encryption at 3,600 MB/s, hardware encryption had a 205% improvement in sequential write operations. There was only a 1.8% difference in sequential write performance between hardware encryption and no encryption at all.

100% SEQUENTIAL WRITE
HW Encryption vs SW Encryption = +205%
HW Encryption vs No Encryption = -1.8%

For CPU utilization, hardware encryption enabled and no encryption delivered comparable results, 1.7% and 1.5% respectively, and no practical difference in CPU utilization. When software encryption was enabled, CPU utilization increased dramatically to 77.1%. The result represented 75.4% less CPU cycles required for hardware encryption.

100% SEQUENTIAL WRITE CPU UTILIZATION
HW Encryption vs SW Encryption = -75.4%
HW Encryption vs No Encryption = +0.2%

Workload C: 100% Random Read

When 100% random read operations were tested, the CM6 Series SSDs with hardware encryption enabled delivered 3,595,000 IOPS. In comparison to software encryption at 882,000 IOPS, hardware encryption had a 307% improvement in random read operations. There was only a 2% difference in random read performance between hardware encryption and no encryption at all.

100% RANDOM READ
HW Encryption vs SW Encryption = +307%
HW Encryption vs No Encryption = +2%

For CPU utilization, hardware encryption enabled and no encryption delivered comparable results, 88% and 87% respectively, and no practical difference in CPU utilization. When software encryption was enabled, CPU utilization increased dramatically to 99.8%. The result represented 11.8% less CPU cycles required for hardware encryption.

100% RANDOM READ CPU UTILIZATION
HW Encryption vs SW Encryption = -11.8%
HW Encryption vs No Encryption = +1%

Workload D: 100% Random Write

When 100% random write operations were tested, the CM6 Series SSDs with hardware encryption enabled delivered 319,000 IOPS. In comparison to software encryption at 141,000 IOPS, hardware encryption had a 126% improvement in random write operations. There was a very small difference of 0.3% in random write performance between hardware encryption and no encryption at all.

100% RANDOM WRITE
HW Encryption vs SW Encryption = +126%
HW Encryption vs No Encryption = -0.3%

For CPU utilization, hardware encryption enabled and no encryption delivered equal results at 21% and no practical difference in CPU utilization. When software encryption was enabled, CPU utilization increased dramatically to 99.8%. The result represented 78.8% less CPU cycles required for hardware encryption.

100% RANDOM WRITE CPU UTILIZATION
HW Encryption vs SW Encryption = -78.8%
HW Encryption vs No Encryption = 0%

Findings: From the test results and analysis, systems and applications that use SSDs incorporating encryption with the TCG-OPAL standard can provide encryption protection for data-at-rest without a performance hit. Regardless of whether hardware encryption was enabled or disabled, there was almost no deviation of the drive performance across all four tests run during the testing process.

CM6 Series SSD Overview

As KIOXIA's 6th generation enterprise-class NVMe SSD product line, the CM6 Series features significantly improved performance from PCIe Gen3 to PCIe Gen4, 30.72TB maximum capacity, dual-port for high availability, 1 DWPD for read-intensive applications (CM6-R Series) and 3 DWPD for mixed use applications (CM6-V Series), and up to 6 power settings and security options – all of which are geared to support a wide variety of workload requirements.

The CM6 Series SSD architecture has encryption built into the data path so as the drive is reading and writing from NAND flash memory, the encryption or decryption is performed in a way that it has no material impact to performance under most conditions[13].

CM6 Series SSDs
PCIe 4.0 and NVMe 1.4 Specification Compliant

High-Performance[14]
SeqRead = up to 6,900MB/s
RanRead = up to 1.4M IOPS
SeqWrite = up to 4,200MB/s
RanWrite+ up to 350K IOPS

Configurable Flexibility
1 and 3 DWPD options
800GB - 30,720GB capacities

Summary

Now more than ever, encryption has become more important than ever to secure data and an ideal encryption solution is one that does not impact application or system performance. If a server is using software encryption, and is utilized for any Input/Output (I/O) operation, the test results indicate substantial performance degradation and high CPU utilization dedicated to encryption activities. Best results were seen when hardware encryption is used. When software encryption is deployed, encryption operations can consume 80+% of the CPU, which is essentially dedicating a server for these operations.

The demonstrated approach to encrypt/decrypt data is drive-level encryption. KIOXIA CM6 Series SSDs offer hardware encryption, eliminating the need for resource-heavy software or file system level encryption of data-at-rest. These SSDs support TCG-Opal and Ruby SSCs and utilize security modules designed to comply with FIPS 140-2 Level 2 and FIPS 140-3 Level 2, and encrypt/decrypt data without performance degradation or impact on system resources. As the tests indicate, the CM6 Series SSDs performed workload encryption significantly faster than software encryption. This enables IT departments to get the most out of their storage or system investment where encryption workloads are added to the workload mix without impacting application or system performance.

Bottom line: For encryption / decryption related tasks, hardware-accelerated encryption such as the KIOXIA CM6 Series SSDs do not impact CPU resources or performance, deliver higher levels of data security, as well as maximum performance per dollar.

ADDENDUM

How to Setup Software Encryption and Hardware Encryption

For our readers who would like to replicate these encryption tests, the following are the setup procedures for enabling both software encryption and hardware encryption using software SED utilities.

Create a Multiple Device RAID (mdraid) Set

Zero the superblock to make sure it does not have a residual RAID set:
mdadm --zero-superblock /dev/nvme0n1 /dev/nvme1n1 /dev/nvme2n1 /dev/nvme3n1

Create the MDADM RAID volume on the four CM6 Series drives:
mdadm -C /dev/md0 --assume-clean -l raid0 -n 4 /dev/nvme0n1 /
dev/nvme1n1 /dev/nvme2n1 /dev/nvme3n1

Software Encryption Setup

Create a Key Storage Location and Enter the Directory

mkdir keys
cd keys

Create the Key:
fallocate -l 2M crypt2.img

Setup LUKS Encryption on the Volume:
cryptsetup luksFormat /dev/md0 --header crypt2.img
cryptsetup open --header crypt2.img /dev/md0 cryptvol
ls /dev/mapper/cryptvol

Remove the Encrypted Volume and mdraid Volume:

To remove the encrypted volume and mdraid volume:
cryptsetup remove /dev/mapper/cryptvol

Stop the mdraid Volume:
mdadm --stop /dev/md0

Remove RAID configuration:
mdadm --zero-superblock /dev/nvme0n1 /dev/nvme1n1 /dev/nvme2n1 /dev/nvme3n1

Hardware Encryption Setup

The SED utilities (sedutil) enables hardware encryption inside the CM6 Series SSD via a command line on the server -- #set up sedutil-cli.

Install Git, Make Clean and g++:

To Install Git:
sudo apt install git make g++ -y

Use Git to download the sedutil software:
sudo git clone https://github.com/Drive-Trust-Alliance/sedutil.git
cd sedutil

To Install and Setup sedutil:
autoreconf -i
./configure --enable-silent-rules
make clean
make
make install
sudo nano /etc/default/grub
#add “GRUB_CMDLINE_LINUX_DEFAULT=”quiet splash libata.allow_tpm=1”
sudo update-grub
sudo reboot

Setup CM6 Series Drives with SED Utilities
(Turn on encryption at the hardware level)

NOTE: *The PSID is available from the drive label and must be used to erase all of the drives first BEFORE running the commands below.*

sedutil-cli --yesIreallywanttoERASEALLmydatausingthePSID <PSID> /dev/nvme1n1
sedutil-cli --yesIreallywanttoERASEALLmydatausingthePSID <PSID> /dev/nvme2n1
sedutil-cli --yesIreallywanttoERASEALLmydatausingthePSID <PSID> /dev/nvme3n1
sedutil-cli --yesIreallywanttoERASEALLmydatausingthePSID <PSID> /dev/nvme4n1

Enable Hardware SSD Encryption via sedutil-cli

To enable hardware SSD encryption as root via sedutil-cli:

```
sedutil-cli --scan

sedutil-cli --query /dev/nvme1
sedutil-cli --query /dev/nvme2
sedutil-cli --query /dev/nvme3
sedutil-cli --query /dev/nvme4

sedutil-cli --initialsetup <password> /dev/nvme1
sedutil-cli --initialsetup <password> /dev/nvme2
sedutil-cli --initialsetup <password> /dev/nvme3
sedutil-cli --initialsetup <password> /dev/nvme4

sedutil-cli --enableLockingRange 0 <password> /dev/nvme1
sedutil-cli --enableLockingRange 0 <password> /dev/nvme2
sedutil-cli --enableLockingRange 0 <password> /dev/nvme3
sedutil-cli --enableLockingRange 0 <password> /dev/nvme4
```

Lock SSDs

(No reads or writes can be performed)

To lock the drives:

```
sedutil-cli --setLockingRange 0 LK <password> /dev/nvme1
sedutil-cli --setLockingRange 0 LK <password> /dev/nvme2
sedutil-cli --setLockingRange 0 LK <password> /dev/nvme3
sedutil-cli --setLockingRange 0 LK <password> /dev/nvme4
```

Unlock SSDs

(Reverts back to provide read or write access)

To unlock the drives:

```
sedutil-cli --setLockingRange 0 RW <password> /dev/nvme1
sedutil-cli --setLockingRange 0 RW <password> /dev/nvme2
sedutil-cli --setLockingRange 0 RW <password> /dev/nvme3
sedutil-cli --setLockingRange 0 RW <password> /dev/nvme4
```

Test Read / Write for Locking
(Tests read or write locking)

To test write locking:

```
nvme write /dev/nvme1n1 -s 0x0000 -c 0x0000 -z 512 -d 512x10.bin
nvme write /dev/nvme2n1 -s 0x0000 -c 0x0000 -z 512 -d 512x10.bin
nvme write /dev/nvme3n1 -s 0x0000 -c 0x0000 -z 512 -d 512x10.bin
nvme write /dev/nvme4n1 -s 0x0000 -c 0x0000 -z 512 -d 512x10.bin
```

To test read locking:

```
nvme read /dev/nvme1n1 -s 0x0000 -c 0x0000 -z 512 | hexdump -C
nvme read /dev/nvme2n1 -s 0x0000 -c 0x0000 -z 512 | hexdump -C
nvme read /dev/nvme3n1 -s 0x0000 -c 0x0000 -z 512 | hexdump -C
nvme read /dev/nvme4n1 -s 0x0000 -c 0x0000 -z 512 | hexdump -C
```

Once the CM6 Series SSDs are encrypted and set in a read/write state, they can be used in their normal manner. The RAID set can now be configured, formatted and mounted for production workloads.

Clean the SSDs after Testing

To clean the drives after testing:

Revert to a No Erase Password:

```
sedutil-cli --revertNoErase <password> /dev/nvme1
sedutil-cli --revertNoErase <password> /dev/nvme2
sedutil-cli --revertNoErase <password> /dev/nvme3
sedutil-cli --revertNoErase <password> /dev/nvme4
```

Revert to an Erase Password:

```
sedutil-cli --revertTPer <password> /dev/nvme1
sedutil-cli --revertTPer <password> /dev/nvme2
sedutil-cli --revertTPer <password> /dev/nvme3
sedutil-cli --revertTPer <password> /dev/nvme4
```

NOTES:

[1] Self-Encrypting Drives encrypt all data to SSDs and decrypt all data from SSDs, via an alphanumeric key (or password protection) to prevent data theft. It continuously scrambles and descrambles data written to and retrieved from SSDs.

[2] The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology in 2001.

[3] In support of the SED (TCG-Opal/Ruby) security options, some features may not be supported.

[4] The TCG-Opal Security Subsystem Class (SSC) is a set of specifications for SEDs developed by the Trusted Computing Group (TCG), a non-profit organization that develops, defines, and promotes open standards and specifications for secure computing.

[5] FIPS 140-2 Level 2 and FIPS 140-3 Level 2 define security requirements for cryptographic modules by the U.S. National Institute of Standards and Technology (NIST) Cryptographic Security Requirements, and available at: https://csrc.nist.gov/publications/detail/fips/140/2/final.

[6] Flexible I/O (FIO) is a free and open source disk I/O tool used both for benchmark and stress/hardware verification. The software displays a variety of I/O performance results, including complete I/O latencies and percentiles.

[7] Definition of capacity - KIOXIA Corporation defines a kilobyte (KB) as 1,000 bytes, a megabyte (MB) as 1,000,000 bytes, a gigabyte (GB) as 1,000,000,000 bytes and a terabyte (TB) as 1,000,000,000,000 bytes. A computer operating system, however, reports storage capacity using powers of 2 for the definition of 1Gbit = 2^{30} bits = 1,073,741,824 bits, 1GB = 2^{30} bytes = 1,073,741,824 bytes and 1TB = 2^{40} bytes = 1,099,511,627,776 bytes and therefore shows less storage capacity. Available storage capacity (including examples of various media files) will vary based on file size, formatting, settings, software and operating system, and/or pre-installed software applications, or media content. Actual formatted capacity may vary.

[8] 2.5-inch indicates the form factor of the SSD and not the drive's physical size.

[9] Drive Write(s) per Day: One full drive write per day means the drive can be written and re-written to full capacity once a day, every day, for the specified lifetime. Actual results may vary due to system configuration, usage, and other factors.

[10] MDADM is a standard Linux® operating system tool that manages and monitors software RAID sets and devices.

[11] LUKS or Linux Unified Key Setup is a standard software encryption tool for SSDs and a kernel module that handles encryption at the block device level.

[12] The Self Encrypting Drive Utility (SEDutil) is an open source set of tools that provides locking and unlocking of TCG-OPAL 2.0 boot and non-boot drives in Windows® and Linux operating systems, and available at https://sedutil.com/#:~:text=SEDutil%20is%20an%20open%20source,drives%20in%20Windows%20and%20Linux.

[13] Variances in individual test queries may occur in normal test runs. Average performance over time was consistent for encryption enabled and encryption disabled.

[14] Read and write speed may vary depending on the host device, read and write conditions, and the file size.

Trademarks:

AMD EPYC is a trademark of Advanced Micro Devices, Inc. Dell, Dell EMC and PowerEdge are either registered trademarks or trademarks of Dell Inc. Linux is a registered trademark of Linus Torvalds. NVMe is a registered trademark of NVM Express, Inc. PCIe is a registered trademark of PCI-SIG. Ubuntu is a registered trademark of Canonical Ltd. Windows is a registered trademark of Microsoft Corporation in the United States and/or other countries. All company names, product names and service names may be the trademarks of their respective companies.

Disclaimers:

 Information in this white paper, including product specifications, tested content, and assessments are current and believed to be accurate as of the date that the document was published, but is subject to change without prior notice. Technical and application information contained here is subject to the most recent applicable KIOXIA product specifications.