Next-Generation Dell EMC® PowerEdge™ Servers Deliver Encryption Protection without a Performance Hit Using KIOXIA PCIe® 4.0 NVMe® SSDs

Tech Note by

Seamus Jones
Technical Marketing Engineer, Dell

Mohan Rokkam
Technical Marketing Engineer, Dell

Tyler Nelson
Sr. Manager, Application Performance Lab, KIOXIA

Adil Rahman
Application Performance Lab Engineer, KIOXIA

Summary

This document is a summary of the performance comparison between SSDs that use encryption enabled vs. encryption disabled in a Dell PowerEdge server with PCIe 4.0 technology.

All performance and characteristics discussed are based on performance testing conducted in the Americas Data Center (CET) labs.

Results are accurate as of 5/1/21.

Ad Ref #PROJ-000072

Introduction

Data encryption has been used for decades in data center computing environments to protect both data in transit and data at rest. In these environments, clients generate data continuously (24 hours per day, 7 days per week), and data collection continues to grow. This massive data generation comes from many different client devices such as desktops and laptops, smartphones and tablets, as well as IoT devices such as robots, drones, machines, and surveillance cameras, whether on-premises or 'at-the-edge' of the data center network (where data is captured and processed).

Massive data generation makes it more important than ever for companies to protect what they've captured both for short-term use and archival purposes, especially with technologies like artificial intelligence (AI) and machine learning (ML) that can help maximize the value of captured/archived data. Companies are turning more to encrypting data stored in their data centers to protect business-critical and sensitive information from unauthorized parties and hackers.

With each new generation of hardware and software that is produced, coupled with the exponential growth of data, it is critical for encryption methods to keep pace with technological advances. An ideal solution is to enable encryption so that access speed is comparable as if encryption was disabled, thereby delivering optimal system performance. The ability to protect data through encryption without experiencing performance degradation is the basis of this brief.

Data Encryption Performance Issues

Data encryption is the process of taking digital content (such as a document or email) and translating it into an unreadable format so that clients with a 'secret key' or password are the only ones that can view, access or read it. This helps protect the confidentiality of digital data stored on computer systems or transmitted over wireless networks and the Internet. A good example is when a smartphone is used for an ATM transaction or online purchase - encryption protects the information being transmitted.

Being a calculation-intensive operation, encryption is limited in use because of the amount of time and CPU cycles which can be lost to encrypting and decrypting data. These limitations may cause reduced system and application-level performance challenges that not only affect the applications themselves, but also the customer experience. To reduce CPU cycles being used for encryption, storage manufacturers have created devices that support encryption protocols inside of the drive itself. These drives are called Self Encrypting Drives[1] (SEDs).

An SED implements on-board crypto-processers and uses an AES[2]-256 cryptographic module and media encryption key to encrypt plain-text data traversing through the SSD to the media inside of the SSD itself. This process ensures that data at rest is encrypted at a hardware layer to prevent unauthorized access.

System and Application Test Scenario

Mainstream servers and SSDs deployed with the PCIe 4.0 interface and NVMe protocol are becoming commercially available and typically deliver significant performance advantages over previous PCIe interface generations. Given the importance of encryption, delivering a solution that provides this capability without compromising performance was an SSD design goal for KIOXIA.

To find out if encryption leads to a performance hit, KIOXIA conducted transactions per minute (TPM) tests in a Dell® PCIe 4.0 server lab environment with and without encryption enabled. The test configuration included a Dell EMC PowerEdge R7525 rack server (with 3rd generation AMD EPYC™ CPUs) deployed with KIOXIA CM6 Series PCIe 4.0 enterprise NVMe SSDs that support the TCG-OPAL[3] specification for SEDs. During the initial server boot-up, hardware level encryption was enabled throughout the BIOS on a Dell PowerEdge RAID Card (PERC) Model H755N. The 'logical volume' was created as an 'encrypted volume' that enables TCG-OPAL encryption across the KIOXIA CM6 Series SSDs, also creating a secured logical device.

The tests utilized an operational, high-performance Microsoft® SQL Server™ database workload based on comparable TPC-C™ benchmarks created by HammerDB software[4]. Supporting details include a description of the benchmark test criteria and the set-up and associated test procedures, as well as a visual representation of the test results, and a test analysis.

The test results provide a real-world scenario of the effects that encryption has on TPM performance when running a Microsoft SQL Server database using comparable equipment and performing queries against it. In this test configuration, a Dell EMC PowerEdge 7525 server utilizes KIOXIA CM6 Series enterprise SSDs when running this database application to demonstrate performance of a system with and without data encryption.

Test Criteria:
The hardware and software equipment used for these encryption tests included:

- **Dell R7525 Server:** One (1) dual socket server with two (2) AMD EPYC 7352 processors, featuring 24 processing cores, 2.3 GHz frequency, and 240 gigabytes[5] (GB) of DDR4 RAM
- **Operating System:** Microsoft Windows® Server 2019
- **Application:** Microsoft SQL Server 2019.150.1600.8 – Database size of 440GB
- **Test Software:** Comparable TPC-C benchmark tests generated through HammerDB v4.0 test software

- **PCIe 4.0 NVMe RAID Card:** Dell PERC H755N
- **Storage Devices** (Table 1)**:** Three (3) KIOXIA CM6-R Series PCIe 4.0 NVMe SSDs with 1.6 terabyte[5] (TB) capacities

Specifications	CM6-R Series
Interface	PCIe 4.0 NVMe U.3
Capacity	1.6TB
Form Factor	2.5-inch[6] (15mm)
NAND Flash Type	BiCS FLASH™3D flash memory
Drive Writes per Day[7] (DWPD)	3 (5 years)
Power	18W
DRAM Allocation	96GB

Table 1: SSD specifications and set-up parameters

Set-up & Test Procedures

Set-up: The test system was configured using the hardware and software equipment outlined above. An unsecured RAID5 set was created on the Dell H755N PERC using three (3) CM6-R Series SSDs with the SED option. RAID5 was selected because it is commonly used in data center environments. Once the SSD array was initialized, the RAID5 set was formatted to a Microsoft Windows NT file system (NTFS). The Microsoft SQL Server application was then installed and limited to 96GB of memory. A 440GB database was then loaded using HammerDB test software.

Test Procedures: The first test was run ***with encryption disabled***. The comparable TPC-C workload utilized HammerDB software to run the test. The three (3) KIOXIA CM6-R Series SSDs were placed into a RAID5 set and the test was conducted with encryption disabled. Multiple iterations of the test were run on both configurations to determine an optimal configuration of virtual users. Both test scenarios showed the highest TPM performance when running a configuration of 480 virtual users. *See Test Results section.*

The second test was then run ***with encryption enabled***. The RAID5 set was destroyed and a secure RAID5 set based on the TCG-OPAL specification was created. The three (3) KIOXIA CM6-R Series SSDs were placed into the secure RAID5 set and the same test was conducted with encryption enabled. The objective of this test was to showcase how the application and system provide the same level of performance whether data was encrypted or unencrypted. The comparable TPC-C workload was run using HammerDB test software. The same test process for this configuration was repeated to obtain the TPM performance results with encryption enabled. *See Test Results section.*

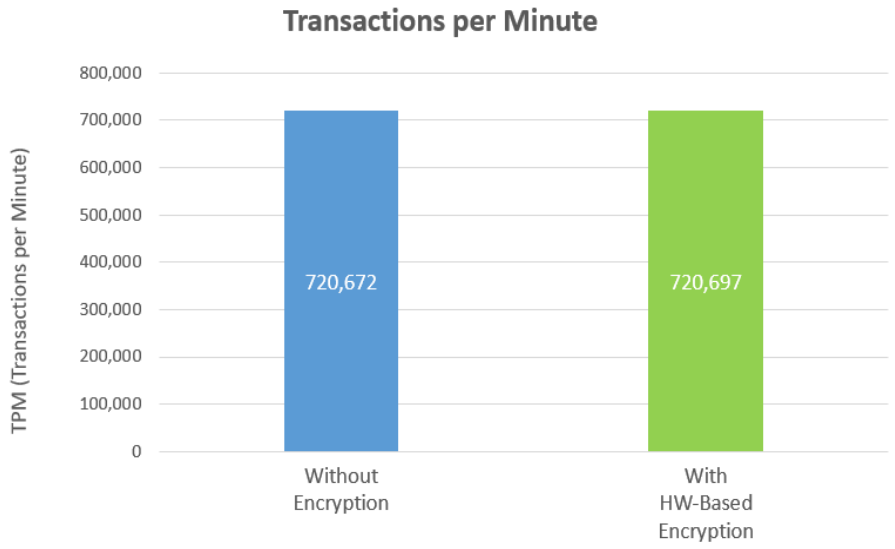
The TPM tests were conducted, with and without encryption enabled, with the performance result recorded. As it relates to TPM, the higher the test value, the better the result.

The CPU utilization tests were also conducted, with and without encryption enabled, with the result recorded. In this test instance, the lower the test value, the better the utilization.

Transactions Per Minute

In an Online Transaction Processing (OLTP) database environment, TPM is a measure of how many transactions in the TPC-C transaction profile are being executed per minute. HammerDB software, executing the HammerDB TPC-C transaction profile, randomly performs new order transactions and randomly executes additional transaction types such as payment, order status, delivery and stock levels. This benchmark simulates an OLTP environment where there are a large number of users that conduct simple, yet short transactions that require sub-second response times and return relatively few records. The TPM test results:

CM6-R Series Tests: SQL Server Comparable TPC-C Workload	Without Encryption	With Encryption
Transactions per Minute	720,672	720,697
Performance Difference	-	**0%**

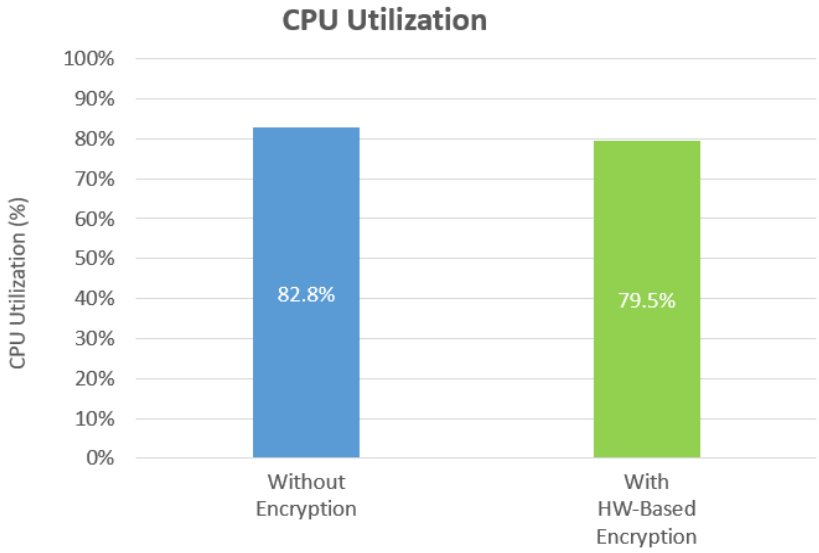


In both test cases, the margin of deviation when measuring the TPM, with or without encryption, was close to 0%, which implies no discernable difference in application level performance between the two approaches.

CPU Utilization

In general, CPU utilization represents a percentage of the total amount of computing tasks that are handled by the CPU, and is another estimation of system performance. Some forms of encryption require CPU cycles to encrypt and decrypt data on the storage media itself which can lead to a performance impact. For these tests, CPU utilization was measured to ensure the CPU was not incurring any extra processing for encryption, which should be handled in hardware at the RAID controller and SSD levels. The hardware based configuration from Dell with KIOXIA CM6-R Series SSDs enables the R7525

server CPU to be utilized for compute tasks instead of encryption. The graphs below show the CPU utilization was comparable (82.8% utilization without encryption and 79.5% utilization with encryption):



Test Analysis

The test results validated that KIOXIA CM6-R Series SSDs enabled the Dell R7525 rack server to deliver nearly identical TPM performance whether encryption was enabled or not. This particular PCIe 4.0 NVMe server/storage configuration was able to deliver more than 720,000 TPM without any TPM-related performance degradation regardless of encryption being enabled or disabled. As a result, systems and applications that use SSDs based on the TCG-OPAL standard are enabled to utilize the CPU for performance tasks instead of encryption tasks.

Whether hardware encryption was enabled or disabled, there was about 3% deviation of the CPU utilization during the testing process which demonstrated that the CPU wasn't processing any extra workloads for encryption.

CM6 Series SSDs

PCIe 4.0 and NVMe 1.4 Specification Compliant

High-Performance[8]

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

CM6 Series SSD Overview

The CM6 Series is KIOXIA's 3rd generation enterprise-class NVMe SSD product line that 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), up to a 25-watt power envelope and a host of 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[9].

Summary

Encryption becomes more important than ever to secure data. An ideal encrypted solution does not impact application or system performance. The test results presented validate that a PowerEdge R7525 PCIe 4.0 enabled server with KIOXIA CM6-R Series SSDs effectively delivered identical TPM performance of more than 720,000 TPM, whether encryption was enabled or not. As data usage scales over time, performance is not affected by encryption no matter how much data is being encrypted at rest.

CPU utilization was also comparable with or without encryption enabled which validated that the CPU (at approximately 80% utilization) was not impacted when encryption was enabled.

The Dell EMC and KIOXIA server solution delivered encryption protection without a performance hit!!!

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] Developed by the Trusted Computing Group (TCG), a not-for-profit international standards organization, the OPAL specification is used for applying hardware-based encryption to solid state drives and often referred to as TCG-OPAL.

[4] HammerDB is benchmarking and load testing software that is used to test popular databases. It simulates the stored workloads of multiple virtual users against specific databases to identify transactional scenarios and derive meaningful information about the data environment, such as performance comparisons. TPC Benchmark C is a supported OLTP benchmark that includes a mix of five concurrent transactions of different types, and nine types of tables with a wide range of record and population sizes and where results are measured in transactions per minute.

[5] Definition of capacity - KIOXIA Corporation defines 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.

[6] 2.5-inch indicates the form factor of the SSD and not the drive's physical size.

[7] 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.

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

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

Trademarks

Disclaimers