Overcoming performance obstacles in data encryption

Using IBM InfoSphere Guardium Data Encryption with Intel® AES-NI technology helps protect sensitive data while sustaining application performance

Data security breaches can be disastrous for any organization. Unauthorized access to stored credit card numbers, patient information, intellectual property, or other sensitive information can cost businesses and their customers money, ruin reputations, and jeopardize compliance with government regulations.

Encrypting data on enterprise servers—where the majority of sensitive data resides—can help organizations prevent those disasters. By encrypting data, organizations can increase their chances of avoiding damaging headlines, prevent extended and expensive compliance investigations, and qualify for regulatory safe harbor provisions that do not require disclosures of breaches with encrypted data.

In the past, the potential performance impact of encryption on enterprise applications discouraged organizations from encrypting some or all of their data. However, new benchmark test results show that by combining the IBM® InfoSphere® Guardium® Data Encryption solution, which is based on Vormetric® Encryption software, with the Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) available for Intel® Xeon® processor families, enterprises can dramatically reduce the processing requirements for encryption. The result: enhanced data protection with minimal impact to application performance.

Accelerating data encryption with IBM and Intel solutions

IBM DB2® offers numerous features and IBM InfoSphere Guardium Data Encryption offers a comprehensive encryption solution for data at rest. Operating above the file level, the solution can encrypt structured and unstructured data across a heterogeneous IT infrastructure. By providing policy-based access controls, separation of duties, and auditing capabilities from a single centralized management console, the solution can help reduce the time and costs of managing encryption and achieving compliance.

Running this solution on servers equipped with Intel® Xeon® processor E5 and E7 families, such as the latest-generation IBM System x® servers, enables organizations to take advantage of the Intel AES-NI capabilities built into those processors. Intel AES-NI is a set of seven new instructions in the Intel Xeon processor that help accelerate encryption, decryption, key generation, matrix manipulation, and carry-less multiplication. By implementing complex and costly sub-steps of the AES algorithm in hardware, Intel AES-NI speeds the execution of the AES-based encryption. By delivering faster, more secure encryption while minimizing performance overhead, Intel AES-NI makes encryption feasible where it was not before. Intel AES-NI can dramatically accelerate AES encryption performance by more than eight times and decryption by 33 times compared with software-only approaches.[1]

Minimizing the performance impact with Intel AES-NI

A recent TPoX (Transaction Processing over XML) benchmark test conducted by Intel demonstrates the substantial performance improvements that this combination of technologies can deliver.[2] The test measured

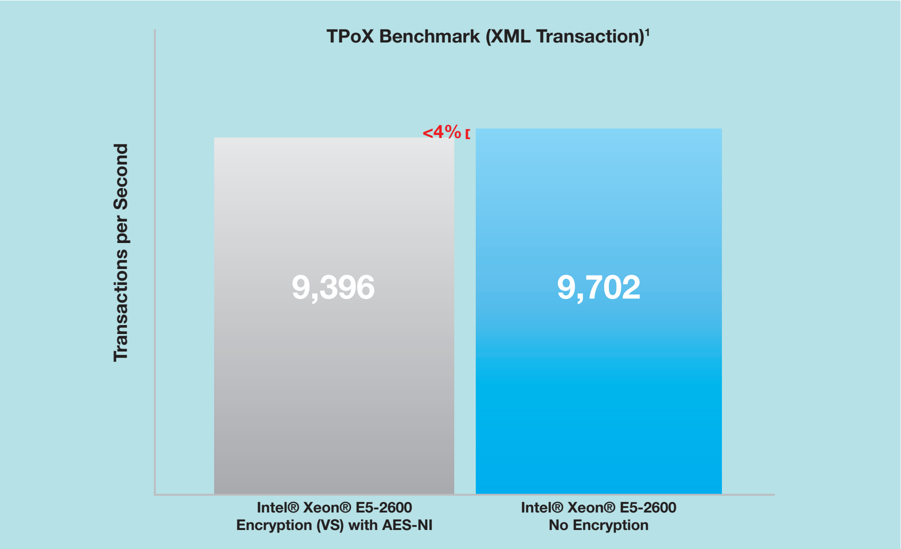

Figure 1: Benchmark testing showed minimal performance impact for data encryption when using Intel® AES-NI capabilities.

transaction-per-second performance of a server equipped with Intel Xeon processor E5 family and built-in Intel AES-NI capabilities encrypting an IBM DB2 database with IBM InfoSphere Guardium Data Encryption, which is built on Vormetric Encryption technology. Compared with a similarly configured server that was not encrypting data, the encrypting server delivered less than 4 percent fewer transactions per second at peak system performance. In other words, the performance overhead for encrypting this mission-critical workload at heavy system utilization was almost negligible.

Running the TPoX benchmark using the Intel Xeon processor E7 family delivered comparable results.

Protecting more data and increasing ROI

For organizations that already encrypt data, using the IBM InfoSphere Guardium Data Encryption solution in conjunction with Intel AES-NI capabilities can help accelerate application performance. In the case of database transaction processing, for example, businesses could support more users and deliver improved response times.

Dramatically reducing the performance penalty for encryption should encourage organizations to encrypt more data than before. Rather than restricting encryption to financial data, for example, and leaving e-mails unencrypted, organizations can tighten security for a broader range of sensitive information.

In virtualized server environments, reducing the processing performance required for encryption will also free up server resources for running additional workloads on each physical server. These technologies will help organizations protect information while maximizing the return on their hardware investments.

Intel AES-NI capabilities were introduced with Intel® Xeon® processor 5600 series in 2010, so many organizations with existing Intel Xeon processor–based servers already have access to Intel AES-NI capabilities. Servers based on the current generation of the Intel Xeon processor E5 and E7 families provide enhanced AES-NI performance. Using InfoSphere Guardium Data Encryption with those servers will enable organizations to enhance protection through data encryption while delivering exceptional application performance.

To learn more about IBM InfoSphere Guardium Data Encryption, contact your IBM sales representative or IBM Business Partner, or visit: **ibm.com/software/data/guardium/encryption-expert**

To learn more about Vormetric Encryption, visit: **vormetric.com/products/encryption/index.html**

For more information about Intel AES-NI, visit: **intel.com/technology/security**

[1] See "Improving OpenSSL Performance," October 2011, http://download.intel.com/design/intarch/papers/326232.pdf.

[2] The testing environment used a 64-bit SuSE Linux Enterprise 11, SP1 operating system; IBM DB2 9.7; Vormetric Encryption V4.4 without Intel AES-NI support; Vormetric Encryption V5 with Intel AES-NI support; and TPoX 2.0. Transactions per second measured with Intel Xeon processor E5-2690 (2.9 GHz). Data points were obtained at same load, same memory capacity, and same storage.

Disclaimer: Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as TPoX, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. Intel® AES-NI requires a computer system with an AES-NI enabled processor, as well as non-Intel software to execute the instructions in the correct sequence. AES-NI is available on select Intel® processors. For availability, consult your reseller or system manufacturer. For more information, see Intel® Advanced Encryption Standard Instructions (AES-NI).