Cloudera Hadoop* Single-Node Encryption Performance Case Study on Intel® Xeon® E5-2600 v3 Product Family

Cloudera software, specifically in its distribution of Hadoop*, Navigator Encrypt*, provides transparent data encryption and key management to secure sensitive data at rest. Cloudera solutions are in place at some of the world’s largest financial institutions, healthcare organizations, and retailers to protect personally identifiable information, corporate IP, and other sensitive data that may be subject to federal, industry, or internal compliance.

When processing and storing large amounts of sensitive data, any performance gain quickly converts to faster results, lower power costs, and less resource utilization. For organizations to stay competitive, any of these factors can provide the edge they need. This case study, authored by Eddie Garcia, Cloudera chief security architect, explains how its data security solutions leverage the Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) included in the 4th generation Intel® Core™ processor family (codenamed Haswell) and available on the Intel® Xeon® E5-2600 v3 product family and the next generation Intel® Xeon® E7 family (codenamed Haswell-EX), to enhance encryption performance. This case study includes how Intel® Solid-State Drive P3700 series [1] storage can be used to improve I/O throughput and performance.

Why encrypt your data?

We see data breaches in the news all the time: credit card numbers, passwords, social security numbers, email addresses and even selfies are being stolen. For large organizations, such thefts may cost millions of dollars and, even worse, an organization’s reputation, brand, and bottom line.

Information security is all about layers. There is no silver bullet to protect all data, so the next best thing is to make breaches as difficult as possible. Reducing the exposure to hackers through multiple security layers and making the cost of getting to the data more expensive are often more costly than the value of the data itself.

Encryption has been used for centuries to protect data from those not authorized to view it. Today data encryption is a well-known method to protect data in all types of devices from smartphones and laptops to hard drives.

Data is growing at a rate never seen before: every 6 months we are generating more data than the rest of the previous years combined starting with the first bit stored on a computer tape. With
such an explosion of data it is certain that not all the needed controls are in place to protect this
data. Every day, people are more concerned about who has their data and how it is being used,
from their personal habits to their financial and health records.

It is not a surprise that many security conscious organizations are starting to encrypt their data.
Many do so because they want to lower their risk and protect their data, while others do it as a
matter of policy and regulatory compliance.

**Intel® Advanced Encryption Standard New Instructions Basics**

The Advanced Encryption Standard, or AES, is one of many cryptographic algorithms. Good
cryptographic algorithms are those that are very expensive to attack with brute force and very
inexpensive to use in terms of performance overhead. AES has both of these characteristics and
for that reason it is widely adopted and used behind the scenes in things you may do on a daily
basis like login to your laptop, make a purchase online, or even swipe a security card.

Encryption comes with a price in terms of performance. Encryption is never free, but getting it as
free as possible is good. Intel recognized this and introduced Intel Advanced Encryption Standard
New Instructions (Intel AES-NI) [see Note 1], which is a hardware implementation of math
functions used by AES that improves the performance of encrypting and decrypting data faster
than in software. Intel AES-NI is not new to the 4th gen Intel Core microarchitecture, but an array
of other enhancements and math instructions on this latest processor generation make encryption
even faster than on the previous generation.

AES is used with what we call symmetric keys, much like traditional door locks where you have a
key that can both open or close a lock. This is in contrast to more specialized keys that can only
be used to either lock or unlock.

AES in its most basic form applies a symmetric key to a block of data the same size as the key,
and it generates an encrypted block of equal size as output. An encrypted file consists of
hundreds, thousands, or millions of these encrypted blocks. The larger the key, the more difficult
it is for a hacker to try combinations of keys that can unlock the data. The downside is that using
larger keys results in slower encryption and decryption of data.

Intel AES-NI allows organizations to encrypt data faster using stronger and larger keys with the
least amount of performance overhead. In the following section are some results using encryption
on Intel AES-NI, comparing the latest generation Intel® Xeon® E5-2600 v3 processors to the
Intel® Xeon® E5-2600 v2 processors. We will also touch on the performance improvements
when using Intel data storage on solid-state drives.
Cloudera Hadoop data-at-rest encryption

Cloudera Navigator Encrypt is a transparent data encryption solution that takes advantage of the Intel AES-NI to boost performance.

To encrypt and decrypt data, Navigator Encrypt generates a 256-bit encryption key and calls the Intel AES-NI instruction with this key to encrypt/decrypt data. Cloudera Navigator Encrypt also relies on good entropy (randomness) to generate a strong encryption key, such as that available from the RDRAND instruction found in Intel® Data Protection Technology with Intel® Secure Key. For more information on RDRAND and this technology refer to https://software.intel.com/en-us/articles/intel-data-protection-technology-with-secure-key-gazzang-use-case-study.

Hadoop performance testing

Hadoop comes with some built-in performance tests, and while some may argue that these tests are not representative of real-world workloads, they are helpful when comparing two systems against each other. These measurements are much like a car's published top speed or sticker fuel consumption, which may not be representative of your use, but are good reference points when comparing one car to another.

We chose two Hadoop performance tests, TestDFSIO and TeraSort, to measure performance in different areas. TestDFSIO is more storage I/O- and throughput-focused, while TeraSort is representative of running a workload that is not only I/O- but also CPU-intensive. Both of these tests use the Hadoop distributed file system (HDFS). We ran the tests comparing encrypted data in different configurations.

Performance test procedure

To eliminate some of the noise that can be generated in performance tests, each test was executed 3 times and all 3 runs had to have similar results; otherwise, the test was run again until results were conclusive. On each run, data was cleared to prevent any caching, ensuring the configuration remained fairly static with no keyboard or mouse connected, no additional services running, and no external network activity. Even then, we still encountered some variances.

The tests were executed on a single node server. While we would never find a production Hadoop single node cluster, a single node reduces variables in our configuration to focus on the minimal system changes when comparing one test’s result to another.

Test environment software

The tests were run on the Cloudera 5.2 distribution of Hadoop. The test configuration uses Red Hat* Enterprise Linux* 7 [2], the Sun Java* Development Kit 1.8, and OpenSSL* 1.02. These software versions make calls to Intel AES-NI taking advantage of the most current hardware optimizations. While this configuration is not one officially supported by Cloudera as of the writing
of this article, these tests demonstrate the latest and greatest results on not yet publicly available configurations. RNGD 5 (rng-tools version 5) was used to generate entropy, also taking advantage of the RDRAND instruction in Intel Secure Key.

Test environment hardware

The tests were run on Intel® Xeon® processor E5-2699 v3 (18 core) and E5-2697 v2 (12 core) servers. Both systems are equipped with two CPUs and the same amount of RAM and software configuration. While the latest E5-2699 v3 has more cores, it is representative of what you would find replacing the previous E5-2697 v2 for the server model out in the market.

Test results

Intel® Xeon® Processor E5-2699 v3 and E5-2697 v2

The TeraSort test was configured to sort 50GB of encrypted data stored in HDFS. The input data was 50GB of encrypted unsorted data, while the output result was 50GB of encrypted sorted data. This test is read/write/CPU intensive, reading the encrypted data, computing the sort, and writing the results. In comparing the E5-2699 v3 (18 Core) to the E5-2697 v2 (12 Core) results we observed a significant difference in performance. As Figure 1 shows, E5-2699 v3 with encryption is more than 2.5X faster than the E5-2697 while the difference in the number of cores is only 36 vs 24 cores [see Note 2].

While the core count difference may not seem to be a fair comparison, as mentioned previously, it is the next step up in the Intel Xeon E5-269X family. So a 2.5X performance improvement with a street price difference of about 50% (box price $4115 vs. $2618) is definitely more bang for your buck.
50GB encrypted TeraSort with Intel® AES-NI on HDD
Intel® Xeon® Processor E5-2699 v3 (18C) vs. E5-2697 v2 (12C)

Figure 1. E5-2699 v3 processors show a significant improvement over E5-2697 in TeraSort
operations. [Reprinted with permission from Cloudera Inc., Copyright © 2014] [See Note 2]

If you are interested in understanding the true number of core seconds across all cores, the math
comes out to 1.69x total performance improvement in core-seconds spent for the same workload.

Additionally, it should be noted that the E5-2699 v3 processor consumes 2.27 times less power
than the E5-2697 v2 to process the same workload.

Solid-State Drives on EXT4 versus HDD on EXT4

As SSD drives become more readily available at lower costs and at I/O rates that we have never
seen before, it is common for Cloudera customers to ask, what kind of performance improvement
should they expect if they use Solid State Drives (SSD) instead of spinning hard disk drives
(HDD).

The answer is it depends on the workload. If the workload is significantly I/O bound, you will
experience better performance improvement than if the workload is CPU bound where the
performance improvement may not be as significant.

We ran the same TeraSort tests on SSD and HDD and found 31% faster performance on SSD.
Since TeraSort is more CPU-bound than I/O-bound we would expect even better results on an
I/O-bound workload as seen in the next section.
TestDFSIO, Raw I/O Performance

We performed TestDFSIO, a read/write-intensive test for HDFS, to contrast the results of the SSD vs. HDD test above. While the TeraSort test stresses the compute capacity, the TestDFSIO test puts more emphasis on raw I/O performance. This test was configured to read/write 20 files of 16GB each for a total size of 320GB of data per run.

We saw a significant performance difference between SSD-encrypted data vs HDD-encrypted data when we ran TestDFSIO. On write operations we saw over 11X performance improvement! 
The I/O performance gain further demonstrates that the actual performance you may obtain in your environment is highly dependent on the type of workload.

If most of your operations are write intensive vs read or CPU bound, then SSDs can make a huge performance impact.

On read operations we also saw a significant performance improvement of 2X faster reads on SSD vs HDD.

**Conclusion**

In this exercise we saw the benefits of running Hadoop on improved hardware. Upgrading from Intel Xeon E5-2697 v2 to E5-2699 v3 processors resulted in a significant increase in performance under our test scenarios.

Additionally, drive configuration plays an important role when dealing with file systems. In our tests we saw performance improvements when using SSD I/O bound tests.
Hadoop is meant to be used in clustered servers, and the real power of Hadoop is unlocked when you have all your data in a cluster of tens, hundreds, or in some cases thousands of servers. These multi-node clusters allow both Hadoop and Cloudera to shine with their enterprise data hub management and security solutions. In a future article, we will show results from additional tests on Cloudera Distribution of Hadoop 5.2 in a cluster of servers to demonstrate performance of maintaining data encryption within the clusters.

NOTE 1:

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)](http://www.intel.com)

NOTE 2:

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark® and MobileMark®, 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. For more information go to [http://www.intel.com/performance](http://www.intel.com/performance)

**Test Environment Configurations**

**Software specifications**

- Hadoop 2.5.0-cdh5.2.0
- redhat-release-server-7.0-1.el7.x86_64
- Linux 3.10.0-123.6.3.el7.x86_64
- cryptsetup 1.6.3
  - cipher: aes-cbc-plain,
  - keysize: 256 bits
  - hashspec: sha1
- Java* SE Runtime Environment (build 1.8.0_20-b26)
- OpenSSL 1.0.2-beta1 24 Feb 2014
- dmcrypt 3.10.0-123.6.3.el7.x86_64
  - cipher: aes-cbc-plain, hashspec sha1
  - keysize: 256 bits
- driver: xts-aes-aesni
- driver: cbc-aes-aesni

**3rd gen Intel Xeon processor-based Server**

- 2 x Intel® Xeon® CPU E5-2699 v3 @ 2.3GHz
- cache size: 45 MB
siblings : 36
cpu cores : 18

Drive 1
  WDC WD1002FAEX-00Z3A0
  1 x 1TB SATA 7200 RPM

Drive 2
  Intel SSD P3700
  1 x 400 GB

RAM
  128GB (DDR4 -1333MHz?)

**2nd gen Intel Xeon processor-based Server**
  Intel® Xeon® CPU E5-2697 v2 @ 2.7GHz
  cache size : 30 MB
  siblings : 24
  cpu cores : 12

Drive
  WDC WD1002FAEX-00Z3A0
  1 x 1TB SATA 7200 RPM

RAM
  128GB (DDR3 -1333MHz)

**References**

[1] Intel® SSD DC P3700 Series

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL’S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to:
http://www.intel.com/design/literature.htm

Any software source code reprinted in this document is furnished under a software license and may only be used or copied in accordance with the terms of that license.

Intel, the Intel logo, Intel Core, and Intel Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

Copyright © 2015 Intel Corporation. All rights reserved.
*Other names and brands may be claimed as the property of others.