PowerEdge Product Group

Direct from Development

PowerEdge MX & Intel® QuickAssist Technology (Intel® QAT)

Tech Note by:
Andy Butcher

SUMMARY

PowerEdge MX is the first Dell EMC server to offer a software licensing option to enable Intel® QuickAssist Technology.

It provides a software-enabled foundation for security, authentication, and compression, and significantly increases the performance and efficiency of standard platform solutions.

Intel® QAT on PowerEdge MX servers offer performance across applications. That includes symmetric encryption and authentication, asymmetric encryption, digital signatures, RSA, DH, and ECC, and lossless data compression.

Encryption and Key Generation

Many users will be familiar with the "https" prefix on frequently-visited websites. Behind all of these secure websites is an implementation of TLS (transport layer security) or its predecessor SSL (secure sockets layer). Each protocol entails a "handshake" between the client and server that establishes authenticity of the server and creates a session key for encrypting the exchanged data. These Public Key Encryption (PKE) algorithms, historically performed by software, can be offloaded from the CPU into the Intel® QAT engine for providing significant performance gains for Web Server, eCommerce, VPN, Firewall or Security Load Balancer and Wan Acceleration solutions.

Data Compression and Decompression

Users of "zip" files will be familiar with the benefit of another common software function, data compression. Like cryptography, compression and decompression can be compute-intensive functions. Intel® QAT is comprised of acceleration engines for data compression as well, yielding faster performance and higher throughput for software and systems that rely on compressed data such as storage, web compression, big data, or high performance computing (HPC).

Benefit of Intel® QAT

It really boils down to the TCO, or total cost of ownership. A web server, cloud load balancer, or security gateway that can handle significantly more secure connections per second and provide high performance encrypted data throughput for reduced infrastructure cost. A storage system that uses accelerated compression to decrease the total required capacity vastly reduces storage footprint and subsequent costs. Application efficiency also reduces the thermal footprint of a datacenter or computing cluster, lowering energy costs. Improved efficiency and reduced active power for security and compression translate to reduced infrastructure.

Supported Operations

- Symmetric (Bulk) Cryptography
- Ciphers (AES, 3DES/DES, RC4, KASUMI*, ZUC, Snow 3G)
- Message digest/hash (MD5, SHA1, SHA2, SHA3) and authentication (HMAC, AES-XCBC)

Supported Operations (cont)

- Algorithm chaining (one cipher and one hash in a single operation)
- Authenticated encryption (AES-GCM, AES-CCM)
- AES-XTS
- Wireless
- KASUMI, Snow 3G and ZUC in encryption and authentication modes
- Asymmetric (Public Key) Cryptography
- Modular exponentiation for Diffie-Hellman (DH)
- RSA key generation, encryption/decryption and digital signature generation/verification
- DSA parameter generation and digital signature generation/verification
- Elliptic Curve Cryptography: ECDSA, ECDHE, Curve25519, SM2
- Compression/Decompression *DEFLATE (Lempel-Ziv77) & Huffman.*

Introducing Optional Software Licenses for Intel® QAT in PowerEdge MX

Intel® QAT has a long history with the deliveries of the 8920 model and the subsequent 8955 on PCIe cards. In the Intel® Xeon® Processor Scalable Family, Intel® is making the next generation of Intel® QAT available with significantly improved performance in a chipset-integrated version. Dell EMC is offering hardware-enabling licenses for chipset Intel® QAT on the MX series blade servers (MX740c and MX840c). These licenses can be installed *without* the need to add hardware to the system and occupy slots. Depending on the license level installed and the performance level desired, the chipset based Intel® QAT will be programmed to offer the bandwidth performance as defined below, mimicking the performance of the latest model 8960 and model 8970 PCIe cards. The licenses are installed through the iDRAC license manager.

Intel® QAT Optional License	Compression	Encryption	RSA
40G 'mid-range'	28 Gb/s	40 Gb/s	40K Ops/s
100G 'top performance'	65 Gb/s	100 Gb/s	100K Ops/s

Software

Software is provided through the Intel open source site https://01.org/intel-quickassist-technology. The applicable drivers are associated with the C62x chipset. Application and library examples are posted here along with the API reference manuals, allowing users to build upon these open source libraries and examples or build their own applications. Release notes identify operating system compatibility.

Openssl

Openssl is a software library that implements cryptographic functions that secure communications over computer networks. It implements the aforementioned protocols SSL and TLS. OpenSSL versions 1.1.0 and beyond now have asynchronous support for hardware accelerators, which helps achieve power, performance, cost, capacity and efficiency benefits discussed above. Prior to this support, all cryptographic function calls were performed in a synchronous manner, which meant that any given CPU thread was "blocked" awaiting the result of an operation. With asynchronous operation, several operations can be queued for Intel® QAT engine, and the responses can be collected and consumed as soon as they are completed in rapid succession. The following resources describe how to get Intel® QAT working with openssl:

- https://www.openssl.org/source/
- https://github.com/01org/QAT_Engine
- https://github.com/openssl/openssl

Instructions to use openssl to integrate with applications such as NGINX web server and HAProxy, a load balancer and proxy, can be found on https://01.org/intel-quickassist-technology. NGINX has been demonstrated to handle more connections per second with the benefit of Intel® QAT.

DPDK (Data Plane Development Kit)

An open source project consisting of a set of libraries and drivers for fast packet processing, DPDK employs PMDs (Poll Mode Drivers) to interact with user space software, avoiding latency expensive context switches between kernel and user space. Instructions on installing the Intel® QAT PMD can be found at DPDK GUIDES LINK. Using DPDK, performance benefit has been demonstrated for IPsec (Internet Protocol Security), which provides security at a lower level in the protocol stack than TLS. For further reading on IPSEC, see the links
Getting Started Guidehttps://software.intel.com/en-us/articles/get-started-with-ipsec-acceleration-in-the-fdio-vpp-project
Sample Application Usage https://doc.dpdk.org/guides-16.04/sample_app_ug/ipsec_secgw.html.

Compression and Decompression

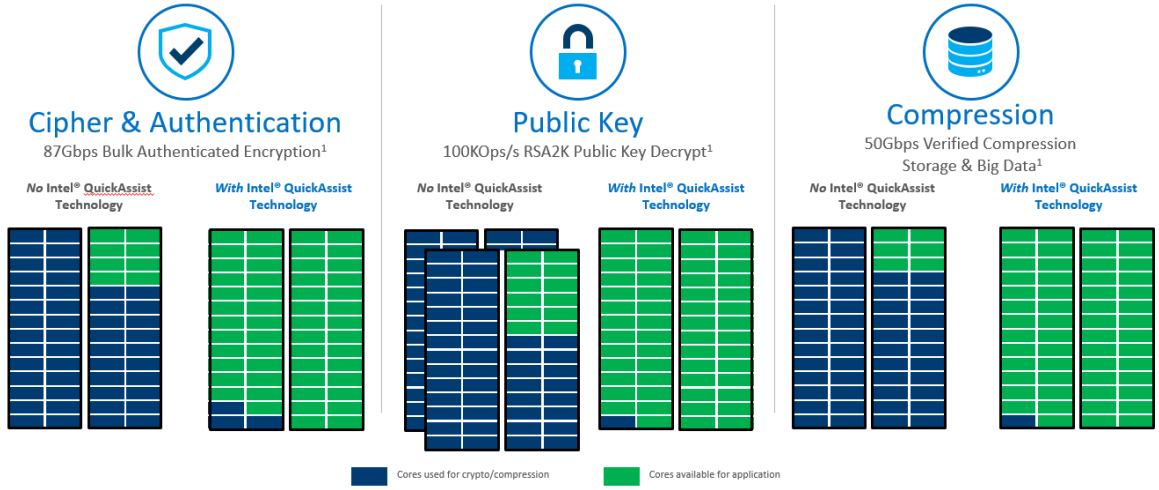
The primary vehicle for delivering sample code for data compression and decompression for Linux is QATZip, which is a user space library that produces data in standard gzip format. See the most recent release notes for the drivers and the API application guides for more information on data compression.

Intel® Key Protection Technology (Intel® KPT)

Inside the Intel chipset, there is a path for delivering keys directly from the key store in the chipset to the Intel® QAT engines. Software applications can utilize Intel® KPT to manage secure asymmetric and private key transactions for applications such as Hardware Security Modules(HSM) or Security Middle Box solutions.

Performance

Server workload performance is dependent on a wide variety of factors. The amount of CPU load on the system, the number of cores, the amount of memory, packet sizes, and compression levels are among many of such factors. Dell recommends specific testing to determine the exact improvements realizable by this offload. Below are some expected performance enhancements according to testing conducted Intel(r) Xeon Processor Scalable Family & Intel(r) C627 Chipset.



Crypto
NGINX* and OpenSSL* connections/second. Conducted by Intel Applications Integration Team. Claim is actual performance measurement.
Intel® microprocessor. Processor: Intel® Xeon® processor Scalable family with C6xxB0 ES2
Performance tests use cores from a single CPU, Memory configuration:, DDR4–2400. Populated with 1 (16 GB) DIMM per channel, total of 6 DIMMs
Intel® QuickAssist Technology driver: QAT1.7.Upstream.L.0.8.0-37 Fedora* 22 (Kernel 4.2.7) BIOS:
PLYDCRB1.86B.0088.D09.1606011736
Compression
24 Core Intel(r) Xeon Scalable Platform -SP @1.8GHz, Single (UP) Processor configuration. Intel(r) C627 PCH with crypto acceleration capability (in x16 mode) Neon City platform. DDR4 2400MHz RDIMMs 6x16GB(total 96 GB), 6 Channels, 1 x Intel® Corporation Red Rock Canyon 100GbE Ethernet Switch in the x16 PCIe slot on Socket 0. 8 cache ways allocated for DDIO.