Intel® QuickAssist Technology and Intel® Crypto Acceleration - Accelerating HAProxy* Performance on Intel Instances of Alibaba Cloud*

Authors

Divya Pendyala

Pan Zhang

Heqing Zhu

1 Introduction

As more and more enterprises migrate to cloud for better flexibility and security, businesses need the compute power to support their complex portfolio of workloads. Whether it is for large-scale data storage and analytics, delivering a web-based service, scaling infrastructure, or disaster recovery purposes, stronger compute can deliver cost-effective and scalable solutions.

4th Gen Intel® Xeon® Scalable processors are designed to accelerate performance across the fastest-growing workloads. These processors have built-in accelerators to help improve performance efficiency for demanding workloads, including those powered by AI. In addition to performance improvements, 4th Gen Intel Xeon Scalable processors have advanced security technologies to help protect data in an ever-changing landscape of threats while unlocking new opportunities for business insights.

Alibaba Cloud* launched a new generation of enterprise-class elastic computing instance types, ECS g8i, r8i, and c8i, based on 4th Gen Intel Xeon Scalable processors. These instance types provide high-performance and efficient computing services for customers to meet their growing performance needs. Rich hardware acceleration capability and comprehensive security protection are the two major features of ECS g8i instances. These instances based on 4th Gen Intel Xeon Scalable processors, provide a variety of hardware native acceleration capabilities that enhance the computing power of cryptographic and AI workloads.

This document explains the Intel® Crypto Acceleration technologies on Intel® processors available in Alibaba Cloud. It provides detailed information on configuring TLS workloads like HAProxy load balancer software on the latest Alibaba ECS g8i instance type based on 4th Gen Intel Xeon Scalable processors with integrated accelerators including Intel® QuickAssist Technology (Intel® QAT).

This document is part of the Network Transformation Experience Kits.

Table of Contents

Figures

Tables

Document Revision History

Revision	Date	Description
001	February 2024	Initial release.

1.1 Terminology

Table 1. Terminology

Abbreviation	Description
CPS	Connection per second
FMA	Fused-multiply add
HPC	High performance computing
SIMD	Single Instruction, Multiple Data
SLA	Service-level agreements
SR-IOV	Single Root I/O Virtualization
UX	User Experience

1.2 Reference Documentation

Table 2. Reference Documents

Reference	Source
4th Gen Intel® Xeon® Scalable Processors	https://www.intel.com/content/www/us/en/products/details/processors/xeon/scalable.html
Intel® QuickAssist Technology (Intel® QAT)	https://www.intel.com/content/www/us/en/architecture-and-technology/intel-quick-assist-technology-overview.html
Intel® QuickAssist Technology Engine for OpenSSL* (Intel® QAT Engine for OpenSSL*)	https://github.com/intel/QAT_Engine#installation-instructions
GitHub for Intel QuickAssist Technology Engine for OpenSSL	https://github.com/intel/QAT_Engine
GitHub for Intel® Integrated Performance Primitives Cryptography (Intel® IPP Cryptography)	https://github.com/intel/ipp-crypto
GitHub for Intel® Multi-Buffer Crypto for IPSec	https://github.com/intel/intel-ipsec-mb
GitHub for HAProxy Software Load Balancer	https://github.com/haproxy/haproxy/
GitHub for h1load Traffic Generator	https://github.com/wtarreau/h1load

2 Overview - Accelerate Cloud with Intel® Technologies

4th Gen Intel Xeon Scalable processors have built-in accelerators to deliver performance and power efficiency advantages across the fast-growing cloud workloads, including AI, analytics, networking, storage, and high-performance computing (HPC). With an integrated accelerator like Intel® QuickAssist Technology (Intel® QAT), 4th Gen Intel Xeon Scalable processors speed up encrypted data movement and compression for faster networking, boost query throughput for more responsive analytics, and offload scheduling and queue management to dynamically balance loads across multiple cores in cloud platforms. To enable the built-in accelerator features within a hyper-scaler environment, Intel supports the ecosystem with the most common cloud APIs, libraries, and OS-level software. With built-in accelerators and software optimizations, the latest generation of Intel® Xeon® Scalable processors have shown to deliver leading performance per watt on targeted real-world cloud workloads. This results in more efficient CPU utilization, lower cloud electricity consumption, and higher services ROI, while helping businesses achieve their sustainability goals.

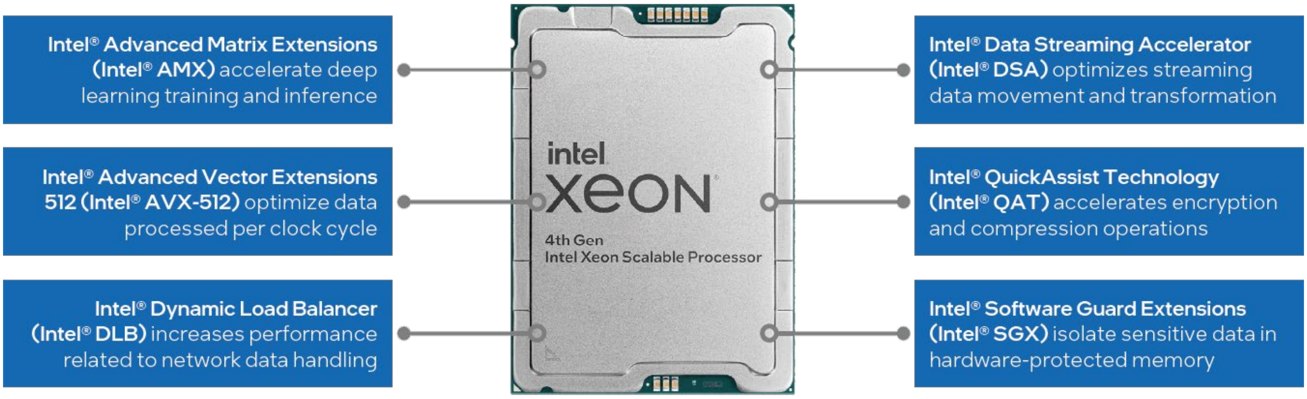

Intel® Advanced Matrix Extensions (Intel® AMX) accelerate deep learning training and inference
Intel® Advanced Vector Extensions 512 (Intel® AVX-512) optimize data processed per clock cycle
Intel® Dynamic Load Balancer (Intel® DLB) increases performance related to network data handling
intel
XEON
4th Gen
Intel Xeon Scalable Processor
Intel® Data Streaming Accelerator (Intel® DSA) optimizes streaming data movement and transformation
Intel® QuickAssist Technology (Intel® QAT) accelerates encryption and compression operations
Intel® Software Guard Extensions (Intel® SGX) isolate sensitive data in hardware-protected memory

Figure 1. 4th Gen Intel® Xeon® Scalable Processor with Integrated Accelerators

2.1 HAProxy

HAProxy is a widely used open-source software load balancer. It is particularly suited for very high traffic web sites and offers high availability, load balancing, traffic offloading, and a broad spectrum of proxy-based features aimed at optimizing application delivery and keeping applications responsive under heavy loads.

HAProxy load balancer provides high-performance SSL/TLS termination, allowing to encrypt and decrypt web traffic. This provides improved web server performance and simplifies certificate management securing web traffic.

HAProxy is compiled with OpenSSL, which allows it to encrypt and decrypt traffic as it passes.

2.2 Intel® Accelerator Engines Redefine Encryption Performance

4th Gen Intel Xeon Scalable processors feature a broad and wide range of built-in accelerator engines for today's most demanding workloads. Whether on-prem, in the cloud, or at the edge, Intel® Accelerator Engines can help take your business to new heights, increasing application performance, reducing costs, and improving power efficiency.

2.3 Intel® Crypto Acceleration

For security workloads, maintaining performance while preserving data confidentiality and code integrity is highly important. Intel® Crypto Acceleration helps achieve this, by reducing the impact of implementing pervasive data encryption while increasing the performance of encryption-sensitive workload.

The advanced crypto acceleration technologies embedded in the cores of 4th Gen Intel Xeon Scalable processors enable greater levels of cryptographic security, enhance performance, and enable a more seamless user experience—and without having to add more cores and more processors to the data center.

Intel Crypto Acceleration instructions use stronger encryption protocols, like larger key sizes, stronger algorithms, and more types of data encrypted—with minimal impact upon user experience (UX). By utilizing faster cryptographic algorithms, users can see improved performance, support for better service-level agreements (SLAs), and a reduction in compute cycles typically spent on cryptography processing.

2.4 Intel® Advanced Vector Extensions 512 (Intel® AVX-512)

Intel® Advanced Vector Extensions 512 (Intel® AVX-512) is an advanced set of CPU instructions introduced by Intel® to enhance the performance of compute-intensive and data-centric workloads. AVX-512 builds upon the foundation of earlier SSE and AVX instruction sets, providing even more powerful vector processing capabilities for modern processors. These vectorized instructions used in software acceleration libraries, namely Intel® IPP Cryptography and Intel® Multi-Buffer Crypto for IPsec with Intel® QAT Engine for OpenSSL, commonly known as QATSW or Intel Crypto acceleration, provide the computational power for HAProxy.

Intel AVX-512 helps accelerate the performance of scientific simulations, financial analytics, AI/deep learning, 3D modeling and analysis, image and audio/video processing, cryptography, data compression, and other intensive workloads. Intel AVX-512 is the latest Intel architecture processor vector instruction set, with up to two fused multiply add (FMA) units and other optimizations to help accelerate the performance of demanding computational tasks.

2.5 Intel® QuickAssist Technology (Intel® QAT)

Previously available in PCIe plug-in card or in Intel server chipset for Intel® Xeon® processors, Intel QuickAssist Technology (Intel QAT) is now built directly into 4th Gen Intel Xeon Scalable processors. Intel QAT accelerates cryptography and compression. The accelerator offloads encryption, compression, and public key exchange workloads, freeing up CPU cycles for other workloads. As network architects look to virtualize more functions and capabilities—such as network security workloads—Intel QAT helps create vital processing capacity that benefits the whole network.

Intel QAT can significantly boost CPU efficiency and application throughput, while reducing data footprint and power utilization, enabling organizations to strengthen encryption without sacrificing performance.

2.6 Intel QAT Engine for OpenSSL

Intel QAT Engine for OpenSSL (referred to as QAT_Engine) is a software package that supports acceleration for both hardware and optimized software based on vectorized instructions. The advancement in cryptographic acceleration starting from the 3rd Gen Intel Xeon Scalable processors provides users more options to accelerate their workloads. The QAT_Engine supports the ability to accelerate the standard OpenSSL using basic Intel instruction sets to either the accelerator path (Intel QAT) or the optimized software path (using vAES instructions and crypto libraries).

3 Intel QAT Deployment on Alibaba Cloud*

Alibaba Cloud has introduced 4th Gen Intel Xeon Scalable processors in its instance type fleet. Intel QAT integrated in the latest gen Intel Xeon processor is available as a resource for tenants, specifically for compression and cryptographic workloads. The maximum number of Intel QAT devices available per processor is four. Users can scale the Intel QAT devices, starting from one to four, with the increment needed for acceleration. Intel QAT is available on Alibaba ECS g8i, c8i, and r8i instances starting from 8 vCPUs.

Intel QAT deployment in a virtualized environment can be configured in the following ways:

- *Physical device direct assignment* : Hardware is exposed as 1 PF (Physical Function) to host. The hypervisor passes through 1 PF to a single virtual machine (VM)/guest.
- *Single Root IOV (SR-IOV)* : With SR-IOV enabled, HW exposes 1 PF and n virtual functions (VFs) to host. Hypervisor passes through one or more VFs to different VMs/guests. Intel QAT in 4th Gen Intel Xeon Scalable processor provides 4 PFs. 16V VFs per PF are available.

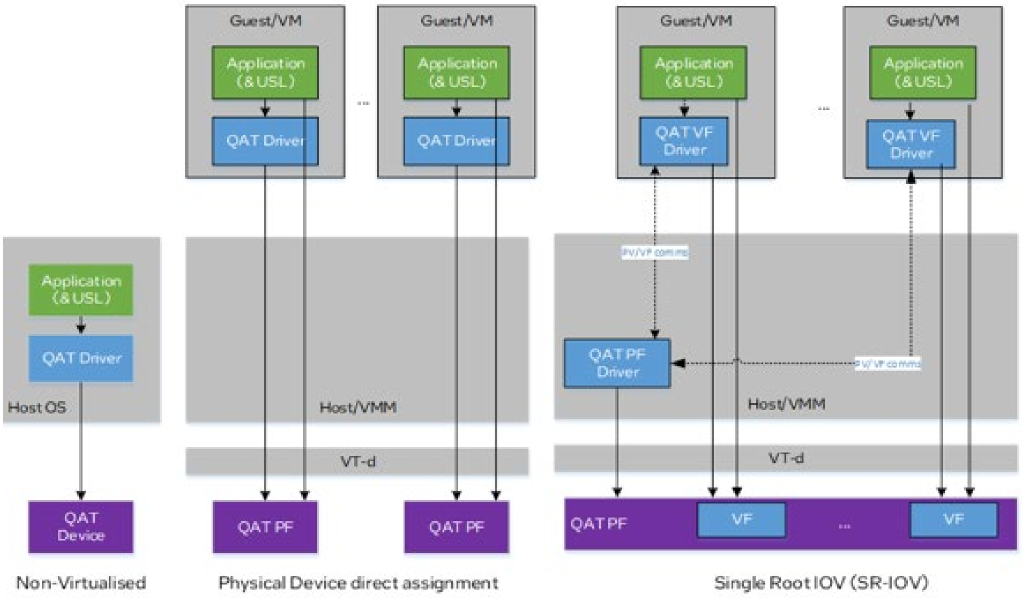


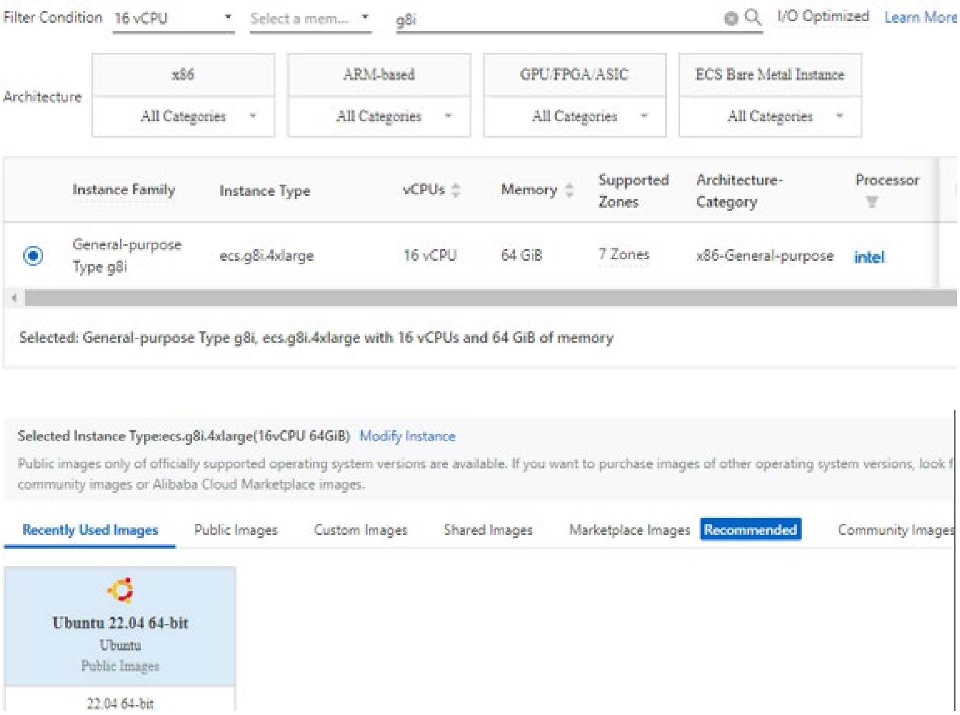
Figure 2. Intel QAT Virtualization Deployment Model

4 Steps to Configure Intel QAT on Alibaba Cloud Instance

4.1 Instance Selection

Intel QAT hardware accelerator is available on Alibaba ECS g8i, c8i, and r8i instances starting from eight vCPUs.

Alibaba ecs.g8i.4xlarge instance (16 vCPUs) with Ubuntu 22.04 is chosen in this test configuration. By default, this instance type has integrated QAT devices.



Filter Condition: 16 vCPU | Select a mem... | g8i

Architecture:

x86	ARM-based	GPU/FPGA/ASIC	ECS Bare Metal Instance
All Categories	All Categories	All Categories	All Categories

	Instance Family	Instance Type	vCPUs	Memory	Supported Zones	Architecture-Category	Processor
●	General-purpose Type g8i	ecs.g8i.4xlarge	16 vCPU	64 GiB	7 Zones	x86-General-purpose	intel

Selected: General-purpose Type g8i, ecs.g8i.4xlarge with 16 vCPUs and 64 GiB of memory

Selected Instance Type:ecs.g8i.4xlarge(16vCPU 64GiB) Modify Instance

Public images only of officially supported operating system versions are available. If you want to purchase images of other operating system versions, look f

community images or Alibaba Cloud Marketplace images.

Ubuntu 22.04 64-bit
Ubuntu
Public Images
22.04 64-bit

Figure 3. Alibaba ecs.g8i.4xlarge Instance Based on 4th Gen Intel Xeon Scalable Processor with Integrated QAT

4.2 Install OpenSSL

Verify prebuilt OpenSSL software is available on the instance. Replace it with the preferred version of OpenSSL as needed.

4.3 Configure Intel QAT Software

Following is the step-by step procedure to configure Intel QAT on Alibaba Cloud:

1. Intel QAT Virtual Device assignment – QAT devices are available on the g8i.4xlarge instance by default.
2. Detect Intel QAT devices on g8i.4xlarge instance

   Detect the Intel QAT devices on the guest VM.

   QAT device ID = 8086:0da5. Tenant user can use this device id to detect QAT availability using the following command:

   ```
   lspci -v -d 8086:0da5 -vmm | grep -E 'SDevice'
   SDevice:        Device 0001
   SDevice:        Device 0002
   ```

   Device 0001 refers to asymmetric crypto VQAT device and Device 0002 refers to compression VQAT device on the host.
3. Configure Intel QAT driver Install Intel QAT out-of-tree driver on the guest.

   a. Download officially released latest Intel QAT driver: https://www.intel.com/content/www/us/en/download/765501/intel-quickassist-technology-driver-for-linux-hw-version-2-0.html?wapkw=qat%20driver

      Unzip the file and extract the Intel QAT package included in the release.

      ```
      tar -zxvf qat20.L.1.0.10-00005.tar.gz
      ```

      QAT software creates virtual device files and detects the QAT devices automatically.

   b. Configure the Intel QAT driver.

      ```
      ./configure
      ```

   c. Install the Intel QAT software and sample codes using the following commands:

      ```
      make -j install
      make samples-install
      ```

   d. QAT virtual device config file: Make sure the ServicesEnabled parameter is set to `asym` for PKE operations in the QAT device config file *vqat-adi_devx.conf* under `/etc`.

      ```
      Example: vqat-adi_dev0.conf
      [GENERAL]
      ServicesEnabled = asym
      ```

```
 ConfigVersion = 2
```

4. Install Intel QAT_engine.

   Build and Install Intel QAT Engine for OpenSSL – v1.0.0 at the time of this testing.

   ```
   git clone https://github.com/intel/QAT_Engine.git
   git checkout
   cd /QAT_Engine
   ./configure --with-qat_hw_dir=/QAT
   make
   make install
   ```

   Successful configuration of QAT_engine gives the following status messages:

   ```
   Checking status of all devices.
   There is 2 QAT acceleration device(s) in the system:
    qat_dev0 - type: vqat-adi,  inst_id: 0,  node_id: 0,  bsf: 0000:00:08.0,  #accel: 1 
   #engines: 1 state: up
    qat_dev1 - type: vqat-adi,  inst_id: 1,  node_id: 0,  bsf: 0000:00:09.0,  #accel: 1 
   #engines: 1 state: up
   make[1]: Nothing to be done for 'install-data-am'.
   make[1]: Leaving directory '/root'
   ```

5 Steps to Configure Intel Crypto Acceleration on Alibaba Cloud Instance

Intel Crypto Acceleration can be configured using the latest vAES and Intel AVX-512 instructions available on the 4th Gen Intel Xeon Scalable processor along with installing two crypto libraries that can accelerate symmetric and asymmetric crypto. This software-based acceleration has been incorporated into the Intel QAT Engine for OpenSSL, a dynamically loadable module that uses the OpenSSL ENGINE framework, allowing users to add this capability to OpenSSL without having to rebuild or replace their existing OpenSSL libraries.

Following is the step-by step procedure to configure Intel Crypto Acceleration on Alibaba Cloud:

1. Build OpenSSL (skip if installed already).

   ```
   git clone https://github.com/openssl/openssl.git
    cd /openssl
   git checkout 1.1.1k
   ./config [options] -Wl,-rpath,\${LIBRPATH}
   make
   make install
   ```

2. Build ipp-crypto for Asymmetric Crypto.

   ```
   git clone --recursive https://github.com/intel/ipp-crypto
   cd /ipp-crypto/sources/ippcp/crypto_mb
   cmake . -Bbuild -DCMAKE_INSTALL_PREFIX=/usr
   cd build/
   make -j
   make install
   ```

3. Build ipsec_mb for Symmetric Crypto.

   ```
   git clone https://github.com/intel/intel-ipsec-mb.git
   cd intel-ipsec-mb/
   git checkout v1.3-226-g05bccb6a
   make -j
   make install NOLDCONFIG=y
   ```

4. Build Intel QAT_engine.

   ```
   git clone https://github.com/intel/QAT_Engine.git
   cd /QAT_Engine
   ./configure --enable-qat_sw --disable-qat_hw
   make
   make install
   ```

   `--enable-qat_sw` checks crypto_mb and IPSec_MB libraries in their respective default paths or in the path provided in the config flag `--with-qat_sw_install_dir`. If any of the libraries were not installed, then their corresponding algorithm support is disabled (cryto_mb library for PKE algorithms and IPSec_mb library for AES-GCM).

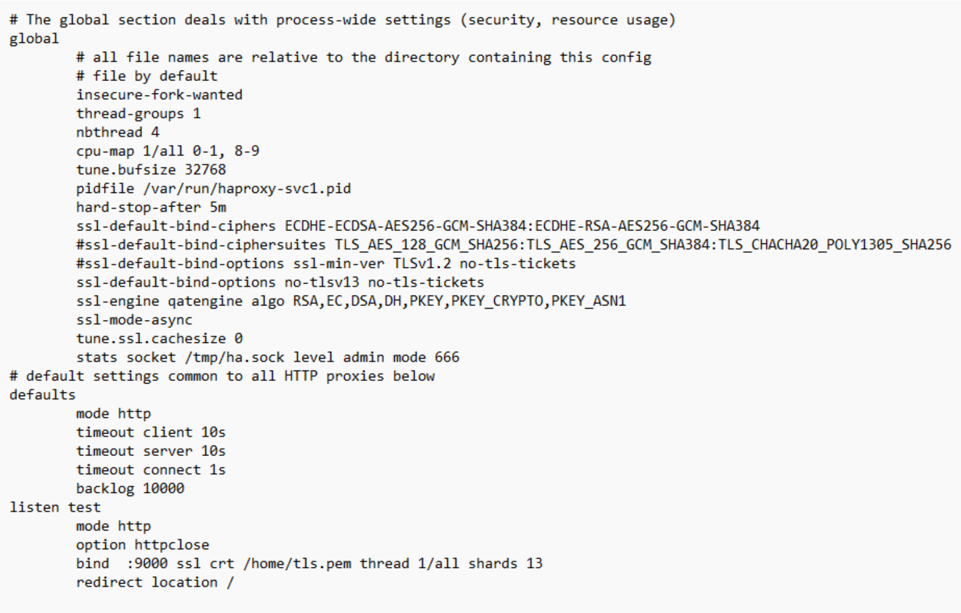
6 HAProxy SSL Termination

HAProxy enables SSL encryption and decryption by editing its configuration file and requires no additional tools. Adding `ssl` and `cert` parameters to a bind line in the front-end section allows SSL termination for the listener and identifies the location of the PEM-formatted SSL certificate, which should contain both public certificate and private key.

More information on the HAProxy SSL configuration can be found here: https://www.haproxy.com/blog/haproxy-ssl-termination

HAProxy supports asynchronous TLS I/O operations and seamlessly integrates with async Intel QAT_engine to offload crypto operations to Intel QAT and Intel Crypto Acceleration software by setting `ssl-engine` to `qatengine` in the HAProxy config file.

```
ssl-engine qatengine algo RSA,EC,DSA,DH,PKEY,PKEY_CRYPTO,PKEY_ASN1
```



```
# The global section deals with process-wide settings (security, resource usage)
global
        # all file names are relative to the directory containing this config
        # file by default
        insecure-fork-wanted
        thread-groups 1
        nbthread 4
        cpu-map 1/all 0-1, 8-9
        tune.bufsize 32768
        pidfile /var/run/haproxy-svc1.pid
        hard-stop-after 5m
        ssl-default-bind-ciphers ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384
        #ssl-default-bind-ciphersuites TLS_AES_128_GCM_SHA256:TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256
        #ssl-default-bind-options ssl-min-ver TLSv1.2 no-tls-tickets
        ssl-default-bind-options no-tlsv13 no-tls-tickets
        ssl-engine qatengine algo RSA,EC,DSA,DH,PKEY,PKEY_CRYPTO,PKEY_ASN1
        ssl-mode-async
        tune.ssl.cachesize 0
        stats socket /tmp/ha.sock level admin mode 666
# default settings common to all HTTP proxies below
defaults
        mode http
        timeout client 10s
        timeout server 10s
        timeout connect 1s
        backlog 10000
listen test
        mode http
        option httpclose
        bind  :9000 ssl crt /home/tls.pem thread 1/all shards 13
        redirect location /
```

Figure 4. HAProxy sample configuration file (haproxy.conf) for Intel QAT_engine

7 Performance Benchmarks and Key Performance Indicators[1]

7.1 Connections per Second (CPS)

Application or web servers receive thousands of user requests every second. Securing the web traffic while delivering timely static web content is a tedious task and costs more CPU usage on web servers, slowing down performance. HAProxy deployed as a proxy server can handle SSL/TLS termination and load balancing of incoming request, improving the back end server performance to do more meaningful work.

In this testing, clients send HTTPS connection requests without requesting data. This utilizes key exchange and certificate authentication while exercising the TLS-1.2 handshake only with no data transfer.

7.2 Test Setup

For this testing, Alibaba Cloud instance ecs.g8i.4xlarge based on 4th Gen Intel Xeon Scalable processor is used.

This instance type supports integrated Intel QAT and has one vQAT device for cryptography. Two ecs.g8i.xlarge instances, installed with openssl 1.1.1k and h1load, HAProxy's own implementation of load generator, are used as hosts, for benchmarking https handshakes. Two client machines are used to ensure that there are no limitations from the client side. Each client process establishes a secure connection, exits gracefully, and sends a new request to establish a secure connection. When the load reaches its max value, the CPS from each client are summed up. One haproxy process is allocated for every hyper-thread (nbthread) in the HAProxy configuration file (*haproxy.conf*). For example: 2C4T (2 core, 4 thread config) has 4 haproxy threads. Each test is mapped to CPU cores and hyperthreads for consistency of results. For example: 2C4T: nbthread 4, and cpu-map

[1] See backup for workloads and configurations. Results may vary.

1/all 0-1,8-9 are defined in *haproxy4t.cfg*, the HAProxy configuration file. Reference h1load command to test connection-per-sec from client machine is as below:

"h1load -e -t 48 -c 2016 -s 5 --cipher-list ECDHE-RSA-AES256-GCM-SHA384 --tls-ver TLS1.2 https://serverIP:9000/"

Here h1load command sends around 2K concurrent connection requests, distributed evenly over 48 threads, at 5s ramp-up time, to negotiate TLS1.2 handshakes with the server through port 9000.

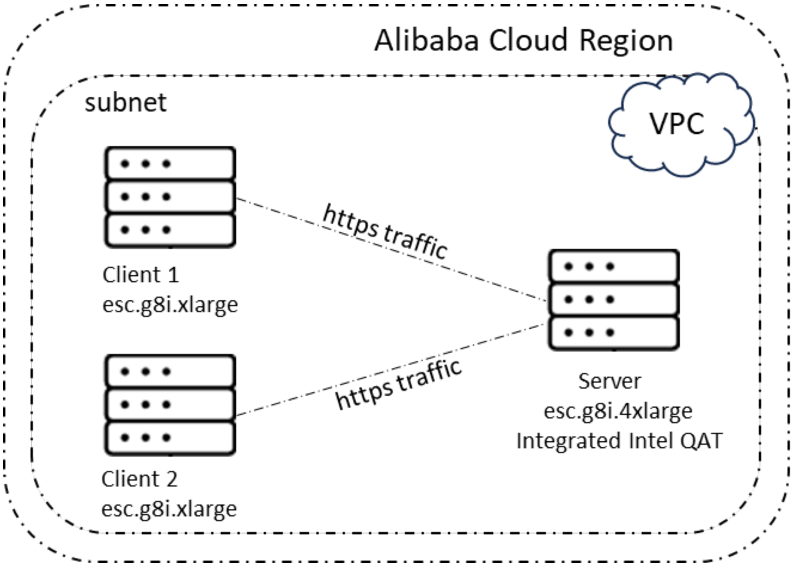


Figure 5. Hardware Configuration: Alibaba Cloud Instance on 4th Gen Intel Xeon Scalable Processor

Table 3. Hardware Configuration[2]

Component	4th Gen Intel Xeon Scalable Processor Instance Type at Alibaba Cloud ECS
Alibaba Cloud Instance	ecs.g8i.4xlarge
CPU Model	Intel® Xeon® Platinum 8475B
CPUs	16
Hyperthreading	Enabled
Cores Per Socket	8
Sockets	1
NUMA Nodes	1
NUMA CPU List	0-15
Memory	64 GB (4 x 16 GB RAM)
Ethernet Adaptor	Virtio
Intel QAT Hardware	Intel QAT
Intel Turbo Boost	Enabled
Base Frequency	2.7 GHz
Microcode	0x1
Tested by Intel as of	04/29/2023

[2] See backup for workloads and configurations. Results may vary.

Table 4. Software Configuration

Component	4th Gen Intel Xeon Scalable Processor Instance Type at Alibaba Cloud ECS
Operating System	Ubuntu 22.04.2 LTS
Kernel	5.15.0-73-generic
OpenSSL	v1.1.1k
HAProxy	v2.7
Client Benchmarking Tool	H1load
Intel QAT Driver	QAT20.L.1.0.10-00005.tar.gz
Intel QAT Engine for OpenSSL	v1.0.0-0701210
Intel® Multi-Buffer Crypto for IPsec Library	v1.3 -226-g05bccb6a
Intel® Integrated Performance Primitives Cryptography (Intel® IPP Cryptography)	v2021.7.1-8e1f90d

7.3 Performance Results[3]

As Figure 5 demonstrates, offloading ECDHE-RSA-AES256-GCM-SHA384 to Intel QAT provides the highest performance per core. Intel QAT (QATHW) provides up to 5x higher performance than default software stack, native OpenSSL and Intel Crypto acceleration (QATSW) provide up to 3x higher performance than native OpenSSL stack, at four vCPUs. It must be noted that Intel QAT has a peak performance, and it is hitting this point at 4 vCPUs. After Intel QAT reaches its maximum performance per device, its performance plateaus.

The maximum performance that Intel QAT offers for asymmetric operations with RSA authentication is ~64K CPS with four QAT devices on a 4th Gen Intel Xeon Scalable processor CPU with integrated QAT accelerator. In this case, with oneQAT device on the Alibaba 4th Gen Intel Xeon Scalable processor instance, the maximum performance QAT offers is ~16K CPS as seen in the following graph.

However, Intel Crypto acceleration or QATSW has no such performance limitation and can scale linearly with more vCPUs. The performance per core benefit is higher with Intel QAT while linearity in scaling with increased cores is achieved with QATSW.

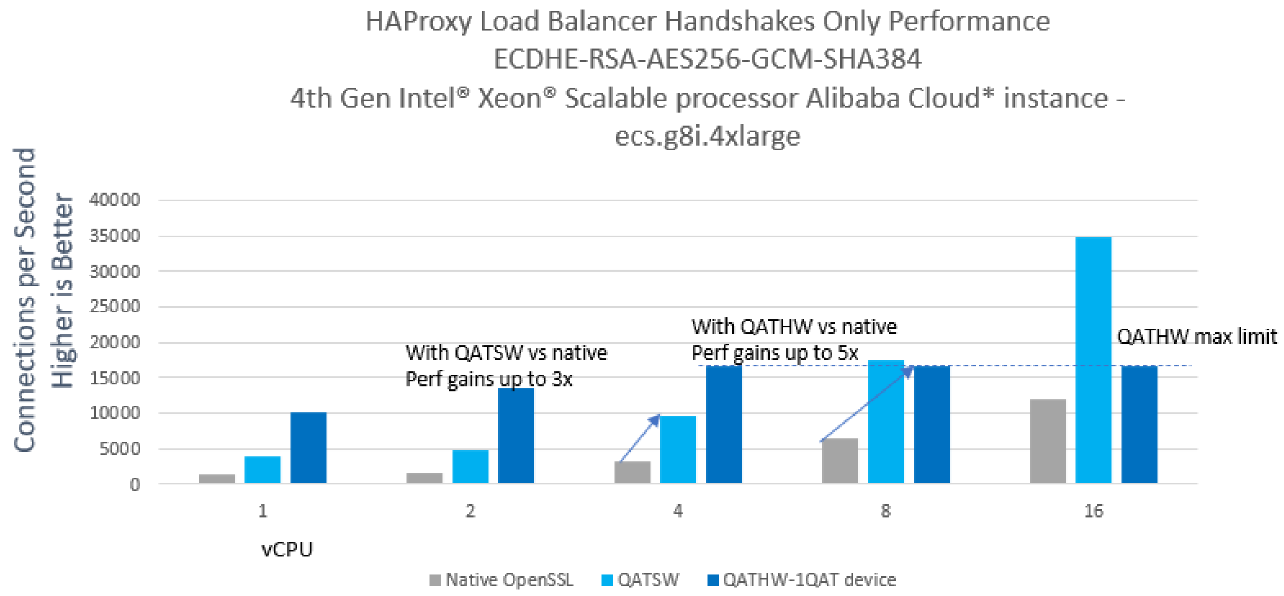


Figure 6. HAProxy Load Balancer Handshake Performance on 4th Gen Intel Xeon Scalable Processor on Alibaba Cloud

The 4th Gen Intel Xeon Scalable processor on Alibaba Cloud provides significant performance gains per core, especially when utilizing Intel QAT for establishing the TLS connections.

[3] See backup for workloads and configurations. Results may vary.

8 Benefits

Intel QAT, built into 4th Gen Intel Xeon Scalable processors, is now available on Alibaba Cloud including c8i, r8i, g8i, and accelerates cryptography and compression workloads. Intel QAT can significantly boost CPU efficiency and application throughput while reducing data footprint and power utilization, thereby enabling organizations to strengthen encryption without sacrificing performance and CPU utilization. Performance is delivered using a mainstream release of OpenSSL and HAProxy for asynchronous processing of TLS handshake operations, plugging in accelerated cryptographic implementations through a standard provider/engine into OpenSSL. HAProxy load balancer delivers up to 6x better crypto performance[4] using Intel QAT on a 4th Gen Intel Xeon Scalable processor compared to the native OpenSSL stack. By using Intel Crypto acceleration on this latest platform, performance can be linearly scaled up by adding more cores.

9 Summary

Data centers today rely on cryptography for processes spanning across networking and storage and data compression, in addition to traditional perimeter defense. With cryptography being a mandatory requirement in organizations, an explosion in the number of encryption cycles that need to be performed by the CPUs is inevitable. This, in turn, can lead to potential impacts on performance and user experience. The advanced crypto-acceleration technologies available in 4th Gen Intel Xeon Scalable processors enable greater levels of cryptographic security, enhance performance, and enable a seamless user experience — without having to add more cores and more processors to the data center or cloud environment.

This paper demonstrates the value proposition of integrated Intel QAT and Intel Crypto Acceleration on 4th Gen Intel Xeon Scalable processors on Alibaba Cloud. In this benchmarking, the performance of Intel QAT and Intel Crypto Acceleration over native stack on various vCPUs is compared and the benchmarking results show Intel QAT consistently outperforms crypto acceleration in terms of connections per second at lower number of cores, which helps establish faster and more secure handshakes. As Intel QAT reaches its maximum threshold at four vCPUs, the performance plateaus. However, crypto software acceleration linearly scales up with more CPU cores, which can benefit symmetric operations. Intel QAT and Intel Crypto Acceleration can also be used in coexistence to achieve consistent performance depending on the user needs.

Performance varies by use, configuration and other factors. Learn more at www.Intel.com/PerformanceIndex.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel technologies may require enabled hardware, software or service activation.

Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

The products described 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.

0224/DN/WIT/PDF 792594-001US

[4] See backup for workloads and configurations. Results may vary.