Impact of enabling file system encryption in MQ 9.2.5 on the IBM MQ Appliance (M2002)

Objective

A new feature has been released in MQ 9.2.5 which enables the Queue Manager (QM) to be created with an encrypted filesystem. This prevents access to the data stored in MQ queues (and the recovery log) in the event the appliance SSD disks are removed from the M2002 appliance. Storage used to retain QM configuration backup or diagnostic information can also be encrypted.

Background

It has been noted that more IBM MQ customers often require message payloads to be encrypted while in transit and at rest to comply with various security mandates. Before the release of this feature, customers who wished to ensure their data was encrypted at rest had to used AMS (Advanced Message Security).

Now customers can use TLS to protect the message data in transit and an encrypted QM filesystem to protect that data when at rest in the appliance. Note that the use of an encrypted filesystem does not require that all messaging is TLS enabled.

It is also possible to enable an encrypted fs for an HA and/or DR QM as well as a standalone QM. The impact on HA performance will also be examined in this whitepaper.

Scenario

A couple of different scenarios will be used to compare the encrypted and non-encrypted Performance:

- Single QM – All clients send and receive from a set of queues on 1 QM
- Multiple QM – All clients send and receive from a set of queues on 10 QM
- Single HA QM – All clients send and receive from a set of queues on 1 HA QM
- Multiple HA QM – All clients send and receive from a set of queues on 10 HA QM

For this investigation, our standard range of message sizes (256byte, 2KB, 20KB, 200KB) will be used and persistent messages are used in all tests. The messaging scenario is a request responder scenario as featured in the current MQ appliance performance reports. Results will be provided for both M2002A and M2002B models.

Environment

These tests use 2 x86_64 Linux servers for the application clients (see Appendix A for their specification); Server 1 hosts the requester applications, the M2002 MQ appliance hosts the QM under test and Server 2 hosts the responder applications.

The version of MQ used in these tests is MQ V9.2.5.

Results

Single QM

The graph below shows the results from the single QM test using a 2KB message size on a M2002A appliance:

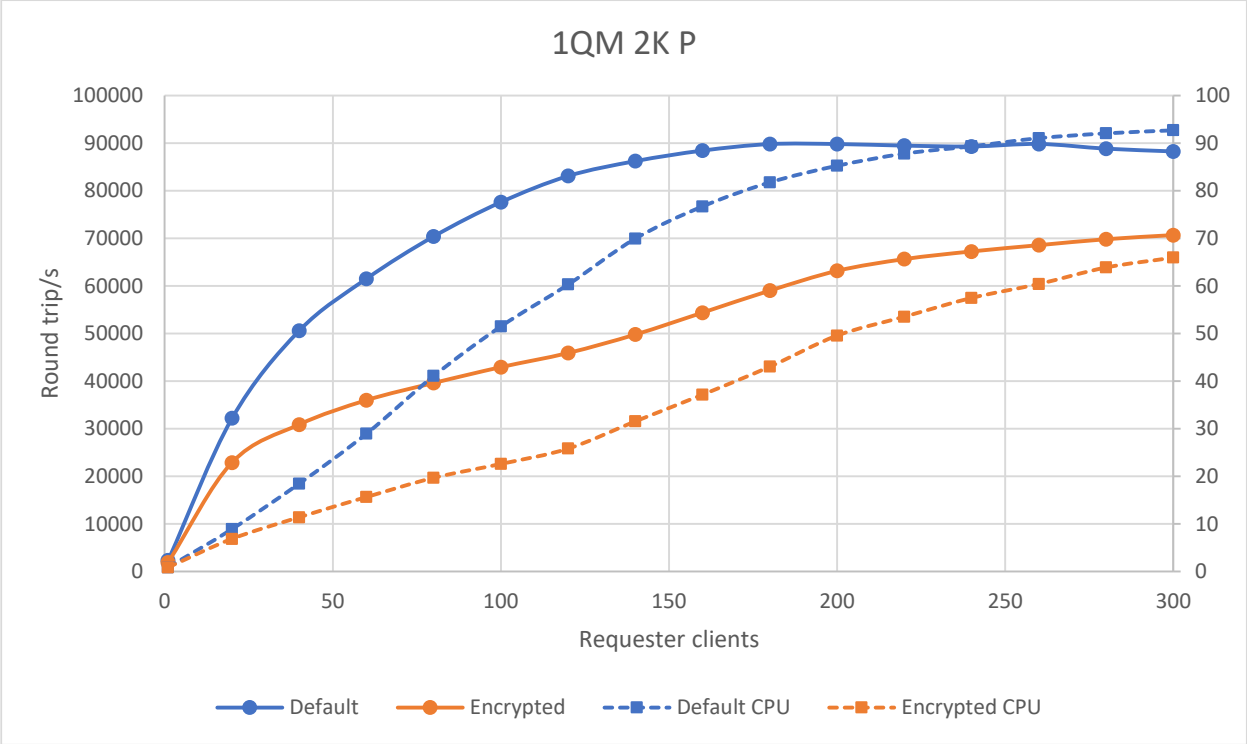

Figure 1 - Impact of filesystem encryption on a single QM on M2002A

The impact of enabling encryption increases latency of a single requester thread sending and receiving 2KB messages by 23%. The maximum throughput achieved across a varying number of requester threads is reduced by up to 45%.

The following table contains the datapoints for the other message sizes in this scenario:

Message Size	Single thread latency increase	Maximum impact on throughput (round trips/s)
256b	23%	-25%
2K	23%	-45%
20K	35%	-55%
200K	56%	-35%

Table 1 - Impact on latency and throughput at various message sizes for a single QM on M2002A

The graph below shows the results from the single QM test using a 2KB message size on a M2002B appliance:

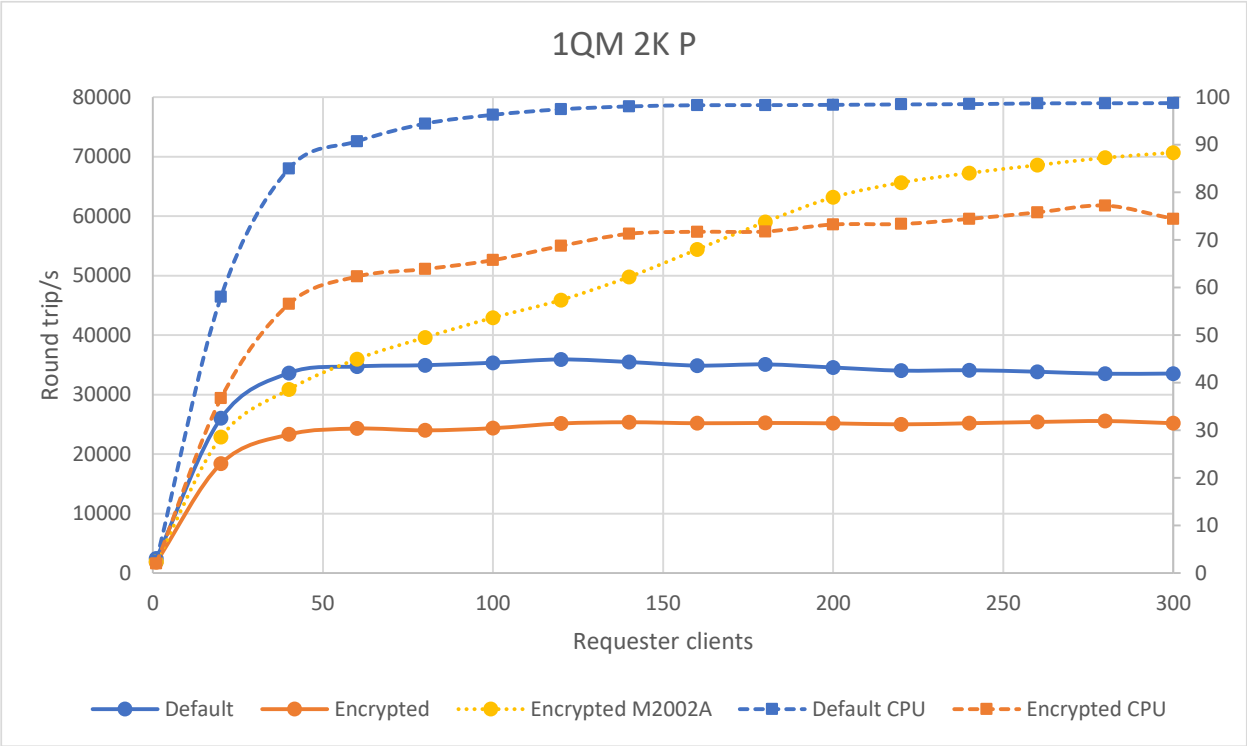

Figure 2 - Impact of filesystem encryption on a single QM on M2002B

The impact of enabling encryption increases latency of a single requester thread sending and receiving 2KB messages by 35%. The maximum throughput achieved across a varying number of requester threads is reduced by up to 31%.

The following table contains the datapoints for the other message sizes in this scenario:

Message Size	**Single thread latency increase**	**Maximum impact on throughput (round trips/s)**
256b	24%	-17%
2K	35%	-31%
20K	41%	-51%
200K	56%	-39%

Table 2 - Impact on latency and throughput at various message sizes for a single QM on M2002B

Multiple QM

The graph below shows the results from the multiple QM test using a 2KB message size on a M2002A appliance:

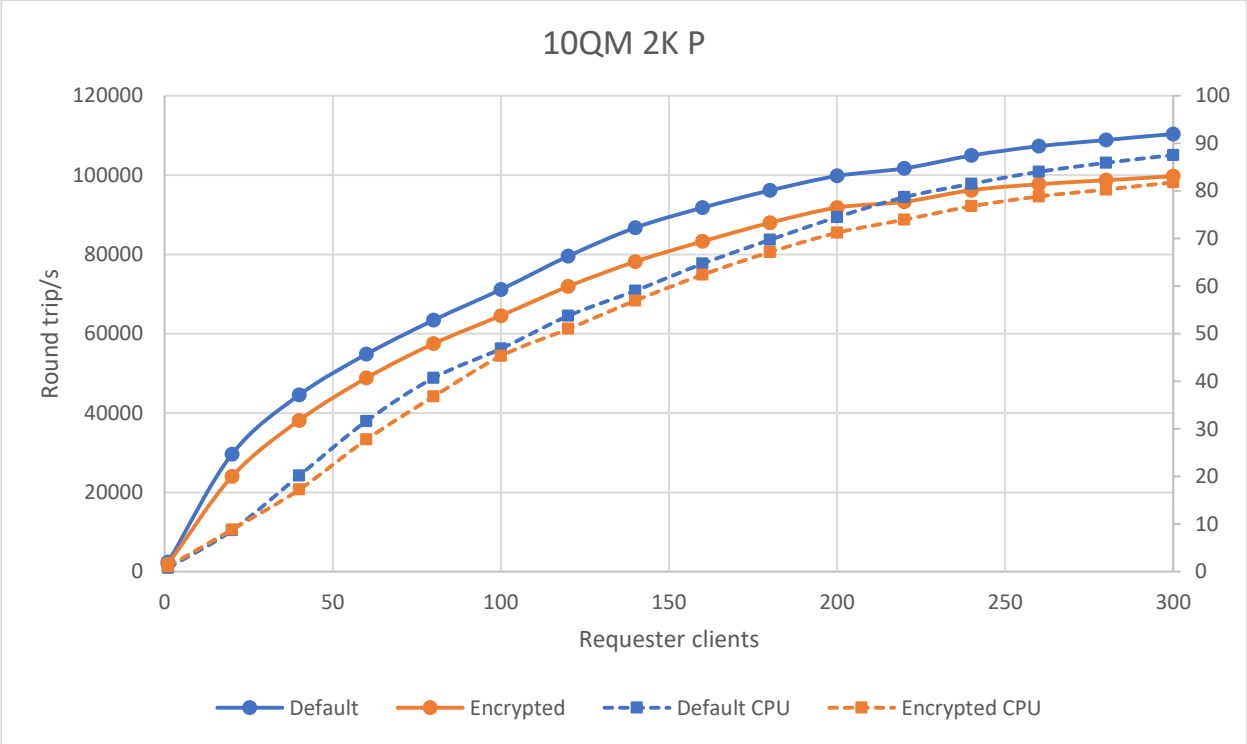

Figure 3 - Impact of filesystem encryption on multiple QM on M2002A

The impact of enabling encryption has a reduced effect on multiple QM because there are multiple threads processing the encryption and recovery log writes. The maximum throughput achieved across a varying number of requester threads is only reduced by up to 11%.

The following table contains the datapoints for the other message sizes in this scenario:

Message Size	**Maximum impact on throughput (round trips/s)**
256b	-11%
2K	-11%
20K	-31%
200K	-28%

Table 3 - Impact on throughput at various message sizes for multiple QM on M2002A

The graph below shows the results from the multiple QM test using a 2KB message size on a M2002B appliance:

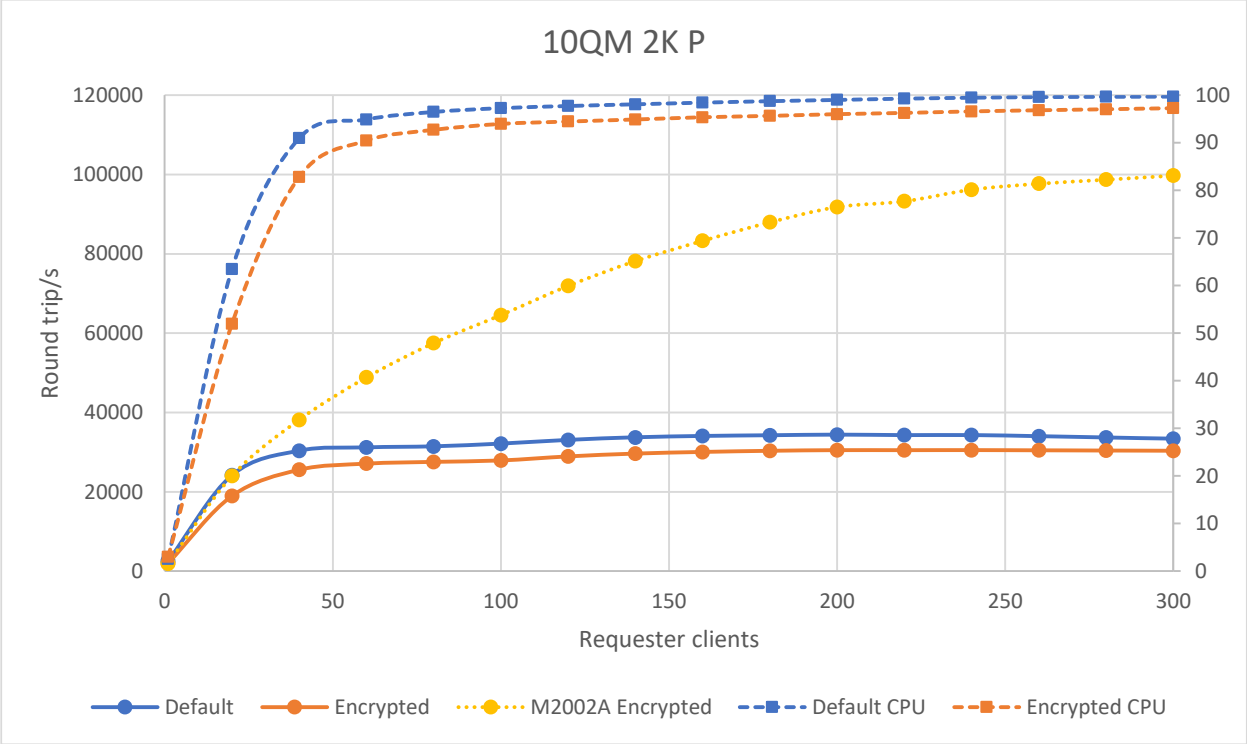

Figure 4 - Impact of filesystem encryption on multiple QM on M2002B

The impact of enabling encryption has a reduced effect on multiple QM because there are multiple threads processing the encryption and recovery log writes. The maximum throughput achieved across a varying number of requester threads is reduced by up to 13%.

The following table contains the datapoints for the other message sizes in this scenario:

Message Size	**Maximum impact on throughput (round trips/s)**
256b	-11%
2K	-13%
20K	-35%
200K	-36%

Table 4 - Impact on throughput at various message sizes for multiple QM on M2002B

Single HA QM

The graph below shows the results from the single HA QM test using a 2KB message size on a M2002A appliance:

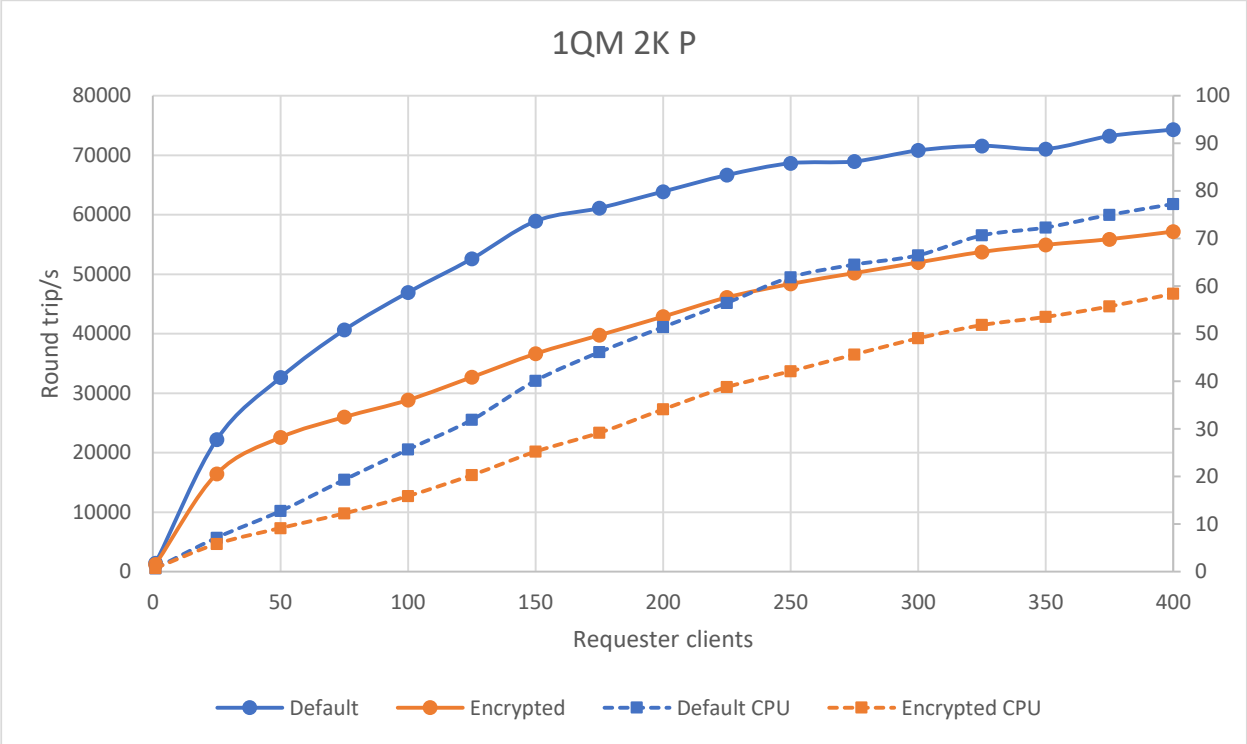

Figure 5 - Impact of filesystem encryption on a single HA QM on M2002A

The impact of enabling encryption increases latency of a single requester thread sending and receiving 2KB messages by 14%. The maximum throughput achieved across a varying number of requester threads is reduced by up to 39%.

The following table contains the datapoints for the other message sizes in this scenario:

Message Size	Single thread latency increase	Maximum impact on throughput (round trips/s)
256b	14%	-33%
2K	14%	-39%
20K	22%	-36%
200K	27%	-25%

Table 5 - Impact on latency and throughput at various message sizes for a single HA QM on M2002A

The graph below shows the results from the single HA QM test using a 2KB message size on a M2002B appliance:

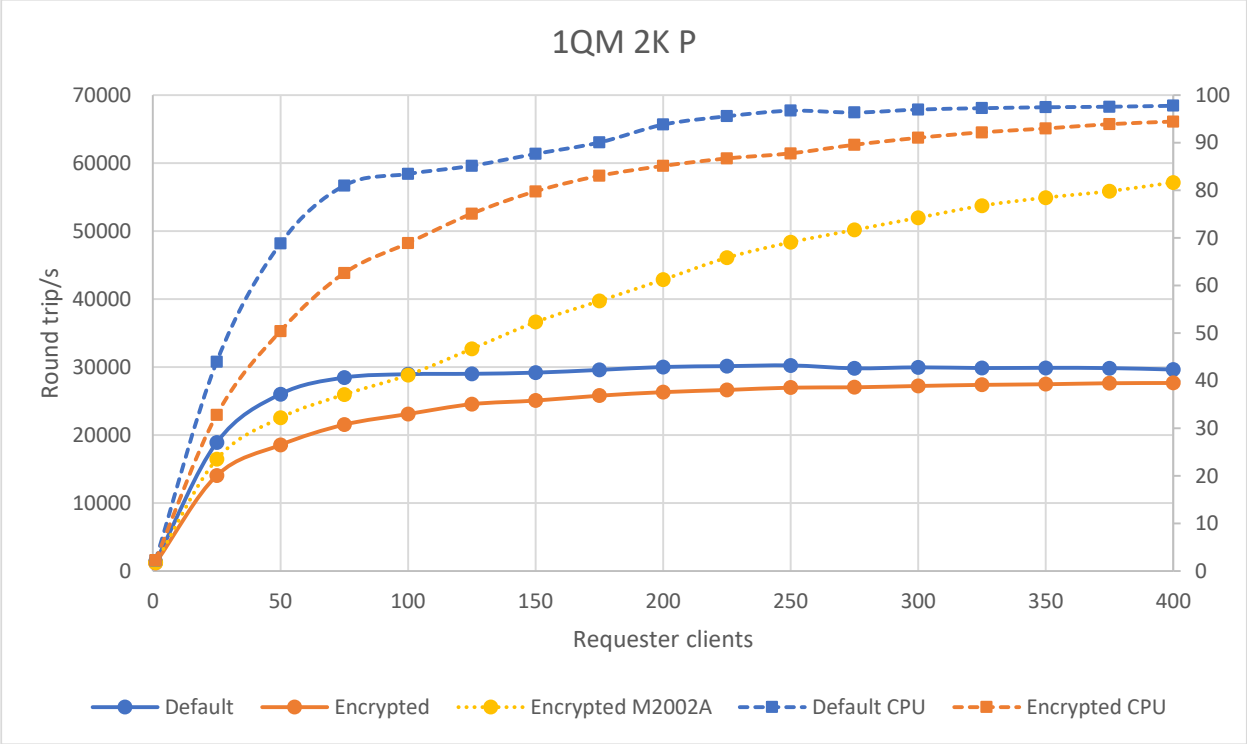

Figure 6 - Impact of filesystem encryption on a single HA QM on M2002B

The impact of enabling encryption increases latency of a single requester thread sending and receiving 2KB messages by 16%. The maximum throughput achieved across a varying number of requester threads is reduced by up to 29%.

The following table contains the datapoints for the other message sizes in this scenario:

Message Size	**Single thread latency increase**	**Maximum impact on throughput (round trips/s)**
256b	14%	-13%
2K	16%	-29%
20K	23%	-33%
200K	27%	-22%

Table 6 - Impact on latency and throughput at various message sizes for a single HA QM on M2002B

Multiple HA QM

The graph below shows the results from the multiple HA QM test using a 2KB message size on M2002A appliances:

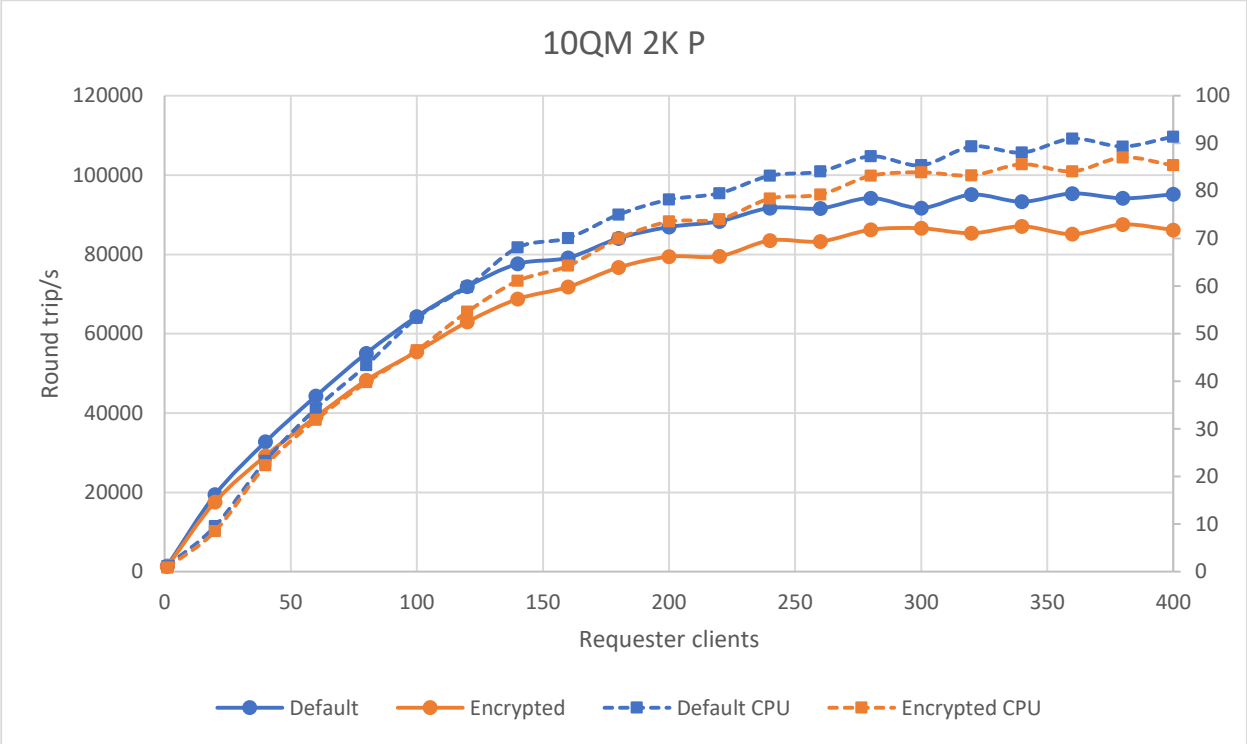

Figure 7 - Impact of filesystem encryption on multiple HA QM on M2002A

The impact of enabling encryption has a reduced effect on multiple QM because there are multiple threads processing the encryption and recovery log writes. The maximum throughput achieved across a varying number of requester threads is only reduced by up to 14%.

The following table contains the datapoints for the other message sizes in this scenario:

Message Size	**Maximum impact on throughput (round trips/s)**
256b	-10%
2K	-14%
20K	-14%
200K	-4%

Table 7 - Impact on throughput at various message sizes for multiple HA QM on M2002A

The graph below shows the results from the multiple HA QM test using a 2KB message size on M2002B appliances:

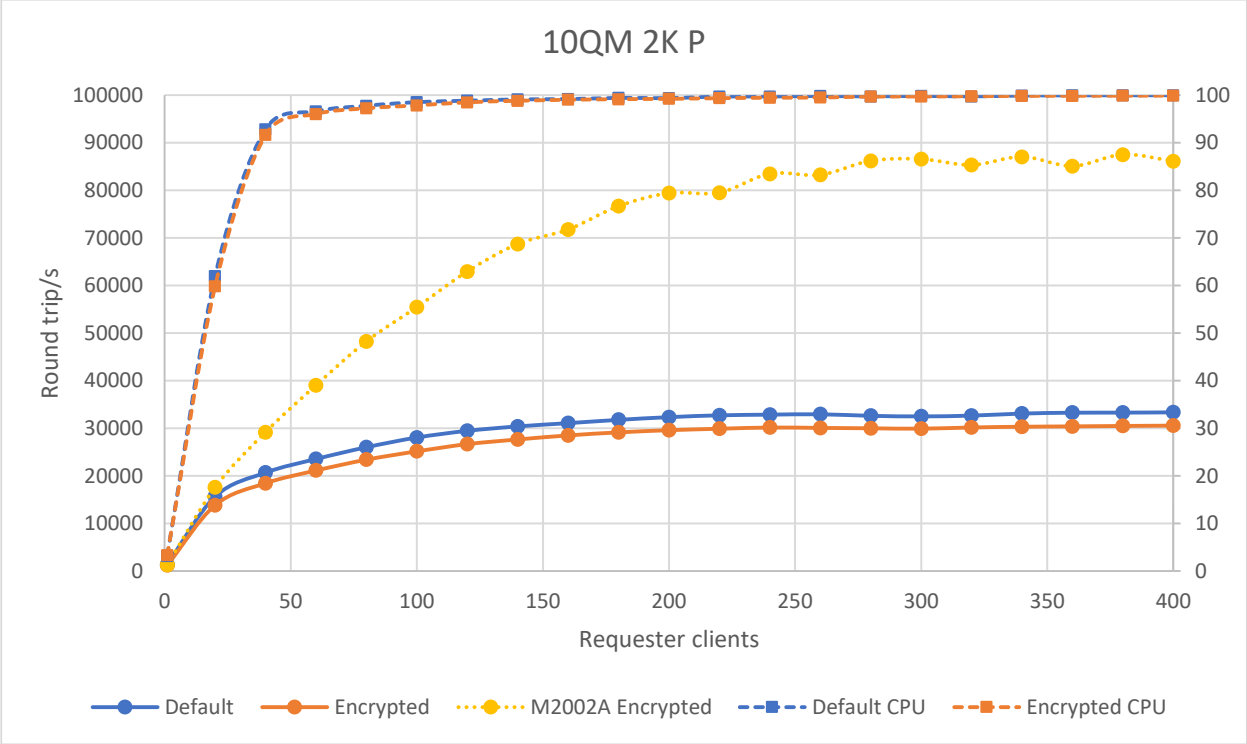

Figure 8 - Impact of filesystem encryption on multiple HA QM on M2002B

The impact of enabling encryption has a reduced effect on multiple QM because there are multiple threads processing the encryption and recovery log writes. The maximum throughput achieved across a varying number of requester threads is only reduced by up to 10%.

The following table contains the datapoints for the other message sizes in this scenario:

Message Size	**Maximum impact on throughput (round trips/s)**
256b	-9%
2K	-10%
20K	-22%
200K	-7%

Table 8 - Impact on throughput at various message sizes for multiple HA QM on M2002B

Conclusions

The new filesystem encryption functionality offers protection for your data at rest within the MQ appliance. There is a small increase in CPU which reflects the cost of encrypting the message payload before persisting that data to storage. There is a similar cost when decrypting the message data after retrieval from storage. Note that in many scenarios, the QM (and the OS) optimize message retrieval by avoiding reading (and therefore decryption) from the IO subsystem.

Throughput on a single Non HA QM will be impacted by up to 45% as the latency of writing data is increased for a 2KB message size. Using multiple Non HA QM helps mitigate the impact of this increase in latency, resulting in a regression of up to 11% of maximum throughput.

Throughput on a single HA QM for a 2KB message size will be impacted by up to 39% as the latency of writing encrypted data to both appliances in the HA group is increased. Using multiple HA QM helps mitigate the impact of this increase in latency, resulting in a regression of up to 14% of maximum throughput.

The data from the M2002B appliance has also been included to help guide you to which model is most appropriate for your deployment.

Author

The author of this whitepaper is Sam Massey who works in the MQ Performance Team at the IBM UK Laboratory, Hursley. If you have any questions or comments on this paper, please contact him at smassey@uk.ibm.com

Appendix A

The two client machines used for the performance tests in this report have the following specification:

Category	Value
Machine	x3550 M5
OS	Red Hat Enterprise Linux Server 7.9
CPU	2x12 (2.6Ghz)
RAM	128GB RAM
Network	10Gb/40Gb Ethernet
Disks	2x 480GB SSD
RAID	ServeRAID M5210 (4GB Flash RAID cache)