AMS 机密性能

目的

验证新的 AMS 机密模式的性能。

背景

MQ 客户通常希望能够对消息有效负载进行静态加密，以确保符合各种安全法规。

由于会频繁出现非对称密钥操作，因此在与非 AMS 消息传递进行对比时，初始 AMS 性能测试的结果会令用户大吃一惊。对于许多用户来说，在签署每个消息并针对每个预期接收者加密对称密钥时所涉及的重复非对称密钥操作往往都会超出他们的需求；他们通常只希望加密有效负载，而不需要对每个消息进行签署，也不需要为每个消息创建对称密钥。

MQ V9 提供了一种全新的 AMS 保护质量功能，即"机密"功能，该功能以对称密钥为基础，而无需进行消息签署，进而可快速实现消息的安全传输，同时也可对有效的静态数据进行妥善保护。

情境

我们将使用一系列不同的情境来分析 AMS 性能：

- 单个队列 - 所有的客户端通过单个队列发送和接收消息
- 多个队列 - 所有的客户端通过 21 个队列中的某个队列发送和接收消息

在本次调研中，所有测试均采用 2KB 持久性消息，而且针对单个接收者对每个消息进行加密。所采用的消息传递情境是当前分布式报告及设备性能报告中常用的请求响应情境。

之后，将会对各种 AMS 保护质量设定下的性能进行对比：

- 无 - 不采用签署或加密
- 完整性 - 对消息进行签署
- 隐私 - 对消息进行签署和加密
- 机密 - 对消息进行加密，可能会复用密钥
    - 使用密钥复用次数设置为 32 次

密钥复用次数设置用于控制重新生成对称密钥的频率。有关保护质量的设置信息及更多信息，请登录 IBM 知识中心：
http://www.ibm.com/support/knowledgecenter/SSFKSJ_9.0.0/com.ibm.mq.sec.doc/q127085.htm

完整性模式和隐私模式中所用的签署算法是 SHA512。隐私模式和机密模式中所用的加密算法是 AES256。

环境

这些测试采用了 3 台 x86_64 Linux 服务器（详细规格见附录 A）；服务器 1 用于托管请求者客户端，服务器 2 用于托管 QM，而服务器 3 用于托管响应者应用。

在向用于接收 AMS 消息的 MQGET API 提供消息缓冲器时，要确保该缓冲器的大小超过预期的消息大小，因为加密后的有效负载大小会远远超过原始消息长度。本报告所对应的测试采用的是一个 20KB 缓冲器，

其中所用的 MQ 版本是 MQ V9.0。

结果

单个队列

下图所示为单个队列测试的结果：

请注意：图中所示的 CPU 百分比是指测试中两个典型客户机的平均值；相比传统示意图中所采用的服务器的 CPU 百分比指标，该指标更具意义，因为加密和解密的成本均核算到客户机成本之中。

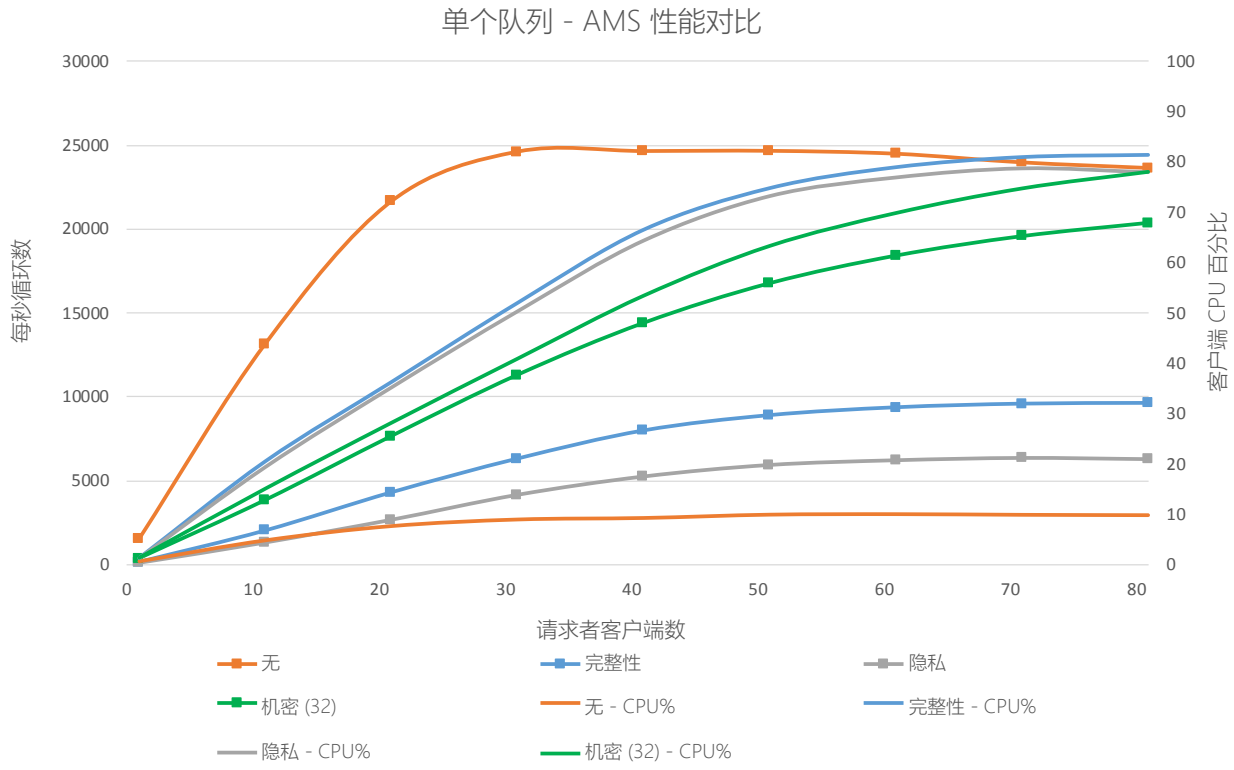

图 1 - 单个队列 AMS 对比

与 AMS 隐私模式相比，AMS 机密模式下的性能高出了 3 倍。当客户端数量为 81 时，尽管 CPU 使用率更高，但 AMS 机密模式下的性能仅比不使用 AMS 的情况低 14%。

多个队列

下图所示为多个队列测试的结果：

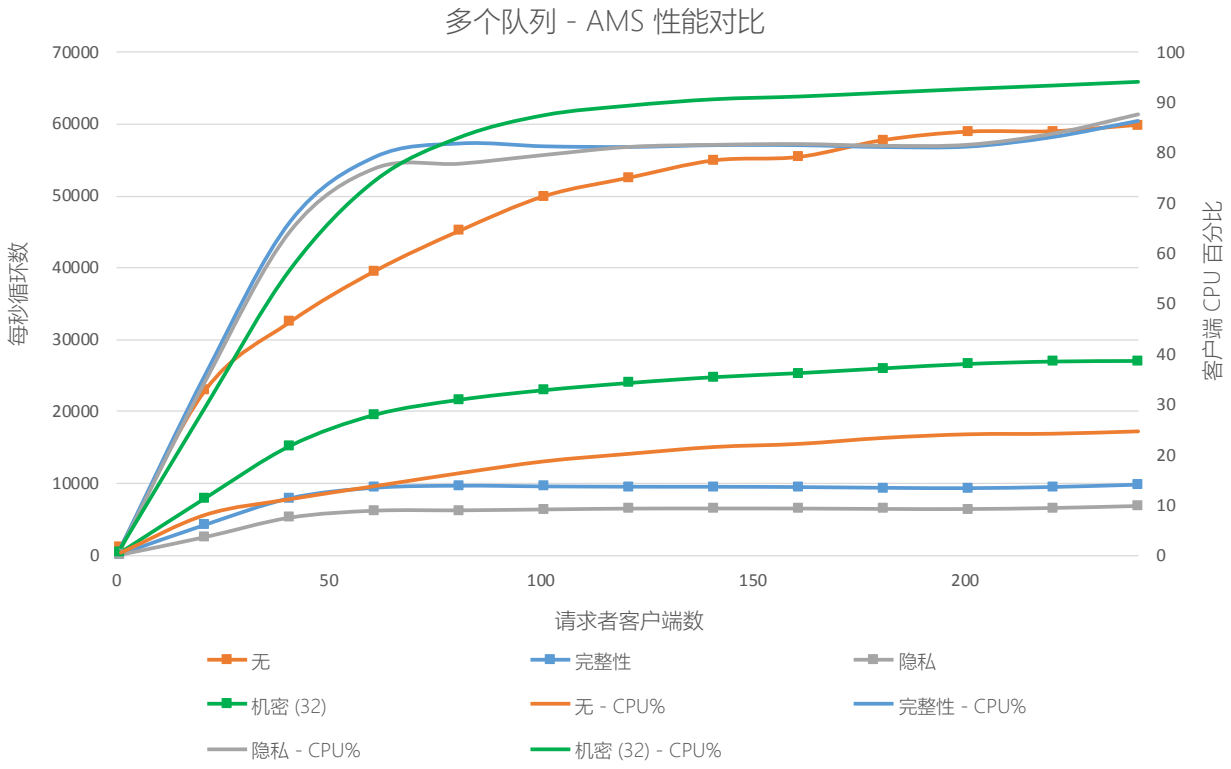

图 2 - 多个队列 AMS 对比

在情境中添加多个队列后，AMS 机密 (32) 模式下的性能可比 AMS 隐私模式提升近 4 倍。此外，在非 AMS 情境下，通过解除队列锁也会导致性能提升，而且当客户端数量为 241 时，AMS 机密 (32) 模式下的性能仅为不使用 AMS 情况时的一半。

当客户数量为 241 时，AMS 机密 (32) 模式下测得的峰值吞吐量刚刚超过 27,000 次循环/秒。在请求/响应者情境中，采用一个请求队列和一个回复队列，因此对于每个消息传递循环来说，会出现 2 次消息推送和 2 次消息获取。在单个推送/单个获取情境中，在相同环境中可获得的最大性能是 54,000 次循环/秒。

AMS 策略对比

在本白皮书所述的对比中，所选择的密钥复用次数为 32 次；之所以选择该数值，是综合考虑密钥重新生成成本（即情境性能）与安全性之后而得出的权衡结果。在对比中，我们收集了一系列数据，旨在验证性能与密钥复用配置之间的线性关系。在下图所示的情境中，每个请求者线程和响应者线程均通过单独的队列发送和接收消息；图中记录了在采用 21 个请求者客户端、21 个响应者线程时的性能结果：

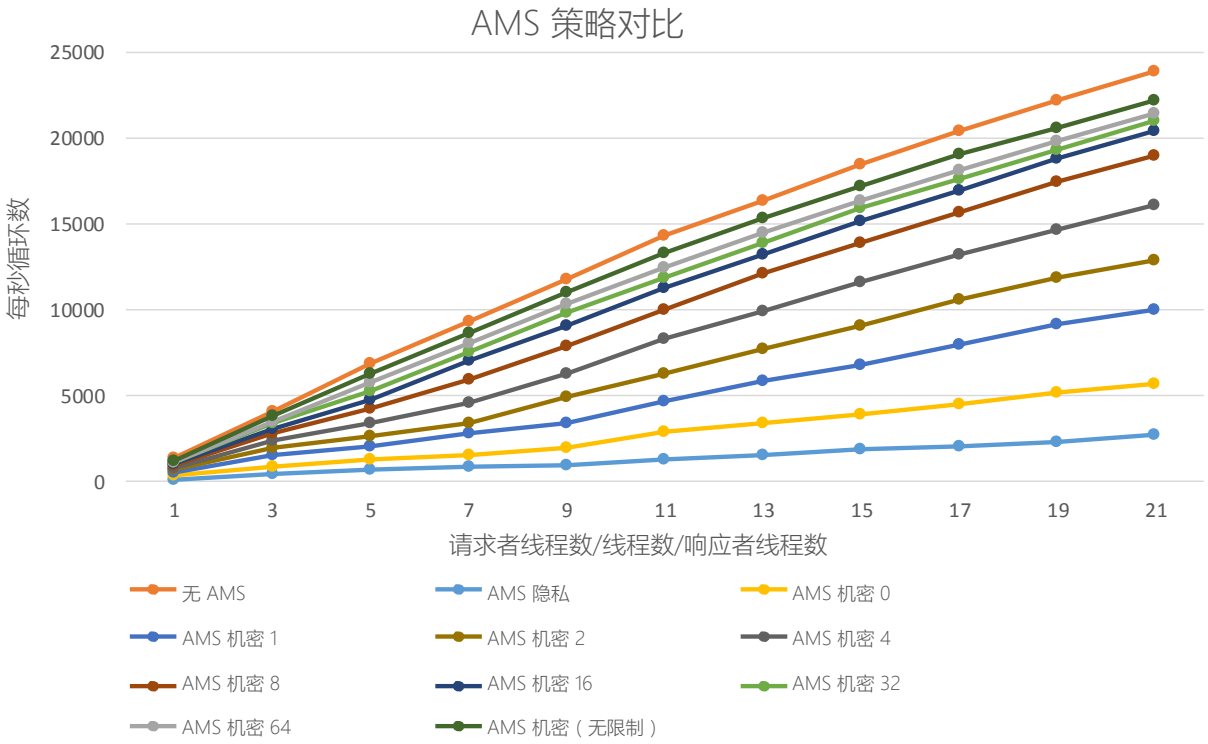

图 3 - AMS 策略对比

AMS 机密 (32) 模式下的性能是 AMS 机密（无限制）模式的 94%，但是仅能针对 32 个消息复用同一对称密钥。

接收缓冲器大小不足的影响

如果缓冲器的大小不足以执行 MQ Get 操作，MQ 客户端就会出现性能低下的现象，导致必须从 MQ QM 执行多个消息检索。下图所示的是多个队列情境中 AMS 机密 (32) 模式下的性能结果，并将其与仅提供大小为 2K 的消息缓冲器时的性能进行了对比：

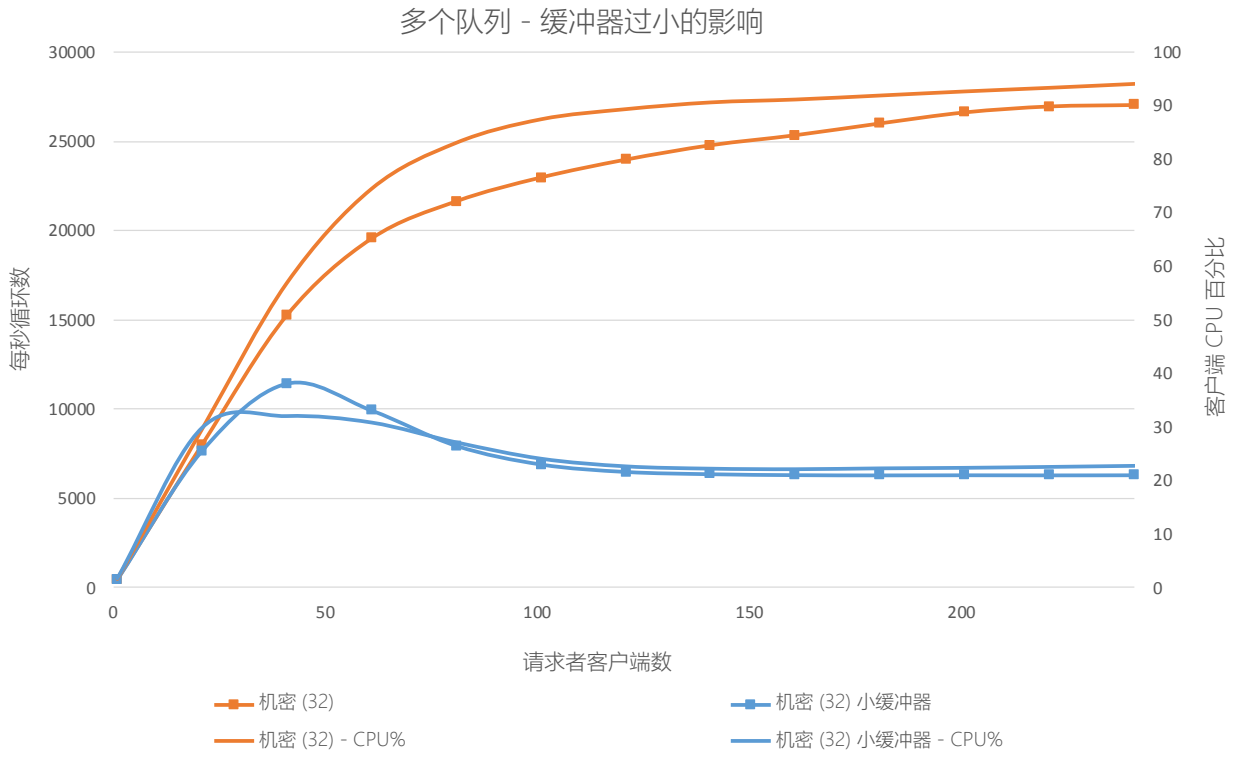

图 4 - 接收缓冲器过小的影响

结论

新的 AMS 机密模式可实现消息有效负载的端到端安全性，可在队列管理器文件系统中确保数据的动态安全和静态安全。该模式有助于减少非对称密钥加密，因此相比之前支持的 AMS 策略，可提供更高的性能。此外，该模式还允许用户定义进行有效负载加密时复用同一对称密钥的频率，因此可在密钥重新生成频率与性能之间进行灵活选择。

作者

本白皮书的作者是 Sam Massey，目前工作于赫斯利 IBM 英国实验室的 MQ 性能团队。如果您对本文有任何疑问或意见，请发送电子邮件至 smassey@uk.ibm.com。

附录 A

本报告中性能测试所使用三台机器的规格如下：

目录	价值
机器	x3550 M5
操作系统	Red Hat Enterprise Linux Server 7.2
CPU	2x12 (2.6Ghz)
RAM	128GB RAM
网络	10Gb/40Gb 以太网
磁盘	2x 480GB SSD
RAID	ServeRAID M5210（4GB 闪存 RAID 缓存）