Crash in qpidd.exe after updating Message Broker server certificate to SHA2

Last Modified on 02/07/2022 10:58 am EST

Symptom

Some customers have experienced crashes when their Secure Hash Algorithm 1 (SHA1) certificates approached expiration and they installed Secure Hash Algorithm 2 (SHA2) server certificates for the Message Broker. The crashes occur between 15 minutes and 45 minutes after the certificate is installed.

Resolution

Either:

- Install SHA1 Message Broker certificate on OnGuard versions 7.0 through 7.4, or
- Upgrade to OnGuard 7.5 or later.

Applies To

OnGuard versions 7.0 through 7.4

Additional Information

In OnGuard 7.4 and earlier, the qpidd.exe Message Broker application is a version of Apache Qpid, which does not provide reliable support for SHA2 server certificates. In OnGuard 7.5 and later, we standardized OnGuard on the Pivotal RabbitMQ Message Broker for Advanced Message Queuing Protocol (AMQP).

For customers experiencing issues with their SHA2 certificates in OnGuard 7.4 or earlier, we recommend upgrading to the latest version of OnGuard and following our Hardening Guide to ensure the most secure profile. Until upgrading to OnGuard 7.5 and later, continue to use SHA1 certificates for the Message Broker. You can also upgrade the other server certificates (NGINX) to SHA2 certificates.

LenelS2 understands the seriousness of customer security concerns, and this motivated our migration to the RabbitMQ messaging platform with more robust security offerings in our latest OnGuard releases.

While we are aware that SHA1 is not considered secure, the threat impact of temporarily allowing SHA1 Transport Layer Security (TLS) is minimal since AMQP is utilized within OnGuard only as an internal protocol.