biwin.co.uk

Additional Considerations

This solution leverages Microsoft Internet Information Services as a reverse proxy in order to account for the following:

- The POODLE vulnerability (CVE-2014-3566 and CVE-2014-8730) affects protocols currently required for OPERA communication. Legacy V5 application servers (OPERA version 5.0.04.02 and below) are affected. In order to properly mitigate POODLE, SSLv3 and TLS 1.0 support should be disabled in favor of TLS 1.2 instead. This can be completed via the updates to SCHANNEL registry settings for IIS.

- SSL certificates issued by a public Certificate Authority must be issued using a SHA-2 cipher after January 1, 2016. The Legacy V5 application server (OPERA version 5.0.04.02 and below) cannot support this cipher. IIS 7.5 allows for SHA-2 support.