SOLUTION

1. Enable OS TLS 1.2 – with reg key
2. SQL Server
   1. SQL Server 2012 SP4  
      SQL Server 2012 – 11.0.6216.27 SP3 GDR TLS 1.2 Update  
      SQL Server 2012 – 11.0.5352.0 SP2 GDR TLS 1.2 Update  
      For additional version info check [here](https://support.microsoft.com/en-us/topic/kb3135244-tls-1-2-support-for-microsoft-sql-server-e4472ef8-90a9-13c1-e4d8-44aad198cdbe)
   2. SQL Server 2014 – check [here](https://support.microsoft.com/en-us/topic/kb3135244-tls-1-2-support-for-microsoft-sql-server-e4472ef8-90a9-13c1-e4d8-44aad198cdbe)
   3. SQL Server 2016 and 2017
3. IIS
   1. Check Sites TLS 1.2 support
4. WSUS
   1. Supports TLS 1.2 if OS is patched
5. SCCM
   1. All clients must have OS enabled support for TLS 1.2
   2. All clients must have .NET 4.6.2 or greater to support TLS 1.2
   3. Read more [here](https://docs.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2)
6. ADFS
7. Check .net installed versions.

**(Get-ItemProperty "HKLM:SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\Full").Version**

* 1. 4.6.2 or greater is required to use TLS 1.2
  2. 3.5 SP1 supports TLS 1.2  
     HKLM\Software\Microsoft\NET Framework Setup\NDP\v3.5\SP dword=1 means .NET 3.5 is SP1

1. Set .NET to give OS permission to choose the protocol – with reg key
2. Disable SSL 3.0, TLS 1.0, TLS 1.1 – with reg key
3. Restart computer
4. Test connection to Domain Controller with Powershell  
   Test-ComputerSecureChannel