SQL Server Installation

The following are the installation procedures for a standard install of SQL server on a new server through GUI.

1. Set server power plan to High.
2. Create local “Documents” folder on C: drive and copy SQL-Setup-AuxilaryFiles there.
3. Navigate to the local folder containing the RTM install and launch the Setup.exe
4. Click the Installation option on the left pane then choose New SQL Server stand-alone installation or features to an existing installation
5. Cycle through each screen. On the Feature Selection screen, select Database Engine Service and other features as needed.
6. Unless applications specify a named instance, use Default instance on the Instance Configuration screen
7. On The Server Configuration screen change the Account Name for SQL Server Agent and SQL Server Database Engine, SQL Server Analysis Services, & SQL Server Integration Services to the service account that was created for this instance.
   1. Enter the password for each account.
   2. Set Startup Type to Automatic for all services (except SQL Server Browser which should be disabled by default)
8. On the Database Engine Configuration screen:
   1. Server Configuration Tab
      1. We will typically use Mixed Mode
      2. Enter the strong SA password that was generated in the Prerequisites tasks
      3. Add DBA group in the SQL Server Administrators box
   2. Data Directories Tab
      1. Data Root Directory: J:\sqldata
      2. User database log directory: L:\sqllogs
      3. Backup directory: Z:\sqlbackups
      4. Temp DB directory: T:\sqldata and T:\sqllogs
9. Begin Install
10. After install, ensure services are running and connection through SSMS can be made
    1. Disable the CEIP services
11. Enable permanent trace flags by opening SQL Configuration Manager, right-click the "SQL Server" service an choose properties
    1. Click Startup Parameters and add the following entries
       1. -T1117 (autogrow equally) DISCONTINUED for 2017
       2. -T1118 (full extents only) DISCONTINUED for 2017
       3. -T1224 (disables lock escalation)
       4. -T2371 (dynamic threshhold for stat update instead of 20% so triggers at lower level for large tables)
       5. -T4199 (enable query optimizer hotfixes)
    2. Click Apply then OK
    3. Restart SQL Service
    4. Using SSMS run DBCC TRACESTATUS to ensure flags have been turned on
12. Open Administrative tools | Local Security Policy
    1. Go to Local Policies then User Rights Assignment
       1. Open Perform volume maintenance tasks and add the SQL Server service account for this server (done during install with SQL 2017)
13. Install latest SQL Service Pack and CU. (if available)
14. Run SQL-Setup-DBAWORK\DBAWORK\_Setup.sql
    1. If needed detach and move .mdf and .log files to correct folders
15. SQL Server Properties (use the following defaults unless otherwise specified)
    1. Set Maximum Server Memory - leave 10% for OS
    2. Set Max Degree of Parallelism as needed
16. Configure Tempdb - Determine number of files and calculate maximum size for data files and log
    1. Total tempdb size should be approximately 10% of the total size of databases
    2. If your server has less than 8 logical cores (e.g. a one CPU server with 4 physical cores and hyperthreading enabled has 8 logical cores), use # tempdb data files = # logical cores, equally sized

* If your server has more than 8 logical cores, start with 8 tempdb data files
* Data and log file to be presized to use most of disk and auto growth disabled.

1. Install prerequisite scripts
   1. OlaMaintenanceSolution.sql -this creates backup, index defrag, and db integrity check jobs
      1. <https://ola.hallengren.com/>
      2. Schedule maintenance jobs - Run OlaJobSchedules.sql to set initial times
   2. Who\_Is\_Active.sql -this creates the sp\_WhoIsActive proc in the master database
      1. http://whoisactive.com/
2. Run Post-Installation scripts located in SQL-Setup-PerformanceMonitor
   1. IndexAllFragmentation.sql - performance monitoring
3. Once Production Databases have been setup run SQL-Setup-Alerts: Generate SQL\_alerts.sql. Change the output to "Results to Text" and copy and run the results in a new query window. You may need to change the text output on your machine to max characters to get the full script.
4. If SQL 2017 or higher Run: Tasks > Vulnerability Assessment on each database and review/remediate findings