**Windows OS Installation**

1. All drives partition aligned.
2. Hyper threading enabled in the Bios.
3. OS and installed applications drive use RAID 1 and use NTFS with default Allocation Unit Size.
4. OS installed to C Drive.
5. Domain Administrators group added to the Local Administrators group.
6. Account Policies enforced by GPO or set explicitly.
   1. Password Policy
      1. Enforce password history = Last 10
      2. Maximum password age = 90 days
      3. Minimum password age = 7 days
      4. Minimum password length = 8
      5. Password must meet complexity requirements = Enabled
   2. Account Lockout Policy
      1. Account lockout threshold = 5 invalid login attempts
7. Local Policies enforced by GPO or set explicitly.
   1. Audit Policy set to audit Success and Failure of
      1. Audit account logon events
      2. Audit account management
      3. Audit logon events
      4. Audit policy change
      5. Audit system events
   2. Security Options
      1. Interactive logon: Do not display last user name – Enabled
      2. Interactive logon: Message text for users attempting to log on – Set to Legal Disclaimer for access to production servers
      3. Interactive logon: Message title for users attempting to log on – Set to Legal Message Titled for access to production servers.
8. Everyone User removed from non-C drives.
9. All applications installed to D Drive and not C Drive.
10. Windows Updates configured to download but not install.
11. NIC’s configured as teamed (if appropriate), set to Full Duplex and maximum network speed (usually 1GB).
12. Validate IO Subsystem configuration is optimal using SQLIO and test alternate configurations to determine optimum configuration for SQL.
13. If using SAN Storage test HBA Queue Depth settings at 64 and 128 in conjunction with SAN admin to determine the optimal setting for the server based on IO demands and impact to other systems using the SAN, ensure that MPIO is configured properly.  (Going to high on the SQL Server can allow it to dominate the SAN, reducing performance of other systems using SAN storage on different disk arrays)
14. Anti-Virus Software installed and configured to update from root server.
15. System Added to SCOM for monitoring.

**Pre-Installation of SQL Server**

1. Separate RAID Arrays for Data and Log files.  Tempdb on dedicated array.
2. Data, Log, and Tempdb drives formatted with 64K Allocation Unit Size.
3. SQL Server Admins Group added to the Local Administrators Group.
4. Create AD Service User Account, or Local User Account for non-domain servers, with no permissions.
   1. Add the **readServicePrincipalName** and **writeServicePrincipalName** permissions to the Service Account in AD (<http://support.microsoft.com/kb/319723>) & grant **Perform Volume Maintenance Tasks** **& Lock Pages in Memory** under local security policy to the SQL service account.
5. Configure the Data drive with Drive letter E in Windows.
6. Configure the Log drive with Drive letter L in Windows.
7. Configure the TempDB drive with Drive letter T in Windows.
8. Configure additional Data drives with Drive letter F, G, etc. skipping previously reserved Drive letters and M (cluster MSDTC) and Q (cluster Quorum).
9. Add the AD Service User Account to the Root path with Full Control of D, and List Folder Contents Permissions for Data, Log and Tempdb Drives.
10. Create SQLData folder on Data and Tempdb Drives
11. Add the AD Service User Account with Full Control of SQLData folder on Data and Tempdb Drives
12. Create SQLLogs folder on Log Drive
13. Add the AD Service User Account with Full Control of SQLLogs folder on Log Drive

**SQL Server Installation**

1. Use the previously configured Service Account as the startup account for the SQL Service.
2. Install the binaries to the D Drive.
3. If installing SQL Server 2008 set the default file paths according to the previous drive configuration.
4. Set SQL Server, and SQL Agent to startup Automatically.  Disable the Browser Service unless installing Named Instances or multiple instances on the Server.
5. Apply latest Service Pack and Cumulative Update based on SQL Server version.
6. Provision SQL Admins group in the sysadmin fixed server role.

**Post-Installation Steps**

1. Add the SQLServerMSSQLUser$<ServerName>$<InstanceName> group to the Root path with Full Control of D, and List Folder Contents Permissions for Data, Log and Tempdb Drives.
2. Add the SQLServerMSSQLUser$<ServerName>$<InstanceName> group with Full Control of SQLData folder on Data and Tempdb Drives.
3. Add the SQLServerMSSQLUser$<ServerName>$<InstanceName> group with Full Control of SQLLogs folder on Log Drive.
4. Remove the AD Service User Account from the Root Path. (This decouples the Service Account explicitly and relys on the group)
5. Add the SQLServerMSSQLUser$<ServerName>$<InstanceName>, SQLServerSQLAgentUser$<ServerName>$<InstanceName>, or other group accounts to any Backup, or processing folders as needed.
6. In the Local Security Policy, add the SQLServerMSSQLUser$<ServerName>$<InstanceName> group to the Perform Volume Maintenance Tasks and Lock Pages in Memory objects.
7. Exclude Data, Log, Tempdb, any Backup file paths, and the SQL Server Binaries folders from AntiVirus Scans.
8. Remove Builtin\Admins from sysadmin fixed server role.
9. Enable Failed Login Auditing in the SQL Server Security Settings
10. Enable TCP/IP and change default port from 1433.
11. Enable remote DAC connections.
12. Enable as required xp\_cmdshell, SQLCLR, and OLE Automation for the SQL Server Instance.
    1. Configure xp\_cmdshell proxy account as required.
13. Enable DatabaseMail and configure default public and private accounts.
14. Configure SQL Error Log retention for 30 log files
15. Configure SQL Agent job to perform nightly log rollover.
16. Configure SQL Agent jobs for database backups, CHECKDB, index maintenance, statistics updates, backup cleanup, and history cleanup.
17. Move MSDB Database files to SQLData and SQLLogs respectively.
18. Reconfigure Tempdb with data files equal to 1/2-1/4 the physical CPU’s on the server based on load characteristics.  Set data files to the same size based on load characteristics in 4096MB increments for Datafiles, and 1024MB increments for Log files.  Set AutoGrowth to 1024MB for data files and 512MB for Log file.
19. Enable Trace Flag 1118 on SQL Server 2000 and SQL Server 2005 for Tempdb.
20. Set Model database to SIMPLE recovery, 2048MB default datafile size and 1024MB default logfile size.  Set AutoGrowth to 1024MB for data files and 512MB for Log file.
21. Set Max Server Memory based on installed RAM and installation type (Newer Servers are all 64bit, but enable AWE as needed on 32 bit servers).
    1. 8GB RAM = 6144 Max Server Memory
    2. 16GB RAM = 12228 Max Server Memory
    3. 32GB RAM = 28672 Max Server Memory
    4. These are base values that will later be adjusted based on the Memory\Available MBytes counter being > 150 on the Server.
22. Set **max degree of parallelism**sp\_configure option based on the number of physical CPU cores installed and anticipated workload
    1. For OLTP, generally set to 1/2 or 1/4 of the physical cores available on the server.
    2. Adjusted up or down based on wait stats and load.
23. Set **cost threshold of parallelism** sp\_configure option based on the anticipated load.
    1. General default value of 5 is low for most OLTP workloads and should be increased.
    2. Base value of 20-25 used for most server installs.
24. Add AD login (standard for environment and locked out in AD by default) for patching and emergency server access to Local Administrators Group.
25. Set SA user password to standardized password that is changed quarterly on all servers and maintained in password safe.
26. Have Server Team remove SQL Admins from Local Administrators Group. ( Not yet implemented in my environment but coming very soon! )

As you can see there are a number of steps involved in provisioning a new SQL Server.  Checklists such as this one ensure that all of the require steps have been accomplished and ensure that the servers are configured identically.   This simplifies documentation and management of the systems in the environment.  If you read Brent’s blog posts, you will notice that there are steps included in his checklist, such as setting up alerts for critical errors, that aren’t in my own list.   The reason for this is that we use SCOM for monitoring, and have built custom Rules into SCOM that capture these errors and generate alerts through SCOM for those events.  This simplifies the configuration of individual servers since the rules are standard for all SQL Servers managed by SCOM.