**Microsoft SQL Server Installation and Configuration Guide**

1. **Description**

MSSQL installation and configuration guide.

1. **Overview**

The following are the configuration and setup steps for installing and setting up a new MSSQL instance in any environment.

1. **Reporting/Stakeholders**

Nessus CIS benchmark scans should be reviewed by NOC/DBA post install to be sure that the new instance conforms to the company’s security standards.

1. **Detailed Procedure**
   1. Update the MSSQL instance to the latest SP and CU
   2. Layout multi-file tempdb following Microsoft best practices
      1. <https://support.microsoft.com/en-us/help/2154845/recommendations-to-reduce-allocation-contention-in-sql-server-tempdb-d>
   3. Create separate data, log & tempdb drives (optional)
   4. Set memory settings
   5. Adjust model database sizes
   6. Grant ‘lock pages in memory’ and ‘volume management’ rights to SQL service account
   7. Setup standard management and monitoring accounts
      1. \_sqlmeta
   8. Create standard database maintenance jobs
      1. Integrity Checks
      2. Index maintenance
      3. Statistics maintenance
      4. Backups (as needed)
         1. Full
         2. Diff
         3. T-Logs
   9. Enable trace flag -T1118 (enabled by default in 2016+)
   10. Adjust Remote Query Timeout as needed
   11. Adjust MDOP as needed
   12. Adjust cost threshold for parallelism as needed (50 should be default)
       1. Prevent small query parallel processing SPID storms
   13. Make sure backups are configured (Either SQL or DPM)
   14. Check TCP port used and change to a static; use non-standard port (not 1433) for hardening
   15. Review PCI hardening standards and apply as possible
       1. MSSQL Configuration Settings
          1. Ensure 'Ad Hoc Distributed Queries' Server Configuration Option is set to '0'
          2. Ensure 'CLR Enabled' Server Configuration Option is set to '0'
          3. Ensure 'Cross DB Ownership Chaining' Server Configuration Option is set to '0'
          4. Ensure 'Database Mail XPs' Server Configuration Option is set to '0'
          5. Ensure 'Ole Automation Procedures' Server Configuration Option is set to '0'
          6. Ensure 'Remote Access' Server Configuration Option is set to '0'
             1. Cannot disable if using Windows core
          7. Ensure 'Remote Admin Connections' Server Configuration Option is set to '0'
          8. Ensure 'Scan for Startup Procs' Server Configuration Option is set to '0'
          9. Ensure 'Trustworthy' Database Property is set to 'Off'
          10. Ensure 'xp\_cmdshell' Server Configuration Option is set to '0'
          11. Ensure 'Default Trace Enabled' Server Configuration Option is set to '1'
       2. Ensure 'Orphaned Users' are Dropped from SQL Server Databases
       3. Ensure CONNECT permissions on the 'guest user' is Revoked within all SQL Server databases excluding the master, msdb and tempdb
       4. Ensure 'AUTO\_CLOSE OFF' is set on contained databases
       5. Ensure Unnecessary SQL Server Protocols are set to 'Disabled'
       6. Disable and rename ‘sa’
       7. Use windows authentication mode
       8. Use different AD accounts for all SQL services on each server
          1. Do not make service accounts admins
          2. Use GMSA’s if possible
       9. Enable ‘Hide Instance’ in network settings (careful with this, can screw up SSIS package execution and other SQL Agent job related stuff)
          1. If not doing this disable SQL browser service
       10. All connections must specify port to connect
       11. Configure SQL auditing to Windows Event Logs
           1. Enable logging of all successful and failed logins
       12. Bump SQL error logs to 12
   16. Be sure all SQL related services are set for automatic startup
   17. Be sure bitlocker 'Symmetric Key encryption algorithm' is set to 'AES\_128' or higher
   18. Be sure user database(s) are set with the appropriate database recovery model
   19. Be sure user database(s) data and log files are set to grow appropriately (fixed sizes are better than percentages)
   20. Add new instance info to SQL meta collector node
   21. SQL Server 2016+ - Disable CEI
       1. SQLDisableCEI.ps script

Notes:

* If you are seeing a problem with the SQL Server Agent not wanting to start you may need to check SQL Server Agent->Properties->Connection and set the Alias local host server to use the correct instance and port connection string.

Revision History

Document Change Contributor Change Date Reviewer Approval Date

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Procedure Creation |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |