

IT Security Hardening Guide for SQL Server Databases



Copyright© 20

Document Control

Document Information

Information	
Document Id	
Document Owner	
Issue Date	
File Name	Hardening Guide for SQL Server Databases

Document History

The document history and versions are maintained when the document is uploaded to the <<Project SharePoint Site>>.

Copyright© 2014

IT Security Hardening Guide for SQL Server Databases

Version	Date	Changed By	Purpose of Revision
1.0	07/22/2011		

This document applies to all new and existing SQL Servers starting [redacted] and outlines the baseline configuration and additional hardening of SQL Server configurations to ensure compliance with IT security configuration standards for currency and validity.

Approving Authority: IT security configuration standards and changes are approved by the System Owner and ISO

1. **Responsibility**
   IT Network Engineers and Database Administrators

2. **Description**
   This document outlines the baseline configuration and hardening of SQL servers configurations to ensure compliance with IT Security configuration standards. This document applies to all SQL Server database servers.

3. **Guidance Websites**

   SQL Server 2008 R2 Security Best Practices Whitepaper
   (available from Microsoft Download Center)

Copyright© [redacted]

SQL Server instance-level fixed roles
(http://msdn.microsoft.com/en-us/library/ms188659.aspx)

SQL Server database level fixed roles
(http://msdn.microsoft.com/en-us/library/ms189612.aspx)

4. SQL Server Security Configuration Standards / Hardening Practices

1. General Requirements
   i. This document applies to all SQL Servers.
   ii. This document assumes compliance with Windows Server configuration and hardening document.
   iii. Install only the services required for the environment.
   iv. Place the SQL Server in a physically secured area.
   v. Place the SQL Server on a dedicated physical or virtual server. Do not install on a Domain Controller.
   vi. Format all drive volumes with NTFS.
   vii. Avoid applications such as Adobe, MS Office, and Java unless required by the SQL Server on the specific server.

2. SQL Server Installation
   i. Ensure that all Microsoft Windows patches have been applied before beginning SQL Server installation.
   ii. Run pre-security scan (networking)
   iii. Install only the SQL services required for the environment.
      - Coordinate with the DBA to understand which SQL services are required for the specific environment. Options include: Database Engine, Integration Services (SSIS, Reporting Services (SSRS), Analysis Services (SSAS), Client Tools (SSMS), Developer Tool Kits, and Full Text Search.
        SQL Server Express options include Database Engine and Management Studio.
      - Do not install Developer Resource Tool Kits or sample databases (i.e. AdventureWorks) in Staging or Production environments.
      - SSRS is only approved for internal-facing use at this time. It uses port 80 by default but you can use the Reporting Services Configuration Manager to change the default port and import a SSL certificate. Configure this to run over 443 for **Client** Servers
      - Unnecessary SQL components running on the server can impact performance.
   iv. Prepare separate SAN disk volumes (separate arrays preferred) to hold the following SQL Server related files:
      1. TempDB
      2. Data files (may require multiple disks to avoid performance impact of disk contention)

Copyright© [redacted]

3. Log files
4. Backup files

Do not store these files on the operating system drive(s) C.
Exception 1: SQL Server Express is a free small-footprint database engine with maximum database size 10GB (sql2008r2), therefore the files may be consolidated on a local non-OS drive (D, E,etc.).

v. When creating instance name, limit the name to less than 16 characters with no reference to a version number or other sensitive information.
vi. Service accounts for the SQL Services (MS SQL, SQLAgent, SSRS, SSAS) should use domain accounts designed for SQL Server.
    1. Requests for new service accounts will follow the standard request process.
    2. Grant permissions to SQL Service accounts to the SQL Server Files mentioned above.
    3. The service account(s) do not require "Log on locally"
    4. Administrators will login using their individual network accounts, unless there is a specific functionality that is only available by the service account.
    5. The account names and passwords must be saved in the password management system.
vii. When assigning database administrators to the server system admin role, map their Windows DBA group name, not the individual DBAs.
viii. The SQL Server SA account must have a strong password, and is recorded in the password management system.
ix. The SA account owns SQL objects (databases) and is required during upgrades, therefore should remain enabled. Only, if the application supports the disabling of SA will it be disabled.
x. The SA account is renamed to help protect its identity. (Compliancy with existing systems is 2nd quarter 2014.) Non-compliance will be documented in either the application's administration guide, hardening guide, or as an exception request.
xi. Ensure all current SQL Server service packs and hotfixes are installed.

3. Network Configurations for SQL Server
    i. Establish a firewall between SQL Servers and the Internet.
    Block TCP port 1433 and UDP port on your perimeter firewall.
    ii. On Production environments, and optionally on Staging, change the SQL Server default ports (1433, 1434) to further protect sensitive data. **Client** has set a standard to use ports 9003 and 9004.
        - Exception – In a cluster, SQL requires UPD port 1434 to control the SQL Server Browser service which is required on named instances.
        - Exception – Vendor solutions may be excluded with a letter from Vendor verifying that change is not supported.

Copyright© 2[redacted]

- Exception – SQL Express is configured to dynamically select a TCP port. This enables several instances of SQL Express to be installed on the same computer.
- The use of different SQL ports in other environments is guideline only.

4. SQL Server Configuration
   i. Disable Named Pipes network protocol
      - Exception – Named Pipes is required in a cluster to communicate with the SQL instances.
   ii. Disable SQL Mail (use database mail instead)
   iii. Disable SQL Server Browser Service
      - Exception – Browser is required for SQL named instances, typically found in clustered environments
      - Exception – The Browser Service is installed with SQL Express. The Browser Service informs client computers which port each instance of SQL Express is using. If the SQL Server Browser Service is not running, remote clients may not be able to connect to SQL Server Express.
   iv. Disable access to extended stored procedures and registry extended stored procedures if possible.
   v. Coordinate with IT engineers to enable a 3rd party backup software's schedule

5. Access Controls
   i. Users will be added to Domain groups, and those groups will be used as SQL logins. Users will not be added as logins and should not use SQL Authentication.
   ii. If SQL Authentication is required by the application, the password should be strong following **Client** policy, and the account/password must be saved in the password management system.
   iii. Permissions should be granted to roles, not individual user accounts.
   iv. Use fixed server roles sysadmin, serveradmin, setupadmin etc, to support administrative activities.
   v. Remove default BUILTIN\Administrators SQL login
   vi. Remove default NT AUTHORITY\SYSTEM SQL login [Guidance only, Compliance not required. This control is under review for impact. According to Microsoft their recommendation is not to remove this account. http://support.microsoft.com/kb/932881]
   vii. Secure Guest and Public
      1. Remove the guest user from all databases
      2. Do not grant object permissions to PUBLIC or GUEST
      3. Avoid assigning predefined roles to PUBLIC or GUEST
   viii. Do not assign the GRANT option of object permission to a user or role
   ix. Create user-defined database roles to assign permissions to objects in the database when a pre-defined database role does not supply the appropriate permissions to a group of users.

Copyright© [redacted]

x. Grant DDL statement permissions to only the database and schema owner, not individual users
xi. Grant execute permissions on stored procedures to database roles (not users)
xii. Use linked servers rather than remote servers where required. Enable Kerberos to securely manage linked servers.
xiii. When storing sensitive data such as SSN, pins, bank account numbers, an encryption routine is required at the database level, if encryption is not occurring at the application level.
xiv. If possible implement TDE

6. Final Verification
   i. Run post security scan procedures to include security approval. (networking)

5. Review

This IT Hardening Guide is reviewed yearly by the Business Solutions Manager, and by the Data Custodians of the **Client** Administration.

Approval Signatures			
Printed Name	**Signature**	**Date**	**Title**

Copyright© [redacted]