SQL Server Security Checklist

By: Tibor Nagy | Last Updated: 2014-02-06 | Comments (3) | Related Tips: More > Security

Problem

I have to install a new Microsoft SQL Server box and configure it as a production server. I know that there are many security related settings and I do not want anyone to hack the system on the first day on the network. Which are the basic steps to harden the security of my SQL Server? Do you have a checklist to start with? Check out this tip to learn more.

Solution

There are many security related settings in the Microsoft SQL Server and you should also consider setting up processes to ensure that the security is maintained in the future. The security related tasks can be divided into four main categories: physical security, operating system level security, SQL Server configuration and user management. You should protect your server physically, have a secure OS and then you can start thinking about your SQL Server.

Physical Security

The first line of your security is the physical security of your on premise hardware. You have to protect your server from being tampered with. Here are the basic items I would recommend:

- **Limit the number of employees who have access to the physical hardware.** You can limit access with access codes, entry cards or even with armed security guards. The most important point is to have a minimal number of people who have access and you should have written procedures to access the server, preferably with managerial approval for physical access rights.
- **Store the backup media at a secure offsite location.** To increase security, it is recommended to have one location for the production server and a separate location for the backup files.
- **Configure alerts for hardware warnings.** To be proactive, you can configure e-mail alerts for example with HP iLO or Dell DRAC, but you can also use VMware vSphere.

Operating System Security

We live in the era of the internet, so physical security is not enough. You should build your protection plan to include Windows. The operating system should be secured to reduce the vulnerability of your system. Here are the basic items to consider:

- **Install all service packs and critical fixes for Windows (and for VMware if applicable).** It is necessary to implement all critical fixes to ensure that there are no known holes on your security. Consider creating a process to apply the latest Windows security patches on a regular basis.
- **Configure a firewall.** You need a protective firewall on your server to defend your system. If there is no other firewall installed on your server, then configure Windows Firewall to work with the Database Engine, Integration Services and Analysis Services components of SQL Server.
- **Limit the number of employees who have Windows Administrator access on the SQL Server**. As a best practice, you should limit the administrative access only to those who really require it. This should include the VMware console as well as

Remote Desktop Services. Maybe you can consider limiting the OS level admin access to the SQL Server administrators and Network administrators.

SQL Server Installation

Now we reached the point when you can finally work with your beloved SQL Server. There are a number of security related tasks which should be completed before you can start to use a production SQL Server. Here is what I recommend as a starting point:

- **Install only the required components.** The less installed components, the less security problems can occur.
- **Install all service packs and critical fixes for SQL Server.** It is necessary to implement all critical fixes to ensure that there are no known holes on your security.
- **Disable unnecessary features and services.** You can use the SQL Server Configuration Manager to disable unused SQL Server services.
- **Disable the unused SQL Server protocols.** SQL Server supports four type of protocols: Shared Memory, Named Pipes, TCP/IP and VIA. You should use the bare minimum of these protocols and disable the others using the SQL Server Configuration Manager.
- **Change the default SQL Server ports.** The SQL Server gets installed with the default TCP port 1433 which is well known by admins and attackers too. You can avoid some targeted SQL attacks if you do not use the default ports. You can change the port in SQL Server Configuration Manager.
- **Hide the SQL Server instance and/or turn off the SQL Server Browser Service.** You can configure the SQL Server instance as hidden using the SQL Server Configuration Manager. This will prevent advertisement of your server by the SQL Server Browser service. If you use fully qualified connection strings then you can disable the SQL Server Browser.
- **Restrict the access to the SQL Server configuration and database file.** Apart from the database level access, you should also protect the file system to prevent unauthorized file deletion, copying or alteration of data.
- **Restrict the access to the SQL Server backup folders.** Read this tip to learn how to protect your SQL Server Backup folder.
- **Use Transparent Data Encryption whenever it is an option.** You can secure your data, logs and backup with TDE in Evaluation, Developer, Enterprise and Datacenter versions of SQL Server 2008, 2008 R2 and 2012.
- **Create only the required databases**. Do not create demo or test databases on production servers, keep it clean and safe.
- **Run the SQL Server Best Practice Analyzer to verify your installation.** The Microsoft SQL Server 2012 Best Practice Analyzer can quickly identify if your server is configured according to industry best practices or not.
- **Revoke execute rights to 'PUBLIC' on extended stored procedures.** Extended stored procedures will be removed in a future version of SQL Server and it is not recommended to use them. You can use CLR Integration instead. The following extended stored procedures should not be executed by your applications: *xp_availablemedia, xp_dirtree, xp_enumgroups, xp_fixeddrives, xp_regaddmultistring, xp_regdeletekey, xp_regdeletevalue, xp_regenumvalues, xp_regremovemultistring, xp_regwrite, xp_regread*, *xp_servicecontrol, xp_subdirs.*
- **Disable the xp_cmdshell option.** It is highly recommended to disable the xp_cmdshell stored procedure even if other administrators can enable it again.

User Accounts

After your basic SQL Server security is configured, you can start to address the traditional user access and security topics. The administrators and the service accounts require extra attention. Here is how to get started:

- **Rename and disable the SA account if your applications allow it.** You can use the *sp_SetAutoSAPasswordAndDisable* stored procedure to disable the SA account as described in this tip. This will prevent the attacker from trying to login with the default admin account.
- **Remove the BUILTIN\Administrators group from the SQL Server Logins.** You can read more about the security issues with the SQL Server BUILTIN\Administrators group in this tip.

- **Use Windows Authentication mode.** You can check and change the authentication mode in three different ways: using SQL Server Management Studio, with T-SQL or in the Windows registry.
- **Every administrator should have a named login, shared logins should not be allowed.** This is required in order to be able to identify the people behind each and every database change. It is also critical to have an up-to-date list of all the accounts.
- **All accounts for named user access should be controlled by Active Directory.** Use Active Directory and do not create SQL Server logins. It makes the administration easier if you grant access rights through Active Directory groups or Group Policy.
- **Use service accounts for applications.** It is a best practice to create a different service account with a descriptive name for every service. You can use SQL Server logins, but a complex password is a must. Restrict the access only to data required: if an application updates only 1-2 tables then it does not require full control of every object in the database.
- **Configure service accounts with the least privileges.** You can read this tip if you would like to know how to determine service related privileges for SQL Server service account. Do not grant more rights than required.
- **The user privileges should be minimized.** Try to assign the minimum sufficient rights to every user. It is a best practice to document any elevated user permission and request managerial approval.
- **All administrator accounts should have a complex password and password change should be enforced.** You should identify blank and weak passwords and configure password enforcement options.
- **Configure SQL Server login auditing to log both failed and successful logins.** Details of the login audit configuration can be found in this tip and there is also a tip about SYSADMIN login auditing.

The above checklist can be used to ensure that the minimum requirements are fulfilled. Every company should have an information security policy and you should apply those requirements to your SQL Server as well. In case that policy does not exist then you can use this checklist as the basic checklist.

Next Steps

- Check out the Security category articles to learn more about SQL Server security.
- Read more tips by the author here.

Last Updated: 2014-02-06

About the author

Tibor Nagy is a SQL Server professional in the financial industry with experience in SQL 2000-2012, DB2 and MySQL.

View all my tips

Related Resources

- More SQL Server DBA Tips...