SQL Server Audit Checklist

By K. Brian Kelley, MCSE, CISA, Security+, MVP-SQL Server

Administrative rights over the Domain where SQL Server is installed

- Who are the Enterprise Admins group for the Active Directory forest?[^1]
- Who are the members of the Domain Admins group for every domain in the Active Directory forest?[^1]
- Who are the members of the Administrators group for every domain in the Active Directory forest?

Administrative rights on the OS where SQL Server is installed

- Who can modify the group policies that are applied to the SQL Servers?[^2]
- Who are the members of the Administrators group on the systems where SQL Server is installed?
- Who are the members of the Server Operators group in the domain?

Local logon rights on system where SQL Server is installed[^3]

- What groups/users does the local security policy (or inherited from a group policy) permit to log on locally?
- Who are the members of the Remote Desktop Users group?
- Who are the members of the Power Users group?

Permissions to manage users/groups

- Who are the members of the Account Operators group for the domain?
- Who has delegated rights to manage users and groups in the domain?[^4]

Access to SQL Server backups

- Are the SQL Server backups encrypted? Do they need to be?
- If the SQL Server backups are encrypted, who has access to the encryption keys?
- Who are the members of the Administrators group where the backups are stored (assuming a separate server)?[^5]
- Who has physical access to the backup storage (such as tape)?[^5]
- Who has access to the SQL Server backups through the backup software if a 3rd party product is in use?

---

[^2]: Membership of local groups can be controlled via group policy. Also, startup scripts can be specified.
[^3]: We’re guarding against privilege escalation techniques by a user who already has access to the system.
[^4]: This one can be harder to track and will likely require an AD audit to determine the answer.
[^5]: Tape replacement appliances should be considered, too.
Access to the OS through Agents
- What agents (backup, monitoring) are running on the servers?
- Do any of those agents have accounts which have local administrator rights, such as through System?
- Can any of those agents run scripts against the OS or against SQL Server?
- Who controls those agents?

OS Surface Area
- Does the server have the ability to access the Internet?
- Is the Enhanced Security Configuration for the web browser turned on?
- Are the non-essential services blocked off from end-users (SMB, RPC, etc.)?

SQL Server Surface Area
- What network libraries is the SQL Server instance using?
- Are remote connections allowed?
- Is remote DAC allowed?\(^6\)
- Is there a need to use an IPSEC policy to restrict what systems can access the SQL Server?
- Can the SQL Server be restricted using network devices/hardware such as firewalls, routers, and/or switches?

SQL Server Service Accounts
- Are the SQL Server service accounts running with the least privileges possible?
  - Are any of them System?
  - Are any members of the server’s local Administrators group?
- If you are running on Windows Server 2008 and SQL Server 2008 or higher, is service isolation being used?
- Are there different SQL Server service accounts for each SQL Server instance?

SQL Server Internals – Server Level – Logins
- Is the SQL Server instance set to only accept Windows logins? Can it be?
- What logins exist on the SQL Server instance?
- Are Windows user logins being used (ones that aren’t “service accounts”)?
- Are there a lot of SQL Server logins?
- Should all of these logins have access to the SQL Server instance?
- Is the sa account being used by applications?
- How many people know the sa account password?

SQL Server Internals – Server Level – SQL Server Logins/Passwords\(^7\)
- What SQL Server logins are ignoring the password policy altogether?
- What SQL Server logins are honoring the policy but have non-expiring passwords?

---
\(^6\) DAC = Dedicated Administrator Connection, a new feature as of SQL Server 2005
\(^7\) Only applies to SQL Server 2005 and above. SQL Server 2000 doesn’t support password policy enforcement.
SQL Server Internals – Server Level – Server Roles

- Who is a member of the `sysadmin` server role?
- Who is a member of the `securityadmin` server role?
- Who is a member of the `processadmin` server role?
- Who is a member of the `serveradmin` server role?

SQL Server Internals – Server Level – Server Securable

- Does any login have CONTROL SERVER permissions?
- Does any login have IMPERSONATE privileges?
  - Specifically, IMPERSONATE of the `sa` account or any other member of the `sysadmin` role?
  - Specifically, IMPERSONATE of a member of the `securityadmin` role?

SQL Server Internals – Database Level – Users

- How do the logins map in as users in the particular database?
- If this is a user database (not master, msdb, or tempdb), is the `guest` user enabled?
- Who is the owner of the database?\textsuperscript{9}
- Are there any users which do not correspond to logins?\textsuperscript{10}

SQL Server Internals – Database Level – Database Roles

- Who is a member of the `db_owner` role?
- Who is a member of the `db_ddladmin` role?
- Who is a member of the `db_securityadmin` role?
- Are user-defined database roles being used?

SQL Server Internals – Database Level – Database Permissions

- Who has the CREATE permissions in the database?
- Who has CONTROL permissions at the database level?\textsuperscript{11}
- Do the permissions on the objects make sense and follow the principle of least privilege?
- When you look at scope permissions, do the permissions against the securables they contain make sense and follow the principle of least privilege?\textsuperscript{12}
- Are the permissions being assigned against database roles and not users?
- Does the `public` role have permissions outside of the defaults?
- Are any of the following roles being used?
  - `db_datareader`
  - `db_datawriter`
  - `db_denydatareader`
  - `db_denydatawriter`

\textsuperscript{8} This also only applies to SQL Server 2005 and above.
\textsuperscript{9} The owner of the database maps in as the `dbo` user.
\textsuperscript{10} This could either be due to orphaned logins or in 2005+, CREATE USER [SomeUser] WITHOUT LOGIN;
\textsuperscript{11} SQL Server 2005 and above only.
\textsuperscript{12} This is SQL Server 2005 and above only. Scopes are securables that can contain other securables.