Installation, Updates and Patches

This section contains recommendations related to installing and patching SQL Server.

1.1 Ensure Latest SQL Server Service Packs and Hotfixes are Installed

Status APPLIED

Description:

SQL Server patches contain program updates that fix security and product functionality issues found in the software. These patches can be installed with a hotfix which is a single patch, a cumulative update which is a small group of patches or a service pack which is a large collection of patches. The SQL Server version and patch levels should be the most recent compatible with the organizations' operational needs.

Rationale:

Using the most recent SQL Server software, along with all applicable patches can help limit the possibilities for vulnerabilities in the software, the installation version and/or patches applied during setup should be established according to the needs of the organization.

Audit:

To determine your SQL Server service pack level, run the following code snippet.

```
SELECT SERVERPROPERTY('ProductLevel') as SP_installed, SERVERPROPERTY
('ProductVersion') as Version;
```

First column returns the installed Service Pack level, the second is the exact build number.

Remediation:

Identify the current version and patch level of your SQL Server instances and ensure they contain the latest security fixes. Make sure to test these fixes in your test environments before updating production instances.
The most recent SQL Server patches can be found here:

- Hotfixes and Cumulative updates: http://blogs.msdn.com/b/sqlreleaseservices/
- Service Packs: https://support.microsoft.com/en-us/kb/3177534

Default Value:

Service packs and patches are not installed by default.

References:

1. https://support.microsoft.com/en-us/kb/3177534

Control:

SQL server builds are deployed using a standard template and configuration options using the upgrade options to slipstream the build to the latest service packs, cumulative updates, and hotfixes. The source for these updates are maintained via Microsoft Security Bulletins on a monthly basis and updates to contain the latest patches.

References:

1. Install SQL Server from the Command Prompt

back to Installation, Updates and Patches

Status APPLIED

1.2 Ensure Single-Function Member Servers are Used

Description:

It is recommended that SQL Server software be installed on a dedicated server. This architectural consideration affords security flexibility in that the database server can be placed on a separate subnet allowing access only from particular hosts and over particular protocols. Degrees of availability are easier to achieve as well - over time, an enterprise can move from a single database server to a failover to a cluster using load balancing or to some combination thereof.

Rationale:

It is easier to manage (i.e. reduce) the attack surface of the server hosting SQL Server software if the only surfaces to consider are the underlying operating system, SQL Server itself, and any security /operational tooling that may additionally be installed. As noted in the description, availability can be more easily addressed if the database is on a dedicated server.

Audit:

Ensure that no other roles are enabled for the underlying operating system and that no excess tooling is installed, per enterprise policy.

Remediation:

Uninstall excess tooling and/or remove unnecessary roles from the underlying operating system.

Impact:

It is difficult to see any reasonably adverse impact to making this architectural change, once the costs of making the change have been paid. Custom applications may need to be modified to accommodate database connections over the wire rather than on the host (i.e. using TCP/IP instead of Named Pipes). Additional hardware and operating system licenses may be required to make these architectural changes.

Control:

The operating system is deployed using the standard Aviva Golden AMIs, and the SQL server build using a standard template with the features required by the application.

Feature options available in the template are:

- SQL Server Database Engine
- SQL Server Integration Services

back to Installation, Updates and Patches

back to SQL Server Security Controls