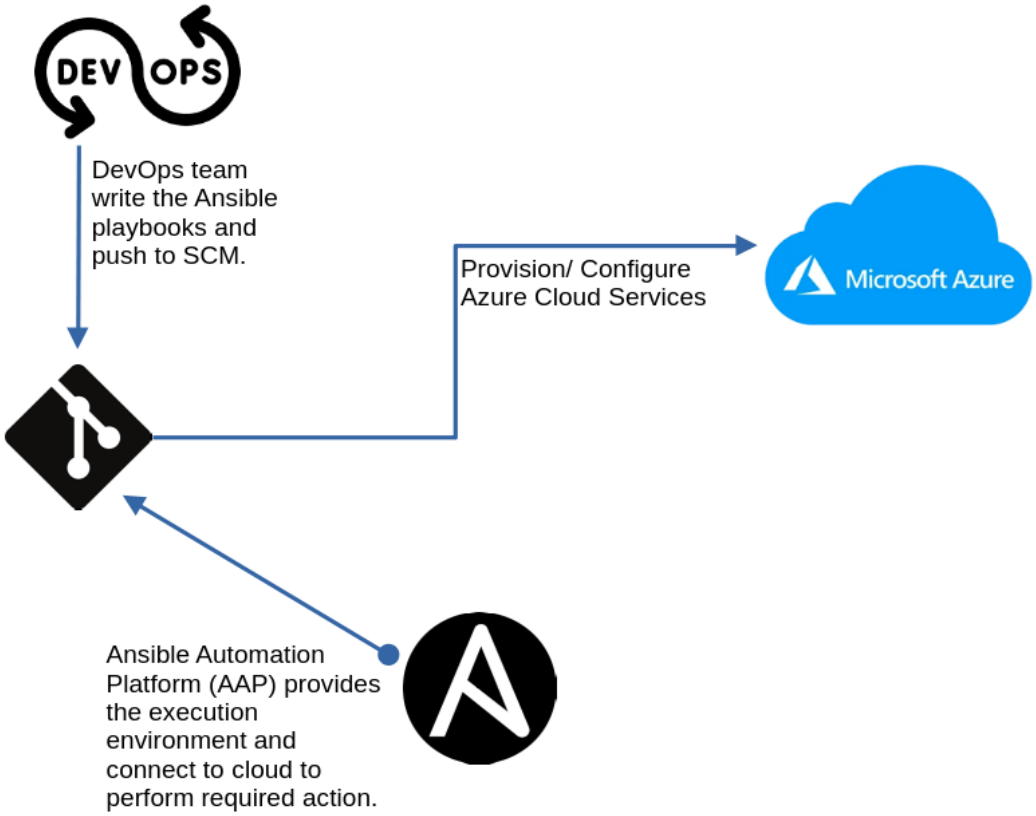
Azure-MSSQL

Azure SQL Database, a fully managed platform as a service (PaaS) database engine that handles most of the database management functions such as upgrading, patching, backups, and monitoring without user involvement.

Ansible Automation Controller will be used to pull the playbooks from SCM and deploy on Azure Cloud.



There are several steps which need to be taken to ensure the Azure SQL DataBase is hardened and secure. The various playbooks perform those steps for you. The below table corresponds to various action items needed to ensure this.

Control Family	Control Name(s)	Requirement ID	Requirements
Identity, access and privilege management	Identification and Authentication	R_2.6	Local authentication for Azure SQL database must be disabled
Infrastructure protection	Transmission Confidentiality And Integrity	R_2.12	Access and connectivity to the Azure SQL Database must be restricted to only clients using Manulife approved protocol such as TLS 1.2 or above to ensure a secure connection.
Infrastructure protection	Network traffic filtering	R_2.10	Ensure Azure SQL database is accessible through a private endpoint such that access to the Azure SQL database is restricted to Manulife's private networks
Infrastructure protection	Network traffic filtering	R_2.14	Public network access to Azure SQL server and database must not be allowed.
Threat detection and monitoring	Audit Events	R_2.15	Azure SQL auditing must be enabled to track database events. Logs must be forwarded to the Manulife approved log repository
Threat detection and monitoring	Audit Events	R_2.17	Ensure to collect logs from the Azure SQL Database and store them in the Manulife approved log repository

Threat detection and monitoring	Audit Review, Analysis, And Reporting	R_2.20	A Manulife approved Threat Protection solution such as MICROSOFT DEFENDER FOR SQL for Azure SQL Database must be used to continuously monitor traffic for anomalous SQL database access attempts, prevent SQL injection attempts etc. A periodic recurring scan should be established

Playbook **1.1_Azure_SQL_Install.yml** will help you install the SQL server and create a DB with the respective provided parameters. and post installation, if you need sqlcmd binary to perform SQL commands from ansible playbooks, run playbook **1.2_Azure_SQL-sqlcmd_Install.yml** to make sqlcmd binary available in execution environment.

Post installation, playbooks can be run independently to perform individual hardening task and there is no dependency of any other task/playbook.

The playbooks are listed below with requirement id:

R_2.6_Azure_SQL_Authentication_AD.yml
R_2.13-2.14-Azure_SQL_Network-Filtering.yml
R_2.15_Azure_SQL_Audit.yml
R_2.20_Azure_SQL_Data_Security.yml