**Tech Challenge #6**

**MySQL Server Installation, Configuration and Audit**

1. Attach 5 new disks to TUA12345-SQL1
   1. Disks should be default name and type with size 100 GiB
2. Restart server after these changes
3. Login to TUA12345-SQL1
4. Create a RAID volume out of the 3 disk drives that were added
   1. Initialize the 4 new disks using the MBR partition style
   2. Select one of the volumes, right click, and choose “New RAID-5 volume”
   3. Add the remaining two disks and continue
   4. Assign this the drive letter “M”
   5. Format this volume as NTFS and accept the default size unit and label it “RAID-5”
   6. The system will convert these to “Dynamic Disks” to continue
5. Create a mirrored pair out of the last two drives with a driver letter of “N” and volume label of “MIRROR”. Go to This PC and provide a screenshot of the M and N drives:
6. Turn off Enhanced Security Configuration for Administrators in Internet Explorer
7. Download the prerequisite software found at: <http://dev.mysql.com/resources/wb62_prerequisites.html>
   1. Download and install vcredist\_x64.exe
8. Download the MySQL installer found at: <http://dev.mysql.com/downloads/installer>
   1. Setup type is “Developer Default”
   2. Ignore the warning and error messages
   3. Set the Root Account password to “sesame”.
9. Update the MySQL57 service so that it runs under the “Local System account” and start the service. Provide a screenshot of the services module showing the MySQL57 service:

mysql

1. Move the MySQL data directory to the RAID-5 volume you just created
2. Enable binary logs and store the binary logs to the mirrored volume you just created
3. Update the MySQLservers so that it runs under the “Local System account” and start the service.
4. Start MySQL Workbench and display the location of the data files by executing the SQL command “show variables like 'datadir';”. Create a screen shot of the output and paste the screen shot here:
5. Go to Options File…Logging on the MySQL Workbench. Scroll down to show the value of log-bin. Take a screen shot of this and past the screen shot here:
6. Download the files used to create and populate the databases and tables posted to the course website. Run this script to create and populate these databases. Run a SQL query to display a list of vendors. Paste a screen shot of this information here:
7. Display the files that are on the volume that contain your binary logs by going to “Start…Computer” and selecting this volume. Paste a legible screen shot of this information here:
8. **AUDIT YOUR SERVER**

For this step I am looking for you to do some research both in your textbook as well as on the internet to find a good method of obtaining the info. In addition to attempting to satisfy each control with a proper command and screenshot I would like you to provide some analysis of why each control is important. Your analysis of each step is vital and should be provided regardless of whether each step can be fully completed.

* 1. Obtain the database version and verify that it is up to date and supported
  2. Verify that policies and procedures are in place to identify when a patch is available. Ensure that all approved patches are installed per your database management policy.
  3. Determine whether a standard build is available for new database systems and whether that baseline has adequate security settings.
  4. Ensure that access to the operating system is properly restricted
  5. Ensure that permissions on the directory in which the database is installed and the database files themselves are properly restricted.
  6. Ensure that permissions on the registry keys used by the database are properly restricted
  7. Review and evaluate procedures for creating user accounts and ensuring that accounts are created only when there’s a legitimate business need.
  8. Check for default usernames and passwords
  9. Check for easily guessed passwords
  10. Check that password management capabilities are enabled.
  11. Verify that database permissions are granted or revoked appropriately for the required level of authorization
  12. Review database permissions granted to individuals instead of groups or roles.
  13. Ensure that database permissions are not implicitly granted incorrectly.
  14. Review dynamic SQL executed in stored procedures
  15. Ensure that row-level access to table data is implemented properly
  16. Revoke PUBLIC permissions where not needed
  17. Verify that network encryption is implemented
  18. Verify that encryption of data at rest is implemented where appropriate
  19. Verify the appropriate use of database auditing and activity monitoring.
  20. Evaluate how capacity is managed for is managed for the database environments to support existing and anticipating business requirements
  21. Evaluate how performance is managed and monitored for the database environment to support existing and anticipated business requirements.

1. This concludes Tech Challenge #6