**Creating and monitoring resources in Azure: Project solution exemplar**

**Important disclaimer for the Azure UI**

Given the dynamic nature of Microsoft Cloud tools, you might experience changes in the Azure UI that have taken place after the development of this training content. As a result, the screenshots in the videos, readings, exercises, or project solution exemplars might not align exactly with how you currently experience the UI. However, please note that these changes do not impact the functionalities of the UI. Hence, you can still perform all the steps shown in the videos, readings, exercises, or project solution exemplars.

**Task: Creating and monitoring resources in Azure**

|  |  |
| --- | --- |
| **Activity #** | **Steps** |
| **Activity 1:**  Create an Azure SQL Database | Step 1: Create an Azure SQL page.      On the Azure portal, select **+ Create a resource** option from the upper left corner and search for Azure SQL.     * Select **Create** in the resulting Azure SQL page. * Review all the available Azure SQL options, and then in the SQL databases title, ensure a single database is selected and select **Create**. |
|  | Step 2: Populate the information in the SQL database.    A created SQL database page will pop up. Populate the necessary information as follows:   1. Subscription: Select your Azure subscription in which you wish to create the resource. 2. Resource group: Choose the resource group where you wish to create the resource or create a new one by selecting **Create new option** and entering the name of your choice. 3. Database name: Enter the name you wish to give to the database. 4. Server: Select the **Create new** option and create a new server with a unique name in any location. Use SQL authentication and specify your name as the server admin login and a suitably complex password for security. |
|  | Step 3: Deploy the resources.   1. Select the **Networking** tab. Then, on the Networking tab, configure the networking settings. 2. In the Network connectivity section, select Public endpoint.      1. Select **Yes** for both options in the Firewall rules section to allow access to the database server from Azure services and your current client IP address.      1. Select **Next: Security** option to configure the security for the database. For now, set the Enable Microsoft Defender for SQL option to Not now. 2. Select **Additional Settings** option to configure some additional settings for the database. For now, set the use existing data option to Sample. 3. Finally, select **Review + create** and review the different configurations of the database.      1. Once everything is configured, select **Create** to create an Azure SQL Database.      1. Wait for deployment to complete and go to the resource that was deployed. |
| **Activity 2:**  Query in the Azure SQL Database. | Step 1: Sign in using specific credentials.  In the pane on the left side of the page, select the **Query editor** and then sign in using the administrator login and password we had specified for our server. |
|  | Step 2: Expand the Tables folder to see the tables in the database. |
|  | Step 3: Enter a query.  In the Query 1 pane that appears, enter the following SQL code:  **SELECT \* FROM [SalesLT].[SalesOrderHeader]** |
|  | Step 4: Run the query.  Select **Run** above the query to run it and view the results, which will include all the columns for all rows in the table. |
|  | Step 5: Save the query.  Close the query editor pane, which discards all edits and saves the query. This way, you can run all your SQL queries. |
| **Activity 3:**  Enable advanced threat protection | Step 1: Click the **Advanced-Data Security**option. This feature is already enabled on the server level, which means that you enable it for all databases. |
|  | Step 2: Turn the option ON.    *Note: Here, you can configure a weekly security assessment and have the results sent to you. The scans will be stored in the storage accounts that you can configure here. You can also leave it OFF after you have finished the task since you want to enable advanced threat protection. Here, you can also put in an e-mail address to where the security alerts will be sent. You can leave this to send the alerts to admins and owners.*  *Here, you can see which types of threats will be detected and alerted to. These are the most common vulnerabilities and attacks that can happen to your data.* |
|  | Step 3: After enabling all of them, click **OK**. |
|  | Step 4: Configure auditing.  This helps to troubleshoot any anomalies that are detected. Turn it **ON**. |
|  | Step 5: You also need a place to store the logs, like in Azure Storage. Here, you select an existing Azure storage account and then click **OK**.    Finally, save the settings applied. |