Exercise: Access Azure Storage with key vault-backed secrets

In your Azure Databricks workspace, open the **08-Azure-Databricks-Security-Data-Protection** folder that you imported within your user folder.

Unit notebook

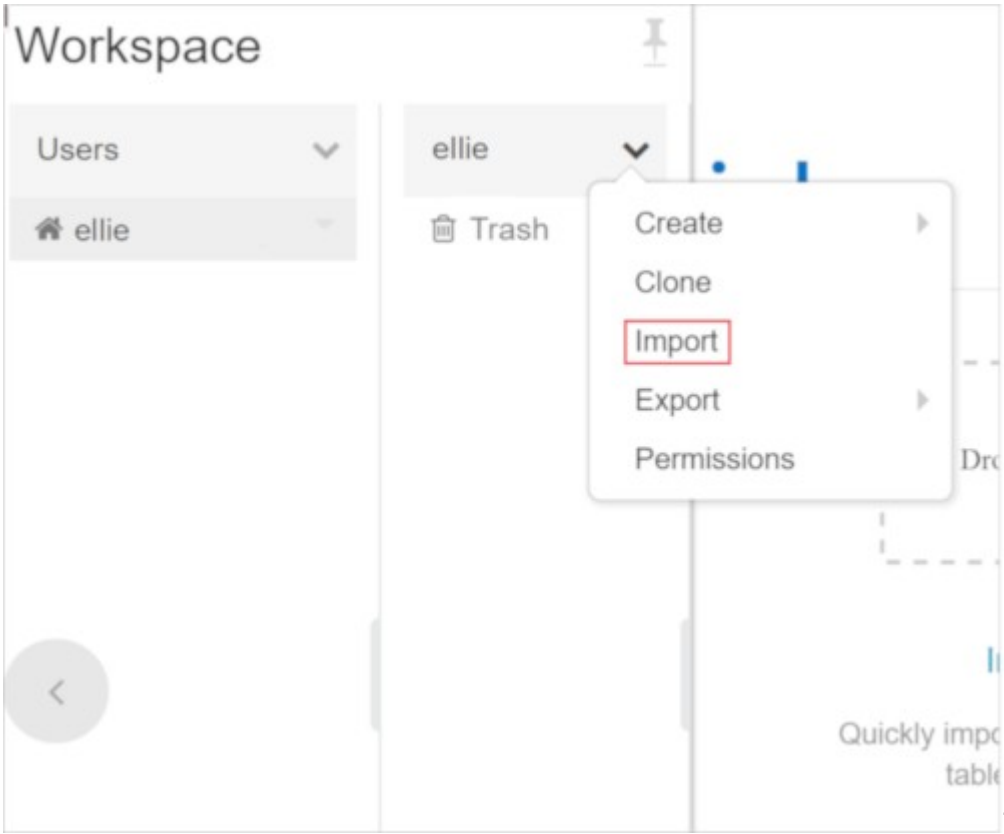
In this unit, you need to complete the exercises within two Databricks Notebooks. To begin, you must first import the notebooks by cloning a Databricks archive.

Clone the Databricks archive

1. If you do not currently have your Azure Databricks workspace open then access the Azure portal, navigate to your deployed Azure Databricks workspace and select **Launch Workspace**.

2. In the left pane, select **Workspace** > **Users**, and then select your username (the entry with the house icon).

3. In the pane that appears, select the arrow next to your name, and select **Import**.



The menu option to import the archive.

4. In the **Import Notebooks** dialog box, select the URL bar and paste in the following address:

1

https://github.com/solliancenet/microsoft-learning-paths-databricks-notebooks/blob/master/data-engineering/DBC/08-Azure-Databricks-Security-Data-Protection.dbc?raw=true

5. Select **Import**.

6. Select the **08-Azure-Databricks-Security-Data-Protection** folder that appears.

Complete the following notebooks

Open the **3-Key-Vault-Backed-Secret-Scopes** notebook. Make sure you attach your cluster to the notebook before following the instructions and running the cells within.

Within the notebook, you will:

- Create a Secret Scope connected to Azure Key Vault.
- Mount Blob Storage to DBFS using a SAS token.
- Write data to Blob using a SAS token in Spark Configuration.

After you've completed the notebook, return to this screen, and continue to the next step.