Describe Azure key vault and Databricks security scopes

Note: *In this reading you can see the steps involved in the process of working with the Azure key vault.* Azure Key Vault is used to securely store, and tightly control, access to tokens, passwords, certificates, API keys, and other secrets.

In addition, secrets that are stored in Azure Key Vault are centralized. This offers the added benefits of only needing to update secrets in one place, such as an application key value after recycling the key for security purposes.

Unit notebook

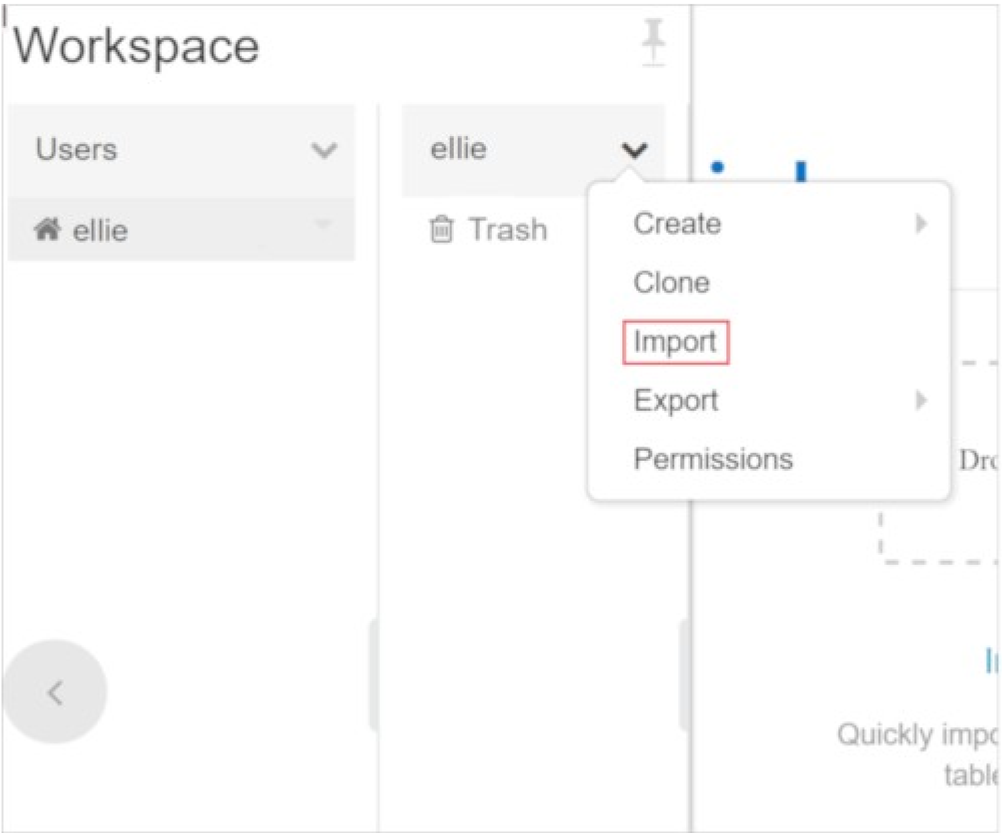
In this unit, you need to complete the exercises within two Databricks Notebooks. To begin, you must first import the notebooks by cloning a Databricks archive.

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 **1-Blob-Storage** 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 blob storage containers
- Load data into a container
- Create a read/list SAS token
- Create a SAS token with full privileges

After you've completed the notebook, open the **2-Key-Vault** notebook. Make sure you attach your cluster to the notebook before running it.

Within the notebook, you will:

- Configure Key Vault Access Policies
- Create Secrets that store SAS Tokens in a Key Vault

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