Shaheed Zulfikar Ali Bhutto Institute of Science and Technology

Department of Software Engineering
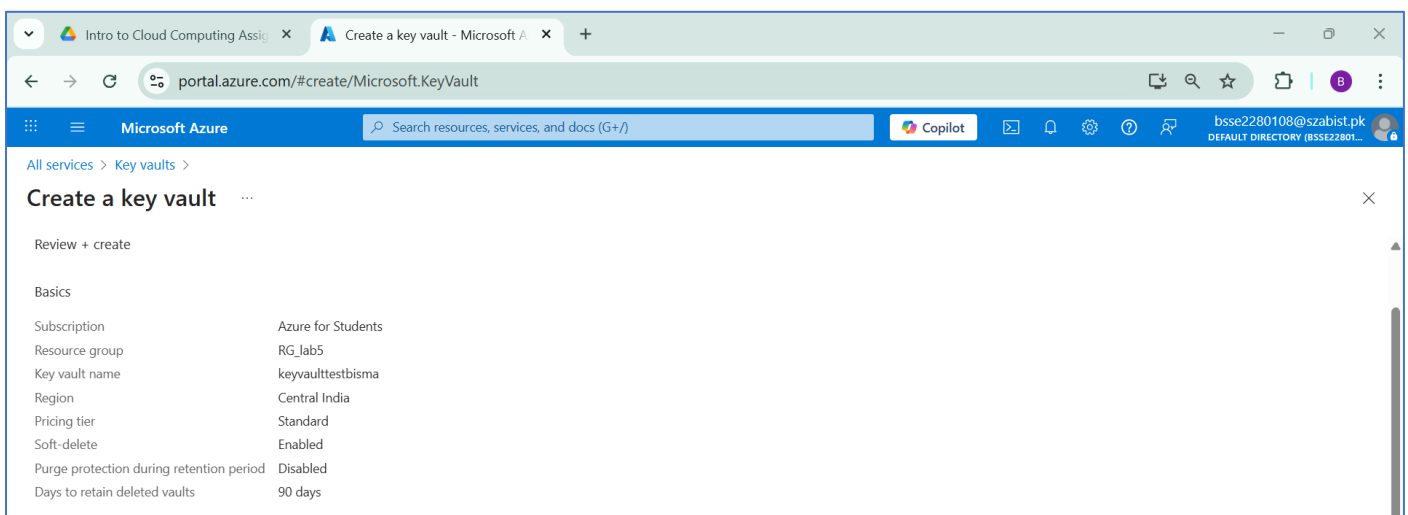
Bisma Saeed – 2280108

BSSE – 7A

Lab: 05

Task 1: Create an Azure Key Vault

1. Sign in to the Azure portal.

2. From the All services blade, search for and select Key vaults, then select **+Add +New +Create **.

3. Configure the key vault

4. Note replace xxxx to find a unique name.

5. Click Review + create, and then click Create.

6. Once the new key vault is provisioned, click Go to resource. Or you can locate your new key vault by search.

7. Click on the key vault Overview tab and take note of the Vault URI. Applications that use your vault through the REST APIs will need this URI.

Task 2: Add a secret to the Key Vault

In this task, we will add a password to the key vault.

Assigned the role first:

1. Under Settings click Secrets, then click + Generate/Import.

2. Configure the secret. Leave the other values at their defaults. Notice you can set an activation and expiration date.

3. Click Create.

4. Once the secret has been successfully created, click on the ExamplePassword, and note it has a status of Enabled

5. Select the secret you just created, note the Secret Identifier. This is the url value that you can now use with applications. It provides a centrally managed and securely stored password.

6. Click the button Show Secret Value, to display the password you specified earlier.

Congratulations! You have created an Azure Key vault and then created a password secret in that key vault, providing a securely stored, centrally managed password for use with applications.