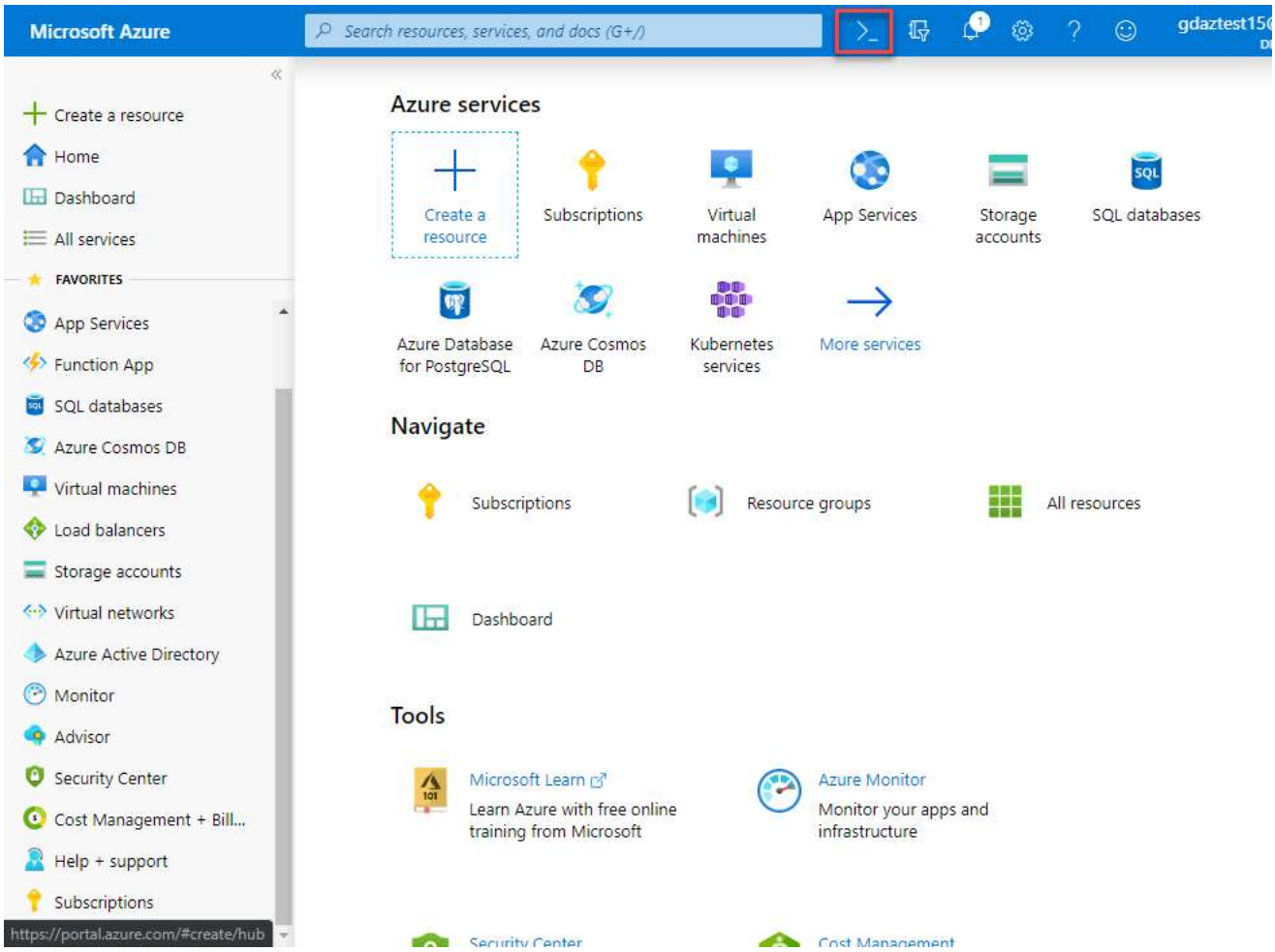
Module 4 - Lab 4 - Encrypting Azure VM Disks

Overview

In this lab, you will learn how to use encryption to protect the disks of virtual machines deployed in Azure using the Azure CLI (Bash).

Task 1: Login to the Azure Portal and open Cloud Shell

- [ ] 1. Login to the Azure Portal https://portal.azure.com with the username sheikhnasirYOT4A@gdcs1.com and password 3nJrjyfREZxFijg6
- [ ] 2. Select **Cloud Shell** from the Azure Portal tool bar.



- [ ] 3. Select **Bash** on the Welcome screen.
- [ ] 4. In the **You have no storage mounted** pane, click **Show advanced settings**, perform the following tasks:
    - Leave the **Subscription** drop-down list entry set to its default value.
    - In the **Cloud Shell region:** East US.
    - In the **Resource group** section, select the Resource Group that has been created for you.
    - In the **Storage account** section, ensure that the **Create new** option is selected and then, in the text box below, type a unique name consisting of a combination of between 3 and 24 characters and digits.
    - In the **File share** section, ensure that the **Create new** option is selected and then, in the text box below, type **cloudshell**.
    - Click the **Create storage** button.
- [ ] 5. Wait for the **Cloud Shell** to finish its first-time setup procedures before you proceed to the next task.

Task 2: Create a Key Vault configured for encryption keys

Azure disk encryption stores its encryption key in an Azure Key Vault. Create a Key Vault with **az keyvault create**. To enable the Key Vault to store encryption keys, use the **--enabled-for-disk-encryption** parameter.

> ⚠ **Note**: Each Key Vault must have a unique name. The following example creates a Key Vault named *myKV*, but you must name yours something different.

- [ ] 1. Run the following command to add the parameter for your precreated Resource Group.

```
resource_group=$(az group list --query [].name --output tsv)
```

- [ ] 2. Run the following command to create a KeyVault remembering to replace **myKV-XXXXXX** with something unique.

```
az keyvault create --name "myKV-XXXXXX" --resource-group $resource_group --location eastus --enabled-for-disk-encryption --enable-soft-d
```

Task 3: Encrypt the virtual machine

> ⚠ **Note**: A VM has been deployed for you called **MyVM**

- [ ] 1. Encrypt your VM with **az vm encryption** providing your unique Key Vault name to the **--disk-encryption-keyvault** parameter. Remember to replace **myKV-XXXXXX** with the unique name created previously.

```
az vm encryption enable -g $resource_group --name MyVM --disk-encryption-keyvault myKV-XXXXXX
```

- [ ] 2. You can verify that encryption is enabled on your VM with the **az vm show** command.

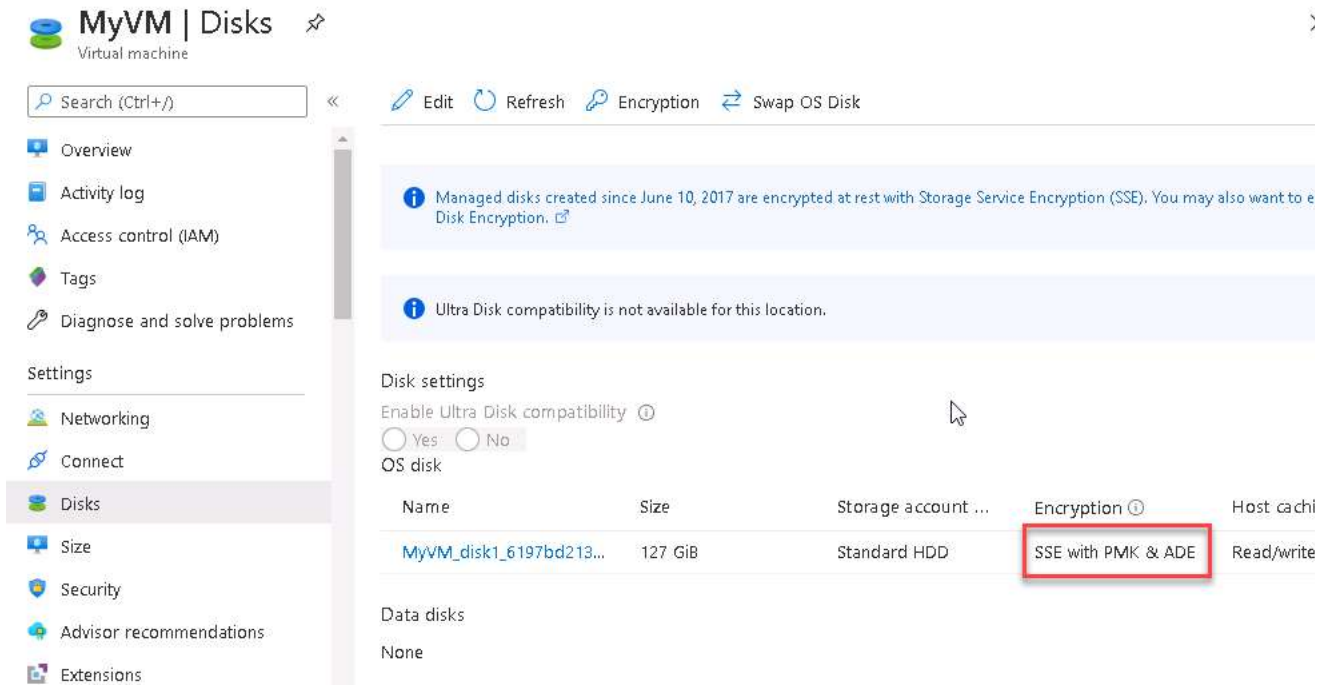
```
az vm show --name MyVM -g $resource_group
```

You will see the following in the returned output:

```
"EncryptionOperation": "EnableEncryption"
```

```
"provisioningState": "Succeeded",
"publisher": "Microsoft.Azure.Security",
"resourceGroup": "myResourceGroup-UPCJ5EAGWD",
"settings": {
  "EncryptionOperation": "EnableEncryption",
  "KekVaultResourceId": "",
  "KeyEncryptionAlgorithm": "RSA-OAEP",
  "KeyEncryptionKeyURL": null,
```

- [ ] 3. In the Azure Portal navigate to **Virtual Machines**.
- [ ] 4. Select **MyVM** > **Disks**.
- [ ] 5. Once the process completes, you will see that **Encryption** is enabled.



> ✓ **Summary**

In this lab you encrypted an Azure Virtual Machine disk.