

Exercise - Create an Azure virtual network

- 20 minutes

In this exercise, you will create a virtual network in Microsoft Azure. You will then create two virtual machines and use the virtual network to connect the virtual machines and to the Internet.

Log in to your subscription with the Azure CLI

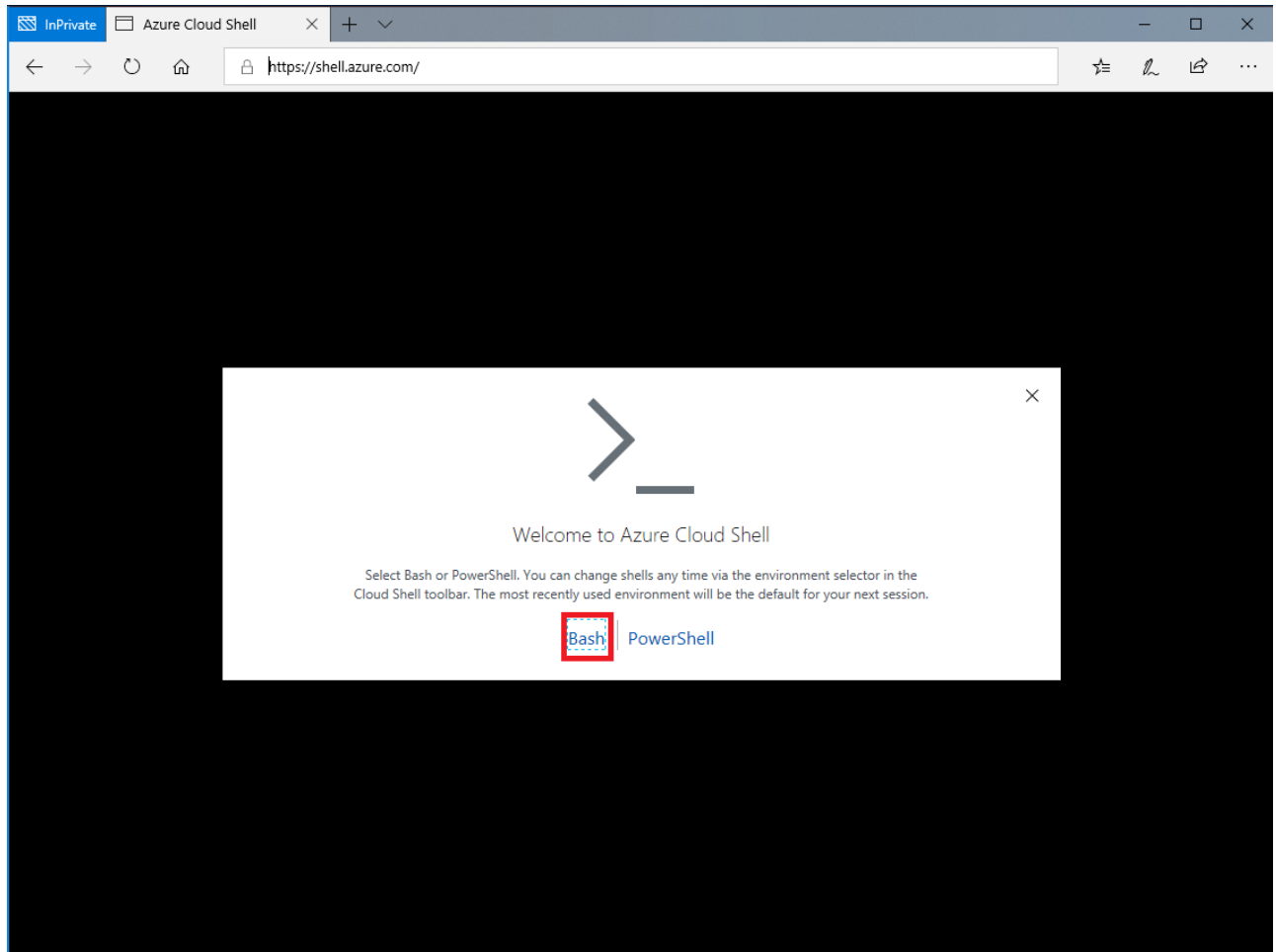
This first lab will use the Azure CLI. If you have a local installation of the Azure CLI, feel free to use it — make sure to use `az account` to log in to the subscription you want to use. If not, you can log into your Azure account and use the Cloud Shell, either in-line, or in a separate browser window.

You will also be using **Bash** in the **Azure Cloud Shell** in this lab. For more information please refer to [Quickstart for Bash in Azure Cloud Shell](#).

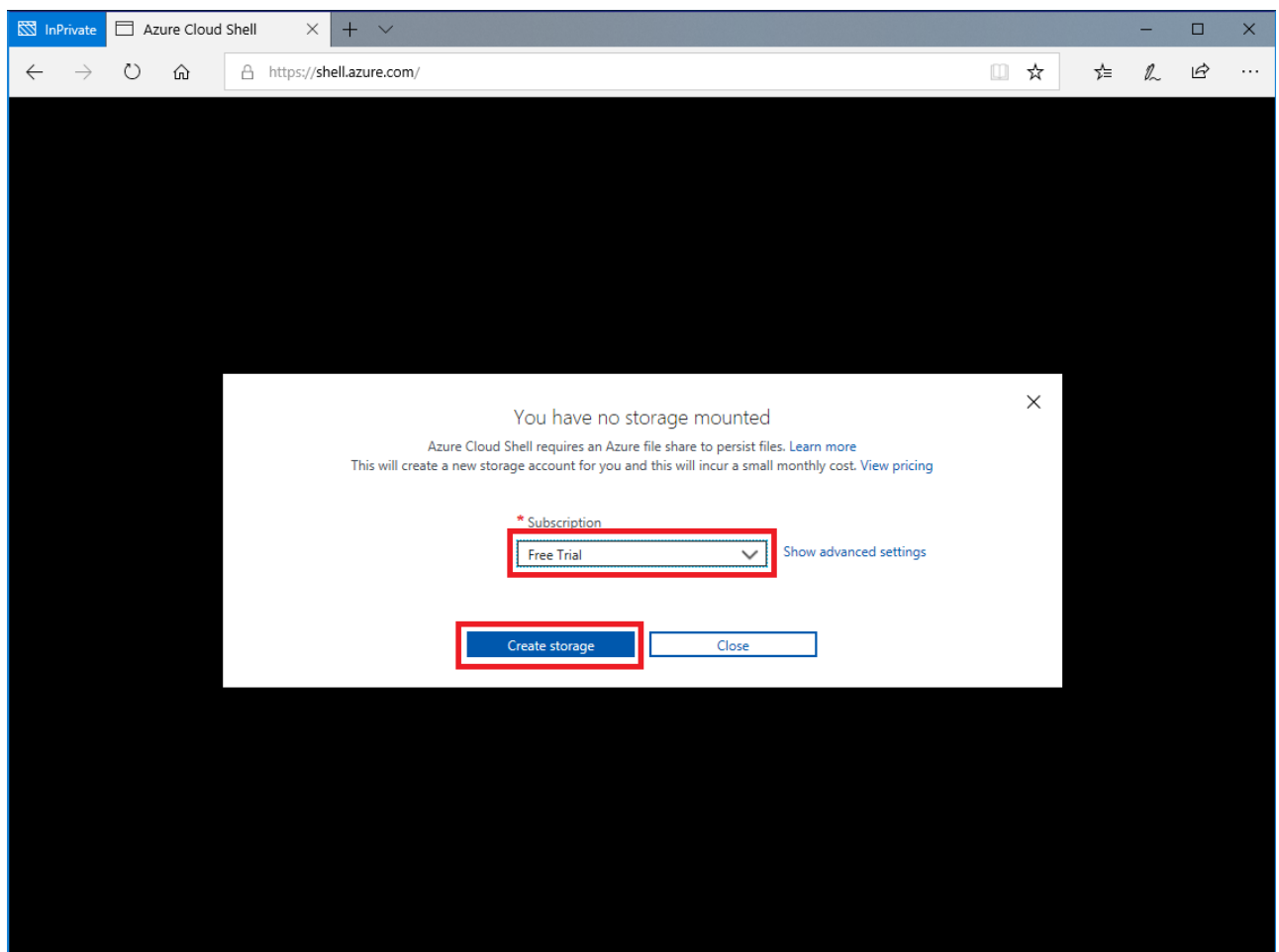
Note If you are using the CloudShell environment, select the **Bash** shell option. If you are using PowerShell, locally or in the cloud, then you will need to escape all empty parameters by changing `""` to `''` to properly pass an empty string into the command. Without this, PowerShell will not pass the empty string, and you will get an error from the command indicating it's missing a parameter. All labs assume you are using Bash.

Option 1 - Open Azure Cloud Shell in a separate browser window

1. Open the [Azure Cloud Shell](#) in a new **InPrivate browser window**.
2. Sign into Azure using the Microsoft account email address and password you created for this session.
3. If prompted, select your **Default Directory**.
4. If prompted, Click **Bash**.

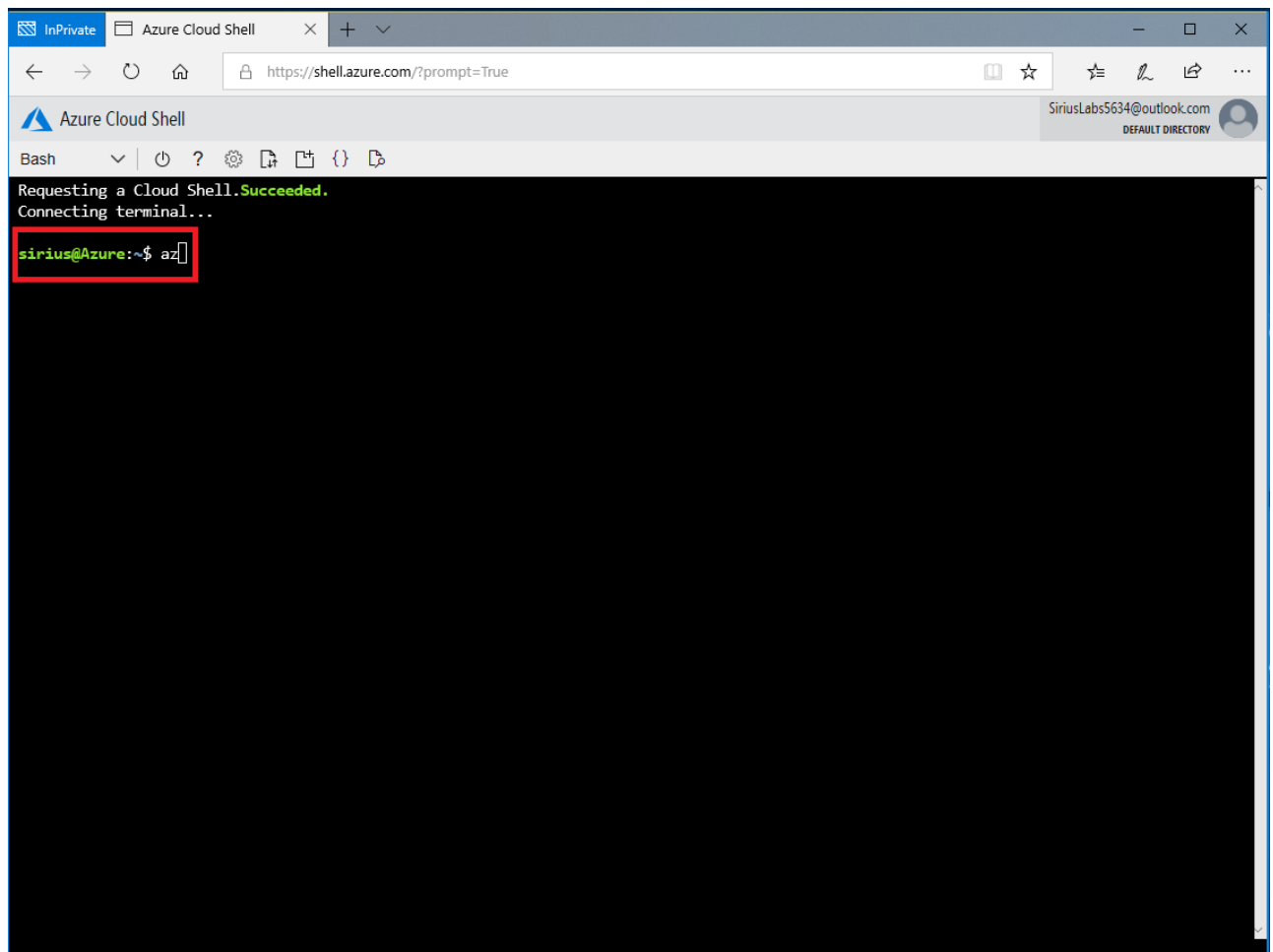


5. Select your subscription, and click **Create storage**.

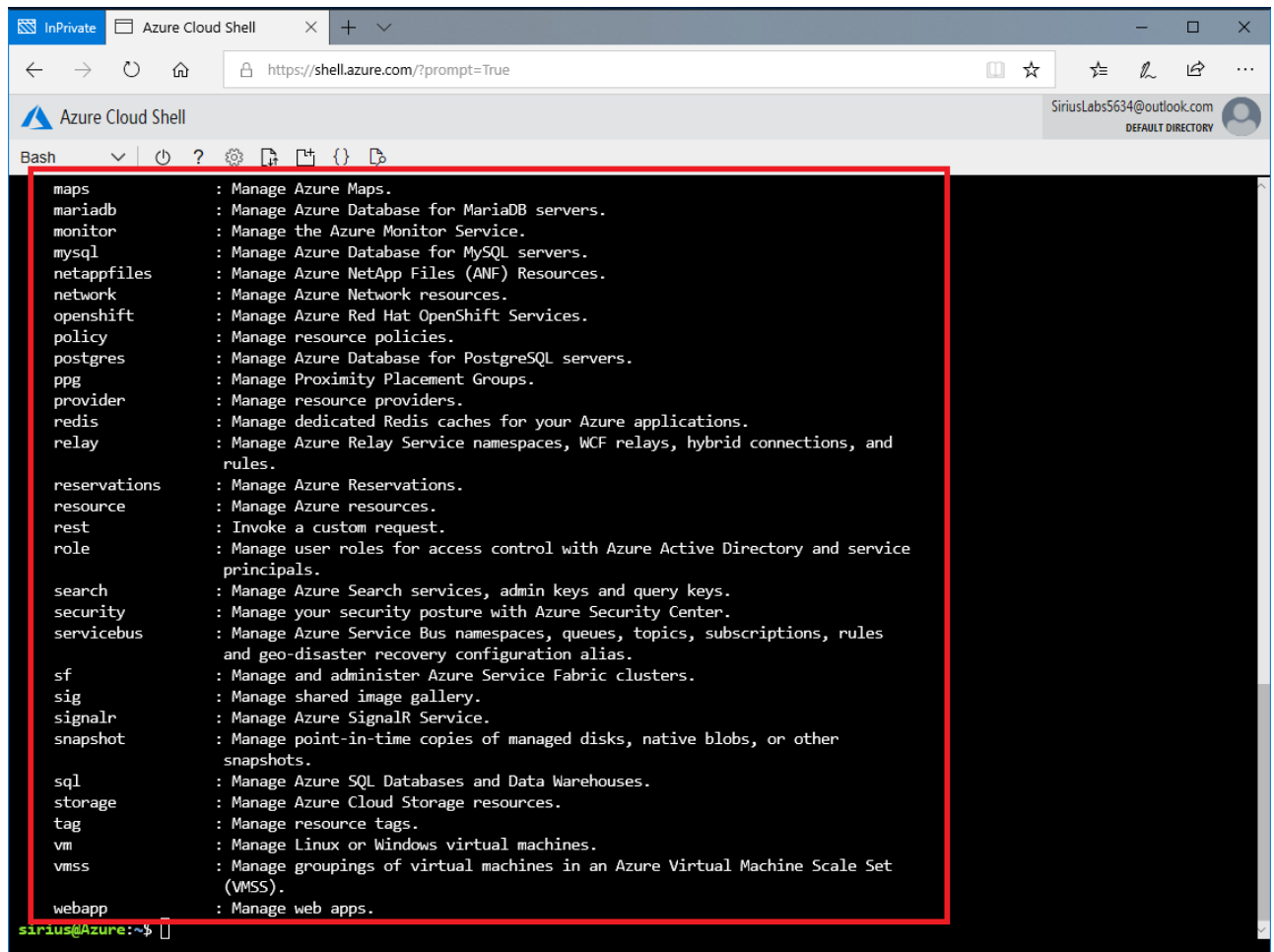


6. To start the Azure CLI, enter the following command and press Enter.

```
az
```



You should see something like the following list of available commands:



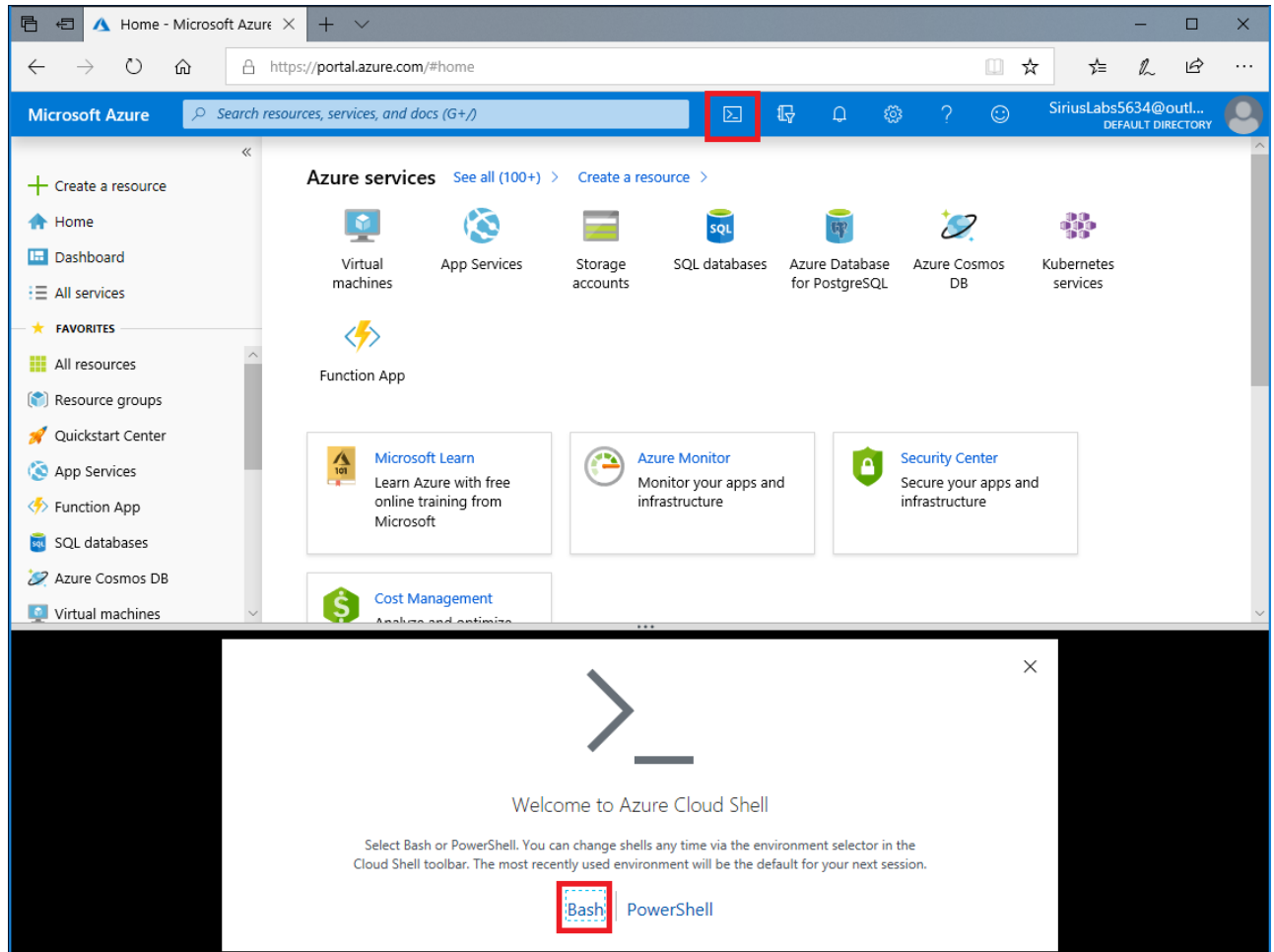
The screenshot shows the Azure Cloud Shell interface in a web browser. The browser address bar shows `https://shell.azure.com/?prompt=True`. The page title is "Azure Cloud Shell". The user's email address, "SiriusLabs5634@outlook.com", is displayed in the top right corner. The main content area shows a list of Azure services and their management descriptions, enclosed in a red rectangular box. The list includes:

- maps : Manage Azure Maps.
- mariadb : Manage Azure Database for MariaDB servers.
- monitor : Manage the Azure Monitor Service.
- mysql : Manage Azure Database for MySQL servers.
- netappfiles : Manage Azure NetApp Files (ANF) Resources.
- network : Manage Azure Network resources.
- openshift : Manage Azure Red Hat OpenShift Services.
- policy : Manage resource policies.
- postgres : Manage Azure Database for PostgreSQL servers.
- ppg : Manage Proximity Placement Groups.
- provider : Manage resource providers.
- redis : Manage dedicated Redis caches for your Azure applications.
- relay : Manage Azure Relay Service namespaces, WCF relays, hybrid connections, and rules.
- reservations : Manage Azure Reservations.
- resource : Manage Azure resources.
- rest : Invoke a custom request.
- role : Manage user roles for access control with Azure Active Directory and service principals.
- search : Manage Azure Search services, admin keys and query keys.
- security : Manage your security posture with Azure Security Center.
- servicebus : Manage Azure Service Bus namespaces, queues, topics, subscriptions, rules and geo-disaster recovery configuration alias.
- sf : Manage and administer Azure Service Fabric clusters.
- sig : Manage shared image gallery.
- signalr : Manage Azure SignalR Service.
- snapshot : Manage point-in-time copies of managed disks, native blobs, or other snapshots.
- sql : Manage Azure SQL Databases and Data Warehouses.
- storage : Manage Azure Cloud Storage resources.
- tag : Manage resource tags.
- vm : Manage Linux or Windows virtual machines.
- vmss : Manage groupings of virtual machines in an Azure Virtual Machine Scale Set (VMSS).
- webapp : Manage web apps.

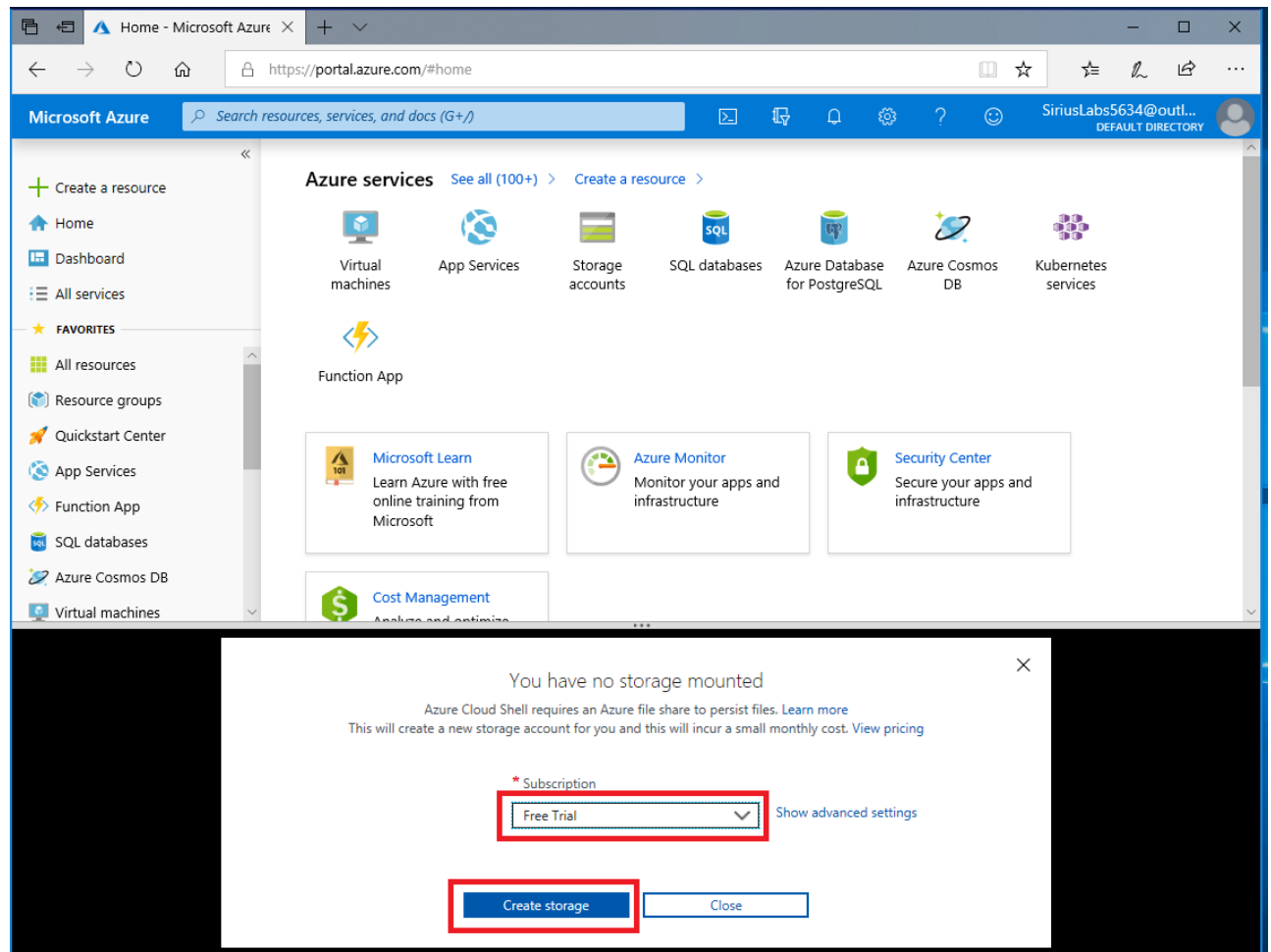
The prompt at the bottom left of the terminal window is `sirius@Azure:~$`.

Option 2 - Login to the Azure Portal and Open Azure Cloud Shell in-line

1. Open the [Azure portal](#) in a browser.
2. Sign into Azure using the Microsoft account email address and password you created for this session.
3. Click the **Cloud Shell** icon in the toolbar to launch the in-line Cloud Shell window, then click **Bash** in the window.

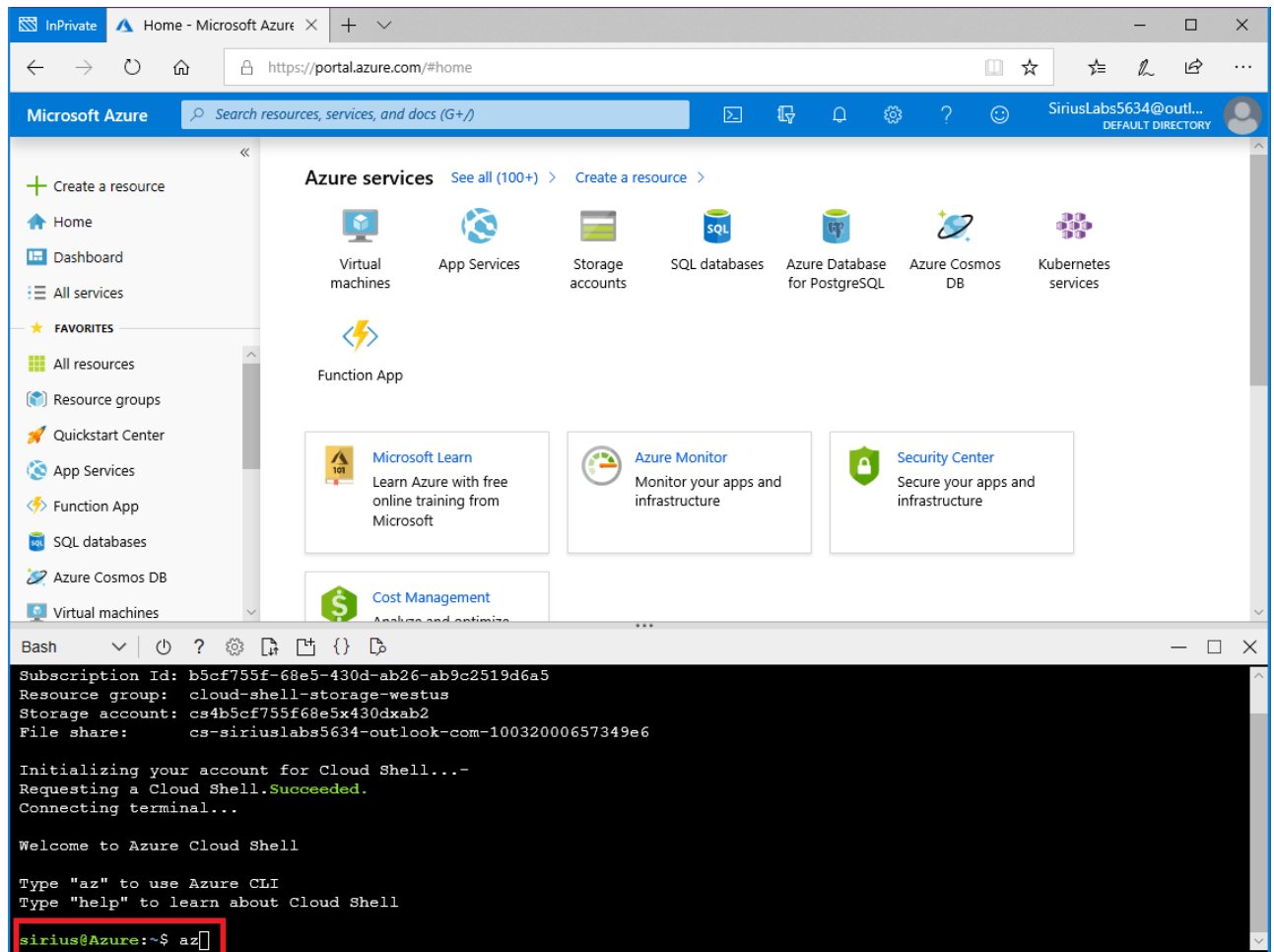


4. Select your subscription, and click **Create storage**.

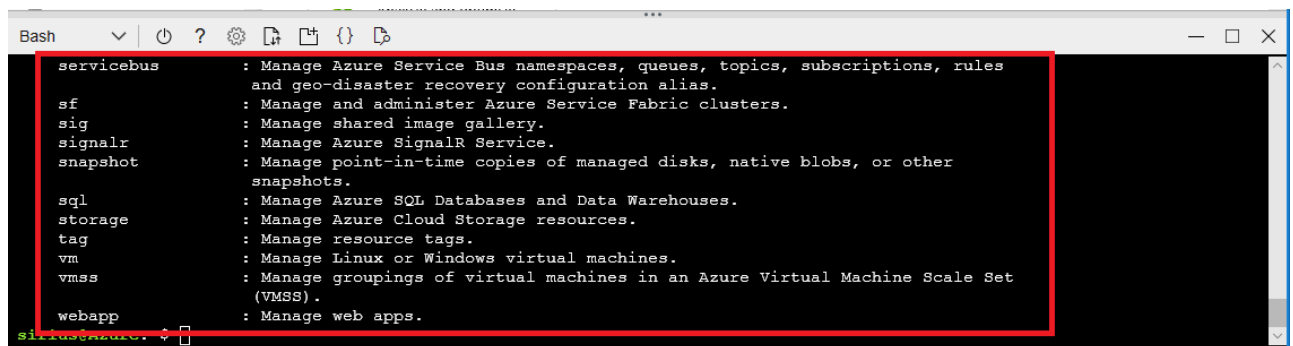


5. To start the Azure CLI, enter the following command and press Enter.

```
az
```



You should see something like the following list of available commands:



Create a resource group

First, create a resource group to contain all of the resources you'll create in this module. Name it **vm-networks** and replace **<location>** in the following command with the name of the region in which you'd like the group to be created.

Note - Chose a location (region) close to you, from the list. Document this location (region) name for use in all future labs.

```
az group create --location <location> --name vm-networks
```

Create a virtual network

To create a virtual network, enter the following command and press Enter.

```
az network vnet create \  
  --name myVnet \  
  --resource-group vm-networks \  
  --subnet-name default
```

Create two virtual machines

All Azure virtual machines are connected to a virtual network. If you create a virtual machine using the Azure CLI and don't specify the name of an existing virtual network, the CLI will search the target resource group for an appropriate virtual network to use, based on location and subnet availability. If no match is found, a new virtual network will be created automatically.

Here, we create two virtual machines without specifying any virtual network information. The default network specifications match the attributes of **myVnet**, so the CLI will automatically locate and use it.

1. To create the first virtual machine, execute the following command to create a Windows VM with a public IP address that is accessible over port 3389 (Remote Desktop). This will create a Windows 2016 Datacenter VM named **dataProcStage1**.

```
az vm create \  
  --name dataProcStage1 \  
  --resource-group vm-networks \  
  --admin-username "DataAdmin" \  
  --image Win2016Datacenter
```

Note

Port 3389 is opened automatically by default when you create a Windows VM in Azure.

2. Supply values for your password at the prompts. Remember to write this password down as you'll need it later to access the server.
3. Copy the **publicIpAddress** value in the returned JSON from creating your VM so you can use it later.
4. You'll now create the second VM. This VM will be named **dataProcStage2** and will not have a public IP address.

```
az vm create \  
  --name dataProcStage2 \  
  --resource-group vm-networks \  
  --public-ip-address "" \  
  --admin-username "DataAdmin" \  
  --image Win2016Datacenter
```


Connect to dataProcStage1 using Remote Desktop

1. Open Remote Desktop and connect to **dataProcStage1** with the public IP address you noted from the previous steps.
2. Log into the remote machine with the username **DataAdmin** and the password you created.
3. In the remote session, open the Windows command prompt and run the following command:

```
ping dataProcStage2 -4
```

4. In the results, you'll see that all requests to **dataProcStage2** time out. This is because the default Windows Firewall configuration on **dataProcStage2** prevents it from responding to pings.

Connect to dataProcStage2 using Remote Desktop

You'll configure the Windows Firewall on **dataProcStage2** using a new remote desktop session. However, you'll not able to access **dataProcStage2** from your desktop. Recall, **dataProcStage2** does not have a public IP address. You will use remote desktop from **dataProcStage1** to connect to **dataProcStage2**.

1. In the **dataProcStage1** remote session, open Remote Desktop.
2. Connect to **dataProcStage2** by name. Based on the default network configuration, **dataProcStage1** can resolve the address for **dataProcStage2** using the computer name.
3. Log in to **dataProcStage2** with the username **DataAdmin** and the password you created.
4. On **dataProcStage2**, click the Start Menu, type **Firewall**, and press Enter. The **Windows Firewall with Advanced Security** console appears.
5. In the left-hand pane, click **Inbound Rules**.
6. In the right-hand pane, scroll down, and right-click **File and Printer Sharing (Echo Request - ICMPv4-In)**, and then click **Enable Rule**.
7. Switch back to the **dataProcStage1** remote session and run the following command in the command prompt.

```
ping dataProcStage2 -4
```

8. **dataProcStage2** responds with four replies, demonstrating connectivity between the two VMs.

You have successfully created a virtual network, created two VMs that are attached to that virtual network, connected to one of the VMs and shown network connectivity to the other VM within the same virtual network. You can use Azure Virtual Network to connect resources within the Azure network. However, those resources need to be within the same resource group and subscription. Next, we will look at VPN gateways, which enable you to connect virtual network in different resource groups, subscriptions, and even geographical regions.

