



## Restricting Network Access to Azure Storage Account Using Virtual Network Service Endpoints

*Virtual network service endpoints offer a direct and secure connection to Azure services using an optimized route over the Azure backbone network.*

### ICON KEY

Valuable information

Test your knowledge

Web exercise

Workbook review

### Lab Scenario

Virtual network service endpoints limit network access to Azure service resources in a virtual network subnet. To safeguard an Azure storage account from unauthorized access, you can restrict network access using virtual network service endpoints.

### Lab Objectives

In this lab, you will learn how to create a resource group, virtual network, network security group, and Azure storage account, and also to create a file share, restrict network access to a subnet, create a VM, etc.

In this lab you will:

- Create a resource group
- Create a virtual network
- Enable a service endpoint
- Restrict network access for a subnet
- Create an Azure storage account
- Create a file share in Azure storage account
- Restrict network access to a subnet
- Create virtual machines
- Confirm access to a storage account
- Confirm a denied access to a storage account

## Lab Environment

To perform this lab, you need the following:

- Admin Machine VM
- Registered Microsoft Azure account

## Lab Duration

Time: 30 minutes

## Overview of Virtual Network Service Endpoints

An Azure virtual network service endpoint helps Azure resources connect and communicate directly and securely over the Azure backbone (instead of connecting over the Internet). A cloud security administrator can use the virtual network service endpoints to secure and directly connect the Azure service resources through an optimized route in the Azure backbone.

In a virtual network, the service endpoints enable the private IP addresses to reach the Azure service's endpoint, ruling out the need for a public IP address. An administrator can restrict the service resource to accept traffic only from a subnet linked to the service endpoint. Using a network security group (NSG), the administrator can lock down or restrict the virtual network to only allow outbound traffic to the desired Azure service and block all other outbound traffic.

Suppose a VM in a virtual network wants to communicate with a storage account in Azure. The administrator can club the storage account, a service endpoint, and NSG to ensure the traffic from a VM in a private subnet does not use the Internet to reach the storage account. All traffic to the storage account is blocked unless it is from this subnet and outbound traffic to the Internet from this subnet is restricted by NSG.

## Lab Tasks

**Note:** Web applications in a cloud environment may undergo frequent updates. As we are working on a cloud-based environment for this lab (i.e., Azure), the application interface may be updated with time. Hence, in case you happen to work on an updated version of Azure, the user interface you see on the application might differ from what you see in the lab. Consequently, the steps and screenshots demonstrated in this lab might also differ.

**Note:** Before starting this lab, you should create an Azure Free Account using the following link: <https://azure.microsoft.com/free>, in case you have already not created it for the previous module. Once the registration is complete, perform the following tasks:

**Note:** You can also use any existing Azure account but be aware that it may incur significant charges to your account.

1. Launch the **Admin Machine VM**. Log in with the following credentials:  
user **Admin** and password **admin@123**.

 **T A S K 1**

**Creating a  
Resource Group**

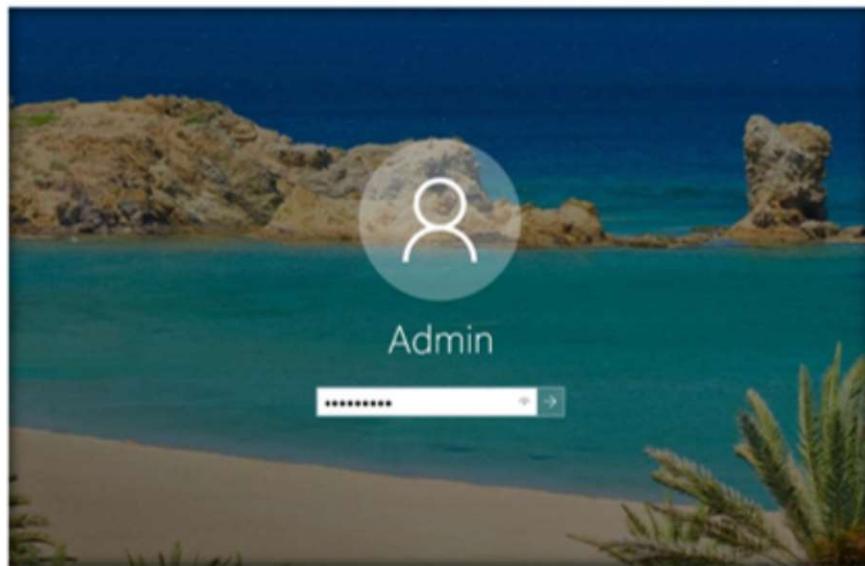


FIGURE 4.10.1: Launch Admin Machine and Log in

2. To open the browser, double-click on the **Google Chrome** icon on the desktop.



FIGURE 4.10.2: Navigating to the Chrome Browser from Taskbar

**Module 04 – Data Security in Cloud**

3. The **Google Chrome** browser opens. Go to the address bar, type <https://azure.microsoft.com/en-in/account/>, and press **Enter**.

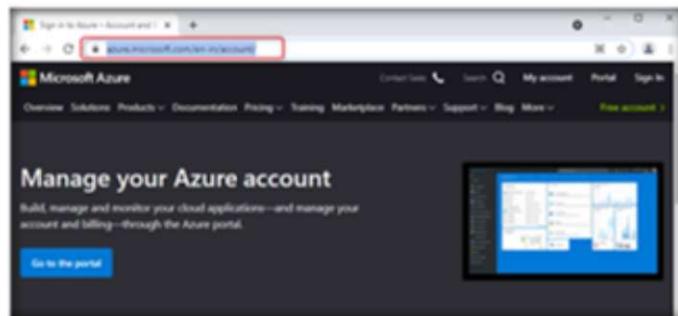


FIGURE 4.10.3: Entering the URL of Microsoft Azure

4. The **Microsoft Azure** page will appear. Click on **Portal**.

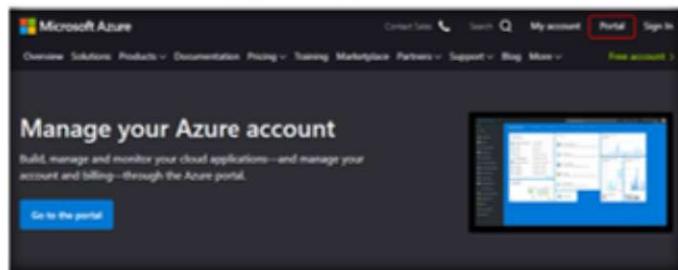


FIGURE 4.10.4: Sign in to Azure Portal

5. In the Sign in page, enter the **Account ID** and click on **Next**.

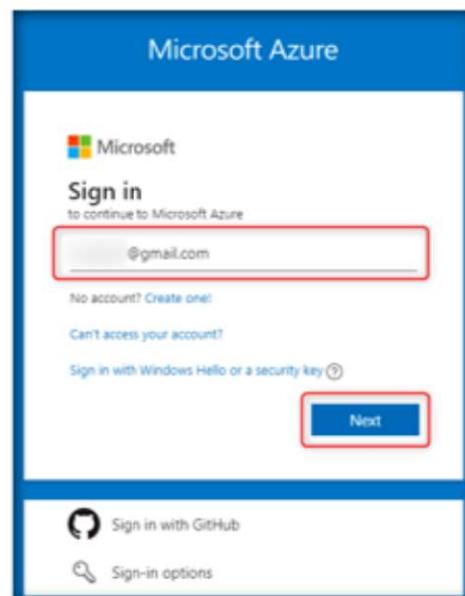


FIGURE 4.10.5: Entering Account ID to continue

6. In the next window, enter the password and click on **Sign in**.

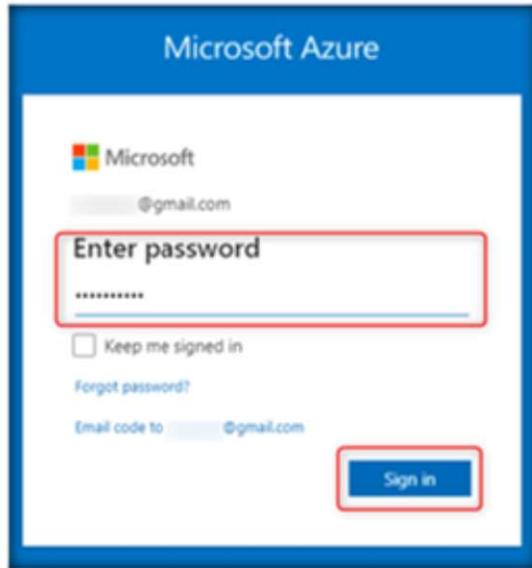


FIGURE 4.10.6: Sign in to Azure Account

7. You will be successfully logged in **Microsoft Azure portal**. Now, to create a resource group, click on **Resource groups**.

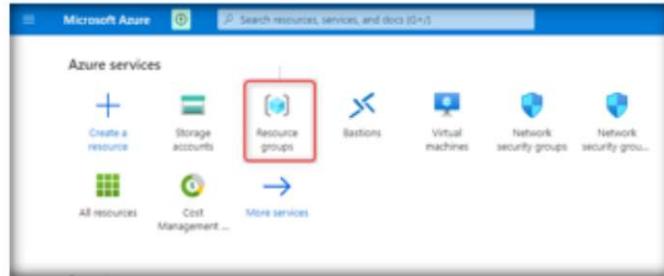


FIGURE 4.10.7: Selecting Resource Groups

8. In the **Resource groups** page, click on **+Add**.

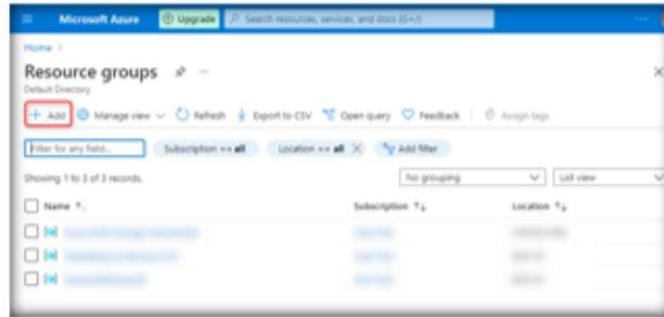


FIGURE 4.10.8: Adding New Resource Group

#### Module 04 – Data Security in Cloud

9. A **Create a resource group** page will open. Enter the resource group name in the **Resource group** field (here, you can use **securityengRG**) and select **(US) East US** in the **Region** field. Now, click on the **Next: Tags >** button.

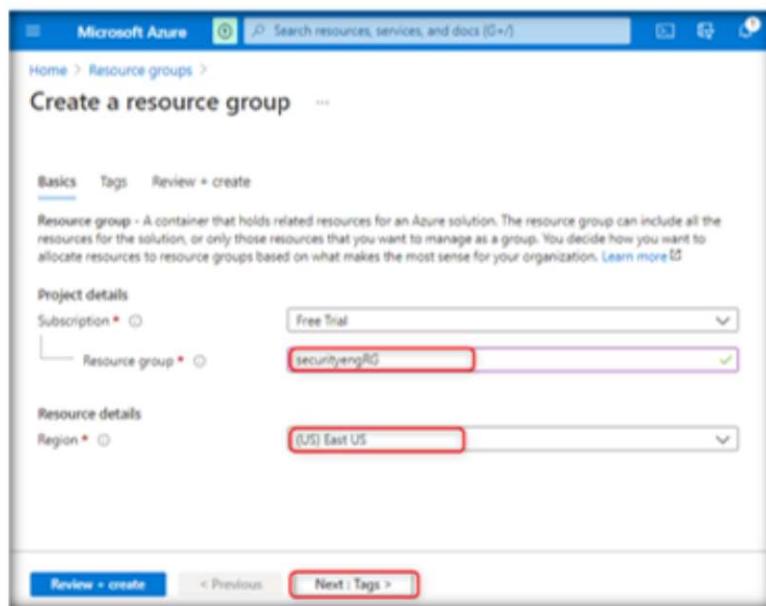


FIGURE 4.10.9: Entering Resource Group Name and Location

10. Leave the **Tags** tab in its default state and click on the **Next: Review + create>** button.

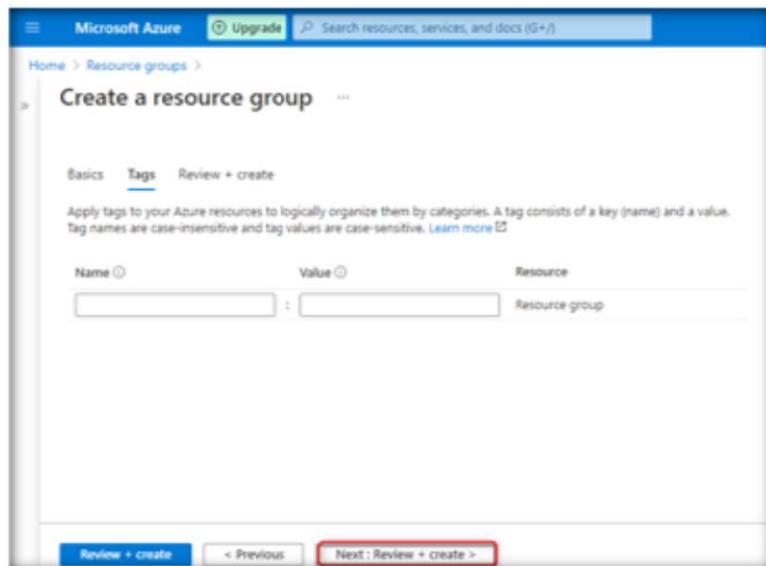


FIGURE 4.10.10: Leaving Tags Tab in Default State

11. After seeing the **Validation passed** message, click on the **Create** button.

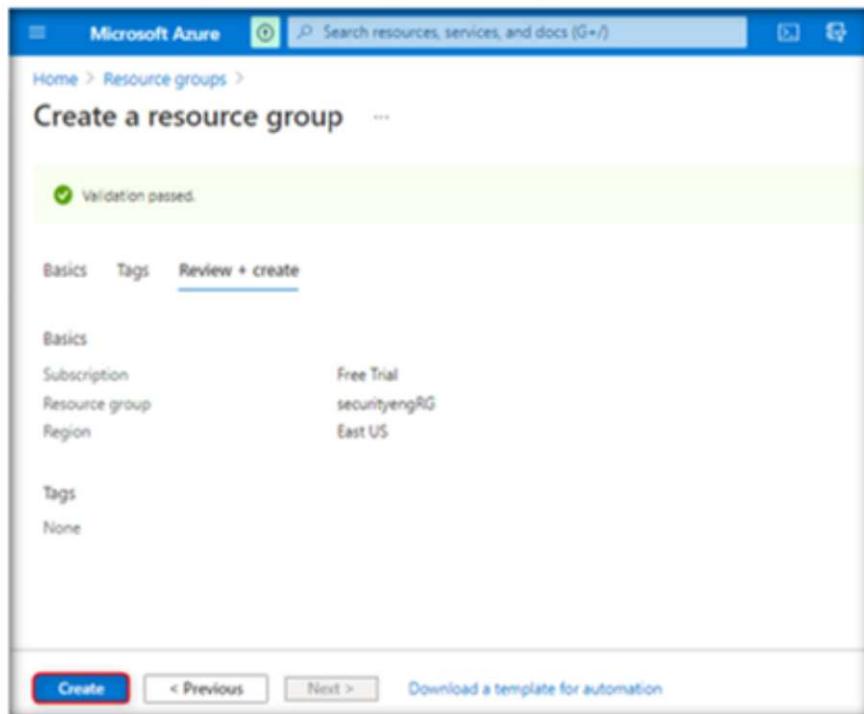


FIGURE 4.10.11: Validation Passed for Creating a Resource Group

12. The **securityengRG** resource group has been successfully created.

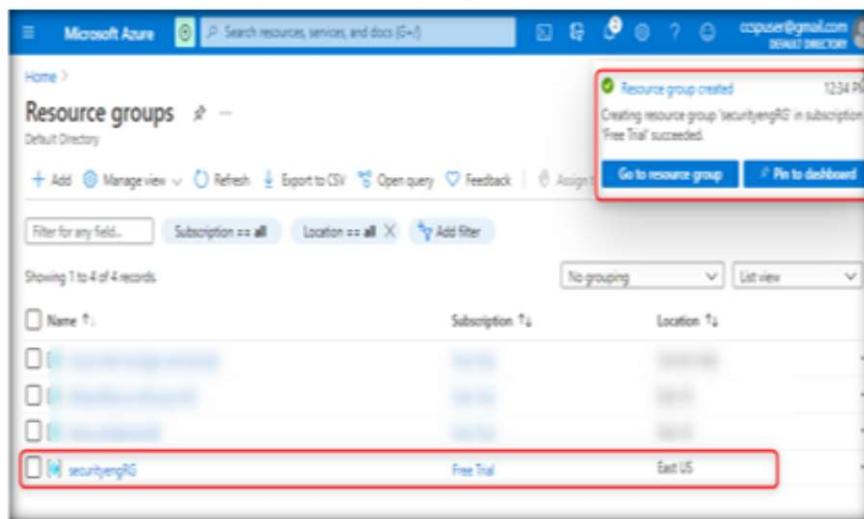


FIGURE 4.10.12: Successfully Creating Resource Group

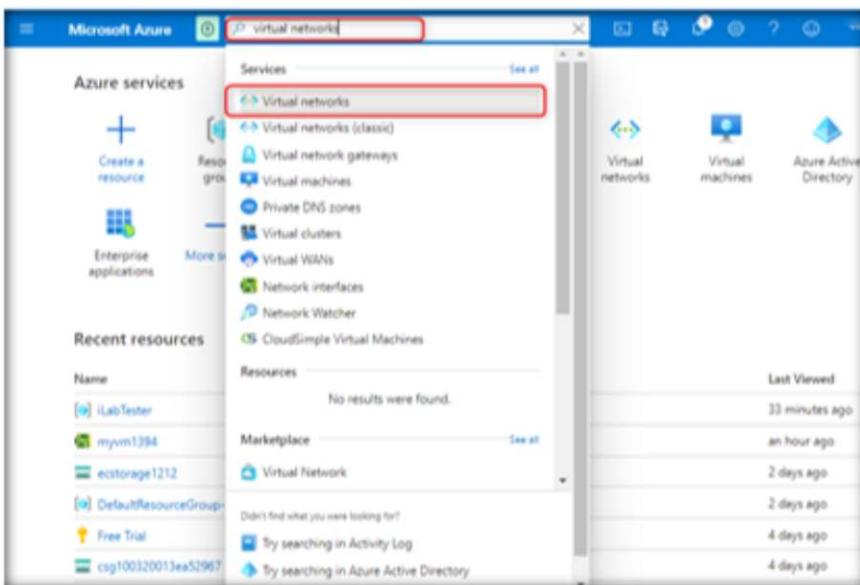
**TASK 2****Create a Virtual Network**

FIGURE 4.10.13: Selecting Virtual Network in Azure Portal

13. Next, to create a virtual network in the resource group (**securityengRG**), go back to Azure portal, type **virtual networks** in the portal search box, and select **Virtual networks**.

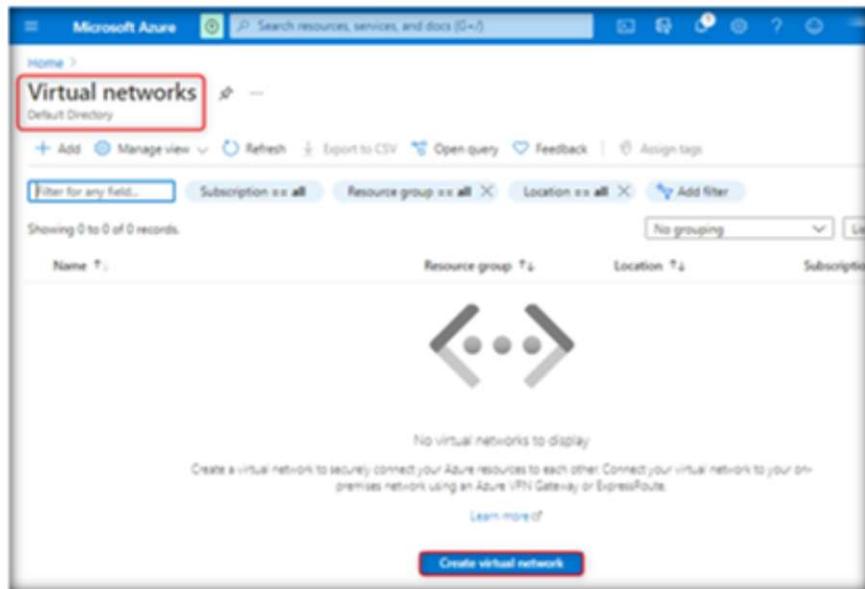


FIGURE 4.10.14 Creating a New Virtual Network

#### Module 04 – Data Security in Cloud

15. In the **Create virtual network** window, select the **Resource group** (here, we have selected **securityengRG**) and enter the name of the virtual network in the **Name** field (here, we have used **SecEng-VNET**). Then, click on **Next: IP Addresses >**.

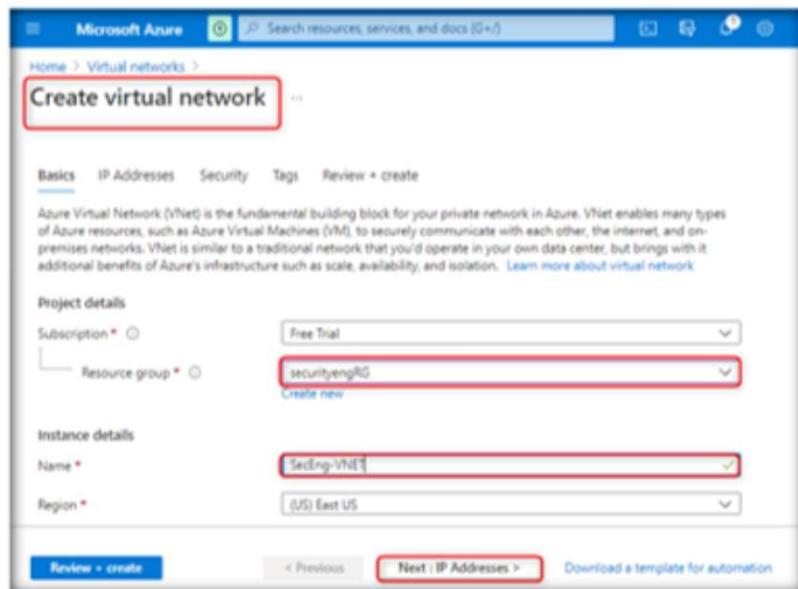


FIGURE 4.10.15: Entering the Name of Resource Group and Virtual Network

16. Keep **IP4 address space** as **4.12.0.0/16**. In the **IP addresses** tab, select the **default** option. An **Edit subnet** pane will open on the left side. Enter the Subnet name as **Public**, leave everything else in their default state, and then click on the **Save** button.

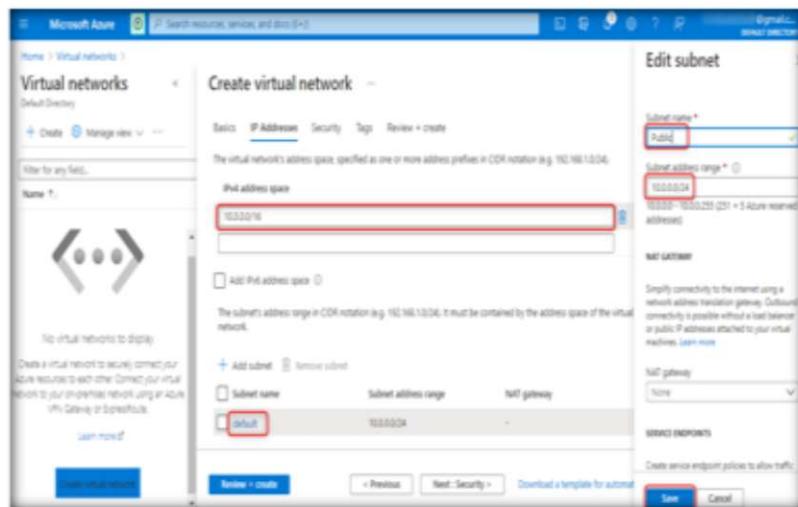


FIGURE 4.10.16: Entering Subnet Details

17. Click on the **Next: Security >** button.

#### Module 04 – Data Security in Cloud

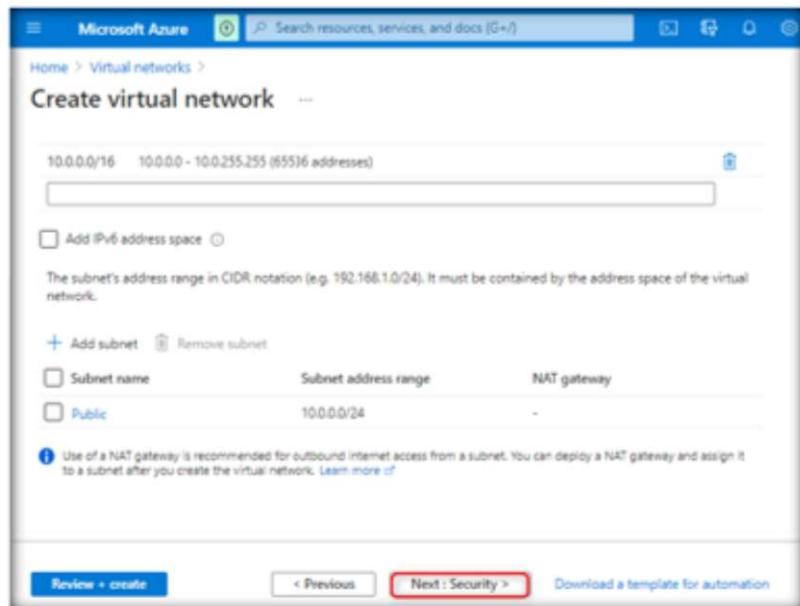


FIGURE 4.10.17: Selecting Security Button

18. In the Security tab, leave everything in their default state, and click on the **Next: Tags >** button.

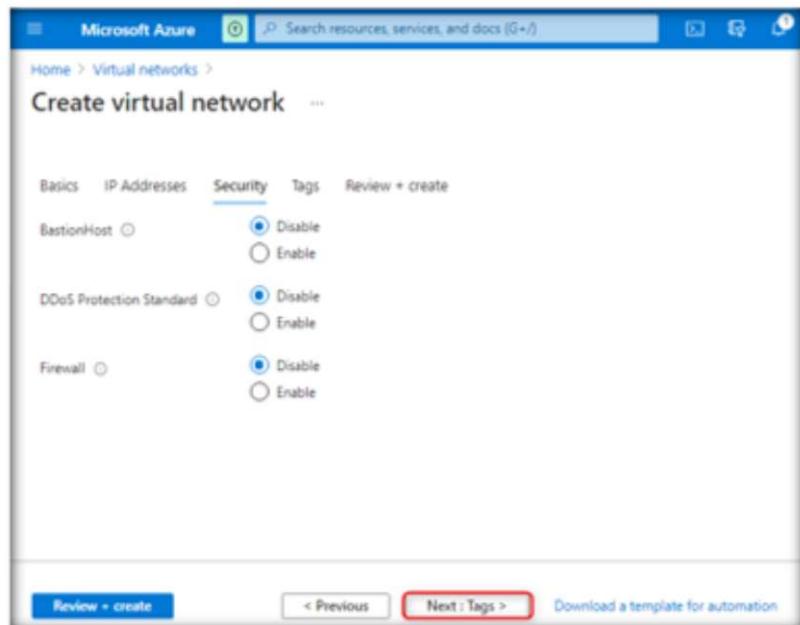


FIGURE 4.10.18: Leaving Security Tab in Default State

19. In the Tags tab, leave everything in their default state and click on the **Next: Review + create >** button.

The screenshot shows the Microsoft Azure portal interface for creating a virtual network. At the top, the title 'Create virtual network' is visible above a form. Below the title, there are tabs: 'Basics', 'IP Addresses', 'Security', 'Tags', and 'Review + create'. The 'Tags' tab is currently selected, indicated by an underline. A note below the tabs explains that tags are name/value pairs used for categorization and billing. It includes a link to learn more about tags. A table for adding tags is present, with two columns: 'Name' and 'Value'. In the first row, there is a blank 'Name' field and a blank 'Value' field separated by a colon. At the bottom of the screen, there are navigation buttons: 'Review + create' (in a blue box), '< Previous', 'Next : Review + create >' (which is highlighted with a red box), and 'Download a template for automation'.

FIGURE 4.10.19: Leaving Tags Tab in Default State

**Module 04 – Data Security in Cloud**

20. After seeing the **Validation passed** message, click on the **Create** button.

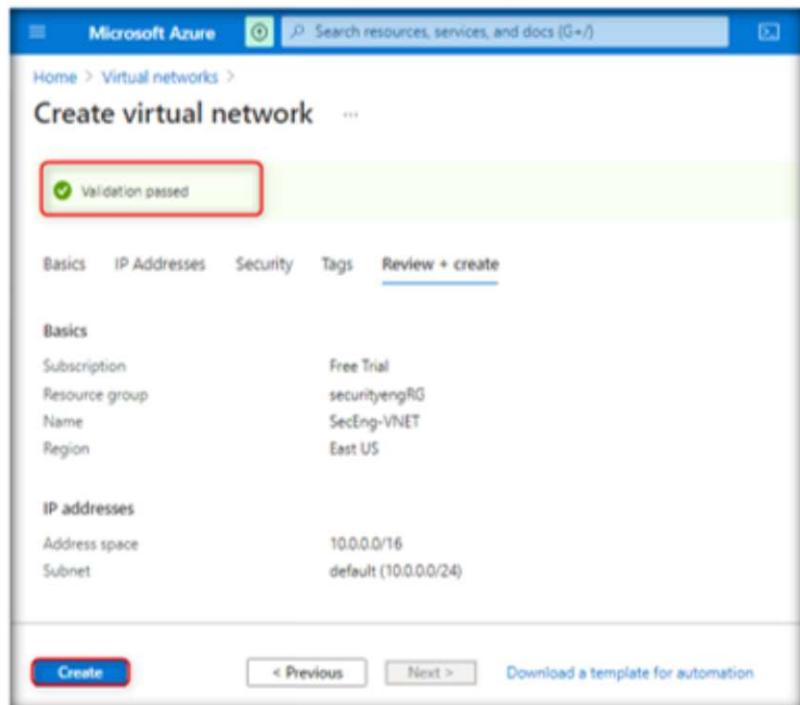


FIGURE 4.10.20: Creating a Virtual Network after Passing the Validation

21. After the successful deployment of the virtual network, click on the **Go to resource** button.

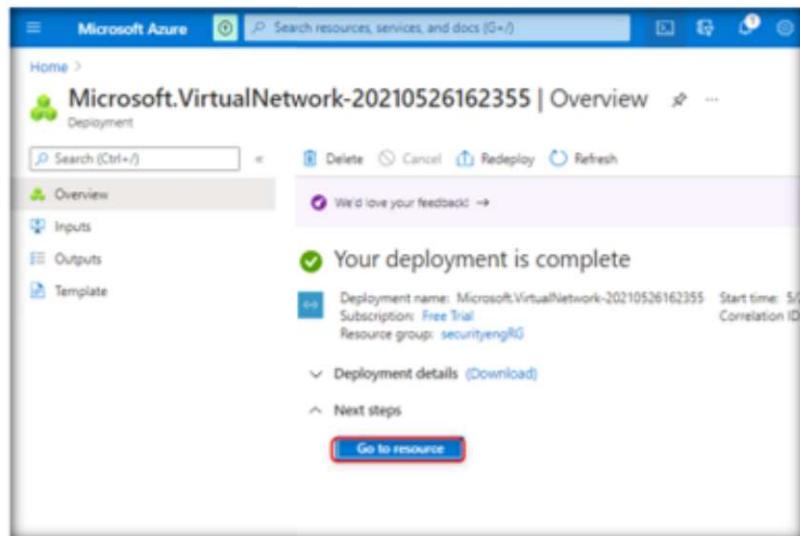


FIGURE 4.10.21: Successful Deployment of Virtual Network

**T A S K 3****Enable a Service Endpoint**

The screenshot shows the Microsoft Azure portal interface for a virtual network named 'SecEng-VNET'. The left sidebar has a 'Subnets' option highlighted with a red box. The main pane displays basic information about the resource group, location, and subscription, along with a table for connected devices which is currently empty.

FIGURE 4.10.22: Selecting Subnets in SecEng-VNET

22. A **SecEng-VNET** window will open. Here, navigate and click on **Subnets** under **Settings** to add a private subnet.

The screenshot shows the 'Add subnet' dialog box within the Azure portal. The 'Name' field is populated with 'Private' and is highlighted with a red box. Other fields include 'Subnet address range' (10.0.1.0/24), 'IPv6 address space' (unchecked), 'NAT gateway' (None), 'Network security group' (None), and 'Route table' (None). At the bottom are 'Save' and 'Cancel' buttons.

FIGURE 4.10.23: Adding Subnet Details

**Module 04 – Data Security in Cloud**

24. Leave the other fields in their default state. Under **SERVICE ENDPOINTS**, click on the **Services** dropdown and select **Microsoft.Storage**. Then, click on the **Save** button.

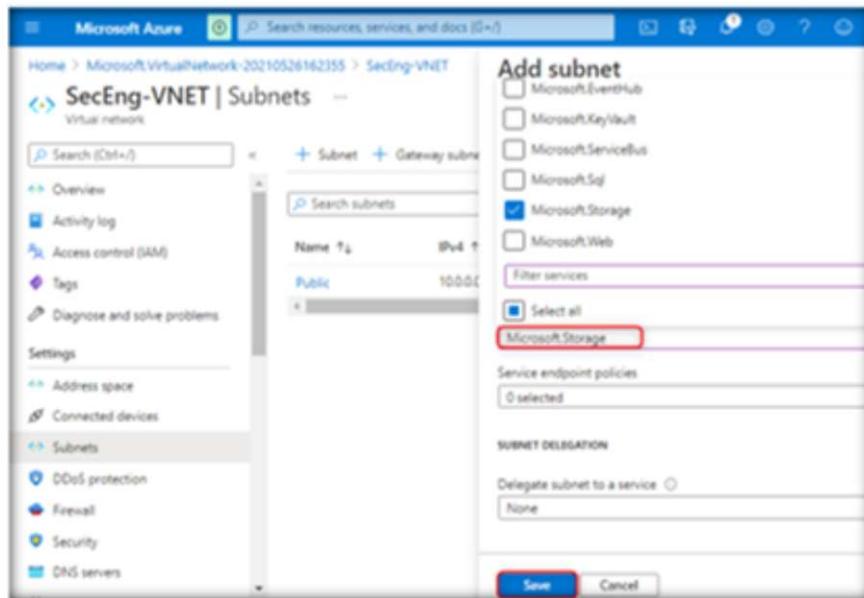


FIGURE 4.10.24: Selecting Service Endpoints

25. **Private** subnet is successfully added to the **SecEng-VNET** virtual network.

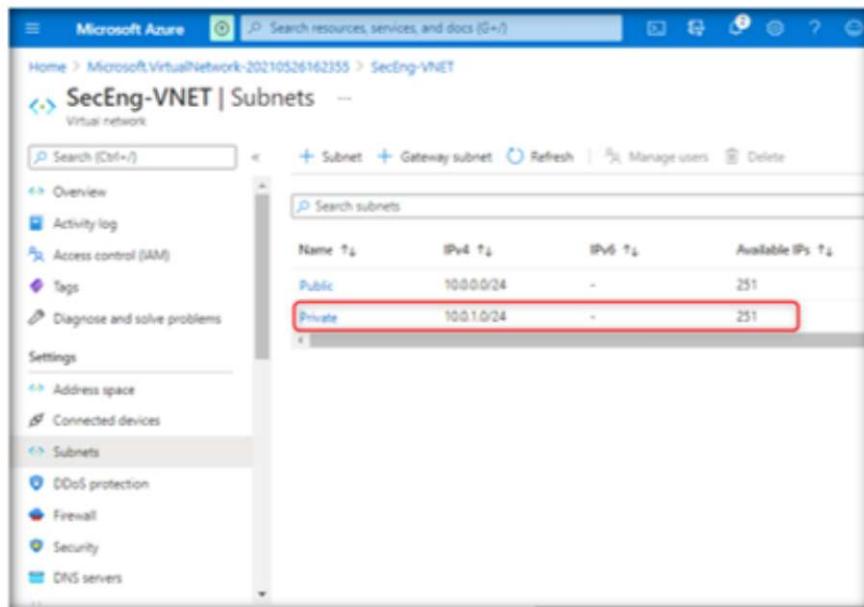


FIGURE 4.10.25: Addition of Private Subnet to SecEng-VNET

**TASK 4****Restrict Network Access for a Subnet**

26. Click on **Home** in the **SecEng-VNET** window to go back to Azure portal.

Name	IPv4	IPv6	Available IPs	Delegated to
Public	10.0.0.0/24	-	251	-
Private	10.0.1.0/24	-	251	-

FIGURE 4.10.26: Going Back to Azure Portal

27. Now, to create a network security group, type **network security group** in the Azure portal search box and select **Network security groups**.

**(Note:** Do not select **Network security groups (classic)**)

- Services
  - Network security groups
  - Network security groups (classic)
  - Virtual networks
  - Application security groups
  - Security
  - Groups
  - Network interfaces
  - Network Watcher
  - Security Baselines
  - Security Center

FIGURE 4.10.27: Selecting Network Security Groups

**Module 04 – Data Security in Cloud**

28. In the **Network Security groups** window, click on the **Create network security group** button.

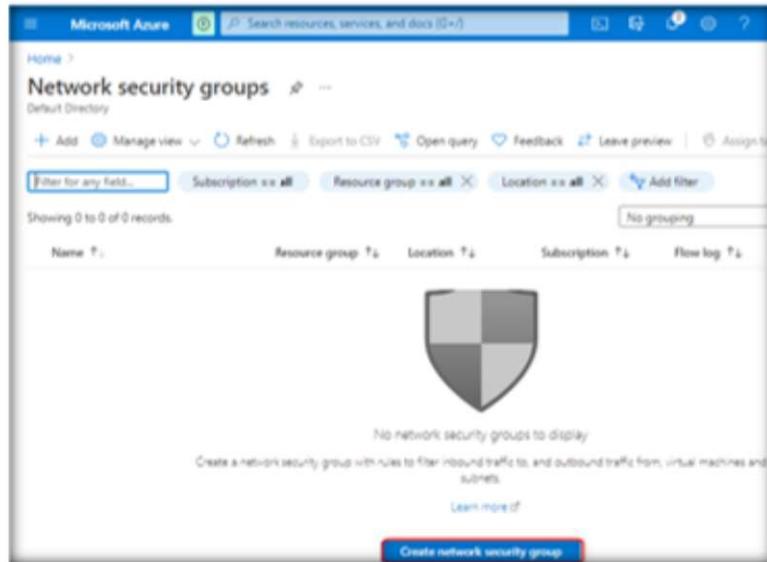


FIGURE 4.10.28: Creating Network Security Group

29. A **Create network security group** window will open. In the **Resource group** field, select **securityengRG** resource group from the dropdown. In the **Name** field, enter **SecEng-NSG**. Then, click on the **Next: Tags >** button.

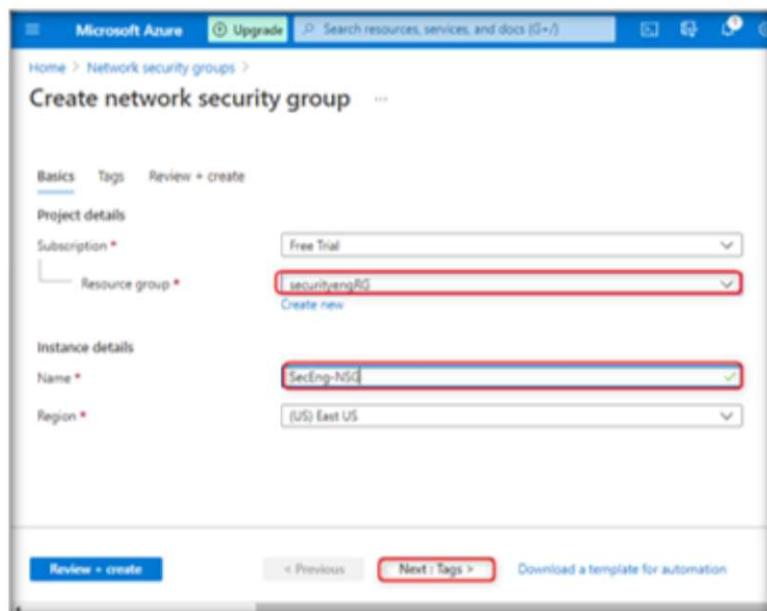


FIGURE 4.10.29: Selecting Resource Group and Entering the Name of the NSG

#### Module 04 – Data Security in Cloud

30. In the **Tags** tab, leave everything in their default state and click on **Next: Review + create >**.

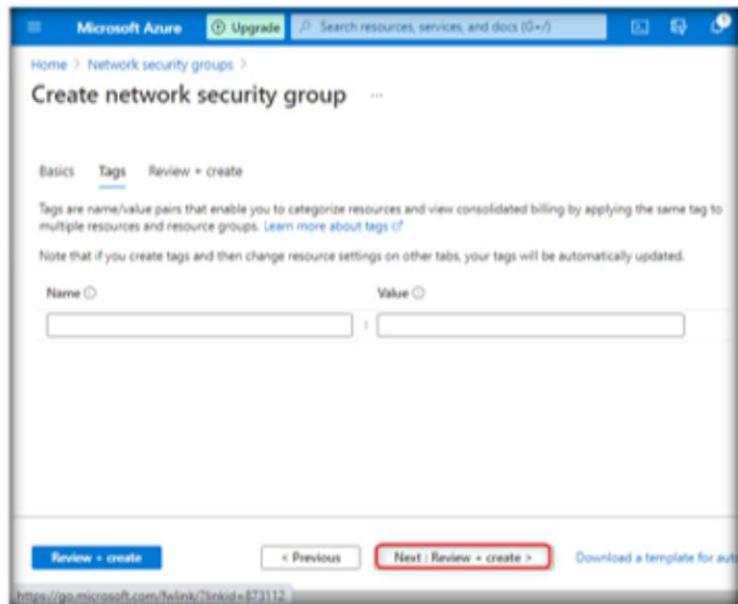


FIGURE 4.10.30: Leaving Tags Tab in Default State

31. After receiving the **Validation passed** message, click on the **Create** button.

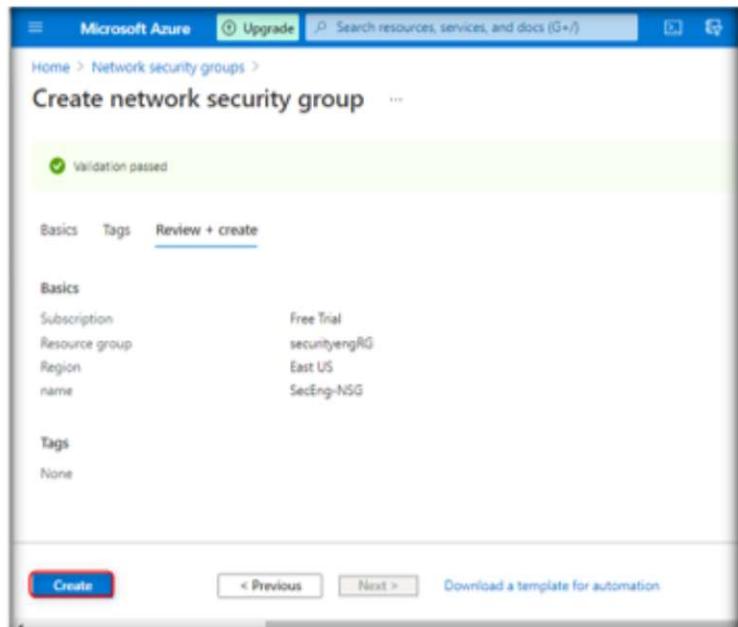


FIGURE 4.10.31: Creating Network Security Group

**Module 04 – Data Security in Cloud**

32. After a successful deployment of the network security group, click on the **Go to resource** button.

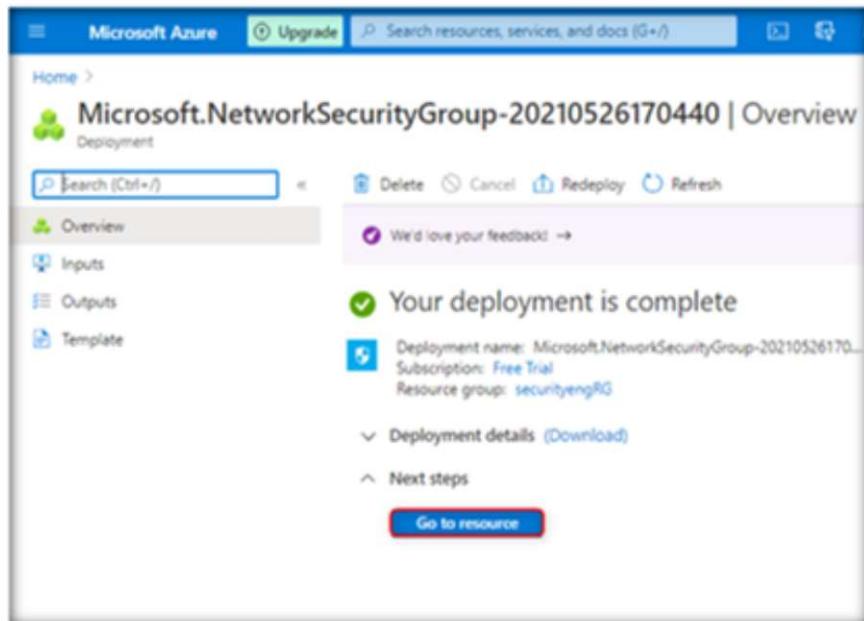


FIGURE 4.10.32: Successful Deployment of Network Security Group

33. A **SecEng-NSG** window will open. Next, you will restrict network access for your created subnet. To do this, navigate and click on **Outbound security rules** under **Settings**.

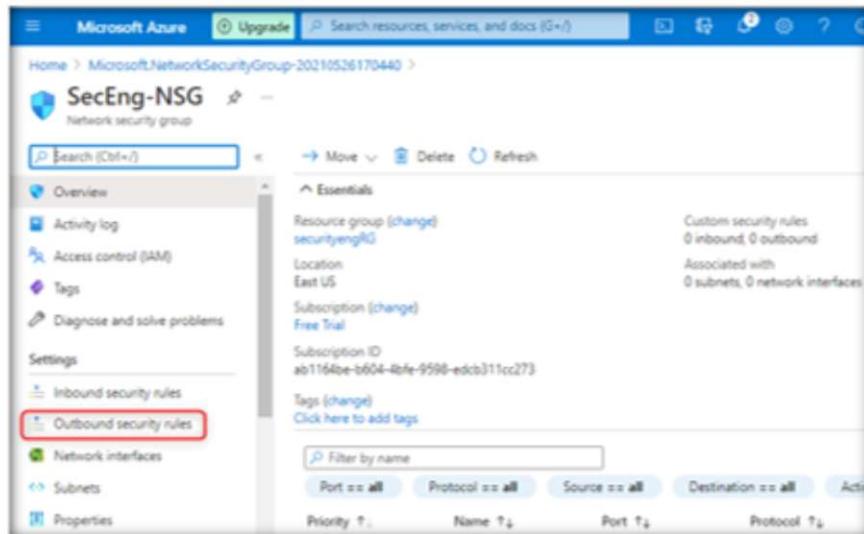


FIGURE 4.10.33: Selecting Outbound Security Rules

34. Click on **+Add**. An **Add outbound security rule** pane will open on the left side. Select the following:

**Source:** Virtual Network

**Destination:** Service Tag

**Destination service tag:** Storage

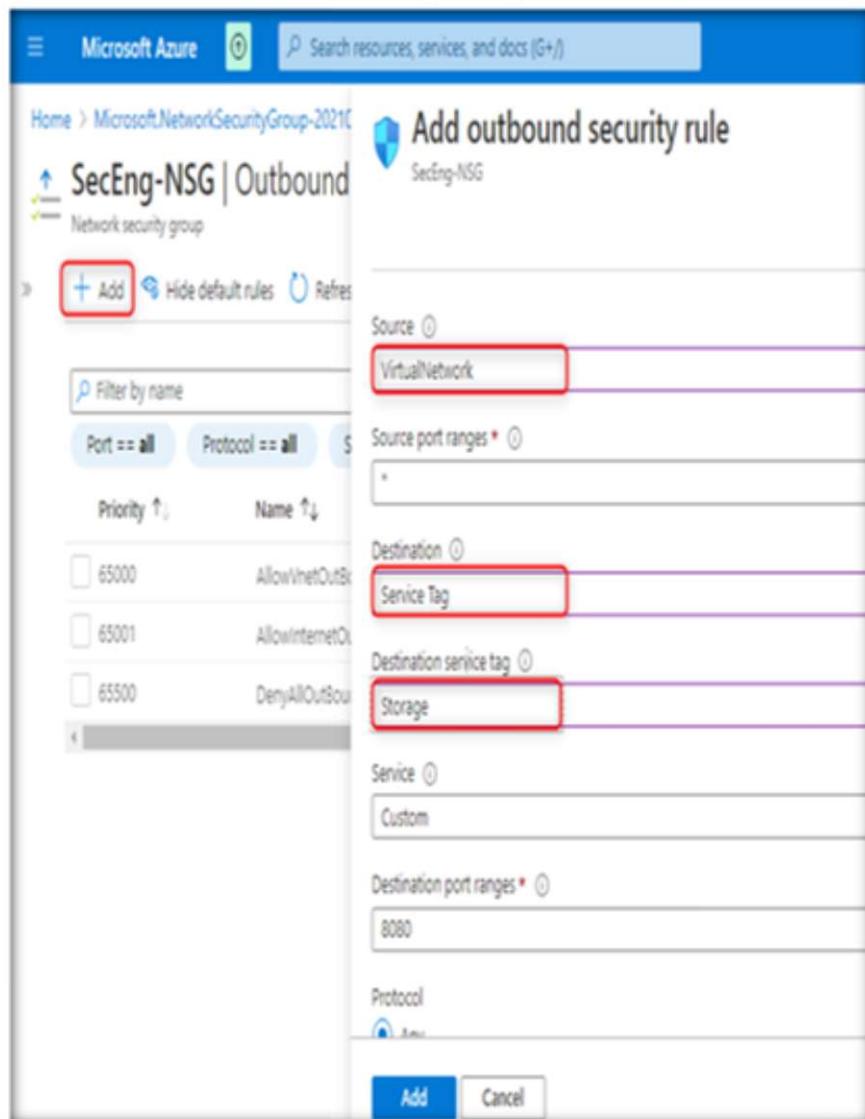


FIGURE 4.10.34: Adding Source, Destination, and Destination Service Tag

35. Scroll down the Add outbound security rule pane and select the following:

**Destination port range:** \*

**Protocol:** Any

**Action:** Allow

**Priority:** 100

**Name:** Allow-Storage-All

Then, click on the **Add** button.

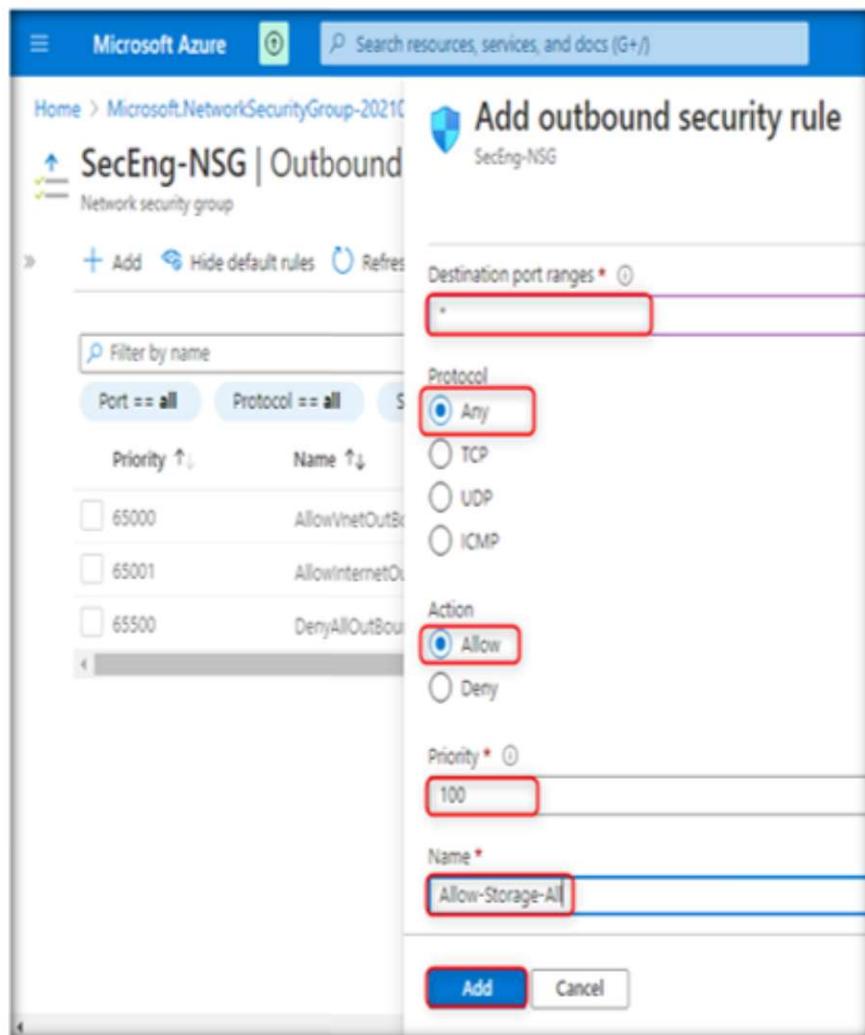


FIGURE 4.10.35: Adding Destination Port Ranges, Protocol, Action, Priority, and Name

#### Module 04 – Data Security in Cloud

36. The outbound security rule **Allow-Storage-All** is successfully created now.

The screenshot shows the 'Outbound security rules' section of the SecEng-NSG Network security group. A table lists five rules:

Priority	Name	Port	Protocol	Source	Destination
100	Allow-Storage-All	Any	Any	VirtualNetwork	Storage
110	Deny-Internet-All	Any	Any	VirtualNetwork	Internet
65000	AllowVnetOutbound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowInternetOutbound	Any	Any	Any	Internet
65500	DenyAllOutbound	Any	Any	Any	Any

FIGURE 4.10.36: Allow-Storage-All Rule is Created

37. We will create another outbound security rule that denies a communication with the Internet. Click on the **+Add** button and select the following:

**Source:** Virtual Network

**Destination:** Service Tag

**Destination service tag:** Internet

**Destination port ranges:** \*

The screenshot shows the 'Add outbound security rule' dialog for the SecEng-NSG Network security group. The configuration fields are:

- Source:** VirtualNetwork (highlighted with a red box)
- Source port ranges:** \* (highlighted with a red box)
- Destination:** Service Tag (highlighted with a red box)
- Destination service tag:** Internet (highlighted with a red box)
- Service:** Custom
- Destination port ranges:** \* (highlighted with a red box)
- Protocol:** All

FIGURE 4.10.37: Adding Source, Destination, Destination Service Tag, and Destination Port Ranges

38. Scroll down the Add outbound security rule pane and select the following:

**Protocol:** Any

**Priority:** 110

**Name:** Deny-Internet-All

Click the **Add** button.

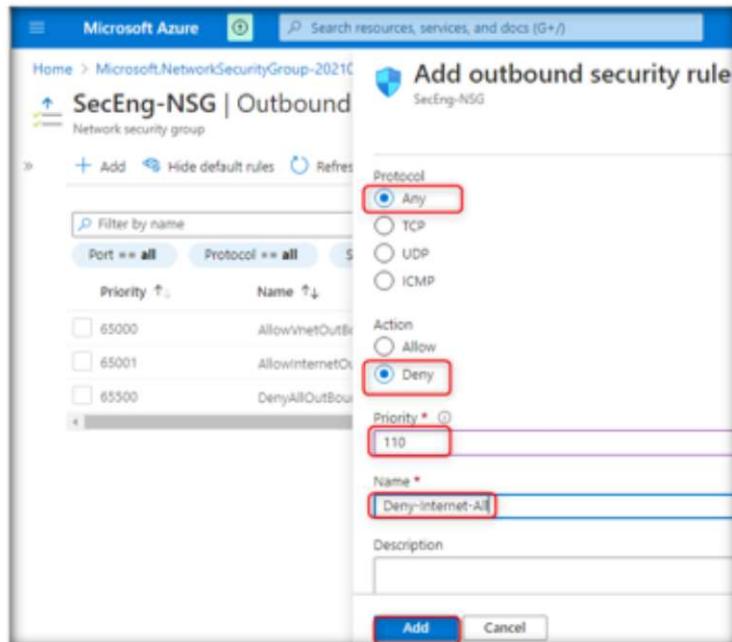


FIGURE 4.10.38: Selecting Protocol, Action, Priority, and Name

39. Click the **Refresh** button. The outbound security rule **Deny-Internet-All** has been successfully created.

Priority	Name To	From To	Protocol	Source To	Destination
100	Allow-Storage-All	Any	Any	VirtualNetwork	Storage
110	Deny-Internet-All	Any	Any	VirtualNetwork	Internet
65000	AllowVNetOutbound	Any	Any	VirtualNetwork	VirtualNet
65001	AllowInternetOutbound	Any	Any	Any	Internet
65500	DenyAllOutbound	Any	Any	Any	Any

FIGURE 4.10.39: Deny-Internet-All Rule is Created

40. Click on Inbound security rules under Settings.

Port xx all	Protocol xx all	Source xx all	Destination xx all
65000	AllowVnetInbound	Any	Any
65001	AllowAzureLoadBalancerInbound	Any	Any
65500	DenyAllInbound	Any	Any

FIGURE 4.10.40: Selecting Inbound Security Rules

41. Click on **+Add**, and select the following under the **Add inbound security rule** window:

**Source:** Any

**Source port ranges:** \*

**Destination:** VirtualNetwork

**Destination port ranges:** 3389

**Protocol:** Any

FIGURE 4.10.41: Adding Source, Source Port Ranges, Destination, and Destination Port Ranges, and Selecting Protocol

42. Scroll down the **Add inbound security rule** pane and select the following:

**Action:** Allow

**Priority:** 120

**Name:** Allow-RDP-All

Then, click on **Add** button.

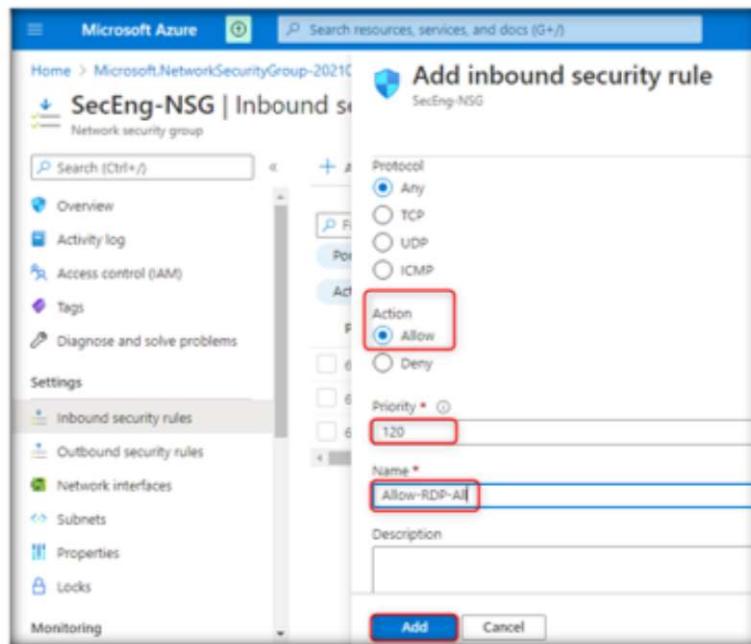


FIGURE 4.10.42: Selecting Action and Adding Priority and Name

43. Click **Refresh** button. The inbound security rule **Allow-RDP-All** is successfully created now.

Priority	Name	Port	Protocol
120	Allow-RDP-All	3389	Any
85000	AllowVnetInbound	Any	Any
85001	AllowAzureLoadBalanc-	Any	Any
65300	DenyAllInbound	Any	Any

FIGURE 4.10.43: Inbound Security Rule is Created

44. Click on Subnets under Settings, and then click on +Associate.

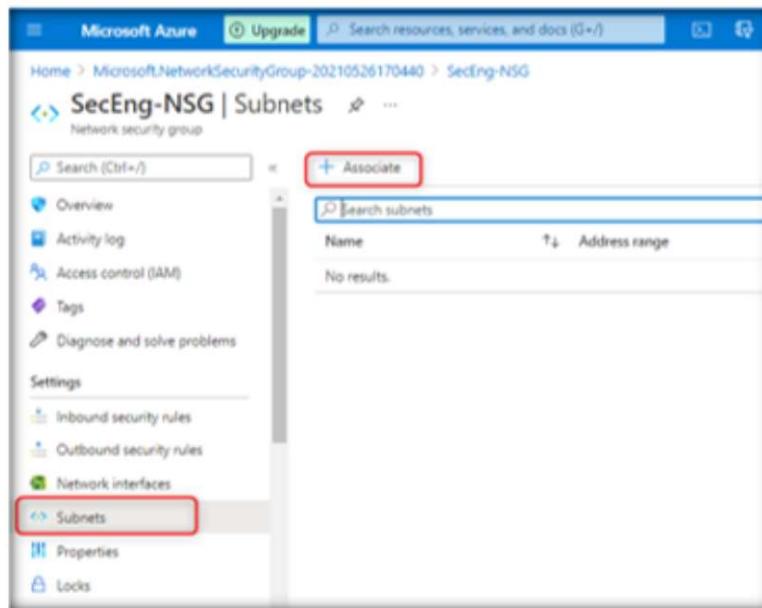


FIGURE 4.10.44: Selecting Subnets

45. An **Associate subnet** pane will open on the left side. Select **SecEng-VNET**, in the **Virtual network** dropdown and **Private** in the **Subnet** field. Then, click on **OK** button.

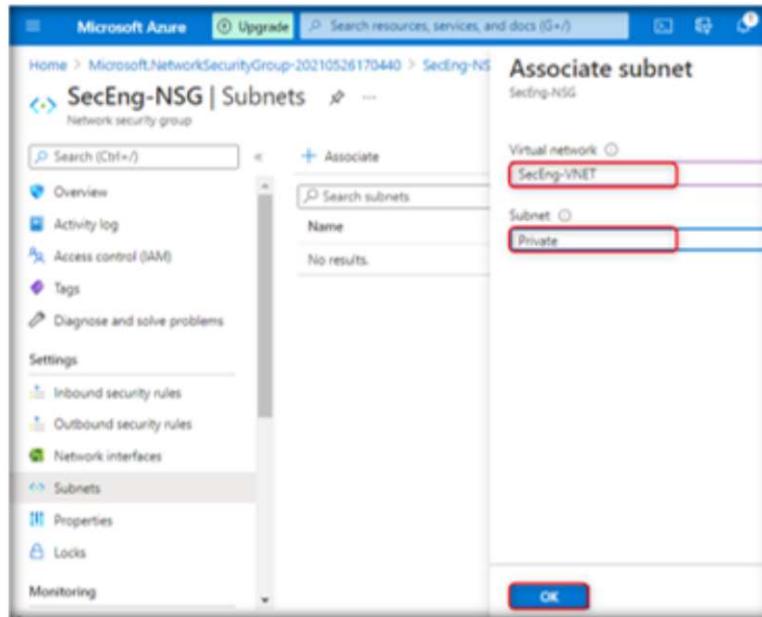


FIGURE 4.10.45: Associating Subnet

## Module 04 – Data Security in Cloud

46. The NSG is successfully saved for the **Private** subnet.

Name	IP Address range	Virtual network
Private	10.0.1.0/24	SecEng-VNET

FIGURE 4.10.46: Private Subnet Successfully Associated with NSG

### T A S K 5

#### Create Azure Storage Account

47. Click on **Home** to go back to Azure portal.

FIGURE 4.10.47: Going Back to Azure Portal

48. Now, create an Azure storage account. To do this, click on the Azure portal menu, and navigate and click on **Storage accounts**.

FIGURE 4.10.48: Selecting Storage Accounts

**Module 04 – Data Security in Cloud**

49. In the **Storage account** window, click **+Add**.

The screenshot shows the Microsoft Azure Storage accounts page. At the top, there's a search bar and several filter options: 'Subscription == all', 'Resource group == all', and 'Location == all'. Below the filters, a table header includes columns for Name, Type, Kind, Resource group, and Location. A red box highlights the '+ Add' button in the top-left corner of the table area.

FIGURE 4.10.49: Adding a Storage Account

50. A **Create a storage account** window will open. In the **Resource group** field, select **securityengRG**.

The screenshot shows the 'Create a storage account' wizard. The 'Basics' tab is selected. Under 'Project details', it says: 'Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.' A red box highlights the 'Resource group' dropdown menu. Inside the menu, 'securityengRG' is selected and highlighted with a red box.

FIGURE 4.10.50: Selecting Resource Group for Storage Account

**Module 04 – Data Security in Cloud**

51. Scroll down the **Create a storage account** window. In the **Storage account name** field, enter the name of the storage account (here, we have used **mystorage25**) and then click on the **Next: Advanced >** button.

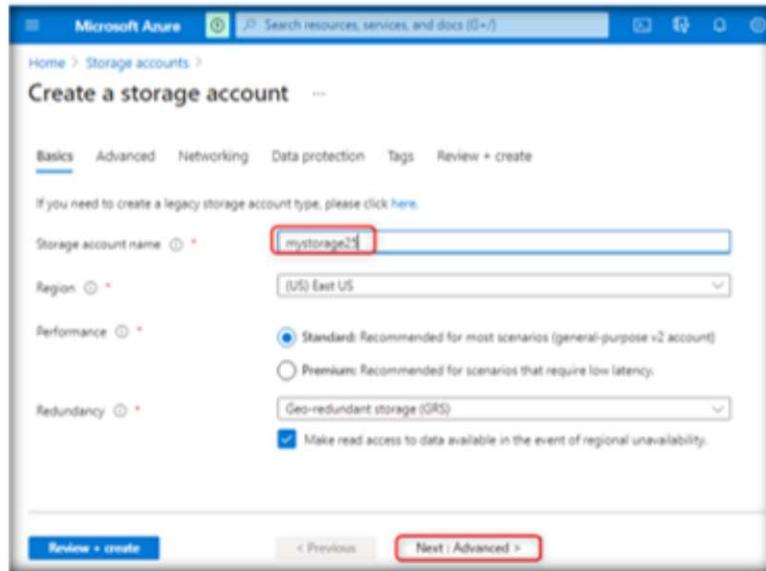


FIGURE 4.10.51: Entering Storage Account Name

52. In the **Advanced** tab, leave everything in their default state and click on **Next: Networking >**.

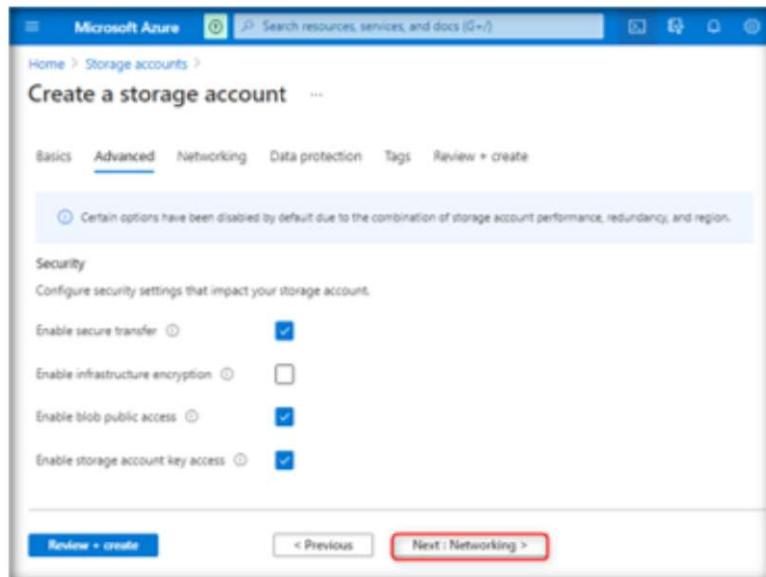


FIGURE 4.10.52: Leaving Advanced Tab in Default State

#### Module 04 – Data Security in Cloud

53. In the **Networking** tab, leave everything in their default state and click on **Next: Data Protection >**.

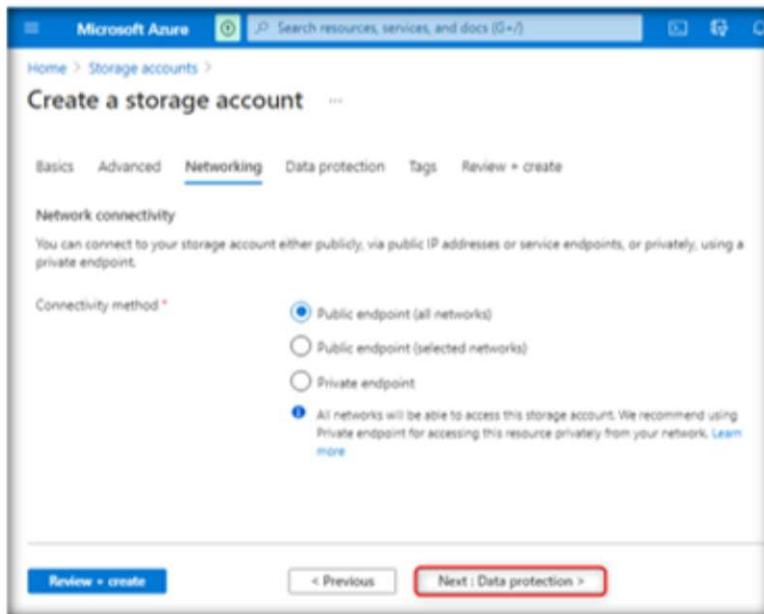


FIGURE 4.10.53: Leaving Networking Tab in Default State

54. In the **Data protection** tab, leave everything in their default state and click on **Next: Tags >**.

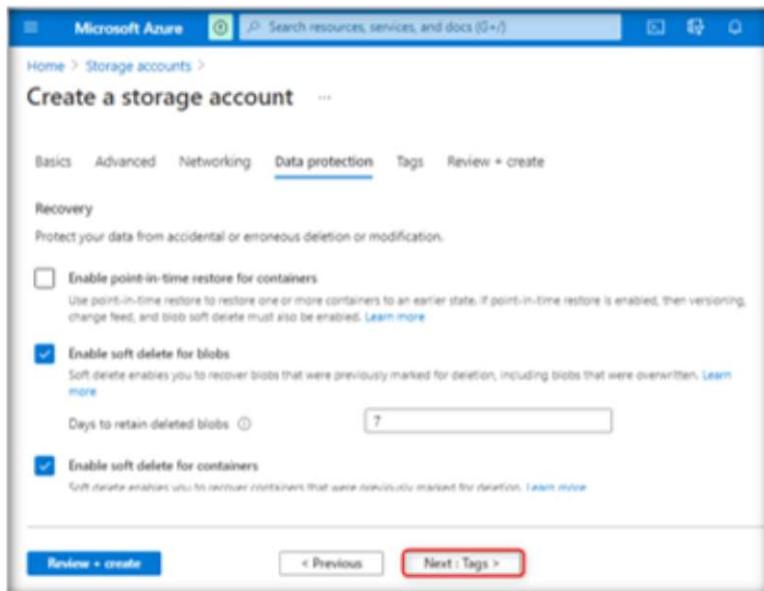


FIGURE 4.10.54: Leaving Data protection Tab in Default State

#### Module 04 – Data Security in Cloud

55. In the **Tags** tab, leave everything in their default state and click on **Next: Review + create >**.

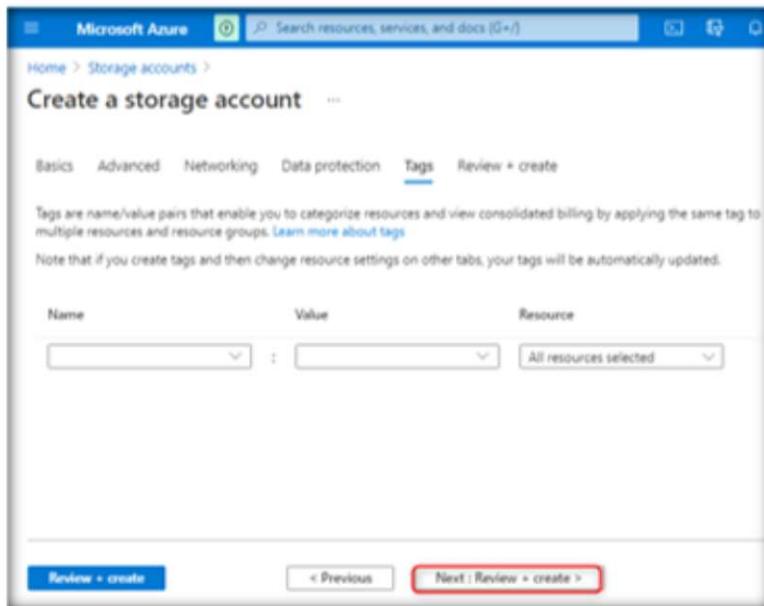


FIGURE 4.10.55: Leaving Tags Tab in Default State

56. After viewing the **Validation passed** message, click on the **Create** button.

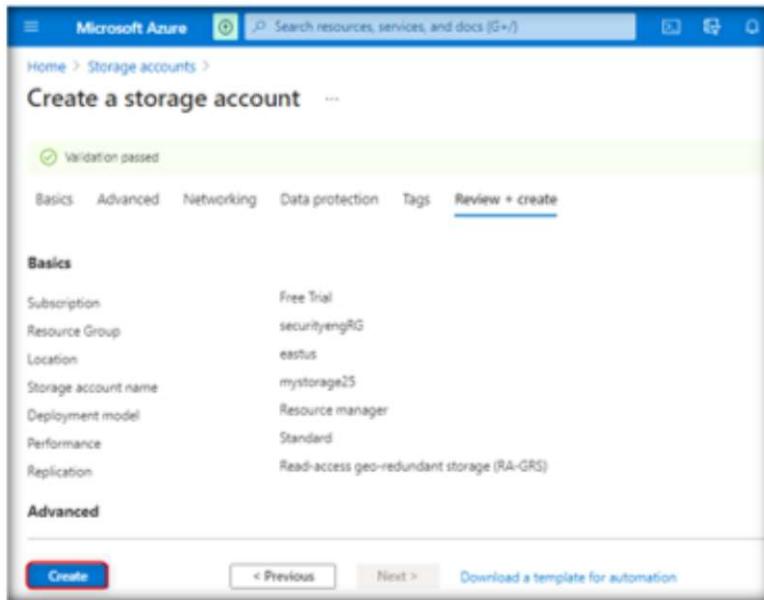


FIGURE 4.10.56: Creating Storage Account after Validation Passed

57. Wait for few seconds for the deployment to complete.

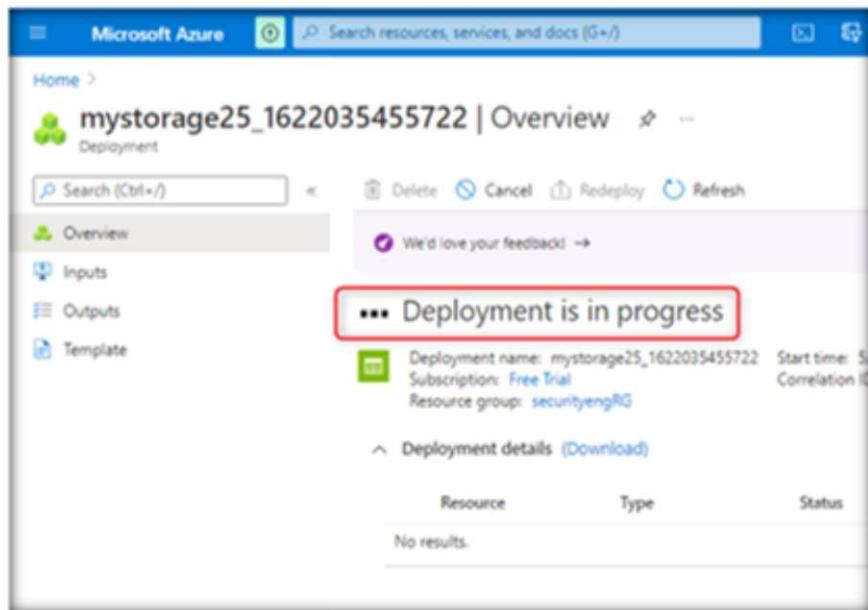


FIGURE 4.10.57: Storage Account Deployment in Progress

58. After the successful deployment of the storage account, click on the **Go to resource** button.

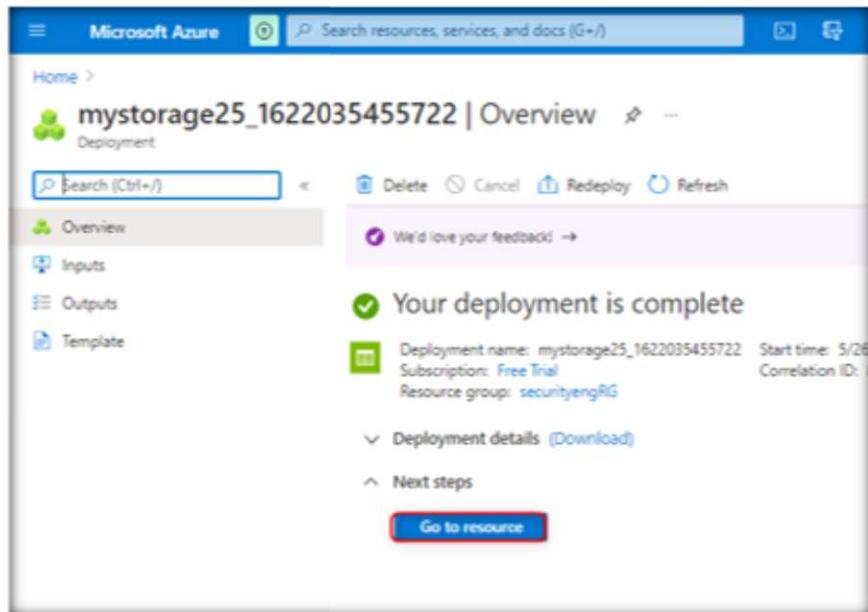


FIGURE 4.10.58: Storage Account Successfully Deployed

**T A S K 6****Create a File Share in Azure Storage Account**

The screenshot shows the Azure Storage account 'mystorage25' overview. The 'File shares' option in the left sidebar is highlighted with a red box. The main pane displays storage details such as Resource group (securityRG), Location (East US), Secondary location (West US), Subscription (Free Trial), and Disk state (Primary: Available, Secondary: Available). The 'File shares' section is currently empty.

FIGURE 4.10.59: Selecting File shares in Storage Account

60. Click on **+ File share**. A New file share pane will open to the left side. In the **Name** field, enter **my-file-share** and click on the **Create** button.

The screenshot shows the 'New file share' dialog box. The 'Name' field is filled with 'my-file-share'. The 'Tiers' section shows 'Premium' selected. The 'Create' button is at the bottom right.

FIGURE 4.10.60: Entering Name of the File Share

#### Module 04 – Data Security in Cloud

61. The storage file share is successfully created now.

The screenshot shows the 'File shares' section of the Azure Storage account 'mystorage25'. A new file share named 'my-file-share' has been created, highlighted with a red border. The table lists the share name, modified date, tier, and quota.

Name	Modified	Tier	Quota
my-file-share	5/27/2021, 10:55:34 ...	Transaction-optimized	3.1TB

FIGURE 4.10.61: my-file-share is created

62. Click on **mystorage25** to go back to the storage account.

The screenshot shows the 'File shares' section of the Azure Storage account 'mystorage25'. The 'my-file-share' entry is visible in the list.

FIGURE 4.10.62: Going Back to Storage Account

63. In the **mystorage25** window, navigate and click on **Networking** under **Security + networking**.

The screenshot shows the 'Networking' settings for the 'mystorage25' storage account. The 'Networking' option is selected in the left sidebar. The right pane displays basic account information and networking details.

FIGURE 4.10.63: Selecting Networking in Storage Account

64. Select the Firewalls and virtual networks tab.

FIGURE 4.10.64: Selecting Firewalls and Virtual Networks Tab

65. Under Allow access from, choose the Selected networks radio button. Then, click on +Add existing virtual network under Virtual networks. An Add networks pane will open on the left side.

FIGURE 4.10.65: Adding an Existing Virtual Network

**Module 04 – Data Security in Cloud**

66. In the **Add networks** pane, select **SecEng-VNET** under **Virtual networks** and **Private** under **Subnets**. Then, click on the **Add** button.

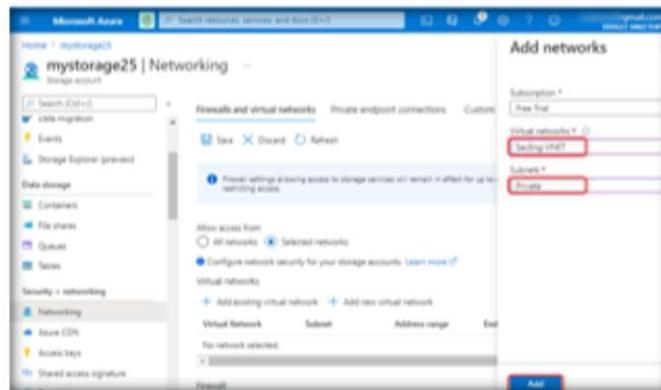


FIGURE 4.10.66: Adding Networks Details

67. The virtual network has been successfully added. Now, click on **Save** to save the settings.

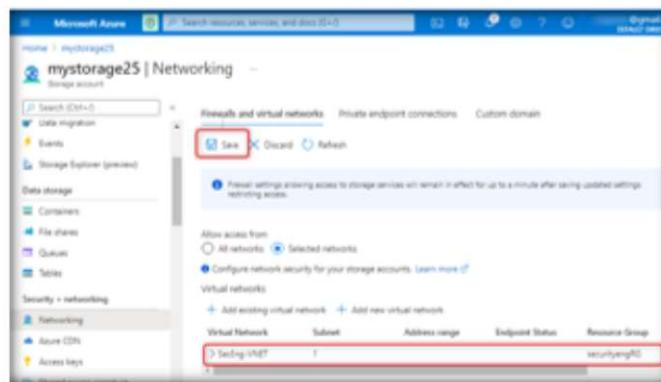


FIGURE 4.10.67: Saving the Virtual Networks

68. The firewall and virtual network settings for the selected storage have been successfully updated.

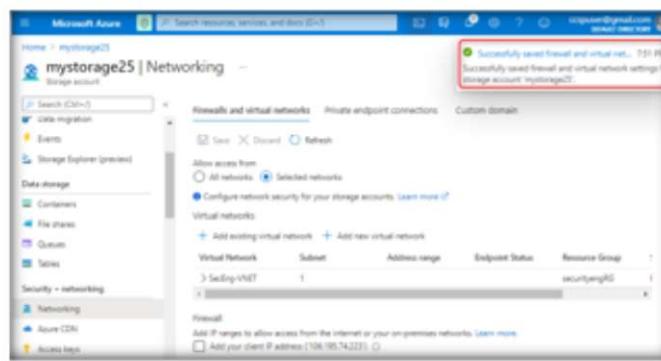


FIGURE 4.10.68: Successfully Saved Firewalls and Virtual Networks

69. In mystorage25, click on Access Keys under Security + networking.

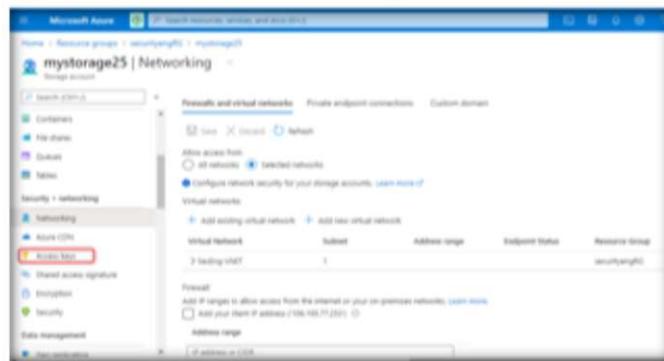


FIGURE 4.10.69: Selecting Access Keys in Storage Account

70. Note down the storage account name (here, **mystorage25**), and then click on the **Hide keys** button.

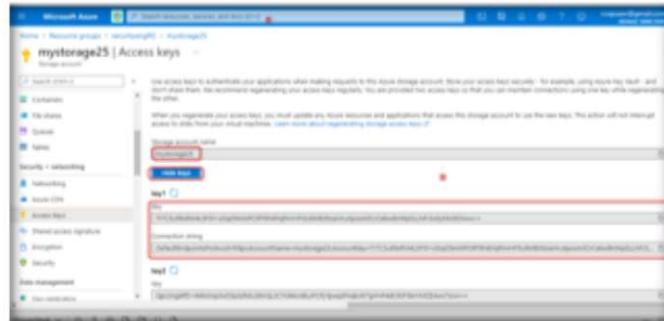


FIGURE 4.10.70: Storage Account Key1

71. Copy the **Key** and **Connection string** in notepad and **Save** it on your desktop.

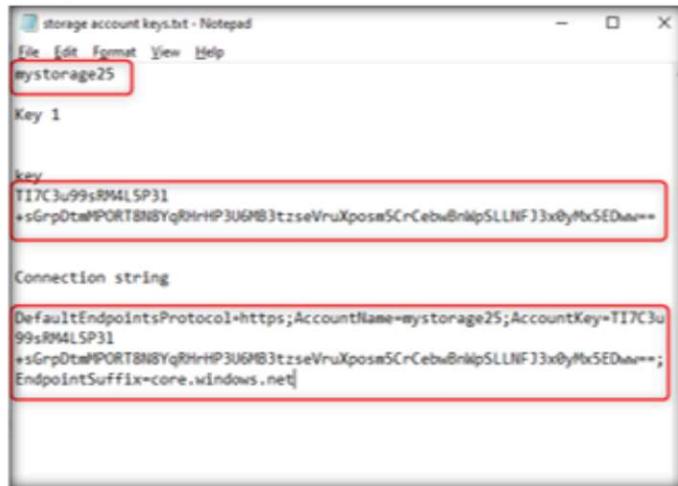


FIGURE 4.10.71: Saving the Storage Account Key1 in Notepad

72. You need to create two virtual machines. First, create a virtual machine that will be deployed in a public subnet.

**TASK 8**

**Create Virtual Machines**

The screenshot shows the Azure portal's Networking settings for a storage account. The 'Selected networks' option is chosen for allowing access. A table lists a single virtual network named 'Selling-VMNET' with a subnet of 1 and an address range of 192.168.1.0/24. A 'Firewall' section at the bottom allows adding IP ranges or client IP addresses.

FIGURE 4.10.72: Go Back to Azure Portal

73. Click on **Virtual machines**.

The screenshot shows the Azure services dashboard with various icons for different services like Storage accounts, Network security groups, and Virtual machines. The 'Virtual machines' icon is highlighted with a red box.

FIGURE 4.10.73: Selecting Virtual Machines

74. Click on **+Add** and then click on **+ Virtual machine**.

The screenshot shows the 'Virtual machines' blade in the Azure portal. The '+ Add' button and the '+ Virtual machine' link are both highlighted with red boxes.

FIGURE 4.10.74: Adding Virtual Machine

75. A **Create a virtual machine** window will open. Select **securityengRG** from the dropdown in **Resource group**. In **Virtual machine name**, type **myVMPublic**.

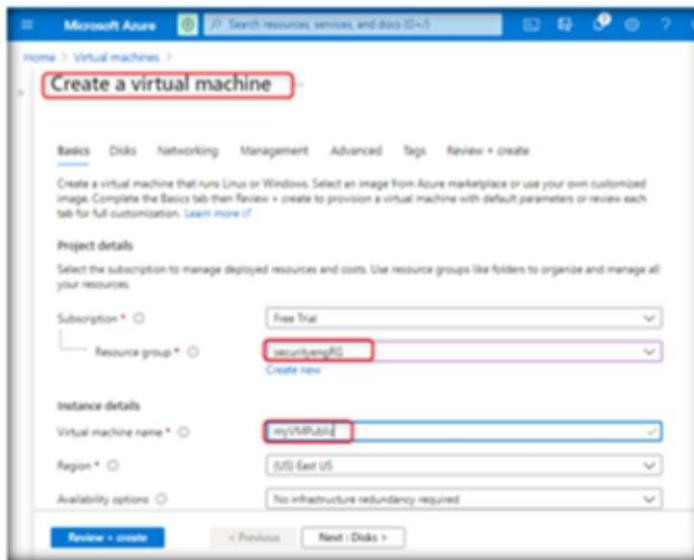


FIGURE 4.10.75: Entering Resource Group and Virtual Machine Name

76. In the **Image** field, select **Window Server 2016 Datacenter – Gen 1**. Under **Administrator account**, type **Username** as **CCSEtester1** and **Password** as **Administrator@321** and confirm the same password. Then, click on **Next: Disks >**.

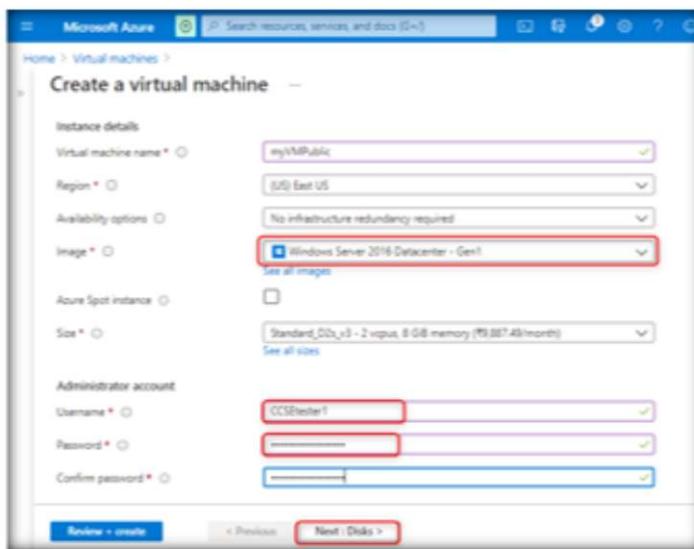


FIGURE 4.10.76: Selecting Image and Filling Login Credentials for VM

#### Module 04 – Data Security in Cloud

77. In the **Disks** tab, leave everything in their default state and click on **Next: Networking >**.

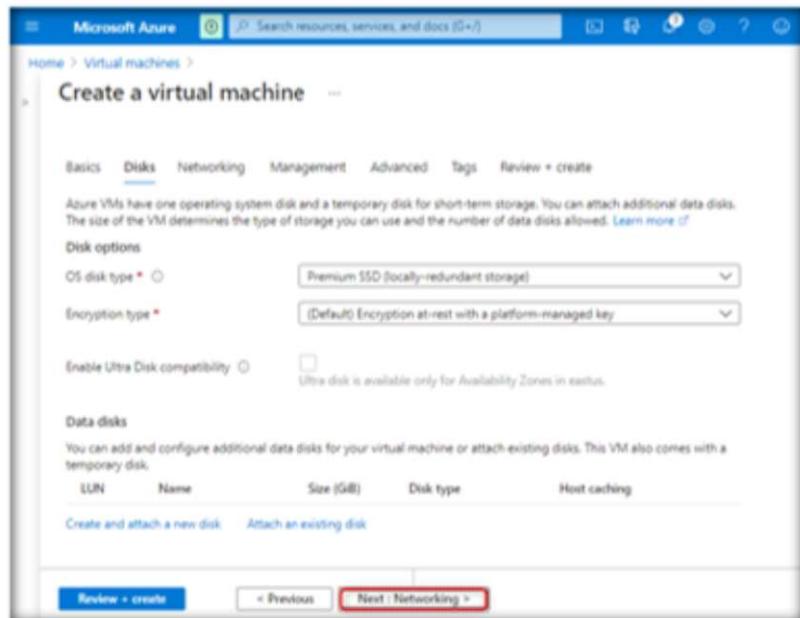


FIGURE 4.10.77: Leaving Disk Tab in Default State

78. In the **Networking** tab, select **Subnet** as **Public**, **NIC network security group** as **Basic**, and **Select inbound ports** as **RDP (3389)**. Then, click on **Next: Management >**.

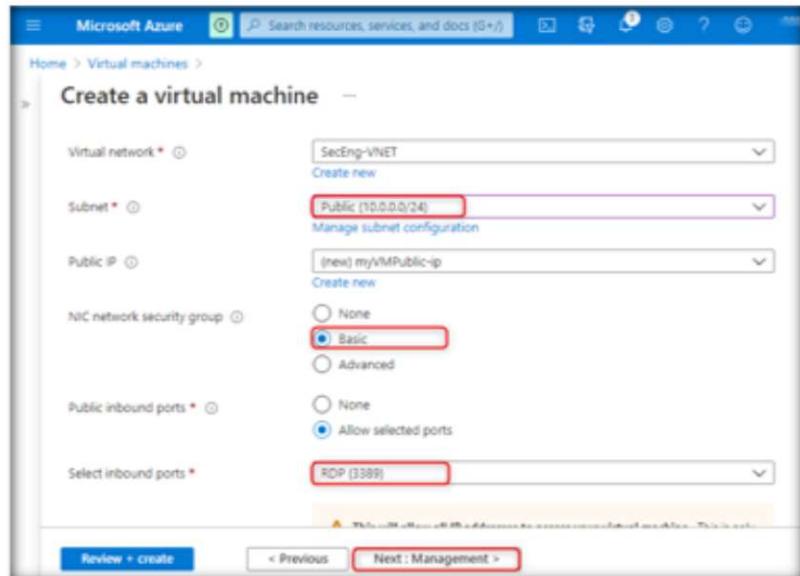


FIGURE 4.10.78: Selecting Subnet, NIC network Security Group, and Inbound Ports

79. In the **Management** tab, select the **Disable** radio button under **Boot diagnostics**. Then, click on **Next: Advanced >**.

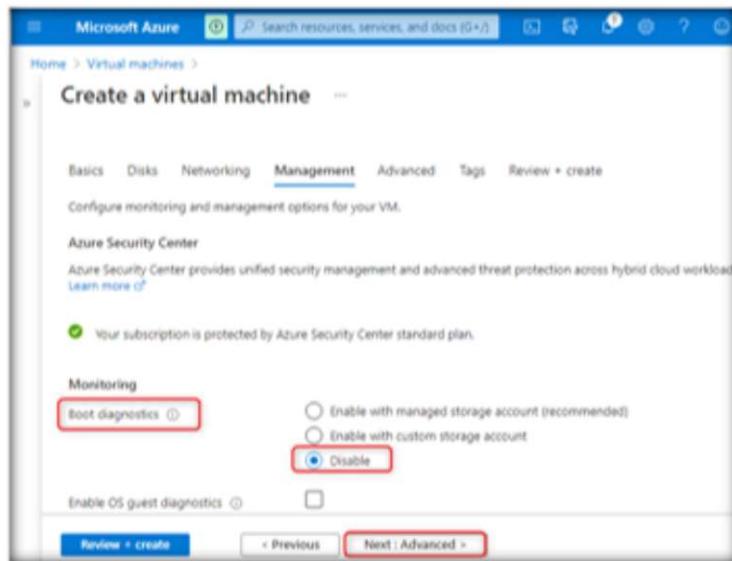


FIGURE 4.10.79: Selecting Disable Radio Button for Boot Diagnostics

80. In the **Advanced** tab, leave everything in their default state and click on the **Next: Tags** button.

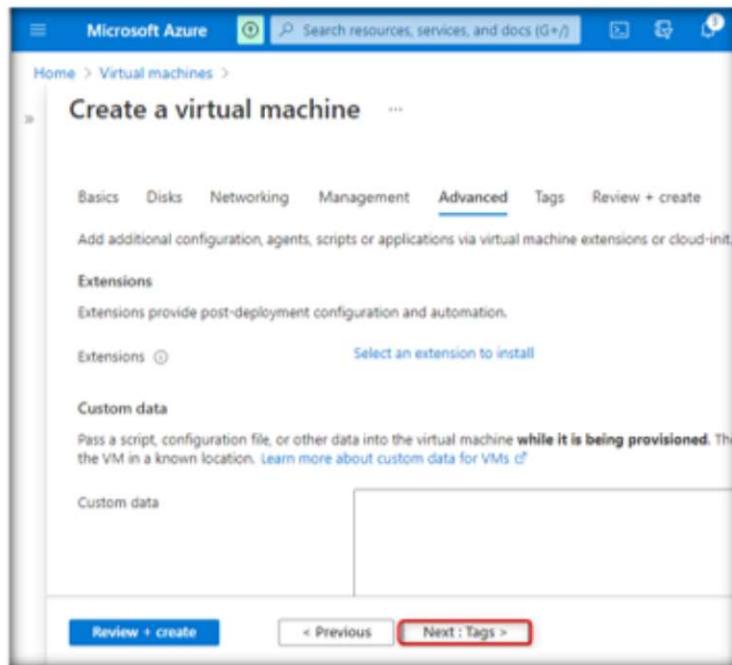


FIGURE 4.10.80: Leaving Advanced Tab in Default State

#### Module 04 – Data Security in Cloud

81. In the **Tags** tab, leave everything in their default state and click on **Next: Review + create >**.

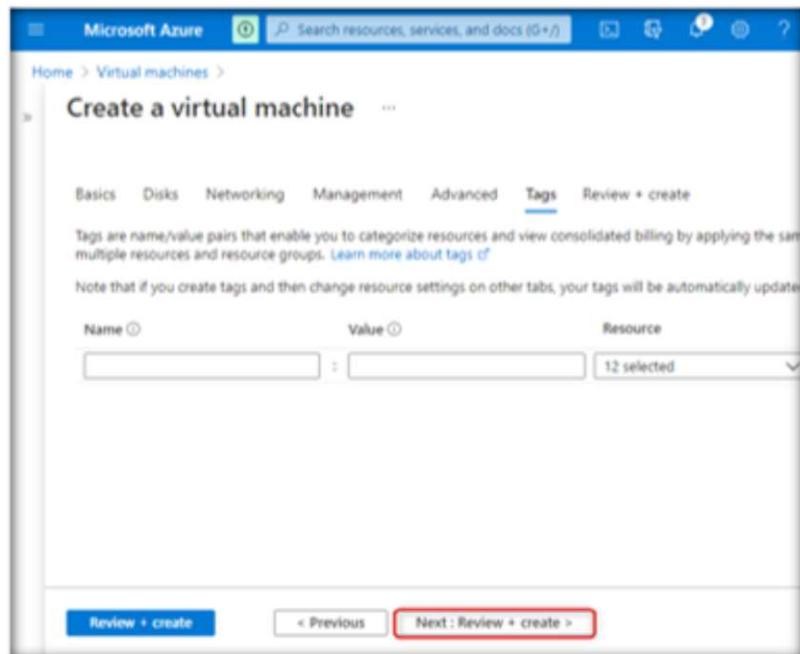


FIGURE 4.10.81: Leaving Tags Tab in Default State

82. After seeing the **Validation passed** message, click on **Create**.

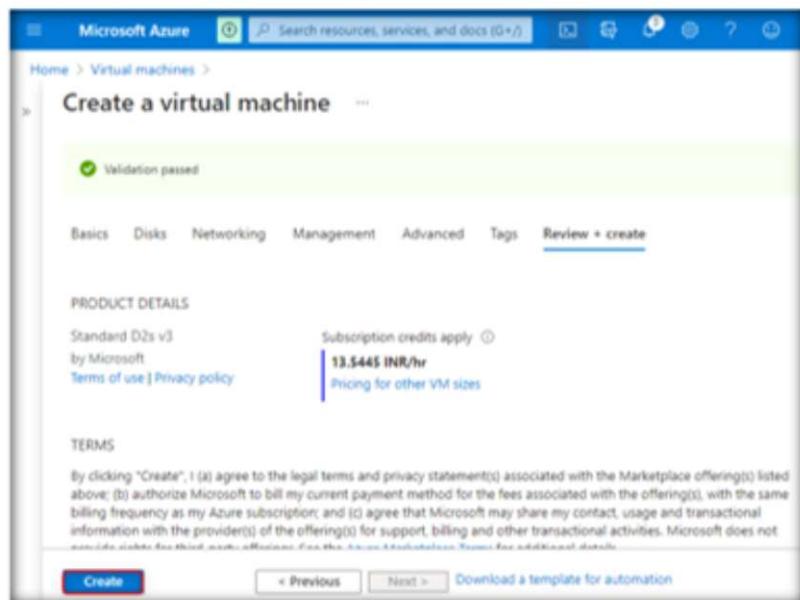


FIGURE 4.10.82: Creating a VM after Validation Passed

**Module 04 – Data Security in Cloud**

83. After the successful deployment of the virtual machine, click on the **Go to resource** button.

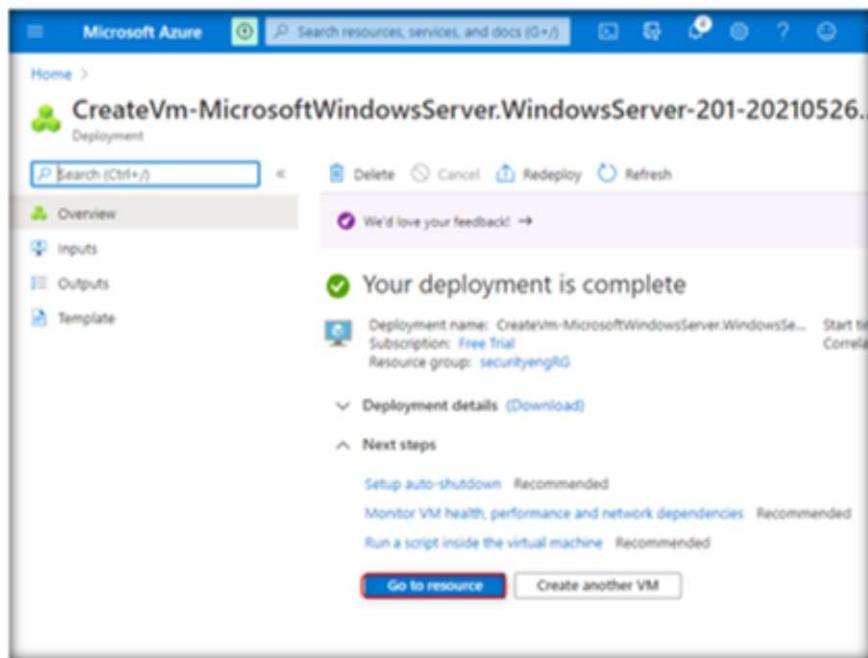


FIGURE 4.10.83: Successful Deployment of VM

84. myVMPublic virtual machine has been successfully created.

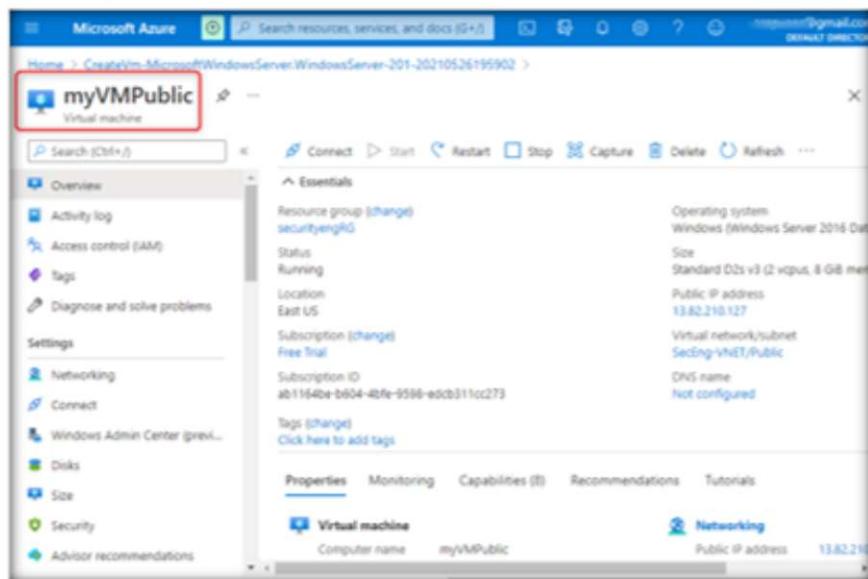


FIGURE 4.10.84: Successful Creation of myVMPublic Virtual Machine

#### Module 04 – Data Security in Cloud

85. Now, you will create a second virtual machine. Click on **Home** to go back to the Azure portal.

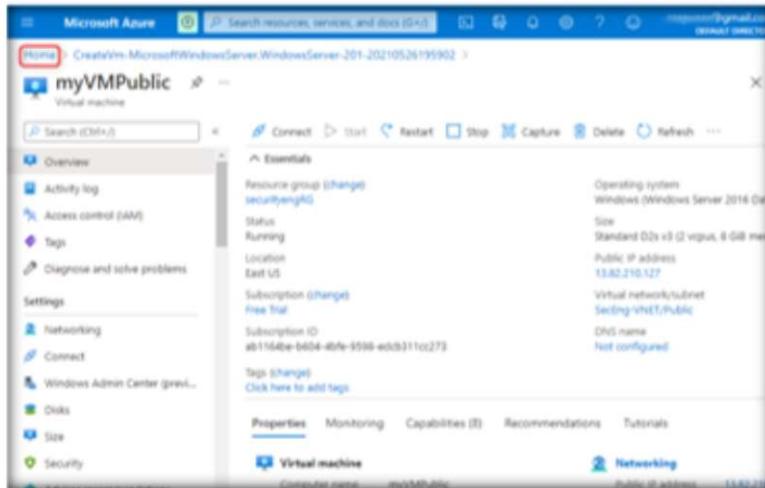


FIGURE 4.10.85: Selecting Home to Go Back to Azure Portal

86. Click on **Virtual machines**.

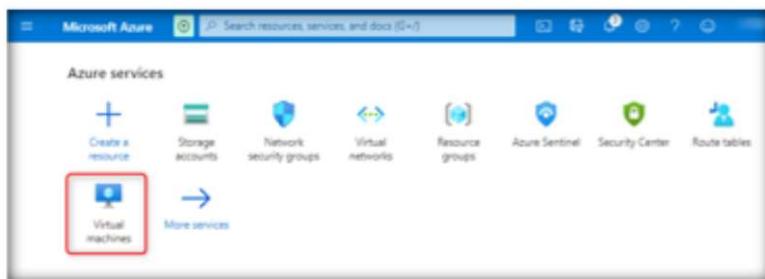


FIGURE 4.10.86: Selecting Virtual Machines

87. Click on **+Add** and then on **+ Virtual machine**.

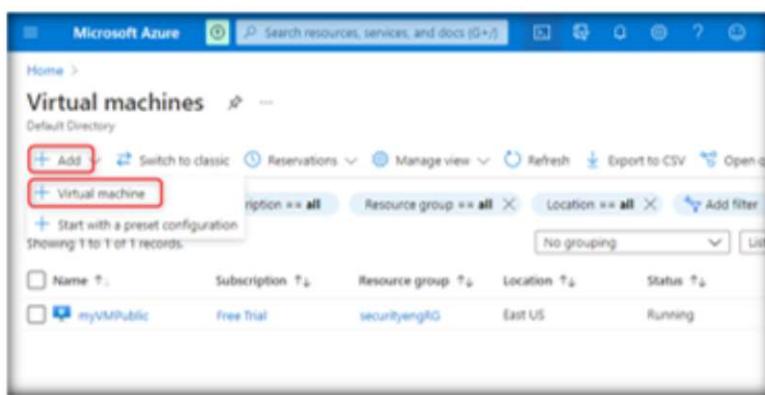


FIGURE 4.10.87: Adding Virtual Machine

**Module 04 – Data Security in Cloud**

88. A **Create a virtual machine** window will open. In the **Resource group** field, select **securityengRG** from the dropdown. In the **Virtual machine name** field, type **myVMPrivate**.

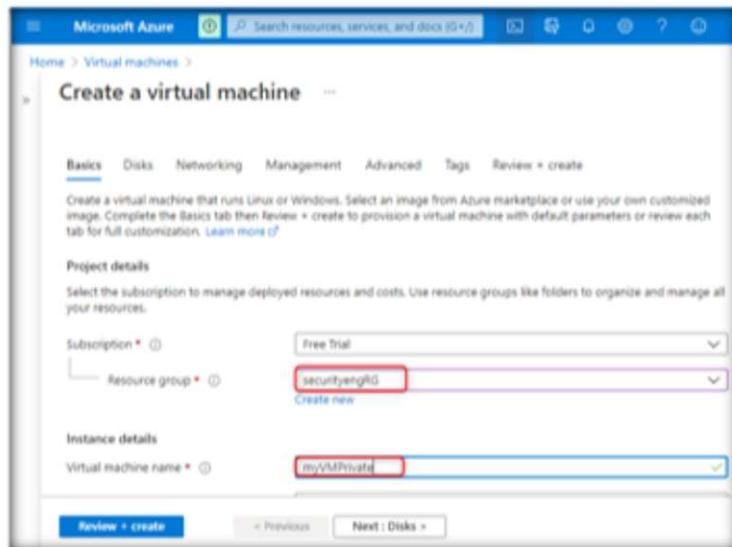


FIGURE 4.10.88: Entering Resource Group and Virtual Machine Name

89. For the **Image** field, select **Window Server 2016 Datacenter – Gen 1**. Under **Administrator account**, type **Username** as **CCSEtester2** and **Password** as **Administrator@456**, and then confirm the same password. Then, click on **Next: Disks >**.

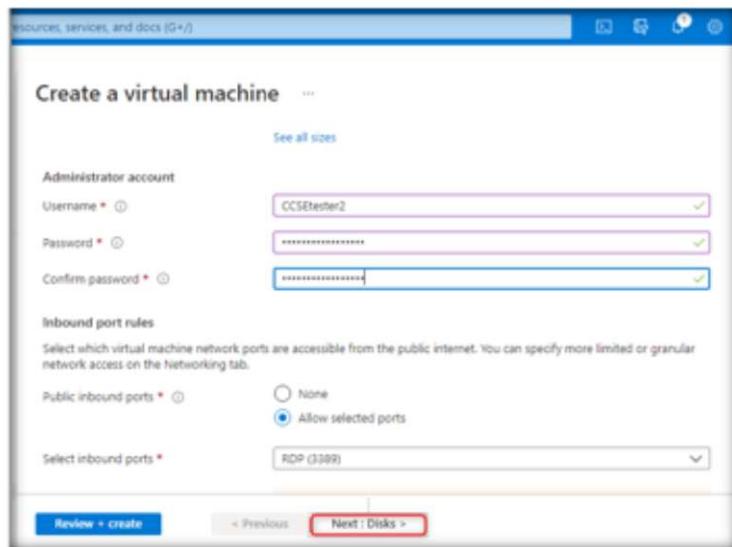


FIGURE 4.10.89: Entering Login Credentials for VM

90. In the **Disks** tab, leave everything in their default state and click on **Next: Networking >**.

## Module 04 – Data Security in Cloud

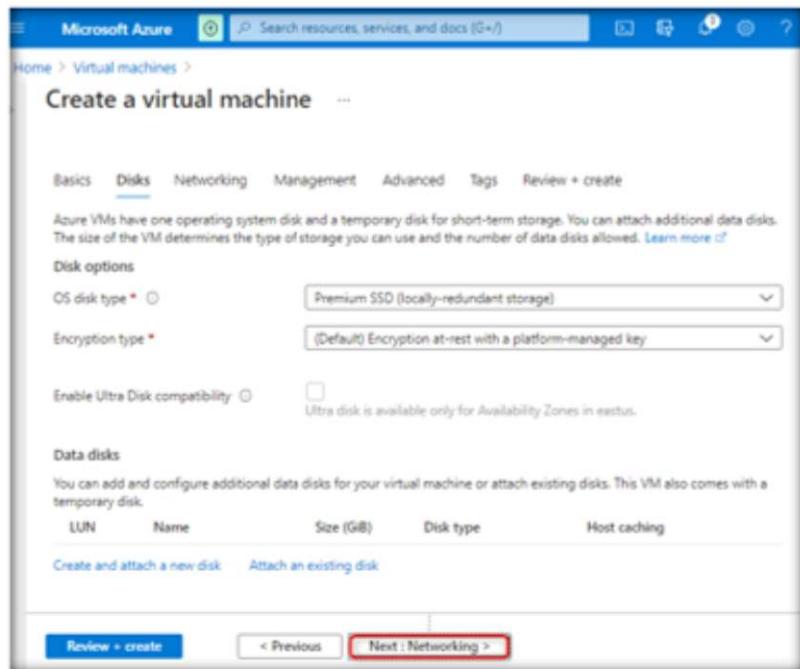


FIGURE 4.10.90: Leaving Disk Tab in Default State

91. In the **Networking** tab, select **Subnet** as **Private**, and in **NIC network security group**, select the **Basic** radio button.

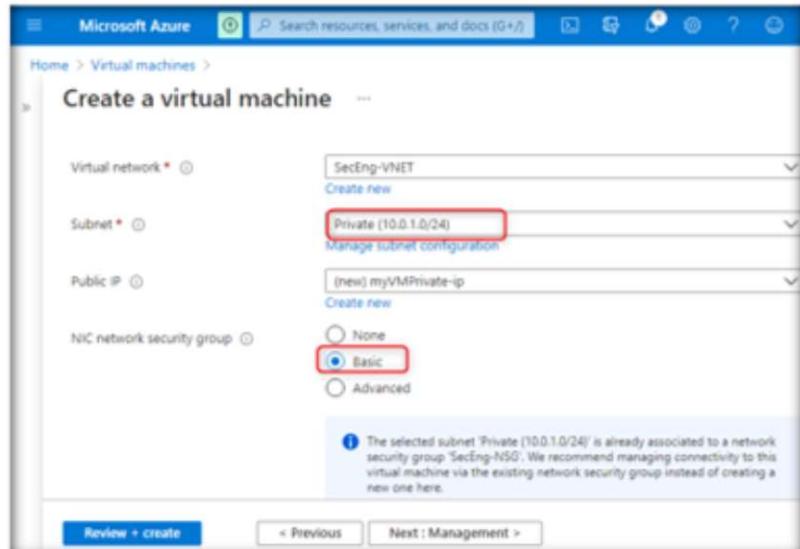


FIGURE 4.10.91: Selecting Subnet and NIC network Security Group

92. In **Public inbound ports**, select the **Allow selected ports** radio button. In the **Select inbound ports** field, select **RDP (3389)**. Then, click on **Next: Management >**.

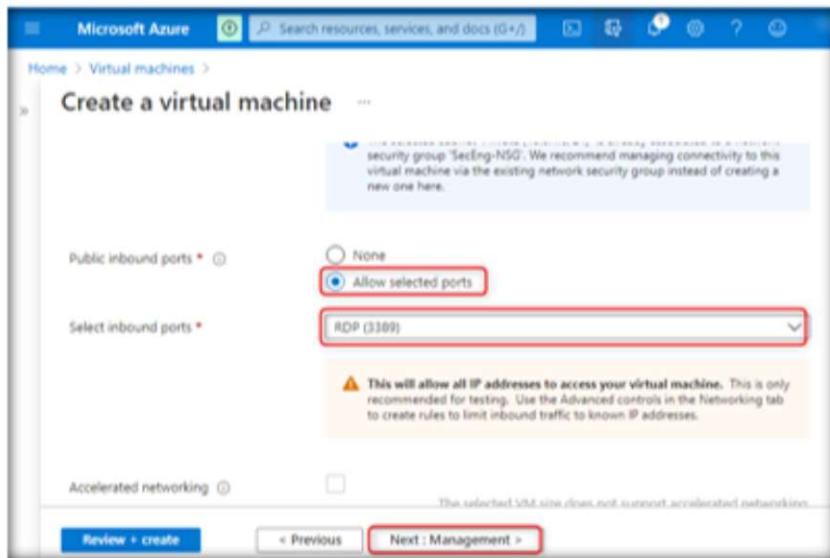


FIGURE 4.10.92: Selecting Inbound Ports

93. In the **Management** tab, select the **Disable** radio button under **Boot diagnostics**. Then, click on **Next: Advanced >**.

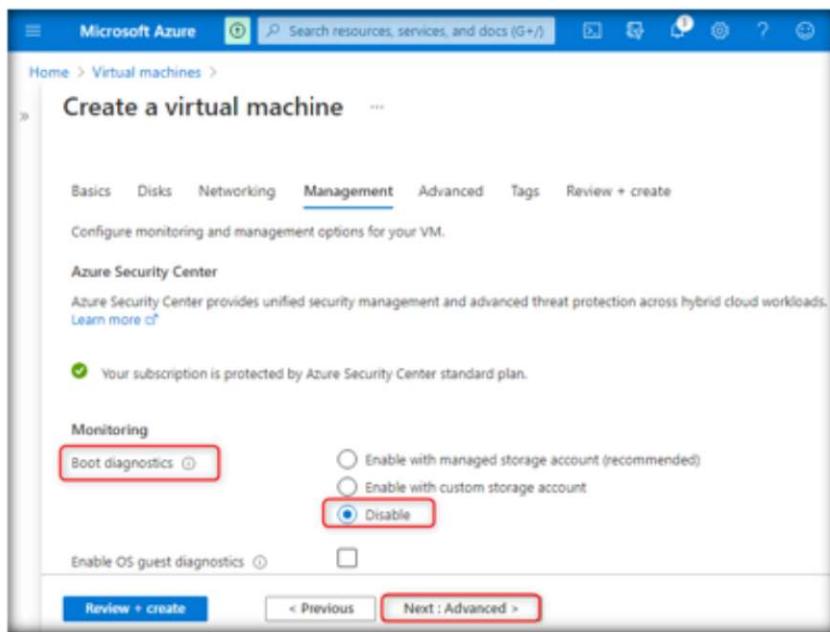


FIGURE 4.10.93: Selecting Disable Radio Button for Boot Diagnostics

#### Module 04 – Data Security in Cloud

94. In the **Advanced** tab, leave everything in their default state and click on the **Next: Tags** button.

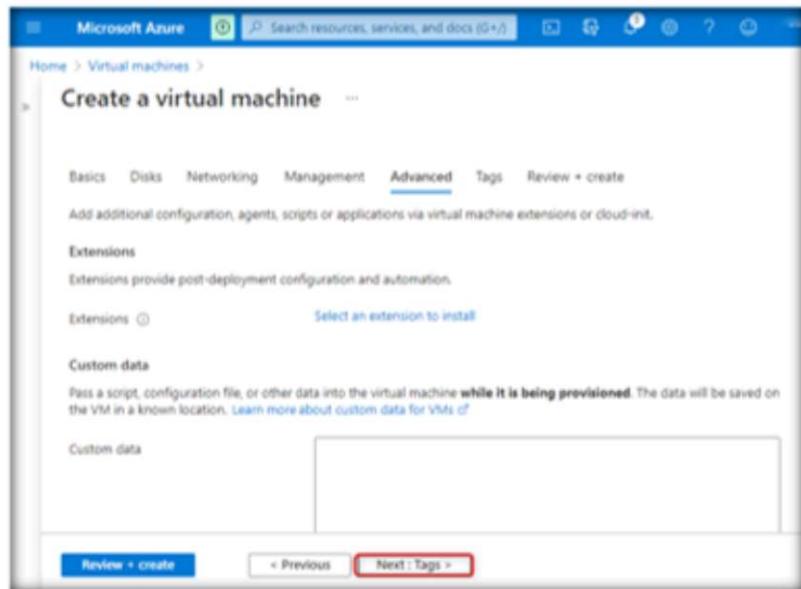


FIGURE 4.10.94: Leaving Advanced Tab in Default State

95. In the **Tags** tab, leave everything in their default state and click on the **Next: Review + create >** button.

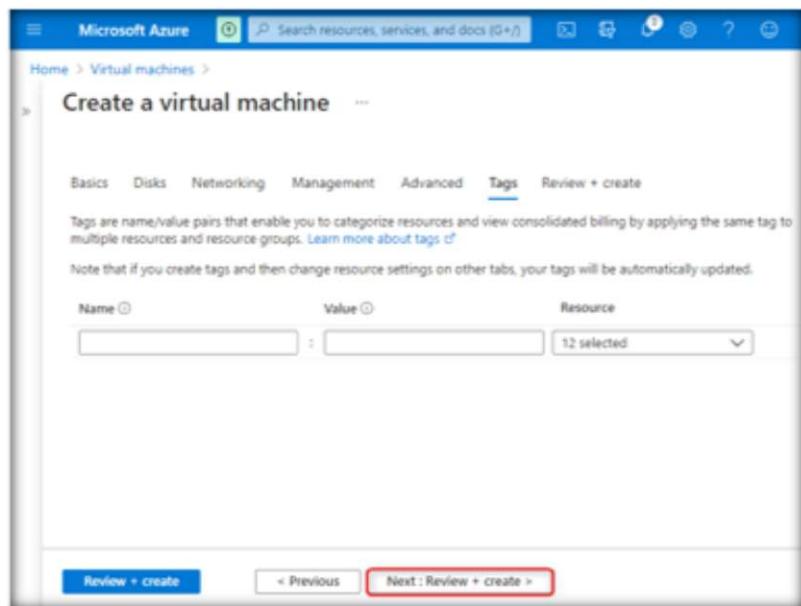


FIGURE 4.10.95: Leaving Tags Tab in Default State

96. After seeing the **Validation passed** message, click on the **Create** button.

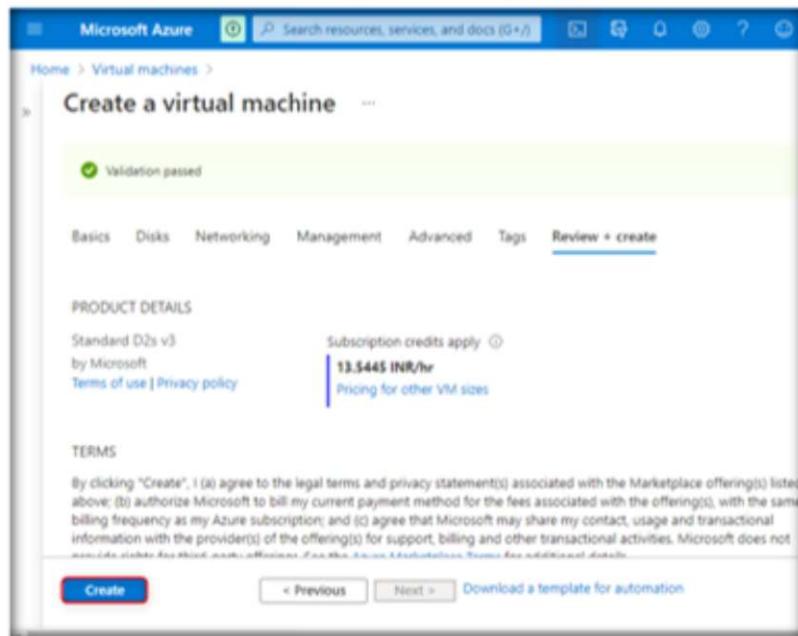


FIGURE 4.10.96: Creating a VM after Validation Passed

97. After the successful deployment of the virtual machine, click on the **Go to resource** button.

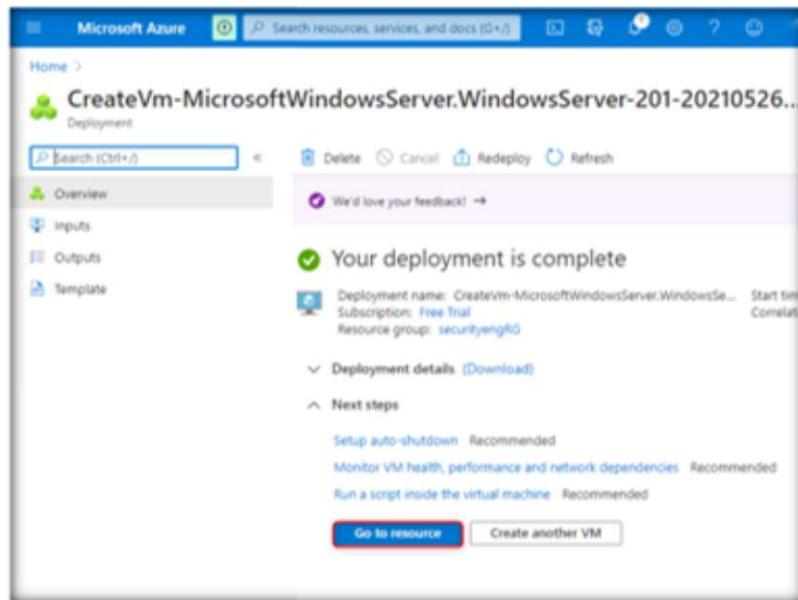


FIGURE 4.10.97: Successful Deployment of VM

98. **myVMPrivate** virtual machine has been successfully created.

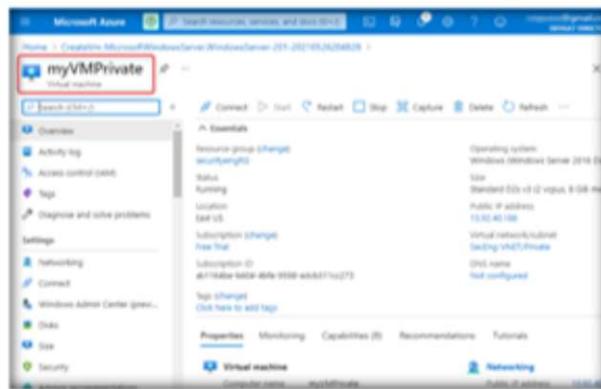


FIGURE 4.10.98: Successful Creation of myVMPublic Virtual Machine

### **TASK 9** Confirming access to storage account

99. Next, you will confirm access to the storage account. In **myVMPrivate** virtual machine, navigate and click on **Connect**, and then on **RDP**. Under **Connect with RDP**, click on **Download RDP File**.

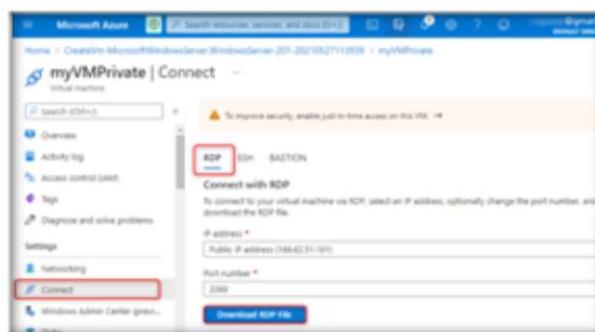


FIGURE 4.10.99: Connecting VM with RDP

100. We will be connecting to **myVMPrivate** virtual machine using remote desktop connection (RDP). Click on the RDP file after it is successfully downloaded.

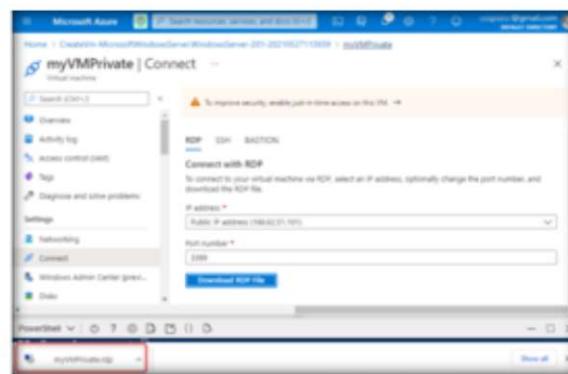


FIGURE 4.10.100: myVMPrivate RDP File is Downloaded

101. In the **Remote Desktop Connection** window, click on the **Connect** button.

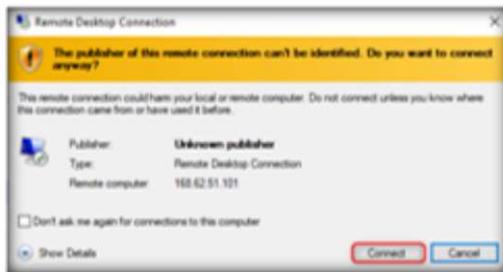


FIGURE 4.10.101: Connecting to myVMPrivate Virtual Machine

102. A **Windows Security Enter your credentials** window will open. Enter **myVMPrivate** virtual machine **Username** (here, **CCSEtester2**) and **Password** (**Administrator@456**). Then, click on the **OK** button.

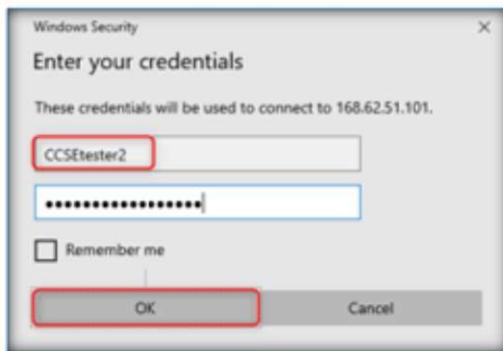


FIGURE 4.10.102: Entering VM Login Credentials

103. The **Remote Desktop Connection** certificate will appear, indicating **Certificate errors**. Click on the **Yes** button.

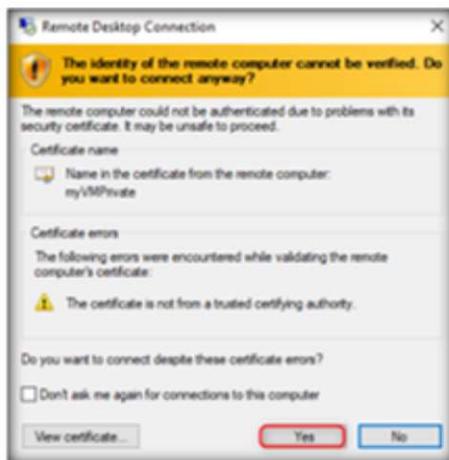


FIGURE 4.10.103: Certification Error

104. myVMPrivate virtual machine will be successfully connected now. In the Networks window, click on the Yes button.

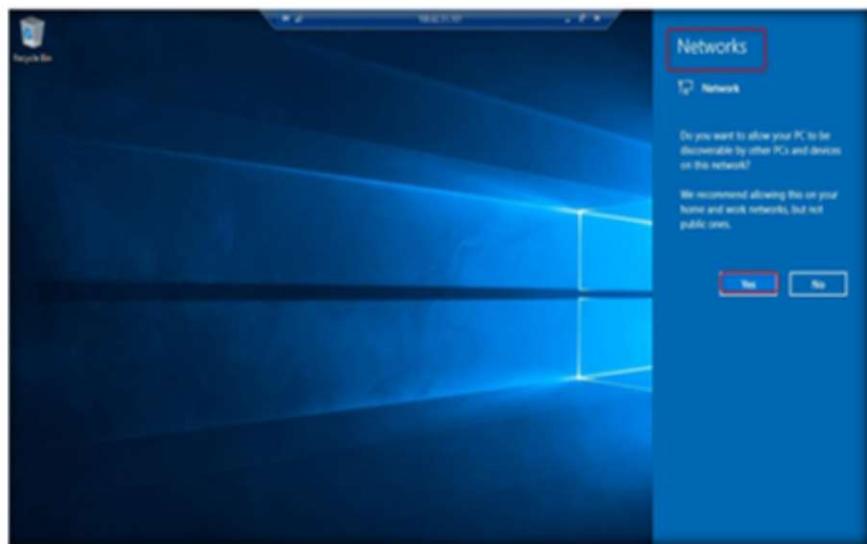


FIGURE 4.10.104: Selecting Yes in Networks Window

105. In the myVMPrivate VM search box, type power shell. Windows PowerShell will appear as the best match. Click on it.

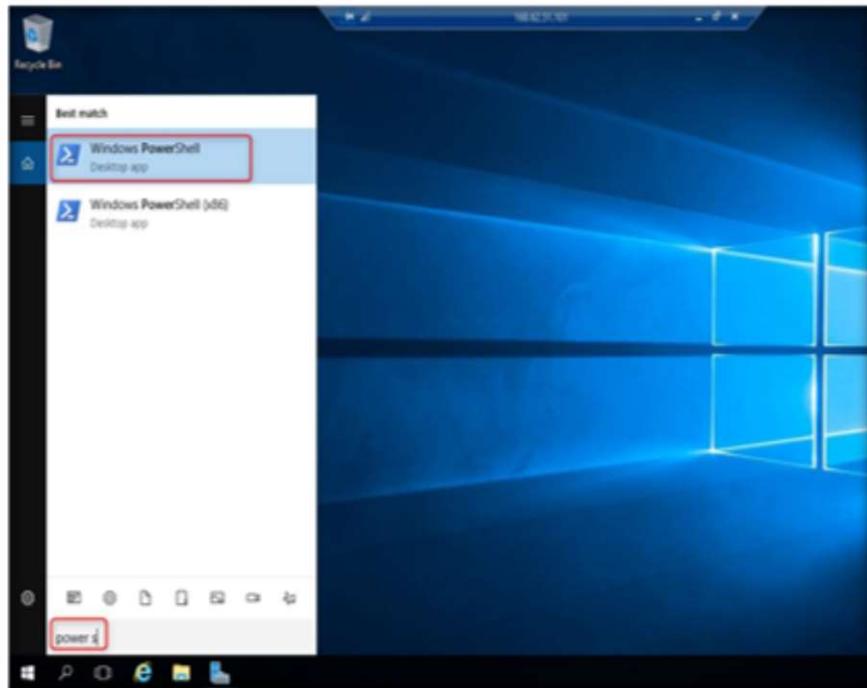


FIGURE 4.10.105: Selecting Windows PowerShell

106. In myVMPrivate VM, use **PowerShell** to map the Azure file share utilizing drive Z using the following commands sequentially:

```
$acctKey = ConvertTo-SecureString -String "<storage-account-key>" -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential -ArgumentList "Azure\<storage-account-name>", $acctKey
New-PSDrive -Name Z -PSProvider FileSystem -Root "\\.file.core.windows.net\my-file-share" -Credential $credential
```

**Note:** Before running the above command, replace the <storage-account-key> and <storage-account-name> with those you saved in the notepad at the time of creating a storage account.

**Note:** You will have a different key. Ensure you input the correct key in the command line.

**Note:** Type the command, minimize the remote desktop connection, copy the key from the notepad, go to the command line and delete **storage-account-key** along with > and < symbols, paste the key between inverted commas.

```
$acctKey = ConvertTo-SecureString -String "TI7C3u99sRM4L5P3l+sGrpDtmMPORT8N8YqRHrHP3U6MB3tzseVruXposm5CrCebwBnWpSLLNFJ3x0yMx5EDww==" -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential -ArgumentList "Azure\mystorage25", $acctKey
New-PSDrive -Name Z -PSProvider FileSystem -Root "\\\mystorage25.file.core.windows.net\my-file-share" -Credential $credential
```

Azure file share has been successfully mapped to Z drive.

Name	Used (GB)	Free (GB)	Provider	Root	CurrentLocation
Z			Filesystem	\\\mystorage25.file.core.windows....	

FIGURE 4.10.10c: Command to Map the Azure file share utilizing drive Z

107. Use the following command to confirm that **myVMPrivate** VM does not have an outbound connectivity with the Internet.

```
ping bing.com
```



```
Administrator: Windows PowerShell
PS C:\Users\CCSEtester2> ping bing.com
Pinging bing.com [204.79.197.200] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 204.79.197.200:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\CCSEtester2>
```

FIGURE 4.10.107: Command to Check the VM Outbound Connectivity with Internet

You will not receive any reply as the NSG associated with **Private** subnet will not allow an outbound access to the Internet.

108. Now, close **Windows PowerShell**. Right click on **Windows** icon, click on **Shut down or sign out**, and then click on **Disconnect** to close **myVMPrivate** VM.

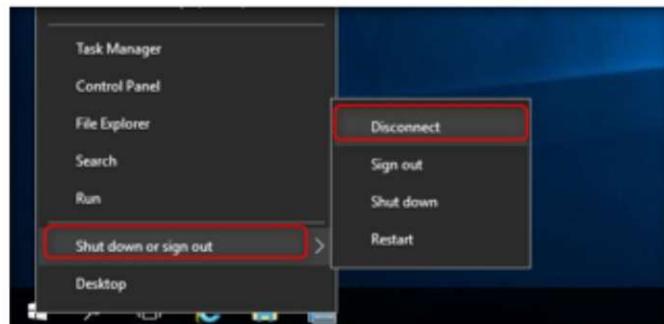


FIGURE 4.10.108: Disconnecting VM

109. If you are in the **myVMPrivate** window, click on **Home** to go back to the Azure portal.

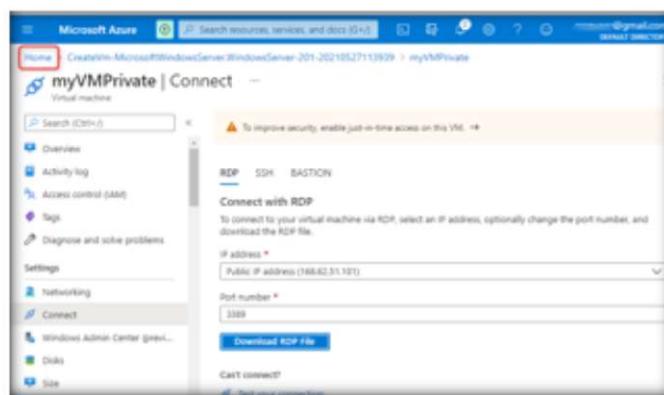


FIGURE 4.10.109: Selecting Home to Go Back to Azure Portal

#### **TASK 10**

110. From Azure portal, click on **Resource groups**.

**Confirming Access is Denied to Storage Account**

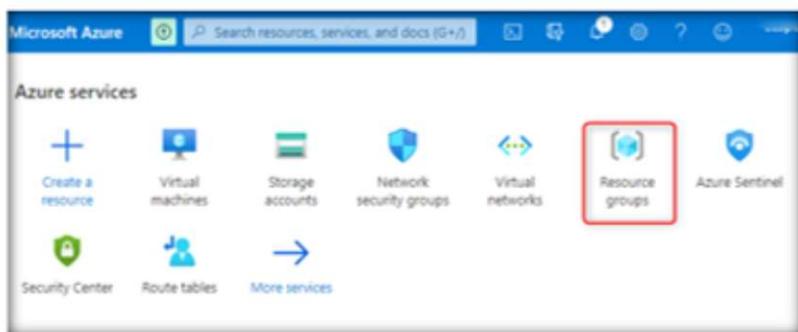


FIGURE 4.10.110: Selecting Resource Groups

111. In Resource groups, click on securityengRG.

Name	Subscription	Location
cloud-shell-storage-centralindia	Free Trial	Central India
DefaultResourceGroup-EUS	Free Trial	East US
NetworkWatcherRG	Free Trial	East US
<b>securityengRG</b>	Free Trial	East US

FIGURE 4.10.111: Selecting securityengRG Resource Group

112. In securityengRG, click on myVMPublic virtual machine.

Name	Type	Location
myVMPublic	Virtual machine	East US
myVMPublic_ip	Public IP address	East US

FIGURE 4.10.112: Selecting myVMPublic Virtual Machine

**Module 04 – Data Security in Cloud**

113. myVMPublic virtual machine will open now. Click on **Connect** and then on **RDP**.

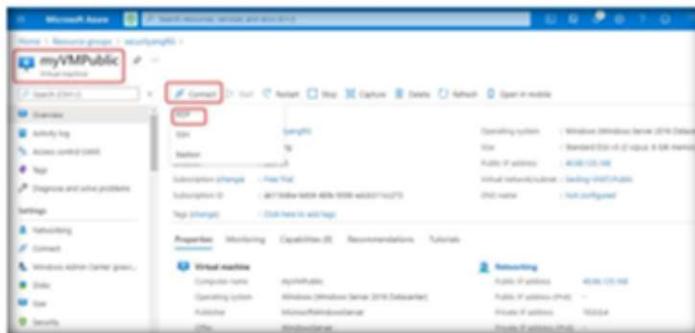


FIGURE 4.10.113: Connecting myVMPublic with RDP

114. Under **Connect with RDP**, click on **Download RDP File**.

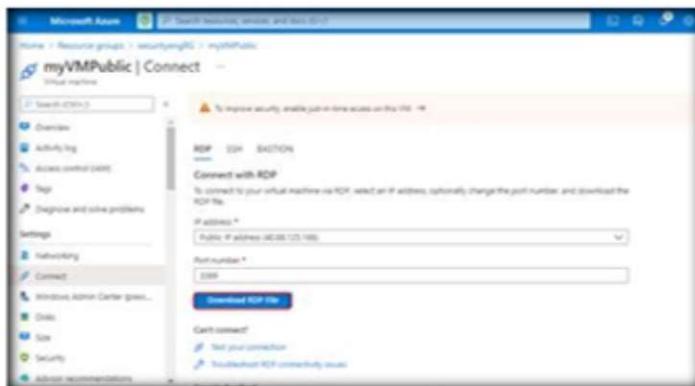


FIGURE 4.10.114: Downloading RDP File

115. Click on the **myVMPublic** RDP file after it is successfully downloaded.

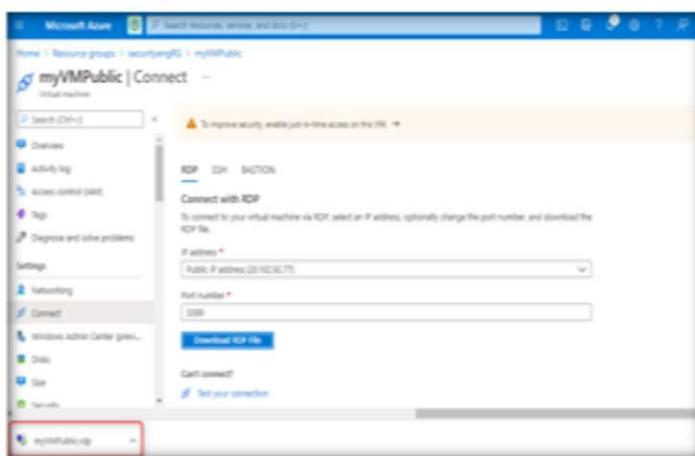


FIGURE 4.10.115: Opening myVMPublic RDP File

116. In the **Remote Desktop Connection** window, click on the **Connect** button.

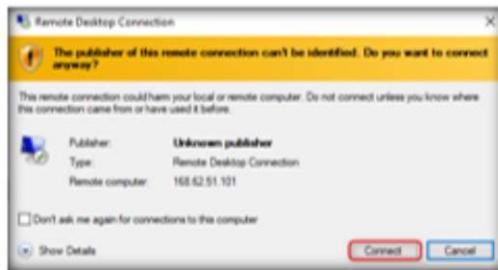


FIGURE 4.10.116: Connecting myVMPublic Virtual Machine

117. A **Windows Security Enter your credentials** window will open. Enter myVMPublic virtual machine **Username** (here, **CCSEtester1**) and **Password** (**Administrator@321**). Then, click **OK**.

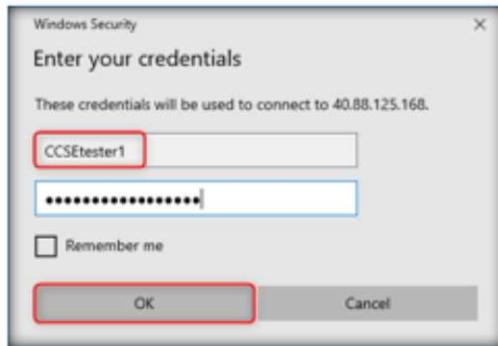


FIGURE 4.10.117: Entering Login Credentials of myVMPublic

118. A **Remote Desktop Connection** certificate will appear, indicating **Certificate errors**. Click on the **Yes** button.

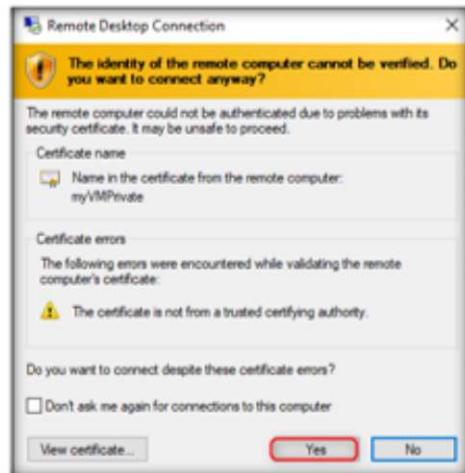


FIGURE 4.10.118: Certificate Errors

119. myVMPublic virtual machine will be successfully connected now. In the Networks window, click on the Yes button.

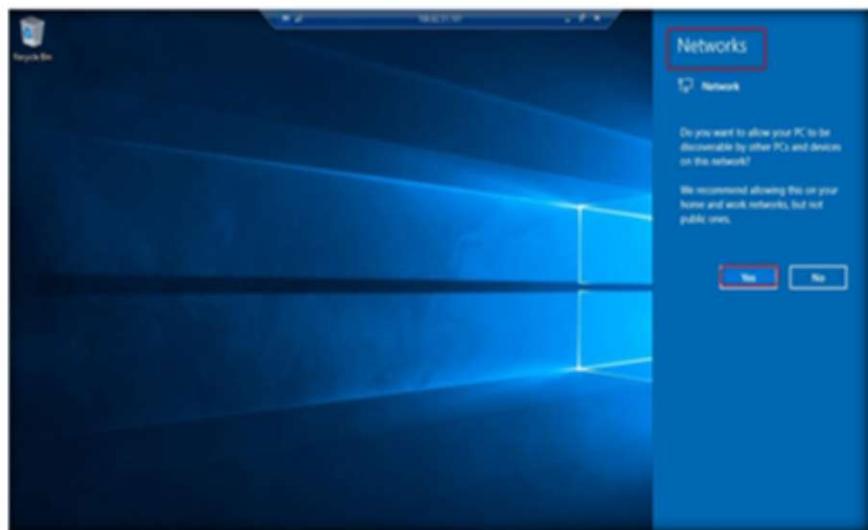


FIGURE 4.10.119: Selecting Yes in Networks Window

120. In the myVMPrivate VM search box, type **power shell**. Windows PowerShell will appear as the best match. Now, click on **Windows PowerShell**.

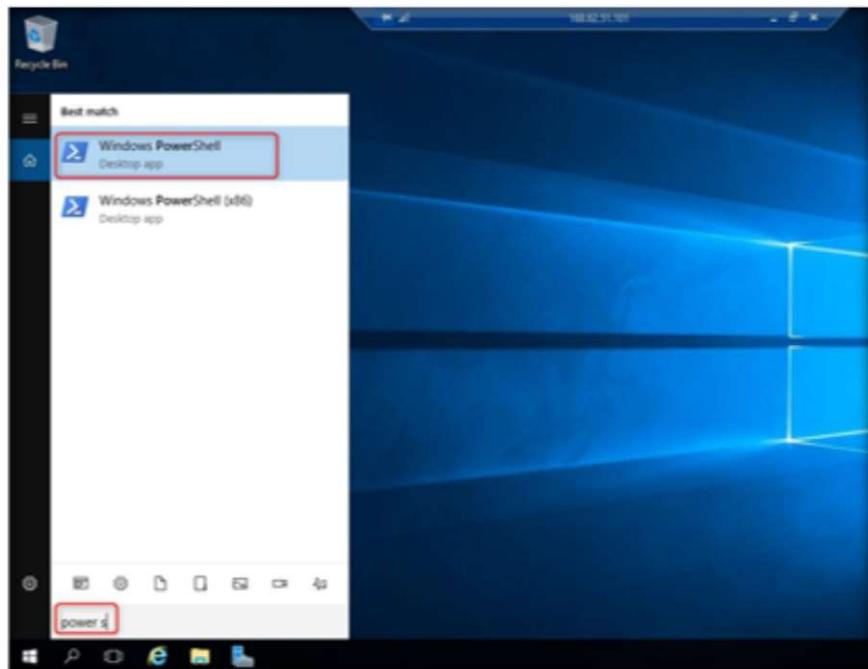


FIGURE 4.10.120: Opening Windows PowerShell

121. In myVMPublic VM, use PowerShell to map the Azure file share utilizing drive Z using the following commands:

```
$acctKey = ConvertTo-SecureString -String "<storage-account-key>" -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential -ArgumentList "Azure\<storage-account-name>", $acctKey
New-PSDrive -Name Z -PSProvider FileSystem -Root "\\<storage-account-name>.file.core.windows.net\my-file-share" -Credential $credential
```

**Note:** Before running the above command, replace the <storage-account-key> and <storage-account-name> with those you saved in the notepad at the time of creating a storage account.

**Note:** You would have a different key. Ensure you input the correct key in the command line.

```
$acctKey = ConvertTo-SecureString -String "TI7C3u99sRM4L5P3l+sGrpDtmMPORT8N8YqRHrHP3U6MB3tzseVruXposm5CrCebwBnWpSLLNFJ3x0yMx5EDww==" -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential -ArgumentList "Azure\mystorage25", $acctKey
New-PSDrive -Name Z -PSProvider FileSystem -Root "\\mystorage25.file.core.windows.net\my-file-share" -Credential $credential
```

You will receive a New-PSDrive: Access is denied error.

The access is denied because we have deployed **myVMPublic** virtual machine in the public subnet,. The public subnet does not have any service endpoints enabled for Azure storage. The Azure storage account allows network access only from the private subnet.

```
Administrator: Windows PowerShell (v6)
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\CCSEtester1> $acctKey = ConvertTo-SecureString -String "TI7C3u99sRM4L5P3l+sGrpDtmMPORT8N8YqRHrHP3U6MB3tzseVruXposm5CrCebwBnWpSLLNFJ3x0yMx5EDww==" -AsPlainText -Force
PS C:\Users\CCSEtester1> $credential = New-Object System.Management.Automation.PSCredential -ArgumentList "Azure\mystorage25", $acctKey
PS C:\Users\CCSEtester1> New-PSDrive -Name Z -PSProvider FileSystem -Root "\\mystorage25.file.core.windows.net\my-file-share" -Credential $credential
New-PSDrive : Access is denied
At line:1 char:1
+ New-PSDrive -Name Z -PSProvider FileSystem -Root "\\mystorage25.file.core.windows.net\my-file-share" -Cred ...
+ CategoryInfo          : ObjectNotFound: (Z:IPSSDriveInfo) [New-PSDrive], Win32Exception
+ FullyQualifiedErrorId : CreateFileSystemDriveForMicrosoftPowerShellCommands, NewPSDriveCommand
```

FIGURE 4.10.121: Access is Denied Error

122. Close Windows PowerShell. Right click on the Windows icon, click on Shut down or sign out, and then click on Disconnect to close myVMPublic VM.

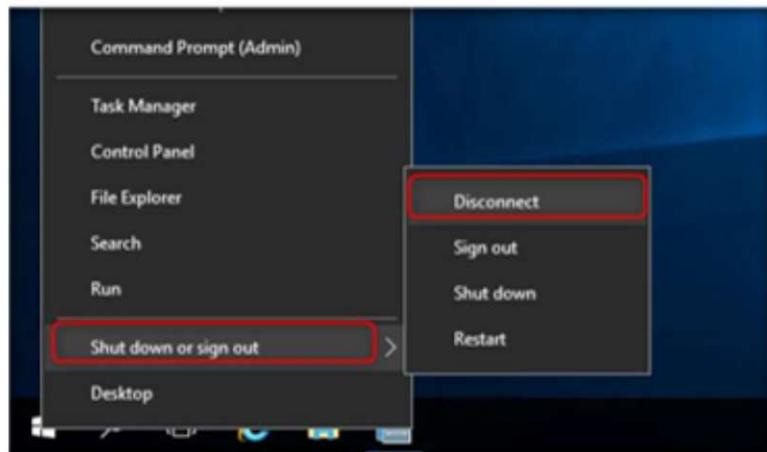


FIGURE 4.10.122: Disconnecting Virtual Machine

123. If you are in myVMPublic virtual machine, click on Home to go back to Azure portal.

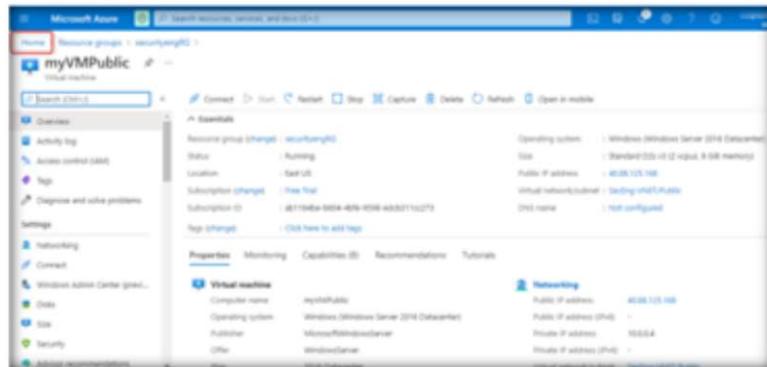


FIGURE 4.10.123: Selecting Home to Go Back to Azure Portal

124. From Azure portal, click on Resource groups.

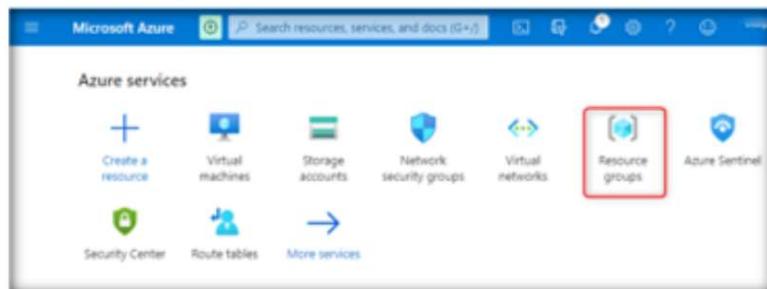


FIGURE 4.10.124: Selecting Resource Group

125. In Resource groups, click securityengRG.

Name	Subscription	Location
cloud-shell-storage-centralindia	Free Trial	Central India
DefaultResourceGroup-EU5	Free Trial	East US
NetworkWatcherRG	Free Trial	East US
<b>securityengRG</b>	Free Trial	East US

FIGURE 4.10.125: Selecting securityengRG Resource Group

126. In securityengRG, click on mystorage25 storage account.

Name	Type
mystorage25	Storage account
myVMprivate	Virtual machine
myVMprivate-ip	Public IP address
myVMprivate-nsg	Network security group

FIGURE 4.10.126: Selecting mystorage25 Storage Account

127. In mystorage25 storage account, navigate and click on File shares.

Properties	Monitoring	Capabilities	Recommendations	Tutorials	Developer Tools
Block service	Hierarchical namespace	Disabled			Secure transfer required

FIGURE 4.10.127: Selecting File Share

128. Then, click on my-file-share.

## Module 04 – Data Security in Cloud

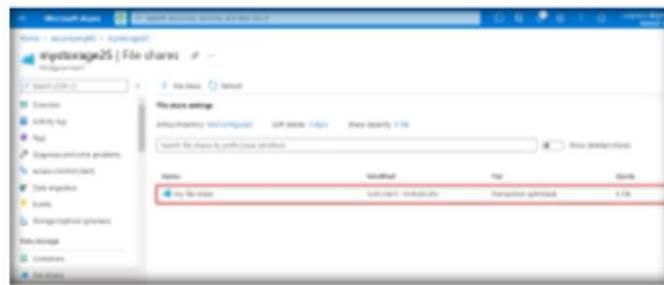


FIGURE 4.10.128: Selecting my-file-share

129. You will observe a message stating **This machine doesn't seem to have access**. The access is denied because your computer is not in the private subnet of the SecEng-VNET virtual network.

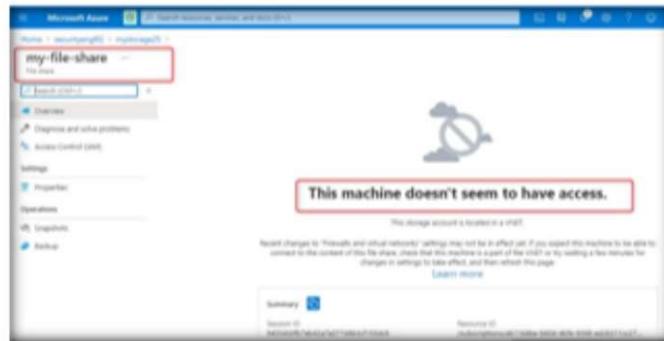


FIGURE 4.10.129: Access is Denied in my-file-share Window

**Caution:** Ensure you delete, shut down, or terminate all resources created and used in this lab to prevent their billing.

130. To delete securityengRG resource group, click on **securityengRG**. You will be redirected to **securityengRG** storage group. In **securityengRG**, click on **Delete resource group**.

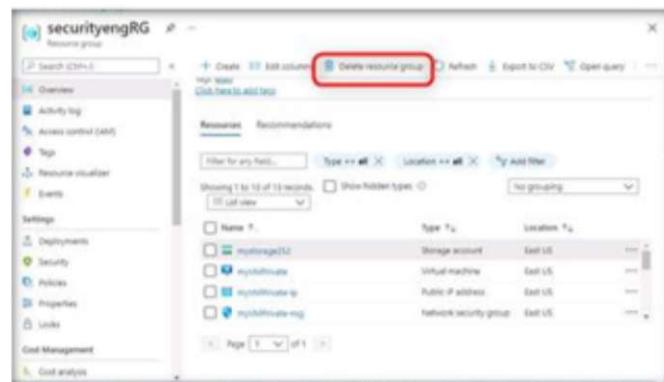


FIGURE 4.10.130: Deleting Resource Group

131. Type the resource group name as **securityengRG** and click on the **Delete** button. After a few minutes, the securityengRG resource group will be successfully deleted.

## Module 04 – Data Security in Cloud

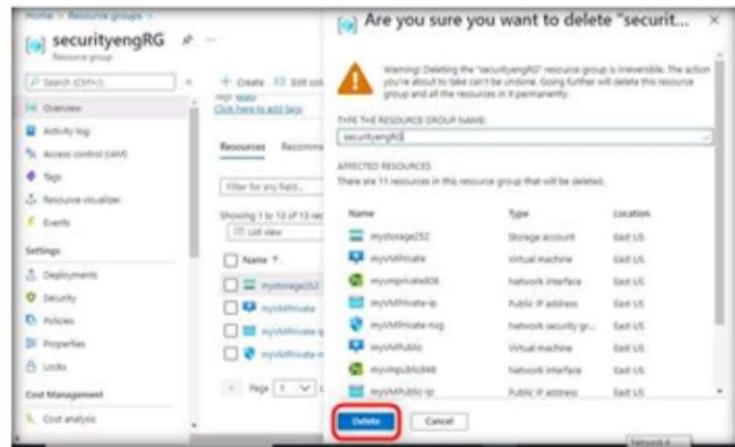


FIGURE 4.10.131: Deleting Resource Group

## Lab Analysis

Analyze and document the results of this lab exercise. Provide your opinion on your target's security posture and exposure through free public information.

PLEASE TALK TO YOUR INSTRUCTOR IF YOU HAVE QUESTIONS ABOUT THIS LAB.

---