


Lab
5

Securing RDP/SSH Access to Azure Virtual Machines Using Azure Bastion

Azure Bastion is a platform-managed PaaS service which provides a secure connection with a virtual machine through browsers and Azure portal.

ICON KEY Valuable information Test your knowledge Web exercise Workbook review

Lab Scenario

A cloud security engineer can use Azure Bastion to secure RDP and SSH connectivity to all provisioned VMs in a virtual network. Azure Bastion is provisioned directly in a virtual network (VNet) and can access its VMs using SSL without a single hardened access point.

Lab Objectives

In this lab, you will learn how to create a Bastion host and how to connect a virtual machine using Azure Bastion.

In this lab you will:

- Create a resource group
- Create a virtual machine (VM)
- Create a Bastion host for the VM
- Connect a VM using Bastion

Lab Environment

To perform this lab, you need the following:

- Admin Machine VM
- Registered Microsoft Azure account

Lab Duration

Time: 15 minutes

Overview of Azure Bastion

Azure Bastion is a platform-managed service that can be provided inside a virtual network. Use this service to prevent VMs from exposing SSH/RDP ports while maintaining a secure RDP/SSH access to VMs. Azure Bastion offers protection from zero-day exploits. It eliminates the need for a public IP to connect a VM and provides perimeter security to Azure VMs.

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 a Microsoft Azure account using the following link: <https://azure.microsoft.com/en-in/free/>. Once you have created your Microsoft Azure account, 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.

TASK 1

Creating a Resource Group

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

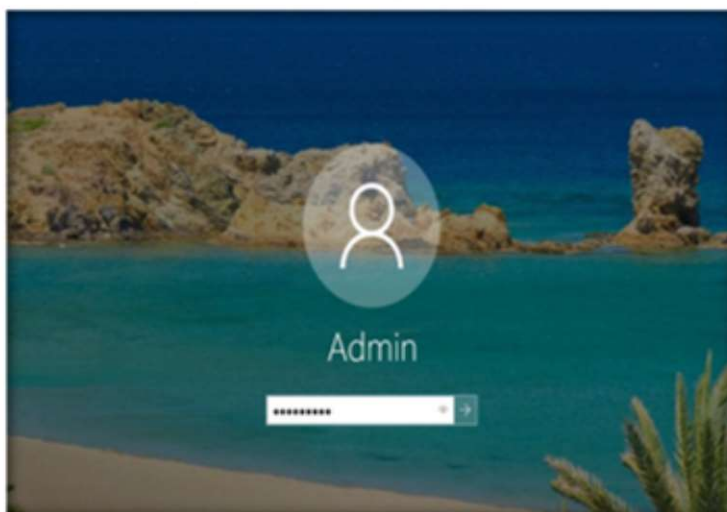


FIGURE 5.5.1: Launch Admin Machine and Log in

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



FIGURE 5.5.2: Navigating to the Chrome Browser from Taskbar

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

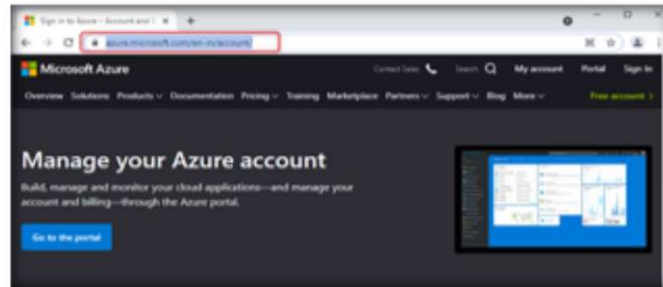


FIGURE 5.5.3: Entering the URL of Microsoft Azure

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

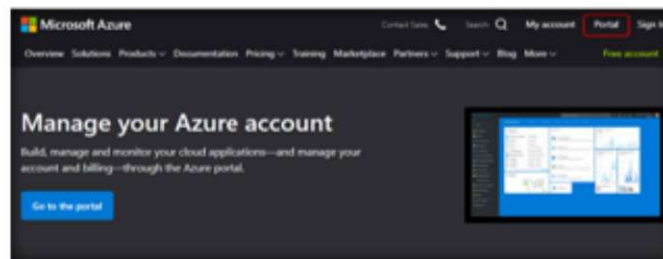


FIGURE 5.5.4: Sign into Azure Portal

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

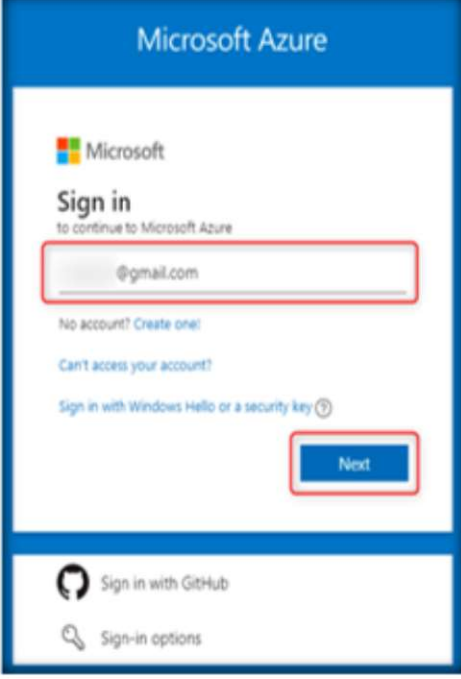
The image shows the Microsoft Azure sign-in interface. At the top, it says "Microsoft Azure". Below that is the Microsoft logo and the text "Sign in to continue to Microsoft Azure". There is a text input field containing "@gmail.com", which is highlighted with a red rectangle. Below the input field are links for "No account? Create one!", "Can't access your account?", and "Sign in with Windows Hello or a security key". A blue "Next" button is highlighted with a red rectangle. At the bottom, there are links for "Sign in with GitHub" and "Sign-in options".

FIGURE 5.5.5: Entering Account ID to continue

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

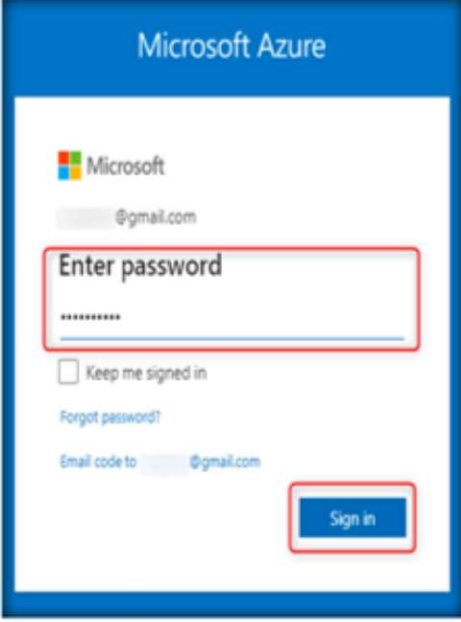
The image shows the Microsoft Azure "Enter password" page. At the top, it says "Microsoft Azure". Below that is the Microsoft logo and the text "Enter password". There is a text input field containing "*****", which is highlighted with a red rectangle. Below the input field is a checkbox labeled "Keep me signed in". There are links for "Forgot password?" and "Email code to @gmail.com". A blue "Sign in" button is highlighted with a red rectangle.

FIGURE 5.5.6: Entering the Log In Password

7. You will be successfully logged in to the **Microsoft Azure** portal. In Azure portal, select and click on **Resource groups**.

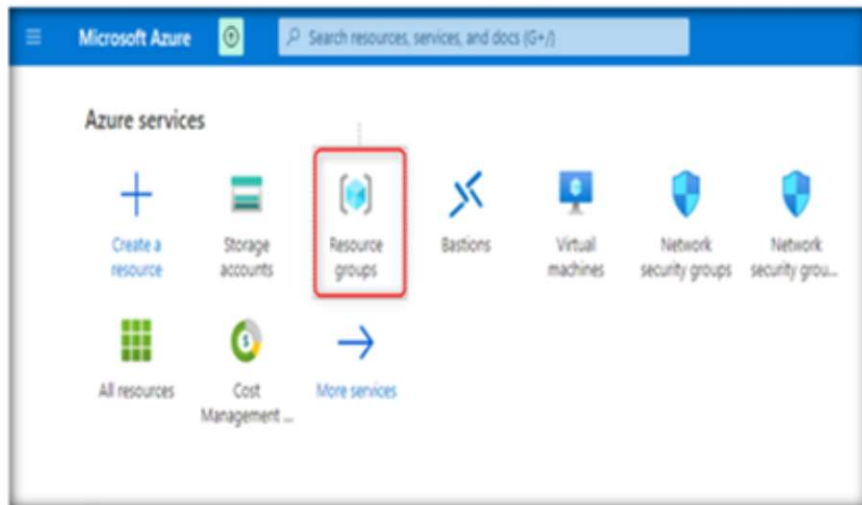


FIGURE 5.5.7: Selecting Resource Groups

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

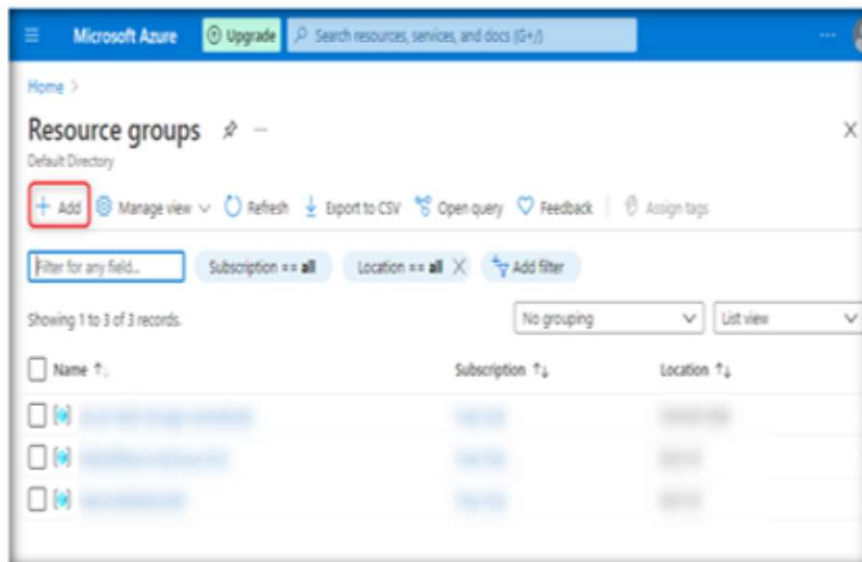


FIGURE 5.5.8: Adding New Resource Group

9. A **Create a resource group** page will open. In the **Resource group** field, provide a name for the resource group (in this lab, we have used **bastionRG** as the **Resource group** name) and select an appropriate region in the **Region** field (in this lab, we have selected **(US) East US**). Then, click on the **Next: Tags >** button.

Create a resource group

Basics | Tags | Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Project details

Subscription * ⓘ Free Trial

Resource group * ⓘ bastionRG

Resource details

Region * ⓘ (US) East US

Review + create < Previous Next: Tags >

FIGURE 5.5.9: Entering Resource Group Name and Location

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

Create a resource group

Basics | Tags | Review + create

Apply tags to your Azure resources to logically organize them by categories. A tag consists of a key (name) and a value. Tag names are case-insensitive and tag values are case-sensitive. [Learn more](#)

Name ⓘ	Value ⓘ	Resource
		Resource group

Review + create < Previous Next: Review + create >

FIGURE 5.5.10: Reviewing and Creating Resource Group

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

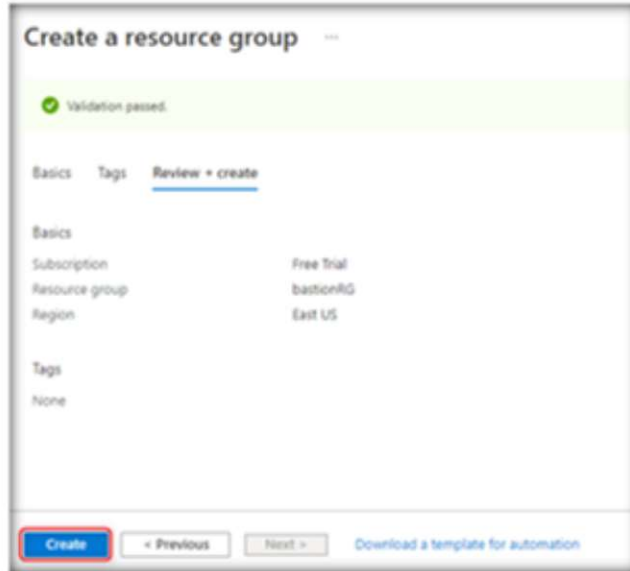


FIGURE 5.5.11: Validation Passed for Creating a Resource Group

12. Resource group **bastionRG** is successfully created now.

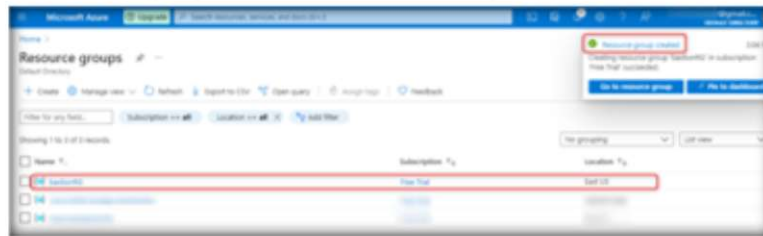


FIGURE 5.5.12: Successfully Creating Resource Group

13. Now, we will create a VM in **bastionRG** resource group. Go back to Azure portal and click on **Virtual machines**.

TASK 2

Creating a Virtual Machine

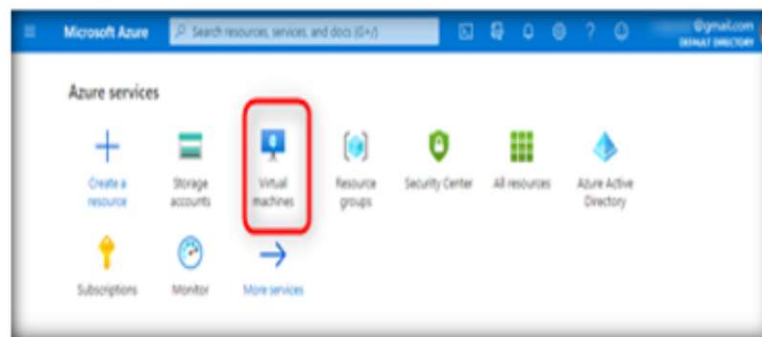


FIGURE 5.5.13: Selecting Virtual machine in Azure portal

14. Click on the **Add** dropdown and then click on **Virtual machine**.

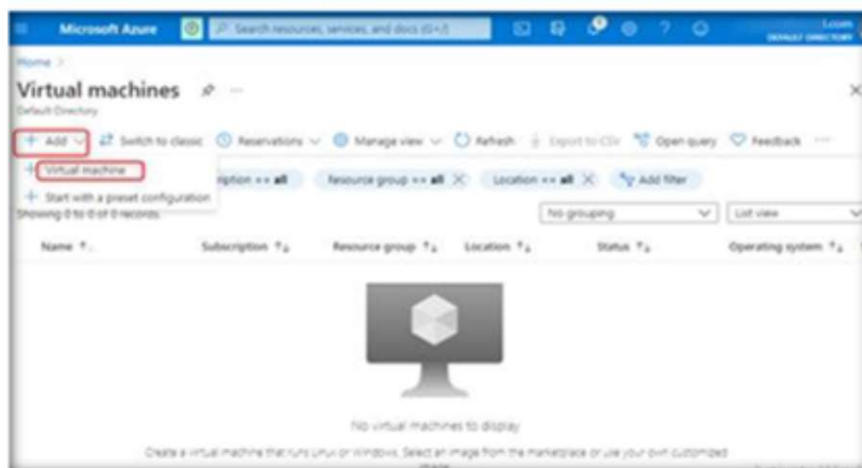


FIGURE 5.5.14 Creating a New Virtual Machine

15. Now, a **Create a virtual machine** window will open. Under the **Basics** tab, select the created **Resource group** (here, **bastionRG**). Then, give an appropriate name to the virtual machine. In this lab, we used **bastiontestVM** as the **Virtual machine name**.

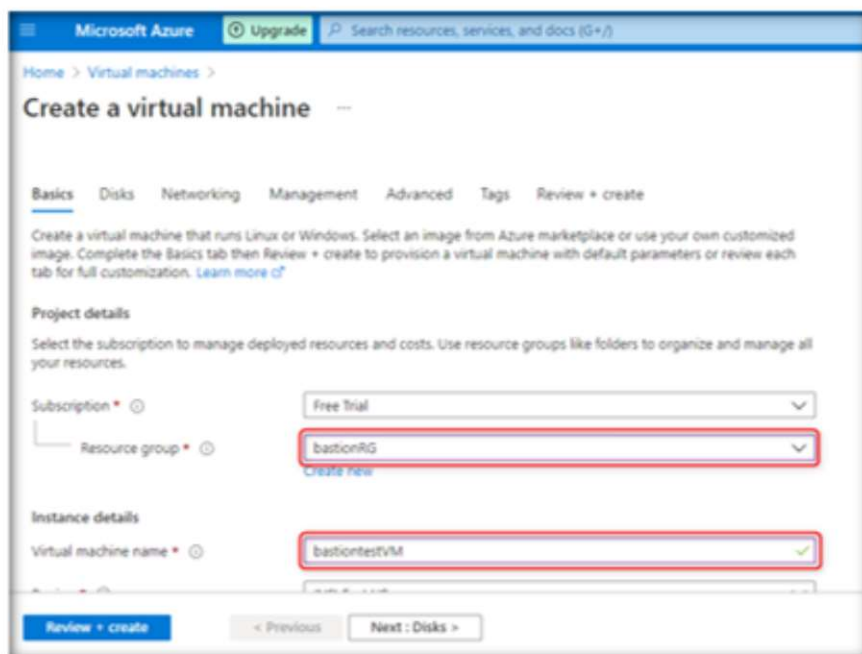


FIGURE 5.5.15: Entering the Name of Resource Group and VM

16. In this lab, we are keeping **Region**, **Availability Options**, and **Size** in their default states, but you can change them as per your requirements. In the **Image** field, ensure you select a **Windows server** image.

The screenshot shows the 'Create a virtual machine' page in the Microsoft Azure portal. The 'Image' dropdown menu is open, and 'Windows Server 2016 Datacenter - Gen1' is selected. The other configuration options are as follows:

- Resource group: bastionRG
- Virtual machine name: bastiontestvm
- Region: (US) East US
- Availability options: Availability zone
- Availability zone: 1
- Image: Windows Server 2016 Datacenter - Gen1
- Azure Spot instance: ☐
- Size: Standard_B1s - 1 vcpu, 1 GiB memory (₹736.30/month)

FIGURE 5.5.16: Selecting the Image of VM

17. Under **Administrator account**, enter the **Username** and **Password**, and then confirm the password.

The screenshot shows the 'Create a virtual machine' page in the Microsoft Azure portal, specifically the 'Administrator account' section. The fields are filled as follows:

- Username: CCSEtestuser
- Password: [Masked]
- Confirm password: [Masked]

The 'Image' dropdown is still set to 'Windows Server 2016 Datacenter - Gen1'.

FIGURE 5.5.17: Entering Username and Password

18. Keep **inbound port rules** and **Licensing** in their default states and click on the **Next: Disks >** button.

Microsoft Azure Upgrade Search resources, services, and docs (G+J)

Home > Virtual machines >

Create a virtual machine

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports

☐ None

☒ Allow selected ports

Select inbound ports *

RDP (3389)

Warning: This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Would you like to use an existing Windows Server license?

☐

[Review + create](#) < Previous **Next: Disks >**

FIGURE 5.5.18: Moving to Disks tab

19. Under the **Disks** tab, keep all the fields in their default state, and then click on the **Next: Networking >** button.

Microsoft Azure Upgrade Search resources, services, and docs (G+J)

Home > Virtual machines >

Create a virtual machine

Basics **Disks** Networking Management Advanced Tags [Review + create](#)

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type

Premium SSD (locally-redundant storage)

Encryption type *

(Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility

☐

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
Create and attach a new disk Attach an existing disk				

[Review + create](#) < Previous **Next: Networking >**

FIGURE 5.5.19: Leaving all fields in Default State and moving to Networking tab

20. Under the **Networking** tab, keep all fields in their default state and click on the **Next: Management >** button.

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal, specifically the 'Networking' tab. The tabs at the top are 'Basics', 'Disks', 'Networking' (selected), 'Management', 'Advanced', 'Tags', and 'Review + create'. Below the tabs, there is a description of network connectivity and a 'Learn more' link. The 'Network interface' section states that a network interface will be created for the VM. The configuration fields are as follows:

- Virtual network:** A dropdown menu showing 'bastionRG-vnet' with a 'Create new' link below it.
- Subnet:** A dropdown menu showing 'default (10.0.0.0/24)' with a 'Manage subnet configuration' link below it.
- Public IP:** A dropdown menu showing '(new) bastiontestVM-ip' with a 'Create new' link below it.
- NIC network security group:** A radio button selection with 'None' selected.

 At the bottom, there are three buttons: 'Review + create' (blue), '< Previous' (disabled), and 'Next: Management >' (highlighted with a red rectangle).

FIGURE 5.5.20: Leaving all Fields in Default State and moving to Management tab

21. Under the **Management** tab, keep all fields in their default state and click on the **Next: Advanced>** button.

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal, specifically the 'Management' tab. The tabs at the top are 'Basics', 'Disks', 'Networking', 'Management' (selected), 'Advanced', 'Tags', and 'Review + create'. Below the tabs, there is a description of monitoring and management options and a 'Learn more' link. The 'Azure Security Center' section shows a green checkmark indicating that the subscription is protected by the Azure Security Center basic plan. The 'Monitoring' section has the following options:

- Boot diagnostics:** Three radio button options: 'Enable with managed storage account (recommended)' (selected), 'Enable with custom storage account', and 'Disable'.
- Enable OS guest diagnostics:** A checkbox that is currently unchecked.

 At the bottom, there are three buttons: 'Review + create' (blue), '< Previous' (disabled), and 'Next: Advanced >' (highlighted with a red rectangle).

FIGURE 5.5.21: Leaving all Fields in Default State and moving to Advanced tab

22. Under the **Advanced** tab, click on **Select an extension to install** beside **Extensions**.

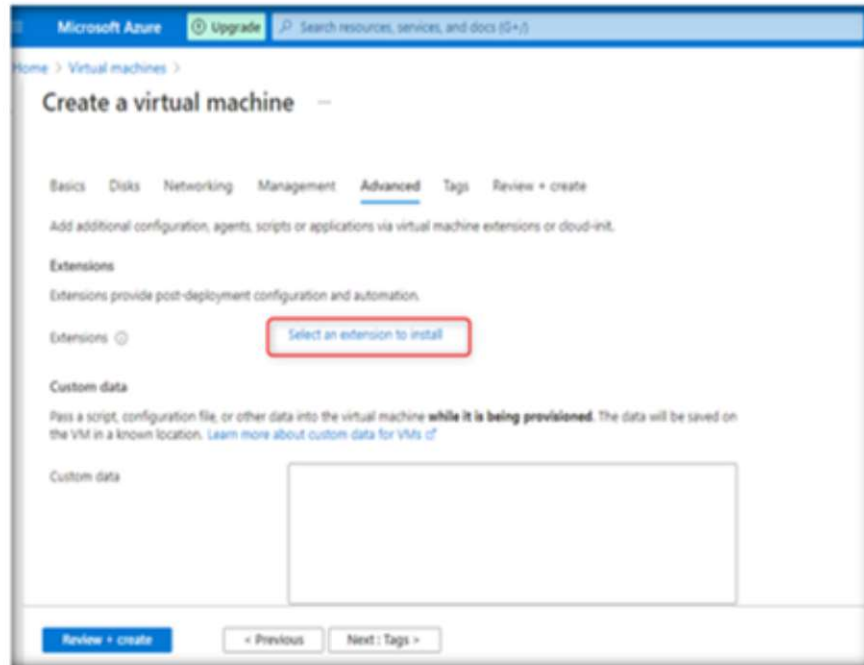


FIGURE 5.5.22: Selecting Antimalware Extension for Installation

23. A **New Resource** window will open. Scroll down on this window and click on **Microsoft Antimalware**.

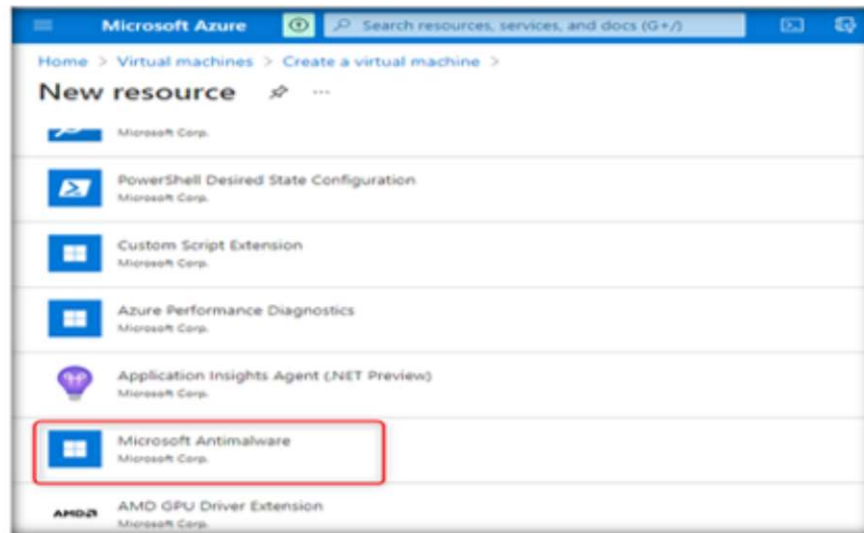


FIGURE 5.5.23: Selecting Microsoft Antimalware

24. Now, click on the **Create** button.

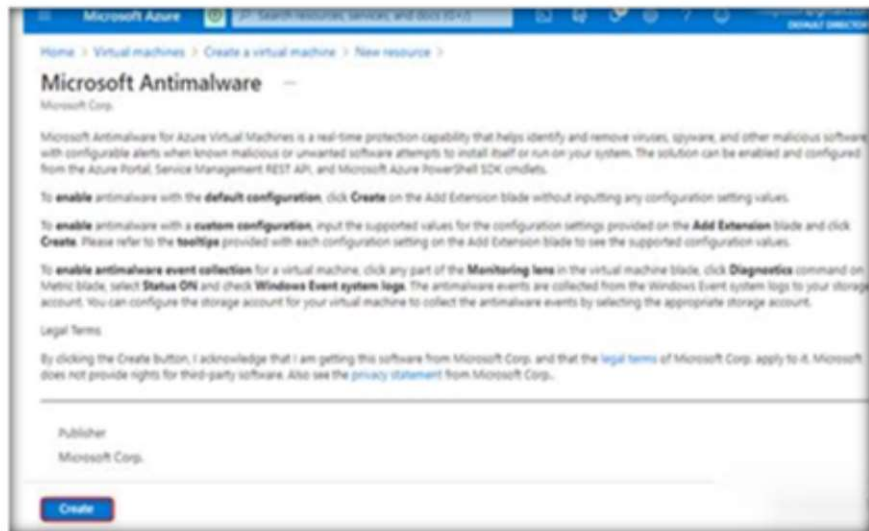


FIGURE 5.5.24: Installing Microsoft Antimalware

25. In the **Install extension** window that will open, enter **.log** under **Excluded file extensions** and **SQLServr.exe** under **Excluded process**. Leave the other fields in their default state and click on **OK**.

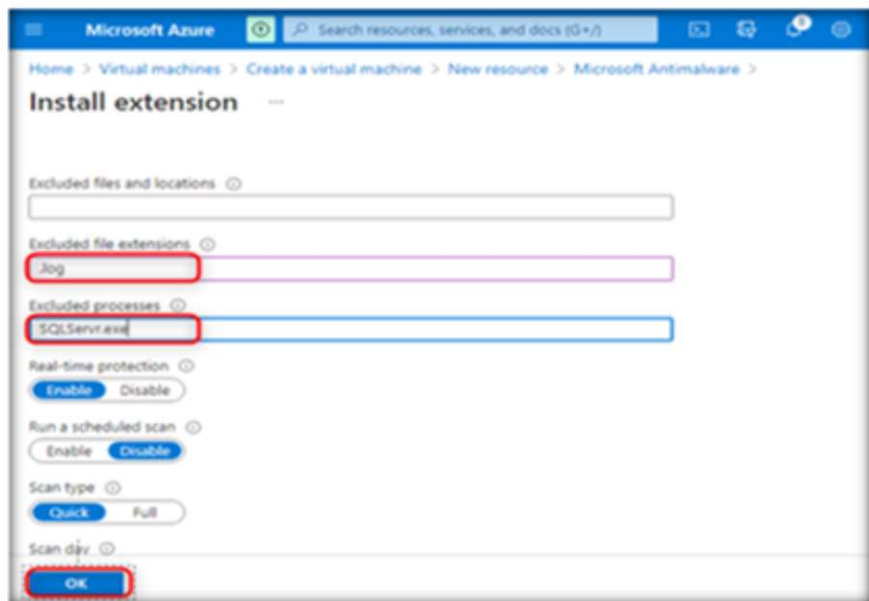


FIGURE 5.5.25: Entering Details in Install Extension Window

26. Leave the other fields in their default state and click on the **Next: Tags >** button.

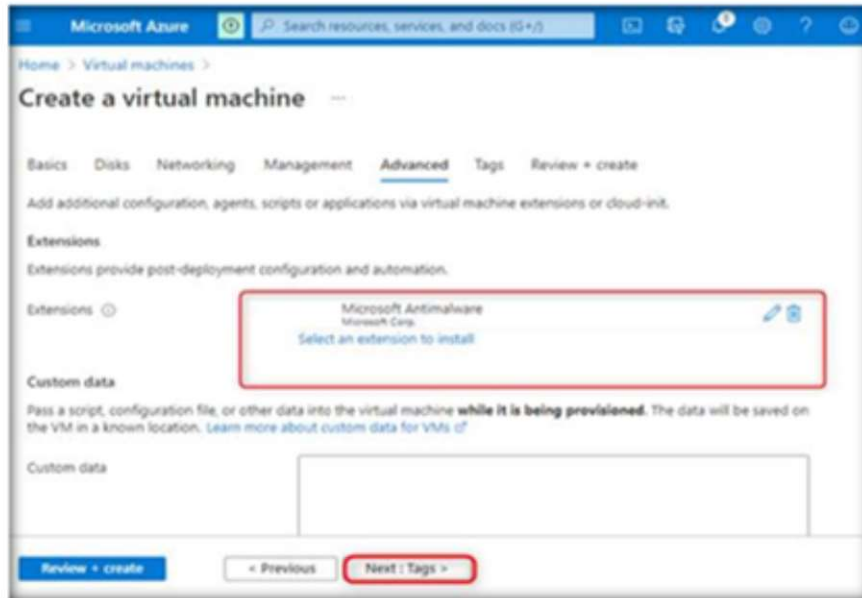


FIGURE 5.5.26: Moving to Tags tab

27. Leave the fields under **Tags** in their default state and click on **Review + create**.

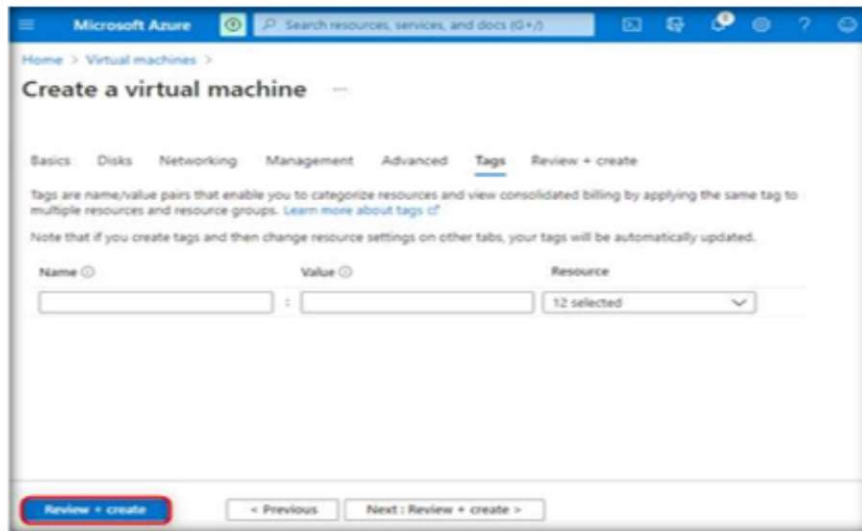


FIGURE 5.5.27: Reviewing and Creating VM

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

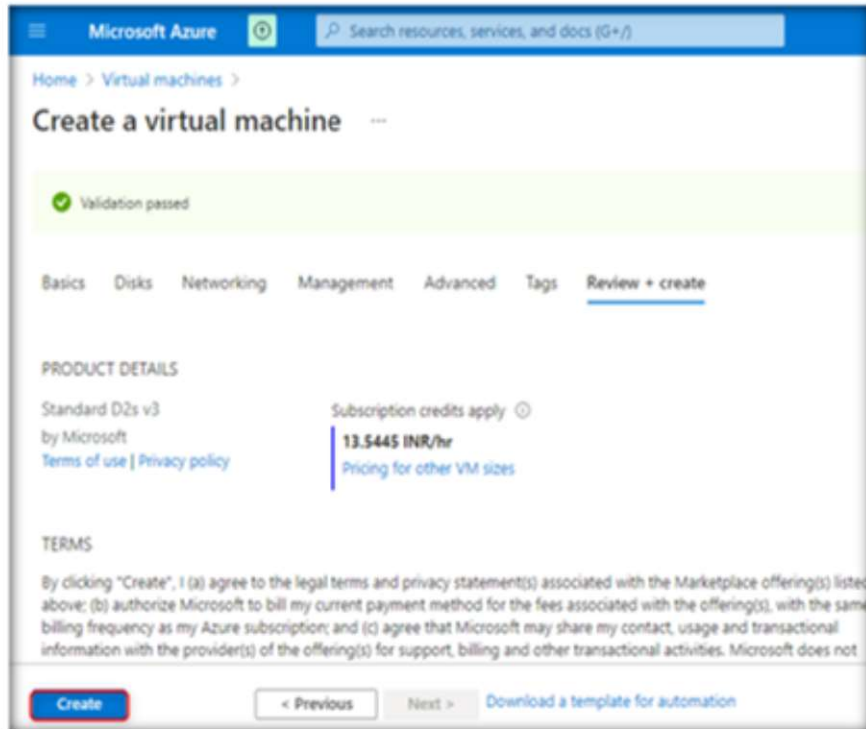


FIGURE 5.5.28: VM Passing the Validation

29. After the completion of deployment, click on the **Go to resource** button.

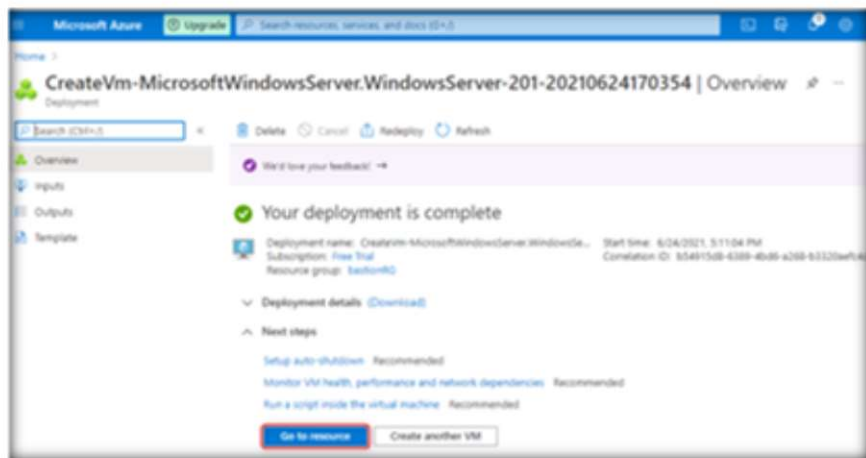


FIGURE 5.5.29: Successfully Completion of VM Deployment

30. **bastiontestVM** virtual machine is successfully created in **bastionRG** resource group.

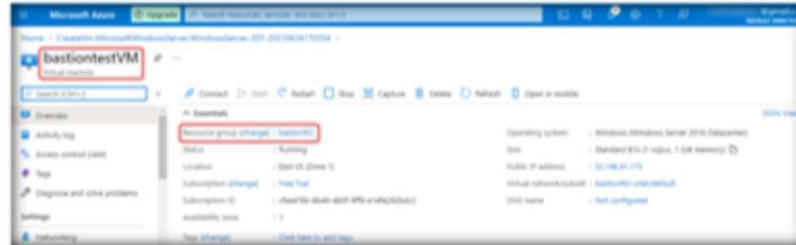


FIGURE 5.5.30: Copying the Public IP address of the VM

TASK 3

Creating a Bastion Host for the VM

31. Now, to create a Bastion host for the created VM, navigate to Azure portal and click on **Resource Groups**.

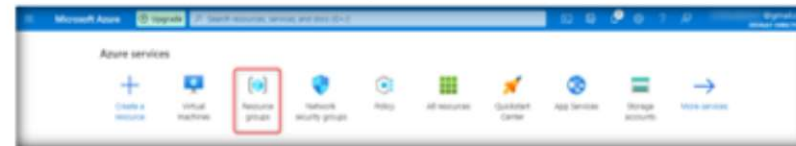


FIGURE 5.5.31: clicking Resource groups

32. To select the resource group of the created VM, click on **bastionRG** in the **Resource groups** pane.

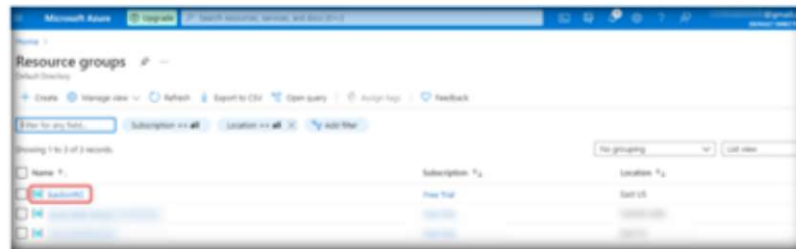


FIGURE 5.5.32: Clicking bastionRG

33. Now, in the **bastionRG** resource group, scroll up and select **bastiontestVM** to configure the Azure Bastion host.

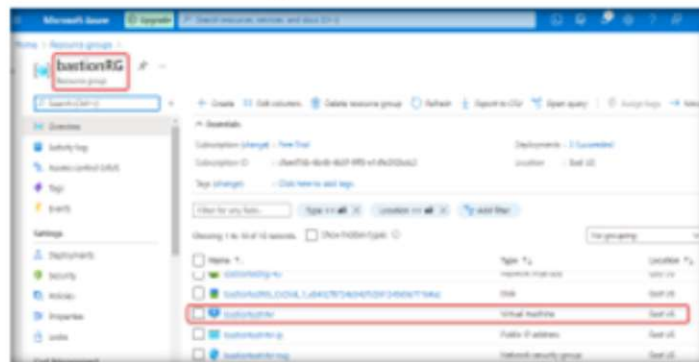


FIGURE 5.5.33: Selecting bastiontestVM

34. In **bastiontestVM** page, click on the **Connect** button, and then click on **Bastion** in the dropdown.



FIGURE 5.5.34: Selecting Bastion for bastiontestVM

35. To secure the connection to the VM using Azure Bastion, click on the **Use Bastion** button in the **Bastion** tab.

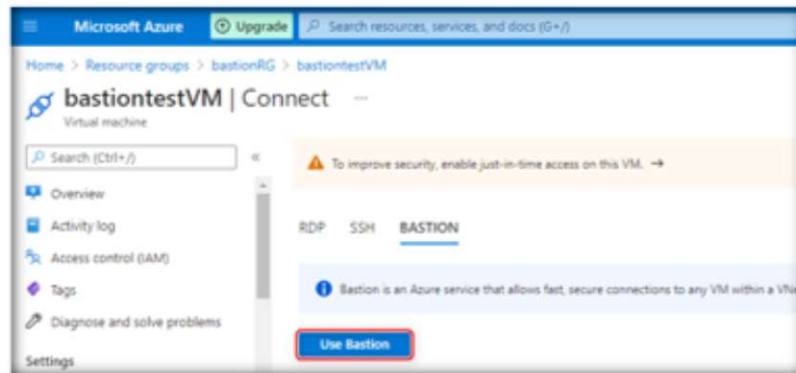


FIGURE 5.5.35: Using Bastion for bastiontestVM1

36. In **Step 2 of 3** of Azure Bastion wizard, click on the **Create Subnet** button. This will create a subnet named **AzureBastionSubnet**.

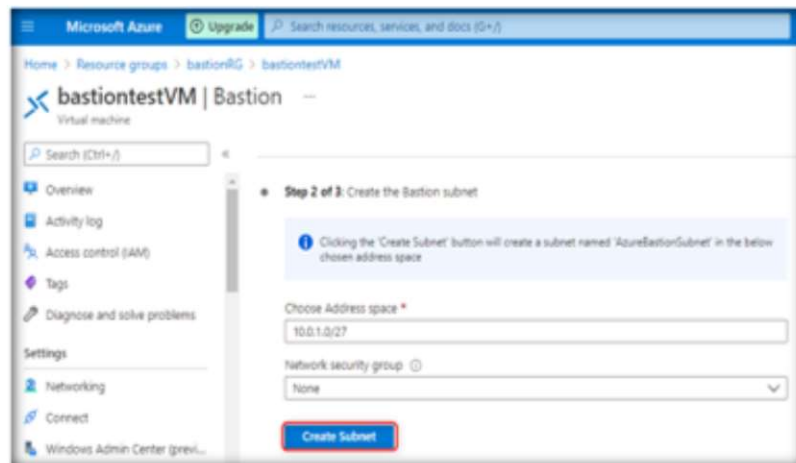


FIGURE 5.5.36: Creating Subnet for bastiontestVM1

37. Then, under **Step 3 of 3**, click on the **Create Azure Bastion using defaults** button to create Azure Bastion with default configurations.

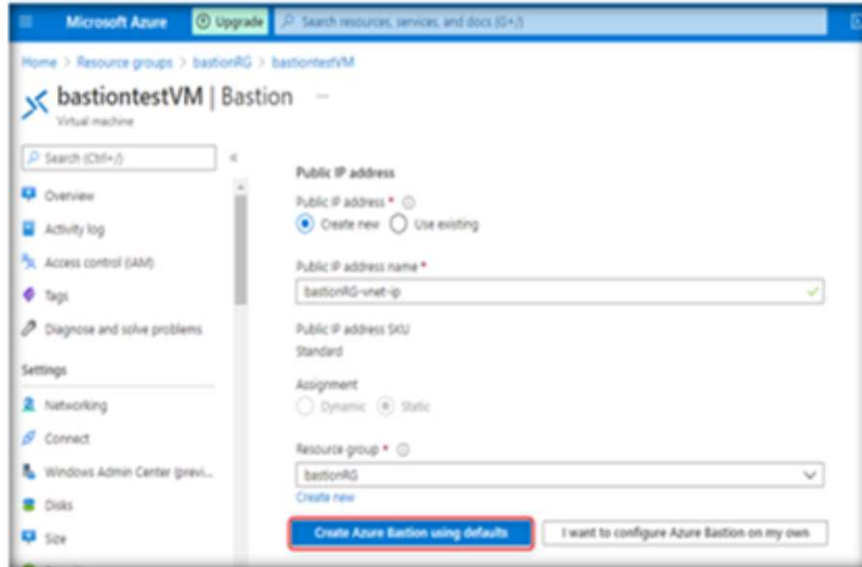


FIGURE 5.5.37: Creating Azure Bastion using Defaults

38. Wait for a few minutes. After 15 minutes, if the **Creating a new bastion...** process still continues, then proceed with the next step.

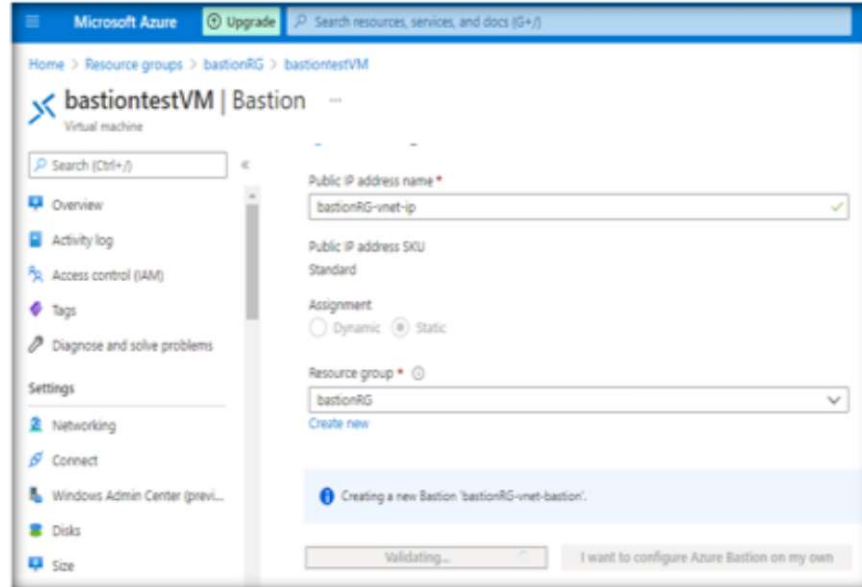


FIGURE 5.5.38: Creation of New Bastion for bastiontestVM

TASK 4

Connecting the VM Using Bastion

39. Now, to connect to **bastiontestVM** using the created **Azure Bastion** host, click on **Connect** from the left menu in the **bastiontestVM** page.

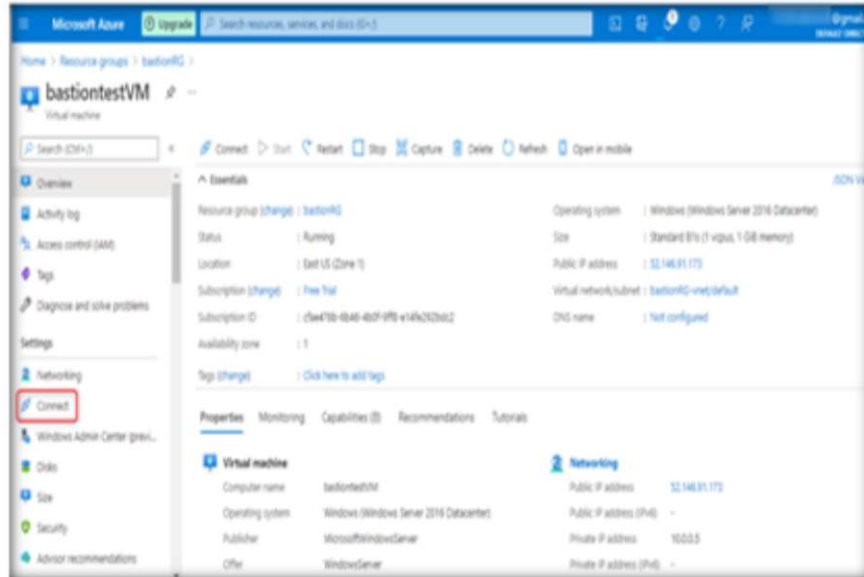


FIGURE 5.5.39: Connecting to bastiontestVM

40. Click on **BASTION**.

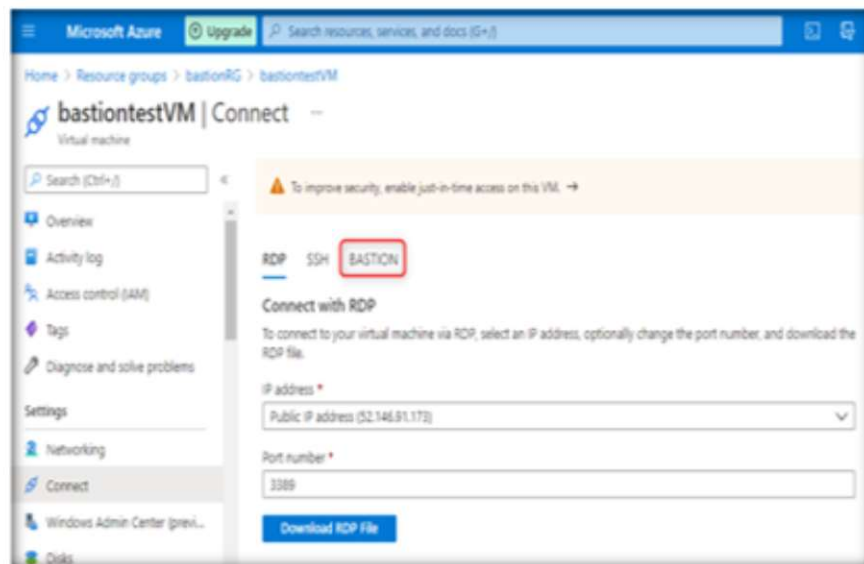


FIGURE 5.5.40: Selecting BASTION Connection for bastiontestVM

41. Then, click on the **Use Bastion** button.

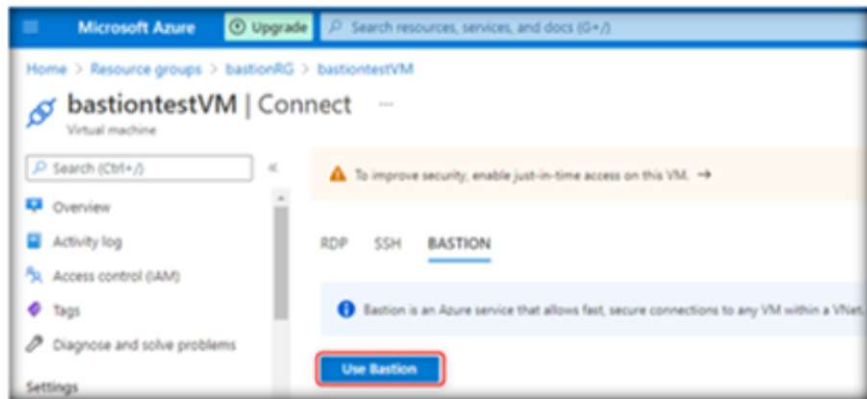


FIGURE 5.5.41: Connecting to bastiontestVM using BASTION

42. Enter VM username (**CCSEtestuser**) and password and then click on the **Connect** button.

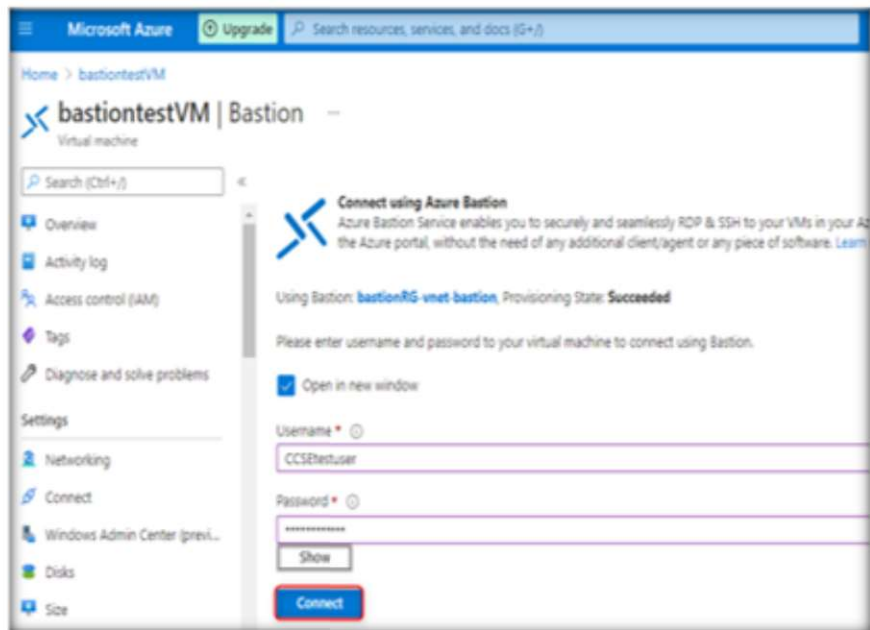


FIGURE 5.5.42: Entering Login Credentials of bastiontestVM

43. Click on the **Allow** button in the new window that opens.

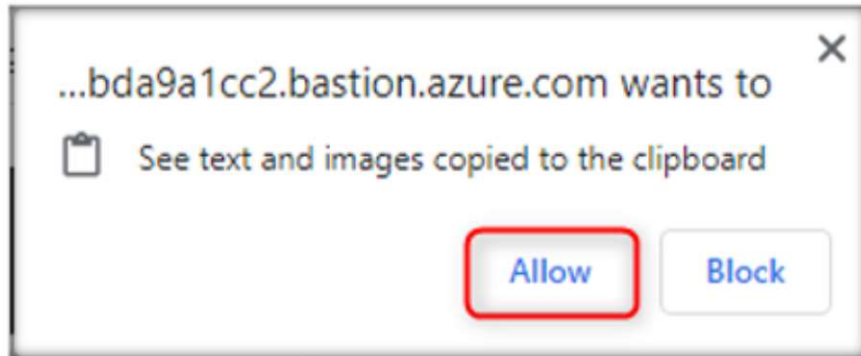


FIGURE 5.5.43: Selecting Allow for Pop Up Message

44. A **Networks** window will appear. Click on the **Yes** button.

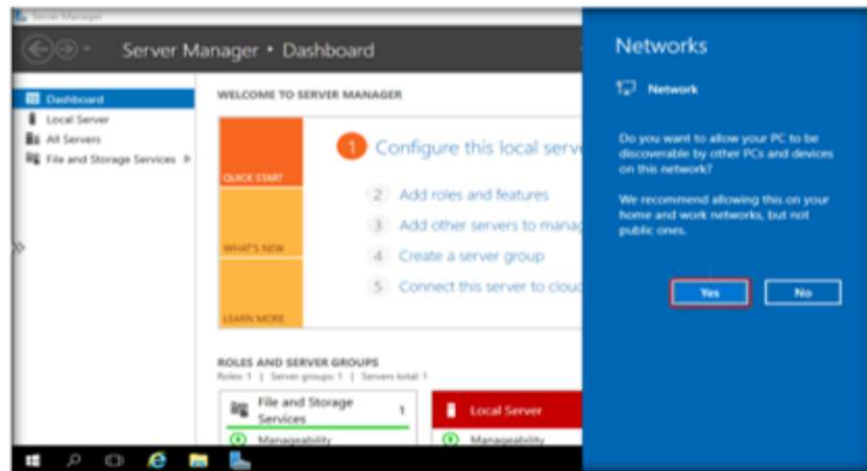


FIGURE 5.5.44: Selecting Networks

45. In Azure portal, an RDP session is opened over SSL. The VM is now successfully connected to the Bastion network. Click on the left side arrow on **Server Manager - Dashboard** to see the **Clipboard**.

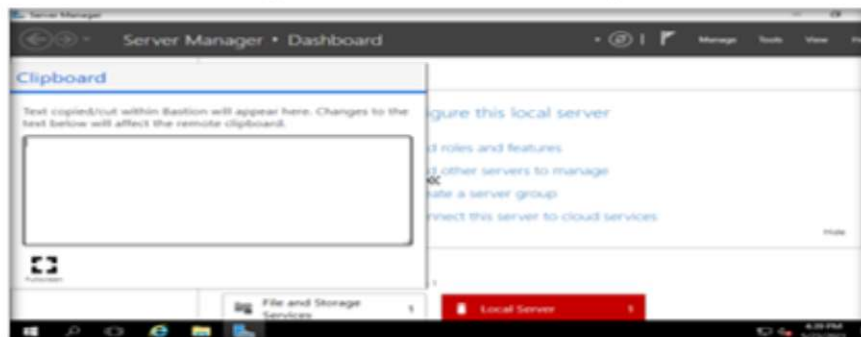


FIGURE 5.5.45: bastiontestVM is successfully connected to the Bastion network

46. In the **Windows Start** menu, click on the **Power** button and then on **Disconnect**.

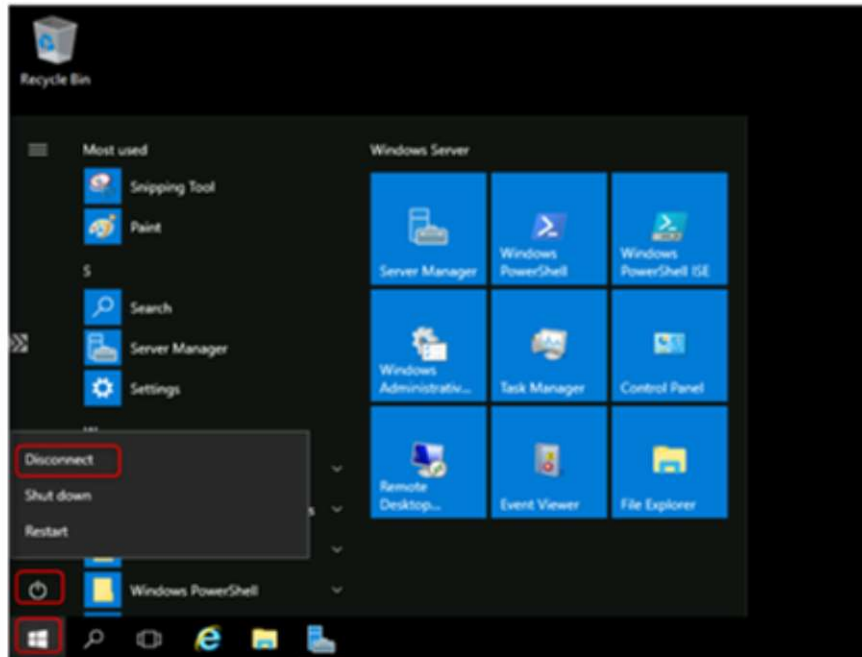


FIGURE 5.5.46: Disconnecting bastiontestVM

47. Click on the **Close** button.

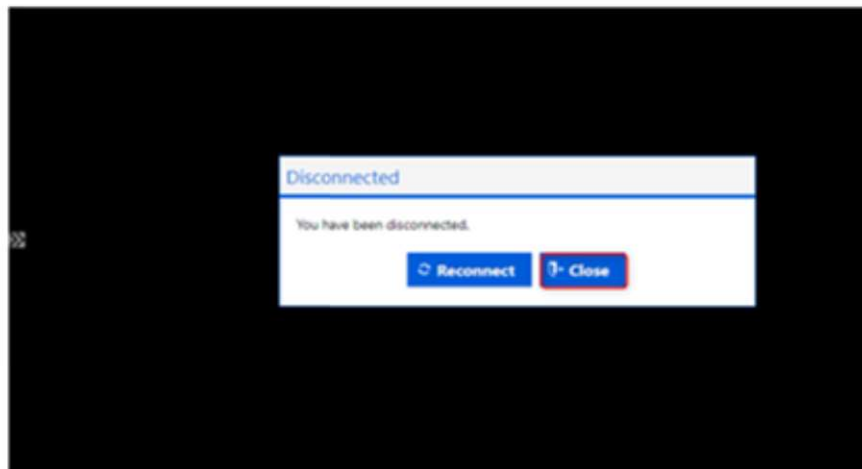


FIGURE 5.5.47: Closing bastiontestVM Connection

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

48. Navigate to **Resource groups** in the Azure portal. Click on the name of the resource group (**bastionRG**) to view the resource group details. Click on **Delete resource group** at the top.

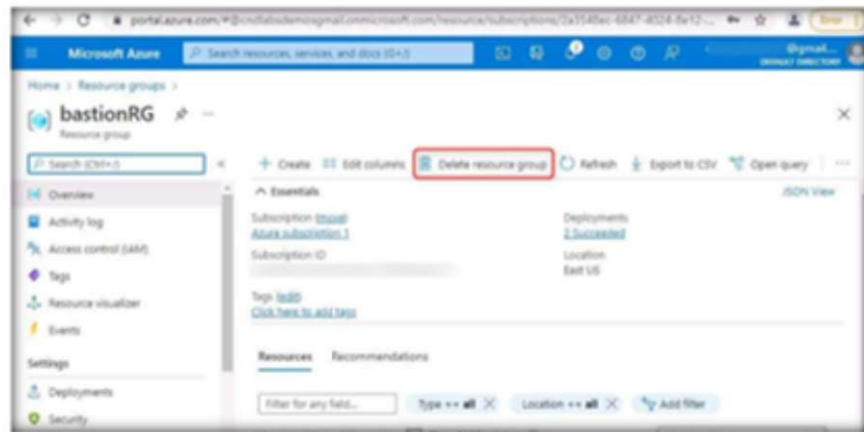


FIGURE 5.5.48: Deleting Resource Group

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.