

Home / Azure / Guided Lab / Create a Virtual Network

Create a Virtual Network

Level: Fundamental

Azure Virtual Network Azure

⌚ 0h 43m 19s left



End Lab

Open Console

Validation

Lab Credentials

User Name (i)

labuser_142282_80569579@instructorwhizlabs.onmicrosoft.com



Password (i)

3#Ln\$ZF7iep0r9?B



Resource Group (i)

rg_eastus_142282_1_168967653061



Lab Resources

No Lab Resources Found

Support Documents

No Support Documents Found

Need help?

 How to use Hands on Lab Troubleshooting Lab FAQs

Submit Feedback

Share

Lab Overview

Lab Steps

Lab Validation

Lab FAQs

 Azure Administrator Associate

Lab Steps

Task 1: Sign in to Azure Portal

1. Go to the Azure portal by clicking on the **Open Console** button or by using URL <https://portal.azure.com>.
 - **Note:** It is recommended to use incognito mode to avoid Azure portal cache related issues.
2. If it automatically logs into any other azure account, please logout of it and clear cache.
3. Sign in with your given **username** and **password** on Azure portal.
4. If login is not working. Click on **End Lab** and start the lab again.

Task 2: Create a Virtual Network

In this task, we will create Virtual Network on Azure Portal.

1. At the top of the Azure portal, in the search box, enter **Virtual network**. Select **Virtual Networks** in the search results.

The screenshot shows the Microsoft Azure portal interface. At the top left is the 'Microsoft Azure' logo. To its right is a search bar with the placeholder text 'virtual network'. Below the search bar are three buttons: 'All', 'Services (20)', and 'Marketplace (5)'. Under the 'Services' button, there is a list titled 'Recent resources' with a 'Name' column. Two items are listed: 'myWhiz' and 'WhizRes'. To the right of this list is a vertical sidebar titled 'Services' containing four items: 'Virtual networks' (which is highlighted with a red box), 'Virtual network gateways', 'Virtual networks (classic)', and 'Network Managers'.

2. In **Virtual networks**, select **+ Create**.

The screenshot shows the 'Virtual networks' list page. At the top left is the title 'Virtual networks'. Below it is a subtitle 'Default Directory (instructorwhizlabs.onmicrosoft.com)'. The main area contains a table with columns for 'Name', 'Status', and 'Actions'. The first row shows 'myWhiz' with status 'Active' and actions 'Edit' and 'Delete'. Below the table is a toolbar with several buttons: '+ Create' (highlighted with a red box), 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags'. At the bottom of the page are three filter buttons: 'Filter for any field...', 'Subscription equals all', 'Resource group equals all', and 'Location equals all'.

3. In **Create virtual network** page, enter or select the following information in the **Basics** tab:

- Resource group : Select **rg_eastus_XXXXX**
- Instance details :
 - Name : Enter **vnet1**
 - Region : Select **East US**

Create virtual network ...

Basics Security IP addresses Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *

Pay-As-You-Go

Resource group *

rg_eastus_55277_1_168715651621

[Create new](#)

Instance details

Virtual network name

vnet1

Region ⓘ *

(US) East US

[Deploy to an edge zone](#)

NOTE: If you are seeing a different UI to create a Virtual Network then check FAQs



4. Select the **IP Addresses** tab or click on the **Next: IP Addresses** button at the bottom of the page. In the **IP Addresses** tab, click on **Add IP address space** and enter this information:

- Address space type : Select **IPv4**
- Starting address : Enter **10.0.0.0**
- Address space size : Select **/16**
- Click **Add**.

Add an IP address space

The address space for a virtual network has one or more non-overlapping address ranges. It is recommended to use private (RFC 1918), shared (RFC 6598), or local (RFC 4193) address ranges. [Learn more](#).

Address space type IPv4 IPv6

Starting address

Address space size

IP address space

- In **Add a subnet** section, enter the following information :
 - IP address space : Select **10.0.0.0/16**
 - Subnet template : Select **default**
 - Name : **default**
 - Subnet Address range: Enter **10.1.0.0/24**
 - NAT gateway: Leave the defaults
 - Service gateway: Leave the defaults
 - Click on **Save**.



Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. [Learn more ↗](#)

IP address space ⓘ

10.0.0.0/16

10.0.0.0 - 10.0.255.255 (65536 addresses)

Subnet details

Subnet template ⓘ

Default

Name * ⓘ

default2

Starting address * ⓘ

10.0.1.0

Subnet size ⓘ

/24 (256 addresses)

IP address space ⓘ

10.0.1.0 - 10.0.1.255 (256 addresses)

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. [Learn more ↗](#)

NAT gateway ⓘ

None

[Create new](#)

Network security group ⓘ

None

Add

Cancel

Note: The IP address may already exist there. Then no need to enter the IP.

Create virtual network ...

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more ↗](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more ↗](#)

Add an IP address space

10.0.0.0/16

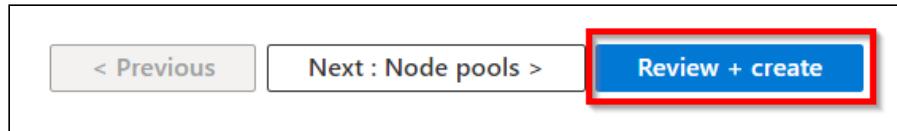
+ Add a subnet ...

10.0.0.0 - 10.0.255.255 (65536 addresses)

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-

A NAT gateway is recommended for outbound internet access from subnets. Edit the subnet to add a NAT gateway. [Learn more ↗](#)

5. Leave all the settings as default and select the **Review + Create** button and then click on **Create**. This step may take a few minutes.



6. You will now see a page displaying **Your deployment is complete**.

Your deployment is complete

Deployment name: Microsoft.VirtualNetwork-20220201152248	Start time: 2/1/2022, 3:24:34 PM
Subscription: Pay-As-You-Go	Correlation ID: 98dd1cb8-978e-479b-b832-da3e19a62d0d
Resource group: WhizResourceGroup_ananya	

✓ Deployment details ([Download](#))
 ^ Next steps
[Go to resource](#)

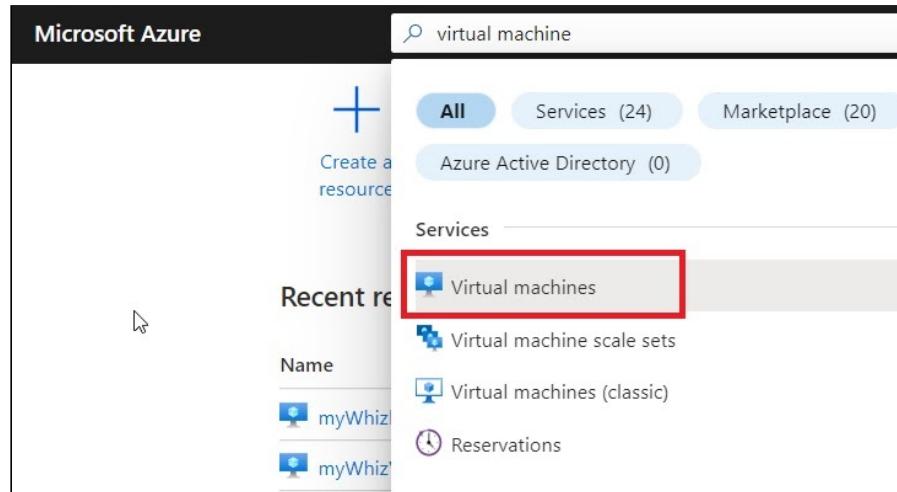
Do you Know?

Azure Virtual Network provides built-in Azure DDoS Protection Standard, ensuring automatic and scalable defense against DDoS attacks for enhanced network security.

Task 3: Create two virtual machines

In this task, we will create Virtual Machines to test the connection.

1. In the search box at the top of the Azure portal, enter **Virtual machine**. Select **Virtual machines** from the search results.



2. In the **Virtual machines** section, select **+ Create a Virtual machine** and enter the following values in the **Basics** tab.

- Resource group : Select **rg_eastus_XXXXX**
- Instance details :
 - Virtual Machine Name : Enter **vm1**
 - Region : Select **(US) East US**
 - Availability Options : Leave as default
 - Image : Select **Windows Server 2022 Datacenter : Azure Edition - Gen2**
 - Azure Spot instance : Leave the default of unchecked.
 - Size : Click on **see all sizes** then select **B2s** and then **click on select**
- Administrator Account :
 - Username : Enter a **username**
 - Password : Enter a **password**
 - Confirm password : Re-enter **password**
- Inbound Port rules :
 - Public inbound ports : Select **Allow selected ports**
 - Select inbound ports : Select **HTTP, SSH and RDP**

Create a virtual machine ...

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Pay-As-You-Go

Resource group * ⓘ rg_eastus_55277_1_168716026673 Create new

Instance details

Virtual machine name * ⓘ vm1

Region * ⓘ (US) East US

Availability options ⓘ Availability zone

Availability zone * ⓘ Zones 1

3. Now, click on **Next** and go to the **Disks** section. Select the following information:

- OS disk type : Select **Standard SSD**

Create a virtual machine

Basics **Disks** Networking Management Monitoring 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](#)

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host Encryption at host is not registered for the selected subscription.
[Learn more about enabling this feature](#)

OS disk

OS disk type * Standard SSD (locally-redundant storage)

Choose Premium SSD disks for lower latency, higher IOPS and bandwidth, and bursting. Single instance virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA. [Learn more](#)

Delete with VM

Key management Platform-managed key

4. Click on **Next** and on the **Networking** tab, select the following information:

- Virtual network : Select **vnet1**

Create a virtual machine

Basics Disks **Networking** Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.

[Learn more ↗](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *	<input type="text" value="vnet1"/>
Subnet *	<input type="text" value="default (10.0.0.0/24)"/>
Public IP	<input type="text" value="(new) vm1-ip"/>
NIC network security group	<input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced
Public inbound ports *	<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports

5. Go to the **Monitoring** tab, and select the following information:

- Boot diagnostics : Select **Disable**

Create a virtual machine

Basics Disks Networking Management **Monitoring** Advanced Tags Review + create

Configure monitoring options for your VM.

Alerts

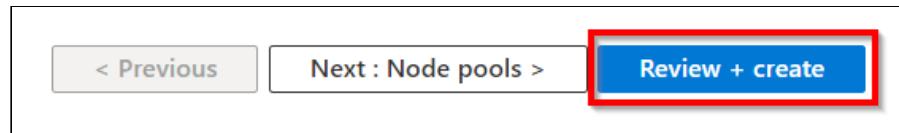
Enable recommended alert rules

Diagnostics

Boot diagnostics Enable with managed storage account (recommended)
 Enable with custom storage account
 Disable

Enable OS guest diagnostics

6. Leave all the settings as default and select the **Review + Create** button and then click on **Create**. This step may take a few minutes.



7. You will now see a page displaying **Your deployment is complete**.

The screenshot shows a summary of a completed deployment. It includes the deployment name (CreateVm-MicrosoftWindowsServer.WindowsSe...), start time (2/1/2022, 4:03:46 PM), subscription (Pay-As-You-Go), correlation ID (372c1afa-48d8-4d75-93d8-bc32c8b92e75), and resource group (WhizResourceGroup_ananya). Below this, there are sections for 'Deployment details' (with a 'Download' link) and 'Next steps' (which include 'Setup auto-shutdown', 'Monitor VM health, performance and network dependencies', and 'Run a script inside the virtual machine', all marked as 'Recommended'). At the bottom are two buttons: 'Go to resource' (blue) and 'Create another VM' (white).

8. Now, create another virtual machine by following the above steps with the following configurations :

- Resource Group : Select **rg_eastus_XXXXX**
- Virtual Machine Name : Enter **vm2**
- Select inbound ports : Select **HTTP, SSH and RDP**
- In **Networking Tab**, Virtual Network : select **vnet1**
- Click on **Review + create** and then **create**

Create a virtual machine ...

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

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ

Pay-As-You-Go

Resource group * ⓘ

rg_eastus_55277_1_168717343529

[Create new](#)

Instance details

Virtual machine name * ⓘ

vm2

Region * ⓘ

(US) East US

Availability options ⓘ

No infrastructure redundancy required

Security type ⓘ

Trusted launch virtual machines

9. You will now see a page displaying **Your deployment is complete.**

✓ Your deployment is complete



Deployment name: CreateVm-MicrosoftWindowsServer.WindowsSe... Start time: 2/1/2022, 3:57:32 PM
Subscription: Pay-As-You-Go Correlation ID: 0c33d3ae-f483-47bf-bdf0-b7e701c7d7ae
Resource group: WhizResourceGroup_ananya

✓ Deployment details [\(Download\)](#)

^ Next steps

[Setup auto-shutdown](#) Recommended

[Monitor VM health, performance and network dependencies](#) Recommended

[Run a script inside the virtual machine](#) Recommended

[Go to resource](#)

[Create another VM](#)

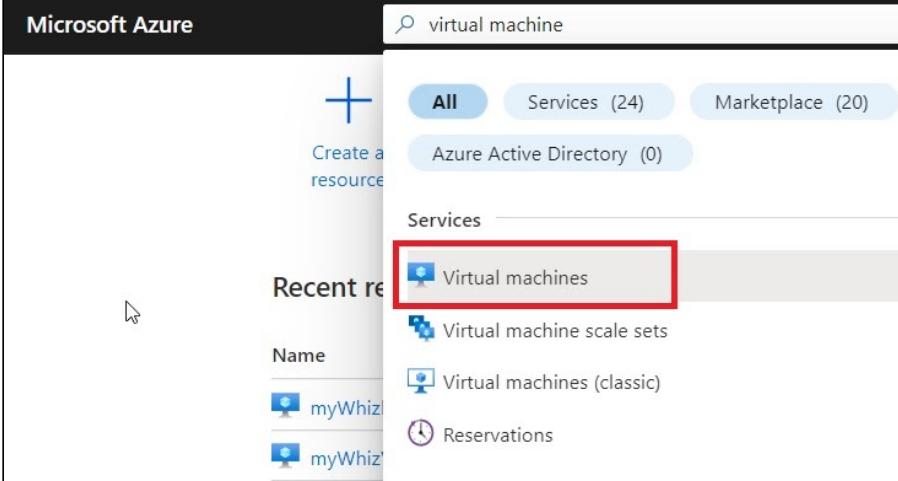
10. You can see that both the virtual machines are created and being displayed.

<input type="checkbox"/> vm1	Pay-As-You-Go	WhizResourceGroup_a...	East US	Running
<input type="checkbox"/> vm2	Pay-As-You-Go	WhizResourceGroup_a...	East US	Running

Task 4: Test the Connection

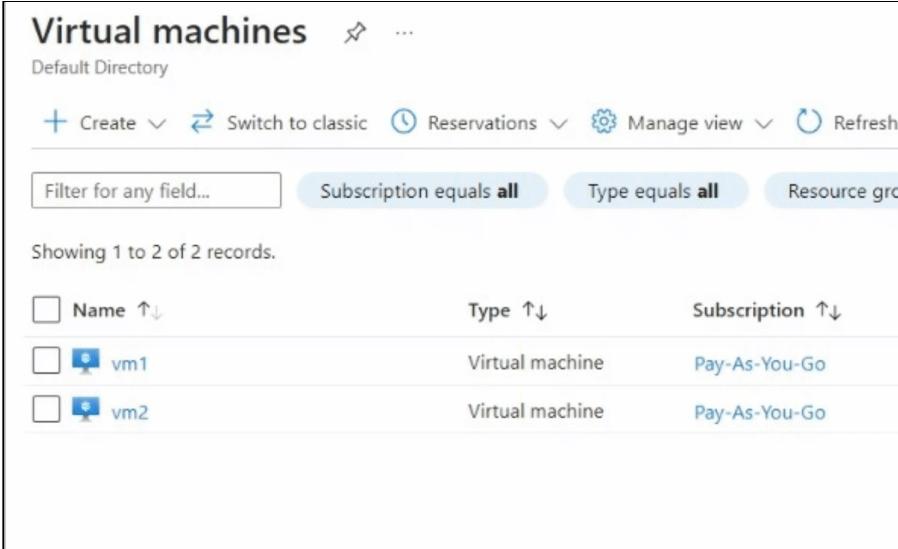
In this task, we will allow ICMP connections between VMs and test whether the virtual machines can communicate (ping) each other.

1. Search for **Virtual machines** in the Search bar and select it.



The screenshot shows the Microsoft Azure search interface. A search bar at the top contains the text "virtual machine". Below the search bar, there are three tabs: "All", "Services (24)", and "Marketplace (20)". The "Services" tab is selected. Under the "Services" heading, there is a list of recent resources. The "Virtual machines" item is highlighted with a red box. Other items in the list include "Virtual machine scale sets", "Virtual machines (classic)", and "Reservations".

2. Select **vm1**, open its **Overview** page.



The screenshot shows the "Virtual machines" overview page. At the top, there are buttons for "Create", "Switch to classic", "Reservations", "Manage view", and "Refresh". Below these are filters for "Subscription equals all", "Type equals all", and "Resource group". The main area displays a table with two records:

Name	Type	Subscription
vm1	Virtual machine	Pay-As-You-Go
vm2	Virtual machine	Pay-As-You-Go

3. On the **Overview** page of your VM, go to the **Networking** section, here you can see the network interface which has the public ip address and the private ip address and also the inbound and outbound port rules.

The screenshot shows the Azure portal interface for a virtual machine named 'vm1'. The left sidebar has 'Networking' selected under 'Settings'. The main content area shows the 'vm1818_z1' network interface with its IP configuration set to 'ipconfig1 (Primary)'. The 'Inbound port rules' tab is active, showing a table of rules:

Priority	Name	Port	Protocol	Source	Destination
300	RDP	3389	TCP	Any	Any
320	HTTP	80	TCP	Any	Any
340	SSH	22	TCP	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBo...	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

A blue callout box points to the 'Add inbound port rule' button at the top right of the table.

4. Click on **Add inbound port rule** and enter or select the following information:

- Protocol : Select **ICMP**
- Name : Enter **ICMP**
- Leave all the settings as default.
- Click on **Add**.

Add inbound security rule

vm1-nsg

Destination ⓘ
Any

Service ⓘ
Custom

Destination port ranges * ⓘ
*

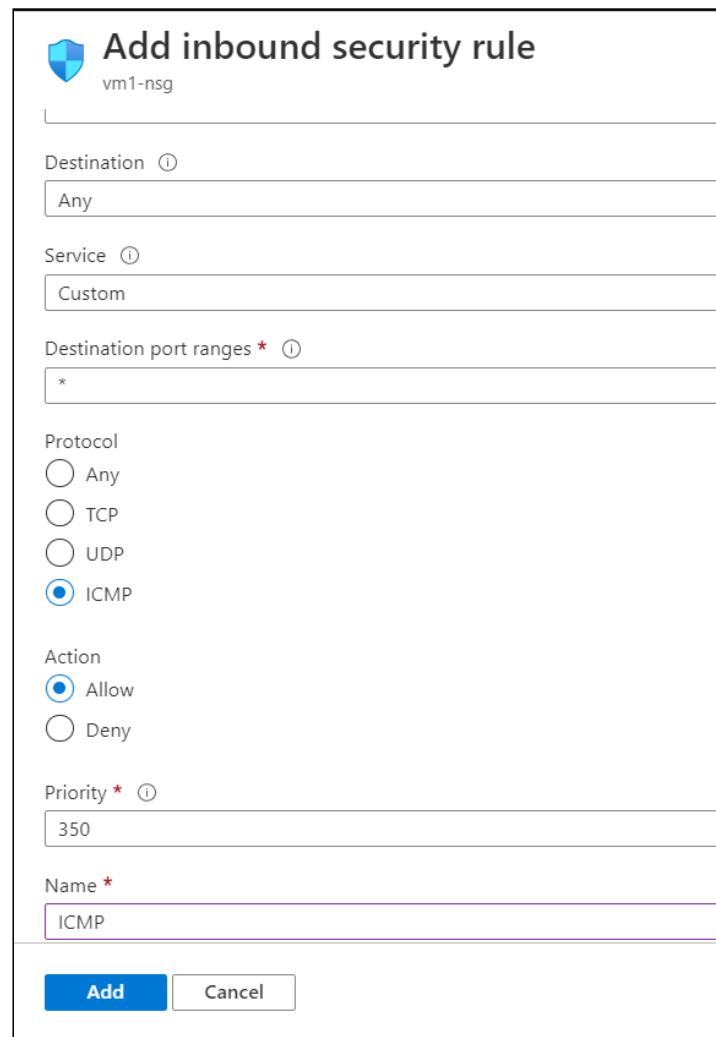
Protocol
 Any
 TCP
 UDP
 ICMP

Action
 Allow
 Deny

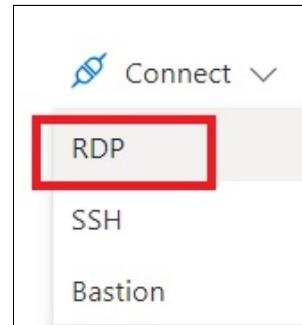
Priority * ⓘ
350

Name *
ICMP

Add **Cancel**



5. Select **RDP** and click on **Download RDP File** button.



NOTE: If you are a **Linux** or **MAC** user:

- Download the [RDP software](#) and install it.
- Once installed, open the software and click on **Add PC**.
- Connect to your virtual machine using its public IP address and click on **Add**.
- Right click and open the PC, Enter **username** and **password** in the popup and click on continue on all further popups.

[RDP](#) [SSH](#) [Bastion](#)

Connect with RDP

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

IP address *

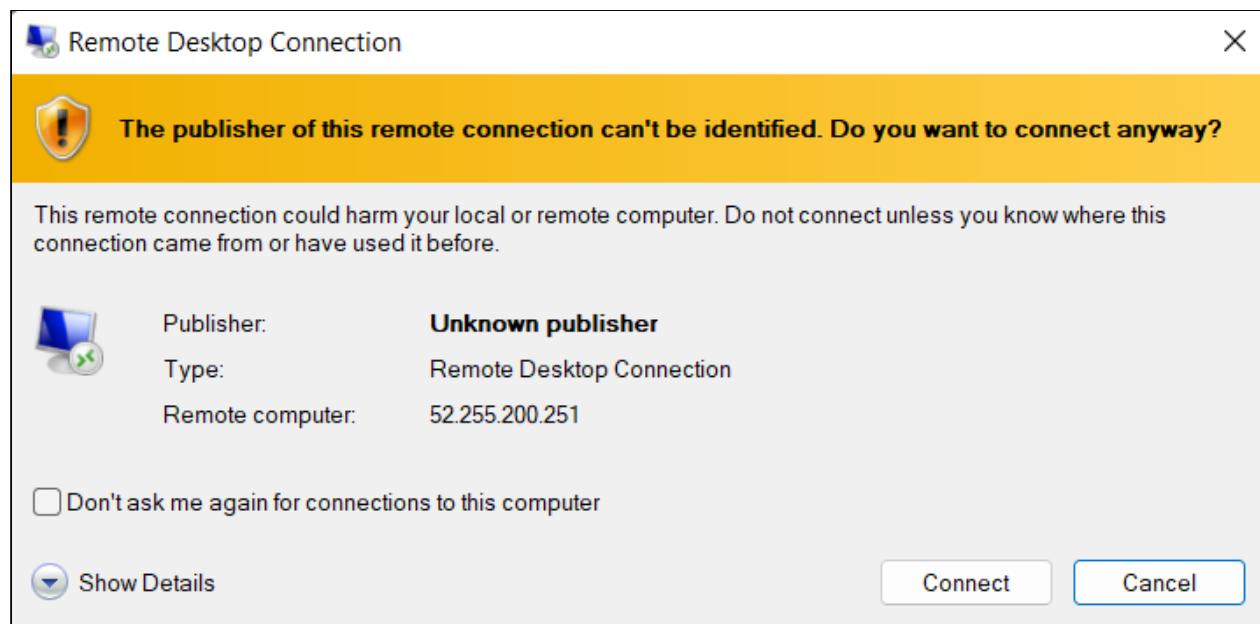
Public IP address (52.255.200.251)

Port number *

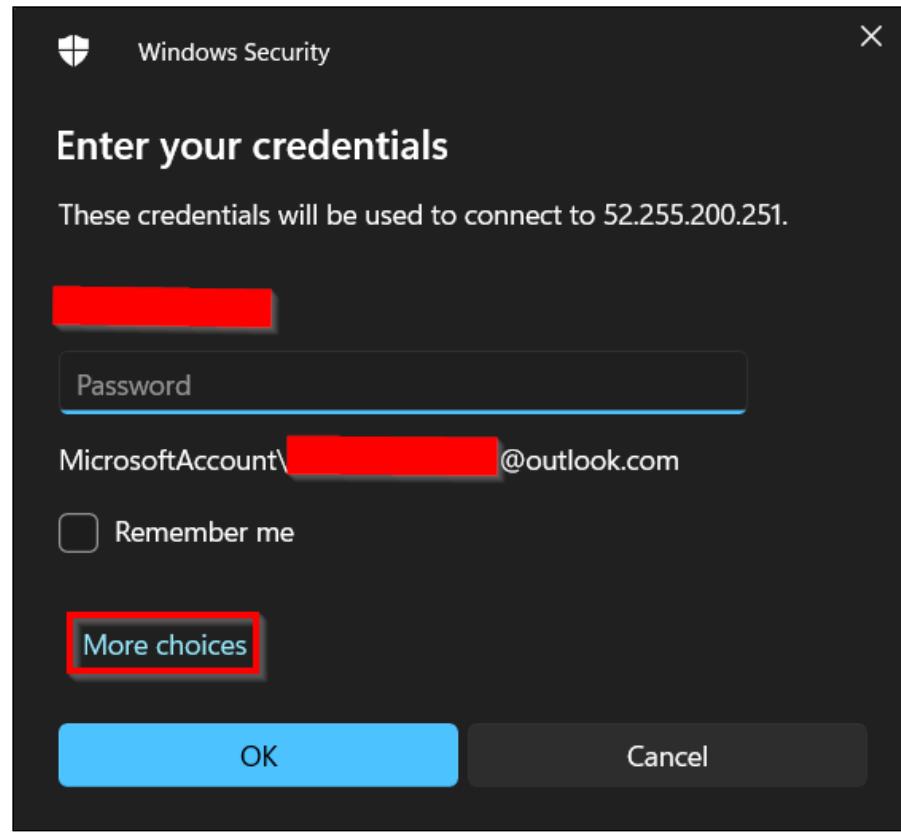
3389

Download RDP File

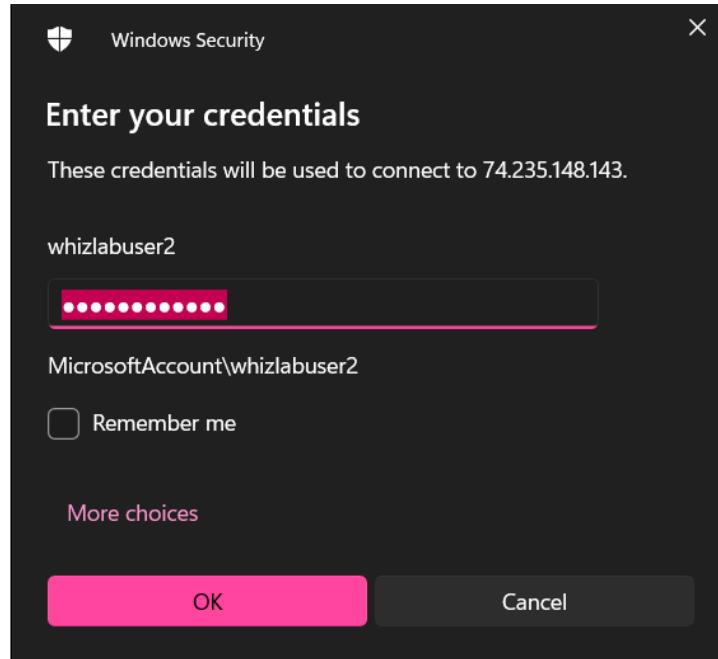
6. Open the download **RDP** file and select **Connect** on the displayed prompt.



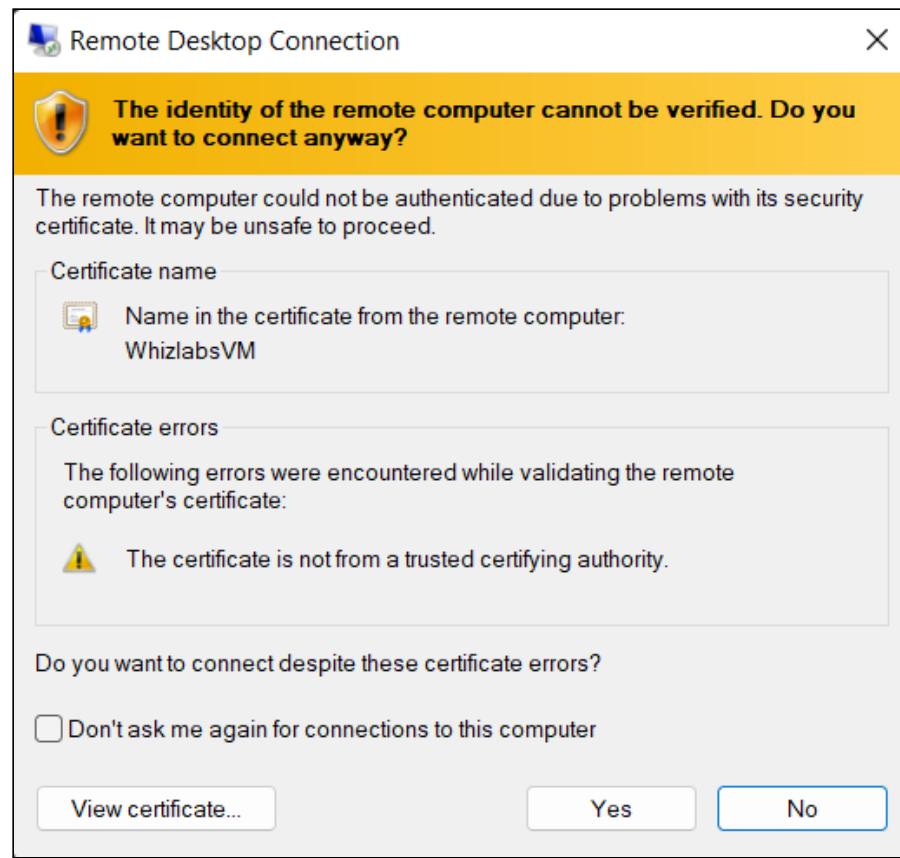
7. On the **Windows Security** prompt, click on **more choices**.



8. Click on **Use a different account** and enter the username and password you specified while creating the Virtual Machine and select **OK**.

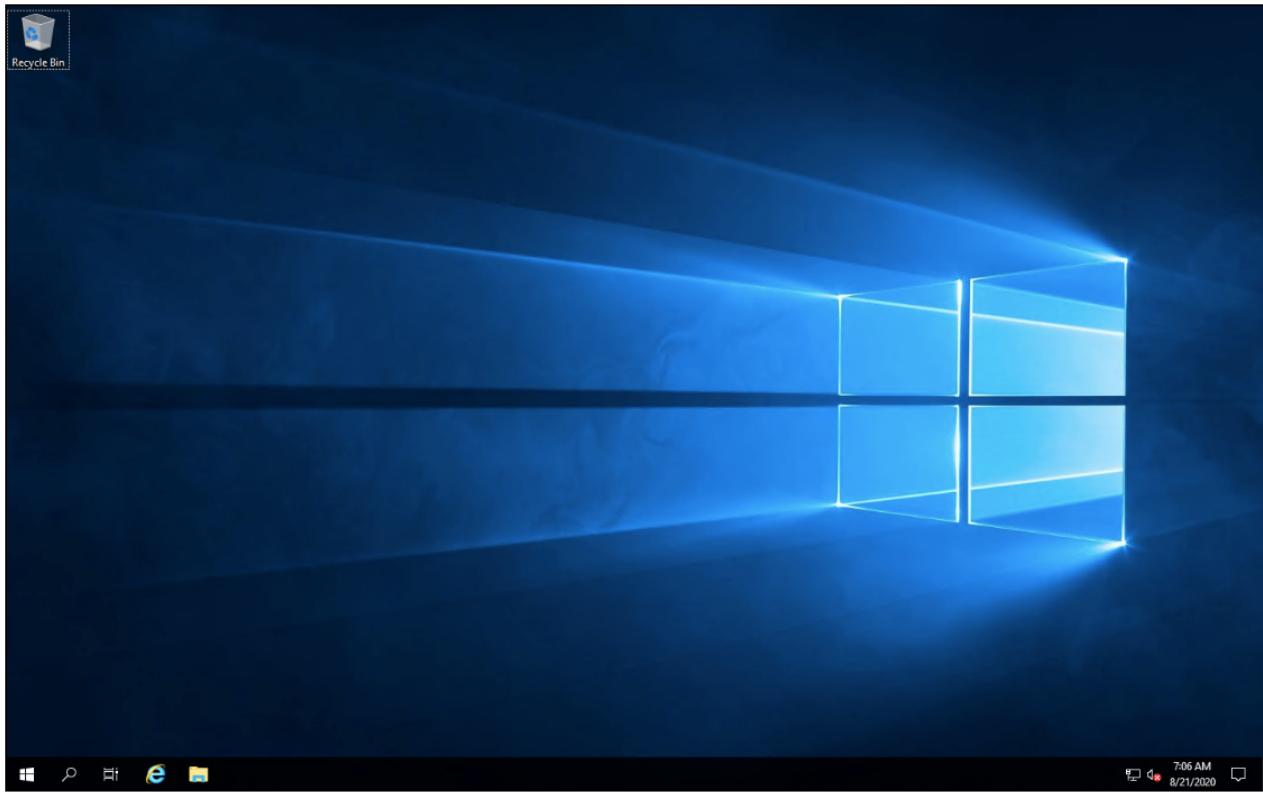


9. You may receive a certificate warning during the sign-in process. Select **Yes** to continue.

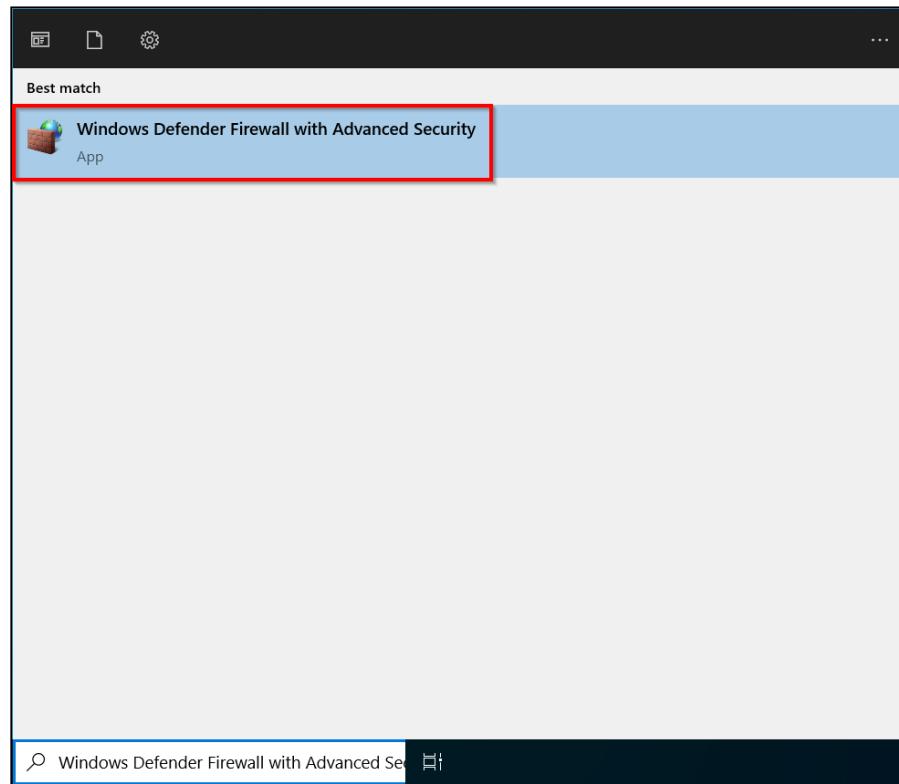


10. After successfully logging into the virtual machine, wait until the windows boots up and is ready to use.

- If you see this message **Do you want to allow your PC to be discoverable by other PCs and devices on this network?** Click on **Yes**
- Your Virtual Machine is ready to use
- A **Server Manager** window might open by default



11. Now, in your virtual environment, search for **Windows Defender Firewall with Advanced Security**.

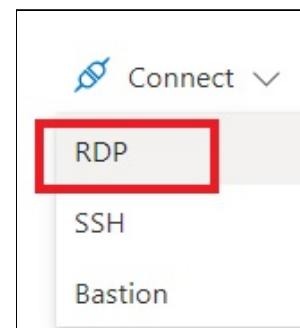


12. Open it and click on **Inbound rules**. Enable the following ICMP rules.

Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol
Core Networking - Neighbor Discovery A...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6
Core Networking - Neighbor Discovery So...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6
Core Networking - Packet Too Big (ICMPv...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6
Core Networking - Parameter Problem (IC...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6
Core Networking - Router Advertisement (...	Core Networking	All	Yes	Allow	No	System	Any	fe80:/64	ICMPv6
Core Networking - Router Solicitation (IC...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6
Core Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow	No	%System%	Any	Any	UDP
Core Networking - Time Exceeded (ICMPv...	Core Networking	All	Yes	Allow	No	System	Any	Any	ICMPv6
Core Networking Diagnostics - ICMP Echo...	Core Networking Diagnostics	Domain	No	Allow	No	System	Any	Any	ICMPv4
Core Networking Diagnostics - ICMP Echo...	Core Networking Diagnostics	Private...	No	Allow	No	System	Any	Local subnet	ICMPv4
Core Networking Diagnostics - ICMP Echo...	Core Networking Diagnostics	Private...	No	Allow	No	System	Any	Local subnet	ICMPv6
Core Networking Diagnostics - ICMP Echo...	Core Networking Diagnostics	Domain	No	Allow	No	System	Any	Any	ICMPv6
Delivery Optimization (TCP-In)	Delivery Optimization	All	Yes	Allow	No	%System%	Any	Any	TCP
Delivery Optimization (UDP-In)	Delivery Optimization	All	Yes	Allow	No	%System%	Any	Any	UDP
Desktop App Web Viewer	Desktop App Web Viewer	All	Yes	Allow	No	Any	Any	Any	Any
DIAL protocol server (HTTP-In)	DIAL protocol server	Domain	Yes	Allow	No	System	Any	Any	TCP
DIAL protocol server (HTTP-In)	DIAL protocol server	Private	Yes	Allow	No	System	Any	Local subnet	TCP
Distributed Transaction Coordinator (RPC)	Distributed Transaction Coor...	All	No	Allow	No	%System%	Any	Any	TCP
Distributed Transaction Coordinator (RPC-...	Distributed Transaction Coor...	All	No	Allow	No	%System%	Any	Any	TCP
Distributed Transaction Coordinator (TCP-I...	Distributed Transaction Coor...	All	No	Allow	No	%System%	Any	Any	TCP
File and Printer Sharing (Echo Request - IC...	File and Printer Sharing	All	Yes	Allow	No	System	Any	Any	ICMPv4
File and Printer Sharing (Echo Request - IC...	File and Printer Sharing	All	Yes	Allow	No	System	Any	Any	ICMPv6
File and Printer Sharing (LLMNR-UDP-In)	File and Printer Sharing	All	No	Allow	No	%System%	Any	Local subnet	UDP
File and Printer Sharing (NB-Datagram-In)	File and Printer Sharing	All	No	Allow	No	System	Any	Any	UDP
File and Printer Sharing (NB-Name-In)	File and Printer Sharing	All	No	Allow	No	System	Any	Any	UDP
File and Printer Sharing (NB-Session-In)	File and Printer Sharing	All	No	Allow	No	System	Any	Any	TCP
File and Printer Sharing (SMB-In)	File and Printer Sharing	All	No	Allow	No	System	Any	Any	TCP
File and Printer Sharing (Spooler Service - ...	File and Printer Sharing	All	No	Allow	No	%System%	Any	Any	TCP

13. Now, close the **vm2** session and return to Azure portal.

14. Now, go to your **vm1**, select **RDP** and click on **Download RDP File** button.



NOTE: If you are a **Linux** or **MAC** user:

- Download the [RDP software](#) and install it.
- Once installed, open the software and click on **Add PC**.
- Connect to your virtual machine using its public IP address and click on **Add**.
- Right click and open the PC, Enter **username** and **password** in the popup and click on continue on all further popups.

[RDP](#) [SSH](#) [Bastion](#)

Connect with RDP

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

IP address *

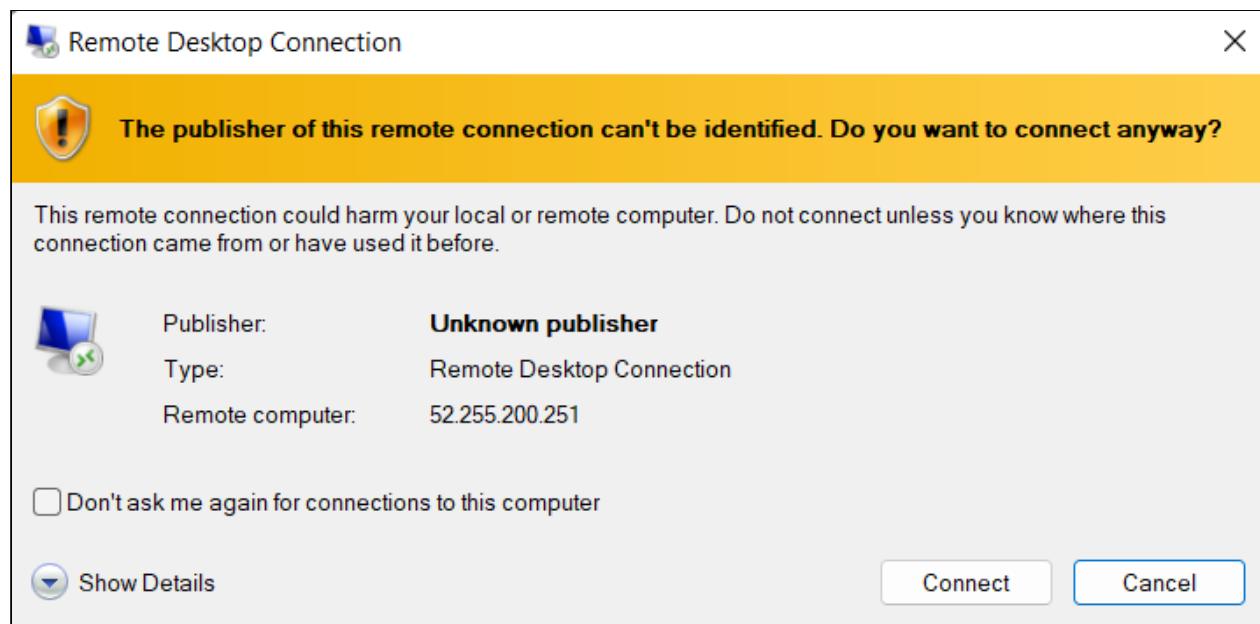
Public IP address (52.255.200.251)

Port number *

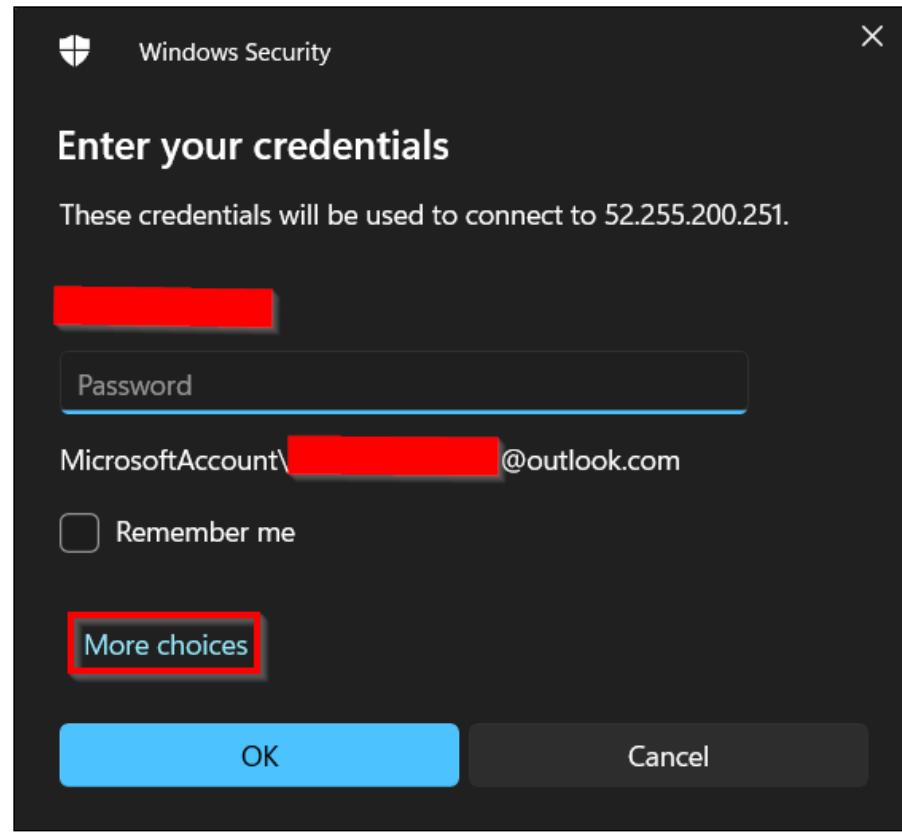
3389

Download RDP File

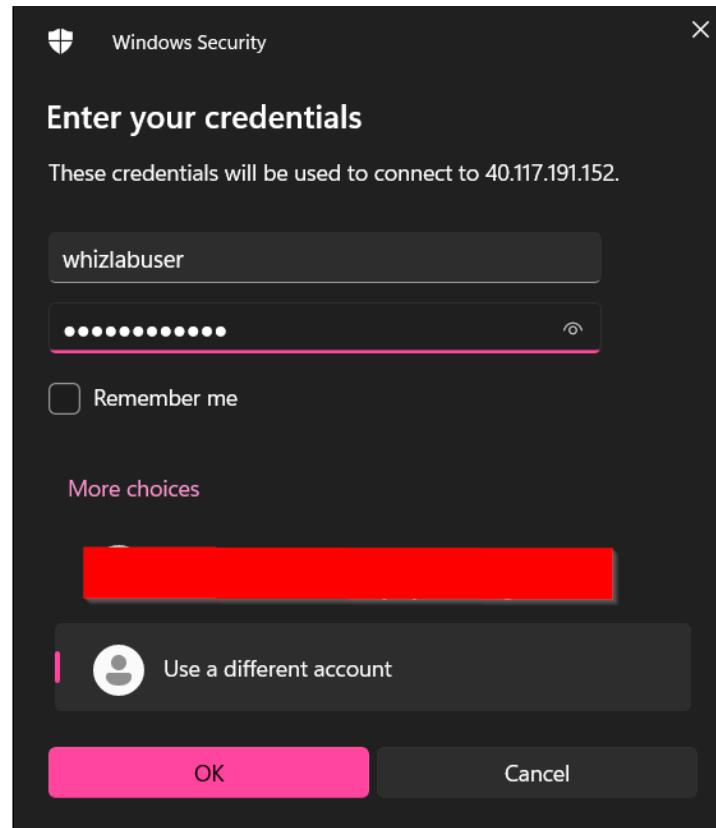
15. Open the download **RDP** file and select **Connect** on the displayed prompt.



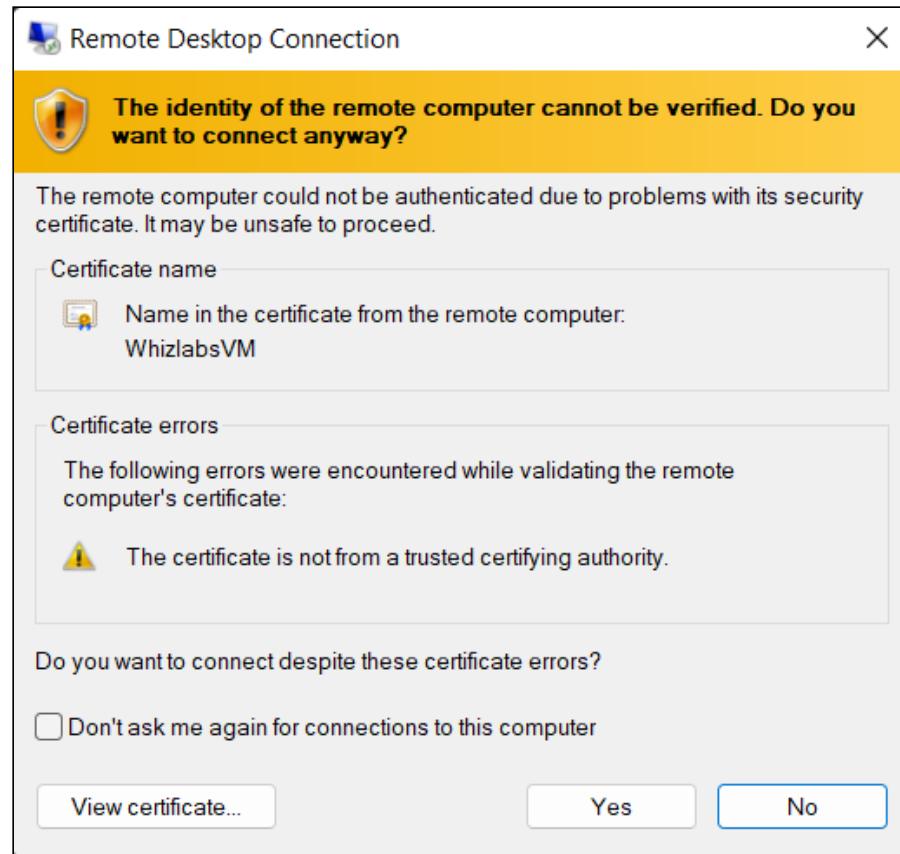
16. On the **Windows Security** prompt, click on **more choices**.



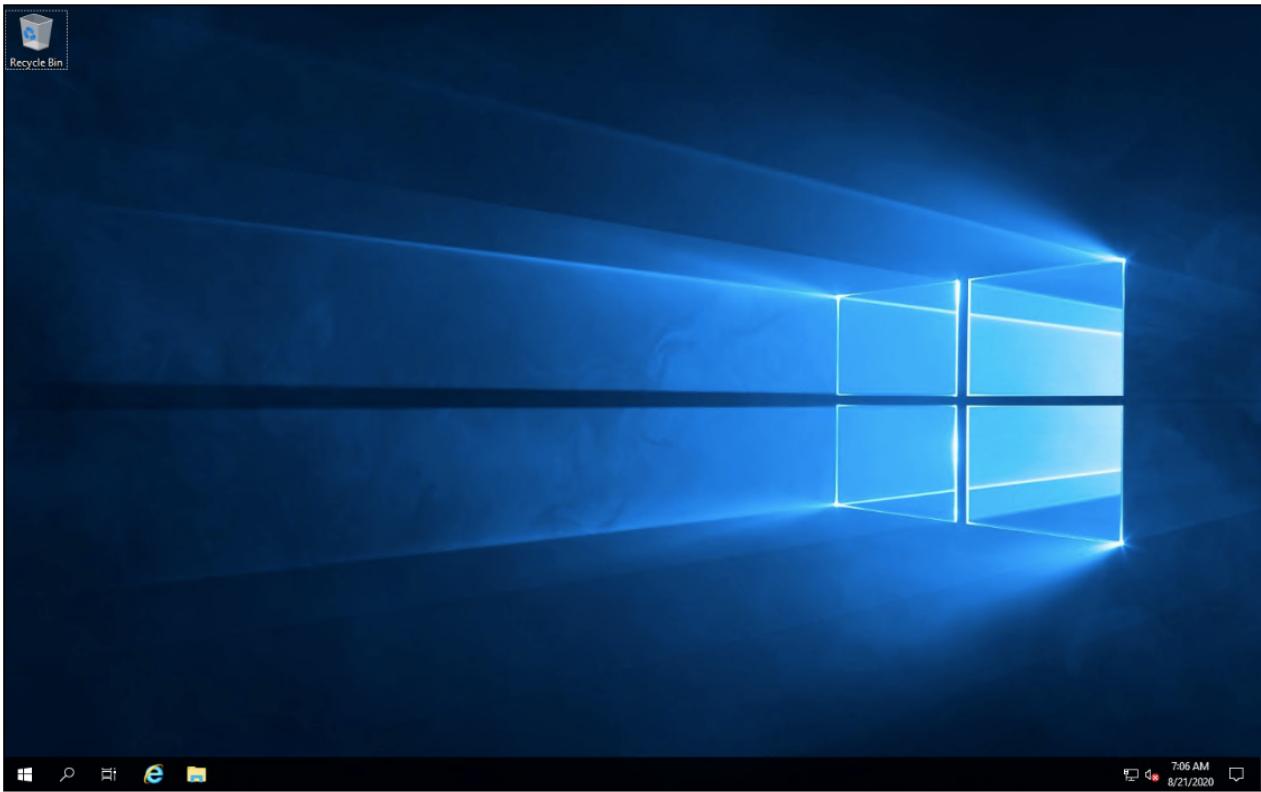
17. Click on **Use a different account** and enter the username and password you specified while creating the Virtual Machine and select **OK**.



18. You may receive a certificate warning during the sign-in process. Select **Yes** to continue.



19. After successfully logging into the virtual machine, wait until the windows boots up and is ready to use.
20. If you see this message **Do you want to allow your PC to be discoverable by other PCs and devices on this network?** Click on **Yes**
21. Your Virtual Machine is ready to use.



22. Now, on the virtual environment which is created for **vm1**, open up **Windows Powershell** and make sure to **run it as administrator**.

23. Try to ping **vm2** by running the command **ping vm2**.

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

PS C:\Users\azureuser> ping vm2

Pinging vm2.oo3aumt3ejhejf0dilwku4o1ne.bx.internal.cloudapp.net [10.0.0.6] with 32 bytes of data:
Reply from 10.0.0.6: bytes=32 time=2ms TTL=128
Reply from 10.0.0.6: bytes=32 time=1ms TTL=128
Reply from 10.0.0.6: bytes=32 time=1ms TTL=128
Reply from 10.0.0.6: bytes=32 time=1ms TTL=128

Ping statistics for 10.0.0.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
PS C:\Users\azureuser>
```

24. You successfully pinged VM2 from VM1.

Task 5: Validation test

- Once the lab steps are completed, click on **Validation** button or go to **Lab Validation** section.
- Click on **Validate My Lab** button. You will get the "**Lab Overall Status**" which will indicate whether or not you have completed the lab successfully.
- Sample output:

Create a Virtual Network

Level: Fundamental

Lab Overview Lab Steps Lab Validation

Azure Administrator Associate

Lab Steps

Task 1: Sign in to Azure Portal

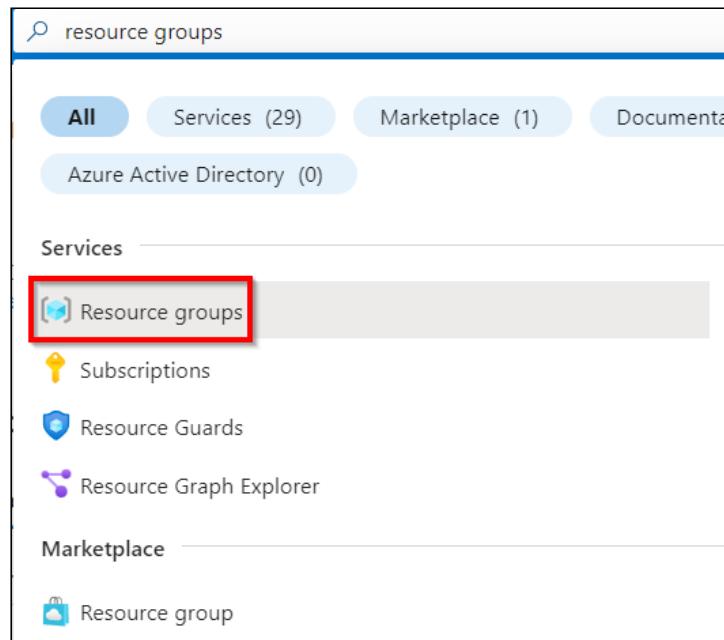
1. Go to the Azure portal by clicking on the **Open Console** button or by using URL <https://portal.azure.com>.

- **Note:** It is recommended to use incognito mode to avoid Azure portal cache related issues.
- 2. If it automatically logs into any other azure account, please logout of it and clear cache.
- 3. Sign in with your given **username** and **password** on Azure portal.
- 4. If login is not working. Click on **End Lab** and start the lab again.

Task 6: Delete the Resources

In this task, we will delete all the resources.

1. In the search box at the top of the Azure portal, enter **Resource groups**. Select **Resource groups** from the search results.



2. Click on the name of the **Resource groups**.

The screenshot shows the 'Resource groups' blade in the Azure portal. It displays one record: 'rg_eastus_1'. The 'Name' column has a red box around it, indicating it's the target for selection. The 'Subscription' and 'Location' columns show 'Pay-As-You-Go' and 'East US' respectively.

3. Select all the Resources in that **Resource groups**.

The screenshot shows the 'Resources' blade in the Azure portal. It lists several resources under the 'rg_eastus_1' resource group. The 'Name' column is sorted by name and has a red box around it, indicating it's the target for selection. Other columns include 'Type', 'Location', and a 'Status' column at the bottom.

Name	Type	Location	Status
vm1	Virtual machine	East US	
vm1-ip	Public IP address	East US	
vm1-nsg	Network security group	East US	
vm1769	Network Interface	East US	
vm1_OsDisk_1_43c0ecd81e314535b5799f0d2898c3a3	Disk	East US	
vm2	Virtual machine	East US	
vm2-ip	Public IP address	East US	

4. Go to three dots to the right and then click **Delete** button.

The screenshot shows the 'Resources' blade in the Azure portal. It lists two records. On the far right, there is a context menu with several options: 'Move', 'Delete', 'Export template', and 'Open in mobile'. The 'Delete' option is highlighted with a red box.

5. Now type **delete** in the box present at the bottom.

Delete Resources

The selected resources along with their related resources and contents will be permanently deleted. If you are unsure of the selected resource dependencies, navigate to the individual resource page to perform the delete operation. More details of the resource dependencies are available in the manage experience.

Resources to be deleted (11)

Name	Resource type	
vm1	Virtual machine	Remove
vm1-ip	Public IP address	Remove
vm1-nsg	Network security gro...	Remove
vm1769	Network Interface	Remove
vm1_OsDisk_1_43c0ecd81e314535b5799f0d2898c3;	Disk	Remove
vm2	Virtual machine	Remove
vm2-ip	Public IP address	Remove
vm2-nsg	Network security gro...	Remove

Apply force delete for selected Virtual machines and Virtual machine scale sets

Enter "delete" to confirm deletion *

[Delete](#)[Cancel](#)

6. Click on **Delete** to confirm deletion of resources.

Delete confirmation

Deleting the selected resources and their internal data is a permanent action and cannot be undone.

[Delete](#)[Go back](#)

Completion and Conclusions

1. You have successfully signed into Azure Portal.
2. You have successfully created a virtual network.
3. You have successfully created virtual machines.
4. You have successfully tested the connection.
5. You have successfully tested the validation.
6. You have successfully deleted the resources.

End Lab

1. You have successfully completed this lab.
2. Click on **Sign out** in Azure Portal by clicking on the logout button in the top right corner inside Azure Profile.
3. Click on **End Lab** once you have completed the Lab.

About Us Subscription Instructions and Guidelines FAQ's Contact Us

© 2023, Whizlabs Software Pvt. Ltd.

