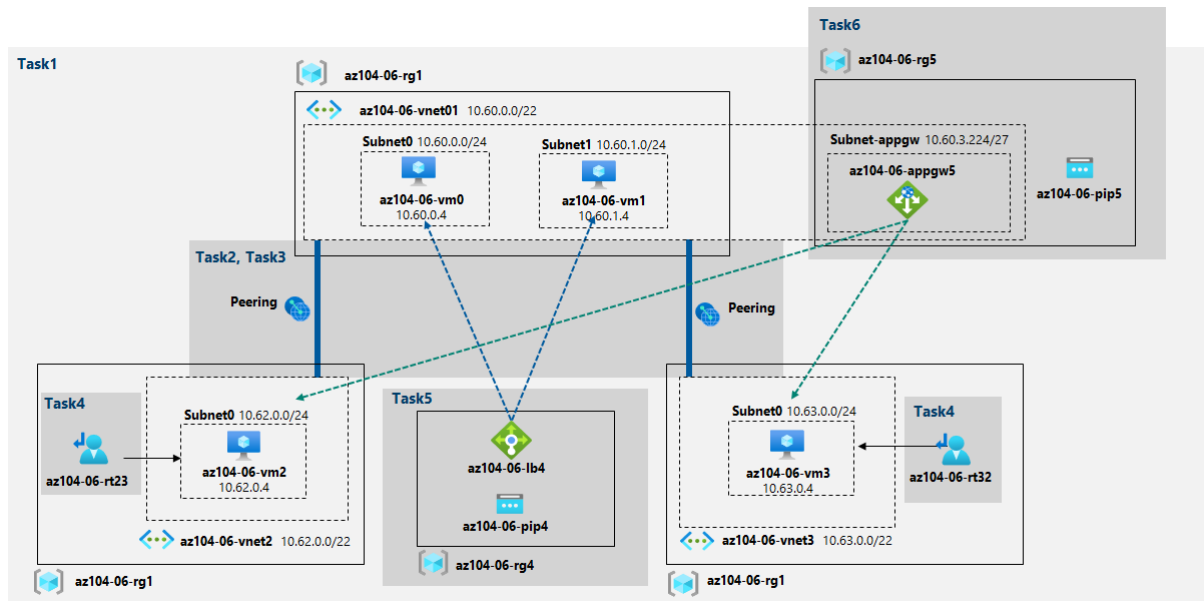
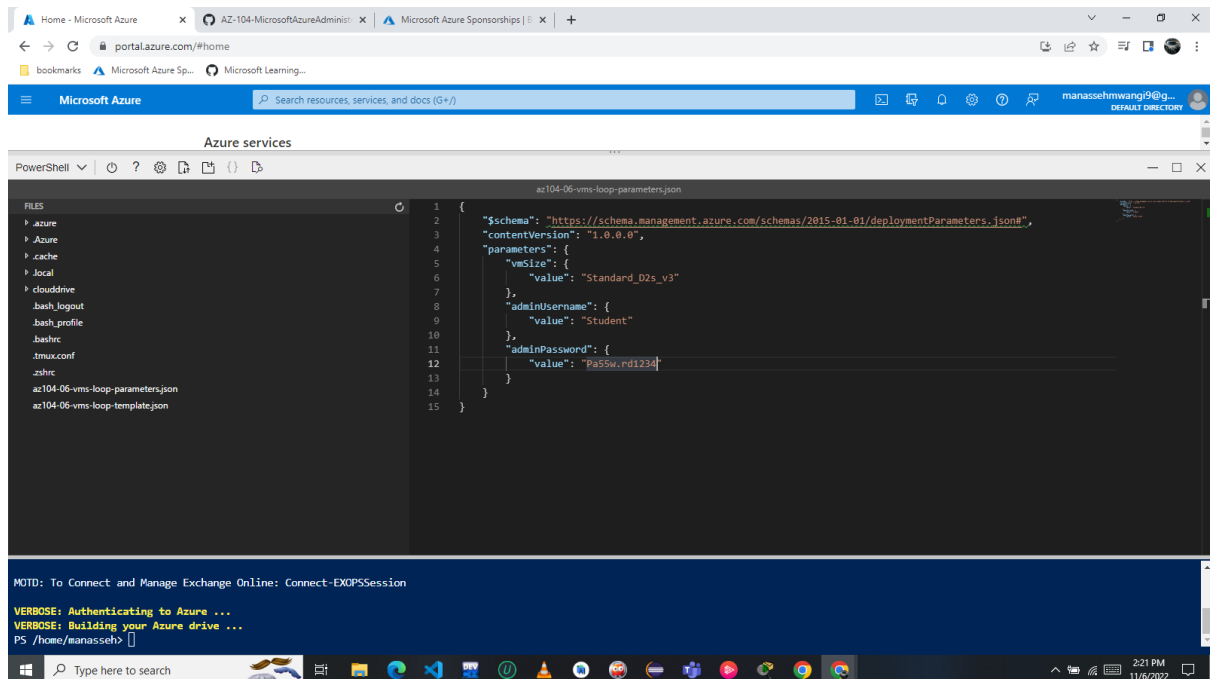


Lab 06 - Implement Traffic Management

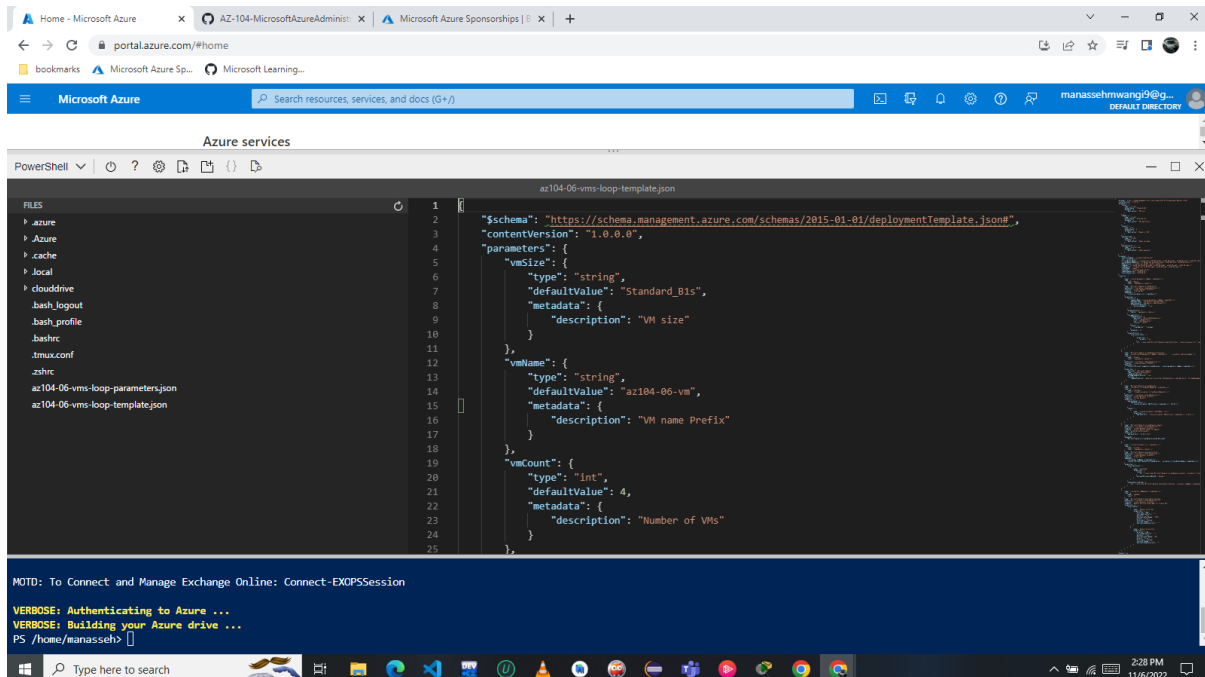
Architecture diagram



In the Azure portal, open the **Azure Cloud Shell**, upload **az104-06-vms-loop-template.json** and **z104-06-vms-loop-parameters.json** into the Cloud Shell home directory.



Edit the **Parameters** file you just uploaded and change the password. Edit the virtual machine to standard_B1s that uses VM size that requires only one vCPU



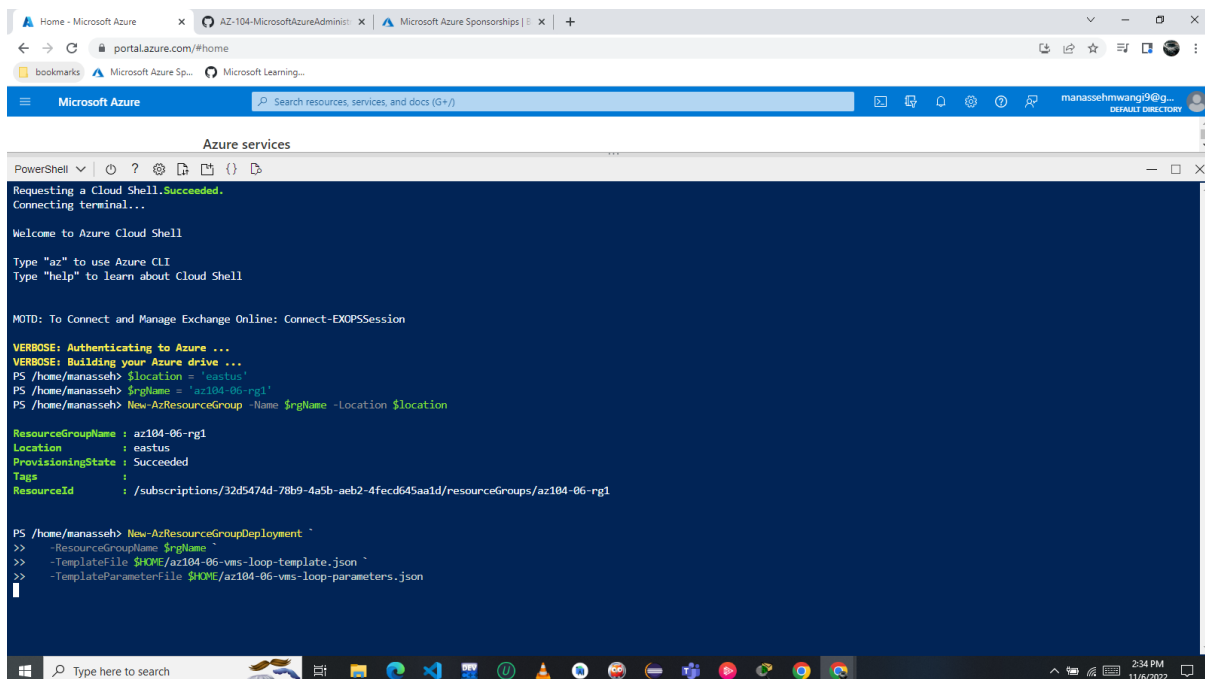
```
FILES
  > azure
  > Azure
  > .cache
  > .local
  > cloudrive
  > .bash_logout
  > .bash_profile
  > .bashrc
  > .tmux.conf
  > .zshrc
  > az104-06-vms-loop-parameters.json
  > az104-06-vms-loop-template.json

az104-06-vms-loop-template.json
1  {
2    "$schema": "https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json#",
3    "contentVersion": "1.0.0.0",
4    "parameters": {
5      "vmSize": {
6        "type": "string",
7        "defaultValue": "Standard_B1s",
8        "metadata": {
9          "description": "VM size"
10       }
11     },
12     "vmName": {
13       "type": "string",
14       "defaultValue": "az104-06-vm",
15       "metadata": {
16         "description": "VM name Prefix"
17       }
18     },
19     "vmCount": {
20       "type": "int",
21       "defaultValue": 4,
22       "metadata": {
23         "description": "Number of VMs"
24       }
25     }
26   }
```

From the Cloud Shell pane, run the following to create the first resource group

Replace the '[Azure region]' placeholder with the name of an Azure region 'East US' where you intend to deploy Azure virtual machines.

Then the resource group name: And finally create the resource group in your desired location:



```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

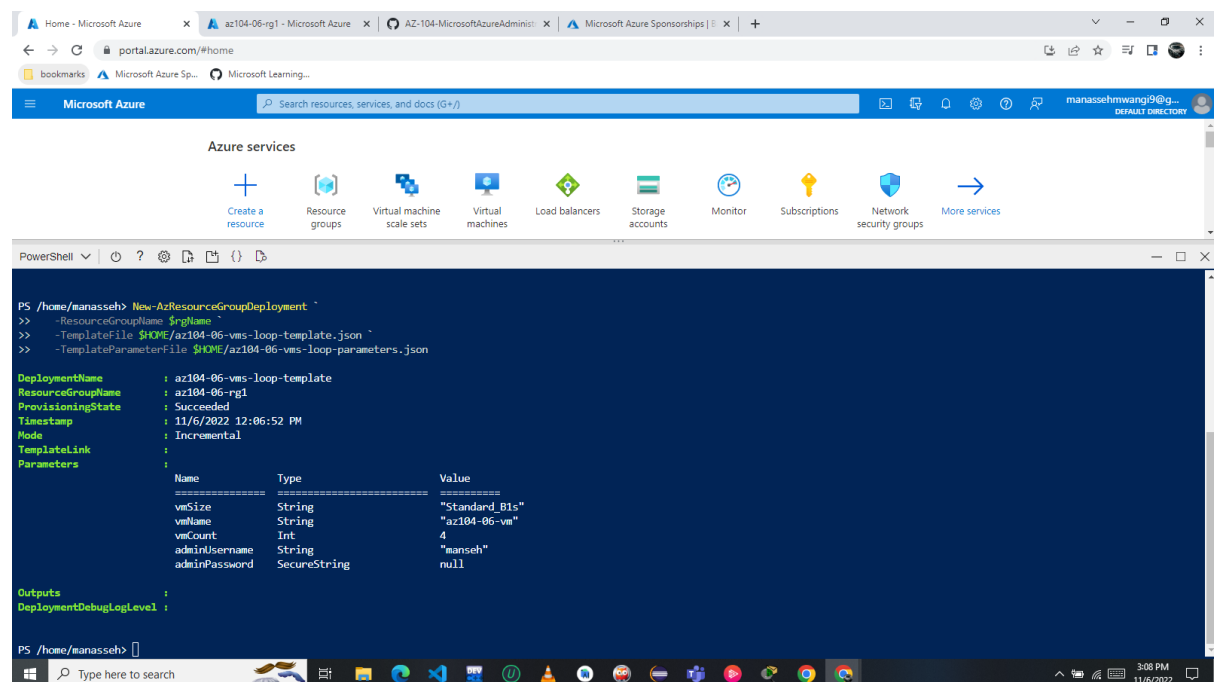
MOTD: To Connect and Manage Exchange Online: Connect-EXOPSSession

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/manasseh> $location = 'eastus'
PS /home/manasseh> $rgName = 'az104-06-rg1'
PS /home/manasseh> New-AzResourceGroup -Name $rgName -Location $location

ResourceGroupName : az104-06-rg1
Location           : eastus
ProvisioningState   : Succeeded
Tags               :
ResourceId          : /subscriptions/32d5474d-78b9-4a5b-aeb2-4fec645a1d/resourceGroups/az104-06-rg1

PS /home/manasseh> New-AzResourceGroupDeployment `
>> -ResourceGroupName $rgName `
>> -TemplateFile $HOME/az104-06-vms-loop-template.json `
>> -TemplateParameterFile $HOME/az104-06-vms-loop-parameters.json
```

Run the following to create the three virtual networks and four Azure VMs into them by using the template and parameter files you uploaded:



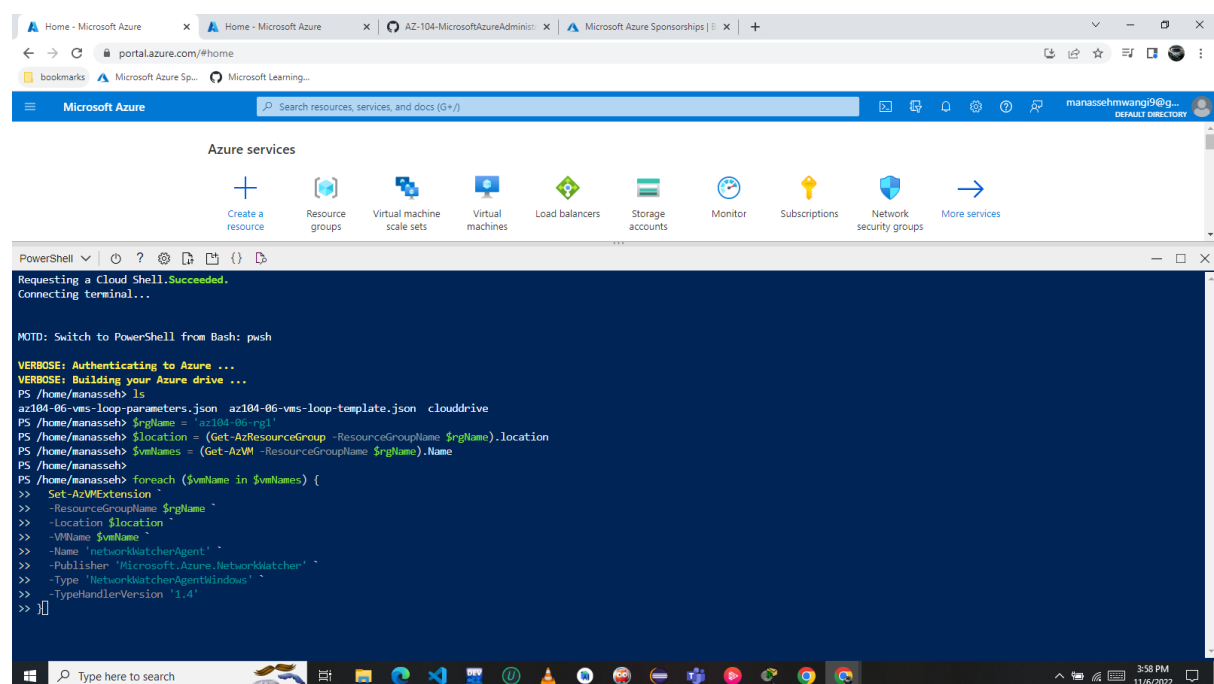
The screenshot shows the Microsoft Azure portal interface with a PowerShell terminal window open. The terminal displays the command to create a new resource group deployment and the resulting output, which includes details about the deployment and the parameters used.

```
PS /home/manasseh> New-AzResourceGroupDeployment `
>> -ResourceGroupName $rgName `
>> -TemplateFile $HOME/az104-06-vms-loop-template.json `
>> -TemplateParameterFile $HOME/az104-06-vms-loop-parameters.json

DeploymentName      : az104-06-vms-loop-template
ResourceGroupName   : az104-06-rg1
ProvisioningState    : Succeeded
Timestamp           : 11/6/2022 12:06:52 PM
Mode                : Incremental
TemplateLink         :
Parameters           :
=====
Name                Type                Value
-----
vmSize              String              "Standard_B1s"
vmName              String              "az104-06-vm"
vmCount             Int                4
adminUsername        String              "manseh"
adminPassword        SecureString         null

Outputs
DeploymentDebugLogLevel :
```

Run the following to install the Network Watcher extension on the Azure VMs deployed in the previous step:



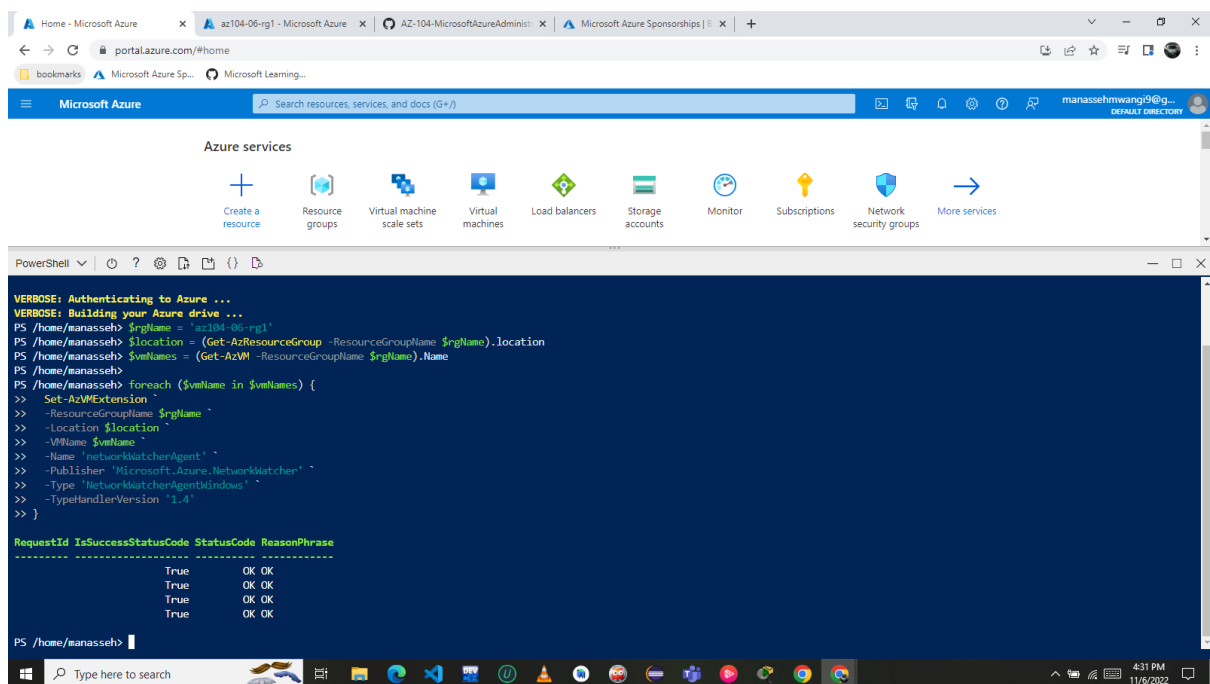
The screenshot shows the Microsoft Azure portal interface with a PowerShell terminal window open. The terminal displays the command to install the Network Watcher extension on the Azure VMs deployed in the previous step.

```
Requesting a Cloud Shell.Succeeded.
Connecting terminal...

MOTD: Switch to PowerShell from Bash: pwsh

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
PS /home/manasseh> ls
az104-06-vms-loop-parameters.json az104-06-vms-loop-template.json clouddrive
PS /home/manasseh> $rgName = 'az104-06-rg1'
PS /home/manasseh> $location = (Get-AzResourceGroup -ResourceGroupName $rgName).Location
PS /home/manasseh> $vmNames = (Get-AzVM -ResourceGroupName $rgName).Name
PS /home/manasseh>
PS /home/manasseh> foreach ($vmName in $vmNames) {
>> Set-AzVMExtension `
>> -ResourceGroupName $rgName `
>> -Location $location `
>> -VMName $vmName `
>> -Name 'networkwatcheragent' `
>> -Publisher 'Microsoft.Azure.NetworkWatcher' `
>> -Type 'NetworkWatcherAgentWindows' `
>> -TypeHandlerVersion '1.4'
>> }
PS /home/manasseh>
```

Wait for the deployment to complete before proceeding to the next step



Task 2: Configure the hub and spoke network topology

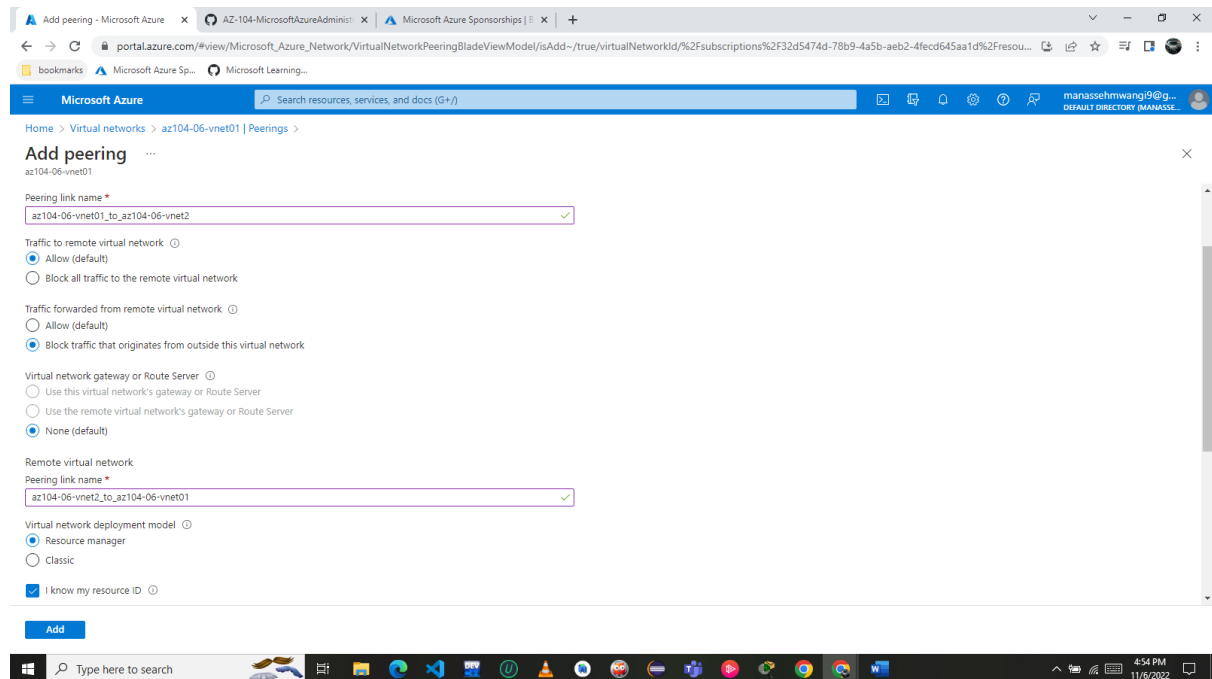
In this task, you will configure local peering between the virtual networks you deployed in the previous tasks in order to create a hub and spoke network topology.

Now examine the vnets and take note of their properties

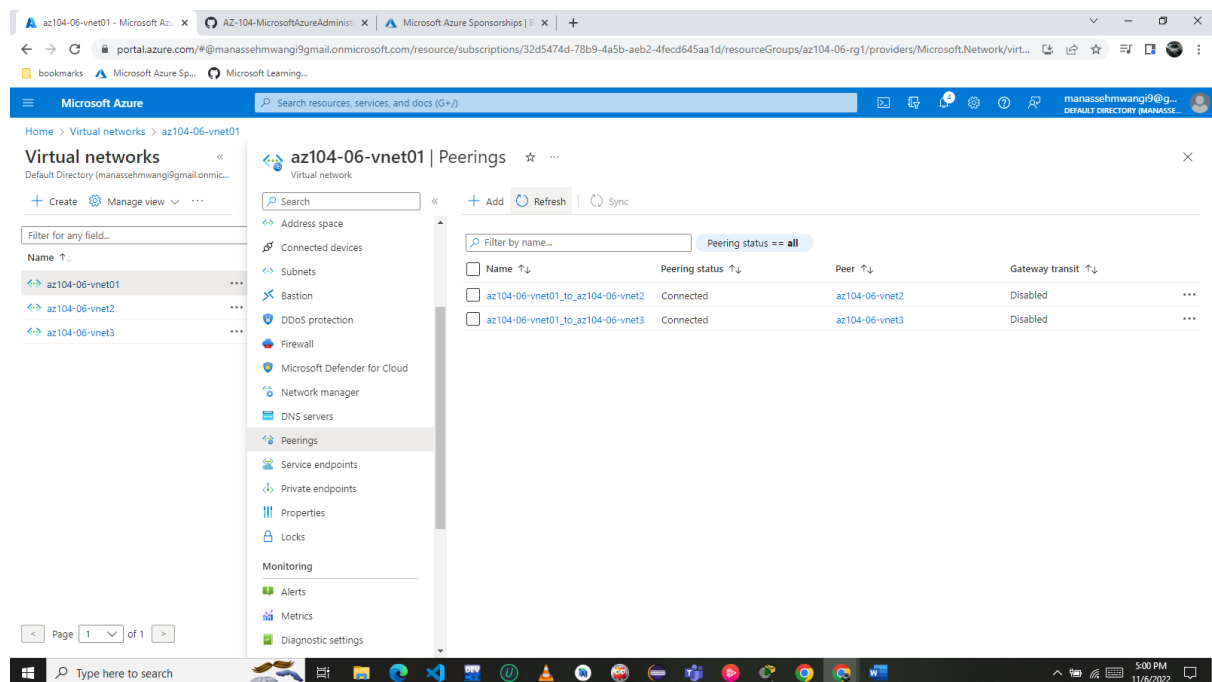
Vnet 01 IP	10.60.0.0/22
Vnet 01 resource ID	/subscriptions/32d5474d-78b9-4a5b-aeb2-4fec645aa1d/resourceGroups/az104-06-rg1/providers/Microsoft.Network/virtualNetworks/az104-06-vnet01
Vnet 02 IP	10.62.0.0/22
Vnet 02 resource ID	/subscriptions/32d5474d-78b9-4a5b-aeb2-4fec645aa1d/resourceGroups/az104-06-rg1/providers/Microsoft.Network/virtualNetworks/az104-06-vnet2
Vnet 03 IP	10.63.0.0/22
Vnet 03 resource ID	/subscriptions/32d5474d-78b9-4a5b-aeb2-4fec645aa1d/resourceGroups/az104-06-rg1/providers/Microsoft.Network/virtualNetworks/az104-06-vnet3

On the **az104-06-vnet01** virtual network blade, click **Peerings** and then click **+ Add**.

This step establishes two local peerings - one from az104-06-vnet01 to az104-06-vnet2 and the other from az104-06-vnet2 to az104-06-vnet01



Repeat the above procedure and this step establishes two local peerings - one from az104-06-vnet01 to az104-06-vnet3 and the other from az104-06-vnet3 to az104-06-vnet01. This completes setting up the hub and spoke topology (with two spoke virtual networks).



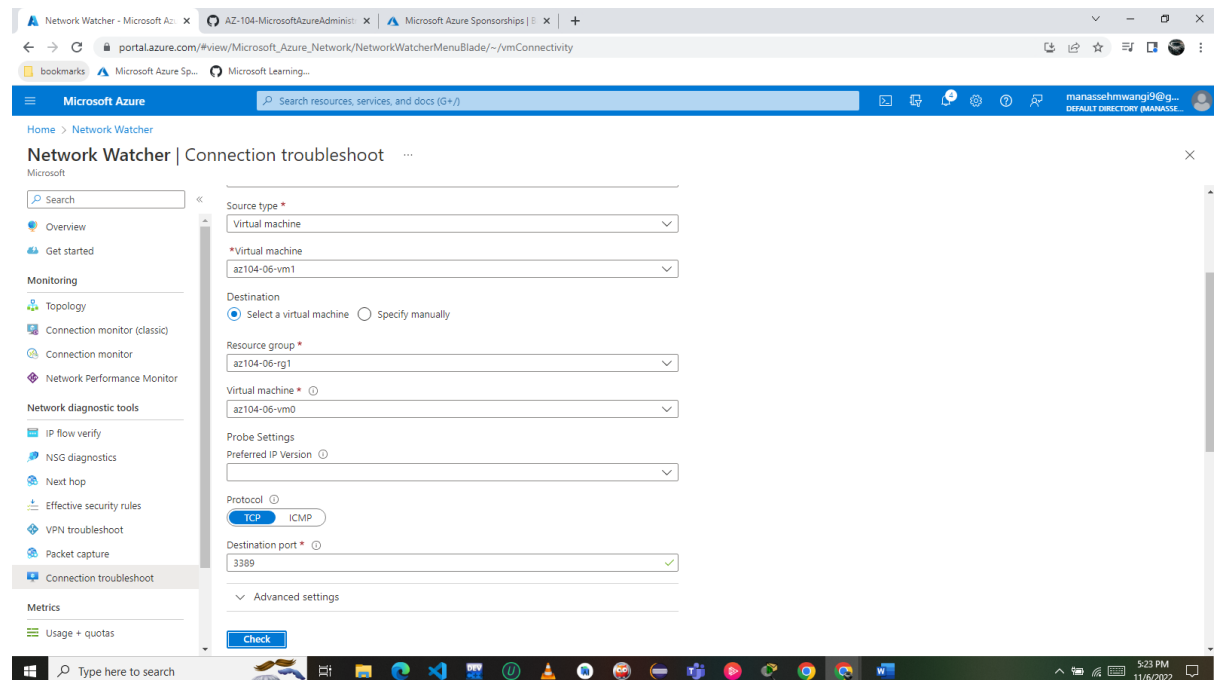
Task 3: Test transitivity of virtual network peering

In this task, you will test transitivity of virtual network peering by using Network Watcher.

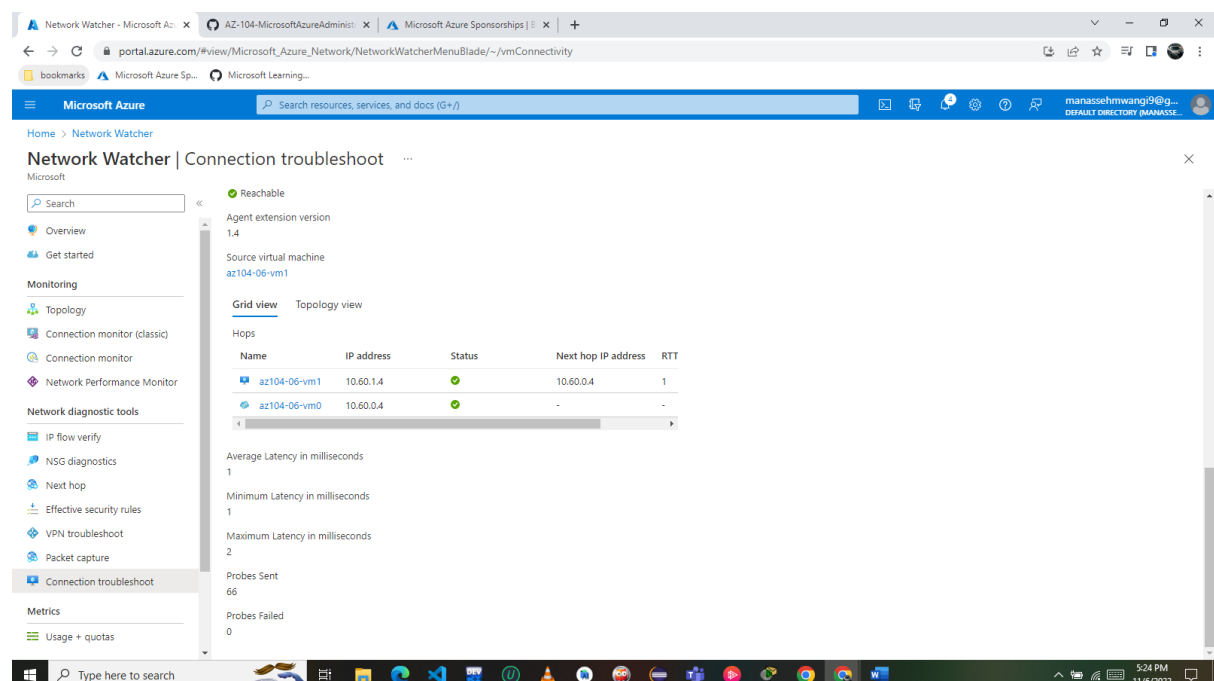
On the **Network Watcher** blade, navigate to the **Connection troubleshoot**.

Note: **10.62.0.4** represents the private IP address of **az104-06-vm2**

One can either the drop down to select the vms or manually key in ip address



From az104-06vm1 the status of vm0 is **Reachable**, since the hub virtual network is peered directly with the first spoke virtual network.



10.63.0.4 represents the private IP address of **az104-06-vm3**

From vm0 the status of vm3 is **Reachable**, the connection was direct, with no intermediate hops in between the VMs.

The screenshot shows the 'Network Watcher | Connection troubleshoot' page in the Azure portal. The left sidebar contains navigation links for Overview, Get started, Monitoring (Topology, Connection monitor, Network Performance Monitor), Network diagnostic tools (IP flow verify, NSG diagnostics, Next hop, Effective security rules, VPN troubleshoot, Packet capture, Connection troubleshoot), Metrics, and Usage + quotas. The main area is titled 'Network Watcher | Connection troubleshoot' and includes a search bar and a 'Learn more' link. Below this, the configuration form is displayed with the following fields: Subscription (Azure Pass - Sponsorship), Resource group (az104-06-rg1), Source type (Virtual machine), Virtual machine (az104-06-vm0), Destination (Specify manually), URI, FQDN or IP address (10.63.0.4), Protocol (TCP), and Destination port (3389).

The screenshot shows the 'Network Watcher | Connection troubleshoot' page displaying the results of a connection test. The status is 'Reachable'. The agent extension version is 1.4. The source virtual machine is az104-06-vm0. The results are shown in a table with columns: Name, IP address, Status, Next hop IP address, and RTT. The table shows two hops: az104-06-vm0 (10.60.0.4) and az104-06-nic3 (10.63.0.4). The average latency is 1 millisecond, minimum latency is 1 millisecond, and maximum latency is 3 milliseconds. The number of probes sent is 66, and the number of probes failed is 0.

Name	IP address	Status	Next hop IP address	RTT
az104-06-vm0	10.60.0.4	Reachable	10.63.0.4	1
az104-06-nic3	10.63.0.4	Reachable	-	-

10.63.0.4 represents the private IP address of az104-06-vm3

Network Watcher | Connection troubleshoot

Search

Overview

Get started

Monitoring

Topology

Connection monitor (classic)

Connection monitor

Network Performance Monitor

Network diagnostic tools

IP flow verify

NSG diagnostics

Next hop

Effective security rules

VPN troubleshoot

Packet capture

Connection troubleshoot

Metrics

Usage + quotas

Network Watcher Connection Troubleshoot provides the capability to check a direct TCP connection from a virtual machine (VM) to a VM, fully qualified domain name (FQDN), URI, or IP4 address. To start, choose a source to start the connection from, and the destination you wish to connect to and select "Check". [Learn more.](#)

Source

Subscription *

Resource group *

Source type *

*Virtual machine

Destination

☐ Select a virtual machine ☒ Specify manually

URI, FQDN or IP address *

Probe Settings

Protocol

Destination port *

From vm2 the status of vm3 is **Unreachable**. This is expected, since the two spoke virtual networks are not peered with each other (virtual network peering is not transitive).

Network Watcher | Connection troubleshoot

Search

Overview

Get started

Monitoring

Topology

Connection monitor (classic)

Connection monitor

Network Performance Monitor

Network diagnostic tools

IP flow verify

NSG diagnostics

Next hop

Effective security rules

VPN troubleshoot

Packet capture

Connection troubleshoot

Metrics

Usage + quotas

Advanced settings

Check

Status

Unreachable

Agent extension version

1.4

Source virtual machine

az104-06-vm2

Grid view Topology view

Hops

Name	IP address	Status	Next hop IP address	RTT
az104-06-vm2	10.62.0.4	Unreachable	10.63.0.4	-
Destination (10.63.0.4)	10.63.0.4	Reachable	-	-

Probes Sent

30

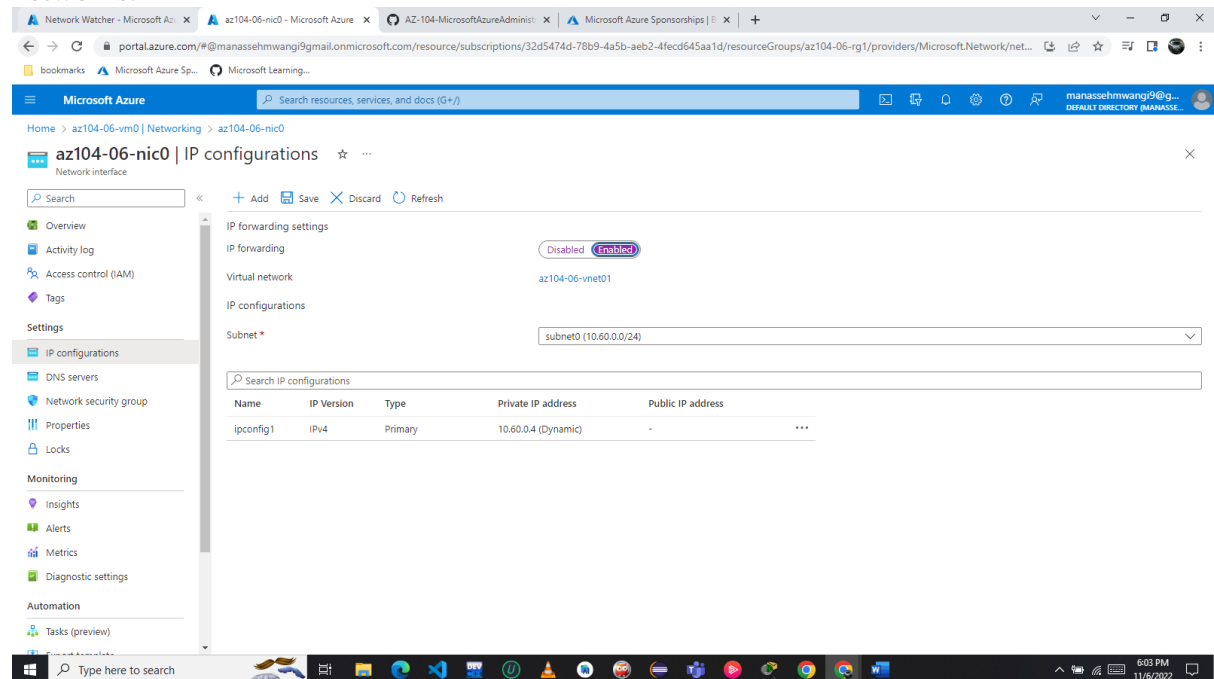
Probes Failed

30

Task 4: Configure routing in the hub and spoke topology

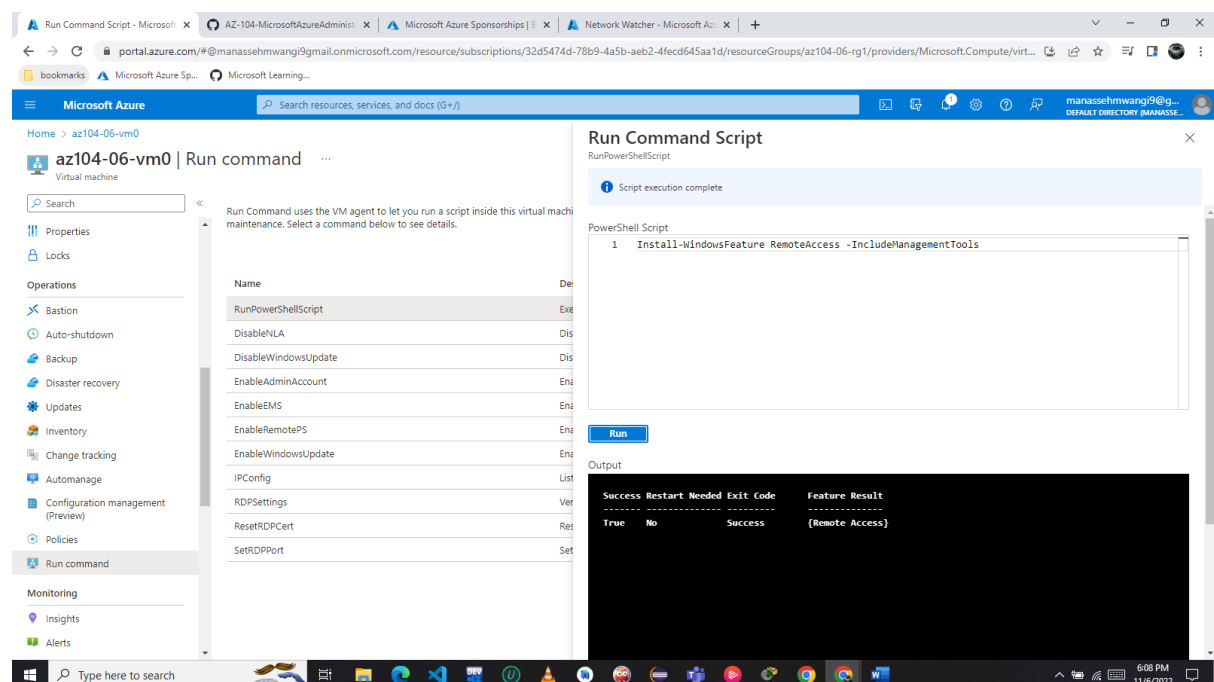
In this task, you will configure and test routing between the two spoke virtual networks by enabling IP forwarding on the network interface of the **az104-06-vm0** virtual machine, enabling routing within its operating system, and configuring user-defined routes on the spoke virtual network.

Set **IP forwarding** to **Enabled** and save the change. This setting is required in order for **az104-06-vm0** to function as a router, which will route traffic between two spoke virtual networks.



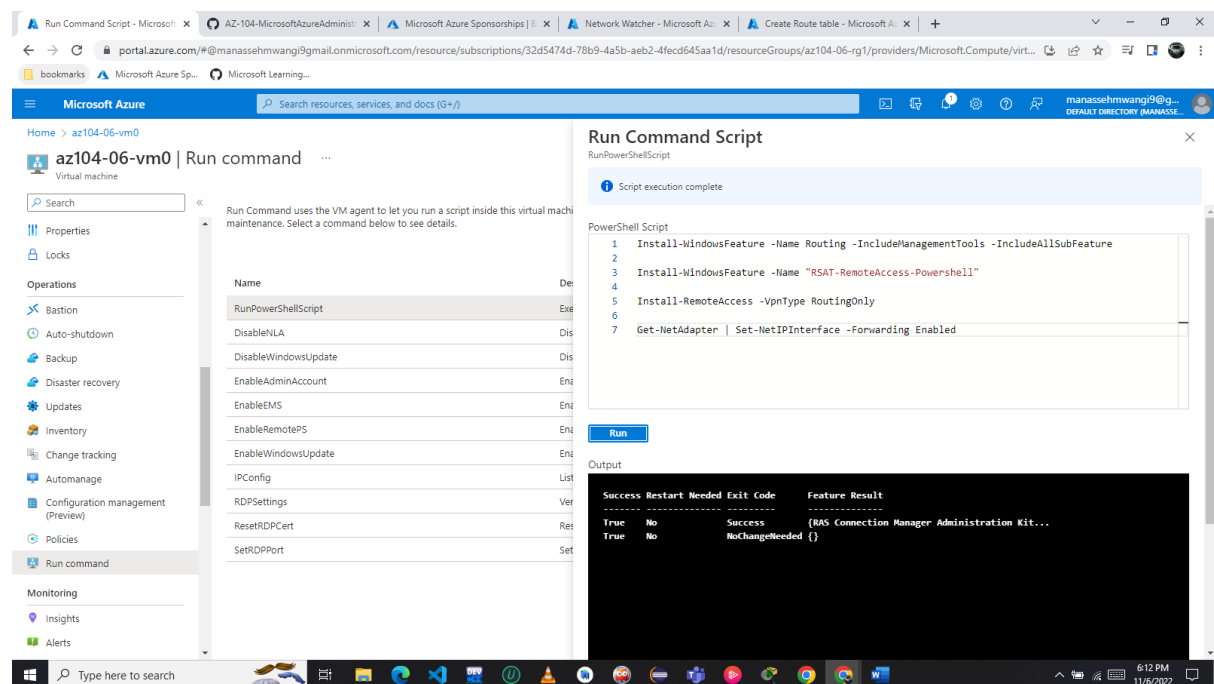
The screenshot shows the Microsoft Azure portal interface for the **az104-06-nic0** network interface. The left sidebar contains navigation options like Overview, Activity log, Access control (IAM), Tags, Settings, IP configurations, DNS servers, Network security group, Properties, Locks, Monitoring, Insights, Alerts, Metrics, Diagnostic settings, Automation, and Tasks (preview). The main pane displays the **IP configurations** for **az104-06-nic0**. The **IP forwarding settings** section shows **IP forwarding** set to **Enabled** (indicated by a green pill). Below this, the **Virtual network** is set to **az104-06-vnet01** and the **Subnet** is **subnet0 (10.60.0.0/24)**. A table lists the IP configurations, showing one configuration named **ipconfig1** with **IPv4** type, **Primary** status, and a **Private IP address** of **10.60.0.4 (Dynamic)**. The **Public IP address** is listed as **-**.

On the **Run Command Script** blade to install the Remote Access Windows Server role.



The screenshot shows the Microsoft Azure portal interface for the **az104-06-vm0** virtual machine. The left sidebar contains navigation options like Properties, Locks, Operations, Bastion, Auto-shutdown, Backup, Disaster recovery, Updates, Inventory, Change tracking, Automate, Configuration management (Preview), Policies, Run command, Monitoring, Insights, and Alerts. The main pane displays the **Run command** blade. The **Run Command Script** blade shows a list of operations, including **RunPowerShellScript**, **DisableNLA**, **DisableWindowsUpdate**, **EnableAdminAccount**, **EnableEMS**, **EnableRemotePS**, **EnableWindowsUpdate**, **IPConfig**, **RDPSettings**, **ResetRDPcert**, and **SetRDPport**. The **RunPowerShellScript** operation is selected, and the script execution is shown as complete. The script executed is `1 Install-WindowsFeature RemoteAccess -IncludeManagementTools`. The output shows the success of the command, with a **Success** status and a **Feature Result** of **(Remote Access)**.

On the **Run Command Script** blade to install the Routing role service.



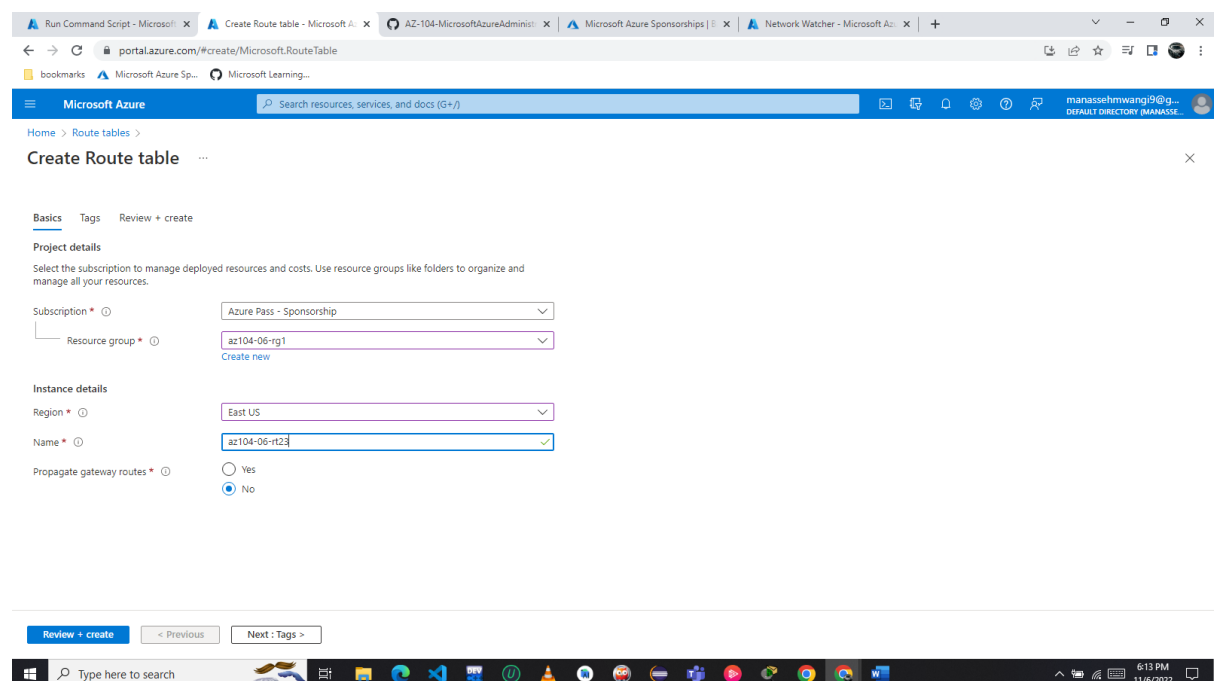
The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane is open, showing the 'Run command' option under the 'Operations' section. The main area displays the 'Run Command Script' blade for the virtual machine 'az104-06-vm0'. The blade shows a PowerShell script that has been executed successfully. The script includes the following commands:

```
1 Install-WindowsFeature -Name Routing -IncludeManagementTools -IncludeAllSubFeature
2
3 Install-WindowsFeature -Name "RSAT-RemoteAccess-Powershell"
4
5 Install-RemoteAccess -VpnType RoutingOnly
6
7 Get-NetAdapter | Set-NetIPInterface -Forwarding Enabled
```

The output of the script execution is displayed in a terminal window, showing the following results:

Success	Restart Needed	Exit Code	Feature	Result
True	No	Success	(RAS Connection Manager Administration Kit...	
True	No	NoChangeNeeded	{}	

In the Azure portal, search and select **Route tables** and click **+ Create**.



The screenshot shows the Microsoft Azure portal interface. On the left, the navigation pane is open, showing the 'Route tables' option under the 'Network' section. The main area displays the 'Create Route table' blade. The blade shows the 'Project details' section, where the subscription is 'Azure Pass - Sponsorship', the resource group is 'az104-06-rg1', and the region is 'East US'. The instance details section shows the name 'az104-06-rt23' and the option to propagate gateway routes is set to 'No'.

Add a new route with the following settings:

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Configuration, Routes, Subnets, Properties, Locks, Monitoring, Alerts, Automation, Tasks (preview), Export template, and Support + troubleshooting. The main content area displays the 'Routes' page for route table 'az104-06-rt23'. A table with columns 'Name' and 'Address prefix' is shown, currently empty. On the right, the 'Add route' dialog is open, showing the following configuration:

- Route name: az104-06-route-vnet2-to-vnet3
- Address prefix destination: IP Addresses
- Destination IP addresses/CIDR ranges: 10.63.0.0/20
- Next hop type: Virtual appliance
- Next hop address: 10.60.0.4

A blue 'Add' button is at the bottom of the dialog. A note at the bottom of the dialog states: 'Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.'

Associate the route table **az104-06-rt23** with the following subnet:

The screenshot shows the Microsoft Azure portal interface. The left sidebar is the same as in the previous screenshot. The main content area displays the 'Subnets' page for route table 'az104-06-rt23'. A table with columns 'Name', 'Address range', and 'Virtual network' is shown, currently empty. On the right, the 'Associate subnet' dialog is open, showing the following configuration:

- Virtual network: az104-06-vnet2
- Subnet: subnet0

A blue 'OK' button is at the bottom of the dialog.

Add a new route table, click **Subnets**, and **Associate**.

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains navigation options: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Configuration, Routes (selected), Subnets, Properties, Locks, Monitoring, Alerts, Automation, Tasks (preview), Export template, and Support + troubleshooting. The main content area displays the 'az104-06-rt32' route table with a search bar and a table showing no results. The right-hand 'Add route' dialog is open, showing fields for: Route name (az104-06-route-vnet3-to-vnet2), Address prefix destination (IP Addresses), Destination IP addresses/CIDR ranges (10.62.0.0/20), Next hop type (Virtual appliance), and Next hop address (10.60.0.4). A blue 'Add' button is at the bottom of the dialog.

The screenshot shows the Microsoft Azure portal interface. The left sidebar is the same as the previous image. The main content area displays the 'az104-06-rt32' route table with a search bar and a table showing no results. The right-hand 'Associate subnet' dialog is open, showing fields for: Virtual network (az104-06-vnet3) and Subnet (subnet0). A blue 'OK' button is at the bottom of the dialog.

On the **Network Watcher - Connection troubleshoot**

Like we had done on task 3 lets know see if the vms 2 and 3 will interact

Microsoft Azure

Search resources, services, and docs (G+)

Home > Network Watcher

Network Watcher | Connection troubleshoot

Microsoft

Search

Overview

Get started

Monitoring

- Topology
- Connection monitor (classic)
- Connection monitor
- Network Performance Monitor

Network diagnostic tools

- IP flow verify
- NSG diagnostics
- Next hop
- Effective security rules
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

Metrics

- Usage + quotas

Network Watcher Connection Troubleshoot provides the capability to check a direct TCP connection from a virtual machine (VM) to a VM, fully qualified domain name (FQDN), URI, or IPv4 address. To start, choose a source to start the connection from, and the destination you wish to connect to and select "Check".

Learn more.

Source

Subscription *
Azure Pass - Sponsorship

Resource group *
az104-06-rg1

Source type *
Virtual machine

*Virtual machine
az104-06-vm2

Destination

Select a virtual machine Specify manually

URI, FQDN or IP address *
10.63.0.4

Probe Settings

Protocol TCP ICMP

Destination port *
10.60.0.4

The traffic was routed via **10.60.0.4**, assigned to the **az104-06-nic0** network adapter.

Vm3 is reachable from vm2 since the traffic between spoke virtual networks is now routed via the virtual machine located in the hub virtual network, which functions as a router.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Network Watcher

Network Watcher | Connection troubleshoot

Microsoft

Search

Overview

Get started

Monitoring

- Topology
- Connection monitor (classic)
- Connection monitor
- Network Performance Monitor

Network diagnostic tools

- IP flow verify
- NSG diagnostics
- Next hop
- Effective security rules
- VPN troubleshoot
- Packet capture
- Connection troubleshoot

Metrics

- Usage + quotas

Status

Reachable

Agent extension version
1.4

Source virtual machine
az104-06-vm2

Grid view Topology view

Hops

Name	IP address	Status	Next hop IP address	RTT
az104-06-vm2	10.62.0.4	Reachable	10.60.0.4	-
az104-06-nic0	10.60.0.4	Reachable	10.63.0.4	-
az104-06-nic3	10.63.0.4	Reachable	-	-

Average Latency in milliseconds
2

Minimum Latency in milliseconds
2

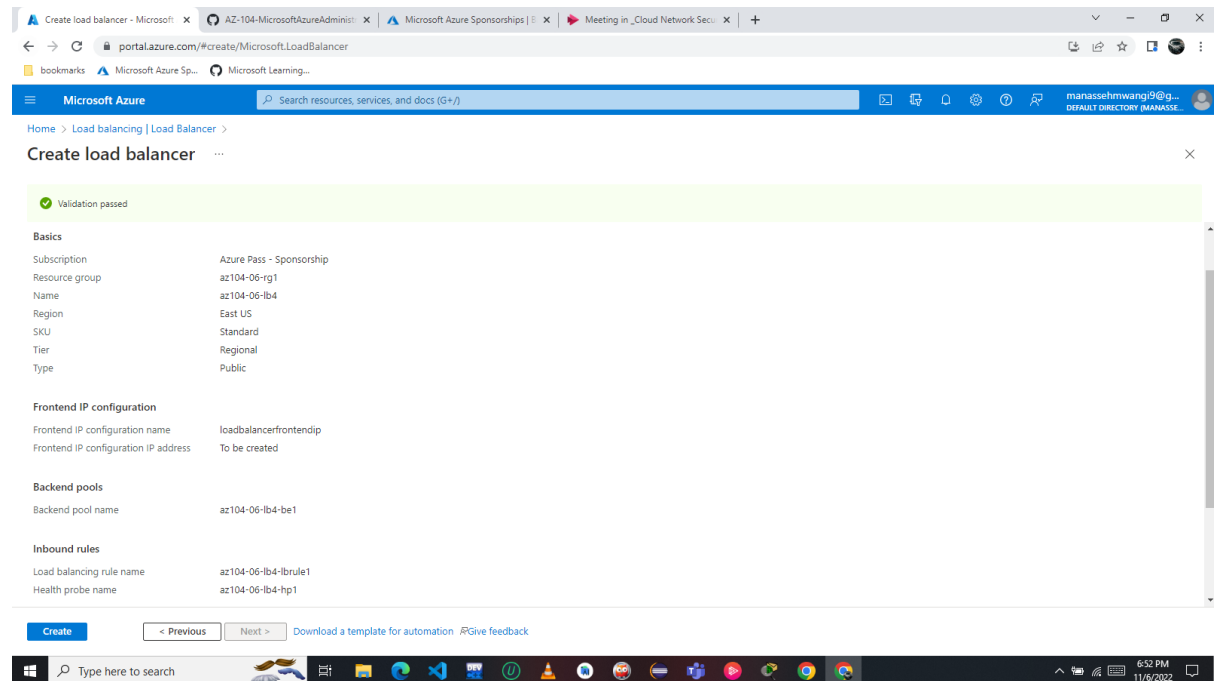
Maximum Latency in milliseconds
4

Probes Sent
66

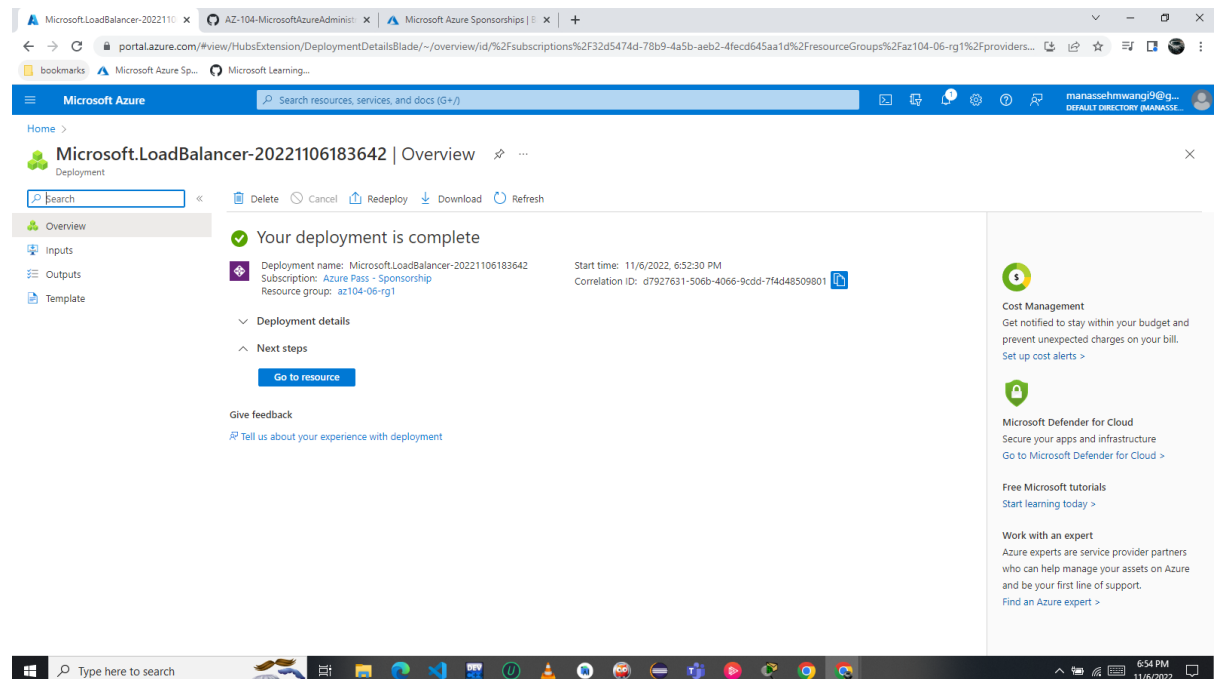
Task 5: Implement Azure Load Balancer

In this task, you will implement an Azure Load Balancer in front of the two Azure virtual machines in the hub virtual network.

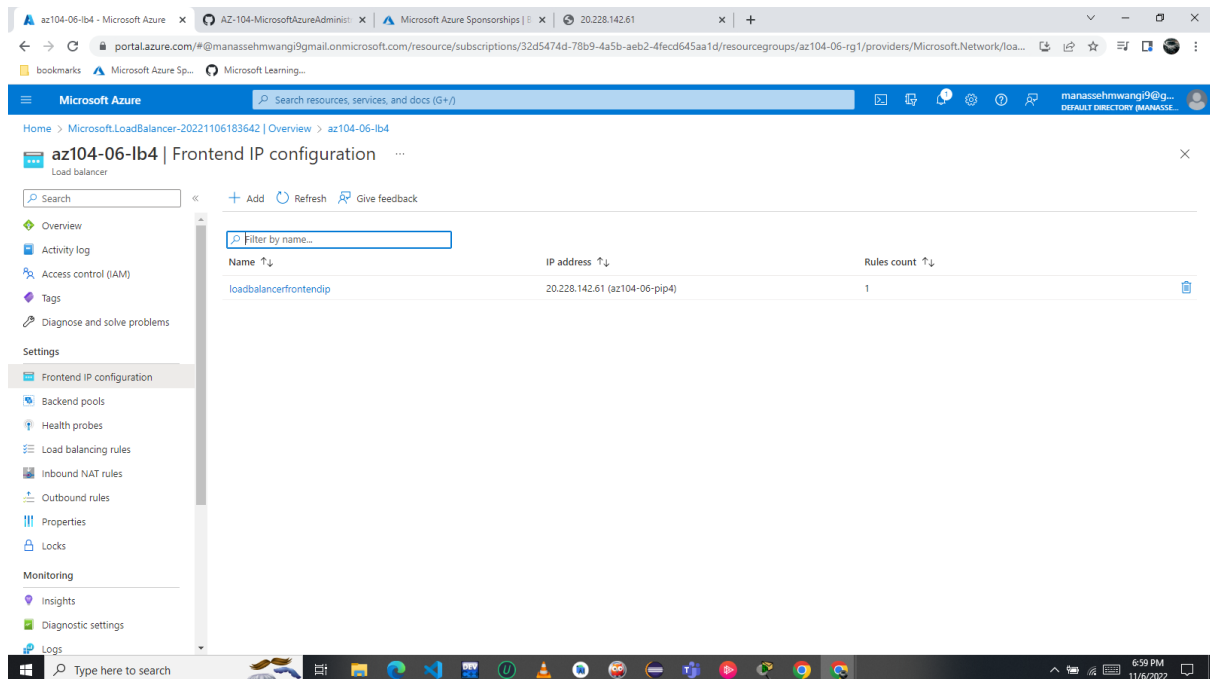
Create a load balancer with the following settings



Wait for the load balancer to deploy

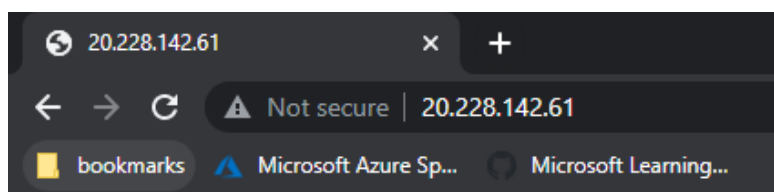
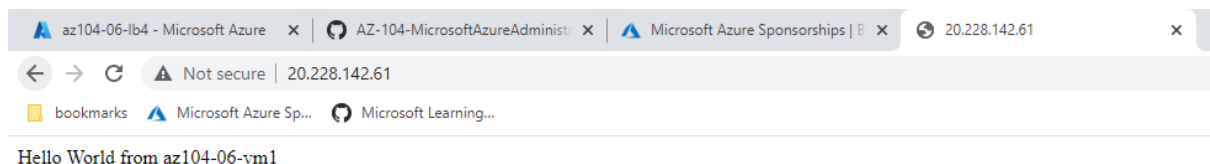


Select **Frontend IP configuration** from the Load Balancer resource page. Copy the IP address.



Open another browser tab and navigate to the IP address

Verify that the browser window displays the message **Hello World from az104-06-vm0** or **Hello World from az104-06-vm1**.



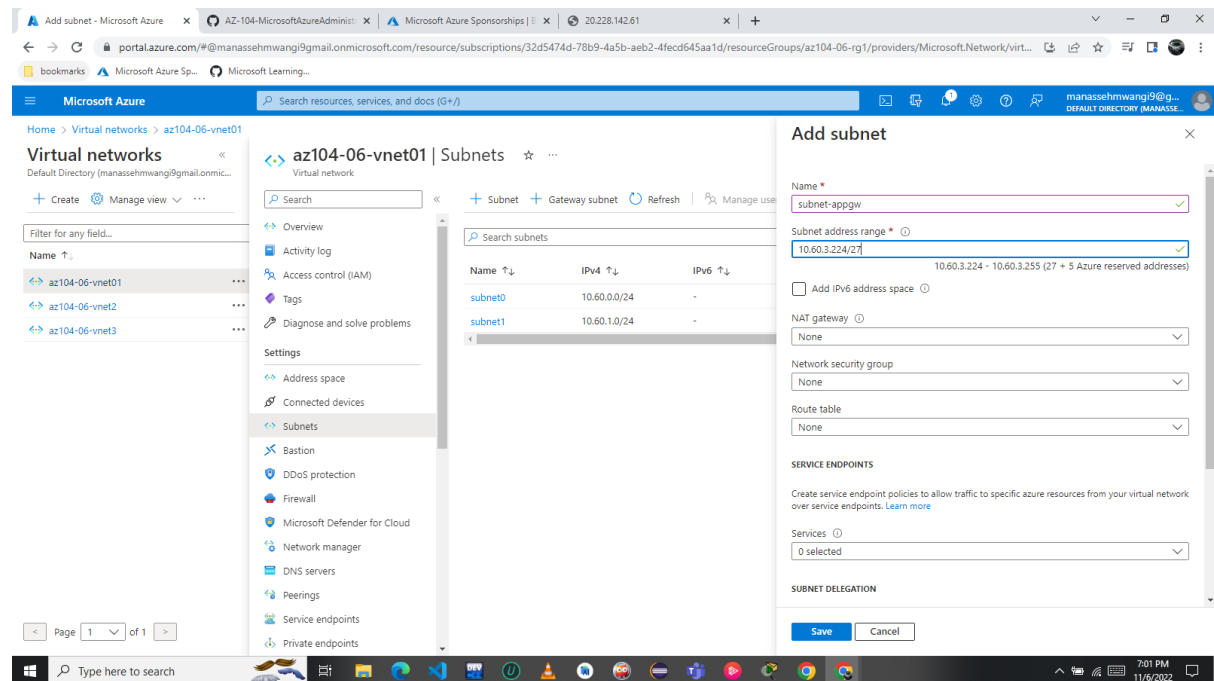
Hello World from az104-06-vm0

Task 6: Implement Azure Application Gateway

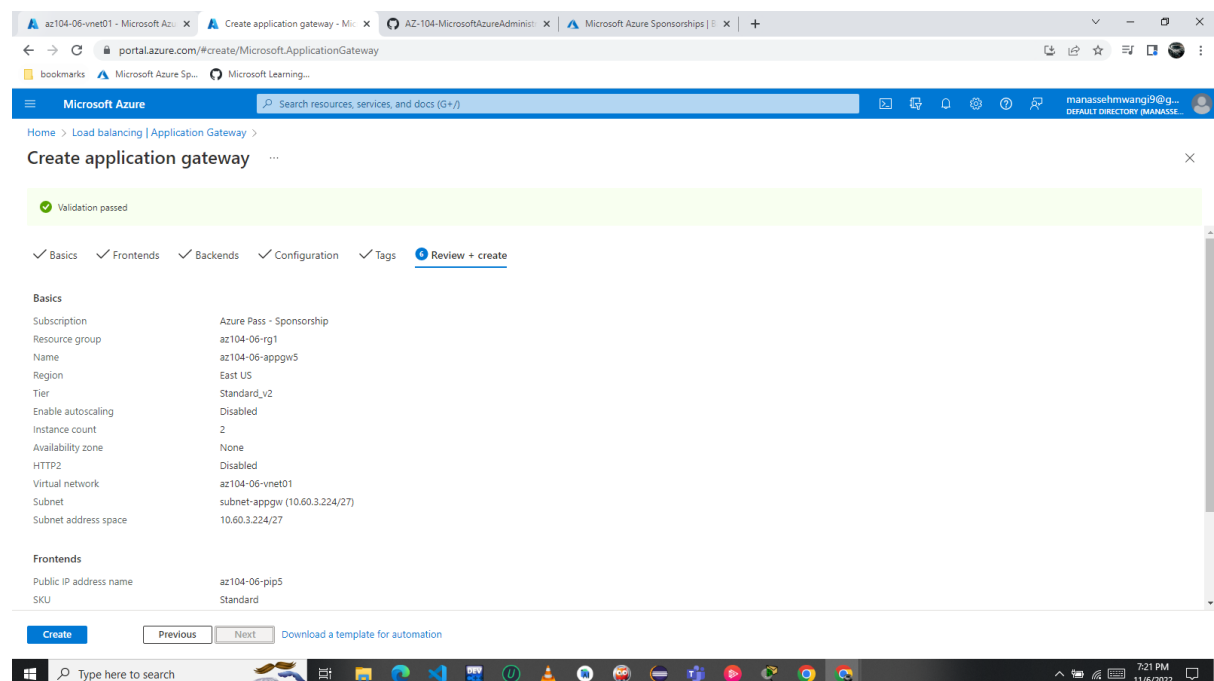
In this task, you will implement an Azure Application Gateway in front of the two Azure virtual machines in the spoke virtual networks.

On the **az104-06-vnet01** virtual network click **Subnets**, and then click **+ Subnet**.

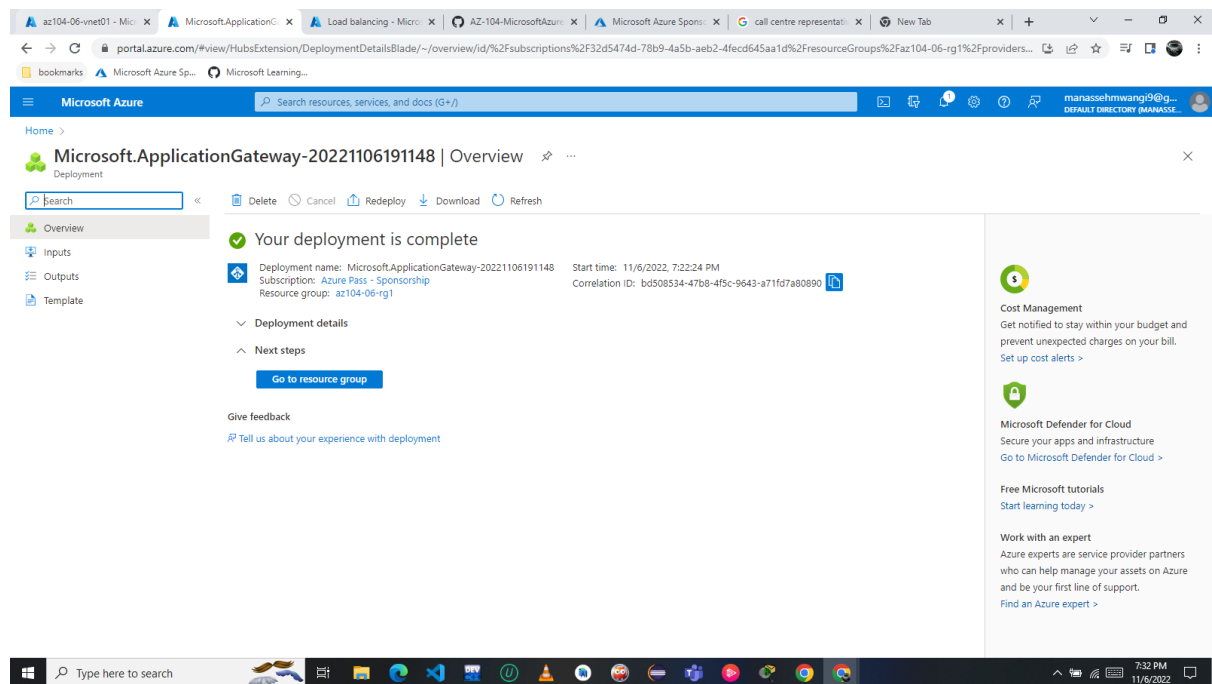
Add a subnet with the following settings



Search and select **Application Gateways** and, on the **Application Gateways** blade, click **+ Create**. Specify the following

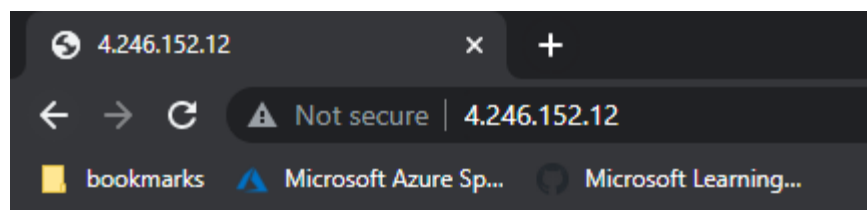
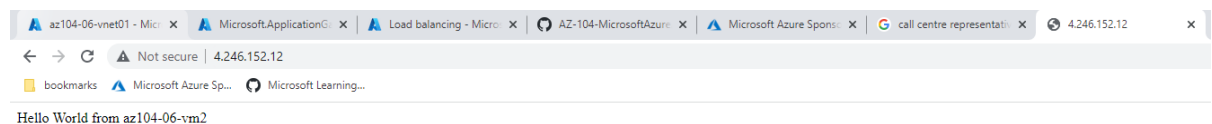


Wait for the Application Gateway instance to be created, this might take 8 minutes.



On the **az104-06-appgw5** Application Gateway blade, copy the value of the **Frontend public IP address**.

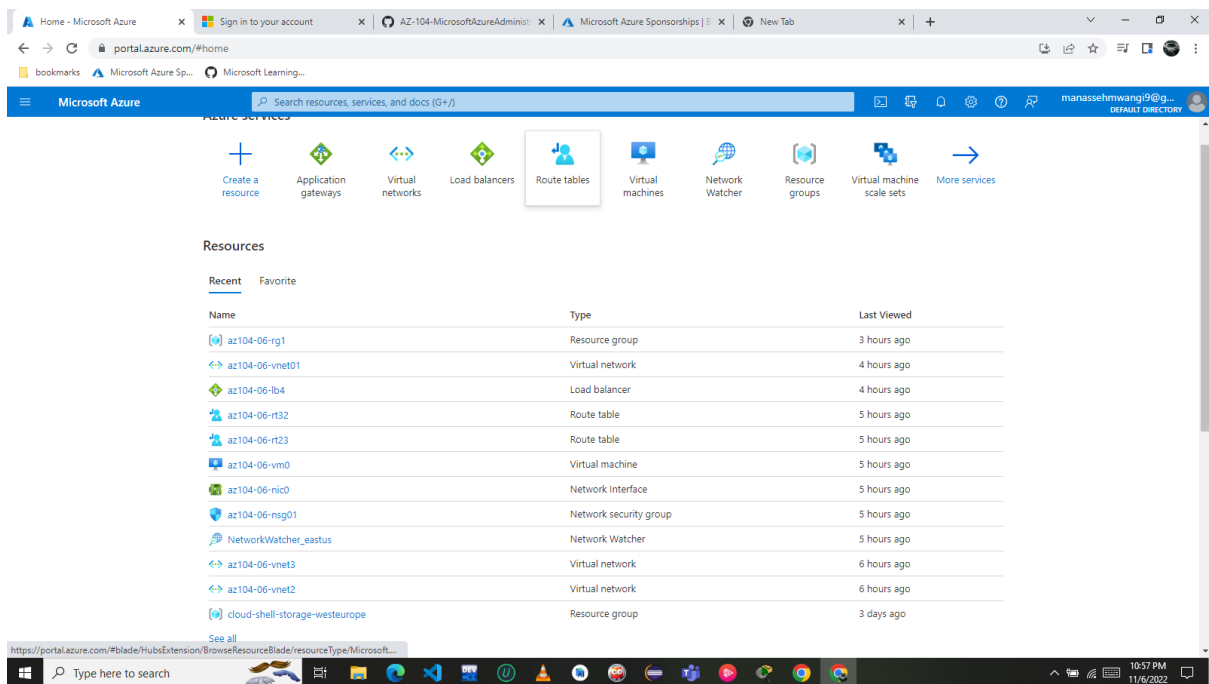
Verify that the browser window displays the message **Hello World from az104-06-vm2** or **Hello World from az104-06-vm3**.



Hello World from az104-06-vm3

Targeting virtual machines on multiple virtual networks is not a common configuration, but it is meant to illustrate the point that Application Gateway is capable of targeting virtual machines on multiple virtual networks (as well as endpoints in other Azure regions or even outside of Azure), unlike Azure Load Balancer, which load balances across virtual machines in the same virtual network.

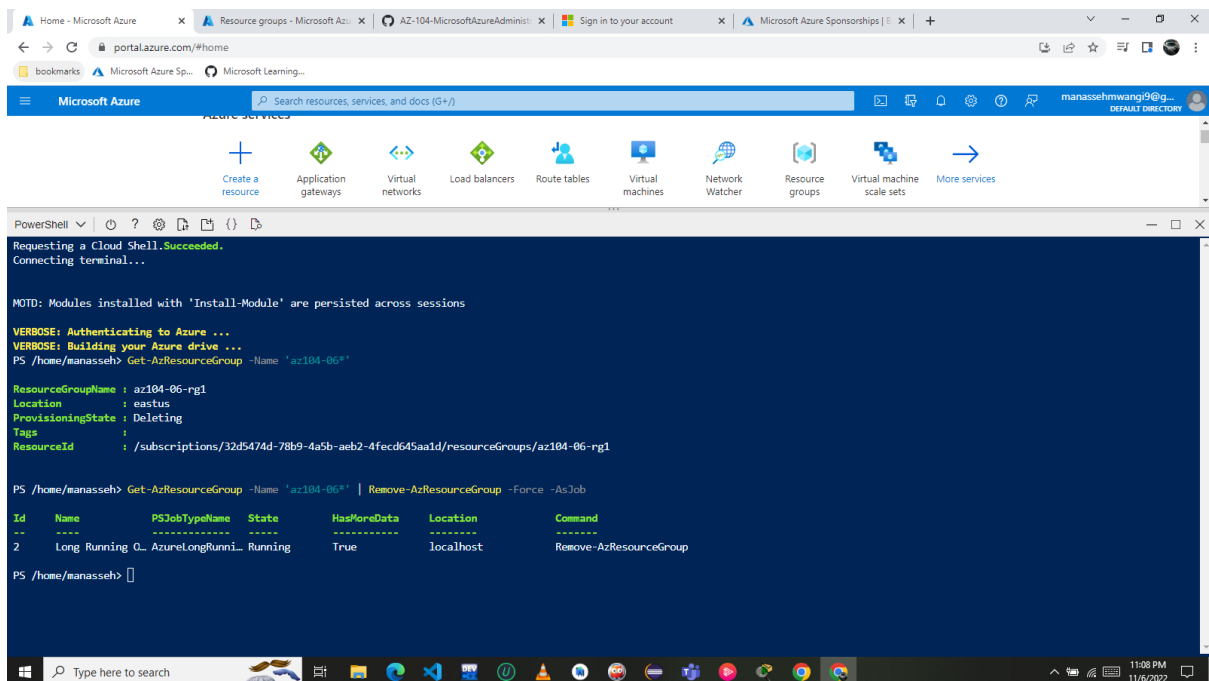
The overall resources used.



The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo and a search bar. Below the navigation bar, there's a section titled "Azure services" with various icons for different services like "Create a resource", "Application gateways", "Virtual networks", "Load balancers", "Route tables", "Virtual machines", "Network Watcher", "Resource groups", "Virtual machine scale sets", and "More services". The "Route tables" icon is highlighted. Below this, there's a "Resources" section with a table listing recent resources. The table has columns for "Name", "Type", and "Last Viewed".

Name	Type	Last Viewed
az104-06-rg1	Resource group	3 hours ago
az104-06-vnet01	Virtual network	4 hours ago
az104-06-lb4	Load balancer	4 hours ago
az104-06-rt32	Route table	5 hours ago
az104-06-rt23	Route table	5 hours ago
az104-06-vm0	Virtual machine	5 hours ago
az104-06-nic0	Network interface	5 hours ago
az104-06-nsg01	Network security group	5 hours ago
NetworkWatcher_eastus	Network Watcher	5 hours ago
az104-06-vnet3	Virtual network	6 hours ago
az104-06-vnet2	Virtual network	6 hours ago
cloud-shell-storage-westurope	Resource group	3 days ago

Remove any newly created Azure resources that you no longer use. Removing unused resources ensures you will not see unexpected charges.



The screenshot shows a PowerShell terminal window with the following commands and output:

```
PS /home/manasseh> Get-AzResourceGroup -Name 'az104-06*'

ResourceGroupName : az104-06-rg1
Location           : eastus
ProvisioningState   : Deleting
Tags               :
ResourceId          : /subscriptions/32d5474d-78b9-4a5b-aeb2-4fec645aa1d/resourceGroups/az104-06-rg1

PS /home/manasseh> Get-AzResourceGroup -Name 'az104-06*' | Remove-AzResourceGroup -Force -AsJob
```

Id	Name	PSJobTypeName	State	HasMoreData	Location	Command
2	Long Running Q...	AzureLongRunni...	Running	True	localhost	Remove-AzResourceGroup