

Site-to-Site Connection

Introduction :-

As an Azure expert, this documentation aims to provide a comprehensive understanding of Site-to-Site Connection in Microsoft Azure. Site-to-Site Connection allows you to securely connect your on-premises network to an Azure Virtual Network (VNet) over the internet, enabling seamless communication between your on-premises resources and resources hosted in Azure.

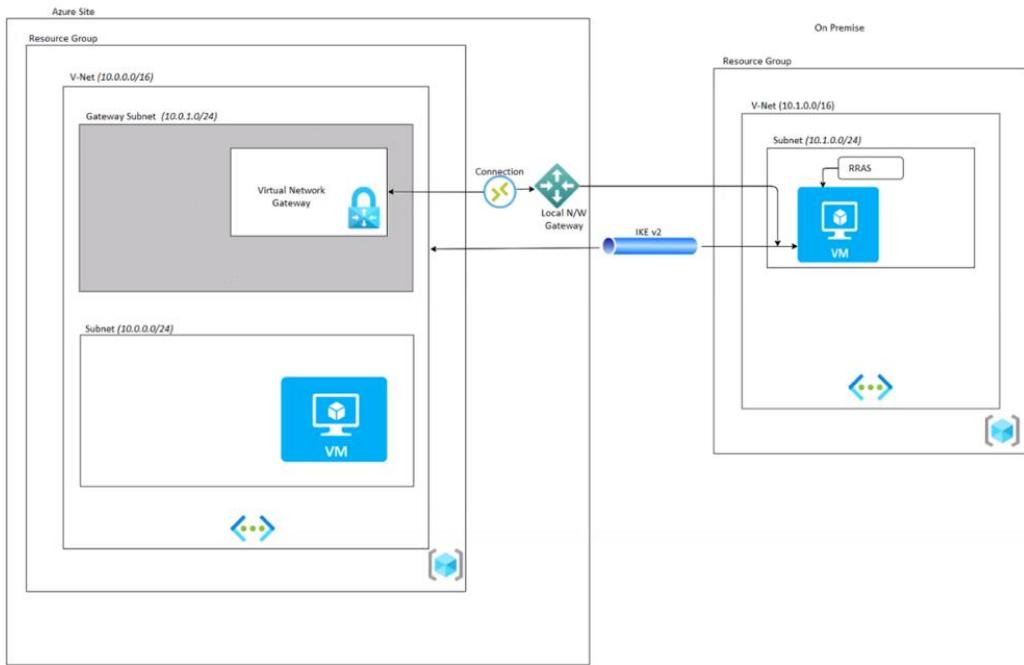
What is Site-to-Site Connection ?

Site-to-Site Connection, also known as S2S VPN, is a networking solution that establishes a secure and encrypted connection between an on-premises network and an Azure Virtual Network. This enables businesses to extend their on-premises data centers to Azure and access resources such as virtual machines, databases, and applications hosted in the cloud.

Benefits of Site-to-Site Connection :

- Hybrid Connectivity: Site-to-Site Connection allows organizations to maintain a hybrid infrastructure, leveraging both on-premises and cloud resources.
- Security: The connection is established over an encrypted VPN tunnel, ensuring data privacy and security during transmission.
- Scalability: Azure's global network infrastructure ensures reliable and scalable connectivity to meet growing business demands.
- Cost-Effective: Instead of investing in dedicated hardware for a direct connection, S2S VPN utilizes the internet to create a cost-effective connection

Architecture :-



Now we will follow a process so that we can establish a Site-to-Site connection between azure and OnPrem.

Step 1 - Create a resource group

Now we will create a Resource group named OnPremRG in the central india region.

The screenshot shows the Microsoft Azure portal interface for creating a new resource group. The page title is "Create a resource group - Microsoft Azure". The URL in the address bar is "portal.azure.com/#create/Microsoft.ResourceGroup". The main content area is titled "Create a resource group" with a "Basic" tab selected. Under "Project details", the "Subscription" dropdown is set to "Azure for Students" and the "Resource group" dropdown is set to "OnPremRG". Under "Resource details", the "Region" dropdown is set to "(Asia Pacific) Central India". At the bottom of the form, there are buttons for "Review + create", "< Previous", and "Next : Tags >". The status bar at the bottom right shows the time as "1:36 AM" and the date as "7/26/2023".

Step 2 - Create a Virtual Network

Now we will create a virtual network named **AzureVnet** in the central india region. Resource group will be a different named **AzureRG**. Now in the networking section, select the default subnet.

The screenshot shows the Azure portal interface for creating a new Virtual Network. The 'IP Addresses' tab is active, displaying the configuration for the IPv4 address space. An IPv4 address space is defined from 10.0.0.0/16 to 10.0.255.255, which covers 65536 addresses. A single subnet named 'default' is present with a subnet address range of 10.0.0.0/24. The 'NAT gateway' section is currently collapsed. Below the address space configuration, the 'Basics' tab is selected, providing an overview of the project details such as subscription and resource group. The instance details section shows the name 'AzureVnet' and the region 'Central India' selected. The overall interface is clean and follows the standard Azure design principles.

Step 3 - Creating a virtual machine

Now we will create a virtual machine in AzureRG named AzureVM. Its image will be windows server 2019 datacenter and size will be Standard_D2s_V3. After this we will create and in the networking section we will select the default subnet.

Instance details

- Virtual machine name: AzureVM
- Region: (Asia Pacific) Central India
- Availability options: No infrastructure redundancy required
- Security type: Trusted launch virtual machines
- Image: Windows Server 2019 Datacenter - x64 Gen2
- VM architecture: x64
- Run with Azure Spot discount: Unchecked
- Size: Standard_D2s_v3 - 2 vcpus, 8 GiB memory (₹11,294.05/month)

Administrator account

- Username: AzureVM
- Password: [REDACTED]
- Confirm password: [REDACTED]

Inbound port rules

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

Review + create

Validation passed

Basics

Cost given below is an estimate and not the final price. Please use [Pricing calculator](#) if for all your pricing needs.

Price

1 X Standard D2s v3 by Microsoft

Subscription credits apply: 15.4713 INR/hr

Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third party offerings. See the Azure Marketplace Terms for additional details.

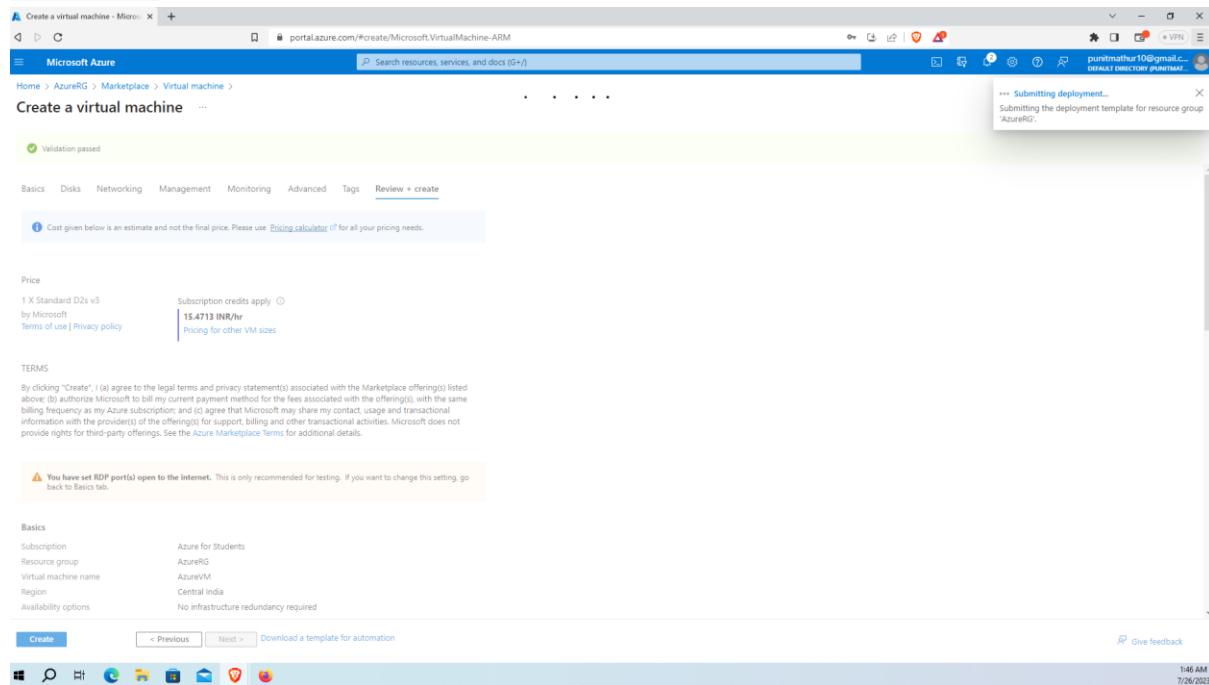
Basics

Subscription	Azure for Students
Resource group	AzureRG
Virtual machine name	AzureVM
Region	Central India
Availability options	No infrastructure redundancy required

Create

Step 4 - Creation of Virtual Network Gateway.

Now using resource group AzureRG we will create a virtual network gateway named **AzureVNG** select gateway type as **VPN** and VPN type as **Route-Based** and then select SKU as **VpnGw1** and generation as **Generation1** and in the virtual network section select **AzureVNet** now in public ip create a new named **VNG-PIP**.



This Deployment will take at least 35-40 minutes to complete.

Step 5 - Create a VM on OnPremiseRG Resource group.

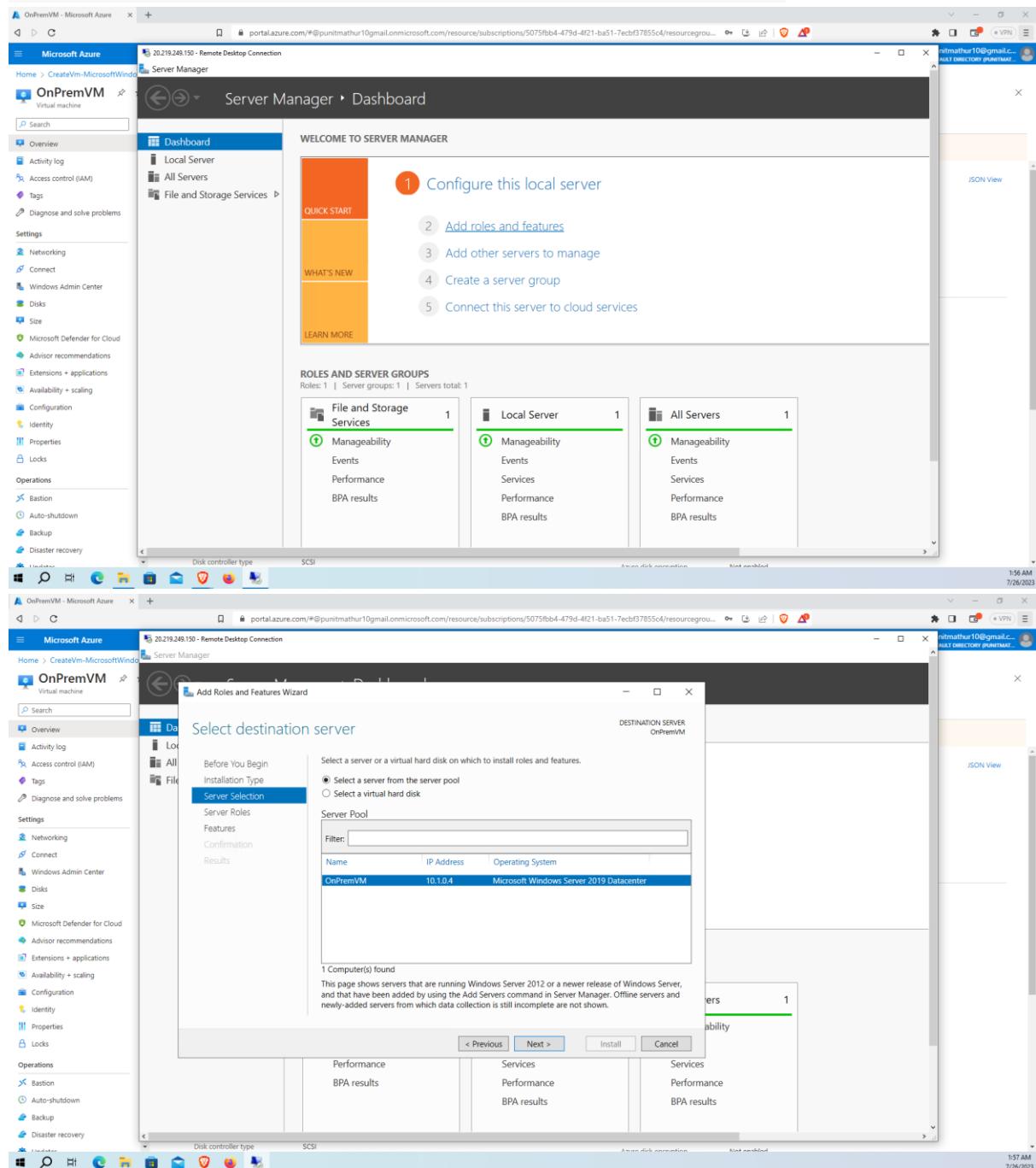
Now we will create a virtual machine named OnPremVM on resource group OnPremiseRg with Windows Server 2019 Datacenter as its image and Standard_D2s_v3 as its size.

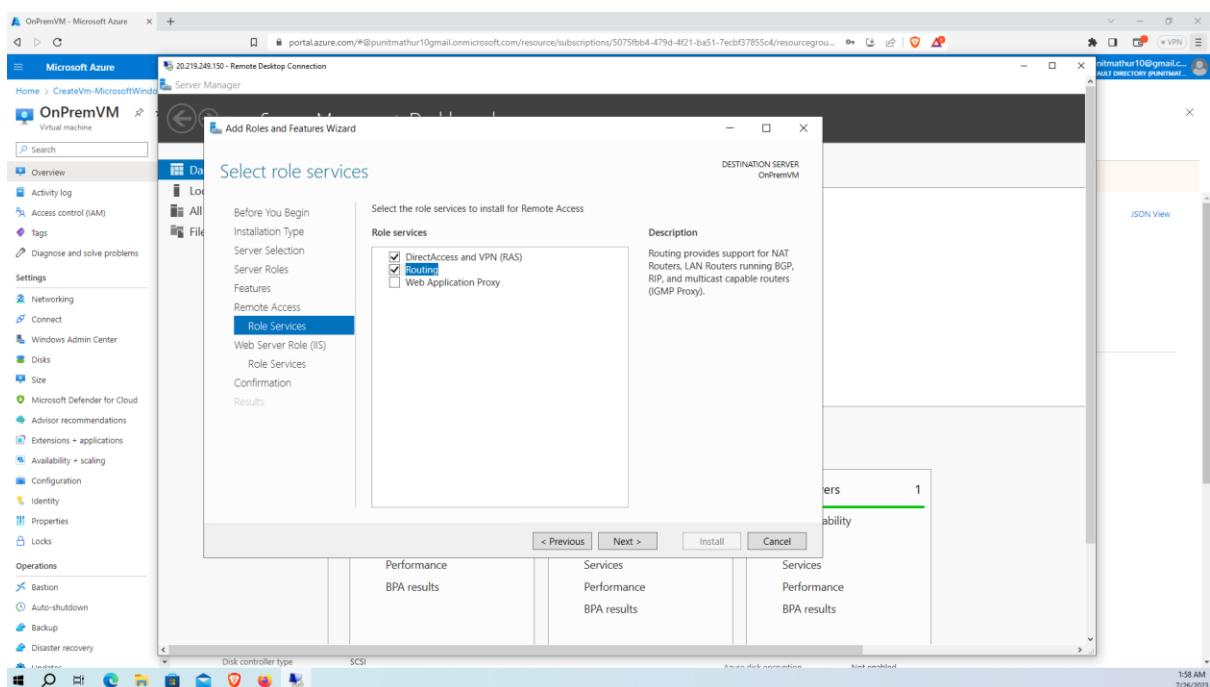
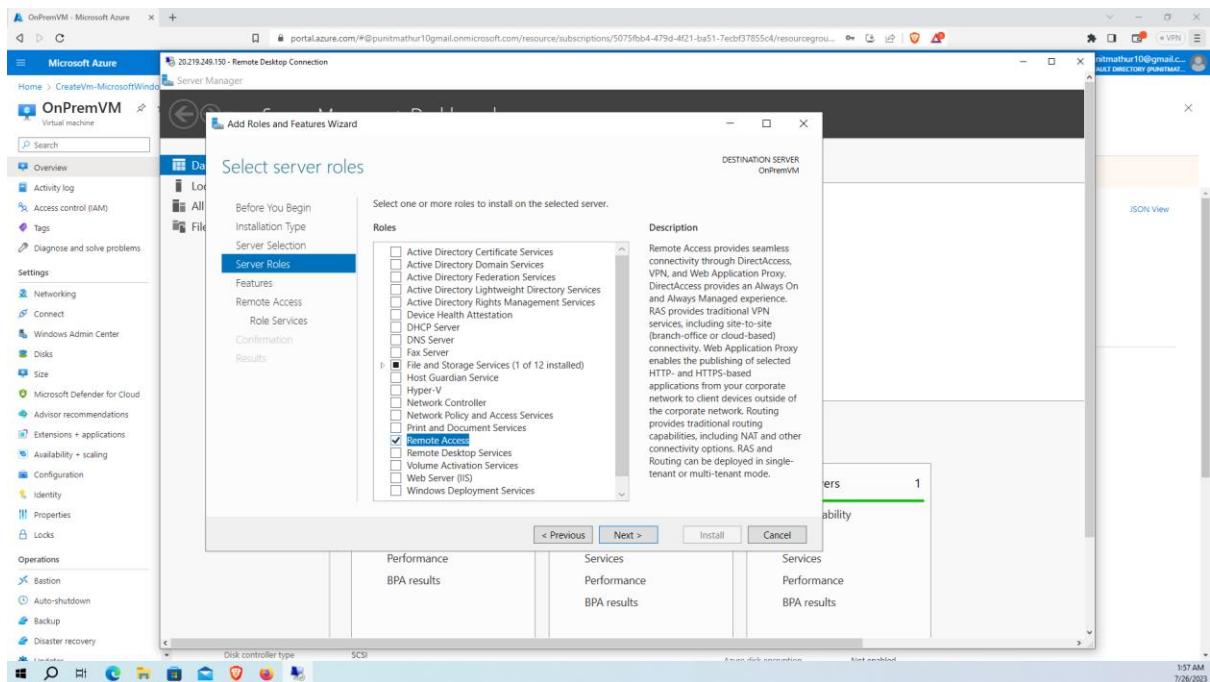
The screenshot shows two consecutive pages from the Azure portal:

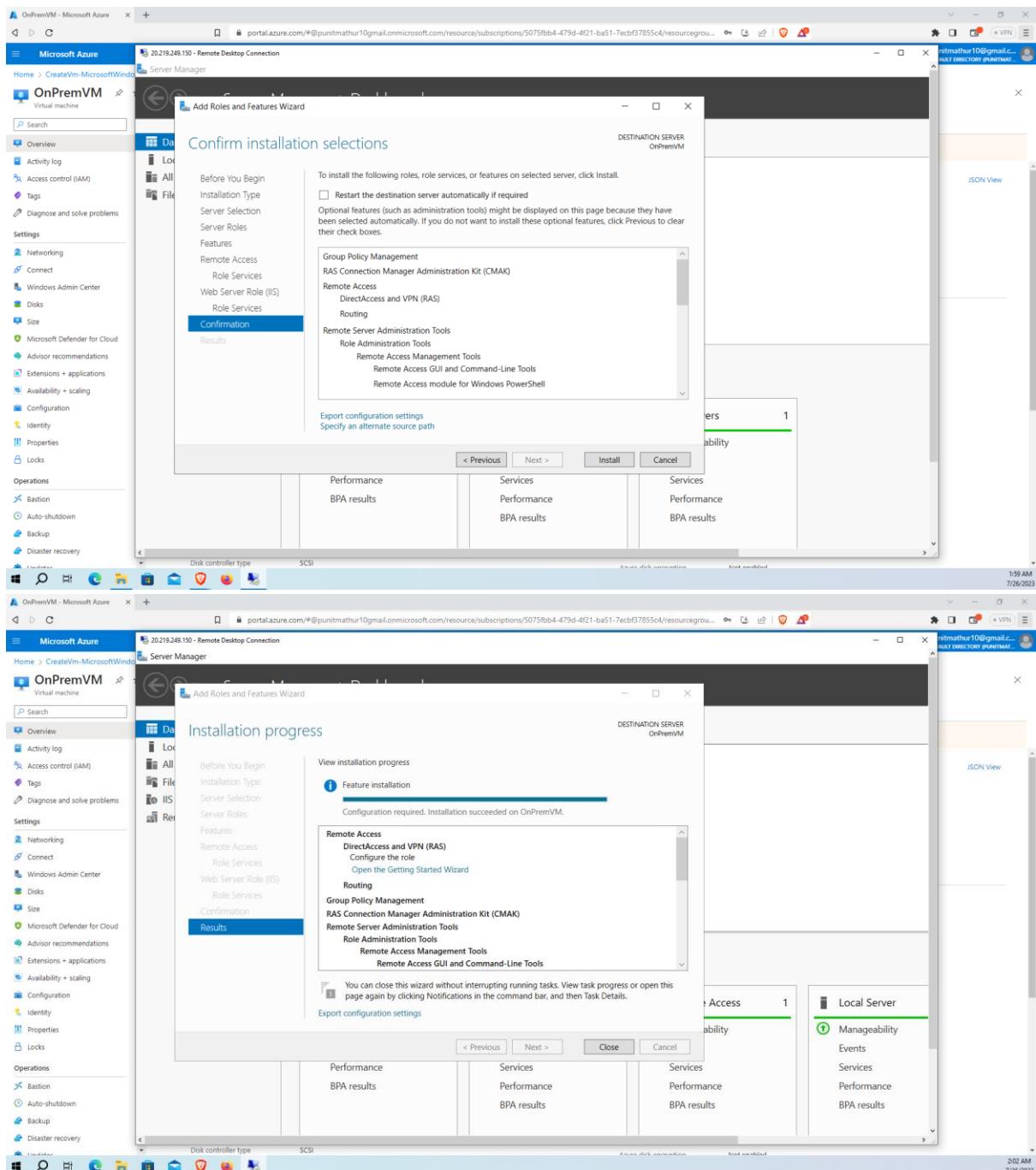
- Create a virtual machine - Microsoft Virtual Machine ARM**: This page is part of the 'Create a virtual machine' wizard. It shows the configuration for creating a VM named 'OnPremVM'. The settings include:
 - Region**: (Asia Pacific) Central India
 - Availability options**: No infrastructure redundancy required
 - Security type**: Trusted launch virtual machines
 - Image**: Windows Server 2019 Datacenter - x64 Gen2
 - VM architecture**: x64 (selected)
 - Run with Azure Spot discount**: Unchecked
 - Size**: Standard_D2s_v3 - 2 vcpus, 8 GiB memory (\$11,294.05/month)
 - Administrator account**: Username: OnPremVM, Password: (redacted), Confirm password: (redacted)
 - Inbound port rules**: Public inbound ports: Allow selected ports (RDP (3389))
- CreateVm-MicrosoftWindowsServer.WindowsServer-201-20230726014943 | Overview**: This page shows the deployment status. It indicates that the deployment is complete, with a start time of 7/26/2023, 1:51:27 AM. It also lists deployment details like auto-shutdown, monitoring, and script execution. Buttons for 'Go to resource' and 'Create another VM' are present. A feedback section and a sidebar with links to Cost Management, Microsoft Defender for Cloud, and Azure experts are also visible.

Step 6- Installation of RRAS Server

Now VM created in resource group OnPremiseRg, we will install the RRAS Server in this VM. For this first we will login to it using RDP and then We will use the Procedure Which is followed in These Screenshots.







Step 7 - Creation of Local Network Gateway (LNG)

Now we will configure the connectivity between Azure Network and OnPrem Network using Local Network Gateway and RRAS Server but first we need to create a Local Network Gateway for that. Now we will create a local network gateway from the marketplace and we will name it as AzLNG. We will use the address space of Virtual Network and IP address of the VM which is created for On Premise Network and then Finally we will Review + Create.



Step 8 - Creation of S2S Connection.

Now using AzLNG we will create a Site-to-Site connection. Just go to connections in AzLNG, click on Add. Now in creating the connection the connection type will be Site-to-Site and Named as AzuretoOnPrem and now in Settings section Type Virtual network gateway as AzureVNG, Local network gateway as AzLNG and type a shared key and remember for further use. Use the IKE protocol as IKEv2 and now review it and then create it.

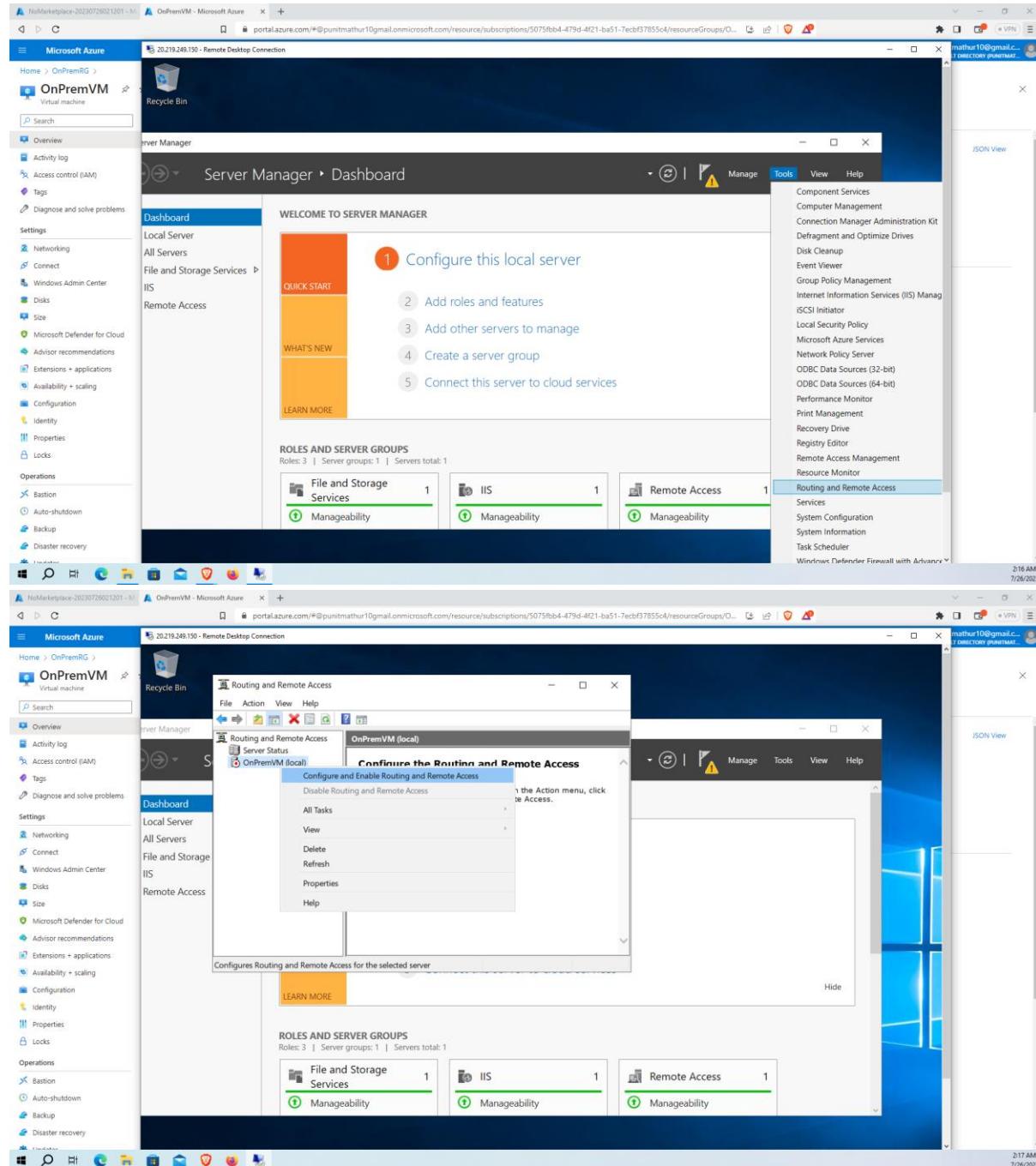
The screenshot shows the 'Create connection' blade in the Microsoft Azure portal. The connection type is set to 'Site-to-site (IPSec)'. The 'Name' field contains 'AzuretoOnPrem'. The 'Region' is set to 'Central India'. The 'Subscription' dropdown shows 'Azure for Students' and the 'Resource group' dropdown shows 'AzureRG'.

The screenshot shows the 'Review + create' blade for the connection settings. It includes fields for 'Virtual network gateway' (AzureVNG), 'Local network gateway' (AzLNG), 'Shared key (PSK)' (*****), 'IKE Protocol' (IKEv2 selected), and other connection parameters like 'IPsec / IKE policy', 'DPD timeout in seconds' (45), and 'Connection Mode' (Default).

The screenshot shows the 'Review + create' blade for the connection settings, identical to the previous screenshot but with a different timestamp (2:14 AM 7/26/2023).

Step 9 - Configure the RRAS Server

Now connect to the OnPremVM using RDP and then go to server manager and then go to tools and open routing and remote access. Then right click on **OnPremVM (local)** and then click on configure and enable routing and remote access. Now follow the steps in the screenshots uploaded below.



20.219.249.150 - Remote Desktop Connection

Routing and Remote Access Server Setup Wizard

Configuration

You can enable any of the following combinations of services, or you can customize this server.

Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.

Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.

Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.

Secure connection between two private networks
Connect the network to a remote network, such as a branch office.

Custom configuration
Select any combination of the features available in Routing and Remote Access.

< Back Next > Cancel

LEARN MORE

ROLES AND SERVER GROUPS

Roles: 3 | Server groups: 1 | Servers total: 1

 File and Storage Services	1	 IIS	1	 Remote Access	1
 Manageability					

2:18 AM 7/26/2023

20.219.249.150 - Remote Desktop Connection

Routing and Remote Access Server Setup Wizard

Demand-Dial Connections

Demand-dial connections allow you to route data to a remote network.

Do you want to use demand-dial connections to access remote networks?

Yes

No

You can set up demand-dial connections after this wizard finishes.

< Back Next > Cancel

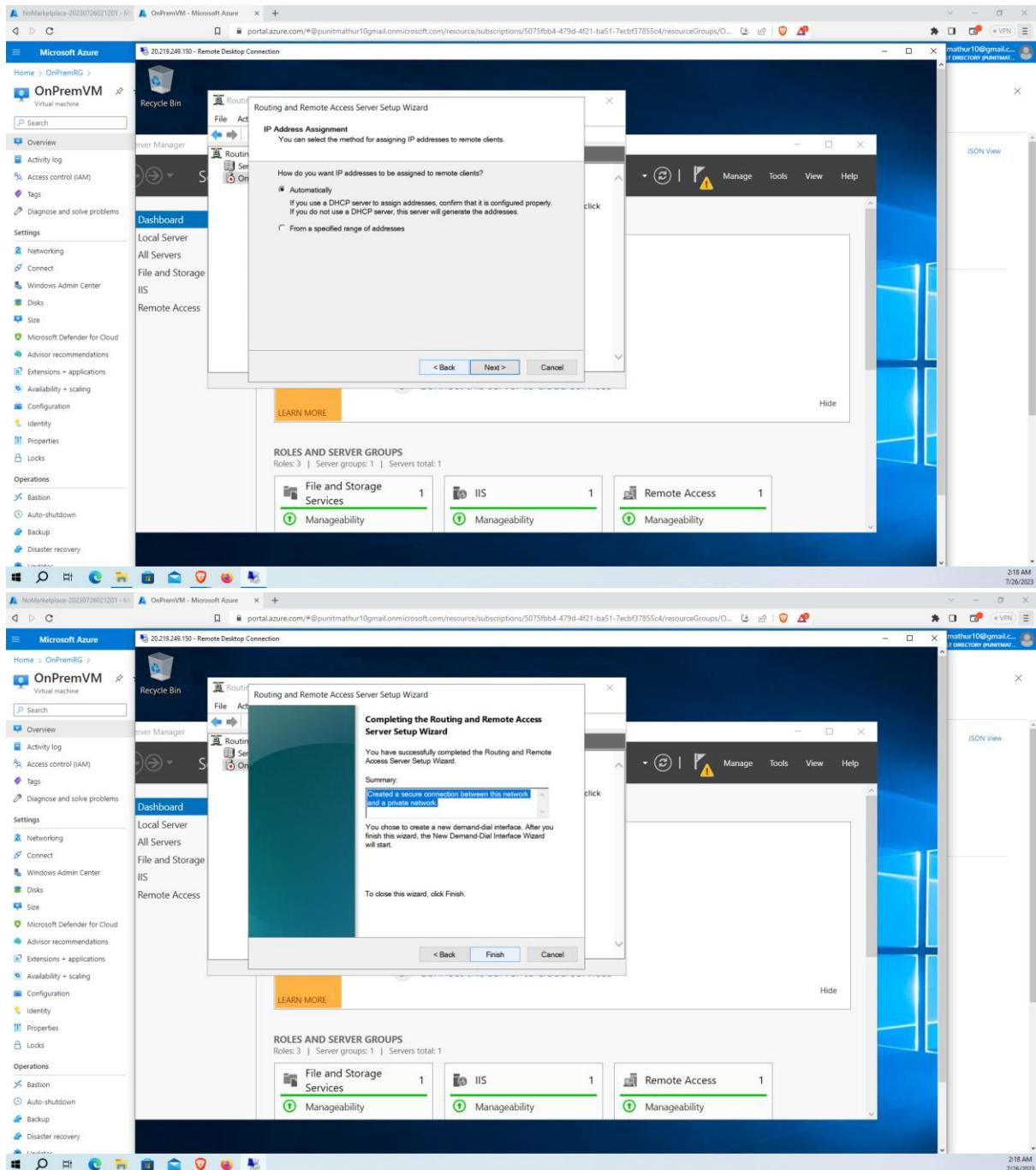
LEARN MORE

ROLES AND SERVER GROUPS

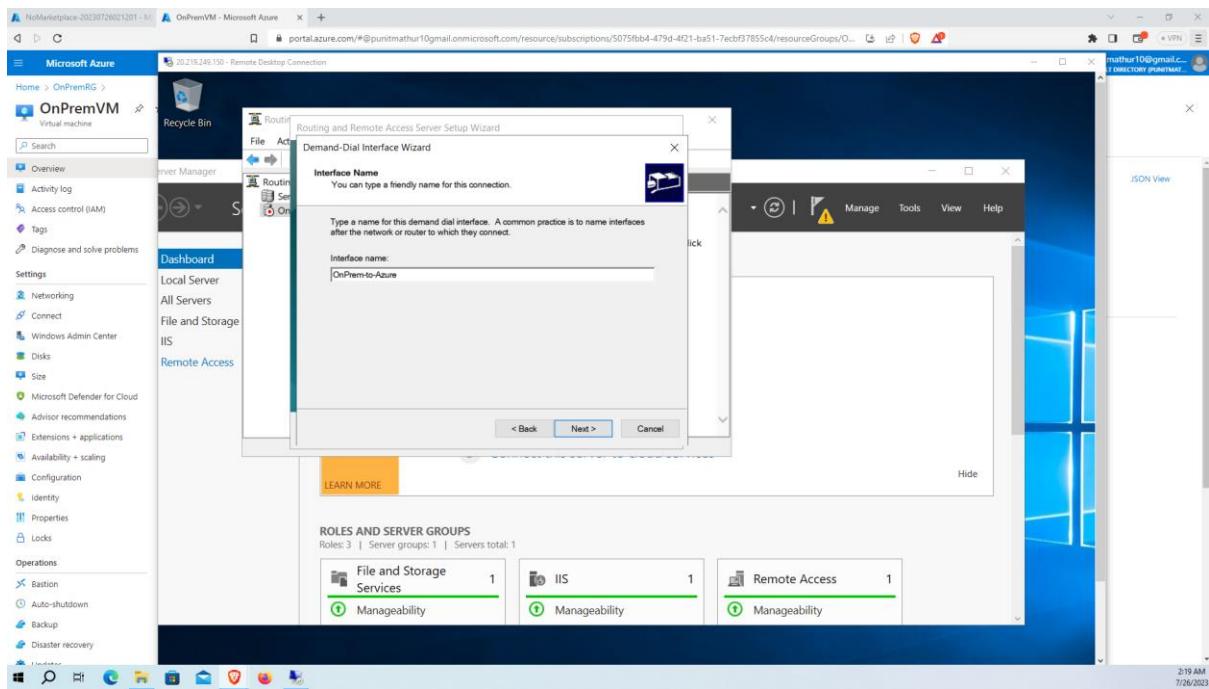
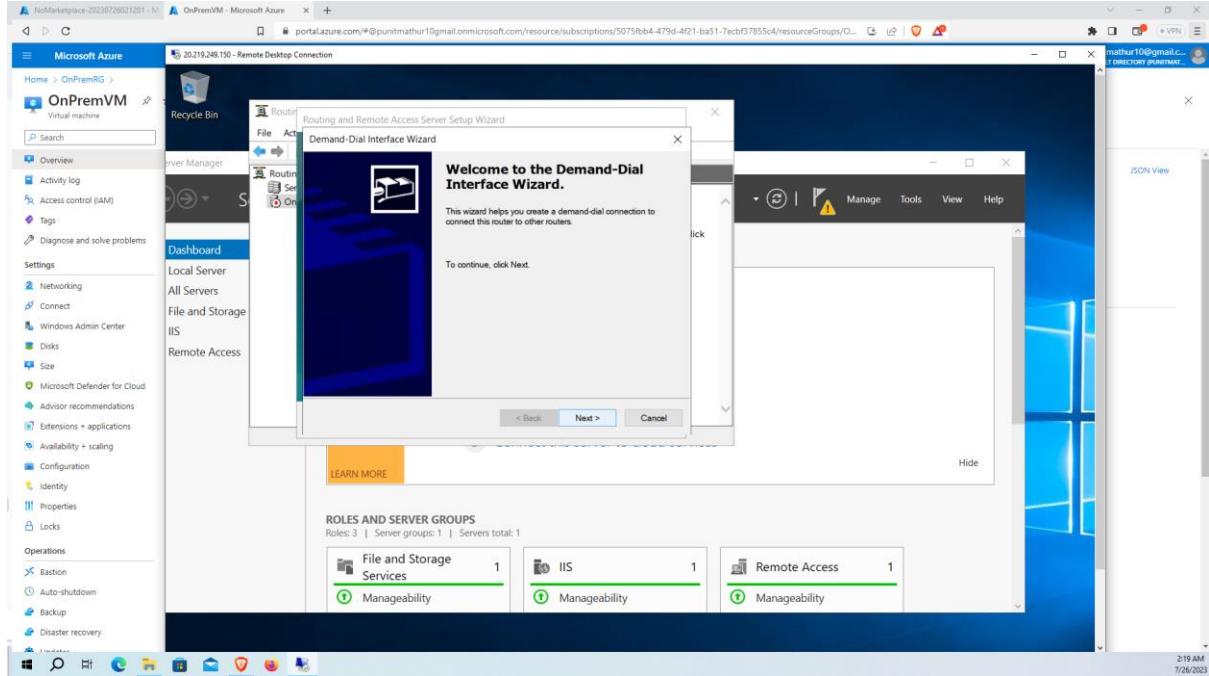
Roles: 3 | Server groups: 1 | Servers total: 1

 File and Storage Services	1	 IIS	1	 Remote Access	1
 Manageability					

2:18 AM 7/26/2023



Step 10 - Now to create and configure the connection between On-Premises and Azure on RRAS server, follow the following steps in Screenshots : -



OnPremVM - Microsoft Azure

20.219.249.150 - Remote Desktop Connection

Routing and Remote Access Server Setup Wizard

Demand-Dial Interface Wizard

Connection Type

Select the type of demand-dial interface you want to create.

- Connect using a modem, ISDN adapter, or other device
- Connect using virtual private networking (VPN)
- Connect using PPP over Ethernet (PPPoE)

< Back Next > Cancel

LEARN MORE

ROLES AND SERVER GROUPS

Roles: 3 | Server groups: 1 | Servers total: 1

File and Storage Services	1	IIS	1	Remote Access	1
Manageability		Manageability		Manageability	

2:19 AM 7/26/2023

AzureVNG - Microsoft Azure

Search resources, services, and docs (G+/-)

Essentials

Resource group (move) : AzureRG

Location : Central India

Subscription (move) : Azure for students

Subscription ID : 5075fb4-479d-4f21-ba51-7ecbf37855c4

SKU : VpnGw1

Gateway type : VPN

VPN type : Route-based

Virtual network : AzureVNet/Gateway Copied

public IP address : 20.219.194.32 (VNG-PPI)

Tags (edit) : Click here to add tags

Health check : Perform a quick health check to detect possible gateway issues

Advanced troubleshooting : Run a troubleshooting tool to investigate failure causes and perform repair actions

Documentation : View guidance on helpful topics related to VPN gateway

Show data for last : 1 hour, 6 hours, 12 hours, 1 day, 7 days, 30 days

Total tunnel ingress

1008
908
808
708
608
508
408
308
208
108

Total tunnel egress

1008
908
808
708
608
508
408
308
208
108

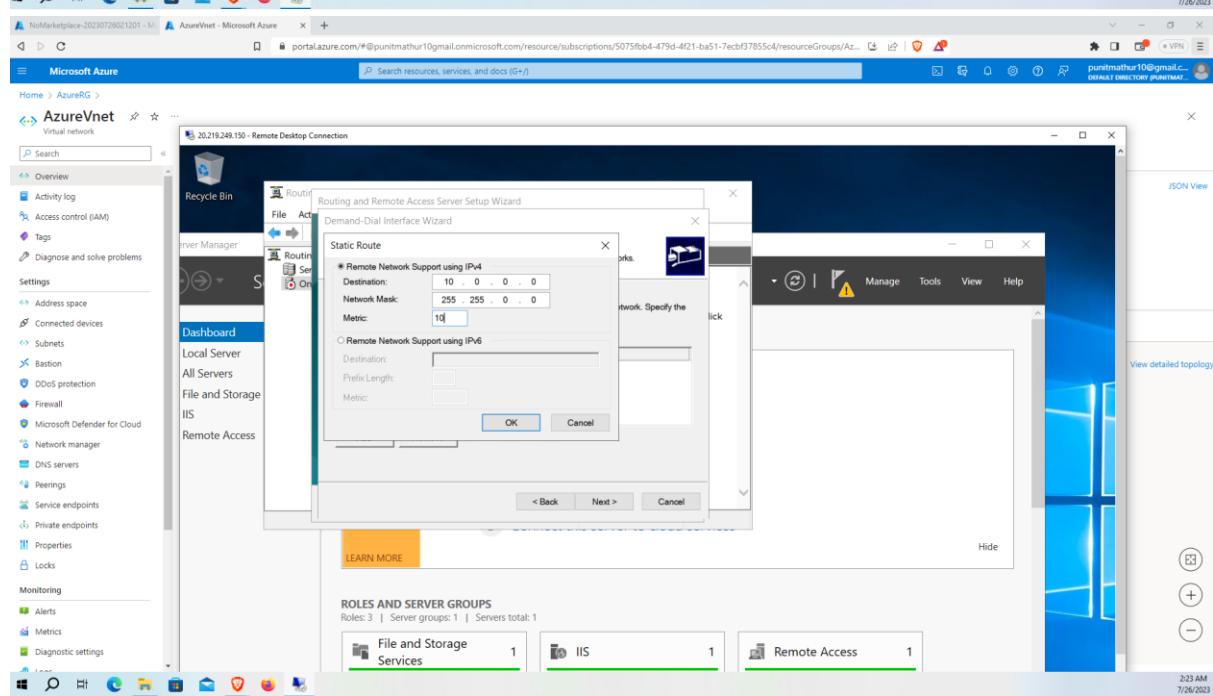
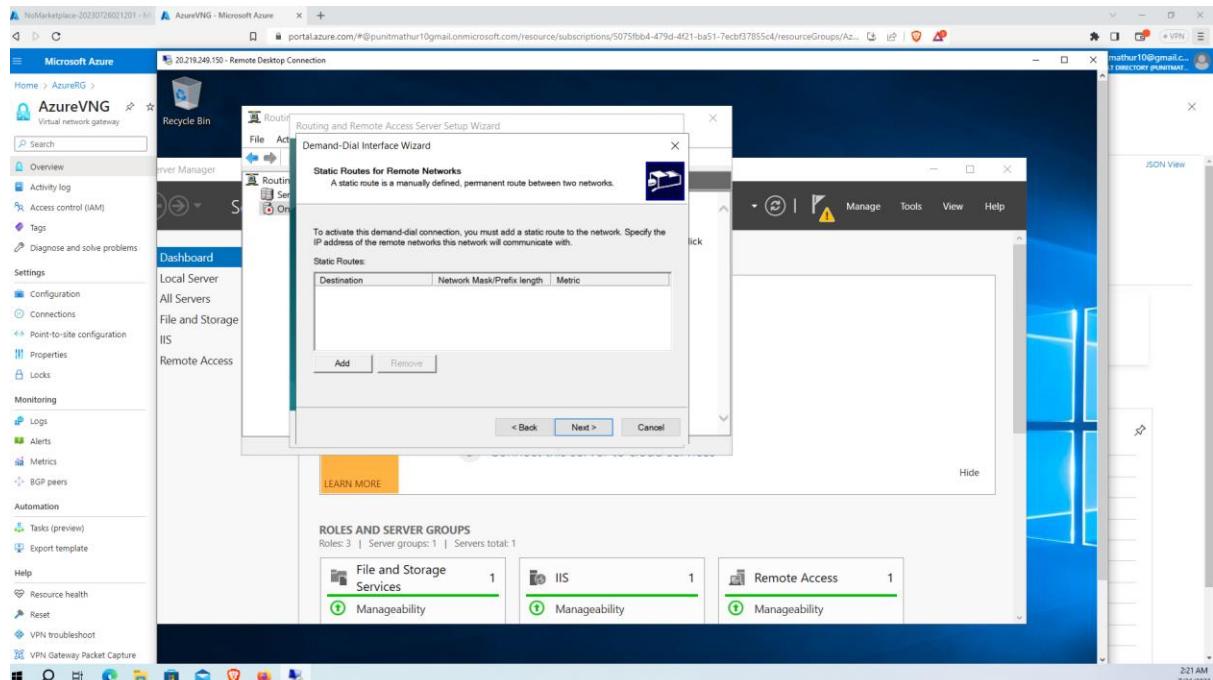
2:20 AM 7/26/2023

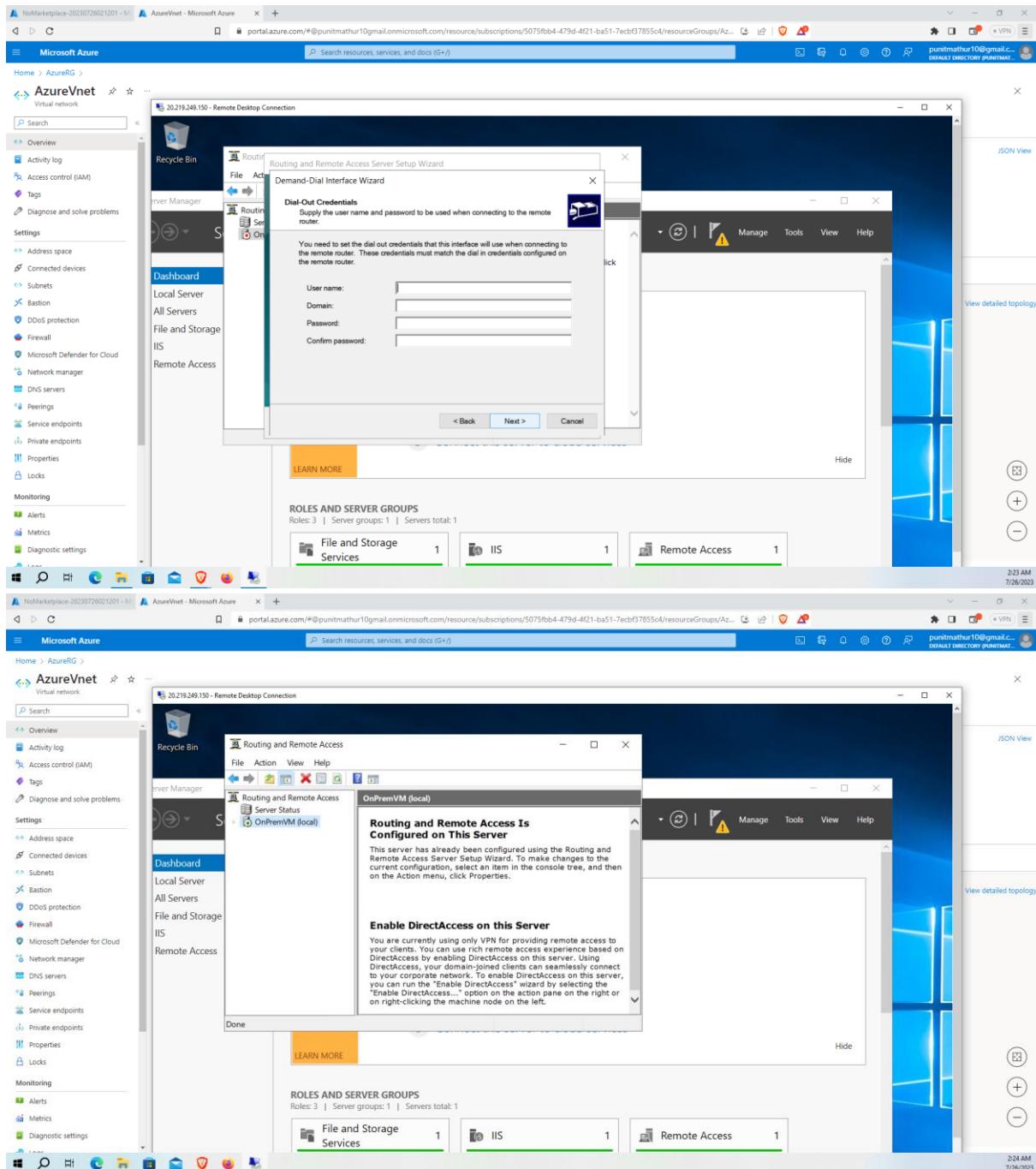
Screenshot 1: Routing and Remote Access Server Setup Wizard - Step 1: Destination Address

The screenshot shows the Microsoft Azure portal on the left and a Remote Desktop Connection window on the right. In the RDS window, the 'Demand-Dial Interface Wizard' is open, specifically the 'Destination Address' step. It asks for the name or IP address of the remote router, with '20.219.194.33' entered into the text field. Below the text field are buttons for '< Back', 'Next >', and 'Cancel'. A 'LEARN MORE' button is also visible.

Screenshot 2: Routing and Remote Access Server Setup Wizard - Step 2: Protocols and Security

The screenshot shows the same setup process. The 'Protocols and Security' step is displayed, showing options for selecting transports and security options. One option, 'Route IP packets on this interface', is checked. Other options like 'Add a user account so a remote router can dial in' and 'Send a plain-text password if that is the only way' are available but not selected. Below this are buttons for '< Back', 'Next >', and 'Cancel', along with a 'LEARN MORE' button.





Two screenshots of the Microsoft Azure portal showing the configuration of a Remote Desktop Connection (RDP) server.

Screenshot 1: Network Interfaces Configuration

The screenshot shows the "Network Interfaces" section of the "Routing and Remote Access" service. It lists the following interfaces:

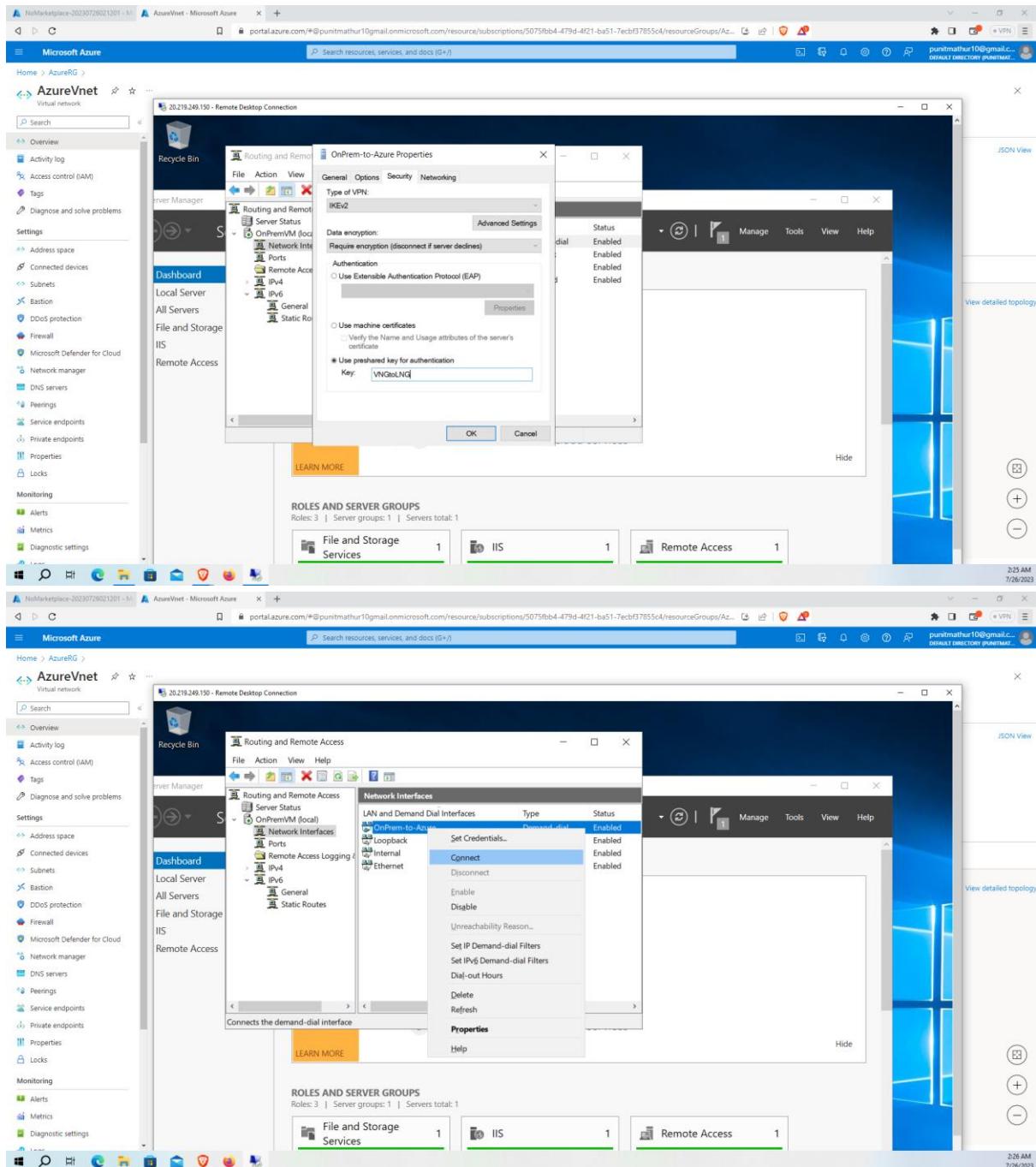
LAN and Demand Dial Interfaces	Type	Status
OnPrem-to-Azure	Demand-dial	Enabled
Loopback	Loopback	Enabled
Internal	Internal	Enabled
Ethernet	Dedicated	Enabled

Screenshot 2: OnPrem-to-Azure Properties Configuration

The screenshot shows the "OnPrem-to-Azure Properties" dialog box. The "General" tab is selected, showing the following settings:

- Type of VPN: IKEv2
- Data encryption: Require encryption (disconnect if server declines)
- Authentication:
 - Use Extensible Authentication Protocol (EAP) (selected)
 - Use machine certificates
 - Verify the Name and Usage attributes of the server's certificate (selected)
 - Use preshared key for authentication (Key: [redacted])

The "Networking" tab is also visible in the background.



Two screenshots of the Microsoft Azure portal showing the configuration of a static route on a Windows Server 2019 VM.

Screenshot 1: Network Interfaces Configuration

The screenshot shows the "Network Interfaces" section of the Routing and Remote Access service. It lists four interfaces:

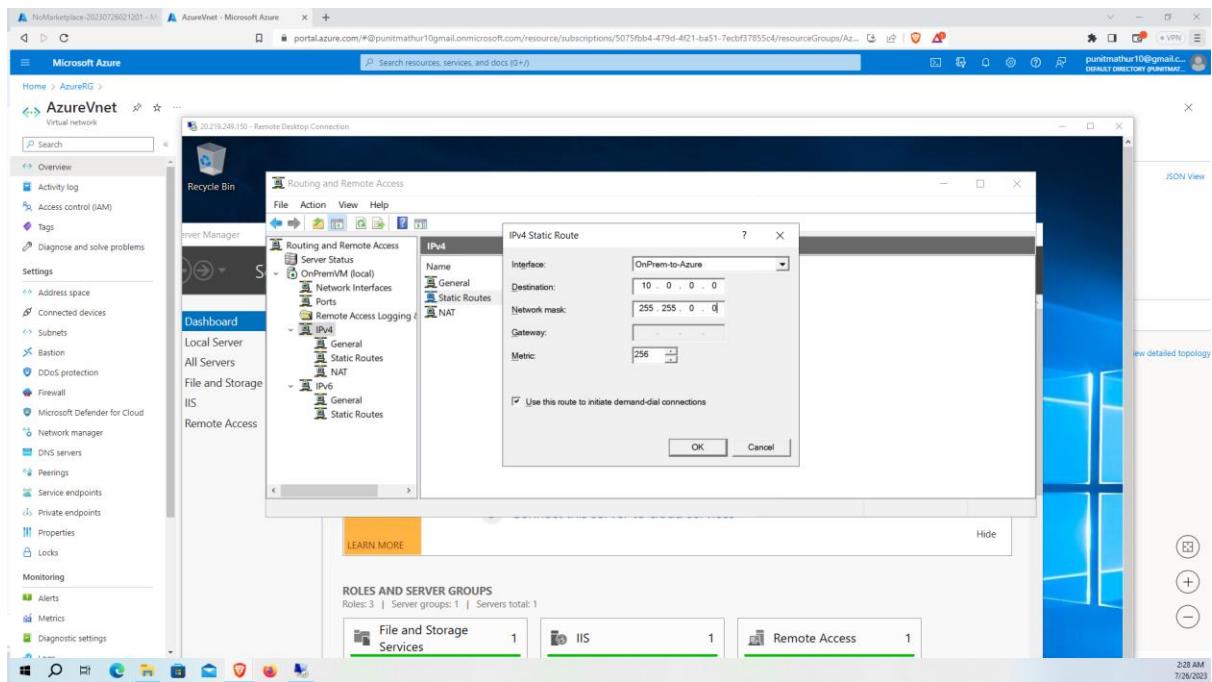
LAN and Demand Dial Interfaces	Type	Status	Connection State	Device Name
OnPrem-to-Azure	Demand-dial	Enabled	Connected	Microsoft Hyper-V Network Adapter
Loopback	Loopback	Enabled	Connected	
Internal	Internal	Enabled	Connected	
Ethernet	Dedicated	Enabled	Connected	

Screenshot 2: Creating a New Static Route

The screenshot shows the "IPv4" configuration page. A context menu is open over the "Static Routes" entry, with the option "New Static Route..." highlighted.

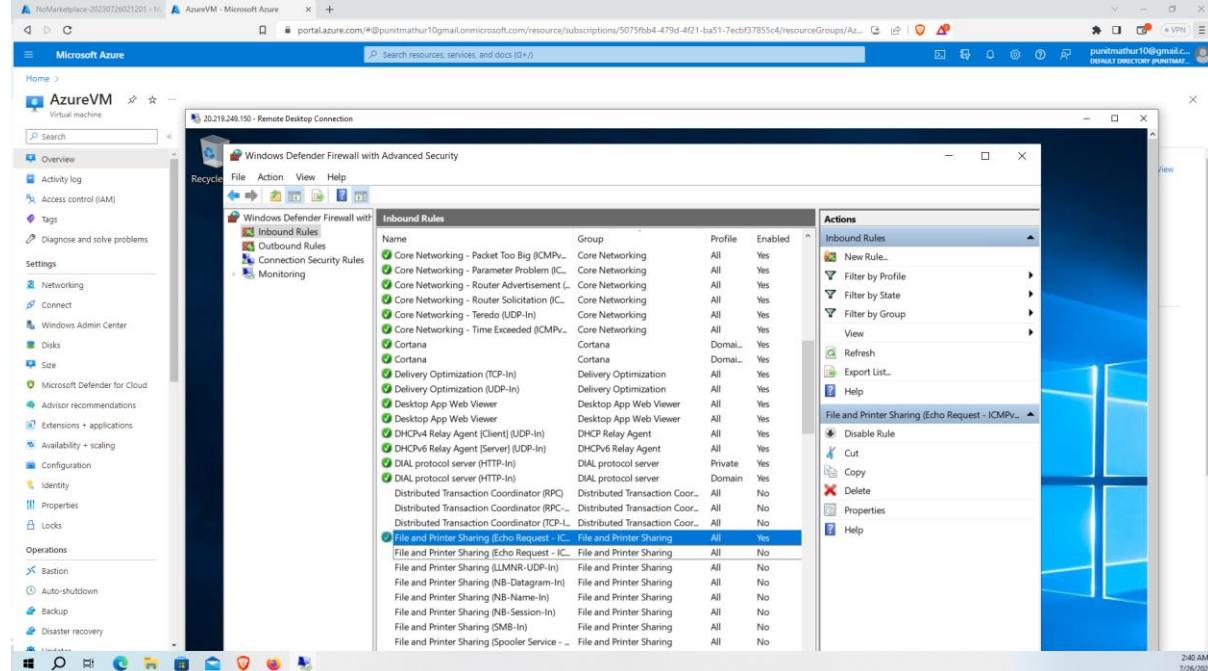
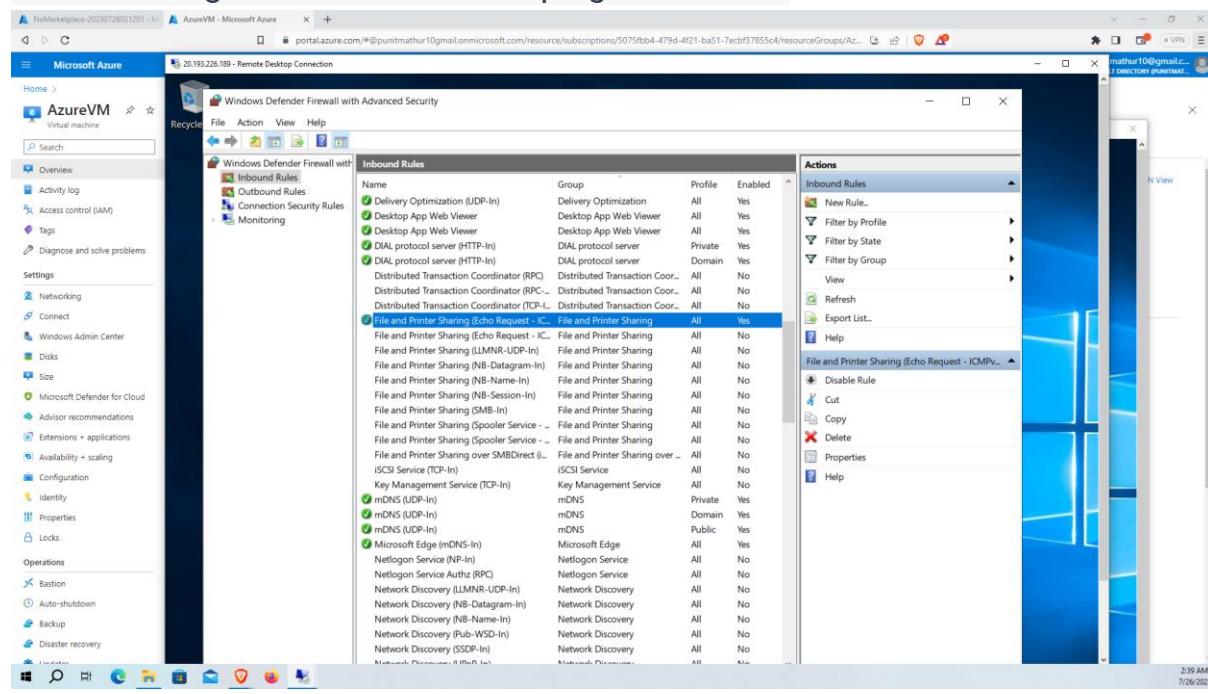
ROLES AND SERVER GROUPS

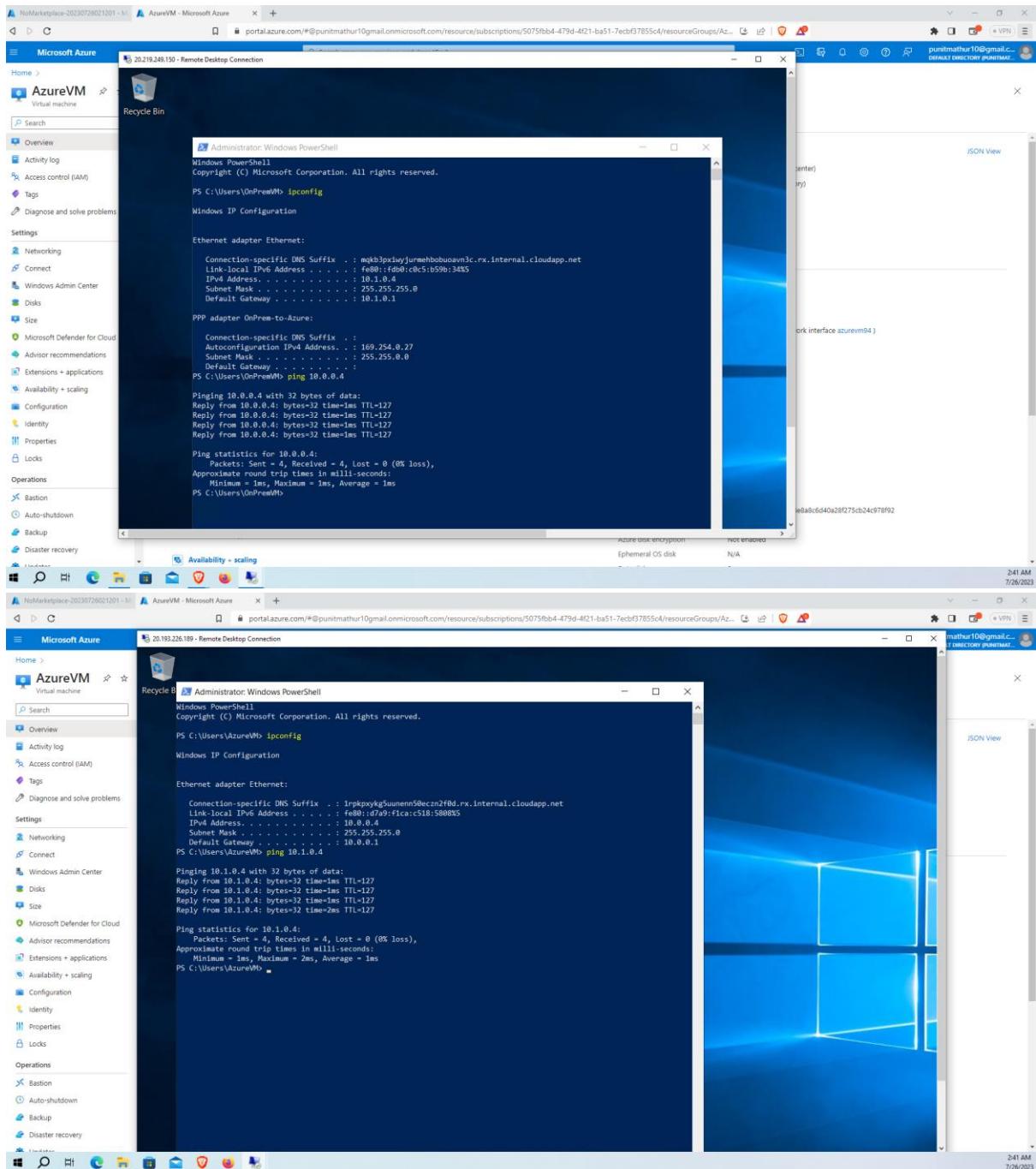
File and Storage Services: 1
IIS: 1
Remote Access: 1



Step 11 - Test Connectivity

Now to create connectivity we will connect to both the Azure VM and On Premise VM using RDP. Now before pinging each other we will first enable ICMP inbound rule in both the VMs using advanced firewall settings. Now after enabling ICMP both VMs will ping each other.





S2S connection is established.