CELEBAL TECHNOLOGY INTERNSHIP (CSI)

Name: Manaf Sherjada Khan

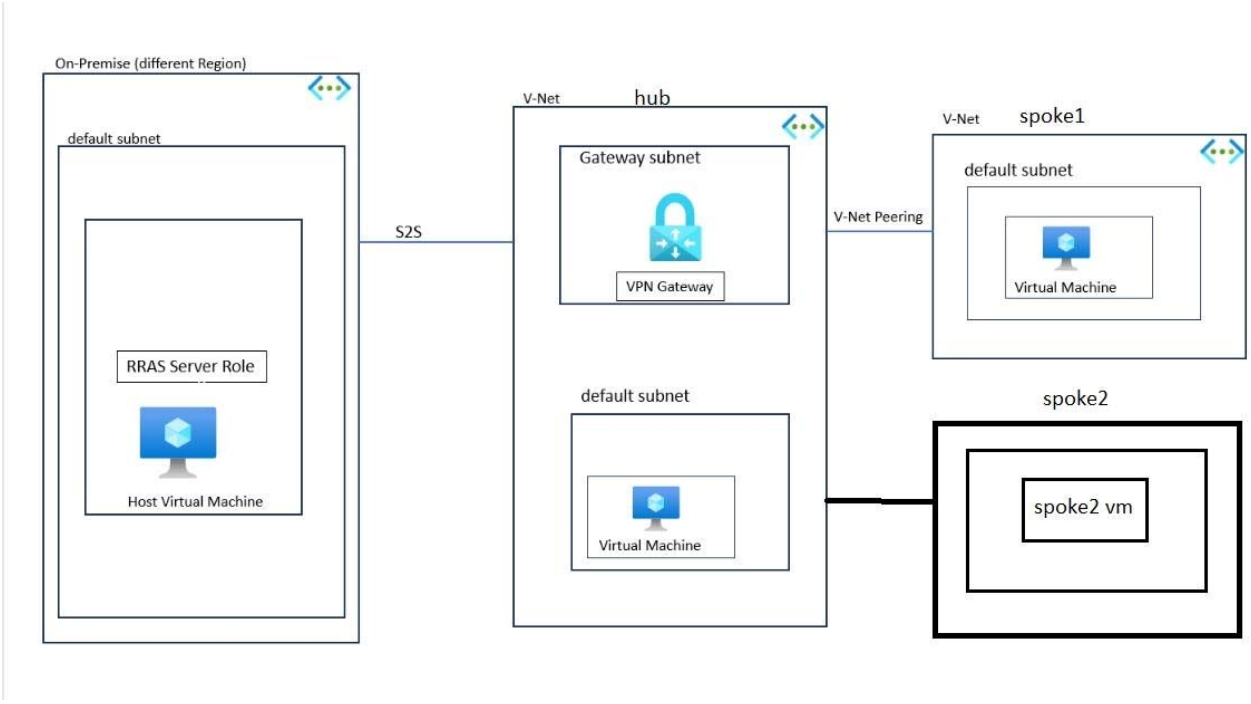
College: Lovely Professional University

Department: Cloud Infra & Security

CSI-ID: CT-CSI23/CIS0239

Project

Description: Configuration of On-premises to Hub and Spoke connectivity using S2S tunnelling from On-premises and hub and Transit Vnet peering from hub to spoke. Configure RRAS on on-premises VM and establish S2S connectivity to the Hub. The On-premise VM should be able to ping both Hub VM and Spoke VM successfully. The connectivity should be bi-directional. There is no direct connectivity established between spoke and On-premises Vnet.



Define site to site VPN in azure?

A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it.

Define Hub and Spoke in azure?

A hub-and-spoke network, often called star network, has a central component that's connected to multiple networks around it. The overall topology resembles a wheel, with a central hub connected to points along the edge of the wheel through multiple spokes.

Define Routing table in azure?

Azure Route Tables, or User Defined Routing, allow you to create network routes so that your CloudGen Firewall VM can handle the traffic both between your subnets and to the Internet. For the network interfaces to be allowed to receive and forward traffic, IP forwarding must be enabled.

Define peering in azure?

Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. The virtual networks appear as one for connectivity purposes. The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure

Overview:

To achieve the described configuration of On-premises to Hub and Spoke connectivity using S2S (Site-to-Site) tunneling and Transit VNet peering, we'll need to follow these steps:

Set up the On-premises VPN (RRAS) on the On-premises VM.

Create a Virtual Network Gateway for the Hub VNet and establish the S2S VPN tunnel between On-premises and Hub.

Set up Transit VNet peering between Hub and Spoke VNets.

Configure the necessary network routes to enable connectivity between On-premises, Hub, and Spoke VMs.

Set up On-premises VPN (RRAS) on the On-premises VM

Provision a Windows VM on your On-premises network and install the Routing and Remote Access Service (RRAS) role on it.

Configure RRAS to act as a VPN server and configure the necessary settings (IP ranges, authentication, encryption, etc.).

Make sure to configure a valid IP range for the VPN clients that does not overlap with any of your existing subnets.

Create Virtual Network Gateway for the Hub VNet

In your Azure portal, navigate to the Hub VNet's settings and click on "Create Gateway" to create a Virtual Network Gateway.

Select the appropriate VPN type (Route-based or Policy-based) based on your RRAS VPN configuration.

Complete the gateway creation process and note down the gateway's public IP address.

Establish S2S VPN Tunnel between On-premises and Hub

On your On-premises RRAS server, create a new S2S VPN connection and provide the public IP address of the Virtual Network Gateway in the Hub VNet.

Configure the authentication settings and any other necessary options to match the settings of the Virtual Network Gateway.

Once the connection is established, you should see "Connected" status on both the On-premises and Hub gateways.

Set up Transit VNet Peering between Hub and Spoke VNets

In the Azure portal, go to the "Peering's" section of the Hub VNet and create a new peering with the Spoke VNet.

Repeat the process in the Spoke VNet to create a peering with the Hub VNet.

Ensure that "Use remote gateways" is enabled in both VNet peerings.

Configure Network Routes

On the Hub VNet, add a route table that directs traffic to the On-premises network via the Virtual Network Gateway.

In the route table, define a route for the On-premises network (configured in RRAS) with the next hop as the Virtual Network Gateway.

Similarly, on the Spoke VNet, add a route table that directs traffic to the On-premises network via the peered connection to the Hub VNet.

In the route table, define a route for the On-premises network with the next hop as the IP address of the peered connection to the Hub VNet.

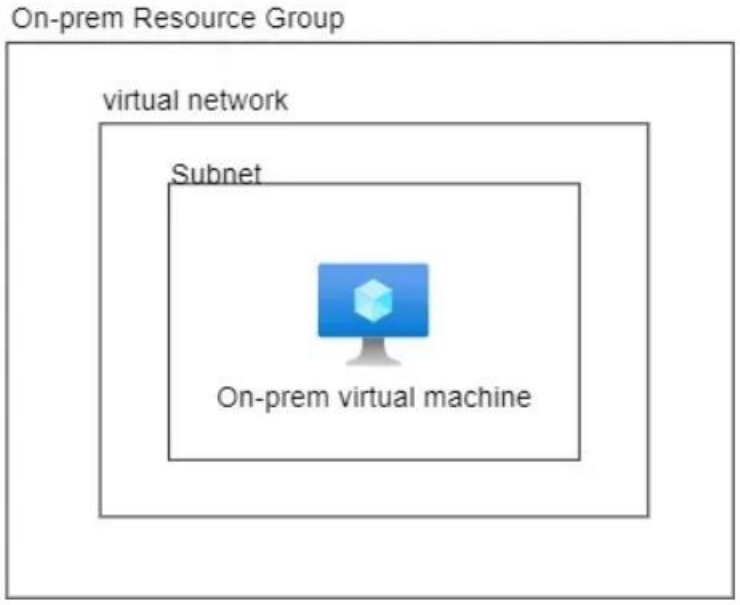
With the above configuration, your On-premises VM should be able to ping both the Hub VM and the Spoke VM successfully, and the connectivity should be bi-directional.

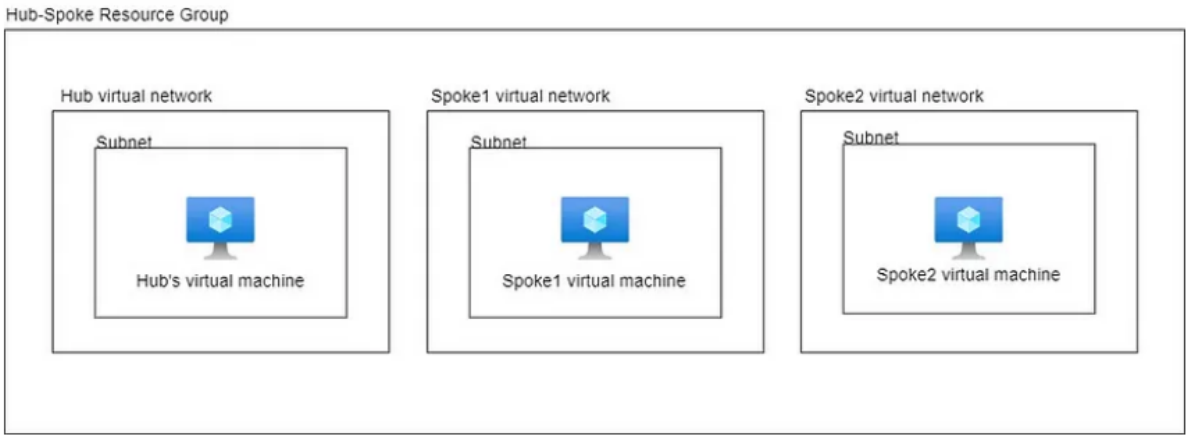
Please note that this setup assumes you have the necessary permissions and access to configure the network settings in your Azure subscription. Also, ensure that the firewall settings on your VMs allow the required traffic for successful communication.

Steps to achieve the complete project

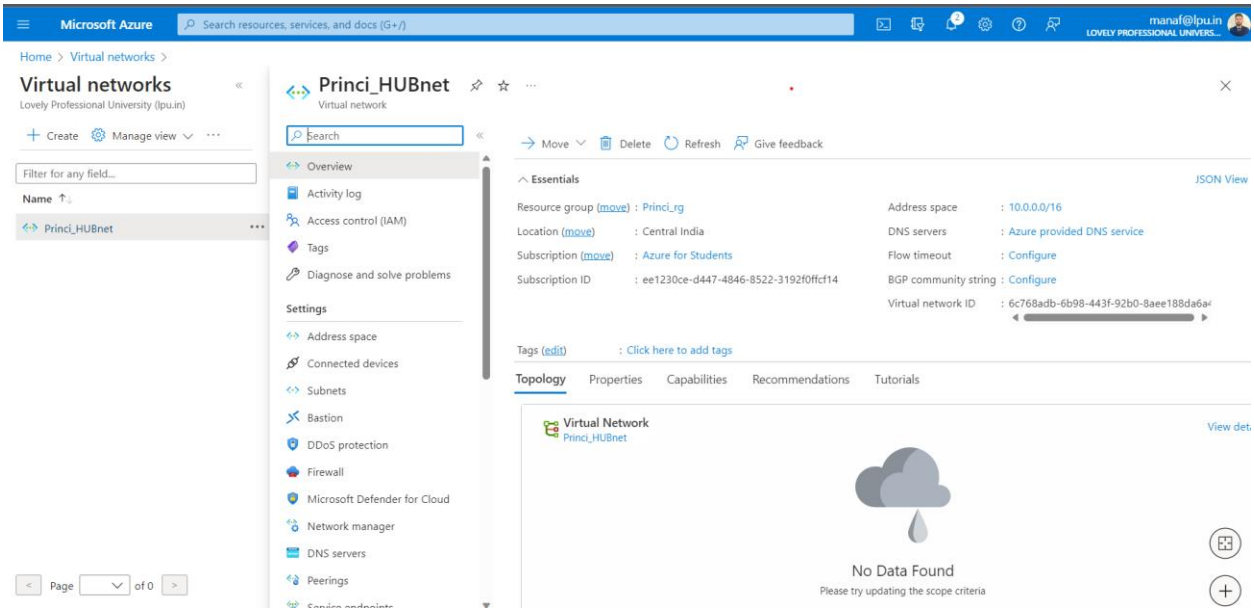
STEPS:

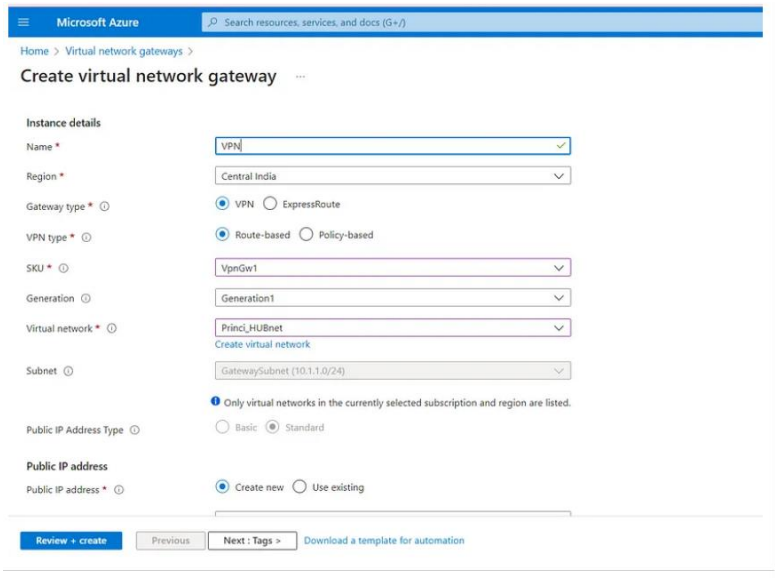
STEP 1: Deploy required resources

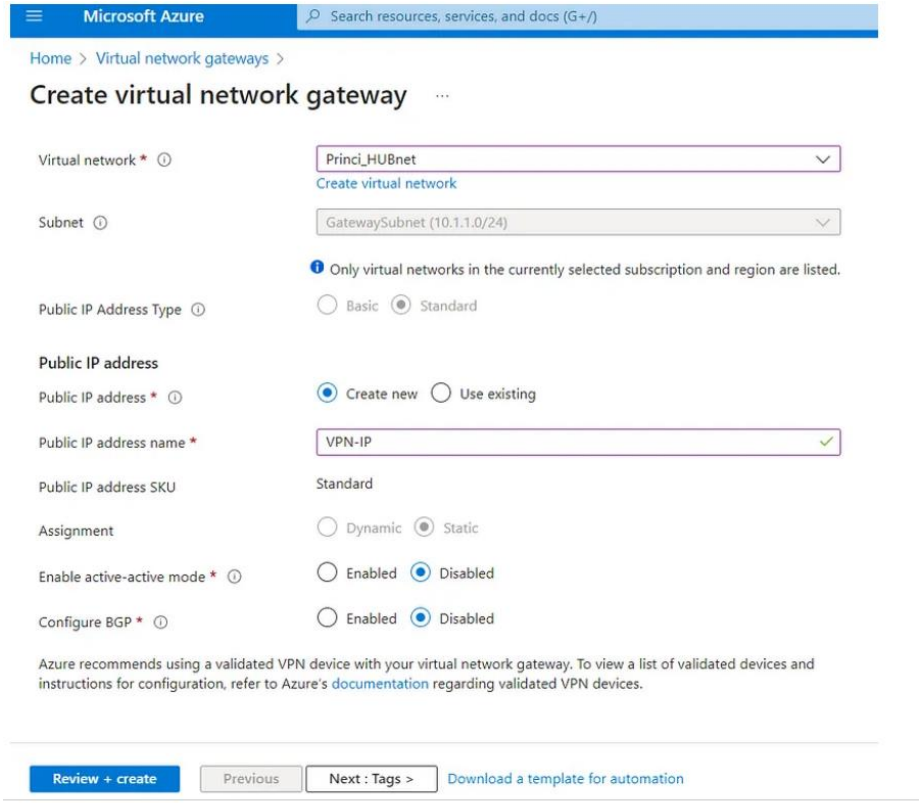


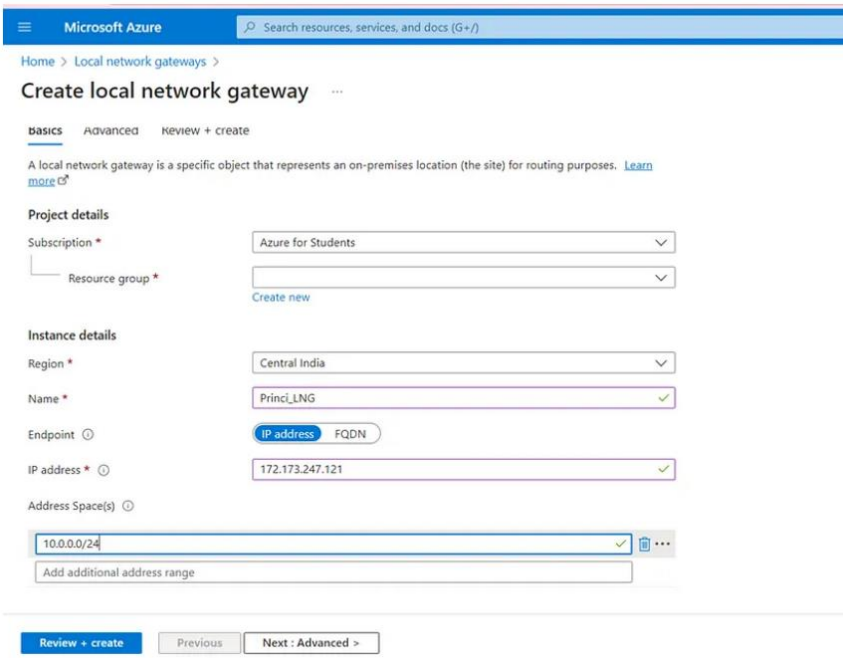


Step 2: Deploy virtual network gateway and local network gateway

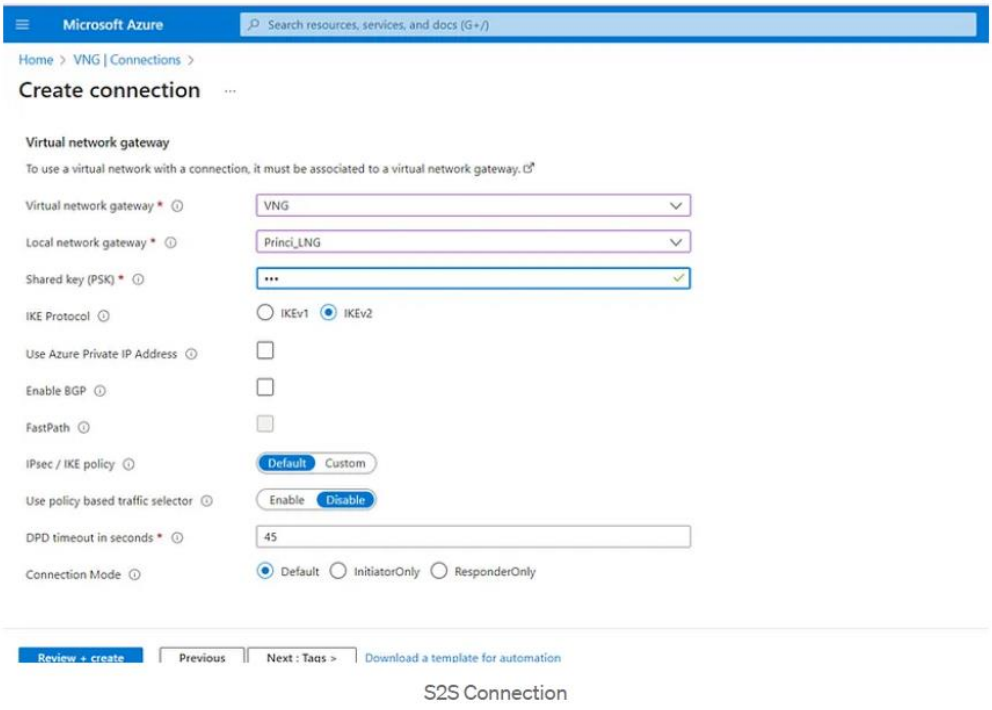





Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual network gateways >
Create virtual network gateway
Virtual network *
Princi_HUBnet
Create virtual network
Subnet
GatewaySubnet (10.1.1.0/24)
Only virtual networks in the currently selected subscription and region are listed.
Public IP Address Type
Basic
Standard
Public IP address
Public IP address *
Create new
Use existing
Public IP address name *
VPN-IP
Public IP address SKU
Standard
Assignment
Dynamic
Static
Enable active-active mode *
Enabled
Disabled
Configure BGP *
Enabled
Disabled
Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's documentation regarding validated VPN devices.
Review + create
Previous
Next : Tags >
Download a template for automation

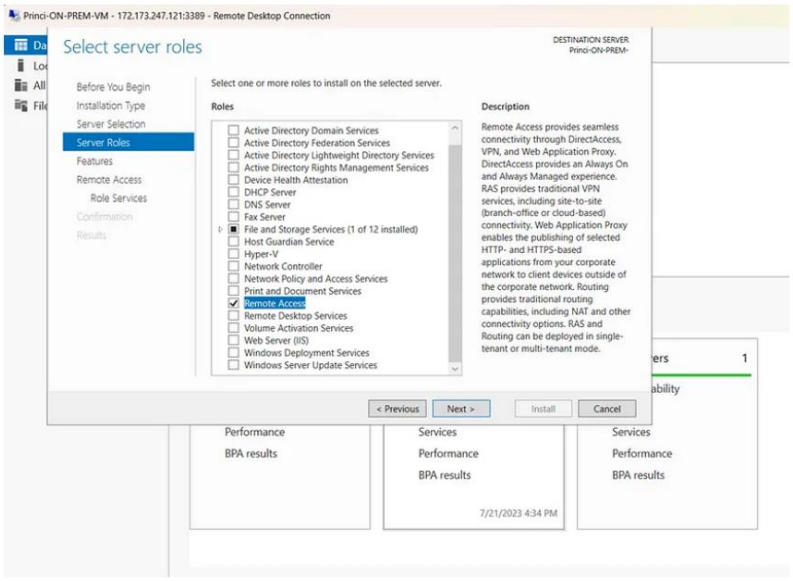


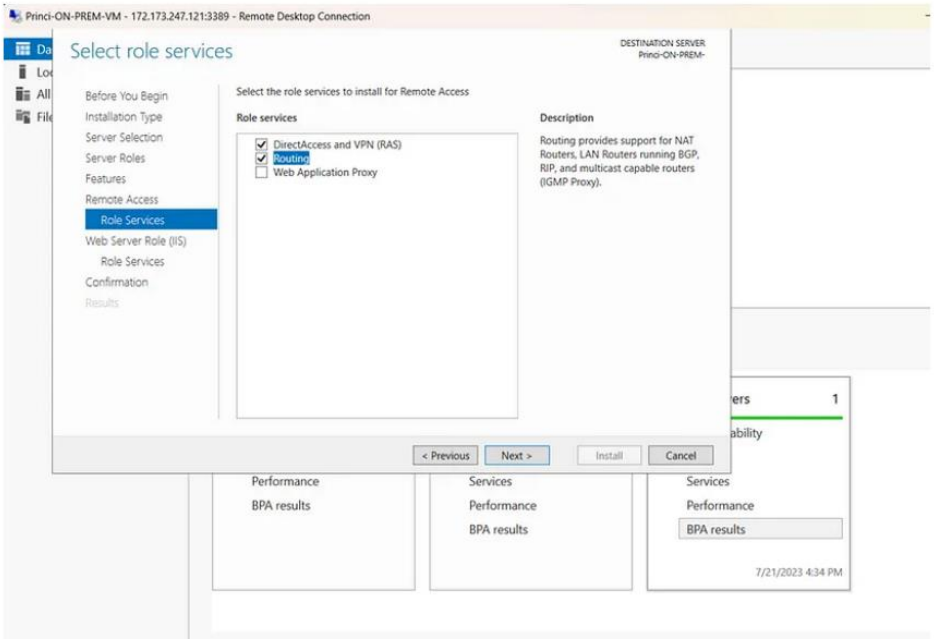
STEP 3: Configure S2S connection

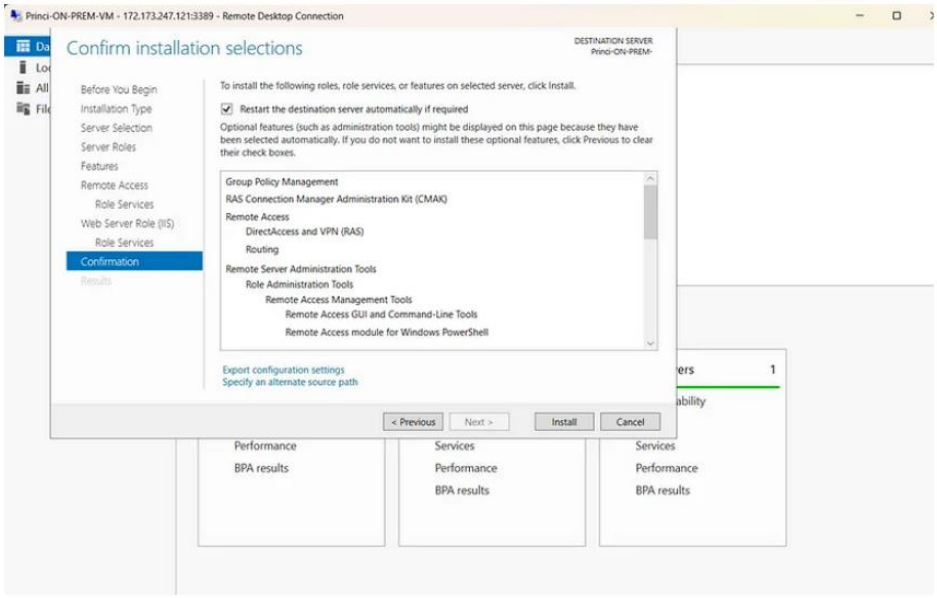


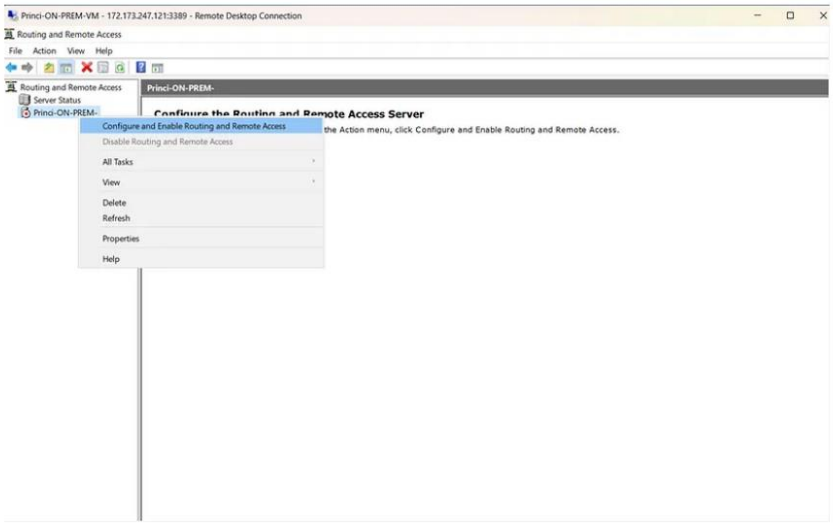
S2S Connection

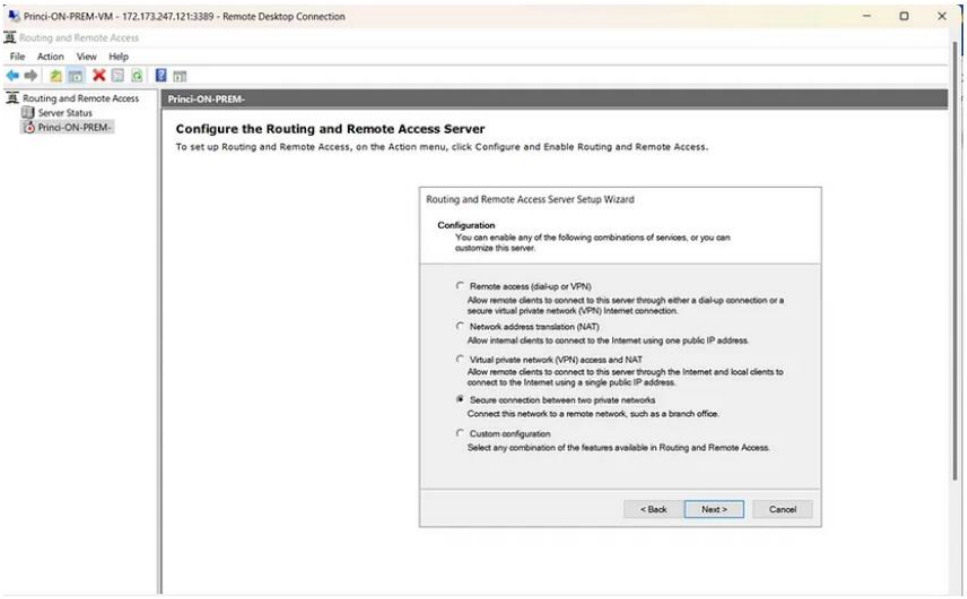
STEP 4: Configure RRAS

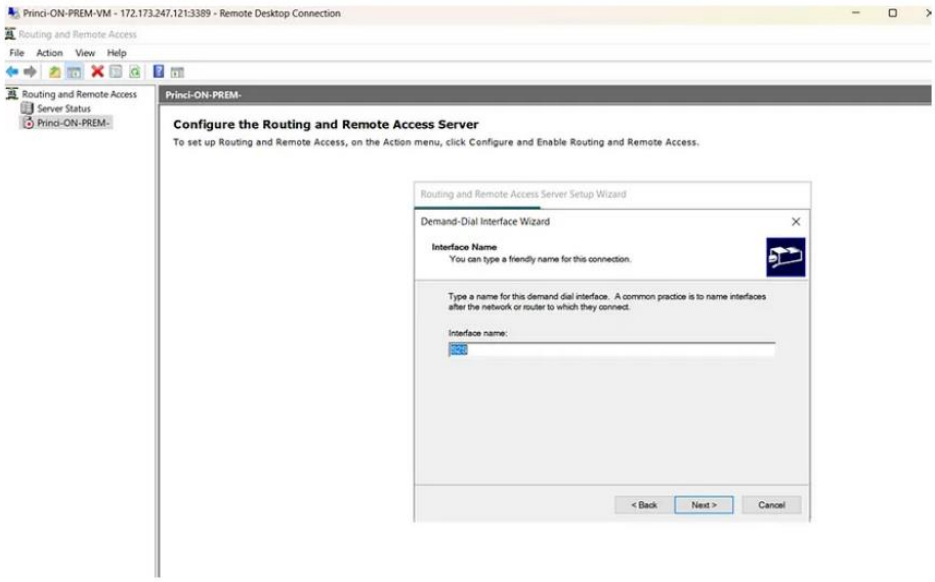


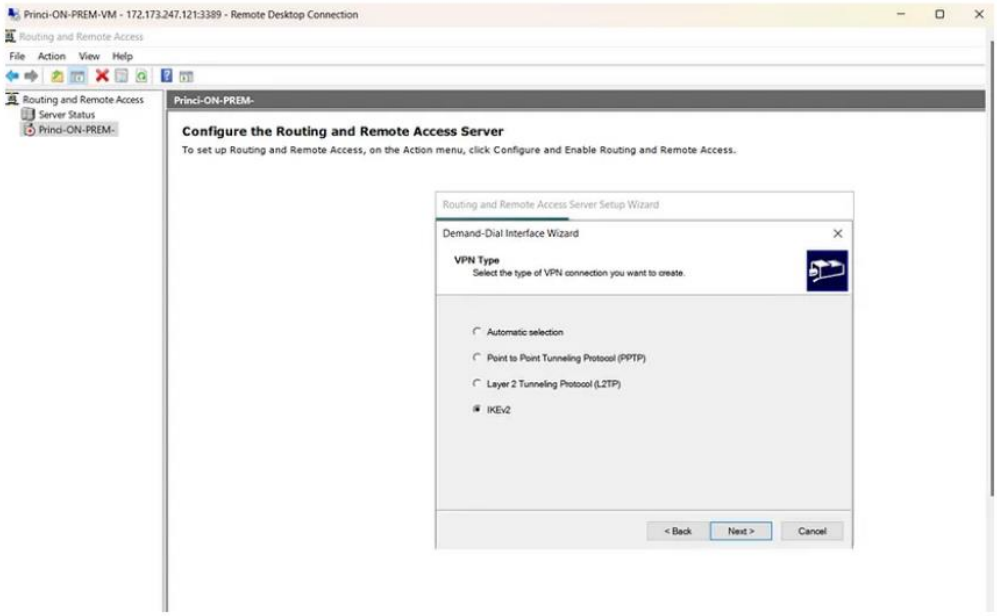


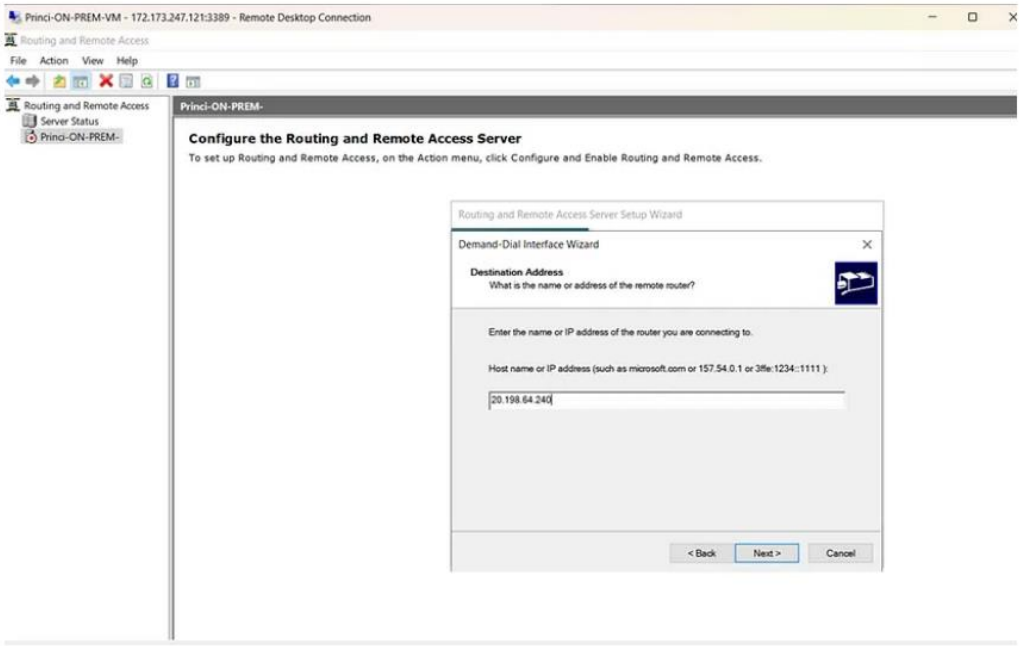

Princi-ON-PREM-VM - 172.173.247.121:3389 - Remote Desktop Connection
Confirm installation selections
DESTINATION SERVER
Princi-ON-PREM-
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Remote Access
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Group Policy Management
RAS Connection Manager Administration Kit (CMAK)
Remote Access
DirectAccess and VPN (RAS)
Routing
Remote Server Administration Tools
Role Administration Tools
Remote Access Management Tools
Remote Access GUI and Command-Line Tools
Remote Access module for Windows PowerShell
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel
Performance
BPA results
Services
Performance
BPA results
Services
Performance
BPA results

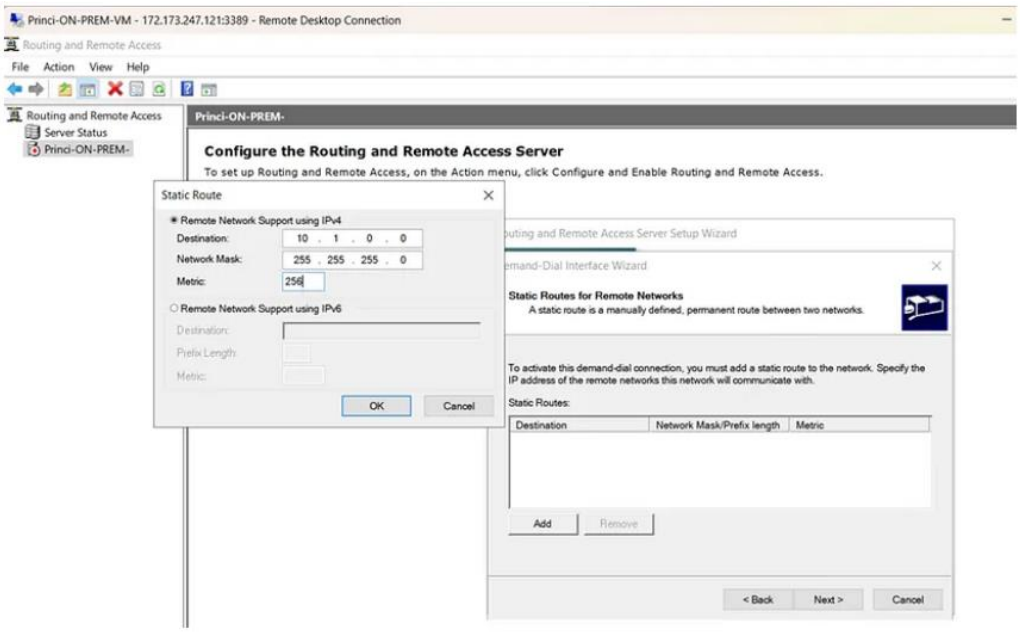

Princi-ON-PREM-VM - 172.173.247.121:3389 - Remote Desktop Connection
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
Princi-ON-PREM-
Princi-ON-PREM-
Configure the Routing and Remote Access Server
the Action menu, click Configure and Enable Routing and Remote Access.
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help

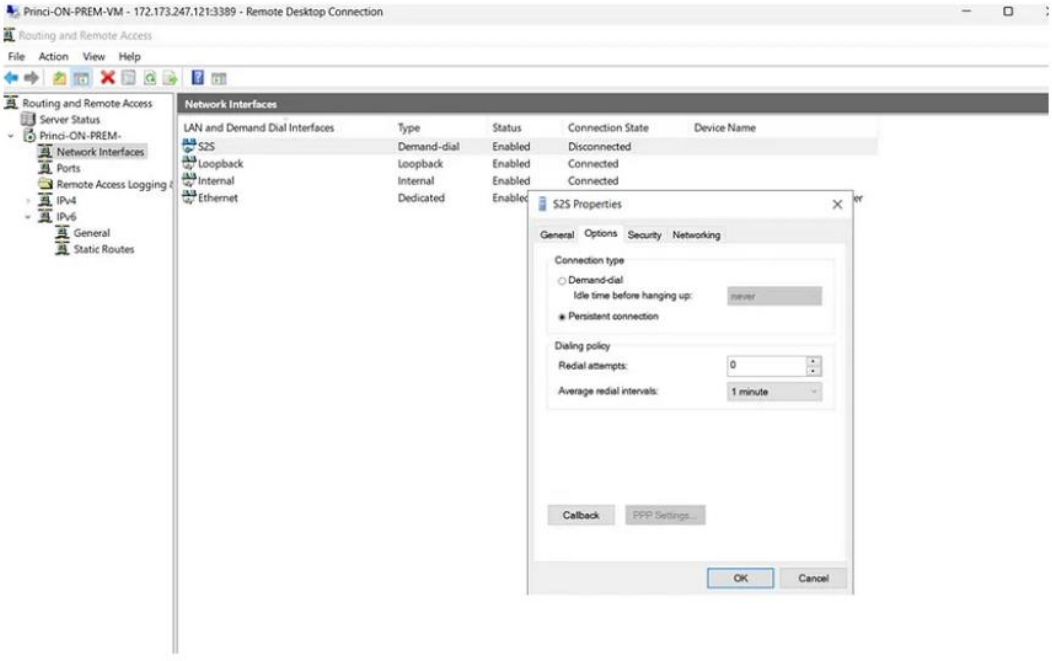

Princi-ON-PREM-VM - 172.173.247.121:3389 - Remote Desktop Connection
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
Princi-ON-PREM-
Princi-ON-PREM-
Configure the Routing and Remote Access Server
To set up Routing and Remote Access, on the Action menu, click Configure and Enable Routing and Remote Access.
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 this 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

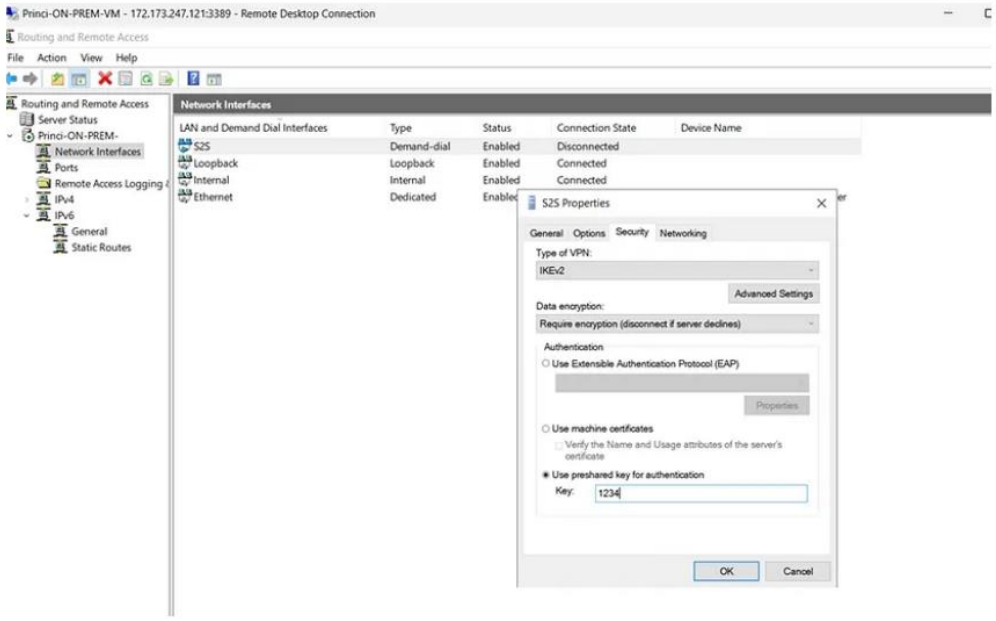

Princi-ON-PREM-VM - 172.173.247.121:3389 - Remote Desktop Connection
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
Princi-ON-PREM-
Princi-ON-PREM-
Configure the Routing and Remote Access Server
To set up Routing and Remote Access, on the Action menu, click Configure and Enable Routing and Remote Access.
Routing and Remote Access Server Setup Wizard
Demand-Dial Interface Wizard
Interface Name
You can type a friendly name for this connection.
Type a name for this demand dial interface. A common practice is to name interfaces after the network or router to which they connect.
Interface name:
< Back
Next >
Cancel

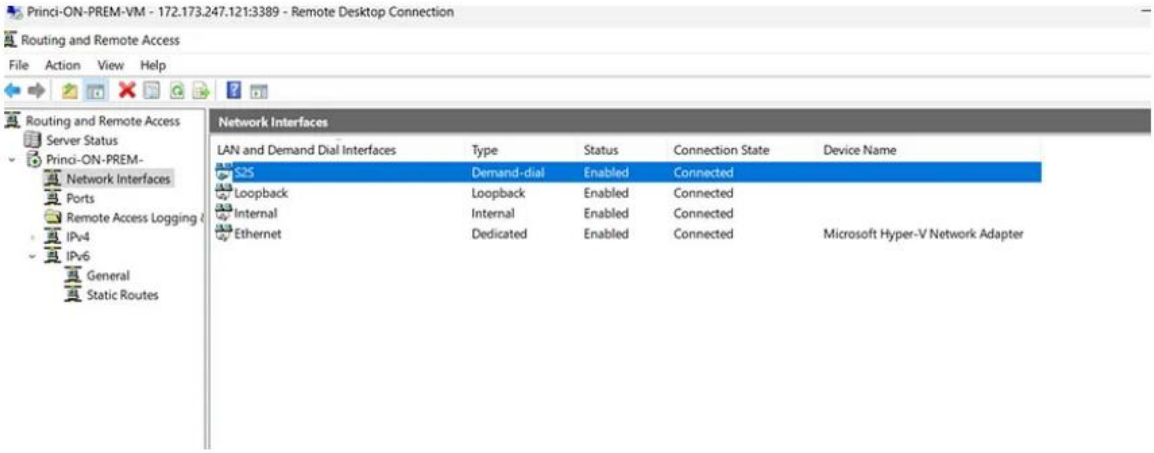

Princi-ON-PREM-VM - 172.173.247.121:3389 - Remote Desktop Connection
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
Princi-ON-PREM-
Princi-ON-PREM-
Configure the Routing and Remote Access Server
To set up Routing and Remote Access, on the Action menu, click Configure and Enable Routing and Remote Access.
Routing and Remote Access Server Setup Wizard
Demand-Dial Interface Wizard
VPN Type
Select the type of VPN connection you want to create.
Automatic selection
Point to Point Tunneling Protocol (PPTP)
Layer 2 Tunneling Protocol (L2TP)
IKEv2
< Back
Next >
Cancel


Princi-ON-PREM-VM - 172.173.247.121:3389 - Remote Desktop Connection
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
Princi-ON-PREM-
Princi-ON-PREM-
Configure the Routing and Remote Access Server
To set up Routing and Remote Access, on the Action menu, click Configure and Enable Routing and Remote Access.
Routing and Remote Access Server Setup Wizard
Demand-Dial Interface Wizard
Destination Address
What is the name or address of the remote router?
Enter the name or IP address of the router you are connecting to.
Host name or IP address (such as microsoft.com or 157.54.0.1 or 3ffe:1234::1111):
20.198.64.240
< Back
Next >
Cancel

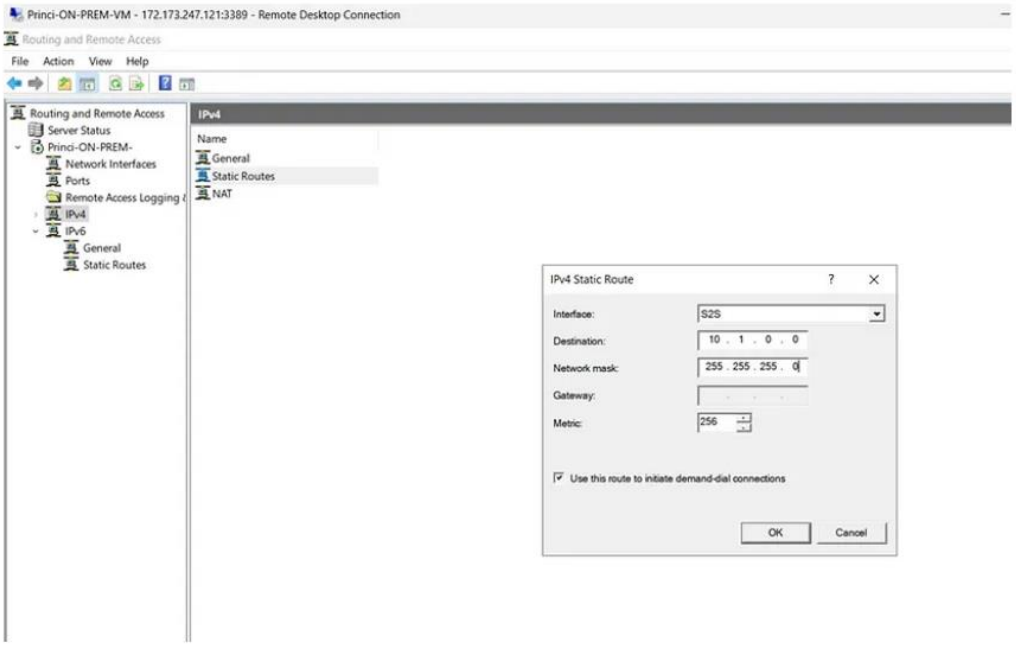

Princi-ON-PREM-VM - 172.173.247.121:3389 - Remote Desktop Connection
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
Princi-ON-PREM-
Princi-ON-PREM-
Configure the Routing and Remote Access Server
To set up Routing and Remote Access, on the Action menu, click Configure and Enable Routing and Remote Access.
Static Route
Remote Network Support using IPv4
Destination: 10 . 1 . 0 . 0
Network Mask: 255 . 255 . 255 . 0
Metric: 256
Remote Network Support using IPv6
Destination:
Prefix Length:
Metric:
OK
Cancel
Routing and Remote Access Server Setup Wizard
Demand-Dial Interface Wizard
Static Routes for Remote Networks
A static route is a manually defined, permanent route between two networks.
To activate this demand-dial connection, you must add a static route to the network. Specify the IP address of the remote networks this network will communicate with.
Static Routes:
Destination
Network Mask/Prefix length
Metric
Add
Remove
< Back
Next >
Cancel

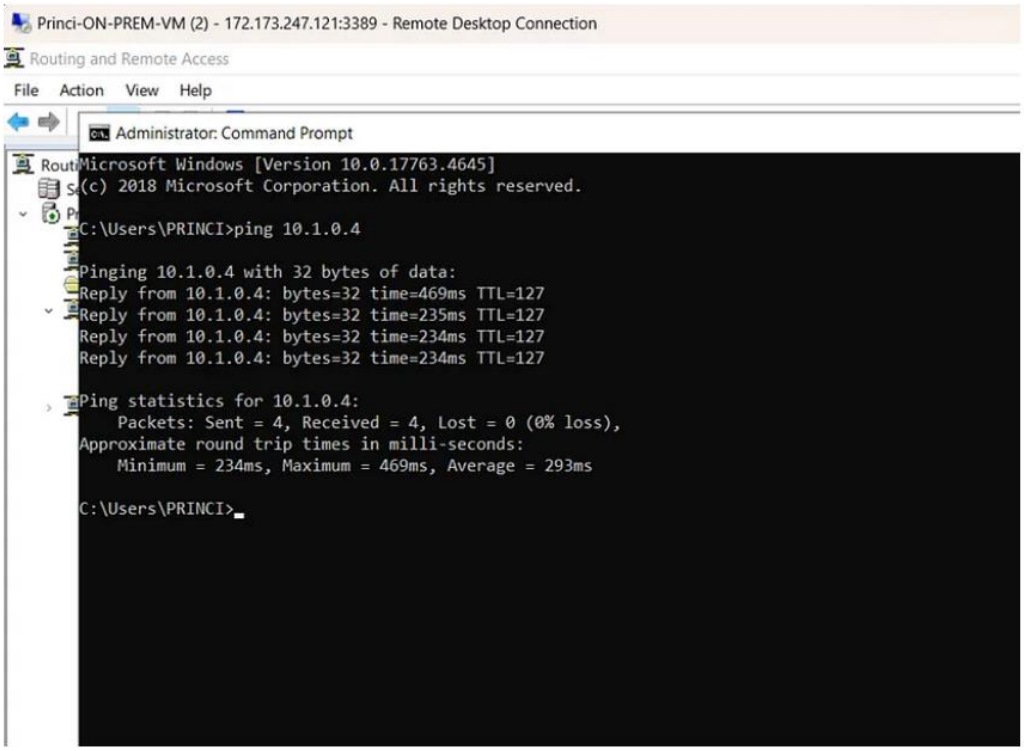

Princi-ON-PREM-VM - 172.173.247.121:3389 - Remote Desktop Connection
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
Princi-ON-PREM-
Network Interfaces
Ports
Remote Access Logging
IPv4
IPv6
General
Static Routes
Network Interfaces
LAN and Demand Dial Interfaces
Type
Status
Connection State
Device Name
S2S
Demand-dial
Enabled
Disconnected
Loopback
Loopback
Enabled
Connected
Internal
Internal
Enabled
Connected
Ethernet
Dedicated
S2S Properties
General
Options
Security
Networking
Connection type
Demand-dial
Idle time before hanging up:
never
Persistent connection
Dialing policy
Redial attempts:
0
Average redial intervals:
1 minute
Callback
PPP Settings...
OK
Cancel

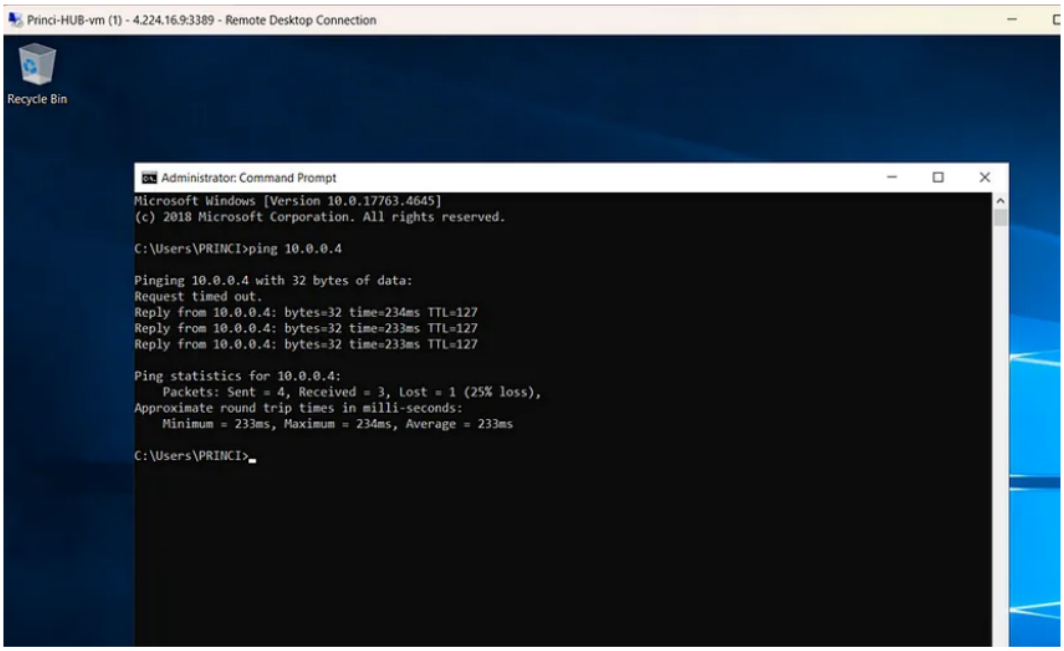

Princi-ON-PREM-VM - 172.173.247.121:3389 - Remote Desktop Connection
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
Princi-ON-PREM-
Network Interfaces
Ports
Remote Access Logging
IPv4
IPv6
General
Static Routes
Network Interfaces
LAN and Demand Dial Interfaces
Type
Status
Connection State
Device Name
S2S
Demand-dial
Enabled
Disconnected
Loopback
Loopback
Enabled
Connected
Internal
Internal
Enabled
Connected
Ethernet
Dedicated
S2S Properties
General
Options
Security
Networking
Type of VPN:
IKEv2
Advanced Settings
Data encryption:
Require encryption (disconnect if server declines)
Authentication
Use Extensible Authentication Protocol (EAP)
Properties
Use machine certificates
Verify the Name and Usage attributes of the server's certificate
Use preshared key for authentication
Key:
1234
OK
Cancel


Princi-ON-PREM-VM - 172.173.247.121:3389 - Remote Desktop Connection
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
Princi-ON-PREM-
Network Interfaces
Ports
Remote Access Logging
IPv4
IPv6
General
Static Routes
Network Interfaces
LAN and Demand Dial Interfaces
Type
Status
Connection State
Device Name
S2S
Demand-dial
Enabled
Connected
Loopback
Loopback
Enabled
Connected
Internal
Internal
Enabled
Connected
Ethernet
Dedicated
Enabled
Connected
Microsoft Hyper-V Network Adapter

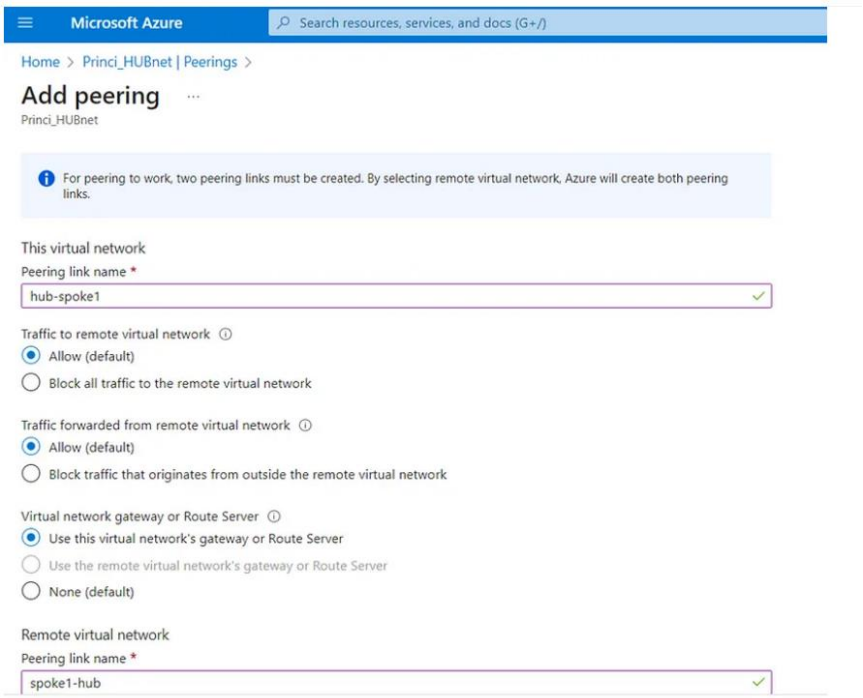
STEP 5: Connect on-premises virtual machine and hub

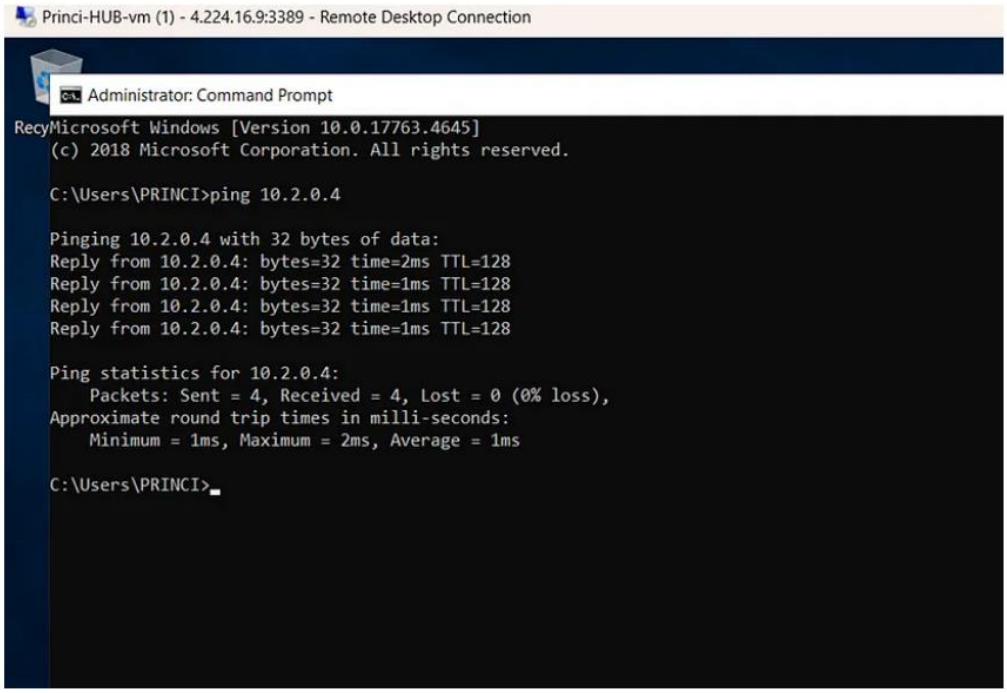


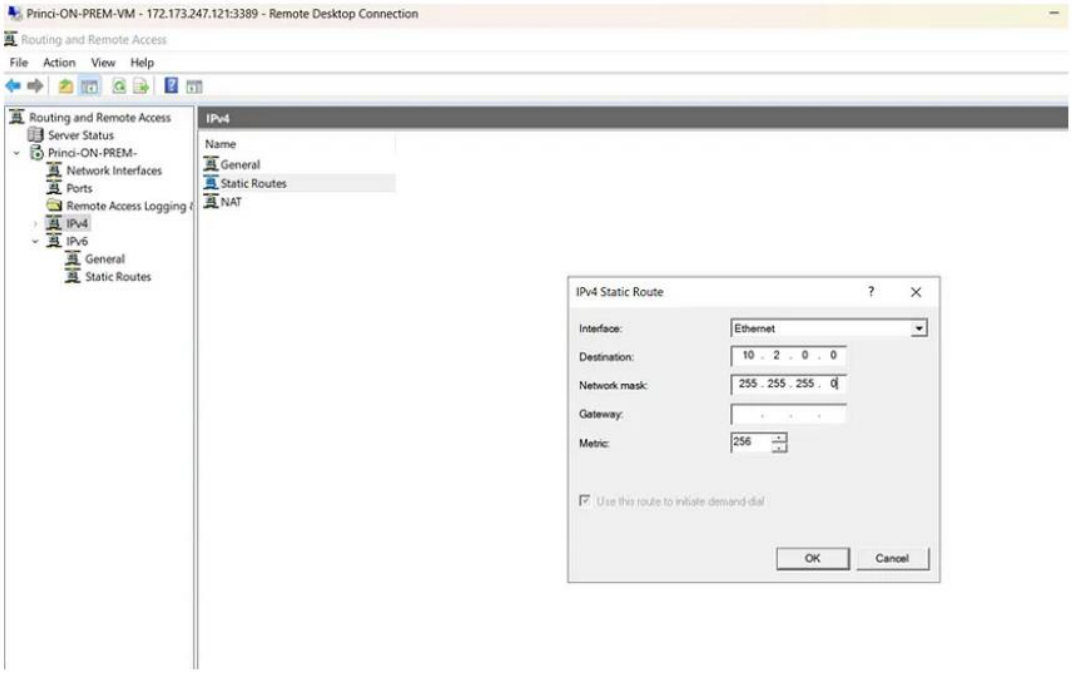


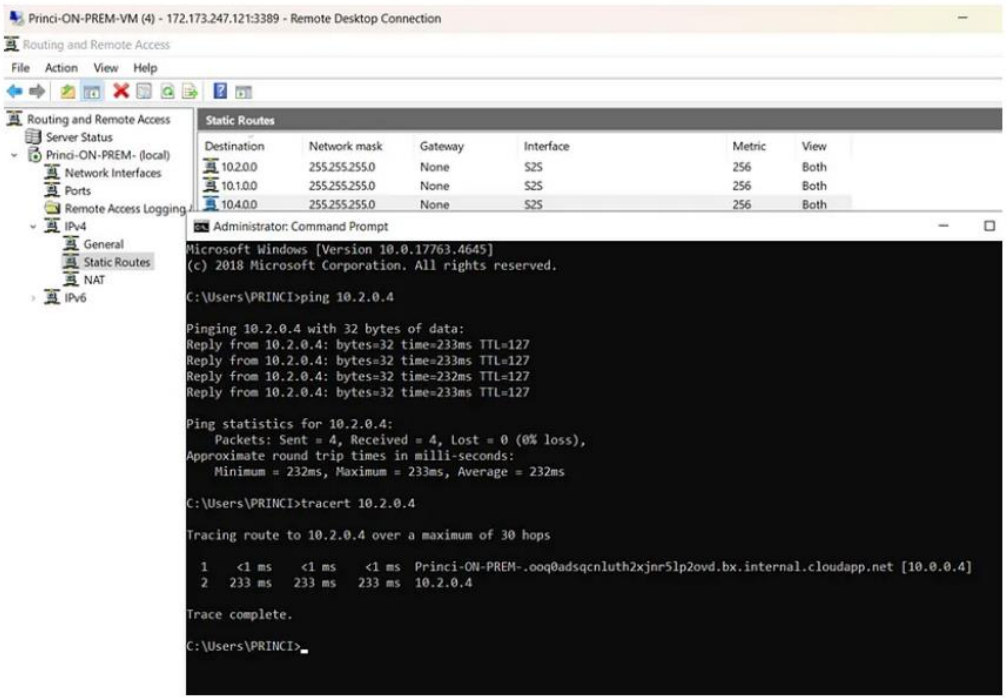


STEP 6: Connect hub to spokes and on-premises to spokes

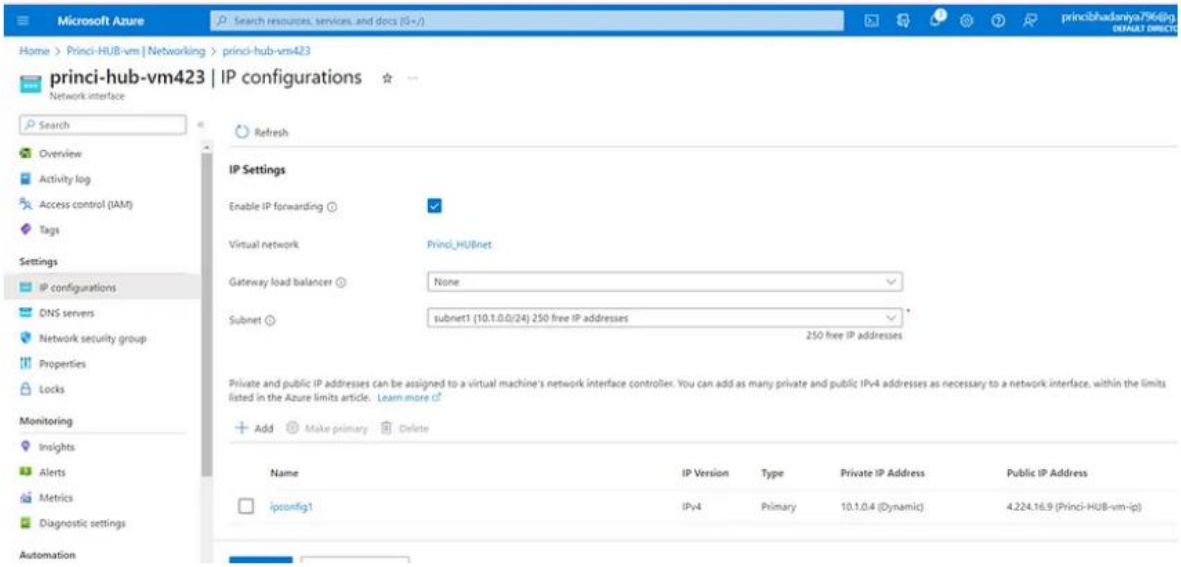



Princi-HUB-vm (1) - 4.224.16.9:3389 - Remote Desktop Connection
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.4645]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\PRINCI>ping 10.2.0.4
Pinging 10.2.0.4 with 32 bytes of data:
Reply from 10.2.0.4: bytes=32 time=2ms TTL=128
Reply from 10.2.0.4: bytes=32 time=1ms TTL=128
Reply from 10.2.0.4: bytes=32 time=1ms TTL=128
Reply from 10.2.0.4: bytes=32 time=1ms TTL=128
Ping statistics for 10.2.0.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 2ms, Average = 1ms
C:\Users\PRINCI>


Princi-ON-PREM-VM - 172.173.247.121:3389 - Remote Desktop Connection
Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
Princi-ON-PREM-
Network Interfaces
Ports
Remote Access Logging
IPv4
IPv6
General
Static Routes
IPv4
Name
General
Static Routes
NAT
IPv4 Static Route
Interface: Ethernet
Destination: 10 . 2 . 0 . 0
Network mask: 255 . 255 . 255 . 0
Gateway:
Metric: 256
Use this route to initiate demand-dial
OK
Cancel



STEP 7: Connect spokes



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

Home > Route tables >

Create Route table ...

Basics 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 * : Azure for Students

Resource group * : HUB

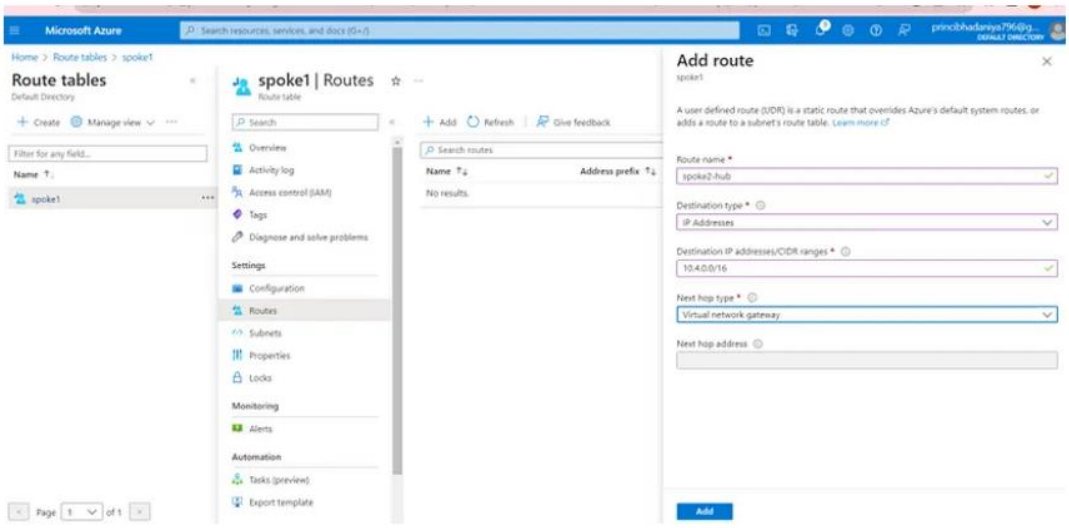
Create new

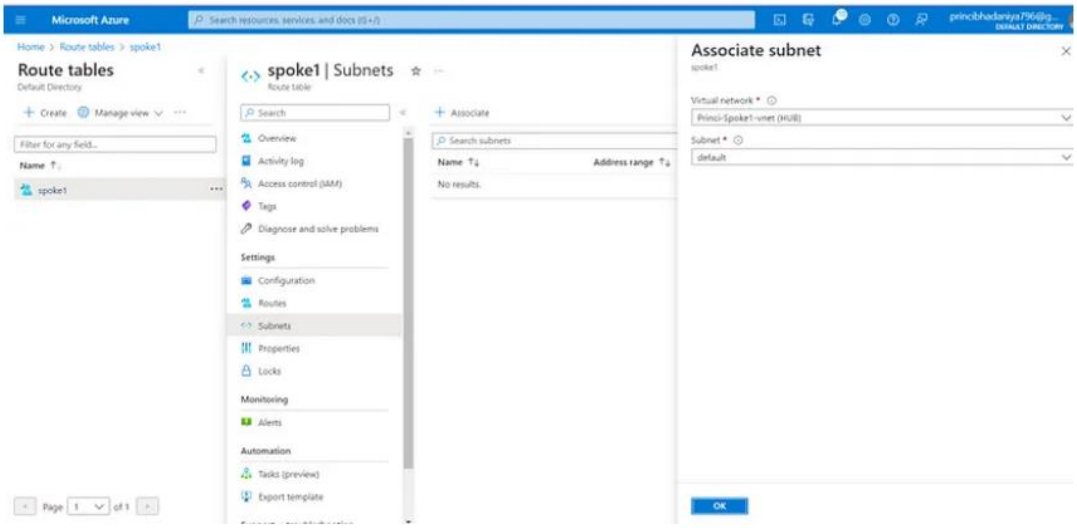
Instance details

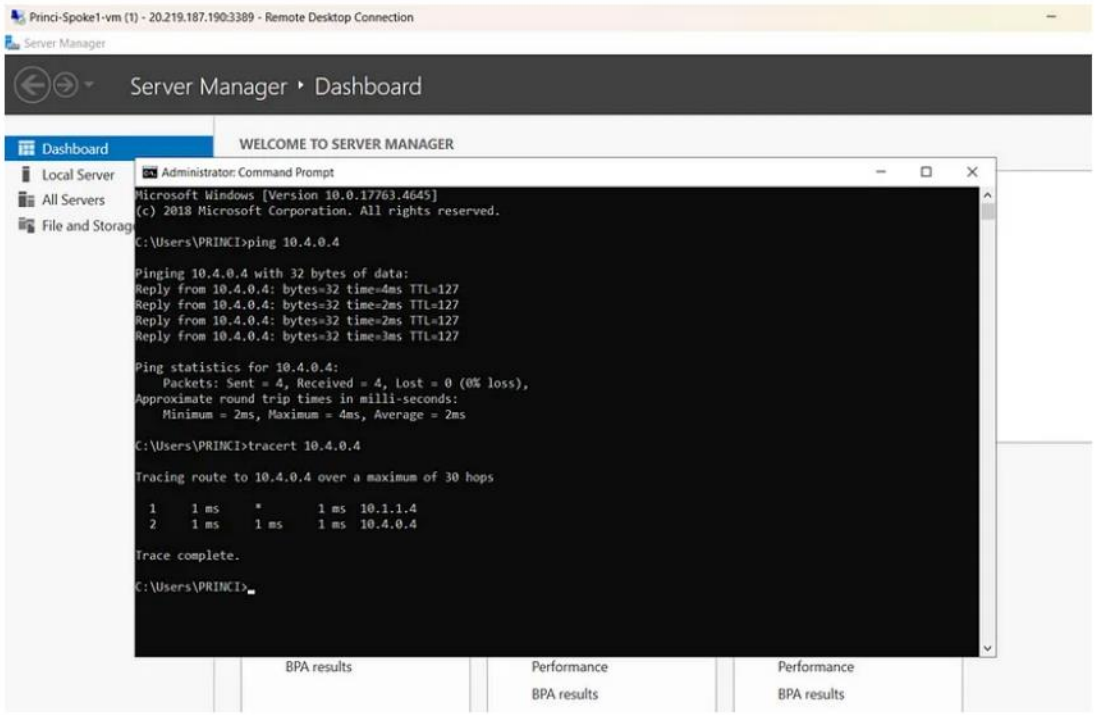
Region * : Central India

Name * : spoke1

Propagate gateway routes * : (•) Yes ( ) No




Microsoft Azure
Search resources, services, and docs (G+/)
princibhadaniya7196@g...
DEFAULT DIRECTORY
Home > Route tables > spoke1
Route tables
Default Directory
Create
Manage view
Filter for any field...
Name
spoke1
Page 1 of 1
spoke1 | Subnets
Route table
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Routes
Subnets
Properties
Locks
Monitoring
Alerts
Automation
Tasks (preview)
Export template
Associate
Search subnets
Name
Address range
No results.
Associate subnet
spoke1
Virtual network *
Princi-Spoke1-vnet (HUB)
Subnet *
default
OK


Princi-Spoke1-vm (1) - 20.219.187.190:3389 - Remote Desktop Connection
Server Manager
Server Manager • Dashboard
Dashboard
Local Server
All Servers
File and Storag
WELCOME TO SERVER MANAGER
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17763.4645]
(c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\PRINCI>ping 10.4.0.4
Pinging 10.4.0.4 with 32 bytes of data:
Reply from 10.4.0.4: bytes=32 time=4ms TTL=127
Reply from 10.4.0.4: bytes=32 time=2ms TTL=127
Reply from 10.4.0.4: bytes=32 time=2ms TTL=127
Reply from 10.4.0.4: bytes=32 time=3ms TTL=127
Ping statistics for 10.4.0.4:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 2ms, Maximum = 4ms, Average = 2ms
C:\Users\PRINCI>tracert 10.4.0.4
Tracing route to 10.4.0.4 over a maximum of 30 hops
1 1 ms * 1 ms 10.1.1.4
2 1 ms 1 ms 1 ms 10.4.0.4
Trace complete.
C:\Users\PRINCI>
BPA results
Performance
BPA results
Performance
BPA results