😊 Azur User-Defined Routes

User-defined routes (UDRs) in Azure allow you to control the routing of network traffic within your Azure virtual network (VNet). By default, Azure routes traffic between subnets within a VNet using system routes. However, with UDRs, you can override these default routes and define custom routes to meet specific networking requirements.

Here's how it works:

1. **Route Tables:** UDRs are implemented using route tables. Each subnet within a VNet is associated with a route table, which contains a set of rules (routes) that specify the next hop for traffic destined to particular IP ranges.
2. **Custom Routes:** You can define custom routes in a route table to direct traffic to specific destinations. For example, you might have a virtual appliance or firewall deployed in your network, and you want all traffic destined for the internet to pass through it. In this case, you would create a custom route in the route table specifying the next hop as the IP address of the virtual appliance.
3. **Route Prioritization:** Routes in a route table are evaluated in priority order, with the most specific route taking precedence. This means that if there are overlapping routes, the more specific route will be chosen.
4. **Associating Route Tables:** You can associate a route table with one or more subnets within a VNet. This allows you to apply different routing configurations to different subnets within the same VNet.
5. **Default Routes:** Even with custom routes, Azure still uses default system routes for certain types of traffic, such as traffic destined for Azure services outside of the VNet.

Overall, user-defined routes give you granular control over how traffic is routed within your Azure virtual network, allowing you to optimize performance, implement security measures, and integrate with on-premises network infrastructure.

😄 Use cases of User Defined Routes:

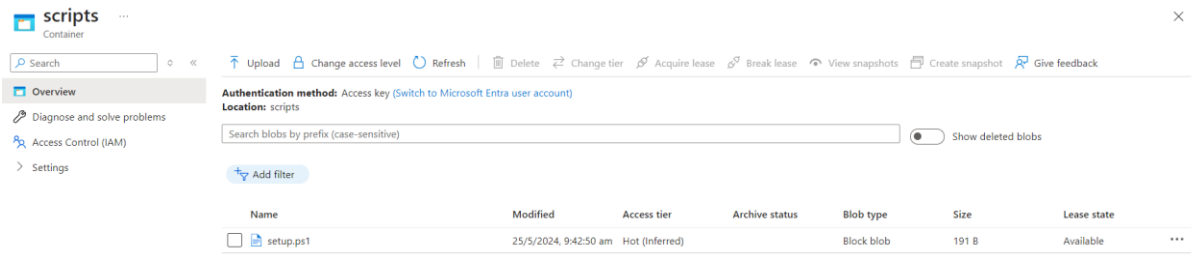
User-defined routes (UDRs) in Azure can be utilized in various scenarios to tailor network traffic routing according to specific requirements. Here are some common use cases:

1. **Network Virtual Appliance (NVA) Integration:** Many organizations deploy network virtual appliances such as firewalls, intrusion detection systems (IDS), or virtual private network (VPN) gateways within their Azure virtual networks. UDRs can be used to direct traffic to these NVAs for inspection, filtering, or encryption before forwarding it to its destination.
2. **Secure Hybrid Connectivity:** When establishing a hybrid network environment connecting on-premises data centers with Azure VNets, UDRs can route traffic through specific paths, such as VPN gateways or ExpressRoute circuits. This ensures secure and optimized communication between on-premises resources and resources deployed in Azure.

3. **Internet Traffic Redirection:** UDRs can redirect internet-bound traffic through a virtual appliance or firewall deployed in the Azure network. This allows organizations to implement centralized security policies and inspect outgoing traffic for threats or compliance purposes before it leaves the Azure environment.
4. **Traffic Optimization:** By defining custom routes, organizations can optimize traffic flow within Azure VNets. For example, you can create routes to direct traffic between subnets through the most efficient paths, reducing latency and improving overall network performance.
5. **Multi-tier Application Architectures:** In complex application architectures with multiple tiers (e.g., web servers, application servers, and databases), UDRs can be used to control traffic flows between different tiers. For example, you can enforce strict communication paths between application tiers while allowing limited access to database servers.
6. **High Availability and Redundancy:** UDRs can be leveraged to implement high availability and redundancy for critical network components. By defining multiple routes with different next-hop addresses, organizations can ensure that traffic can still reach its destination even if one route or network component fails.
7. **Compliance and Regulatory Requirements:** Some industries have strict compliance and regulatory requirements regarding data handling and network security. UDRs enable organizations to enforce specific routing policies that align with these requirements, ensuring data privacy and regulatory compliance.
8. **Traffic Monitoring and Analysis:** By directing traffic through specific network monitoring tools or appliances, organizations can capture, analyze, and visualize network traffic patterns for troubleshooting, performance monitoring, and security analysis purposes.

😄 To begin with the Lab

1. For this lab, we are going to launch 3 Virtual Machines, 1 will be a central machine and the other will be a part of this machine. The central VM will have a public IP address, but the other child machines will only have a Private IP address.
2. Also, you should have a storage account in which you have the set up the file which we will be using to install the Web Server on our machine.
3. Below you can see the set up file in the container of the storage account.



4. Now we will create our central VM. Choose the properties from the snapshot.

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 Pass - Sponsorship

Resource group * ⓘ — demo-grp

Create new

Instance details

Virtual machine name * ⓘ — centralVM

Region * ⓘ — (Europe) North Europe

Availability options ⓘ — No infrastructure redundancy required

Security type ⓘ — Trusted launch virtual machines

Configure security features

Image * ⓘ — Windows Server 2022 Datacenter - x64 Gen2

See all images | Configure VM generation

Run with Azure Spot discount ⓘ

Size * ⓘ — Standard_D2s_v3 - 2 vcpus, 8 GiB memory (₹12,085.69/month)

See all sizes

Enable Hibernation ⓘ

Hibernate is not supported by the size that you have selected. Choose a size that is compatible with Hibernate to enable this feature. Learn more

Administrator account

Username * ⓘ — demouser

Password * — ••••••••••••

Confirm password * — ••••••••••••

5. Now in the networking section in the network interface you have to create a new Virtual network and you need to add the subnet for other machines.

The Microsoft Azure Virtual Network service enables Azure resources to securely communicate with each other in a virtual network which is a logical isolation of the Azure cloud dedicated to your subscription. You can connect virtual networks to other virtual networks, or your on-premises network. Learn more

Name * demo-network

Address space

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

Address range *	Addresses	Overlap
10.0.0.0/16	10.0.0.0 - 10.0.255.255 (65536 addresses)	None
	(0 Addresses)	None

Subnets

The subnet's address range in CIDR notation. It must be contained by the address space of the virtual network.

Subnet name	Address range	Addresses
centralsubnet	10.0.0.0/24	10.0.0.0 - 10.0.0.255 (256 addresses)
demosubnetA	10.0.1.0/24	10.0.1.0 - 10.0.1.255 (256 addresses)
demosubnetB	10.0.2.0/24	10.0.2.0 - 10.0.2.255 (256 addresses)
		(0 Addresses)

6. After that just move on to review and create your virtual machine. Then you need create the first child VM.

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 Pass - Sponsorship

Resource group * demo-grp

Create new

Instance details

Virtual machine name * demoVM-A

Region * (Europe) North Europe

Availability options No infrastructure redundancy required

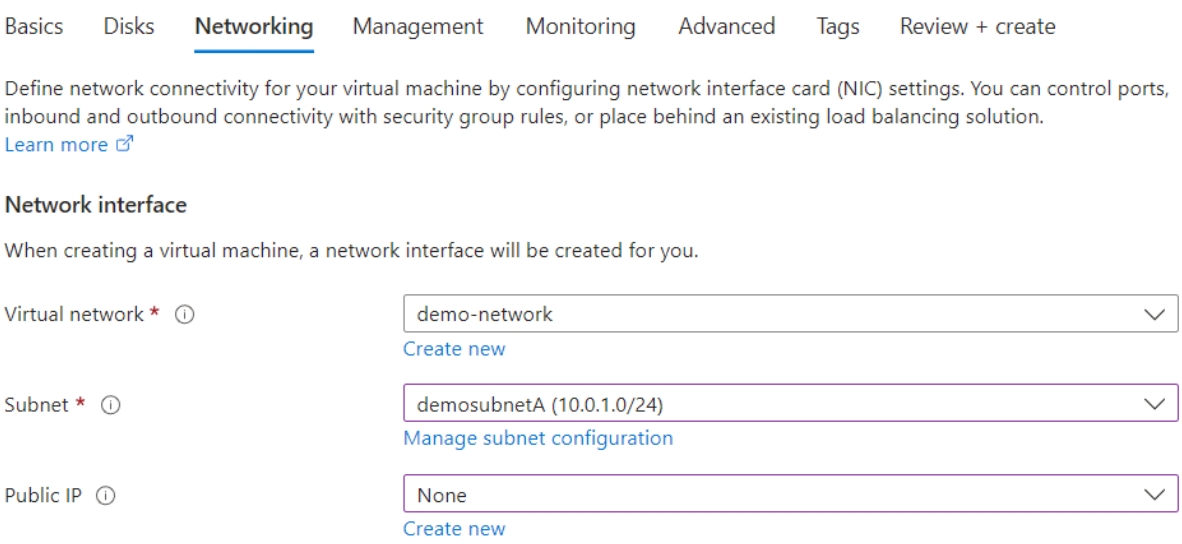
Security type Trusted launch virtual machines

Configure security features

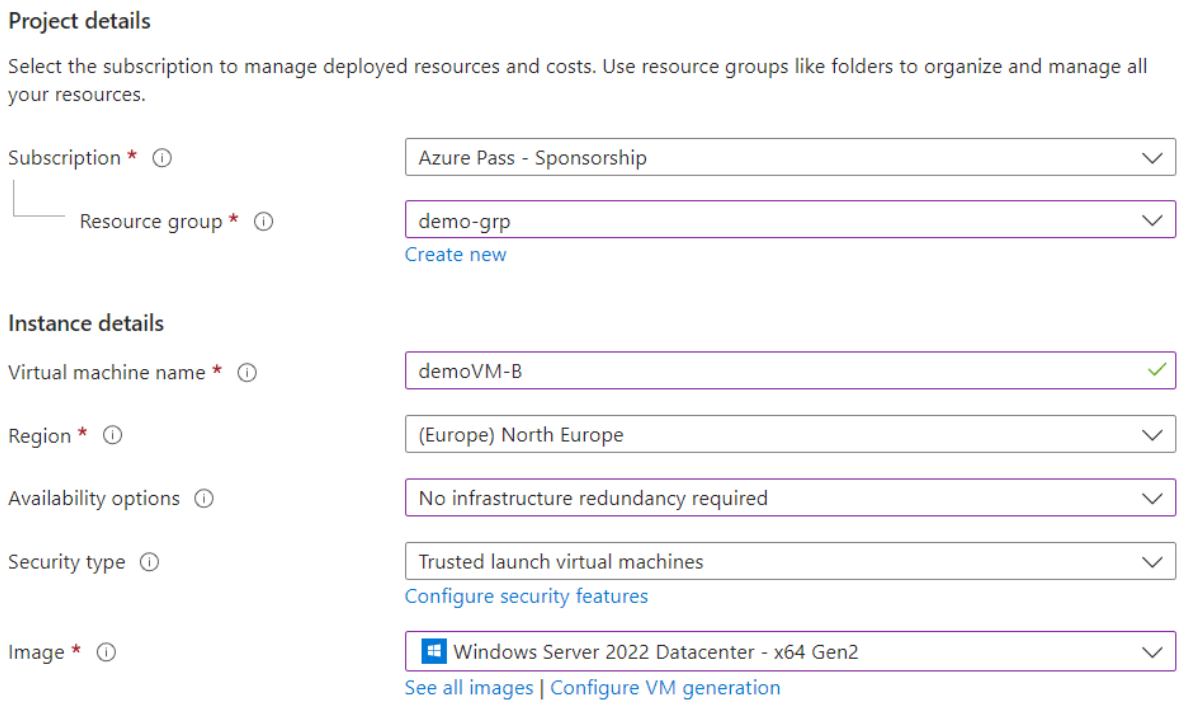
Image * Windows Server 2022 Datacenter - x64 Gen2

See all images | Configure VM generation

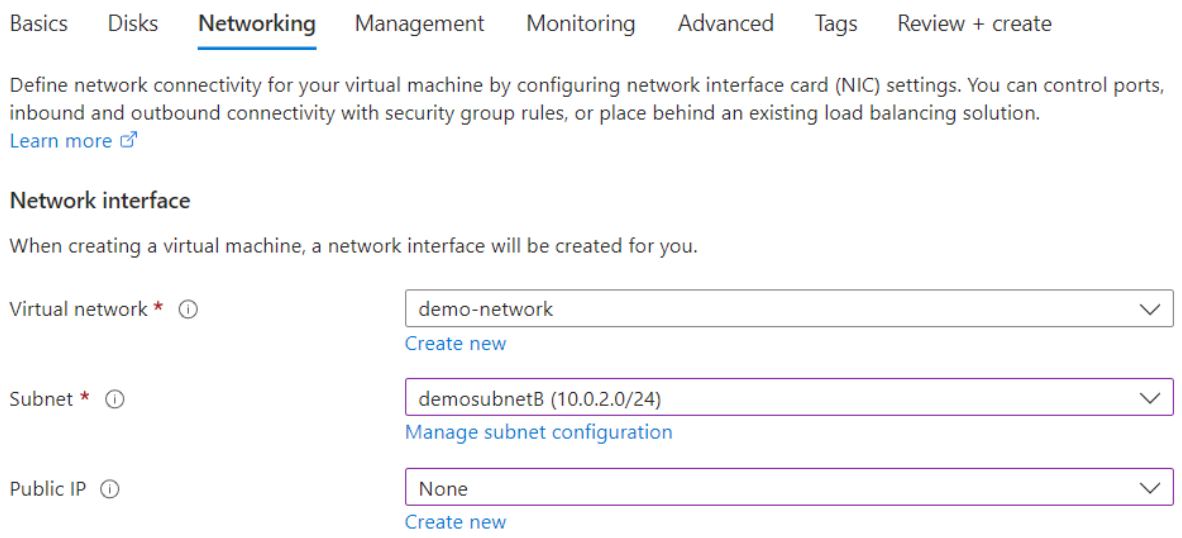
7. In networking just remember to change the subnet for this machine and choose none for public IP.



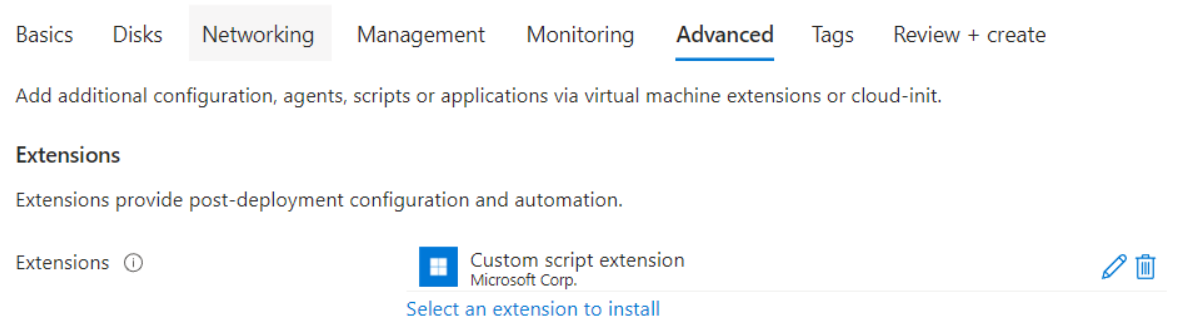
8. Then just move to the review page and create your VM.
9. As it is deploying go back to virtual machine and deploy your 2nd child VM.



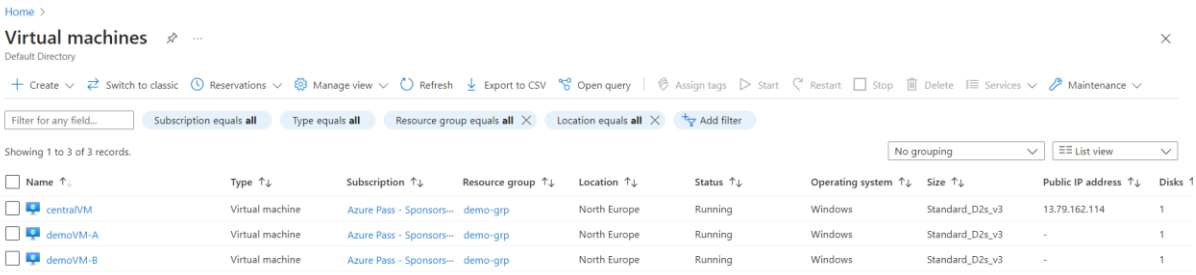
10. Then in the networking section change the subnet and choose none for Public IP.



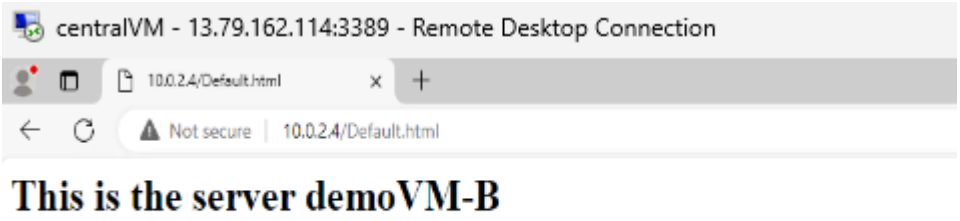
11. From the advanced setting you need to add the custom script in this VM. Then create your VM.



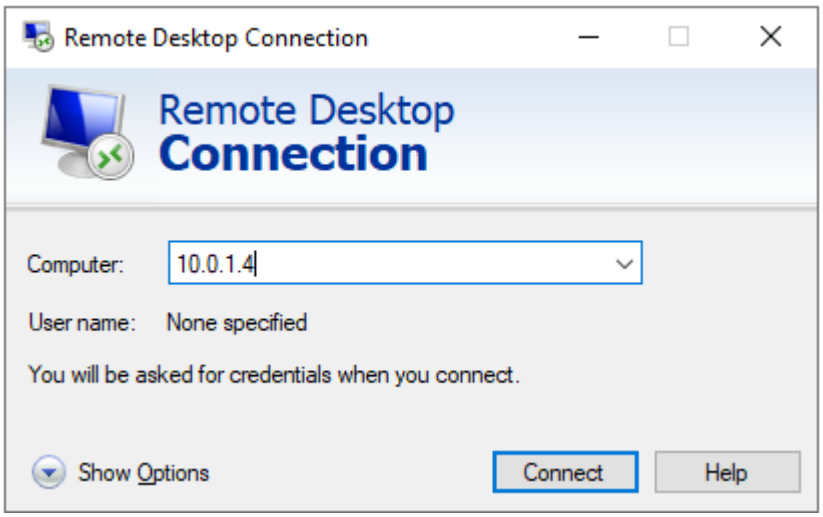
12. Below you can see that only central VM has the public IP.



13. When all your VMs are created and ready then you need to login to your Central VM.
14. Now you need to open the Microsoft Edge browser in your central VM and copy the private IP address of your demo VM-B and paste it with appending default.html you will see the expected output.

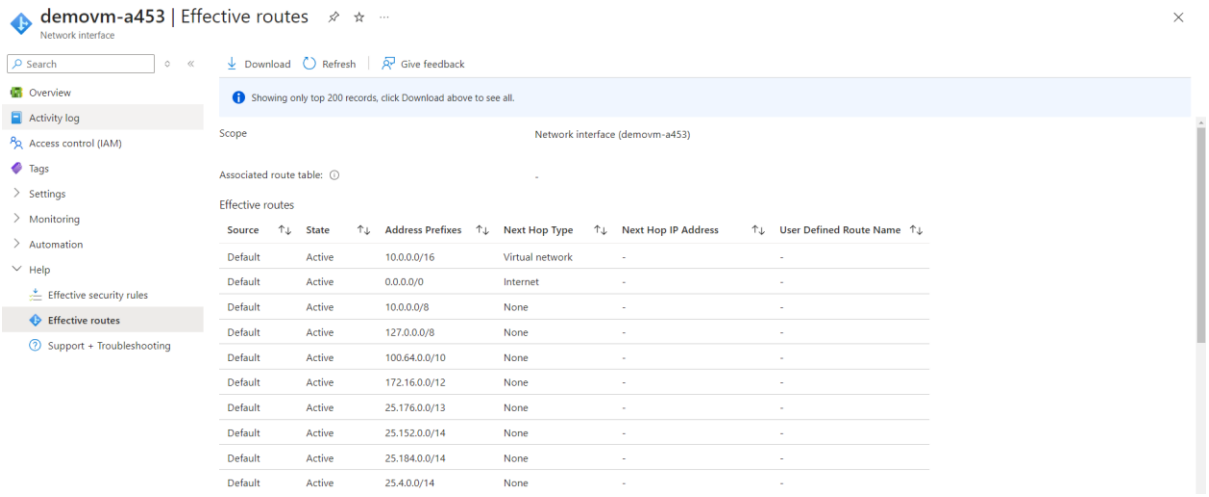


15. Now note that for demo VM-B, if we go to the networking section, we don't have any inbound rule to allow traffic on Port 80. The request is being accepted because of the rule of allowing all V-net inbound traffic because we are taking the private IP address all of the routing of the information the data is happening within the virtual network itself.
16. Now let us try to log in to demo VM-A using its private IP address and we'll do this in central VM.
17. We need to open RDP in our central VM and paste the Private IP of demo VM-A in it. Then hit on Create.

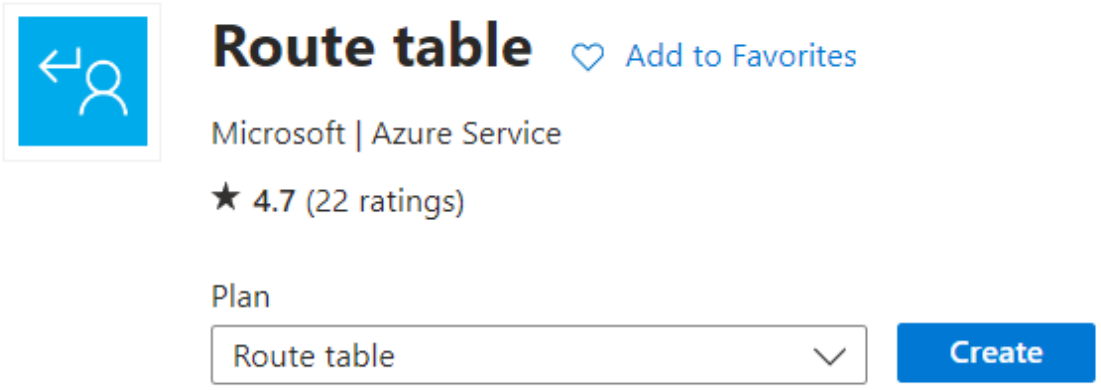


18. Then you will see that you can log in to the machine without needing a public IP address.
19. And now if we open Microsoft Edge and try to reach to IIS of demo VM-B, you can see that we are able to do that.

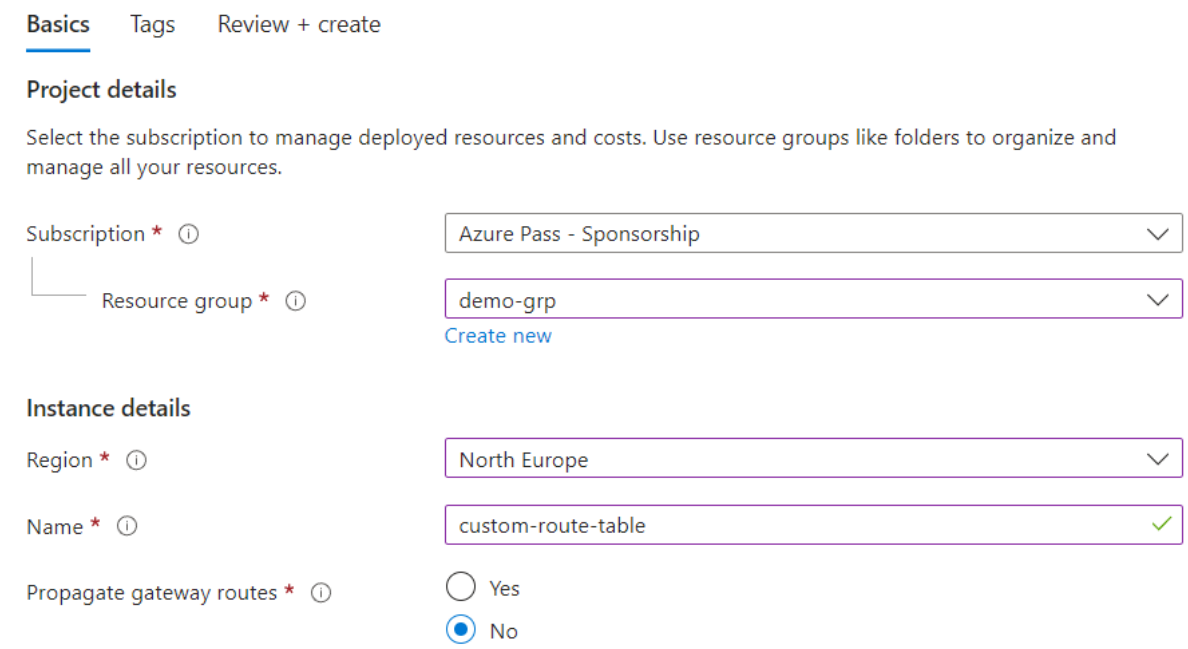
20. So, all of this routing of data within the virtual network is happening automatically and that's because there is inbuilt routes in place. Here you will see the route tables.



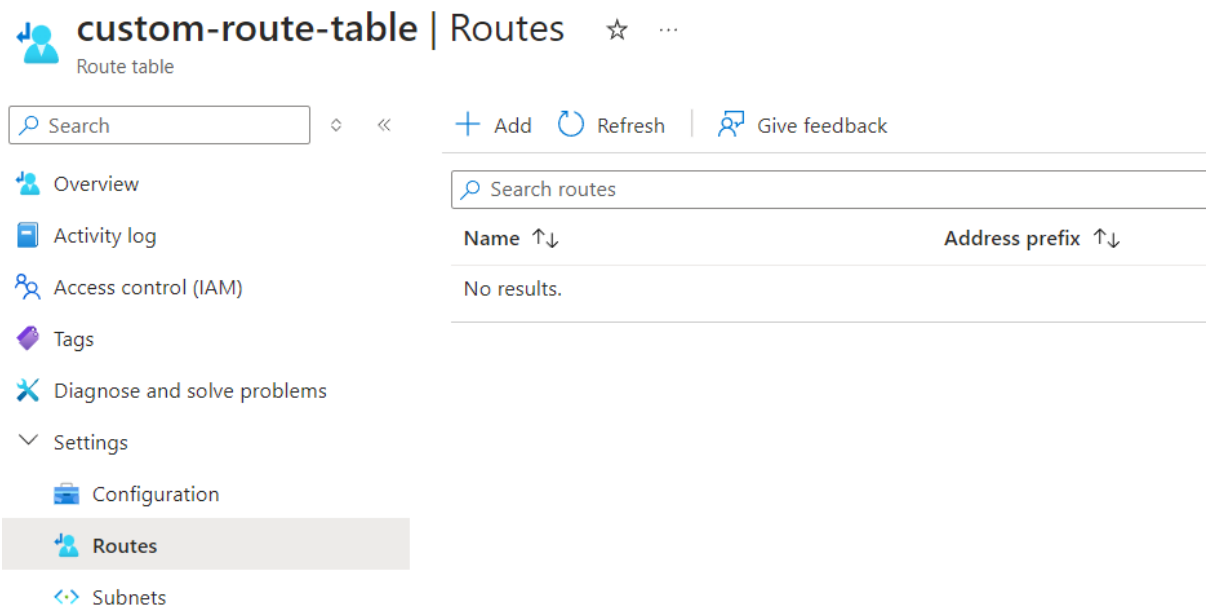
21. We now want to create a user-defined route. In that user-defined route, we want to say that all of the requests now should flow via central VM, that's part of the central subnet.
22. For that first we are going to create a route table our custom route table.
23. In the marketplace search for the route table and choose the server accordingly.



24. Now you just need to choose your resource group then your region and after that give it a name. Choose no for propagating gateway routes. Then just go ahead and create your route table.



25. Then in the route table go to routes and add a new route.



26. Now you need to give it a name first then in the destination type choose IP addresses. Then put the CIDR ranges and the next hop type is virtual appliance.
27. In the next hop address you need to put the Private IP address of your central VM. Then just click on add.

A user defined route (UDR) is a static route that overrides Azure's default system routes, or adds a route to a subnet's route table. Learn more

Route name *

central-route

Destination type *

IP Addresses

Destination IP addresses/CIDR ranges *

10.0.0.0/16

Next hop type *

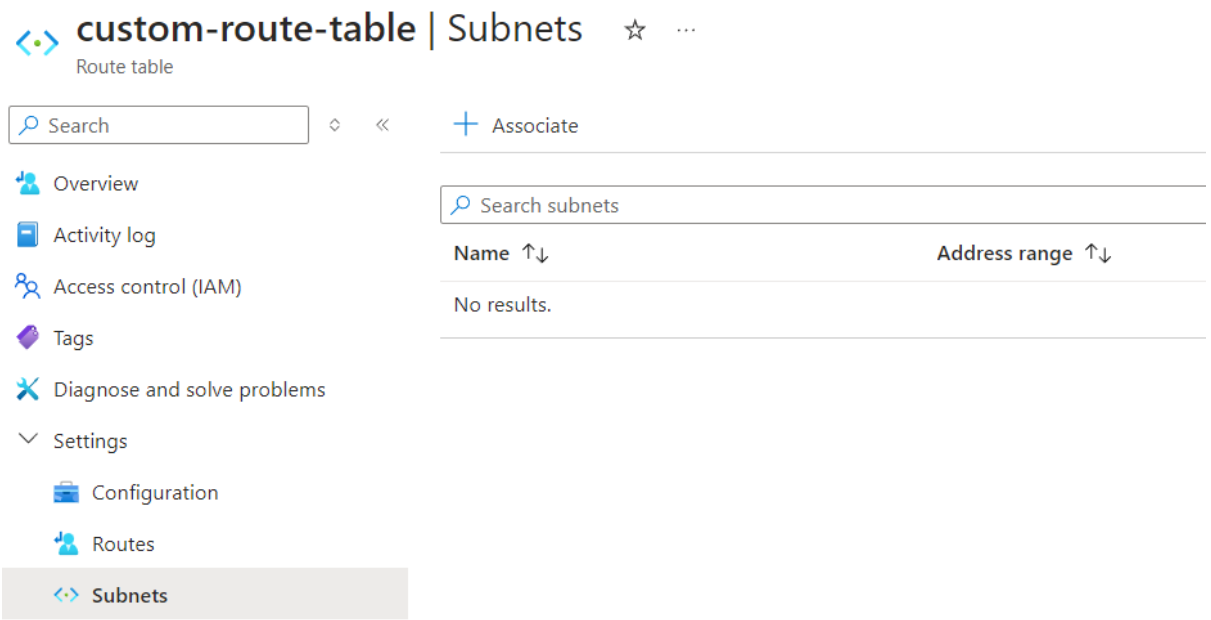
Virtual appliance

Next hop address *

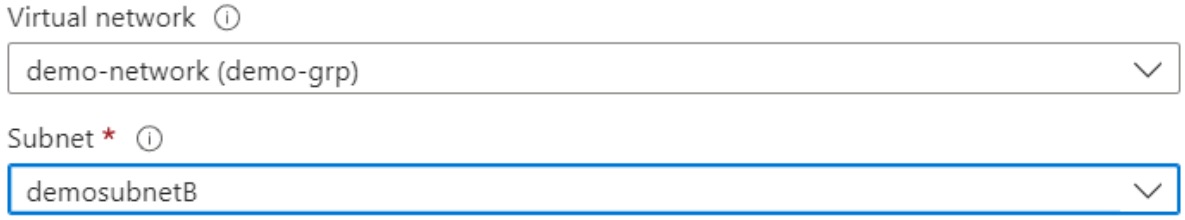
10.0.0.4

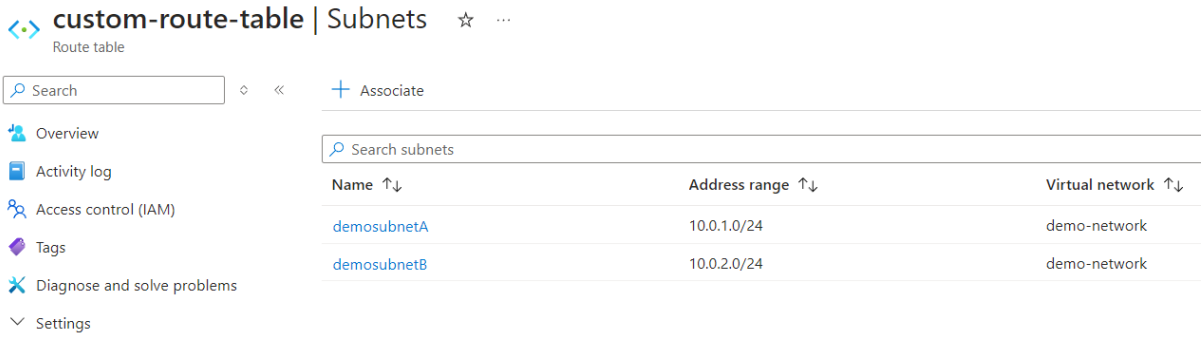
Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

28. Then you need to go subnets and associate the route table.

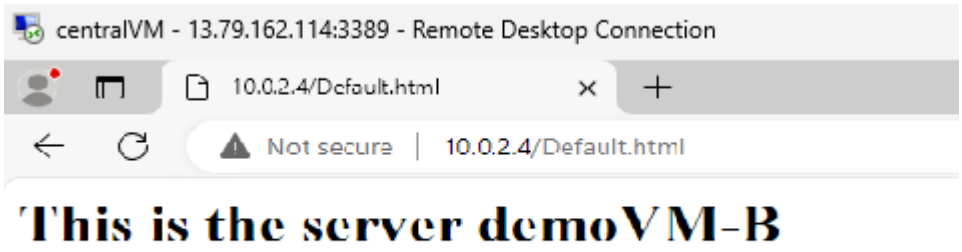


29. Then you need to associate it with subnet A first then to subnet B.

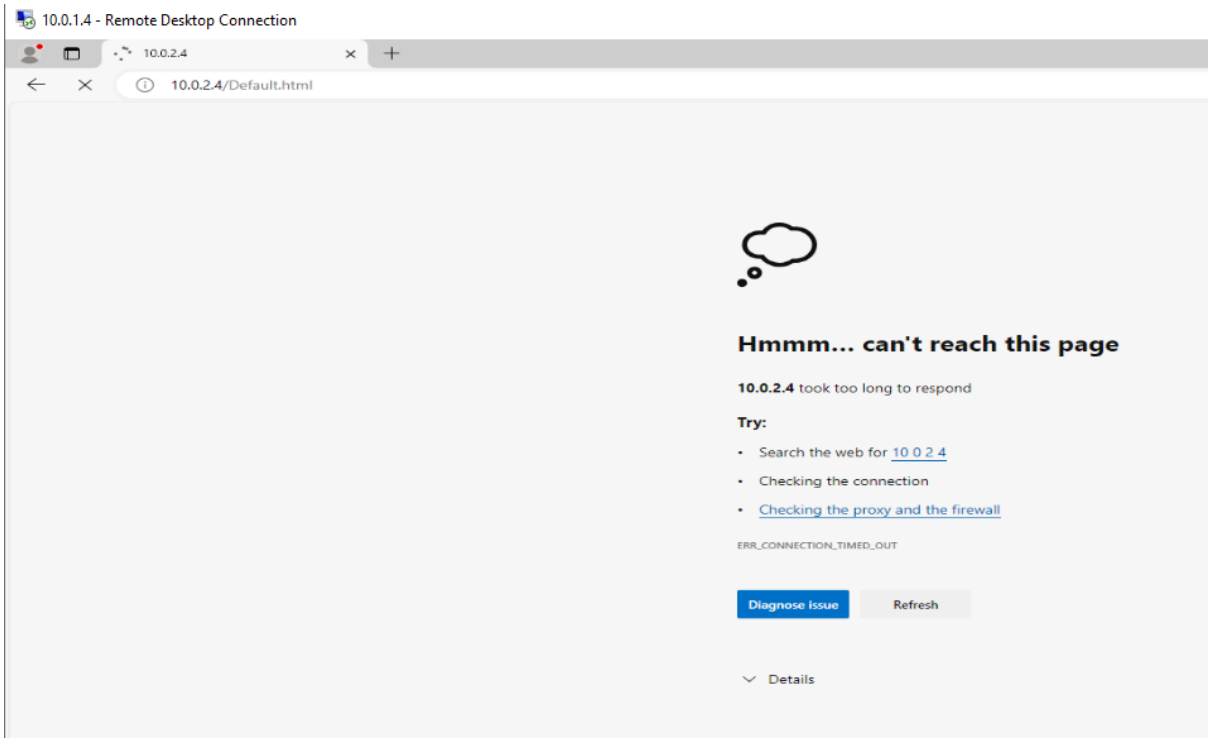




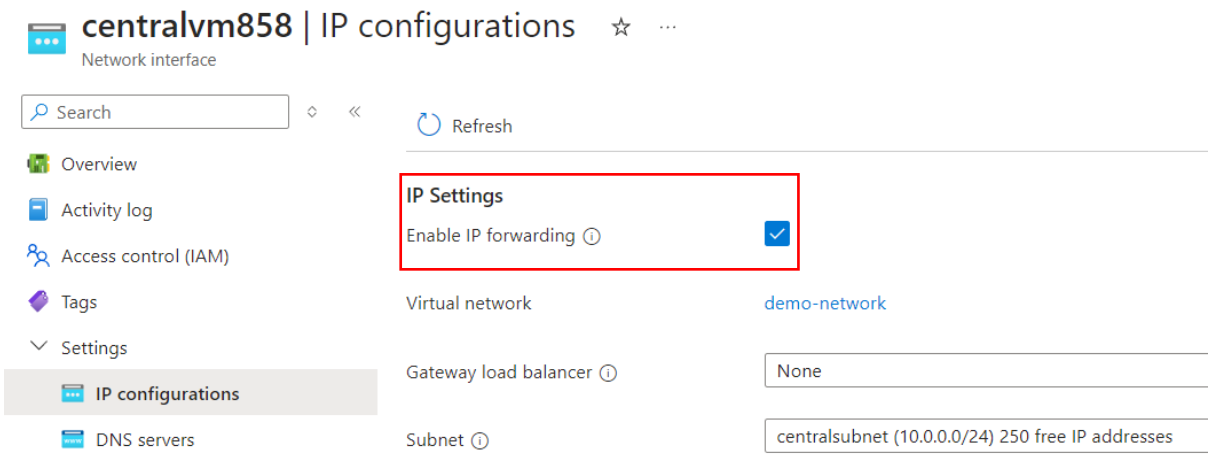
30. So now for any request from machines in subnet A, they will adhere to this custom route and the information will be routed via the central VM.
31. If you go back to your Central VM session and refresh the session you will see that the IIS is working fine.



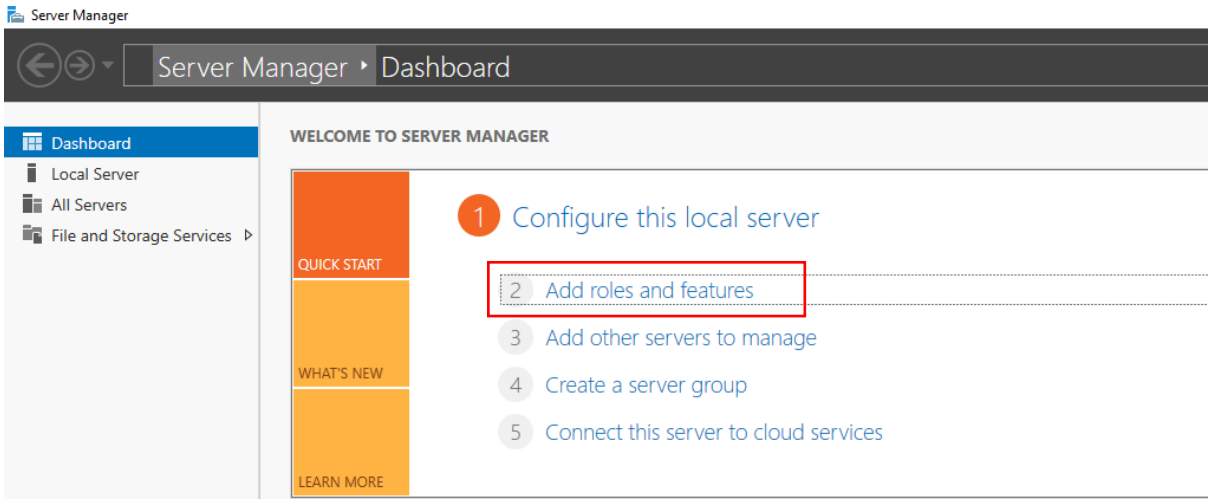
32. But if close the connection for demo VM-A and open it again then try to access the IIS in it then you will see that you are getting an error.



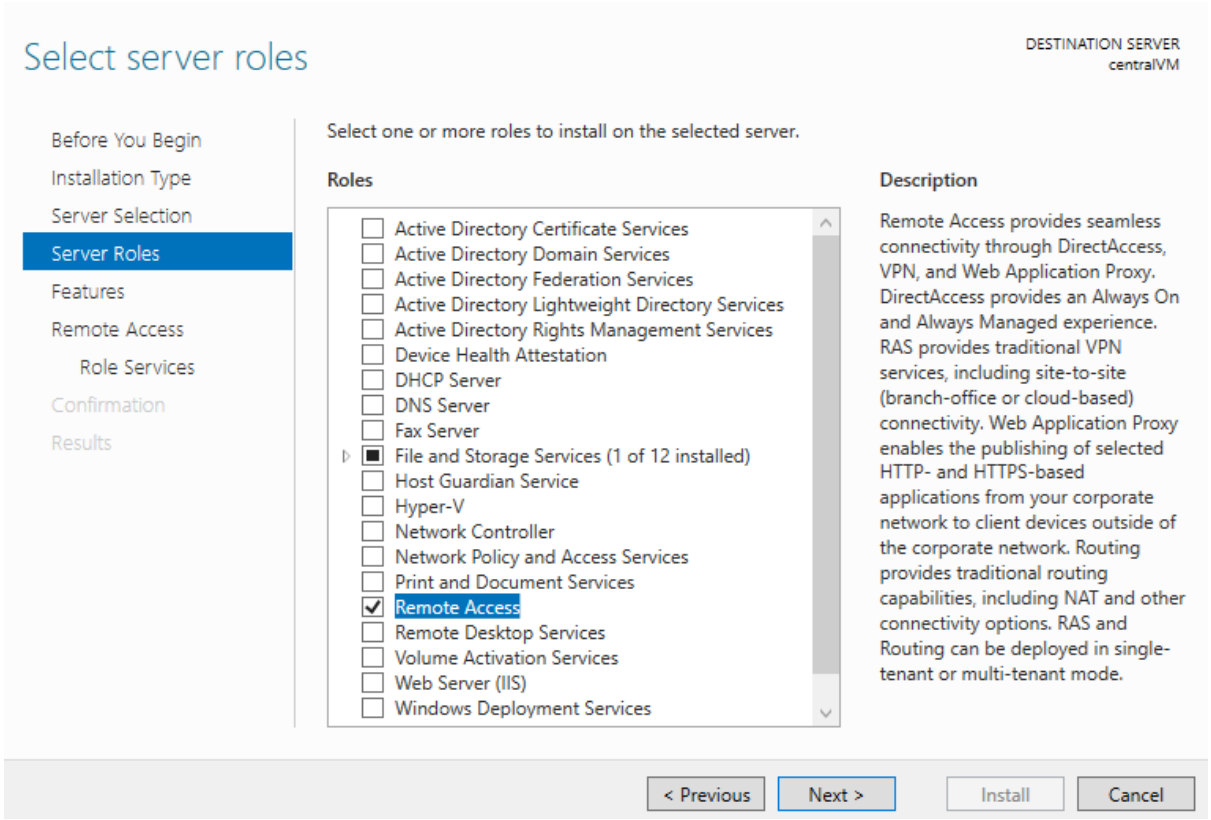
33. To resolve this issue first we need to go to the network interface of the central VM and enable IP forwarding then save it.



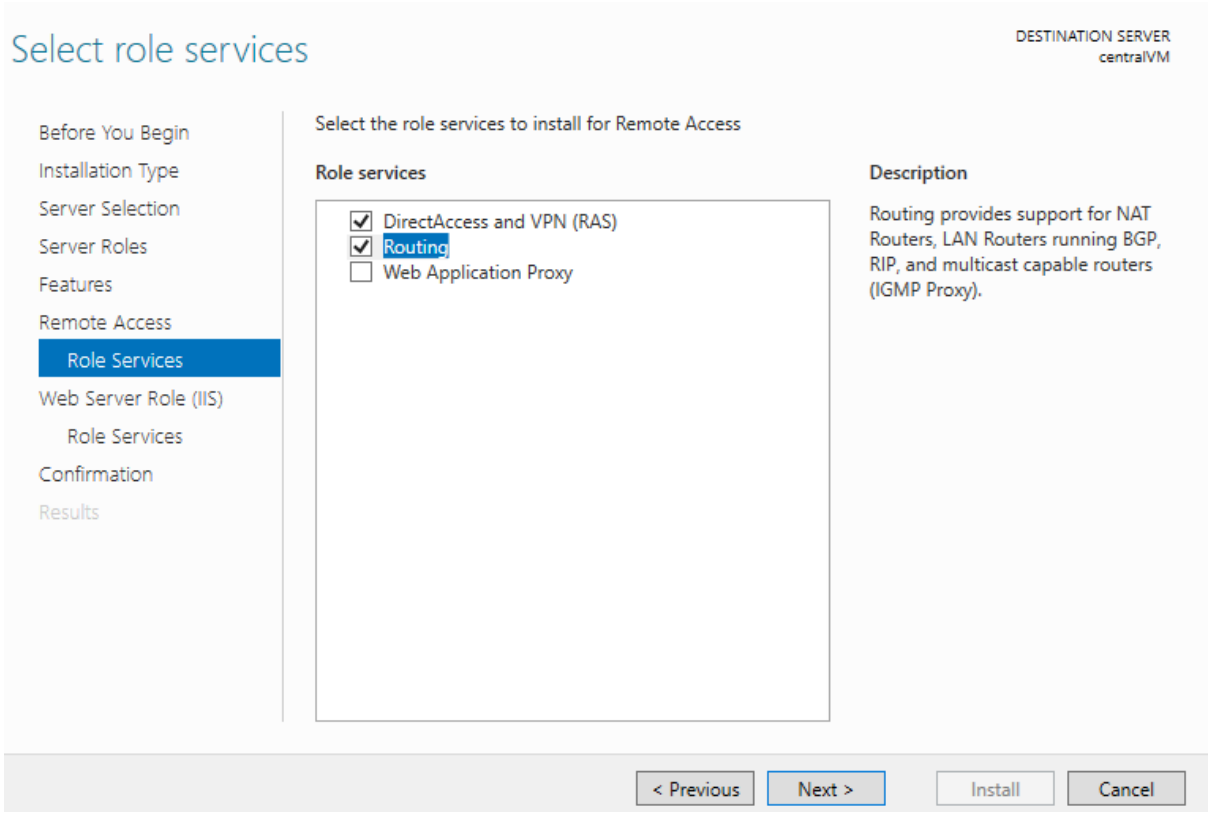
34. Also, at the OS level we need to enable this feature in central VM. For that in our VM in server manager we need to click on add roles and features.



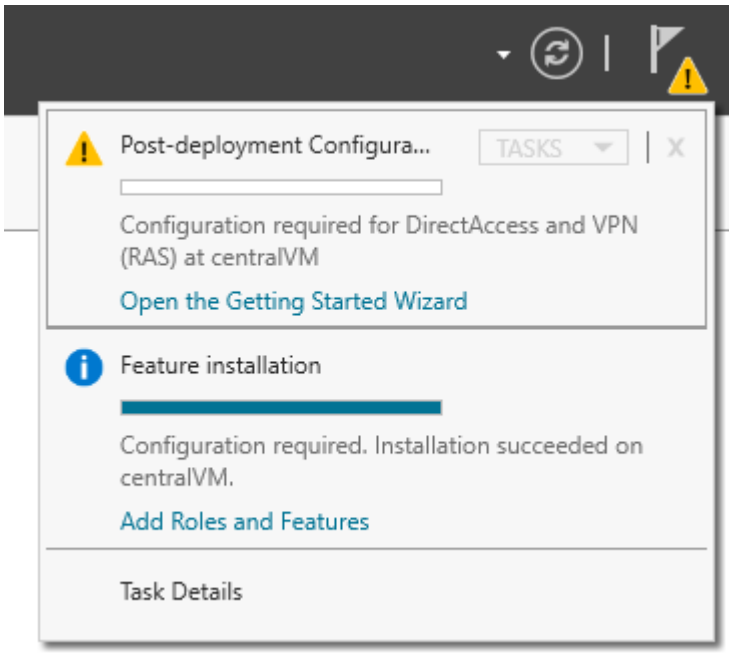
35. Then in server roles we need to add remote access and click on next.

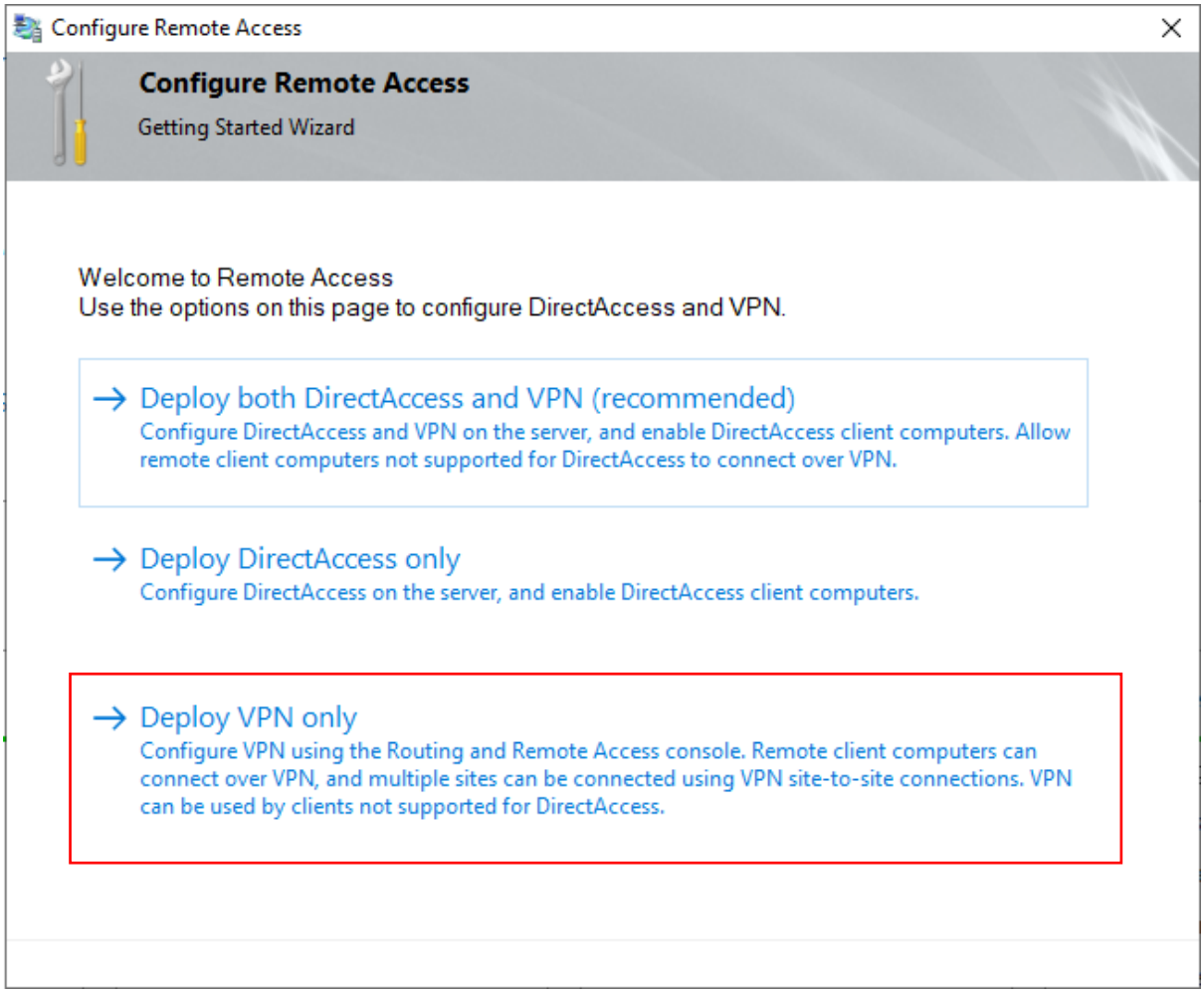


36. Now in role services add direct access and routing then just install them.

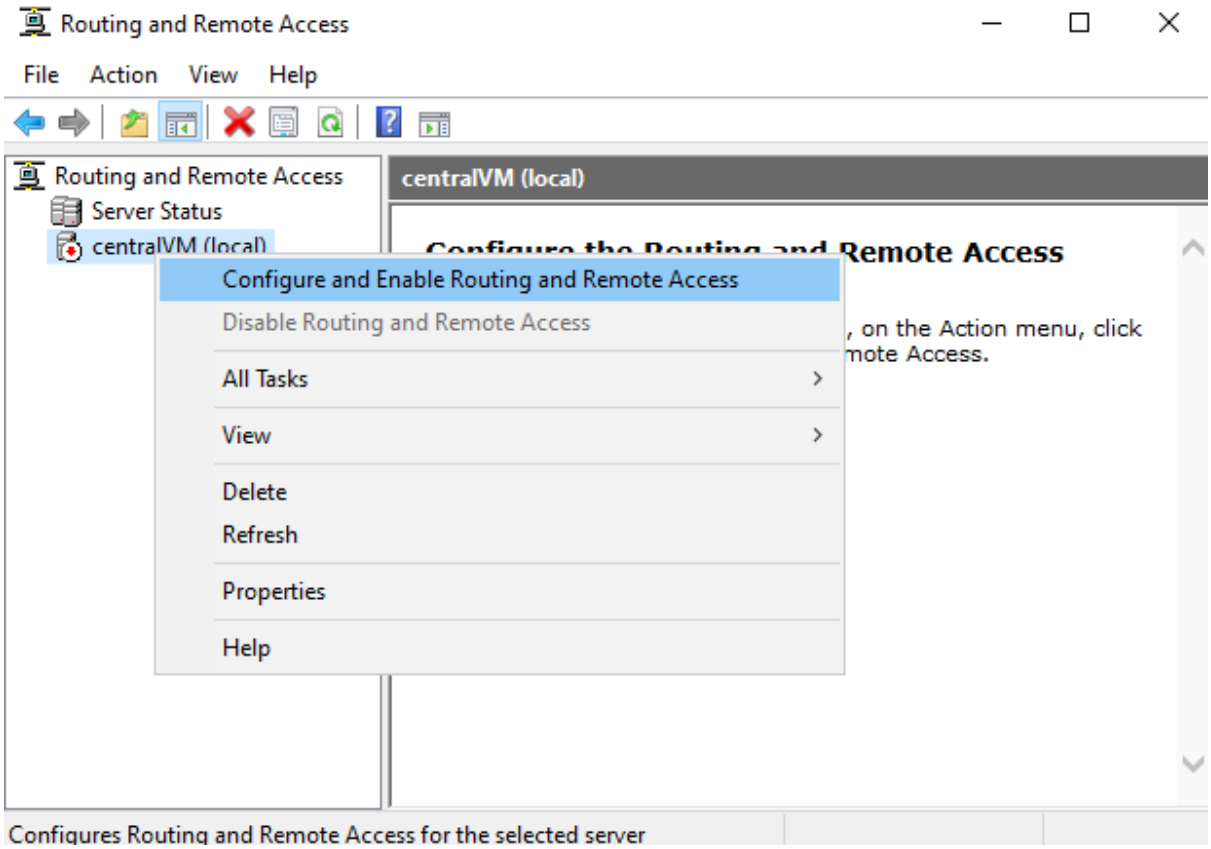


37. After that you need to configure it and then you have to choose VPN only.





38. Then you have to select central VM and right click on it then choose configure and enable routing.
39. Then you have to choose custom configuration. After that choose LAN routing then just finish up the process.,



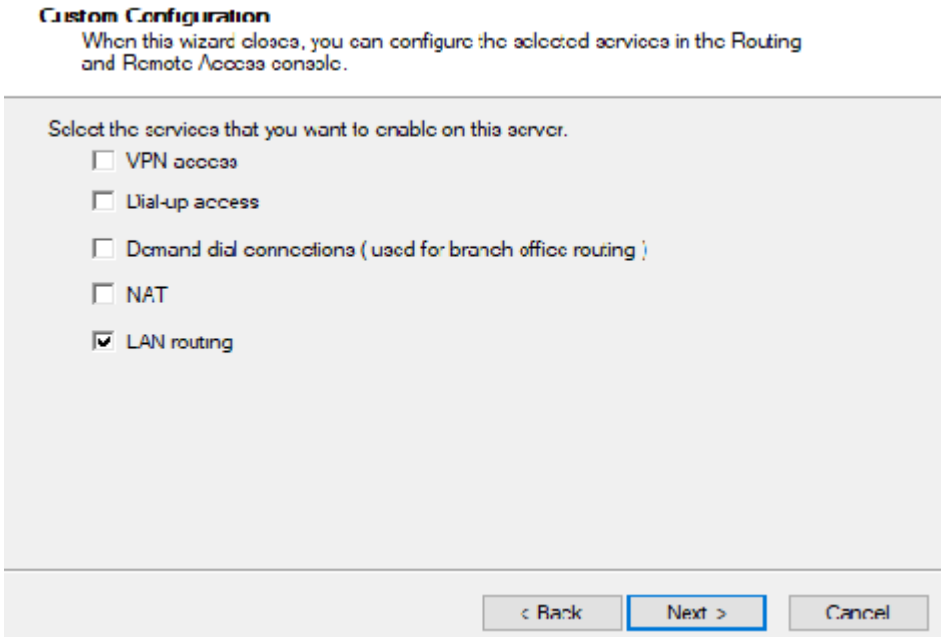
Routing and Remote Access Server Setup Wizard

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



40. This should have enabled the service now go back to demo VM-A and refresh the page. You will see the result as expected.

41. Once you're done just delete all of the resources.