



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:

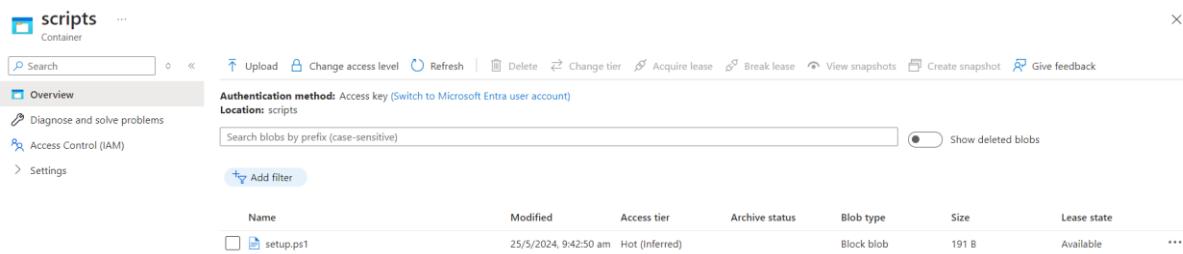
User-defined routes (UDRs) in Azure can be utilized in various scenarios to tailor network traffic routing according to specific requirements. Here are some common use cases:

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 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.



The screenshot shows the Azure Storage Explorer interface. The left sidebar has a tree view with 'Container' selected, showing 'scripts' as the current folder. The main area displays a table of blobs. The table has columns: Name, Modified, Access tier, Archive status, Blob type, Size, Lease state, and an ellipsis button. One row is visible, showing a blob named 'setup.ps1' with a modified date of 25/5/2024, 9:42:50 am, and an access tier of 'Hot (Inferred)'. The blob type is 'Block blob', the size is 191 B, and the lease state is 'Available'.

Name	Modified	Access tier	Archive status	Blob type	Size	Lease state	...
setup.ps1	25/5/2024, 9:42:50 am	Hot (Inferred)		Block blob	191 B	Available	...

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	<input type="checkbox"/>
Size *	Standard_D2s_v3 - 2 vcpus, 8 GiB memory (₹12,085.69/month) See all sizes
Enable Hibernation	<input type="checkbox"/> 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 *	*****

- 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).

<input type="checkbox"/> Address range *	Addresses	Overlap	
<input type="checkbox"/> 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.

<input type="checkbox"/> Subnet name	Address range	Addresses	
<input type="checkbox"/> centralsubnet	10.0.0.0/24	10.0.0.0 - 10.0.0.255 (256 addresses)	...
<input type="checkbox"/> demosubnetA	10.0.1.0/24	10.0.1.0 - 10.0.1.255 (256 addresses)	...
<input type="checkbox"/> 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.

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

[Learn more ↗](#)

Network interface

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

Virtual network *	<input type="text" value="demo-network"/> ⓘ	▼
	Create new	
Subnet *	<input type="text" value="demosubnetA (10.0.1.0/24)"/> ⓘ	▼
	Manage subnet configuration	
Public IP	<input type="text" value="None"/> ⓘ	▼
	Create new	

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.

Project details

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

Subscription *	<input type="text" value="Azure Pass - Sponsorship"/> ⓘ	▼
Resource group *	<input type="text" value="demo-grp"/> ⓘ	▼
	Create new	

Instance details

Virtual machine name *	<input type="text" value="demoVM-B"/> ⓘ	✓
Region *	<input type="text" value="(Europe) North Europe"/> ⓘ	▼
Availability options	<input type="text" value="No infrastructure redundancy required"/> ⓘ	▼
Security type	<input type="text" value="Trusted launch virtual machines"/> ⓘ	▼
	Configure security features	
Image *	<input type="text" value="Windows Server 2022 Datacenter - x64 Gen2"/> ⓘ	▼
	See all images Configure VM generation	

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

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

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

[Learn more](#)

Network interface

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

Virtual network *	<input type="text" value="demo-network"/>
	Create new
Subnet *	<input type="text" value="demosubnetB (10.0.2.0/24)"/>
	Manage subnet configuration
Public IP	<input type="text" value="None"/>
	Create new

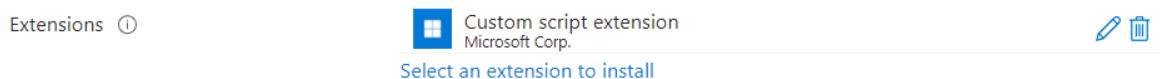
11. From the advanced setting you need to add the custom script in this VM. Then create your VM.

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

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

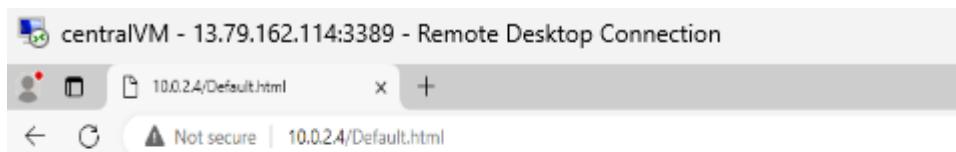


12. Below you can see that only central VM has the public IP.

Name	Type	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disk
centralVM	Virtual machine	Azure Pass - Sponsors--	demo-grp	North Europe	Running	Windows	Standard_D2s_v3	13.79.162.114	1
demoVM-A	Virtual machine	Azure Pass - Sponsors--	demo-grp	North Europe	Running	Windows	Standard_D2s_v3	-	1
demoVM-B	Virtual machine	Azure Pass - Sponsors--	demo-grp	North Europe	Running	Windows	Standard_D2s_v3	-	1

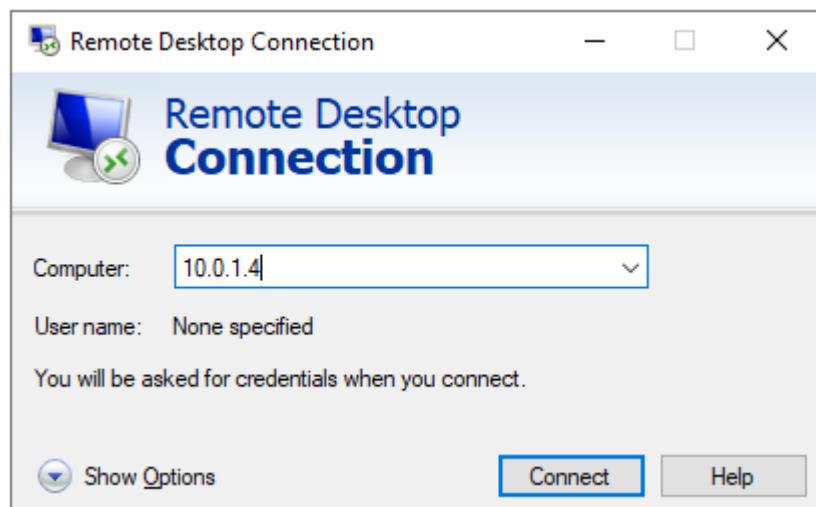
13. When all your VMs are created and ready then you need to login to your Central VM.

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.



This is the server demoVM-B

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.

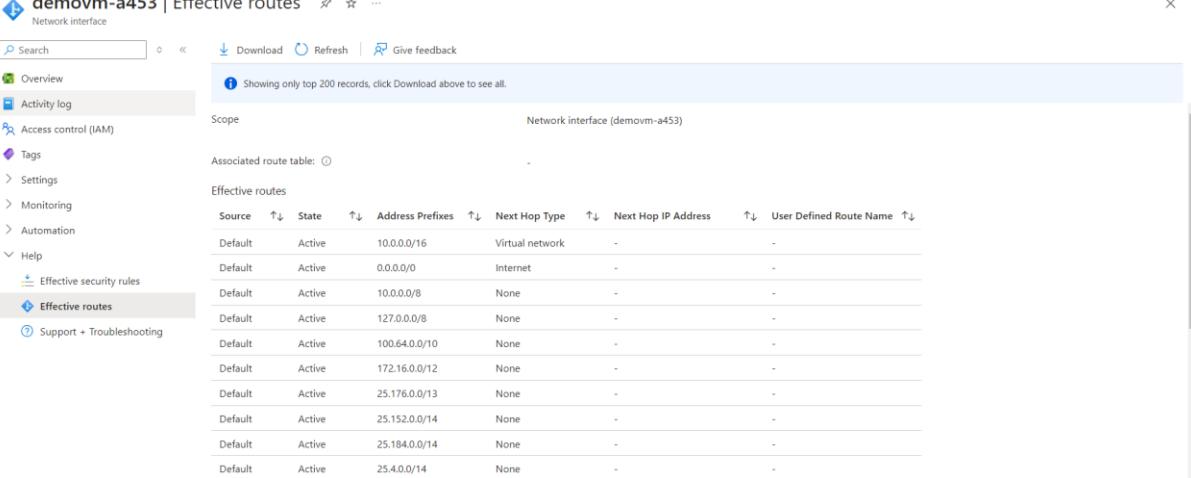


18. Then you will see that you can log in to the machine without needing a public IP address.
19. And now if we open Microsoft Edge and try to reach to IIS of demo VM-B, you can see that we are able to do that.



This is the server demoVM-B

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.



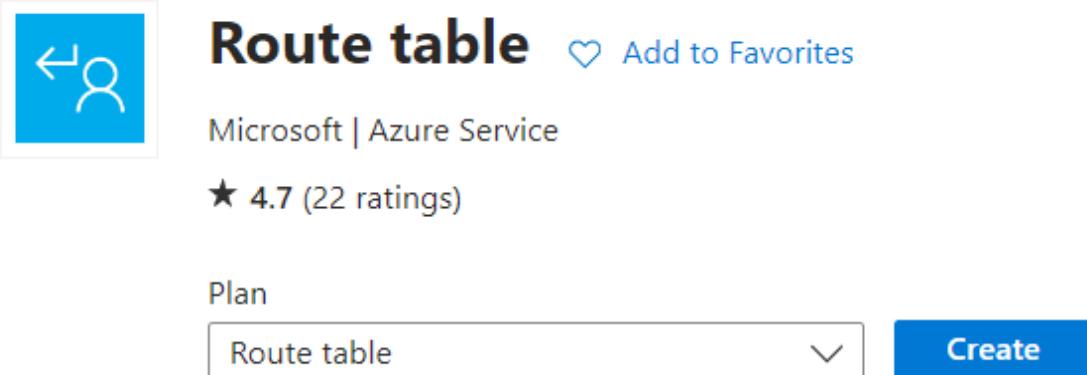
The screenshot shows the Azure portal interface for a network interface named 'demovm-a453'. The left sidebar has a 'Network interface' section with options like Overview, Activity log, Access control (IAM), Tags, Settings, Monitoring, Automation, Help, Effective security rules, and Effective routes (which is selected). The main content area displays the 'Effective routes' table with the following columns: Source, State, Address Prefixes, Next Hop Type, Next Hop IP Address, and User Defined Route Name. The table lists several default routes:

Source	State	Address Prefixes	Next Hop Type	Next Hop IP Address	User Defined Route Name
Default	Active	10.0.0.0/16	Virtual network	-	-
Default	Active	0.0.0.0/0	Internet	-	-
Default	Active	10.0.0.0/8	None	-	-
Default	Active	127.0.0.0/8	None	-	-
Default	Active	100.64.0.0/10	None	-	-
Default	Active	172.16.0.0/12	None	-	-
Default	Active	25.176.0.0/13	None	-	-
Default	Active	25.152.0.0/14	None	-	-
Default	Active	25.184.0.0/14	None	-	-
Default	Active	25.4.0.0/14	None	-	-

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.



The screenshot shows the Azure Marketplace search results for 'Route table'. The top navigation bar includes a Microsoft logo, a search bar, and a 'Create' button. Below the search bar, the results are displayed with the following details:

- Route table** (highlighted in blue)
- Microsoft | Azure Service
- ★ 4.7 (22 ratings)
- Plan (dropdown menu set to 'Route table')
- Create button

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.

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 Pass - Sponsorship

Resource group * ⓘ

demo-grp

[Create new](#)

Instance details

Region * ⓘ

North Europe

Name * ⓘ

custom-route-table

Propagate gateway routes * ⓘ

Yes
 No

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

 **custom-route-table** | Routes ⭐ ...

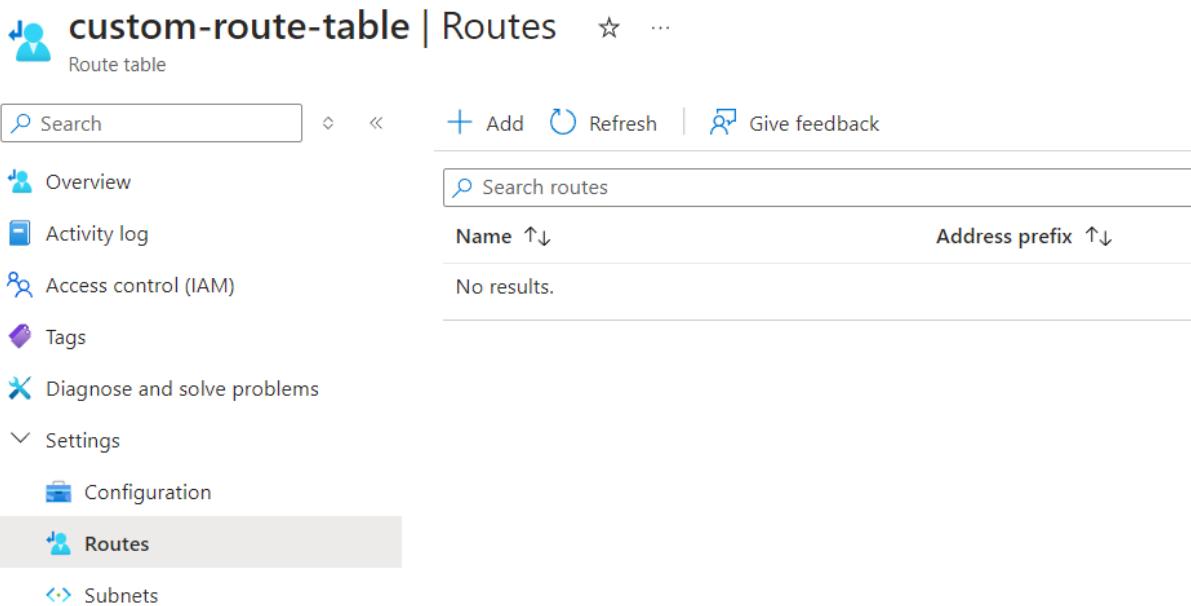
Route table

Search Add Refresh Give feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Configuration Routes Subnets

Search routes Name ↑↓ Address prefix ↑↓

No results.



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



i 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.

< custom-route-table | Subnets ⭐ ...

Route table

Search Associate

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Configuration Routes Subnets

Search subnets Name ↑↓ Address range ↑↓ No results.

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

Virtual network ⓘ
demo-network (demo-grp) ▾

Subnet * ⓘ
demosubnetA ▾

Virtual network ⓘ
demo-network (demo-grp) ▾

Subnet * ⓘ
demosubnetB ▾

custom-route-table | Subnets ⭐ ⋮

Route table

Search

Associate

Overview

Activity log

Access control (IAM)

Tags

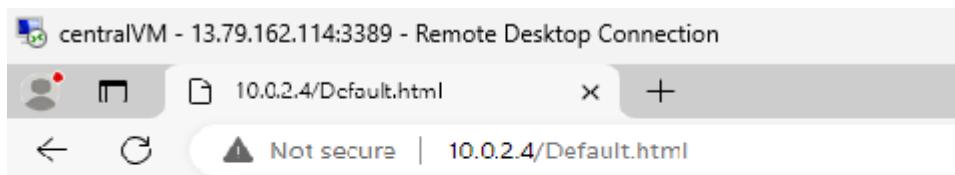
Diagnose and solve problems

Settings

Name ↑↓	Address range ↑↓	Virtual network ↑↓
demosubnetA	10.0.1.0/24	demo-network
demosubnetB	10.0.2.0/24	demo-network

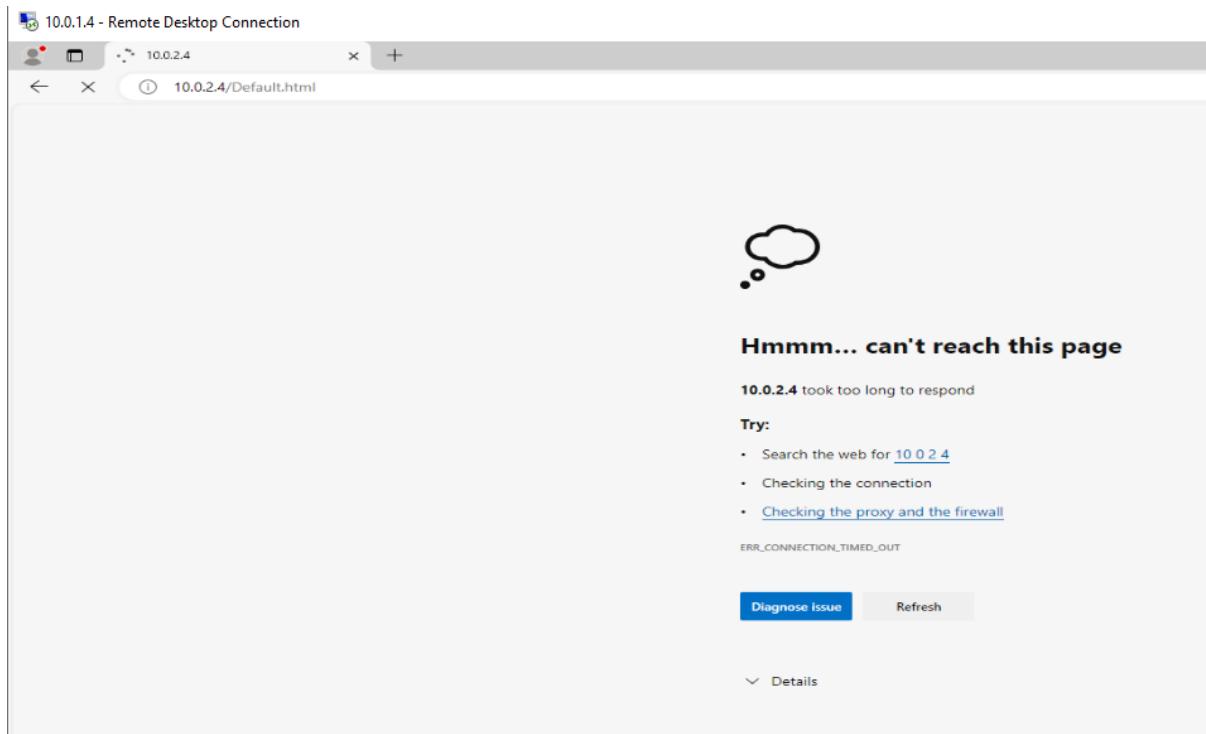
30. So now for any request from machines in subnet A, they will adhere to this custom route and the information will be routed via the central VM.

31. If you go back to your Central VM session and refresh the session you will see that the IIS is working fine.



This is the server demoVM-B

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.

centralvm858 | IP configurations

Network interface

Search

Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

IP configurations

DNS servers

IP Settings

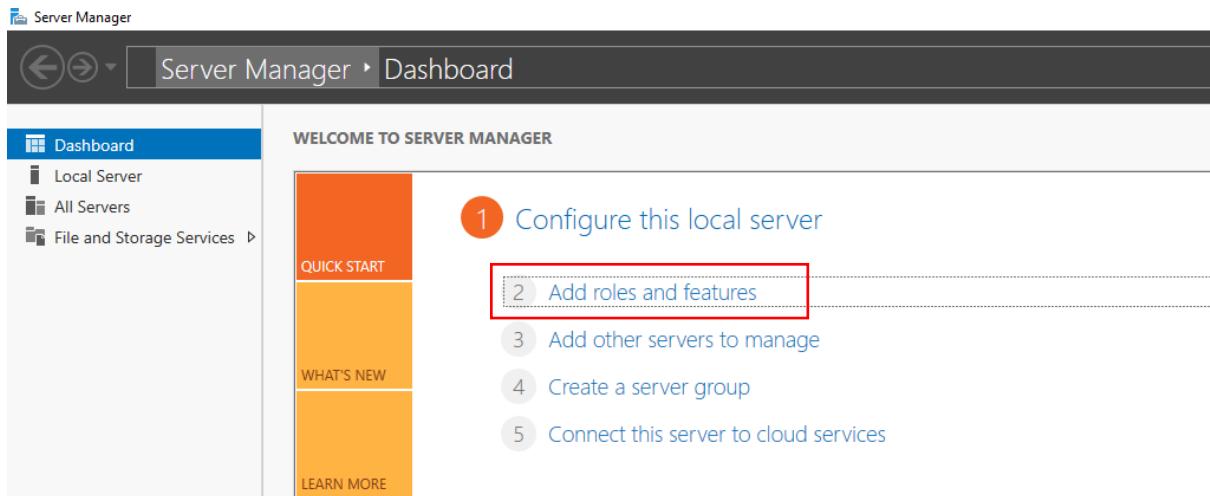
Enable IP forwarding

Virtual network: demo-network

Gateway load balancer: None

Subnet: centralsubnet (10.0.0.0/24) 250 free IP addresses

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.

This screenshot shows the 'Select server roles' step in the 'Select server roles' wizard. The left sidebar lists steps: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles' (which is selected and highlighted in blue), 'Features', 'Remote Access', 'Role Services', 'Confirmation', and 'Results'. The main pane is titled 'Select one or more roles to install on the selected server.' It shows a list of roles under the 'File and Storage Services' category, with 'Remote Access' checked. The right pane provides a detailed description of what Remote Access does. At the bottom are buttons for '< Previous', 'Next >', 'Install', and 'Cancel'.

Role	Description
Active Directory Certificate Services	Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience.
Active Directory Domain Services	RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.
Active Directory Federation Services	
Active Directory Lightweight Directory Services	
Active Directory Rights Management Services	
Device Health Attestation	
DHCP Server	
DNS Server	
Fax Server	
File and Storage Services (1 of 12 installed)	
Host Guardian Service	
Hyper-V	
Network Controller	
Network Policy and Access Services	
Print and Document Services	
Remote Access	Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience.
Remote Desktop Services	RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.
Volume Activation Services	
Web Server (IIS)	
Windows Deployment Services	

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

Select role services

DESTINATION SERVER
centralVM

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Remote Access

Role Services

Web Server Role (IIS)

Role Services

Confirmation

Results

Select the role services to install for Remote Access

Role services

- DirectAccess and VPN (RAS)
- Routing
- Web Application Proxy

Description

Routing provides support for NAT Routers, LAN Routers running BGP, RIP, and multicast capable routers (IGMP Proxy).

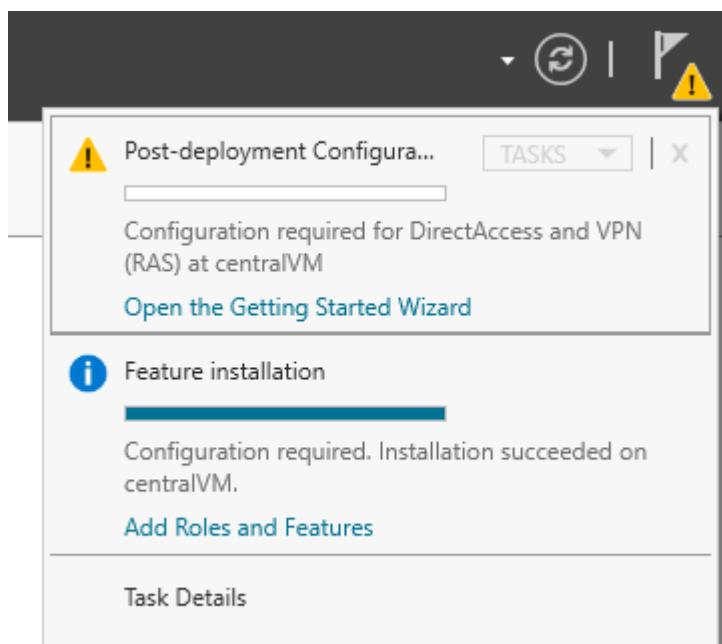
< Previous

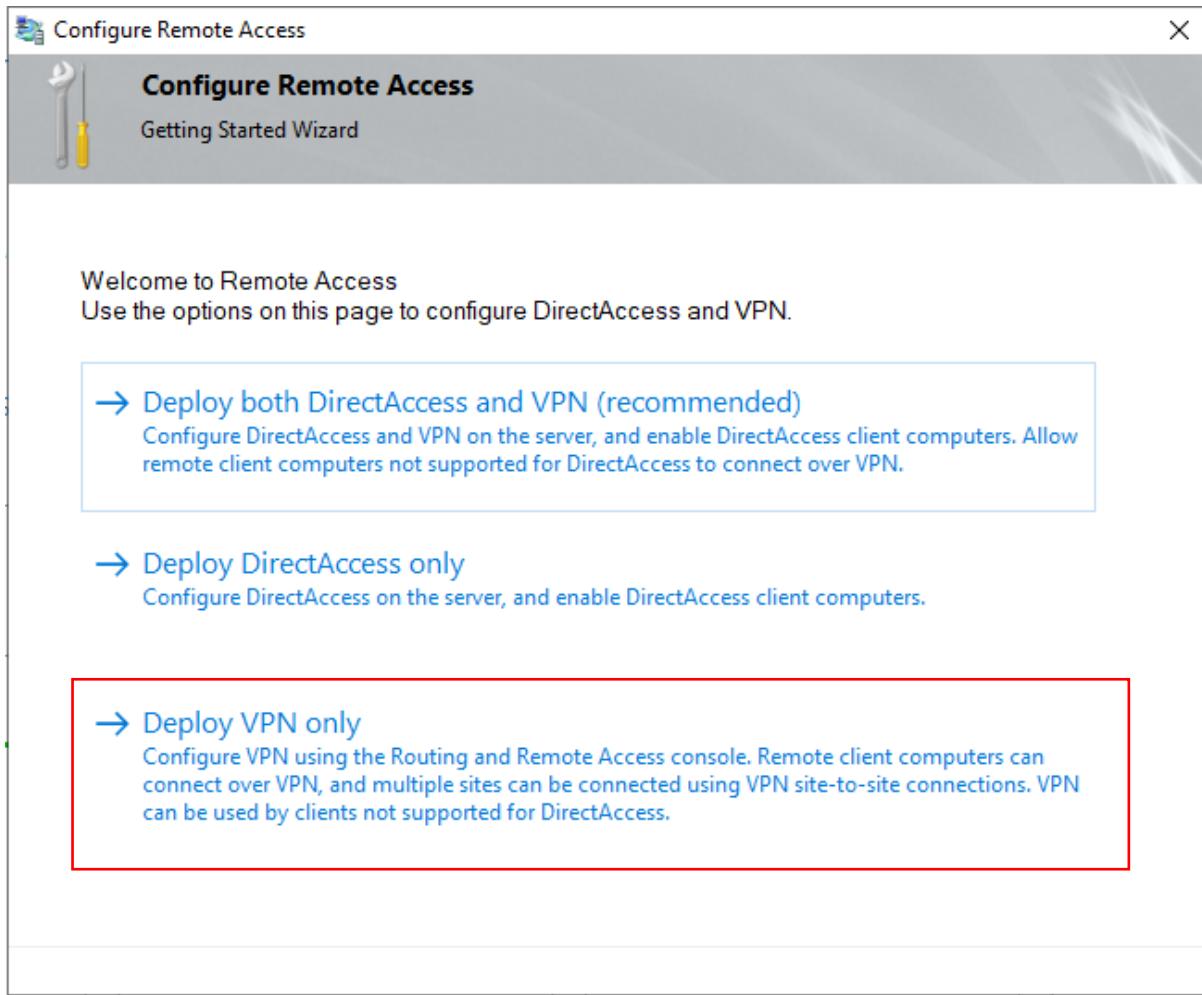
Next >

Install

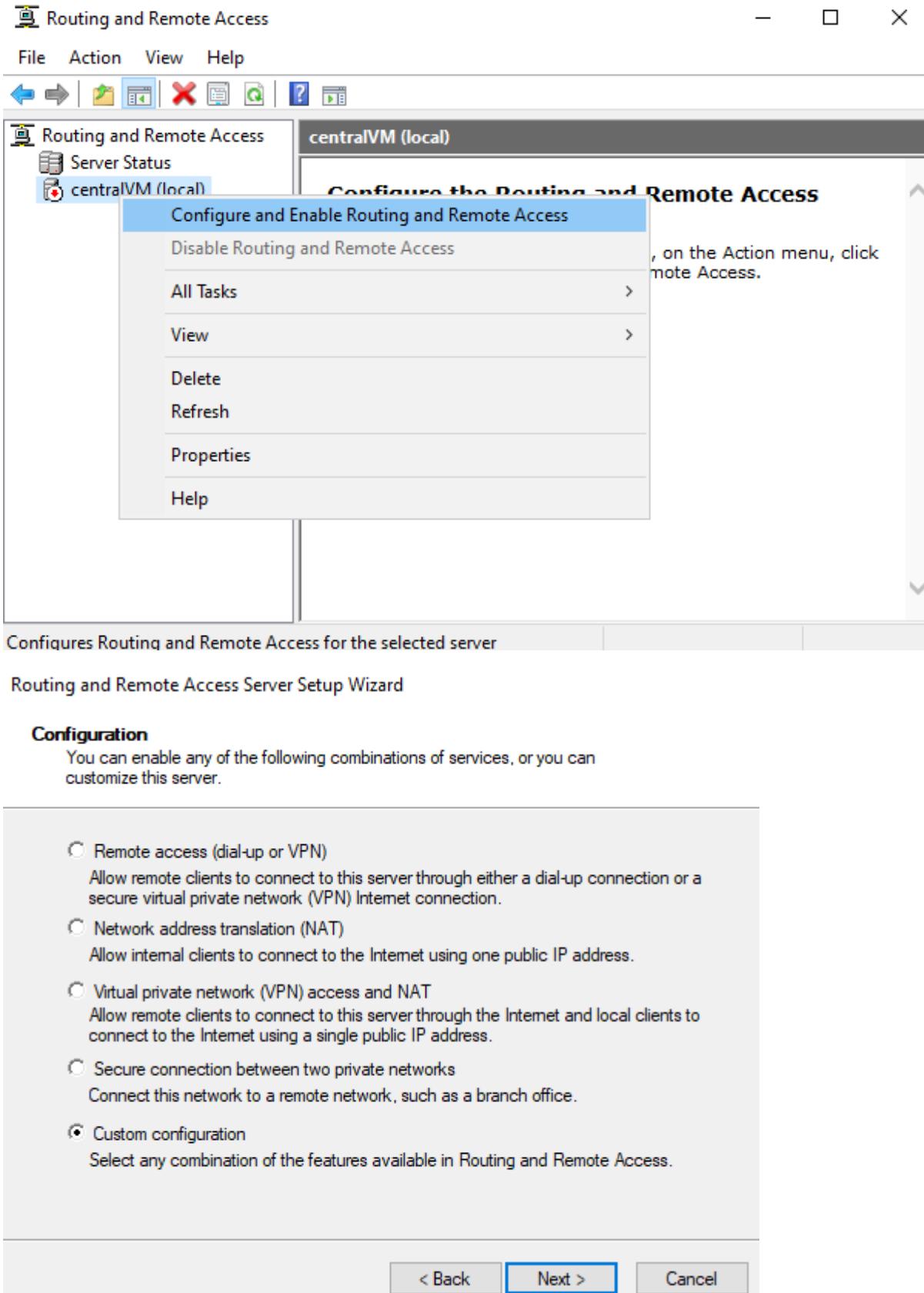
Cancel

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.,



Custom Configuration

When this wizard closes, you can configure the selected services in the Routing and Remote Access console.

Select the services that you want to enable on this server.

- VPN access
- Dial-up access
- Demand dial connections (used for branch office routing)
- NAT
- LAN routing

< 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.