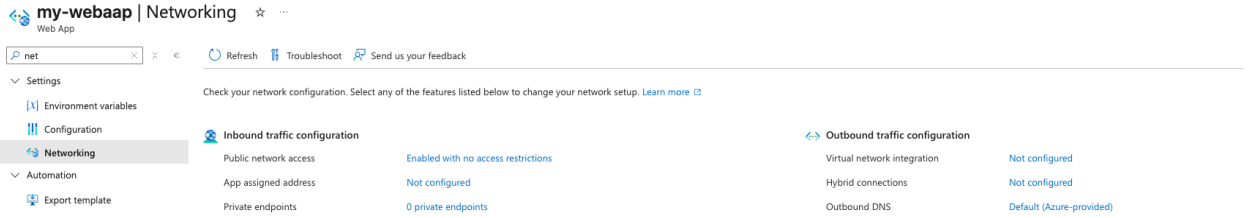
Create an App Service

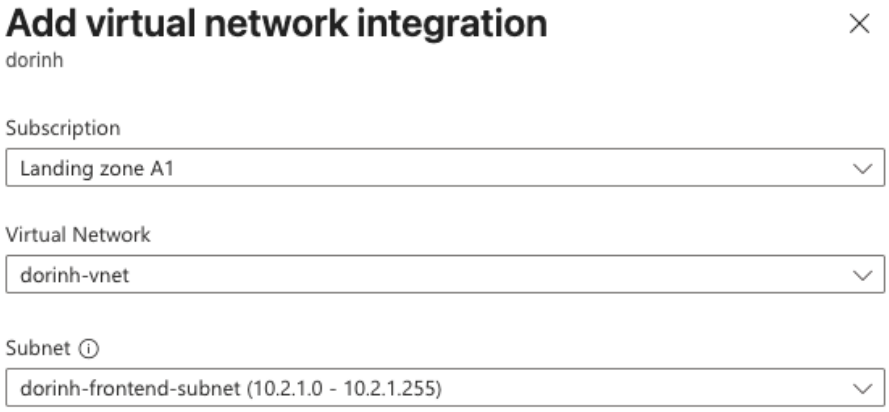
1. Navigate to the Azure Portal.
2. In the left-hand sidebar, click on "+ Create a resource."
3. Search for "Web App" and select it.
4. Click the "Create" button to initiate the setup.
5. Fill in the details for your App Service:
    - **Subscription**: Select the appropriate subscription.
    - **Resource Group**: Choose your RG
    - **Name**: Provide a unique name for the App Service.
    - **Publish**: Select 'Code'.
    - **Runtime stack**: .NET 9
    - **Operating System**: Linux
    - **Region**: Select the desired region.
    - **App Service plan**: Either use an existing plan or create a new one. Note: To use VNet Integration, the App Service plan should be a Premium, **PremiumV2**, or **PremiumV3** tier.
6. Review any additional settings as needed and then click on the "Review + create" button.
7. After validation, click the "Create" button.

Enable VNet Integration for the App Service

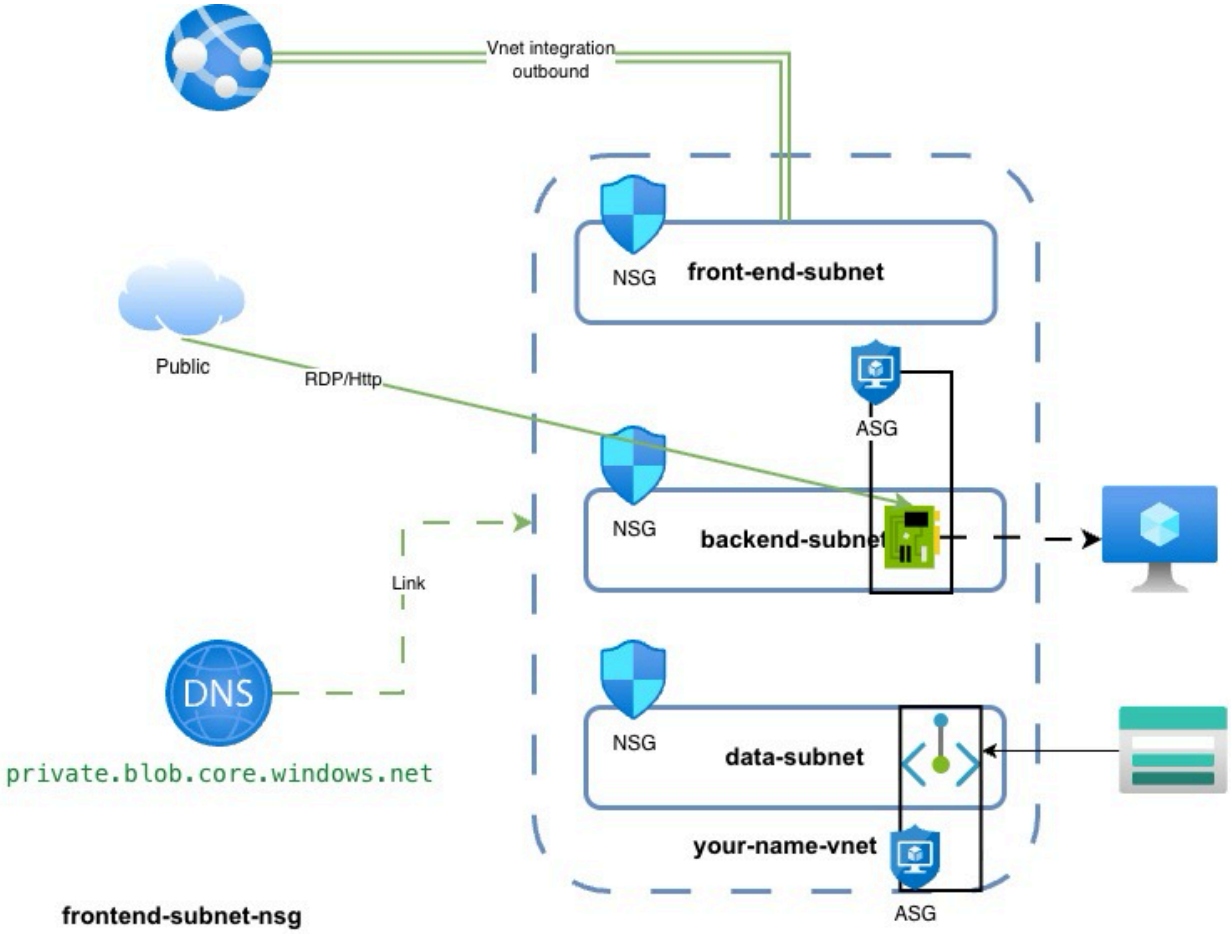
1. Once your App Service is created, go to its overview page.
2. In the left-hand settings pane, under the "Settings" section, click on "Networking."



3. Under the "VNet Integration" section, click on "***Not configured***"
4. Click on "+ Add VNet" to start the VNet Integration setup.
5. Select your VNet
6. Select the frontend-subnet



7. Click "Connect" to initiate the integration.



frontend-subnet-nsg

Priority	Name	Port	Protocol	Source	Destination	Action
4096	Deny-All-Inbound	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow

backend-subnet-nsg

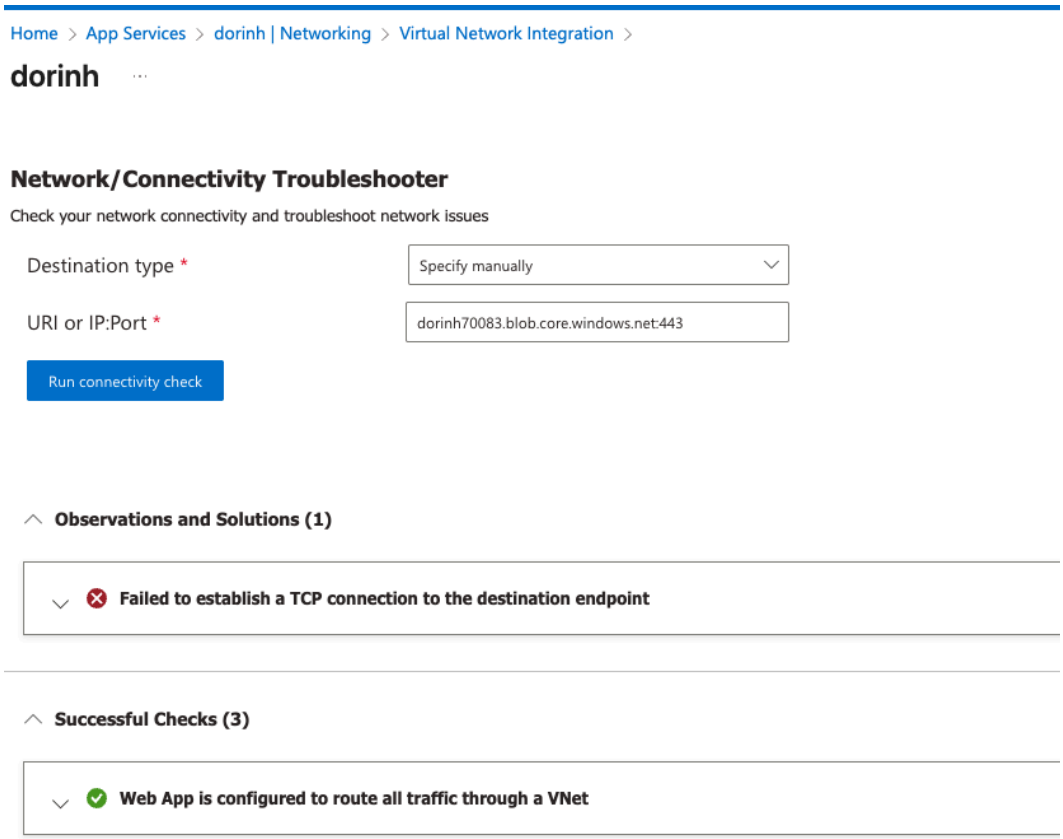
Priority	Name	Port	Protocol	Source	Destination	Action
110	Allow-HTTP-Internet	80	Tcp	Internet	Any	Allow
120	Allow-RDP-Internet	3389	Tcp	Internet	Any	Allow
4096	Deny-All-Inbound	Any	Any	Any	Any	Deny

data-subnet-nsg

Priority	Name	Port	Protocol	Source	Destination	Action
100	VM-to-Data	Any	Tcp	DORINH-VM-ASG	DORINH-DATA-A...	Allow
4096	Deny-All-Inbound	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow

Use App Service Diagnostics

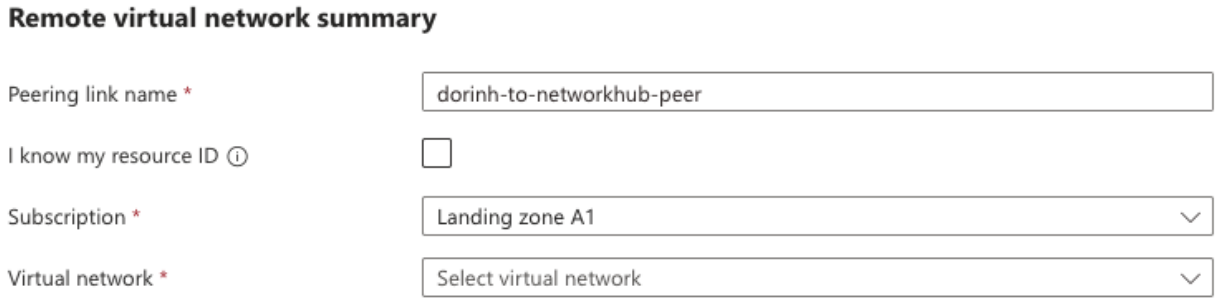
1. Navigate to Your App Service
    - Go to the Azure Portal.
    - In the left-hand sidebar, click on "App Services" and then select your specific App Service from the list.
2. Open App Service Diagnostics
    - In the left-hand settings pane for your App Service, click on “**Diagnose and solve problems**."
3. Access the **“Network/Connectivity Troubleshooter”**
    - Once inside the App Service Diagnostics, look for the section titled "Diagnostic Tools."
    - Click on "Networking Troubleshooter." This category contains diagnostic tools for checking the network-related configurations and issues of your App Service.
4. Use the Connection Issues tool to test the connection to different IPs and services
    - Test the connectivity to your Storage Account



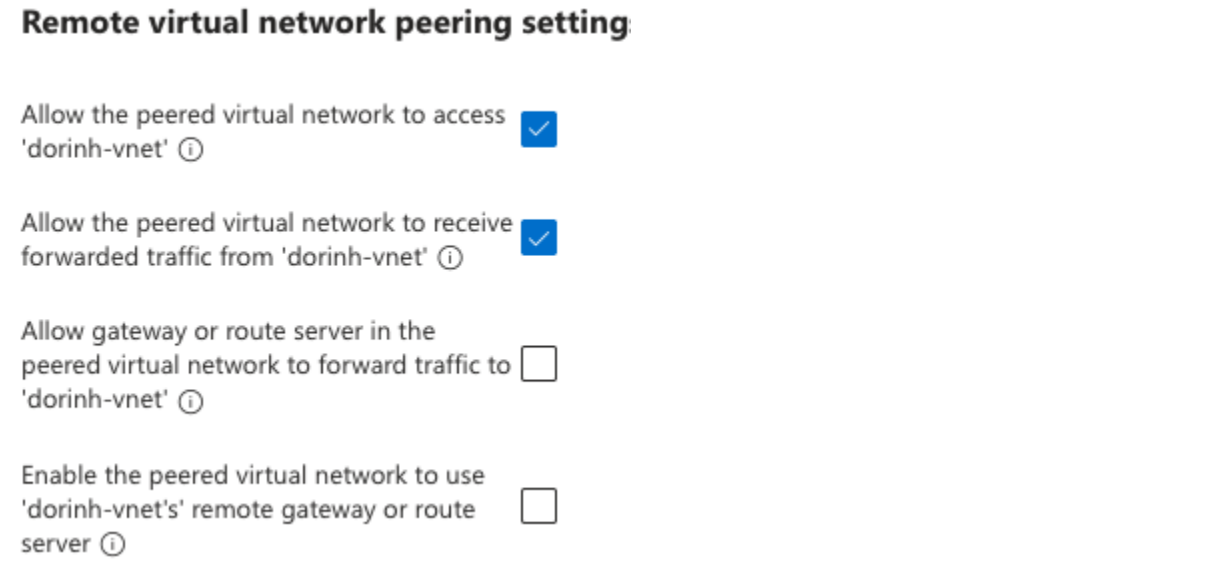
5. Why is the connectivity failing?
    - Discuss with the group a solution
    - Fix it!

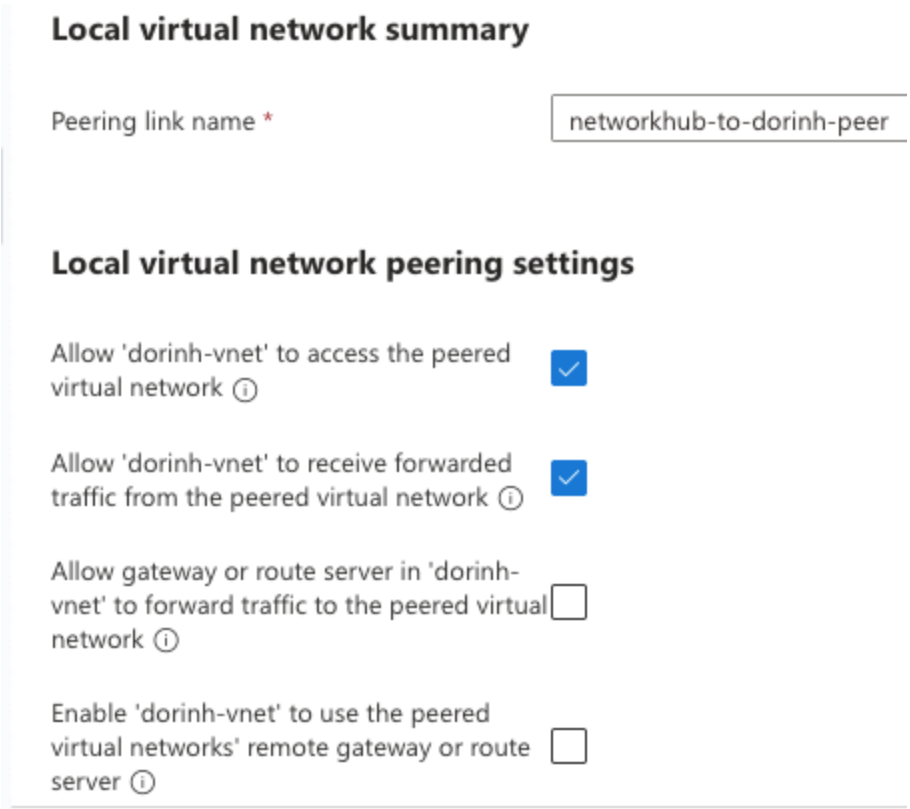
Create Peering from VNet1 to Hub

1. In the Azure Portal, navigate to "Virtual networks" and select VNet (the first VNet).
2. In **yourVnet** settings pane, under the "Settings" section, click on "Peerings."
3. Click on the "+ Add" button.



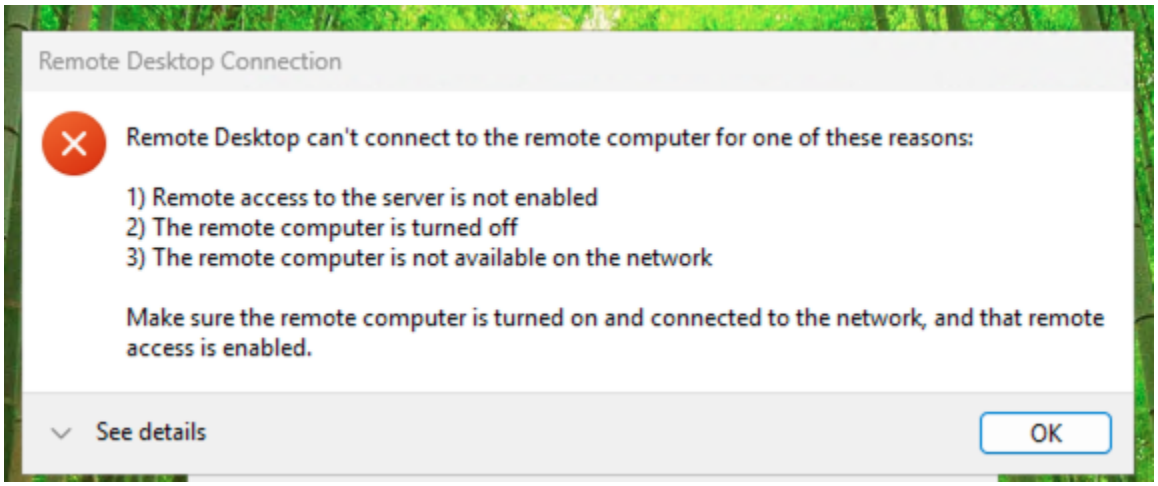
4. Fill in the details for the peering:
   - Name: Enter a descriptive name for the peering from VNet to ***yourName-to-networkhub-peer***
   - Peer details: Select the hub-network
   - Allow virtual network access: Set to "Enabled" to allow resources in VNet to communicate with networking-traning-hub-vnet.
5. Click "OK" to create the peering.





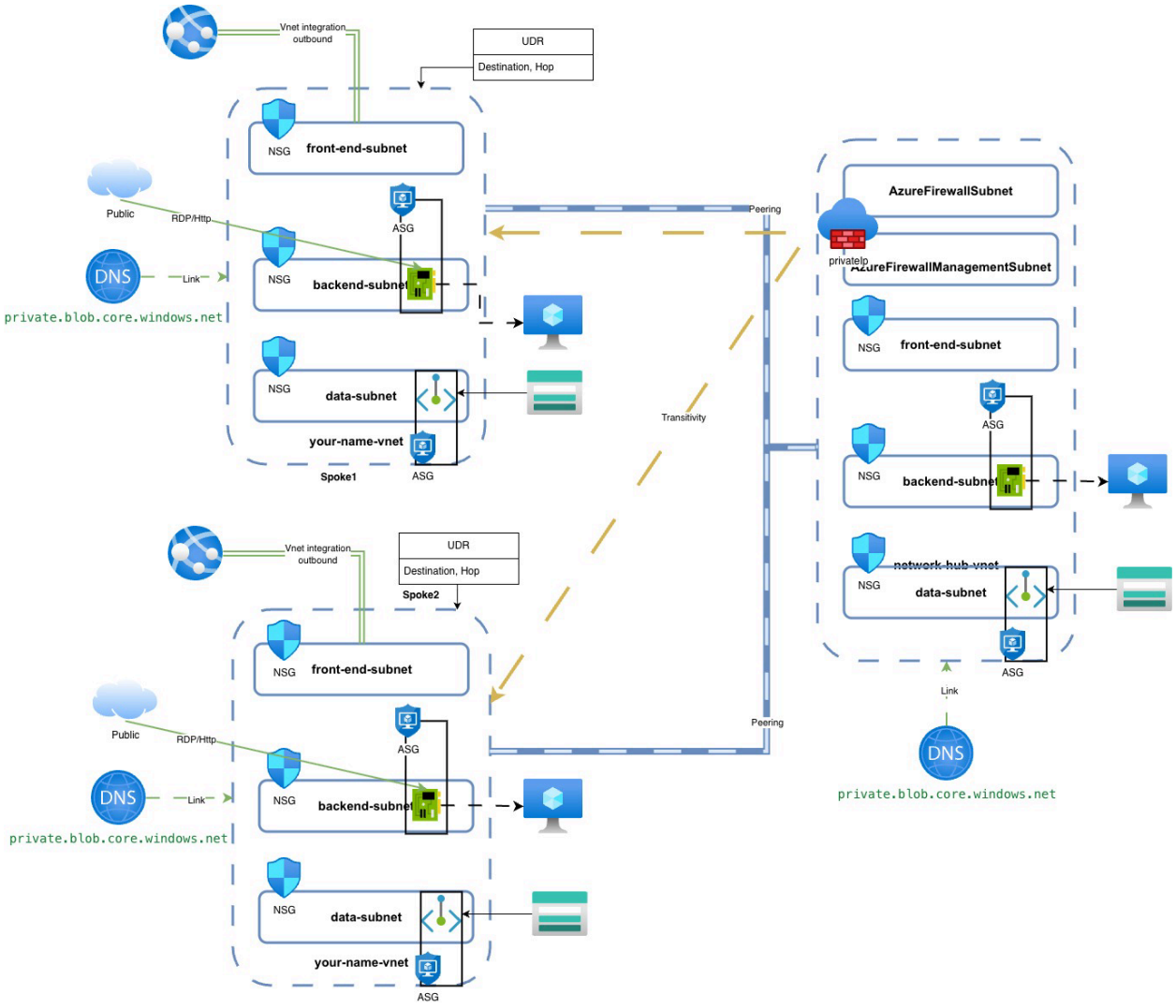
Test VNet Peering

1. Use the existing VM in the hub.
2. Obtain the private IP addresses of the ***networkhub-vm***.
    - ***Networkhub-vm*** is in the Hub and yournameVM is in your Spoke.
    - From yournameVM, try to RDP the private IP address of ***Networkhub-vm***.
    - From yournameVM, try to access the HTTP server on ***Networkhub-vm***



    - Why does it not work?
        i. Make the necessary adjustments to succeed.

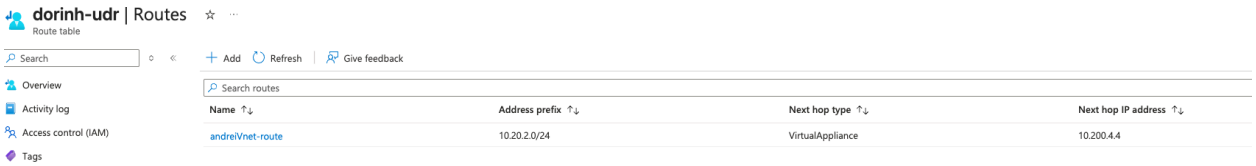
3. If the peering is set up correctly and there are no Network Security Group (NSG) rules blocking traffic, you should receive a response from ***Networkhub-vm***.
4. Play with the peering configurations



Solve the Transitivity problem

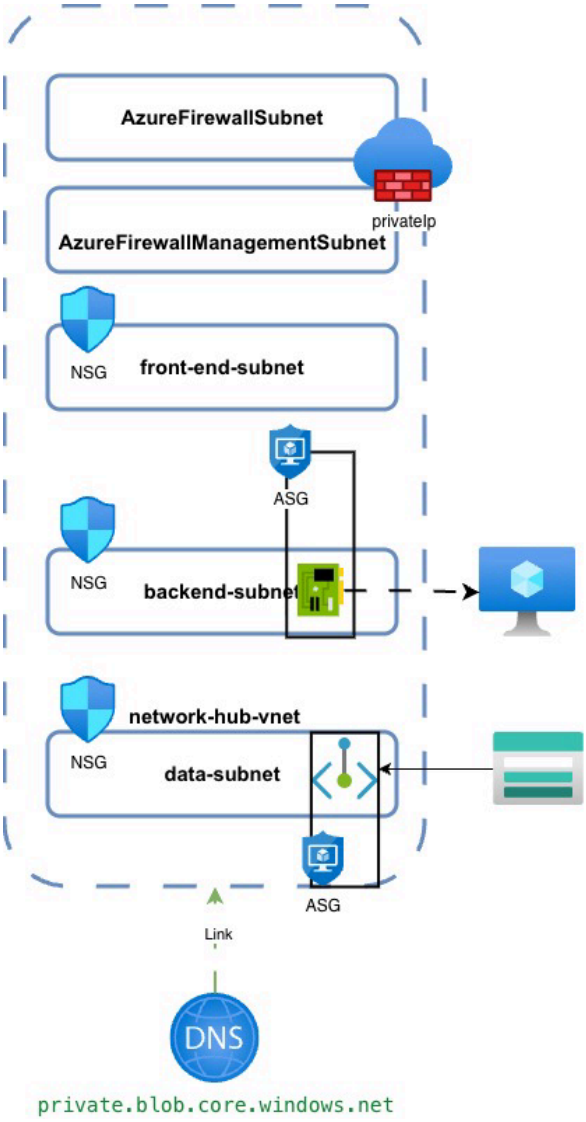
1. Create a route table for your Spoke
    - Go to **Route tables**
    - Click **Create**
    - Resource group: **your-name-rg**
    - Name: **your-name-udr**
    - Region: same as the spoke
    - Click **Review + create → Create**
2. Add a route to Spoke1(Peer) route table

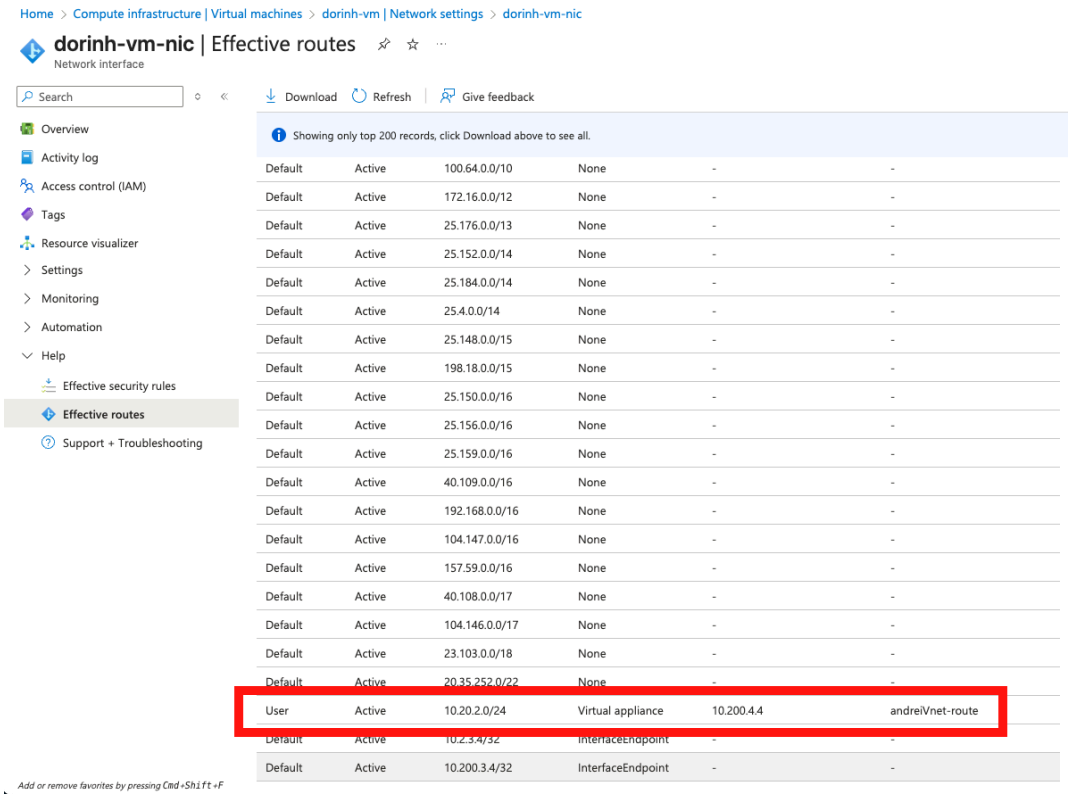
- Open **your-name-udr**

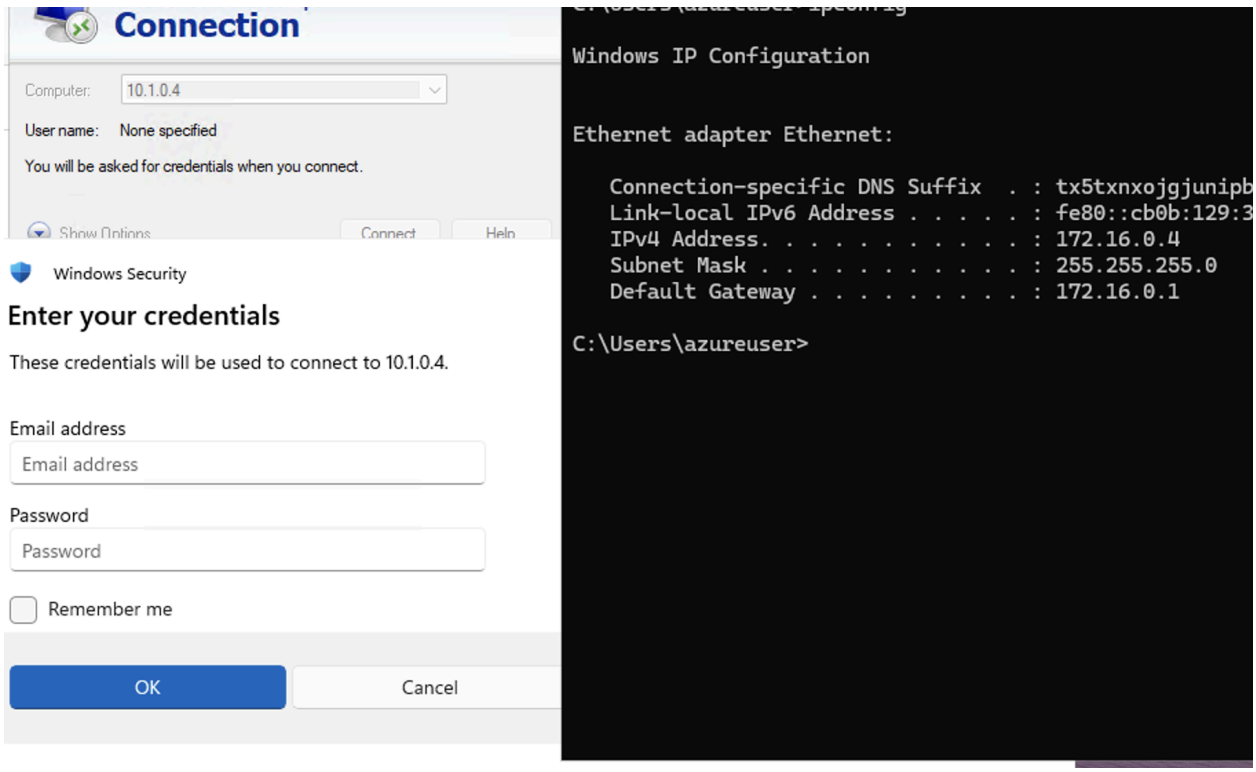


- Click **Routes → Add**
  - Route name: **yourVnet-to-hub-fw**
  - Address prefix: **Select the Vnet address from one of your peers**
  - Next hop type: **Virtual appliance**
  - Next hop address: **private IP of the hub firewall**
- Click **Add**
- **Ask your peer to do the same with your network**

3. Associate Spoke 1 subnet
   - Open **spoke1-udr**
   - Click **Subnets → Associate**
     - Virtual network: **spoke1-vnet**
     - Subnet: **spoke1-subnet**
   - Click **OK**
4. Verify traffic flow
   - Ensure both spokes have the UDR applied
   - Ensure both spokes are peerd to the hub
   - Ensure the firewall has rules allowing traffic
   - Try to RDP on your peer Vm



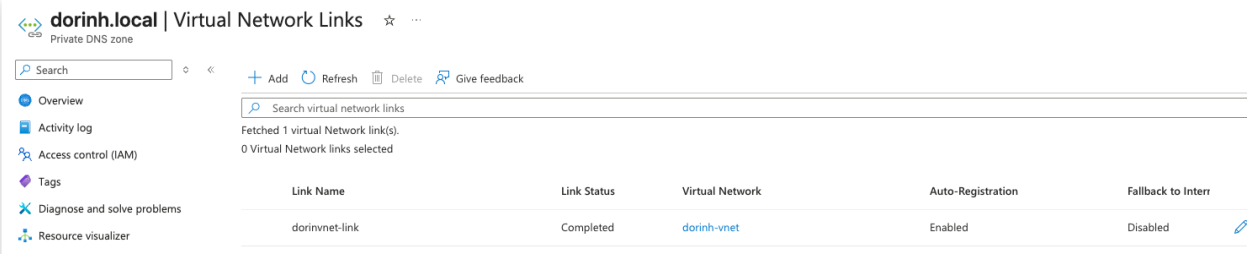

Home > Compute infrastructure | Virtual machines > dorinh-vm | Network settings > dorinh-vm-nic
dorinh-vm-nic | Effective routes
Network interface
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Settings
Monitoring
Automation
Help
Effective security rules
Effective routes
Support + Troubleshooting
Download
Refresh
Give feedback
Showing only top 200 records, click Download above to see all.
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 - -
Default Active 25.148.0.0/15 None - -
Default Active 198.18.0.0/15 None - -
Default Active 25.150.0.0/16 None - -
Default Active 25.156.0.0/16 None - -
Default Active 25.159.0.0/16 None - -
Default Active 40.109.0.0/16 None - -
Default Active 192.168.0.0/16 None - -
Default Active 104.147.0.0/16 None - -
Default Active 157.59.0.0/16 None - -
Default Active 40.108.0.0/17 None - -
Default Active 104.146.0.0/17 None - -
Default Active 23.103.0.0/18 None - -
Default Active 20.35.252.0/22 None - -
User Active 10.20.2.0/24 Virtual appliance 10.200.4.4 andreiVnet-route
Default Active 10.200.3.4/32 InterfaceEndpoint - -
Add or remove favorites by pressing Cmd+Shift+F


Connection
Computer: 10.1.0.4
User name: None specified
You will be asked for credentials when you connect.
Show Options
Connect
Help
Windows Security
Enter your credentials
These credentials will be used to connect to 10.1.0.4.
Email address
Email address
Password
Password
Remember me
OK
Cancel
Windows IP Configuration
Ethernet adapter Ethernet:
Connection-specific DNS Suffix . : tx5txnxojgjunipb
Link-local IPv6 Address . . . . . : fe80::cb0b:129:3
IPv4 Address. . . . . : 172.16.0.4
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 172.16.0.1
C:\Users\azureuser>

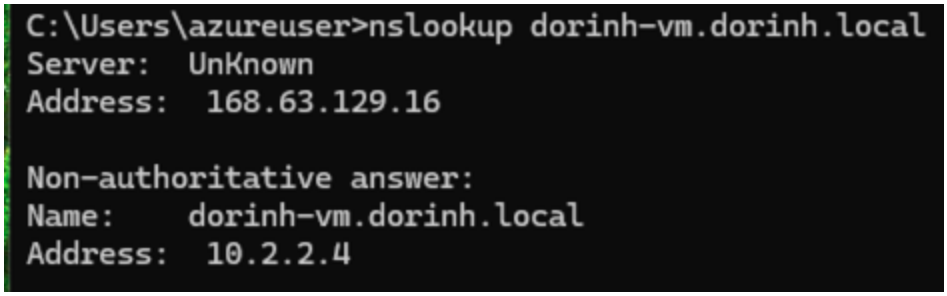
Create a Private DNS Zone

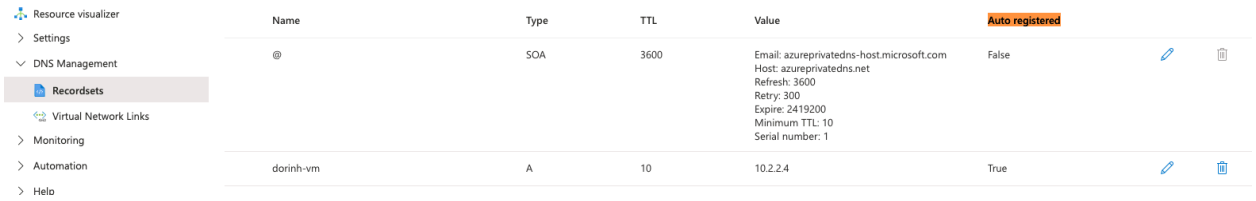
1. Log in to the Azure Portal:
    a. Navigate to https://portal.azure.com and sign in with your Azure account.
2. Go to the 'Private DNS zones' Service:
    a. In the left-hand menu, click on "Create a resource".
    b. In the search box, type “Private DNS zones” and select it.
    c. Click on the + Add button to create a new private DNS zone.
3. Fill in the Basics:
    a. Select your Subscription and Resource Group.
    b. Enter a name for the private DNS zone (e.g., **yourname**.local).
    c. Select the same region as your VNet.
4. Review and Create:
    a. Review the settings.
    b. Click on "Review + Create," then click "Create."

Link the Private DNS Zone to a VNet



1. Navigate to the Created Private DNS Zone:
    - From the Azure portal dashboard, go to Resource groups.
    - Select your resource group and click on the private DNS zone you just created.
2. Link to VNet:
    - In the DNS zone's left menu, under the Settings section, click Virtual Network Links.
    - Click on the + Add button to create a new link.
3. Configure the Link:
    - Provide a name for the link.
    - Choose your Subscription (if it’s not already selected).
    - For the Virtual Network, select the desired VNet from the dropdown list.
    - Set Registration to '**Yes**'
    - Click OK to create the link.
4. Try to perform an nslookup for the VM of one of your peers
    - Eg: *Nslookup andrei-vm.andrei.local*
    - Does it work? Why? Discuss how to fix this.


C:\Users\azureuser>nslookup dorinh-vm.dorinh.local
Server: UnKnown
Address: 168.63.129.16
Non-authoritative answer:
Name: dorinh-vm.dorinh.local
Address: 10.2.2.4


Resource visualizer
Settings
DNS Management
Recordsets
Virtual Network Links
Monitoring
Automation
Help
Name
Type
TTL
Value
Auto registered
@
SOA
3600
Email: azureprivatedns-host.microsoft.com
Host: azureprivatedns.net
Refresh: 3600
Retry: 300
Expire: 2419200
Minimum TTL: 10
Serial number: 1
False
dorinh-vm
A
10
10.2.2.4
True