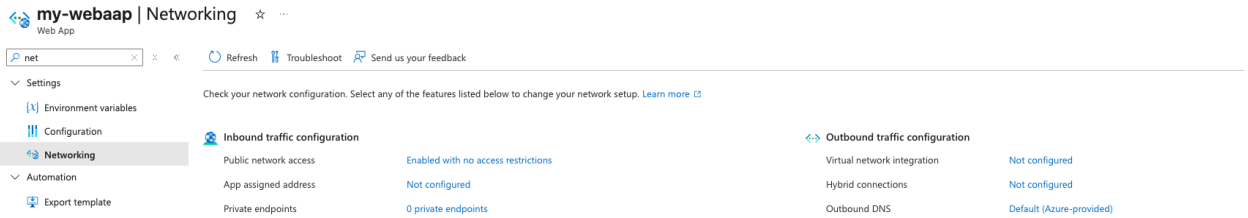
Create an App Service

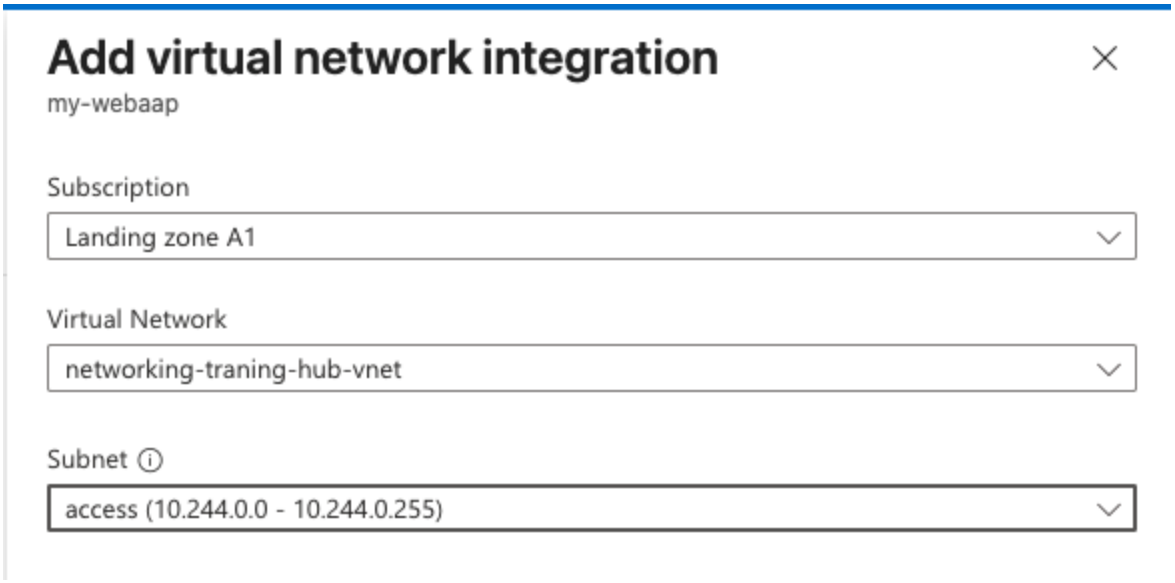
1. Navigate to the Azure Portal.
2. In the left-hand sidebar, click on "+ Create a resource."
3. Search for "Web App" and select it.
4. Click the "Create" button to initiate the setup.
5. Fill in the details for your App Service:
    - Subscription: Select the appropriate subscription.
    - Resource Group: Choose an existing resource group or create a new one.
    - Name: Provide a unique name for the App Service.
    - Publish: Select 'Code' or 'Docker Container' depending on your use case.
    - Runtime stack: Choose the appropriate runtime for your application (e.g., .NET, Node.js).
    - Operating System: Choose between Windows and Linux based on your application's requirements.
    - 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."



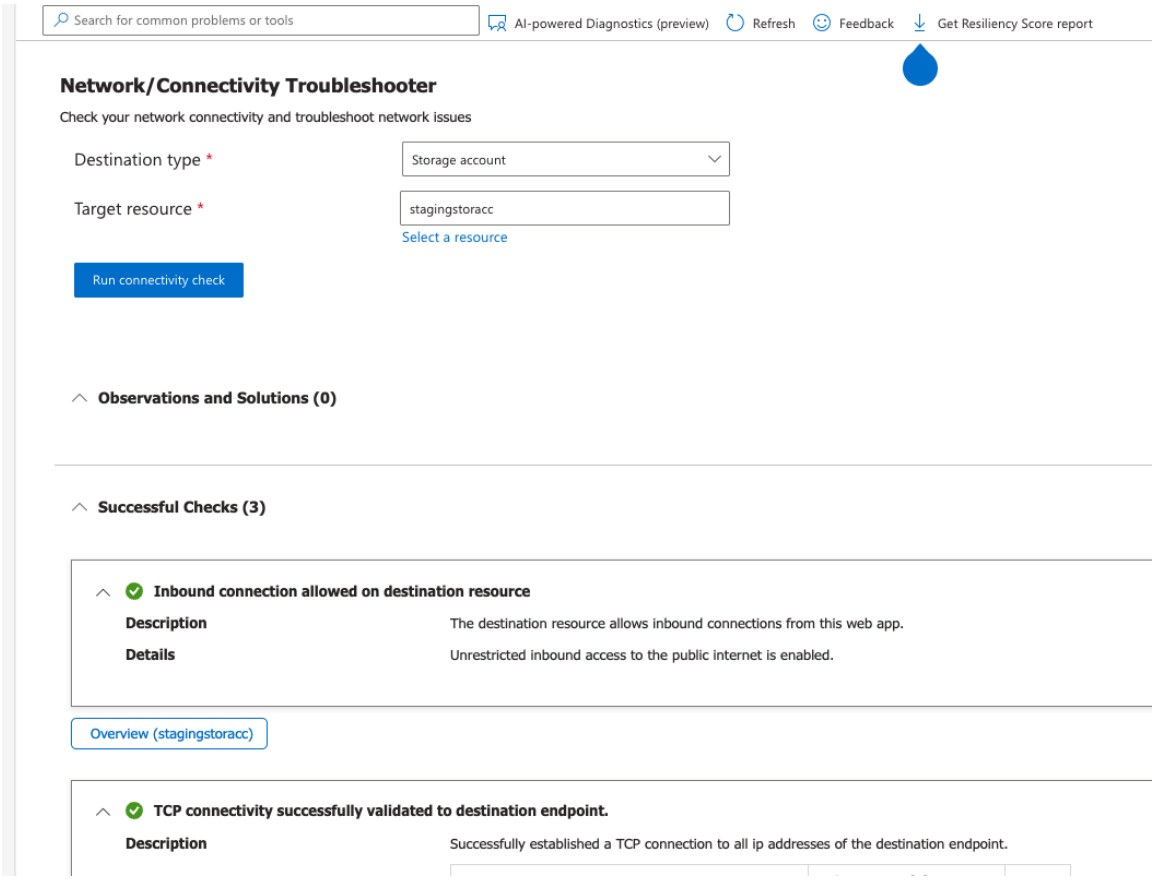
3. Under the "VNet Integration" section, click on "Click here to configure."
4. Click on "+ Add VNet" to start the VNet Integration setup.
5. You'll be presented with two options: "Integrate with an existing virtual network" or "Create a new VNet." If you have an existing VNet you'd like to integrate with, select that. Otherwise, you can set up a new VNet directly from here.



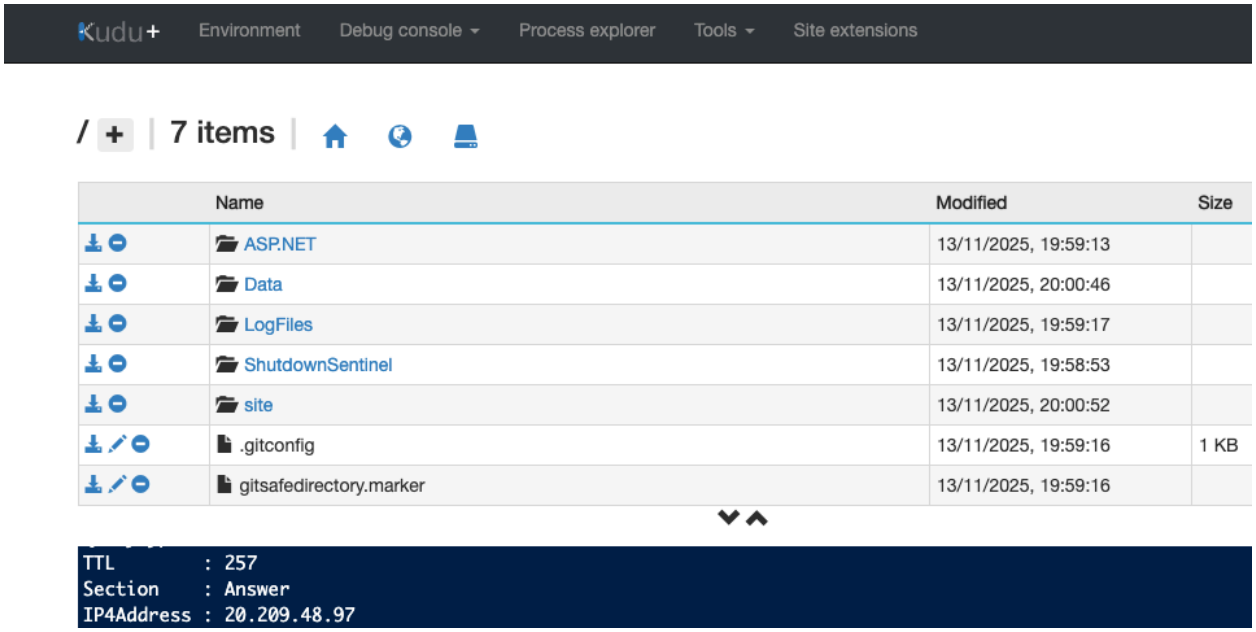
6. Fill in the required details:
    - Virtual Network: If using an existing VNet, select it from the dropdown list.
    - Subnet: Choose the appropriate subnet.
7. Click "OK" to initiate the integration.

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 Networking Tools
    - 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. Use NSGs to block the App Service from accessing the storage account private endpoint, but the VM should retain its access
6. To access the private endpoint, use the Kudu console: Advanced tools



Create Peering from VNet1 to Hub

1. In the Azure Portal, navigate to "Virtual networks" and select VNet (the first VNet).
2. In the VNet1 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 networking-traning-hub-vnet.
    - Peer details: Select "I know my resource ID" or "I know my resource details" and then select networking-traning-hub-vnet as the peer VNet.
    - 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.

Add peering

spoke1-vnet

Remote virtual network summary

Peering link name * Sopoke1-net-hub-vnet

I know my resource ID ⓘ ☐

Subscription * Landing zone A1

Virtual network * networking-traning-hub-vnet (networking-traning-hub-rg)

Remote virtual network peering settings

Allow 'networking-traning-hub-vnet' to access 'spoke1-vnet' ⓘ ☑

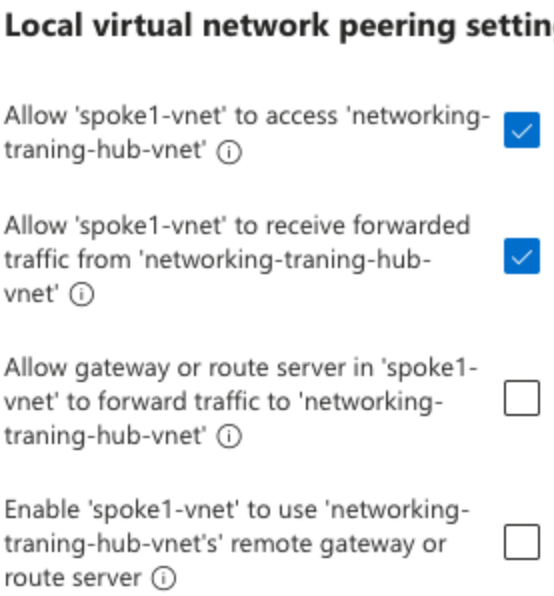
Allow 'networking-traning-hub-vnet' to receive forwarded traffic from 'spoke1-vnet' ⓘ ☑

Allow gateway or route server in 'networking-traning-hub-vnet' to forward traffic to 'spoke1-vnet' ⓘ ☐

Enable 'networking-traning-hub-vnet' to use 'spoke1-vnet's' remote gateway or route server ⓘ ☐

Local virtual network summary

Peering link name * Net-hub-Spoke1-vnet



Test VNet Peering

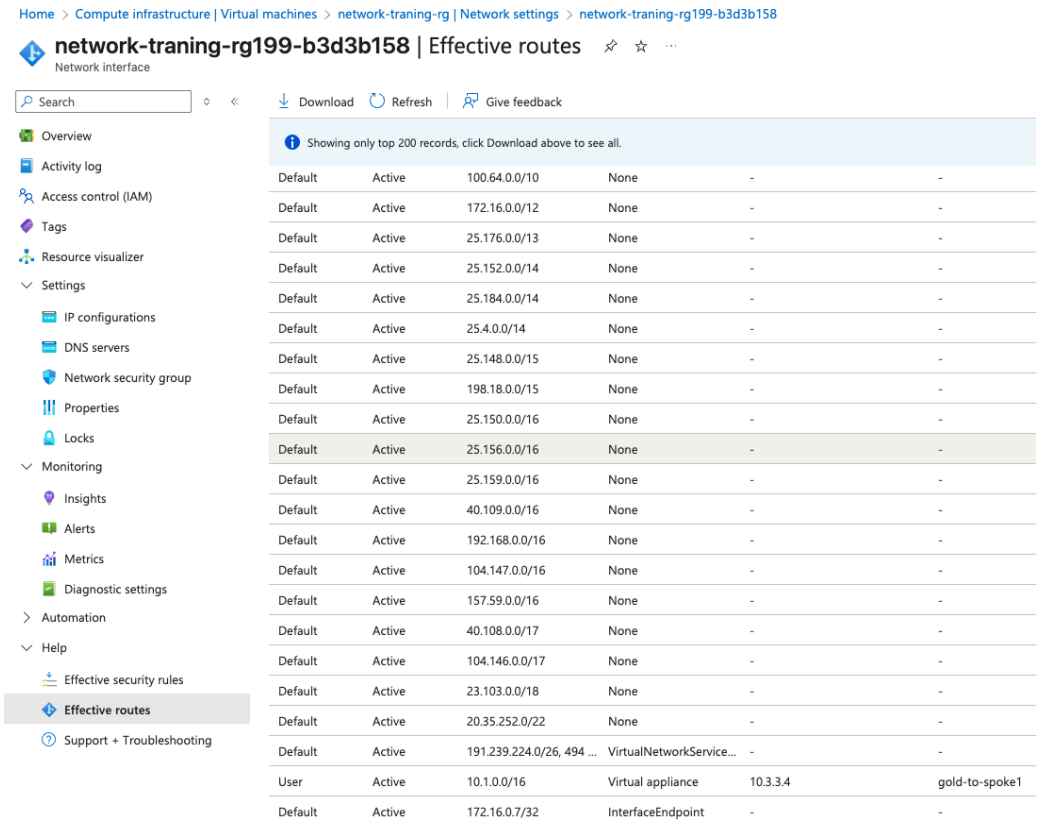
1. Deploy VMs (or use existing ones) in both VNet and networking-traning-hub-vnet.
2. Obtain the private IP addresses of these VMs. Let's say VM1 is in VNet1 and VM2 is in networking-traning-hub-vnet.
3. From VM1, try to RDP the private IP address of VM2.
4. If the peering is set up correctly and there are no Network Security Group (NSG) rules blocking traffic, you should receive a response from VM2.
5. Play with the peering configurations
    - One way peering

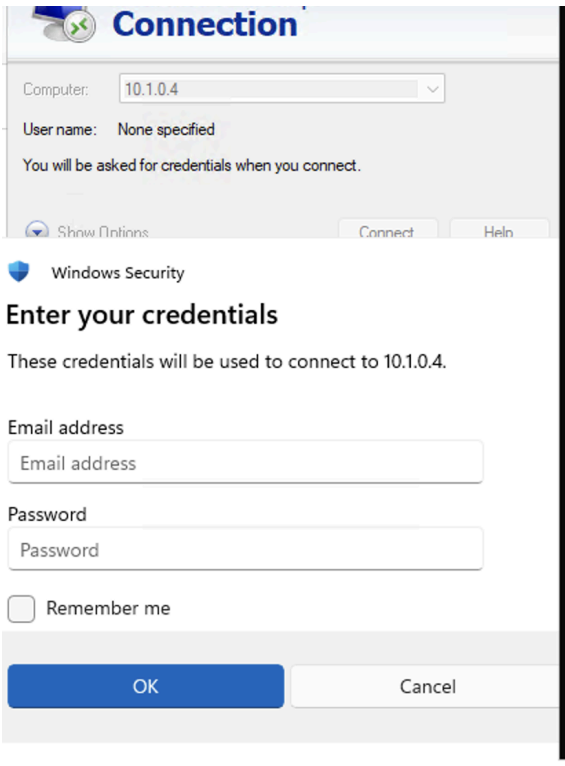
Solve the Transitivity problem

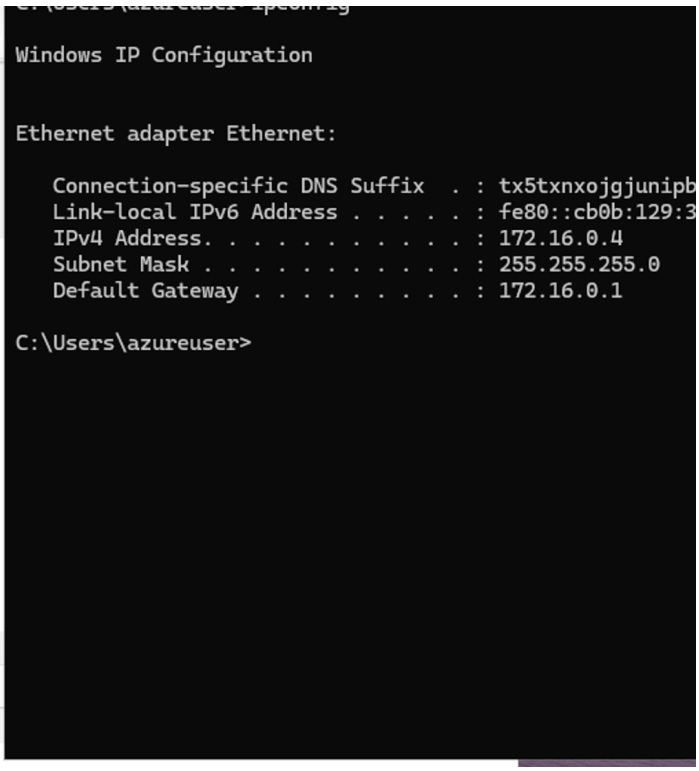
1. Create a route table for your Spoke
    - Go to **Route tables**
    - Click **Create**
    - Resource group: **your-name-rg**
    - Name: **spoke1-udr**
    - Region: same as the spoke
    - Click **Review + create** → **Create**
2. Add a route to Spoke 1 route table
    - Open **spoke1-udr**
    - Click **Routes** → **Add**

        - Route name: **default-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 peered to the hub
    - Ensure the firewall has rules allowing traffic
    - Try to RDP on your peer Vm


Home > Compute infrastructure | Virtual machines > network-traning-rg | Network settings > network-traning-rg199-b3d3b158
network-traning-rg199-b3d3b158 | Effective routes
Network interface
Search
Overview
Activity log
Access control (IAM)
Tags
Resource visualizer
Settings
IP configurations
DNS servers
Network security group
Properties
Locks
Monitoring
Insights
Alerts
Metrics
Diagnostic settings
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 - -
Default Active 191.239.224.0/26, 494 ... VirtualNetworkService... - -
User Active 10.1.0.0/16 Virtual appliance 10.3.3.4 gold-to-spoke1
Default Active 172.16.0.7/32 InterfaceEndpoint - -


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. Login 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 (or create a new resource group).
    b. Enter a name for the private DNS zone (e.g., myprivatezone.local).
    c. Select the desired region (usually 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 on 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' if you want the DNS records of the VMs in the VNet to be automatically registered in this DNS zone. Otherwise, set it to 'No'.
    - Click OK to create the link.