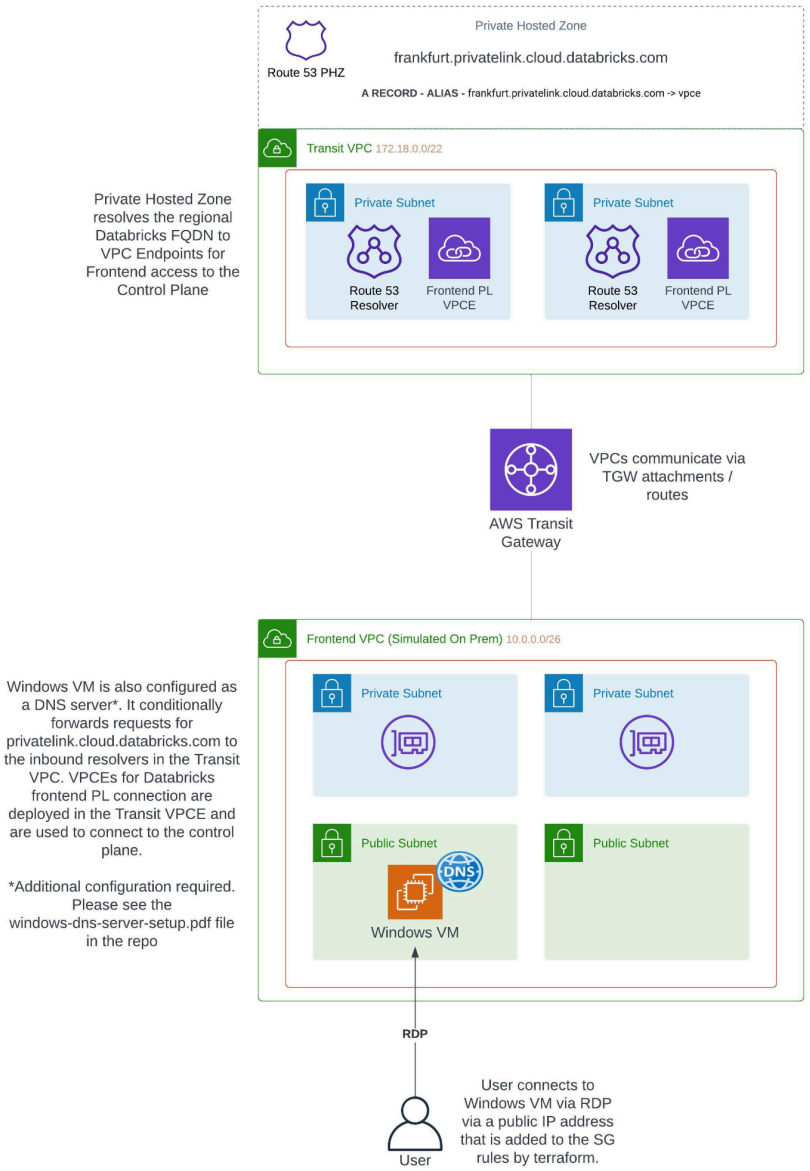
Important Note 1
High Level Architecture 2
Steps to Reproduce 2

Important Note

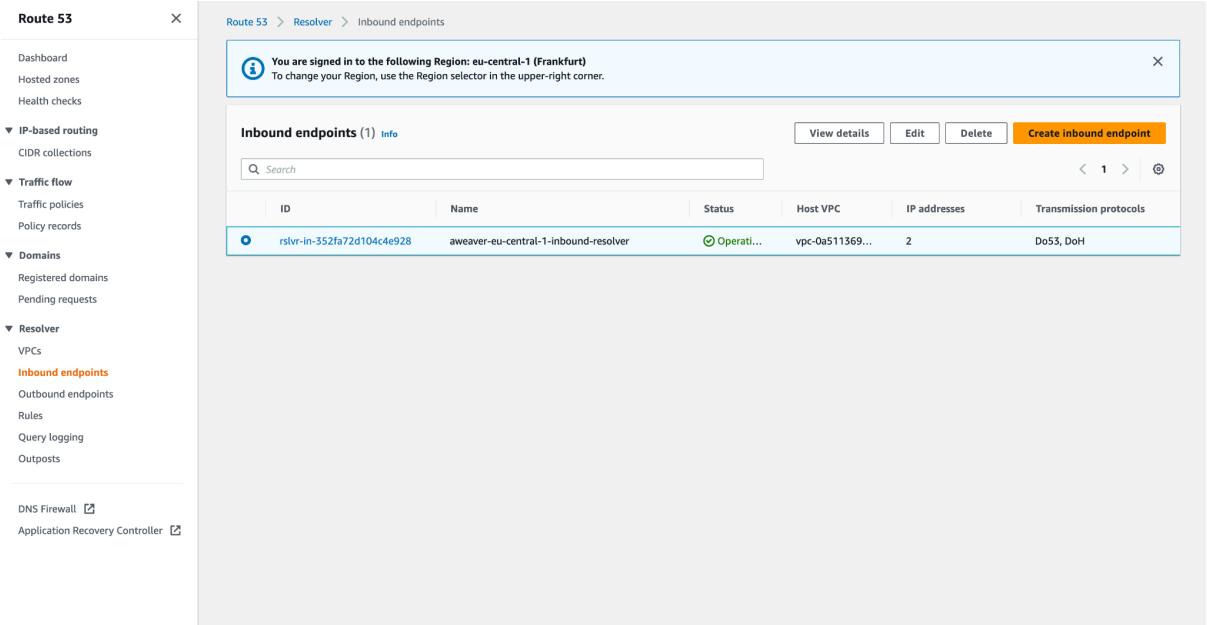
During testing I observed strange behaviour running Windows as a DNS server on AWS - namely that when the TTL for a conditionally forwarded domain expired for some reason the conditional forwarding wouldn't kick in and it would instead use Amazon DNS to resolve locally. When that TTL expired the conditional forwarding would work correctly and we'd be back to the private resolution for that workspace. Unfortunately this intermittently broke the PrivateLink connection (except for within the browser where some kind of caching seemed to be going on). I also experimented with AWS Directory Service and Simple AD but saw the same thing. I was able to get my PrivateLink setup stable by adding my AWS Route 53 Inbound Endpoint IPs as global (not conditional) forwarders. My recommendation if you see the behaviour above would be to add your AWS Route 53 Inbound Endpoint IPs as global forwarders or (if this practice is for some reason disallowed) raise support tickets with Microsoft and AWS for the behaviour observed (based on a few Google searches I am not the only one that has encountered this).

High Level Architecture

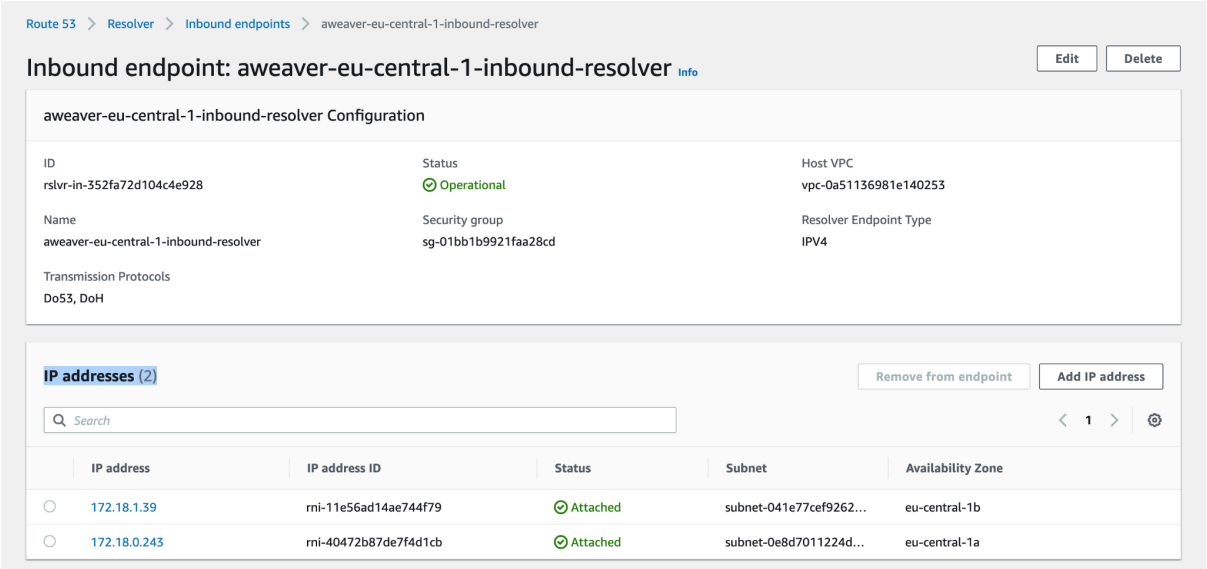


Steps to Reproduce

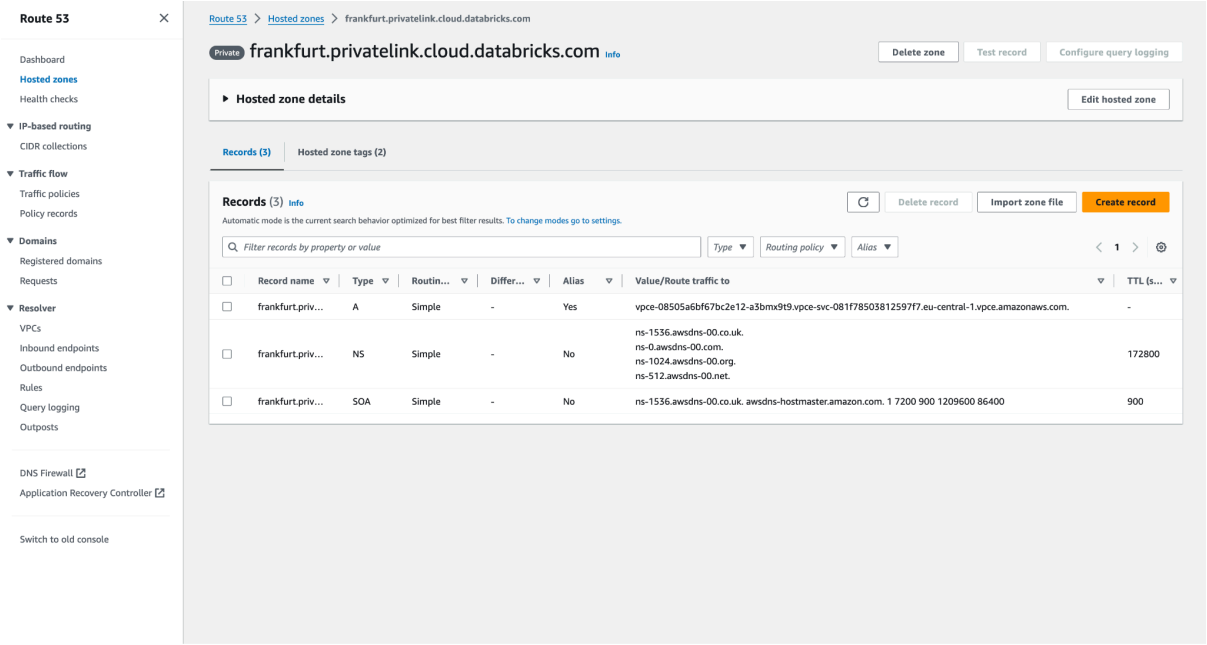
- Clone the repo
- Follow the steps in the README.md
- Login to https://accounts.cloud.databricks.com/, find and add yourself as a user of the workspace. Also make a note of the workspace FQDN
- In the AWS console, go to Route 53 and find the Inbound resolver endpoint created by Terraform:



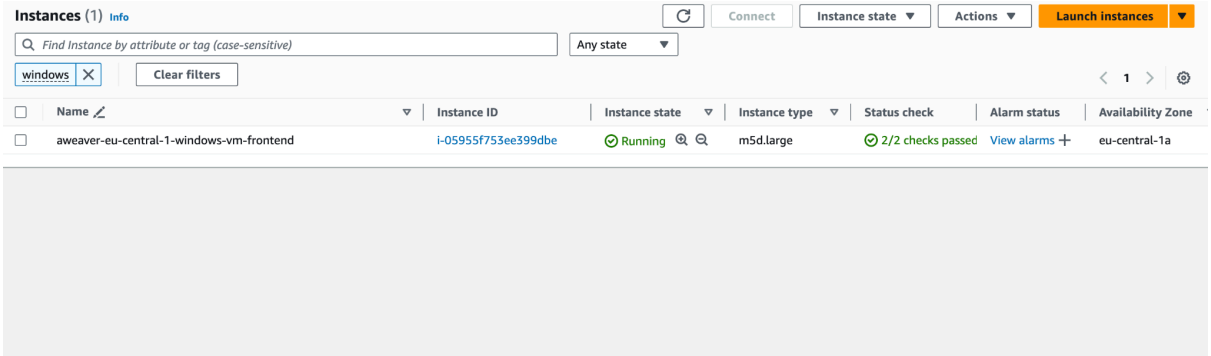
- Select View details and make a note of the IP addresses (2):



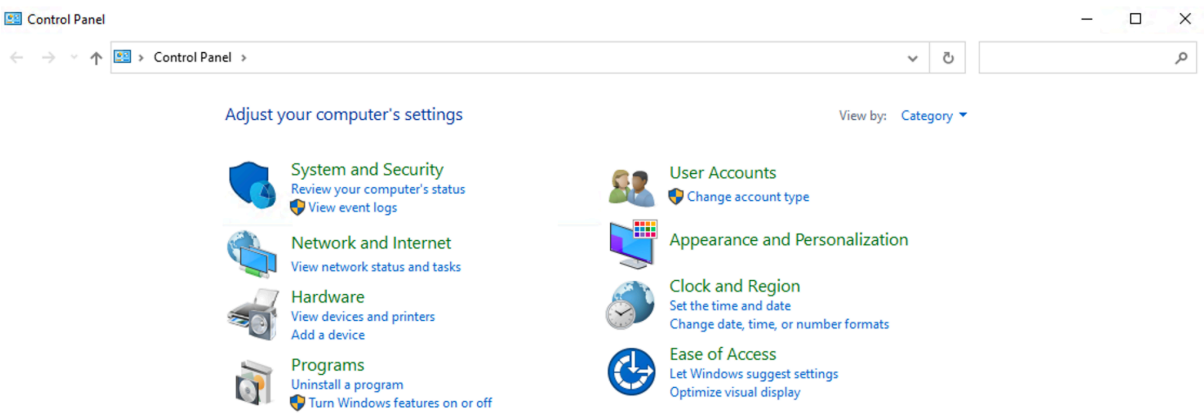
- Go to Hosted zones and find the Private Hosted Zone created by Terraform:

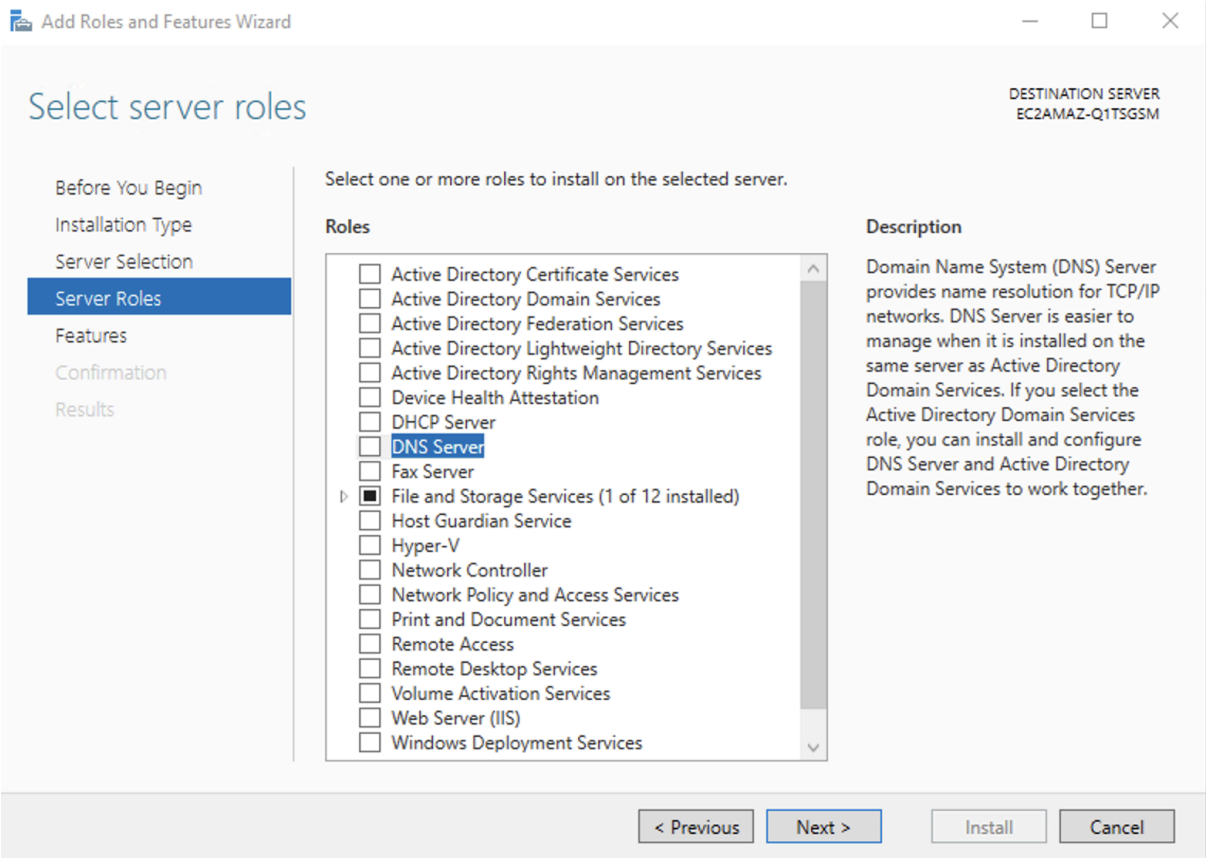


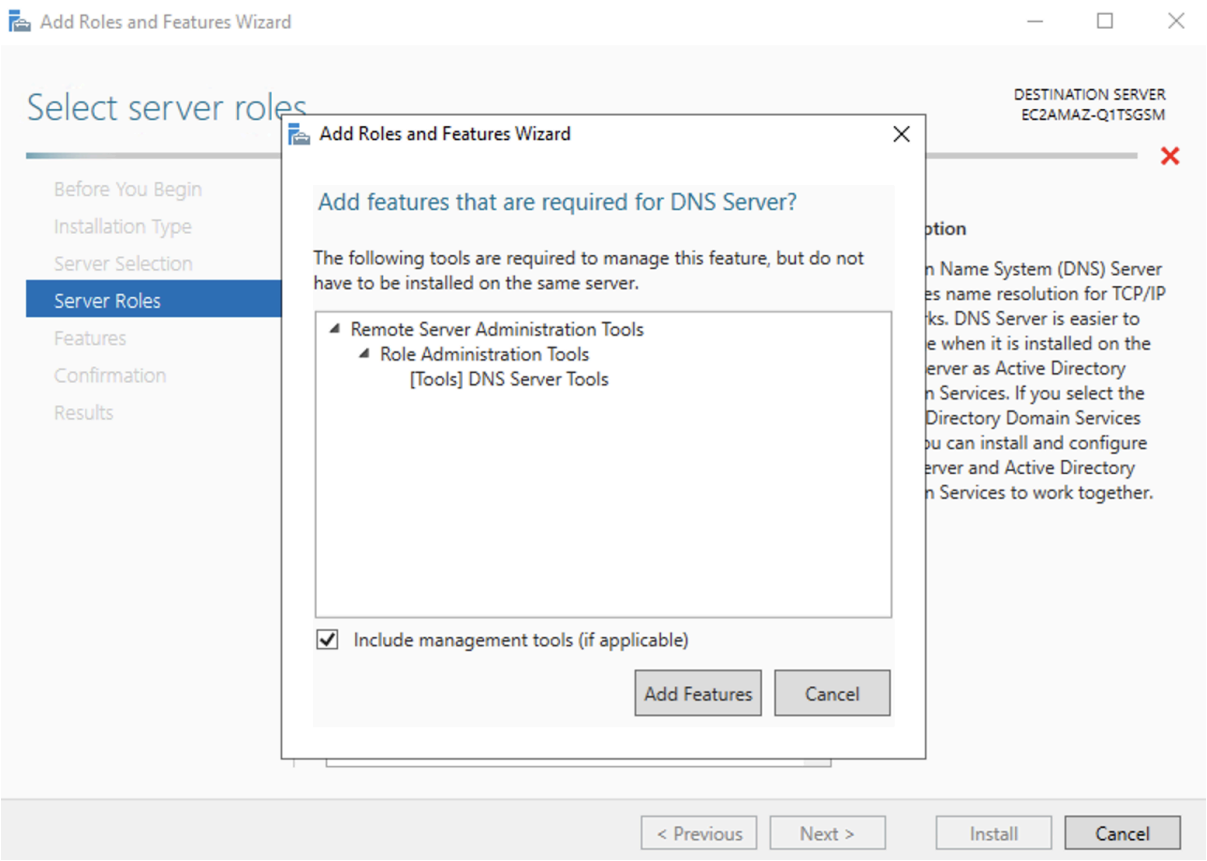
- Make a note of the Zone name and VPC Endpoint FQDN (the Value/Route traffic to for the Type A record). Now go to the VPC pages and find the VPC endpoint in question. Select Subnets and note the Private IP addresses allocated to the VPCEs.
- Now navigate to the EC2 page and find the Windows EC2 instance created by Terraform:

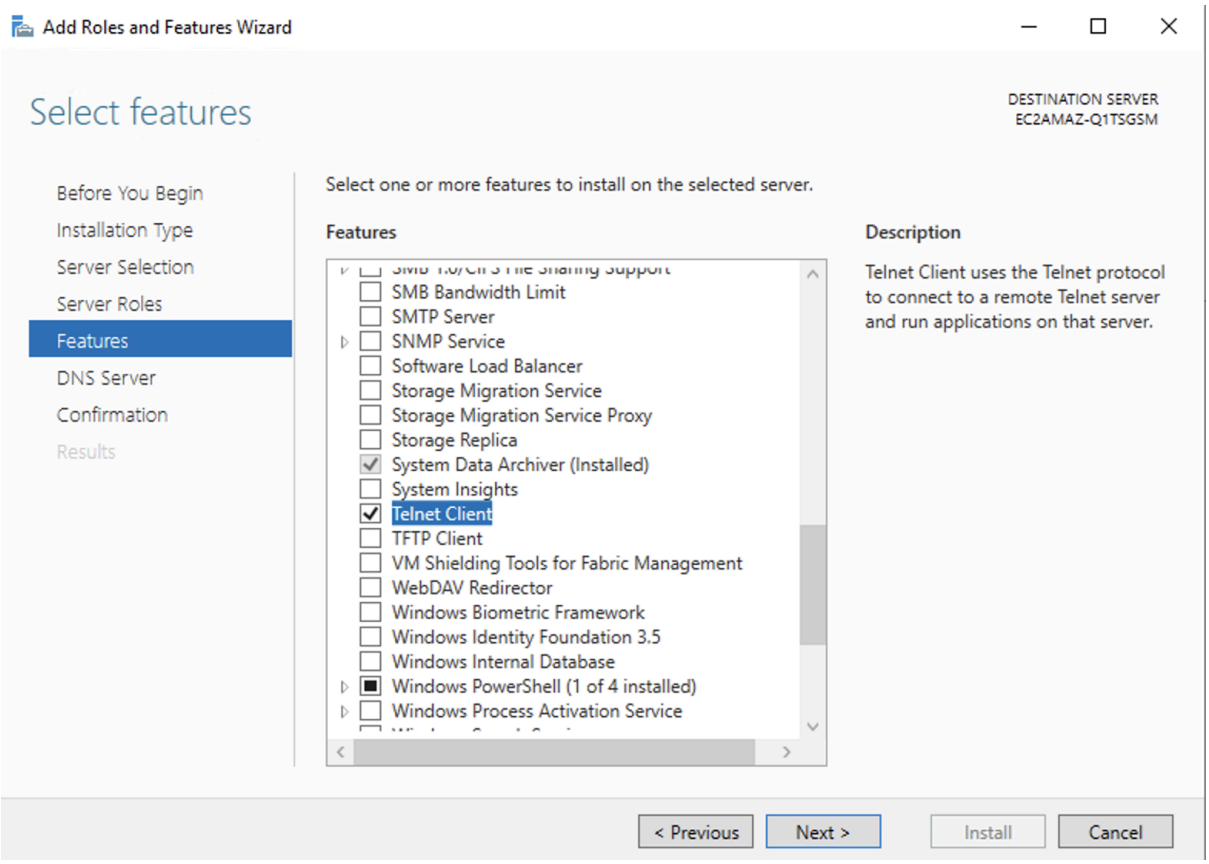


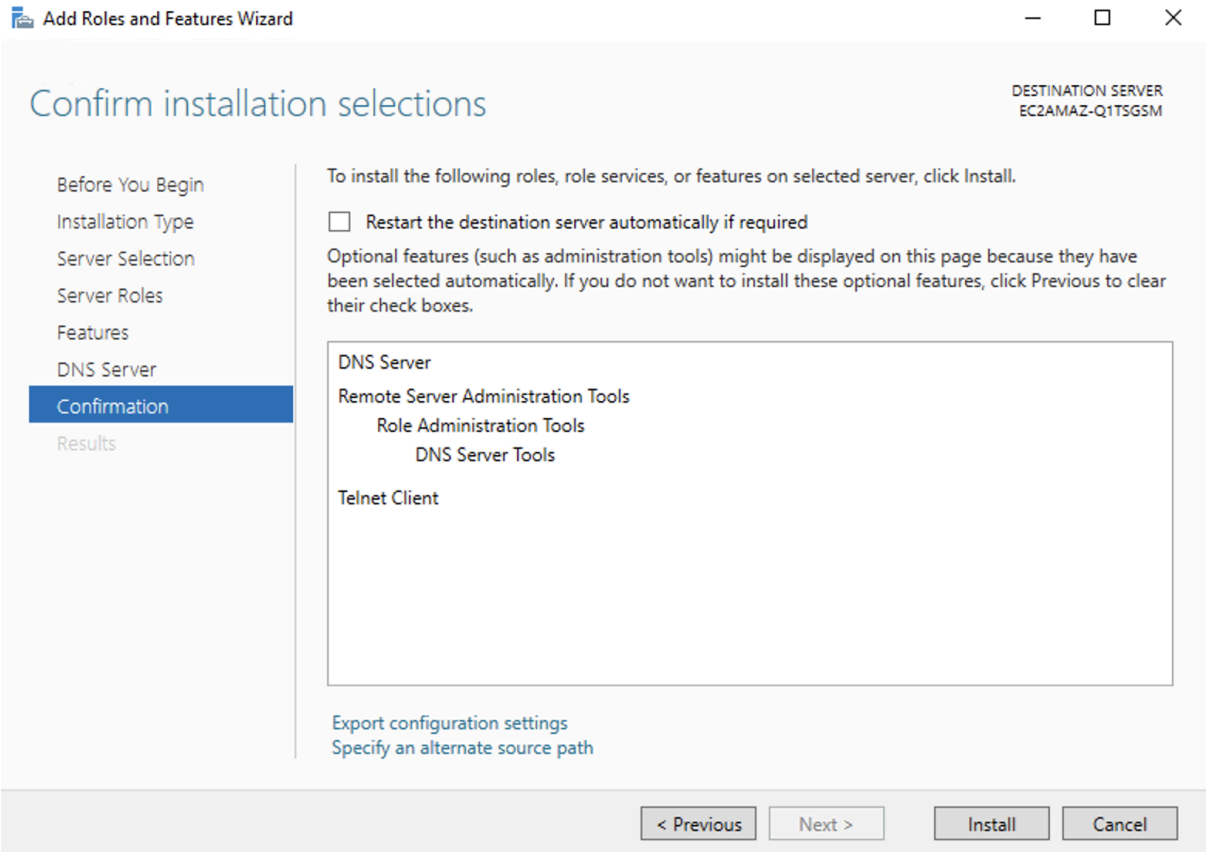
- We’re going to use this EC2 instance to simulate an on prem environment. For ease of setup the EC2 instance will act as both the on prem workstation and the on prem DNS server.
- Select the EC2 instance then:
    - Connect
    - RDP client
- Use your EC2 keypair to get the EC2 instance password
- Select Download remote desktop file and use it to RDP into the EC2 instance (your public IP address should be allow-listed via the rdp_public_ip Terraform variable.
- First let's enable the Windows features we’re going to need. Go to:
    - Control Panel
    - Programs
    - Turn Windows features on or off
- Install the DNS server role and Telnet client:

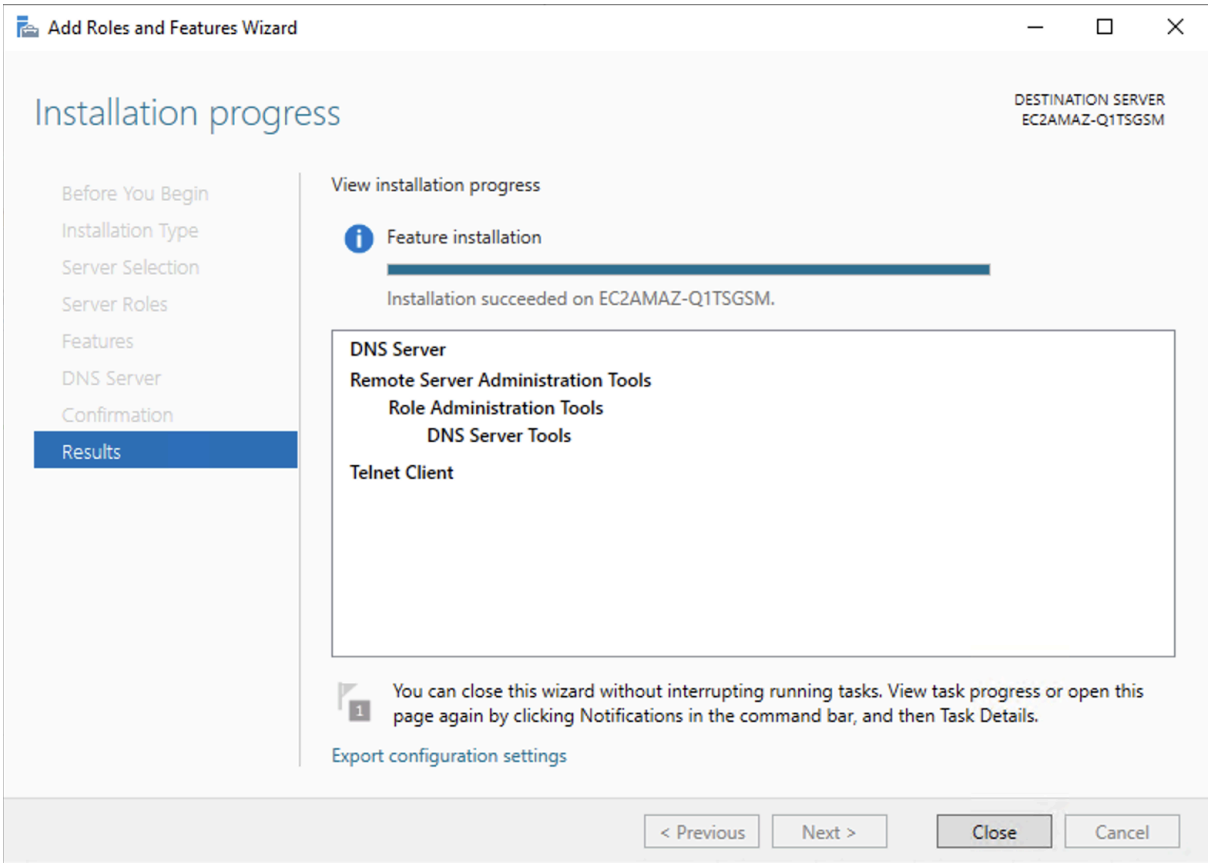

Control Panel
Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
View event logs
Network and Internet
View network status and tasks
Hardware
View devices and printers
Add a device
Programs
Uninstall a program
Turn Windows features on or off
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Set the time and date
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display


Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
EC2AMAZ-Q1TSGSM
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
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 Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Description
Domain Name System (DNS) Server provides name resolution for TCP/IP networks. DNS Server is easier to manage when it is installed on the same server as Active Directory Domain Services. If you select the Active Directory Domain Services role, you can install and configure DNS Server and Active Directory Domain Services to work together.
< Previous
Next >
Install
Cancel


Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
EC2AMAZ-Q1TSGSM
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Confirmation
Results
Add Roles and Features Wizard
Add features that are required for DNS Server?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Remote Server Administration Tools
Role Administration Tools
[Tools] DNS Server Tools
Include management tools (if applicable)
Add Features
Cancel
< Previous
Next >
Install
Cancel

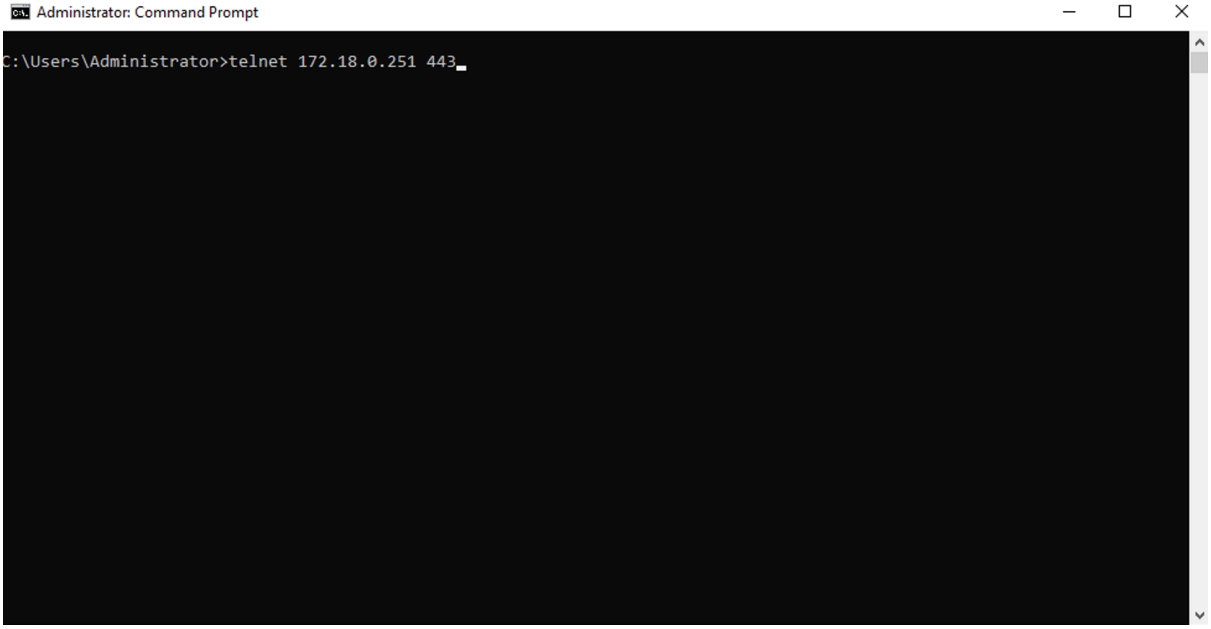

Add Roles and Features Wizard
Select features
DESTINATION SERVER
EC2AMAZ-Q1TSGSM
Before You Begin
Installation Type
Server Selection
Server Roles
Features
DNS Server
Confirmation
Results
Select one or more features to install on the selected server.
Features
Description
SMB Bandwidth Limit
SMTP Server
SNMP Service
Software Load Balancer
Storage Migration Service
Storage Migration Service Proxy
Storage Replica
System Data Archiver (Installed)
System Insights
Telnet Client
TFTP Client
VM Shielding Tools for Fabric Management
WebDAV Redirector
Windows Biometric Framework
Windows Identity Foundation 3.5
Windows Internal Database
Windows PowerShell (1 of 4 installed)
Windows Process Activation Service
Telnet Client uses the Telnet protocol to connect to a remote Telnet server and run applications on that server.
< Previous
Next >
Install
Cancel

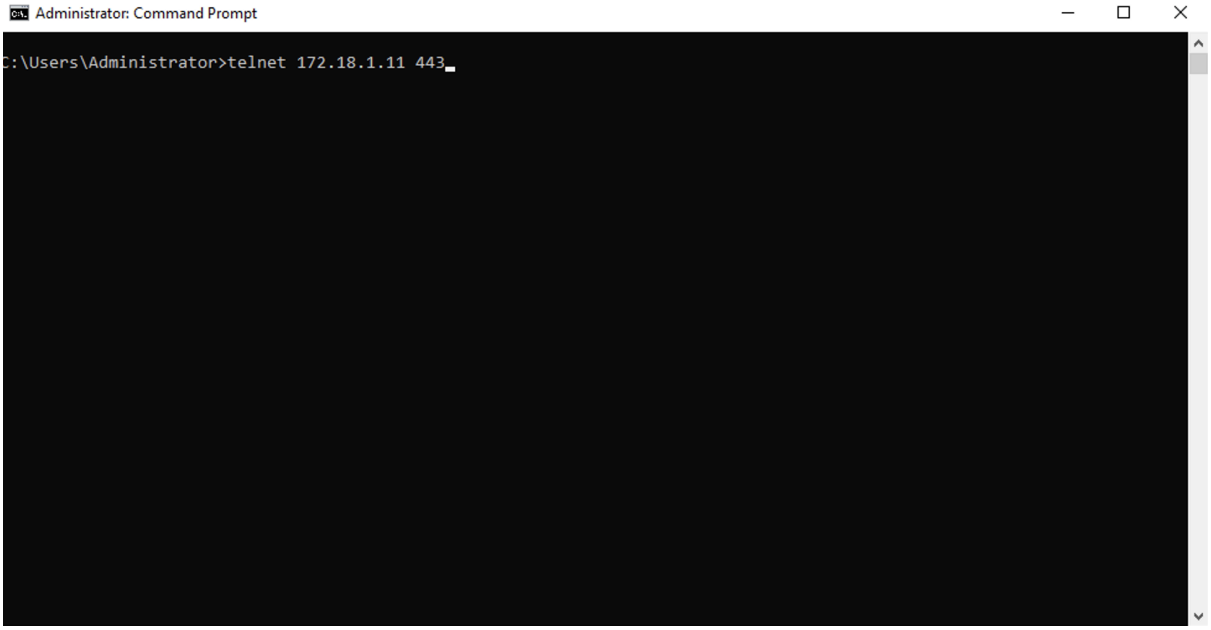




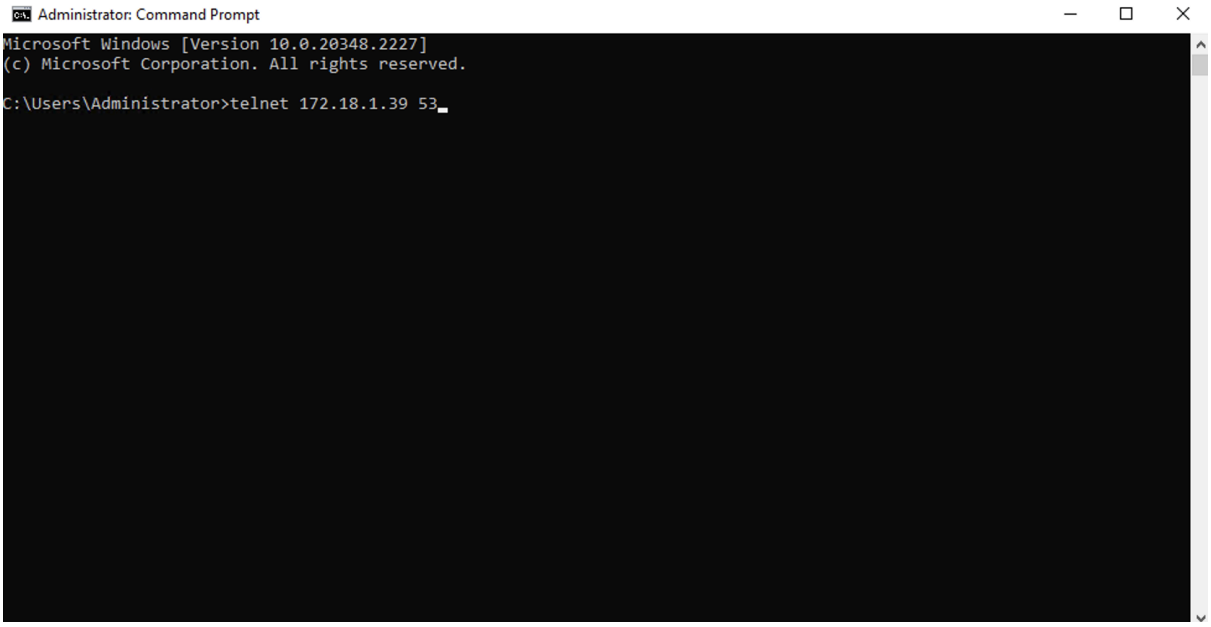
- Open a command prompt and test the connection to the frontend VPC endpoint IPs. If you get `Connect failed`, check the Security Group rules for the

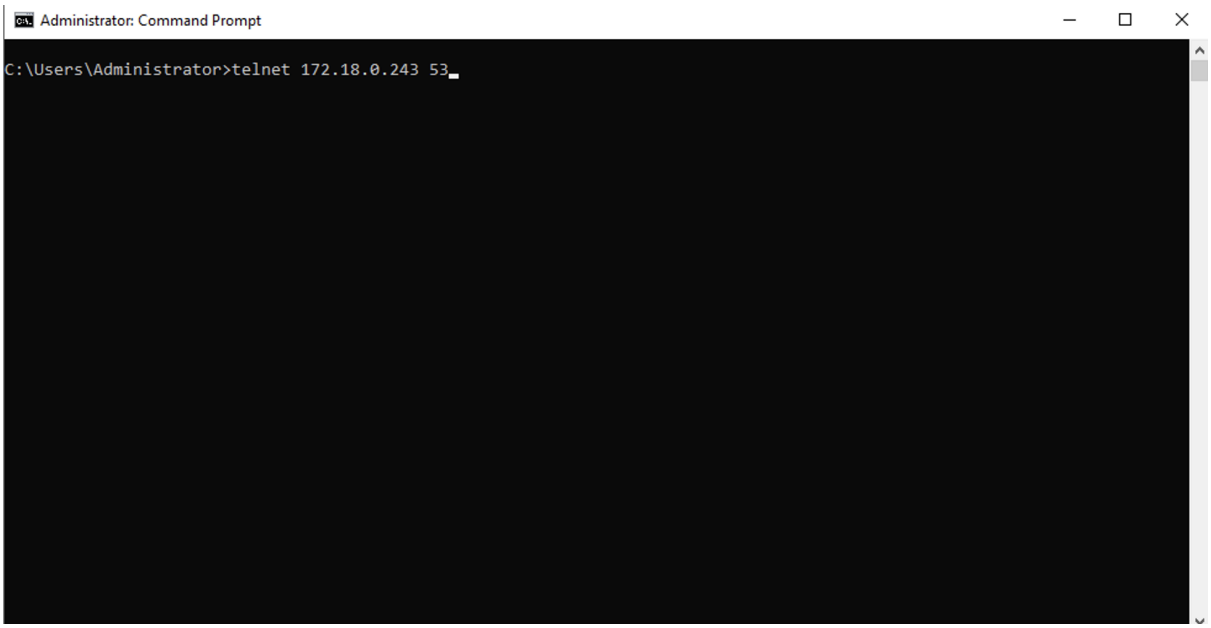
`<resource_prefix>-frontend-sg` and `<resource_prefix>-transit-sg` SGs. Sometimes Terraform doesn't add the rules that allow the frontend VPC (Windows VM) and Transit VPC to talk to each other. If this happens, add inbound and outbound rules to both Security Groups to allow traffic between the CIDR ranges of the VPCs:



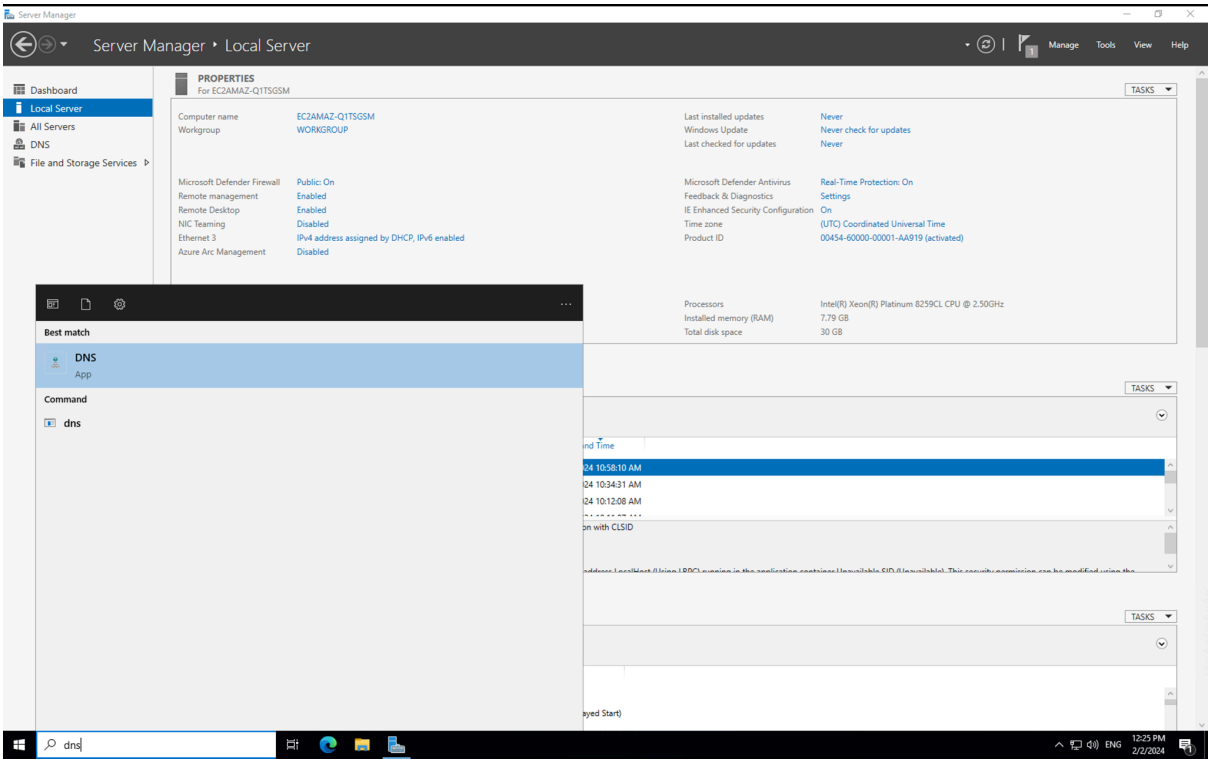


- Next test the connection to the Route 53 inbound resolvers:

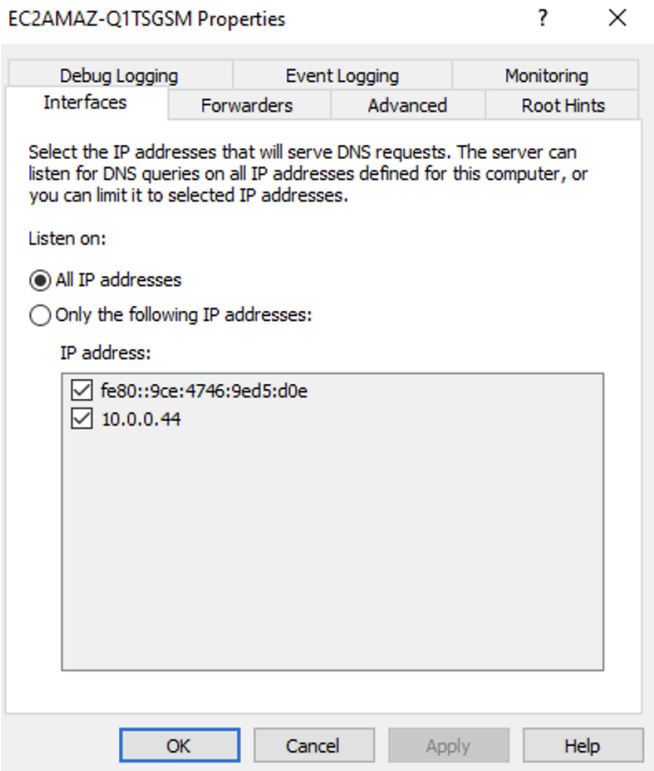




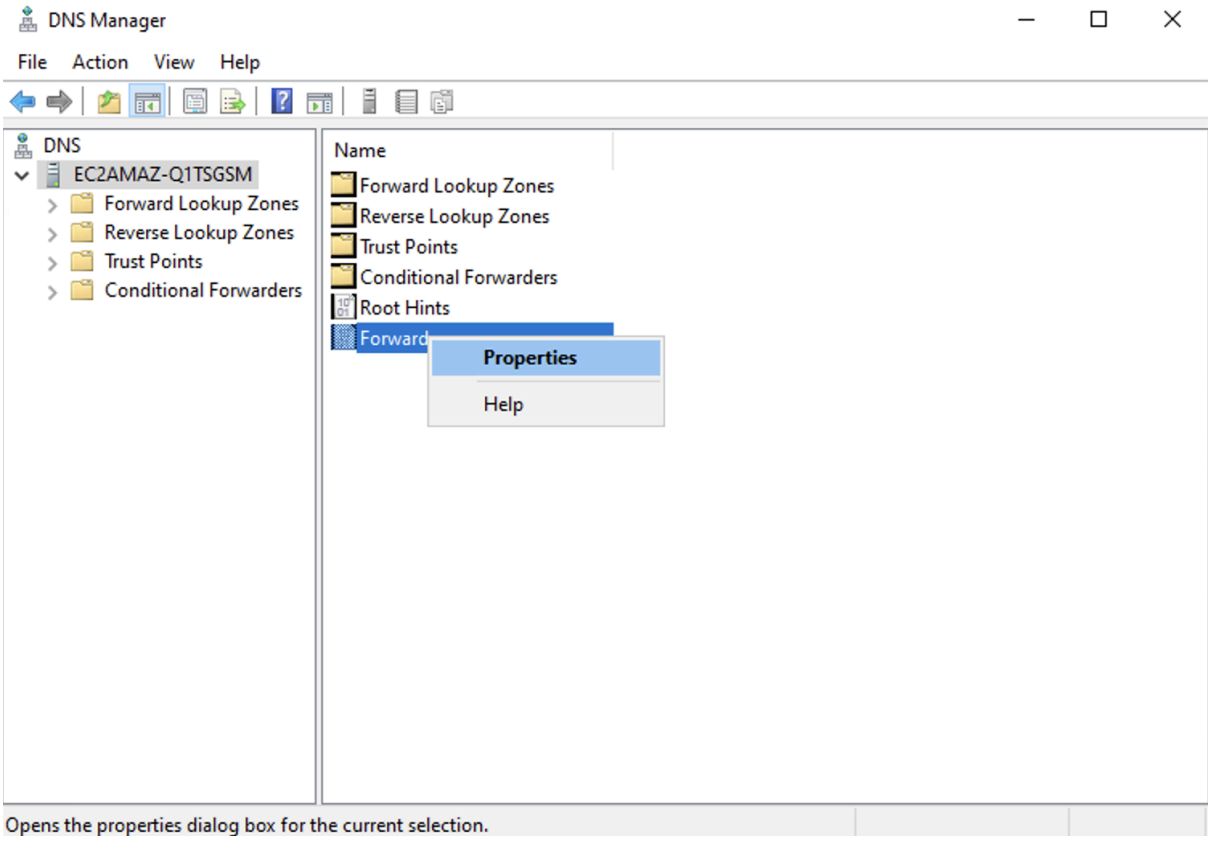
- Now we know the network connectivity is in place, let's set up our DNS server. Enter “dns” in the Windows search bar and select the DNS app:



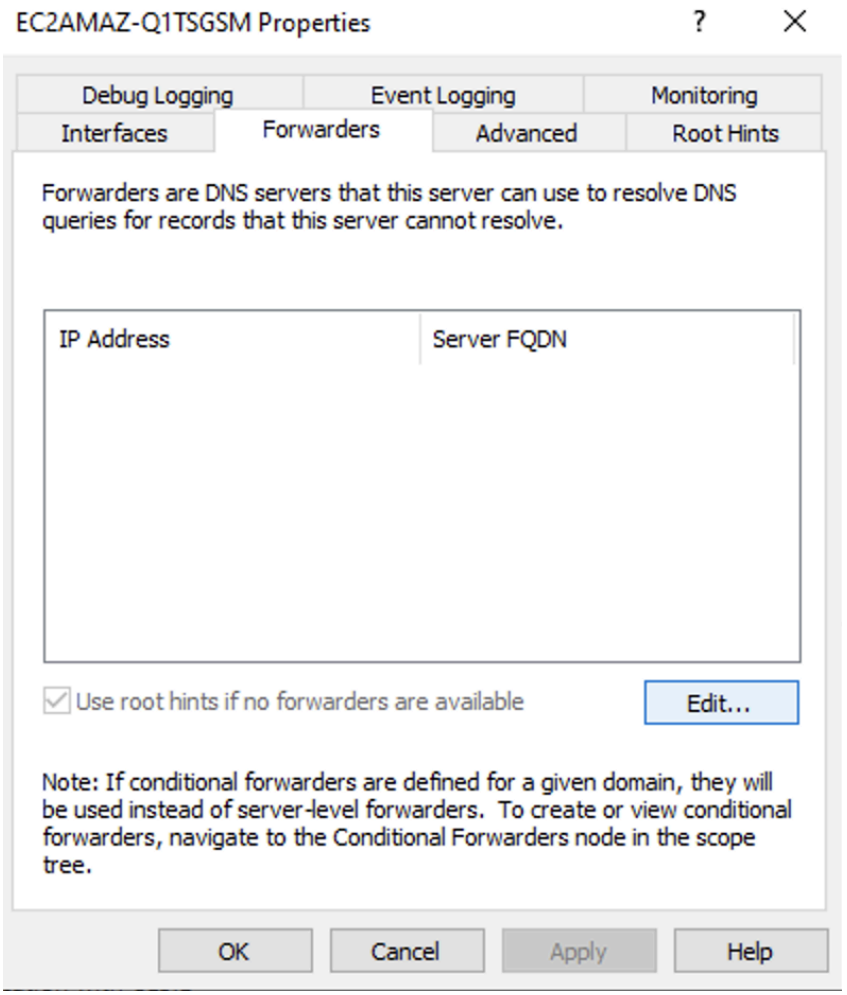
- Select our DNS server and then Properties and make a note of the DNS Server IP address (you could also get this via the `ipconfig` command:

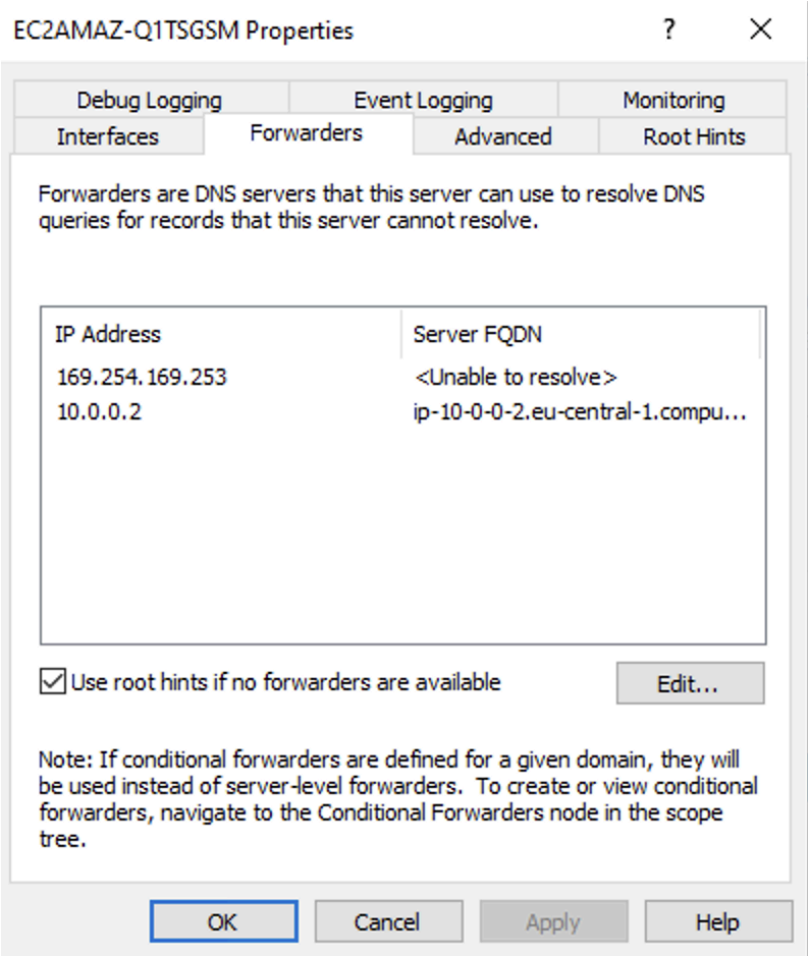


- Expand our DNS server, select Forwarders and select Properties:

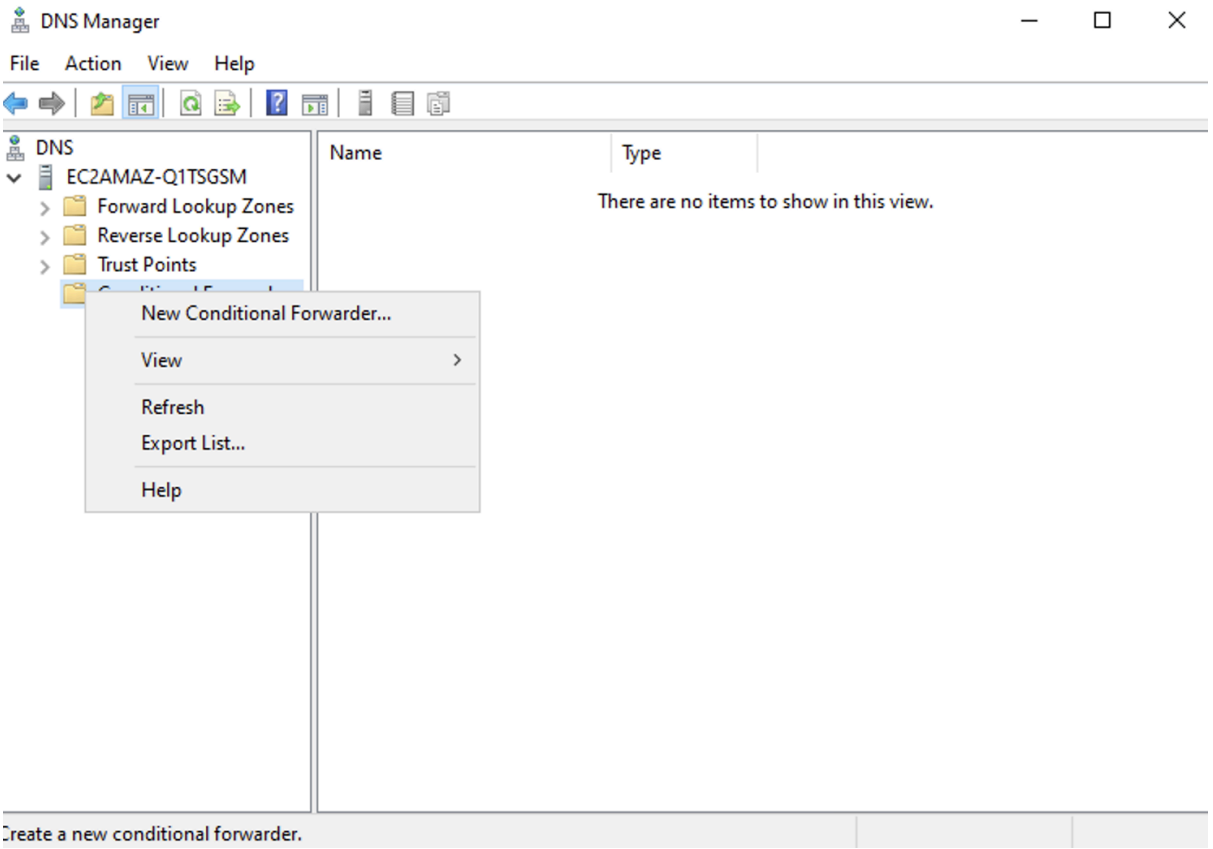


- Add Amazon DNS as a forwarder
    - 10.0.0.2 (may vary depending on your frontend VPC CIDR range) and 169.245.169.253

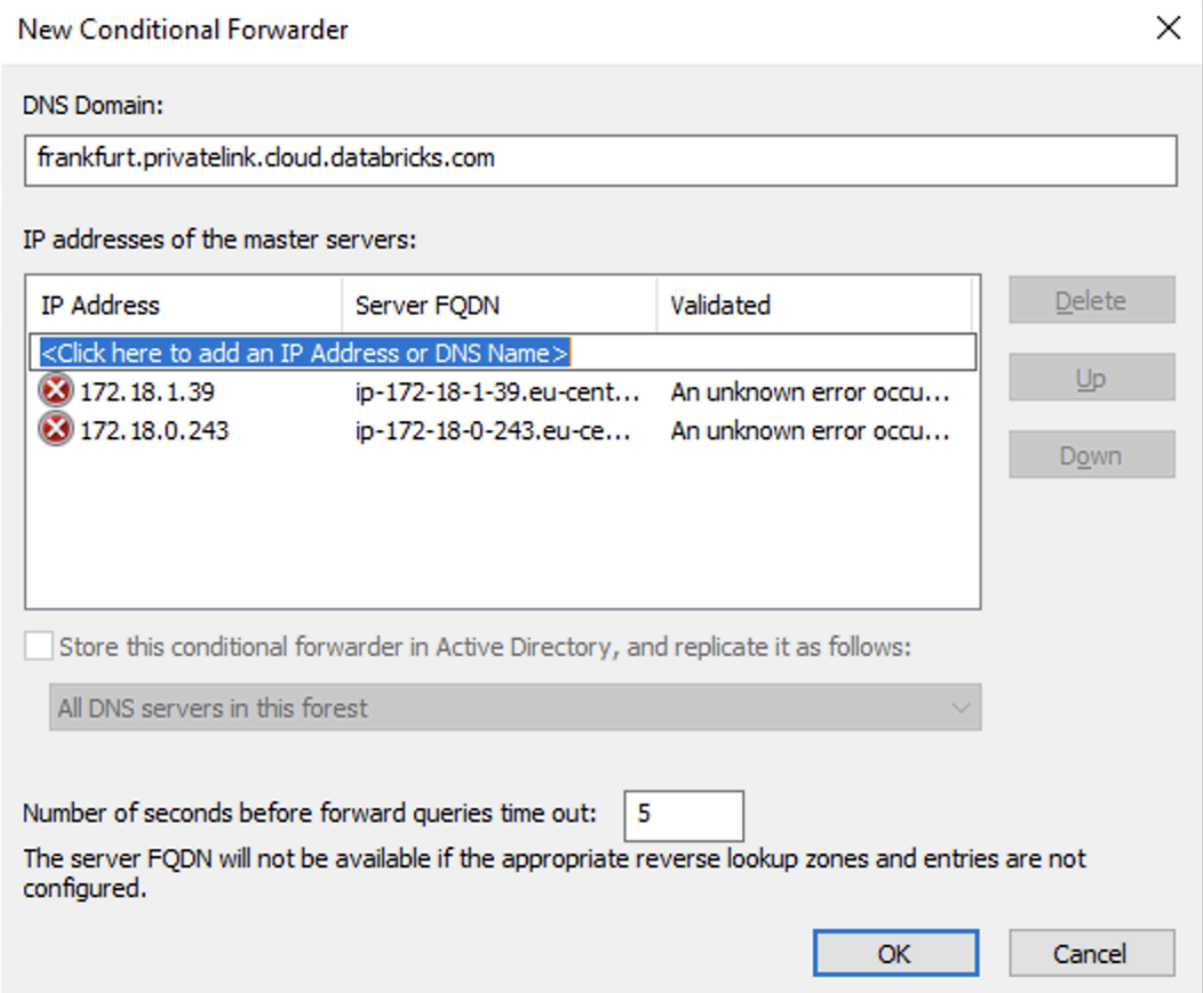

EC2AMAZ-Q1TSGSM Properties
Debug Logging
Event Logging
Monitoring
Interfaces
Forwarders
Advanced
Root Hints
Forwarders are DNS servers that this server can use to resolve DNS queries for records that this server cannot resolve.
IP Address
Server FQDN
Use root hints if no forwarders are available
Edit...
Note: If conditional forwarders are defined for a given domain, they will be used instead of server-level forwarders. To create or view conditional forwarders, navigate to the Conditional Forwarders node in the scope tree.
OK
Cancel
Apply
Help



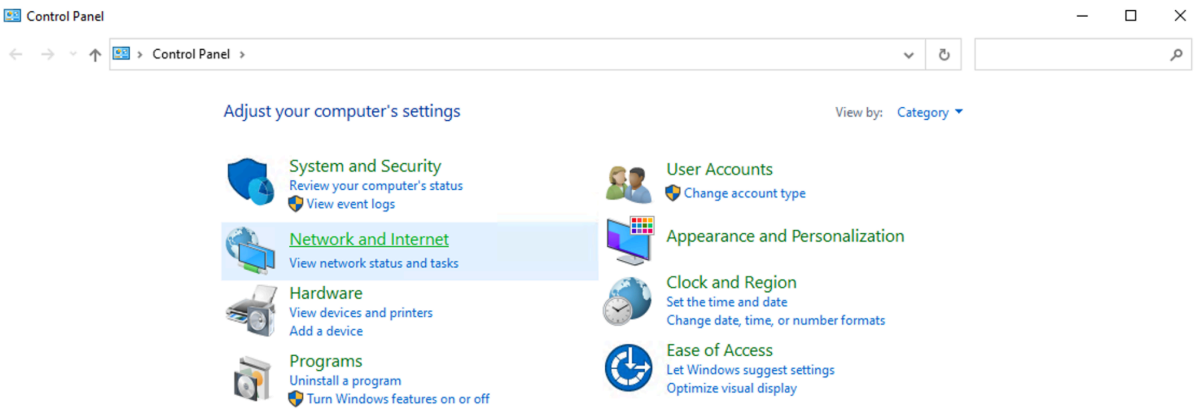
- Now select Conditional Forwarders and New Condition Forwarder:

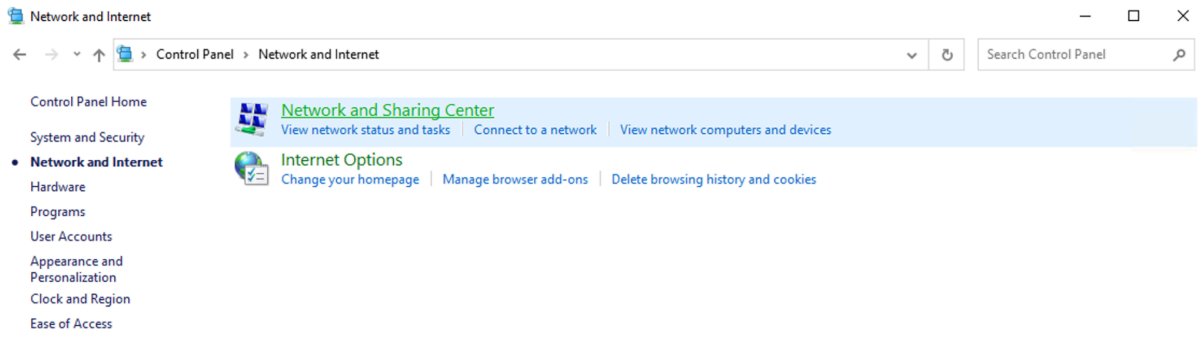


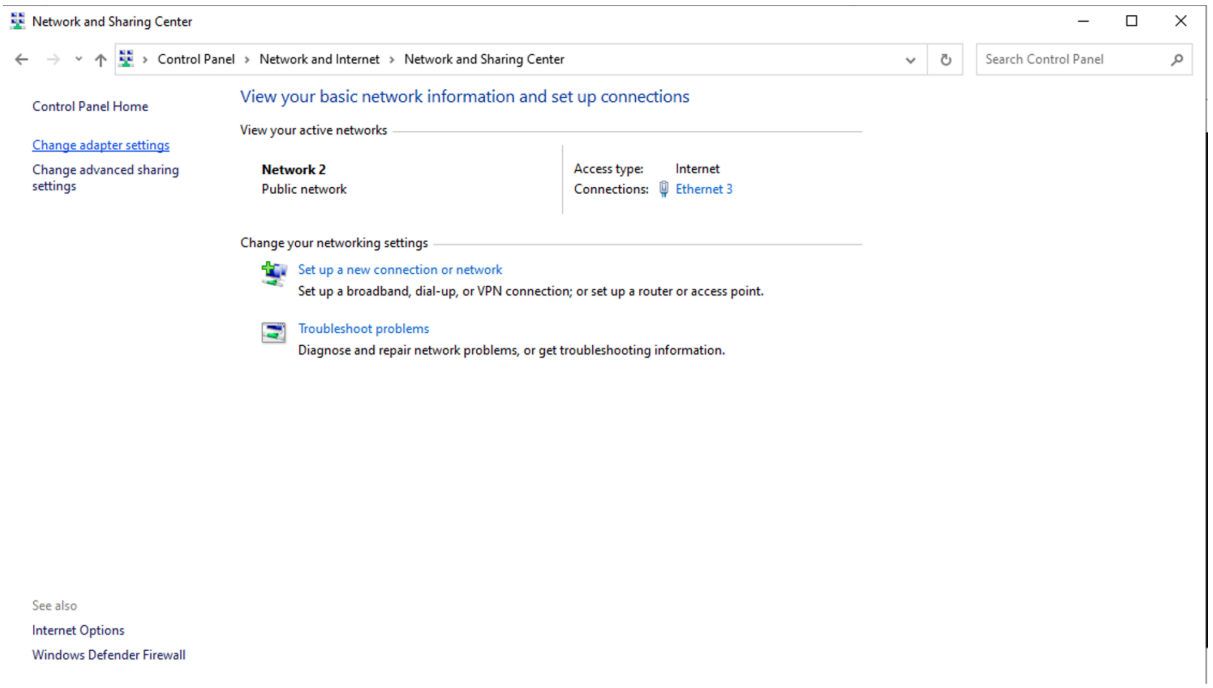
- Add the Private Hosted Zone and your AWS inbound resolver IPs:

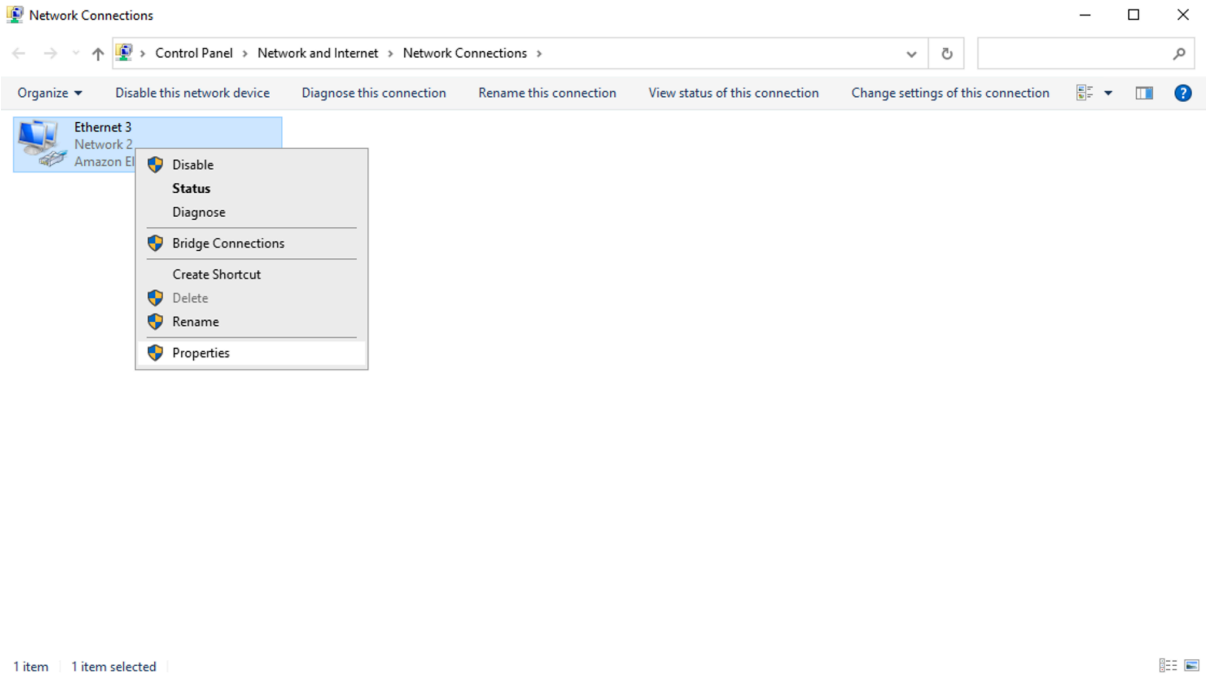


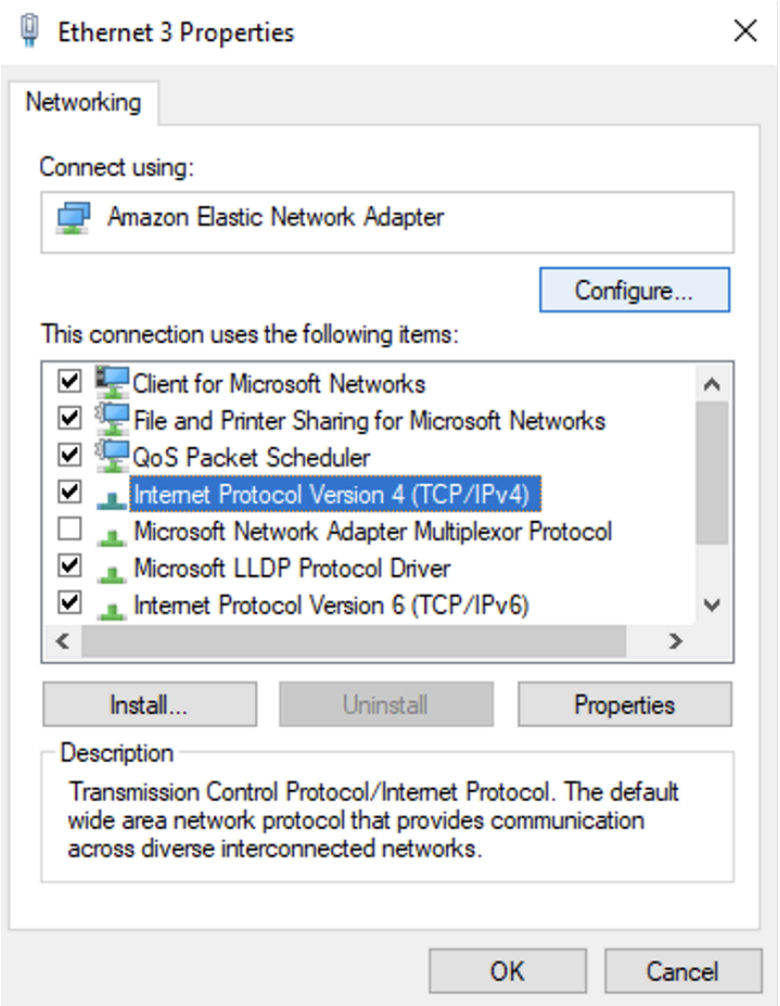
- Now let's configure the EC2 instance to use our DNS server:

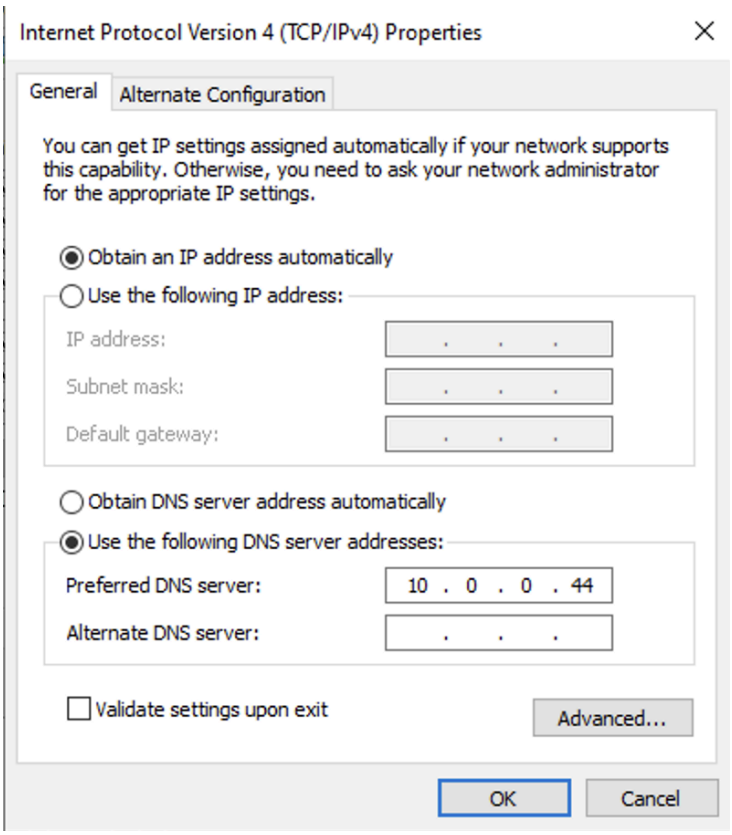



Network and Internet
Control Panel › Network and Internet
Search Control Panel
Control Panel Home
System and Security
Network and Internet
Hardware
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Network and Sharing Center
View network status and tasks
Connect to a network
View network computers and devices
Internet Options
Change your homepage
Manage browser add-ons
Delete browsing history and cookies


Network and Sharing Center
Control Panel › Network and Internet › Network and Sharing Center
Search Control Panel
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
View your active networks
Network 2
Public network
Access type: Internet
Connections: Ethernet 3
Change your networking settings
Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.
See also
Internet Options
Windows Defender Firewall

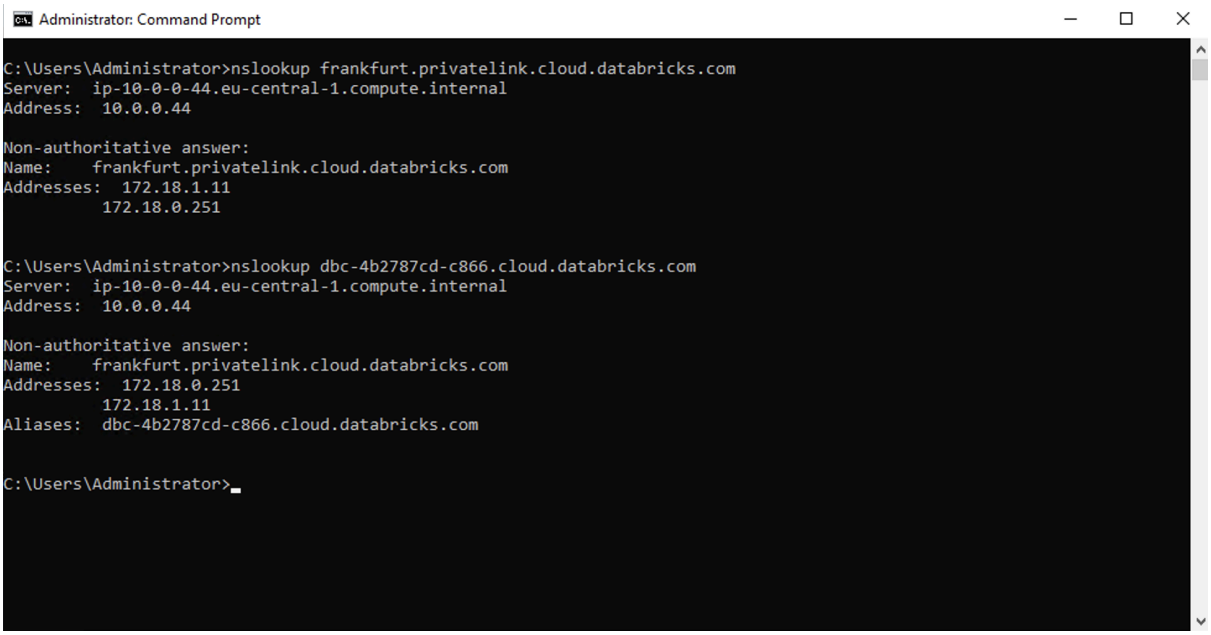

Network Connections
Control Panel › Network and Internet › Network Connections ›
Organize
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Ethernet 3
Network 2
Amazon El
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
1 item
1 item selected


Ethernet 3 Properties
Networking
Connect using:
Amazon Elastic Network Adapter
Configure...
This connection uses the following items:
Client for Microsoft Networks
File and Printer Sharing for Microsoft Networks
QoS Packet Scheduler
Internet Protocol Version 4 (TCP/IPv4)
Microsoft Network Adapter Multiplexor Protocol
Microsoft LLDP Protocol Driver
Internet Protocol Version 6 (TCP/IPv6)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel

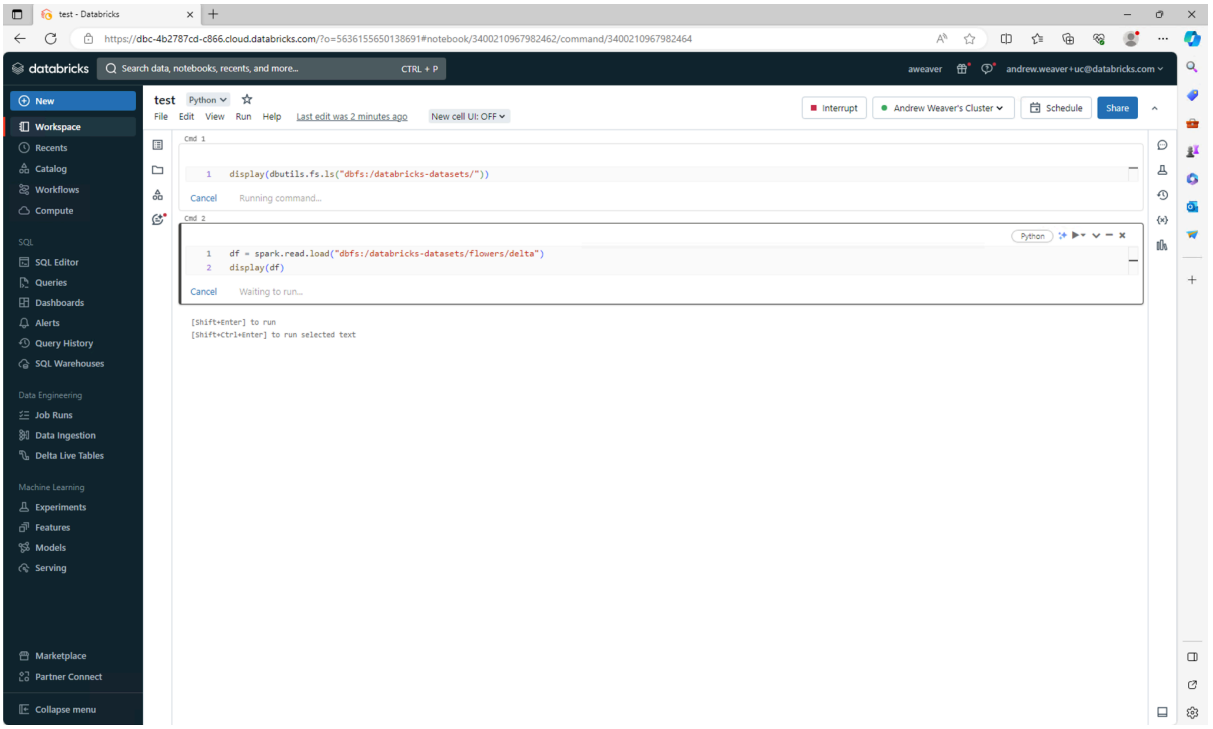


- Open a command prompt and flush DNS:
  - `ipconfig /flushdns`

- Now do an nslookup on the private zone and then the workspace:



- You should be set. Now you can open Edge (I know, I know) and do some testing!



NB - there's no internet access in the data plane VPC, so you might find you need to use config like [Setup an Ephemeral Metastore for the UC-only Workspace on AWS]() to get a stable environment.