# 😊 Virtual Network Peering

Azure Virtual Network Peering is a feature in Microsoft Azure that allows you to connect two or more virtual networks (VNets) within the same Azure region or across different regions. This connectivity is seamless and low-latency, enabling resources in the peered VNets to communicate with each other as if they were on the same network. Here are key aspects and use cases for Azure Virtual Network Peering:

Key Features of Azure Virtual Network Peering

1. **High Throughput and Low Latency:** Peered VNets communicate with each other using Azure's backbone network, providing high throughput and low latency connections
2. **Full Network Transparency:** Resources in the peered VNets can communicate with each other using private IP addresses. There is no need for public internet routing, which improves security and performance.
3. **Global Peering:** Allows peering of VNets across different Azure regions, enabling cross-region connectivity for distributed applications and disaster recovery solutions.
4. **No Bandwidth Limitation:** There is no bandwidth restriction for the data transferred between peered VNets, and data transfer within the same region is free of charge.
5. **Resource Accessibility:** Enables access to resources like virtual machines, load balancers, and databases across peered VNets.
6. **Isolation and Control:** Peered VNets maintain their own network policies and security rules, ensuring that network traffic is controlled and isolated as needed.

Overall, Azure Virtual Network Peering simplifies network connectivity and enhances the security and performance of communication between resources deployed in different Azure VNets. It provides a foundation for building complex network topologies, supporting various deployment scenarios ranging from multi-tier applications to global-scale architectures.

## 😄 Use Cases for Azure Virtual Network Peering

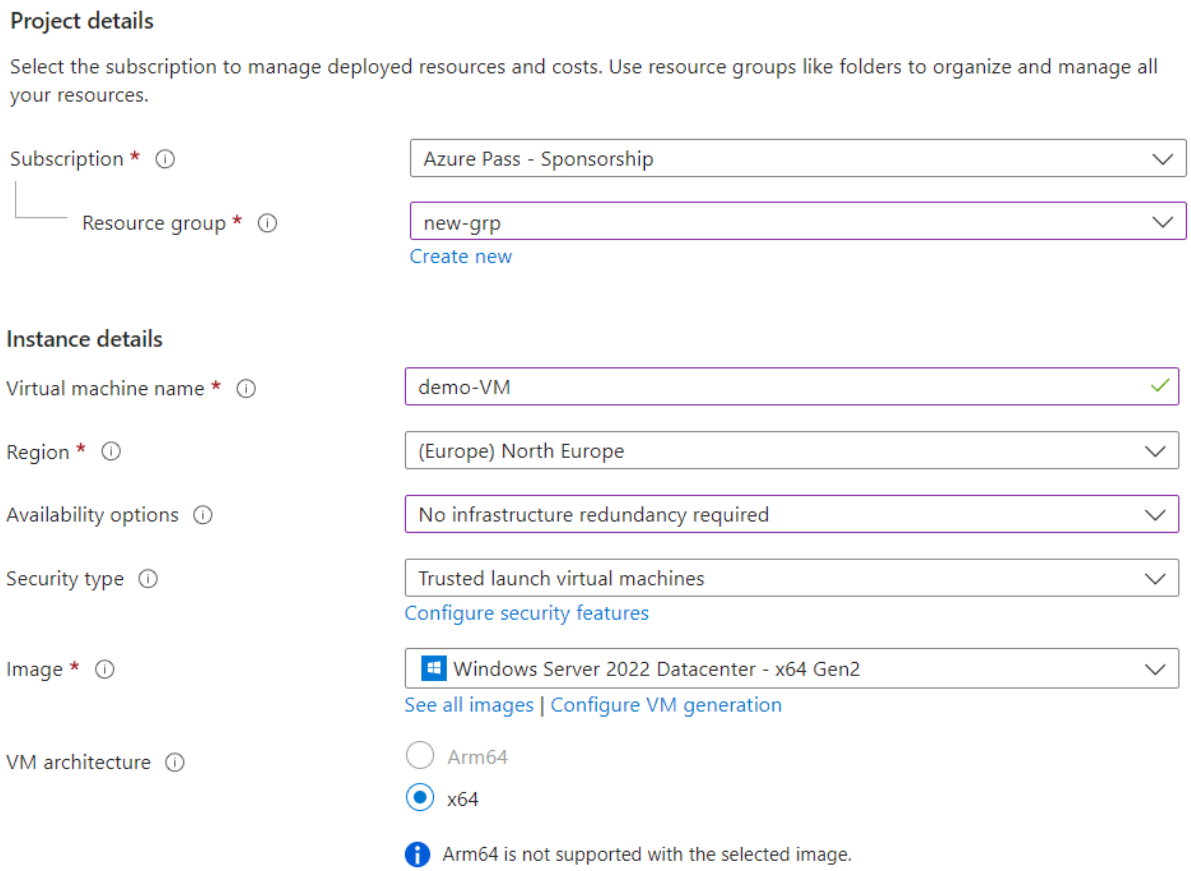
1. **Multi-Region Deployments:** For applications that require high availability and disaster recovery, VNets in different regions can be peered to provide seamless connectivity and data replication.
2. **Resource Sharing:** When different departments or teams need to share resources such as databases, storage, or services across separate VNets, peering provides an efficient way to enable communication without exposing resources to the public internet.
3. **Network Segmentation:** Organizations can segment their network into multiple VNets for security, compliance, or operational reasons, while still allowing necessary communication between segments through peering.

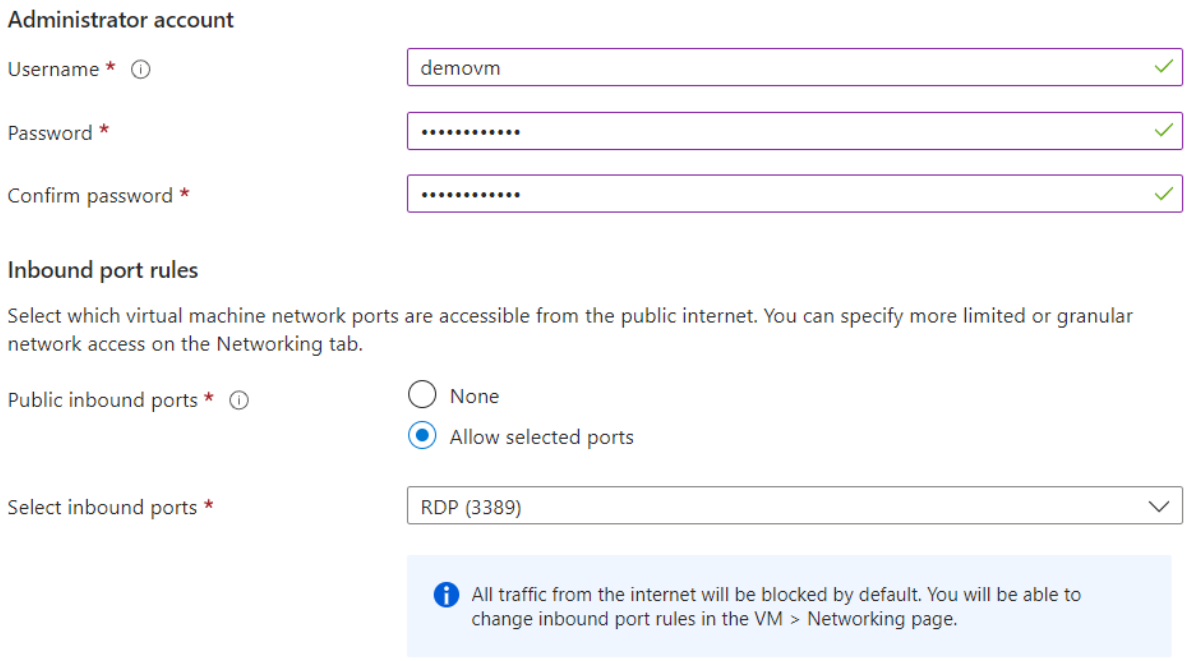
4. **Hybrid Cloud Architectures:** In hybrid cloud scenarios where you have resources on-premises and in Azure, peering can connect different VNets to support a consistent network architecture and facilitate data transfer between cloud resources.
5. **Centralized Services:** Centralizing services like DNS, Active Directory, or firewalls in a single VNet and peering other VNets to it allows centralized management and reduces redundancy.
6. **Development and Testing Environments:** Isolate development, testing, and production environments in different VNets while still enabling necessary communication for integrated workflows.

**The end goal is to demonstrate the ability to connect two virtual networks using Azure Virtual Network Peering, enabling seamless and secure communication between resources in different VNets. This showcases how VNet peering can be used to build scalable, secure, and interconnected network architectures within Azure.**

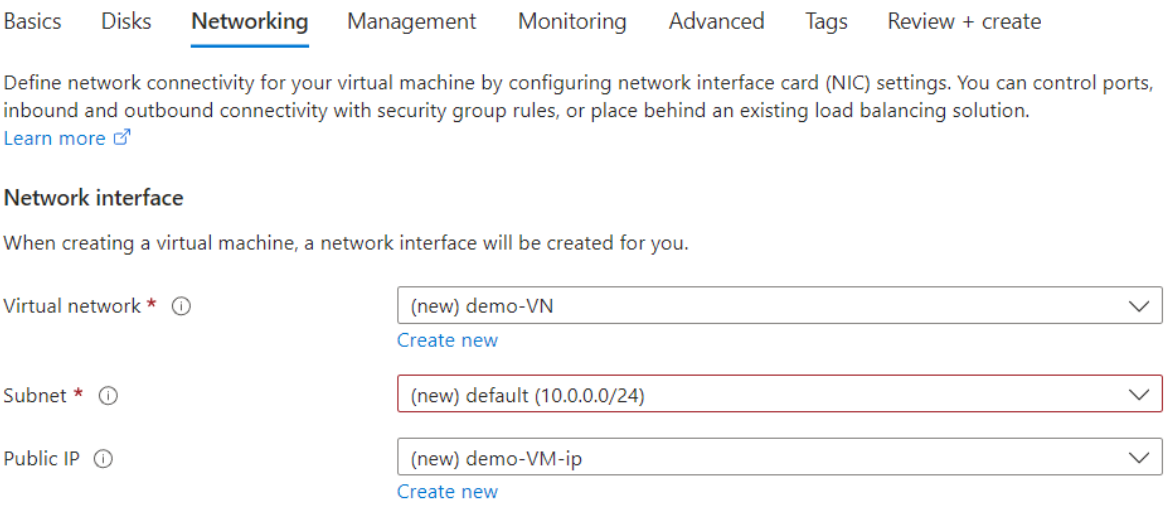
## 😄 To begin with the Lab:

1. First, we are going to create two Virtual Machines based on Windows Server 2022.
2. Now go to Virtual Machines and create a VM. Use the snapshots to fill out the details for your VM.

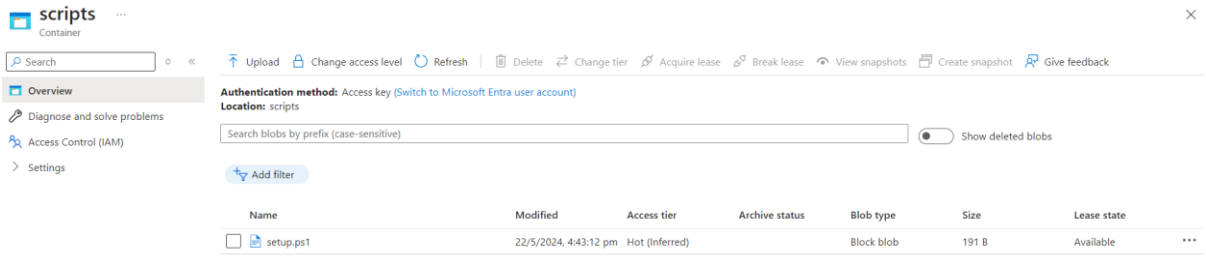




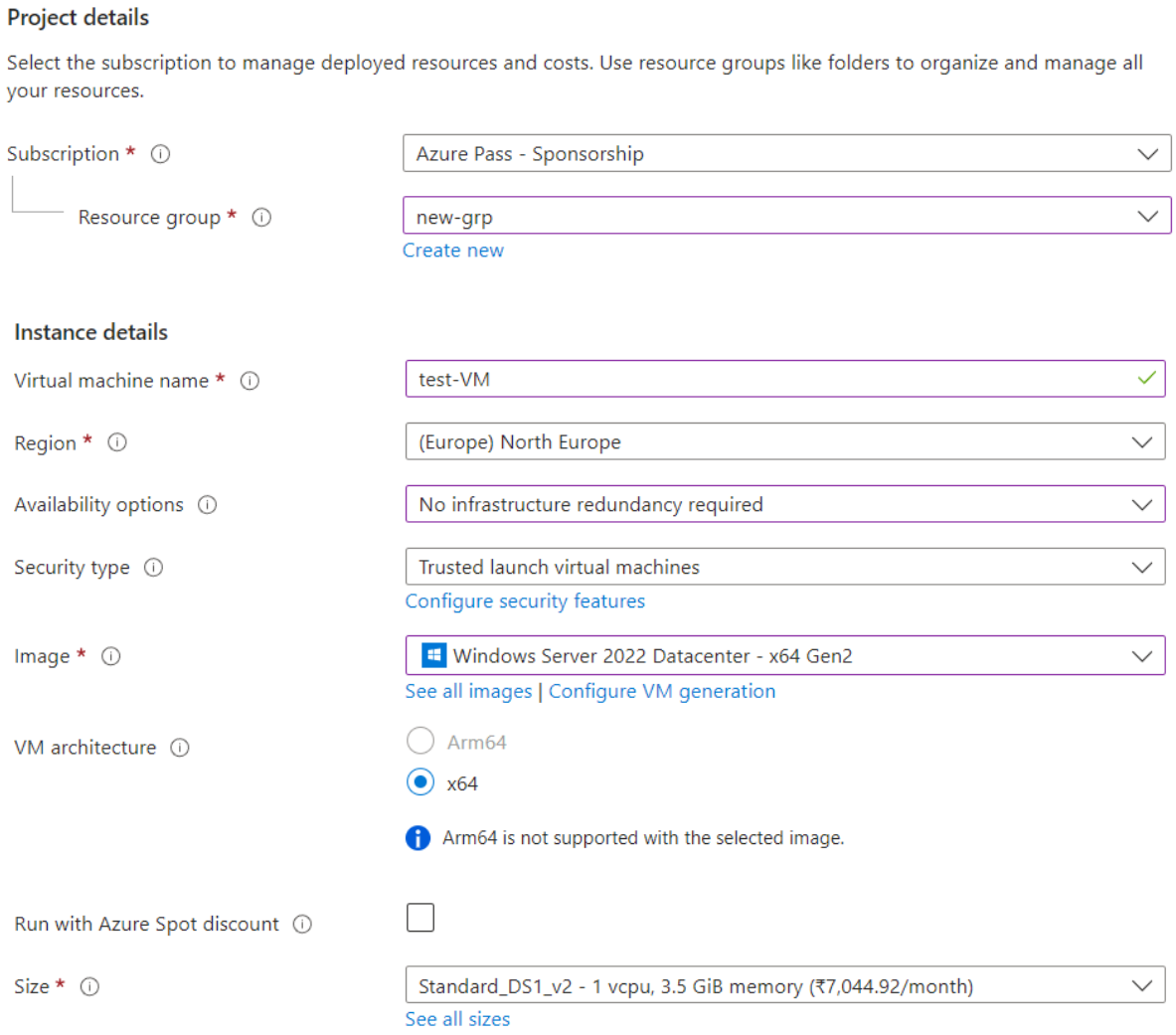

3. Then for the networking section in the network interface you have to create a new virtual network in the default subnet, move forward to the review page and create your Virtual Machine.



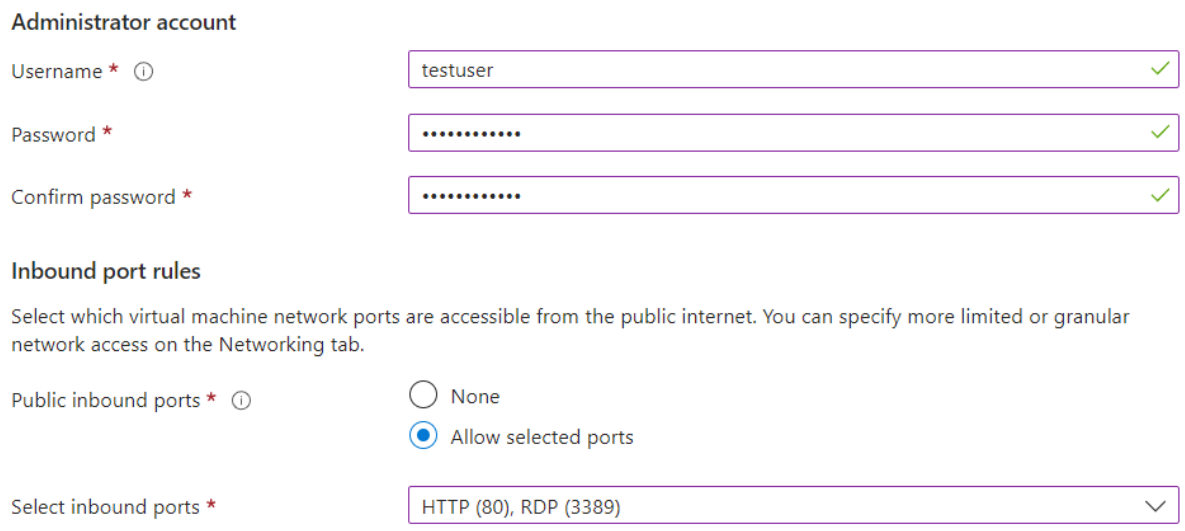

4. Once your deployment is complete then Login to your VM.
5. After that come back to Portal and create another VM.
6. Just before creating your VM first ensure that you have a storage account in place in which you should have a container in which the setup.ps1 file should be present. We will use this file to install Web Server onto our VM without logging into it.



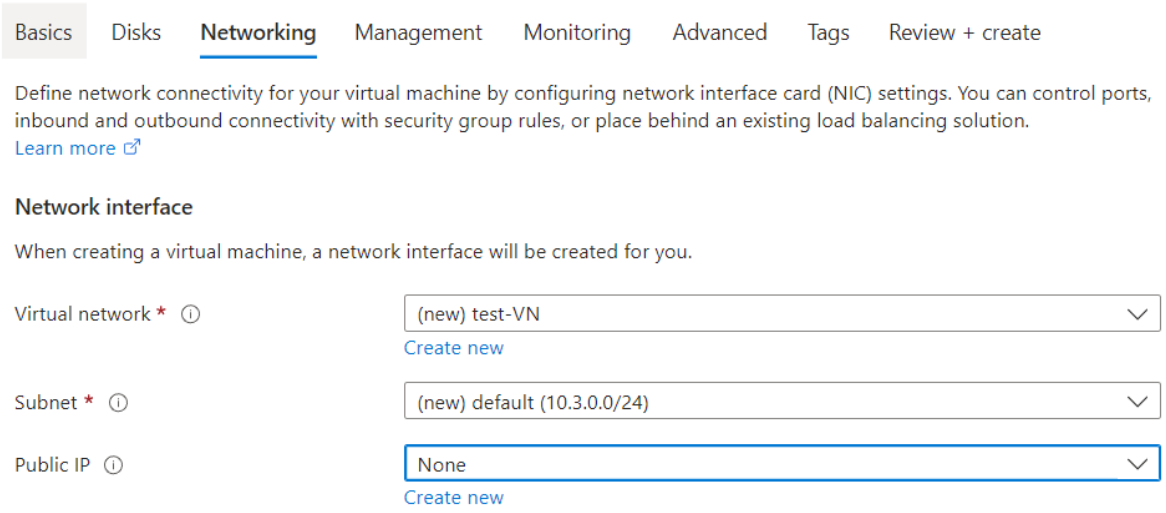

7. Now go to Virtual Machines and create your VM.



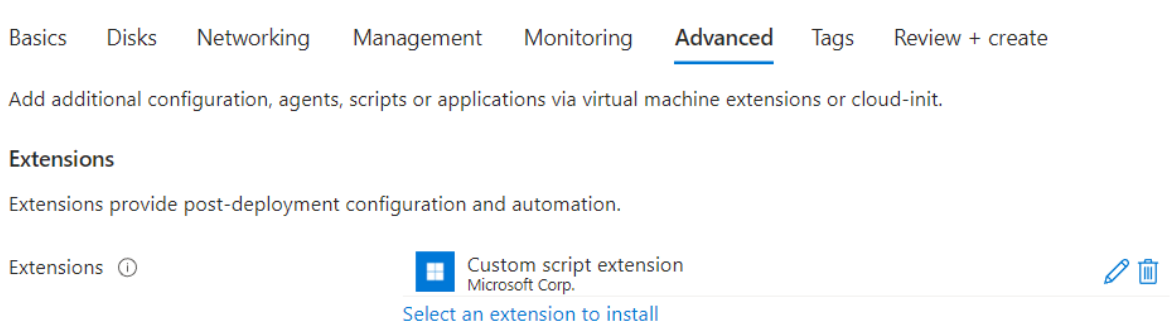

8. But this time you have to allow HTTP in your inbound port rules because we are going to install internet information services.



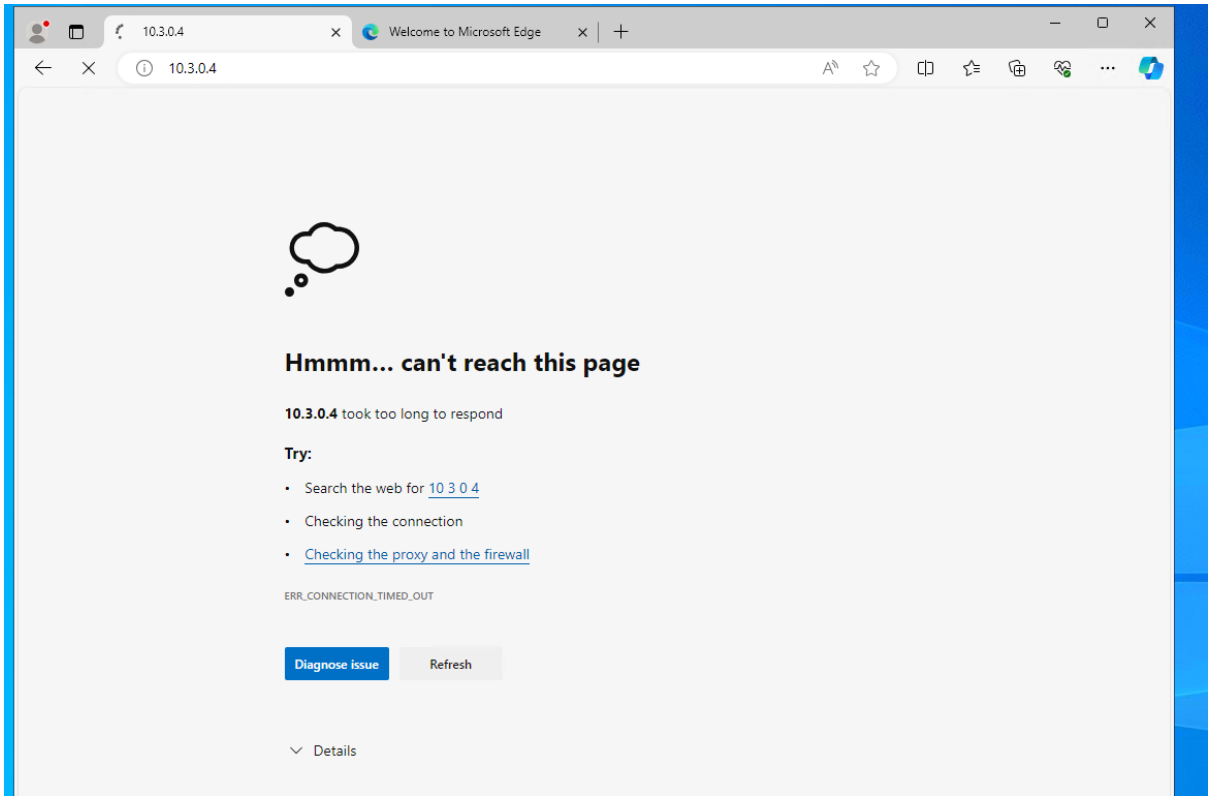

9. Then for the Networking section in Network Interface you have to create a new Virtual Network for this VM. Then we don't need Public IP because we want to connect via



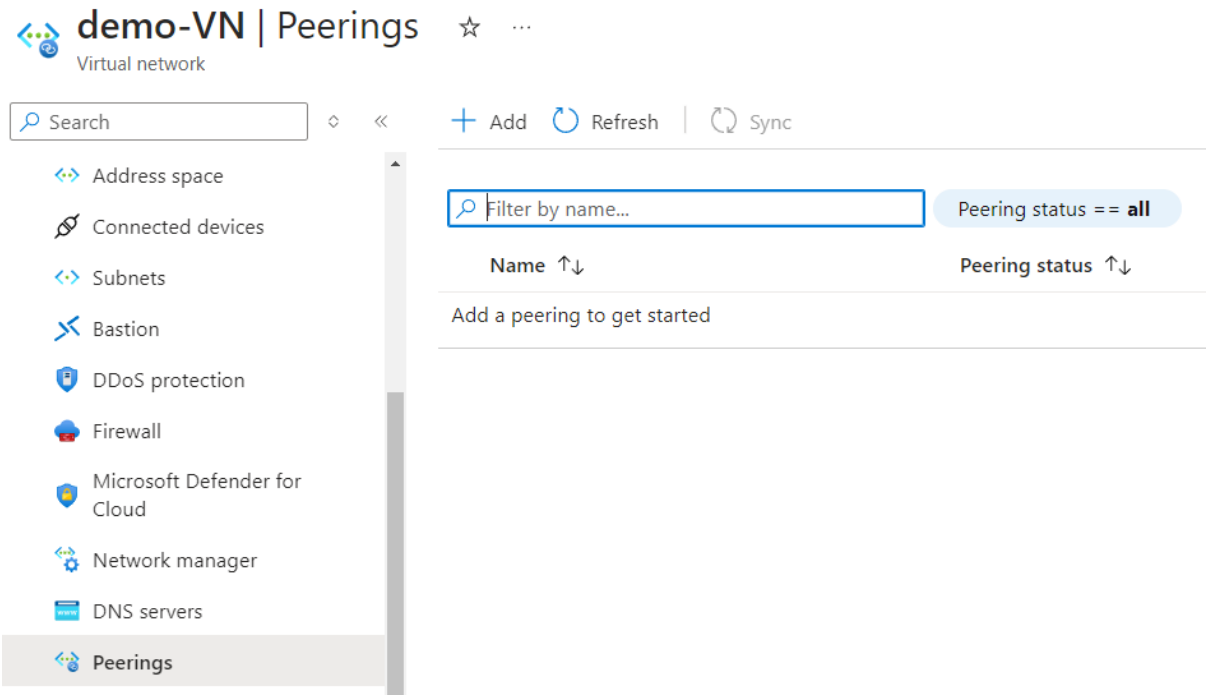

10. After that go to advanced and in the extension select your Custom script extension.
11. Then just move to the review page and create your VM.



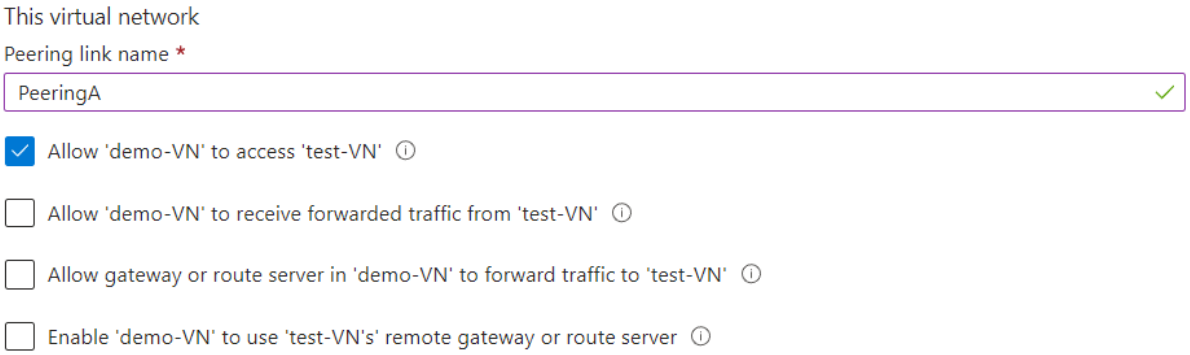
12. Once your deployment is complete then go to your test VM and copy the private IP address then navigate to the demo VM where you have logged in.
13. Then open Microsoft Edge and paste the IP address there and try to access it. You will see that the site can't be reached because there is no connection between them.




14. Now we are going to create a Virtual Network Peering connection between the machines.
15. So, for that go to Demo VM and then go to Network Setting and open Virtual Network. Then go to Peering and click on Add.




16. When it comes to peering, there are going to be two peering connections in place. One from the demo network onto the test network and another one from the test network onto the demo network.
17. Then you need to give the peering link a name and scroll down.




18. After that you have to create a peering link for the remote virtual network. Give it a name first. Then choose your virtual network as the test VN.

Remote virtual network

Peering link name *

PeeringB

Virtual network deployment model

Resource manager

Classic

I know my resource ID

Subscription *

Azure Pass - Sponsorship

Virtual network *

test-VN

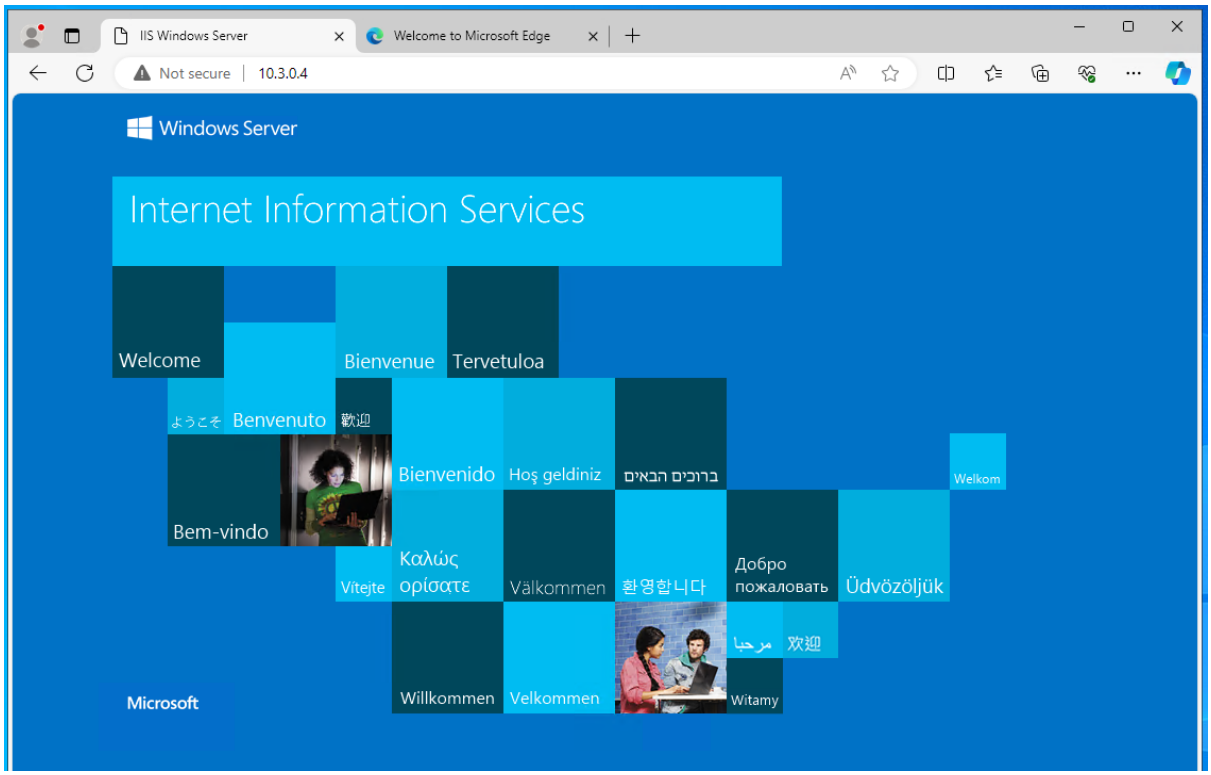
Allow 'test-VN' to access 'demo-VN'

Allow 'test-VN' to receive forwarded traffic from 'demo-VN'

Allow gateway or route server in 'test-VN' to forward traffic to 'demo-VN'

Enable 'test-VN' to use 'demo-VN's' remote gateway or route server

19. Then come back to the VM and refresh the page you will see your web server running as expected which means that our connection was successful.




20. Now do not delete your resources.