😊 Adding a Secondary Network Interface

An Azure network interface (NIC) is a virtual network adapter that enables communication for Azure virtual machines (VMs), cloud services, and other Azure resources. It acts as a bridge between the VM and the Azure Virtual Network (VNet), providing connectivity and configuration options for network traffic.

Here's a summary of key points about Azure network interfaces:

1. **Connectivity:** NICs facilitate network connectivity for Azure resources, allowing them to communicate with other resources within the same VNet, across VNets, or with on-premises networks.
2. **Configuration:** NICs can be configured with various settings such as IP addresses, subnet associations, network security groups (NSGs), load balancer endpoints, and more.
3. **Traffic Management:** NICs enable traffic management by allowing you to control inbound and outbound traffic using NSGs and other Azure networking features.
4. **Scalability:** NICs can be attached or detached from VMs as needed, providing scalability and flexibility in managing network resources.
5. **Security:** NICs play a crucial role in network security by enforcing access controls, filtering traffic, and providing secure communication channels between Azure resources.
6. **Monitoring and Diagnostics:** Azure provides monitoring and diagnostic capabilities for NICs, allowing you to track network performance, troubleshoot connectivity issues, and monitor network traffic.

😄 Use cases of Network Interface:

Azure network interfaces (NICs) serve various use cases across Azure deployments. Here are some common scenarios where NICs play a crucial role:

1. **Virtual Machine Connectivity:** NICs are essential for enabling network connectivity for Azure virtual machines (VMs). Each VM requires at least one NIC to communicate with other resources within the Azure Virtual Network (VNet), internet, or on-premises networks.
2. **Load Balancing:** NICs can be associated with Azure Load Balancer to distribute incoming network traffic across multiple VM instances. This setup ensures high availability, scalability, and fault tolerance for applications and services running on Azure VMs.
3. **Network Security:** NICs are used in conjunction with Network Security Groups (NSGs) to enforce network security policies. By associating NSGs with NICs, you can control inbound

and outbound traffic to and from Azure resources, helping to protect against unauthorized access and potential threats.

4. **Hybrid Connectivity:** NICs play a crucial role in hybrid cloud connectivity scenarios, where Azure resources need to communicate with on-premises networks. By configuring VPN gateways or Azure ExpressRoute, NICs facilitate secure communication between Azure VNets and on-premises networks, enabling seamless integration between cloud and on-premises environments.
5. **Internet-Facing Applications:** NICs can be configured with public IP addresses to make Azure resources accessible from the internet. This is useful for hosting web servers, APIs, or other internet-facing applications that need to accept incoming connections from clients over the public internet.
6. **Private Endpoints:** Azure Private Endpoints enable secure access to Azure PaaS services over a private endpoint within the VNet. NICs are used to connect resources to Private Endpoints, ensuring that traffic between the resource and the PaaS service remains within the Azure network, enhancing security and compliance.
7. **Network Monitoring and Diagnostics:** NICs provide visibility into network performance and health through monitoring and diagnostics features. By monitoring metrics such as bandwidth, latency, and packet loss, administrators can troubleshoot connectivity issues, optimize network performance, and ensure reliability for Azure resources.

Adding a secondary network interface (NIC) to an Azure virtual machine (VM) involves attaching an additional virtual network adapter to the VM. This secondary NIC enables the VM to have multiple network connections, each with its own IP address and network configuration.

The primary NIC is created automatically when you deploy a VM, and it handles the VM's primary network connectivity. Adding a secondary NIC allows you to extend the VM's networking capabilities by providing additional network interfaces for specific purposes, such as load balancing, network segmentation, or implementing specialized network configurations.

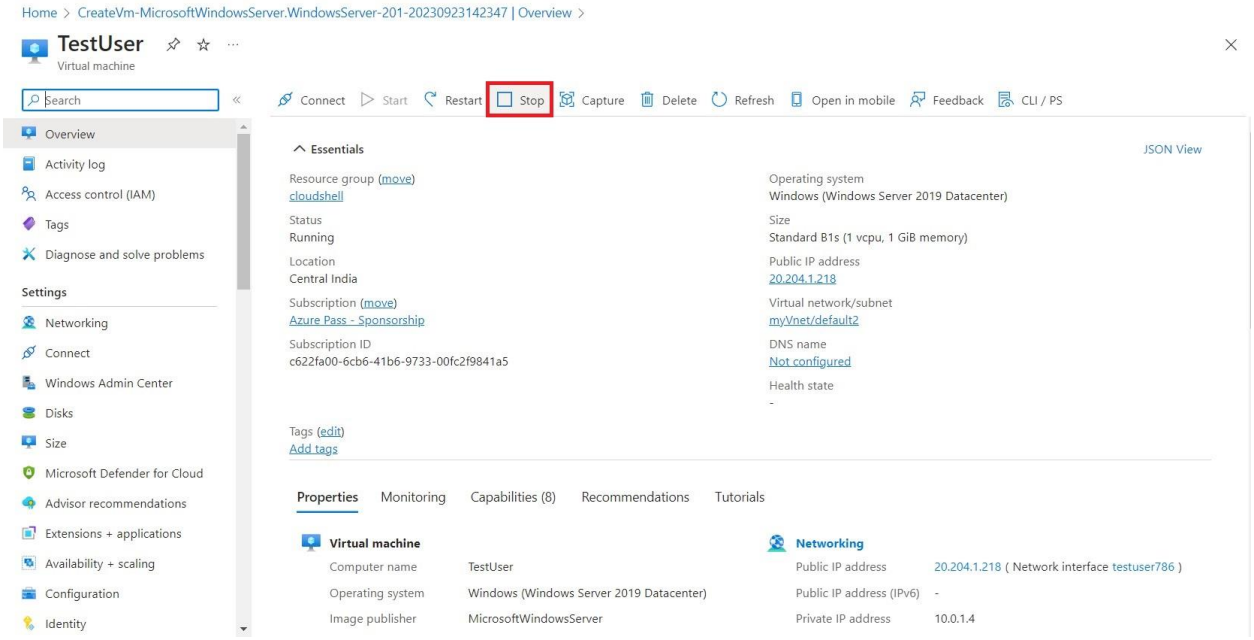
The process typically involves configuring the secondary NIC with its own settings, such as IP address, subnet association, network security group (NSG), and other networking features as needed. Once attached, the secondary NIC enables the VM to communicate over multiple network paths, offering enhanced flexibility and optimization for various networking scenarios within the Azure environment.

In this lab, we're adding a secondary network interface (NIC) to an Azure virtual machine (VM) to expand its networking capabilities. The end goal is to enhance the VM's connectivity, load balancing, security, and other networking functionalities within an Azure deployment. This allows for greater flexibility and optimization of network resources to meet specific application requirements or use cases.

😄 To begin with the Lab:

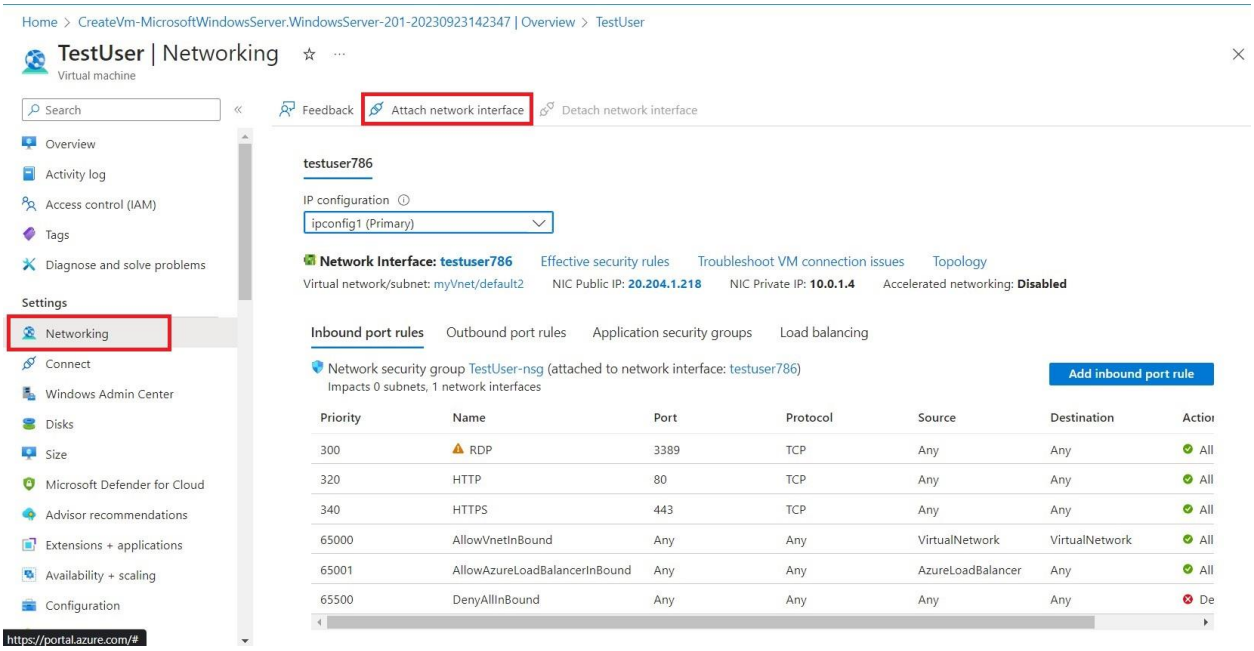
Now to perform this lab there are some pre-requisites. First, you should have a virtual network in place then you should have a virtual machine deployed in that VNet.

Step 1: Now navigate to your virtual machine and stop it.



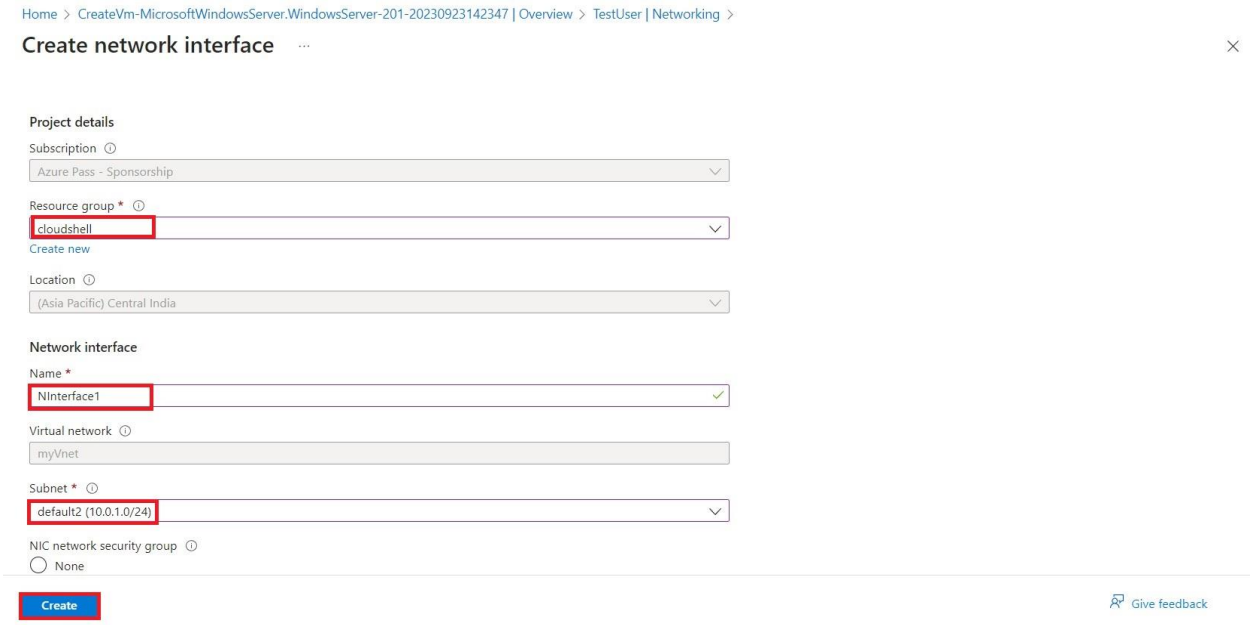
Step 2: Click on Networking from the left-hand side blade.

- Click on the attached network interface.
- Until you don’t stop the VM, the option will be not enabled. So, you have to stop your VM first.

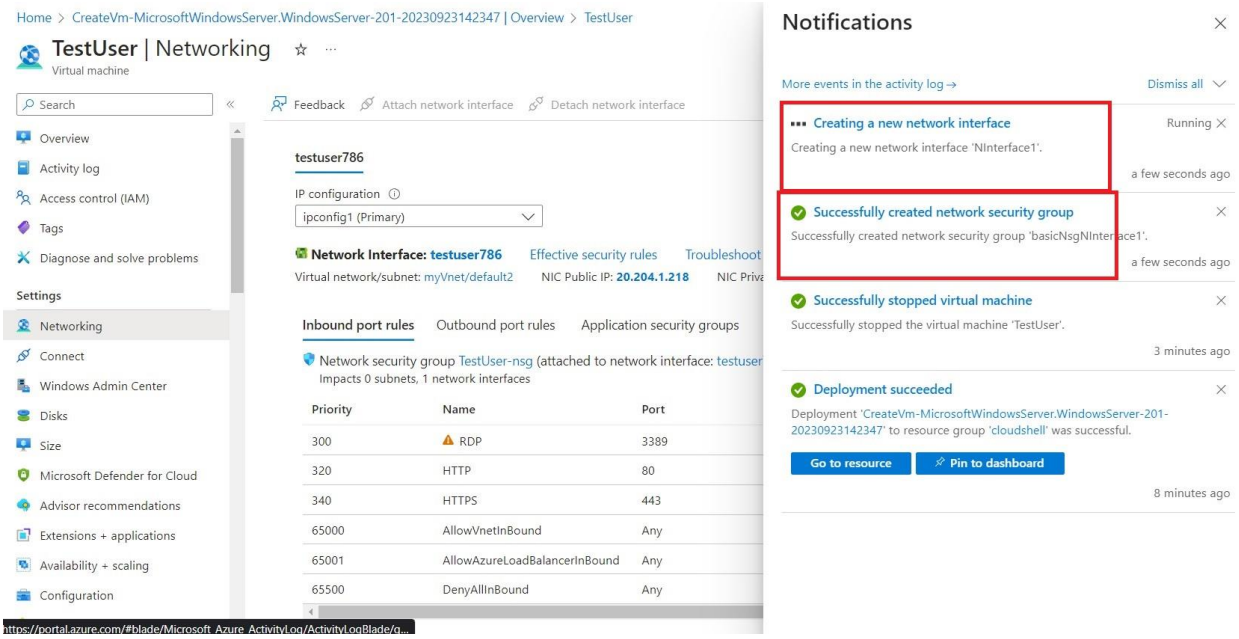


Step 3: Click on Create and attach network interface, and then select the resource group.

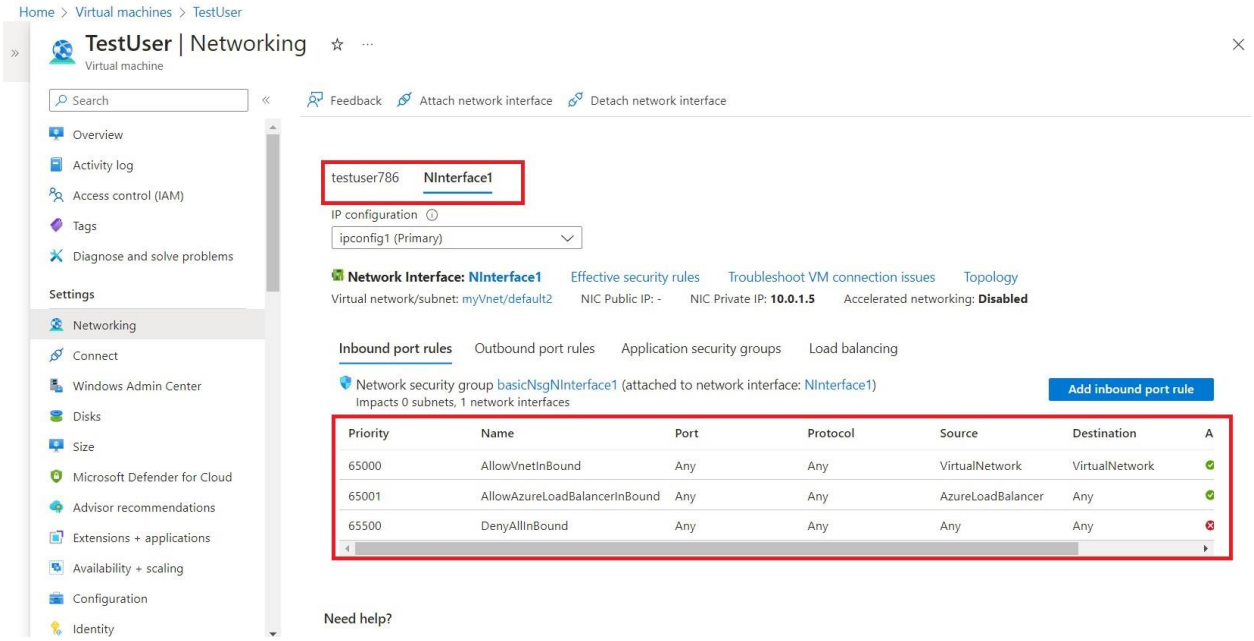
- Enter the name and select the subnet.
- Click on Create.



- A new security group will be created for a new network interface.
- Wait for the creation of the network interface.



- You'll observe the new attached network interface in place.



Now to make use of this secondary network interface, you need to have the software. Whatever software you install on the virtual machine should have the ability, or at least at the operating system level, should have the ability to route traffic on to that secondary network interface.