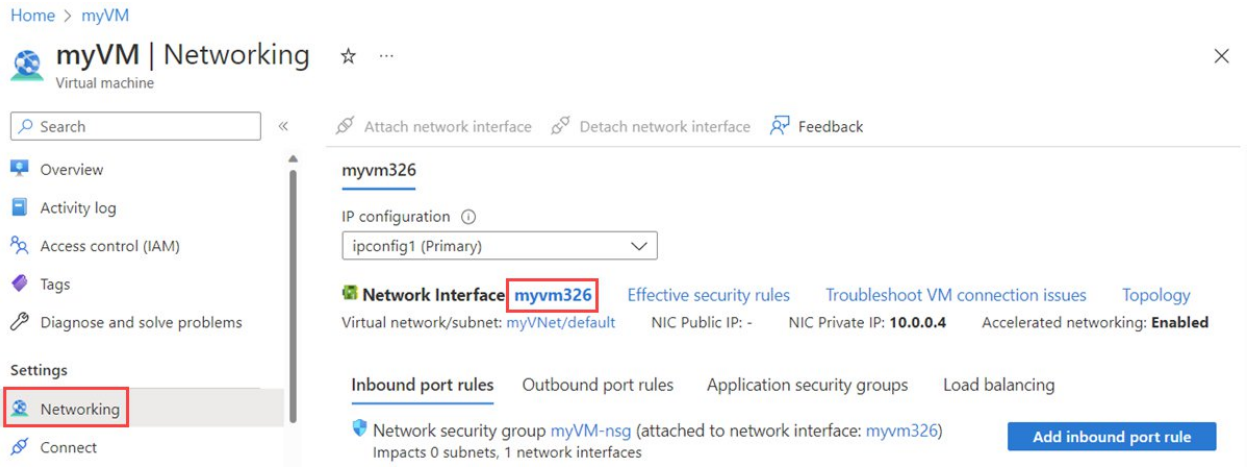
Associate a public IP address to a virtual machine

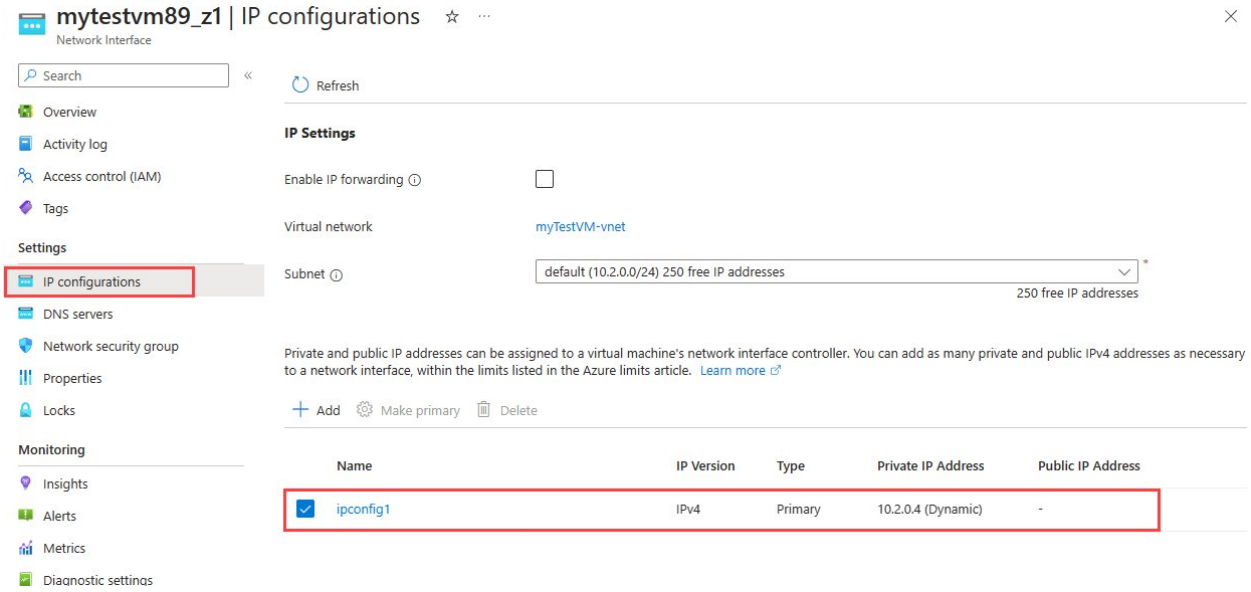
Prerequisites

- An Azure account with an active subscription. You can create an account for free

1. Sign in to the Azure portal.
2. In the portal, search for and select the VM that you want to add the public IP address to.
3. Under **Settings** in the left pane, select **Networking**, and then select the network interface you want to add the public IP address to.



4. From the **Network interface** window, under **Settings**, select **IP configurations***, and then select an IP configuration from the list.



5. In the **Edit IP configuration** window, select **Associate public IP address**, then select **Public IP address** to choose an existing public IP address from the drop-down list. If no public IP addresses are listed, you need to create one. To learn how, see Create a public IP address.

Edit IP configuration

mytestvm89_z1

A primary IP configuration already exists. Any additional IP configurations will be secondary.The virtual network this network interface is attached to only supports IPv4. Learn more

Name: ipconfig1 *

IP version: IPv4, IPv6

Type: Primary, Secondary

Private IP address settings

Allocation: Dynamic, Static

Public IP address settings

Associate public IP address

Public IP address: (New) default-publicIpAddress

Create a public IP address

Add a public IP address

Name *: myPublicIP

SKU: Basic, Standard

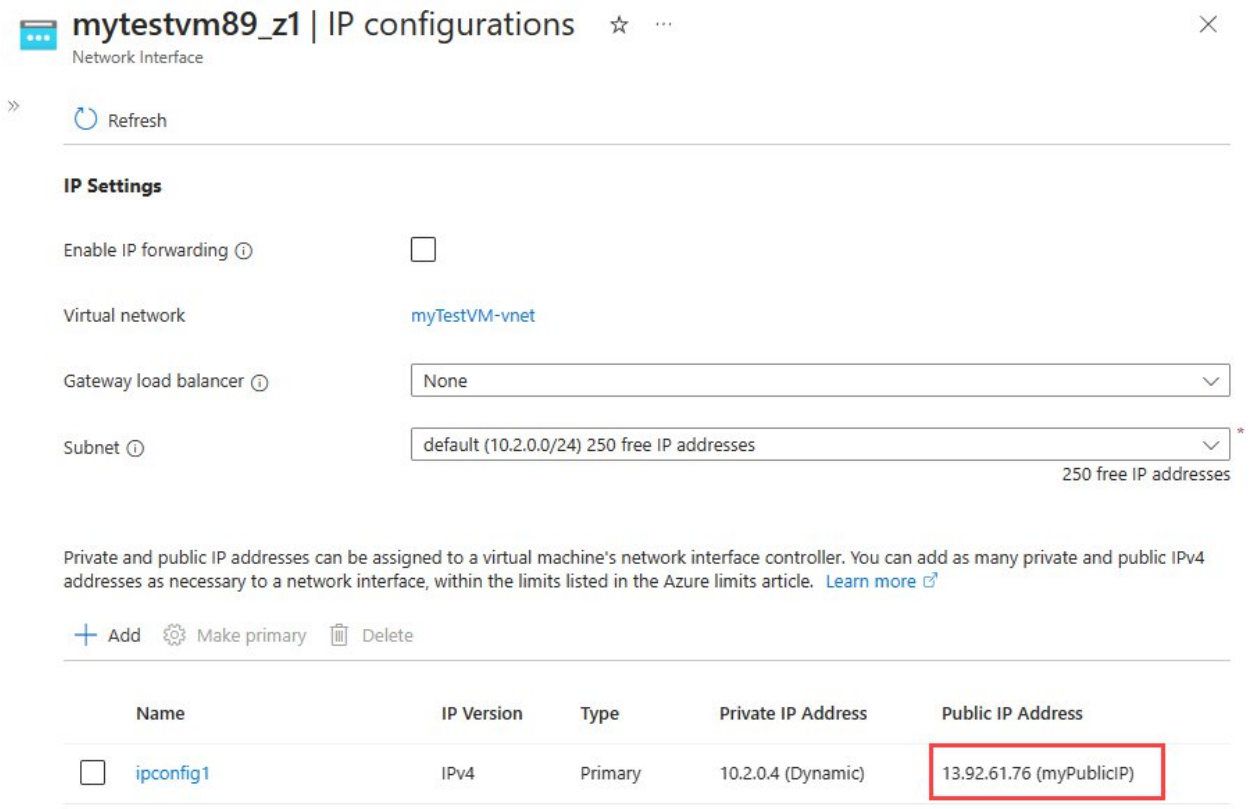
Assignment: Dynamic, Static

OK Cancel

Save Cancel

6.. Select **Save**.

7. In the **IP Configurations** window, view the public IP address assigned to the IP configuration. It might take a few seconds for a newly associated IP address to appear.



8. Open the necessary ports in your security groups by adjusting the security rules in the network security groups. For information, see Allow network traffic to the VM.

Allow network traffic to the VM

Before you can connect to a public IP address from the internet, you must open the necessary ports in your security groups. These ports must be open in any network security group that you might have associated to the network interface, the subnet of the network interface, or both. Although security groups filter traffic to the private IP address of the network interface, after inbound internet traffic arrives at the public IP address, Azure translates the public address to the private IP address. Therefore, if a network security group prevents the traffic flow, the communication with the public IP address fails.

You can view the effective security rules for a network interface and its subnet for the Azure portal, the Azure CLI, or Azure PowerShell.