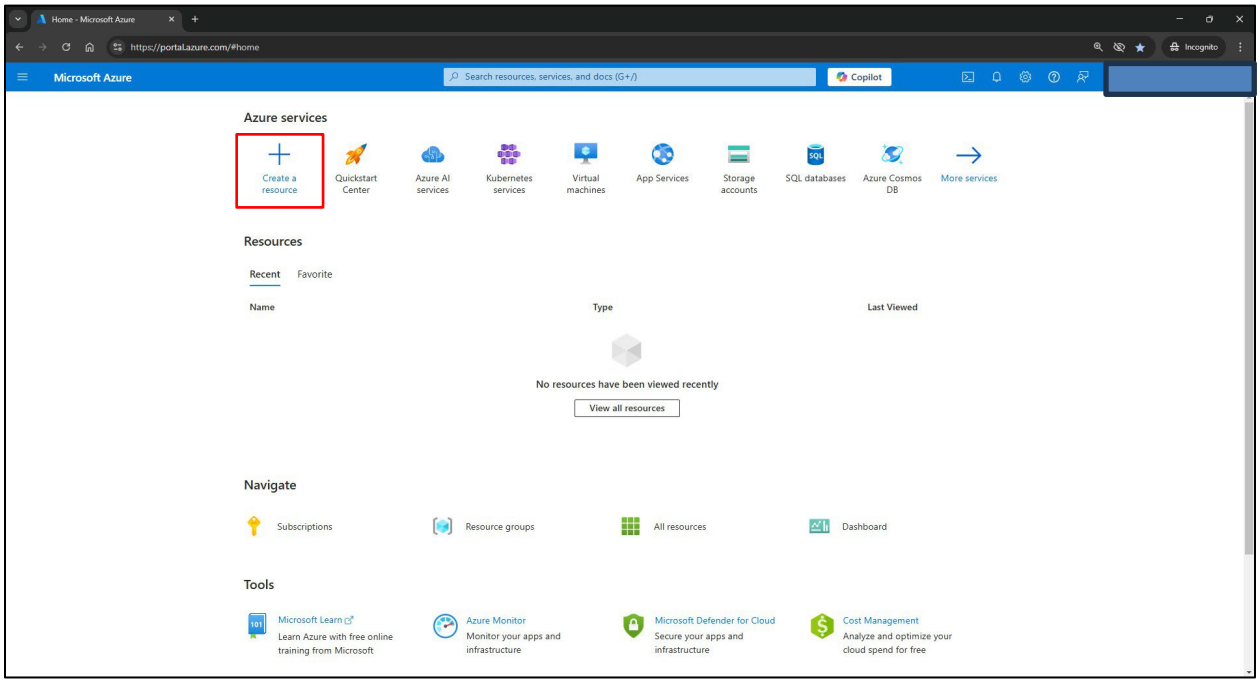
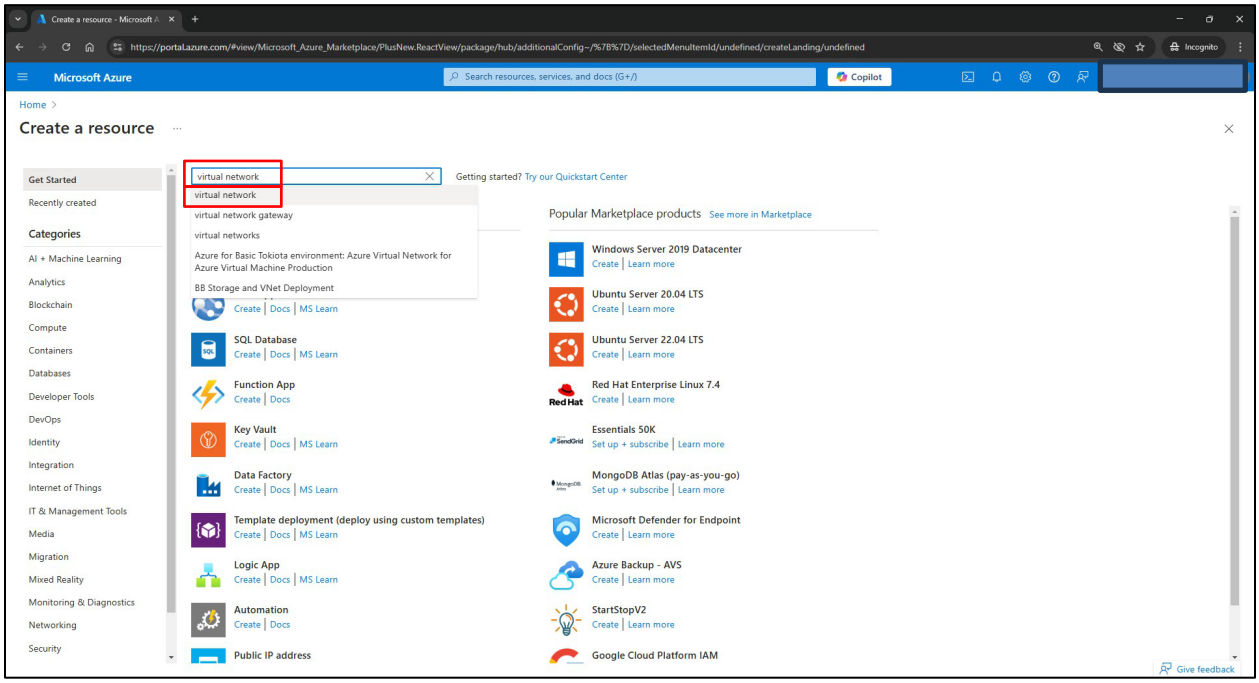
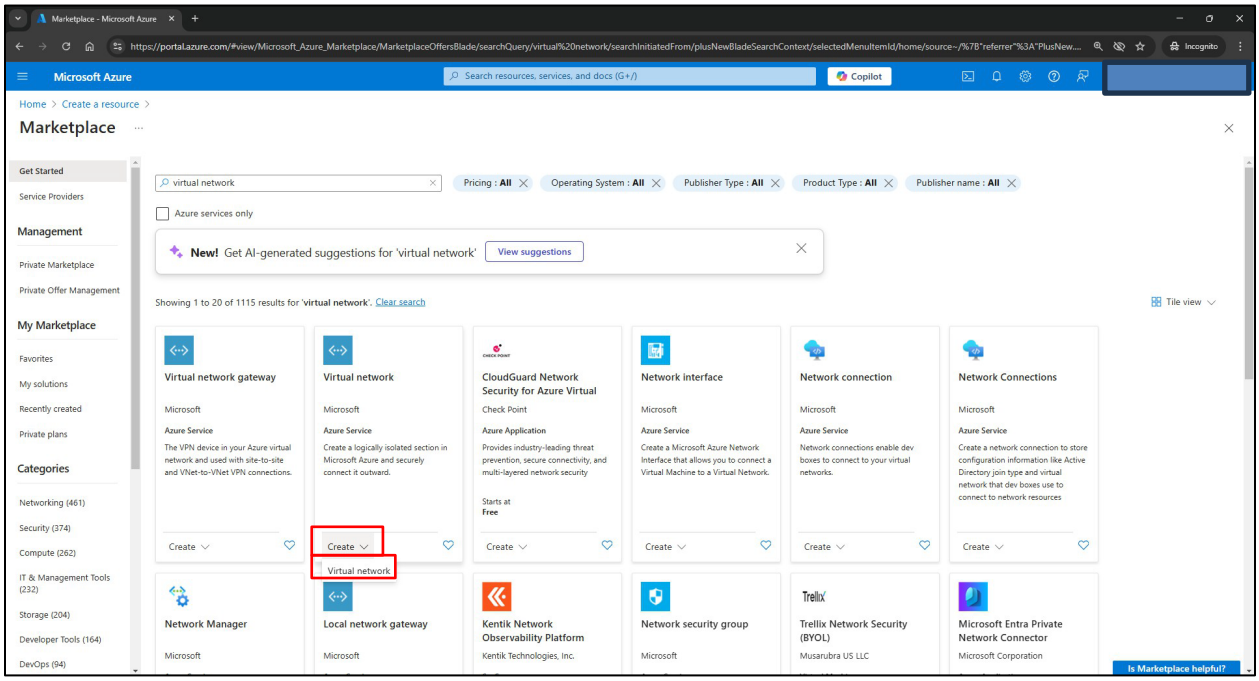
Login with **Username** & **Password** provided by Great Learning lab
Select **Create a resource**



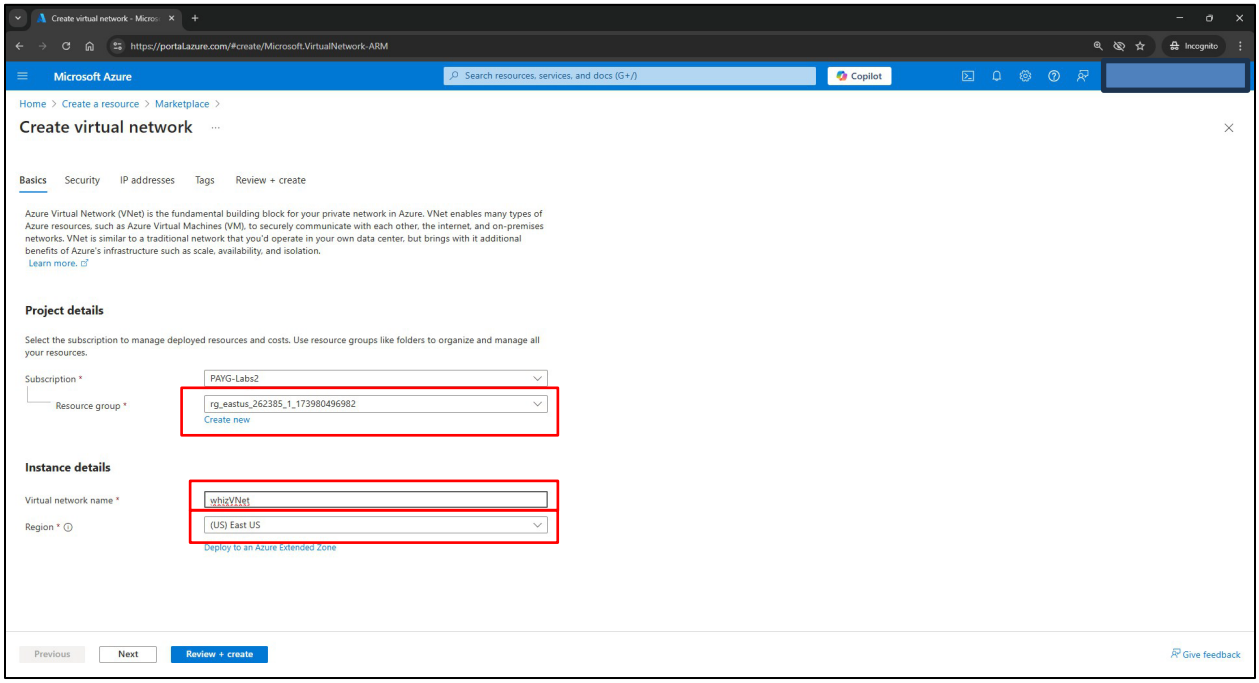
Enter **Virtual Networks** in search bar



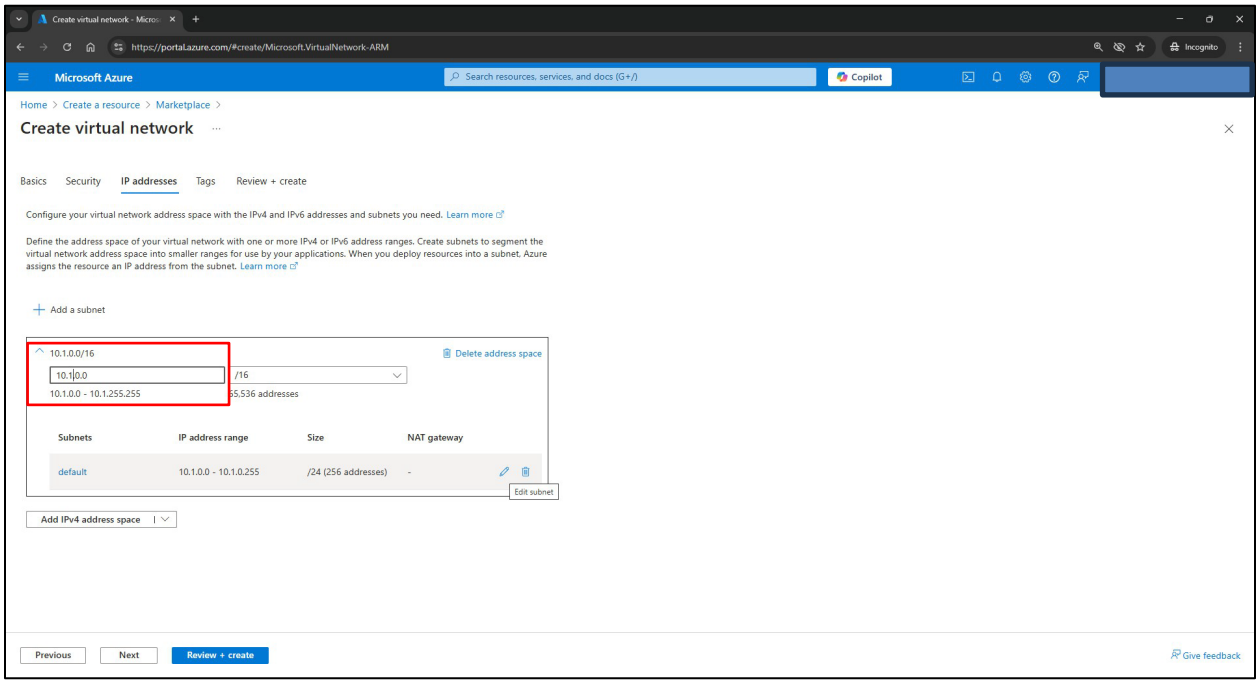
Select **Create**
Select **Virtual Network**



Resource group, select **rg_eastus_262385_1_173980496982**
Enter **whizVNet** in Name
Region: **East US**



Enter **IP Address** of **10.1.0.0**

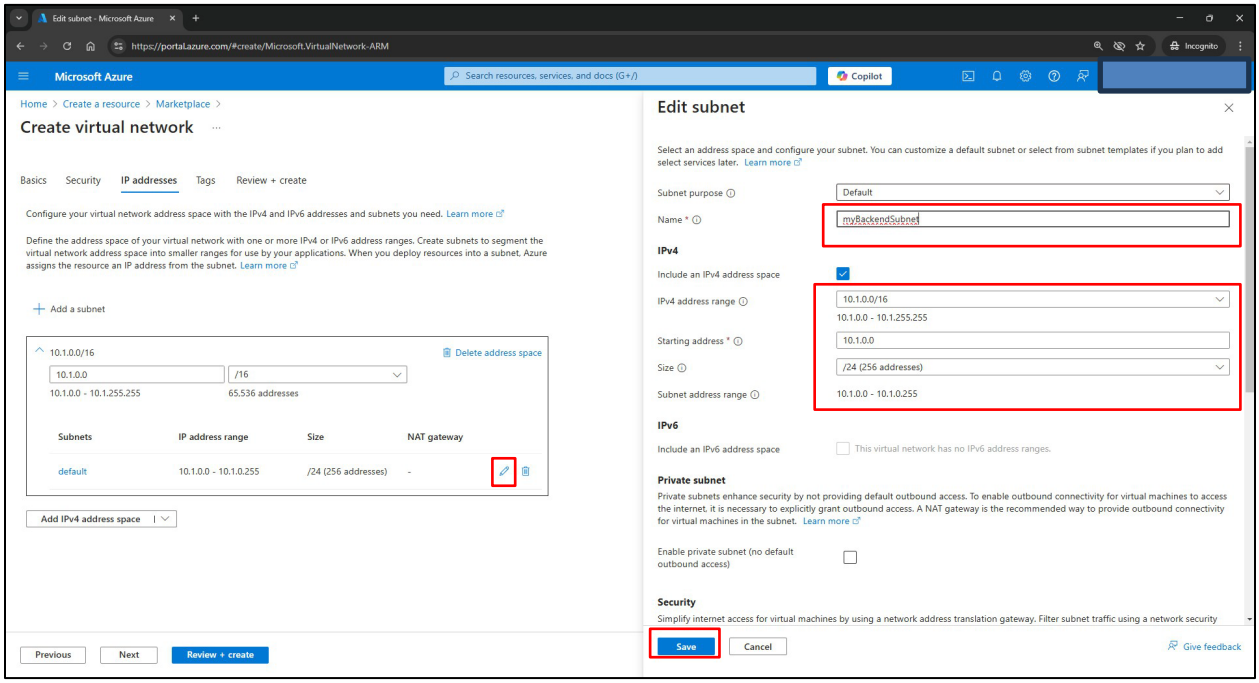


Select **Edit**

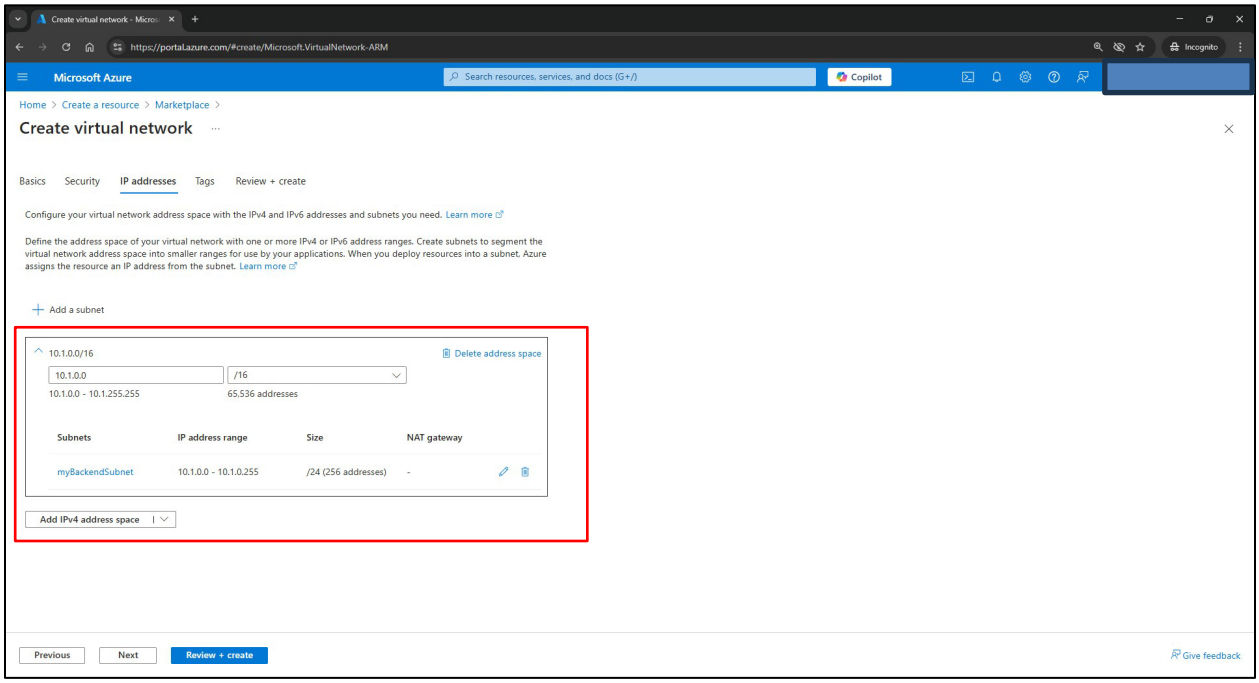
Enter **myBackendSubnet**

Confirm Subnet address range **10.1.0.0/16**, Starting address **10.1.0.0/24**

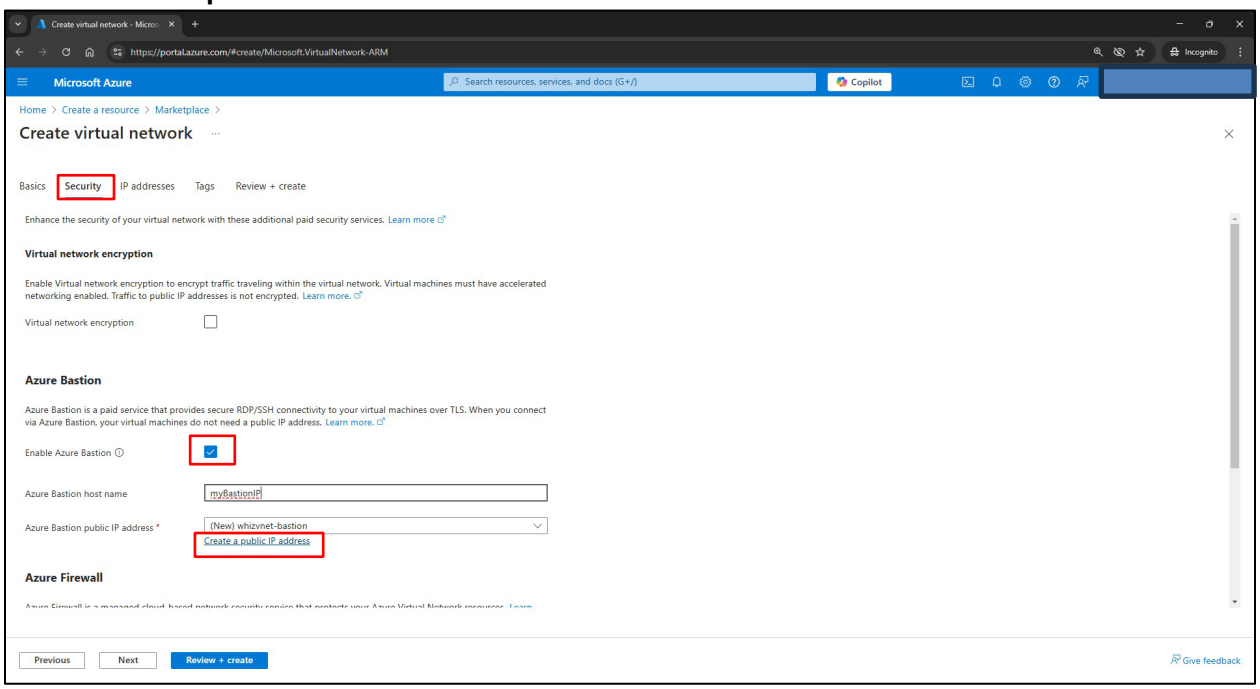
Select **Save**



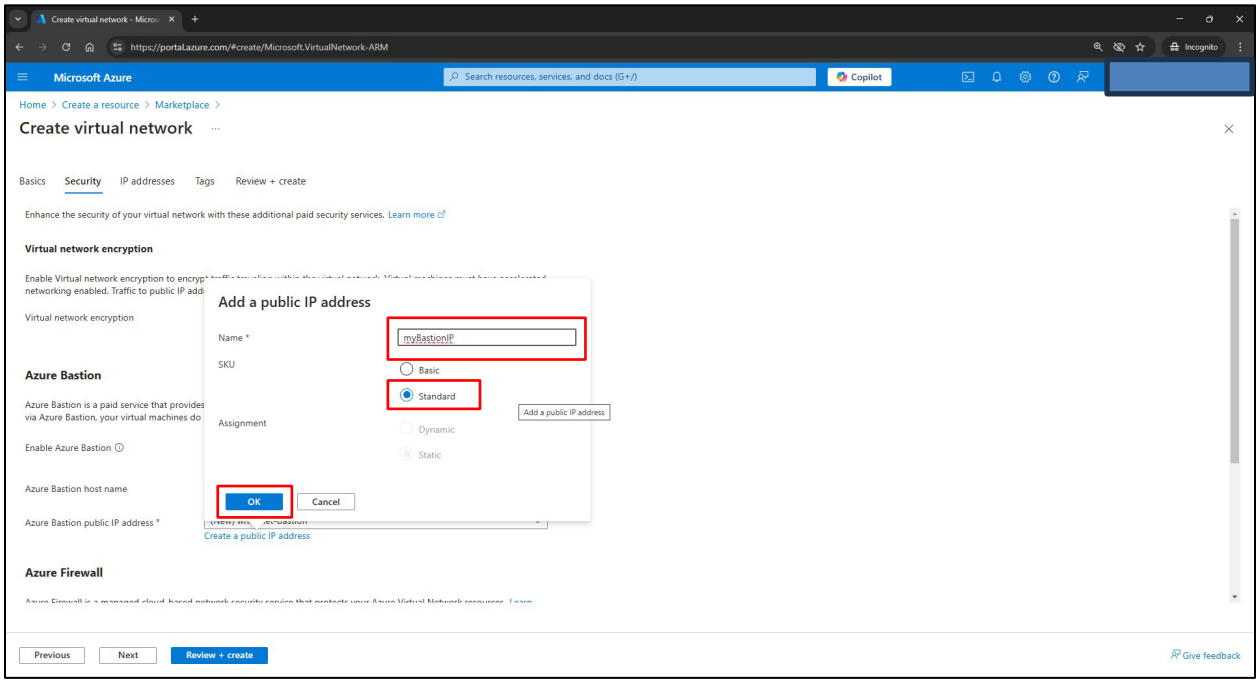
IP address and Subnet saved



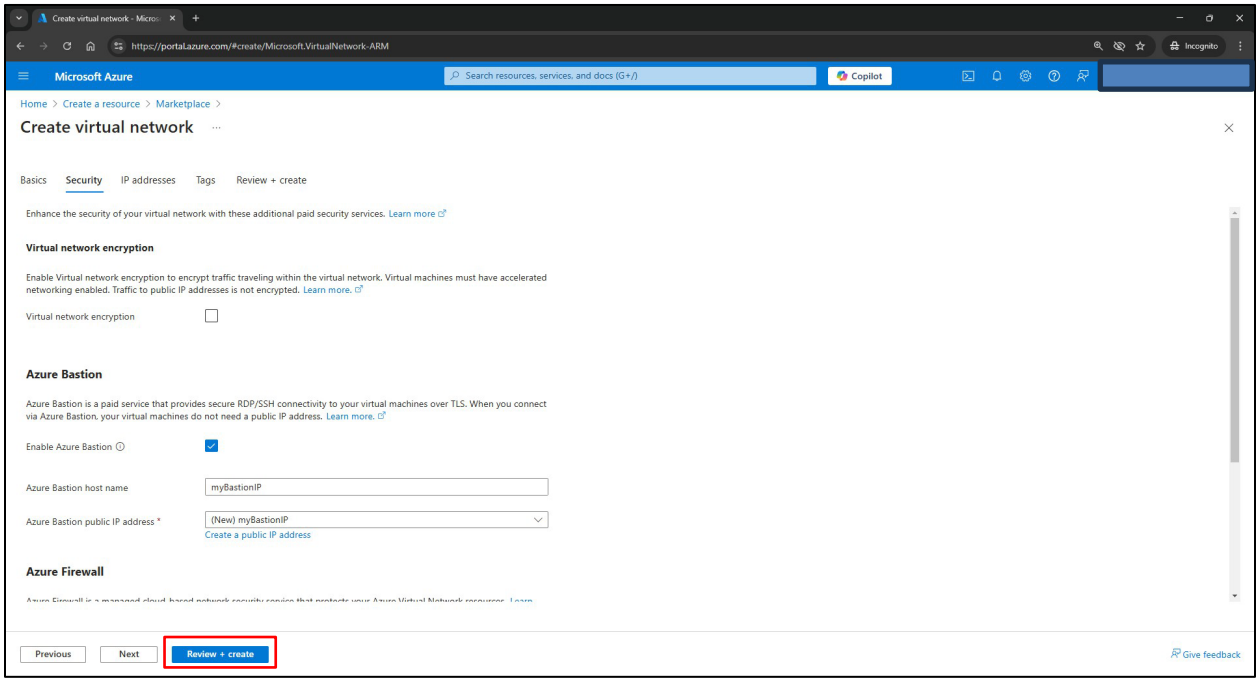
From Security tab, select **Enable Azure Bastion** checkbox
Enter **myBastionIP** under **Azure Bastion host name**
Select **Create a public IP address**



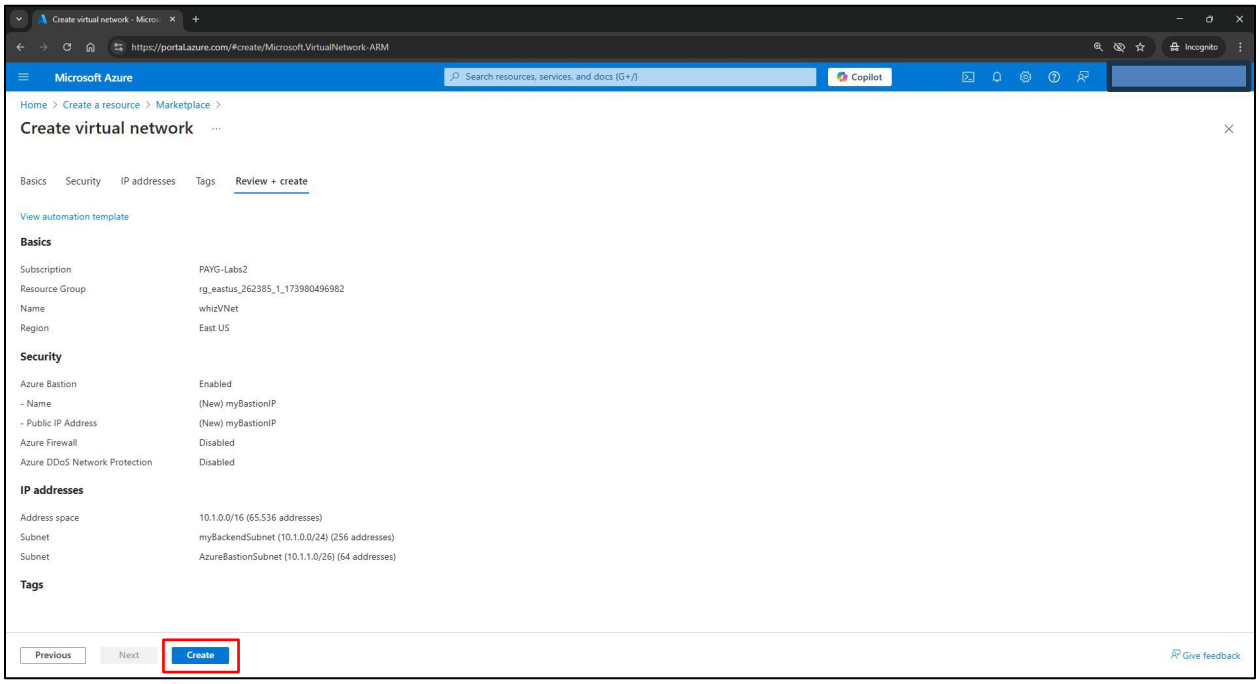
Enter **myBastionIP**
Select **Standard**
Select **OK**



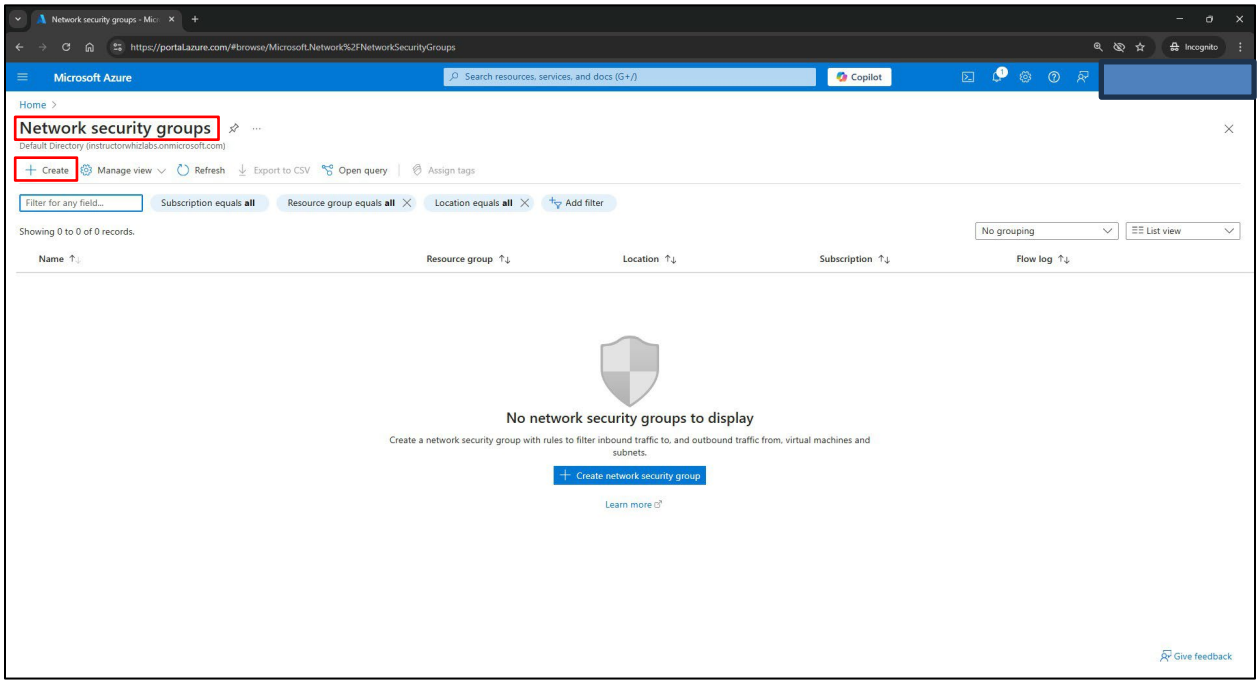
Select **Review + Create**



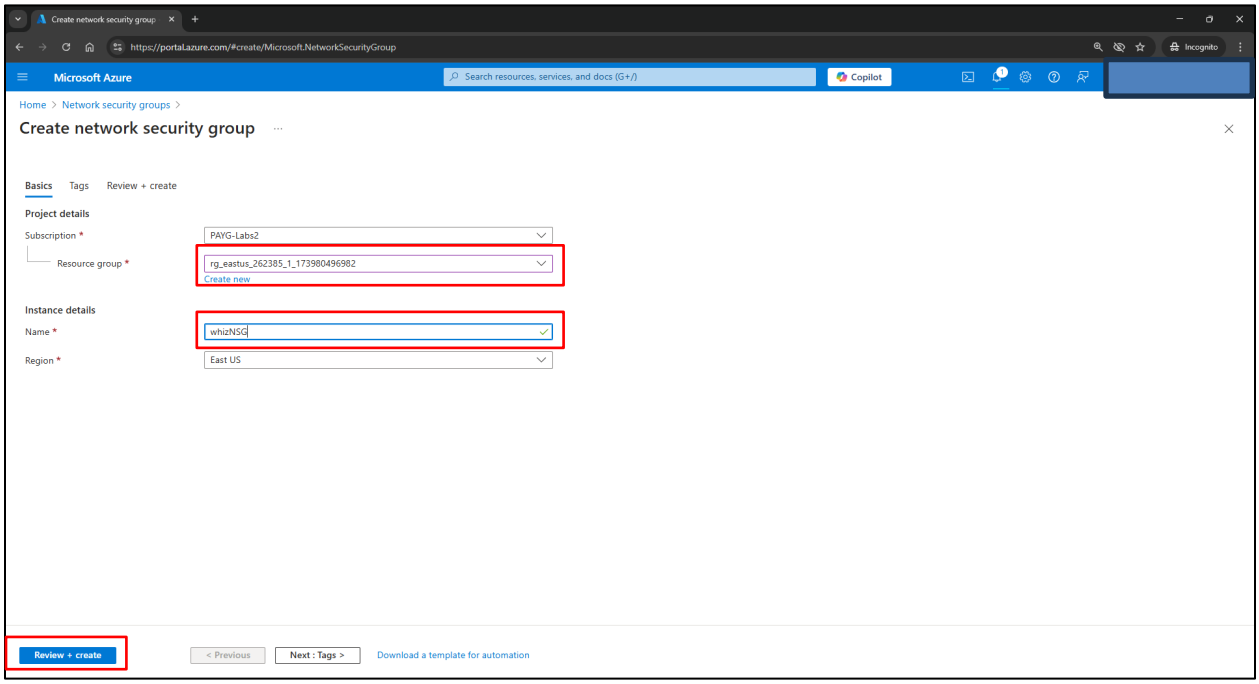
Select **Create**



Navigate to **Network Security Groups**, select **+ Create**

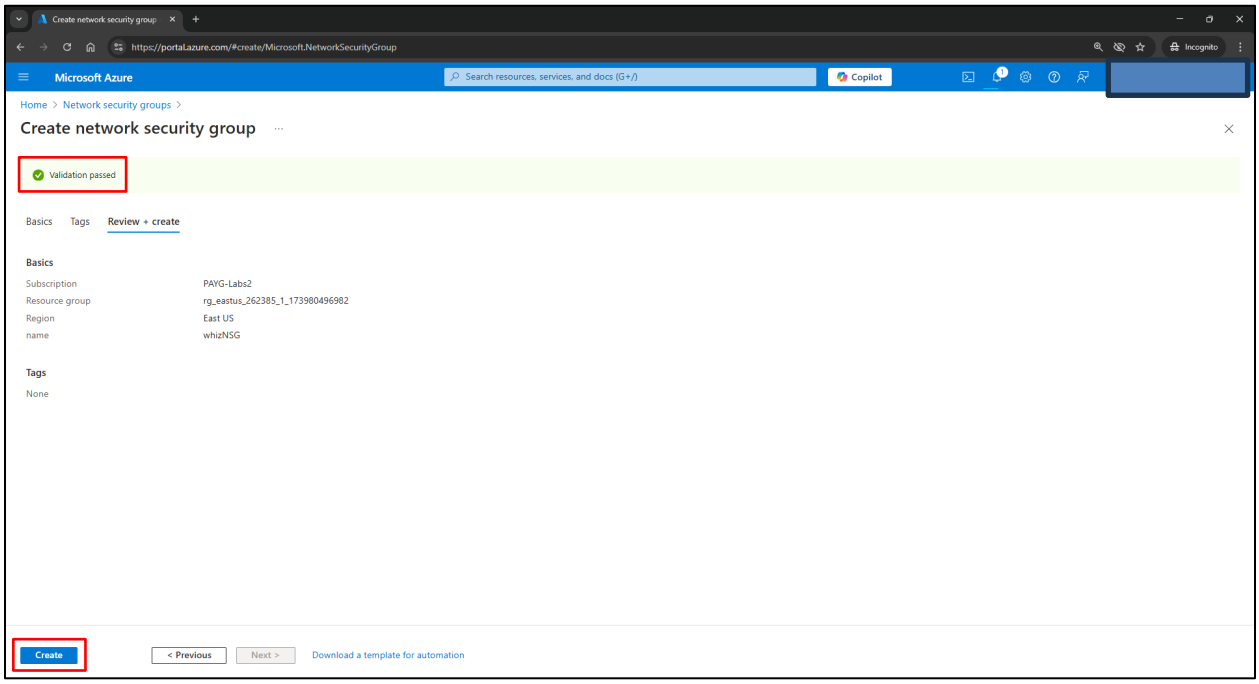


Select drop-down for Resource Group **rg_eastus_262385_1_173980496982**
Enter **whizNSG** in Name
Select **Review + Create**

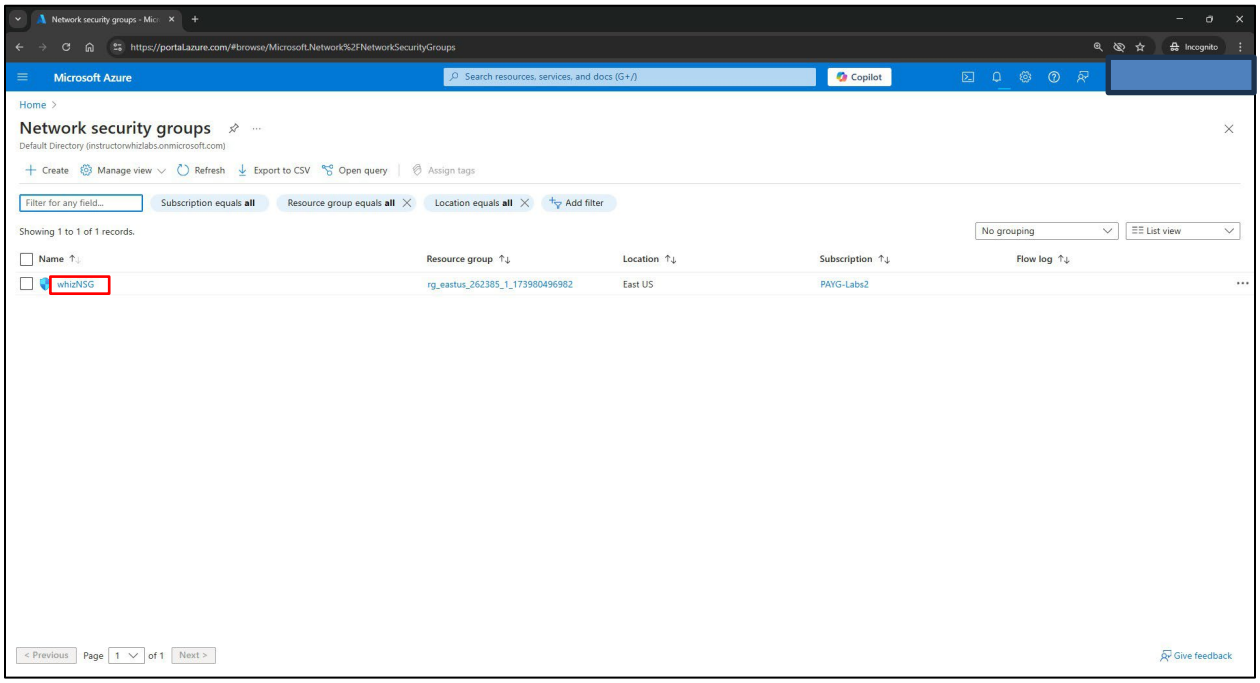


Validation Passed

Select **Create**

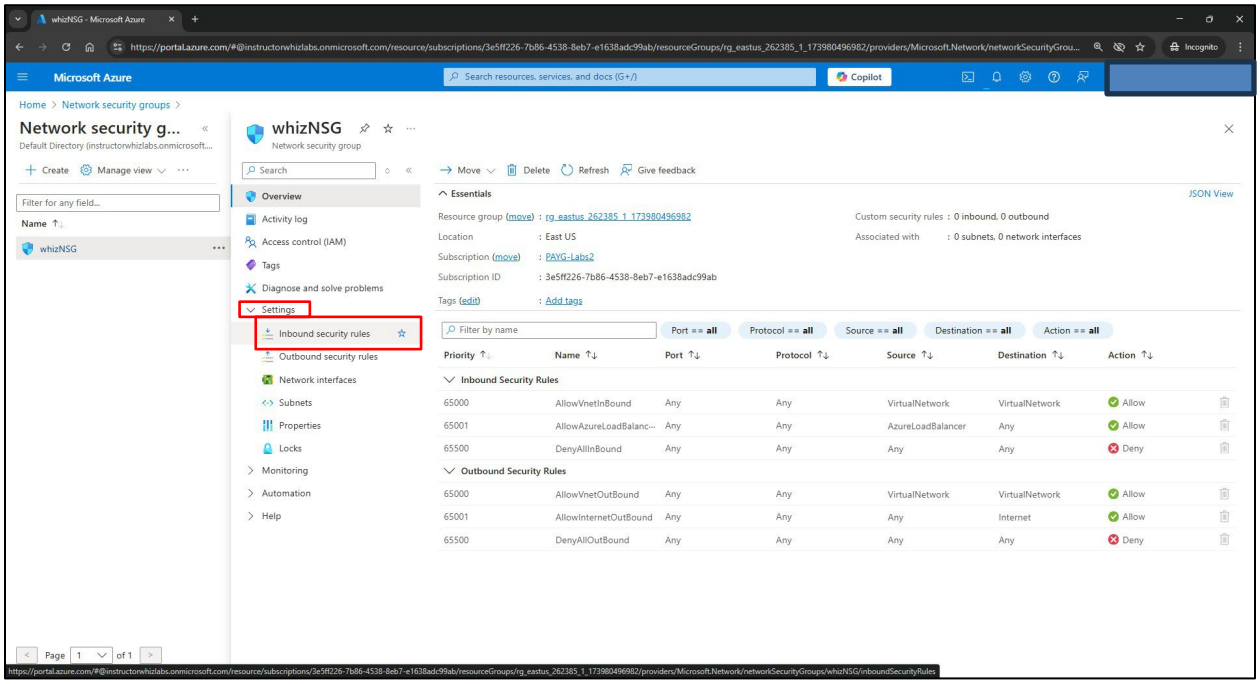


Select **whizNSG**

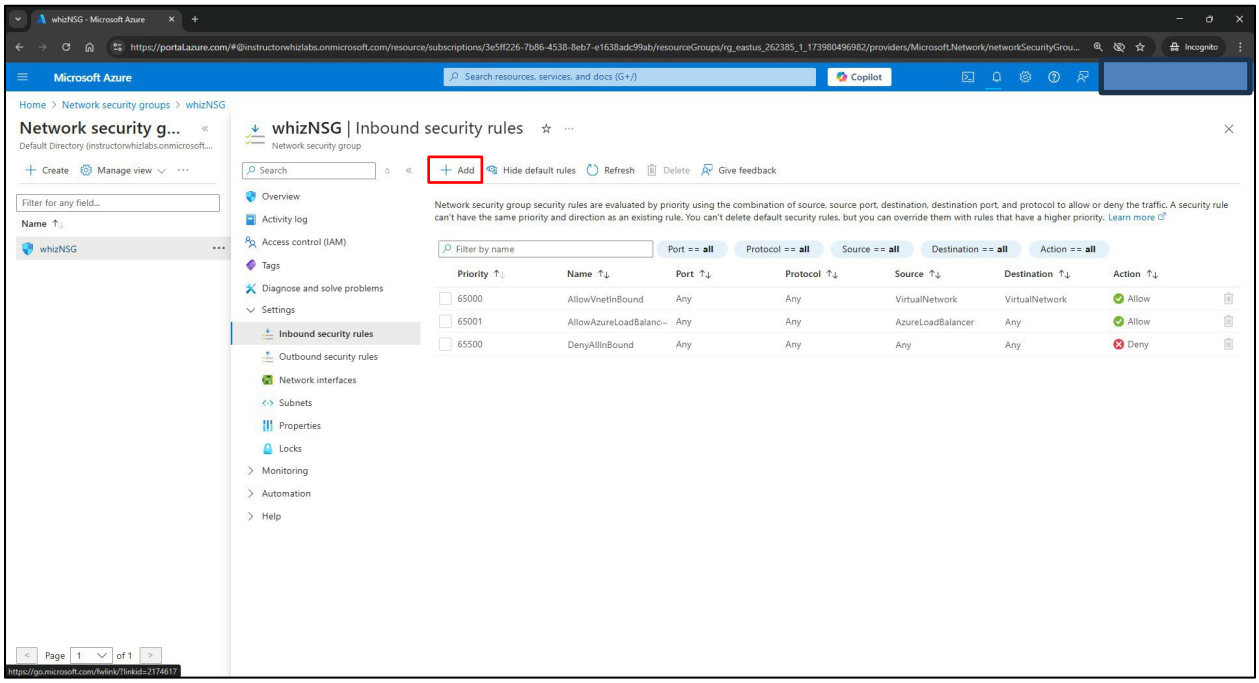


Select **Settings** drop down

Select **Inbound security rules**

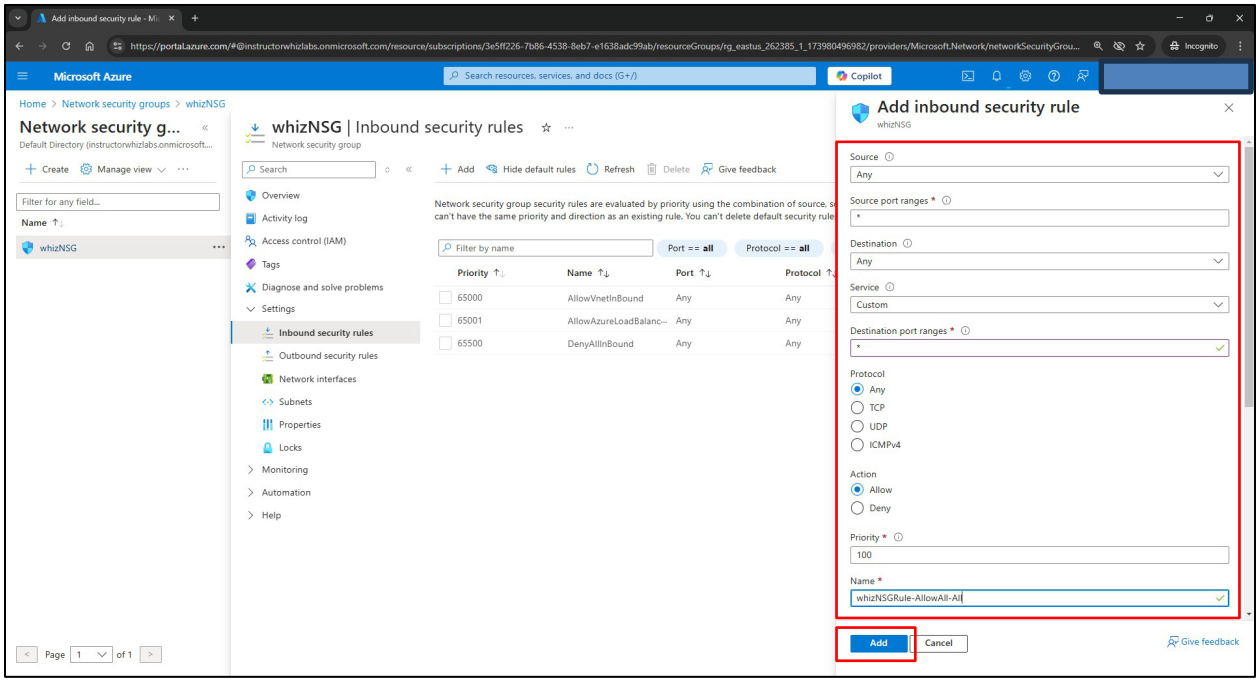


Select **+ Add**

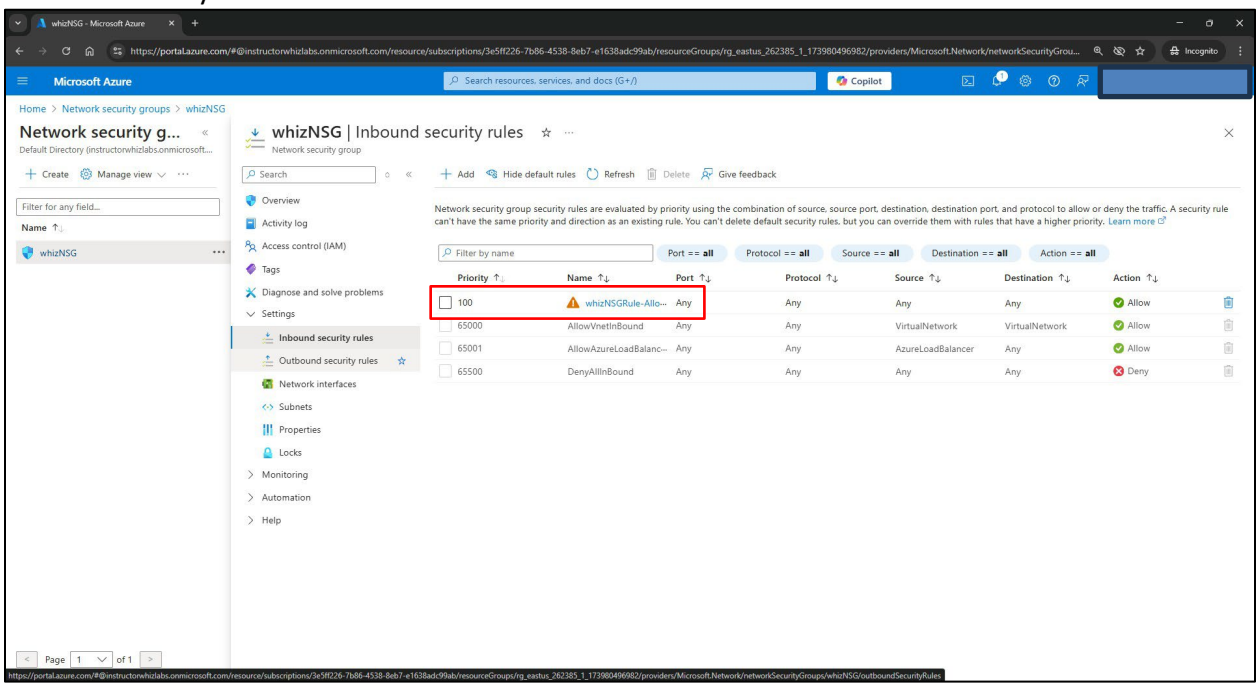

whizNSG - Microsoft Azure
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > Network security groups > whizNSG
Network security g...
Default Directory (instructorwhizlabs.onmicrosoft....
Create
Manage view
Filter for any field...
Name
whizNSG
Page 1 of 1
whizNSG | Inbound security rules
Network security group
Search
Add
Hide default rules
Refresh
Delete
Give feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Automation
Help
Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. Learn more
Filter by name
Port == all
Protocol == all
Source == all
Destination == all
Action == all
Priority
Name
Port
Protocol
Source
Destination
Action
65000 AllowVnetInBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowAzureLoadBalanc... Any Any AzureLoadBalancer Any Allow
65500 DenyAllInBound Any Any Any Any Deny

- Source: Leave the default of **Any**.
- Source port ranges: Leave the default of ***'*'***.
- Destination: Leave the default of **Any**.
- Service: Leave the default of **Custom**.
- Destination port ranges: Enter ***'*'***.
- Protocol: Select **Any**.
- Action: Leave the default of **Allow**.
- Priority: Enter ***100***.
- Name: Enter ***whizNSGRule-AllowAll-All***

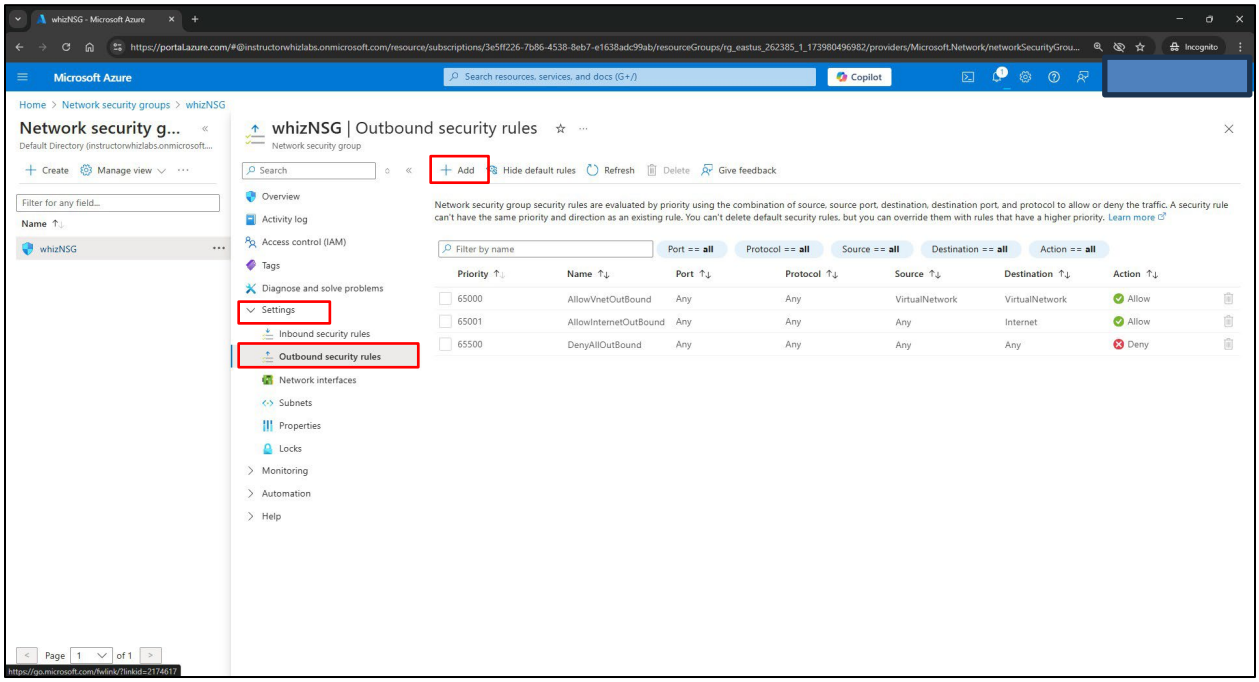
Select **Add**



Inbound security rule created

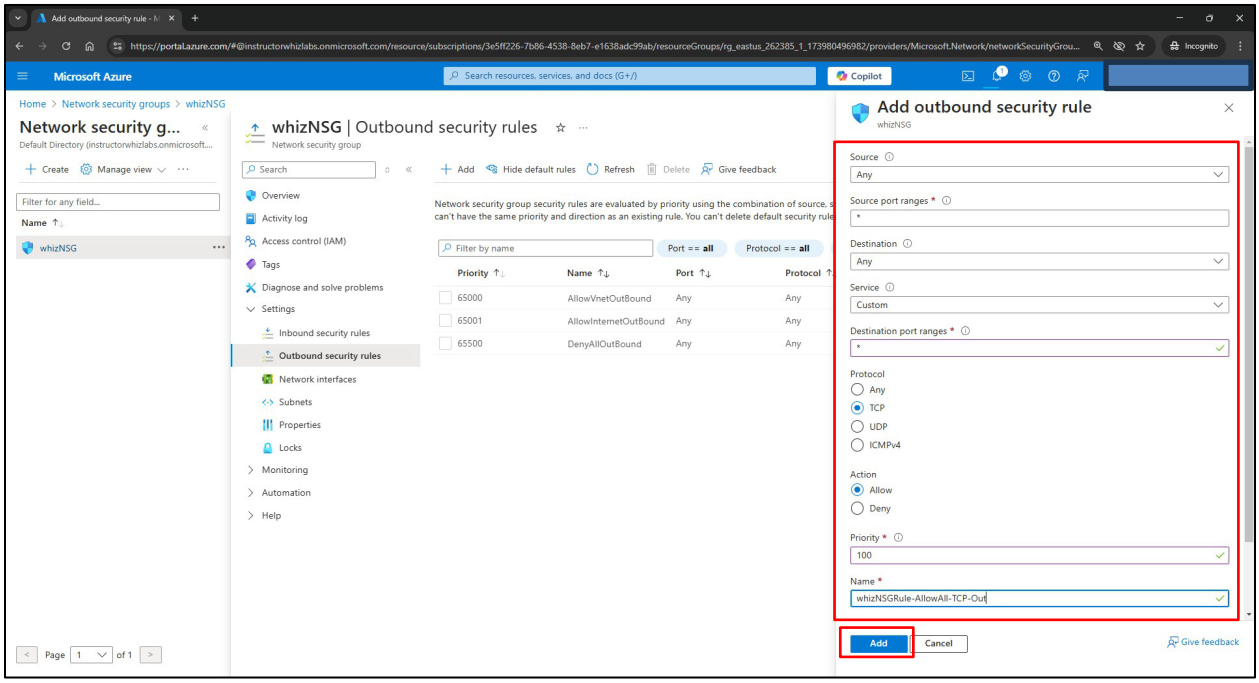


Under Settings, select **Outbound security rules**
Select **+ Add**

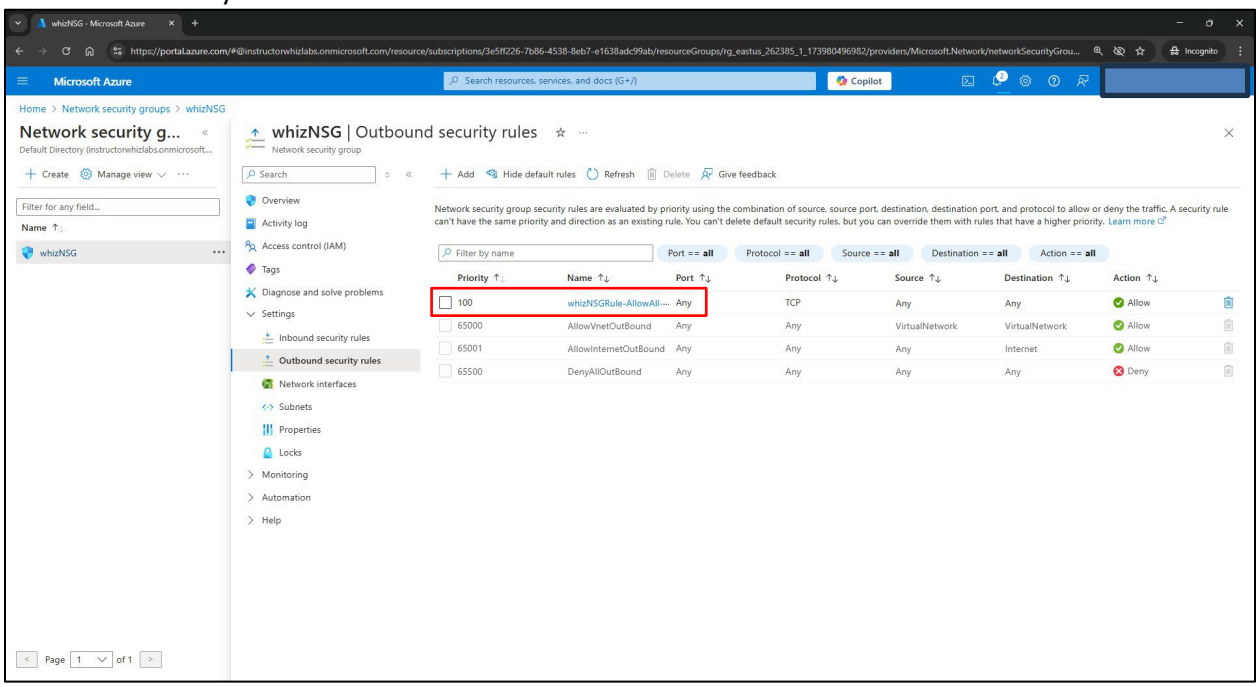


- Source: Leave the default of **Any**.
- Source port ranges: Leave the default of ***'*'***.
- Destination: Leave the default of **Any**.
- Service: Leave the default of **Custom**.
- Destination port ranges: Enter ***'*'***.
- Protocol: Select **TCP**.
- Action: Leave the default of **Allow**.
- Priority: Enter ***100***.
- Name: Enter ***whizNSGRule-AllowAll-TCP-Out***

Select **Add**

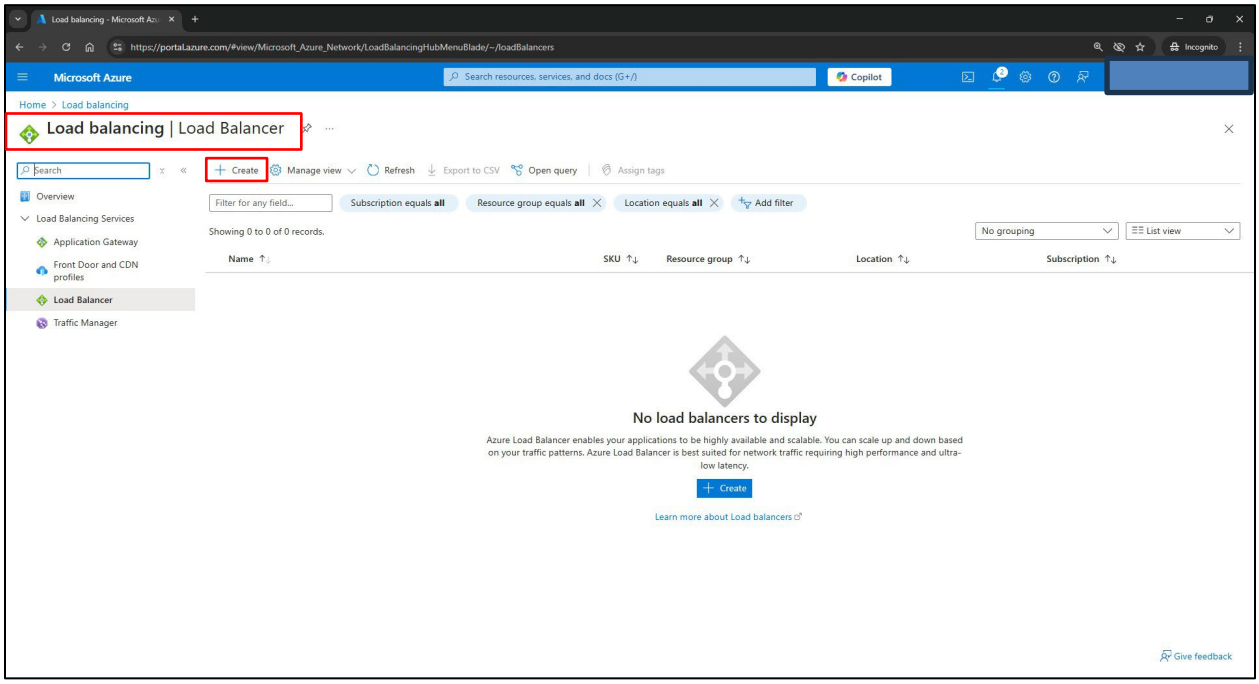


Outbound security rule added

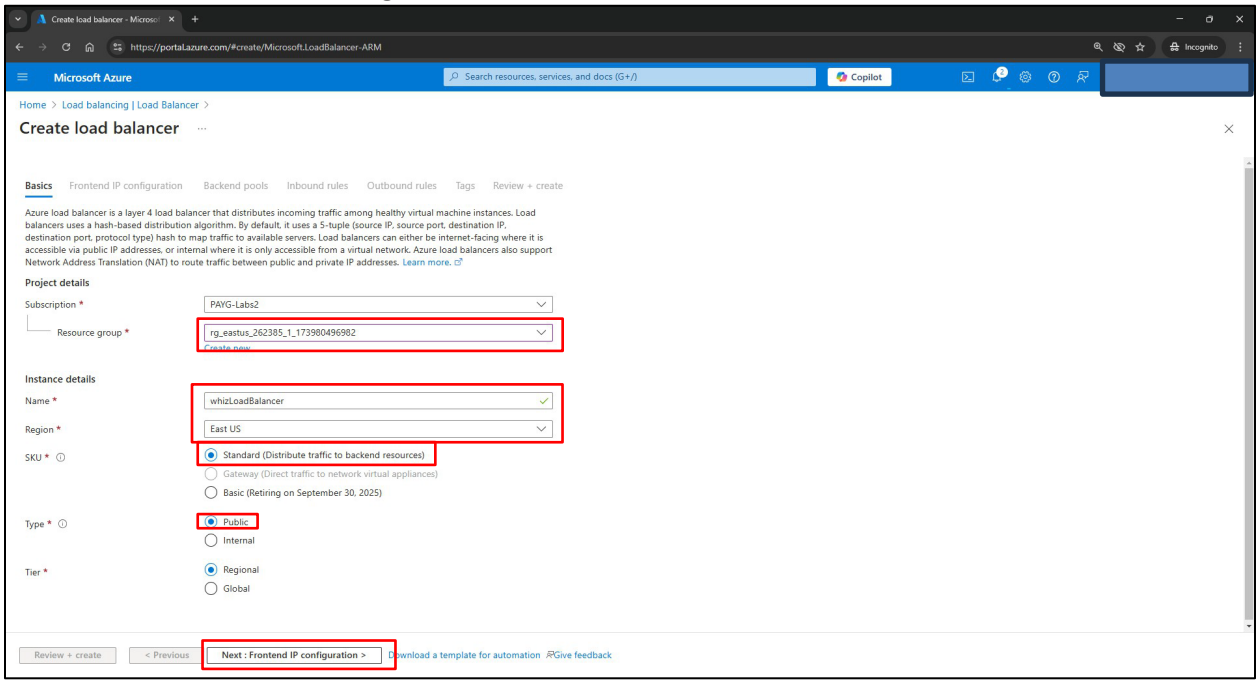


Navigate to **Load balancer**

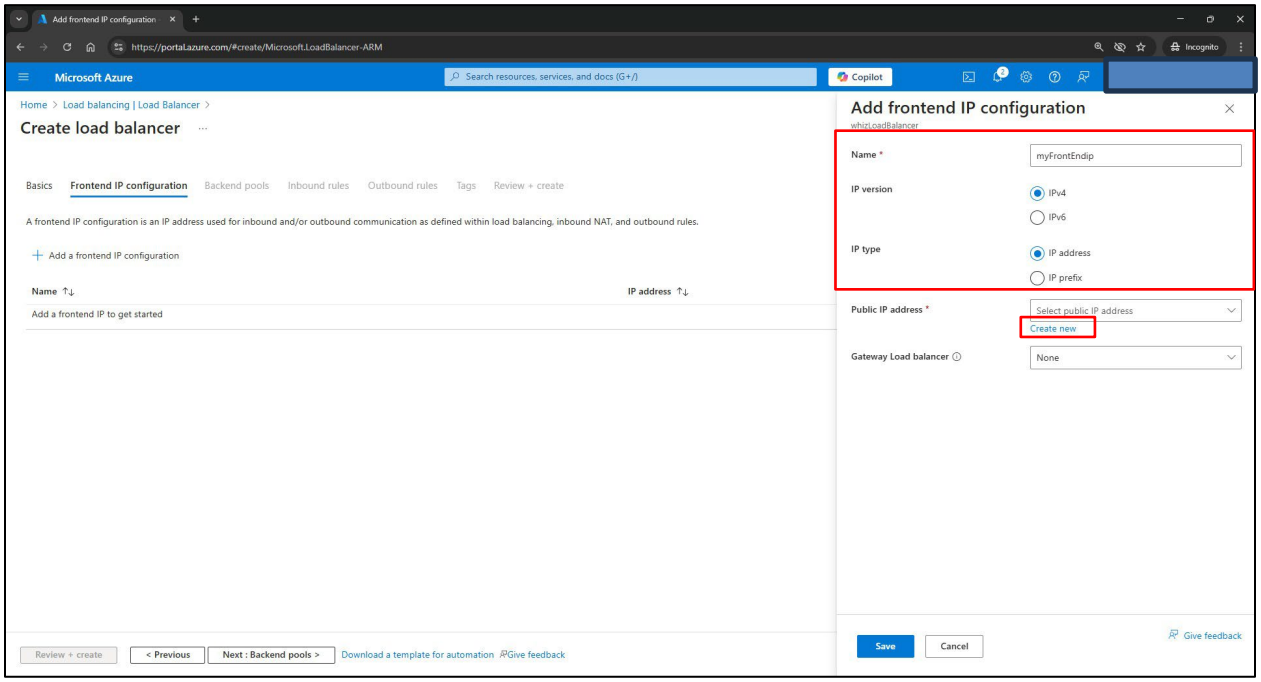
Select **Create**



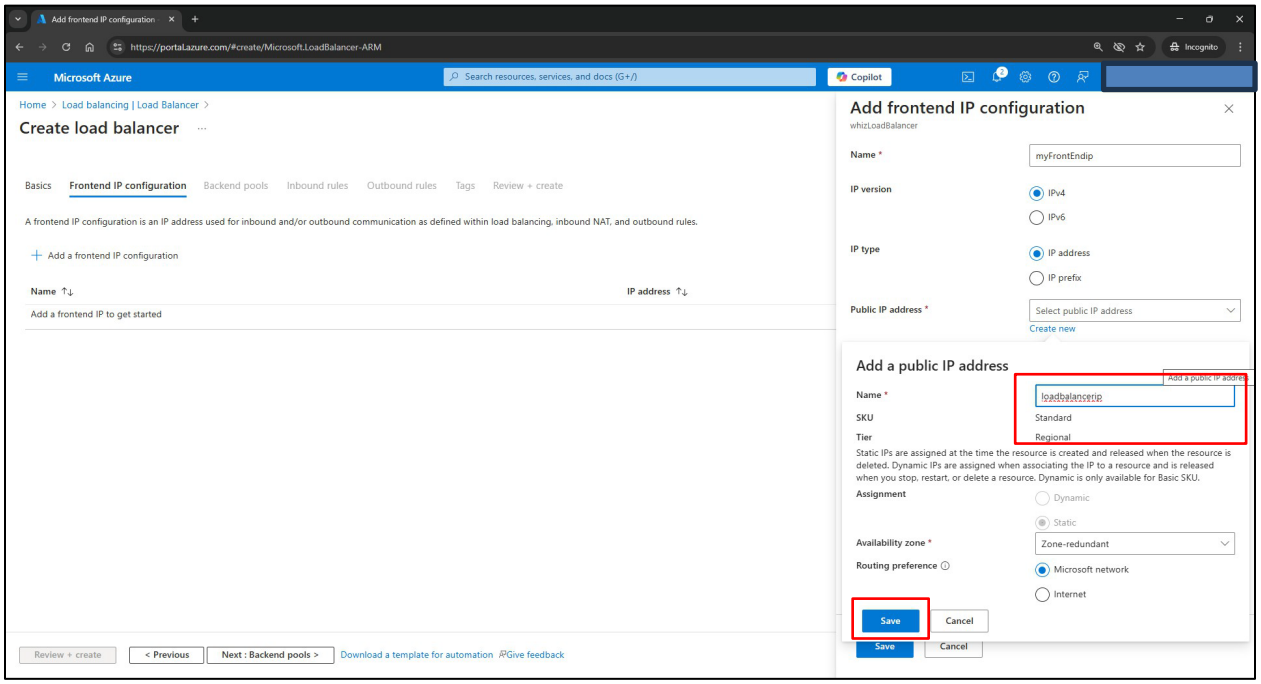
Select Resource group drop down, select **rg_eastus_262385_1_173980496982**
Enter name **whizLoadBalancer**
Region: **East US**
Select **Standard**
Select **Public**
Select **Next: Frontend IP configuration**



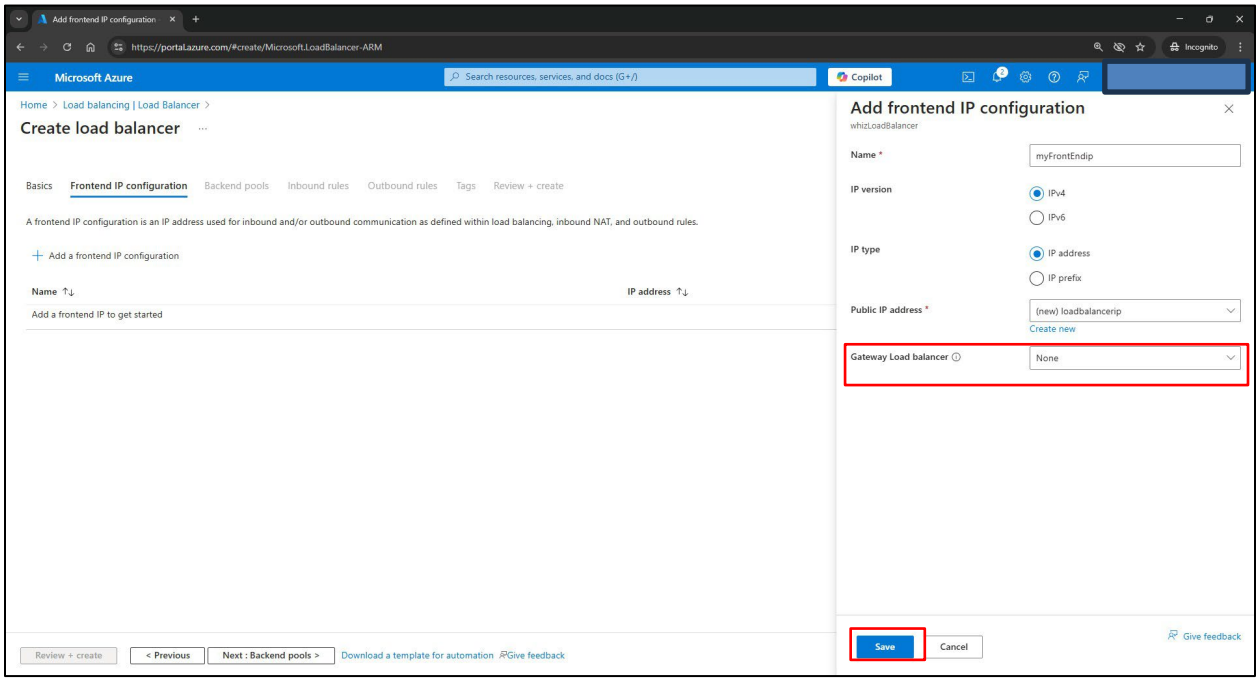
Enter **myFrontEndIP** under Name
IP version: **IPv4**
IP type: **IP address**
Select **Create new** under Public IP address



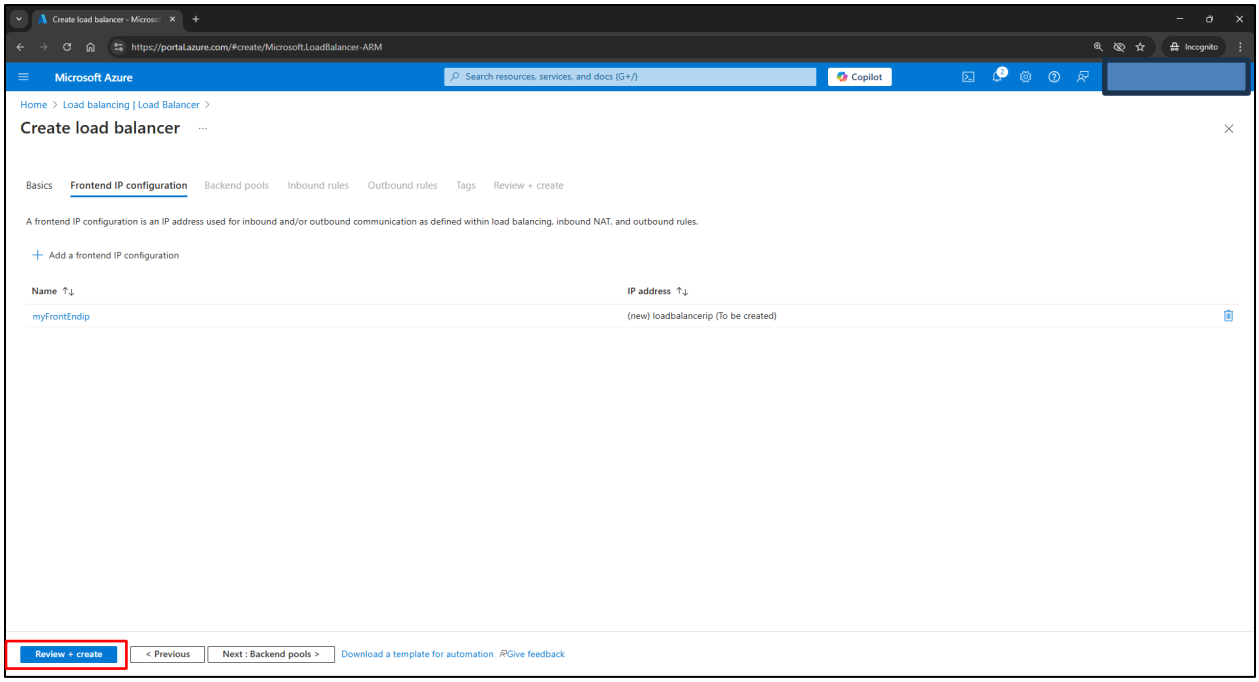
Under Add a public IP address, enter **loadbalancerip** under Name
Select **Save**



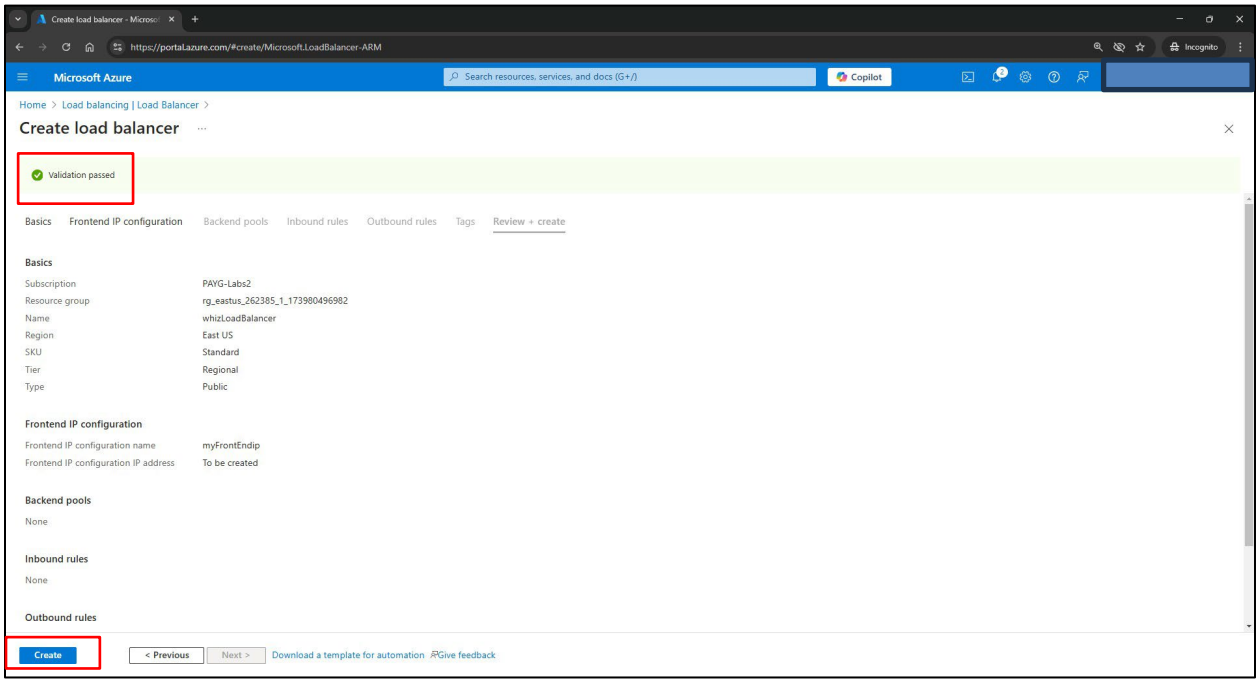
Gateway Load balancer: **None**
Select **Save**



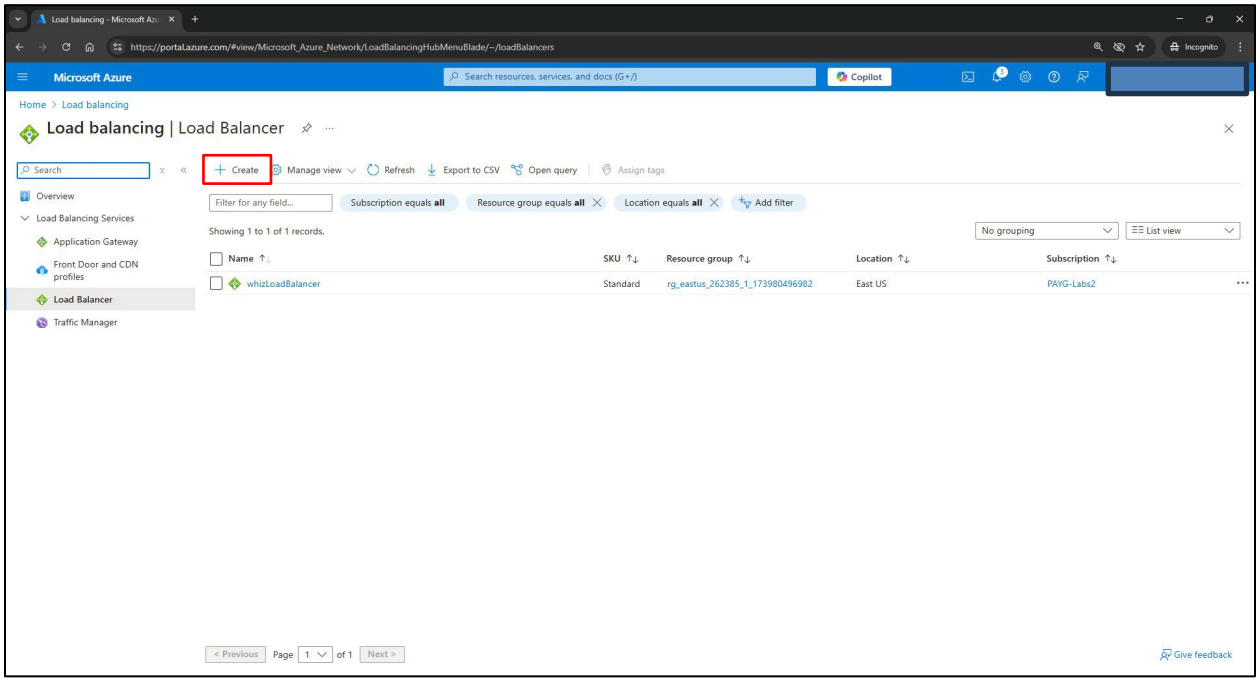
Frontend IP configuration created
Select **Review + Create**



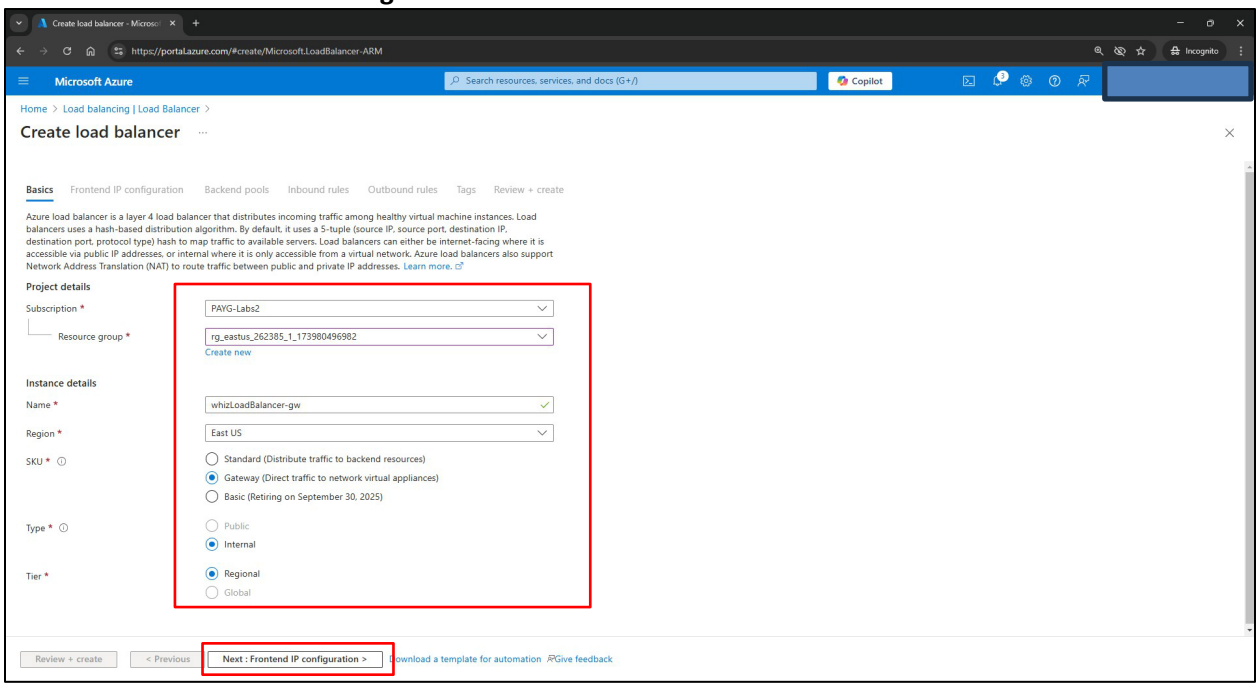
Validation Passed
Select **Create**



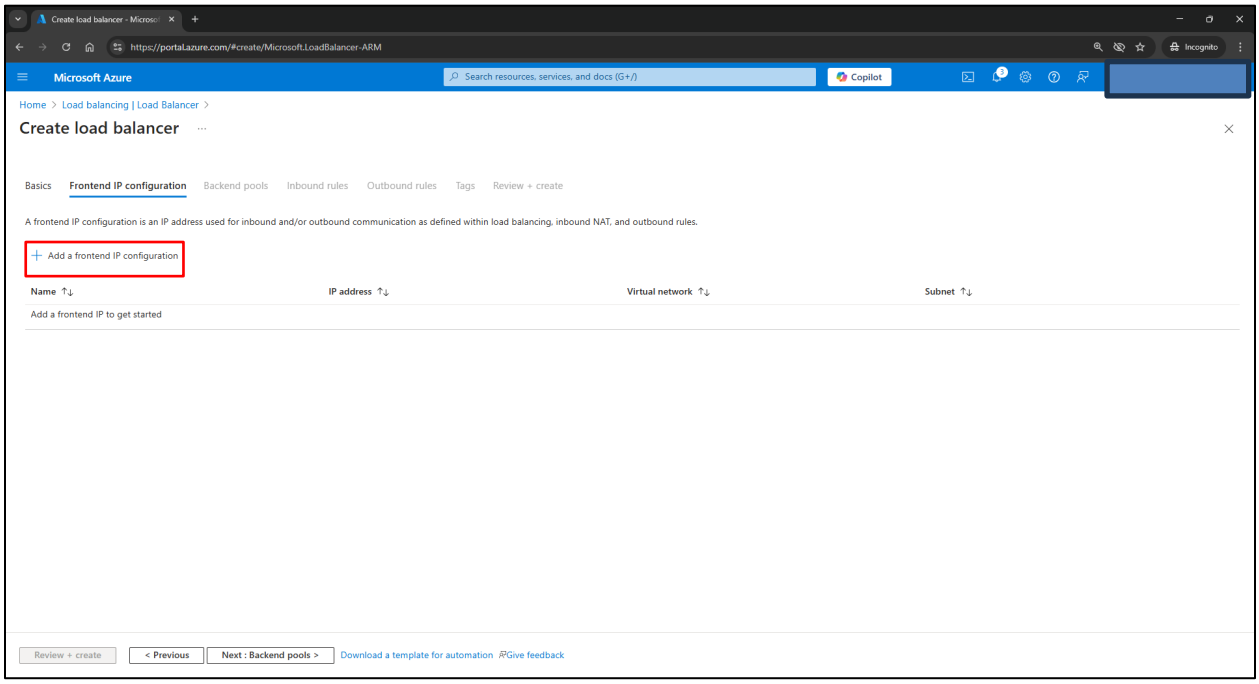
From Load Balancer page, select **+ Create**



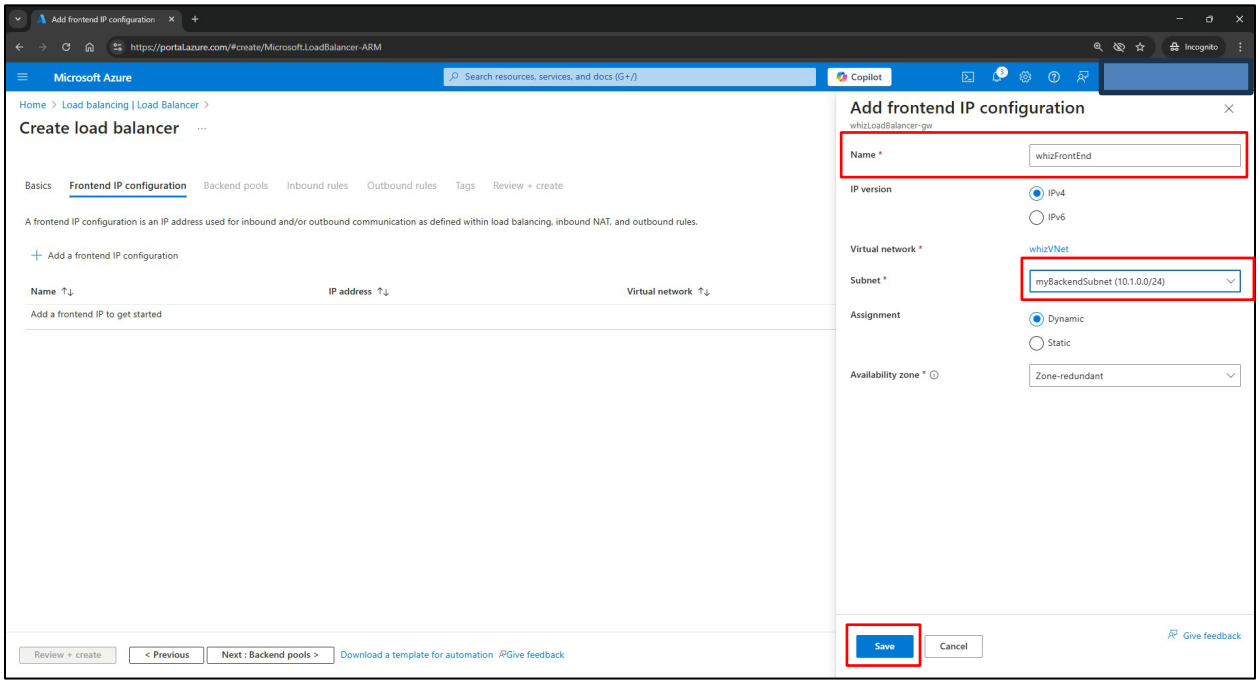
Enter Resource group **rg_eastus_262385_1_173980496982**
Name: **whizLoadBalancer-gw**
SKU: **Gateway**
Type: **Internal**
Select **Next: Frontend IP configuration**



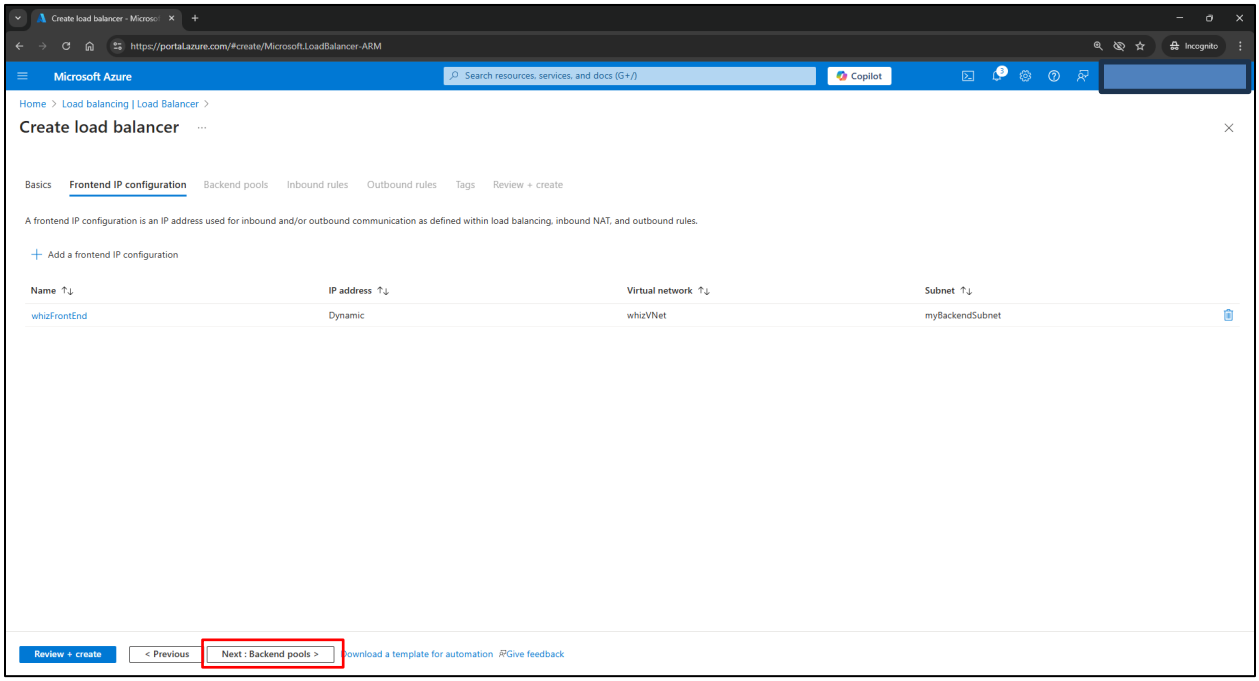
Select **+ Add a frontend IP configuration**



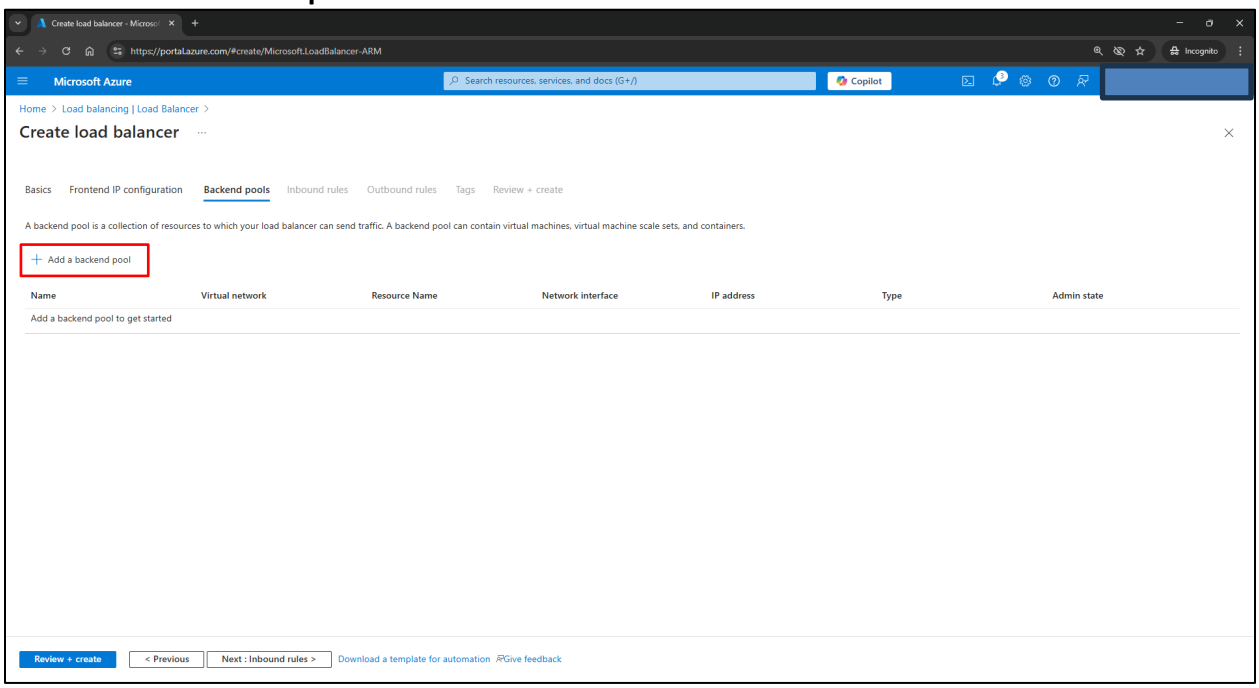
Name: **whizFrontEnd**
Subnet, select **myBackendSubnet**
Select **Save**



Select **Next: Backend pools**



Select **+ Add a backend pool**

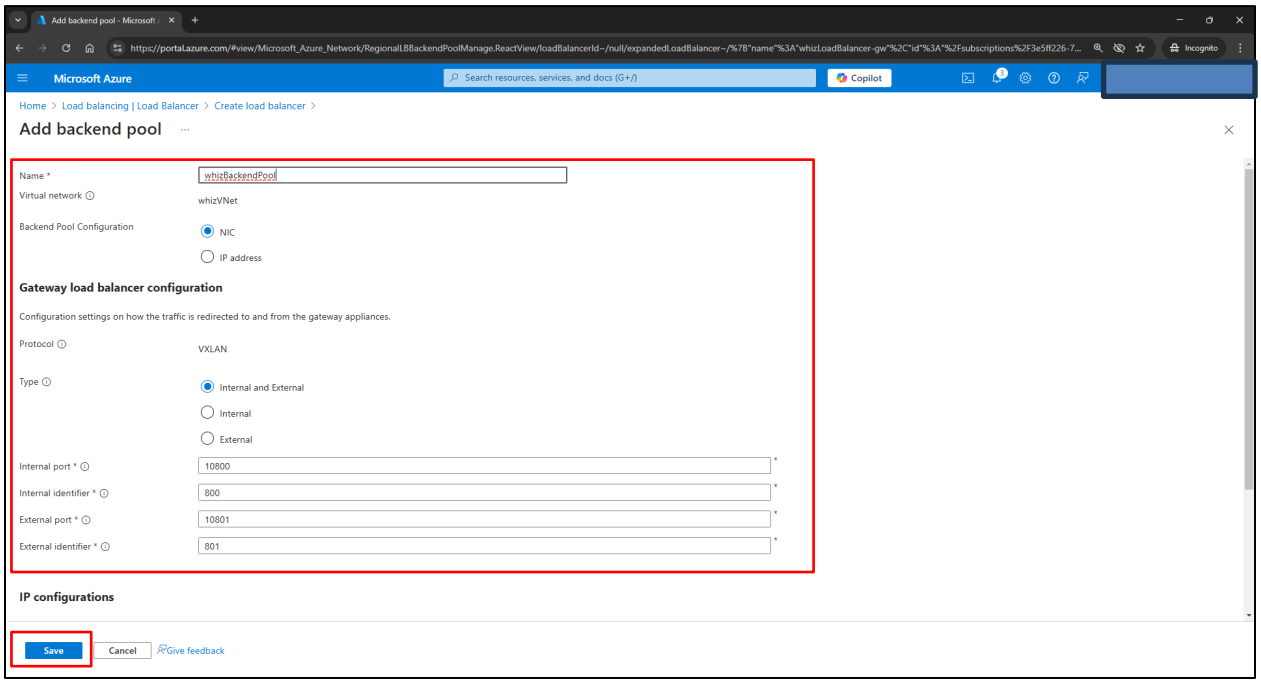


Enter **whizBackendPool**

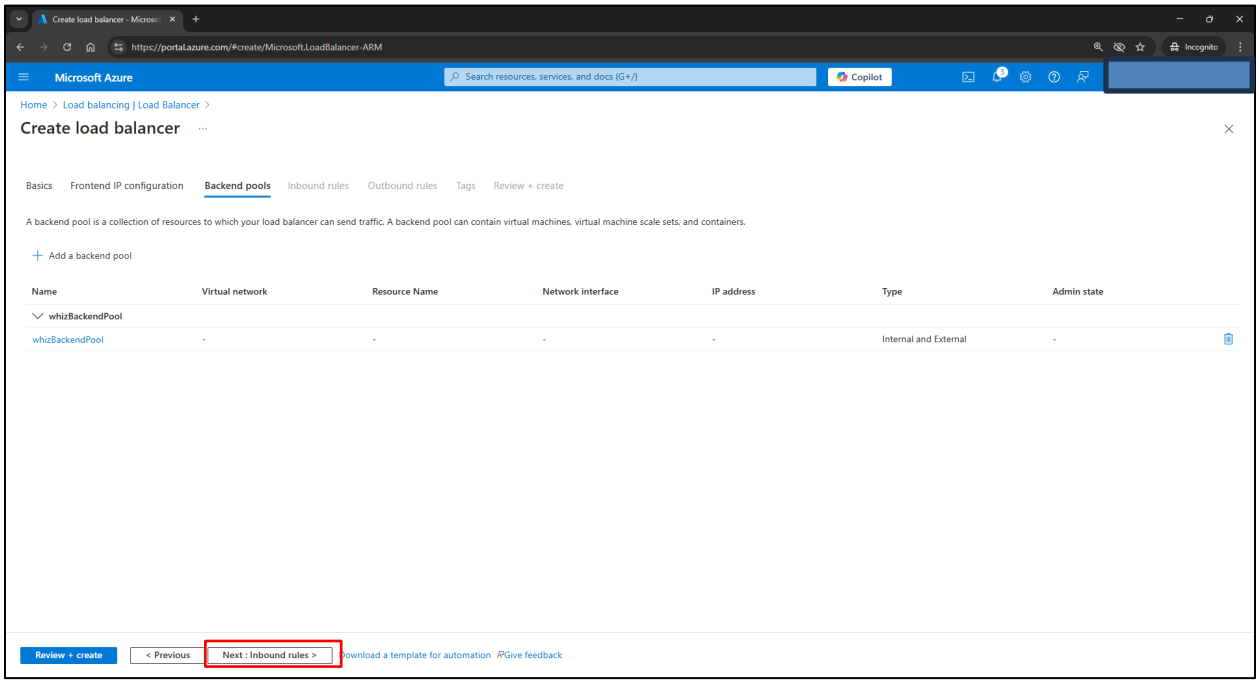
Under **Gateway load balancer configuration**

- Type: Select **Internal and External**
- Internal port: Leave the default of **10800**
- Internal identifier: Leave the default of **800**
- External port: Leave the default of **10801**
- External identifier: Leave the default of **801**

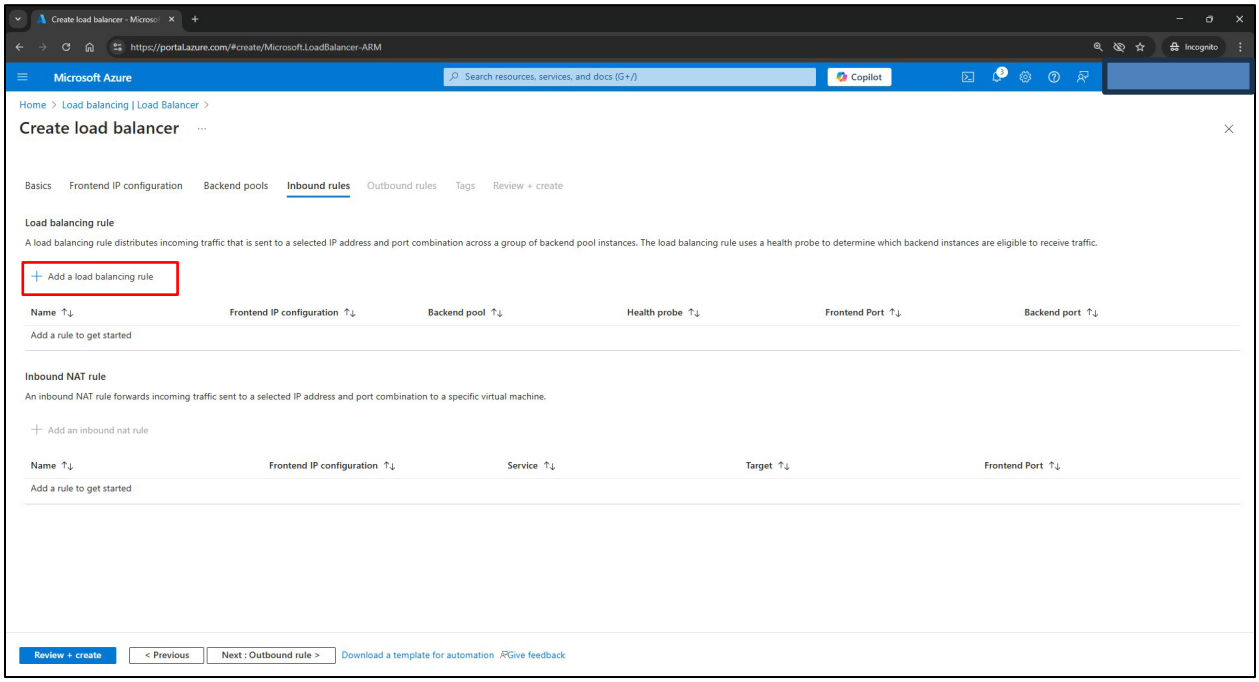
Select **Save**



Backend pool created
Select **Next: Inbound rules**

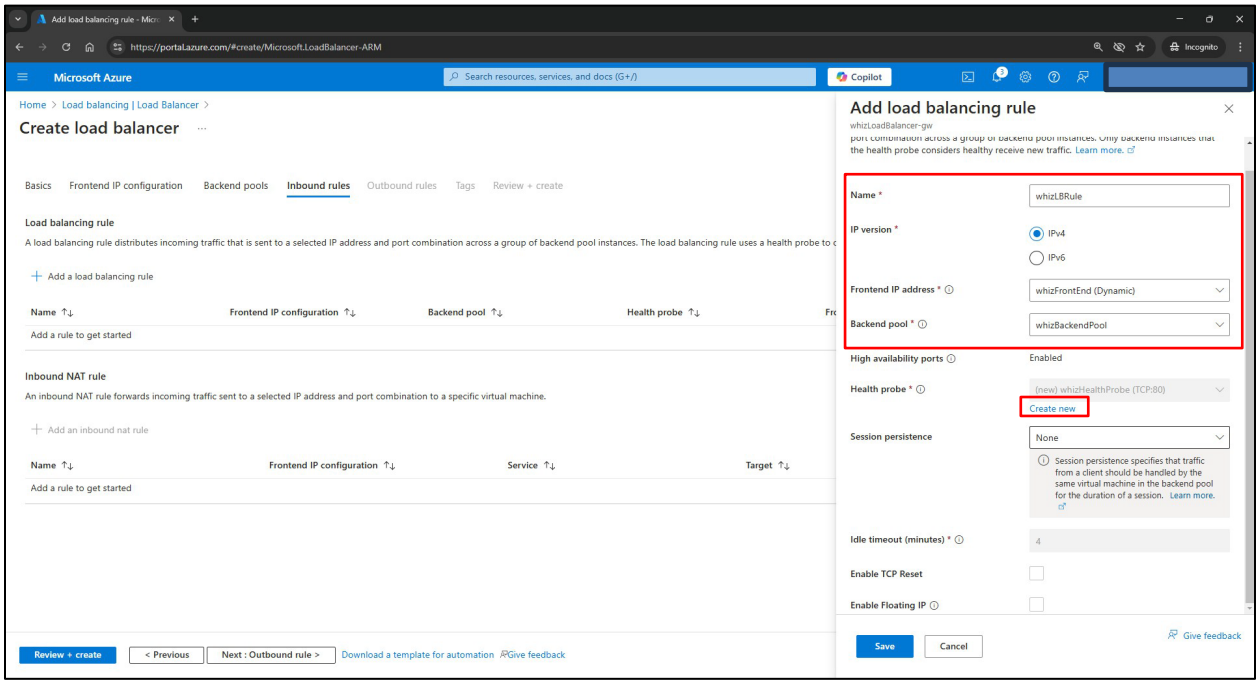


Select **+ Add a load balancing rule**

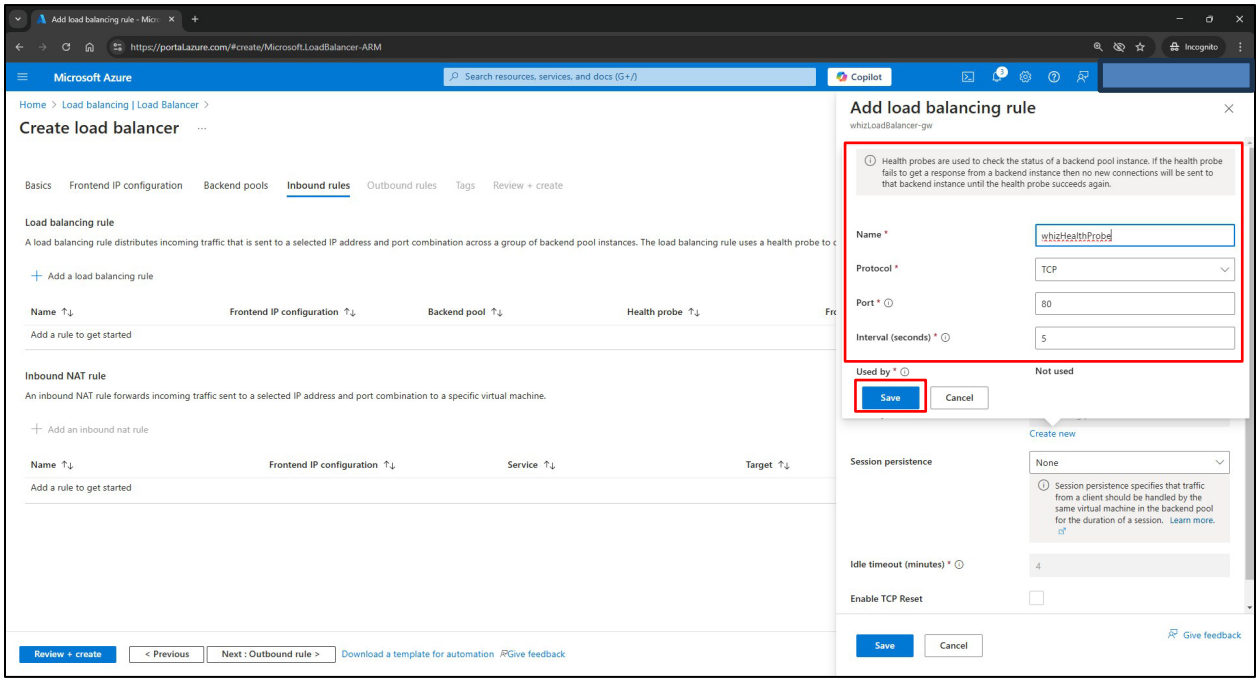


Under **Add load balancing rule**, enter:

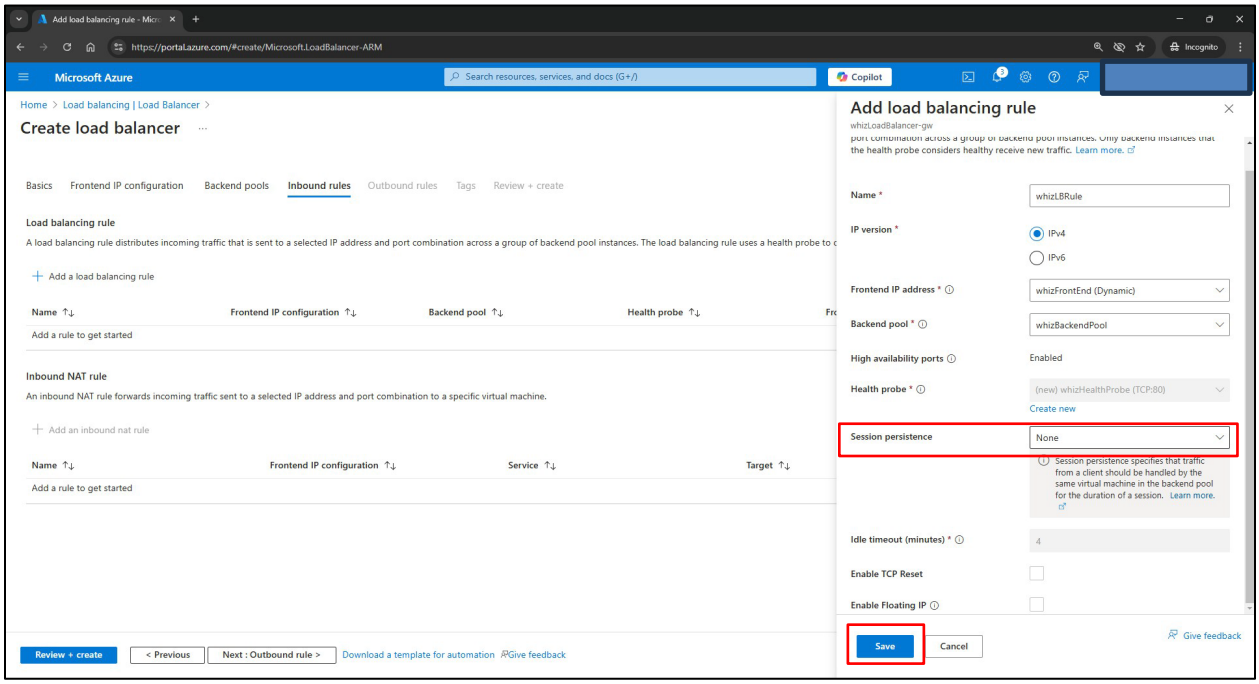
- Name: Enter ***whizLBRule***
- IP Version: Select **IPv4 or IPv6** depending on your requirements.
- Frontend IP address: Select **whizFrontEnd**
- Backend pool: Select **whizBackendPool**
- Health probe: Select **Create new**



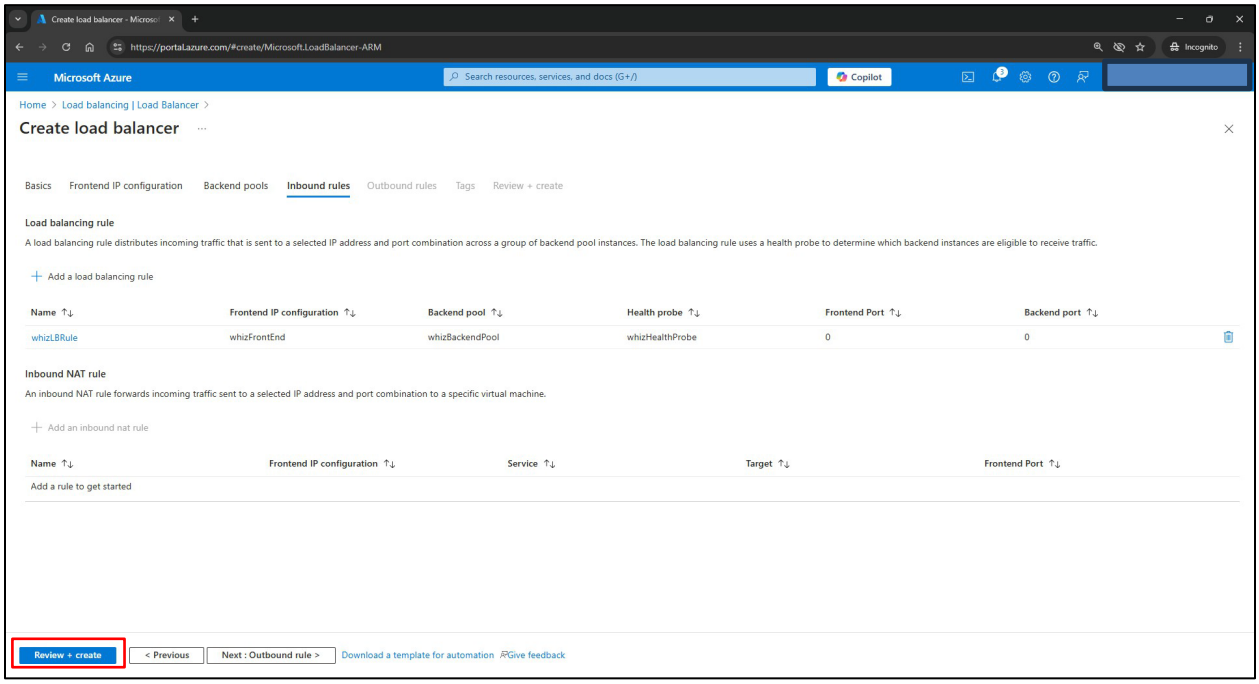
- Name: enter ***whizHealthProbe***
- Select **TCP** in Protocol.
- Leave the rest of the defaults, and select **Save.**



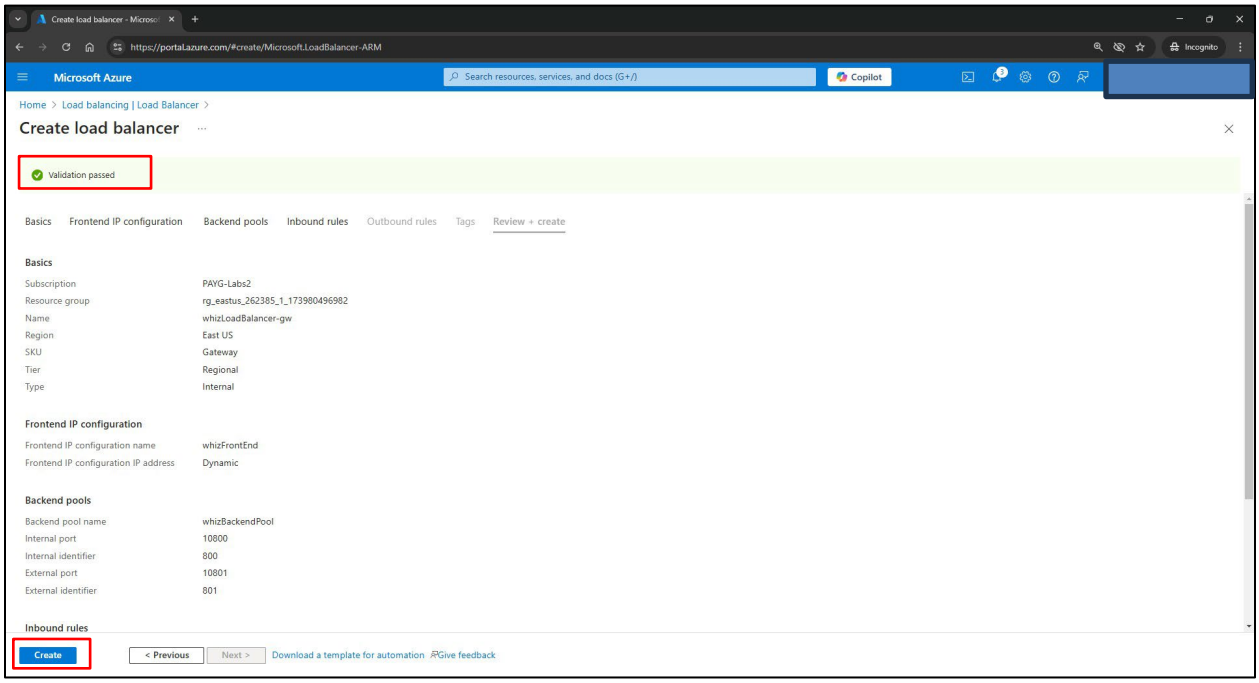
Session persistence: Select **None**
Select **Save**



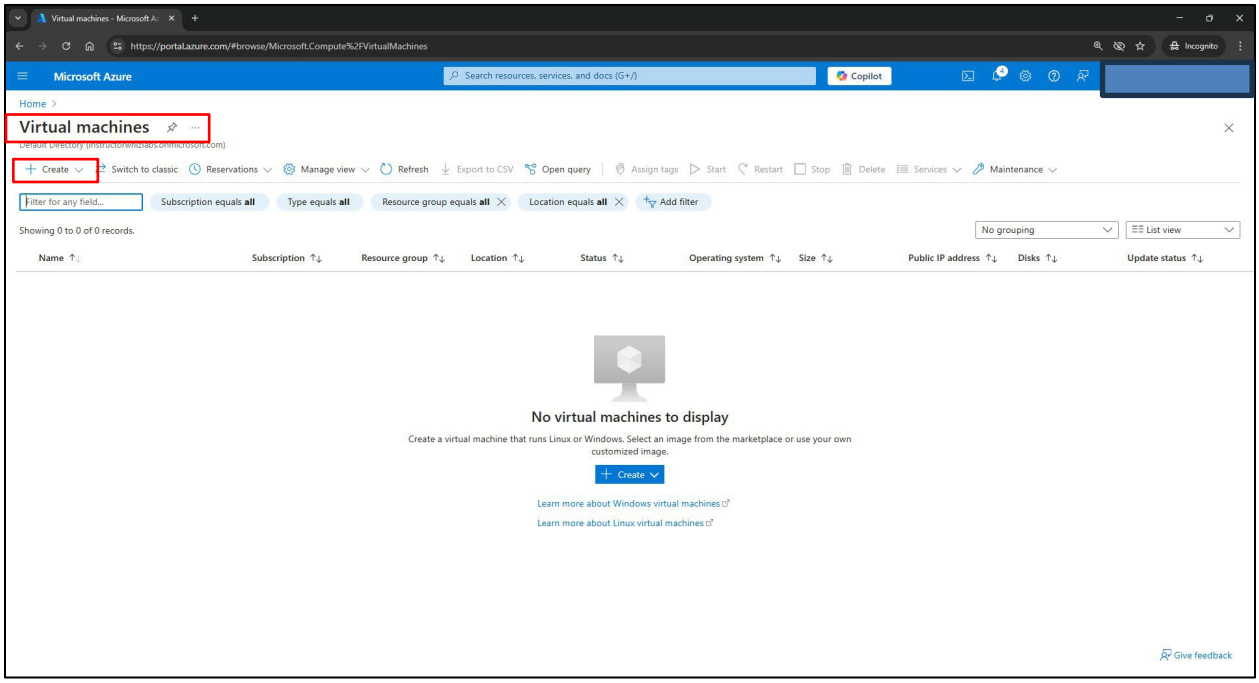
Select **Review + Create**



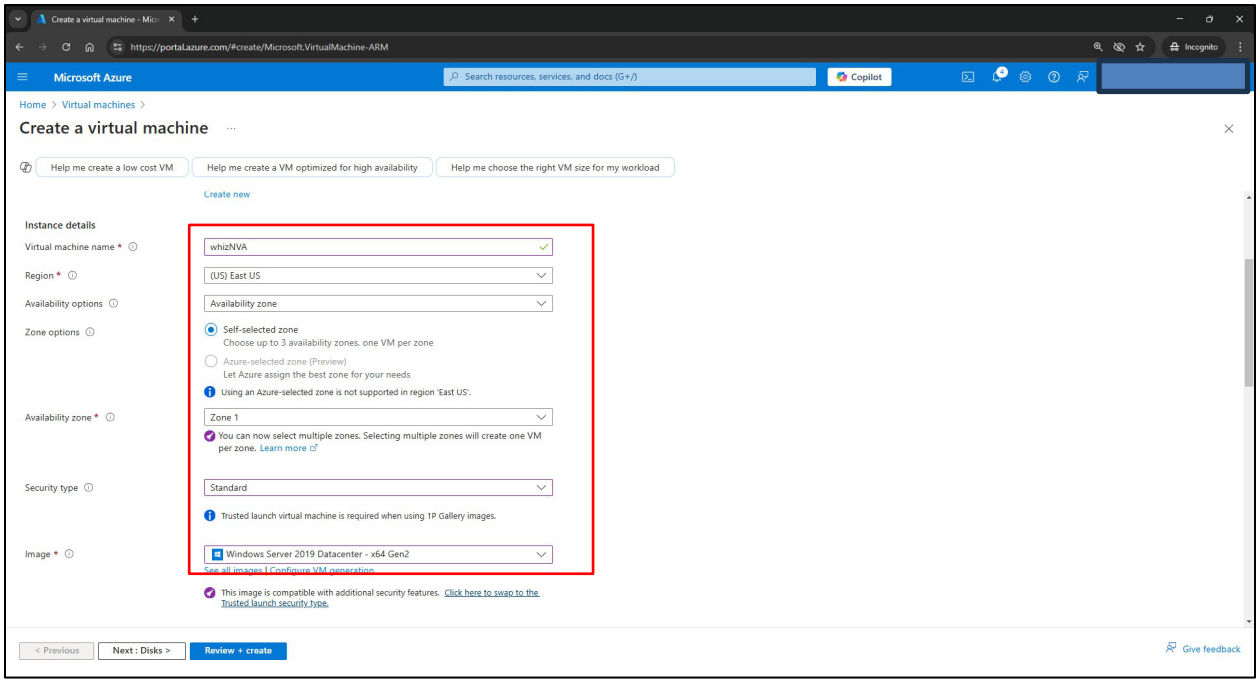
Validation passed
Select **Create**



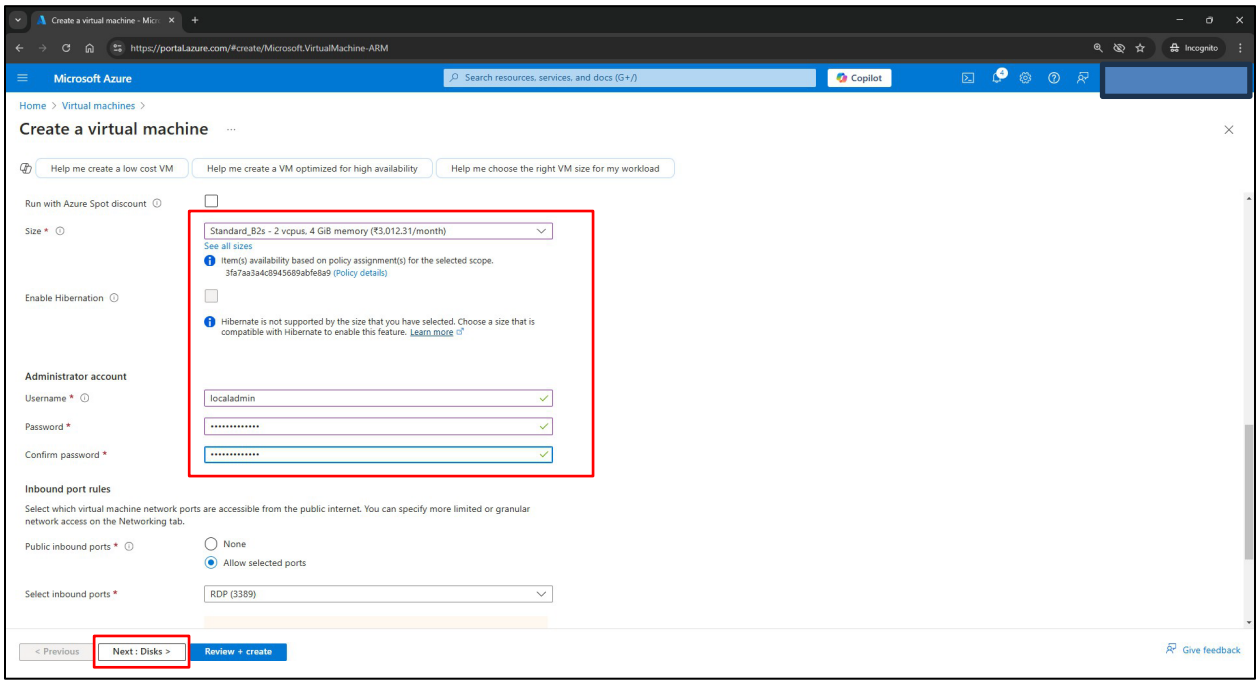
Navigate to **Virtual Machines**
Select **+ Create**



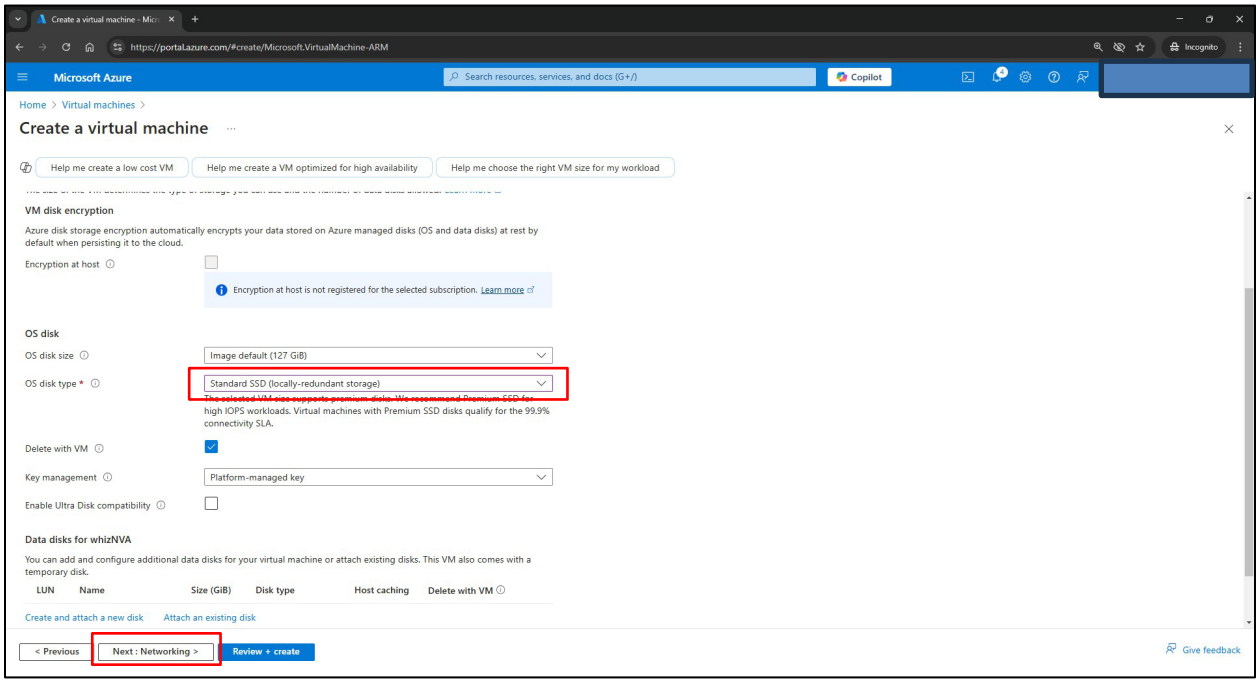
Virtual machine name: **whizNVA**
Region: **East US**
Security type: **Standard**
Image: **Windows Server 2019 Datacenter – x64 Gen 2**
Scroll down



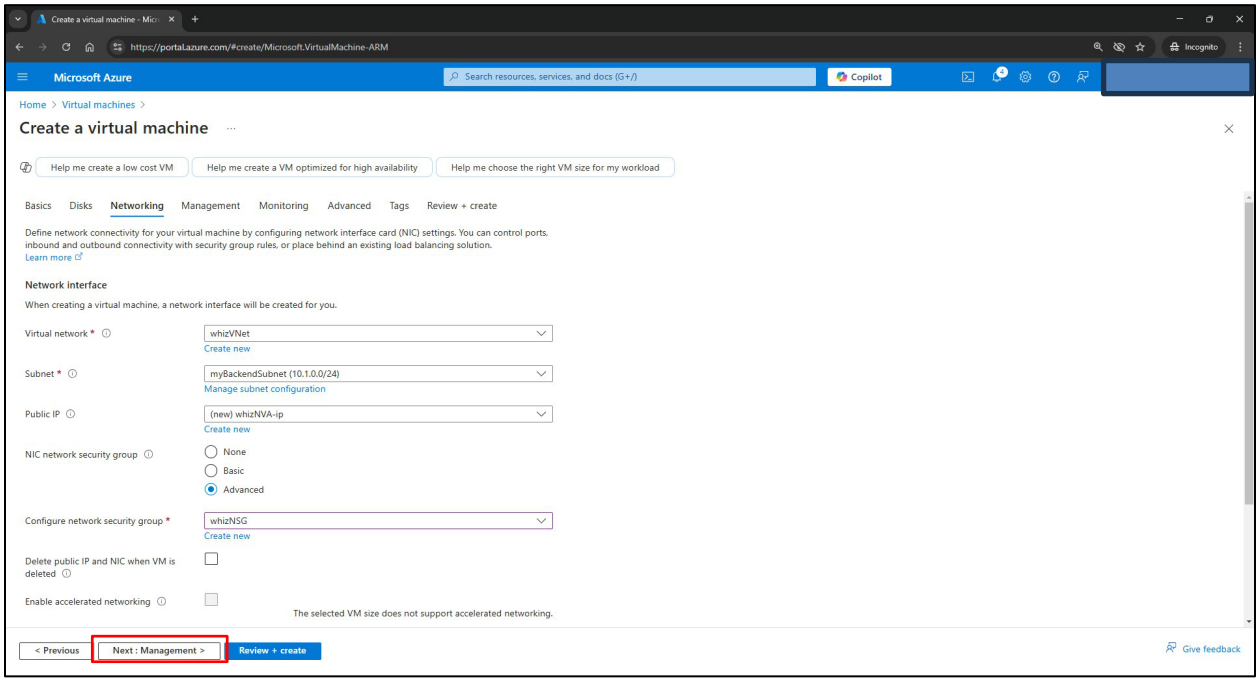
Size: **Standard_B2**
Username: **localadmin**
Password: **Password12345**
Select **Disks**



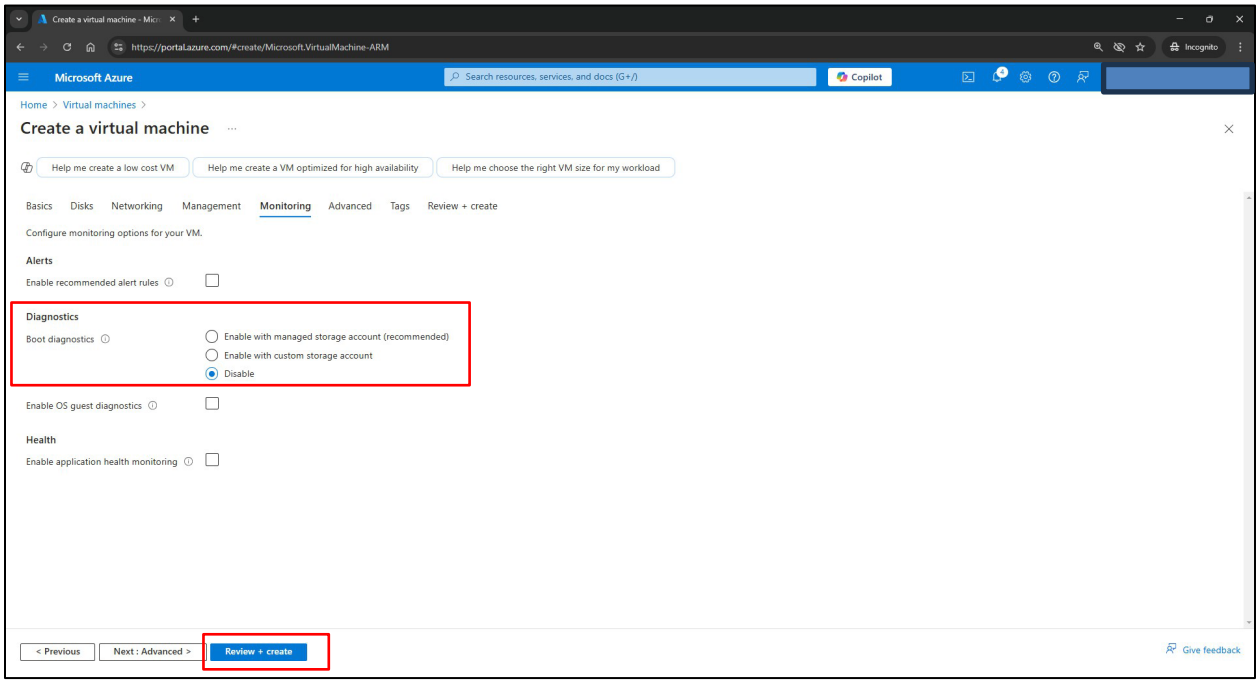
OS disk type: **Standard SSD**
Select **Networking**



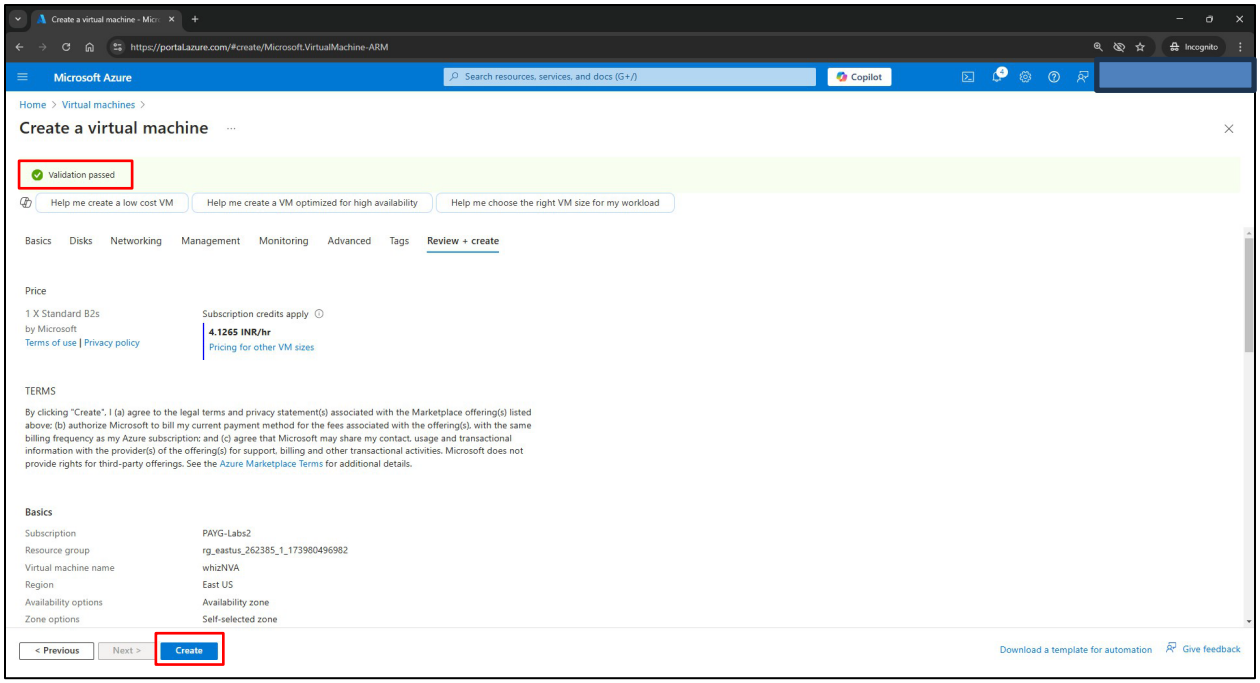
Select **Next: Management**



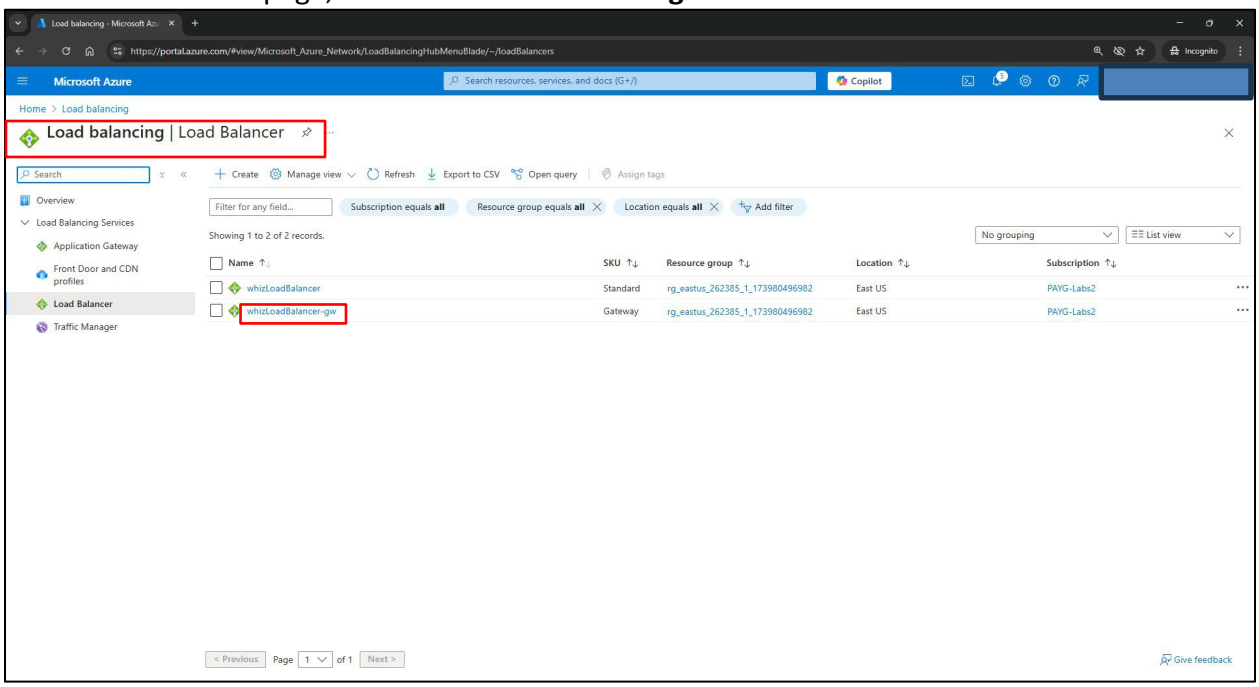
Diagnostics, Boot Diagnostics, select **Disable**
Select **Review + Create**



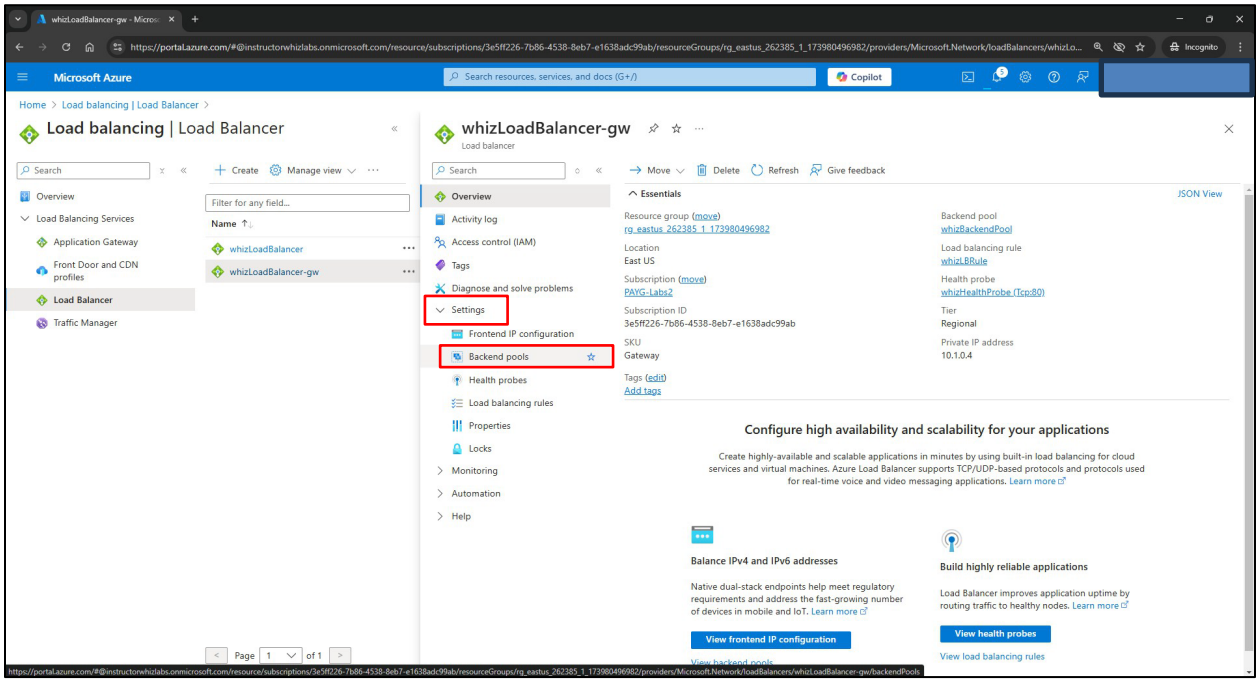
Validation Passed
Select **Create**



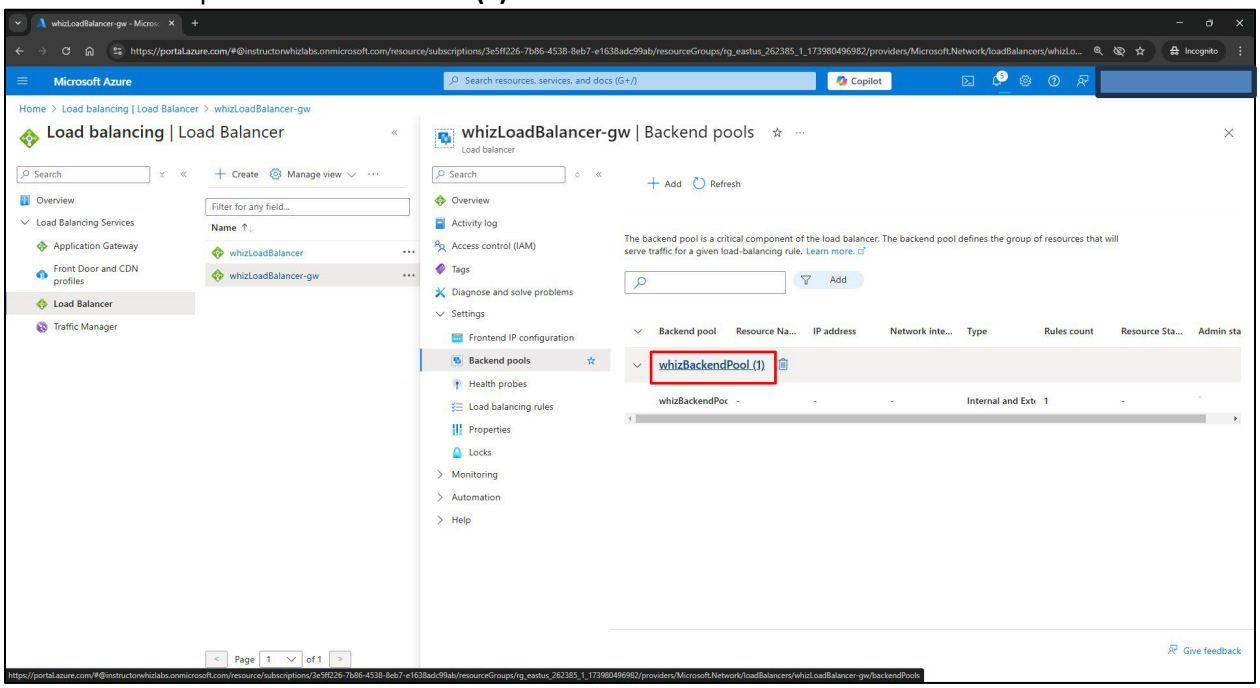
From Load Balancer page, select **whizLoadBalancer-gw**



Select **Settings** drop down
Select **Backend pools**

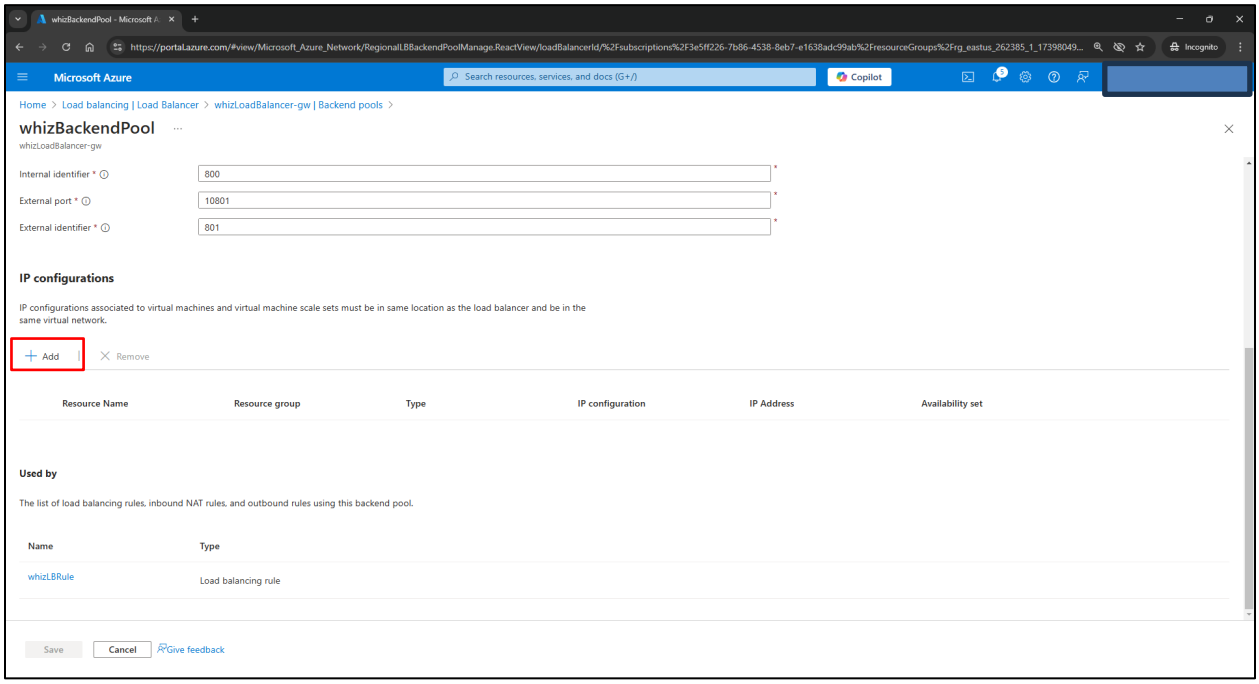


Select Backend pool **whizBackendPool(1)**

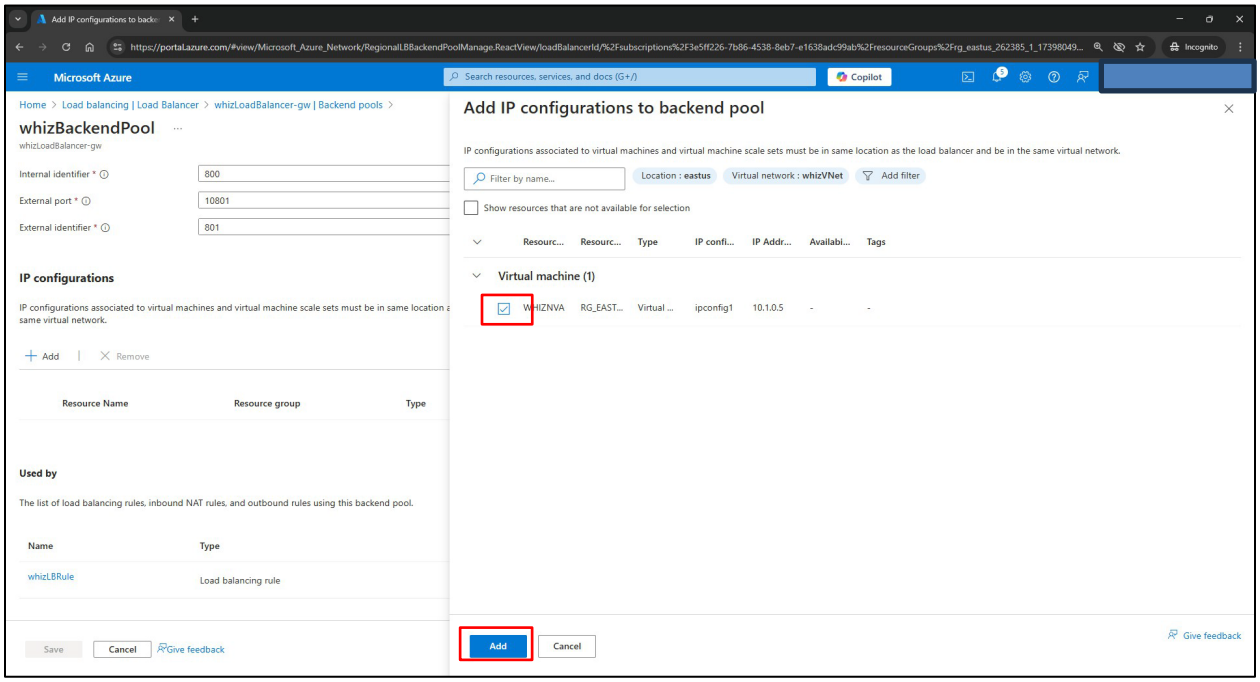


Scroll down

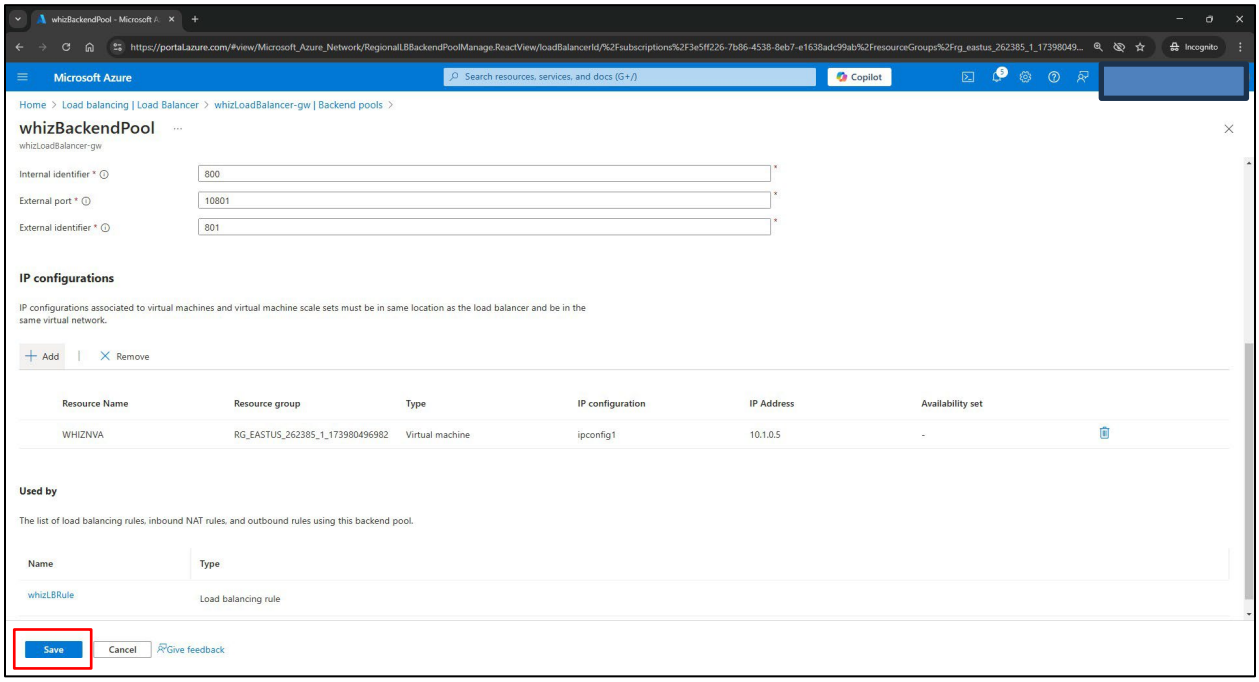
Under **IP configuration**, select **+ Add**



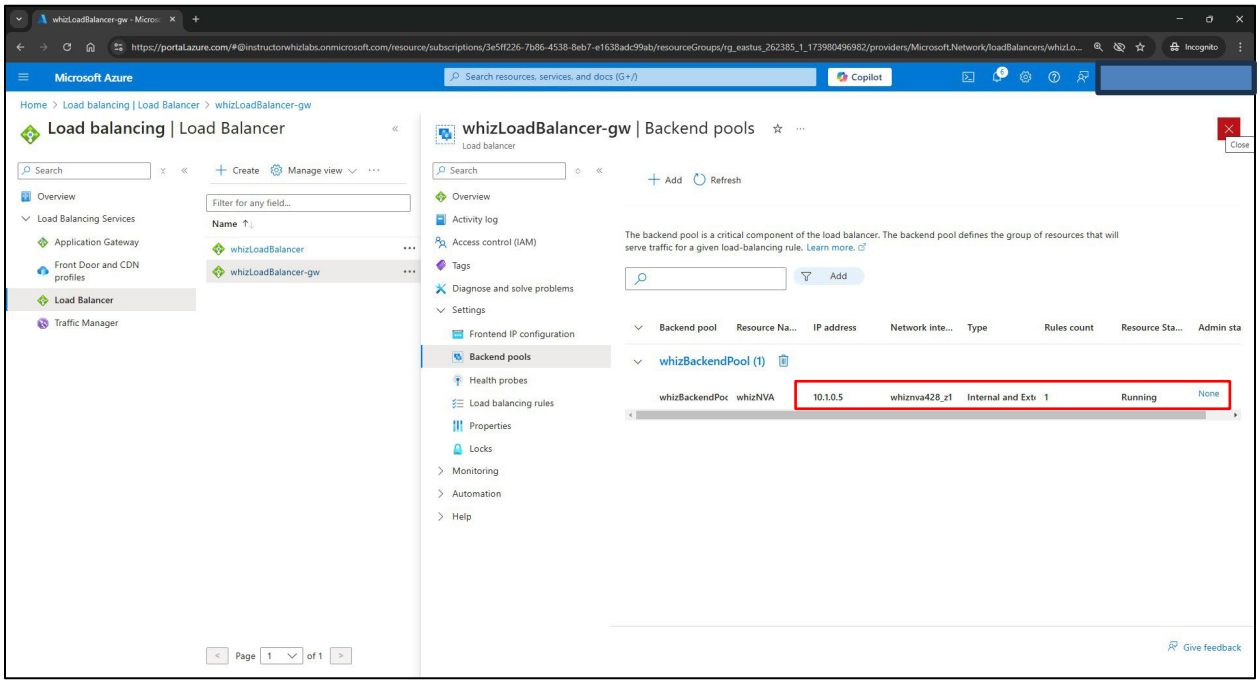
Select checkbox next to **WHIZNVA**
Select **Add**



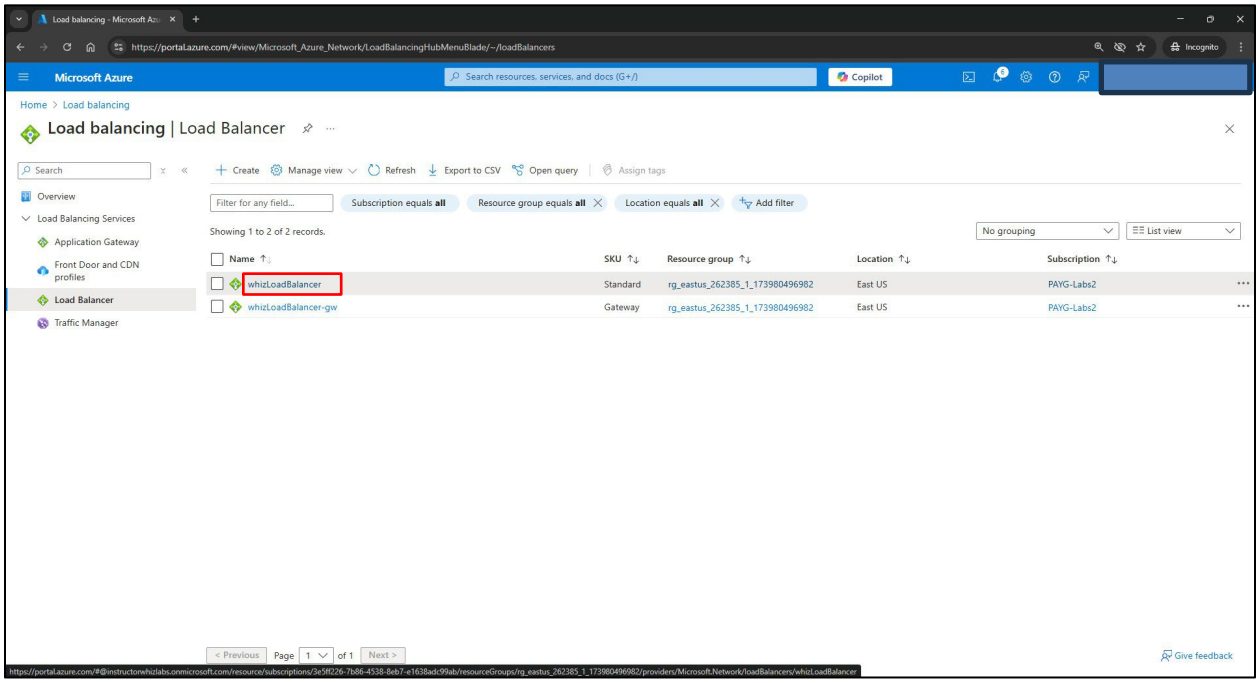
Select **Save**



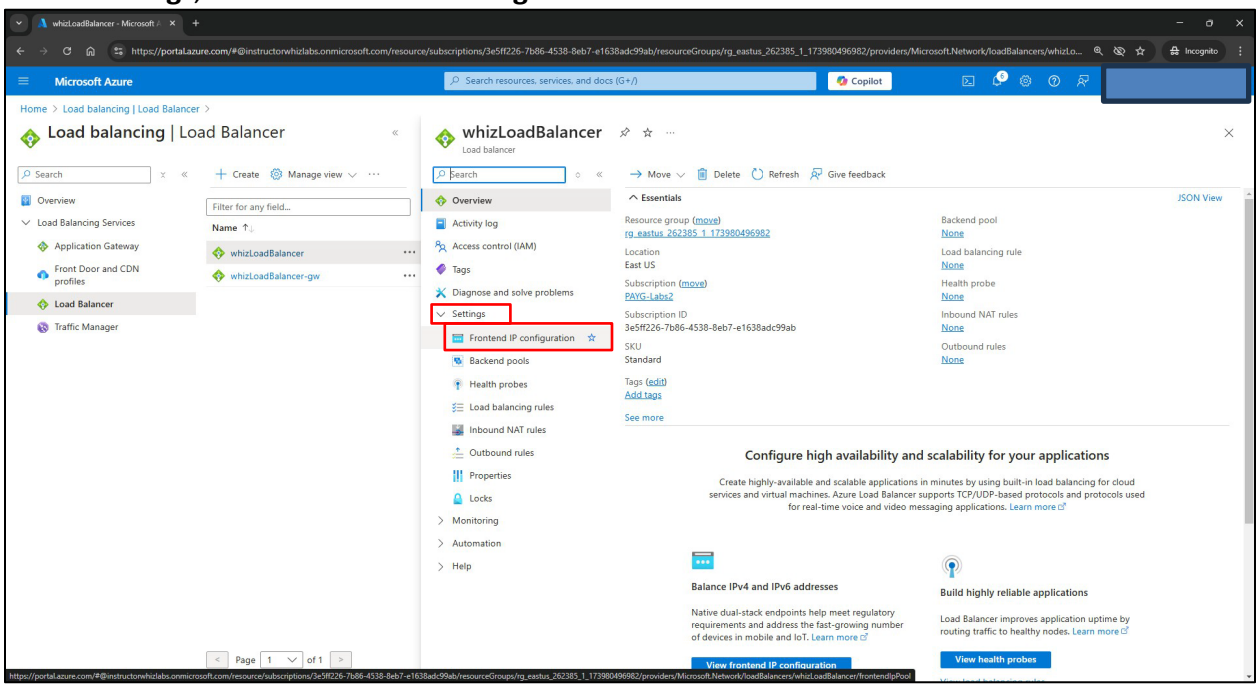
Added to the **whizBackendPool**



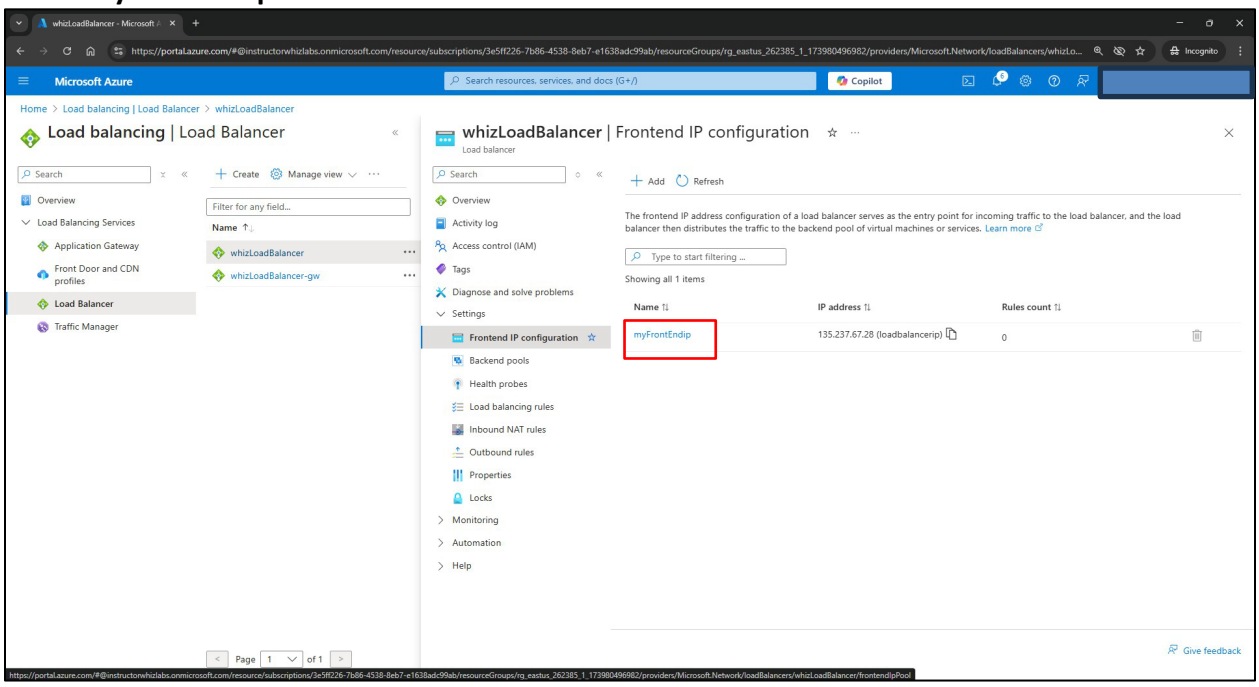
Select **whizLoadBalancer**



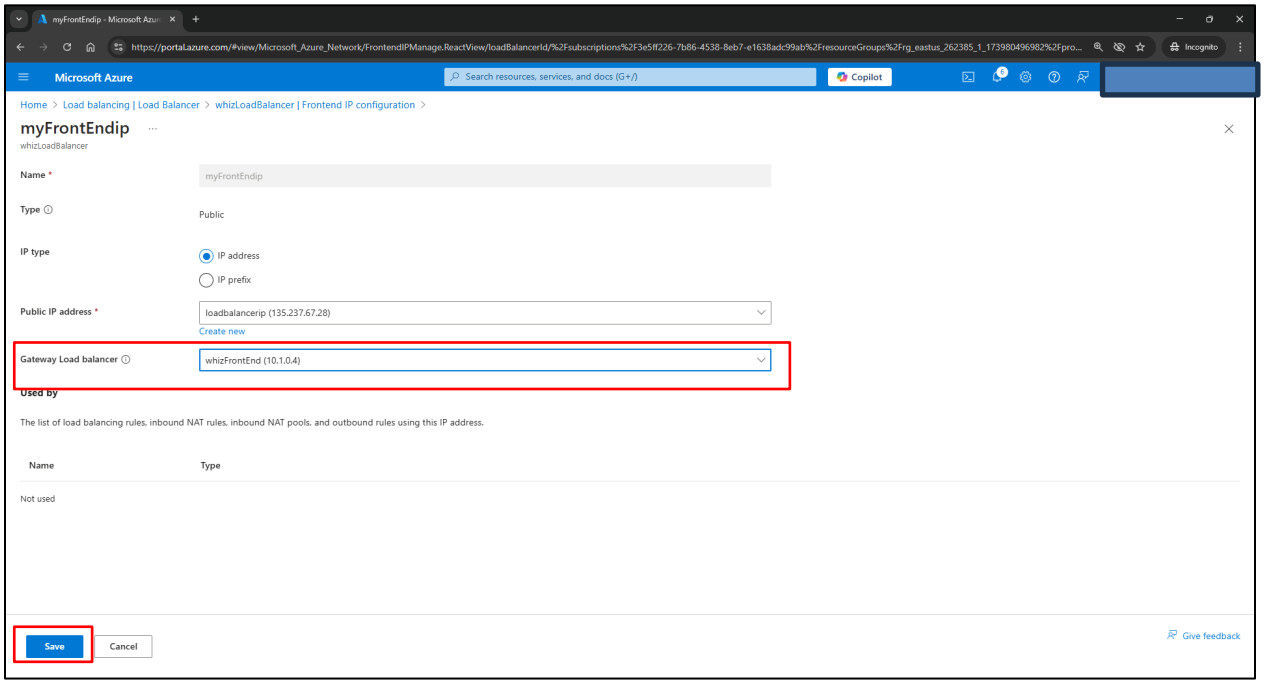
Under **Settings**, select **Frontend IP configuration**



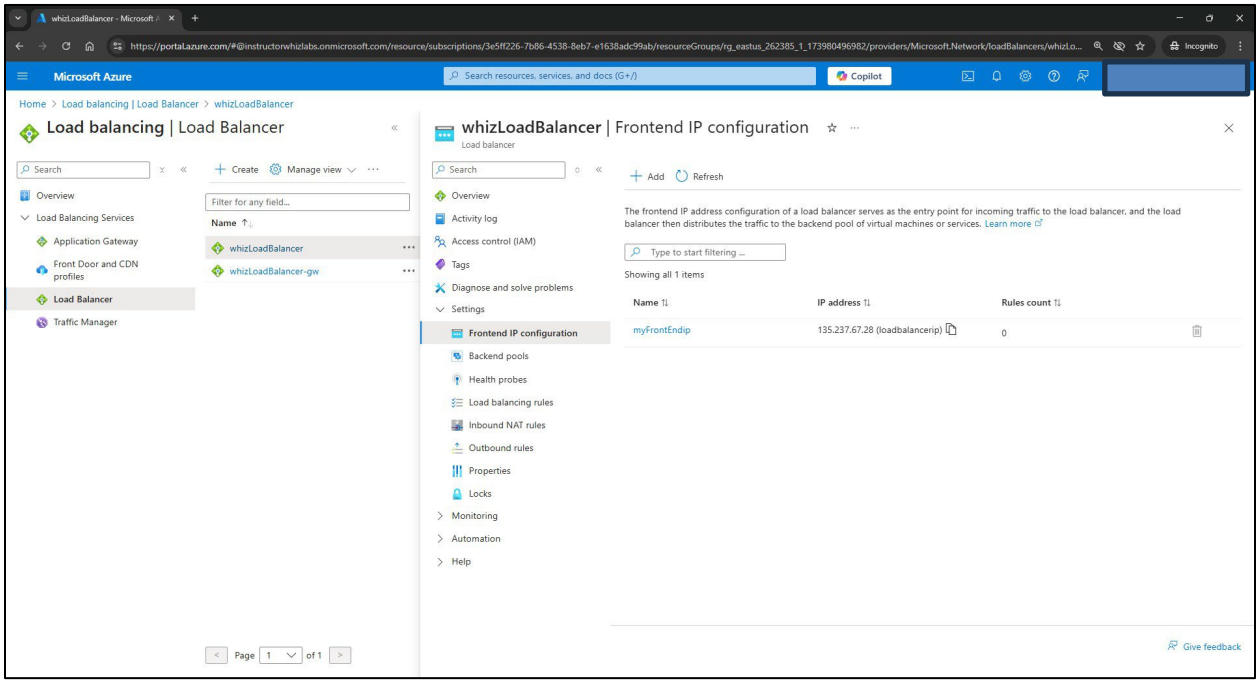
Select **myFrontEndip**



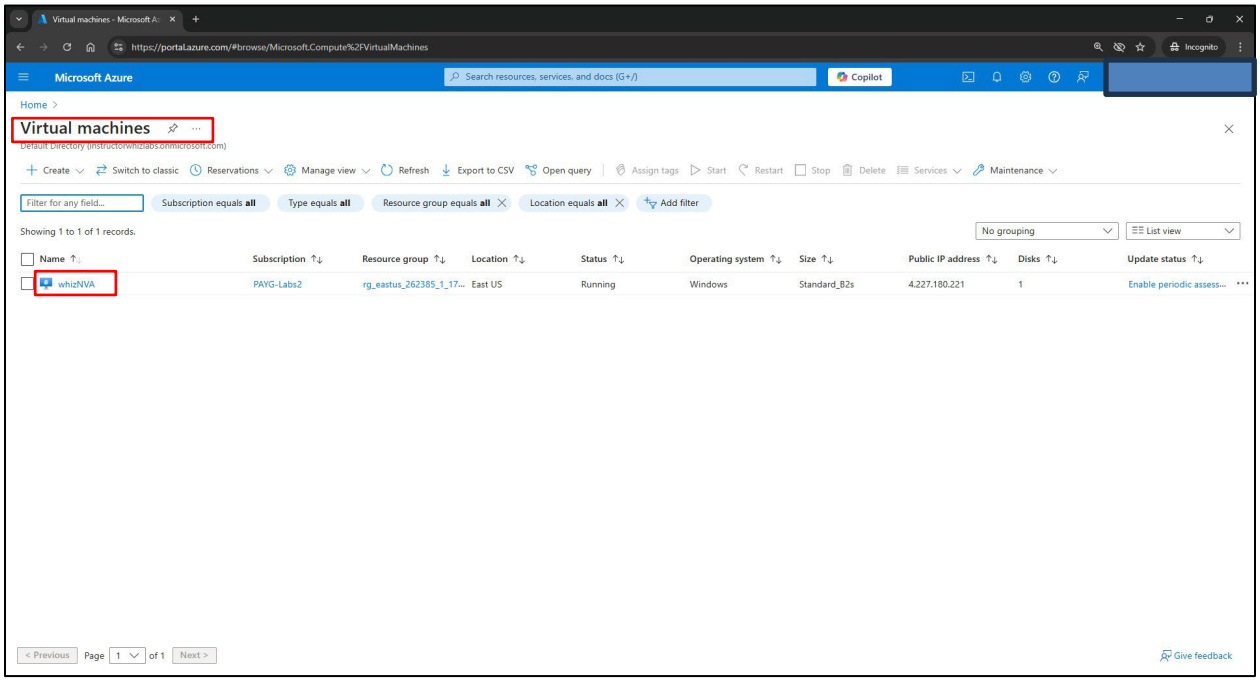
Select drop down next to **Gateway Load balancer**
Select **whizFrontEnd (10.1.0.4)**
Select **Save**



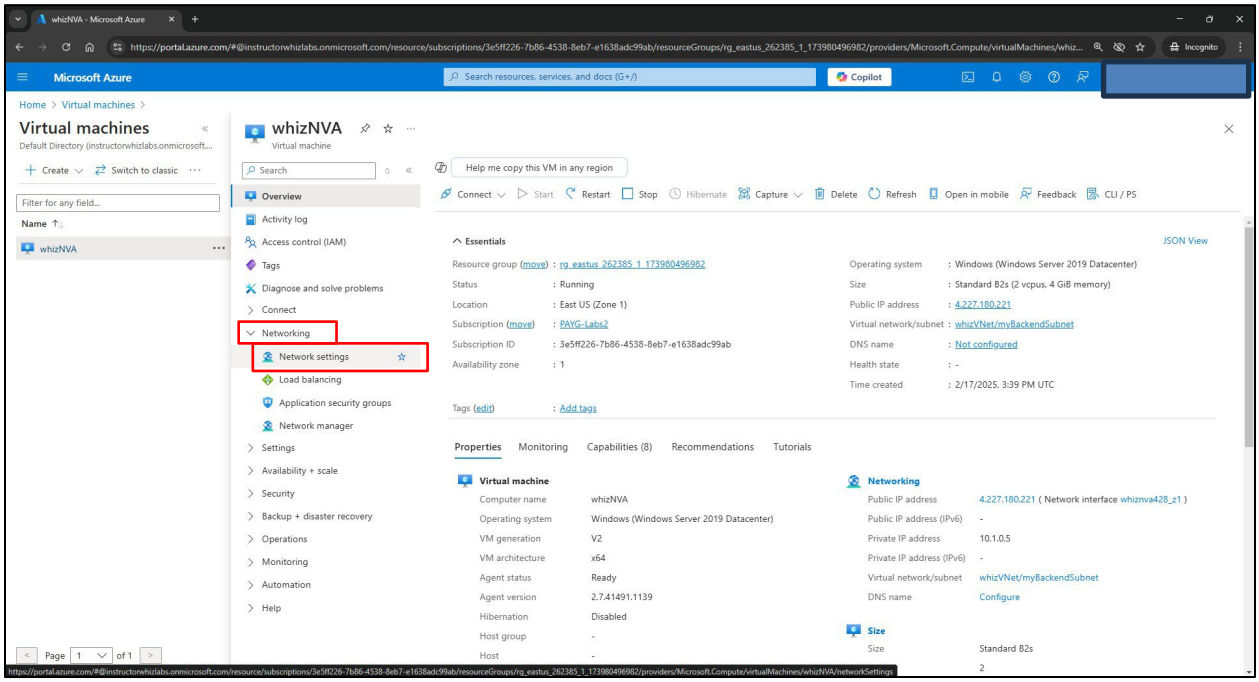
myFrontEndip added to the **Frontend IP configuration**



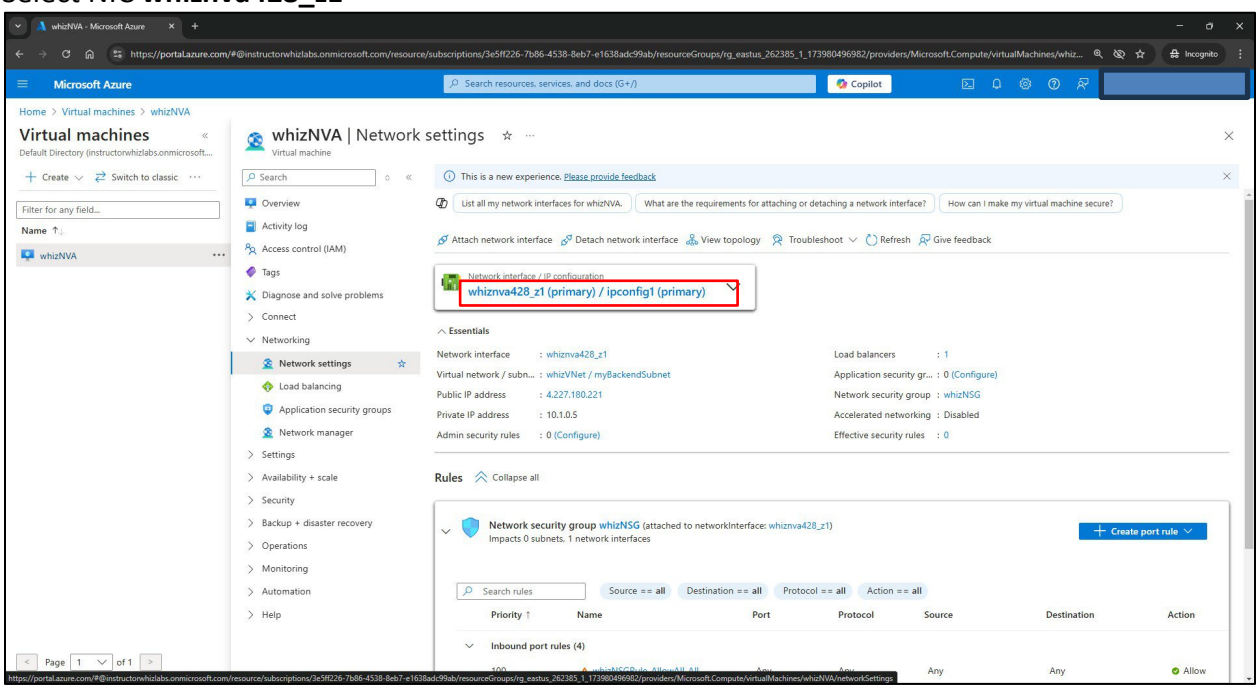
Navigate to **Virtual Machines**
Select **whizNVA**



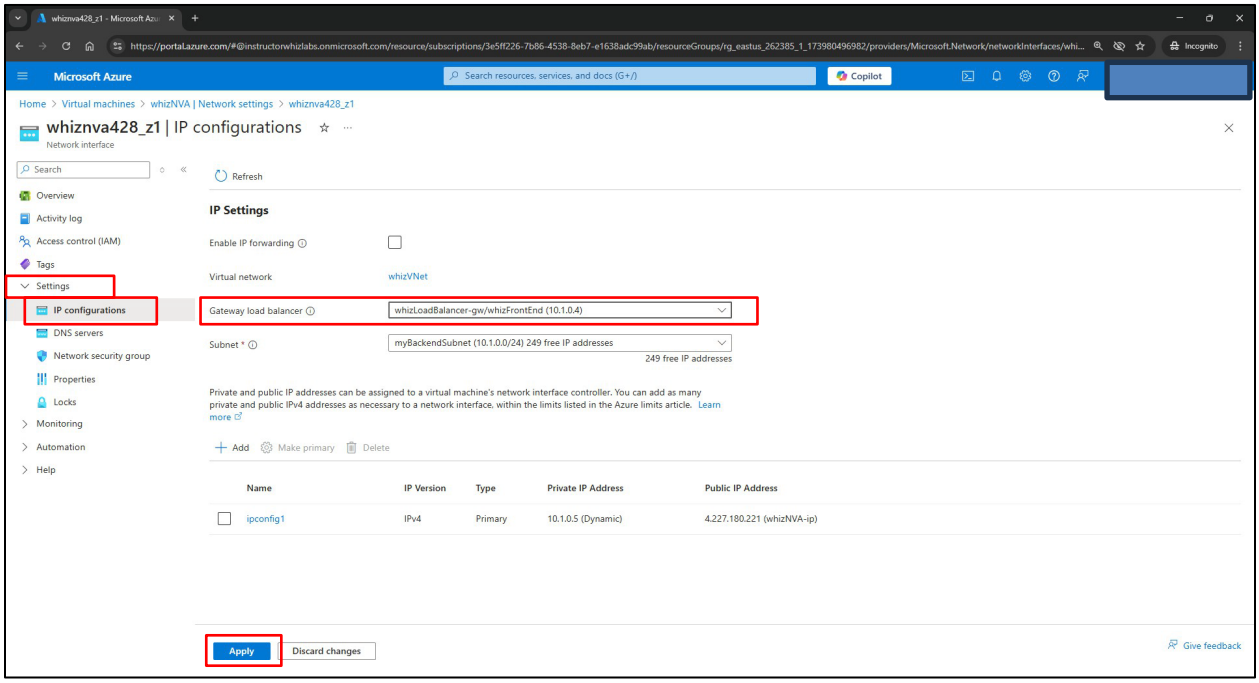
Under **Networking** tab, select **Network settings**



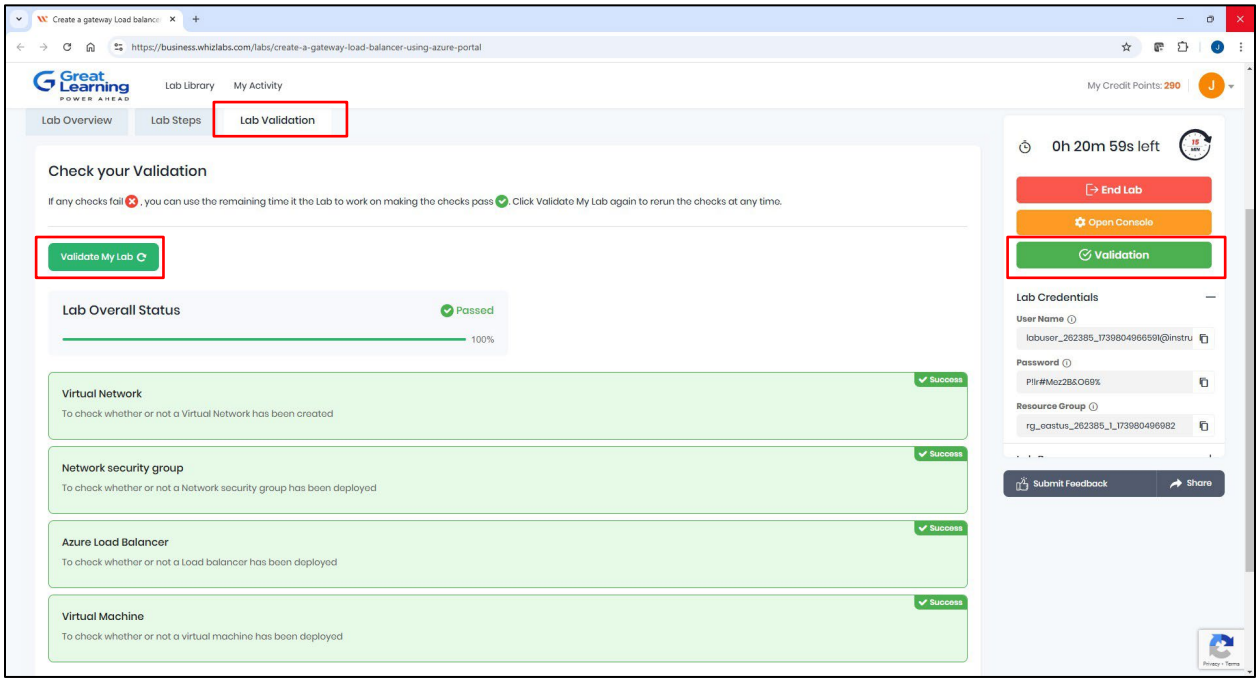
Select NIC **whiznva428_z1**



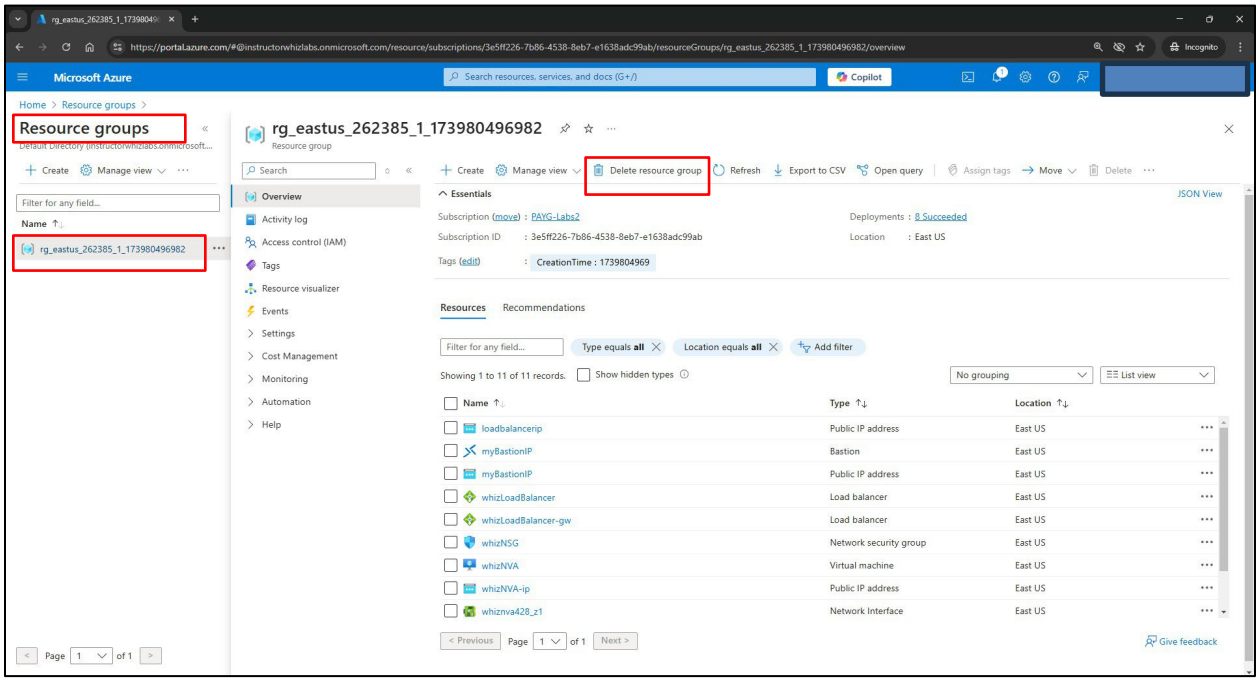
Under **Settings** drop down, select **IP configuration**
Under **Gateway load balancer,** select drop down for **whizLoadBalancer-gw/whizFrontEnd**
Select **Apply**



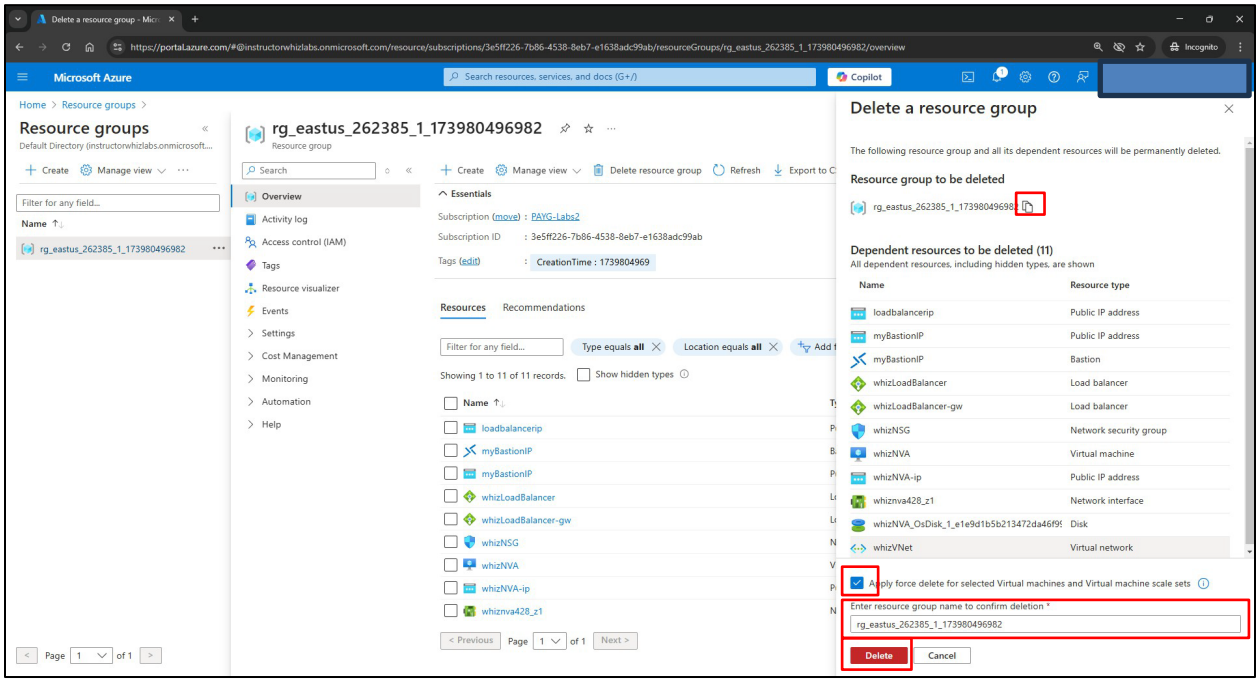
Navigate to **Lab Validation** tab
Select **Validation**
Select **Validate My Lab**



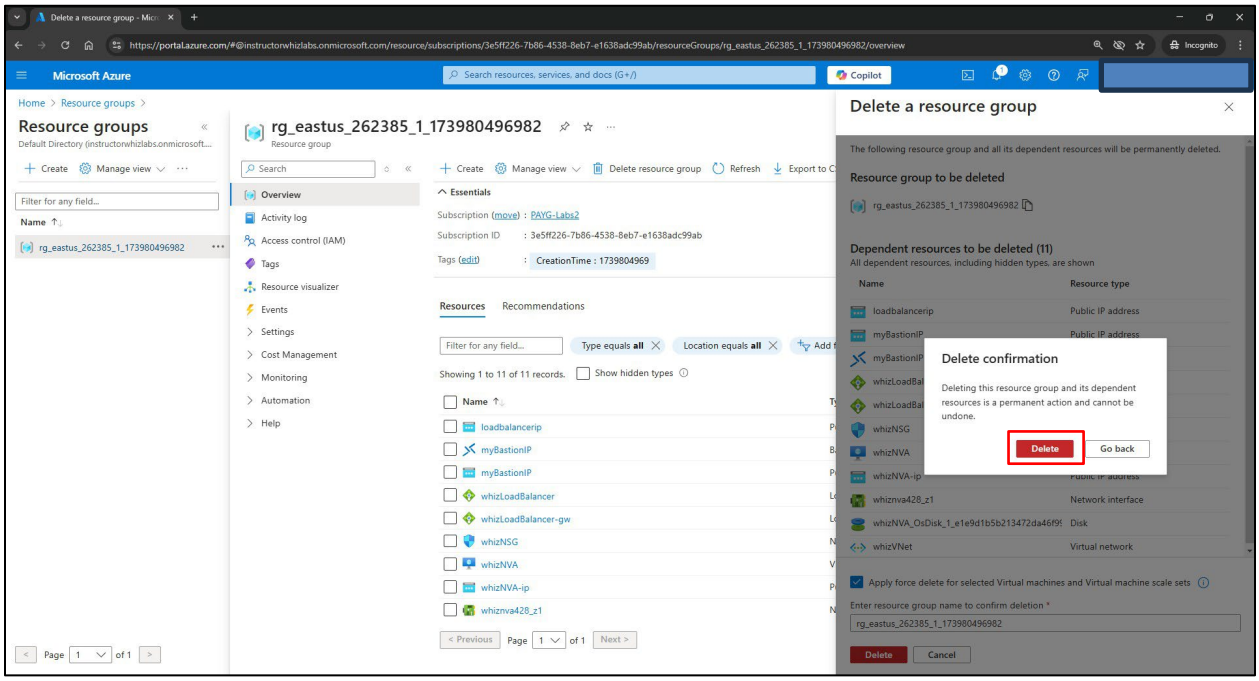
Navigate to **Resource Groups**
Select Resource group **rg_eastus_262385_1_1739804496982**
Select **Delete resource group**



Copy / past Resource Group name in **Enter resource group name to confirm deletion** box
Select checkbox next to **Apply force delete for selected Virtual machines and Virtual machine scale sets**
Select **Delete**



Select **Delete**



Normally, would delete everything, but Business WhizLabs does not allow us to delete Resource Groups