Portfolio Lab Report By THATO KGOLE
Date: November 2025
Cloud PlatForm: Microsoft Azure

OVERVIEW

This lab demonstrates the configuration and security setup of an Azure Virtual Network environment with multiple subnets, Network Security Groups, and connected Virtual Machines.
The goal was to simulate a real-world enterprise network that securely manages internal communication between application tiers

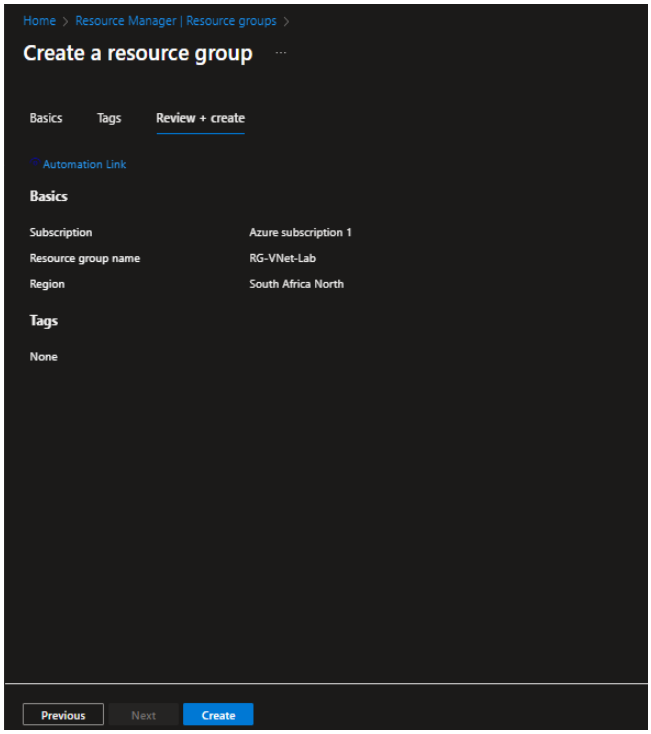
PROBLEM STATEMENT

In cloud environments, multiple services such as virtual machines, databases, and web applications must communicate efficiently and securely.
Without proper network design, services may be exposed to public access or experience internal connection failures

This project explores how to design, configure, and secure Azure Virtual Network to ensure controlled internal communication between resources using subnets and security boundaries.

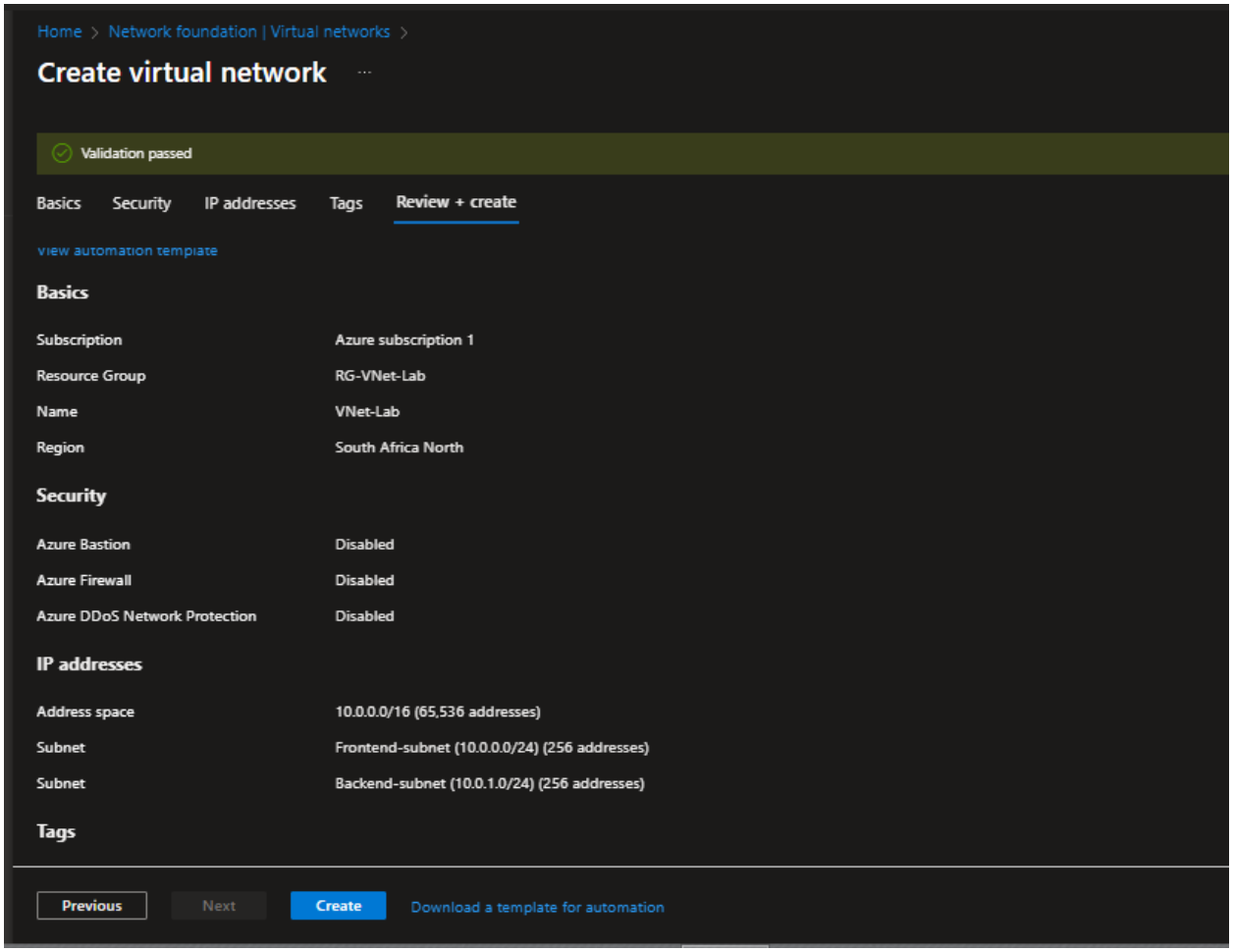
Step 1: Create a Resource Group

This acts as a logical container for all the lab's resources.
In the Azure Portal, navigate to Resource Groups and create one.



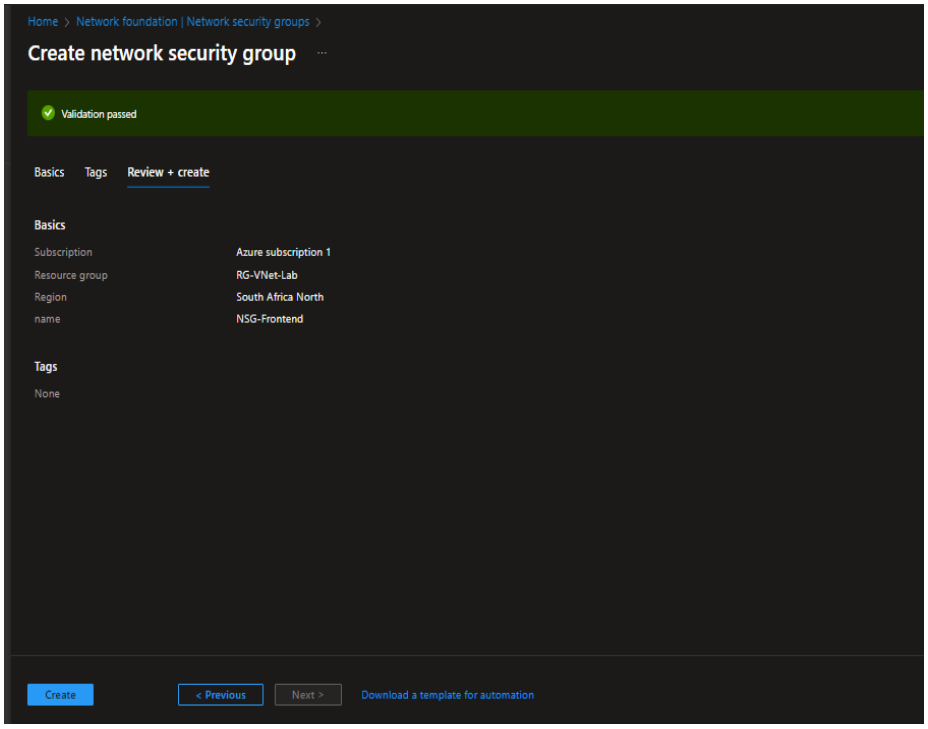
Step 2: Create a Virtual Network (VNet)

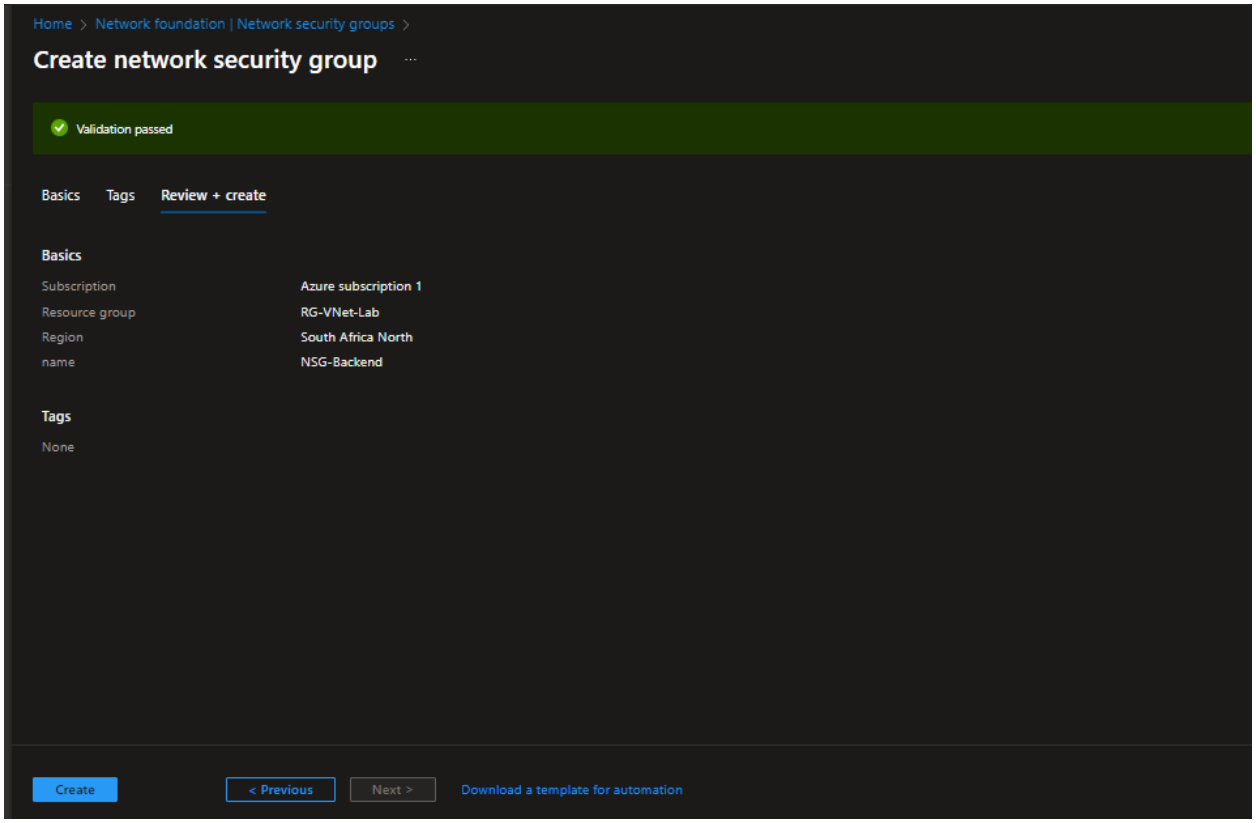
Go to Networking - Virtual Networks and create a new Vnet.
Define two subnets – Frontend and Backend
Ensure both subnets have non-overlapping IP ranges to prevent routing conflicts.



Step 3: Create Network Security Groups

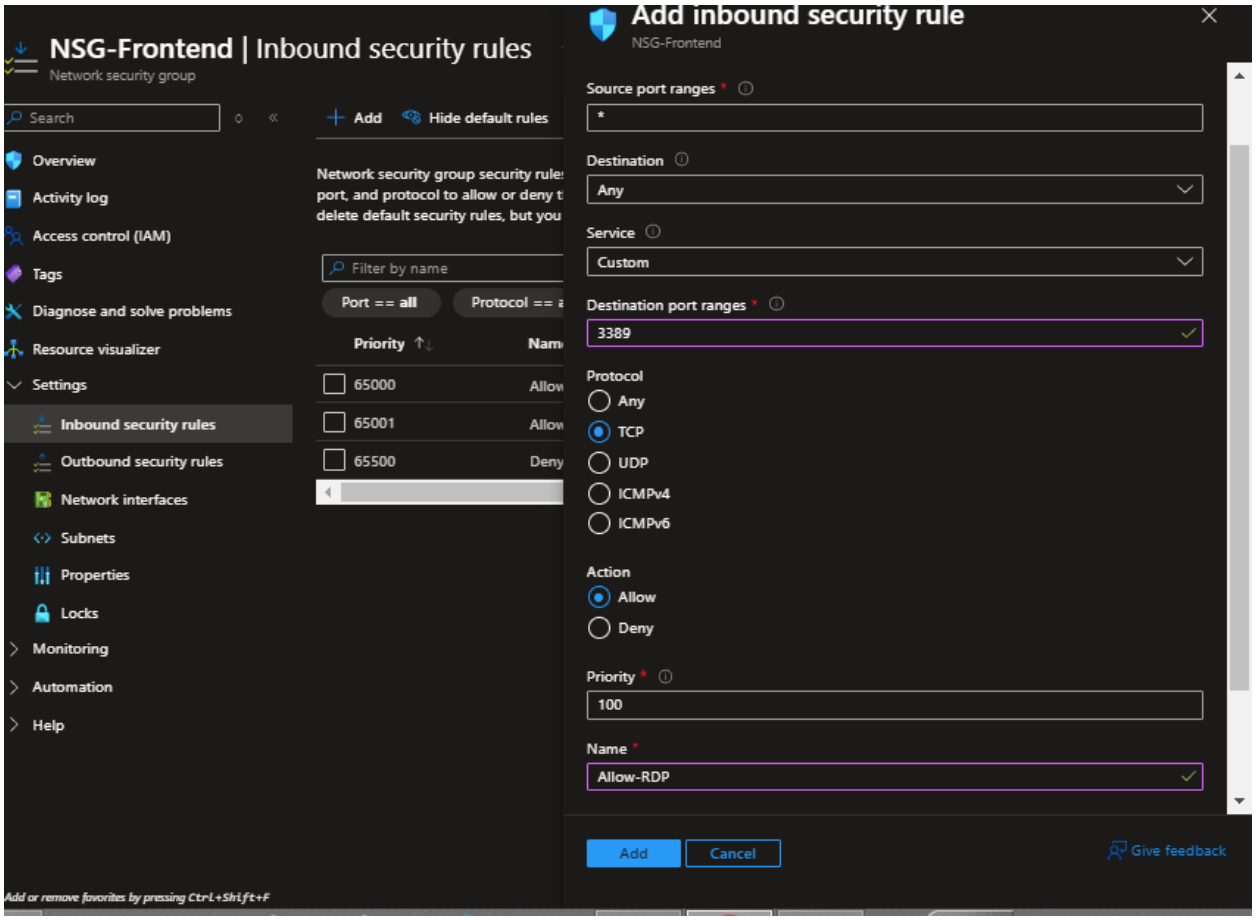
Create two NSGs - one for each subnet
Frontend-NSG
Backend-NSG





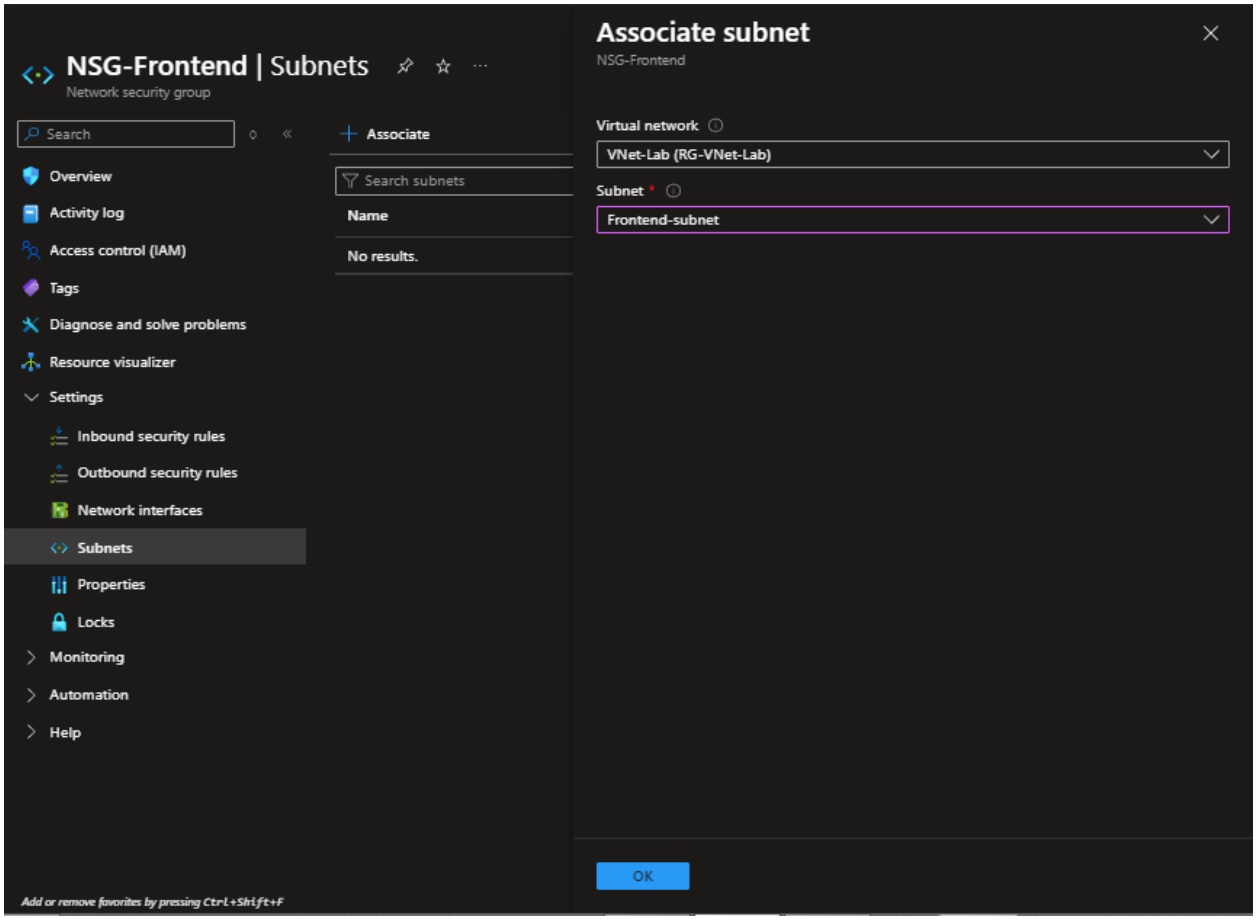
Step 4: Configure NSG Rules

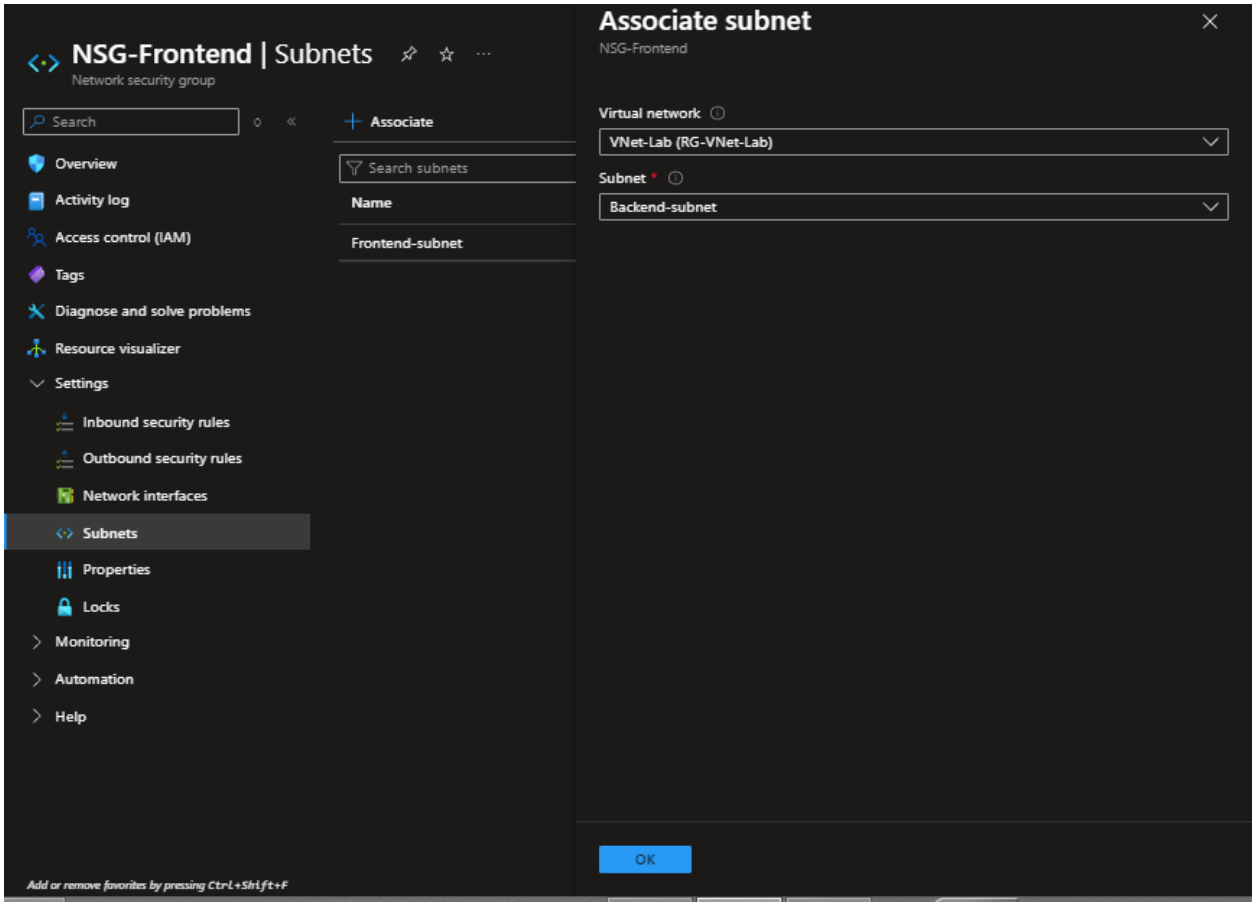
Inbound rule: Allow RDP (port 3389) to the Frontend subnet for administrative access
Outbound rule: Restrict the Backend subnet to only receive traffic from the Frontend subnet



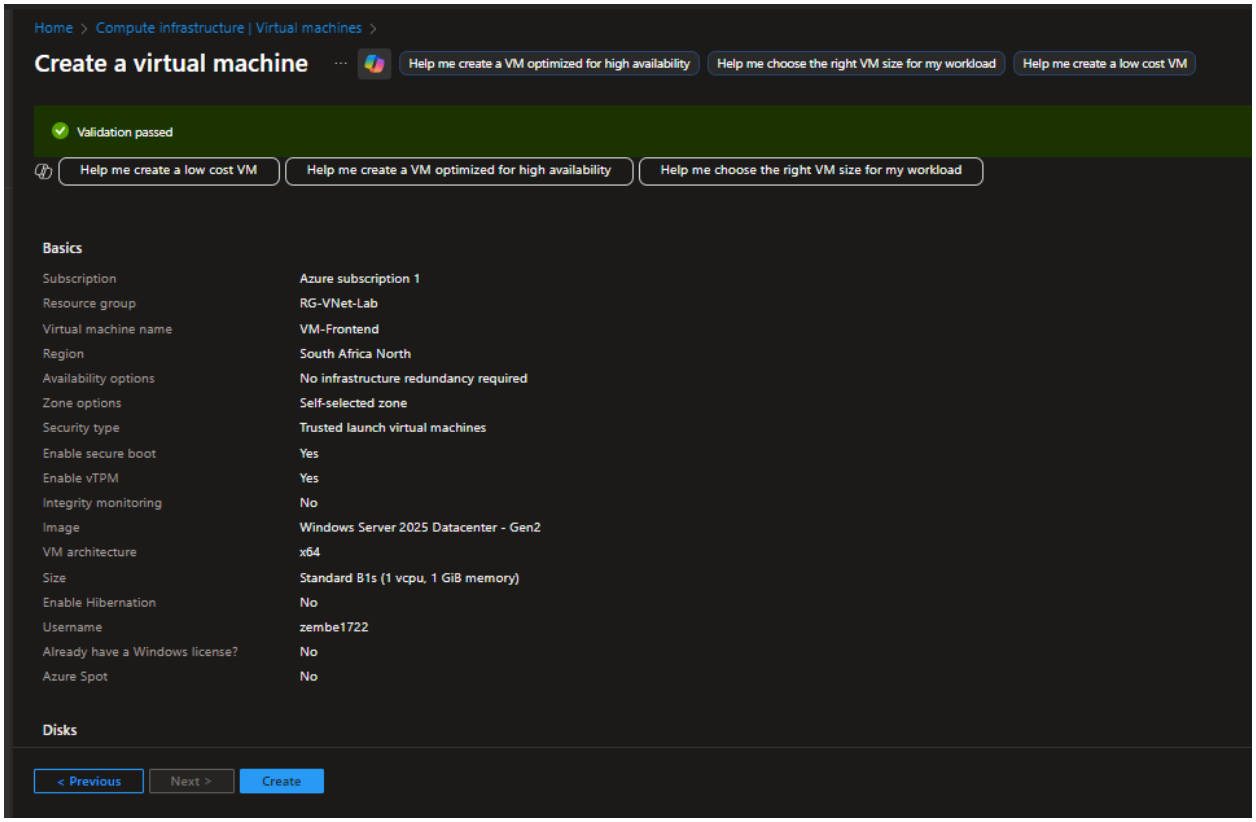
Step 5: Associate NSGs with subnets

Associate each NSG with its corresponding subnet to apply network rules.
This ensures traffic policies are applied automatically to all resources deployed within those subnets


NSG-Frontend | Subnets
Network security group
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Monitoring
Automation
Help
Add or remove favorites by pressing Ctrl+Shift+F
Associate
Search subnets
Name
No results.
Associate subnet
NSG-Frontend
Virtual network
VNet-Lab (RG-VNet-Lab)
Subnet *
Frontend-subnet
OK

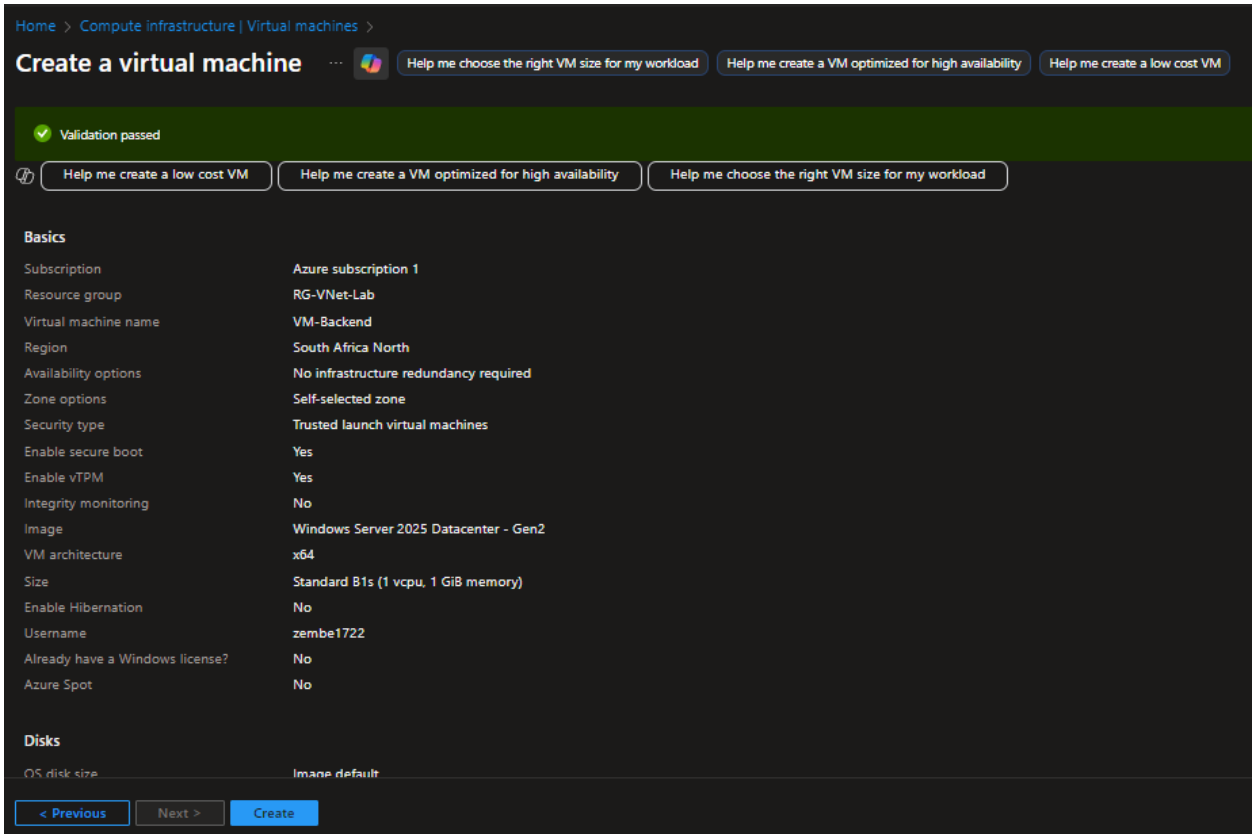


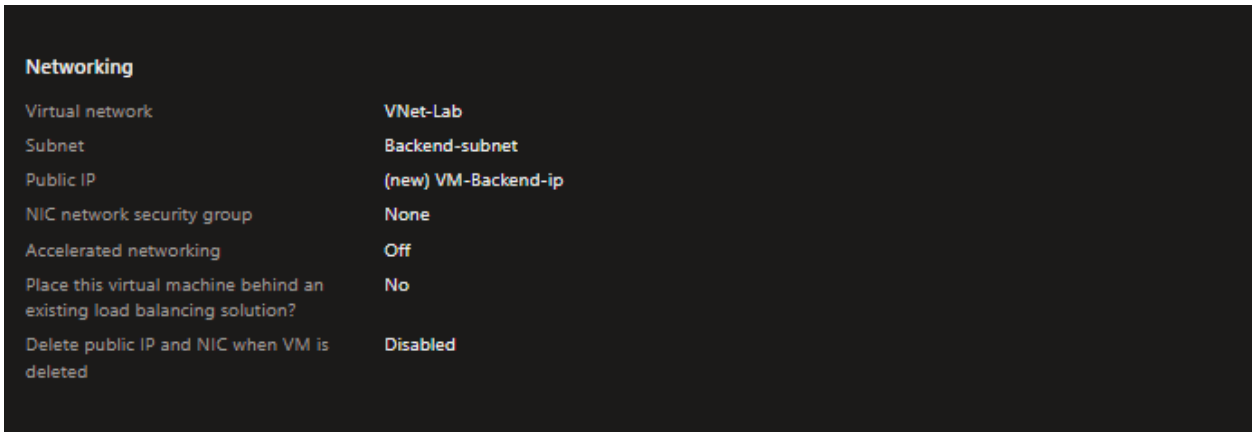
Step 6: Create two Virtual Machines


Home > Compute infrastructure | Virtual machines >
Create a virtual machine
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Help me create a low cost VM
Validation passed
Help me create a low cost VM
Help me create a VM optimized for high availability
Help me choose the right VM size for my workload
Basics
Subscription Azure subscription 1
Resource group RG-VNet-Lab
Virtual machine name VM-Frontend
Region South Africa North
Availability options No infrastructure redundancy required
Zone options Self-selected zone
Security type Trusted launch virtual machines
Enable secure boot Yes
Enable vTPM Yes
Integrity monitoring No
Image Windows Server 2025 Datacenter - Gen2
VM architecture x64
Size Standard B1s (1 vcpu, 1 GiB memory)
Enable Hibernation No
Username zembe1722
Already have a Windows license? No
Azure Spot No
Disks
< Previous
Next >
Create


Networking
Virtual network VNet-Lab
Subnet Frontend-subnet
Public IP (new) VM-Frontend-ip
NIC network security group None
Accelerated networking Off
Place this virtual machine behind an existing load balancing solution? No
Delete public IP and NIC when VM is deleted Disabled

.FRONTEND VM



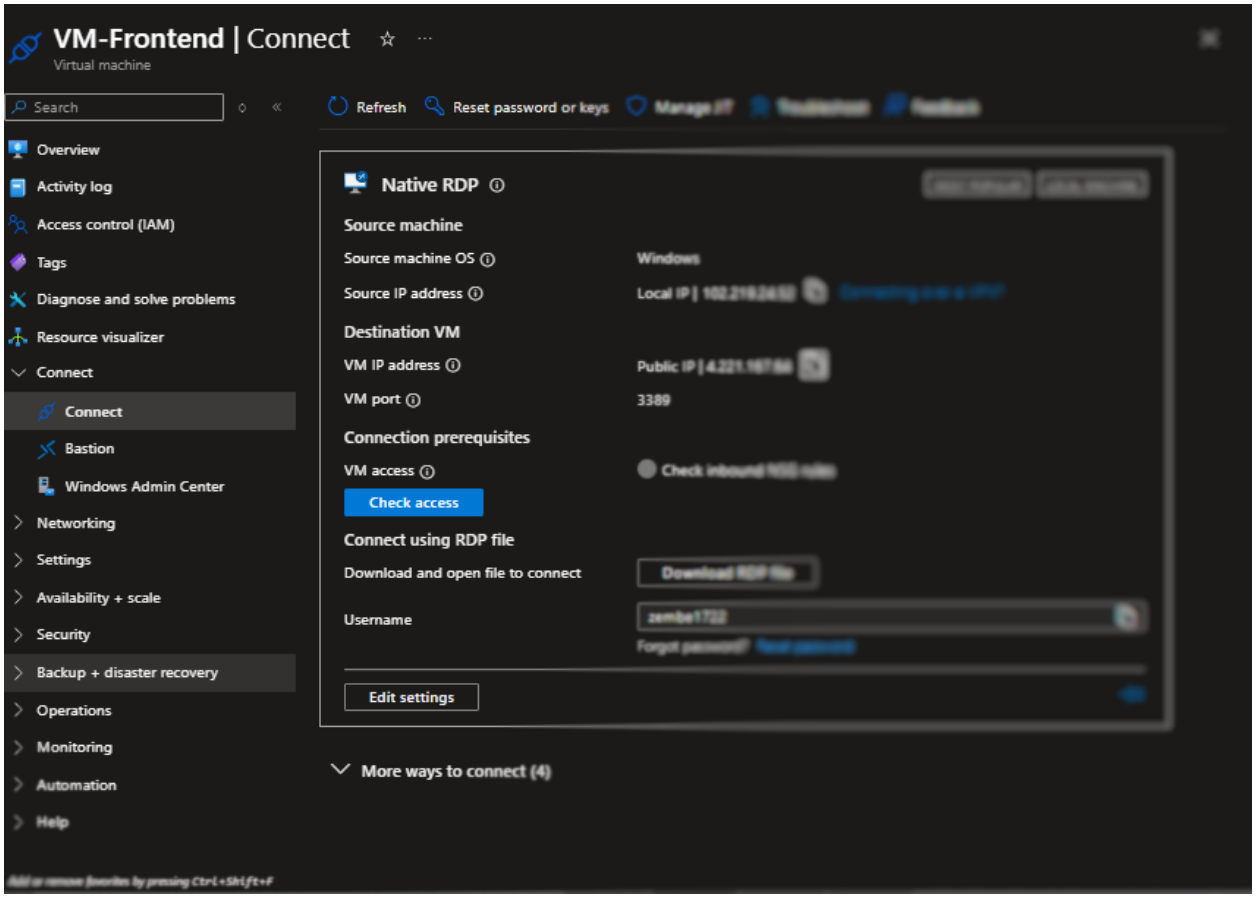


.BACKEND VM

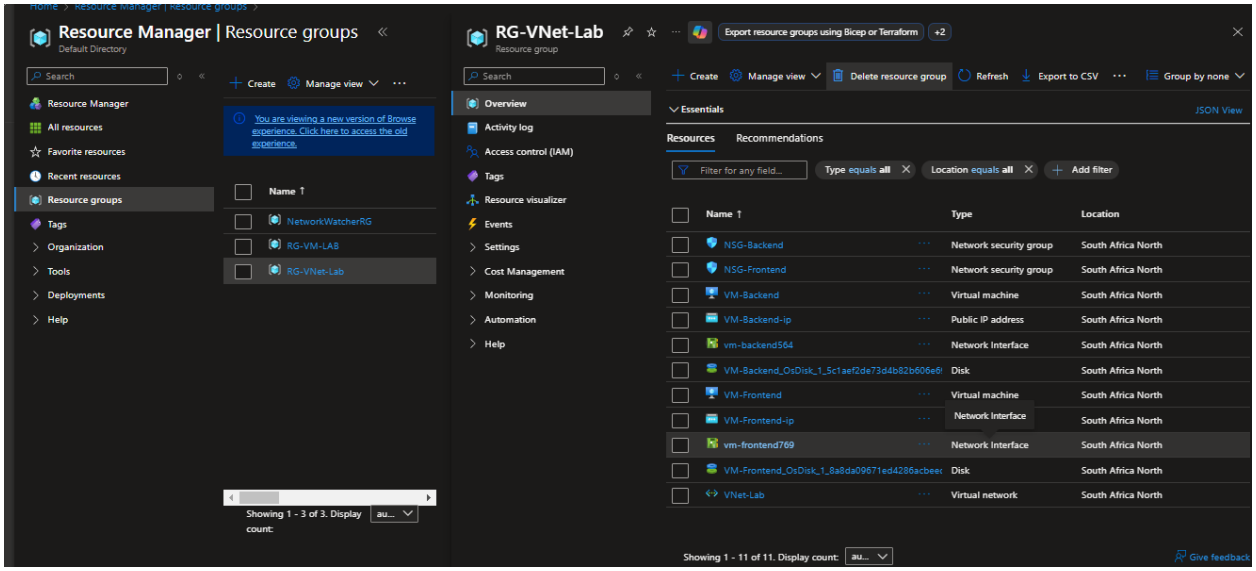
Step 7: Test Connectivity Between VMs

Use RDP to connect to the Frontend VM.
Open the command Prompt and run.

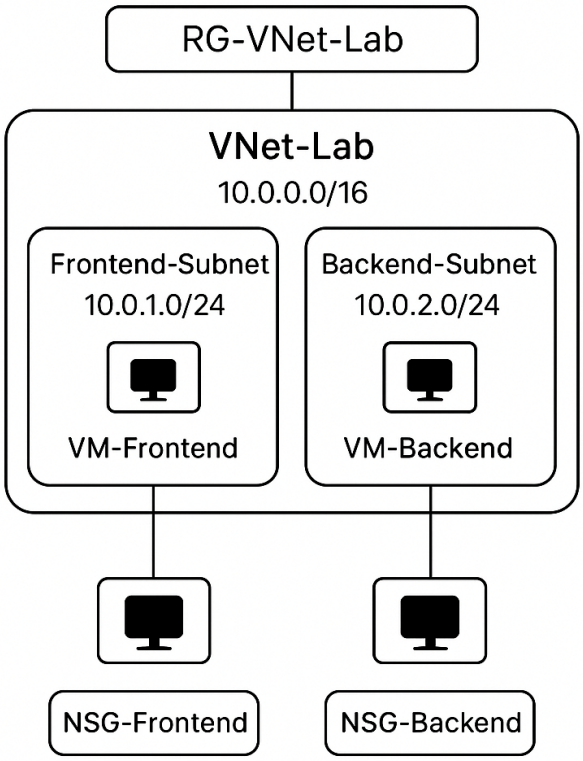
ping <Backend-VM private IP>



Step 8: Verifying All Resource



DIAGRAM



LEARNING OUTCOME

.Configure and managed Azure Virtual Networks (Vnet and Subnets)
.Applied Network Security Groups to control traffic
.Deployed and connected multiple VMs securely