AZURE-MULTI-TIER ARCHITECTURE DEPLOYMENT PROJECT

This project involves deploying a secure multi-tier architecture on Microsoft Azure using Azure CLI and GitHub for version control.

Multi-tier architecture means you divide your application into logical layers, each doing a different job. The architecture consists of a virtual network [VNET] divided into three subnets,Web,App and Database with network security groups [NSGs] configured to enforce tier-to-tier communication rules. The project demonstrates automation, network segmentation, and security in cloud infrastructure.

Objectives

- Create a VNet with three subnets: Web, App and DB.
- Provision Linux VNs in each subnet.
- Create NSGs to allow only necessary communication [Web-App-DB].
- SSH into each VM and verify connectivity rules [ping tests].
- Write a Bash script to automate the full deployment.

Tools and Resource Used

- Azure portal
- Azure CLI
- Ubuntu 22.04 LTS
- GitHub [for version control]
- Bash scripting

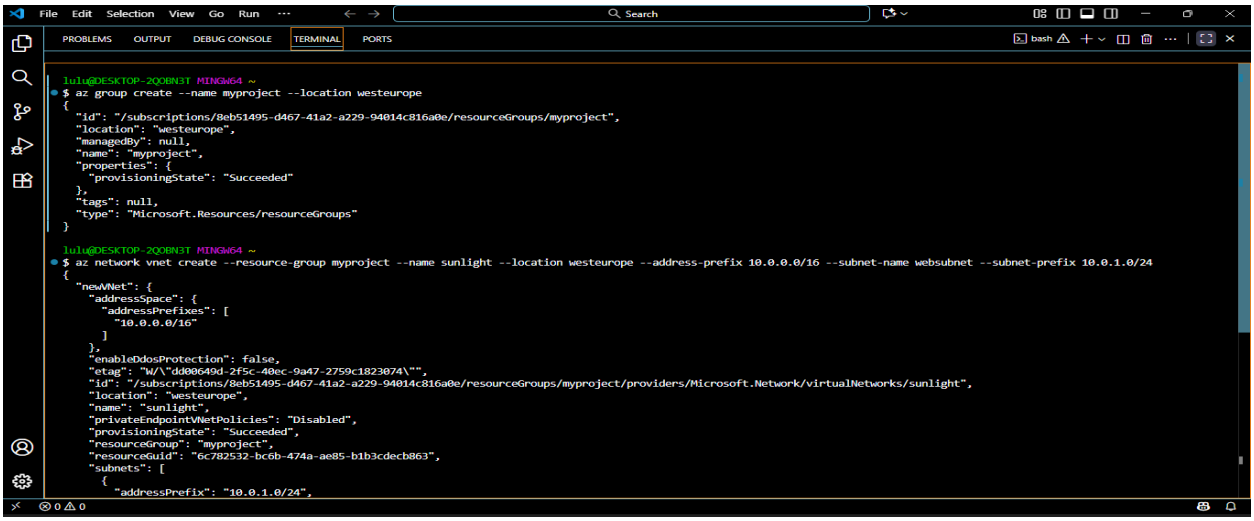
Steps involved

Step 1: Resource group creation

Created a resource group [myproject]; which serves as the central management unit for all that is deployed in the multi-tier architecture.

- Azure CLI command

```
az group create --name myproject --location westeurope
```



Step 2: VNet and subnet creation

The virtual network is a building block for private network communication, it allows resources to securely connect with each other

Created a virtual network named ”sunlight” with an address 10.0.0.0./16 and added three subnets, each subnet has its own address prefix.

Azure CLI command

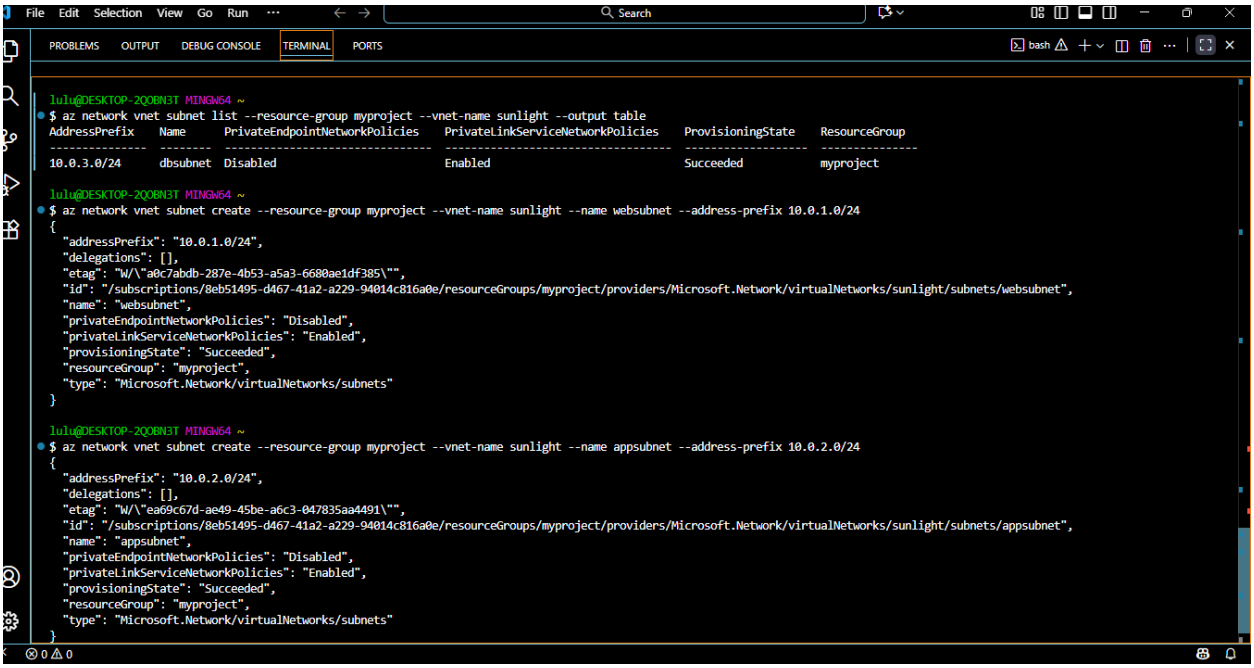
- az network vnet create --resource-group myproject --name sunlight –location westeurope --address-prefix 10.0.0.0/16 --subnet-name dbsubnet --subnet-prefix 10.0.3.0/24

Then went ahead to add three subnets, each subnet has its own address prefix.

- Websubnet [10.0.1.0/24]
- Appsubnet [10.0.2.0/24]
- Dbsubnet [10.0.3.0/24]

Azure CLI command

- az network vnet subnet create --resource-group myproject --vnet-name sunlight --name websubnet --address-prefix 10.0.1.0/24
- az network vnet subnet create --resource-group myproject --vnet-name sunlight --name appsubnet --address-prefix 10.0.2.0/24



- To view the list of created subnets

Azure CLI command

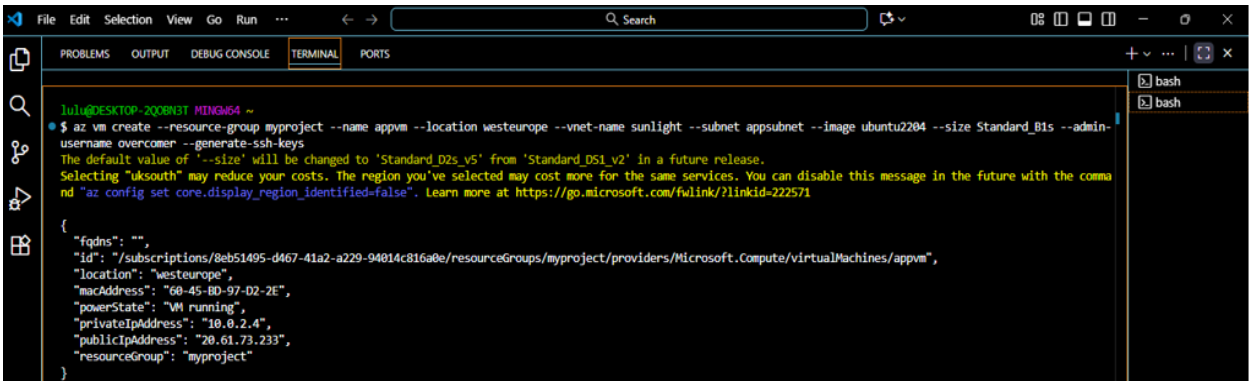
- az network vnet subnet list --resource-group myproject --vnet-name sunlight --output table

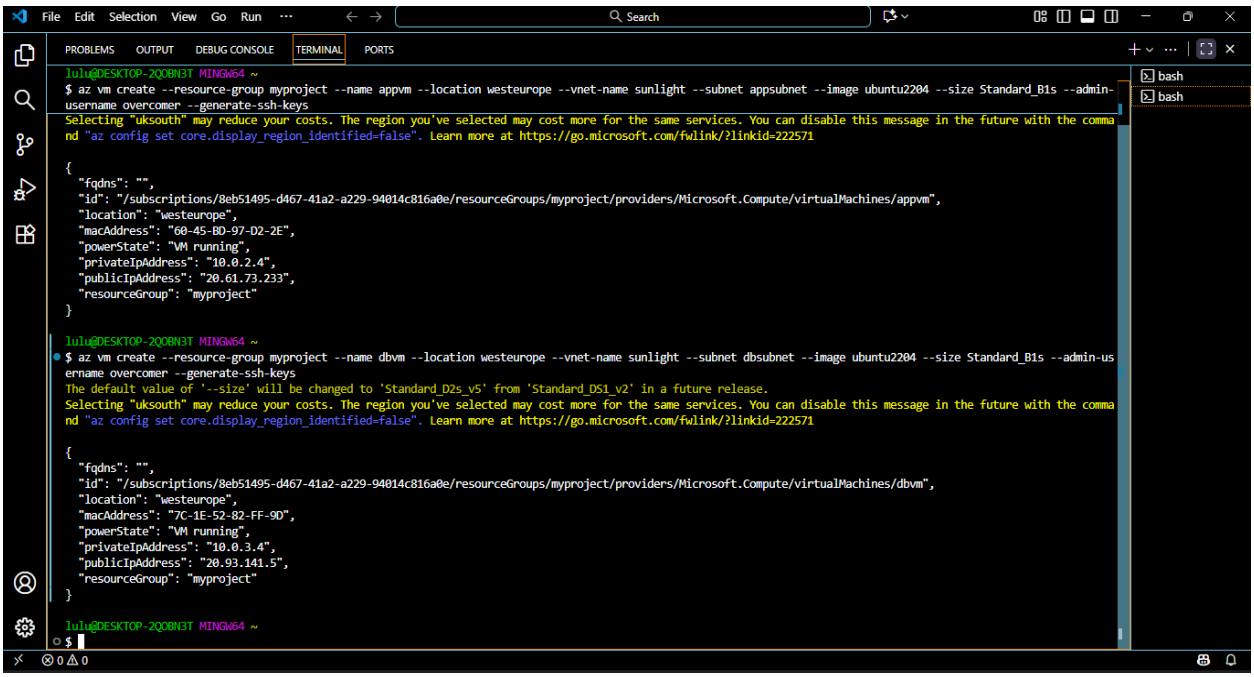
Step 3: Virtual machine deployment

Deployed three [3] linux virtual machines [VMs] each placed in its corresponding subnet [web, app and database], used Ubuntu 22.04 image and Standard_B1s.

Azure CLI command

- az vm create --resource-group myproject --name appvm --location westeurope --vnet-name sunlight --subnet appsubnet --image Ubuntu2204 --size Standard_B1s --admin-username overcomer --generate-ssh-keys.
- az vm create --resource-group myproject --name webvm --location westeurope --vnet-name sunlight --subnet websubnet --image Ubuntu2204 --size Standard_B1s --admin-username overcomer --generate-ssh-keys.
- az vm create –resource-group myproject --name dbvm --location westeurope --vnet-name sunlight --subnet dbsubnet --image Ubuntu2204 --size Standard_B1s --admin-username overcomer --generate-ssh-keys.



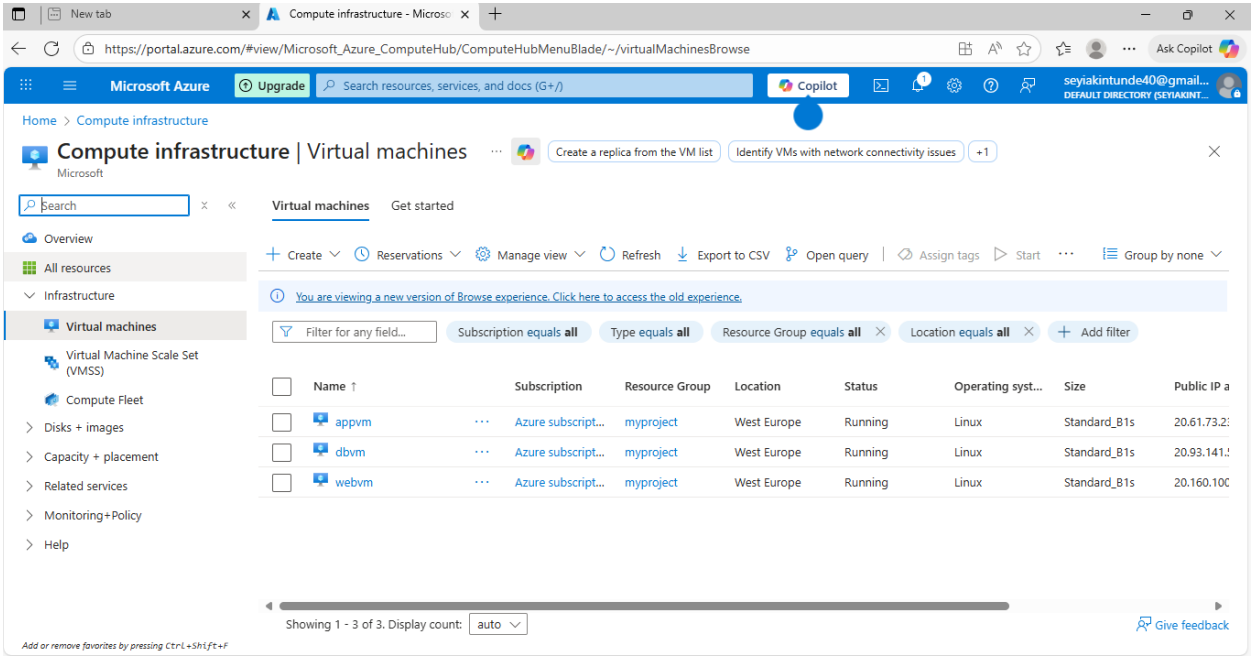


- One major challenge encountered was virtual machine deployment failure due to unavailable VM size in my initial region [uksouth],had to make research on available VM size in the region, after learning that not all size are supported in every region due to capacity limits or subscription restriction

Then had to create a new resource group in West Europe and deployed all VMs there successfully using VM size Standard_ B1s.

- Initially, encountered issues with SSH key configuration, as I was not sure where my key was saved.
  To resolve this I used the –generate-ssh-keys command during VM creation, which automatically created and stored the SSH key pair needed.

Each VM was successfully deployed and associated with its respective subnet to maintain the structure of the multi-tier architecture.



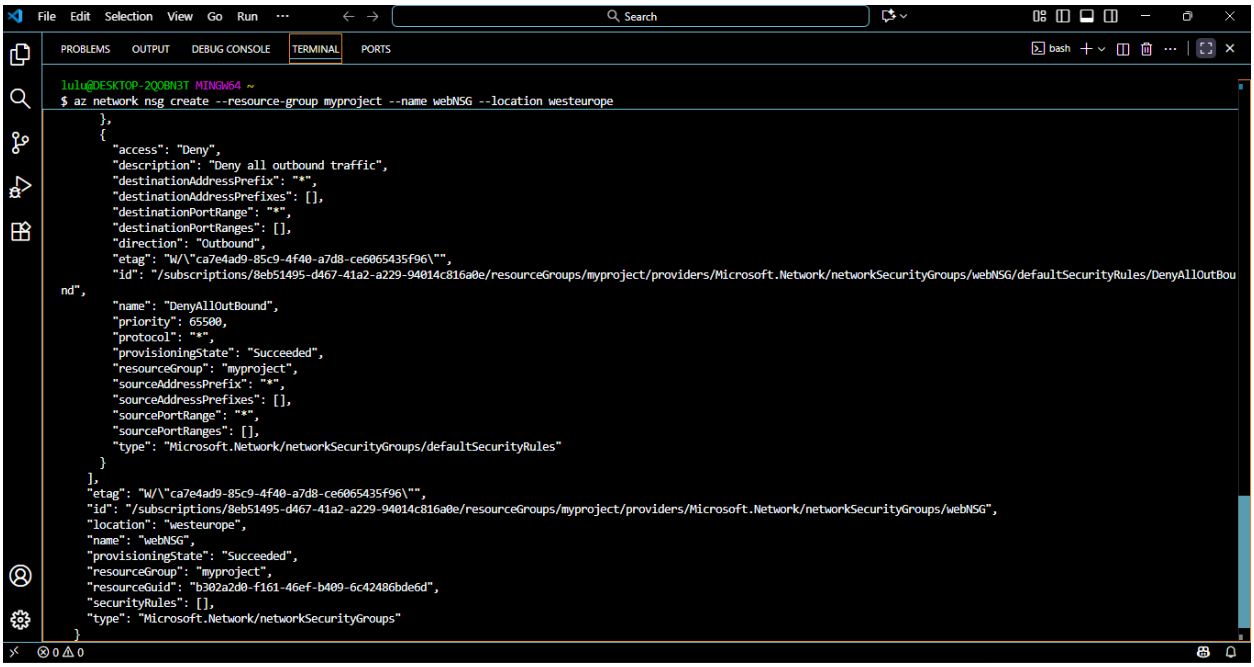
Step 4: Network security group [NSGs] creation

To enhance security and enforce proper traffic flow between the subnets within the virtual networks [Web,App and DB]

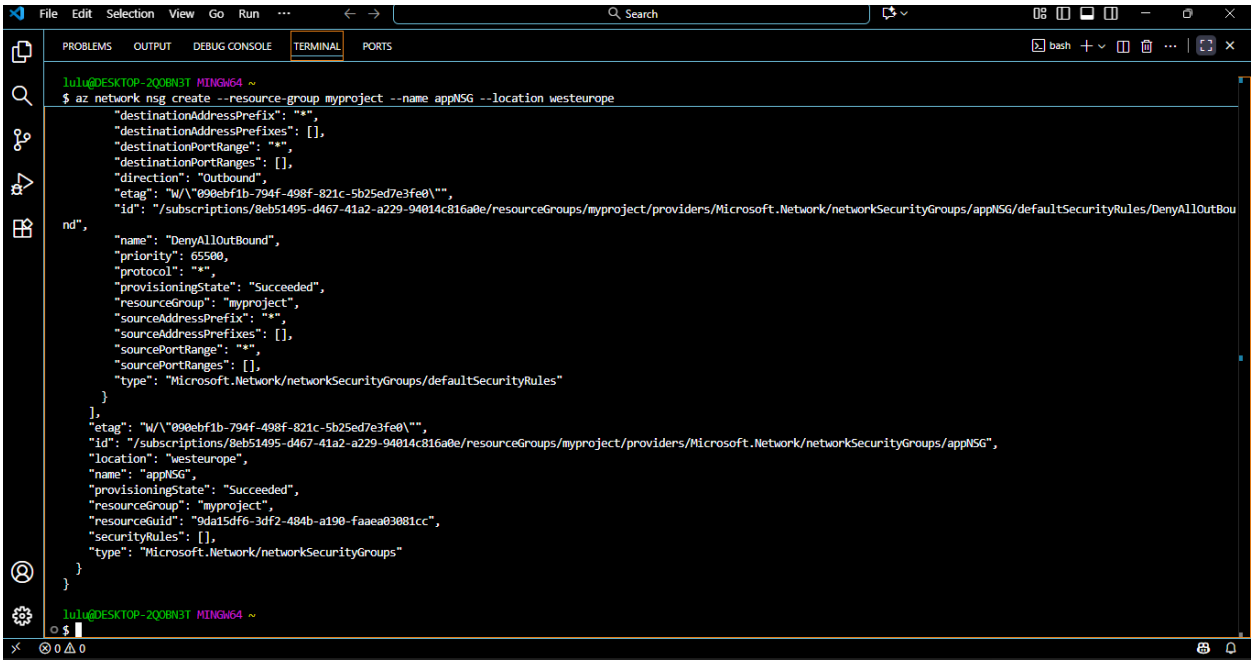
Created three [3] separate NSGs i.e webNSG, appNSG and dbNSG; then liked each subnet with their respective NSG as it requires its own NSG to ensure customized and controlled access rules.

Azure CLI command

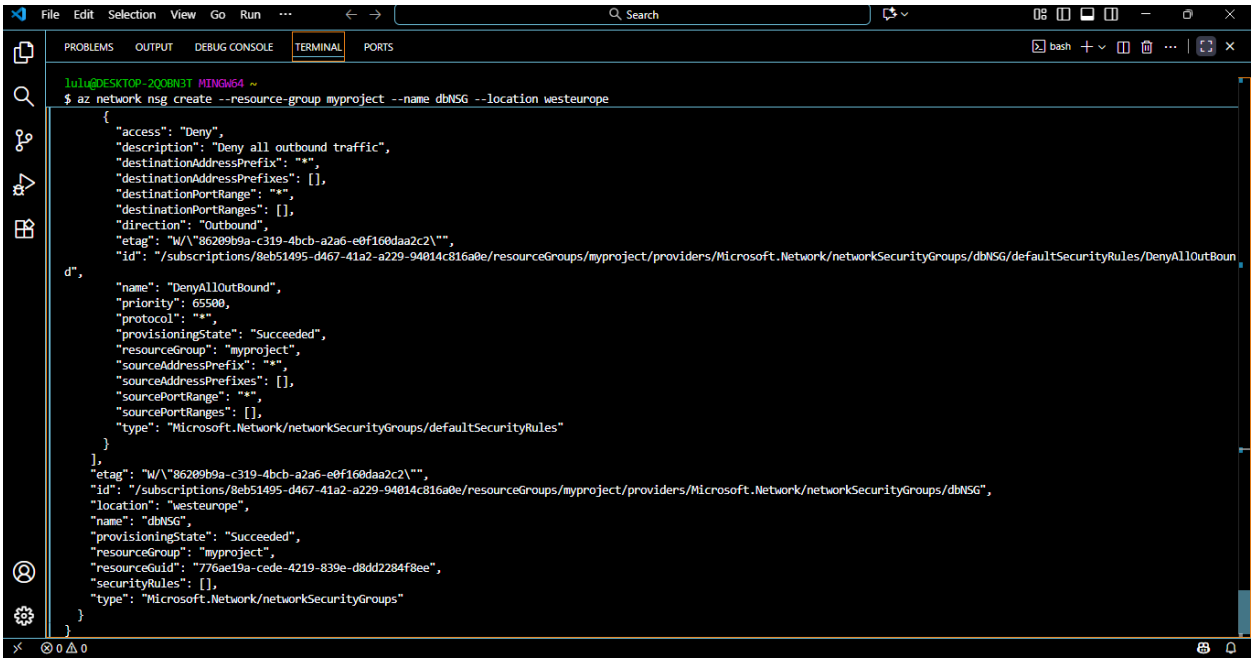
- az network nsg create --resource-group myproject --name webNSG --location westeurope



- az network nsg create --resource-group myproject --name appNSG --location westeurope



- az network nsg create --resource-group myproject --name dbNSG --location westeurope

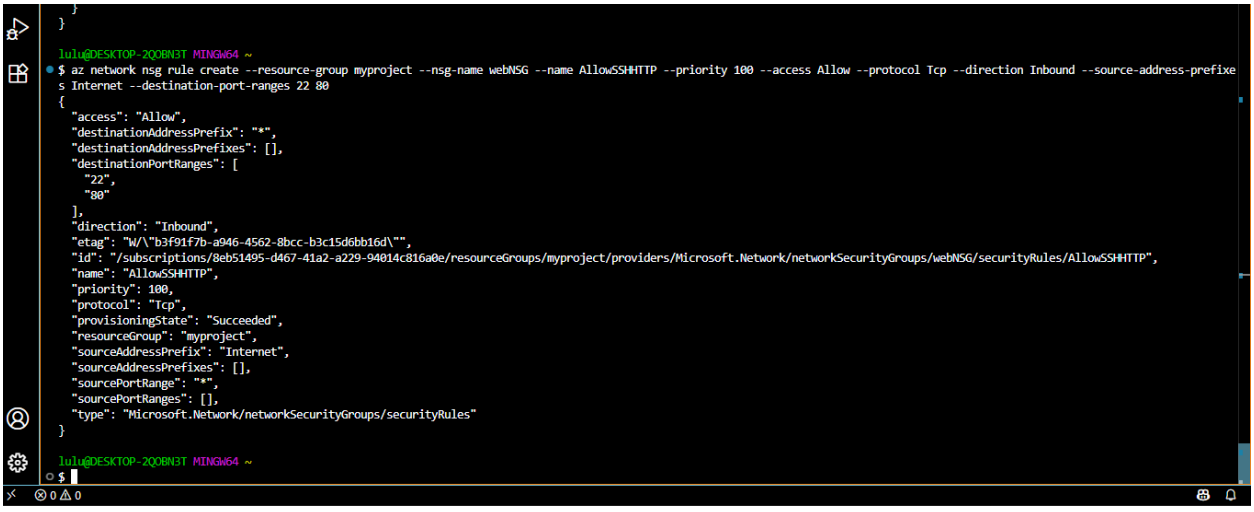


To enforce access control between tiers and external access, configuration of specific inbound rules for each NSG was carried out.

- WebNSG
- inbound:
  - Allow SSH [port 22] from the internet for remote access.
  - Allow HTTP [port 80] from the internet to serve web traffic.

Azure CLI command

- az network nsg rule create --resource-group myproject --nsg-name webNSG --name AllowSSHHTTP --priority 100 --access Allow --protocol Tcp --direction Inbound--source-address-prefixes Internet --destination-port-ranges 22 80.

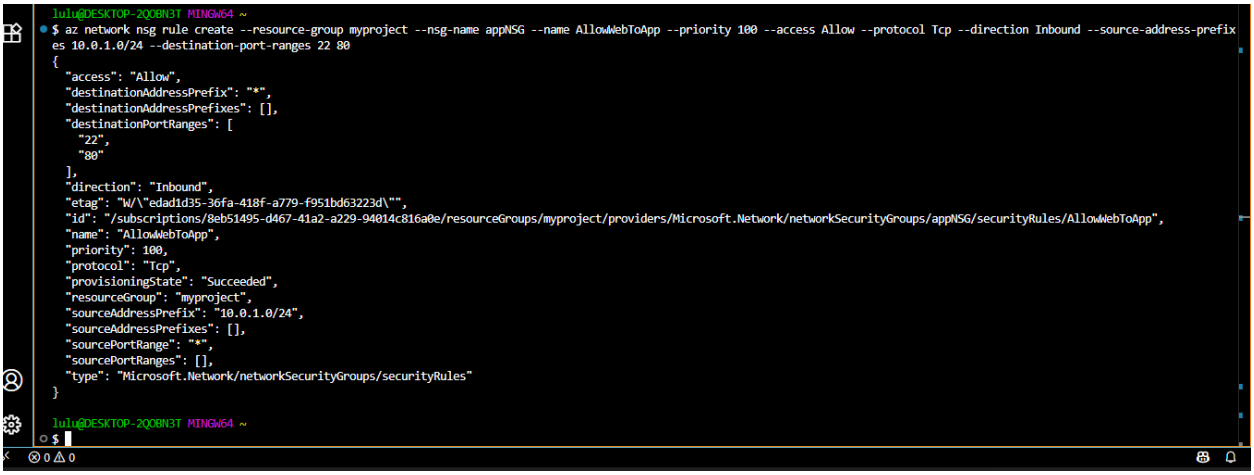


- AppNSG

- Inbound:
    - ➢ Allow HTTP [port 80] traffic only from the web subnet

Azure CLI command

- az network nsg rule create --resource-group myproject --nsg-name appNSG --name AllowWebToApp --priority 100 --access Allow --protocol Tcp --direction Inbound --source-address-prefixes 10.0.1.0/24 --destination-port-ranges 22 80

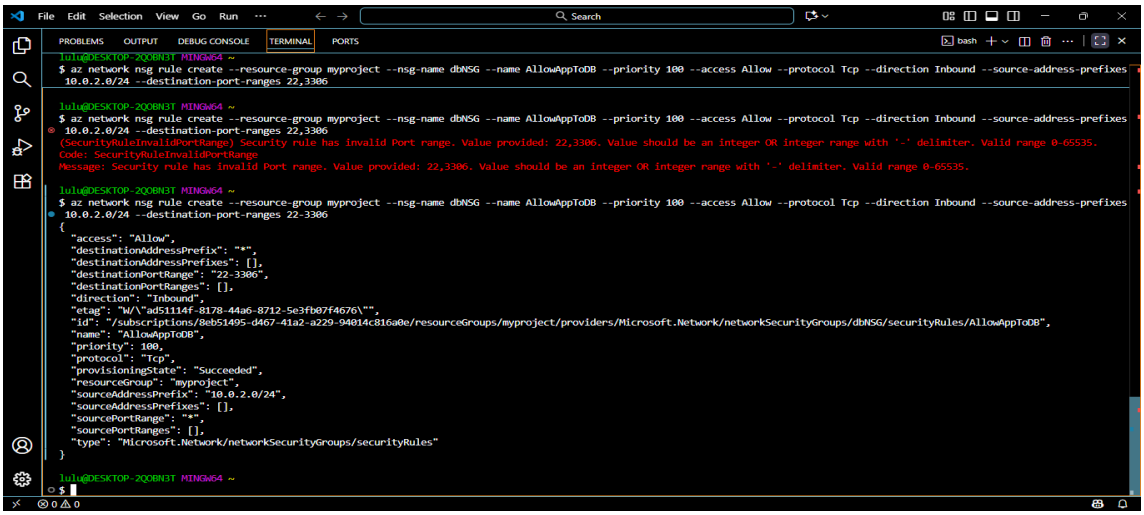


- DbNSG
- Inbound:
    - ➢ Allow traffic from app subnet on port 3306

After deploying the virtual machines and configuring the NSGs, then went ahead to test the connectivity between the subnets to ensure that the access control rules were functioning.

Azure CLI command

- az network rule create --resource-group myproject --nsg-name dbNSG --name AllowAppToDB --priority 100 --Access Allow --protocol Tcp --direction Inbound --source-address-prefixes 10.0.2.0/24 --destination-port-ranges 22-3306.

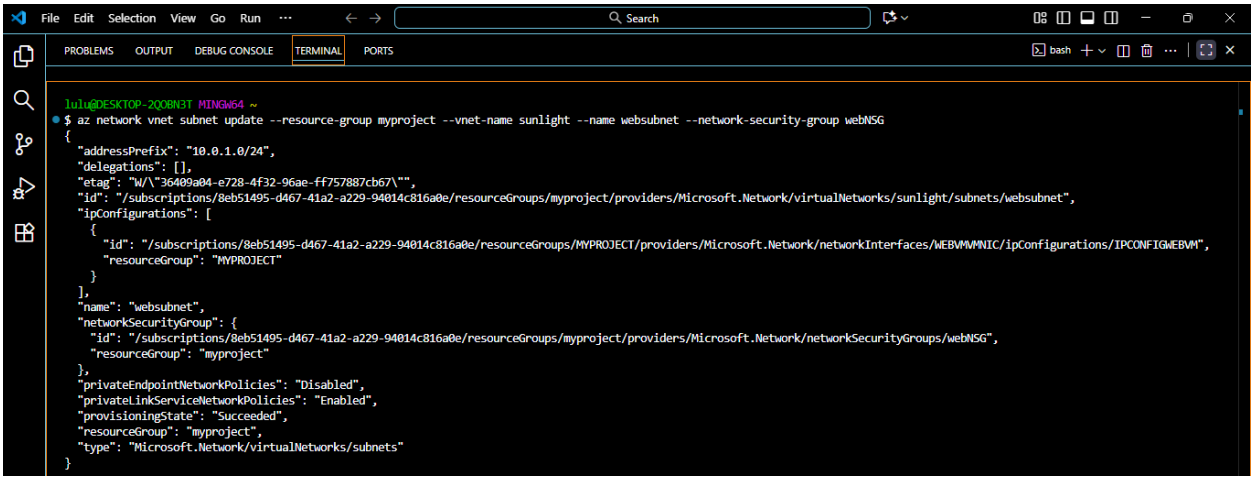


Step 5: Associate NSG to subnet

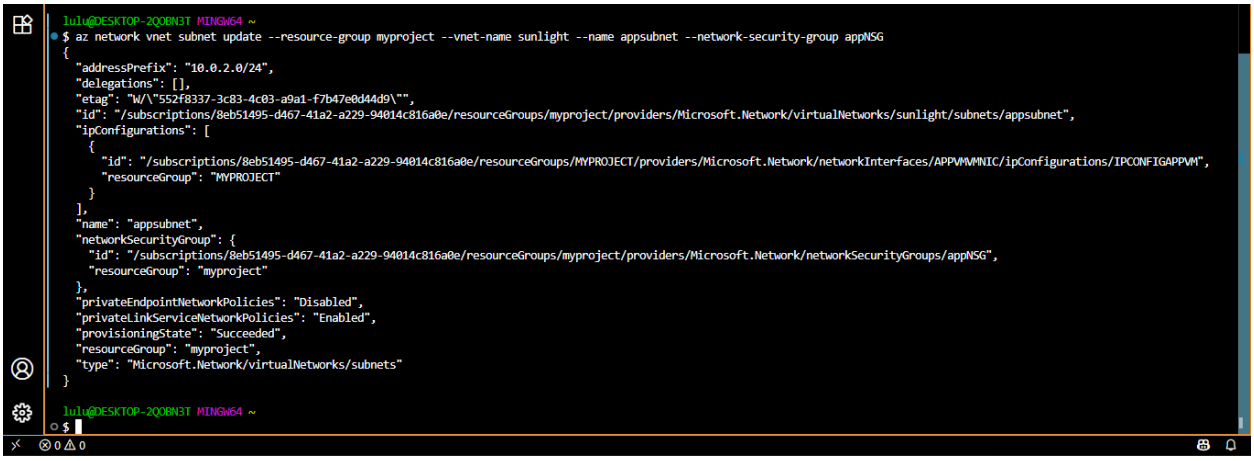
This is to link a specific NSG to a subnet within vnet under the resource group [myproject],this helps control inbound and outbound traffic based on defined security rules.

Azure CLI command

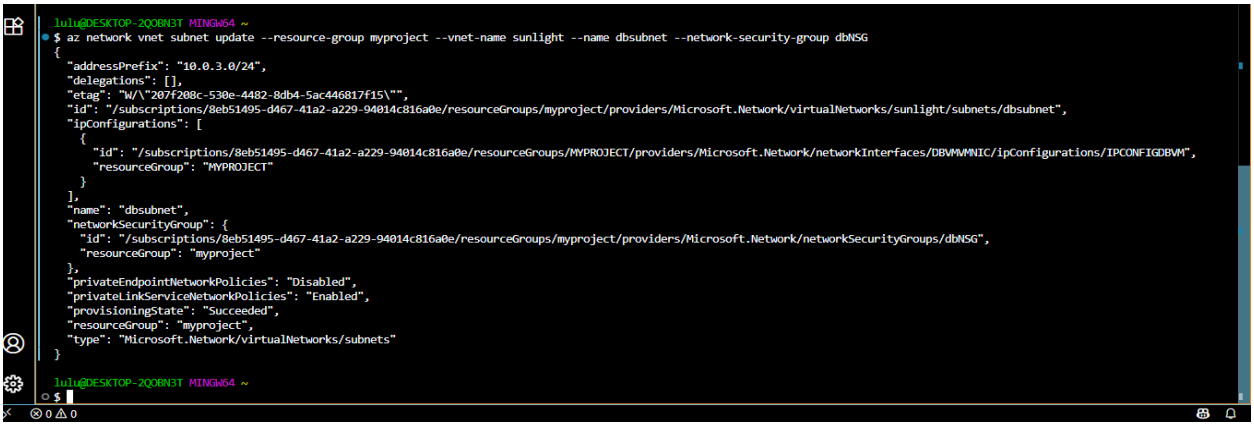
- az network vnet subnet update --resource-group myproject --vnet-name sunlight --name websubnet --network-security-group webNSG



- az network vnet subnet update --resource-group myproject --vnet-name sunlight --name appsubnet --network-security-group appNSG



- az network vnet subnet update --resource-group myproject --vnet-name sunlight --name dbsubnet --network-security-group dbNSG



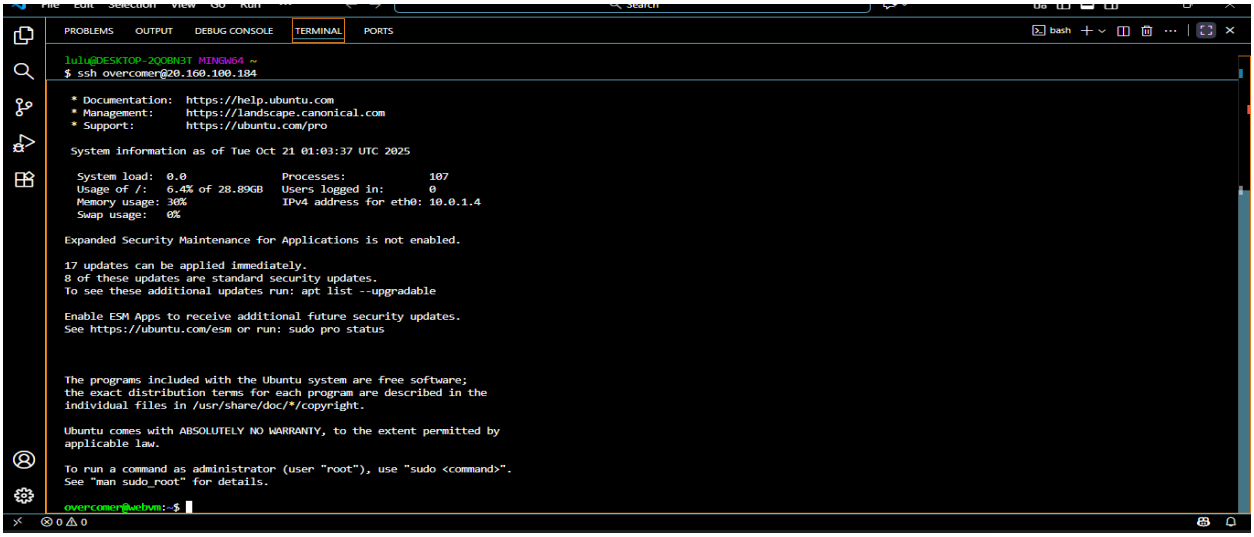
Step 6: Connected to each VM using SSH.

Successfully connected to each VM via SSH using their public/private key pairs, confirming that the VMs were accessible and operational.

SSH connection to webvm; this allows remote access to the webvm to verify configuration and perform connectivity tests.

Azure CLI command

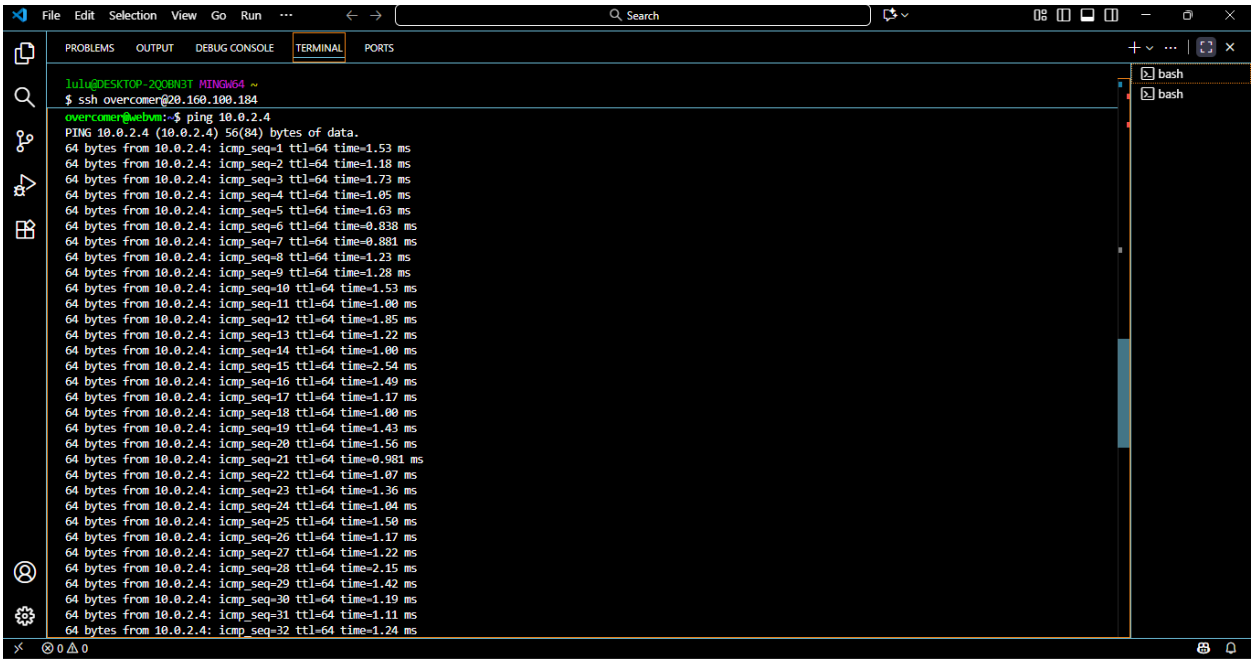
- ssh overcomer@20.160.100.184 [overcomer here is the admin username]

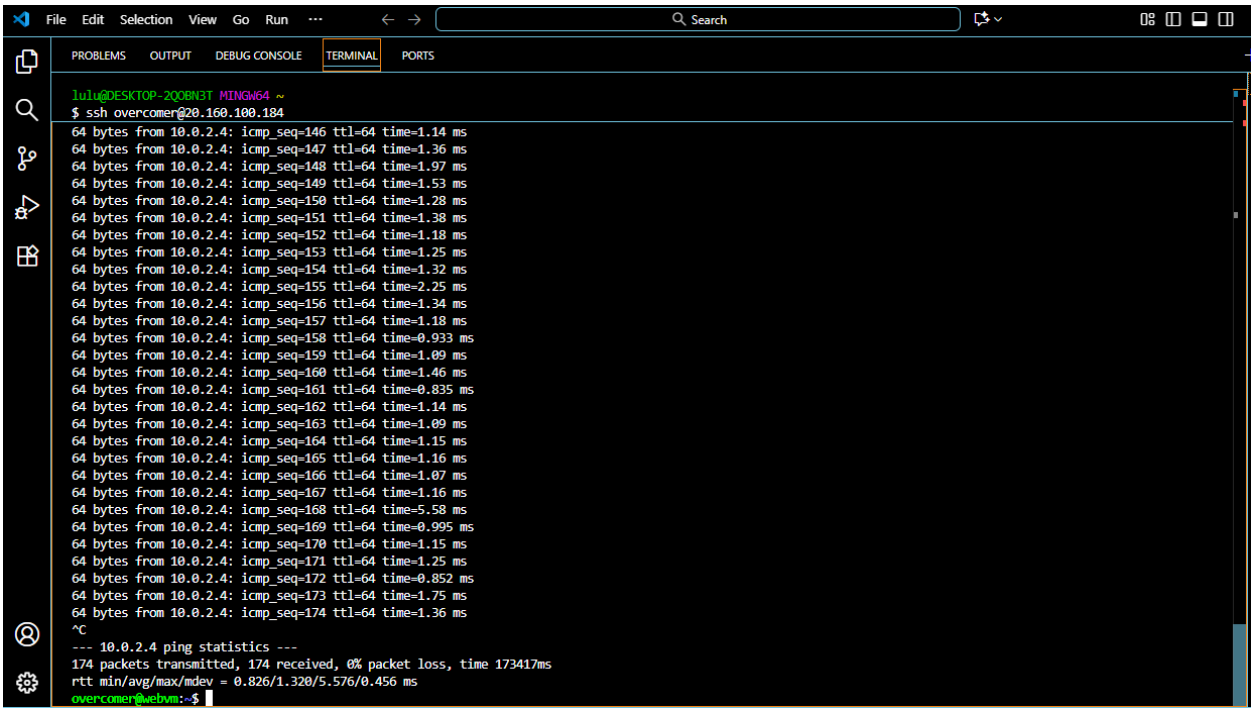


From the webVM, I ran a ping command to the appVM's private IP, the connection was successful.

Azure CLI command

- ping 10.0.2.4

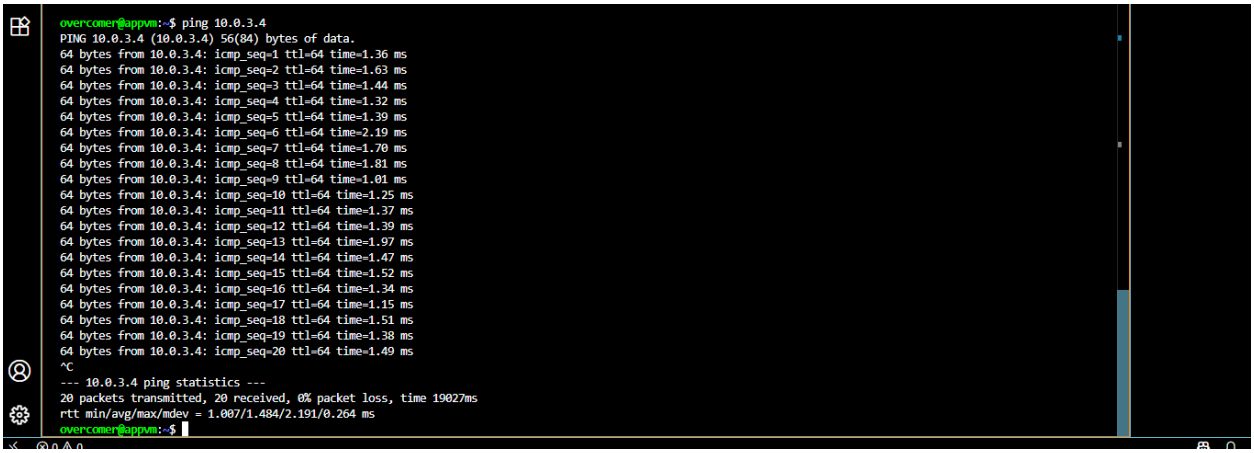




- ssh overcomer@20.61.73.233

From the appVM, I ran a ping command to the dbVM's private IP

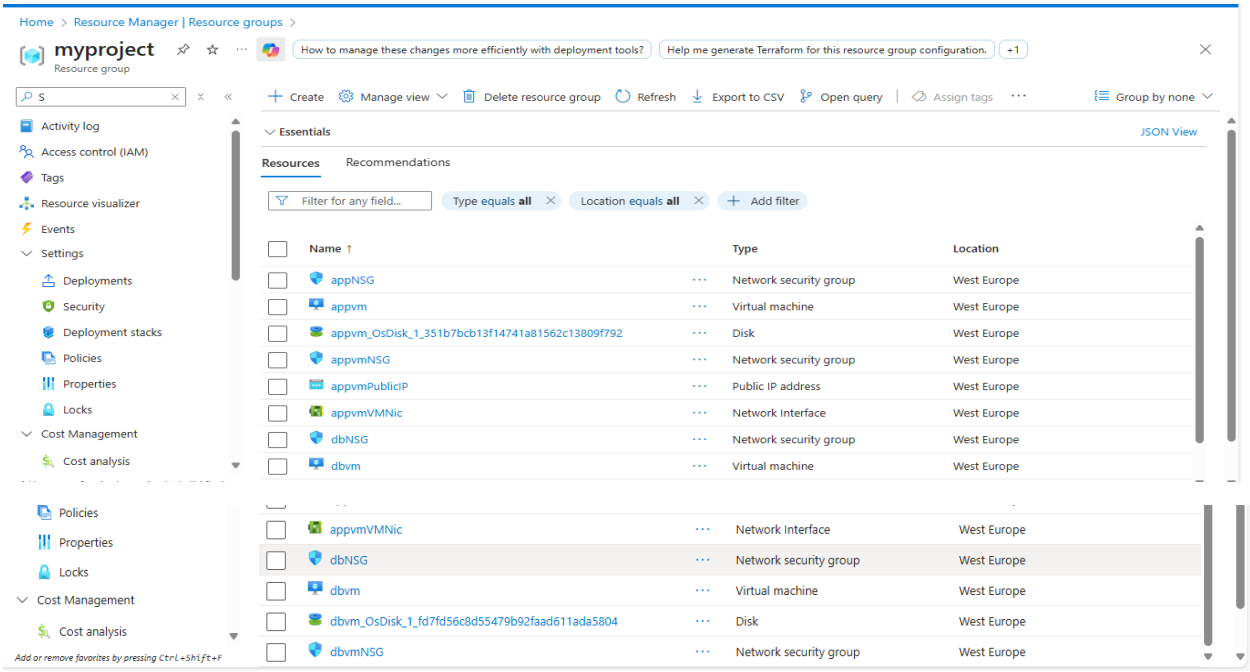
- ping 10.0.3.4

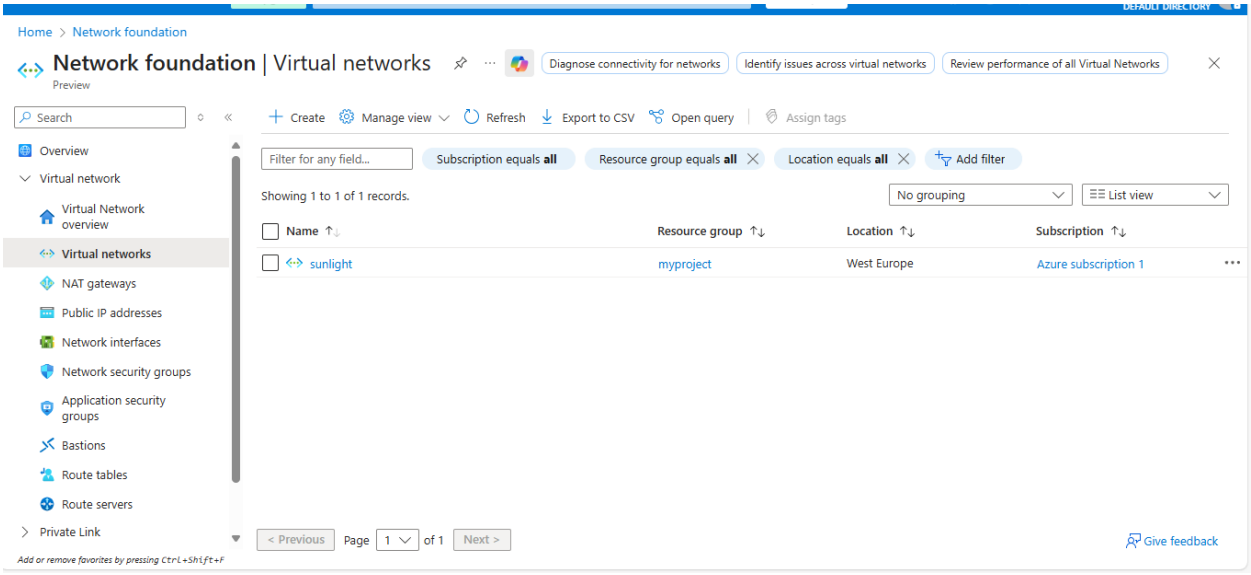


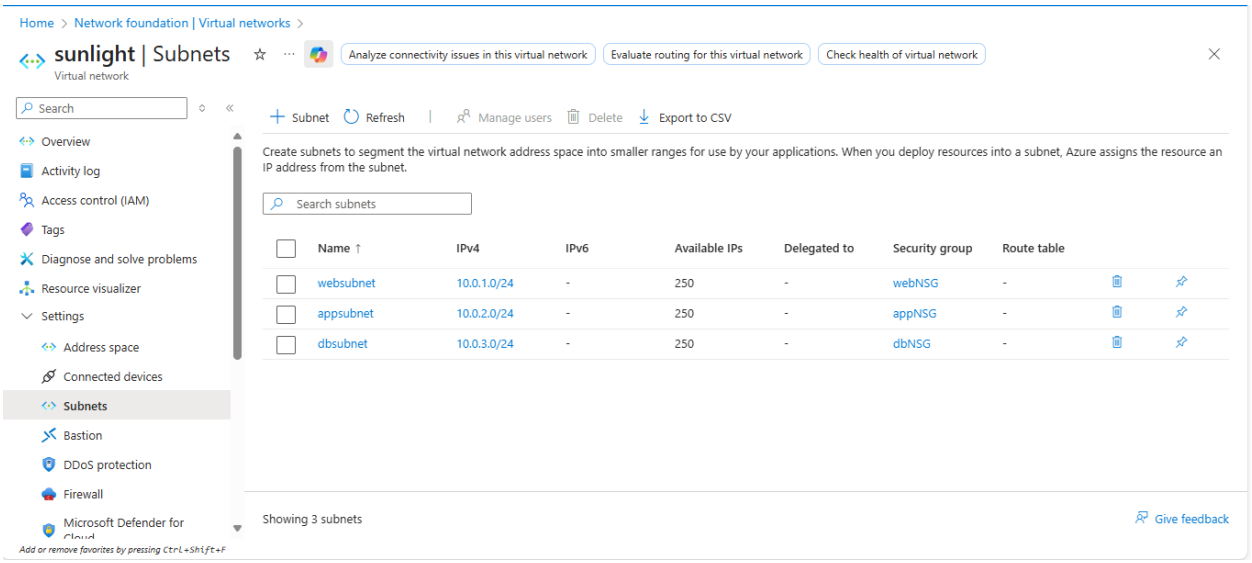
To verify application layer connectivity, I used **"curl"** from the webVM to the appVM's private IP.

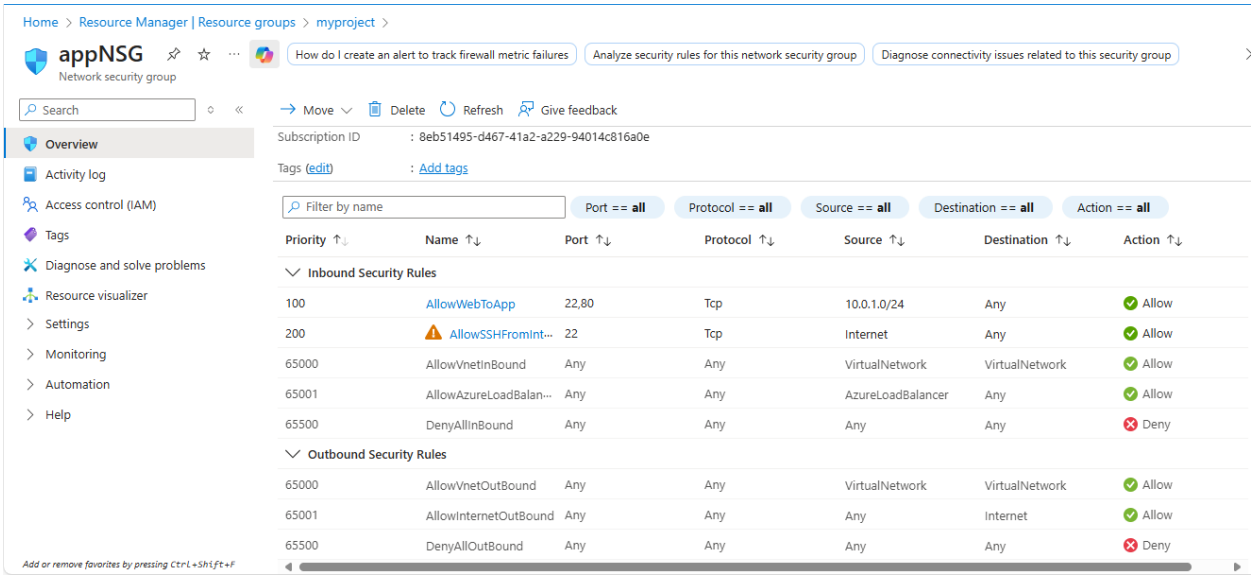
The response was **"Thank you for using nginx"** confirming that the webserver was running and accessible.

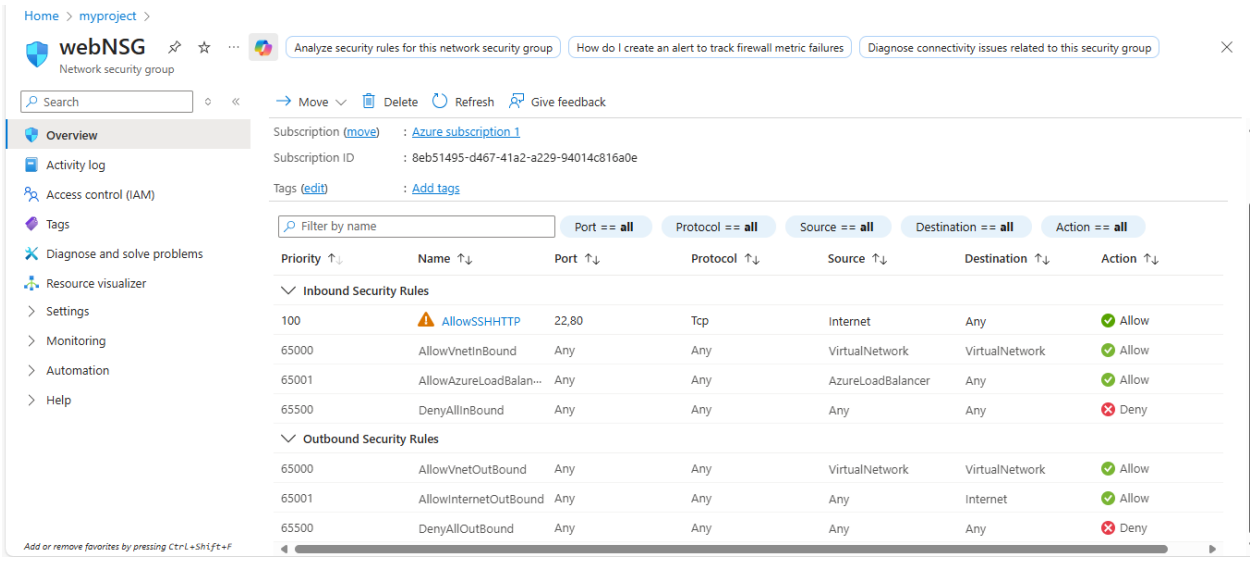
Validation via azure portal

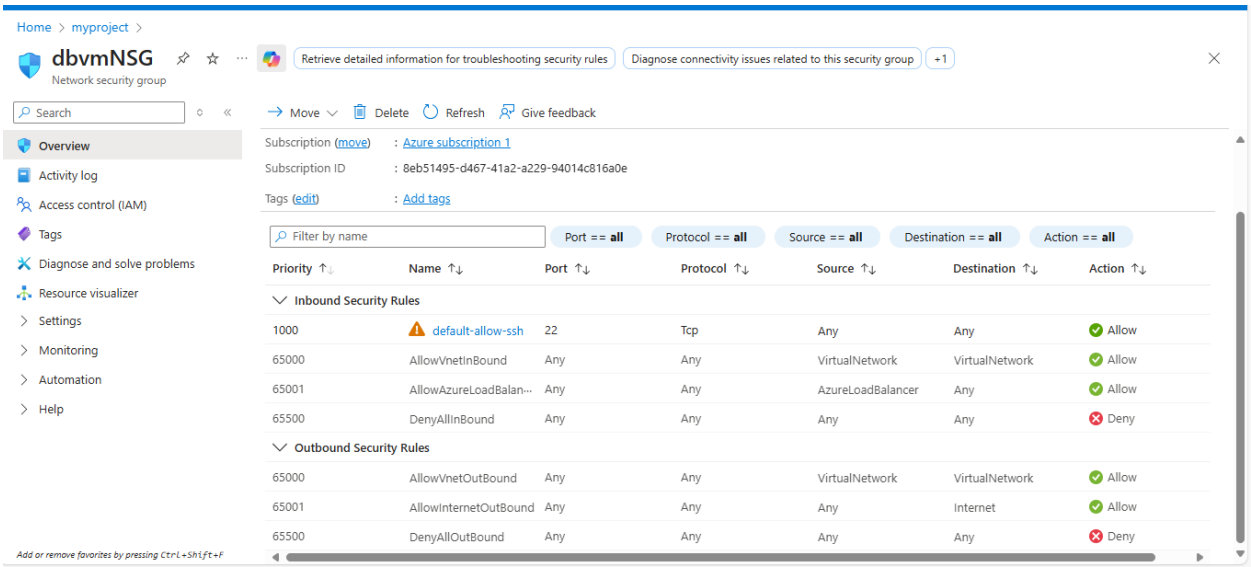


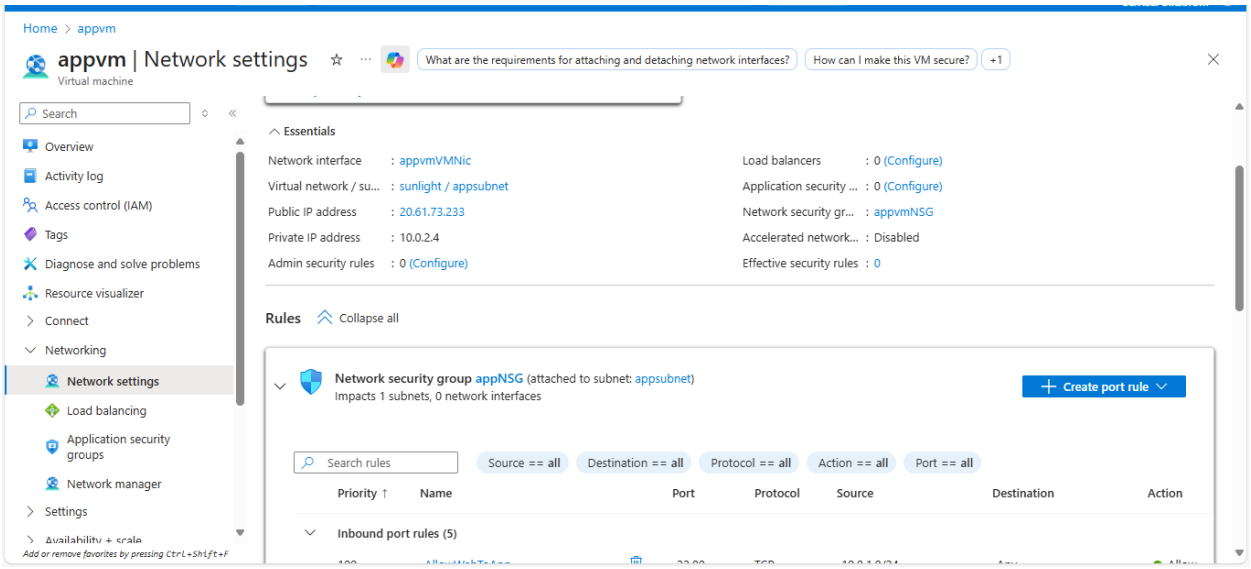


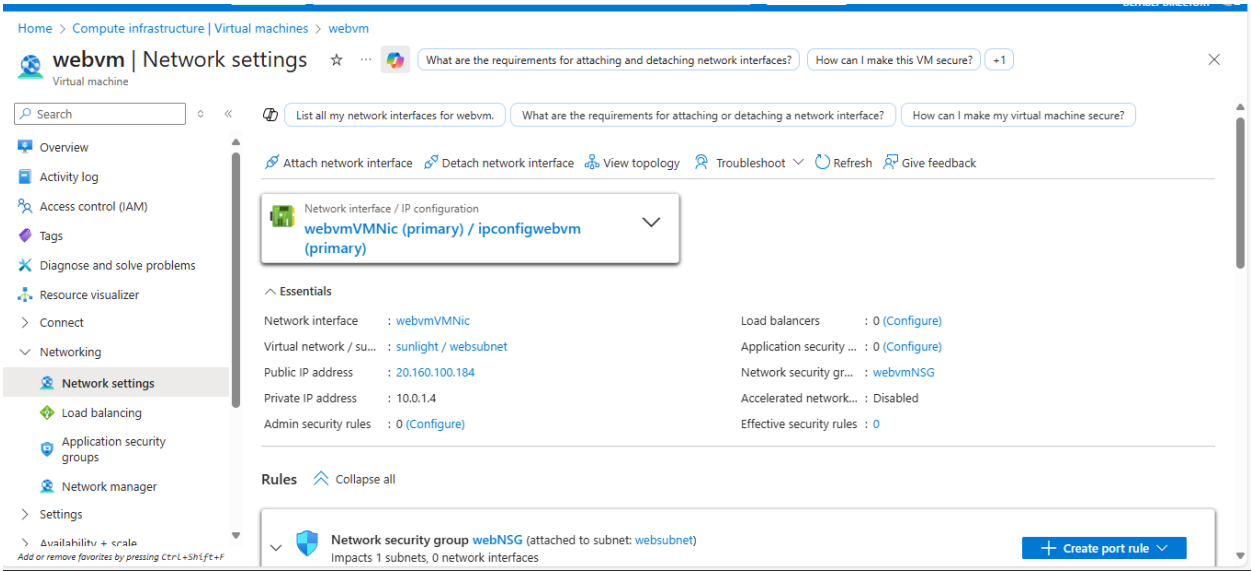

Home > Network foundation | Virtual networks >
sunlight | Subnets
Virtual network
Analyze connectivity issues in this virtual network
Evaluate routing for this virtual network
Check health of virtual network
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Address space
Connected devices
Subnets
Bastion
DDoS protection
Firewall
Microsoft Defender for Cloud
Add or remove favorites by pressing Ctrl+Shift+F
Subnet
Refresh
Manage users
Delete
Export to CSV
Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet.
Search subnets
Name
IPv4
IPv6
Available IPs
Delegated to
Security group
Route table
websubnet 10.0.1.0/24 - 250 - webNSG -
appsubnet 10.0.2.0/24 - 250 - appNSG -
dbsubnet 10.0.3.0/24 - 250 - dbNSG -
Showing 3 subnets
Give feedback

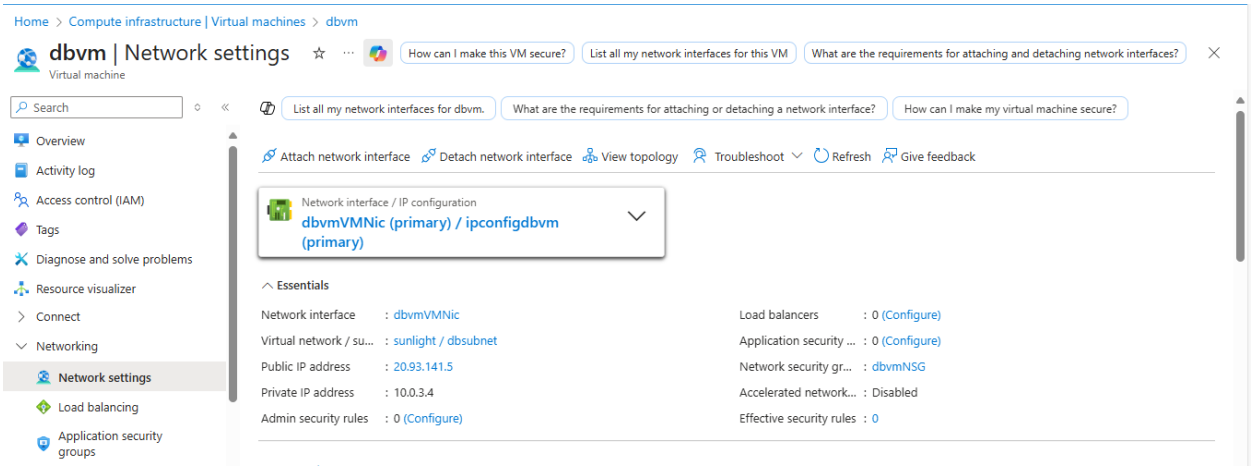

Home > Resource Manager | Resource groups > myproject >
appNSG
Network security group
How do I create an alert to track firewall metric failures
Analyze security rules for this network security group
Diagnose connectivity issues related to this security group
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Monitoring
Automation
Help
Add or remove favorites by pressing Ctrl+Shift+F
Move
Delete
Refresh
Give feedback
Subscription ID : 8eb51495-d467-41a2-a229-94014c816a0e
Tags (edit) : Add tags
Filter by name
Port == all
Protocol == all
Source == all
Destination == all
Action == all
Priority Name Port Protocol Source Destination Action
Inbound Security Rules
100 AllowWebToApp 22,80 Tcp 10.0.1.0/24 Any Allow
200 AllowSSHFromInt... 22 Tcp Internet Any Allow
65000 AllowVnetInBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowAzureLoadBalan... Any Any AzureLoadBalancer Any Allow
65500 DenyAllInBound Any Any Any Any Deny
Outbound Security Rules
65000 AllowVnetOutBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowInternetOutBound Any Any Any Internet Allow
65500 DenyAllOutBound Any Any Any Any Deny


Home > myproject >
webNSG
Network security group
Analyze security rules for this network security group
How do I create an alert to track firewall metric failures
Diagnose connectivity issues related to this security group
Search
Move
Delete
Refresh
Give feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Monitoring
Automation
Help
Subscription (move) : Azure subscription 1
Subscription ID : 8eb51495-d467-41a2-a229-94014c816a0e
Tags (edit) : Add tags
Filter by name
Port == all
Protocol == all
Source == all
Destination == all
Action == all
Priority
Name
Port
Protocol
Source
Destination
Action
Inbound Security Rules
100 AllowSSHHTTP 22,80 Tcp Internet Any Allow
65000 AllowVnetInBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowAzureLoadBalan··· Any Any AzureLoadBalancer Any Allow
65500 DenyAllInBound Any Any Any Any Deny
Outbound Security Rules
65000 AllowVnetOutBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowInternetOutBound Any Any Any Internet Allow
65500 DenyAllOutBound Any Any Any Any Deny
Add or remove favorites by pressing Ctrl+Shift+F


Home > myproject >
dbvmNSG
Network security group
Retrieve detailed information for troubleshooting security rules
Diagnose connectivity issues related to this security group
+1
Search
Move
Delete
Refresh
Give feedback
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Monitoring
Automation
Help
Subscription (move) : Azure subscription 1
Subscription ID : 8eb51495-d467-41a2-a229-94014c816a0e
Tags (edit) : Add tags
Filter by name
Port == all
Protocol == all
Source == all
Destination == all
Action == all
Priority
Name
Port
Protocol
Source
Destination
Action
Inbound Security Rules
1000 default-allow-ssh 22 Tcp Any Any Allow
65000 AllowVnetInBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowAzureLoadBalan··· Any Any AzureLoadBalancer Any Allow
65500 DenyAllInBound Any Any Any Any Deny
Outbound Security Rules
65000 AllowVnetOutBound Any Any VirtualNetwork VirtualNetwork Allow
65001 AllowInternetOutBound Any Any Any Internet Allow
65500 DenyAllOutBound Any Any Any Any Deny
Add or remove favorites by pressing Ctrl+Shift+F


Home > appvm
appvm | Network settings
Virtual machine
What are the requirements for attaching and detaching network interfaces?
How can I make this VM secure?
+1
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Network settings
Load balancing
Application security groups
Network manager
Settings
Essentials
Network interface : appvmVMNic
Virtual network / su... : sunlight / appsubnet
Public IP address : 20.61.73.233
Private IP address : 10.0.2.4
Admin security rules : 0 (Configure)
Load balancers : 0 (Configure)
Application security ... : 0 (Configure)
Network security gr... : appvmNSG
Accelerated network... : Disabled
Effective security rules : 0
Rules
Collapse all
Network security group appNSG (attached to subnet: appsubnet)
Impacts 1 subnets, 0 network interfaces
Create port rule
Search rules
Source == all
Destination == all
Protocol == all
Action == all
Port == all
Priority
Name
Port
Protocol
Source
Destination
Action
Inbound port rules (5)


Home > Compute infrastructure | Virtual machines > webvm
webvm | Network settings
Virtual machine
What are the requirements for attaching and detaching network interfaces?
How can I make this VM secure?
+1
List all my network interfaces for webvm.
What are the requirements for attaching or detaching a network interface?
How can I make my virtual machine secure?
Attach network interface
Detach network interface
View topology
Troubleshoot
Refresh
Give feedback
Network interface / IP configuration
webvmVMNic (primary) / ipconfigwebvm (primary)
Essentials
Network interface : webvmVMNic
Virtual network / su... : sunlight / websubnet
Public IP address : 20.160.100.184
Private IP address : 10.0.1.4
Admin security rules : 0 (Configure)
Load balancers : 0 (Configure)
Application security ... : 0 (Configure)
Network security gr... : webvmNSG
Accelerated network... : Disabled
Effective security rules : 0
Rules
Collapse all
Network security group webNSG (attached to subnet: websubnet)
Impacts 1 subnets, 0 network interfaces
Create port rule


Home > Compute infrastructure | Virtual machines > dbvm
dbvm | Network settings
Virtual machine
How can I make this VM secure?
List all my network interfaces for this VM
What are the requirements for attaching and detaching network interfaces?
List all my network interfaces for dbvm.
What are the requirements for attaching or detaching a network interface?
How can I make my virtual machine secure?
Attach network interface
Detach network interface
View topology
Troubleshoot
Refresh
Give feedback
Network interface / IP configuration
dbvmVMNic (primary) / ipconfigdbvm (primary)
Essentials
Network interface : dbvmVMNic
Virtual network / su... : sunlight / dbsubnet
Public IP address : 20.93.141.5
Private IP address : 10.0.3.4
Admin security rules : 0 (Configure)
Load balancers : 0 (Configure)
Application security ... : 0 (Configure)
Network security gr... : dbvmNSG
Accelerated network... : Disabled
Effective security rules : 0