HUMBER
POLYTECHNIC

Name: Waqas Salman

Student ID: N10017938

Course: CSAI-5002-RN1

Lab 01

Overview:

This lab guides you through the design and deployment of a secure, two-tier cloud infrastructure on Microsoft Azure. The architecture separates web-facing and database services into isolated network segments, enforcing strict access controls through Azure Network Security Groups (NSGs) and the principle of least privilege.

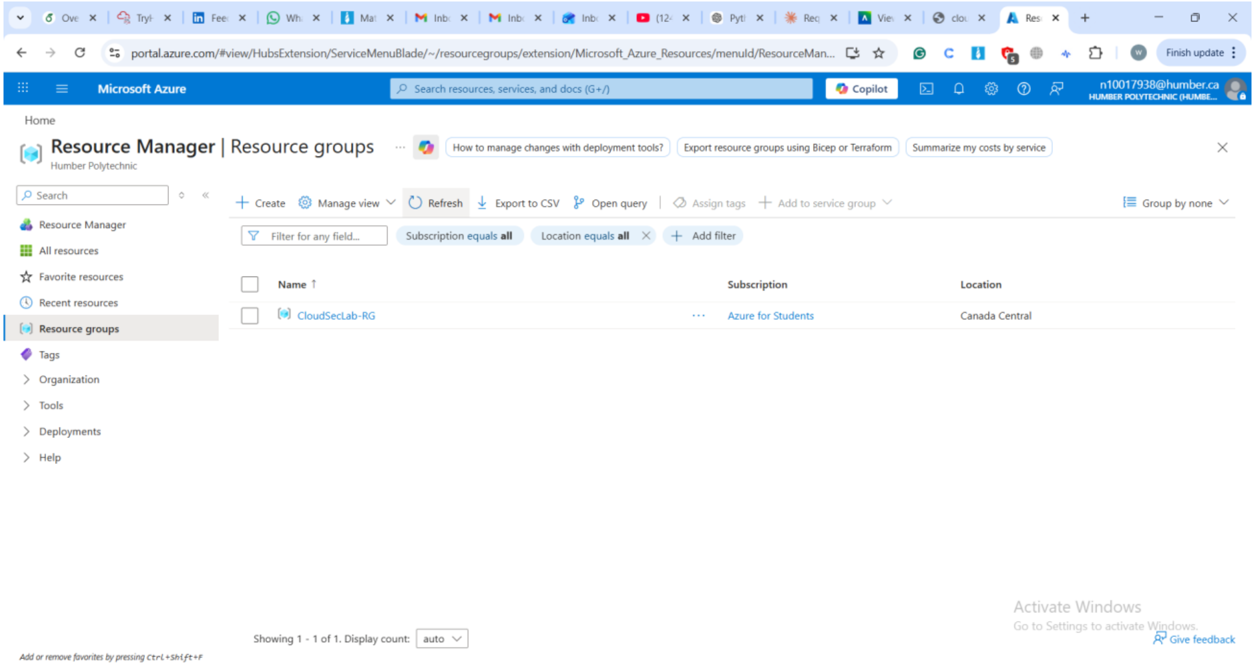
In real-world environments, one of the most common causes of data breaches is the exposure of sensitive backend systems particularly databases directly to the internet. This lab addresses that risk head-on by implementing a defense-in-depth strategy, where multiple layers of security controls work together to protect critical assets even if one layer is compromised.

Step 1: Create the Resource Group

A Resource Group is a logical container in Azure that holds all related resources for a solution. Every Azure resource virtual machines, networks, security groups, IP addresses must belong to a resource group. When you delete a resource group, every resource inside it is automatically deleted as well. This makes cleanup simple and ensures no orphaned resources are left running and incurring costs.

Instructions

1. Sign in to the Azure Portal
2. In the top search bar, type **Resource Groups** and select it from the results
3. Click **+ Create**
4. Fill in the following details:
   - **Subscription:** Select your active subscription
   - **Resource Group Name:** CloudSecLab-RG
   - **Region:** Choose a region close to you (e.g., *Canada Central*)
5. Click **Review + Create**, then **Create**


portal.azure.com/#view/HubsExtension/ServiceMenuBlade/~/resourcegroups/extension/Microsoft_Azure_Resources/menuId/ResourceMan...
Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
n10017938@humber.ca
HUMBER POLYTECHNIC (HUMBE...
Home
Resource Manager | Resource groups
Humber Polytechnic
How to manage changes with deployment tools?
Export resource groups using Bicep or Terraform
Summarize my costs by service
Search
Resource Manager
All resources
Favorite resources
Recent resources
Resource groups
Tags
Organization
Tools
Deployments
Help
Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Add to service group
Group by none
Filter for any field...
Subscription equals all
Location equals all
Add filter
Showing 1 - 1 of 1. Display count: auto
Add or remove favorites by pressing Ctrl+Shift+F
Activate Windows
Go to Settings to activate Windows.
Give feedback

Name ↑	Subscription	Location
CloudSecLab-RG	Azure for Students	Canada Central

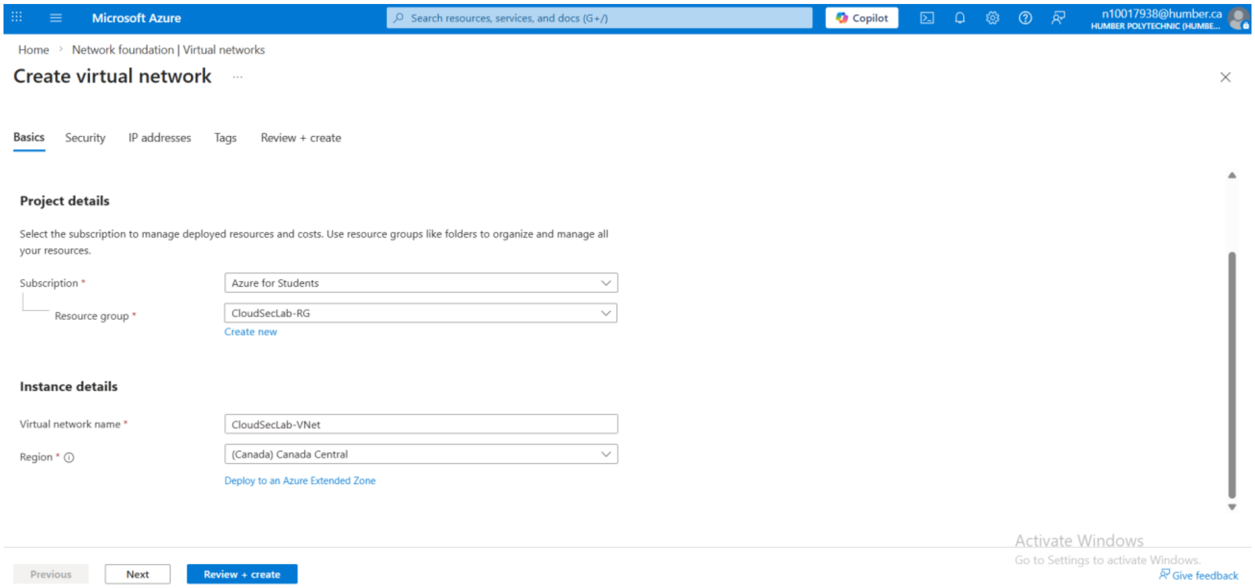
Step 2: Create the Virtual Network

Before creating subnets, we need a Virtual Network (VNet) to contain them. Think of the VNet as the private network boundary for your entire infrastructure nothing inside it is reachable from the internet unless you explicitly allow it.

Instructions

1. In the Azure Portal search bar, type **Virtual Networks** and select it
2. Click **+ Create**
3. Under the **Basics** tab:
   - **Resource Group:** CloudSecLab-RG
   - **Name:** CloudSecLab-VNet
   - **Region:** Same region as your resource group
4. Under the **IP Addresses** tab:
   - Set the **IPv4 address space** to 10.0.0.0/16 this gives the entire VNet a pool of 65,536 IP addresses
   - Delete any default subnet that Azure adds automatically you will create your own in the next steps

5. Click **Review + Create**, then **Create**


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
n10017938@humber.ca
HUMBER POLYTECHNIC (HUMBE...
Home > Network foundation | Virtual networks
Basics
Security
IP addresses
Tags
Review + create
Create new
Deploy to an Azure Extended Zone
Activate Windows
Go to Settings to activate Windows.
Previous
Next
Review + create
Give feedback

Create virtual network

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Azure for Students

Resource group * CloudSecLab-RG

Instance details

Virtual network name * CloudSecLab-VNet

Region * (Canada) Canada Central

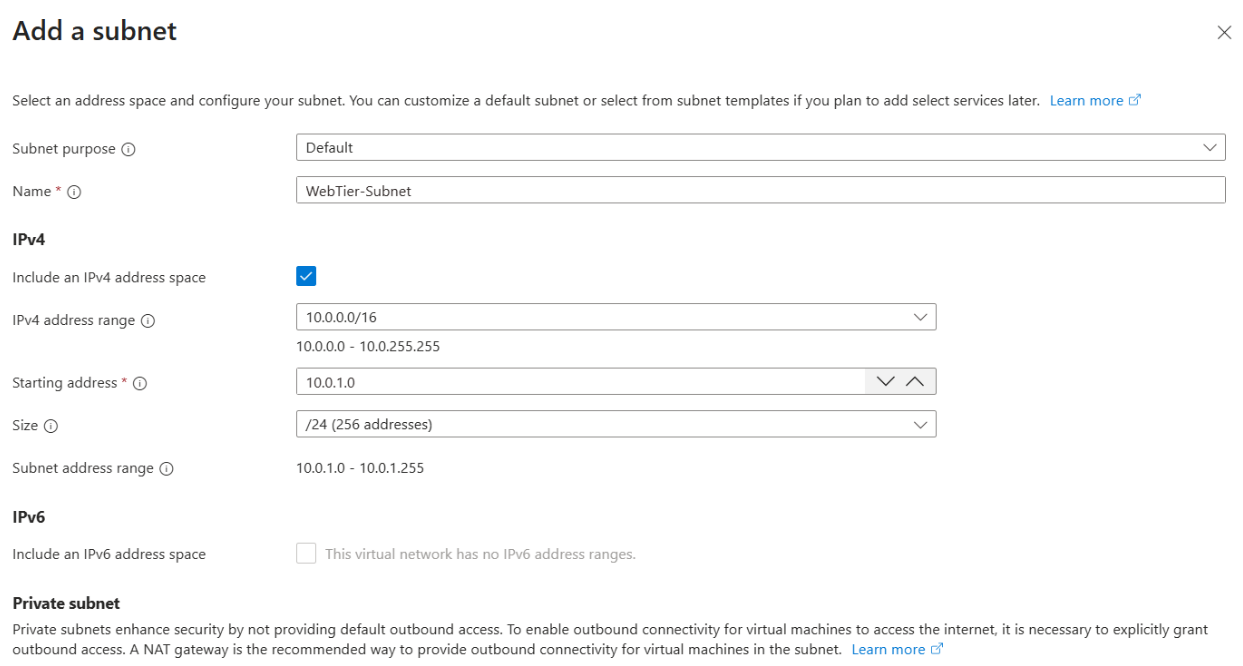
Step 3: Create the Web Tier Subnet

A subnet is a subdivision of your virtual network's address space. Segmenting your infrastructure into separate subnets is a core security practice it lets you apply different access rules to different parts of your system. The Web Tier subnet will host your public-facing web server.

Instructions

1. Navigate to your newly created CloudSecLab-VNet
2. In the left menu, select **Subnets**
3. Click **+ Subnet**
4. Fill in the following:
   - **Name:** WebTier-Subnet
   - **Subnet address range:** 10.0.1.0/24
5. Leave all other settings as default and click **Save**

Note: A /24 subnet provides **256 total IP addresses** (ranging from 10.0.1.0 to 10.0.1.255). Azure reserves the first 4 and last 1 address for internal use, leaving **251 usable IPs** for your resources.



Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more

Subnet purpose: Default

Name *: WebTier-Subnet

IPv4

Include an IPv4 address space: ☑

IPv4 address range: 10.0.0.0/16

10.0.0.0 - 10.0.255.255

Starting address *: 10.0.1.0

Size: /24 (256 addresses)

Subnet address range: 10.0.1.0 - 10.0.1.255

IPv6

Include an IPv6 address space: □ This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more

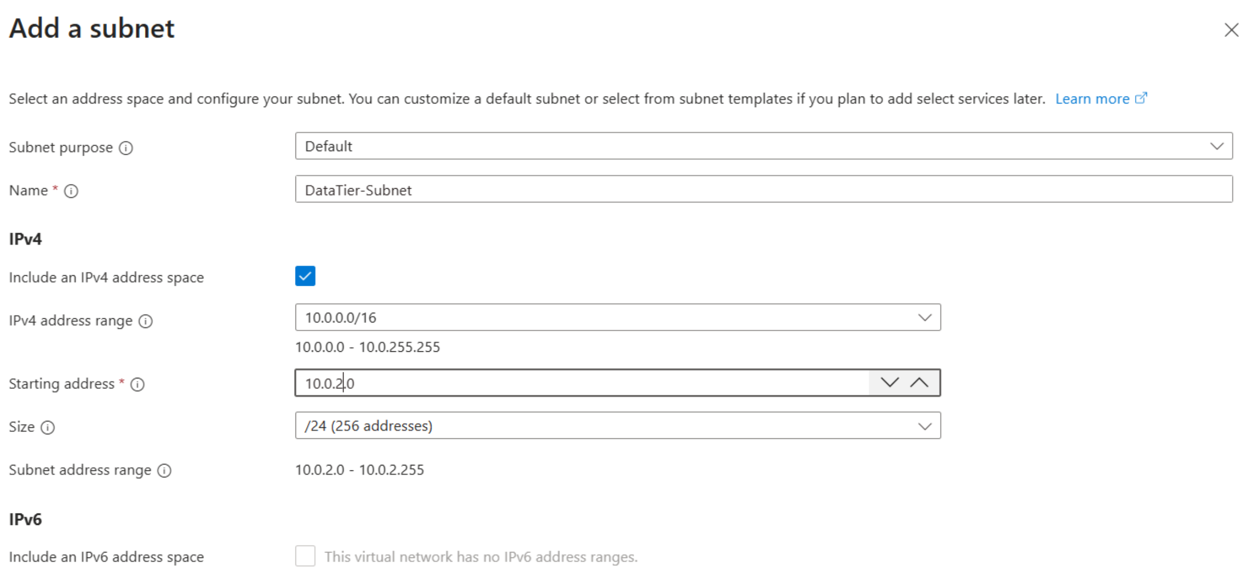
Step 4: Create the Database Tier Subnet

The Database Tier subnet is intentionally hidden from the public internet. No resource in this subnet will be assigned a public IP address all communication to the database will flow through the internal private network from the web tier.

Instructions

1. Within CloudSecLab-VNet, go to **Subnets**
2. Click **+ Subnet**
3. Fill in the following:
   - **Name:** DataTier-Subnet
   - **Subnet address range:** 10.0.2.0/24
4. Leave all other settings as default and click **Save**

Note: Like the WebTier-Subnet, this /24 block provides 256 addresses (10.0.2.0 to 10.0.2.255) with 251 usable. Your database server will be assigned 10.0.2.4.


Add a subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more

Subnet purpose: Default

Name *: DataTier-Subnet

IPv4

Include an IPv4 address space: ☑

IPv4 address range: 10.0.0.0/16

10.0.0.0 - 10.0.255.255

Starting address *: 10.0.2.0

Size: /24 (256 addresses)

Subnet address range: 10.0.2.0 - 10.0.2.255

IPv6

Include an IPv6 address space: □ This virtual network has no IPv6 address ranges.

Step 5: Create the Web Server Virtual Machine

The Web Server VM is the public-facing component of your infrastructure. It runs Apache on Ubuntu and sits inside the WebTier-Subnet, acting as the only entry point for internet traffic into your architecture.

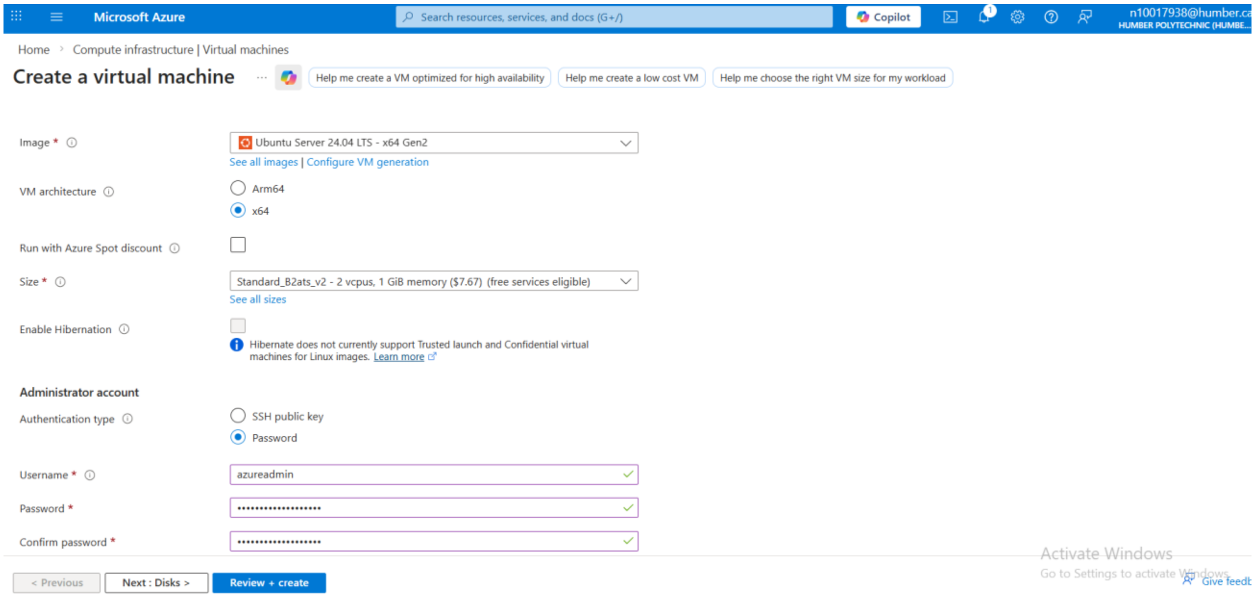
1. In the Azure Portal search bar, type **Virtual Machines** → click **+ Create** → **Azure Virtual Machine**
2. Under the **Basics** tab, configure the following:
   - **Resource Group:** CloudSecLab-RG
   - **Virtual Machine Name:** WebServer-VM
   - **Region:** Same as your VNet
   - **Image:** Ubuntu Server 22.04 LTS
   - **Size:** Standard_B1s (Free Tier)
   - **Authentication Type:** SSH public key
   - **Username:** azureuser
   - **Public Inbound Ports:** Allow selected ports → **HTTP (80), SSH (22)**
3. Click through **Disks** tab leaving all defaults, then proceed to **Networking**

4. Under the **Networking** tab, configure:

   - **Virtual Network:** CloudSecLab-VNet
   - **Subnet:** WebTier-Subnet (10.0.1.0/24)
   - **Public IP:** (new) WebServer-VM-ip
   - **NIC Network Security Group:** Basic
   - **Inbound Ports:** HTTP (80), SSH (22)

5. Click **Review + Create** → once validation passes, click **Create**

6. Once deployed, go to the VM overview and note down the **Public IP address** and confirm the **Private IP** is 10.0.1.4


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
n10017938@humber.ca
HUMBER POLYTECHNIC (HUMBE...
Home › Compute infrastructure | Virtual machines
Help me create a VM optimized for high availability
Help me create a low cost VM
Help me choose the right VM size for my workload
< Previous
Next : Disks >
Review + create
Give feedb

Create a virtual machine

Image * : Ubuntu Server 24.04 LTS - x64 Gen2
See all images | Configure VM generation

VM architecture: ○ Arm64 ● x64

Run with Azure Spot discount: □

Size * : Standard_B2ats_v2 - 2 vcpus, 1 GiB memory ($7.67) (free services eligible)
See all sizes

Enable Hibernation: □
Hibernate does not currently support Trusted launch and Confidential virtual machines for Linux images. Learn more

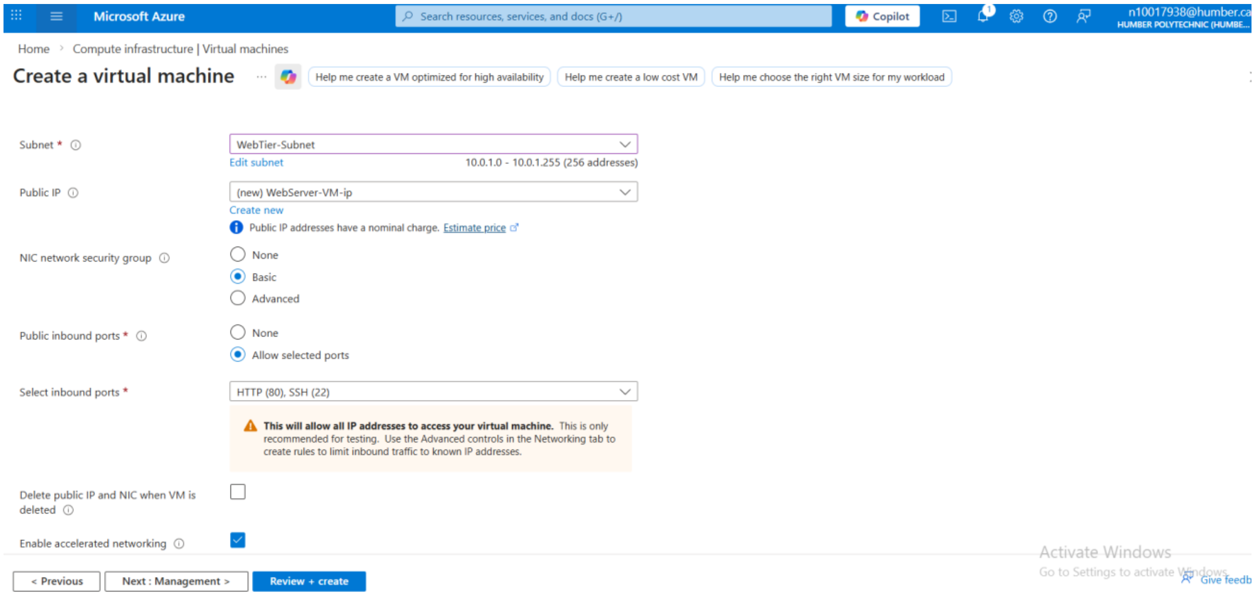
Administrator account

Authentication type: ○ SSH public key ● Password

Username * : azureadmin ✓

Password * : ••••••••••••••••••• ✓

Confirm password * : ••••••••••••••••••• ✓


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
n10017938@humber.ca
HUMBER POLYTECHNIC (HUMBE...
Home > Compute infrastructure | Virtual machines
Help me create a VM optimized for high availability
Help me create a low cost VM
Help me choose the right VM size for my workload
Edit subnet
Create new
Estimate price
< Previous
Next : Management >
Review + create
Activate Windows
Go to Settings to activate Windows.
Give feedb

Create a virtual machine

Subnet *: WebTier-Subnet
10.0.1.0 - 10.0.1.255 (256 addresses)

Public IP: (new) WebServer-VM-ip
Public IP addresses have a nominal charge.

NIC network security group: ○ None ● Basic ○ Advanced

Public inbound ports *: ○ None ● Allow selected ports

Select inbound ports *: HTTP (80), SSH (22)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

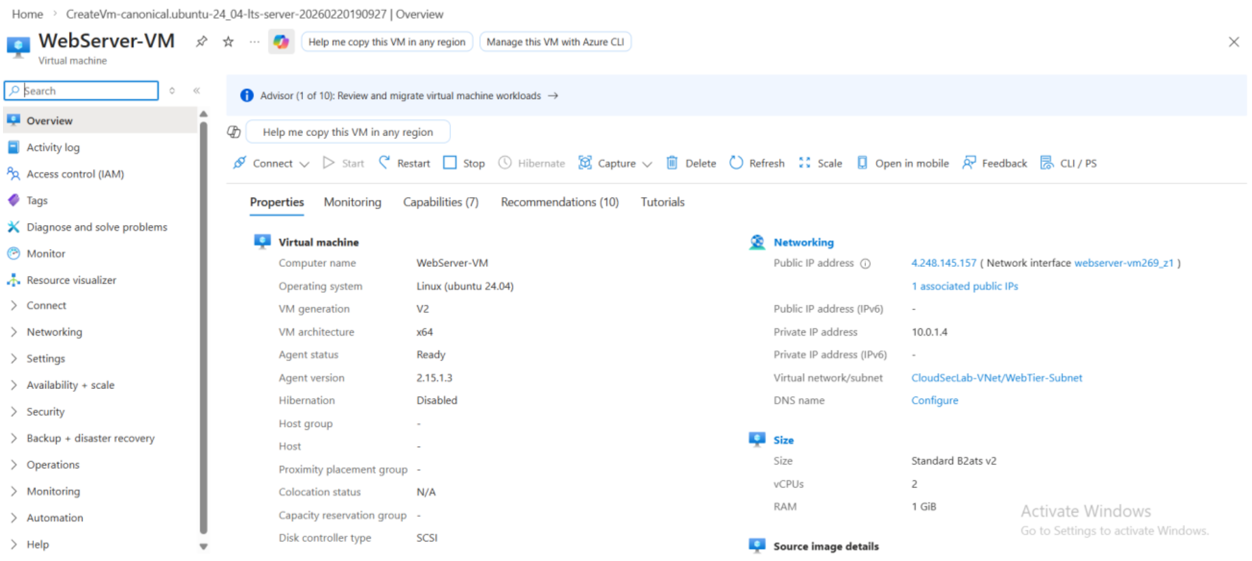
Delete public IP and NIC when VM is deleted: □

Enable accelerated networking: ☑

Step 6.1: Install Web Server

1. Once deployed, click **Go to resource**
2. Note the **Public IP address** (you'll need this)
3. Click **Connect** > **SSH**
4. Open your Azure CLI terminal on the bar and SSH to the VM:
5. Write the Following commands on Bash

```
ssh azureadmin@<PUBLIC_IP>

sudo apt update

sudo apt install apache2 -y

sudo systemctl start apache2

sudo systemctl enable apache2

echo "<h1>Web Server - Cloud Security Lab</h1>" | sudo tee /var/www/html/index.html
```



Virtual machine

Computer name WebServer-VM
Operating system Linux (ubuntu 24.04)
VM generation V2
VM architecture x64
Agent status Ready
Agent version 2.15.1.3
Hibernation Disabled
Host group -
Host -
Proximity placement group -
Colocation status N/A
Capacity reservation group -
Disk controller type SCSI

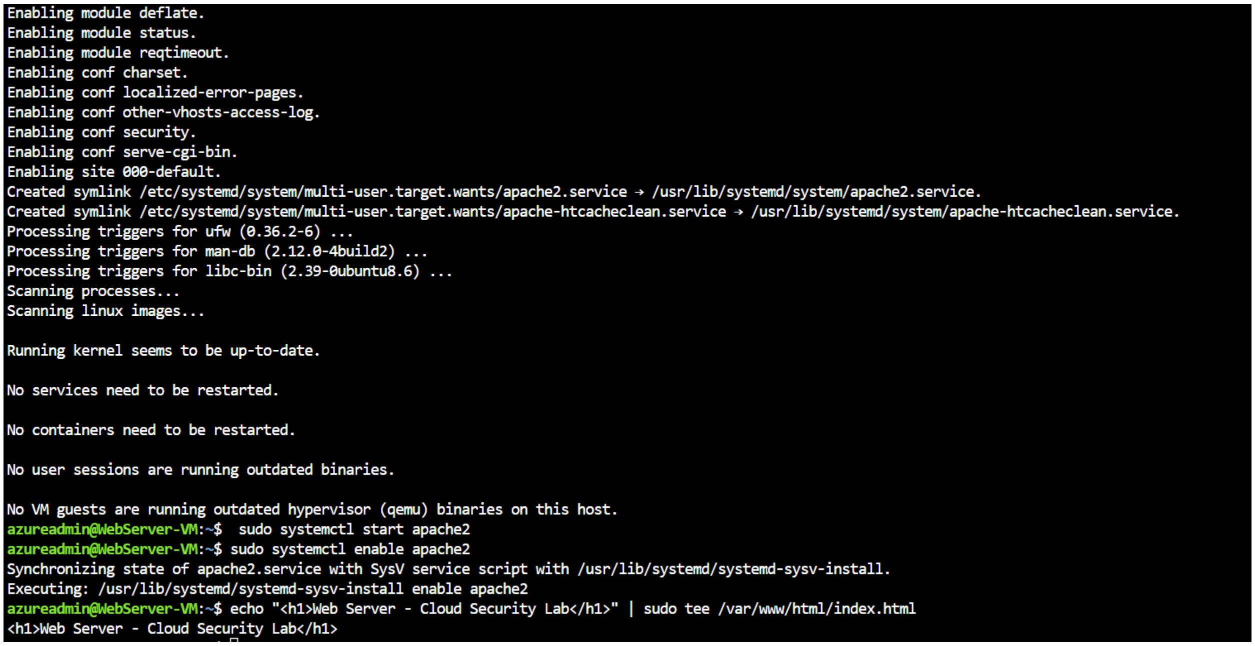
Networking

Public IP address 4.248.145.157 (Network interface webserver-vm269_z1)
1 associated public IPs
Public IP address (IPv6) -
Private IP address 10.0.1.4
Private IP address (IPv6) -
Virtual network/subnet CloudSecLab-VNet/WebTier-Subnet
DNS name Configure

Size

Size Standard B2ats v2
vCPUs 2
RAM 1 GiB

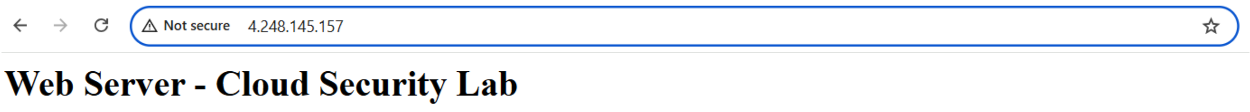
Source image details



```
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /usr/lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /usr/lib/systemd/system/apache-htcacheclean.service.
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu8.6) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
azureadmin@WebServer-VM:~$  sudo systemctl start apache2
azureadmin@WebServer-VM:~$ sudo systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable apache2
azureadmin@WebServer-VM:~$ echo "<h1>Web Server - Cloud Security Lab</h1>" | sudo tee /var/www/html/index.html
<h1>Web Server - Cloud Security Lab</h1>
```

1. Test by opening a browser and navigating to: http://<PUBLIC_IP>

   - You should see "Web Server - Cloud Security Lab"



Web Server - Cloud Security Lab

Step 7.1: Create Database Server

Unlike the Web Server, the Database VM is completely hidden from the internet. It has no public IP address and accepts no direct inbound connections from outside the virtual network. The only machine that can reach it is the Web Server, through the private internal network, this is the core of the defense-in-depth architecture you are building.

1. Go back to **Virtual machines** > **+ Create**
2. Fill in the **Basics** tab:

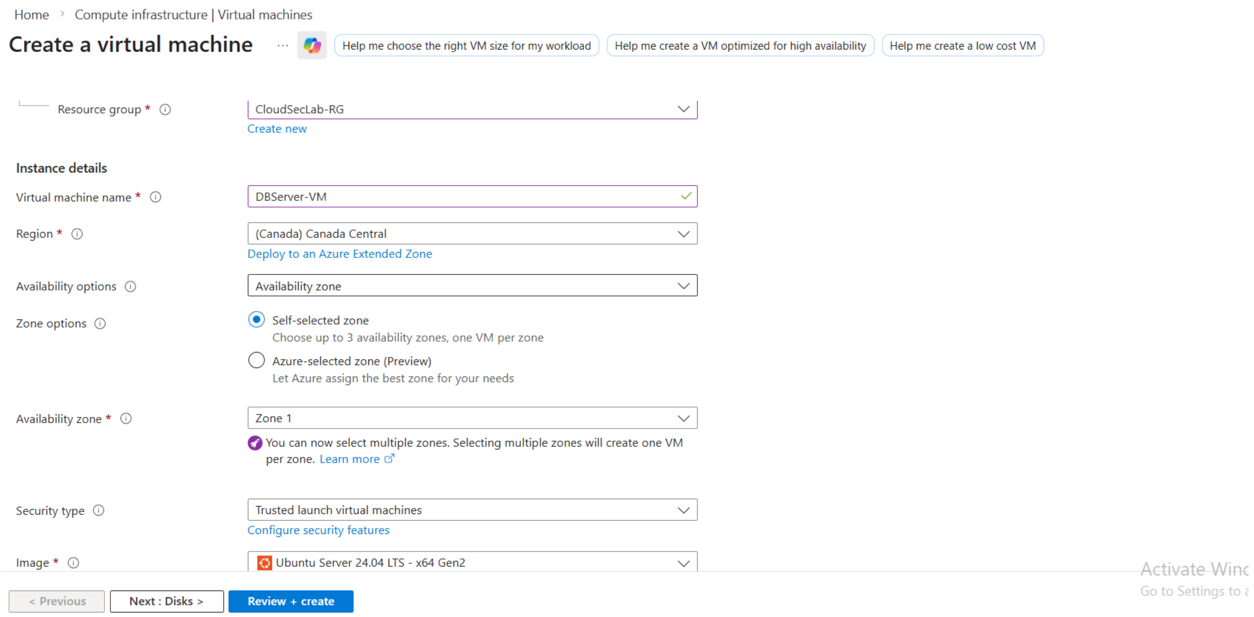
- **Resource group:** CloudSecLab-RG
- **Virtual machine name:** DBServer-VM
- **Region:** Same as before
- **Image:** Ubuntu Server 22.04 LTS - x64 Gen2
- **Size:** Standard_B1s
- **Authentication type:** Password

- **Username:** azureadmin
- **Public inbound ports:** None

1. Click **Next: Networking**:

- **Virtual network:** CloudSecLab-VNet
- **Subnet:** DataTier-Subnet (10.0.2.0/24)
- **Public IP:** None
- **NIC network security group:** Basic
- **Public inbound ports:** None

1. Click **Review + create** > **Create**



Home › Compute infrastructure | Virtual machines

Create a virtual machine

···
Help me choose the right VM size for my workload
Help me create a VM optimized for high availability
Help me create a low cost VM

Resource group * ⓘ CloudSecLab-RG

Instance details

Virtual machine name * ⓘ DBServer-VM ✓

Region * ⓘ (Canada) Canada Central

Deploy to an Azure Extended Zone

Availability options ⓘ Availability zone

Zone options ⓘ

● Self-selected zone
Choose up to 3 availability zones, one VM per zone

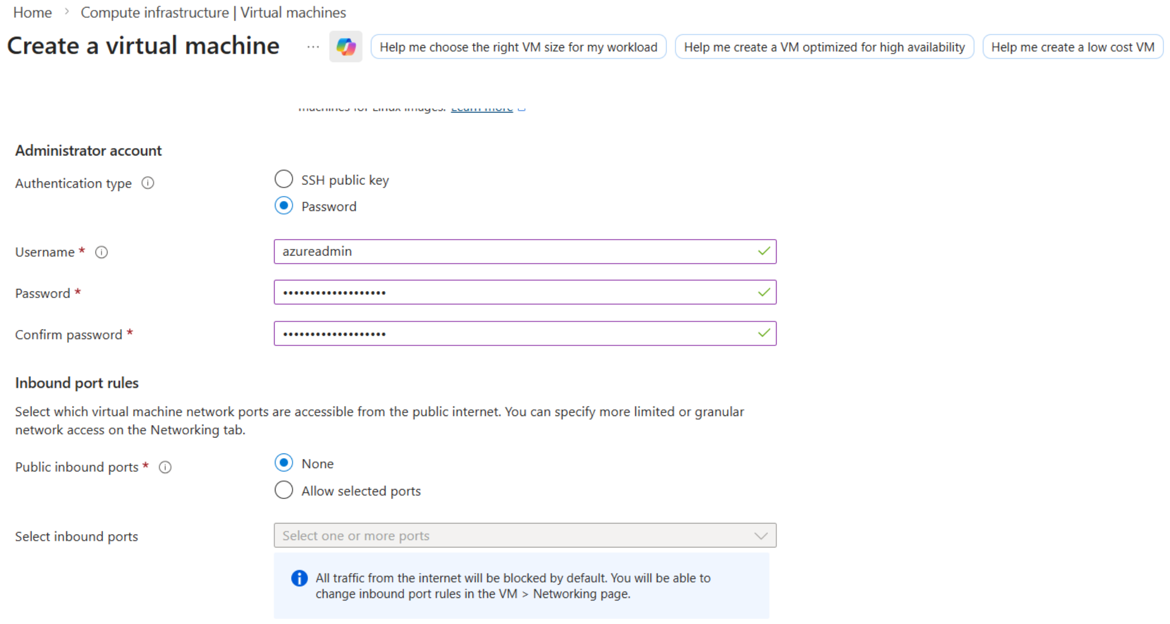
○ Azure-selected zone (Preview)
Let Azure assign the best zone for your needs

Availability zone * ⓘ Zone 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. Learn more

Security type ⓘ Trusted launch virtual machines

Image * ⓘ Ubuntu Server 24.04 LTS - x64 Gen2



Home › Compute infrastructure | Virtual machines

Create a virtual machine

···
Help me choose the right VM size for my workload
Help me create a VM optimized for high availability
Help me create a low cost VM

machines for Linux images. Learn more

Administrator account

Authentication type ⓘ ○ SSH public key ● Password

Username * ⓘ azureadmin ✓

Password * •••••••••••••••••••• ✓

Confirm password * •••••••••••••••••••• ✓

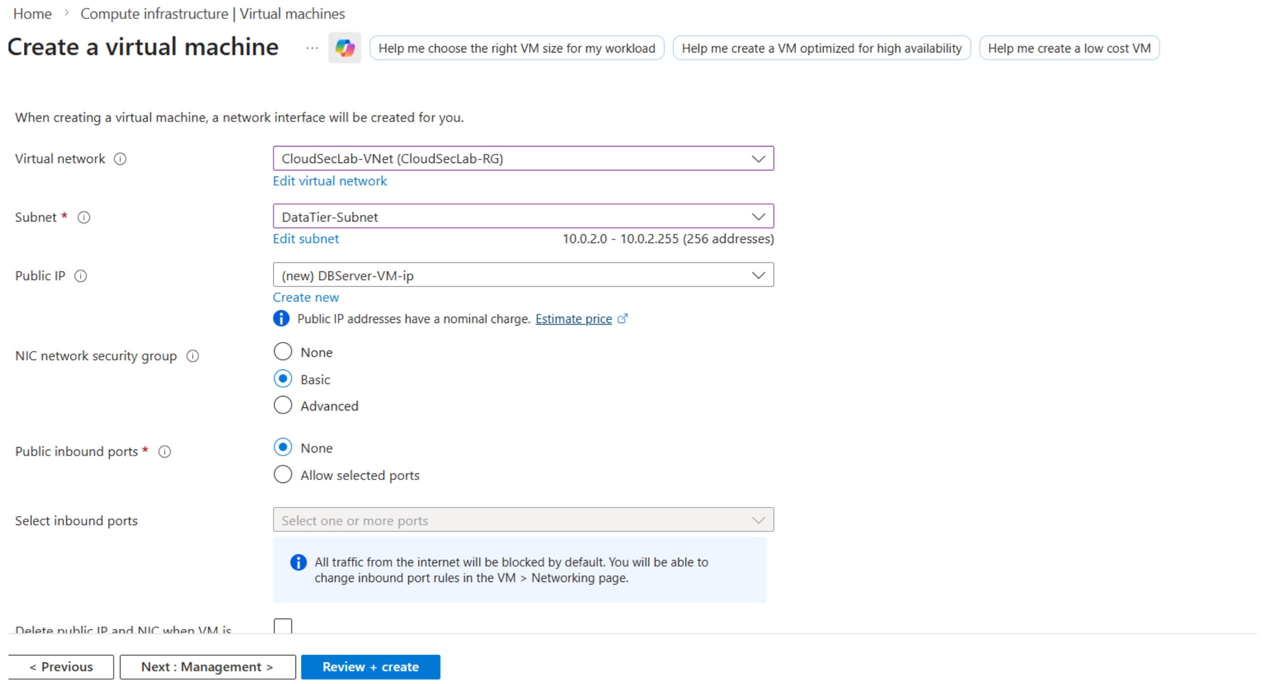
Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ⓘ ● None ○ Allow selected ports

Select inbound ports: Select one or more ports

ⓘ All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.



Home › Compute infrastructure | Virtual machines

Create a virtual machine

···
Help me choose the right VM size for my workload
Help me create a VM optimized for high availability
Help me create a low cost VM

When creating a virtual machine, a network interface will be created for you.

Virtual network ⓘ CloudSecLab-VNet (CloudSecLab-RG)
Edit virtual network

Subnet * ⓘ DataTier-Subnet
Edit subnet 10.0.2.0 - 10.0.2.255 (256 addresses)

Public IP ⓘ (new) DBServer-VM-ip
Create new
ⓘ Public IP addresses have a nominal charge. Estimate price

NIC network security group ⓘ ○ None ● Basic ○ Advanced

Public inbound ports * ⓘ ● None ○ Allow selected ports

Select inbound ports: Select one or more ports

ⓘ All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Delete public IP and NIC when VM is □

Step 7.2: Install MySQL

1. Once deployed, you need to access this VM through the Web Server (since it has no public IP)
2. SSH to your Web Server first using azure admin in your web server using Azure CLI:

```
ssh azureadmin@<WEB_SERVER_PUBLIC_IP>
```

1. From the Web Server, SSH to the DB Server using its **private IP**:
    - Find the DB Server's private IP in the Azure Portal (should be 10.0.2.4 or similar)

ssh azureadmin@10.0.2.4

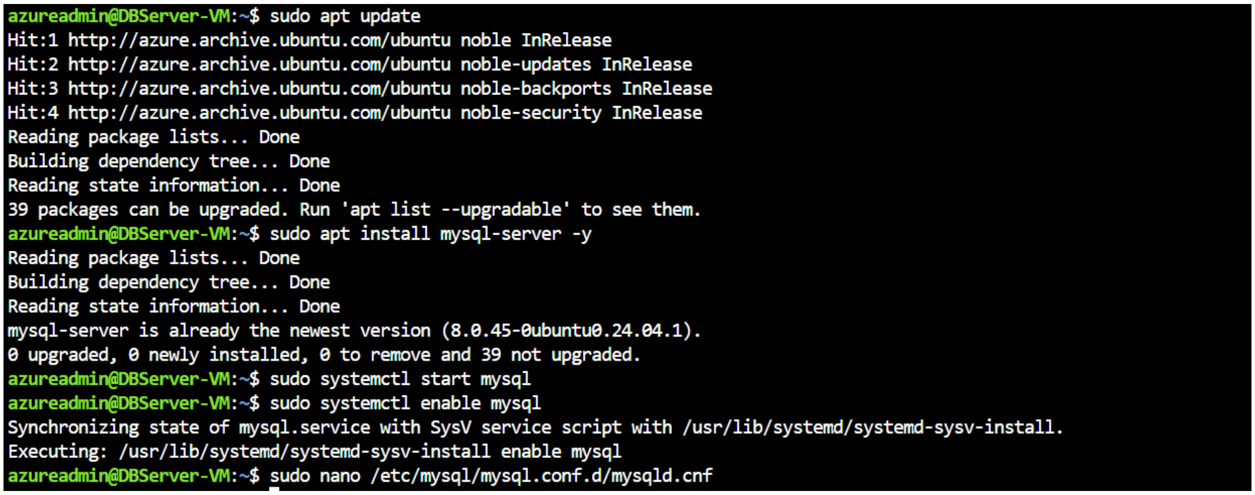
Install MySQL:

sudo apt update

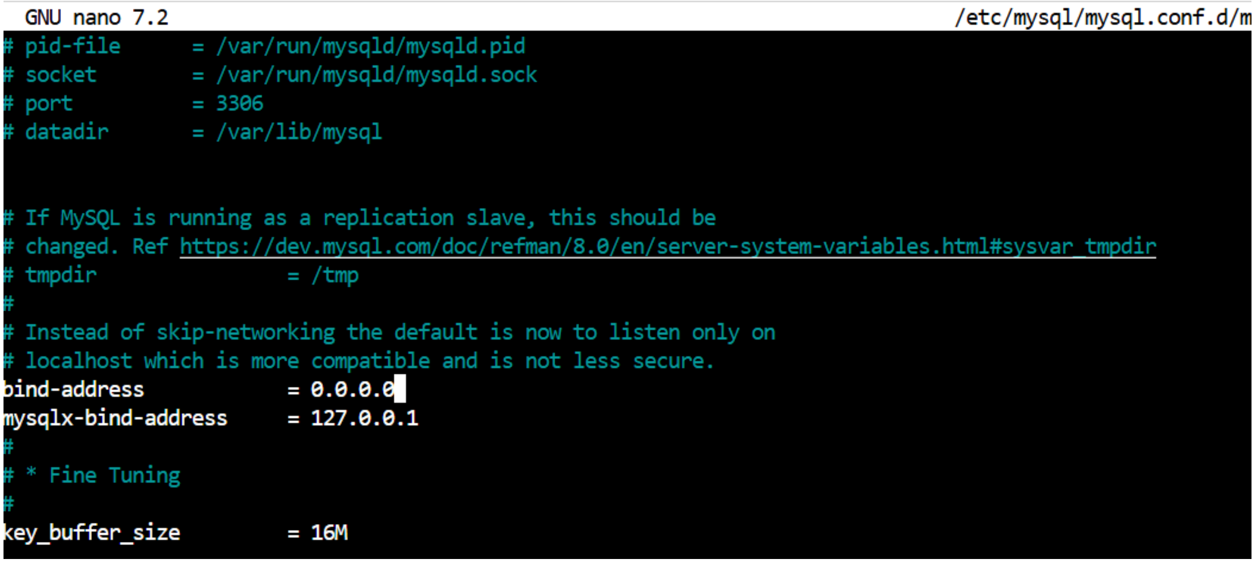
sudo apt install mysql-server -y

sudo systemctl start mysql

sudo systemctl enable mysql



```
azureadmin@DBServer-VM:~$ sudo apt update
Hit:1 http://azure.archive.ubuntu.com/ubuntu noble InRelease
Hit:2 http://azure.archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:3 http://azure.archive.ubuntu.com/ubuntu noble-backports InRelease
Hit:4 http://azure.archive.ubuntu.com/ubuntu noble-security InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
39 packages can be upgraded. Run 'apt list --upgradable' to see them.
azureadmin@DBServer-VM:~$ sudo apt install mysql-server -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
mysql-server is already the newest version (8.0.45-0ubuntu0.24.04.1).
0 upgraded, 0 newly installed, 0 to remove and 39 not upgraded.
azureadmin@DBServer-VM:~$ sudo systemctl start mysql
azureadmin@DBServer-VM:~$ sudo systemctl enable mysql
Synchronizing state of mysql.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable mysql
azureadmin@DBServer-VM:~$ sudo nano /etc/mysql/mysql.conf.d/mysqld.cnf
```



```
  GNU nano 7.2                                              /etc/mysql/mysql.conf.d/m
# pid-file      = /var/run/mysqld/mysqld.pid
# socket        = /var/run/mysqld/mysqld.sock
# port          = 3306
# datadir       = /var/lib/mysql


# If MySQL is running as a replication slave, this should be
# changed. Ref https://dev.mysql.com/doc/refman/8.0/en/server-system-variables.html#sysvar_tmpdir
# tmpdir                = /tmp
#
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 0.0.0.0
mysqlx-bind-address     = 127.0.0.1
#
# * Fine Tuning
#
key_buffer_size         = 16M
```

Part 8: Demonstrate Insecure Configuration

Step 8.1: Test Current Security Posture

Before applying proper Network Security Group rules, it is important to understand what our environment currently looks like from a security perspective. Right now, our VMs are running with minimal controls SSH is open to the entire internet on the web server, and no granular NSG rules are in place.

- From our Web Server, install a MySQL client:

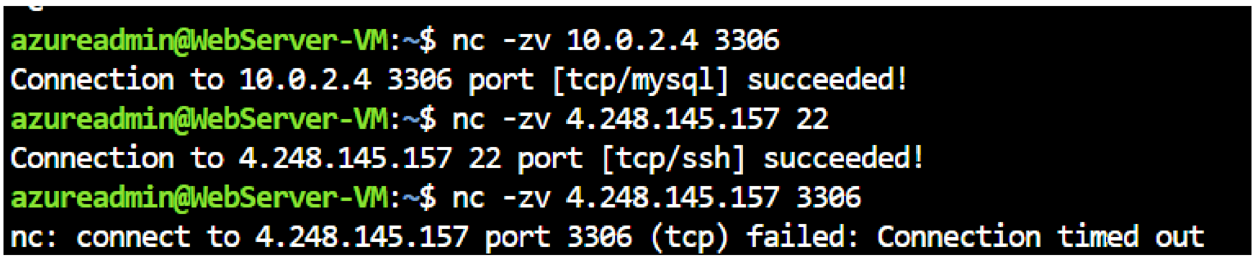
bash

```
 sudo apt install mysql-client -y

 nc -zv 10.0.2.4 3306
```

-From your **local machine**, try to access the Web Server on different ports:

bash

```
 # Test SSH (should work - this is a security risk!)

 nc -zv <WEB_SERVER_PUBLIC_IP> 22

 # Test MySQL (should fail - no public IP)

 nc -zv <WEB_SERVER_PUBLIC_IP> 3306
```



```
azureadmin@WebServer-VM:~$ nc -zv 10.0.2.4 3306
Connection to 10.0.2.4 3306 port [tcp/mysql] succeeded!
azureadmin@WebServer-VM:~$ nc -zv 4.248.145.157 22
Connection to 4.248.145.157 22 port [tcp/ssh] succeeded!
azureadmin@WebServer-VM:~$ nc -zv 4.248.145.157 3306
nc: connect to 4.248.145.157 port 3306 (tcp) failed: Connection timed out
```

Drawbacks:

A successful SSH connection from any IP address means your web server is exposed to the entire internet on a management port. Automated scanning tools can brute force the internet for open SSH ports your VM will typically appear in these scans within minutes of being deployed.

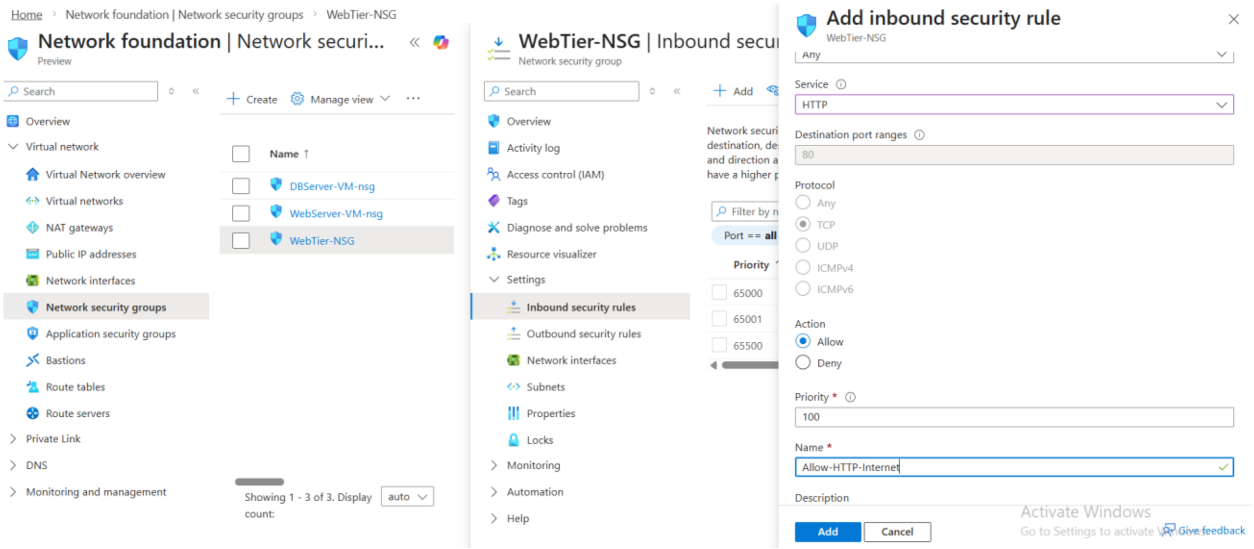
Step 9

Network Security Groups are designed to eliminate. In the next step you will restrict SSH access to your specific IP address only reducing your exposure from the entire internet down to a single trusted source.

Now that your VMs are deployed and you have seen the risks of an unsecured configuration, it is time to implement proper security controls. Network Security Groups (NSGs) act as virtual firewalls, they inspect every packet entering or leaving a subnet and either allow or deny it based on rules you define.

Rule 1: Allow HTTP from Internet

- **Source:** Any
- **Source port ranges:** *
- **Destination:** Any
- **Service:** HTTP
- **Destination port ranges:** 80
- **Protocol:** TCP
- **Action:** Allow
- **Priority:** 100
- **Name:** Allow-HTTP-Internet



Any

Service: HTTP

Destination port ranges: 80

Protocol: ○ Any ● TCP ○ UDP ○ ICMPv4 ○ ICMPv6

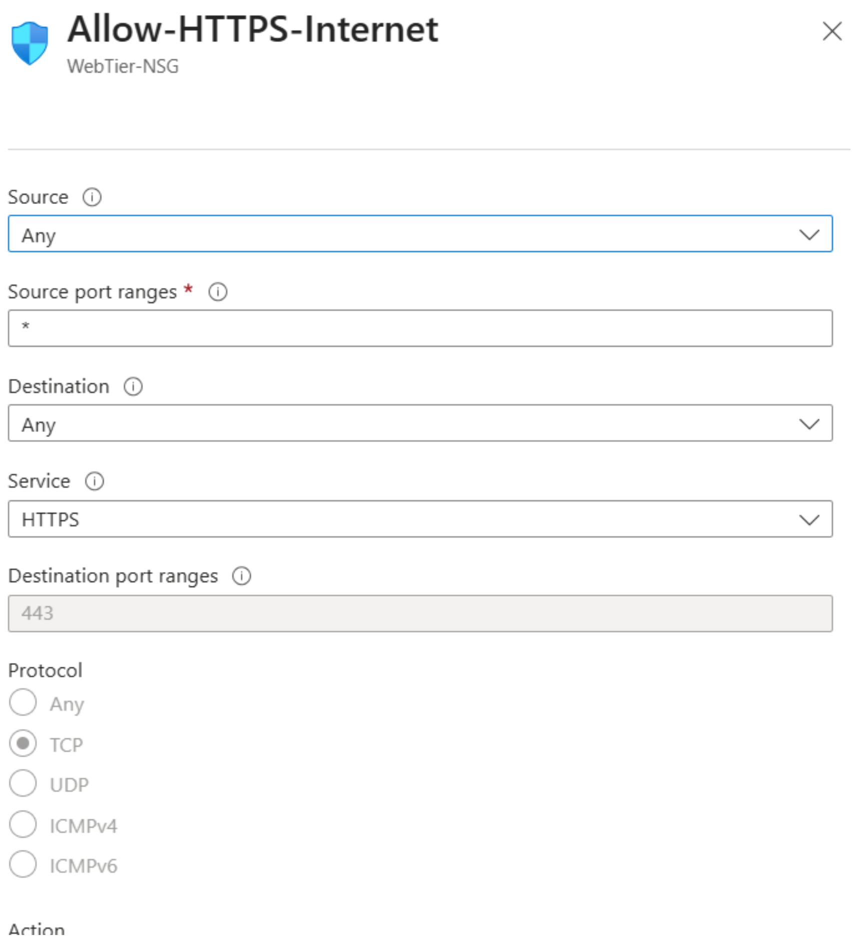
Action: ● Allow ○ Deny

Priority *: 100

Name *: Allow-HTTP-Internet

Rule 2: Allow HTTPS from Internet (for future use)

- **Source:** Any
- **Source port ranges:** *
- **Destination:** Any
- **Service:** HTTPS
- **Destination port ranges:** 443
- **Protocol:** TCP
- **Action:** Allow
- **Priority:** 110
- **Name:** Allow-HTTPS-Internet



Allow-HTTPS-Internet

WebTier-NSG

Source: Any

Source port ranges *: *

Destination: Any

Service: HTTPS

Destination port ranges: 443

Protocol

○ Any

● TCP

○ UDP

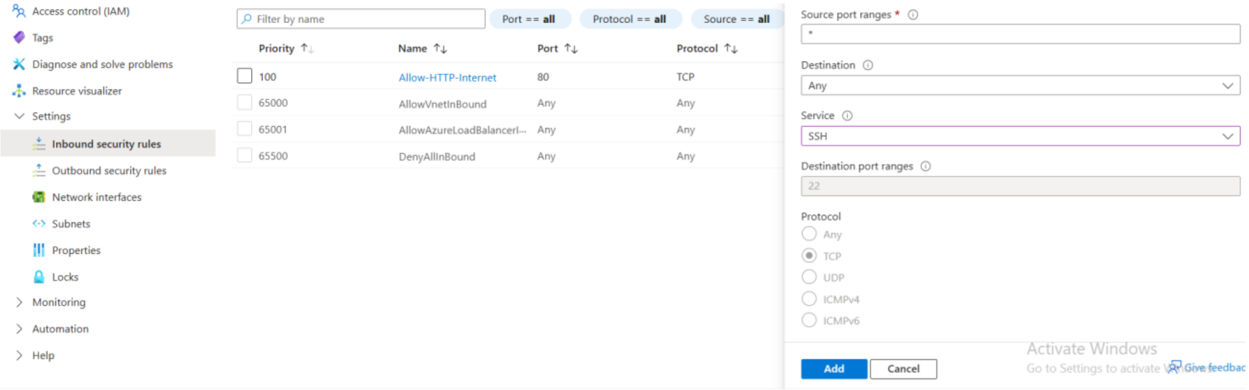
○ ICMPv4

○ ICMPv6

- Action

Rule 3: Allow SSH from Your IP Only (more secure)

- **Source:** IP Addresses
- **Source IP addresses/CIDR ranges:** [Your public IP - find at whatismyip.com]
- **Source port ranges:** *
- **Destination:** Any
- **Service:** SSH
- **Destination port ranges:** 22
- **Protocol:** TCP
- **Action:** Allow
- **Priority:** 120
- **Name:** Allow-SSH-MyIP



	Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓
□	100	Allow-HTTP-Internet	80	TCP
□	65000	AllowVnetInBound	Any	Any
□	65001	AllowAzureLoadBalancerI...	Any	Any
□	65500	DenyAllInBound	Any	Any

Source port ranges * : *

Destination: Any

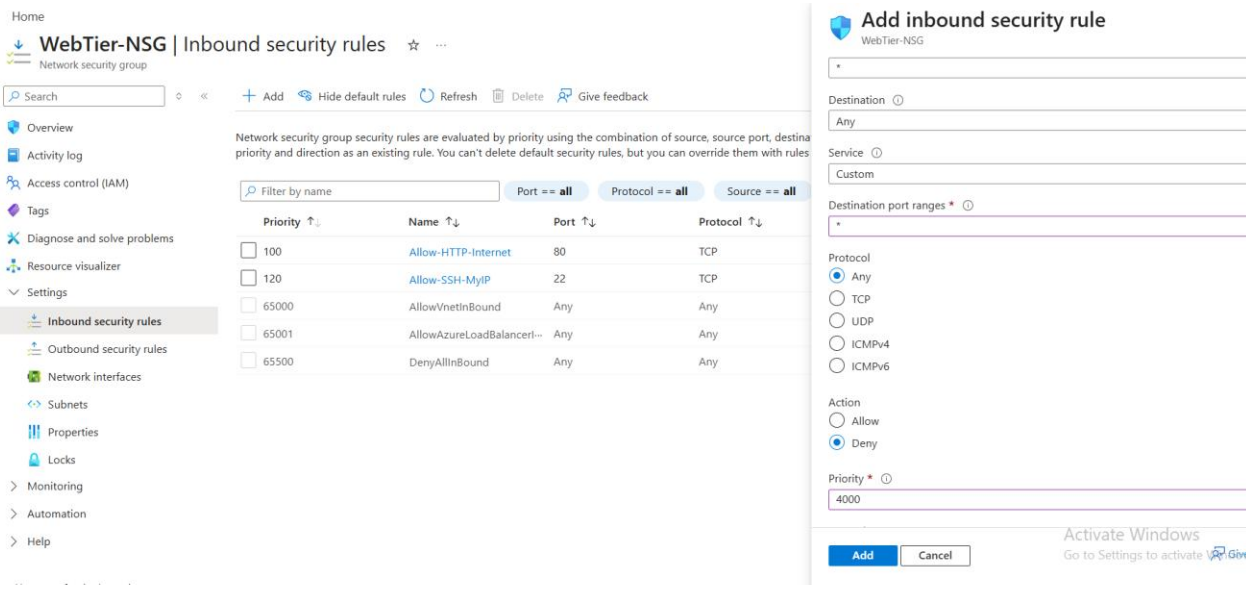
Service: SSH

Destination port ranges: 22

Protocol
○ Any
● TCP
○ UDP
○ ICMPv4
○ ICMPv6

Rule 4: Deny All Other Inbound (explicit deny)

- **Source:** Any
- **Source port ranges:** *
- **Destination:** Any
- **Service:** Custom
- **Destination port ranges:** *
- **Protocol:** Any
- **Action:** Deny
- **Priority:** 4000
- **Name:** Deny-All-Inbound



Network security group security rules are evaluated by priority using the combination of source, source port, destina priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules

	Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓
☐	100	Allow-HTTP-Internet	80	TCP
☐	120	Allow-SSH-MyIP	22	TCP
☐	65000	AllowVnetInBound	Any	Any
☐	65001	AllowAzureLoadBalancerI···	Any	Any
☐	65500	DenyAllInBound	Any	Any

Add inbound security rule
WebTier-NSG

*

Destination ⓘ
Any

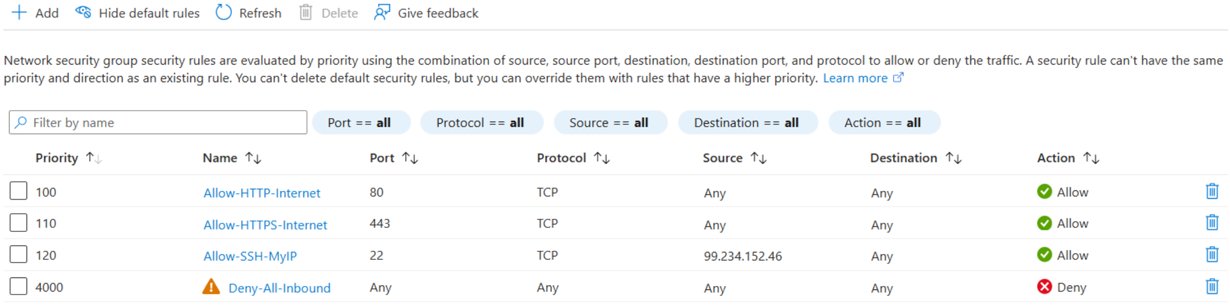
Service ⓘ
Custom

Destination port ranges * ⓘ
*

Protocol
● Any
○ TCP
○ UDP
○ ICMPv4
○ ICMPv6

Action
○ Allow
● Deny

Priority * ⓘ
4000



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

	Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
☐	100	Allow-HTTP-Internet	80	TCP	Any	Any	✓ Allow
☐	110	Allow-HTTPS-Internet	443	TCP	Any	Any	✓ Allow
☐	120	Allow-SSH-MyIP	22	TCP	99.234.152.46	Any	✓ Allow
☐	4000	⚠ Deny-All-Inbound	Any	Any	Any	Any	✕ Deny

Step 10: Create NSG for Data Tier

1. Create another NSG named DataTier-NSG (same steps as 5.1)
2. Configure inbound rules:

Rule 1: Allow MySQL from Web Tier Only

- **Source:** IP Addresses
- **Source IP addresses/CIDR ranges:** 10.0.1.0/24
- **Source port ranges:** *
- **Destination:** Any
- **Service:** Custom
- **Destination port ranges:** 3306
- **Protocol:** TCP
- **Action:** Allow

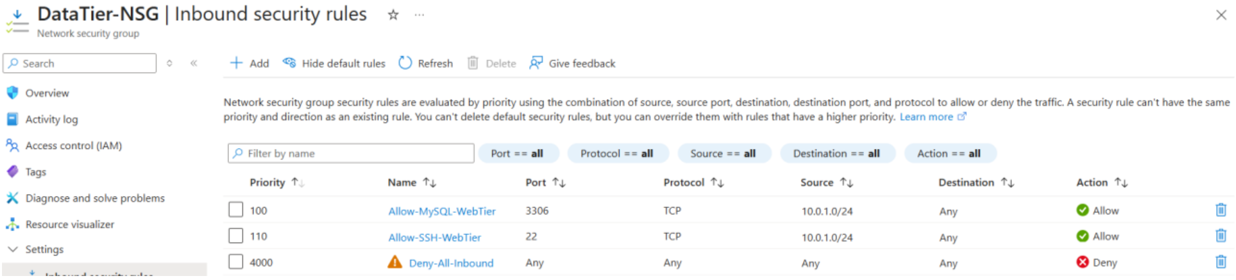
- **Priority:** 100
- **Name:** Allow-MySQL-WebTier
- Click **Add**

Rule 2: Allow SSH from Web Tier Only (for management)

- **Source:** IP Addresses
- **Source IP addresses/CIDR ranges:** 10.0.1.0/24
- **Source port ranges:** *
- **Destination:** Any
- **Service:** SSH
- **Destination port ranges:** 22
- **Protocol:** TCP
- **Action:** Allow
- **Priority:** 110
- **Name:** Allow-SSH-WebTier
- Click **Add**

Rule 3: Deny All Other Inbound

- **Source:** Any
- **Source port ranges:** *
- **Destination:** Any
- **Service:** Custom
- **Destination port ranges:** *
- **Protocol:** Any
- **Action:** Deny
- **Priority:** 4000
- **Name:** Deny-All-Inbound
- Click **Add**



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
100	Allow-MySQL-WebTier	3306	TCP	10.0.1.0/24	Any	✓ Allow
110	Allow-SSH-WebTier	22	TCP	10.0.1.0/24	Any	✓ Allow
4000	Deny-All-Inbound	Any	Any	Any	Any	✗ Deny

Step 11: Associate NSGs with Subnets

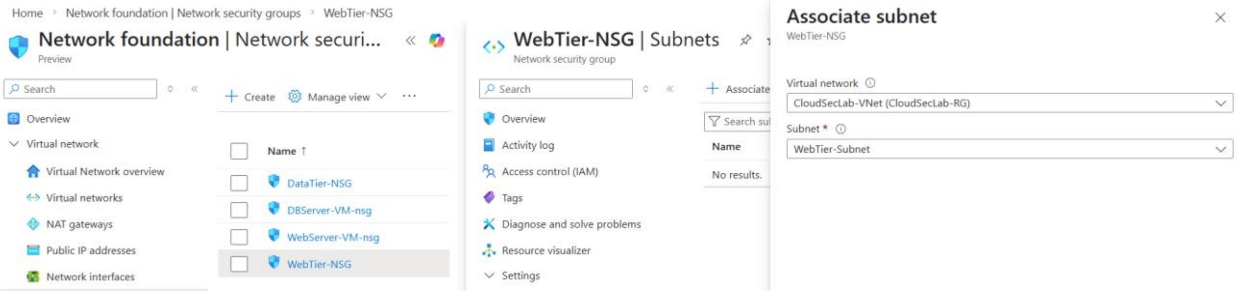
1. Go to **WebTier-NSG**
2. Click **Subnets** on the left
3. Click **+ Associate**

Select:

1. **Virtual network:** CloudSecLab-VNet
2. **Subnet:** WebTier-Subnet

   Click **OK**

1. Repeat for **DataTier-NSG**:
2. Associate with **DataTier-Subnet**

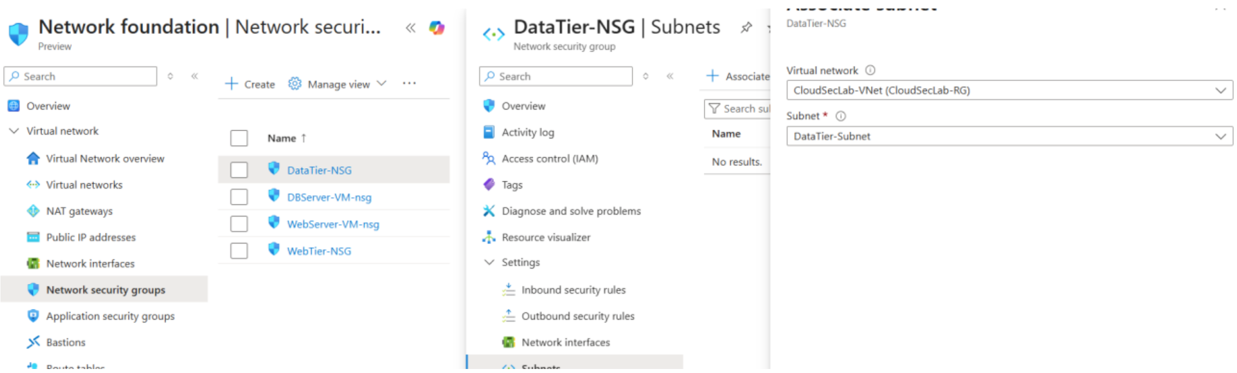


DataTier-NSG
DBServer-VM-nsg
WebServer-VM-nsg
WebTier-NSG

Associate subnet
WebTier-NSG

Virtual network: CloudSecLab-VNet (CloudSecLab-RG)

Subnet *: WebTier-Subnet



Virtual network: CloudSecLab-VNet (CloudSecLab-RG)

Subnet *: DataTier-Subnet

Test Security Controls

Step 12: Test Web Tier Access

From your local machine:

bash

```
curl http://<WEB_SERVER_PUBLIC_IP>
```

- Should display your web page

Test SSH from your your command prompt (it should work):

```
ssh azureadmin@<WEB_SERVER_PUBLIC_IP>
```

- Should connect successfully

1. **Test SSH from a different IP (should fail):**

- Use a VPN or mobile hotspot to change your IP
- Try to SSH - it should timeout/fail

Step 12.1: Test Data Tier Access

1. SSH to Web Server:

bash

```
ssh azureadmin@<WEB_SERVER_PUBLIC_IP>
```

1. From Web Server, test MySQL connection to DB Server:

bash

nc -zv 10.0.2.4 3306

- Should succeed (connection from 10.0.1.0/24 is allowed)

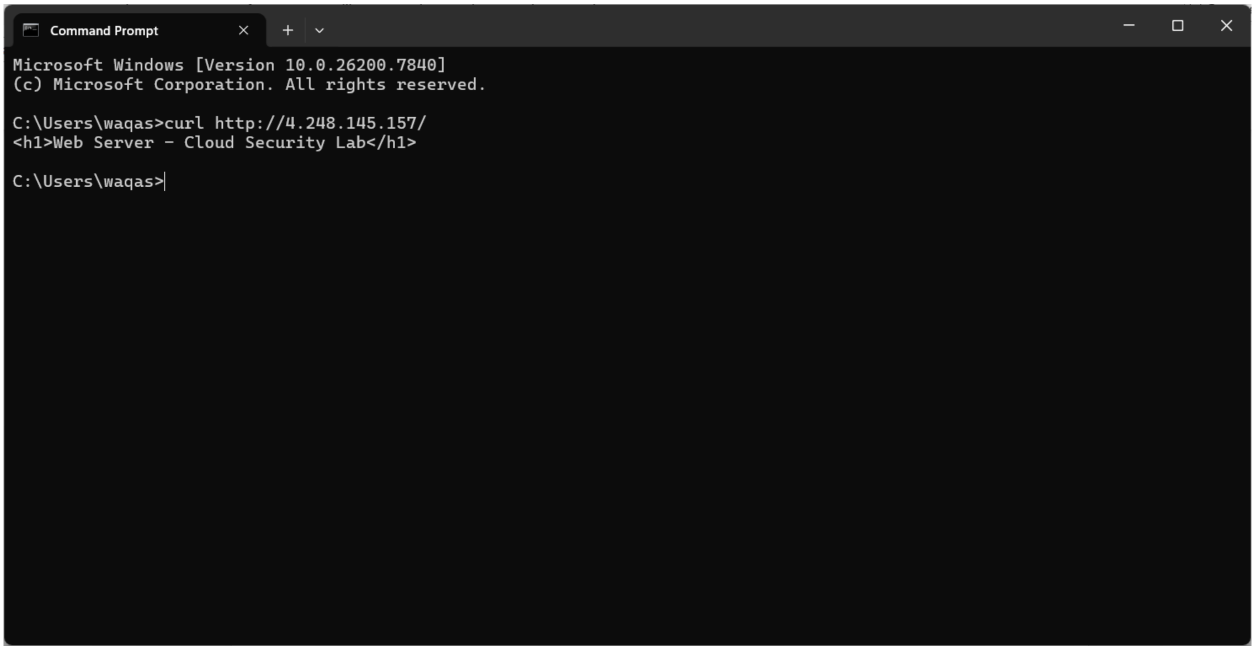
1. From Web Server, SSH to DB Server:

ssh azureadmin@10.0.2.4

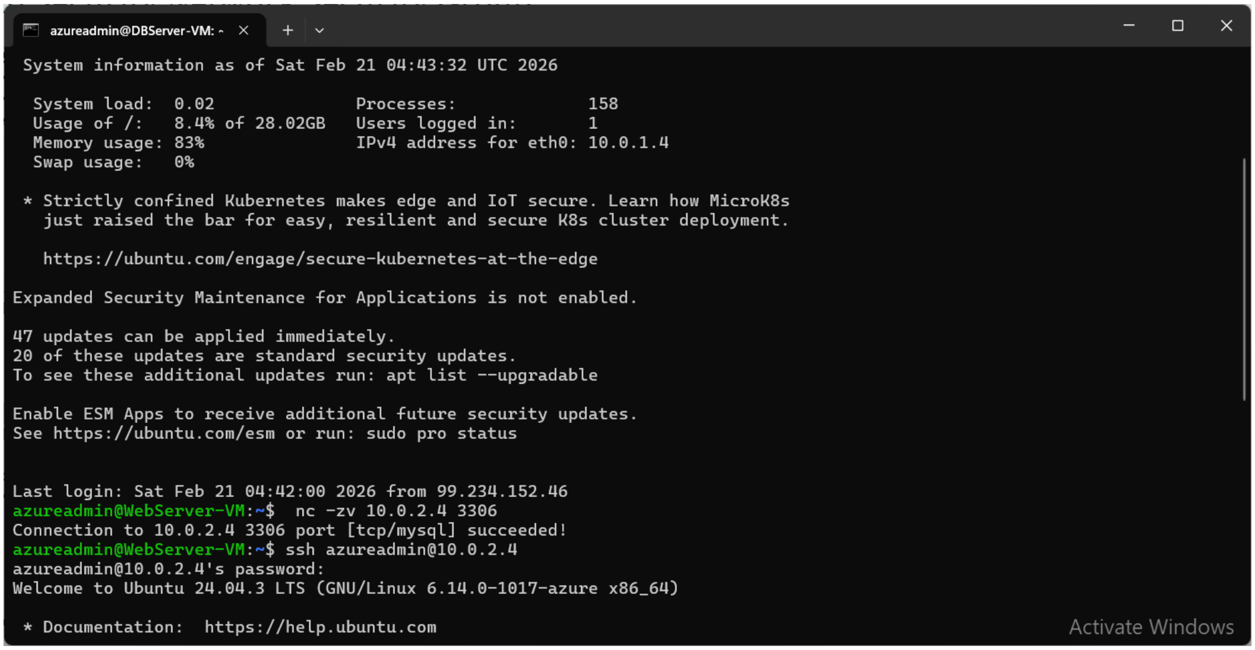
- Should work

1. Try to access MySQL directly from the internet:

- This should be impossible since DB Server has no public IP



```
Microsoft Windows [Version 10.0.26200.7840]
(c) Microsoft Corporation. All rights reserved.

C:\Users\waqas>curl http://4.248.145.157/
<h1>Web Server - Cloud Security Lab</h1>

C:\Users\waqas>
```



```
 System information as of Sat Feb 21 04:43:32 UTC 2026

  System load:  0.02               Processes:             158
  Usage of /:   8.4% of 28.02GB    Users logged in:       1
  Memory usage: 83%                IPv4 address for eth0: 10.0.1.4
  Swap usage:   0%

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

47 updates can be applied immediately.
20 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


Last login: Sat Feb 21 04:42:00 2026 from 99.234.152.46
azureadmin@WebServer-VM:~$  nc -zv 10.0.2.4 3306
Connection to 10.0.2.4 3306 port [tcp/mysql] succeeded!
azureadmin@WebServer-VM:~$ ssh azureadmin@10.0.2.4
azureadmin@10.0.2.4's password:
Welcome to Ubuntu 24.04.3 LTS (GNU/Linux 6.14.0-1017-azure x86_64)

 * Documentation:  https://help.ubuntu.com
```

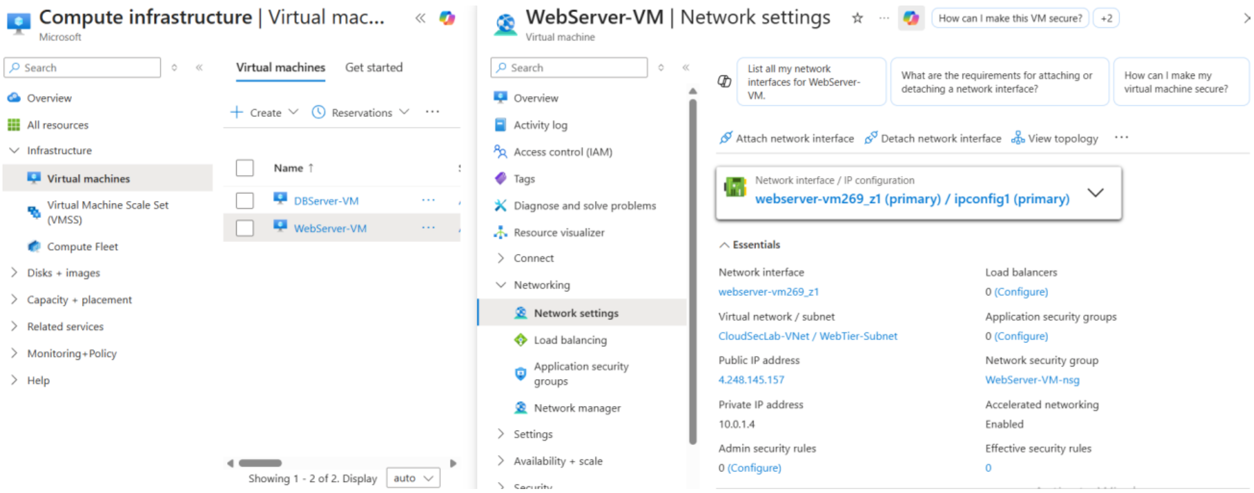
Note:

When creating a Virtual Machine, Azure automatically generates a NIC-level Network Security Group (e.g., WebServer-VM-nsg) attached to the VM's network interface. If you have also created a subnet-level NSG (WebTier-NSG), **both NSGs must allow the traffic** for SSH to work this is a common source of connection timeouts.

To resolve this:

1. Go to your WebServer-VM -> **Networking** -> **Network settings**
2. Under the Rules section you will see two NSGs listed one attached to the subnet and one attached to the network interface
3. Click on the **network interface link** (e.g., webserver-vm269_z1)
4. In the left menu under **Settings**, click **Network Security Group**
5. Click the dropdown and select **None**
6. Click **Save**

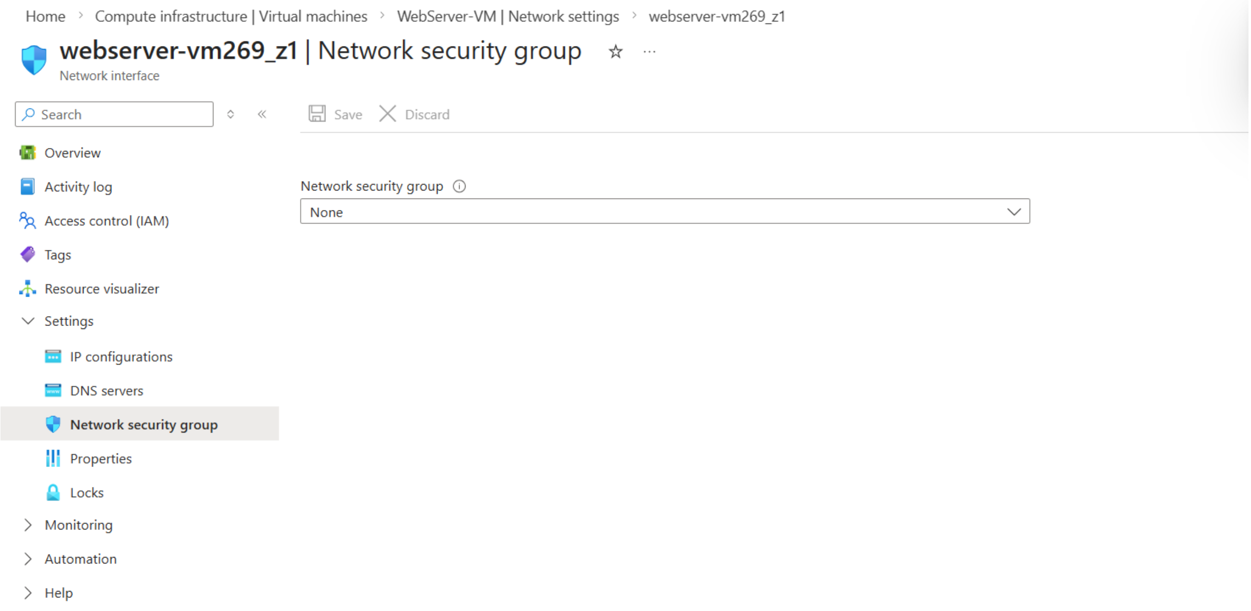
This removes the auto-generated NIC-level NSG, leaving only your WebTier-NSG in control at the subnet level. Your SSH connection should now work correctly using the Allow-SSH-MyIP rule you configured.



Network interface / IP configuration
webserver-vm269_z1 (primary) / ipconfig1 (primary)

Essentials

Network interface webserver-vm269_z1	Load balancers 0 (Configure)
Virtual network / subnet CloudSecLab-VNet / WebTier-Subnet	Application security groups 0 (Configure)
Public IP address 4.248.145.157	Network security group WebServer-VM-nsg
Private IP address 10.0.1.4	Accelerated networking Enabled
Admin security rules 0 (Configure)	Effective security rules 0



Network security group ⓘ
None