



3-Tier-LAB

Status Not Started

step1:- create vnet

Show Microsoft Cloud menu | [Virtual networks](#) >

Create virtual network

Basics Security IP addresses Tags Review + create

Project details

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

Subscription *

Subscription 1

Resource group *

azureskf-T

[Create new](#)

Instance details

Virtual network name *

Clahan-Vnet

Region * ⓘ

(US) East US

[Deploy to an Azure Extended Zone](#)

subnets public, private and database subnet

[Home](#) > [Network foundation](#) | [Virtual networks](#) >

Create virtual network ...

Basics Security **IP addresses** Tags Review + create

192.168.0.0/16

192.168.0.0

/16

192.168.0.0 - 192.168.255.255 65,536 addresses

Delete address space

Subnets	IP address range	Size	NAT gateway
Public	192.168.0.0 - 192.168.0.255	/24 (256 addresses)	-
Private	192.168.1.0 - 192.168.1.255	/24 (256 addresses)	-
database	192.168.2.0 - 192.168.2.255	/24 (256 addresses)	-

create a virtual machines one is public and second one is the private subnet

[Home](#) > [Compute infrastructure](#) | [Virtual machines](#) >

Create a virtual machine ...



Help me choose the right VM size for my workload

Help me create a low cost VM

Help me create a VM optimized for high availability



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 Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

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

Subscription *

Subscription 1

Resource group *

azureskf-T

Create new

Instance details

Virtual machine name *

Public-Vm

Region *

(US) East US

Deploy to an Azure Extended Zone

Availability options

No infrastructure redundancy required

we've chose the resource group and virtual machine name and region currently we don't prefered availability options and image name we have chose the ubuntu

family and size the image also we've to choose below mentioned screenshot



Configure security features

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_D2s_v3 - 2 vcpus, 8 GiB memory (\$70.08/month) ▼
[See all sizes](#)

Enable Hibernation ⓘ ☐
 Hibernate does not currently support Trusted launch and Confidential virtual machines for Linux images. [Learn more](#) 

and next we are chosing the authentication type i'm chosing the user name and passowrd

Administrator account

Authentication type ⓘ ☐ SSH public key ☒ Password

Username * ⓘ clahan-user ✓

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 * 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.

and next we are going to the networking section here we can chose the vnet and subnets and create public IP

Network interface

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

Virtual network * ⓘ Clahan-Vnet ▼
[Create new](#)

Subnet * ⓘ Public (192.168.0.0/24) ▼
[Manage subnet configuration](#)

Public IP ⓘ (new) Public-Vm-ip ▼
[Create new](#)
i 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 * SSH (22) ▼

once click on the create vm it will take time to deploy the resource

now are going to select the nsg while launch vm it have created go inside and add the security rules http and https defaultport 22 available

The screenshot shows the Azure portal interface for managing a Network Security Group (NSG). The main pane displays the 'Public-Vm-nsg' NSG with a list of inbound security rules. The 'Add inbound security rule' dialog is open on the right, showing the configuration for a new rule named 'Allow-HTTP'.

Public-Vm-nsg | Inbound security rules

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, protocol, and action. You can't delete default security rules, but you can override them.

Filter by name: Port == all Protocol == all Source == all

Priority	Name	Port	Protocol
300	SSH	22	TCP
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancer...	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule

Public-Vm-nsg
Destination port ranges: 8080

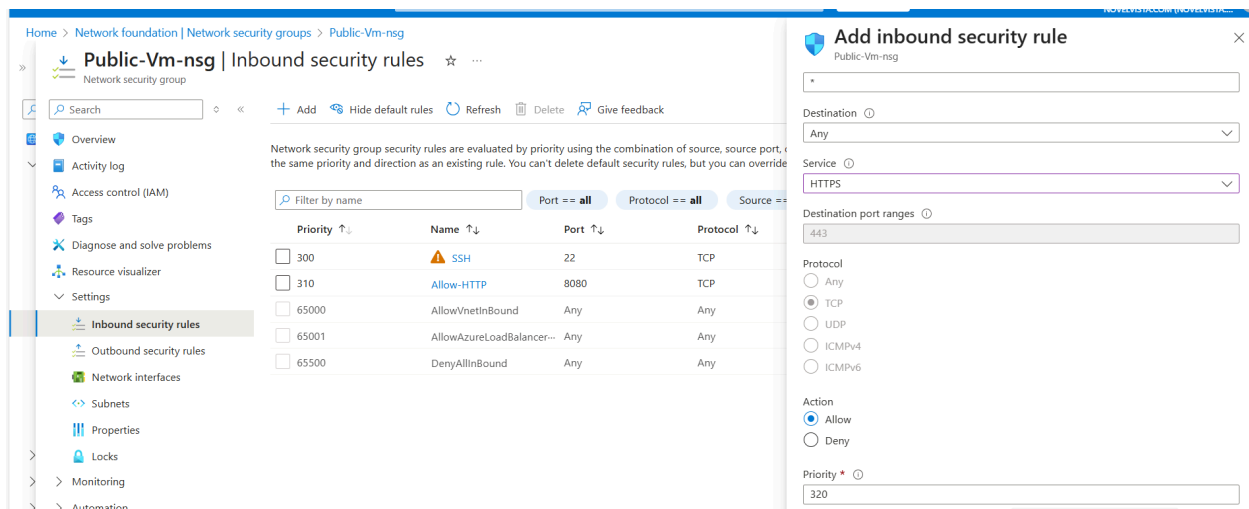
Protocol: ☒ TCP

Action: ☒ Allow

Priority: 310

Name: Allow-HTTP

Description:



before going to lunch the private virtual machine like app server we need to create networksecurity group and firewalls which ports are allow

[Home](#) > [Network foundation | Network security groups](#) >

Create network security group ...

Basics Tags Review + create

Project details

Subscription *

Resource group * [Create new](#)

Instance details

Name * ✓

Region *

add inbound security rules

Home > CreateNetworkSecurityGroupBladeV2-20260116123918 | Overview > Private-NSG

Private-NSG | 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
Resource visualizer
Settings
Inbound security rules
Outbound security rules
Network interfaces

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

Filter by name

Priority	Name	Port	Protocol
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancerInBound	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule

Private-NSG

Source

IP Addresses

Source IP addresses/CIDR ranges

192.168.0.0/24

Source port ranges

*

Destination

Any

Service

Custom

Destination port ranges

80, 443

Protocol

Any

☒ TCP

UDP

ICMPv4

ICMPv6

Action

☒ Allow

Deny

Priority

100

Name

Allow-From-Public-Subnet

Description

Allow web traffic from public subnet

Allow ssh from public subnet

Home > CreateNetworkSecurityGroupBladeV2-20260116123918 | Overview > Private-NSG

Private-NSG | 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
Resource visualizer
Settings
Inbound security rules
Outbound security rules
Network interfaces

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

Filter by name

Priority	Name	Port	Protocol
100	Allow-From-Public-Subnet	80,443	TCP
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancerInBound	Any	Any
65500	DenyAllInBound	Any	Any

Add inbound security rule

Private-NSG

Source

IP Addresses

Source IP addresses/CIDR ranges

192.168.0.0/24

Source port ranges

*

Destination

Any

Service

SSH

Destination port ranges

22

+

Add

🔍

Hide default rules

🔄

Refresh

🗑️

Delete

🗨️

Give feedback

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, protocol, and direction. You can't delete default security rules, but you can override them with your own.

🔍

Filter by name

Port == all

Protocol == all

Source == all

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓
<input type="checkbox"/> 100	Allow-From-Public-Subnet	80,443	TCP
<input type="checkbox"/> 65000	AllowVnetInBound	Any	Any
<input type="checkbox"/> 65001	AllowAzureLoadBalancerInBound	Any	Any
<input type="checkbox"/> 65500	DenyAllInBound	Any	Any

22

Protocol

☐ Any
 ☒ TCP
 ☐ UDP
 ☐ ICMPv4
 ☐ ICMPv6

Action

☒ Allow
 ☐ Deny

Priority * ⓘ

110

Name *

Allow-SSH-From-Public ✓

Description

Allow SSH from public subnet for management

Next we are going to create db security group

[Home](#) > [Network foundation](#) | [Network security groups](#) >

Create network security group ...

Basics Tags Review + create

Project details

Subscription *

Subscription 1

Resource group *

azureskf-T

[Create new](#)

Instance details

Name *

Database-NSG ✓

Region *

East US

add nsg rules for db 3306

Home > CreateNetworkSecurityGroupBladeV2-20260116124452 | Overview > Database-NSG

Database-NSG | 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
Resource visualizer
Settings
Inbound security rules
Outbound security rules
Network interfaces

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

Filter by name

Priority	Name	Port	Protocol
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancerInBound	Any	Any
65500	DenyAllInBound	Any	Any

Port == all Protocol == all Source == all

Add inbound security rule

Database-NSG

Source IP Addresses

Source IP addresses/CIDR ranges * 192.168.1.0/24

Source port ranges * *

Destination Any

Service Custom

Destination port ranges * 3306

add nsg rule for postgresql 5432

Home > CreateNetworkSecurityGroupBladeV2-20260116124452 | Overview > Database-NSG

Database-NSG | 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
Resource visualizer
Settings
Inbound security rules
Outbound security rules
Network interfaces

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

Filter by name

Priority	Name	Port	Protocol
100	Allow-msql	3306	TCP
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancerInBound	Any	Any
65500	DenyAllInBound	Any	Any

Port == all Protocol == all Source == all

Add inbound security rule

Database-NSG

Source IP Addresses

Source IP addresses/CIDR ranges * 192.168.1.0/24

Source port ranges * *

Destination Any

Service Custom

Destination port ranges * 5432

+ Add Hide default rules Refresh Delete Give feedback

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

Filter by name

Port == all Protocol == all Source == all

Priority	Name	Port	Protocol
100	Allow-msql	3306	TCP
65000	AllowVnetInBound	Any	Any
65001	AllowAzureLoadBalancerInBound	Any	Any
65500	DenyAllInBound	Any	Any

Protocol

Any
TCP
UDP
ICMPv4
ICMPv6

Action

Allow
Deny

Priority * 110

Name * Allow-PostgreSQL-From-Private

Description

Allow PostgreSQL from private subnet

Next Associate NSGs with Subnets

Home > CreateNetworkSecurityGroupBladeV2-20260116124452 | Overview > Database-NSG

Database-NSG | Subnets

Network security group

Search

+ Associate

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces
- Subnets**

Name	Address range	Virtual network
database	192.168.2.0/24	Clahan-Vnet

Home > Network foundation | Network security groups > Private-NSG

Private-NSG | Subnets

Network security group

Search

+ Associate

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces
- Subnets**

Name	Address range	Virtual network
Private	192.168.1.0/24	Clahan-Vnet

Home > Network foundation | Network security groups > Public-Vm-nsg

Public-Vm-nsg | Subnets

Network security group

Search

+ Associate

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Resource visualizer

Settings

- Inbound security rules
- Outbound security rules
- Network interfaces
- Subnets**

Name	Address range	Virtual network
Public	192.168.0.0/24	Clahan-Vnet

next we are going to create private virtual machine

Create a virtual machine



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



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 Disks Networking Management Monitoring Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

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

Subscription * ⓘ

Subscription 1

Resource group * ⓘ

azureskf-T

[Create new](#)

Instance details

Virtual machine name * ⓘ

Private-Vm

Region * ⓘ

(US) East US

[Deploy to an Azure Extended Zone](#)

Availability options ⓘ

No infrastructure redundancy required

we can choose the resource group name and vm name configuration of the vm image and size the it means core ram and

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_D2s_v3 - 2 vcpus, 8 GiB memory (\$70.08/month)

[See all sizes](#)

Enable Hibernation ⓘ

☐

i Hibernation does not currently support Trusted launch and Confidential virtual machines for Linux images. [Learn more](#)

next we are going to authentication type

username:- clahan-private

Password:- Clahan@8553370

Administrator account

Authentication type ⓘ

- ☐ SSH public key
☒ Password

Username * ⓘ

clahan-private ✓

Password *

..... ✓

Confirm password *

..... ✓

default inbound rules

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 *

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.

next we are going to the networking section

Home > Compute infrastructure | Virtual machines >

Create a virtual machine

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

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 Disks **Networking** Management Monitoring Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

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

Virtual network * [Create new](#)

Subnet * [Manage subnet configuration](#)

Public IP [Create new](#)

NIC network security group ☒ None ☐ Basic ☐ Advanced

i The selected subnet 'Private (192.168.1.0/24)' is already associated to a network security group 'Private-NSG'. We recommend managing connectivity to this

next going the network interface card section we can choose the already created nsg we need to gave here

[Create new](#)

NIC network security group ☐ None ☐ Basic ☒ Advanced

i The selected subnet 'Private (192.168.1.0/24)' is already associated to a network security group 'Private-NSG'. We recommend managing connectivity to this virtual machine via the existing network security group instead of creating a new one here.

Configure network security group * [Create new](#)

and then review and create

next we are going to create mysql flexible server

in this section we need to chose resource group name and server name region

Flexible server

Microsoft

Basics Tags Review

Create an Azure Database for MySQL server.

Project details

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

Subscription * ⓘ

Resource group * ⓘ [Create new](#)

Server details

Enter required settings for this server, including picking a location and configuring the compute and storage resources.

Server name * ⓘ ✓

Region * ⓘ

Availability zone * ⓘ

Estimated costs

Compute Sku	USD 249.66/month
Standard_D4ads_v5	249.66
Storage	USD 7.36/month
Storage selected 64 GiB (USD 0.115 per GiB)	64 x 0.115
Auto scale IOPS	Auto scale IOPS is billed on usage in per million request increments. Learn more
High availability	USD 257.02/month
Same zone or Zone redundant high availability	
Backup Retention	

authentication

Authentication

Administrator login * ⓘ ✓

Password * ⓘ ✓

Confirm password * ✓

we can use choose the administrator login and password required

adminname: clahan

Password:- Admin@123

and work load type standard

Workload details [\(Compare workload type\)](#)

Workload type * ⓘ

 Dev/Test	 Standard	 Enterprise
--	--	--

Choose one of these workload types to quickly configure the server based on your needs. You can modify the configuration after creation.

next we are going to choose the networking section

Database port * ⓘ 3306

Virtual network

Virtual networks are logically isolated from each other in Azure. Virtual network gives you a highly secure environment to run your MySQL Flexible Server and other types of Azure resources

Subscription * ⓘ Subscription 1

Virtual network * ⓘ Clahan-Vnet

[Manage selected virtual network](#)

[Create virtual network](#)


Subnet * ⓘ Clahan-Vnet/database (192.168.2.0/24) (Delegation required to servi... ▾

- i** This subnet will be delegated for use only with MySQL Flexible Server (Microsoft.DBforMySQL/flexibleServers).
- i** Your current subnet selection has 251 addresses available.
- i** This subnet has Network Security Group (NSG) attached to it. Please make sure that NSG rules do not block outbound traffic to ports 3306 as these are reserved for internal traffic.

next we are going to choose the private DNS integration

Private DNS integration

Private DNS zone integration is required to connect to your Flexible Server in virtual network using server name (fully qualified domain name).

A new private DNS zone will be created or you can optionally choose an existing one linked to the selected virtual network. With private DNS zone integration, the DNS records for the server name will be updated automatically in case the IP address of your Flexible Server changes. [Learn more](#) 

Subscription * ⓘ Subscription 1

Private DNS zone * (New) clahanserver.private.mysql.database.azure.com ▾

and next we are going to configured the vms and dependencies