



3-Tier-LAB

	Status	Not Started
--	--------	-------------

step1:- create vnet

Show Microsoft Cloud menu [Action](#) | [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 * [▼](#)

Resource group * [▼](#)
[Create new](#)

Instance details

Virtual network name *

Region * [\(US\) East US](#) [▼](#)
[Deploy to an Azure Extended Zone](#)

subnets public, private and database subnet

Create virtual network ...

Basics Security IP addresses Tags Review + create

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 machine one is public and second one is the private subnet

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
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 * ⓘ [See all images](#) | [Configure VM generation](#)

VM architecture ⓘ Arm64 x64

Run with Azure Spot discount ⓘ

Size * ⓘ [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 choosing the authentication type i'm choosing the user name and password

Administrator account

Authentication type ⓘ SSH public key Password

Username * ⓘ ✓

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 *

⚠ 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 *	<input type="text" value="Clahan-Vnet"/>
	Create new
Subnet *	<input type="text" value="Public (192.168.0.0/24)"/>
	Manage subnet configuration
Public IP	<input type="text" value="(new) Public-Vm-ip"/>
	Create new
	<small>Public IP addresses have a nominal charge. Estimate price</small>
NIC network security group	<input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced
Public inbound ports *	<input type="radio"/> None <input checked="" type="radio"/> Allow selected ports
Select inbound ports *	<input type="text" value="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). On the left, the 'Inbound security rules' section is visible, listing existing rules:

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

The right pane is a modal window titled 'Add inbound security rule' for creating a new rule. The configuration is as follows:

- Protocol:** TCP (selected)
- Destination port ranges:** 8080
- Action:** Allow (selected)
- Priority:** 310
- Name:** Allow-HTTP
- Description:** (empty)

The screenshot shows the Azure portal's Network foundation | Network security groups page for a group named 'Public-Vm-nsg'. The left sidebar has sections like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Resource visualizer, Settings, Inbound security rules (which is selected), Outbound security rules, Network interfaces, Subnets, Properties, Locks, Monitoring, and Automation. The main area displays the 'Inbound security rules' table with columns: Priority, Name, Port, and Protocol. Existing rules include SSH (Priority 300, Port 22, TCP), Allow-HTTP (Priority 310, Port 8080, TCP), AllowVnetInBound (Priority 65000, Any, Any), AllowAzureLoadBalancer (Priority 65001, Any, Any), and DenyAllInBound (Priority 65500, Any, Any). A modal window titled 'Add inbound security rule' is open, showing fields for Destination (Any), Service (HTTPS), Destination port ranges (443), Protocol (TCP), Action (Allow selected), and Priority (320).

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 ...

The screenshot shows the 'Create network security group' wizard. The 'Basics' step is selected. Under 'Project details', 'Subscription' is set to 'Subscription 1' and 'Resource group' is set to 'azureskf-T'. Under 'Instance details', 'Name' is 'Private-NSG' and 'Region' is 'East US'.

add inbound security rules

The screenshot shows the Azure portal interface for creating an inbound security rule. On the left, the 'Inbound security rules' section is selected. On the right, a modal window titled 'Add inbound security rule' is open, showing the configuration for a new rule.

Inbound security rules (Left Panel):

- Source IP addresses/CIDR ranges: 192.168.0.0/24
- Source port ranges: * (empty)
- Destination: Any
- Service: Custom
- Destination port ranges: 80, 443

Add inbound security rule (Modal Window):

- Protocol: TCP (selected)
- Action: Allow (selected)
- Priority: 100
- Name: Allow-From-Public-Subnet
- Description: Allow web traffic from public subnet

Allow ssh from public subnet

The screenshot shows the Azure portal interface for creating an inbound security rule. On the left, the 'Inbound security rules' section is selected. On the right, a modal window titled 'Add inbound security rule' is open, showing the configuration for a new rule.

Inbound security rules (Left Panel):

- Source IP addresses/CIDR ranges: 192.168.0.0/24
- Source port ranges: * (empty)
- Destination: Any
- Service: SSH (selected)
- Destination port ranges: 22

Add inbound security rule (Modal Window):

- Protocol: TCP (selected)
- Action: Allow (selected)
- Priority: 100
- Name: Allow-From-Public-Subnet
- Description: Allow ssh traffic from public subnet

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

Protocol

- Any
- TCP
- UDP
- ICMPv4
- ICMPv6

Action

- Allow
- Deny

Priority *

Name *

Description

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 *

Resource group *

[Create new](#)

Instance details

Name *

Region *

add nsg rules for db 3306

Add inbound security rule

Source: IP Addresses
Source IP addresses/CIDR ranges: 192.168.1.0/24

Source port ranges: Any

Destination: Any

Service: Custom

Destination port ranges: 3306

add nsg rule for postgresql 5432

Add inbound security rule

Source: IP Addresses
Source IP addresses/CIDR ranges: 192.168.1.0/24

Source port ranges: Any

Destination: Any

Service: Custom

Destination port ranges: 5432

Protocol: TCP
Port: 5432

Action: Allow

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 Properties

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

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

Public-Vm-ns | 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 Properties

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



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 Hibernate 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 * ✓

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 * ▼

⚠ 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

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 * ⓘ Clahan-Vnet [Create new](#)

Subnet * ⓘ Private (192.168.1.0/24) [Manage subnet configuration](#)

Public IP ⓘ None [Create new](#)

NIC network security group ⓘ None Basic Advanced

Info 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

Info 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 * ⓘ Private-NSG [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 * ⓘ

Subscription 1

Resource group * ⓘ

azureskf-T

[Create new](#)

Server details

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

Server name * ⓘ

clahanserver

Region * ⓘ

(US) East US

Availability zone * ⓘ

No preference

Estimated costs



Compute SKU USD 249.66/month

Standard_D4ads_v5 249.66

Storage USD 7.36/month

Storage selected 64 GiB (USD 64 x 0.115 per GiB) 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 * ⓘ

clahan



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 serv...)

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