

# AZURE VNET-1

**My client TVS wants to launch their websites publicly along with its Database server at the backend. Establish Network connectivity between webserver and Database server.**

Note: - No need of public access for Database server Ensure only website can access from public Network.

**Step 1:** - Click on Create Virtual Network

The screenshot shows the 'Virtual networks' blade in the Azure portal. At the top, there are filter options: 'Subscription equals all', 'Resource group equals all', and 'Location equals all'. Below the filters, it says 'Showing 0 to 0 of 0 records.' On the right, there are sorting options: 'Name ↑', 'Resource group ↑', 'Location ↑', and 'Subscription ↑'. In the center, there is a large placeholder icon with three dots and the text 'No virtual networks to display'. Below the icon, there is a descriptive message: 'Create a virtual network to securely connect your Azure resources to each other. Connect your virtual network to your on-premises network using an Azure VPN Gateway or ExpressRoute.' There are two buttons: a blue 'Create virtual network' button and a smaller 'Learn more' link.

**Step 2:** - Select Subscription, Resource Group and Mention Virtual network name along with region and click on next.

The screenshot shows the 'Create virtual network' wizard. At the top, there are tabs: 'Basics' (selected), 'Security', 'IP addresses', 'Tags', and 'Review + create'. Below the tabs, there is a 'Project details' section with a note about managing resources using resource groups. It shows the selected 'Subscription' (Azure subscription 1) and 'Resource group' (azure-class). There is also a 'Create new' button. The 'Instance details' section includes fields for 'Virtual network name' (TVS-Vnet) and 'Region' ((Europe) France Central). There is also a 'Deploy to an edge zone' checkbox.

### Step 3: - Add your IPv4 space and click on add a subnet.

Create virtual network ...

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

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you need. [Learn more](#)

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. 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. [Learn more](#)

Add IPv4 address space | ↴

Subnets	IP address range	Size	NAT gateway
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-

### Step 4: - Add Web subnet.

Edit 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](#)

IP address space 10.10.0.0/16 ▼  
10.10.0.0 - 10.10.255.255 (65536 addresses)

**Subnet details**

Subnet template Default ▼

Name web-sub

Starting address 10.10.1.0

Subnet size /24 (256 addresses) ▼

IP address space 10.10.1.0 - 10.10.1.255 (256 addresses)

**Security**

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. [Learn more](#)

NAT gateway None ▼  
[Create new](#)

Network security group None ▼  
[Create new](#)

Save Cancel

### Step 5: - Add DB Subnet

Add a subnet ×

IP address space 10.10.0.0/16 ▼  
10.10.0.0 - 10.10.255.255 (65536 addresses)

**Subnet details**

Subnet template Default ▼

Name DB-Sub

Starting address 10.10.2.0 ▼

Subnet size /24 (256 addresses) ▼

IP address space 10.10.2.0 - 10.10.2.255 (256 addresses)

**Security**

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. [Learn more](#)

NAT gateway None ▼  
[Create new](#)

Network security group None ▼  
[Create new](#)

Route table None ▼

Add Cancel

## Step 6: - Review and Create the subnet.

The screenshot shows the 'TVS-Vnet' Virtual network overview page. The left sidebar includes links for Activity log, Access control (IAM), Tags, Diagnose and solve problems, Address space, Connected devices, Subnets, Bastion, DDoS protection, Firewall, Microsoft Defender for Cloud, Network manager, DNS servers, Peering, and Service endpoints. The main content area displays the following details:

- Resource group: NetworkWatcherRG
- Location: France Central
- Subscription: Azure subscription 1
- Subscription ID: 369b24a9-76cb-409d-a317-605586f41993
- Address space: 10.10.0.0/16
- DNS servers: Azure provided DNS service
- Flow timeout: Configure
- BGP community string: Configure
- Virtual network ID: 2e803ccc-ed55-45b8-9670-aade38685e4c

The 'Capabilities' tab is selected, showing the following status for various features:

- DDoS protection: Not configured
- Azure Firewall: Not configured
- Peering: Not configured
- Microsoft Defender for Cloud: Strengthen the security posture of your environment.
- Private endpoints: Not configured

## Step 7: - Create a Virtual Machine

The screenshot shows the 'Azure virtual machine' creation interface. It includes the following sections:

- Azure virtual machine**: Create a virtual machine hosted by Azure.
- Azure virtual machine with preset configuration**: Create a virtual machine with presets based on your workloads.
- Azure Arc virtual machine**: Create a new Azure Arc virtual machine in one of your non-Azure environments.
- Azure VMware Solution virtual machine**: Create a VMware virtual machine hosted by Azure.

A large blue 'Create' button is at the bottom.

## Step 8: - Create a Virtual Machine on Ubuntu with a web-server IP address- 10.10.1.0

The screenshot shows the Azure portal's 'Virtual machines' section. A specific VM named 'Web-server' is selected. The 'Overview' tab is active. Key details shown include:

- Computer name:** Web-server
- Operating system:** Linux (ubuntu 20.04)
- Image publisher:** canonical
- Image offer:** 0001-com-ubuntu-server-focal
- Image plan:** 20.04-lts-gen2
- VM generation:** V2
- VM architecture:** x64
- Agent status:** Ready
- Agent version:** 2.9.1.1
- Host group:** None
- Host:** -
- Proximity placement group:** -
- Colocation status:** N/A
- Disk controller type:** SCSI

**Networking:**

- Public IP address:** 20.111.8.220 (Network interface **web-server425**)
- Private IP address (IPv6):** -
- Private IP address:** 10.10.1.4
- Virtual network/subnet:** TSV-Vnet/web-subnet
- DNS name:** Configure

**Size:**

- Size:** Standard B1s
- vCPUs:** 1
- RAM:** 1 GiB

**Disk:**

- OS disk:** Web-server\_disk1\_92f1051d44a149c6b5345b95ed04f49c
- Encryption at host:** Disabled
- Azure disk encryption:** Not enabled
- Enhemeral OS disk:** N/A

## Step 9: - Connect to a Virtual Machine via terminal.

```
Last login: Fri Jul 7 12:38:36 on ttys001
The default interactive shell is now zsh.
To update your account to use zsh, please run `chsh -s /bin/zsh`.
For more details, please visit https://support.apple.com/kb/H17208050.
[Shahil-MacBook-Pro:~ sahilbaaja]$ ssh -i rootadmin@20.111.8.220
Warning: Identity file rootadmin@20.111.8.220 non accessible: No such file or directory.
usage: ssh [-l user] [-c cipher] [-D port] [-o option] [-W bind_interface]
           [-b bind_address] [-C compression_level] [-e escape_char] [-f configfile] [-I pkeysize]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-o ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-S address] [-S ctl_path] [-W host:port]
           [-t local_tun[:remote_tun]] destination [command [argument ...]]
Shahil-MacBook-Pro:~ sahilbaaja]$ ssh -i rootadmin@20.111.8.220
[The authenticity of host '20.111.8.220 (20.111.8.220)' cannot be established.
ED25519 key fingerprint is SHA256:4qnyCYnAxj3+rXPFZorby3/NlKxrg5FBFgmcHezSPV8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '20.111.8.220' (ED25519) to the list of known hosts.
rootadmin@20.111.8.220:~$ password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-1041-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat Jul 8 14:28:44 UTC 2023

System load: 0.81      Processes:          103
Usage of /:  5.2% of 28.89GB   Users logged in:  0
Memory usage: 32%          IPv4 address for eth0: 10.10.1.4
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.

0 updates can be applied immediately.

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

rootadmin@Web-server:~$
```

**Step 10:** - Switch to the root user using the command **sudo su** and check for all package availability using **apt-get update** command.

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

```
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

root@Web-server:/home/rootadmin# $ sudo su
root@Web-server:/home/rootadmin# apt-get update
Hit:1 http://archive.ubuntu.com/ubuntu focal InRelease
Get:2 http://archive.ubuntu.com/ubuntu focal-updates InRelease [114 kB]
Get:3 http://archive.ubuntu.com/ubuntu focal-backports InRelease [108 kB]
Get:4 http://archive.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Get:5 http://archive.ubuntu.com/ubuntu focal/universe amd64 Packages [8628 kB]
Get:6 http://archive.ubuntu.com/ubuntu focal/universe Translation-en [505 kB]
Get:7 http://archive.ubuntu.com/ubuntu focal/universe amd64 c-n-f Metadata [265 kB]
Get:8 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 Packages [144 kB]
Get:9 http://archive.ubuntu.com/ubuntu focal/multiverse Translation-en [104 kB]
Get:10 http://archive.ubuntu.com/ubuntu focal/multiverse amd64 c-n-f Metadata [9136 B]
Get:11 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 Packages [2686 kB]
Get:12 http://archive.ubuntu.com/ubuntu focal-updates/main Translation-en [448 kB]
Get:13 http://archive.ubuntu.com/ubuntu focal-updates/main amd64 c-n-f Metadata [14.9 kB]
Get:14 http://archive.ubuntu.com/ubuntu focal-updates/restricted amd64 Packages [2089 kB]
Get:15 http://archive.ubuntu.com/ubuntu focal-updates/restricted Translation-en [292 kB]
Get:16 http://archive.ubuntu.com/ubuntu focal-updates/restricted amd64 c-n-f Metadata [548 B]
Get:17 http://archive.ubuntu.com/ubuntu focal-updates/universe amd64 Packages [1082 kB]
Get:18 http://archive.ubuntu.com/ubuntu focal-updates/universe Translation-en [258 kB]
Get:19 http://archive.ubuntu.com/ubuntu focal-updates/universe amd64 c-n-f Metadata [125.2 kB]
Get:20 http://archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 Packages [21.5 kB]
Get:21 http://archive.ubuntu.com/ubuntu focal-updates/multiverse Translation-en [8032 B]
Get:22 http://archive.ubuntu.com/ubuntu focal-updates/multiverse amd64 c-n-f Metadata [688 B]
Get:23 http://archive.ubuntu.com/ubuntu focal-backports/main amd64 Packages [45.7 kB]
Get:24 http://archive.ubuntu.com/ubuntu focal-backports/main Translation-en [16.3 kB]
Get:25 http://archive.ubuntu.com/ubuntu focal-backports/main amd64 c-n-f Metadata [14.20 B]
Get:26 http://archive.ubuntu.com/ubuntu focal-backports/restricted amd64 c-n-f Metadata [116 B]
Get:27 http://archive.ubuntu.com/ubuntu focal-backports/universe amd64 Packages [25.0 kB]
Get:28 http://archive.ubuntu.com/ubuntu focal-backports/universe Translation-en [16.3 kB]
Get:29 http://archive.ubuntu.com/ubuntu focal-backports/universe amd64 c-n-f Metadata [888 B]
Get:30 http://archive.ubuntu.com/ubuntu focal-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:31 http://archive.ubuntu.com/ubuntu focal-security/main amd64 Packages [234 kB]
Get:32 http://archive.ubuntu.com/ubuntu focal-security/main Translation-en [136 kB]
Get:33 http://archive.ubuntu.com/ubuntu focal-security/main amd64 c-n-f Metadata [13.8 kB]
Get:34 http://archive.ubuntu.com/ubuntu focal-security/restricted amd64 Packages [1979 kB]
Get:35 http://archive.ubuntu.com/ubuntu focal-security/restricted Translation-en [277 kB]
Get:36 http://archive.ubuntu.com/ubuntu focal-security/restricted amd64 c-n-f Metadata [552 B]
Get:37 http://archive.ubuntu.com/ubuntu focal-security/unix amd64 Packages [68 kB]
Get:38 http://archive.ubuntu.com/ubuntu focal-security/unix Translation-en [374 kB]
Get:39 http://archive.ubuntu.com/ubuntu focal-security/universe amd64 c-n-f Metadata [18.6 kB]
Get:40 http://archive.archive.ubuntu.com/ubuntu focal-security/multiverse amd64 Packages [29.3 kB]
Get:41 http://archive.archive.ubuntu.com/ubuntu focal-security/multiverse Translation-en [6120 B]
Get:42 http://archive.archive.ubuntu.com/ubuntu focal-security/multiverse amd64 c-n-f Metadata [620 B]
Fetched 27.7 MB in 5s (5296 kB/s)
Reading package lists... Done
root@Web-server:/home/rootadmin#
```

**Step 11:** - Install Nginx package using the command **apt-get install nginx -y**  
And add inbound security rule in web-server Virtual Machine.

Add inbound security rule  
Web-server-nsg

Source  Any

Source port ranges \*

Destination  Any

Service  Custom

Destination port ranges \*  ✓

Protocol  Any  
 TCP  
 UDP  
 ICMP

Action  Allow  
 Deny

Priority \*

Add Cancel Give feedback

**Step 12:** - Port 80 is added.

Microsoft Defender for Cloud	310	AllowAnyCustom80Inbound	80	Any	Any	Allow	...
▲	...						

**Step 13:** - Web-server is accessible through browser.

## Welcome to nginx!

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](http://nginx.org).  
Commercial support is available at [nginx.com](http://nginx.com).

*Thank you for using nginx.*