

# Azure 3-Tier Architecture Deployment

---

Submitted by: Sanskar Vishnoi

Batch: Celebal Technologies – Summer Internship 2025 (Batch 2)

Date: July 12, 2025

## Objective

Create three subnets : 1. Web tier 2. App tier 3. DB tier DB Tier should not access any tier(Web & App tier) App tier should access the DB tier and Web tier as well, Web tier should access only App tier. Only Web tier is allowed to connect to the internet.Deploy two VM's in each tier(One VM should be Linux & another should be Windows). Configure Apache Server on Linux VM's And IIS Server on Windows.

## Architecture Summary

Tier	Subnet	IP Range	Internet Access	Access Rules
Web Tier	Subnet-Web	10.0.1.0/24	Yes	Can access App Tier only
App Tier	Subnet-App	10.0.2.0/24	No	Can access Web & DB Tier
DB Tier	Subnet-DB	10.0.3.0/24	No	Cannot access any other tier

Search (Ctrl+/) <<

→ Move ▾ Delete Refresh Give feedback

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Address space
- Connected devices
- Subnets
- Bastion
- DDoS protection
- Firewall
- Microsoft Defender for Cloud
- Network manager
- DNS servers
- Peerings
- Service endpoints
- Private endpoints
- Properties
- Locks

Monitoring

- Alerts
- Metrics
- Diagnostic settings
- Logs
- Connection monitor (classic)
- Diagram

Automation

- Tasks (preview)
- Export template

Support + troubleshooting

- Connection troubleshoot
- New Support Request

Essentials

JSON View

Resource group (move)

contoso

Location (move)

East US

Subscription (move)

Subscription ID

abcdef01-2345-6789-0abc-def012345678

Tags (edit)

Click here to add tags

Address space

10.0.0.0/16

DNS servers

Azure provided DNS service

Flow timeout

Configure

BGP community string

Configure

Virtual network ID

Topology

Capabilities (5)

Recommendations

Tutorials



DDoS protection

Configure additional protection from distributed denial of service

● Not configured



Azure Firewall

Protect your network with a stateful L3-L7 firewall.

● Not configured



Peerings

Seamlessly connect two or more virtual networks.

● Not configured



Security

Filter network traffic to and from Azure resources.



Private endpoints

Privately access Azure services without sending traffic across

● Not configured

# NSG (Security) Rules Summary

NSG	Rule	Action
NSG-Web	Allow Internet + App Tier	Allow
NSG-Web	Deny DB Tier	Deny
NSG-App	Allow Web + DB Tier	Allow
NSG-App	Deny Internet	Deny
NSG-DB	Allow from App Tier only	Allow
NSG-DB	Deny Web & Internet	Deny

Home > Network security groups > myNSG

myNSG | Subnets

Network security group

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Inbound security rules

Outbound security rules

Network interfaces

Subnets

Properties

Locks

Associate

Search subnets

Name	Address range	Virtual network	
mySubnet	10.0.0.0/24	myVNet	...

Network security groups > DefaultNSGforTestvNet

DefaultNSGforTestvNet

Overview

Resource group (change)  
RG-HarvestingCloud-NSGs

Location  
East US

Subscription (change)  
Visual Studio Enterprise

Subscription ID  
d407fb02-4bc4-439a-81b1-1af82b0bb049

Tags (change)  
Department : Finance CostCenter : CC01345

Custom security rules  
0 inbound, 0 outbound  
Associated with  
0 subnets, 0 network interfaces

Inbound security rules

Priority	Name	Port	Protocol	Source	Destination
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowInternetOutBound	Any	Any	Any	Internet
65500	DenyAllOutBound	Any	Any	Any	Any

Activity log	110	vCloud-Web-Application	Any	Any	HTTP (TCP/80)	Allow	...
Access control (IAM)	120	vCloud-Web-Application-SSL	Any	Any	HTTPS (TCP/443)	Allow	...
Tags	130	vCloud-Tomcat-Application0...	199.124.100.11	Any	Custom (Any/8080)	Allow	...
Diagnose and solve problems	140	vCloud-Tomcat-Application0...	AzureLoadBal...	Any	Custom (Any/8010)	Allow	...
SETTINGS	150	vCloud-OtherPorts-Applicati...	10.105.100.0/24	Any	Custom (Any/9000)	Allow	...
Inbound security rules	160	vCloud-OtherPorts-Applicati...	VirtualNetwork	Any	Custom (Any/9001)	Allow	...
Outbound security rules	170	vCloud-OtherPorts-Applicati...	Internet	Any	Custom (Any/9002)	Allow	...
Network interfaces	180	vCloud-OtherPorts-Applicati...	10.10.10.0/25	Any	Custom (Any/9003)	Allow	...
Subnets	190	vCloud-OtherPorts-Applicati...	Any	Any	Custom (Any/10000-10020)	Allow	...
Properties	4095	Block-All	Any	Any	Custom (Any/Any)	Deny	...
Locks							
Automation script							
MONITORING							
Diagnostics logs							

Resource groups > POC-VPN > Windows-VM-Firewall-NSG - Inbound security rules

Windows-VM-Firewall-NSG - Inbound security rules

Default rules

Search (Ctrl+J)

PRIORITY	NAME	SOURCE	DESTINATION	SERVICE	ACTION
100	Open_RDP_Rule	Any	Any	RDP (TCP/3389)	Allow
65000	AllowVnetInBound	VirtualNetwork	VirtualNetwork	Custom (Any/Any)	Allow
65001	AllowAzureLoadBalancerInBound	AzureLoadBalancer	Any	Custom (Any/Any)	Allow
65500	DenyAllInBound	Any	Any	Custom (Any/Any)	Deny

## Virtual Machine Deployment (6 Total)

Tier	Linux VM	Windows VM	Web Server
Web Tier	web-linux-vm	web-win-vm	Apache / IIS
App Tier	app-linux-vm	app-win-vm	Apache / IIS
DB Tier	db-linux-vm	db-win-vm	Optional

The screenshot shows the Azure portal interface for managing virtual machines. On the left, the 'Virtual machines' page lists three VMs: vm1, vm2, and vm3. A red box labeled '1' highlights the 'vm1' entry. In the center, the 'vm1 | Networking' settings page is shown, with a red box labeled '2' highlighting the 'Networking' tab in the left-hand settings menu. On the right, the 'Network Interface: vm141' configuration is displayed, with a red box labeled '3' highlighting the 'vm141' text next to the network interface name.

## Server Configuration

- Apache on Linux VMs:

```
sudo apt update
sudo apt install apache2 -y
sudo systemctl enable apache2
sudo systemctl start apache2
```

- IIS on Windows VMs:

```
Install-WindowsFeature -Name Web-Server -
```

Apache2 Ubuntu Default Page (i) x +

← → ↻ ⚠ Not secure | IP Address

⌵ 📄 👤 Guest ⋮



# Ubuntu

## Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

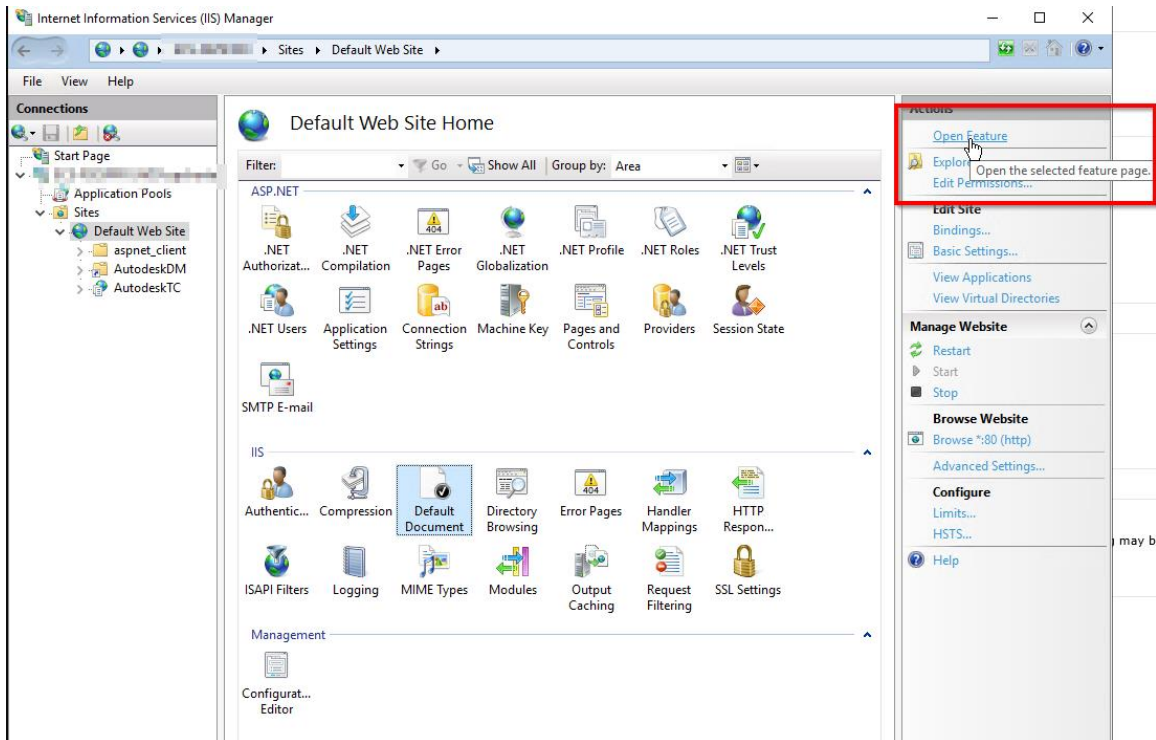
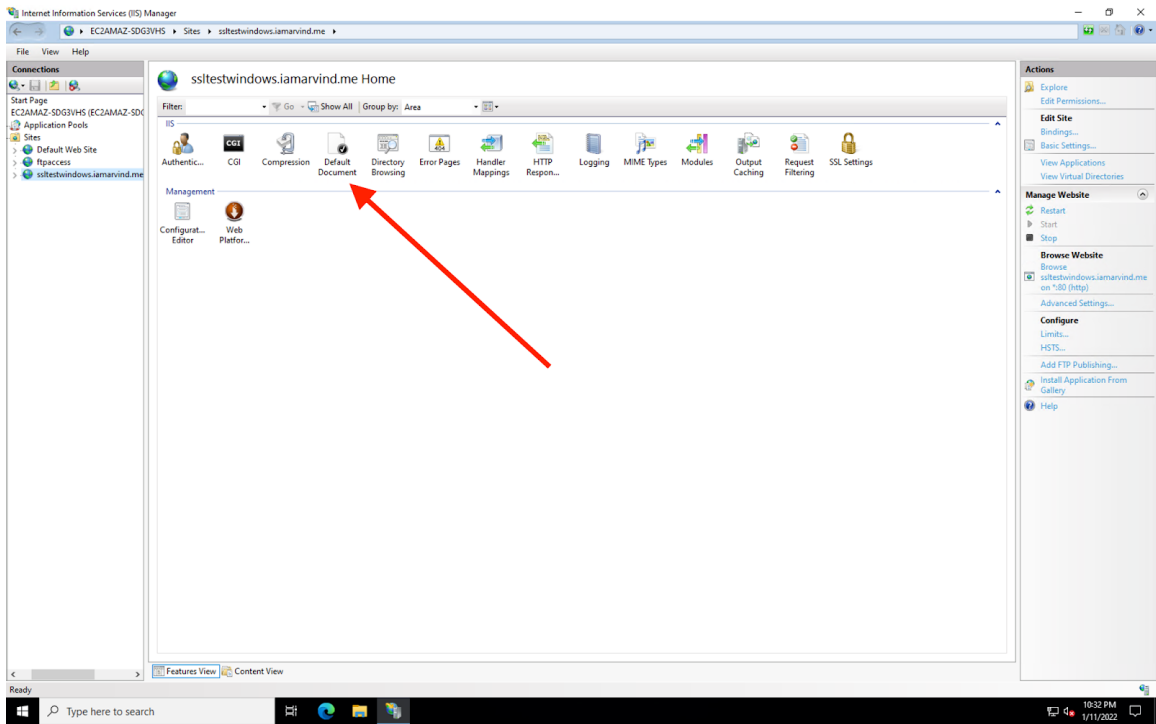
### Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/  
|-- apache2.conf  
|  
|-- ports.conf  
|  
|-- mods-enabled  
|   |-- *.Load  
|   |-- *.conf  
|  
|-- conf-enabled  
|   |-- *.conf  
|  
|-- sites-enabled  
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2` and is managed using `systemd`, so to start/stop the service use





## Access Testing Summary

Source →Target	Result
Web →App	Allowed
App →Web/DB	Allowed
Web →DB	Denied
DB →Any	Denied



Internet → web

Allowed

Dashboard > CreateVm-Canonical.UbuntuServer- - Overview > -vm - Reset password

### ubuntu-prod-vm - Reset password

Virtual machine

Search (Ctrl+/)

Support + troubleshooting

- Resource health
- Boot diagnostics
- Reset password**
- Redeploy
- Ubuntu Advantage support ...
- Serial console
- Connection troubleshoot
- New support request

Update Discard

This uses the VMAccessForLinux extension to reset the credentials of an existing user or create a new user with sudo privileges, and reset the SSH configuration. [Learn more](#)

Mode ⓘ

- ☐ Reset password
- ☒ Reset SSH public key
- ☐ Reset configuration only

\* Username ⓘ

adminuser

\* SSH public key ⓘ

```
Administrator: Command Prompt

Ethernet adapter Ethernet 3:

    Connection-specific DNS Suffix  . : 322s0apa1pyubwfaaifixkmzd.hx.internal.cloudapp.net
    Link-local IPv6 Address . . . . . : fe80::fdfd:83c2:9bea:c003%6
    IPv4 Address. . . . . : 10.0.0.7
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.0.1

Ethernet adapter Ethernet 4:

    Connection-specific DNS Suffix  . : 322s0apa1pyubwfaaifixkmzd.hx.internal.cloudapp.net
    Link-local IPv6 Address . . . . . : fe80::608f:f38d:b78:1a55%7
    IPv4 Address. . . . . : 192.168.0.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . :

Tunnel adapter isatap.322s0apa1pyubwfaaifixkmzd.hx.internal.cloudapp.net:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 322s0apa1pyubwfaaifixkmzd.hx.internal.cloudapp.net

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . :

C:\Users\thomas>route print
```

```
Administrator: Command Prompt

IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
-----
0.0.0.0                    0.0.0.0          10.0.0.1         10.0.0.7         10
0.0.0.0                    0.0.0.0          192.168.0.1      192.168.0.4      266
10.0.0.0                   255.255.255.0    On-link          10.0.0.7         266
10.0.0.7                   255.255.255.255  On-link          10.0.0.7         266
10.0.0.255                 255.255.255.255  On-link          10.0.0.7         266
127.0.0.0                  255.0.0.0        On-link          127.0.0.1        331
127.0.0.1                  255.255.255.255  On-link          127.0.0.1        331
127.255.255.255            255.255.255.255  On-link          127.0.0.1        331
168.63.129.16              255.255.255.255  10.0.0.1         10.0.0.7         11
169.254.169.254            255.255.255.255  10.0.0.1         10.0.0.7         11
192.168.0.0                255.255.255.0    On-link          192.168.0.4      266
192.168.0.4                255.255.255.255  On-link          192.168.0.4      266
192.168.0.255              255.255.255.255  On-link          192.168.0.4      266
224.0.0.0                  240.0.0.0        On-link          127.0.0.1        331
224.0.0.0                  240.0.0.0        On-link          10.0.0.7         266
224.0.0.0                  240.0.0.0        On-link          192.168.0.4      266
255.255.255.255            255.255.255.255  On-link          127.0.0.1        331
255.255.255.255            255.255.255.255  On-link          10.0.0.7         266
255.255.255.255            255.255.255.255  On-link          192.168.0.4      266

Persistent Routes:
Network Address          Netmask  Gateway Address  Metric
-----
0.0.0.0                  0.0.0.0  192.168.0.1      Default
```

## Conclusion

Successfully deployed a secure 3-tier architecture on Azure. All tiers are correctly isolated with NSG rules, web servers are configured, and testing validates controlled access between components.