Azure 3-Tier Architecture Deployment

Submitted by: Sanskar Vishnoi

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

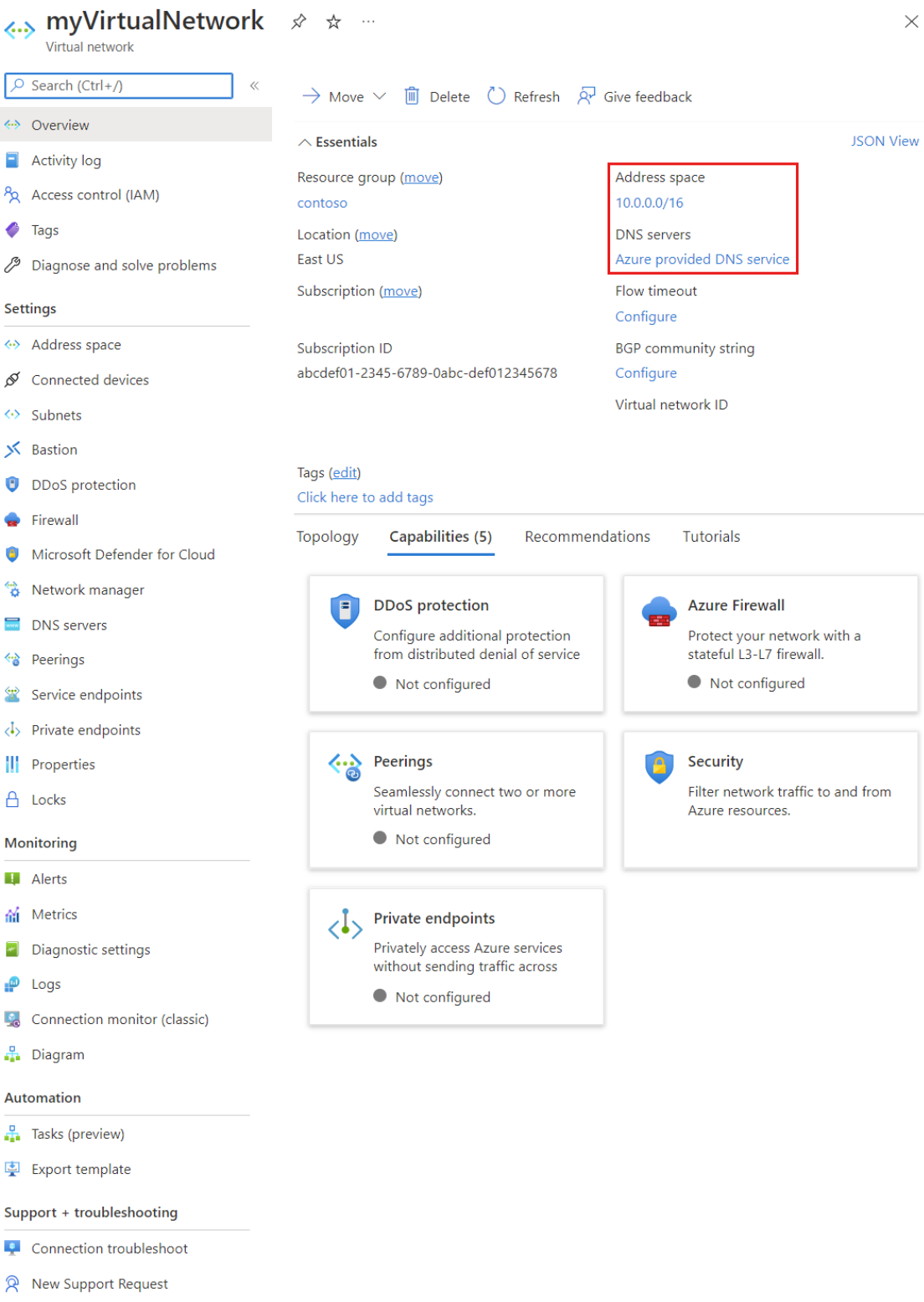
Date: July 12, 2025

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 acccess 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.

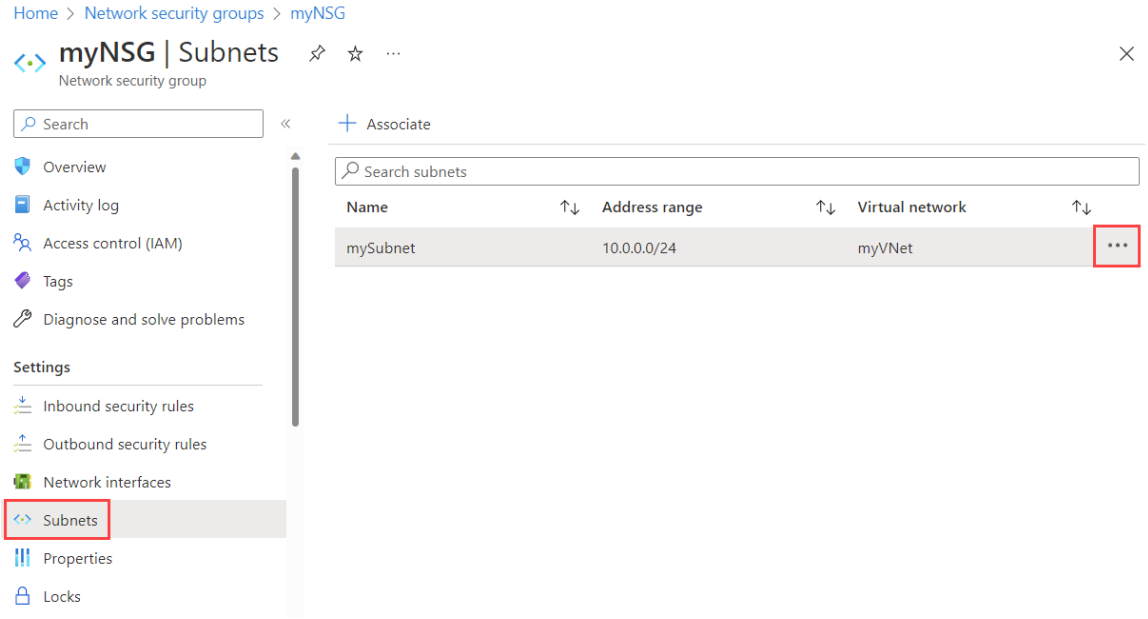
Architecture Summary

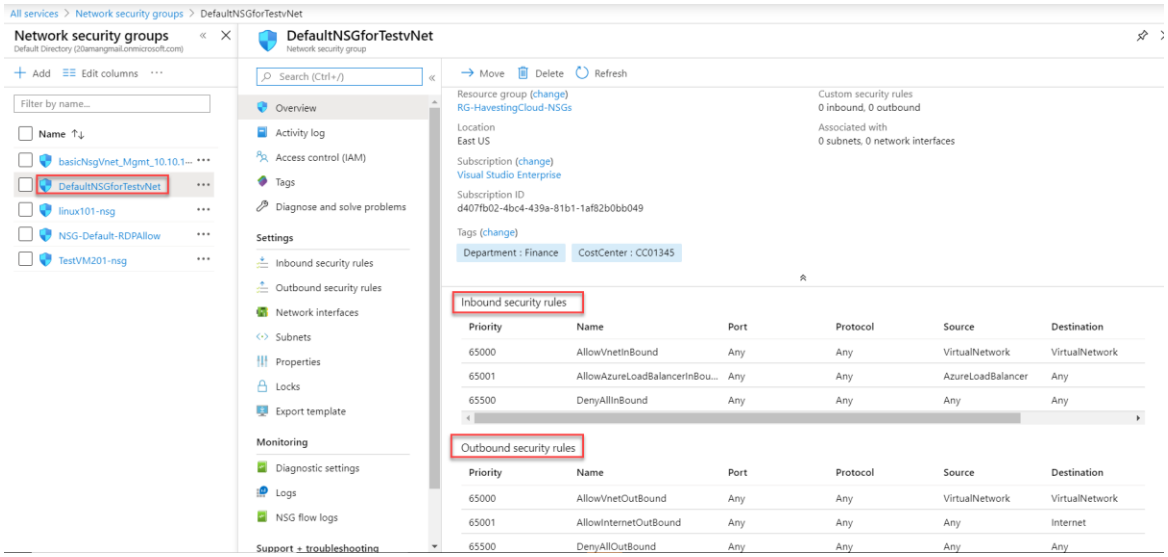
Tier	Subnet	IP Range	Internet Access	Access Rules
Web Tier	Subnet-Web	10.0.1.0/24	Yes	Can access App Tier only
App Tier	Subnet-App	10.0.2.0/24	No	Can access Web & DB Tier
DB Tier	Subnet-DB	10.0.3.0/24	No	Cannot access any other tier

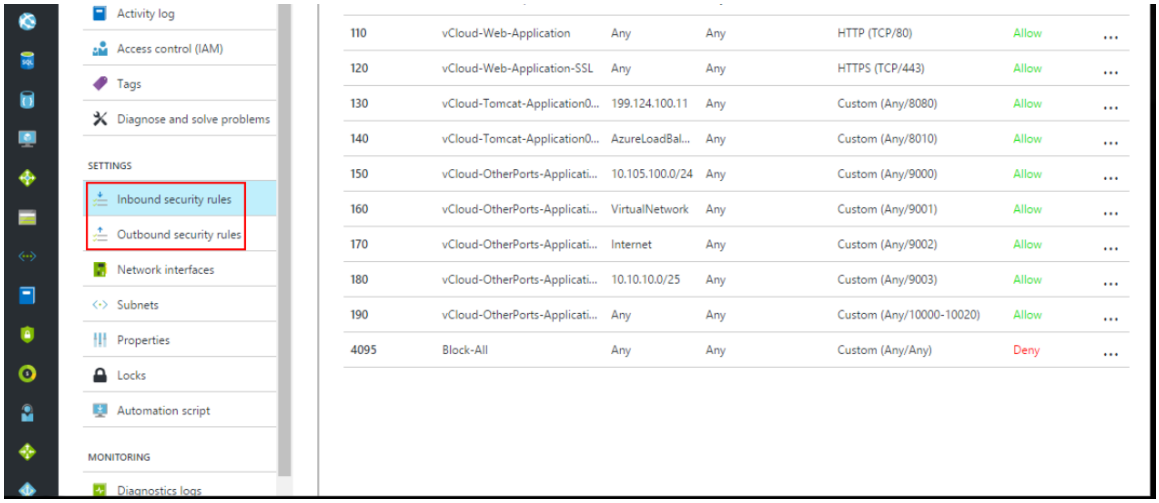

myVirtualNetwork
Virtual network
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
Bastion
DDoS protection
Firewall
Microsoft Defender for Cloud
Network manager
DNS servers
Peerings
Service endpoints
Private endpoints
Properties
Locks
Monitoring
Alerts
Metrics
Diagnostic settings
Logs
Connection monitor (classic)
Diagram
Automation
Tasks (preview)
Export template
Support + troubleshooting
Connection troubleshoot
New Support Request
Move
Delete
Refresh
Give feedback
Essentials
JSON View
Resource group (move)
contoso
Location (move)
East US
Subscription (move)
Subscription ID
abcdef01-2345-6789-0abc-def012345678
Address space
10.0.0.0/16
DNS servers
Azure provided DNS service
Flow timeout
Configure
BGP community string
Configure
Virtual network ID
Tags (edit)
Click here to add tags
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

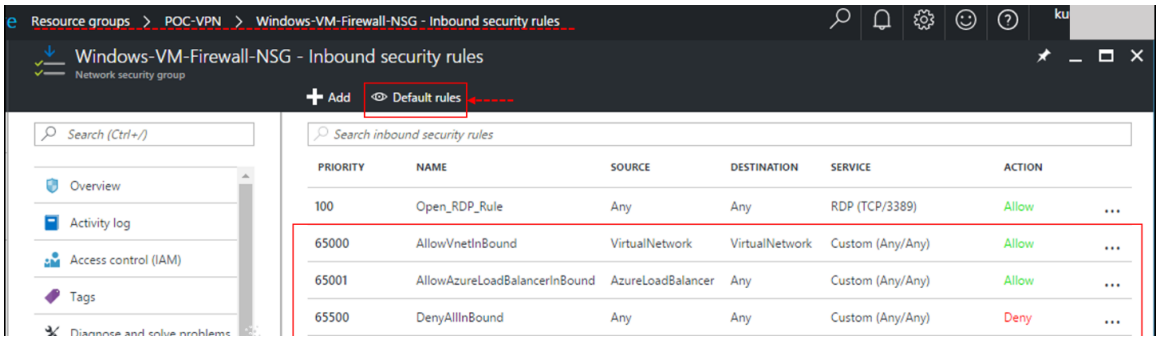
NSG (Security) Rules Summary

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



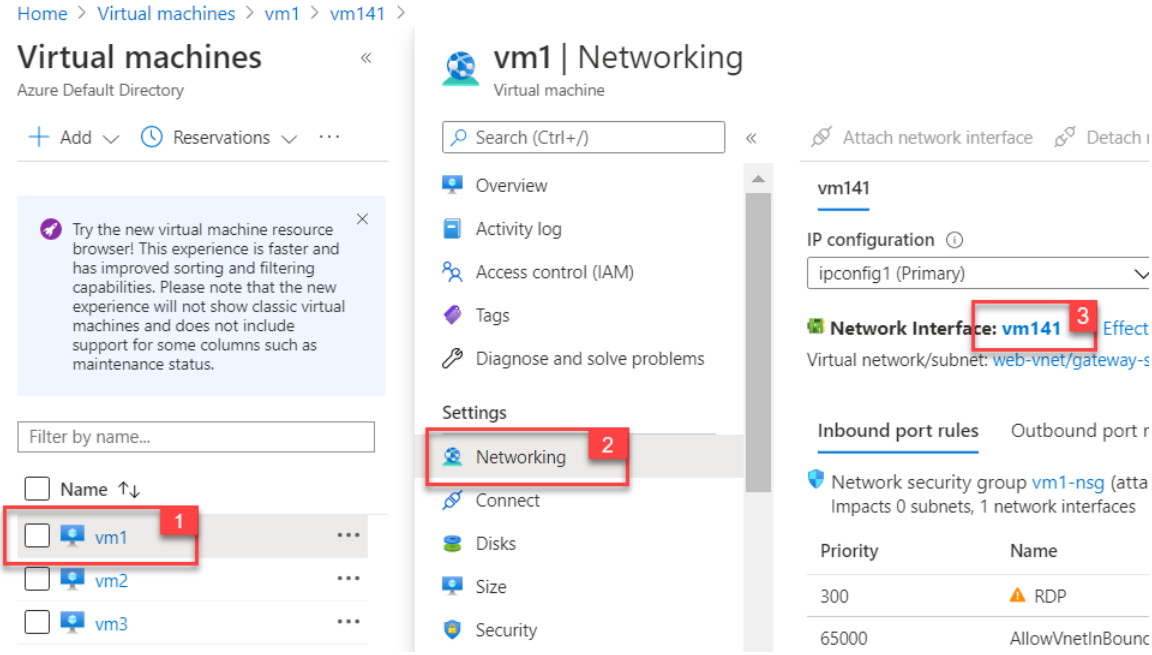

All services > Network security groups > DefaultNSGforTestvNet
Network security groups
Default Directory (20amangmail.onmicrosoft.com)
Add
Edit columns
Filter by name...
Name
basicNsgVnet_Mgmt_10.10.1...
DefaultNSGforTestvNet
linux101-nsg
NSG-Default-RDPAllow
TestVM201-nsg
DefaultNSGforTestvNet
Network security group
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Export template
Monitoring
Diagnostic settings
Logs
NSG flow logs
Support + troubleshooting
Move
Delete
Refresh
Resource group (change)
RG-HavestingCloud-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 AllowAzureLoadBalancerInBou... 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
Access control (IAM)
Tags
Diagnose and solve problems
SETTINGS
Inbound security rules
Outbound security rules
Network interfaces
Subnets
Properties
Locks
Automation script
MONITORING
Diagnostics logs
110 vCloud-Web-Application Any Any HTTP (TCP/80) Allow
120 vCloud-Web-Application-SSL Any Any HTTPS (TCP/443) Allow
130 vCloud-Tomcat-Application0... 199.124.100.11 Any Custom (Any/8080) Allow
140 vCloud-Tomcat-Application0... AzureLoadBal... Any Custom (Any/8010) Allow
150 vCloud-OtherPorts-Applicati... 10.105.100.0/24 Any Custom (Any/9000) Allow
160 vCloud-OtherPorts-Applicati... VirtualNetwork Any Custom (Any/9001) Allow
170 vCloud-OtherPorts-Applicati... Internet Any Custom (Any/9002) Allow
180 vCloud-OtherPorts-Applicati... 10.10.10.0/25 Any Custom (Any/9003) Allow
190 vCloud-OtherPorts-Applicati... Any Any Custom (Any/10000-10020) Allow
4095 Block-All Any Any Custom (Any/Any) Deny


Resource groups > POC-VPN > Windows-VM-Firewall-NSG - Inbound security rules
Windows-VM-Firewall-NSG - Inbound security rules
Network security group
Add
Default rules
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Search inbound security rules
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



Server Configuration

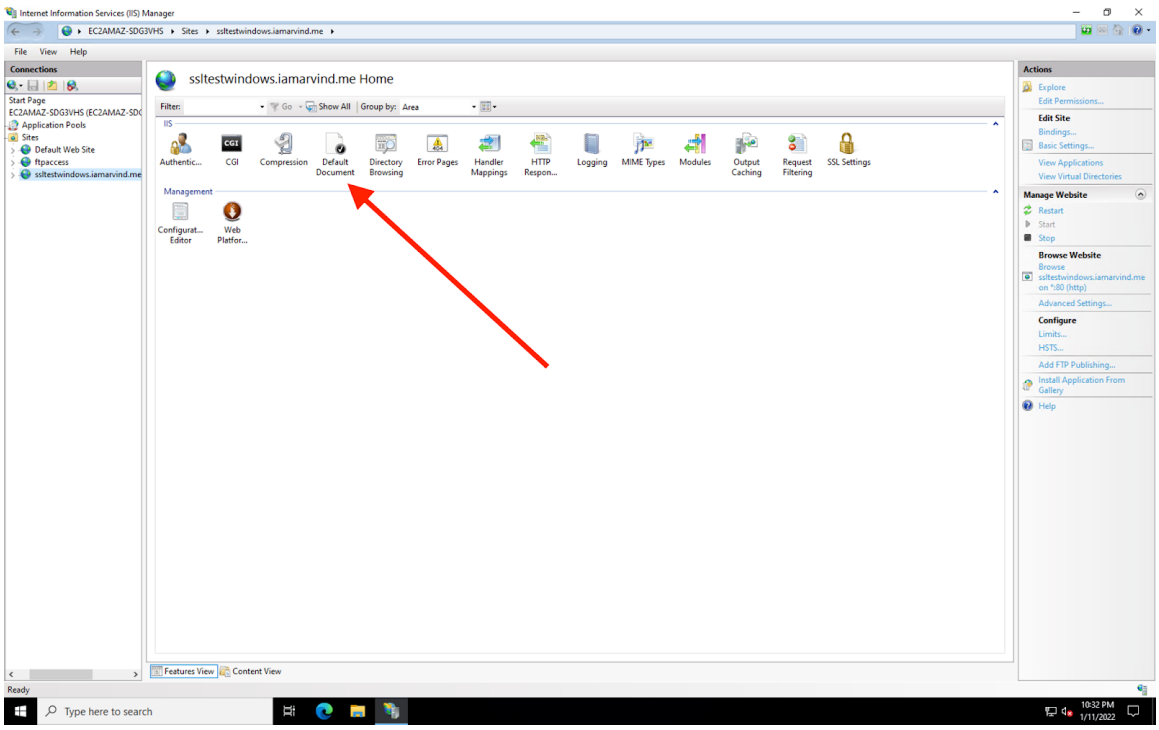
- Apache on Linux VMs:

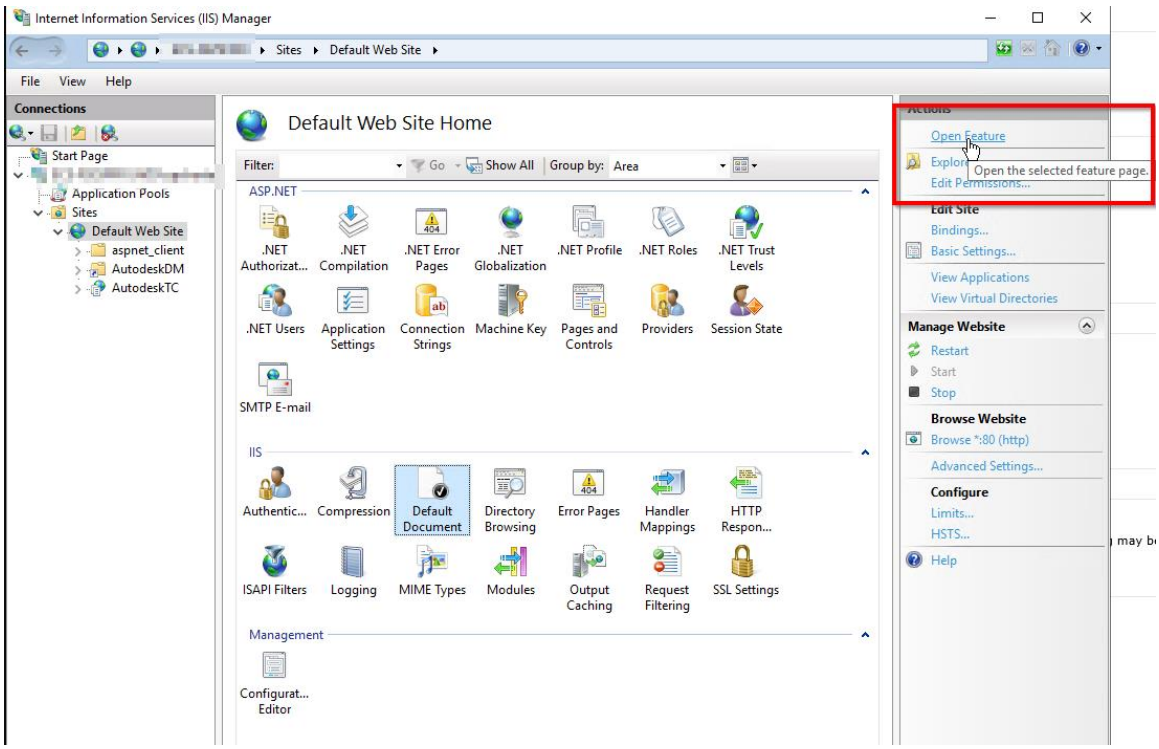
```
sudo apt update
sudo apt install apache2 -y
sudo systemctl enable apache2
sudo systemctl start apache2
```

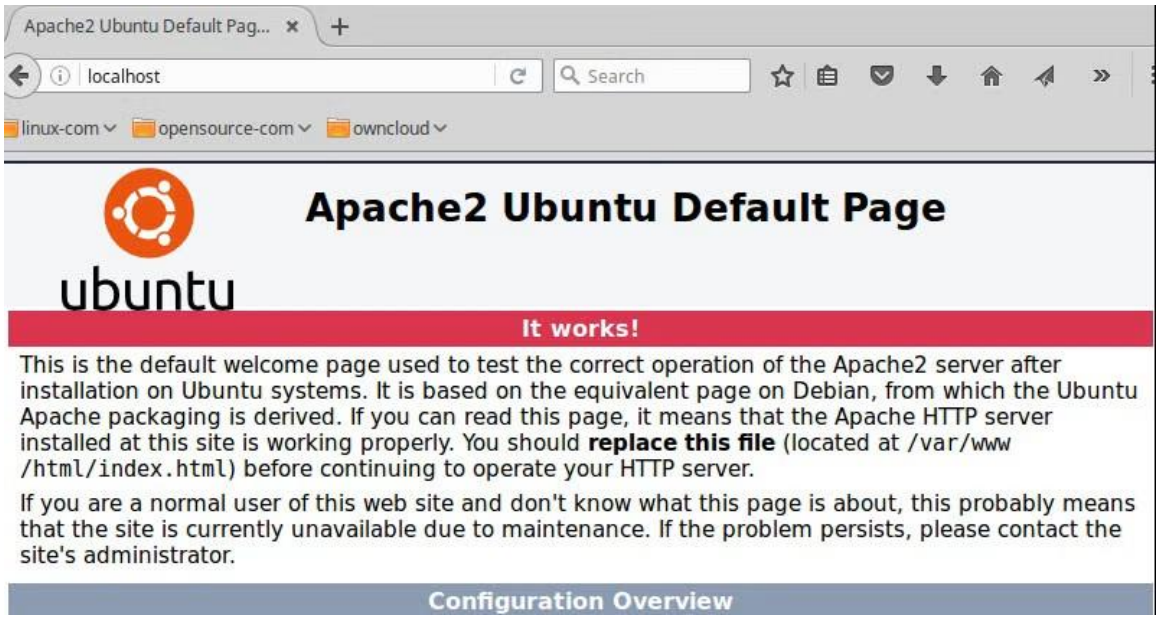
- IIS on Windows VMs:

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

IncludeManagementTools


Internet Information Services (IIS) Manager
ssltestwindows.iamarvind.me Home
Default Document
Actions
Explore
Edit Permissions...
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Advanced Settings...
Configure
Limits...
HSTS...
Add FTP Publishing...
Install Application From Gallery
Help
Features View
Content View
Ready
Type here to search

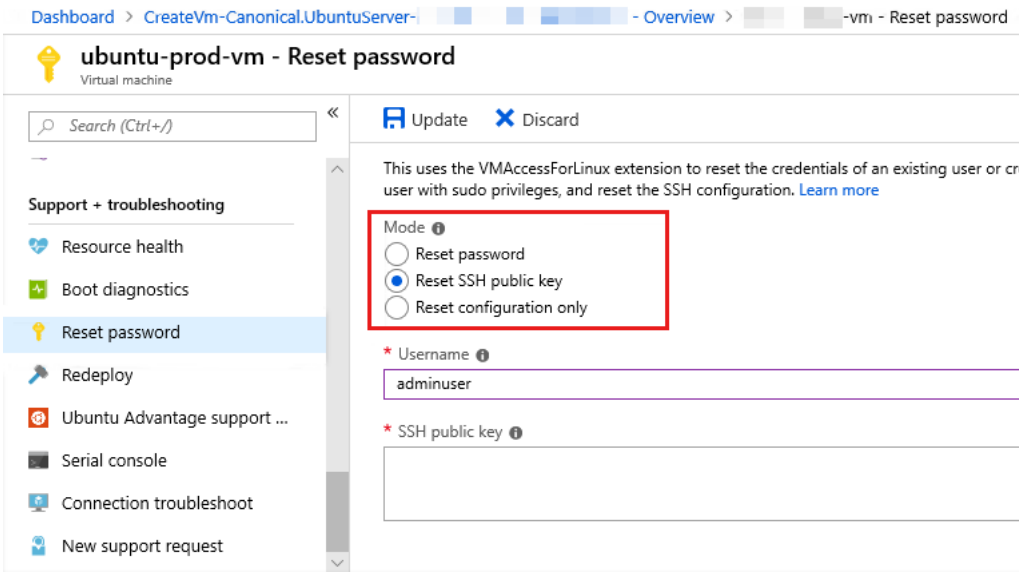

Internet Information Services (IIS) Manager
Sites
Default Web Site
File
View
Help
Connections
Start Page
Application Pools
Sites
Default Web Site
aspnet_client
AutodeskDM
AutodeskTC
Default Web Site Home
Filter:
Show All
Group by:
Area
ASP.NET
.NET Authorizat...
.NET Compilation
.NET Error Pages
.NET Globalization
.NET Profile
.NET Roles
.NET Trust Levels
.NET Users
Application Settings
Connection Strings
Machine Key
Pages and Controls
Providers
Session State
SMTP E-mail
IIS
Authentic...
Compression
Default Document
Directory Browsing
Error Pages
Handler Mappings
HTTP Respon...
ISAPI Filters
Logging
MIME Types
Modules
Output Caching
Request Filtering
SSL Settings
Management
Configurat... Editor
Actions
Open Feature
Explore
Edit Permissions...
Open the selected feature page.
Edit Site
Bindings...
Basic Settings...
View Applications
View Virtual Directories
Manage Website
Restart
Start
Stop
Browse Website
Browse *:80 (http)
Advanced Settings...
Configure
Limits...
HSTS...
Help

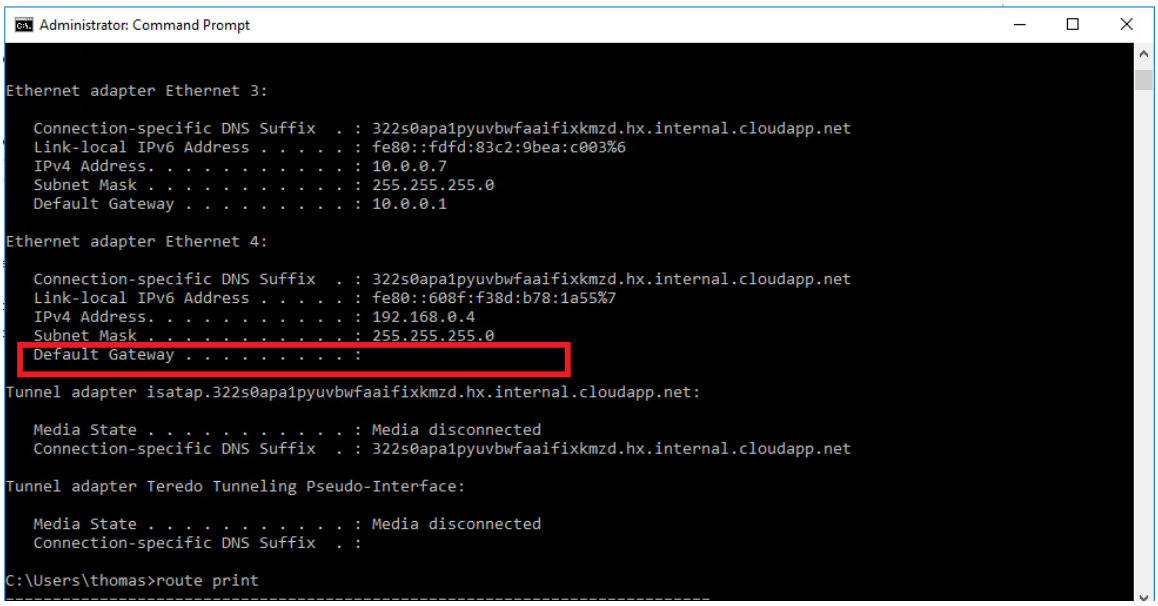


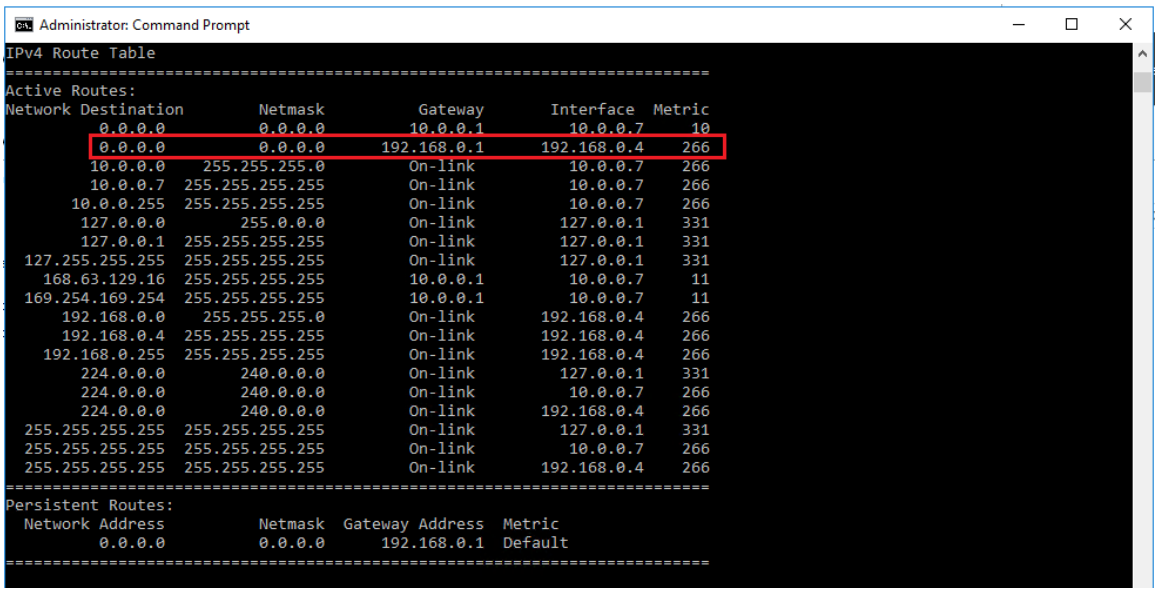
Access Testing Summary

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

Internet ➞web Allowed







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.