Beginner’s Azure Cloud Deployment & Disaster Recovery Tutorial

Author: Abid Us Sobhan
Date: 12/01/26
Purpose: This project demonstrates enterprise-style cloud deployment in Microsoft Azure, including virtual network setup, Windows Server VM deployment, firewall configuration, user access simulation, and backup/disaster recovery planning.

Contents

Beginner’s Azure Cloud Deployment & Disaster Recovery Project 1

1. Introduction 3

2. Architecture Diagram 3

3. Step-by-Step Setup 4

4. Network Security Configuration 6

5. User Access Simulation 7

6. Backup & Disaster Recovery 8

7. Troubleshooting & Learnings 8

8. Conclusion 9

1. Introduction

This project simulates an enterprise cloud environment using Microsoft Azure. It covers the following core objectives:

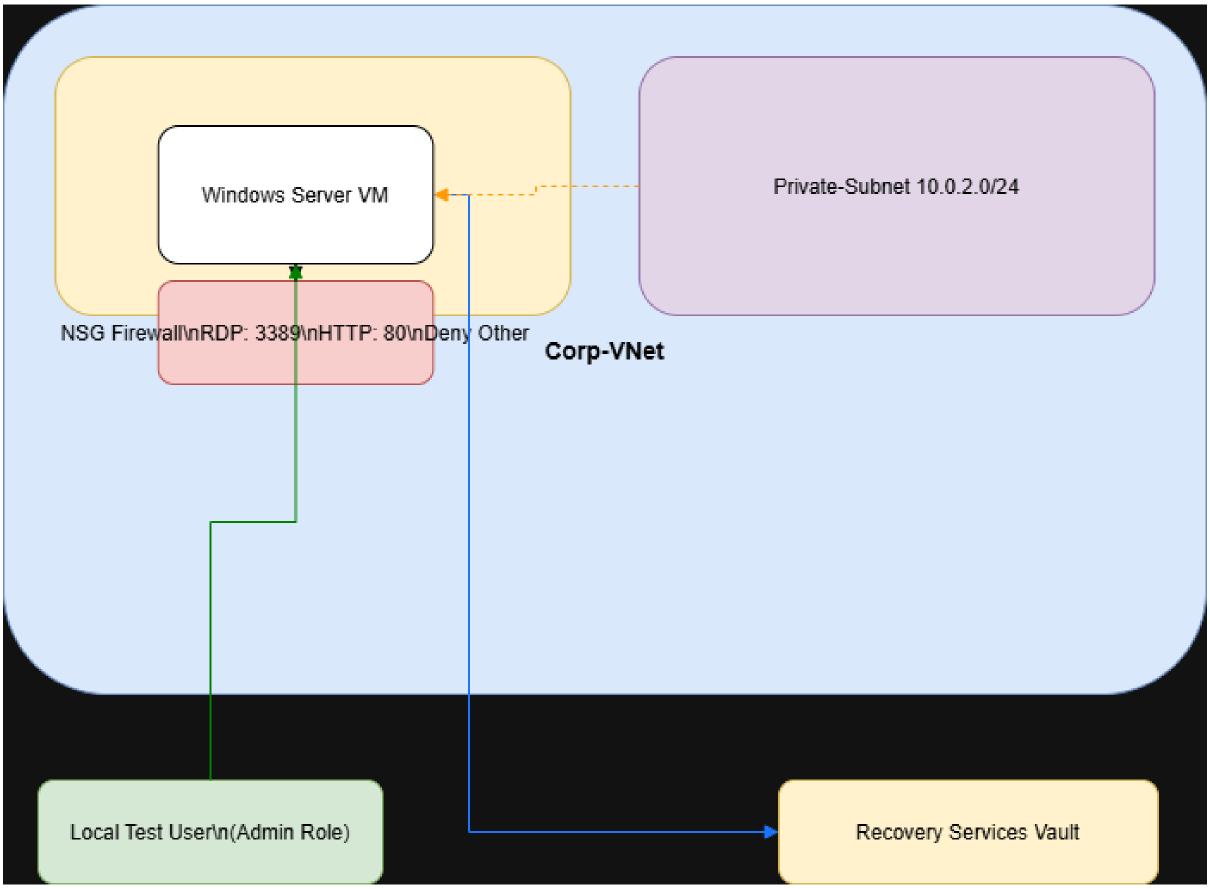
- Deployment of a Windows Server Virtual Machine (VM) within a **subnetted Virtual Network (VNet)**.
- Configuration of **Network Security Groups (NSGs)** to enforce firewall rules and secure inbound traffic.
- Simulation of **role-based access control** using a local user account.
- Implementation of **backup and disaster recovery** using Azure Recovery Services Vault.
- Hands-on troubleshooting of connectivity, firewall rules, and backup restoration.

The project provides practical experience in **cloud networking, security, system administration, and disaster recovery planning**, reflecting skills required in enterprise IT and cybersecurity roles.

2. Architecture Diagram

Planned Architecture Overview:

- **Virtual Network (Corp-VNet)** with two subnets: Public-Subnet and Private-Subnet
- **Windows Server VM** deployed in Public-Subnet
- **NSG** controlling inbound and outbound traffic
- **Local test user** simulating Azure AD role-based access
- **Backup Vault** linked to VM for disaster recovery


Windows Server VM
Private-Subnet 10.0.2.0/24
NSG Firewall\nRDP: 3389\nHTTP: 80\nDeny Other
Corp-VNet
Local Test User\n(Admin Role)
Recovery Services Vault

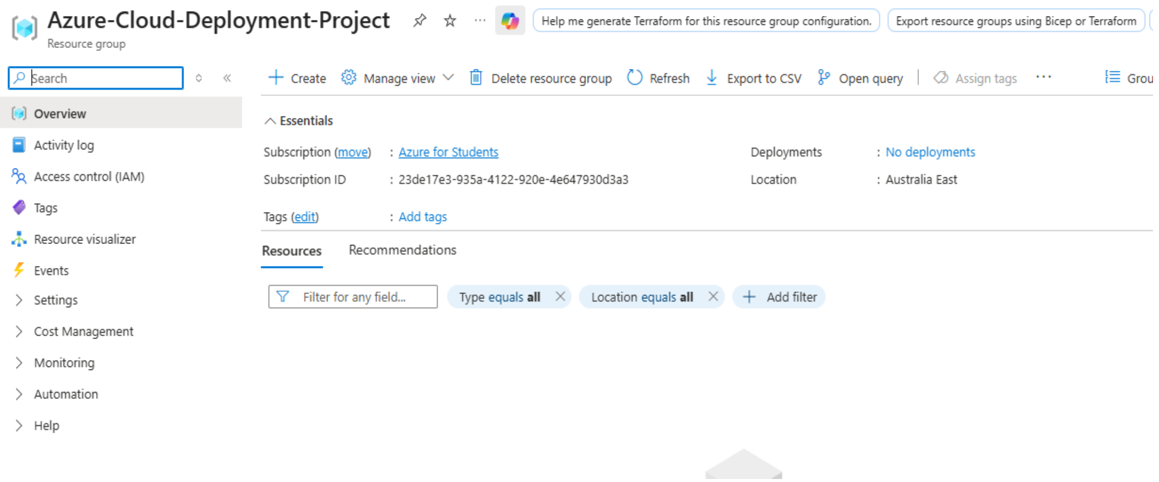
Picture1: diagram.drawio

---

3. Step-by-Step Setup

3.1 Resource Group Creation

- Created **Corp-RG** in Asia East to logically group all project resources.



Essentials

Subscription (move) : Azure for Students

Subscription ID : 23de17e3-935a-4122-920e-4e647930d3a3

Tags (edit) : Add tags

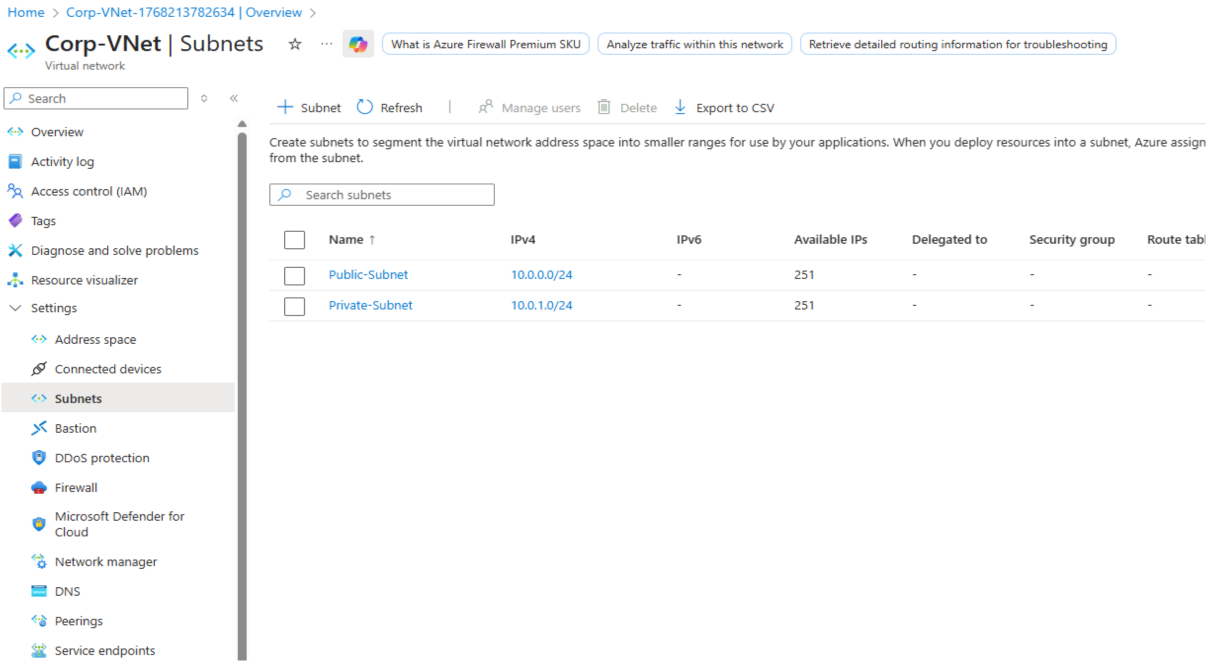
Deployments : No deployments

Location : Australia East

Picture2: resource-group

3.2 Virtual Network & Subnets

- Created **Corp-VNet** with IPv4 address space 10.0.0.0/16.
- Configured two subnets:
  - **Public-Subnet:** 10.0.1.0/24 (for internet-facing VM)
  - **Private-Subnet:** 10.0.2.0/24 (for internal resources)



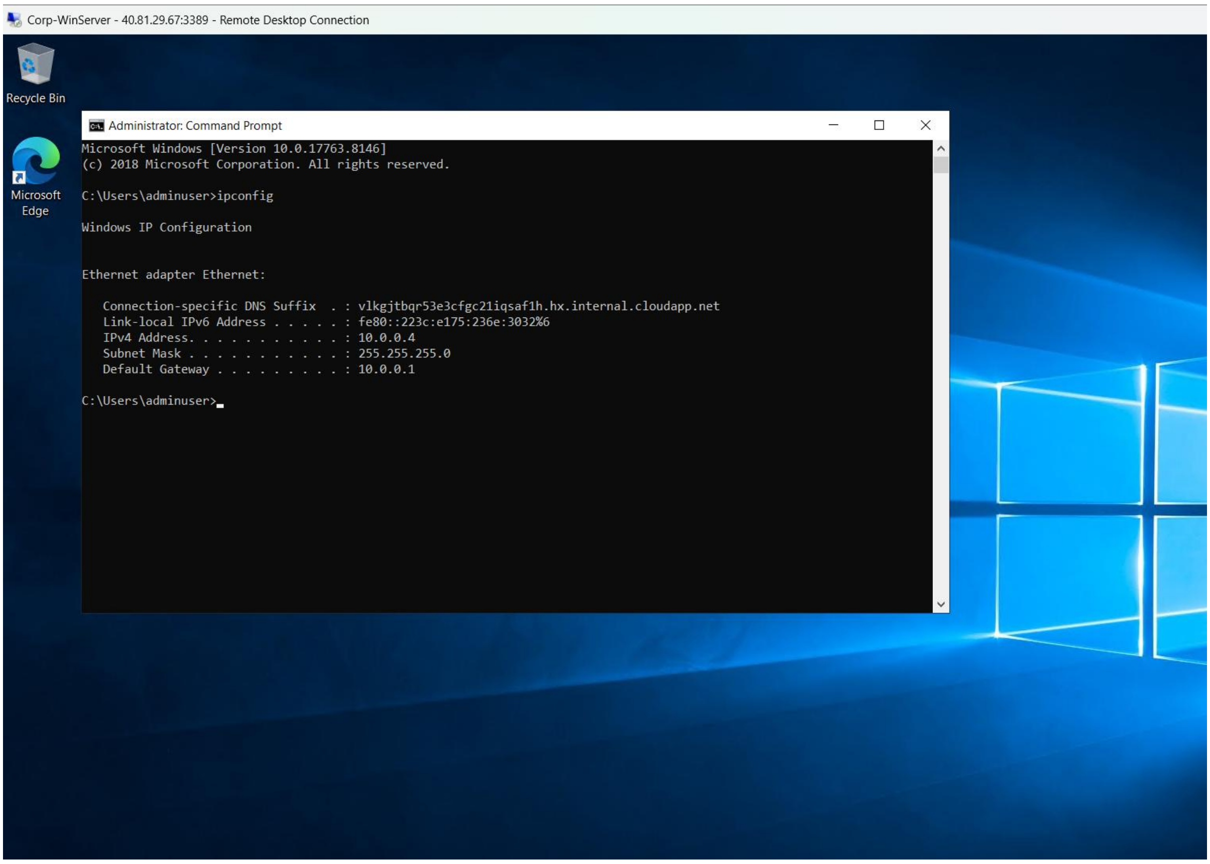
Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assign from the subnet.

□	Name ↑	IPv4	IPv6	Available IPs	Delegated to	Security group	Route tabl
□	Public-Subnet	10.0.0.0/24	-	251	-	-	-
□	Private-Subnet	10.0.1.0/24	-	251	-	-	-

Picture3: subnets

3.3 Windows Server VM Deployment

- Deployed **Windows Server 2019 Datacenter** VM (Corp-VM) in Public-Subnet.
- Assigned admin user: adminuser.
- Configured RDP access for management.



Corp-WinServer - 40.81.29.67:3389 - Remote Desktop Connection
Recycle Bin
Microsoft Edge
Administrator: Command Prompt

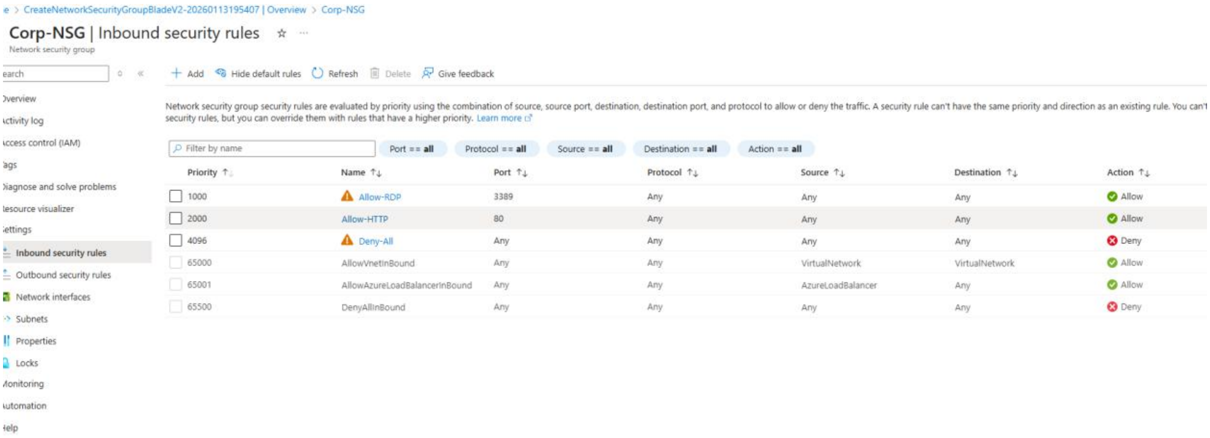
```
Microsoft Windows [Version 10.0.17763.8146]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\adminuser>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : vlkgjtbqr53e3cfgc21iqsaf1h.hx.internal.cloudapp.net
   Link-local IPv6 Address . . . . . : fe80::223c:e175:236e:3032%6
   IPv4 Address. . . . . . . . . . . : 10.0.0.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.0.1

C:\Users\adminuser>
```

Picture4: vm-overview

---

4. Network Security Configuration

- Created **NSG (Corp-NSG)** to control inbound traffic:
  - **Allow RDP (3389)** for remote administration
  - **Allow HTTP (80)** for optional testing
  - **Deny all other inbound ports** to enforce security
- Verified NSG functionality by testing RDP connectivity and temporarily blocking allowed ports to confirm firewall behavior.



e > CreateNetworkSecurityGroupBladeV2-20260113195407 | Overview > Corp-NSG

Corp-NSG | Inbound security rules

Network security group

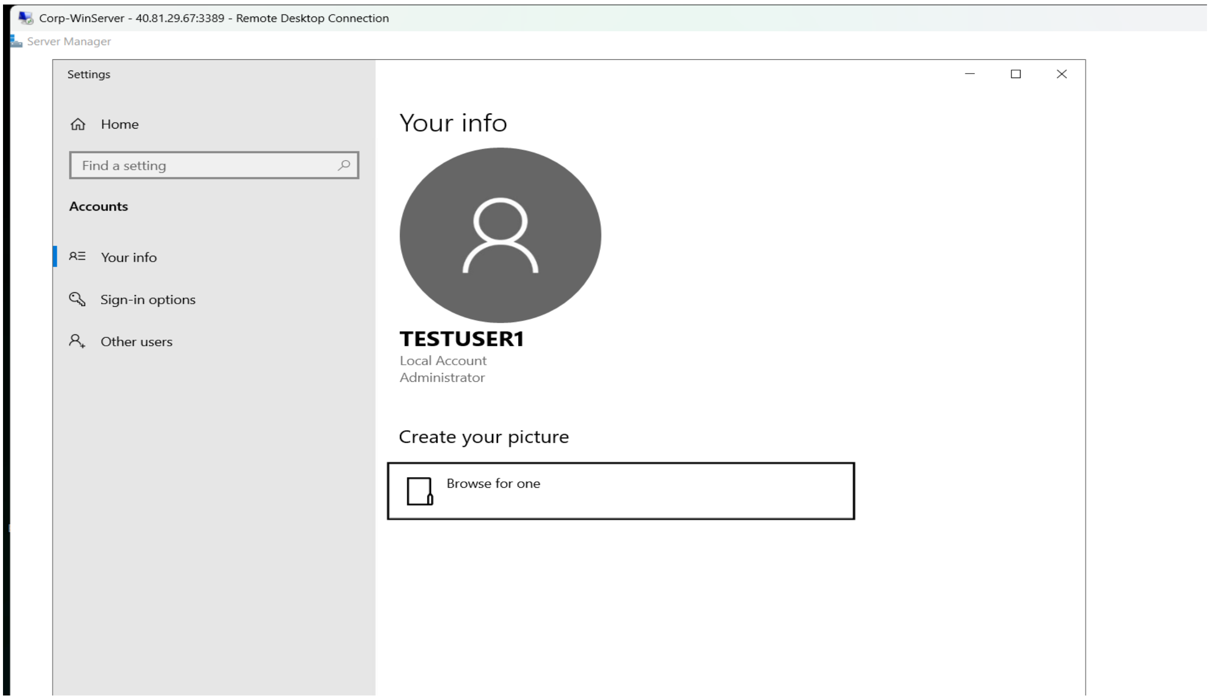
Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't security rules, but you can override them with rules that have a higher priority. Learn more

	Priority	Name	Port	Protocol	Source	Destination	Action
□	1000	⚠ Allow-RDP	3389	Any	Any	Any	✓ Allow
□	2000	Allow-HTTP	80	Any	Any	Any	✓ Allow
□	4096	⚠ Deny-All	Any	Any	Any	Any	✗ Deny
□	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
□	65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
□	65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

Picture5: nsg overview

5. User Access Simulation

- Created a local user **testuser** to simulate Azure AD role-based access due to subscription limitations.
- Assigned **Administrator privileges** to the local user.
- Verified login and access capabilities on the VM.



Corp-WinServer - 40.81.29.67:3389 - Remote Desktop Connection

Your info

TESTUSER1

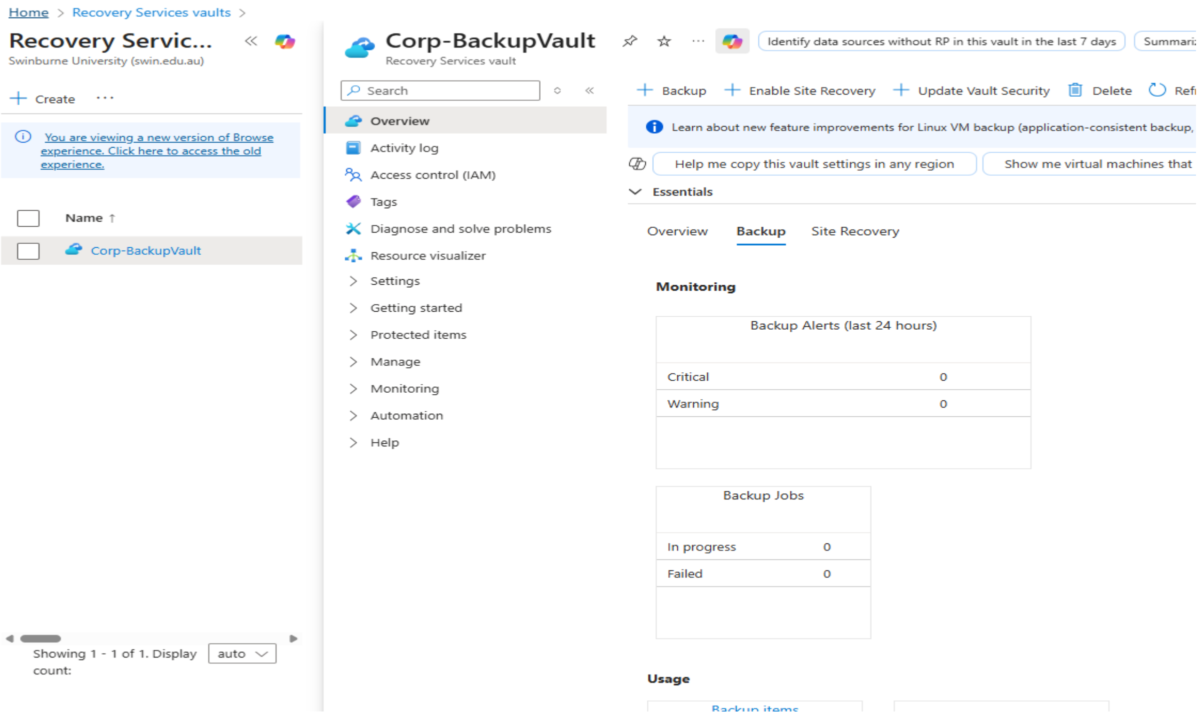
Local Account

Administrator

Picture6: Local user access

6. Backup & Disaster Recovery

- Configured **Recovery Services Vault (Corp-BackupVault)** for the VM.



You are viewing a new version of Browse experience. Click here to access the old experience.

Showing 1 - 1 of 1. Display count: auto

Learn about new feature improvements for Linux VM backup (application-consistent backup,

Backup Alerts (last 24 hours)	
Critical	0
Warning	0

Backup Jobs	
In progress	0
Failed	0

Picture7: Backup vault

- Backup schedule: Daily retention for 7 days.
- **Recommended DR workflow exercises :**

  1. Create test file important.txt in the VM.
  2. Trigger backup (status in progress / planned).
  3. Simulate disaster by deleting the file.
  4. Restore the VM from the backup and verify file recovery.

7. Troubleshooting & Learnings

Recommended troubleshooting exercises included:

- Temporary blocking of RDP and HTTP ports to validate NSG behaviour.
- Moving VM to Private-Subnet and testing connectivity between subnets.
- Monitoring VM metrics and logs using Azure Monitor.

Key Learnings:

- Subnetting provides traffic isolation and security segmentation.
- NSGs allow granular control of network access.
- Local users can simulate role-based access control in absence of Azure AD.
- Recovery Services Vault allows planning for enterprise-grade disaster recovery.
- Troubleshooting connectivity and backup issues mirrors real-world enterprise IT scenarios.

---

8. Conclusion

This project demonstrates **end-to-end cloud deployment**:

- Subnetted Virtual Network with Public/Private subnets
- Windows Server VM deployment and administration
- Firewall configuration using NSG rules
- User access simulation
- Backup and disaster recovery planning
- Troubleshooting of network and VM operations