رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات

Azure Cloud Infrastructure Deployment and Management

Team Members:

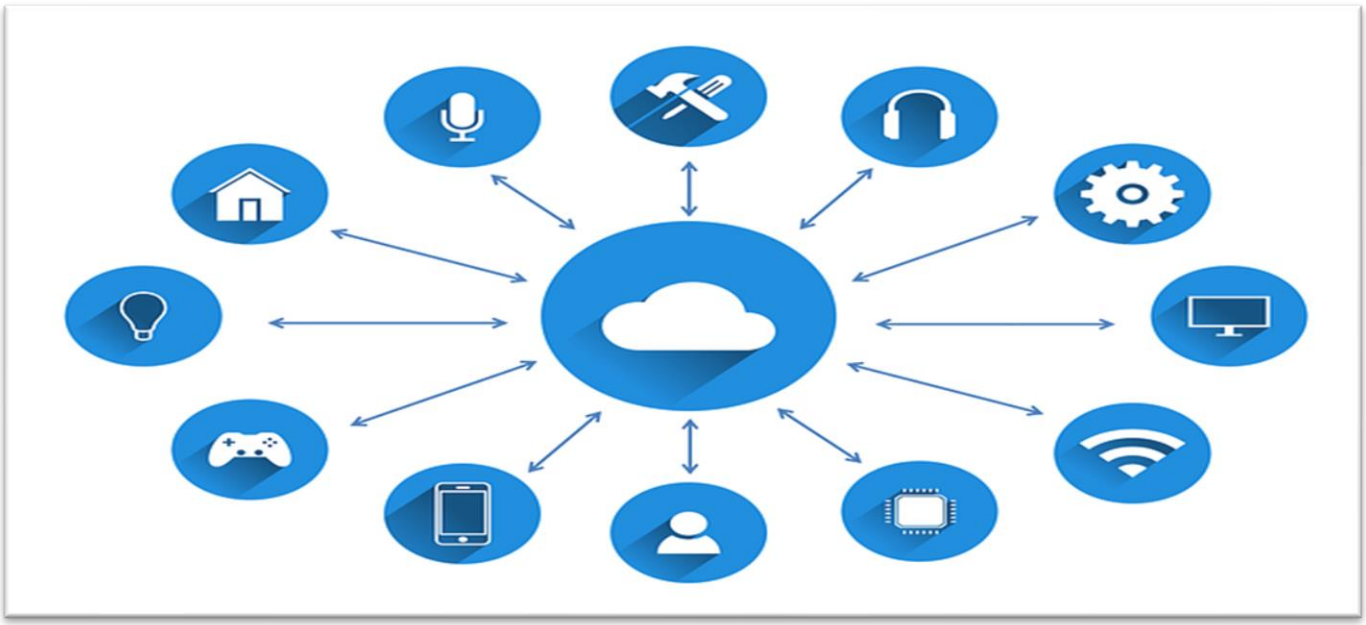
1. Abdelrahman Nasser Fathi
2. Alaa Mamdouh Wanis
3. Engy Hussein Helmy
4. Abdallah Mahmoud Saber
5. Mahmoud Khaled Mohamed
6. Mohamed Essam Elbastawisy
7. Fedaa Yasser

Under the supervision**: *Eng. Omar Hussien***

Contents

Overview of Cloud Computing

Cloud computing refers to the delivery of computing services over the internet, allowing users to access and store data on remote servers instead of local machines. This model provides flexibility, scalability, and cost savings, making it essential in modern IT environments.



1.Types of Services:

Cloud computing typically offers three main service models:

- **Infrastructure as a Service (IaaS):** Provides virtualized computing resources over the internet, allowing users to manage infrastructure without physical hardware.
- **Platform as a Service (PaaS):** Offers a platform that allows developers to build, deploy, and manage applications without worrying about the underlying infrastructure.
- **Software as a Service (SaaS):** Delivers software applications over the internet on a subscription basis, enabling users to access software without installing it locally.

2.Cloud Models:

1. **Public Cloud:**
   - Operated by third-party providers like AWS, Microsoft Azure, or Google Cloud.
   - Resources are shared across multiple users (tenants).
   - Users only pay for the services they use, making it cost-effective.
   - Ideal for businesses with fluctuating workloads.
2. **Private Cloud:**
   - Resources are dedicated to a single organization.
   - Offers greater control over data and security but comes with higher costs since the organization owns and manages the infrastructure.
   - Best for businesses with strict regulatory or security requirements.
3. **Hybrid Cloud:**
   - Combines both public and private clouds, allowing data and applications to be shared between them.
   - Offers flexibility by enabling workloads to move between private and public clouds as needed.
   - Useful for businesses with variable workloads or sensitive data that must stay on-promise

3.Benefits of Cloud Computing:

1. Cost Savings:

- Eliminates the capital expense of buying hardware and software.
- Reduces costs associated with IT management and maintenance.

2. Scalability:

- Easily scale resources up or down based on demand, paying only for what you use.

3. Flexibility:

- Cloud services can be accessed from anywhere with an internet connection, promoting remote work and business continuity.

4. Disaster Recovery:

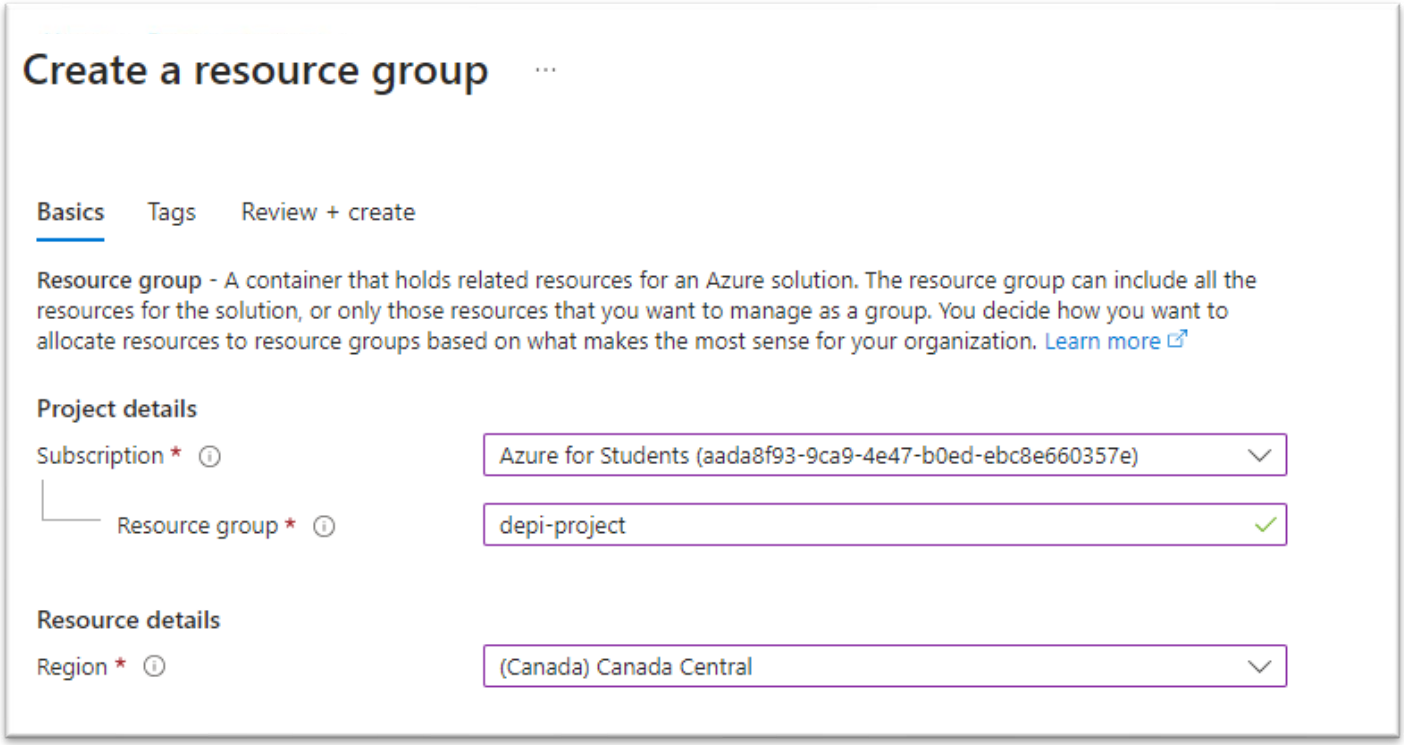
- Built-in disaster recovery options and data backups reduce downtime and protect against data loss.

Week 1

Azure Fundamentals & Setup

Steps to Create Azure Subscription:

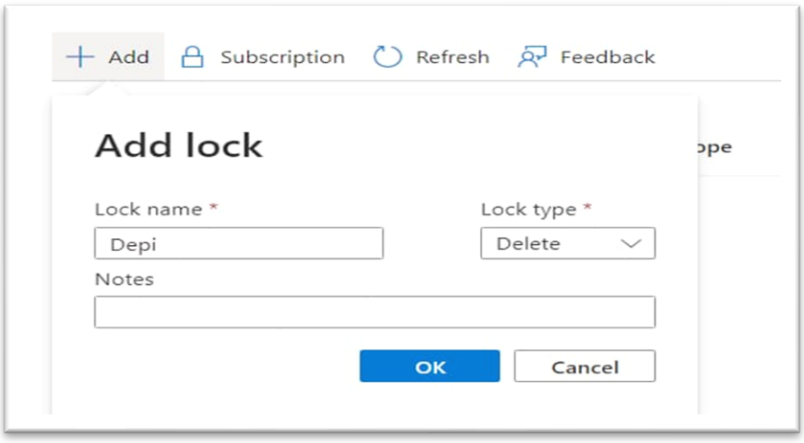
1. Navigate to the Azure Portal.
2. Select the subscription type that fits your needs.
3. Create a Resource Group to organize your resources.
4. Chose the RG Name and Region



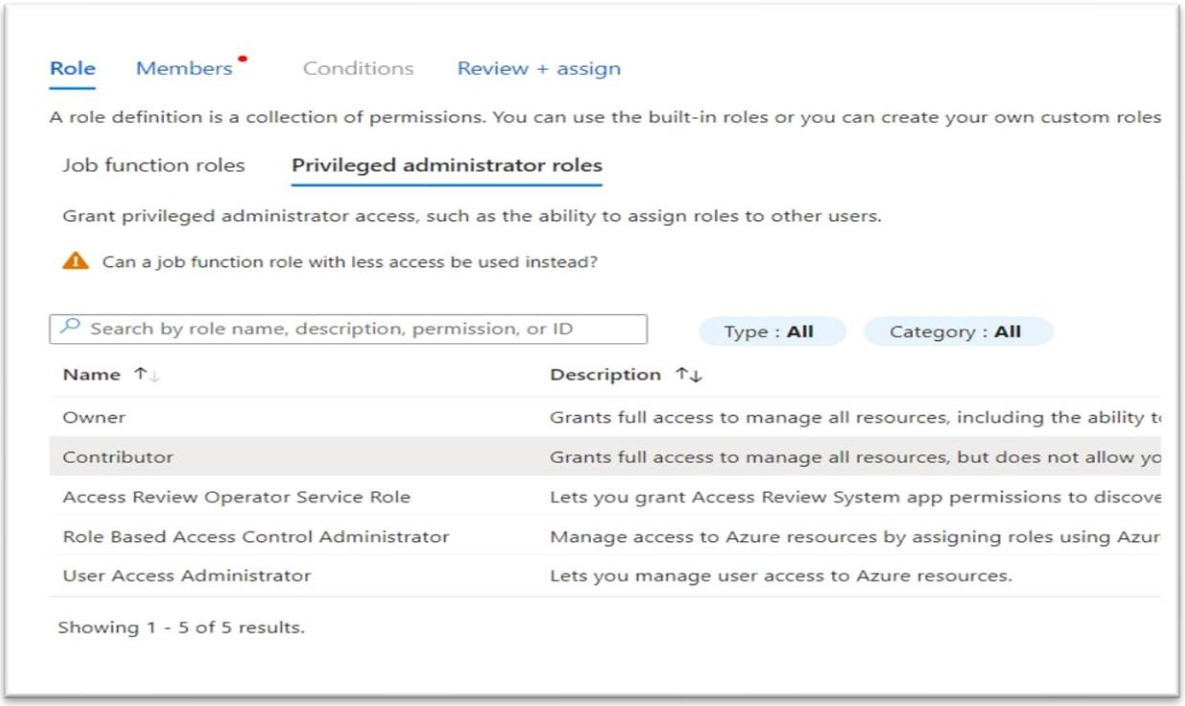
5. Add lock

   Fill in Lock Details:

   - Lock Name - Lock Type:

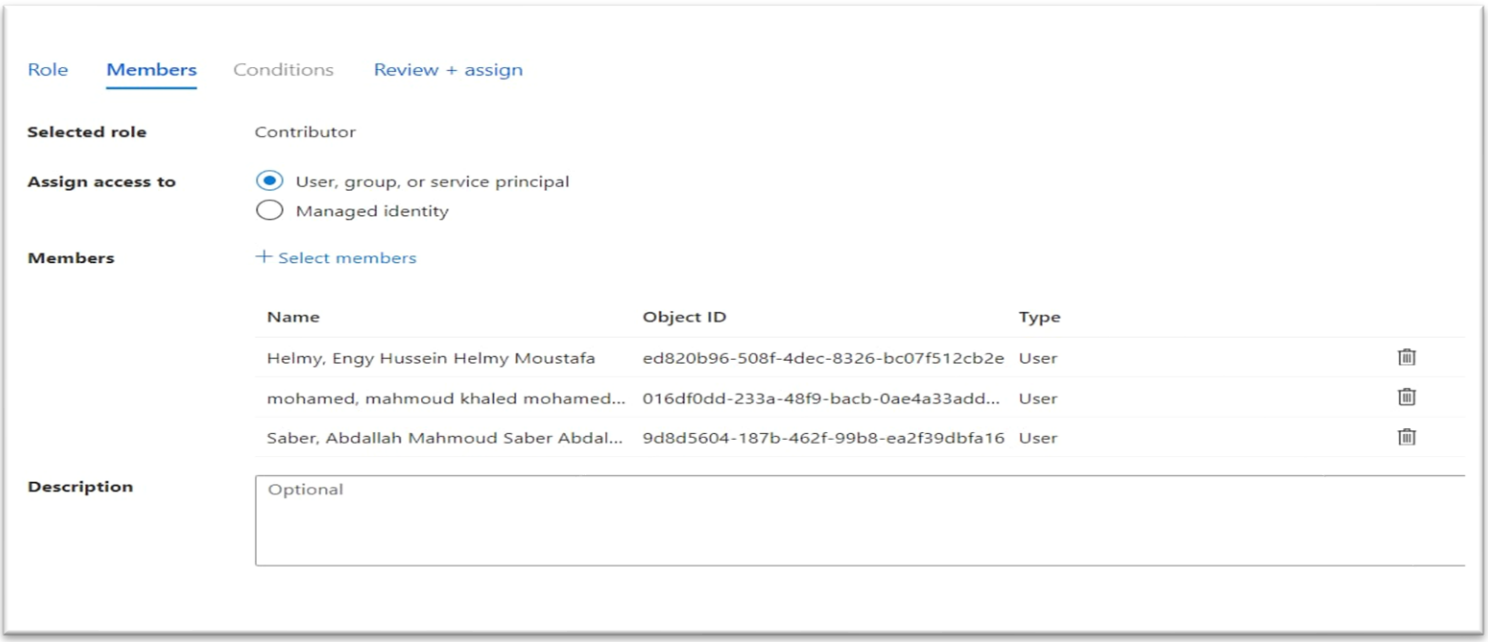


6. Select a Role:



7. Assign Access to:

- all accounts of team members



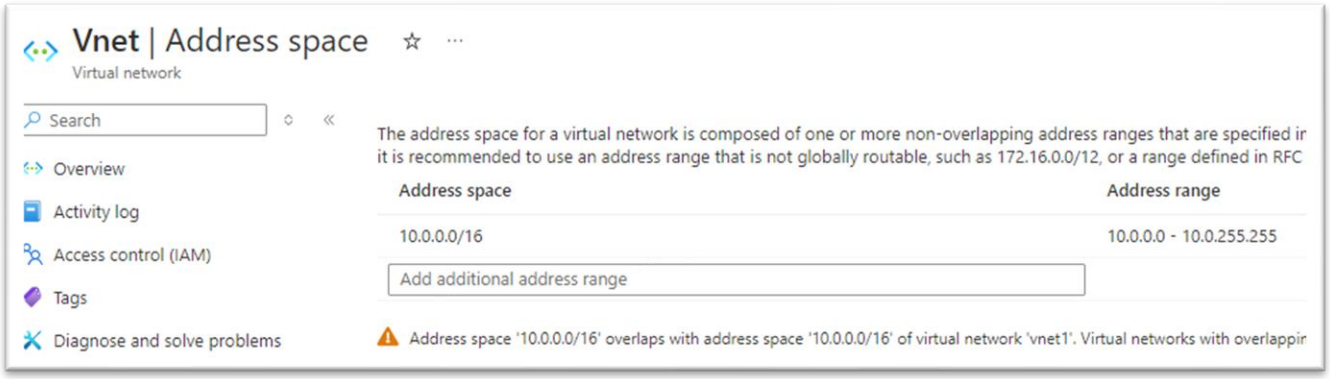
Week 2

Deploy and Manage Azure Resources

Implement Network Settings:

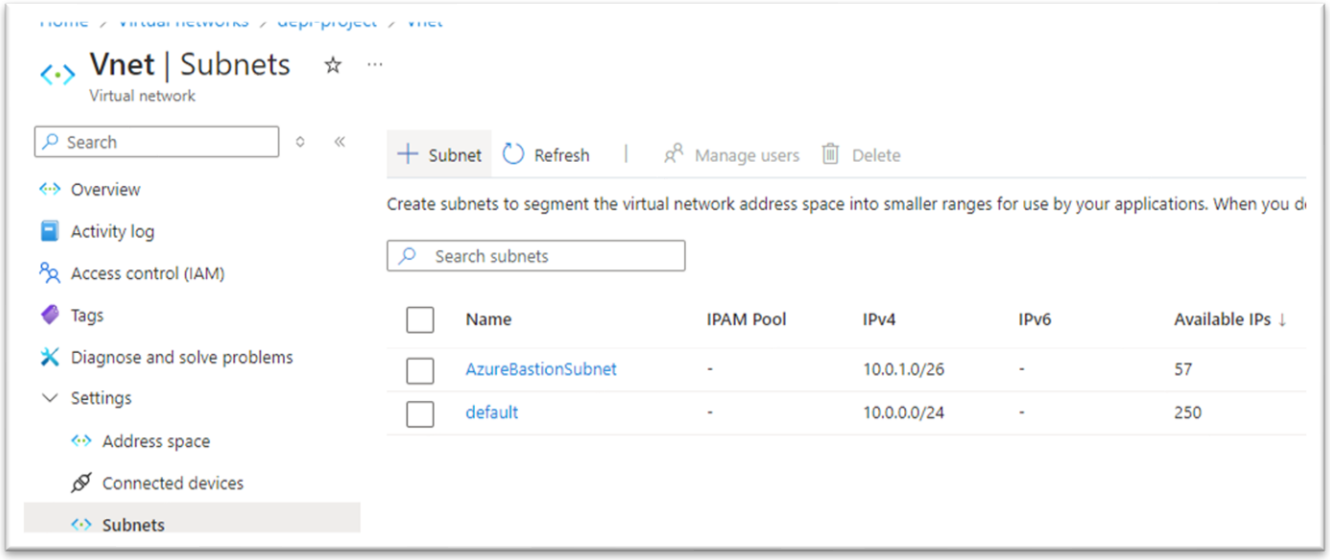
1. Azure Virtual Network (VNet)

- **Purpose**: Azure Virtual Network (VNet) provides a secure and isolated environment to host your virtual machines and other Azure resources.
- Key Features:
  - Isolation: VNets are isolated from each other and can be used to create separate networks for different workloads.
  - Subnets: VNets can be divided into smaller subnets for better organization and security.
  - Network Security Groups (NSGs): Used to control inbound and outbound traffic at the subnet or NIC level by defining security rules.
  - Peering (Not configured): VNet peering allows communication between VNets across different regions.



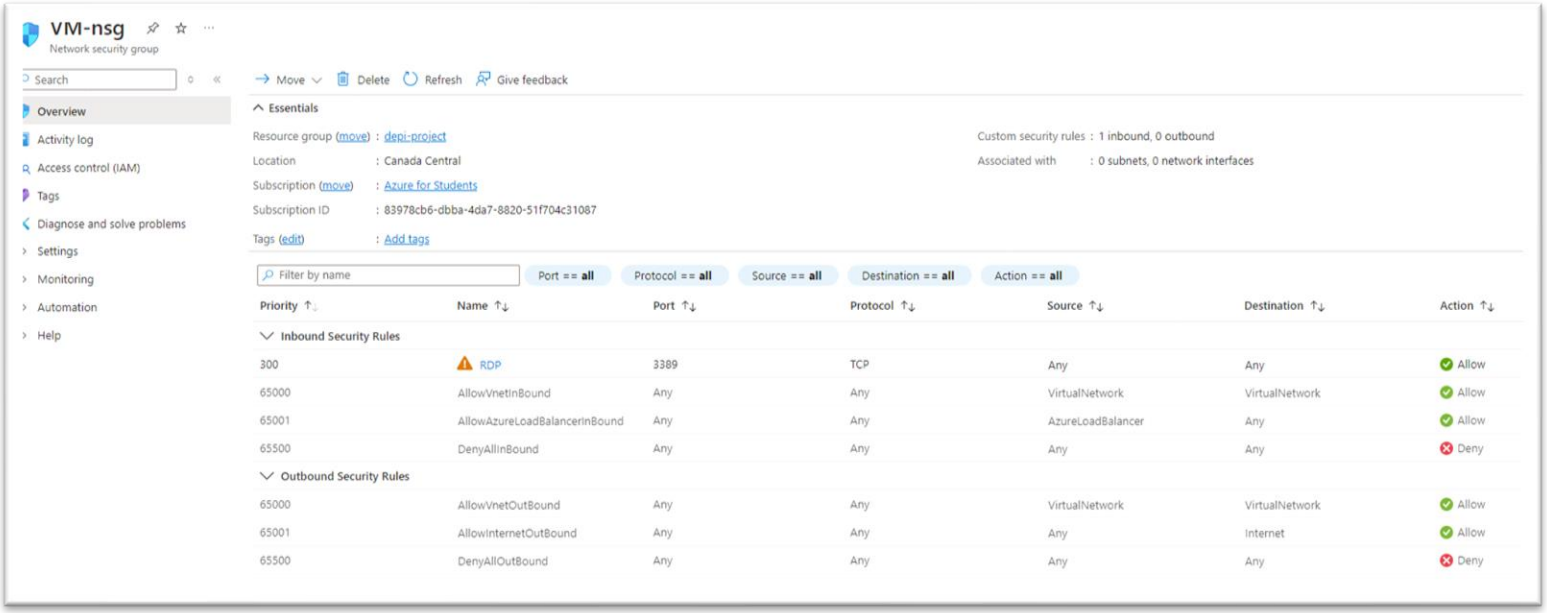
2.Subnets

- **Purpose:** VNets can be divided into smaller subnetworks, or subnets, for better organization and security.
- **Features**:
  - Logical segmentation within a VNet.
  - Each subnet can have its own security rules and Network Security Groups (NSGs).



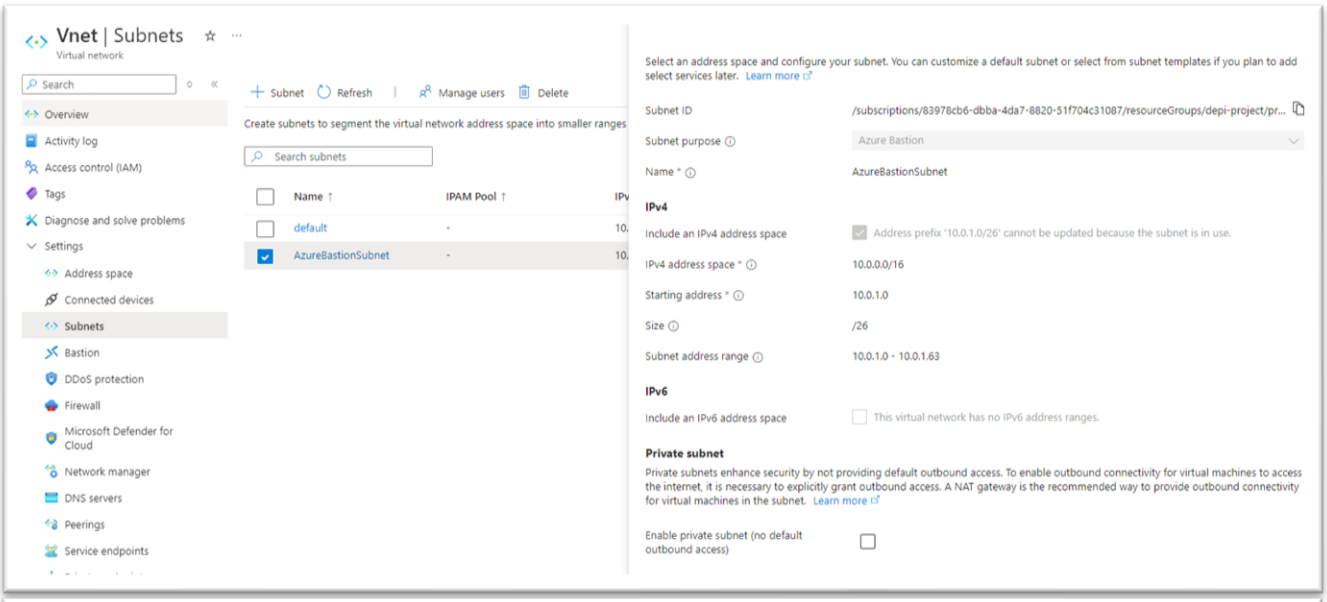
3. Network Security Groups (NSGs)

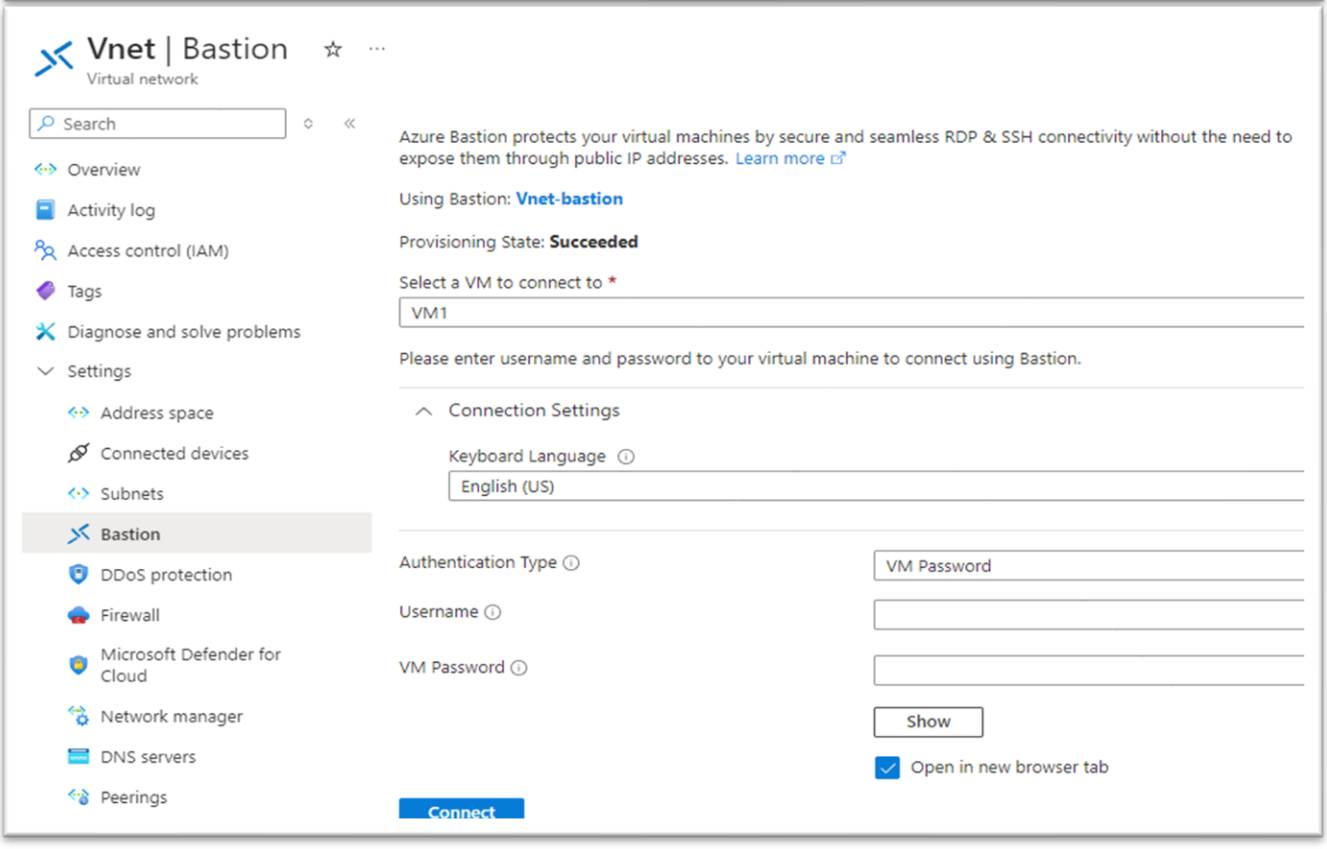
- **Purpose**: Provides a set of firewall rules to control inbound and outbound traffic for network interfaces (NICs), VMs, and subnets.
- **Key Features**:
  - Can be applied at both subnet and NIC levels.
  - Defines **allow/deny** rules based on IP addresses, protocols, and ports.



4. Azure Bastion

- **Purpose**: Provides secure and seamless RDP/SSH access to VMs without exposing them to the public internet.
- **Key Features**:
  - Eliminates the need for a public IP address on VMs.
  - Managed service that secures remote access.





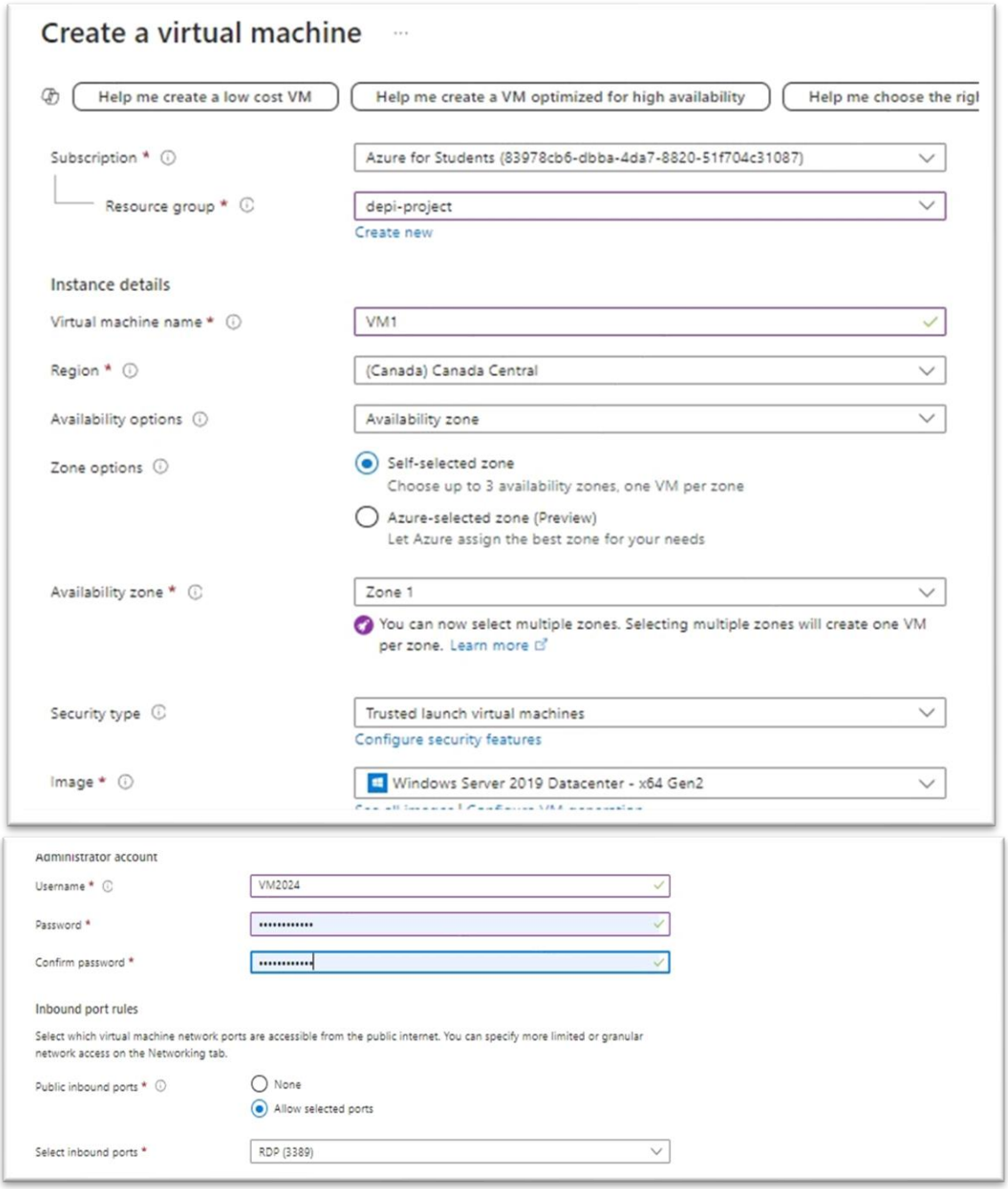
VM Deployment

Process Overview:

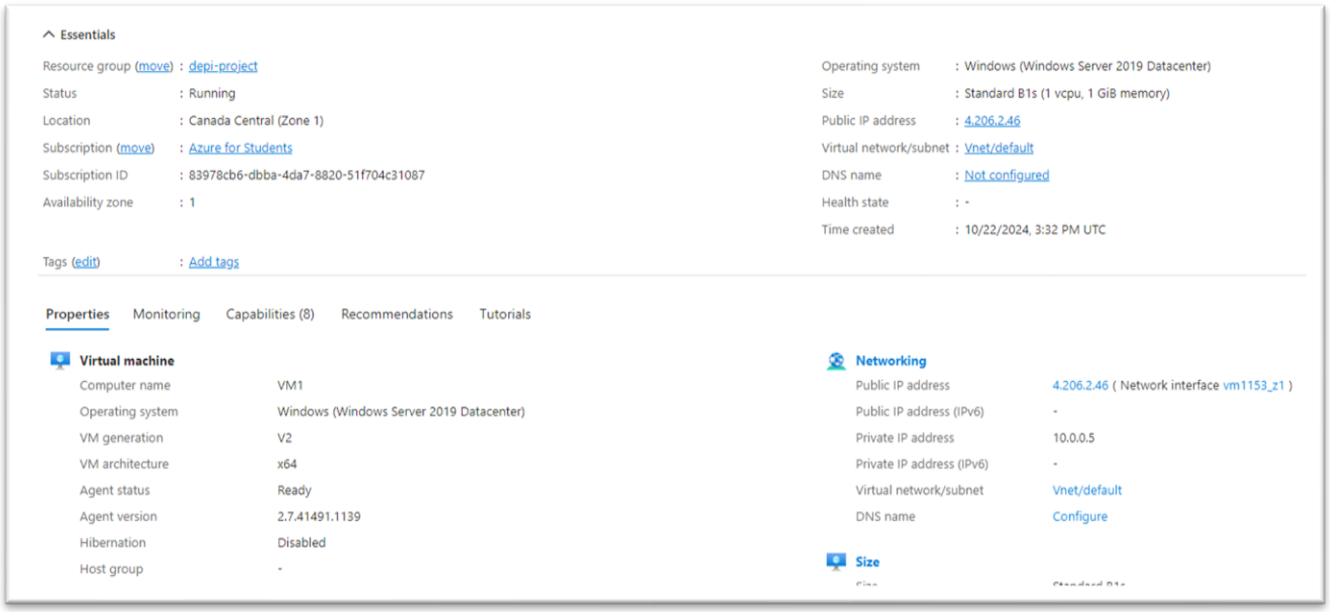
Steps for deploying VMs include selecting the VM size, configuring the operating system, and setting up security features.

Key configurations applied involve networking settings and storage options.

1. the setup for creating a virtual machine in Microsoft Azure



2. details of a virtual machine in Microsoft Azure that is running.



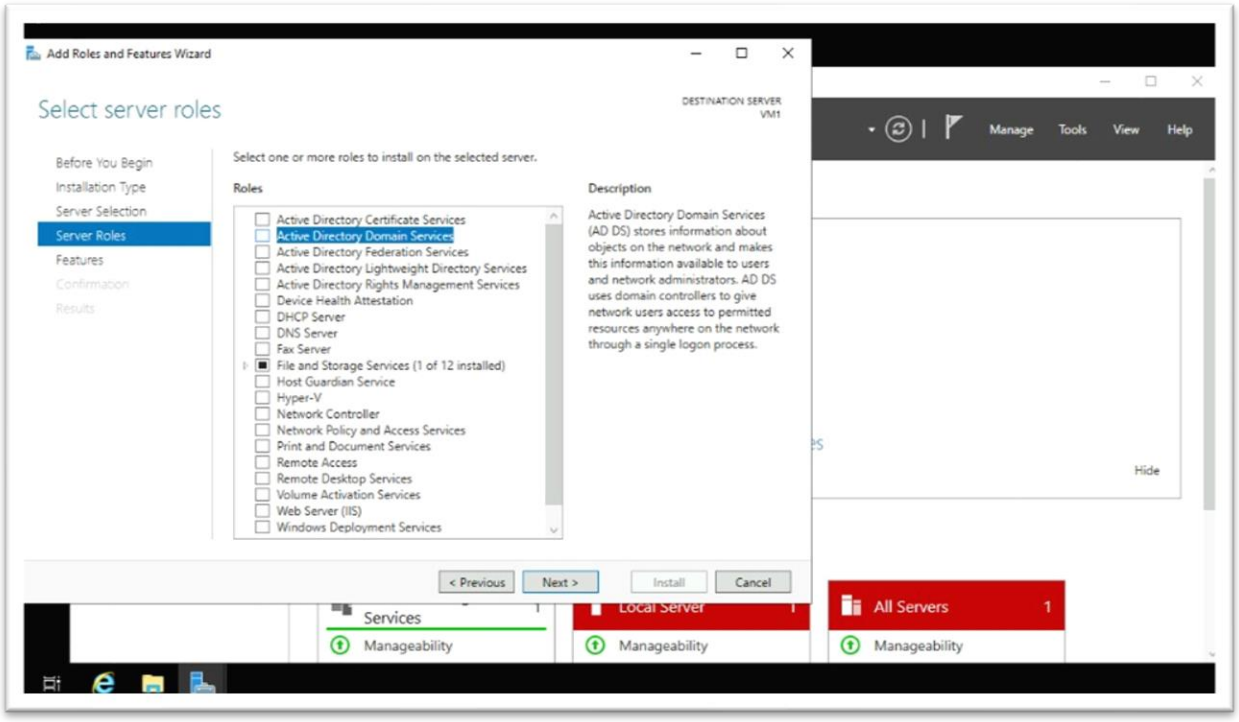
Azure AD Configuration:

- Azure Active Directory manages user identities and access to resources.

Steps:

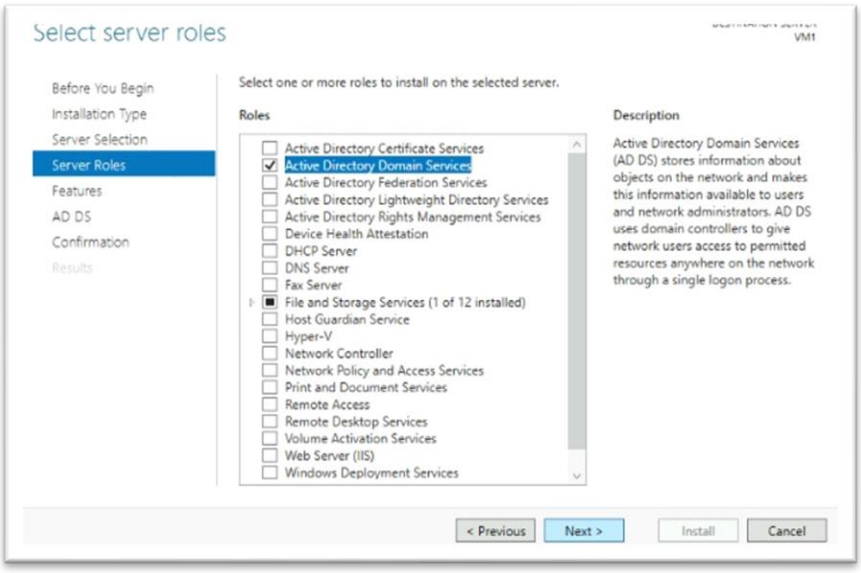
1. Add Roles: Click on Azure Active Directory Domain Services (ADDS):

- Navigate to the VM and open the Server Manager.
- Select “Add Roles and Features” to begin the role installation process.
- Choose the role “Active Directory Domain Services (ADDS)” and proceed.

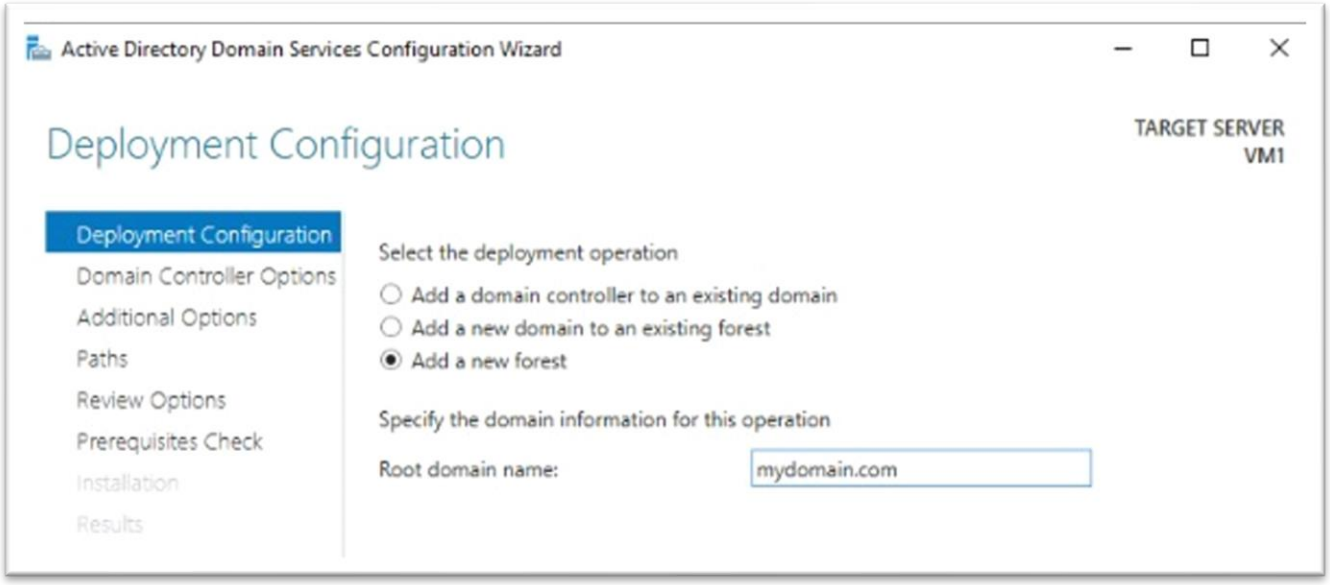


2. Install ADDS

- Follow the prompts to install the ADDS role on your VM.

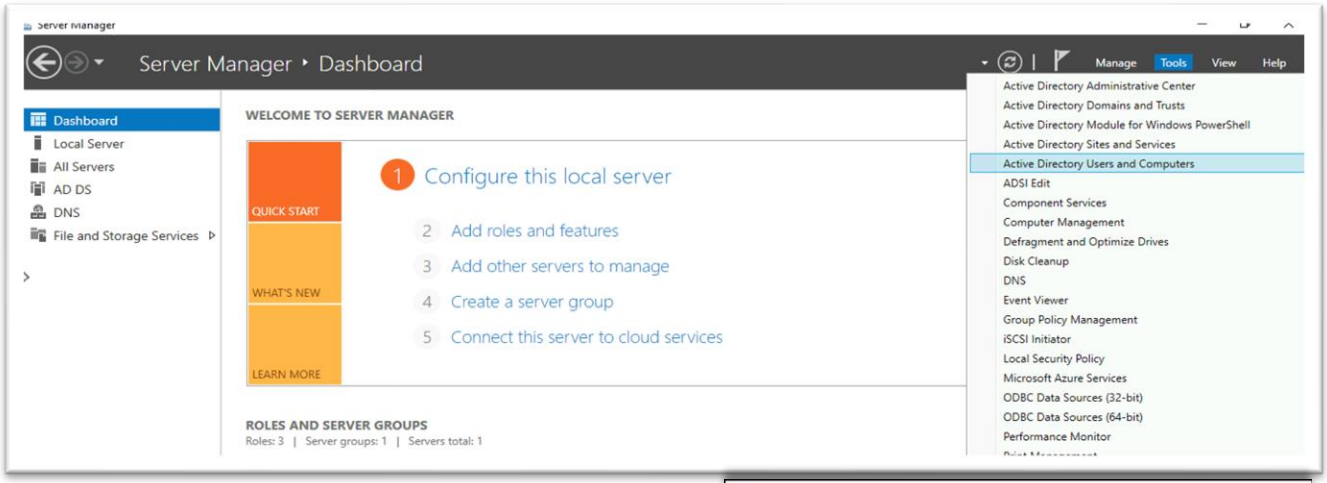


- Deploy forest and finish ADDS configurations

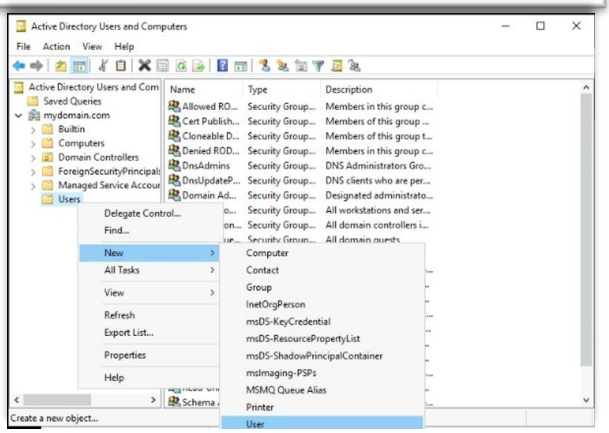


3. Access Active Directory Users and Computers:

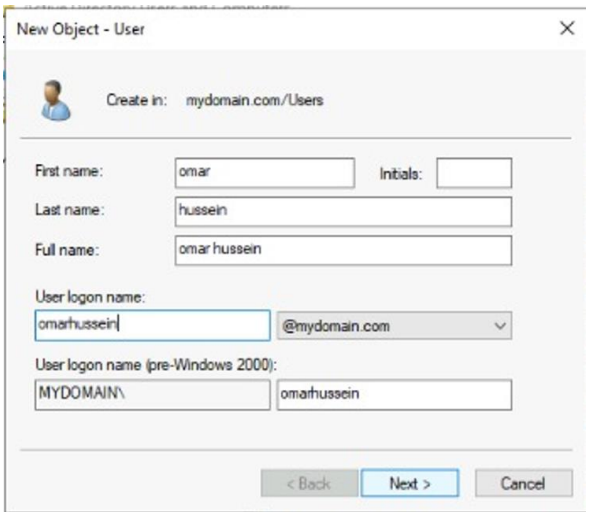
- Click on “Tools” at the top-right corner of the Server Manager.
- Select “Active Directory Users and Computers” from the dropdown menu.



- Create New Users
- Within the “Users” organizational unit, right-click on “New”.

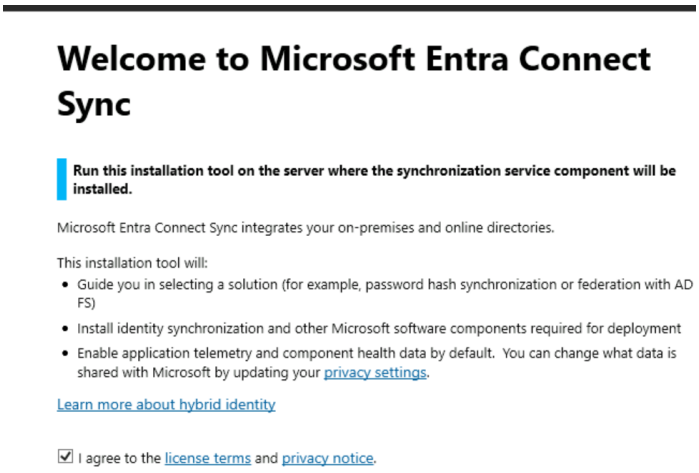


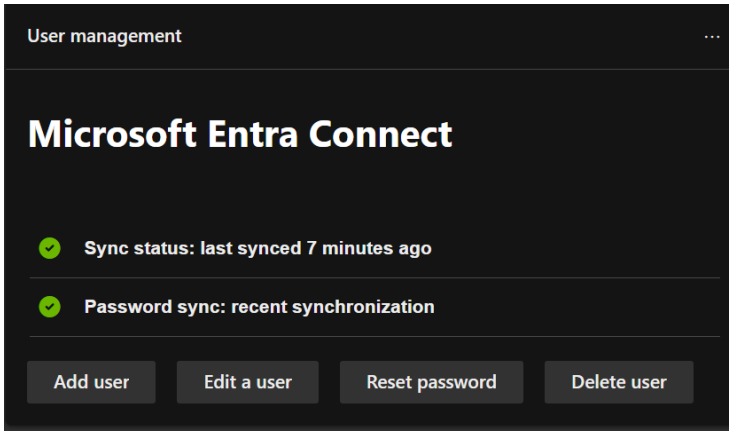
- Select New -> User, and fill in the required details (name and password) to create a new user.



Azure Sync

sync with Entra ID using Entra AD connect “We cannot complete this as we are a normal users not Global admin of the tenant”





Conclusion

By following these steps, you’ve successfully created a Windows VM, configured it as a domain controller, and managed users within Azure Active Directory

Week 3

Implement Storage Solutions

Types of Storage Accounts:

- **General-purpose:** Supports all storage types.
- **Blob storage:** Optimized for storing large amounts of unstructured data.
- **File storage:** Managed file shares for cloud or on-premises deployments.

Purpose:

- The Azure Storage Account is utilized for DEPI project

Blob Storage Configuration:

- Steps taken to configure Blob Storage include defining access tiers and setting up containers.

Storage Account Type

- Type: General-purpose v2
- Performance Tier: Standard

Resource Group

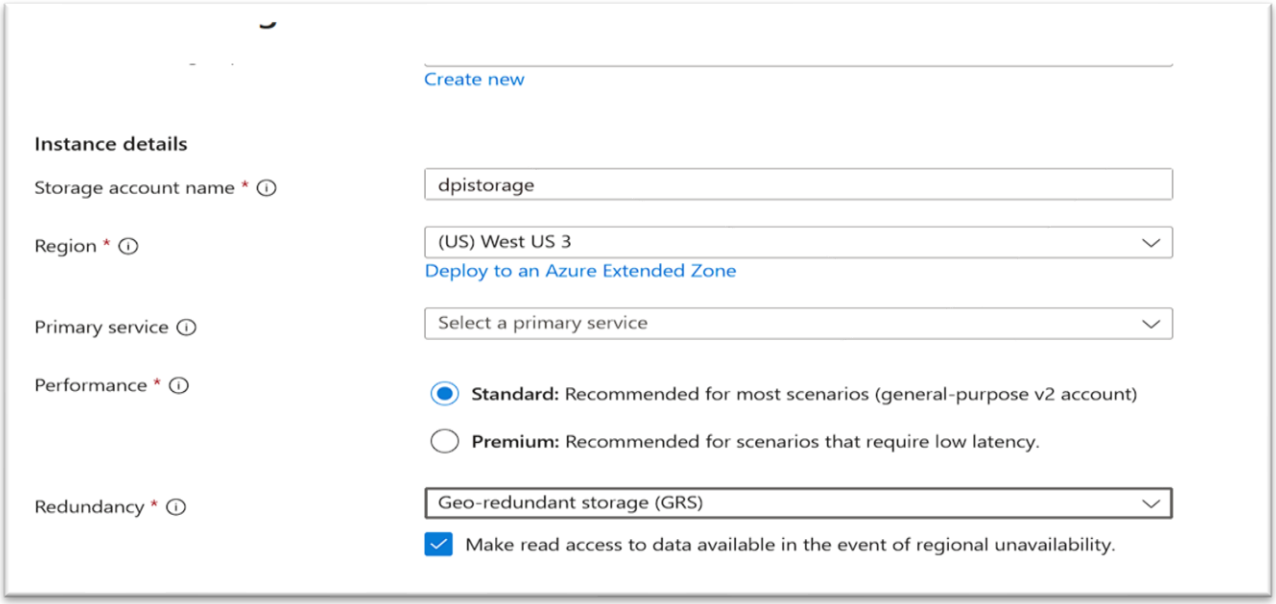
- Resource Group Name: [Depi_project]

Location

- Region: [Central Canada]

Setting	Value
Account Name	depi-project
Replication Type	LRS
Access Tier	Hot
Secure Transfer Required	Enabled

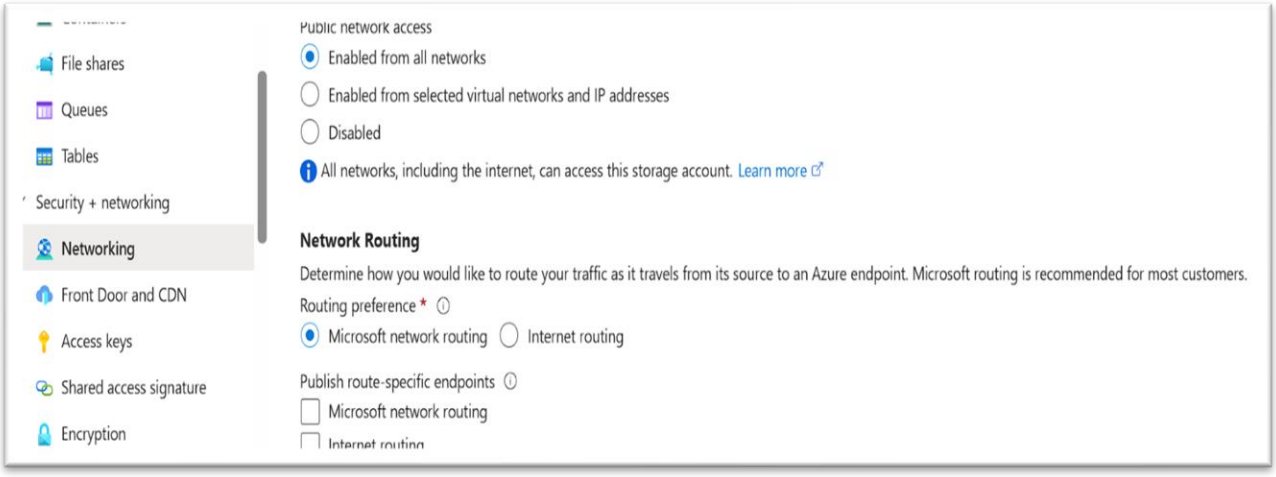
1- basic configuration



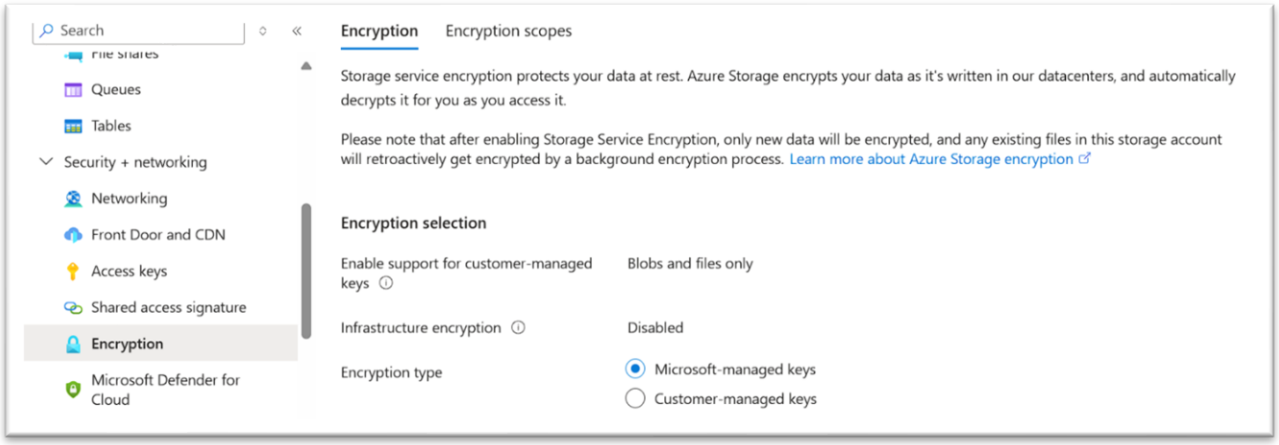
2- manage configuration after the creation of the storage account.

3- network and security configuration

- Enabled from all networks
- **You can use “Allow only access from only selected Vnets”**
- Use Microsoft network routing

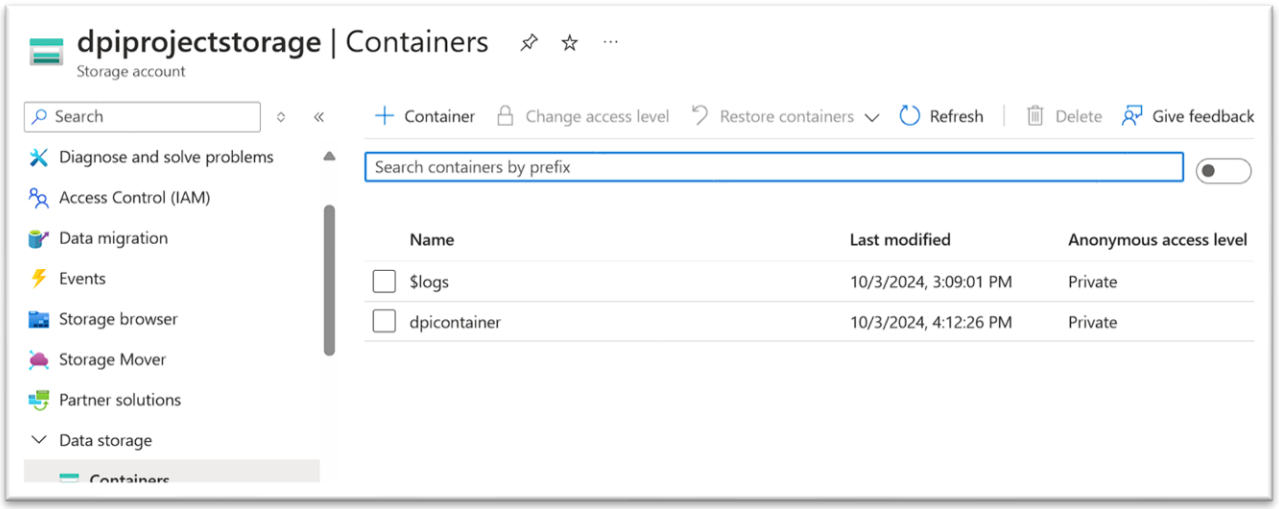


4- Use Microsoft encryption

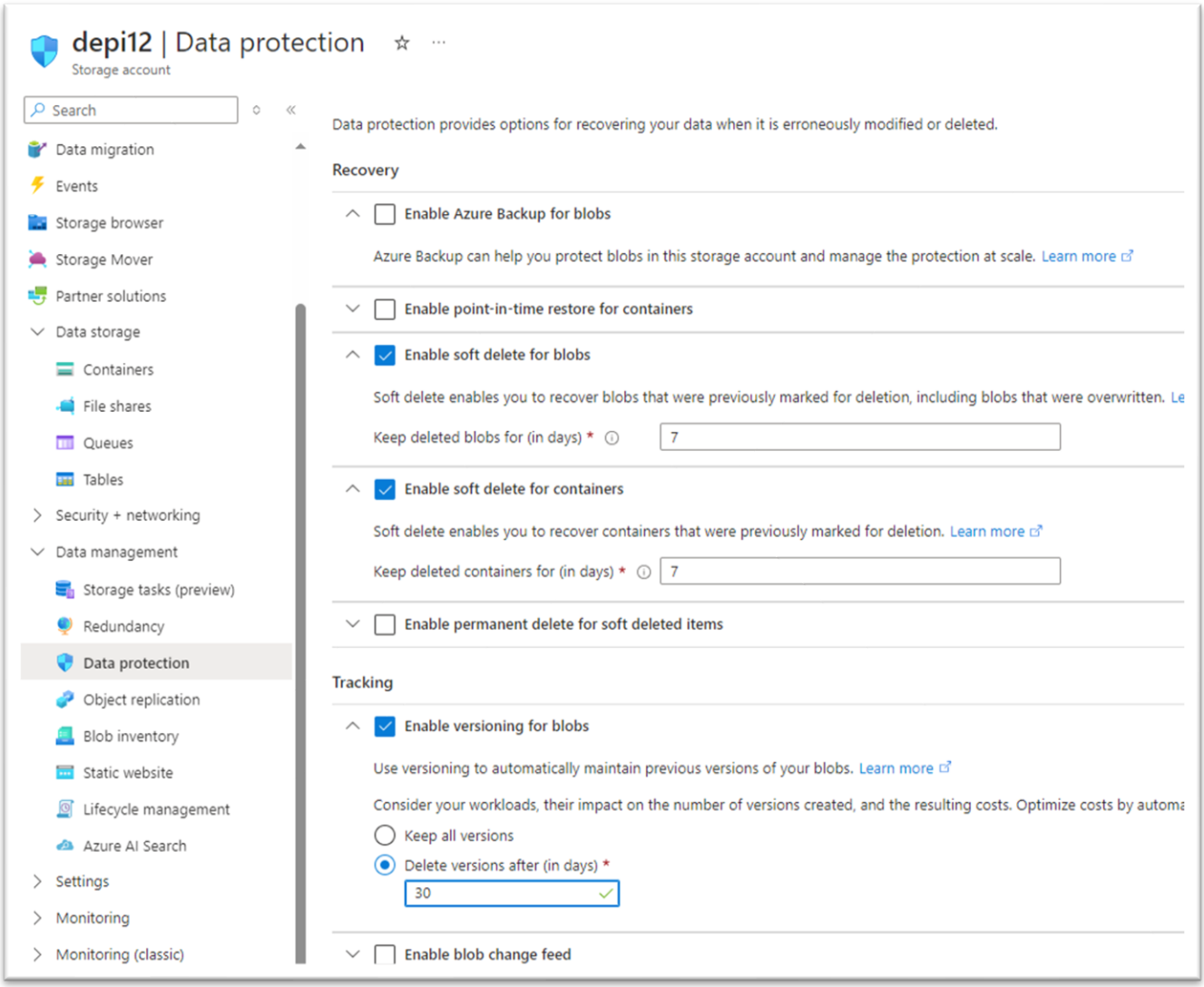


5- blob storage configuration

- crate a container called discontinuer
- allow revisioning as a way of backup



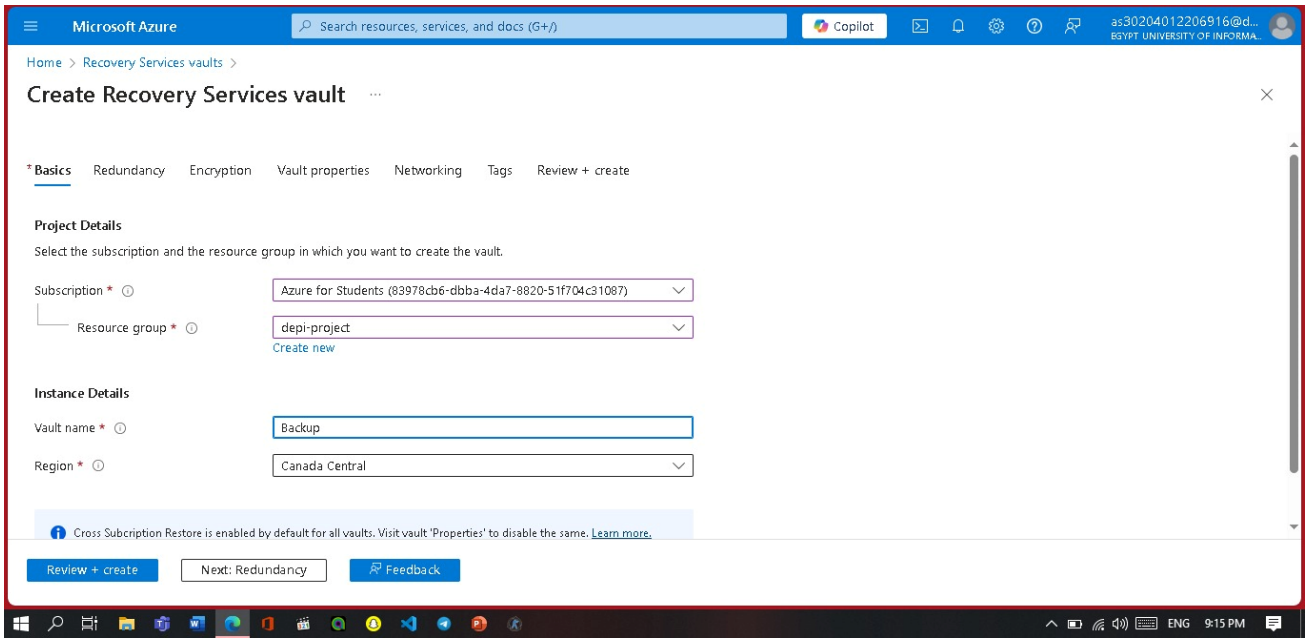
6- Version control



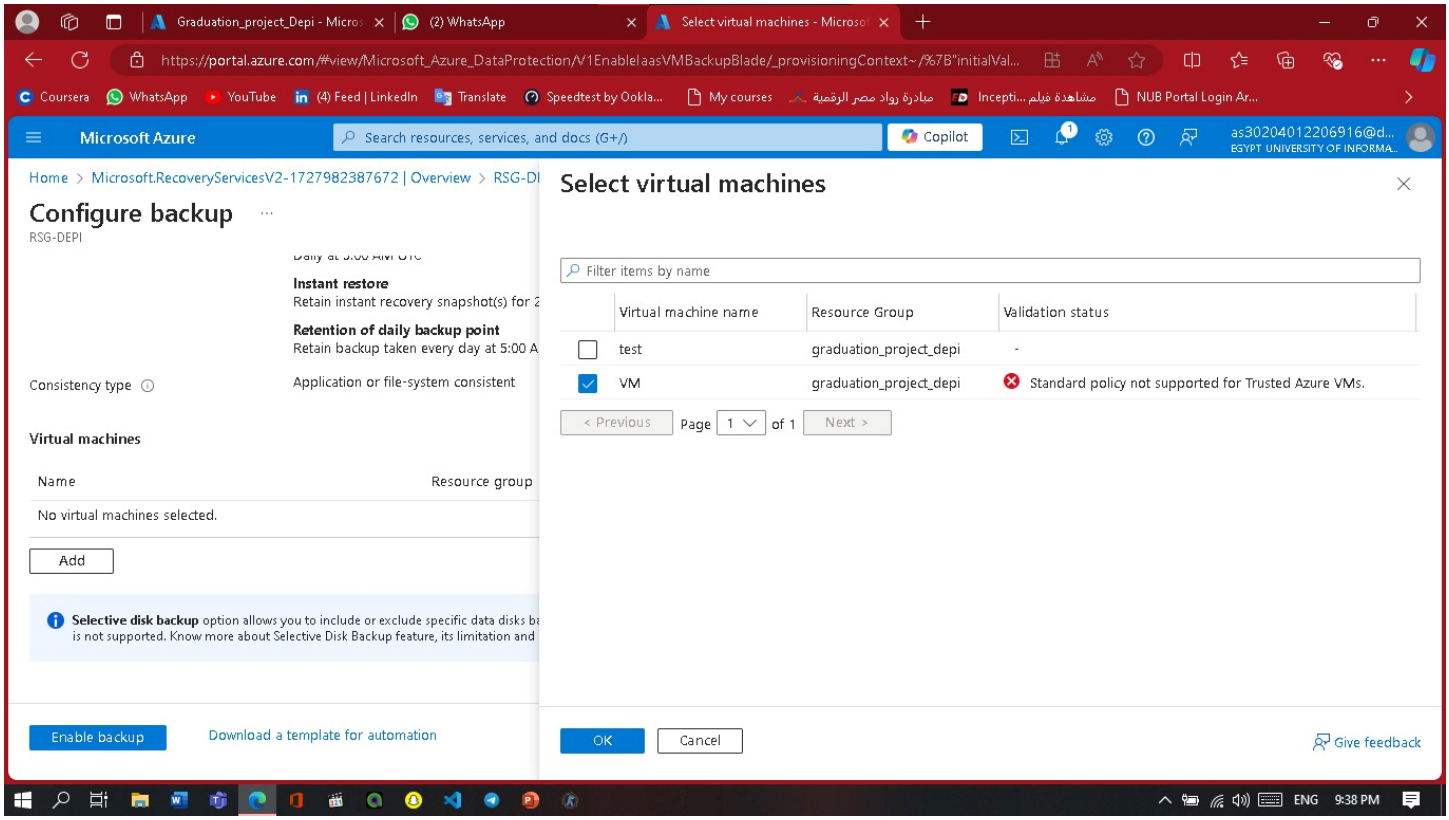
Backup Solutions

Strategy Overview:

- Implemented backup solutions for VMs using Azure Backup services.

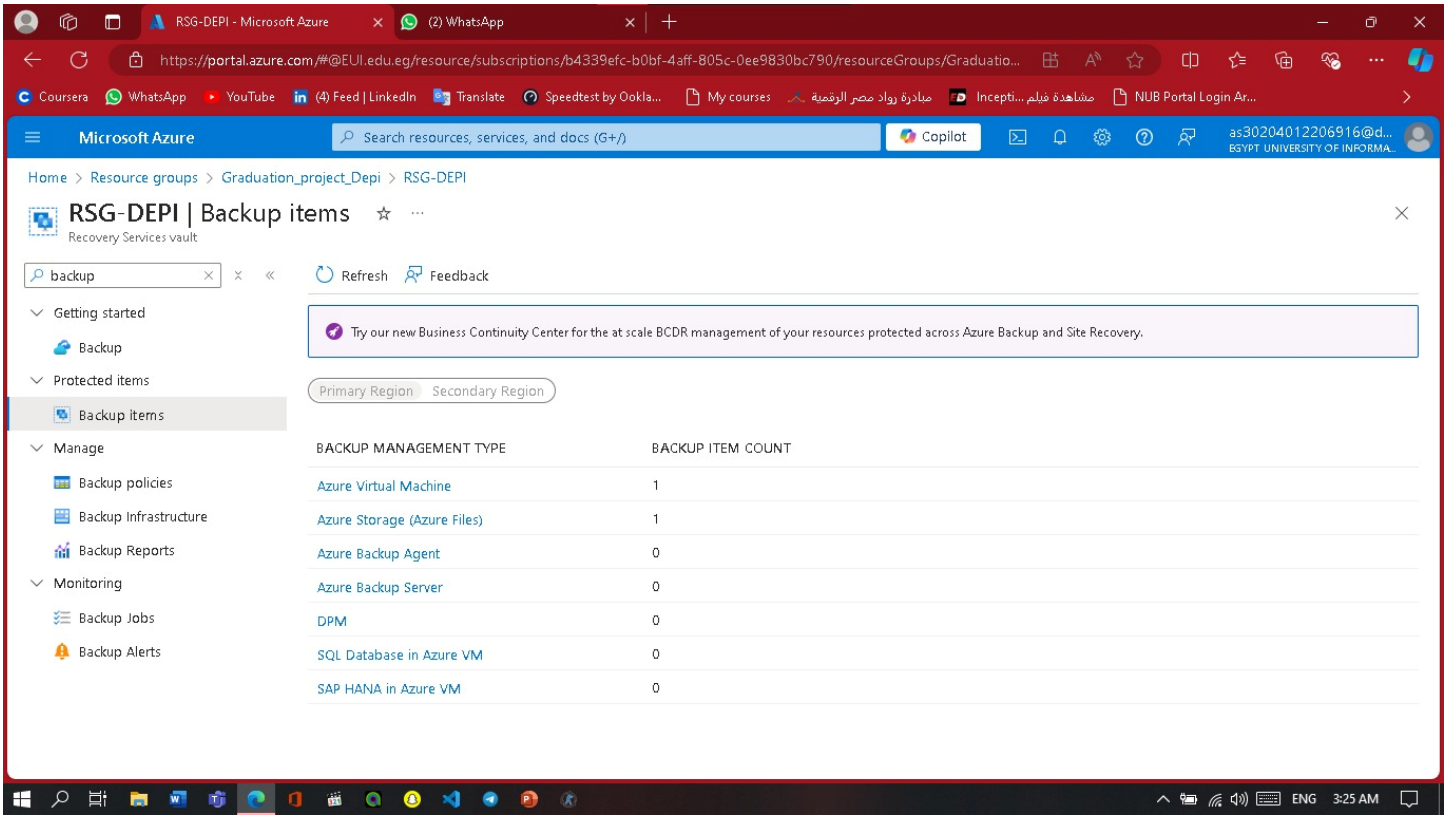


- Ensured data protection through regular backups and recovery plans.



رواد مصر الرقمية

وزارة الاتصـــــالات
وتكنولوجيا المعلومات



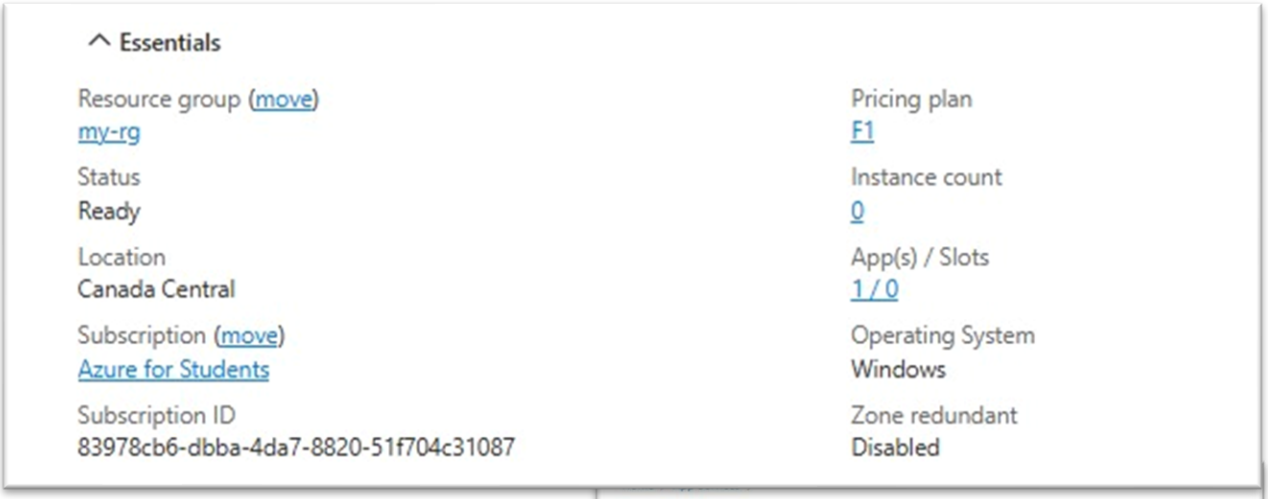
Week 4

Additional part

App Service:

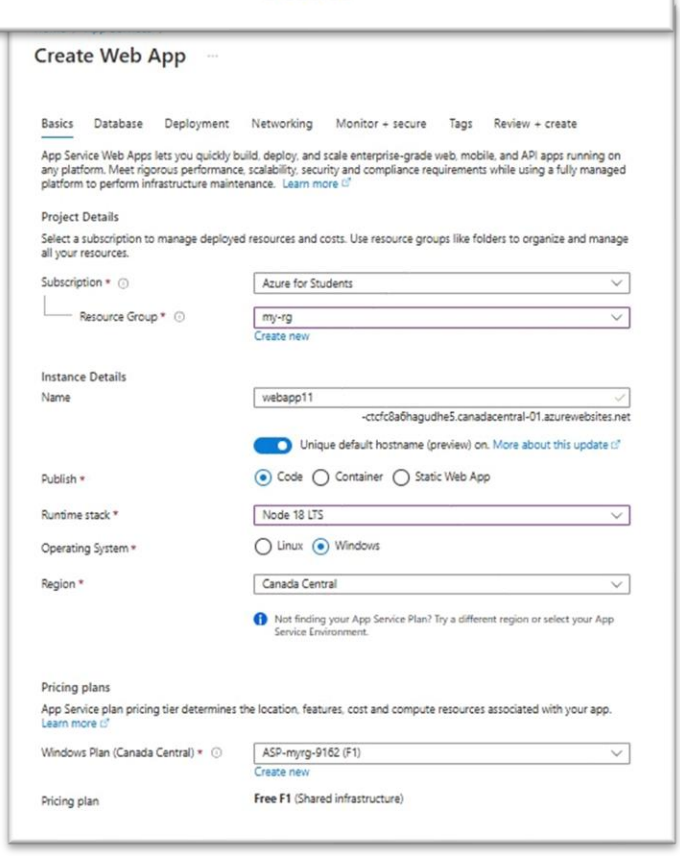
Create App service Plan:

Setting up the environment where the app will run, defines the region, number of instances, size of the instances, and pricing tier.

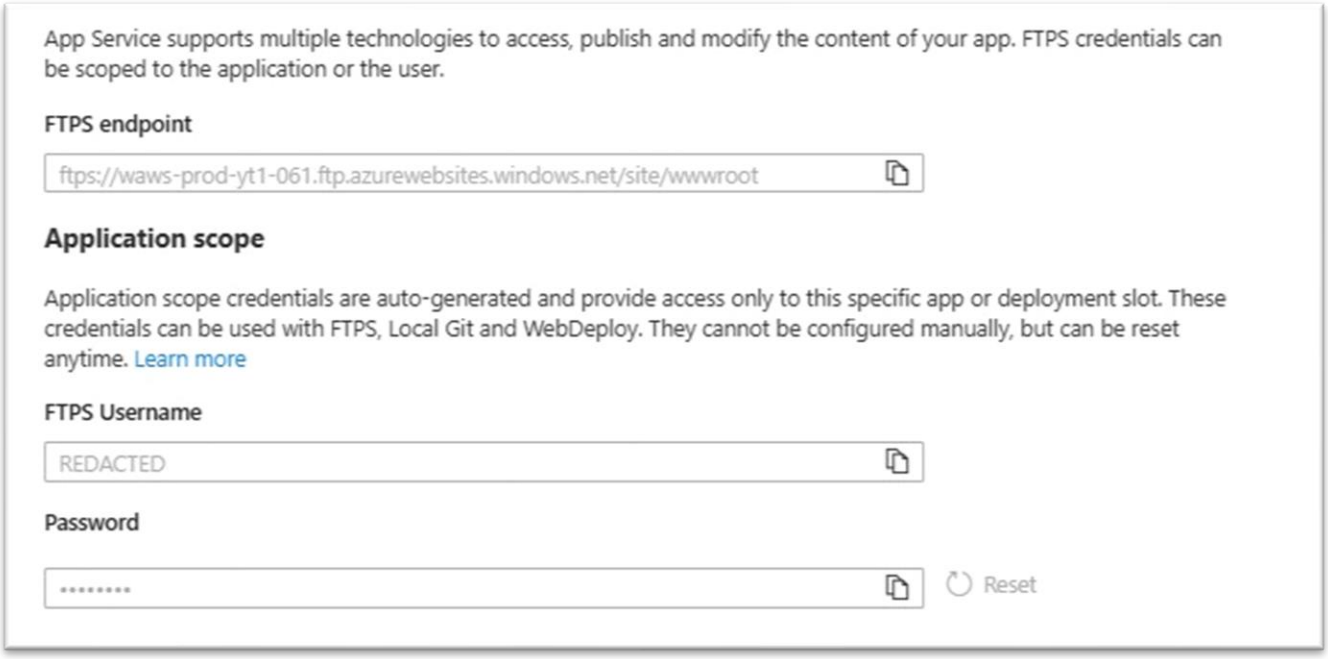


Basic Configuration:

Create App Service: fill in the details: name, runtime stack, and choose the resource group, App Service plan, and region.



Deploy and configure the application:



Network Configuration:

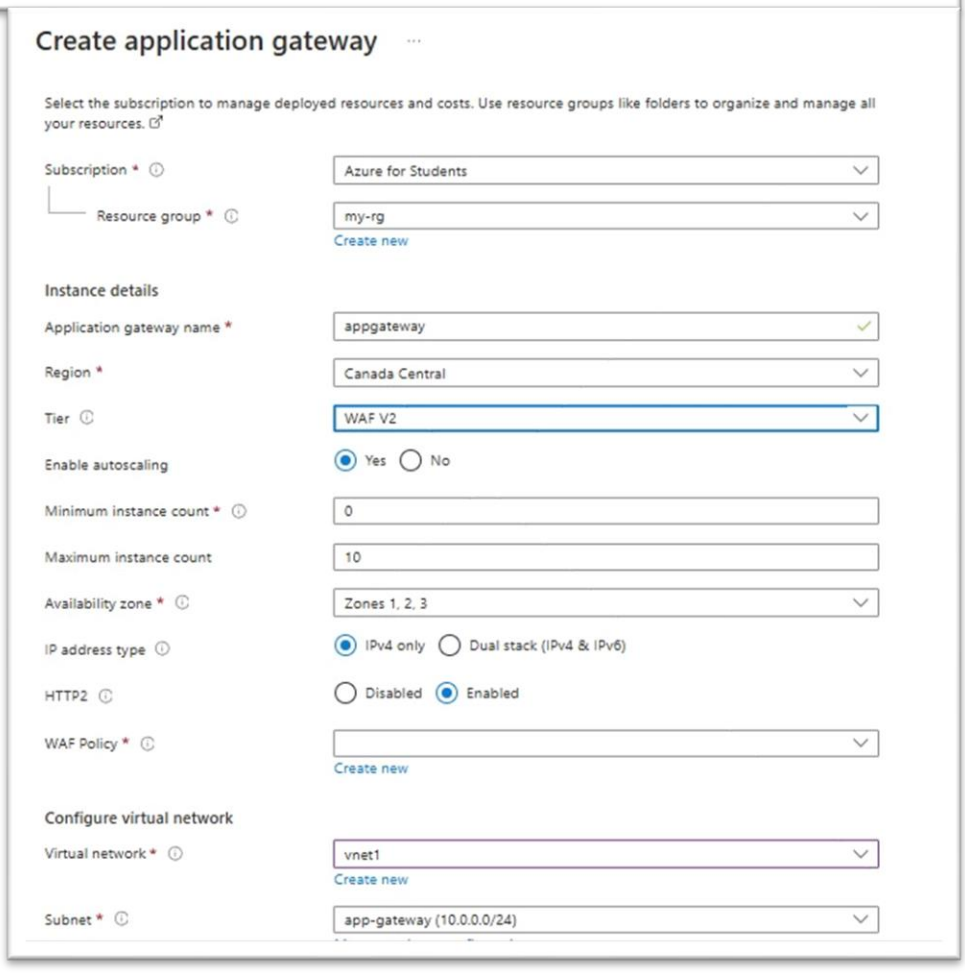
Application Gateway Configuration:

Load balancer to manage traffic to web application includes WAF.

Create Virtual Network:

To manage securely communication between App Gateway and other azure resources.

Basic configuration:



- **Configure frontend IP:**

Type	Status	Name	IP address	Associated listeners
Public	Configured	appGwPublicFrontendIpIPv4	20.220.168.192 (gateway-ip)	listener1
Private	Not configured	-	-	-

- **Configure Backend pool:**

Collection of servers to handle incoming traffic from users after it passes through the gateway depending on load balancing configuration.

Using FQDN based on DNS server.

Name	Rules associated	Targets
pool1	1	1 •••

- **Set HTTP Setting in backend setting:**

To provide communication between application gateway and backend.

Name	Port	Protocol	Cookie based affinity	Custom probe
setting-1	80	Http	Disabled	probe1

- **Configure Routing Rules:**

Define which port can app gateway listen (port 80) to incoming traffic and direct this traffic to backend pool based on URL.

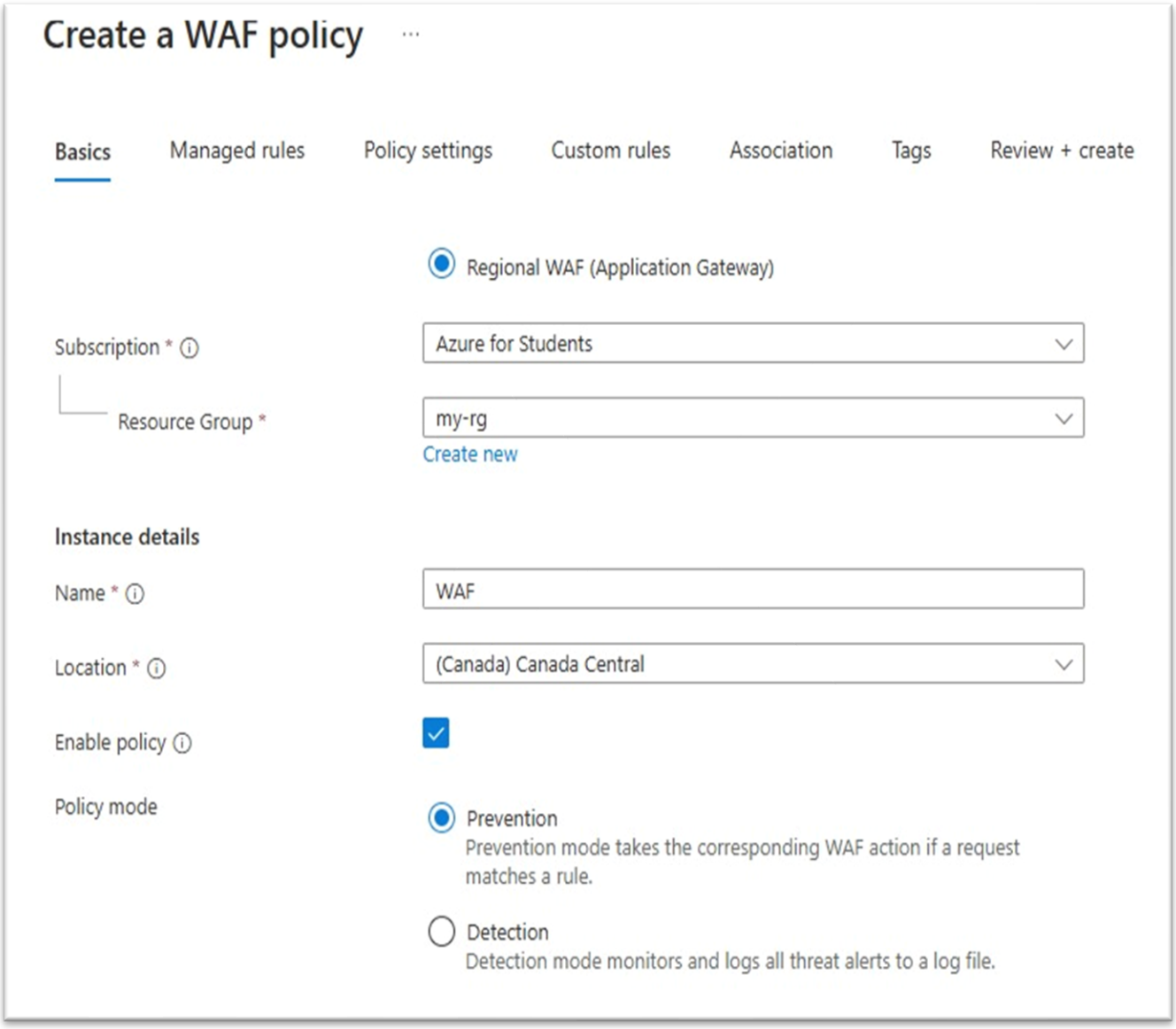
Name	Port	Protocol	Frontend IP	Associated rule	Host name
listener1	80	HTTP	Public IPv4	rool1	> -

Enable WAF and Configure Policy:

Basic configuration:

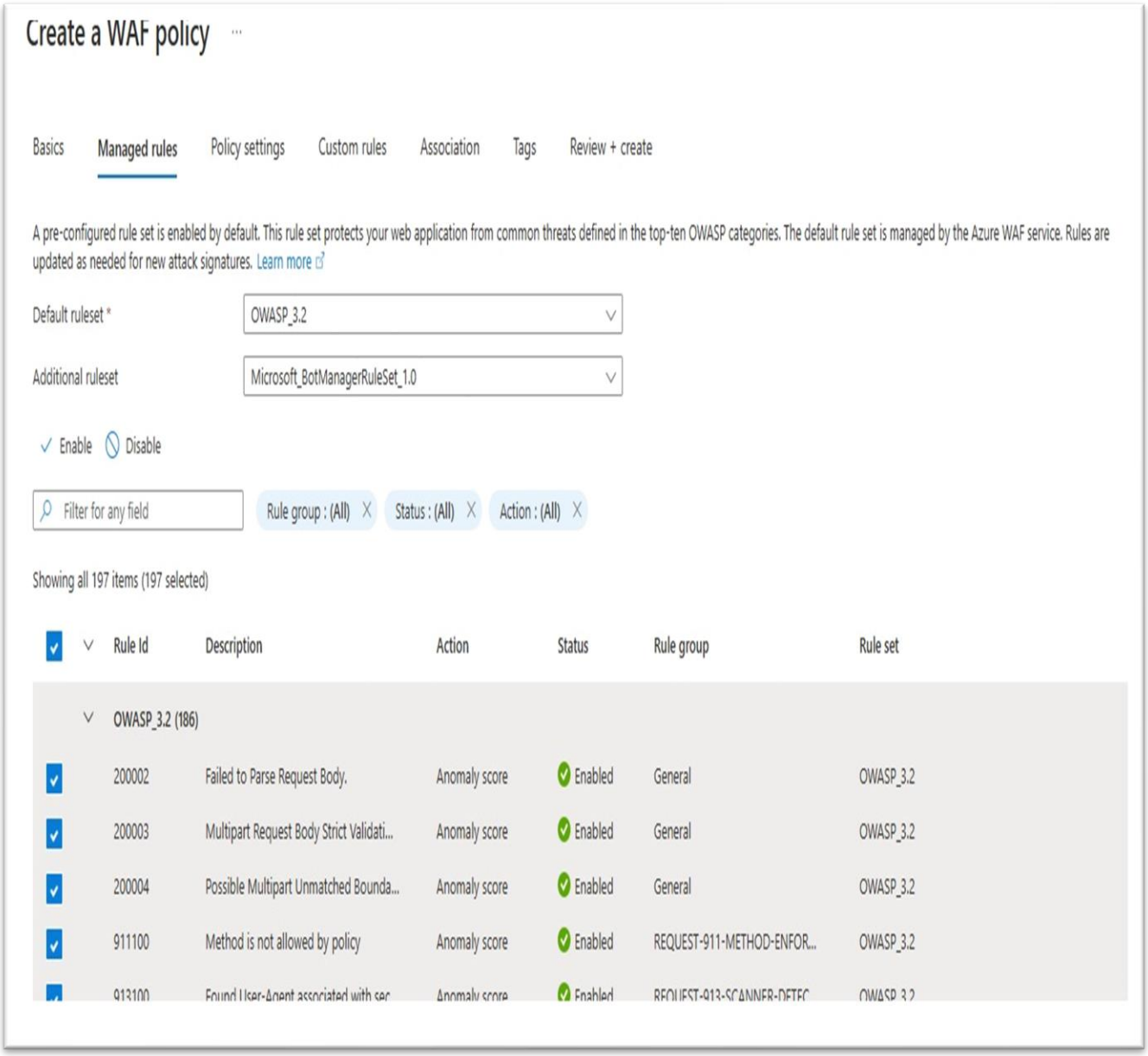
Azure WAF operates in two modes:

- Detection Mode: Monitors and logs all threats but does not block any traffic. (Recommended)
- Prevention Mode: Actively blocks requests that match WAF rules and logs the events.

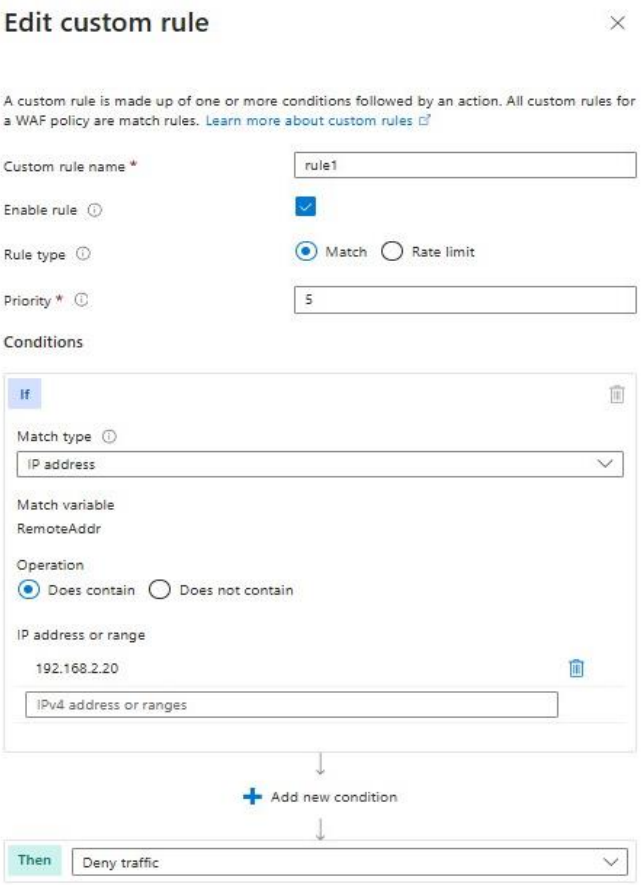


Rule Sets:

Azure WAF uses OWASP core rules: it automatically provides protection against common attacks.



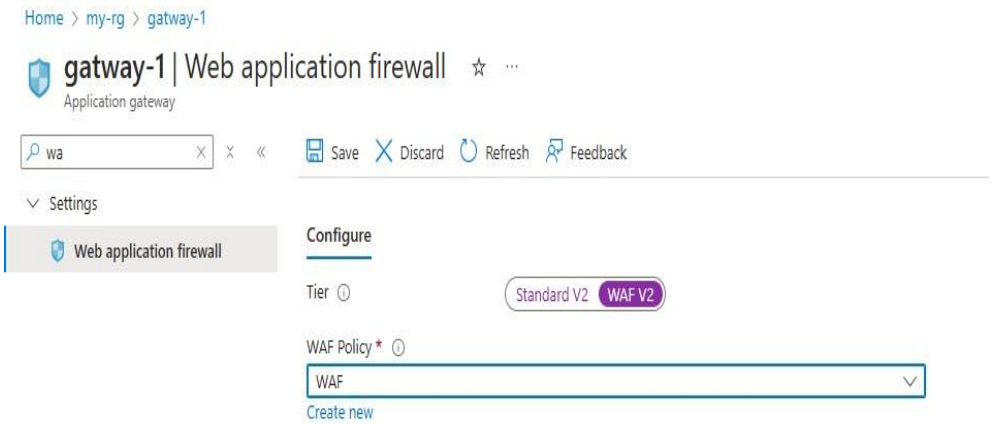
Custom Rules: You can create your own custom rules to meet specific security needs.



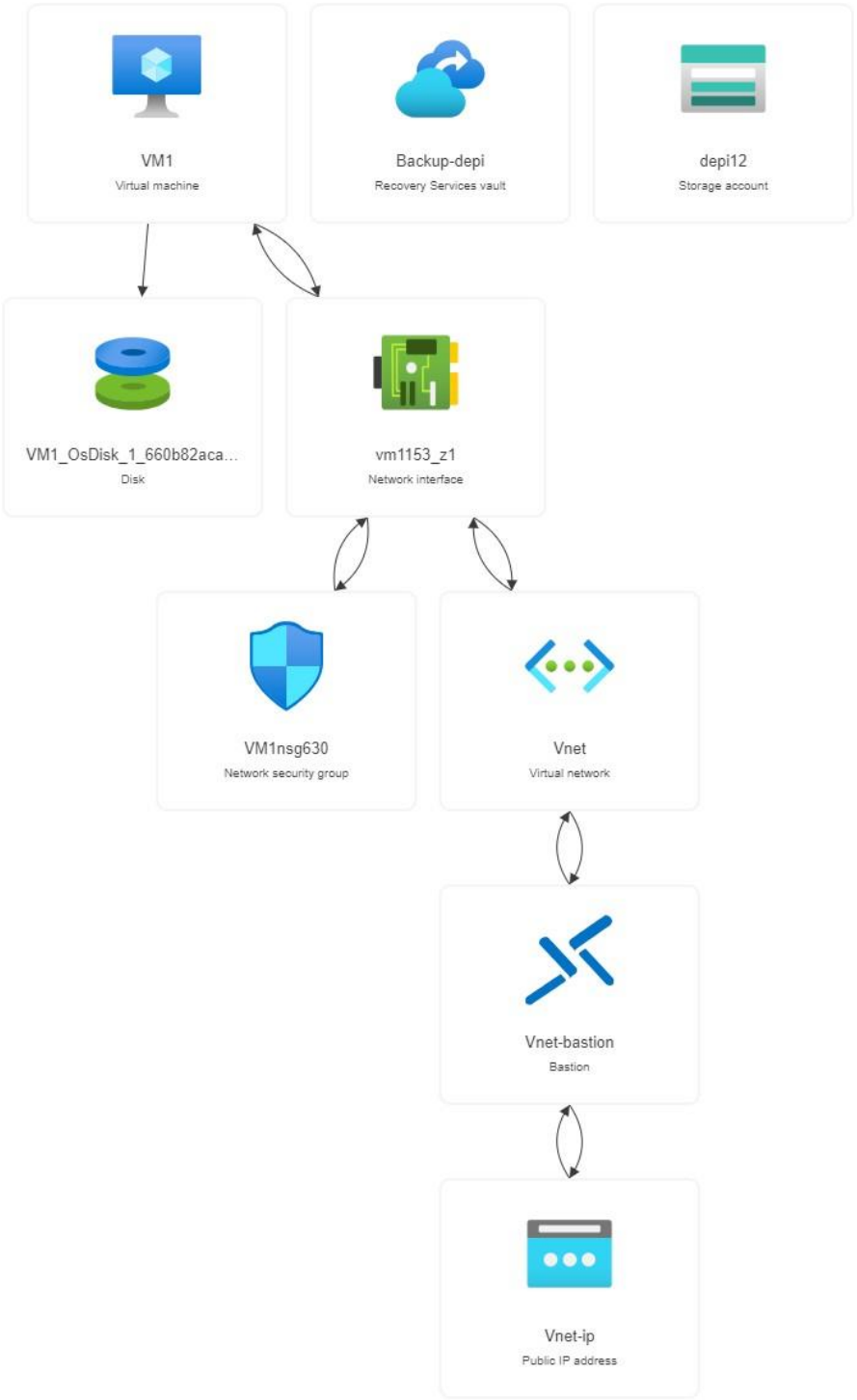
Associated application gateways

Associate this WAF policy with a specific application gateway, listener, or route path. A WAF policy and associate with an application gateway.

Configure it to application gateway:



Final Integration and Documentation



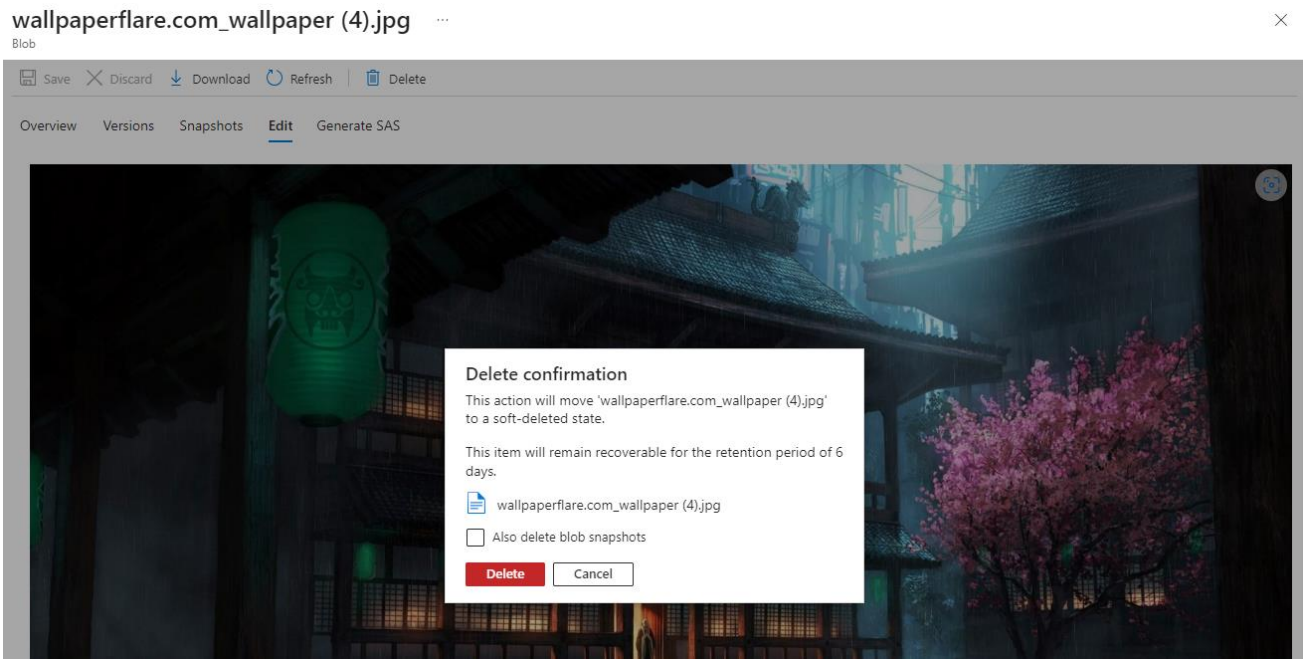
Overview of Integration:

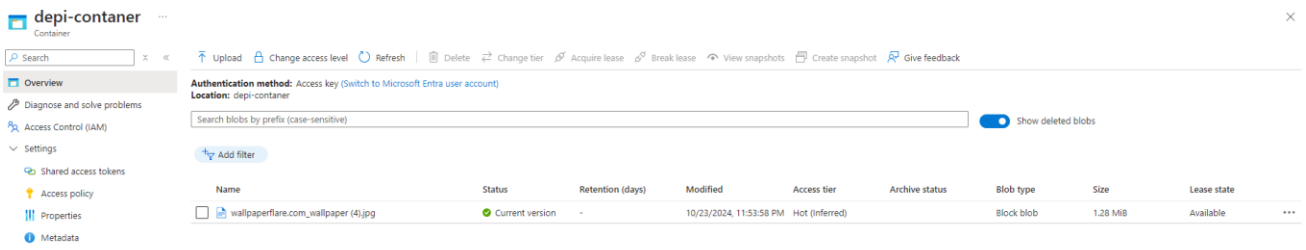
- Steps taken to integrate all components included configuring network settings, storage solutions, and access controls.
- Rationale behind the setup focused on security, performance, and scalability.

Testing and Results

Testing Methods:

- Conducted functional tests, performance tests, and security assessments.
- Summary of results indicated successful deployment and integration of all components.





*Visuals: * Key metrics and outcomes displayed in graphs or tables.

Final Report and Presentation

Key Findings:

- The project successfully demonstrated the capabilities of Azure in deploying and managing cloud infrastructure.

- Stakeholder feedback highlighted the effectiveness and efficiency of the setup.

*Visuals: * Highlights from the final report, including key metrics.

Conclusion

Recap of Project:

- The project highlighted the importance of Azure in cloud infrastructure deployment and management.

- Future considerations include exploring advanced features and optimizing resource usage.