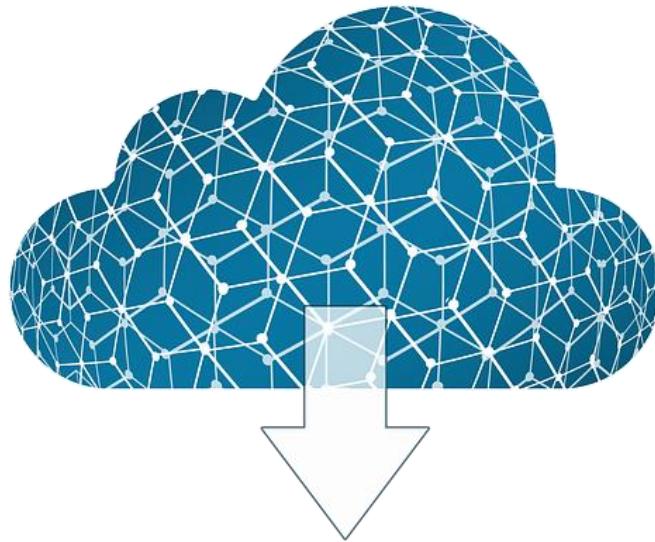


Azure Cloud Infrastructure Deployment and Management

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

1. Overview of Cloud Computing
2. Azure Fundamentals & Setup
3. Deploy and Manage Azure Resources
4. Implement Storage Solutions
5. Final Integration and Documentation

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-premise

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. Choose the RG Name and Region

Create a resource group

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more ↗](#)

Project details

Subscription * ⓘ Azure for Students (aada8f93-9ca9-4e47-b0ed-ebc8e660357e) ▾

Resource group * ⓘ depi-project ✓

Resource details

Region * ⓘ (Canada) Canada Central ▾

5. Add lock

Fill in Lock Details:

- Lock Name - Lock Type:

Add lock

Lock name *	Lock type *
Depi	Delete
Notes	
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	



6. Select a Role:

Role Members * Conditions Review + assign

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles

Job function roles **Privileged administrator roles**

Grant privileged administrator access, such as the ability to assign roles to other users.

⚠️ Can a job function role with less access be used instead?

Name ↑↓	Description ↑↓
Owner	Grants full access to manage all resources, including the ability to
Contributor	Grants full access to manage all resources, but does not allow yo
Access Review Operator Service Role	Lets you grant Access Review System app permissions to discover
Role Based Access Control Administrator	Manage access to Azure resources by assigning roles using Azur
User Access Administrator	Lets you manage user access to Azure resources.

Showing 1 - 5 of 5 results.

7. Assign Access to:

- all accounts of team members

Role **Members** * Conditions Review + assign

Selected role Contributor

Assign access to User, group, or service principal Managed identity

Members [+ Select members](#)

Name	Object ID	Type
Helmy, Engy Hussein Helmy Moustafa	ed820b96-508f-4dec-8326-bc07f512cb2e	User
mohamed, mahmoud khaled mohamed...	016df0dd-233a-48f9-bacb-0ae4a33add...	User
Saber, Abdallah Mahmoud Saber Abdal...	9d8d5604-187b-462f-99b8-ea2f39dbfa16	User

Description [Optional](#)

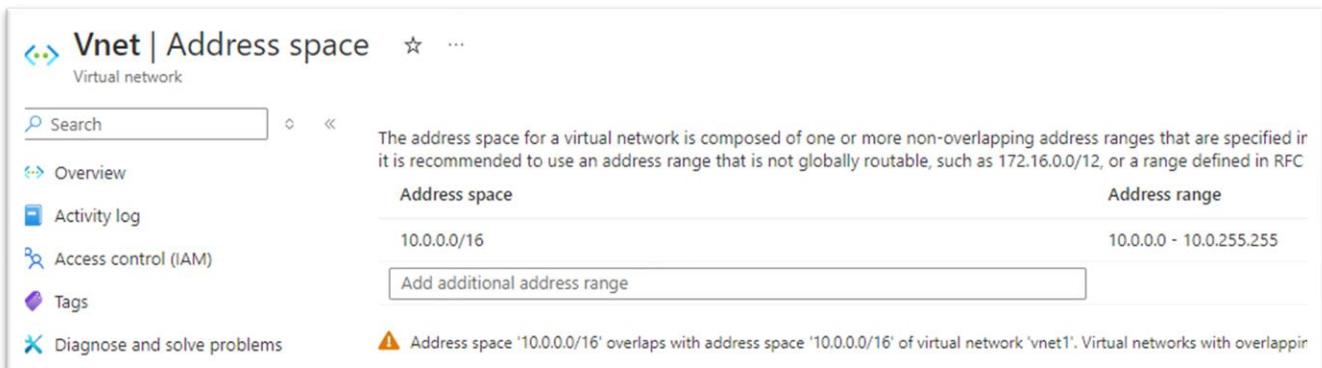
Week 2

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.



The address space for a virtual network is composed of one or more non-overlapping address ranges that are specified in it is recommended to use an address range that is not globally routable, such as 172.16.0.0/12, or a range defined in RFC 1918.

Address space	Address range
10.0.0.0/16	10.0.0.0 - 10.0.255.255

⚠️ Address space '10.0.0.0/16' overlaps with address space '10.0.0.0/16' of virtual network 'vnet1'. Virtual networks with overlapping address spaces cannot communicate directly.

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).



HOME > VIRTUAL NETWORKS > DEPI-PROJECT > VNET

Vnet | Subnets

Virtual network

Search

+ Subnet Refresh Manage users Delete

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Settings Address space Connected devices Subnets

Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you do this, you can assign specific IP ranges to different segments of your network.

Search subnets

<input type="checkbox"/>	Name	IPAM Pool	IPv4	IPv6	Available IPs ↓
<input type="checkbox"/>	AzureBastionSubnet	-	10.0.1.0/26	-	57
<input type="checkbox"/>	default	-	10.0.0.0/24	-	250

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.

VM-nsg

Network security group

Move Delete Refresh Give feedback

Overview

Resource group (move) : depi-project
Location : Canada Central
Subscription (move) : Azure for Students
Subscription ID : 83978cb6-dba-4da7-8820-51f704c31087
Tags (edit) : Add tags

Custom security rules : 1 inbound, 0 outbound
Associated with : 0 subnets, 0 network interfaces

Inbound Security Rules

Priority ↑	Name ↓	Port = all	Protocol = all	Source = all	Destination = all	Action = all
300	RDP	3389	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Outbound Security Rules

Priority ↑	Name ↓	Port = all	Protocol = all	Source = all	Destination = all	Action = all
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny



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.

Vnet | Subnets

Virtual network

Search

+ Subnet Refresh Manage users Delete

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

Create subnets to segment the virtual network address space into smaller ranges

Search subnets

Name	IPAM Pool	IPv4	IPv6	Private subnet
default	-	10.0.0.0/26		private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more ↗
AzureBastionSubnet	-	10.0.1.0/26		Enable private subnet (no default outbound access)

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 ↗](#)

Subnet ID: /subscriptions/83978cb6-dbba-4da7-8820-51f704c31087/resourceGroups/depi-project/pr...
Subnet purpose: Azure Bastion
Name: AzureBastionSubnet
IPv4: Address prefix '10.0.1.0/26' cannot be updated because the subnet is in use.
Include an IPv4 address space: 10.0.0.0/16
Starting address: 10.0.1.0
Size: /26
Subnet address range: 10.0.1.0 - 10.0.1.63
IPv6: This virtual network has no IPv6 address ranges.
Include an IPv6 address space:
Private subnet: private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. [Learn more ↗](#)
Enable private subnet (no default outbound access):

Vnet | Bastion

Virtual network

Search

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

Azure Bastion protects your virtual machines by secure and seamless RDP & SSH connectivity without the need to expose them through public IP addresses. [Learn more ↗](#)

Using Bastion: **Vnet-bastion**

Provisioning State: **Succeeded**

Select a VM to connect to *

VM1

Please enter username and password to your virtual machine to connect using Bastion.

Connection Settings

Keyboard Language: English (US)

Authentication Type: VM Password

Username:

VM Password: Show Open in new browser tab

Connect

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

Create a virtual machine

... Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size

Subscription * Azure for Students (83978cb6-dbba-4da7-8820-51f704c31087)

Resource group * depi-project Create new

Instance details

Virtual machine name * VM1

Region * (Canada) Canada Central

Availability options Availability zone

Self-selected zone Choose up to 3 availability zones, one VM per zone

Azure-selected zone (Preview) Let Azure assign the best zone for your needs

Availability zone * Zone 1

You can now select multiple zones. Selecting multiple zones will create one VM per zone. [Learn more](#)

Security type Trusted launch virtual machines Configure security features

Image * Windows Server 2019 Datacenter - x64 Gen2

Administrator account

Username * VM2024

Password * Confirm password *

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

None Allow selected ports

Select inbound ports * RDP (3389)



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

Essentials

Resource group (move)	: depi-project	Operating system	: Windows (Windows Server 2019 Datacenter)
Status	: Running	Size	: Standard B1s (1 vcpu, 1 GiB memory)
Location	: Canada Central (Zone 1)	Public IP address	: 4.206.2.46
Subscription (move)	: Azure for Students	Virtual network/subnet	: Vnet/default
Subscription ID	: 83978cb6-dbba-4da7-8820-51f704c31087	DNS name	: Not configured
Availability zone	: 1	Health state	: -
Tags (edit)	: Add tags	Time created	: 10/22/2024, 3:32 PM UTC

Properties Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

Computer name	VM1
Operating system	Windows (Windows Server 2019 Datacenter)
VM generation	V2
VM architecture	x64
Agent status	Ready
Agent version	2.7.41491.1139
Hibernation	Disabled
Host group	-

Networking

Public IP address	: 4.206.2.46 (Network interface vm1153_z1)
Public IP address (IPv6)	: -
Private IP address	: 10.0.0.5
Private IP address (IPv6)	: -
Virtual network/subnet	: Vnet/default
DNS name	: Configure

Size

Standard B1s	: Standard B1s (1 vcpu, 1 GiB memory)
--------------	---------------------------------------

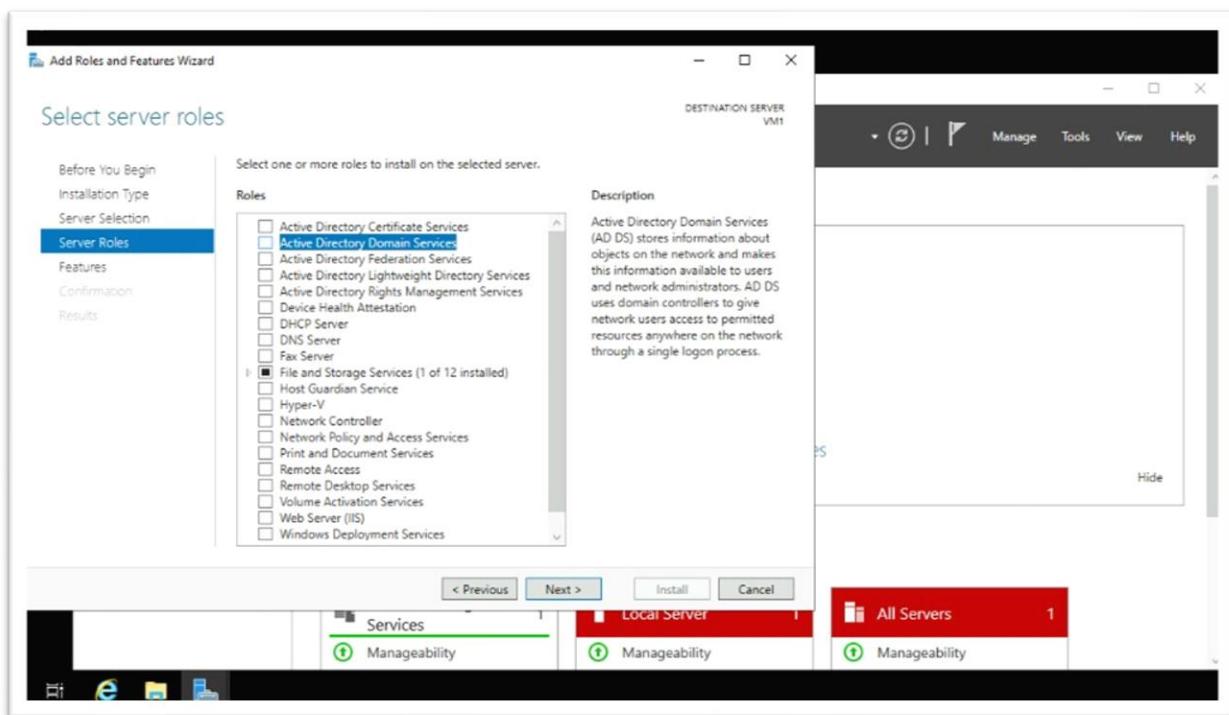
Azure AD Configuration:

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

Steps:

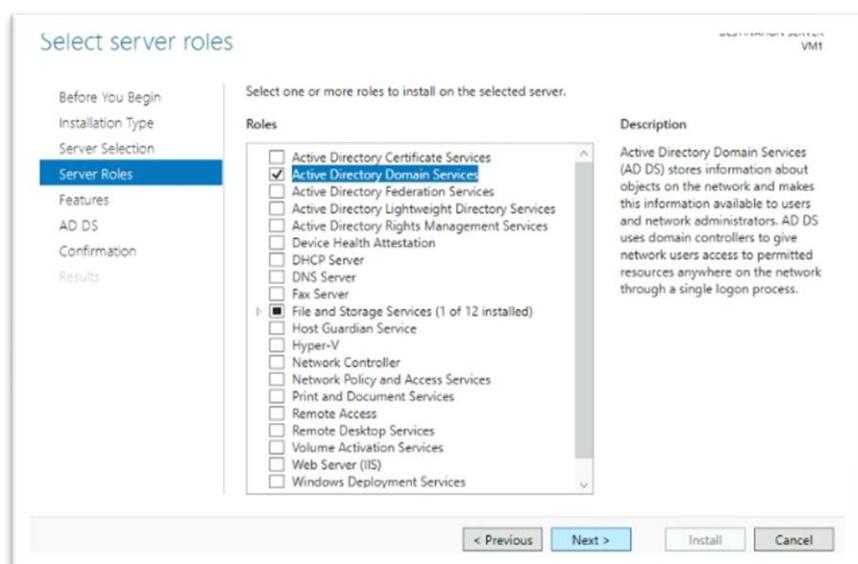
1. Add Roles: Click on Azure Active Directory Domain Services (ADDS):

- 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

Active Directory Domain Services Configuration Wizard

TARGET SERVER
VM1

Deployment Configuration

Select the deployment operation

Add a domain controller to an existing domain

Add a new domain to an existing forest

Add a new forest

Specify the domain information for this operation

Root domain name: mydomain.com

Domain Controller Options
Additional Options
Paths
Review Options
Prerequisites Check
Installation
Results

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.

Server Manager

Dashboard

WELCOME TO SERVER MANAGER

1 Configure this local server

2 Add roles and features

3 Add other servers to manage

4 Create a server group

5 Connect this server to cloud services

QUICK START

WHAT'S NEW

LEARN MORE

ROLES AND SERVER GROUPS

Roles: 3 | Server groups: 1 | Servers total: 1

Tools

Manage Tools View Help

Active Directory Administrative Center

Active Directory Domains and Trusts

Active Directory Module for Windows PowerShell

Active Directory Sites and Services

Active Directory Users and Computers

ADS Edit

Component Services

Computer Management

Defragment and Optimize Drives

Disk Cleanup

DNS

Event Viewer

Group Policy Management

iSCSI Initiator

Local Security Policy

Microsoft Azure Services

ODBC Data Sources (32-bit)

ODBC Data Sources (64-bit)

Performance Monitor

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

Active Directory Users and Computers

New >

All Tasks >

View >

Refresh

Export List...

Properties

Help

Name Type Description

Allowed RO... Security Group... Members in this group ...

Cert Publish... Security Group... Members of this group ...

Cloneable D... Security Group... Members of this group ...

Denied ROD... Security Group... Members in this group ...

DnsAdmin... Security Group... DNS Administrators Gro...

DnsUpdateP... Security Group... DNS clients who are per...

Domain Ad... Security Group... Designated administrato...

o... Security Group... All workstations and ser...

o... Security Group... All domain controllers i...

o... Security Group... All domain users

Delegate Control...

Find...

Computer

Contact

Group

InetOrgPerson

msDS-KeyCredential

msDS-ResourcePropertyList

msDS-ShadowPrincipalContainer

mImaging-PSPs

MSMQ Queue Alias

Printer

User

Create a new object...



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

New Object - User

Create in: mydomain.com/Users

First name: omar Initials: []

Last name: hussein

Full name: omar hussein

User logon name: omarhussein@mydomain.com

User logon name (pre-Windows 2000): MYDOMAIN\omarhussein

< Back Next > Cancel

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”

Welcome to Microsoft Entra Connect Sync

Run this installation tool on the server where the synchronization service component will be installed.

Microsoft Entra Connect Sync integrates your on-premises and online directories.

This installation tool will:

- Guide you in selecting a solution (for example, password hash synchronization or federation with AD FS)
- Install identity synchronization and other Microsoft software components required for deployment
- Enable application telemetry and component health data by default. You can change what data is shared with Microsoft by updating your [privacy settings](#).

[Learn more about hybrid identity](#)

I agree to the [license terms](#) and [privacy notice](#).

User management

Microsoft Entra Connect

Sync status: last synced 7 minutes ago

Password sync: recent synchronization

Add user Edit a user Reset password Delete user

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

Create new

Instance details

Storage account name * ⓘ dpistorage

Region * ⓘ (US) West US 3 Deploy to an Azure Extended Zone

Primary service ⓘ Select a primary service

Performance * ⓘ Standard: Recommended for most scenarios (general-purpose v2 account)
 Premium: Recommended for scenarios that require low latency.

Redundancy * ⓘ Geo-redundant storage (GRS)
 Make read access to data available in the event of regional unavailability.

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

Account kind
StorageV2 (general purpose v2)

Performance ⓘ Standard Premium
This setting cannot be changed after the storage account is created.

Secure transfer required ⓘ Disabled Enabled

Allow Blob anonymous access ⓘ Disabled Enabled

Allow storage account key access ⓘ Disabled Enabled

Allow recommended upper limit for shared access signature (SAS) expiry interval ⓘ Disabled Enabled

Default to Microsoft Entra authorization in the Azure portal ⓘ Disabled Enabled

Minimum TLS version ⓘ Version 1.2

Permitted scope for copy operations (preview) ⓘ From any storage account

Blob access tier (default) ⓘ Hot Cool

Large file shares ⓘ

3- network and security configuration

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



Public network access

- Enabled from all networks
- Enabled from selected virtual networks and IP addresses
- Disabled

All networks, including the internet, can access this storage account. [Learn more](#)

Network Routing

Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.

Routing preference *

- Microsoft network routing Internet routing

Publish route-specific endpoints

- Microsoft network routing
- Internet routing

4- Use Microsoft encryption

Encryption Encryption scopes

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process. [Learn more about Azure Storage encryption](#)

Encryption selection

Enable support for customer-managed keys Blobs and files only

Infrastructure encryption Disabled

Encryption type Microsoft-managed keys Customer-managed keys

5- blob storage configuration

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

dpiprojectstorage | Containers

Storage account

Containers

+ Container Change access level Restore containers Refresh Delete Give feedback

Search containers by prefix

Name	Last modified	Anonymous access level
\$logs	10/3/2024, 3:09:01 PM	Private
dpicontainer	10/3/2024, 4:12:26 PM	Private



6- Version control

dep12 | Data protection

Storage account

Search

Data migration

Events

Storage browser

Storage Mover

Partner solutions

Data storage

- Containers
- File shares
- Queues
- Tables

> Security + networking

> Data management

- Storage tasks (preview)
- Redundancy
- Data protection**
- Object replication
- Blob inventory
- Static website
- Lifecycle management
- Azure AI Search

> Settings

> Monitoring

> Monitoring (classic)

Data protection provides options for recovering your data when it is erroneously modified or deleted.

Recovery

Enable Azure Backup for blobs

Azure Backup can help you protect blobs in this storage account and manage the protection at scale. [Learn more](#)

Enable point-in-time restore for containers

Enable soft delete for blobs

Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)

Keep deleted blobs for (in days) *

Enable soft delete for containers

Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)

Keep deleted containers for (in days) *

Enable permanent delete for soft deleted items

Tracking

Enable versioning for blobs

Use versioning to automatically maintain previous versions of your blobs. [Learn more](#)

Consider your workloads, their impact on the number of versions created, and the resulting costs. Optimize costs by automating blob cleanup.

Keep all versions

Delete versions after (in days) *

Enable blob change feed



Backup Solutions

Strategy Overview:

- Implemented backup solutions for VMs using Azure Backup services.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Recovery Services vaults >

Create Recovery Services vault ...

* Basics Redundancy Encryption Vault properties Networking Tags Review + create

Project Details

Select the subscription and the resource group in which you want to create the vault.

Subscription * ⓘ Azure for Students (83978cb6-dbba-4da7-8820-51f704c31087)

Resource group * ⓘ depi-project

Create new

Instance Details

Vault name * ⓘ Backup

Region * ⓘ Canada Central

Cross Subscription Restore is enabled by default for all vaults. Visit vault 'Properties' to disable the same. [Learn more](#).

Review + create Next: Redundancy Feedback

- Ensured data protection through regular backups and recovery plans.

Graduation_project_Depi - Microsoft Edge | WhatsApp | Select virtual machines - Microsoft Edge

https://portal.azure.com/#view/Microsoft_Azure_DataProtection/V1EnableIaaSVMBackupBlade/_provisioningContext~/%7B%initialValue%7D

Coursera WhatsApp YouTube LinkedIn Translate Speedtest by Ookla... My courses مبادرة رواد مصر الرقمية Inception... مشاهدة فيلم NUB Portal Login Ar...

Microsoft Azure

Search resources, services, and docs (G+)

Home > MicrosoftRecoveryServicesV2-1727982387672 | Overview > RSG-DI

Select virtual machines

Configure backup ...

RSG-DEPI

Daily at 5:00 AM UTC

Instant restore

Retain instant recovery snapshot(s) for 2 days

Retention of daily backup point

Retain backup taken every day at 5:00 AM

Consistency type ⓘ Application or file-system consistent

Virtual machines

Name	Resource group
No virtual machines selected.	

Add

Selective disk backup option allows you to include or exclude specific data disks but is not supported. Know more about Selective Disk Backup feature, its limitation and usage.

Enable backup Download a template for automation OK Cancel Give feedback



RSG-DEPI - Microsoft Azure (2) WhatsApp

Coursera WhatsApp YouTube LinkedIn Translate Speedtest by Ookla... My courses معاشرة رؤاد مصر الرقمية Inception... مشاهدة فيلم... NUB Portal Login Ar... as30204012206916@du.eg EGYPT UNIVERSITY OF INFORMATI...

Microsoft Azure Search resources, services, and docs (G+) Copilot

Home > Resource groups > Graduation_project_Depi > RSG-DEPI

RSG-DEPI | Backup items

Recovery Services vault

backup

Refresh Feedback

Try our new Business Continuity Center for the at scale BCDR management of your resources protected across Azure Backup and Site Recovery.

Primary Region Secondary Region

BACKUP MANAGEMENT TYPE	BACKUP ITEM COUNT
Azure Virtual Machine	1
Azure Storage (Azure Files)	1
Azure Backup Agent	0
Azure Backup Server	0
DPM	0
SQL Database in Azure VM	0
SAP HANA in Azure VM	0



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.

The screenshot shows the 'Essentials' section of an Azure App Service plan. It includes the following details:

Setting	Value
Resource group (move)	my-rg
Status	Ready
Location	Canada Central
Subscription (move)	Azure for Students
Subscription ID	83978cb6-dbba-4da7-8820-51f704c31087
Pricing plan	F1
Instance count	0
App(s) / Slots	1/0
Operating System	Windows
Zone redundant	Disabled

Basic Configuration:

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

The screenshot shows the 'Create Web App' wizard in the Azure portal. The 'Basics' tab is selected. The configuration includes:

- Project Details:** Subscription: Azure for Students, Resource Group: my-rg.
- Instance Details:** Name: webapp11, Unique default hostname (preview) is enabled.
- Publish:** Code is selected.
- Runtime stack:** Node 18 LTS.
- Operating System:** Windows.
- Region:** Canada Central.
- Pricing plans:** Windows Plan (Canada Central) is selected, showing ASP-myrg-9162 (F1).
- Pricing plan:** Free F1 (Shared infrastructure) is listed.



Deploy and configure the application:

App Service supports multiple technologies to access, publish and modify the content of your app. FTPS credentials can be scoped to the application or the user.

FTPS endpoint

ftps://waws-prod-yt1-061.ftp.azurewebsites.windows.net/site/wwwroot



Application scope

Application scope credentials are auto-generated and provide access only to this specific app or deployment slot. These credentials can be used with FTPS, Local Git and WebDeploy. They cannot be configured manually, but can be reset anytime. [Learn more](#)

FTPS Username

REDACTED



Password



Reset

Network Configuration:

Networking

Virtual IP address	20.48.202.170
Outbound IP addresses	20.175.156.99,20.175.157.26,20.175.157... Show More
Additional Outbound IP addresses	20.175.156.99,20.175.157.26,20.175.157... Show More



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.

Network configuration

Address space	10.0.0.0/16	Encryption	Disabled
Subnets	2	DDoS protection plan	Configure
DNS servers	Azure provided DNS service		
Virtual network ID	1415d515-c5aa-4ea5-b754-2777094e1b23		

Connectivity

BGP virtual network community	Configure
BGP regional community	-
Connected devices	1
Flow timeout	Configure
Peerings	Add peerings

Basic configuration:

Create application gateway

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources. [?](#)

Subscription *	Azure for Students
Resource group *	my-rg
	Create new

Instance details

Application gateway name * appgateway

Region * Canada Central

Tier WAF V2

Enable autoscaling Yes

Minimum instance count * 0

Maximum instance count 10

Availability zone * Zones 1, 2, 3

IP address type IPv4 only

IPv4 only Dual stack (IPv4 & IPv6)

HTTP2 Disabled Enabled

WAF Policy * [Create new](#)

Configure virtual network

Virtual network * vnet1

[Create new](#)

Subnet * app-gateway (10.0.0.0/24)



- **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	rule1	> -



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.

Create a WAF policy

Basics Managed rules Policy settings Custom rules Association Tags Review + create

Regional WAF (Application Gateway)

Subscription * ⓘ Azure for Students

Resource Group * my-rg
Create new

Instance details

Name * ⓘ WAF

Location * ⓘ (Canada) Canada Central

Enable policy ⓘ

Policy mode

Prevention
Prevention mode takes the corresponding WAF action if a request matches a rule.

Detection
Detection mode monitors and logs all threat alerts to a log file.



Rule Sets:

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

Create a WAF policy ...

Basics Managed rules Policy settings Custom rules Association Tags Review + create

A pre-configured rule set is enabled by default. This rule set protects your web application from common threats defined in the top-ten OWASP categories. The default rule set is managed by the Azure WAF service. Rules are updated as needed for new attack signatures. [Learn more](#)

Default ruleset * OWASP_3.2

Additional ruleset Microsoft_BotManagerRuleSet_1.0

Enable Disable

Filter for any field Rule group : (All) X Status : (All) X Action : (All) X

Showing all 197 items (197 selected)

Rule Id	Description	Action	Status	Rule group	Rule set
200002	Failed to Parse Request Body.	Anomaly score	Enabled	General	OWASP_3.2
200003	Multipart Request Body Strict Validation	Anomaly score	Enabled	General	OWASP_3.2
200004	Possible Multipart Unmatched Boundary	Anomaly score	Enabled	General	OWASP_3.2
911100	Method is not allowed by policy	Anomaly score	Enabled	REQUEST-911-METHOD-ENFOR...	OWASP_3.2
912100	Found Icar-Dinant associated with car	Anomaly score	Enabled	REQUEST-912-SCANNER-NFTFC...	OWASP_3.2



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

Edit custom rule

A custom rule is made up of one or more conditions followed by an action. All custom rules for a WAF policy are match rules. Learn more about custom rules [↗](#)

Custom rule name *

Enable rule

Rule type Match Rate limit

Priority *

Conditions

If

Match type IP address
 Match variable
RemoteAddr

Operation Does contain Does not contain

IP address or range
192.168.2.20
IPv4 address or ranges

Then

Add new condition

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.

Association type	Application Gateway	Resource Group	HTTP Listener	Route Path
Route Path	gatway-1	my-rg	listener1	target1

Configure it to application gateway:

Home > my-rg > gatway-1

gatway-1 | Web application firewall ⚡ ⋮

Application gateway

wa

Settings

Web application firewall

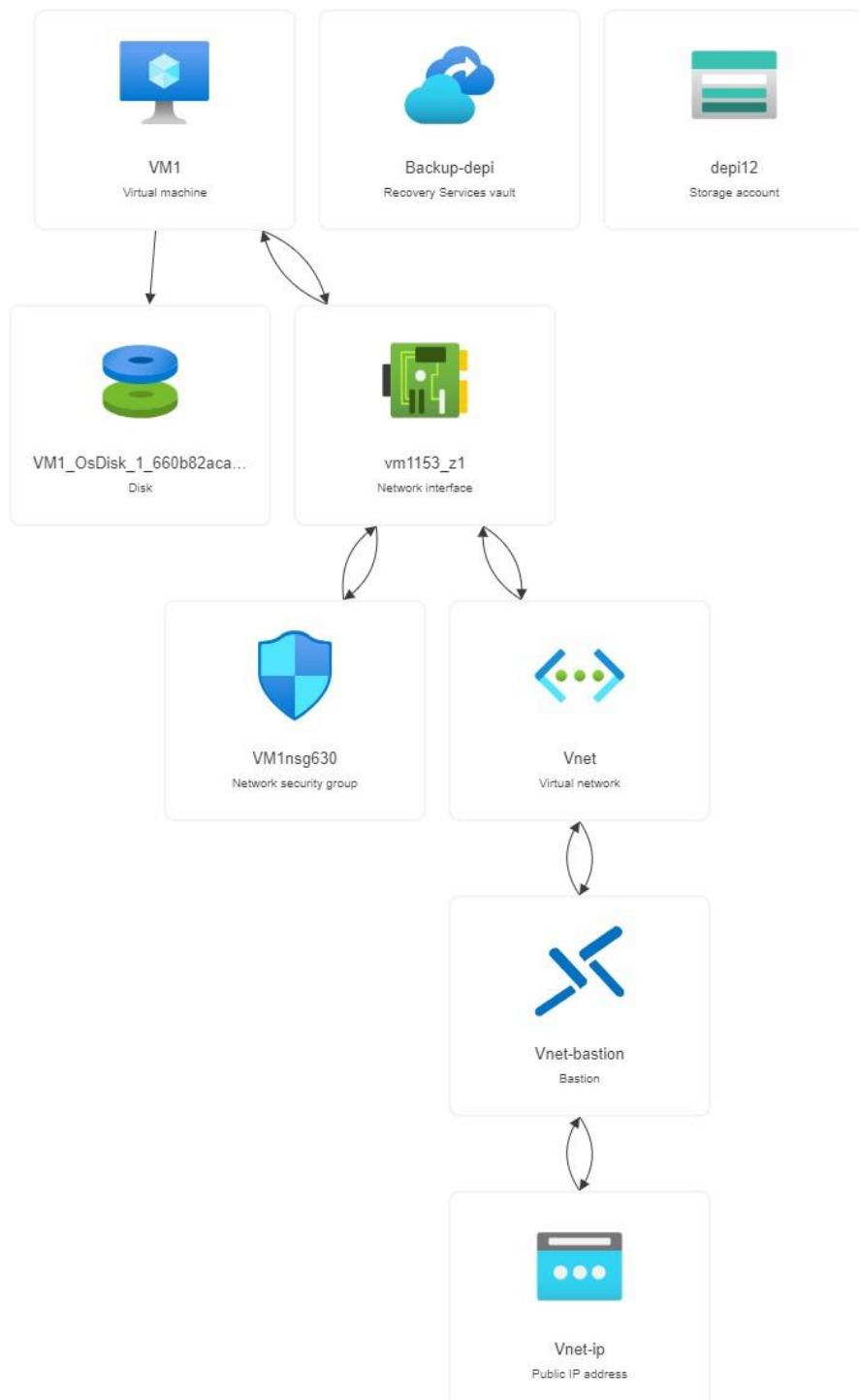
Configure

Tier Standard V2 WAF V2

WAF Policy *

Create new

Final Integration and Documentation



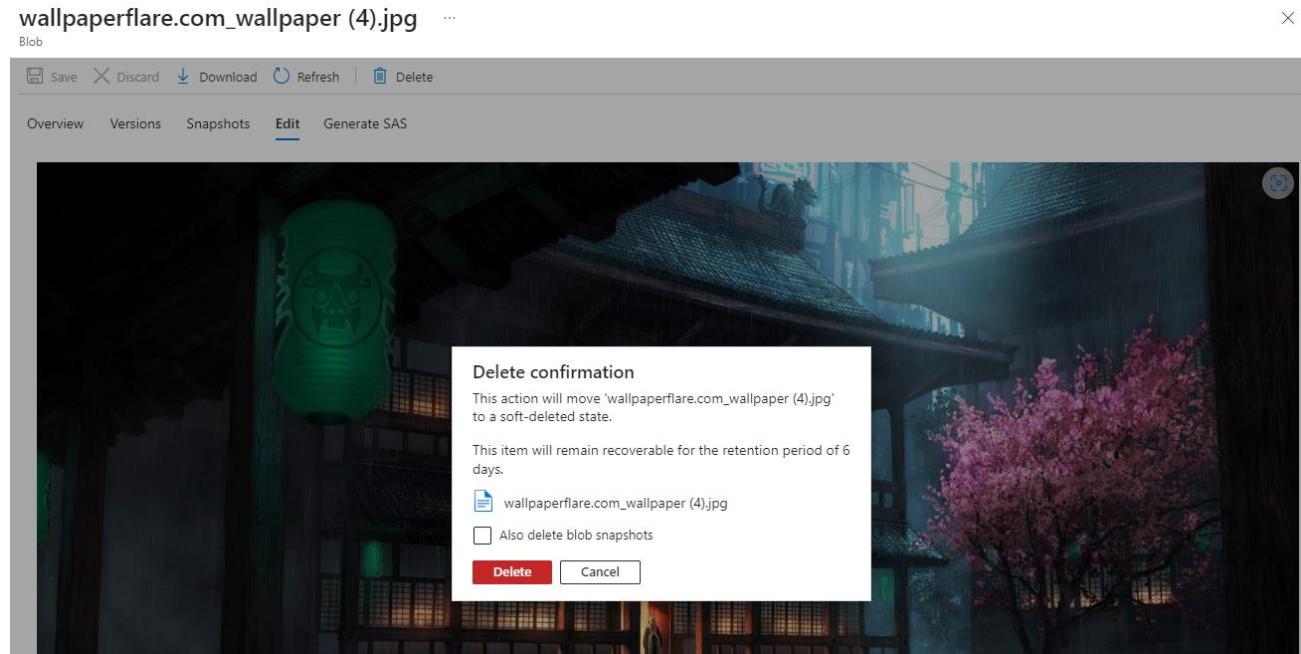
Overview of Integration:

- 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.



Name	Status	Retention (days)	Modified	Access tier	Archive status	Blob type	Size	Lease state
wallpaperflare.com_wallpaper (4).jpg	Current version	-	10/23/2024, 11:53:58 PM	Hot (Inferred)	Not yet archived	Block blob	1.28 MiB	Available



*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.