



Cloud Computing – ZEN Class Microsoft Azure – Project - 2

NAME : DIVYA NVK

MAIL ID : DIVYAKANNAN002@GMAIL.COM

BATCH : CC2WE-E

Project Synopsis:

Using Application Gateway, create a web application that is highly available in multiple regions, secure from web attacks, and load-balanced across regions.

Architectural Overview:

1. High Availability Across Multiple Regions

- Deployment: Deploy your web application in multiple Azure regions (e.g., East US, West Europe).
- Active-Active Configuration: Use an active-active configuration to ensure zero downtime. Both regions handle production traffic simultaneously.
- Failover Mechanism: Implement a failover mechanism to automatically route traffic to the secondary region if the primary region becomes unavailable.

2. Security from Web Attacks

- Azure Web Application Firewall (WAF): Integrate WAF with Azure Application Gateway to protect against common web attacks like SQL injection, cross-site scripting (XSS), and more.
- HTTPS: Ensure all traffic is encrypted using HTTPS.
- Regular Security Audits: Conduct regular security audits and vulnerability scans to identify and fix potential security issues.

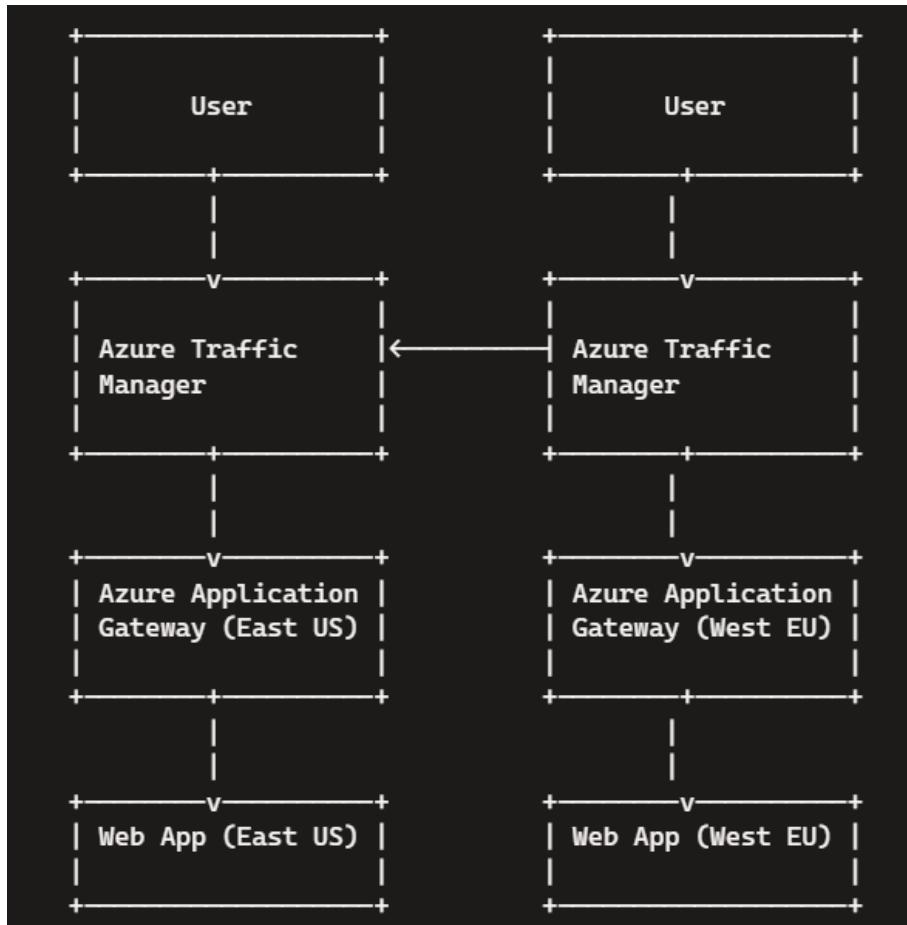
3. Load Balancing Across Regions

- Azure Traffic Manager: Use Azure Traffic Manager for DNS-based global load balancing. It directs user requests to the closest or best-performing region.
- Azure Application Gateway: Deploy Azure Application Gateway in each region to handle HTTP/HTTPS traffic. It provides advanced load-balancing features like URL-path-based routing and SSL termination.

- **Health Probes:** Configure health probes to monitor the health of your web application instances and ensure traffic is only routed to healthy instances.

Diagram:

Here's a simplified diagram to illustrate the architecture



Key Components:

- **Azure Traffic Manager:** Manages DNS-based global load balancing.
- **Azure Application Gateway:** Provides regional load balancing and web application fire wall capabilities.
- **Web Application:** Deployed in multiple regions for high availability.

Procedure:

- Login to Azure Portal
- Create a Resource Group

Home > Resource groups >

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 * ⓘ

Pay-as-you-go



Resource group * ⓘ

Web-app-RG



Resource details

Region * ⓘ

(US) East US



- Skip Tags, Review and Create.

Home > Resource groups >

Create a resource group ...

Validation passed.

Basics Tags Review + create

Basics

Subscription

Pay-as-you-go

Resource group

Web-app-RG

Region

East US

Tags

None

[Create](#)

[< Previous](#)

[Next >](#)

[Download a template for automation](#)

- Create two Virtual Machines in different regions.

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 for

Subscription * ⓘ Pay-as-you-go

Resource group * ⓘ Web-app-RG

[Create new](#)

Instance details

Virtual machine name * ⓘ Linux-VM-1

Region * ⓘ (US) East US

Availability options ⓘ No infrastructure redundancy required

Security type ⓘ Standard

Image * ⓘ Ubuntu Server 24.04 LTS - x64 Gen2

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.

Public inbound ports * ⓘ

None

Allow selected ports

Select inbound ports *

HTTP (80), HTTPS (443), SSH (22)

Info All traffic from the internet will be blocked by default. You will be able to change inbound port rules in the VM > Networking page.

Next: Disks

OS disk size ⓘ Image default (30 GiB)

OS disk type * ⓘ Standard SSD (locally-redundant storage)

The selected VM size supports premium disks. We recommend Premium SSD for high IOPS workloads. Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Delete with VM ⓘ

Key management ⓘ Platform-managed key

Enable Ultra Disk compatibility ⓘ Ultra disk is supported in Availability Zone(s) 1,2,3 for the selected VM size Standard_B2s.

Next: Networking

Virtual network * ⓘ (new) Linux-VM-1-vnet

Create new

Subnet * ⓘ (new) default (10.0.0.0/24)

Public IP ⓘ (new) Linux-VM-1-ip

Create new

NIC network security group ⓘ None Basic Advanced

Public inbound ports * ⓘ None Allow selected ports

Next: Management

Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more ↗](#)

✓ Your subscription is protected by Foundational Cloud Security Posture Management Free Plan.

Identity

Enable system assigned managed identity ⓘ

Microsoft Entra ID

Login with Microsoft Entra ID ⓘ

i RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine

Next: Monitoring

Alerts

Enable recommended alert rules ⓘ

Diagnostics

Boot diagnostics ⓘ Enable with managed storage account (recommended) Enable with custom storage account Disable

Enable OS guest diagnostics ⓘ

Health

Enable application health monitoring ⓘ

Next: Advanced

Extensions provide post-deployment configuration and automation.

Extensions ⓘ

Select an extension to install

VM applications

VM applications contain application files that are securely and reliably downloaded on your VM after deployment. In addition to the application files, an install and uninstall script are included in the application. You can easily add or remove applications on your VM after create. [Learn more ↗](#)

Select a VM application to install

Custom data and cloud init

Pass a cloud-init script, configuration file, or other data into the virtual machine **while it is being provisioned**. The data will be saved on the VM in a known location. [Learn more about custom data for VMs ↗](#)

- Skip Tags, Review and Create
- Repeat the same step for creating VM 2 but in a different region.
- SSH to both the VMs once it's deployed

```
root@LAPTOP-VJGJ8BEB:~# ssh azureuser@13.82.133.171
The authenticity of host '13.82.133.171 (13.82.133.171)' can't be established.
ED25519 key fingerprint is SHA256:/vUaPLWll2B3u8+mpdh/cRQL+DKAtmE5G0ZQND1Sz8I.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '13.82.133.171' (ED25519) to the list of known hosts.
azureuser@13.82.133.171's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Fri Oct 25 18:17:31 UTC 2024

System load:  0.17           Processes:          118
Usage of /:   5.0% of 28.02GB  Users logged in:    0
Memory usage: 7%            IPv4 address for eth0: 10.0.0.4
Swap usage:   0%

* Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s just raised the bar for easy, resilient and secure K8s cluster deployment.

https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
```

```
root@LAPTOP-VJGJ8BEB:~# ssh azureuser@52.172.172.67
The authenticity of host '52.172.172.67 (52.172.172.67)' can't be established.
ED25519 key fingerprint is SHA256:ZfhGijGjim3FMk1Q7XYdd/ZbWbrWduuNyVNoNnDgCpE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '52.172.172.67' (ED25519) to the list of known hosts.
azureuser@52.172.172.67's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1016-azure x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Fri Oct 25 18:19:17 UTC 2024

System load:  0.36           Processes:          126
Usage of /:   5.0% of 28.02GB  Users logged in:    0
Memory usage: 6%            IPv4 address for eth0: 10.0.0.4
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
```

Install a Web Server:

- Install Apache by following the command

```
sudo apt update
```

```
sudo apt install apache2
```

- This will install the Apache web server

Create Colourful HTML pages:

- Navigate to the Web Directory

```
cd /var/www/html
```

- Create an HTML File

```
sudo vi index.html
```

- Add the following sample colorful HTML and CSS code

```

<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <title>Colorful Page</title>
    <style>
        body {
            background: linear-gradient(to right, #ff0000, #ff7f00, #ffff00,
            color: #fff;
            display: flex;
            justify-content: center;
            align-items: center;
            height: 100vh;
            margin: 0;
            font-family: 'Arial', sans-serif;
        }
        .content {
            text-align: center;
        }
        h1 {
            font-size: 3em;
            margin-bottom: 20px;
        }
        p {
            font-size: 1.5em;
        }
    </style>
</head>
<body>
    <div class="content">
        <h1>Welcome to Your Colorful VM!</h1>
        <p>This is your vibrant web page!</p>
    </div>
</body>
</html>

```

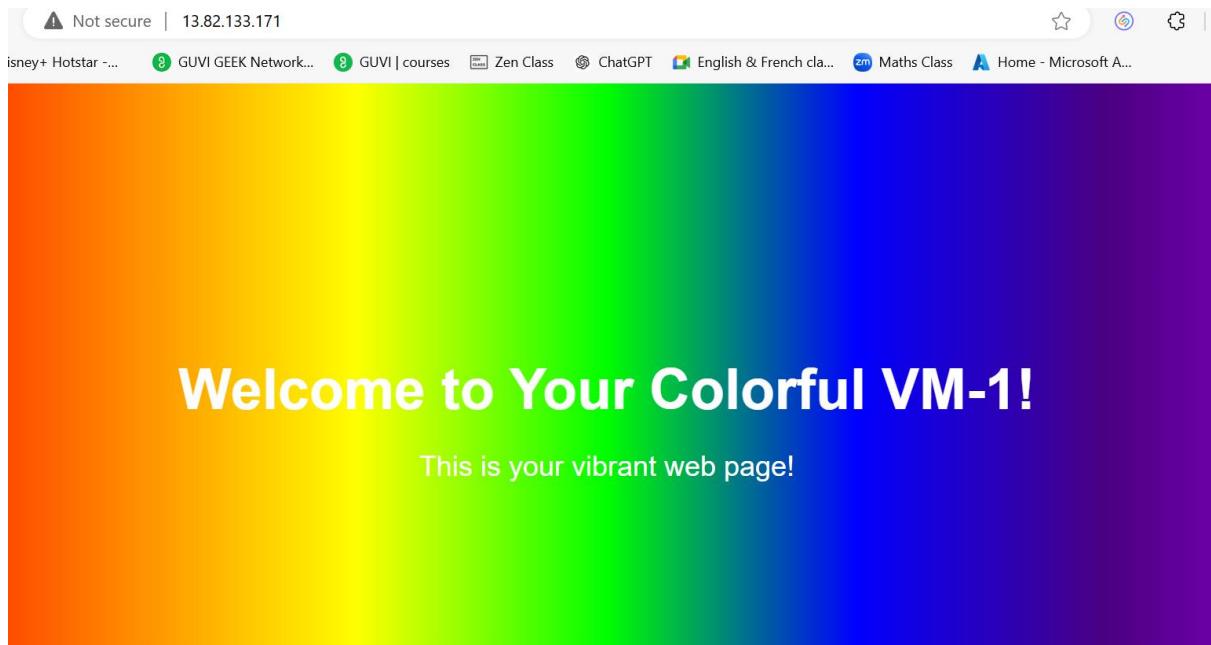
- Click ESC and give :wq! To save and exit the file
- Restart the Apache Service

sudo systemctl restart apache2

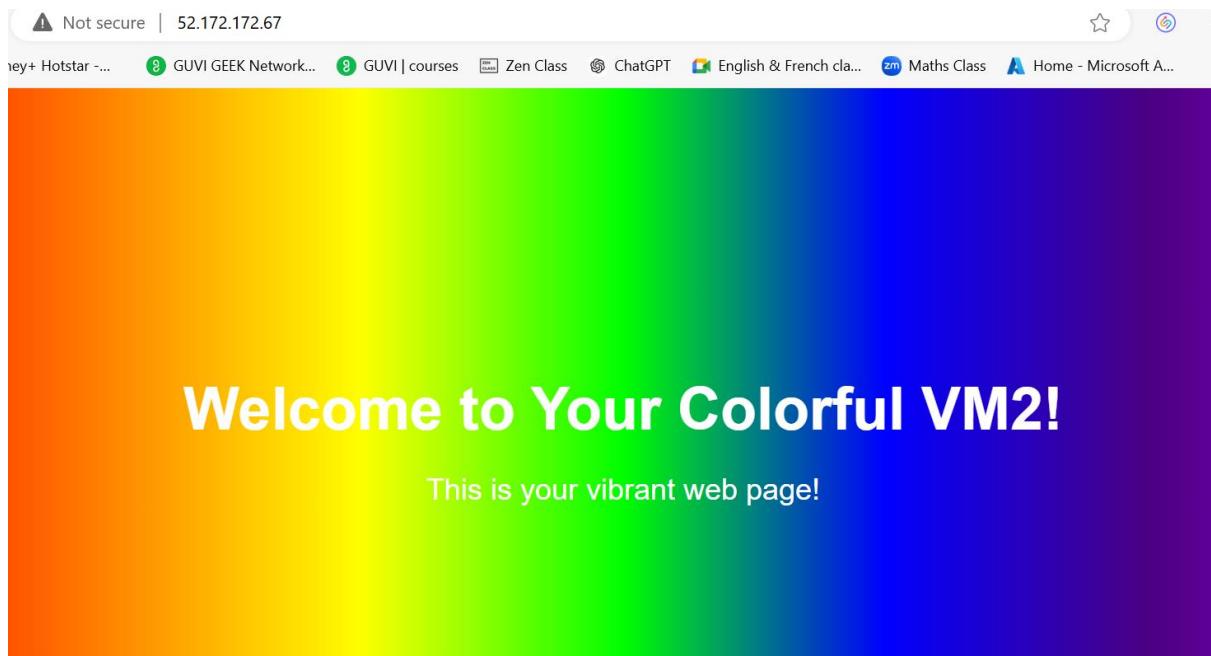
- Now, when you hit your VM's IP address in a browser, you should see a colorful web page! 🌈

Output:

VM 1: 13.82.133.171 (East US Region)



VM 2: 52.172.172.67 (Central India Region)



- Create Application Gateway

Create application gateway

1 Basics [2 Frontends](#) [3 Backends](#) [4 Configuration](#) [5 Tags](#) [6 Review + create](#)

An application gateway is a web traffic load balancer that enables you to manage traffic to your web application. [Learn about creating application gateway](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *	<input type="text" value="Pay-as-you-go"/>
Resource group *	<input type="text" value="Web-app-RG"/> Create new

Instance details

Application gateway name *	<input type="text" value="App-gateway-mywebapp-1"/>
----------------------------	---

[Home](#) > [Load balancing | Application Gateway](#) >

Create application gateway

Region *	<input type="text" value="East US"/>
Tier	<input type="text" value="WAF V2"/>
Enable autoscaling	
Enable autoscaling	<input checked="" type="radio"/> Yes <input type="radio"/> No
Minimum instance count *	<input type="text" value="0"/>
Maximum instance count	<input type="text" value="5"/>
Availability zone *	<input type="text" value="Zones 1, 2, 3"/>
IP address type	<input checked="" type="radio"/> IPv4 only <input type="radio"/> Dual stack (IPv4 & IPv6)
HTTP2	<input type="radio"/> Disabled <input checked="" type="radio"/> Enabled
WAF Policy *	<input type="text" value="(new) WAF-1"/>

Configure virtual network

Virtual network * ⓘ

▼

Create new

Subnet * ⓘ

▼

Manage subnet configuration

[Previous](#)

[Next : Frontends >](#)

- Next: Frontends

[Home](#) > [Load balancing | Application Gateway](#) >

Create application gateway

✓ Basics **2 Frontends** ③ Backends ④ Configuration ⑤ Tags ⑥ Review + create

Traffic enters the application gateway via its frontend IP address(es). An application gateway can use a public IP address, private IP address, or one of each type. ↗

Frontend IP address type ⓘ

Public Private Both

Public IPv4 address *

▼

[Add new](#)

[Previous](#)

[Next : Backends >](#)

- Next: Backends

[Home](#) > [Load balancing | Application Gateway](#) >

Create application gateway

✓ Basics ✓ Frontends **3 Backends** ④ Configuration ⑤ Tags ⑥ Review + create

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, app services, IP addresses, or fully qualified domain names (FQDN). ↗

Add a backend pool

Backend pool

backend-pool-1

Targets

> 1 target

Add a backend pool.

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, app services, IP addresses, or fully qualified domain names (FQDN). ↗

Name *

backend-pool-1

Add backend pool without targets

Yes No

Backend targets

1 item

Target type

Virtual machine

Target

linux-vm-1456

IP address or FQDN

[Previous](#)

[Next : Configuration >](#)

[Add](#) [Cancel](#)

- Next: Configuration
- Click Routing Rule

Add a routing rule

Configure a routing rule to send traffic from a given frontend IP address to one or more backend targets. A routing rule must contain a listener and at least one backend target.

Rule name *

Priority *

*Listener *Backend targets

A listener "listens" on a specified port and IP address for traffic that uses a specified protocol. If the listener criteria are met, the application gateway will apply this routing rule. (?)

Listener name *

Frontend IP *

Protocol HTTP HTTPS

Port *

Listener type Basic Multi site

[Previous](#) [Next : Tags >](#)

<https://portal.azure.com/#>

[Add](#) [Cancel](#)

- Need to add Backend Targets too on the same page before clicking add

Add Backend setting

← Discard changes and go back to routing rules

Backend settings name *

Backend protocol HTTP HTTPS

Backend port *

Additional settings

Cookie-based affinity Enable Disable

Connection draining Enable Disable

Request time-out (seconds) *

Override backend path

Host name

By default, the Application Gateway sends the same HTTP host header to the backend as it receives from the client. If your backend application/service requires a specific host value, you can override it using this setting.

[Yes](#) [No](#)

[Add](#) [Cancel](#)

- It should be like this as shown below after adding all three

Create application gateway ...

X

✓ Basics ✓ Frontends ✓ Backends Configuration Tags Review + create

Create routing rules that link your frontend(s) and backend(s). You can also add more backend pools, add a second frontend IP configuration if you haven't already, or edit previous configurations.

Frontends: Public: (new) IP, + Add a frontend IP

Routing rules: azureuser, + Add a routing rule

Backend pools: backend-pool-1, + Add a backend pool

Manage Backend settings

- Skip Tags
- Validate, Review and Create
- Repeat the same steps to create another Application Gateway for VM2 as mentioned Regions respectively

Create application gateway ...

✓ Validation passed

✓ Basics ✓ Frontends ✓ Backends ✓ Configuration ✓ Tags 6 Review + create

Basics

Subscription	Pay-as-you-go
Resource group	Web-app-RG
Name	App-gateway-mywebapp-1
Region	East US
Tier	WAF_v2
Enable autoscaling	Enabled
Minimum instance count	0
Maximum instance count	5

Create

Previous

Next

Download a template for automation

- After deploying Application Gateway, Go to settings -> health-probs -> add

App-gateway-mywebapp-1 | Health probes

Application gateway

Search Add Refresh Delete Feedback

Configuration
Web application firewall
Backend pools
Backend settings
Frontend IP configurations
Private link
SSL settings
Listeners
Rules
Rewrites
Health probes
Properties

No results.

Add health probe

App-gateway-mywebapp-1

Name *

Protocol * HTTP HTTPS

Pick host name from backend settings Yes No

Host *

Pick port from backend settings Yes No

Path *

Interval (seconds) *

Timeout (seconds) *

Unhealthy threshold *

I want to test the backend health before adding the health probe

Test **Cancel**

PICK port from backend settings

Path * /

Interval (seconds) * 30

Timeout (seconds) * 30

Unhealthy threshold * 3

Use probe matching conditions
① Yes No

Backend settings ① backend-setting-1

I want to test the backend health before adding the health probe

Test **Cancel**

- Test and the result should be like as below, then Add

[Home](#) > Microsoft App-gat Application gateway

Add health probe

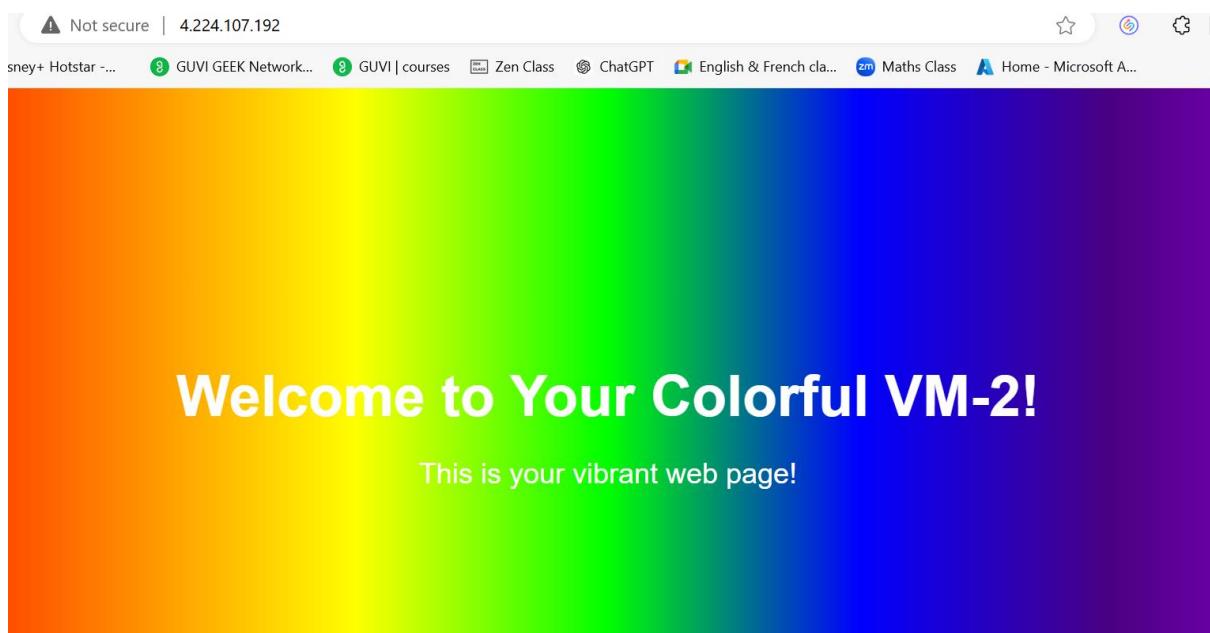
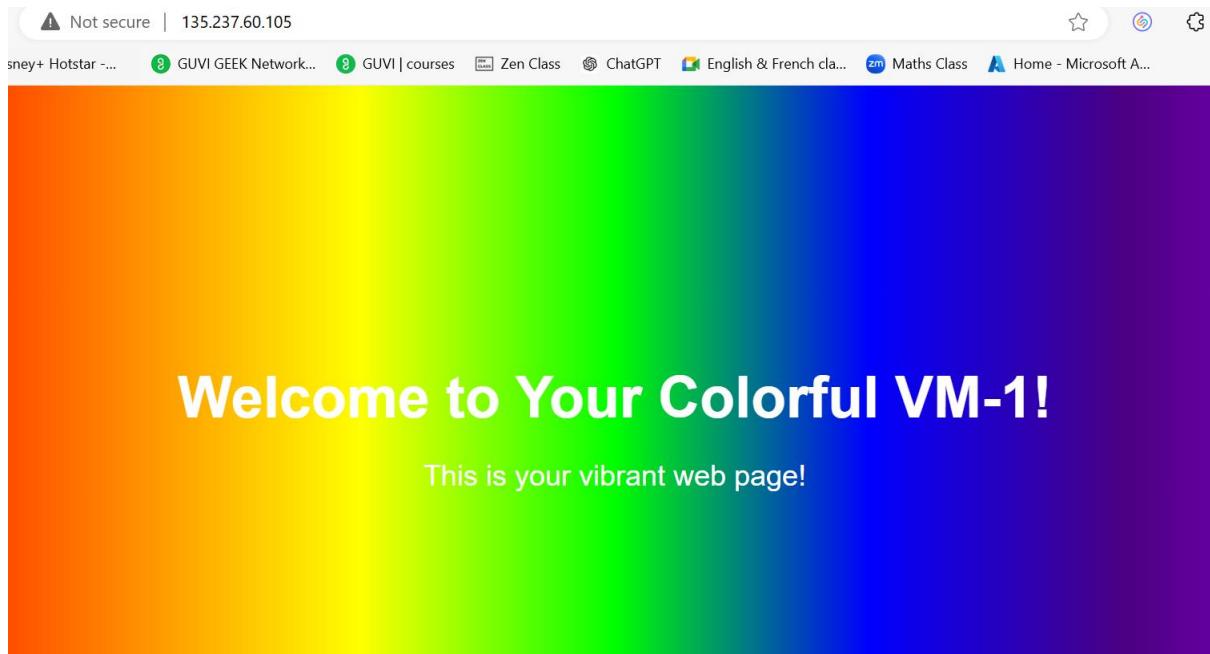
App-gateway-mywebapp-1

[Go back to probe](#)

Backend pool	HTTP setting	Status	Details
> backend-pool-1	backend-setting-1	✓	

Add

- Now, hit the Application Gateway Ip's for both 1 and 2 in the browser to view the result



- Create Traffic Manager Profile

Home > Load balancing | Traffic Manager >

Create Traffic Manager profile

Name * .trafficmanager.net

Routing method

Subscription *

Resource group * Create new

Resource group location

Create Automation options

- Once it's created, Need to add both the IPs and Traffic Manager URL in the DNS
- Type -> A, Data -> IP address -> Save

	Type	Name	Data	TTL	Delete	Edit
Portfolio	A	@	13.82.133.171	1 Hour		
DNS	A	@	52.172.172.67	1 Hour		
Transfers						

- For Traffic Manager URL Type -> CNAME, Name -> WWW, -> Value -> Traffic Manager URL -> Save

Type *	Name *	Value *	TTL
CNAME	www	web-app-2.trafficmanager.net	1 Hour

Save **Close**

- Once the DNS values has been added, Go to Endpoints and add both the IPs to it

Add endpoint

Type * External endpoint

Name * Endpoint-1

Enable Endpoint

Fully-qualified domain name (FQDN) or IP * 13.82.133.171

Priority * 1

Custom Header settings Configure in this format, host:contoso.com,customheader:contoso

Add

Add endpoint

Type * External endpoint

Name * Endpoint-2

Enable Endpoint

Fully-qualified domain name (FQDN) or IP * 52.172.172.67

Priority * 2

Custom Header settings Configure in this format, host:contoso.com,customheader:contoso

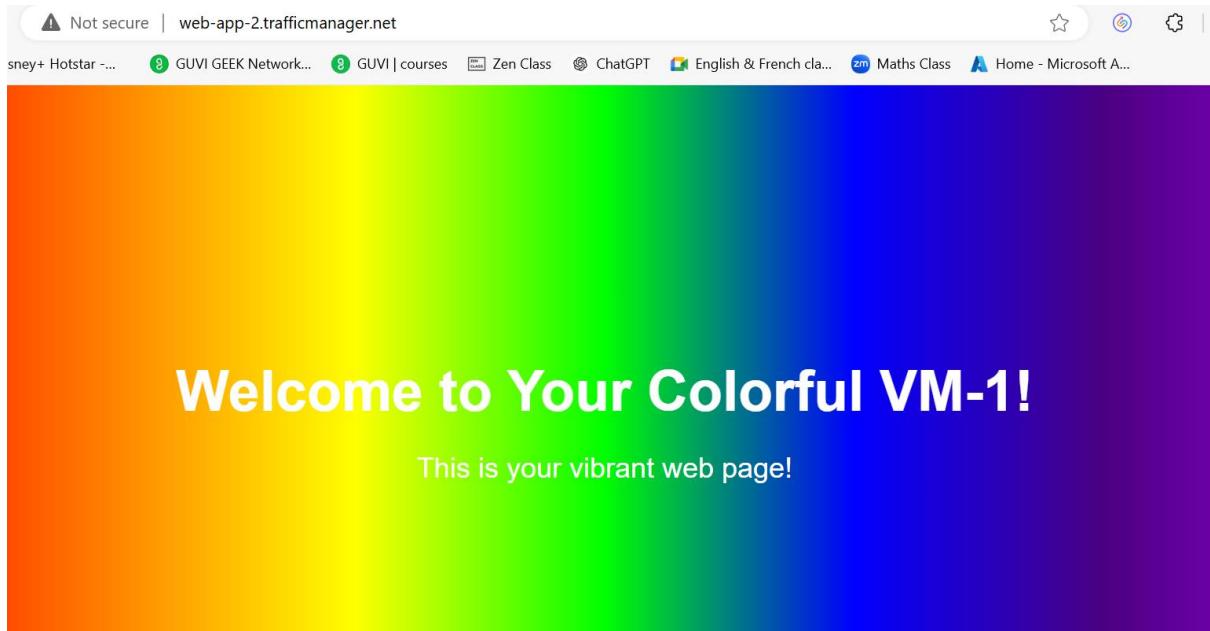
Add

- Wait till the Monitor status turns into “online” from “Checking endpoint”

Name	Status	Monitor status	Type	Priority	...
Endpoint-1	Enabled	Online	External endpoint	1	...
Endpoint-2	Enabled	Online	External endpoint	2	...

- Hit the Traffic Manager URL in the browser to get out output

RESULT:



- Now turn off VM1 to see the traffic pass through Traffic Manager to VM2
- Also once the VM1 is off we can see the Monitor status as “Degraded”

The screenshot shows the Azure portal interface for a virtual machine named "Linux-VM-1". The left sidebar has a "Virtual machine" icon. The main area is titled "Overview". On the left, there is a navigation menu with items like "Activity log", "Access control (IAM)", "Tags", "Diagnose and solve problems", "Connect", "Bastion", "Networking", "Network settings", "Load balancing", and "Application security". The right side shows the "Essentials" section with the following details:

Essentials		JSON View
Resource group	(move)	Operating system
Web-app-RG		Linux
Status	Stopped (deallocated)	Size
Location	East US	Standard B2s (2 vcpus, 4 GiB memory)
Subscription	(move)	Public IP address
Pay-as-you-go		13.82.133.171
Subscription ID	670a5c73-aab7-47c2-a69f-5a2463a525aa	Virtual network/subnet
		Linux-VM-1-vnet/default
DNS name		DNS name
Not configured		Health state
Health state	-	Time created
		25/10/2024, 18:14 UTC

Web-app-2 ...

Traffic Manager profile

Search Enable profile Disable profile Refresh Move Delete profile

Overview

Essentials

Resource group (move) [Web-app-RG](#)
Status Enabled
Subscription (move) [Pay-as-you-go](#)
Subscription ID 670a5c73-aab7-47c2-a69f-5a2463a525aa
Tags (edit) [Add tags](#)

DNS name <http://web-app-2.trafficmanager.net>
Monitor status Degraded
Routing method Priority

Endpoints

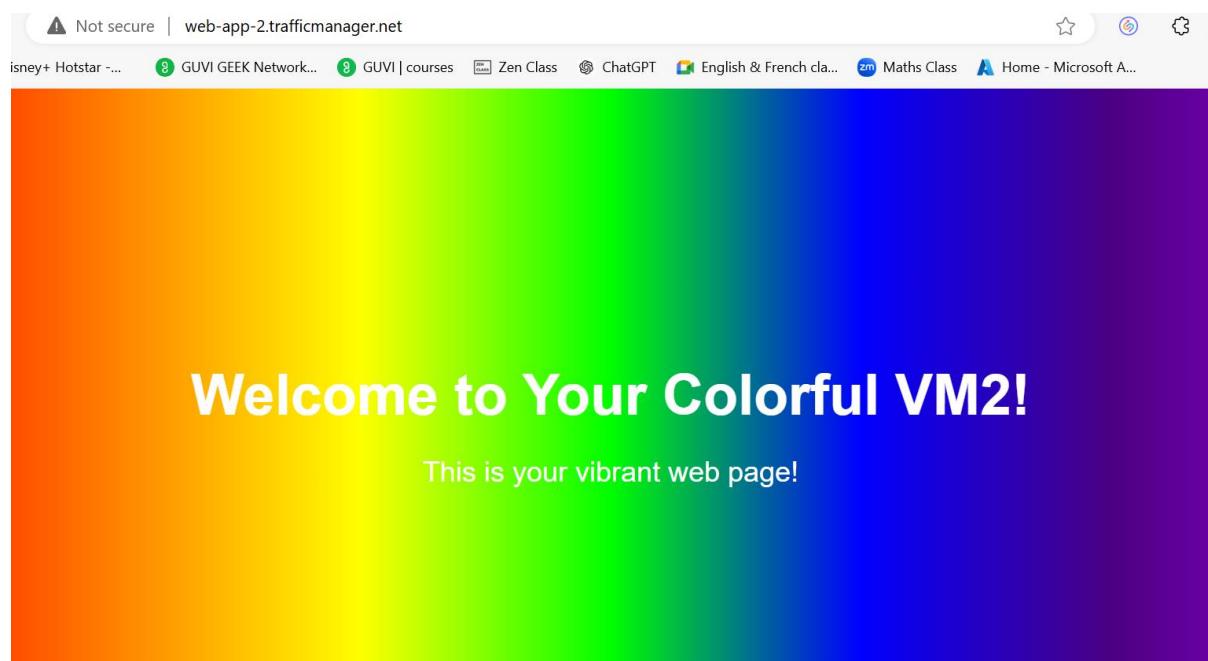
Name	Status	Monitor status	Type	Priority
Endpoint-1	Enabled	Degraded	External endpoint	1
Endpoint-2	Enabled	Online	External endpoint	2

Traffic view

Properties

Locks

[JSON View](#)



- Final step to check the mistake or wrong URL to get the error page

