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.

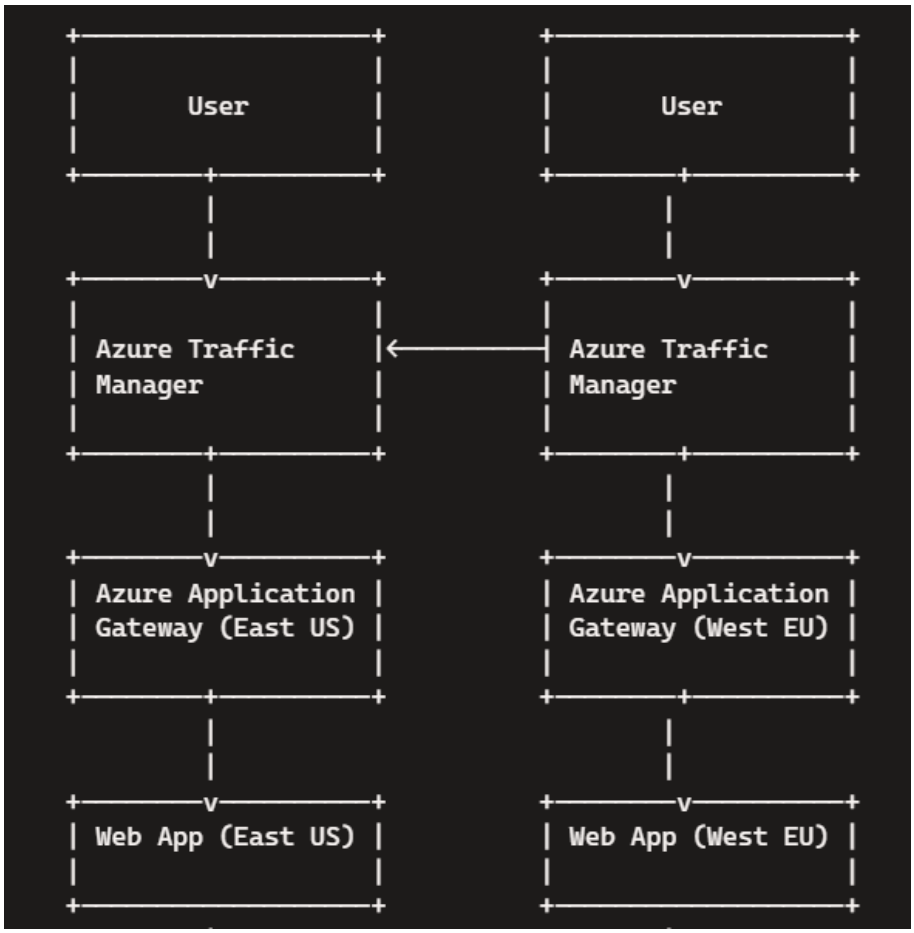
3. Load Balancing Across Regions

- 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 in stances and ensure traffic is only routed to healthy instances.

Diagram:

Here's a simplified diagram to illustrate the architecture

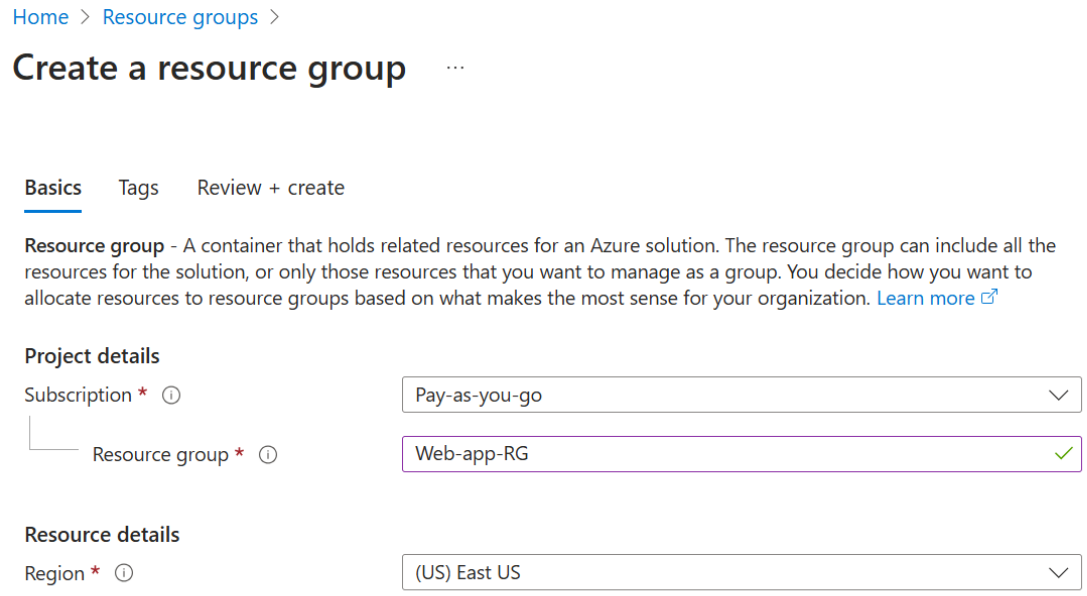


Key Components:

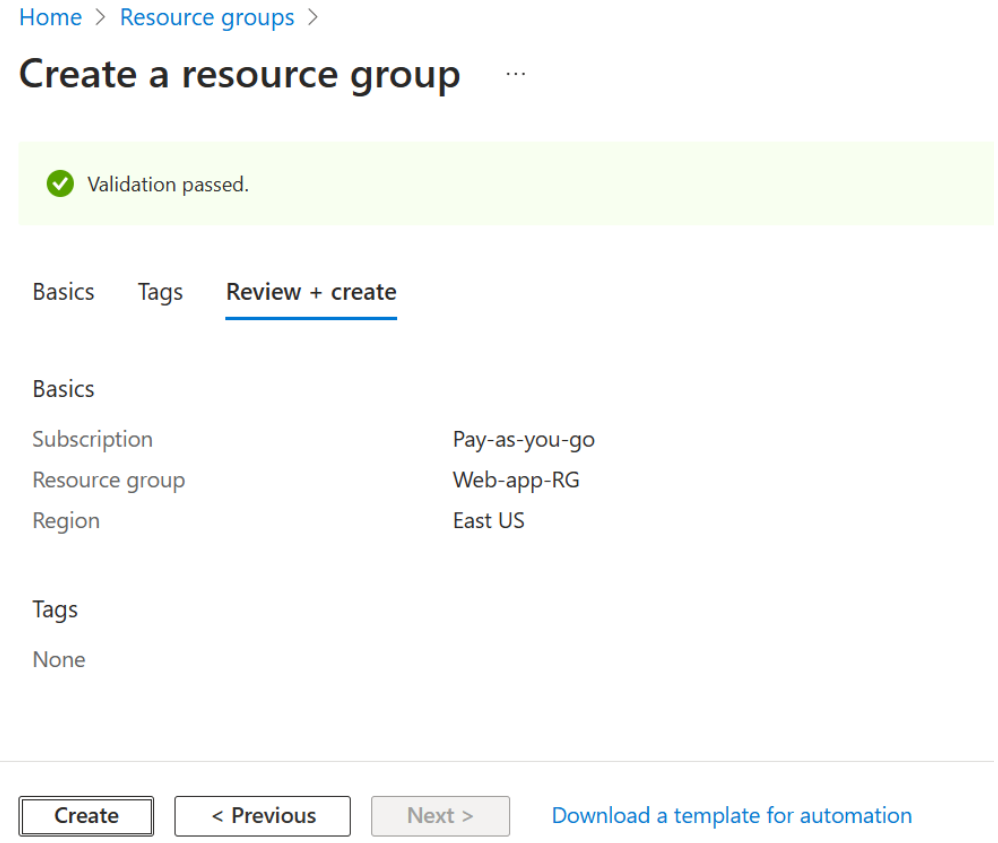
- **Azure Traffic Manager**: Manages DNS-based global load balancing.
- **Azure Application Gateway**: Provides regional load balancing and web application fire wall capabilities.
- **Web Application**: Deployed in multiple regions for high availability.

Procedure:

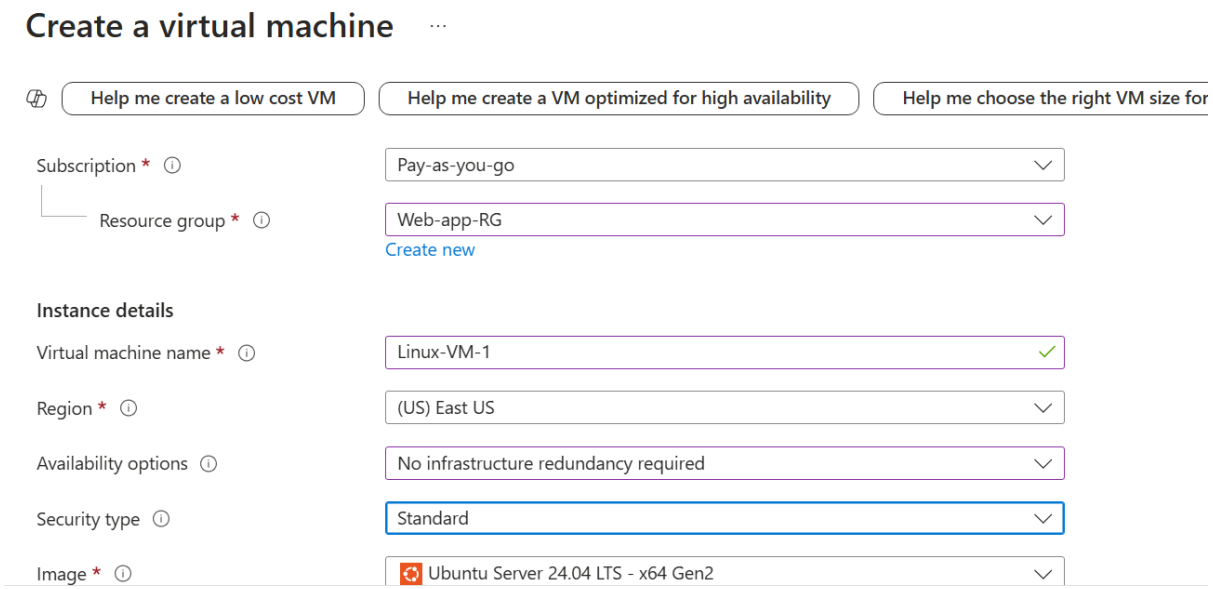
- Login to Azure Portal
- Create a Resource Group

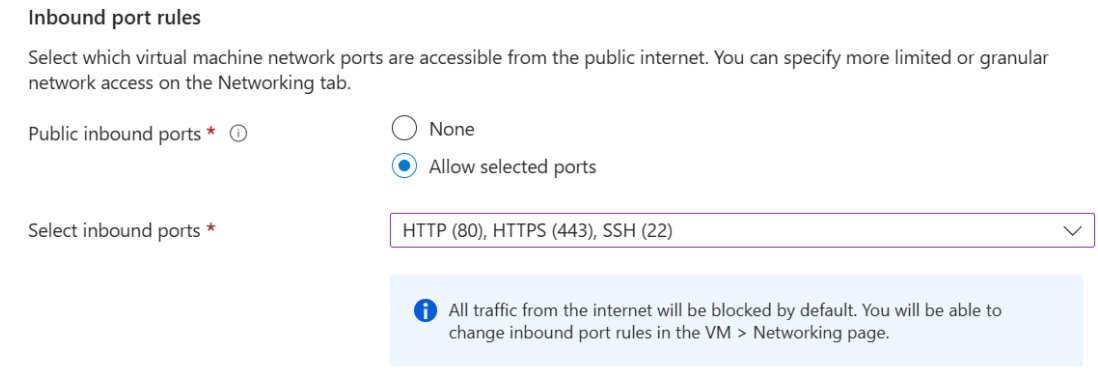


- Skip Tags, Review and Create.

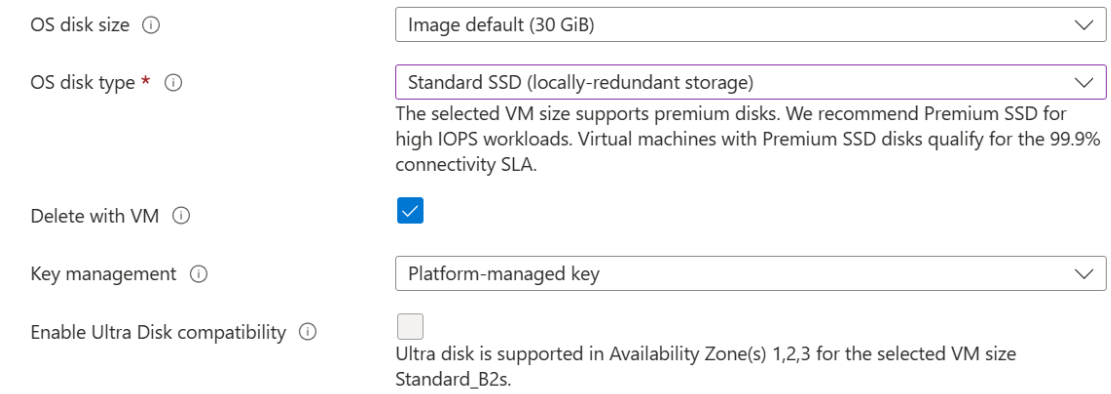


- Create two Virtual Machines in different regions.





Next: Disks



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 ⓘ ☐

RBAC role assignment of Virtual Machine Administrator Login or Virtual Machine

Next: Monitoring

Alerts

Enable recommended alert rules ⓘ ☐

Diagnostics

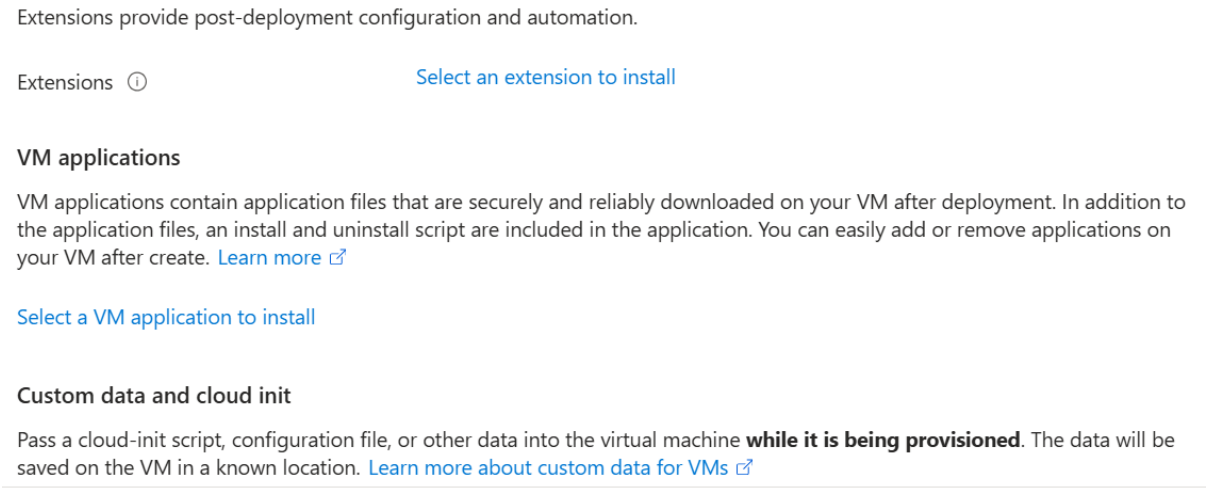
Boot diagnostics ⓘ
- ◉ Enable with managed storage account (recommended)
- ○ Enable with custom storage account
- ○ Disable

Enable OS guest diagnostics ⓘ ☐

Health

Enable application health monitoring ⓘ ☐

Next: Advanced



- 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

```html
<!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>
```

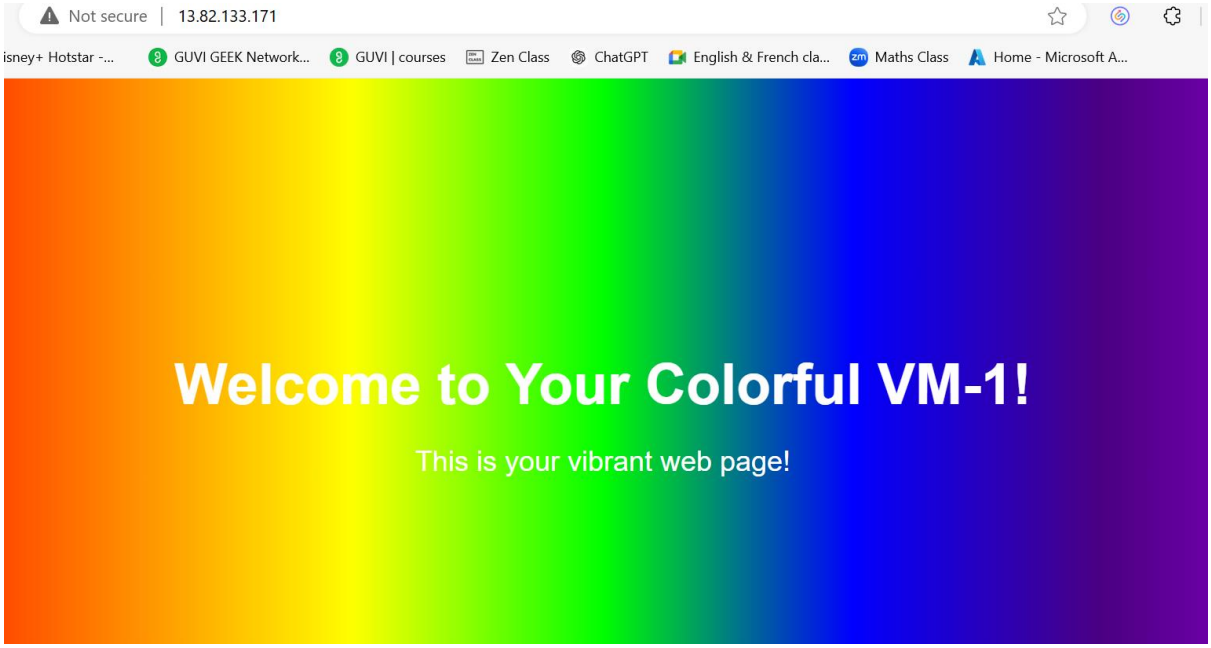
- Click ESC and give :wq! To save and exit the file
- Restart the Apache Service

  sudo systemctl restart apache2

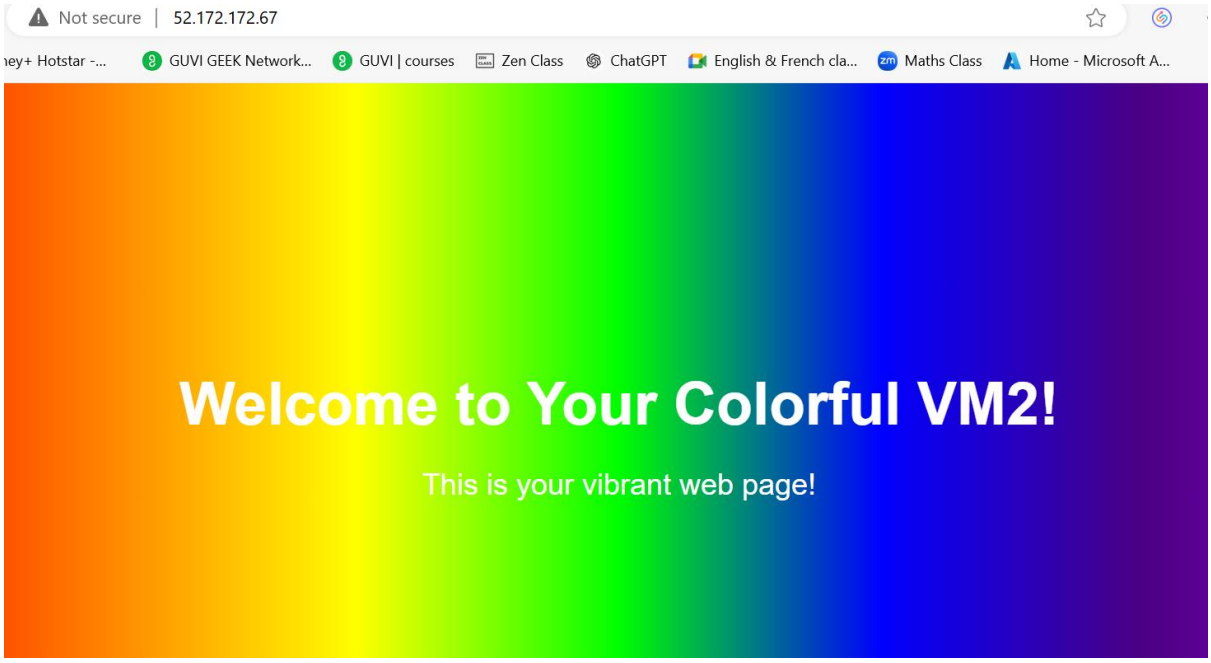
- Now, when you hit your VM's IP address in a browser, you should see a colorful web pag e! 🌈

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 * : Pay-as-you-go

Resource group * : Web-app-RG

Create new

Instance details

Application gateway name * : App-gateway-mywebapp-1

Home > Load balancing | Application Gateway >

Create application gateway ...

Region * : East US

Tier : WAF V2

Enable autoscaling : Yes / No

Minimum instance count * : 0

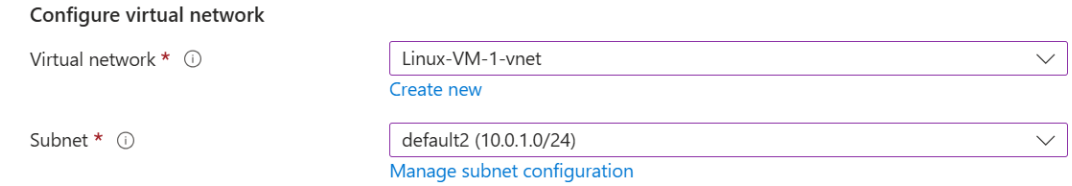
Maximum instance count : 5

Availability zone * : Zones 1, 2, 3

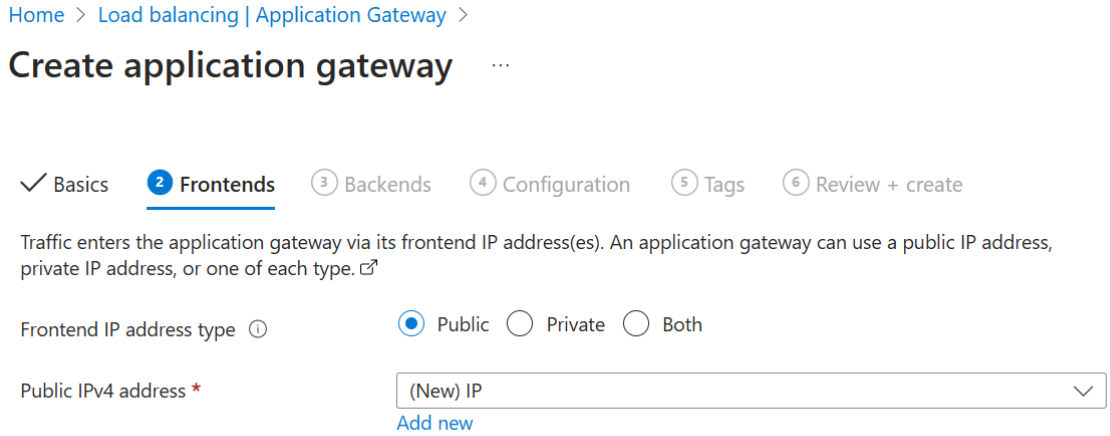
IP address type : IPv4 only / Dual stack (IPv4 & IPv6)

HTTP2 : Disabled / Enabled

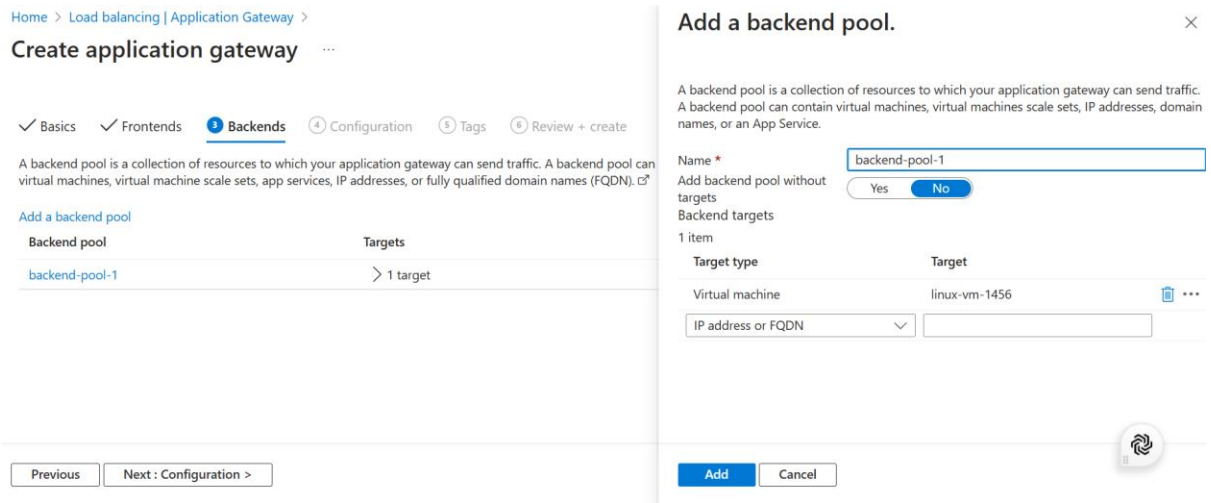
WAF Policy * : (new) WAF-1



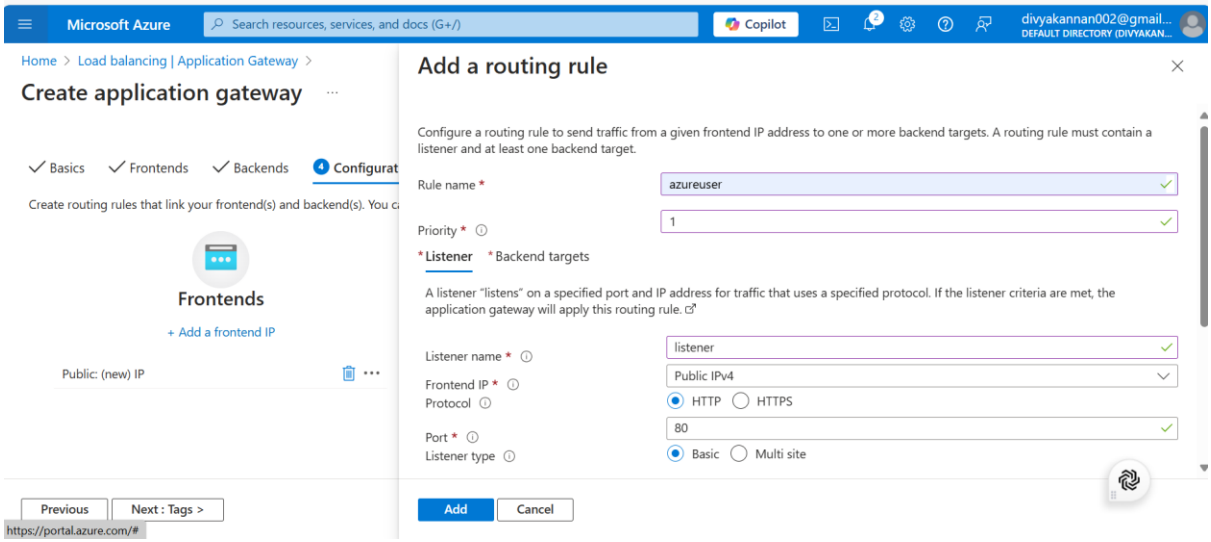
- Next: Frontends



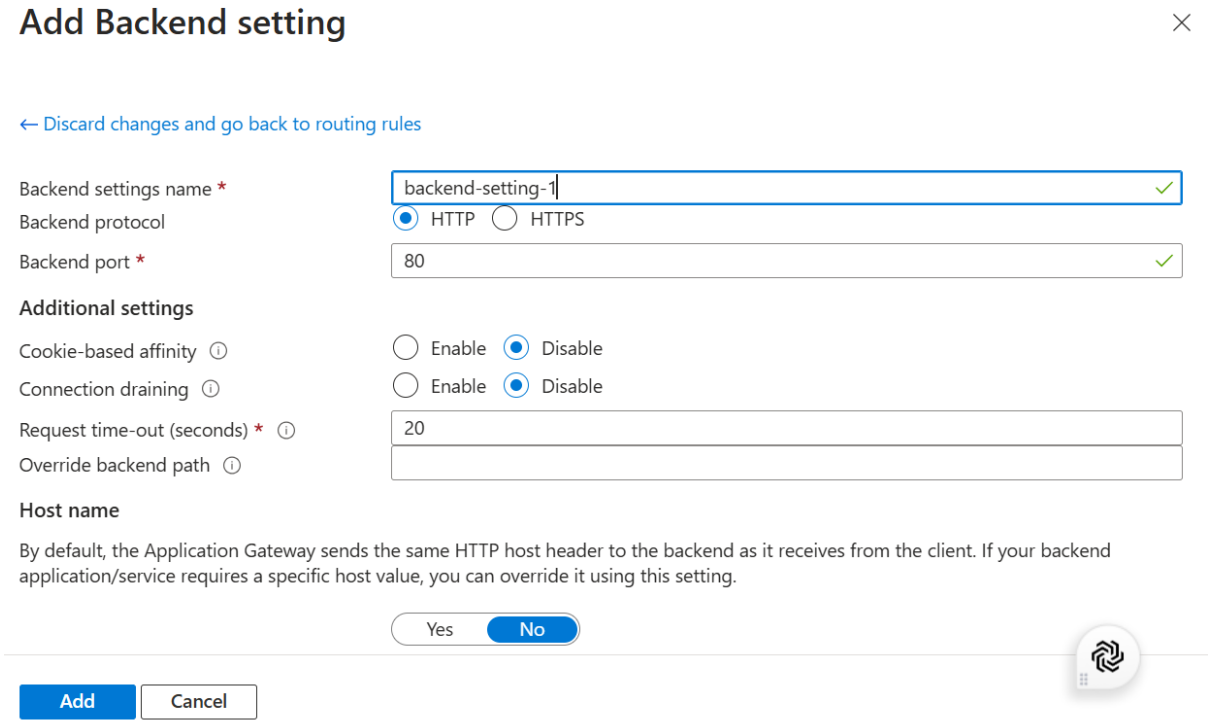
- Next: Backends



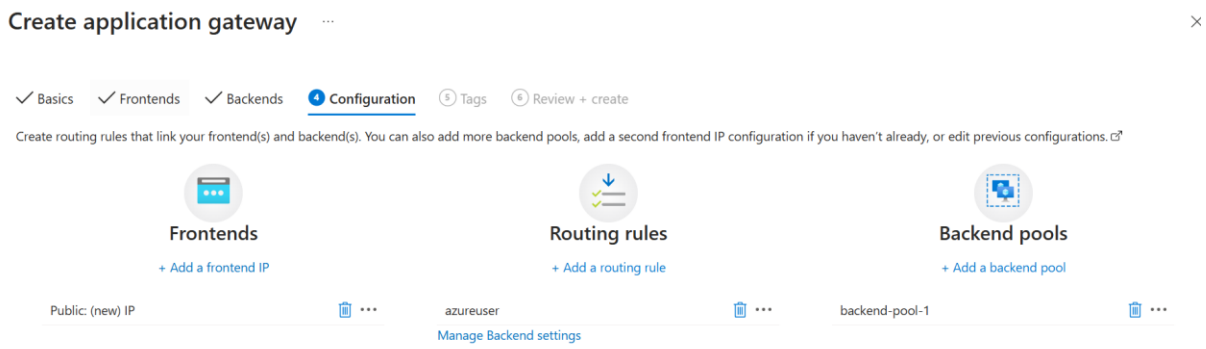
- Next: Configuration
- Click Routing Rule



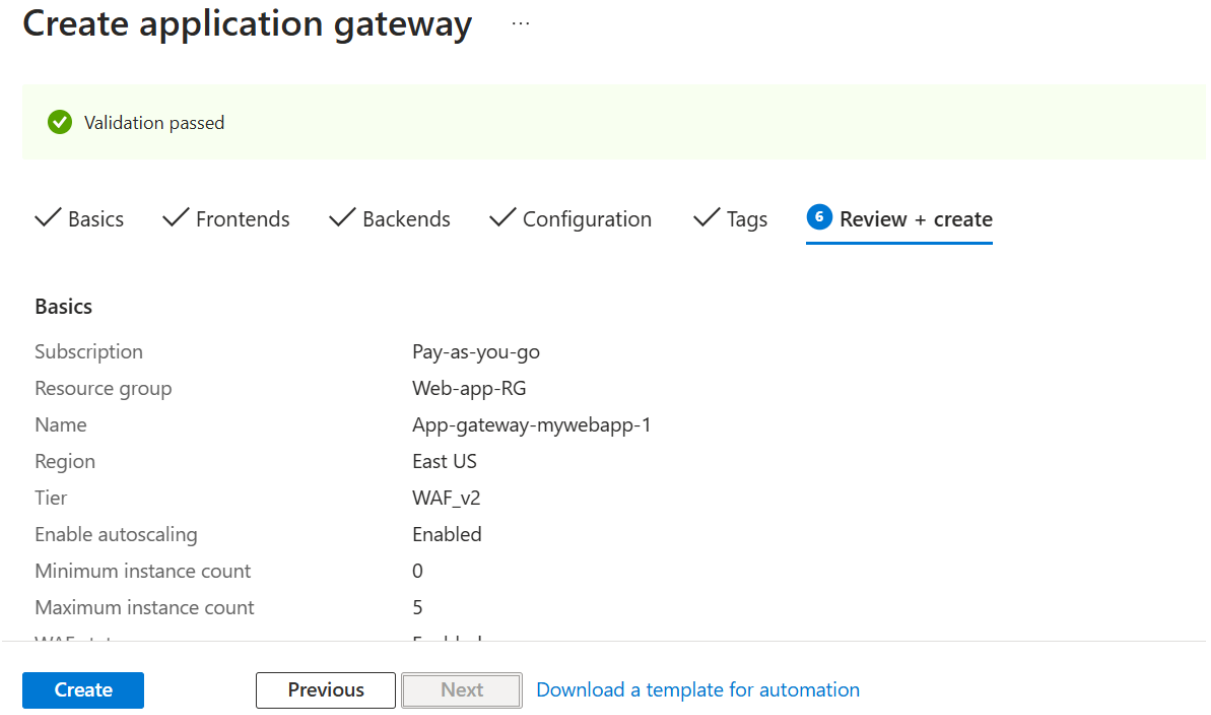
- Need to add Backend Targets too on the same page before clicking add



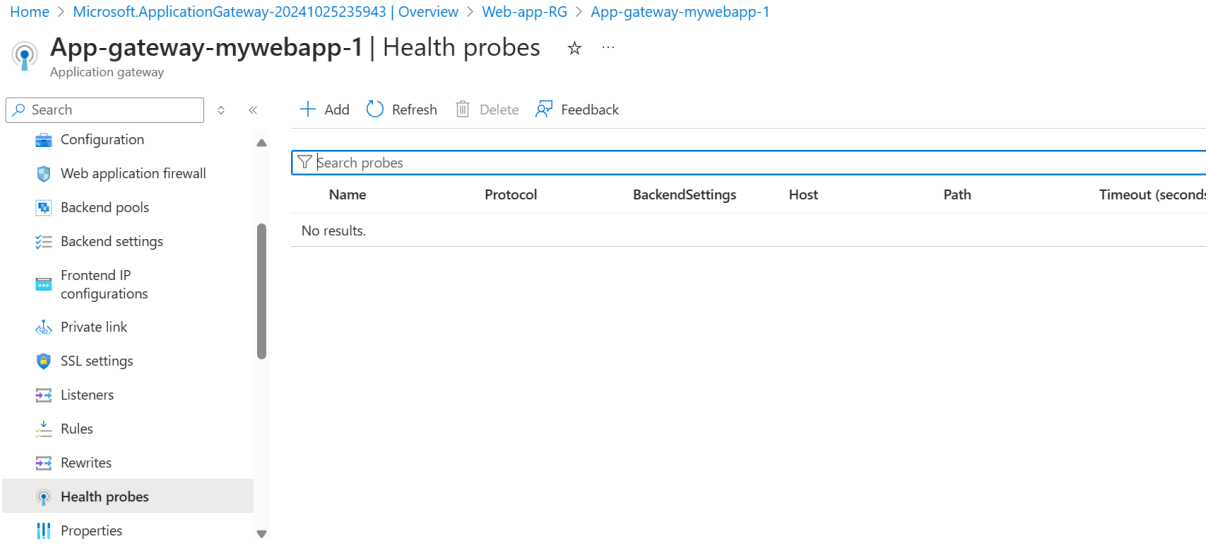
- It should be like this as shown below after adding all three

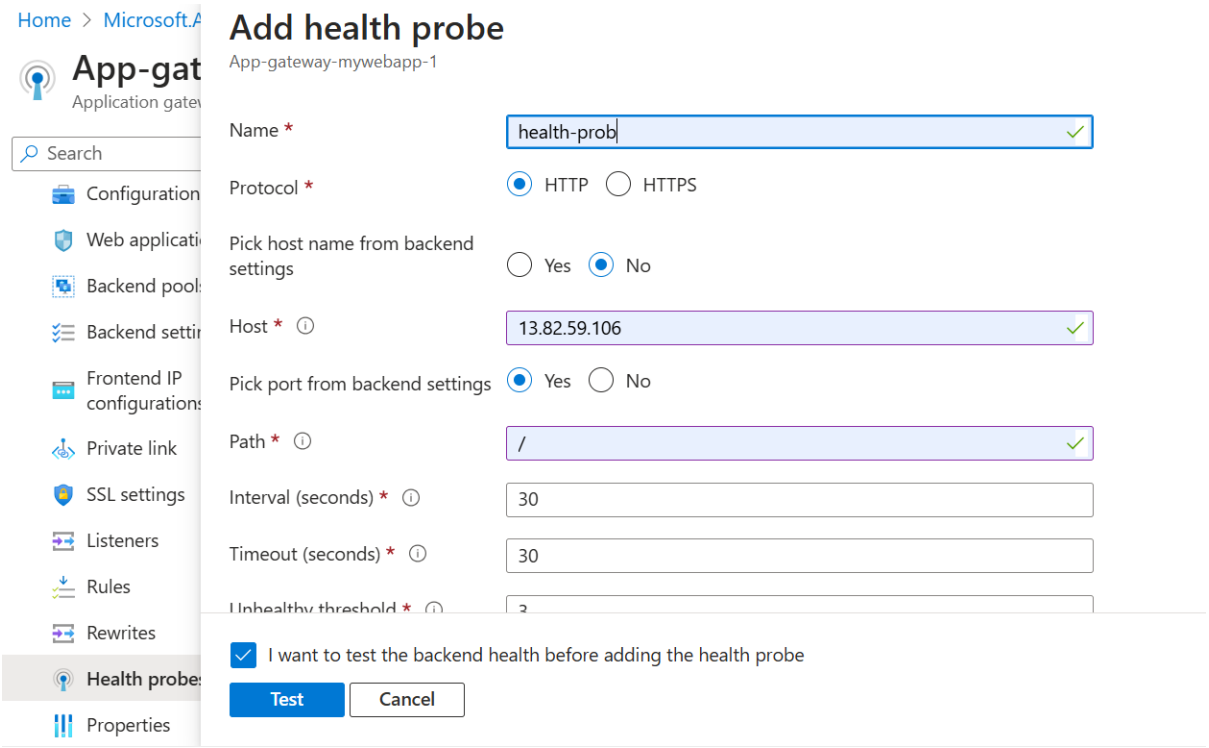


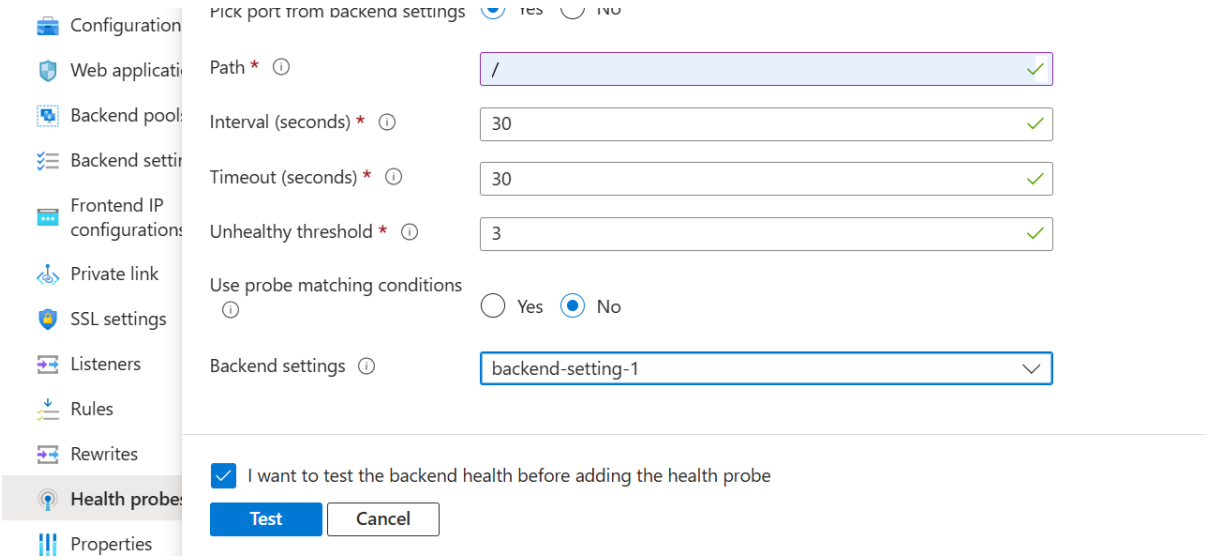
- Skip Tags
- Validate, Review and Create
- Repeat the same steps to create another Application Gateway for VM2 as mentioned Regions respectively



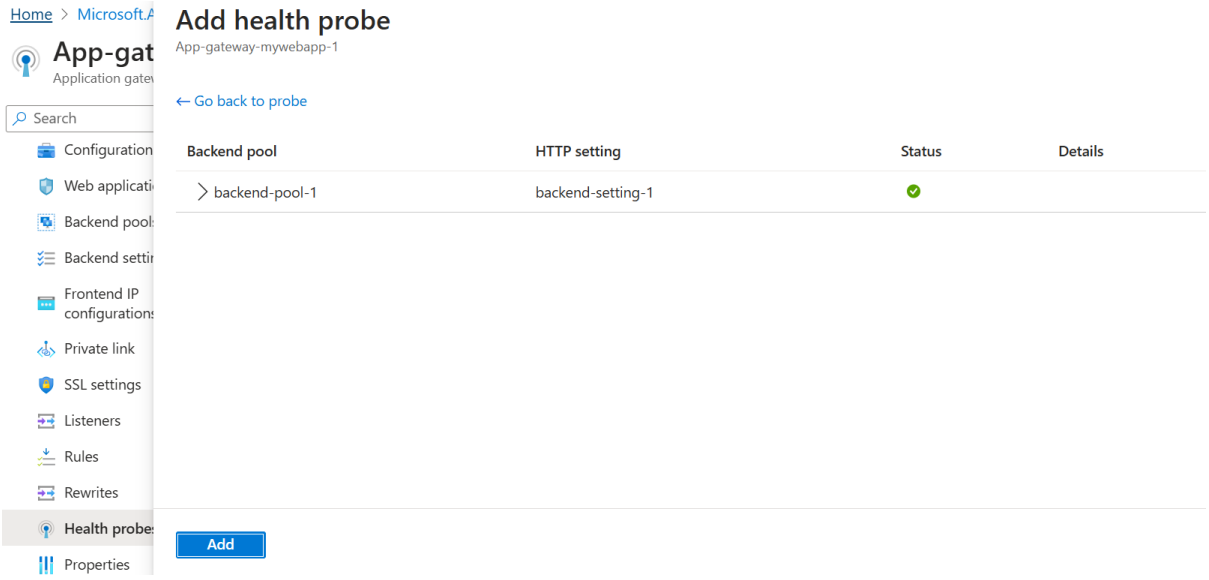
- After deploying Application Gateway, Go to settings -> health-probs -> add


Home > Microsoft.ApplicationGateway-20241025235943 | Overview > Web-app-RG > App-gateway-mywebapp-1
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
Search probes
Name
Protocol
BackendSettings
Host
Path
Timeout (seconds
No results.

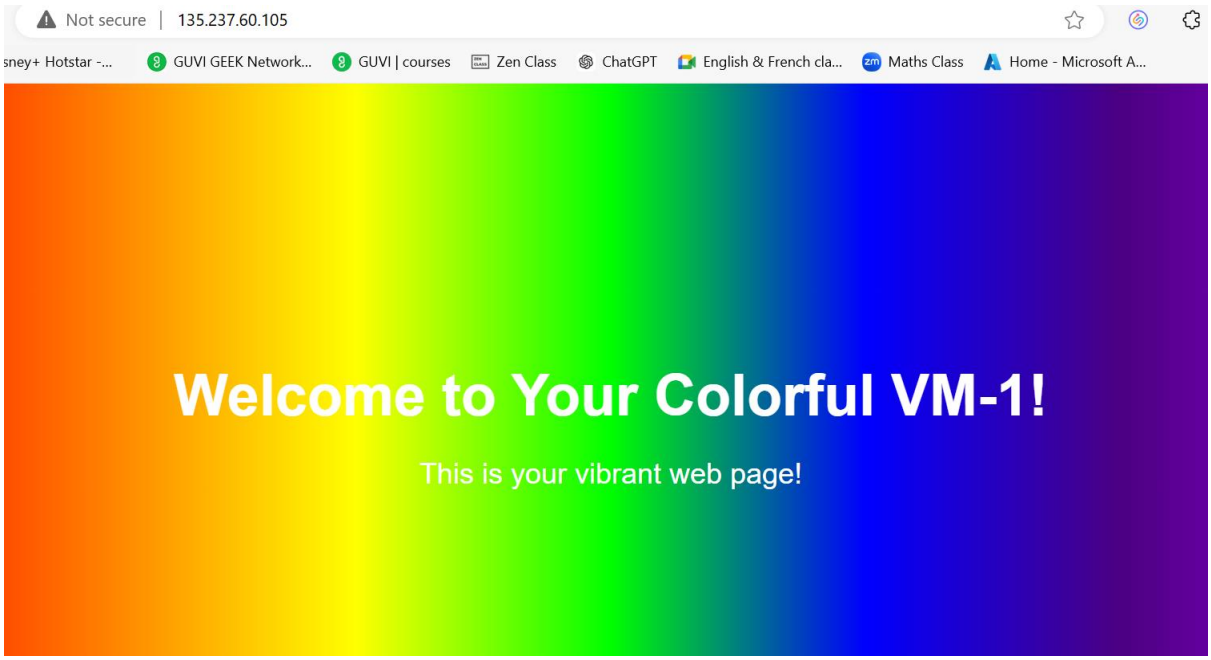

Home > Microsoft.A
App-gat
Application gate
Search
Configuration
Web applicati
Backend pool
Backend setti
Frontend IP configuration
Private link
SSL settings
Listeners
Rules
Rewrites
Health probe
Properties
Add health probe
App-gateway-mywebapp-1
Name *
health-prob
Protocol *
HTTP
HTTPS
Pick host name from backend settings
Yes
No
Host *
13.82.59.106
Pick port from backend settings
Yes
No
Path *
/
Interval (seconds) *
30
Timeout (seconds) *
30
I want to test the backend health before adding the health probe
Test
Cancel

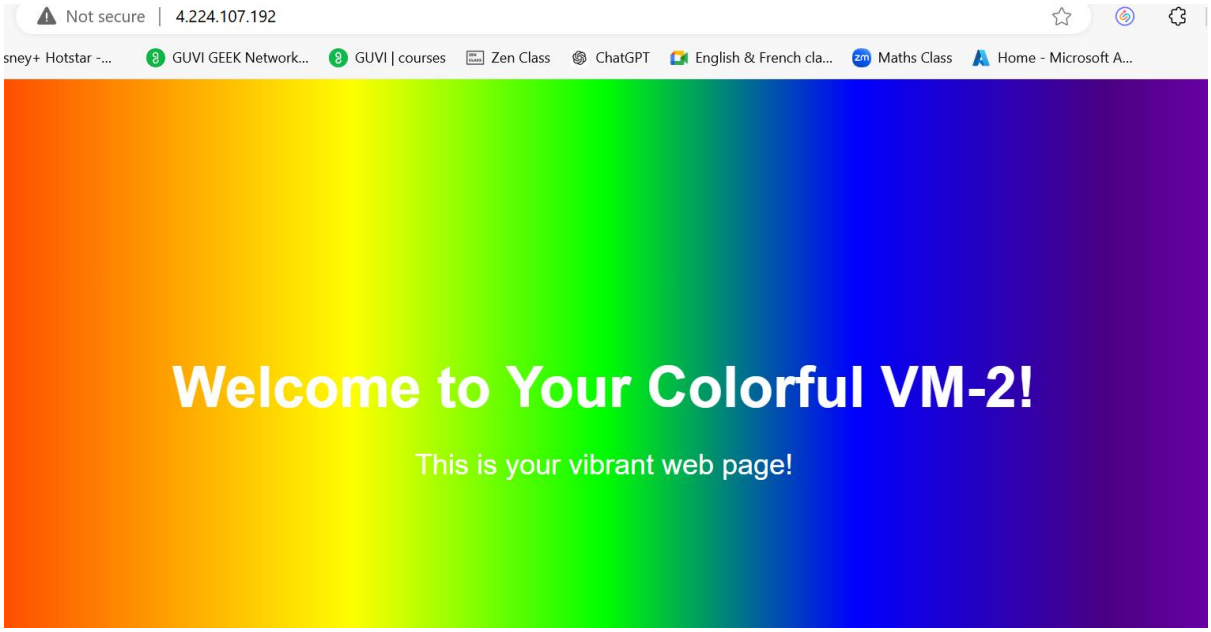


- Test and the result should be like as below, then Add

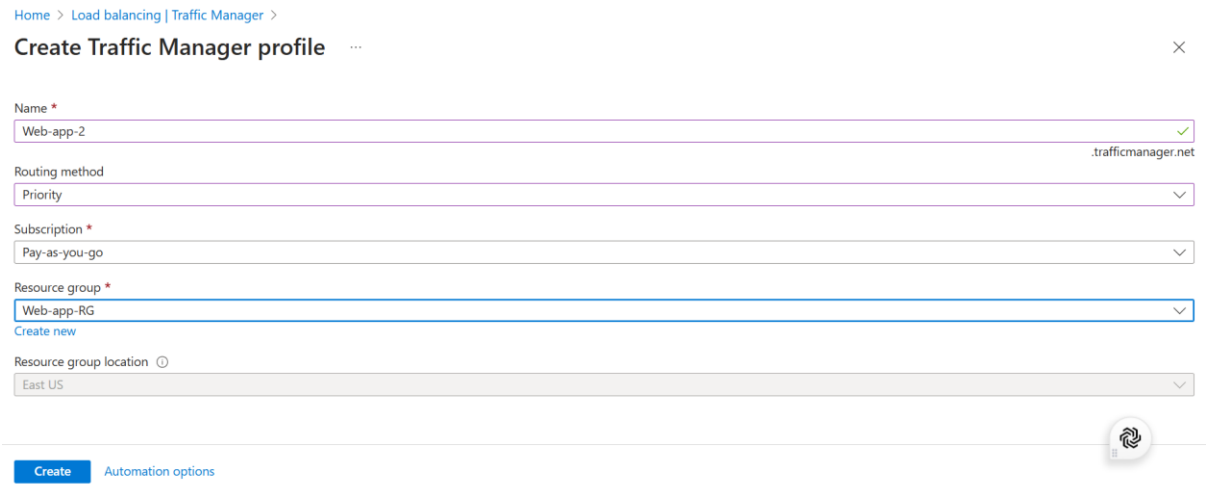


- Now, hit the Application Gateway Ip’s for both 1 and 2 in the browser to view the result

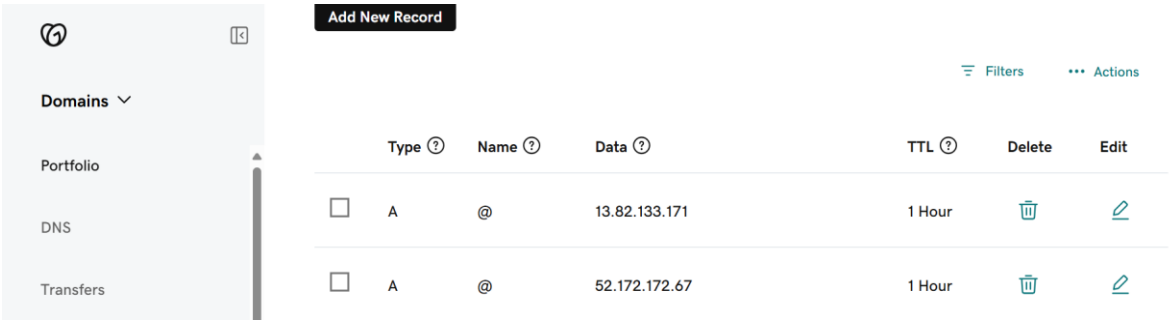




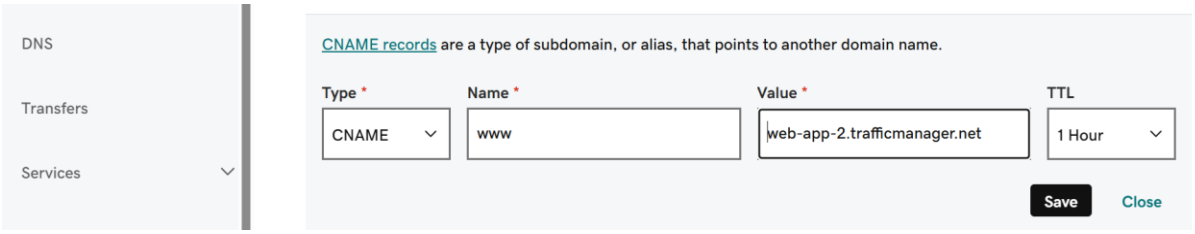
- Create Traffic Manager Profile



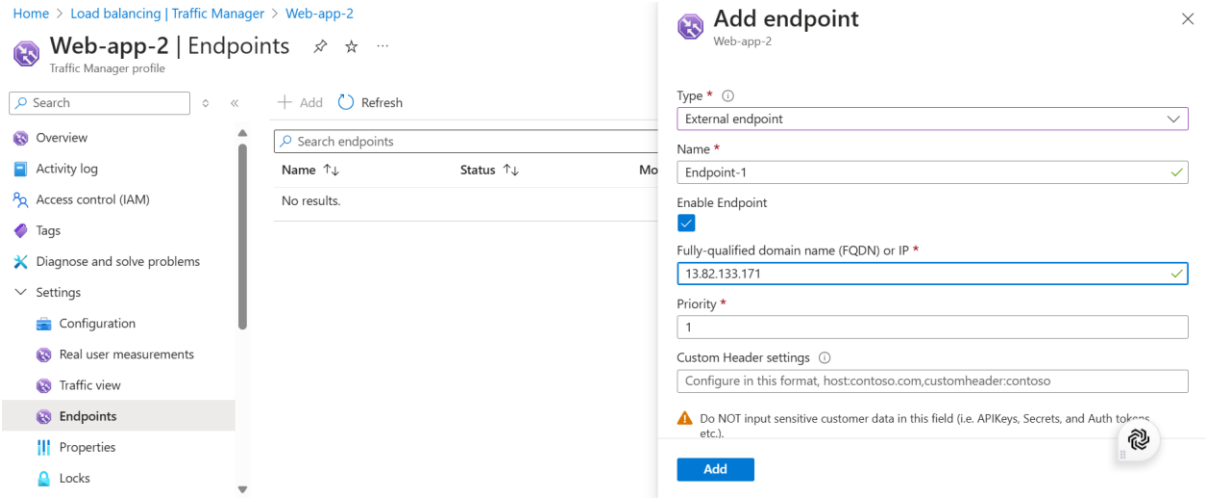
- Once it's created, Need to add both the IPs and Traffic Manager URL in the DNS
- Type -> A, Data -> IP address -> Save

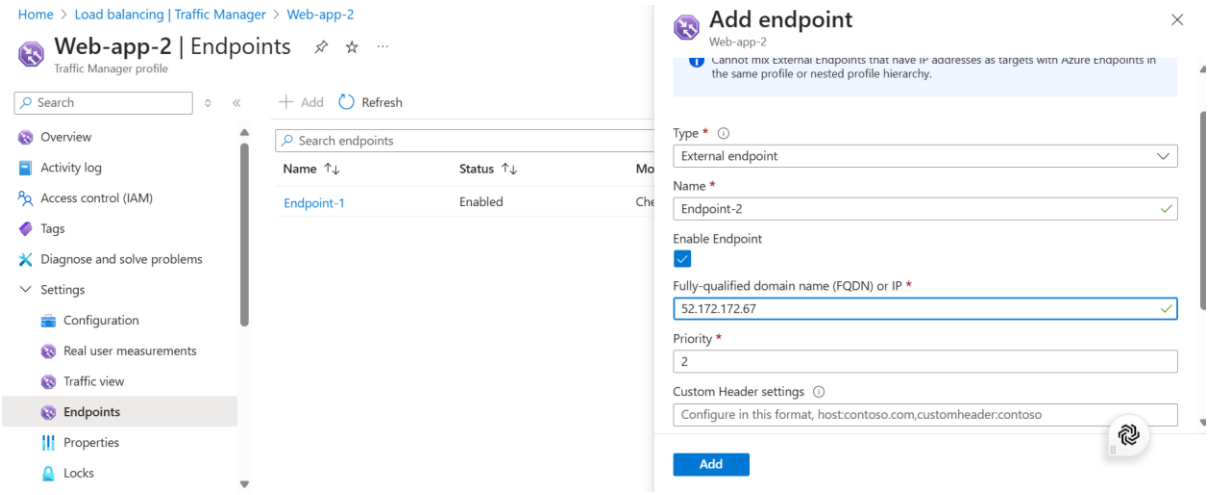


- For Traffic Manager URL Type -> CNAME, Name -> WWW, -> Value -> Traffic Manager URL -> Save

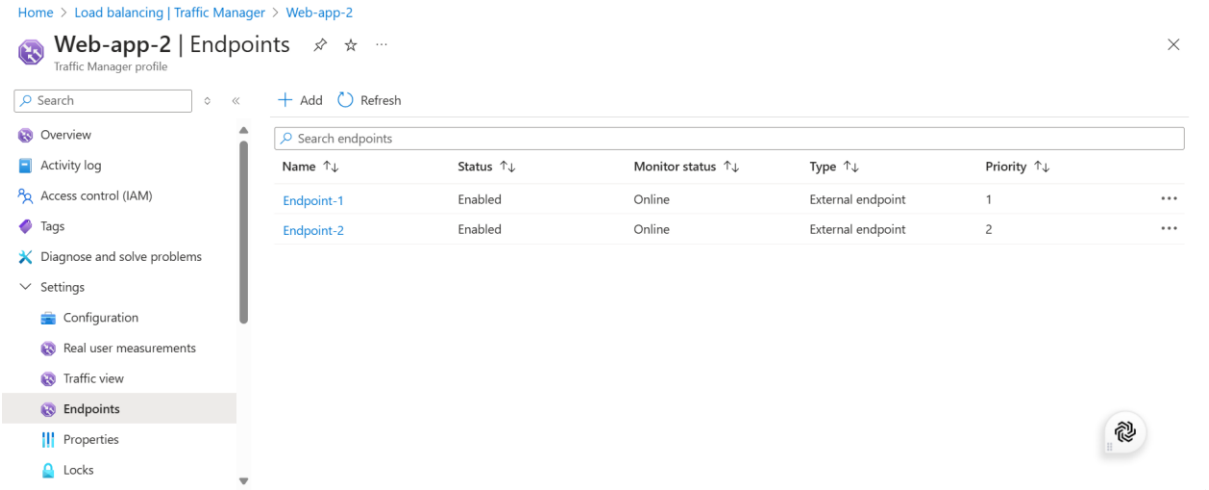


- Once the DNS values has been added, Go to Endpoints and add both the IPs to it



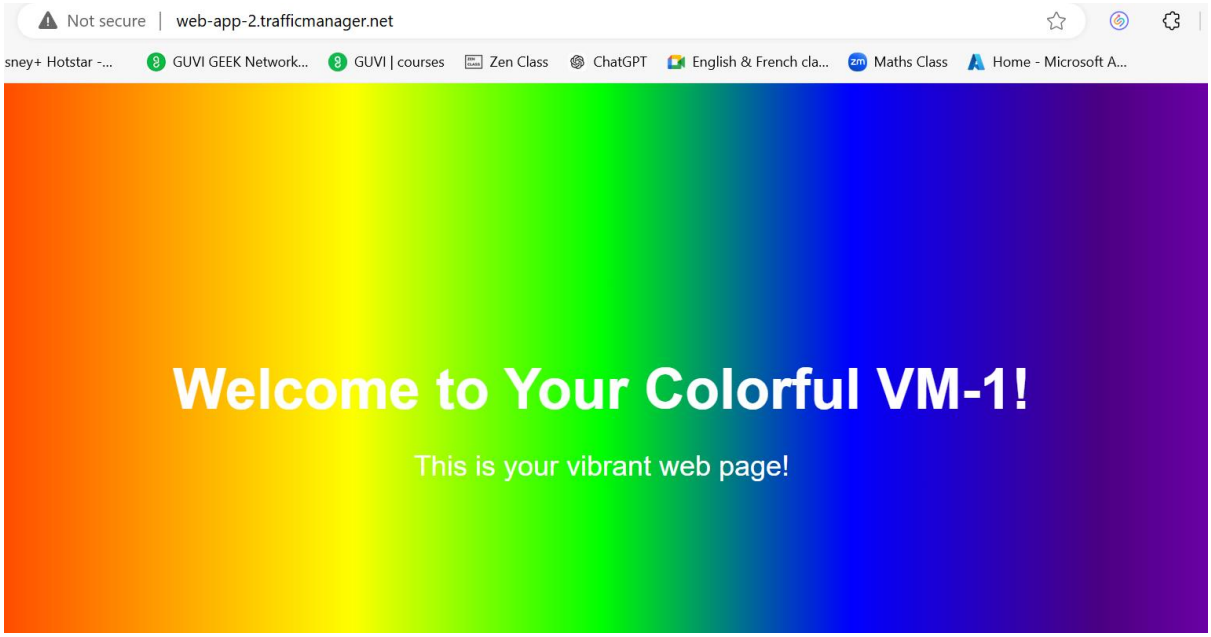


- Wait till the Monitor status turns into “online” from “Checking endpoint”

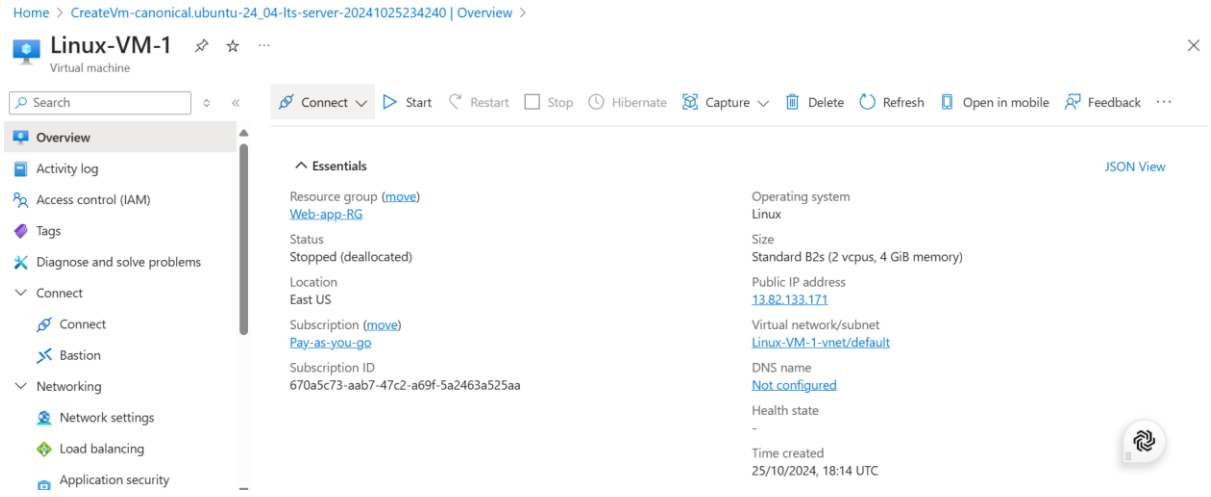


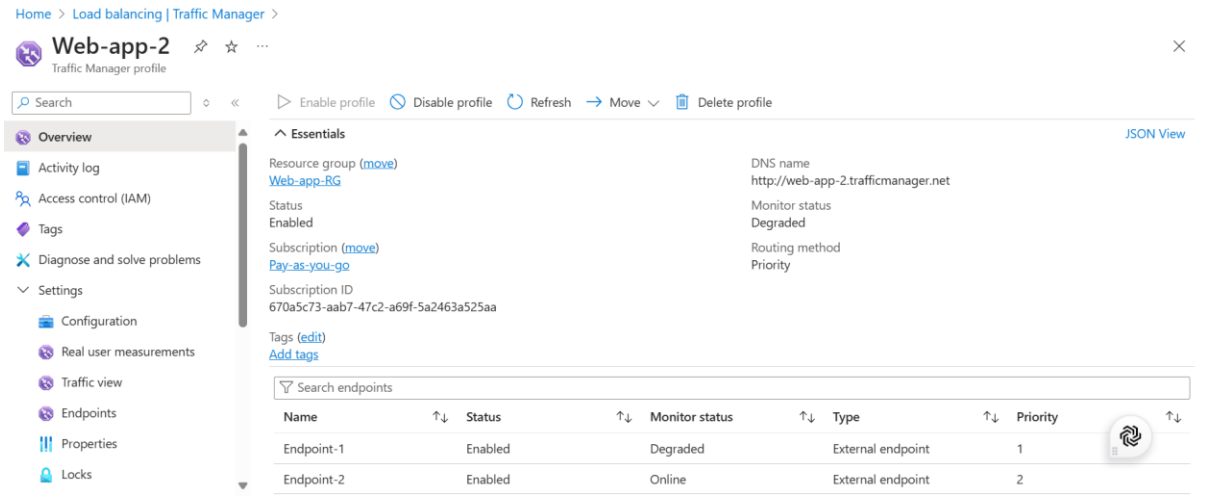
- Hit the Traffic Manager URL in the browser to get out output

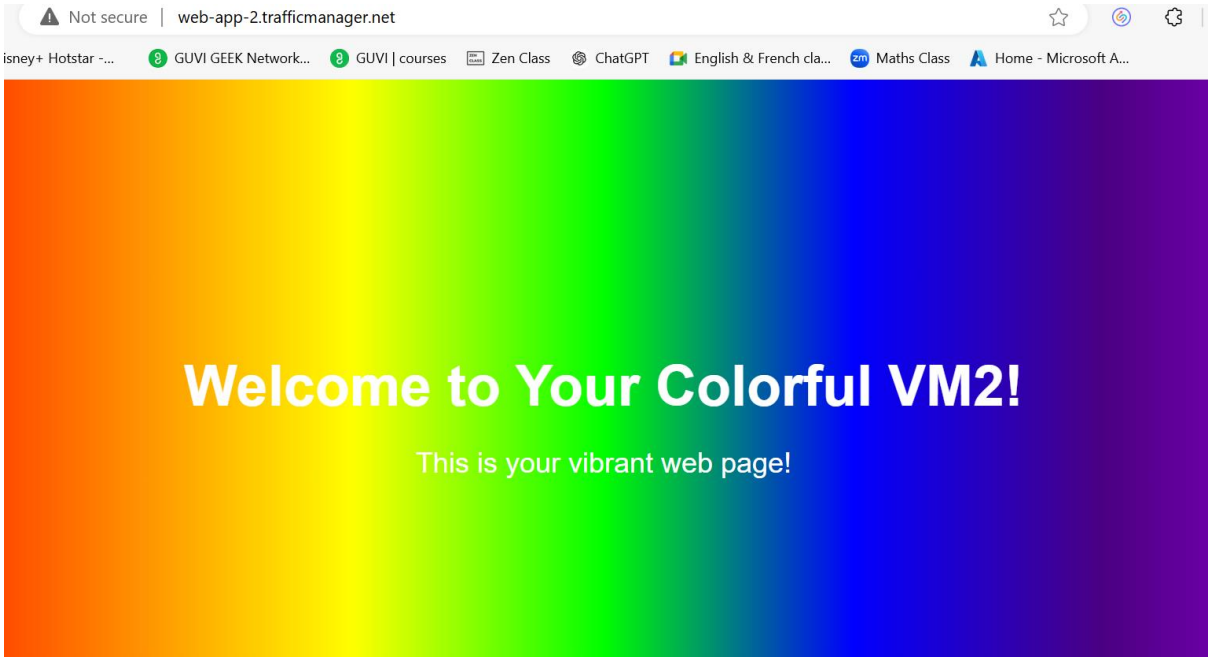
RESULT:



- 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”




Home > Load balancing | Traffic Manager >
Web-app-2
Traffic Manager profile
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Configuration
Real user measurements
Traffic view
Endpoints
Properties
Locks
Enable profile
Disable profile
Refresh
Move
Delete profile
Essentials
JSON View
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
Search endpoints
Name
Status
Monitor status
Type
Priority
Endpoint-1
Enabled
Degraded
External endpoint
1
Endpoint-2
Enabled
Online
External endpoint
2


Not secure
web-app-2.trafficmanager.net
isney+ Hotstar -...
GUVI GEEK Network...
GUVI | courses
Zen Class
ChatGPT
English & French cla...
Maths Class
Home - Microsoft A...
Welcome to Your Colorful VM2!
This is your vibrant web page!

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