



## **Placement Empowerment Program**

### ***Cloud Computing and DevOps Centre***

Implement DNS for Your Application: Set up a DNS record to map your web application's IP or load balancer to a domain name.

Name: Gopinath M

Department: ADS

## Introduction

In cloud computing, establishing a proper **Domain Name System (DNS)** configuration is essential for ensuring that applications are accessible over the internet. AWS offers **Route 53**, a highly available and scalable DNS web service, which allows users to manage domain names and point them to AWS resources like EC2 instances. This Proof of Concept (PoC) demonstrates the process of creating and configuring a DNS record in **AWS Route 53**, pointing it to a web server hosted on an **EC2 instance**, thus making the web application accessible via a custom domain name.

## Overview

This PoC involves:

1. **Launching an EC2 instance** to serve a web application.
2. **Setting up a web server** (Apache or Nginx) on the EC2 instance to host the application.
3. **Creating a hosted zone** in AWS Route 53 for a custom domain (e.g., myapp.local).
4. **Configuring an A record** in Route 53 to map the domain to the EC2 instance's public IP.
5. **Modifying the hosts file** on a local machine to test the custom domain name before making it publicly available.
6. **Testing the configuration** by accessing the application using the custom domain name.

# Objective

The main objectives of this PoC are:

- 1. Familiarize with Route 53 DNS configuration:** Understand how to use AWS Route 53 to manage domain names and map them to cloud resources.
- 2. Learn EC2 setup and configuration:** Gain hands-on experience in launching an EC2 instance and configuring a web server to serve a web application.
- 3. Enable custom domain access:** Configure a custom domain name to point to the EC2 instance, ensuring that the web application is easily accessible through the domain.
- 4. Test and verify the configuration:** Ensure that the domain correctly points to the EC2 instance by testing it in a browser and troubleshooting any issues.

# Importance

- 1. Improves Web Access:** Provides a user-friendly way to access applications via a custom domain.
- 2. Scalable DNS Solution:** Route 53 offers scalable and reliable DNS management.
- 3. Hands-on Cloud Skills:** Essential for cloud architects and developers to work with AWS services.
- 4. Cost-Effective Testing:** Utilizes AWS Free Tier for testing without incurring costs.

# Step-by-Step Overview

## Step 1:

1. Go to [AWS Management Console](#).
2. Enter your username and password to log in.

## Step 2:

Launch an instance named **route instance** .

### **Configure Security Group:**

Add a **new security group** with a rule for **HTTP** (port 80) and **SSH** (port 22).

For HTTP, set the source to **Anywhere (0.0.0.0/0)** to allow access via the web.

For SSH, set the source to your **IP** (recommended for security), or use **Anywhere** for now.

**Create a Key Pair** (or use an existing one) and download the key file (.pem).

Review and click **Launch**.

EC2 > Security Groups > sg-091ff45e68e5f742f - launch-wizard-29

Dashboard  
EC2 Global View  
Events

▼ Instances  
Instances  
Instance Types  
Launch Templates  
Spot Requests  
Savings Plans  
Reserved Instances  
Dedicated Hosts  
Capacity Reservations

▼ Images  
AMIs  
AMI Catalog

▼ Elastic Block Store  
Volumes  
Snapshots  
Lifecycle Manager

▼ Network & Security  
Security Groups  
Elastic IPs

### sg-091ff45e68e5f742f - launch-wizard-29

Actions

**Details**

<b>Security group name</b> launch-wizard-29	<b>Security group ID</b> sg-091ff45e68e5f742f	<b>Description</b> launch-wizard-29 created 2025-02-09T18:07:45.652Z	<b>VPC ID</b> vpc-0f36f0944c12862e5
<b>Owner</b> 343218194491	<b>Inbound rules count</b> 2 Permission entries	<b>Outbound rules count</b> 1 Permission entry	

**Inbound rules** | Outbound rules | Sharing - new | VPC associations - new | Tags

**Inbound rules (2)** Manage tags Edit inbound rules

Search

<input type="checkbox"/>	Name	Security group rule ID	IP version	Type	Protocol	Port range	Score
<input type="checkbox"/>	-	sgr-08cd3a5747836e47	IPv4	SSH	TCP	22	0.0
<input type="checkbox"/>	-	sgr-0fe112bc7cae9defb	IPv4	HTTP	TCP	80	0.0

## Step 3:

Click the 'Connect' option on your launched instance, go to the SSH client section, and copy the command provided under the 'Example' section.

EC2 > Instances > i-004154969b120bb8c > Connect to instance

### Connect to instance

Connect to your instance i-004154969b120bb8c (route instance) using any of these options

EC2 Instance Connect | Session Manager | **SSH client** | EC2 serial console

**Instance ID**  
i-004154969b120bb8c (route instance)

1. Open an SSH client.
2. Locate your private key file. The key used to launch this instance is newkey.pem
3. Run this command, if necessary, to ensure your key is not publicly viewable.  
chmod 400 "newkey.pem"
4. Connect to your instance using its Public DNS:  
ec2-52-91-79-69.compute-1.amazonaws.com

Example:  
ssh -i "newkey.pem" ec2-user@ec2-52-91-79-69.compute-1.amazonaws.com

Note: In most cases, the guessed username is correct. However, read your AMI usage instructions to check if the AMI owner has changed the default AMI username.

Cancel

Open PowerShell, navigate to the 'Downloads' directory where the downloaded key pair is located using the **cd Downloads** command

Paste the command copied from the EC2 Connect's SSH client section, replace the key pair name with your downloaded key (e.g., new.pem), press Enter, and type 'yes' when prompted.

```
PS C:\Users\Hi> cd downloads  
PS C:\Users\Hidownloads> ssh -i "newkey.pem" ec2-user@ec2-52-91-79-69.compute-1.amazonaws.com  
The authenticity of host 'ec2-52-91-79-69.compute-1.amazonaws.com [52.91.79.69]' can't be established.  
ED25519 key fingerprint is SHA256:V4SUI93qczBAzHQxXWzd0m5epjEoSo0SFhgkDx0kw.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added 'ec2-52-91-79-69.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
```

The screenshot shows a Windows Command Prompt session where a user navigates to a directory named 'downloads'. They attempt to establish an SSH connection to an AWS EC2 instance at IP address 52.91.79.69 using a private key file named 'newkey.pem'. The system prompts them about the authenticity of the host's ED25519 key fingerprint. After confirming they wish to proceed ('yes'), it warns that the host has been permanently added to the list of known hosts. Below the command prompt output, there is a stylized ASCII art logo consisting of several rows of tilde (~), hash (#), and backslash (\) symbols arranged to form a tree-like or branching shape. To the right of this logo, the text 'Amazon Linux 2023' is displayed, followed by the URL '<https://aws.amazon.com/linux/amazon-linux-2023>'.

#\_ Amazon Linux 2023  
~ ~ \#####  
~~ ~ \####|  
~~ ~ \|#/ ---  
~~~~ V ~ '~>  
~~~~  
~~ . \_'  
/\_ /'\_

<https://aws.amazon.com/linux/amazon-linux-2023>

## Step 5:

## Install Apache :

```
sudo yum install httpd -y
```

```
[ec2-user@ip-172-31-82-55 ~]$ sudo yum install httpd -y
```

## Step 6:

## Start Apache:

**sudo systemctl start httpd Make**

## Apache start on boot:

```
sudo systemctl enable httpd
```

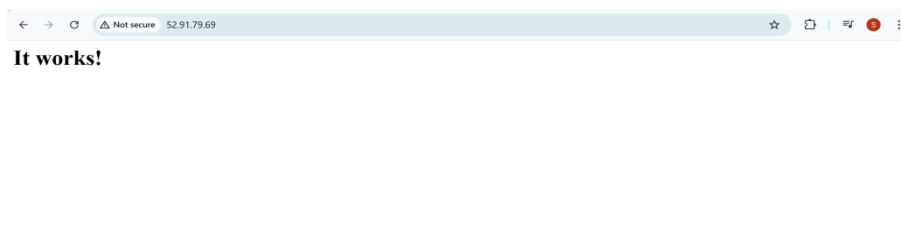
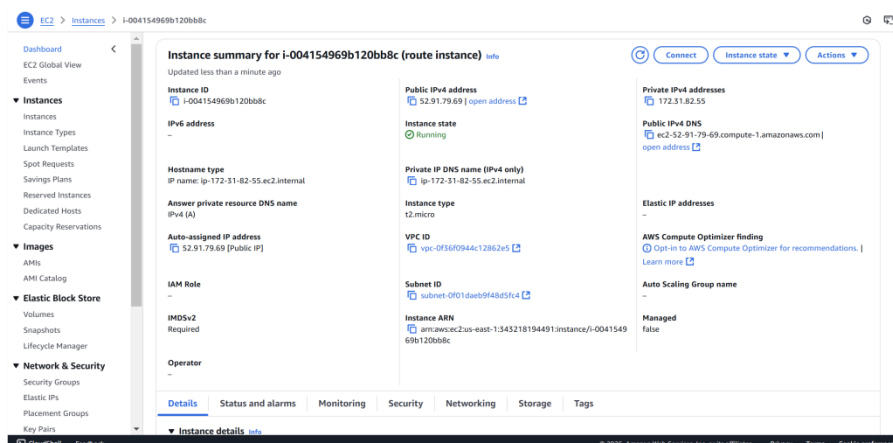
```
[ec2-user@ip-172-31-82-55 ~]$ sudo systemctl start httpd
[ec2-user@ip-172-31-82-55 ~]$ sudo systemctl enable httpd
```

## Step 7:

### Verify Apache is running:

In your browser, enter the **EC2 public IP** (e.g., `http://<your-ec2public-ip>`).

You should see the **Apache default page**. This means your EC2 instance is set up to serve websites.

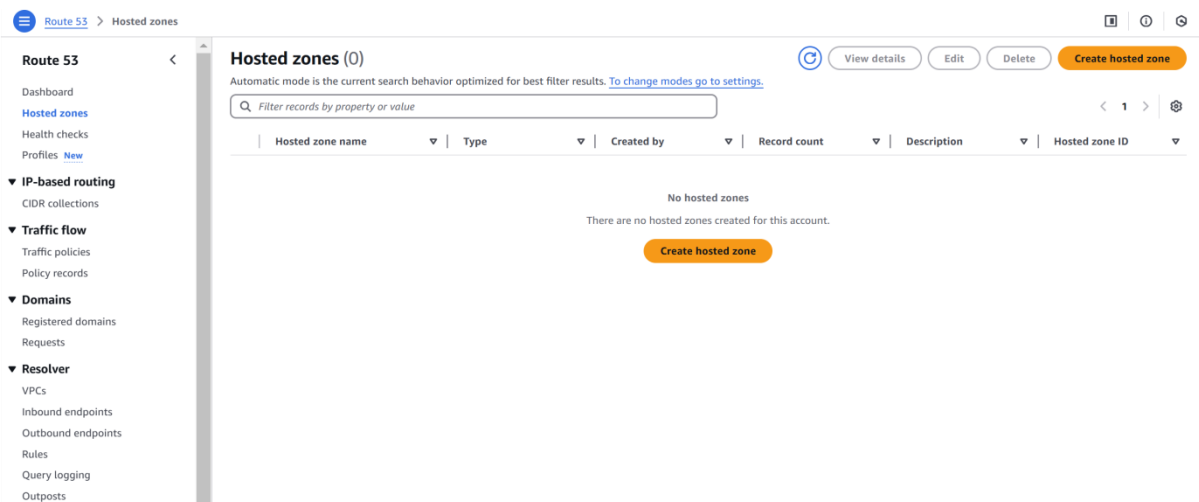


## Step 8:

In the AWS Console, search for **Route 53** and select it.

## Step 8:

1. Click on **Create hosted zone**.
2. Enter a **Domain Name** (e.g., myapp.local).
3. Set the **Type** to **Public Hosted Zone**.
4. Click **Create hosted zone**.





# Step 9:

Route 53 > Hosted zones > Create hosted zone

### Create hosted zone [Info](#)

**Hosted zone configuration**  
A hosted zone is a container that holds information about how you want to route traffic for a domain, such as example.com, and its subdomains.

**Domain name** [Info](#)  
This is the name of the domain that you want to route traffic for.  
  
Valid characters: a-z, 0-9, ! \* # \$ % & ' ( ) \* + , - / : ; < = > ? @ [ \ ] ^ \_ ` { | } . ~

**Description - optional** [Info](#)  
This value lets you distinguish hosted zones that have the same name.  
  
The description can have up to 256 characters. 17/256

**Type** [Info](#)  
The type indicates whether you want to route traffic on the internet or in an Amazon VPC.

☒ **Public hosted zone**  
A public hosted zone determines how traffic is routed on the internet.

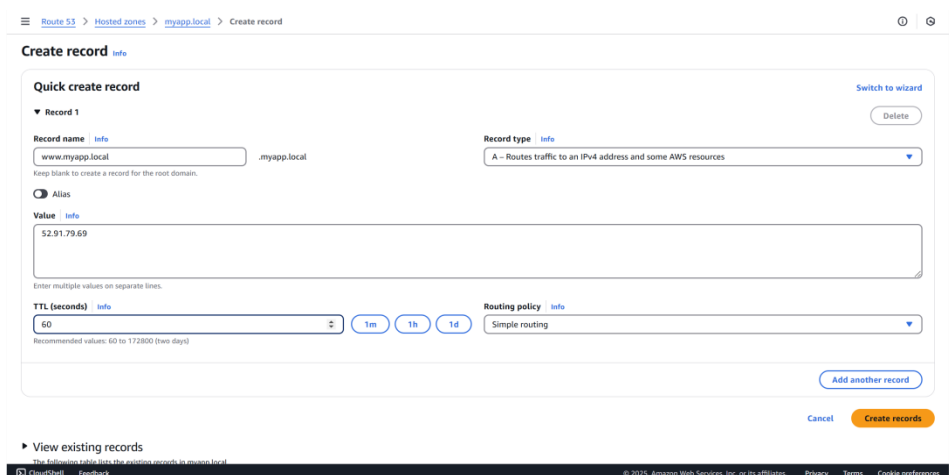
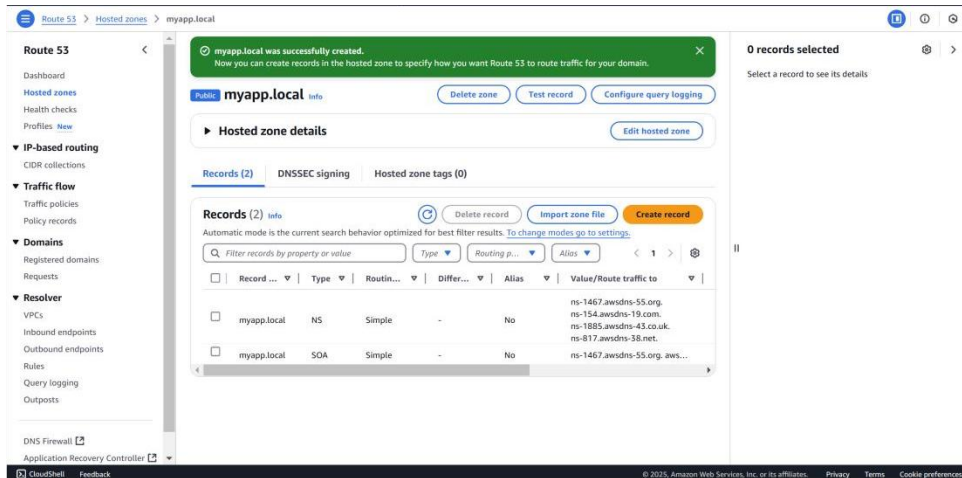
☐ **Private hosted zone**  
A private hosted zone determines how traffic is routed within an Amazon VPC.

**Tags** [Info](#)  
Apply tags to hosted zones to help organize and identify them.  
No tags associated with the resource.  
[Add tag](#)  
You can add up to 50 more tags.

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

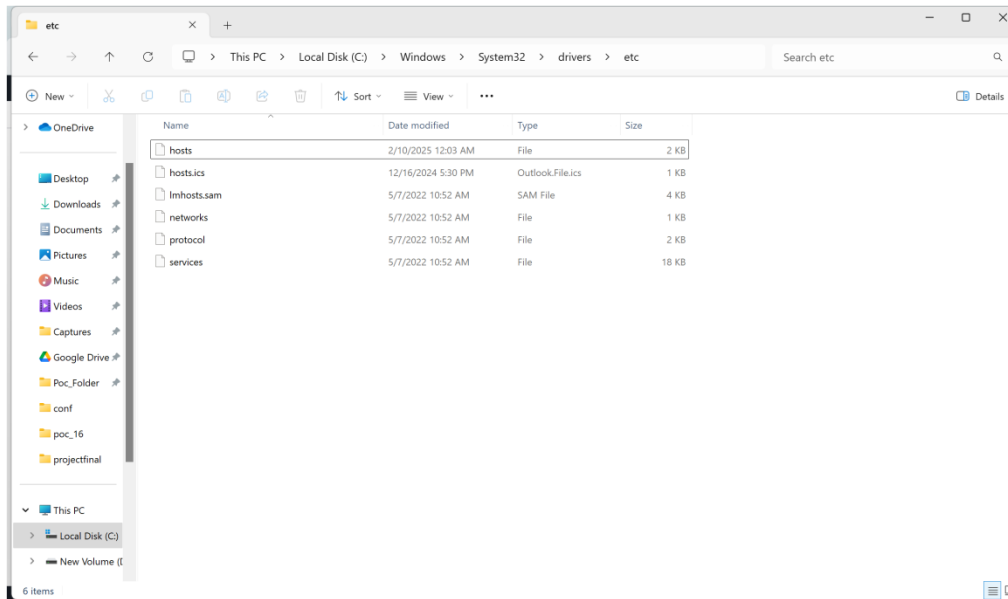
1. In your hosted zone, click **Create Record**.
2. **Record Name**: Leave it empty for the root domain (myapp.local),
3. **Record Type**: Select **A – IPv4 address**.
4. **Value**: Enter the **Public IP** of your EC2 instance.
5. **TTL**: Set to 60 seconds.
6. Click **Create records**.

# Step 10:



1. Go to **FileExplorer** > **Open**.
2. Navigate to: **C:\Windows\System32\drivers\etc**.
3. In the file name field, type **hosts** and press **Enter**.

## Step 11:



## Step 12:

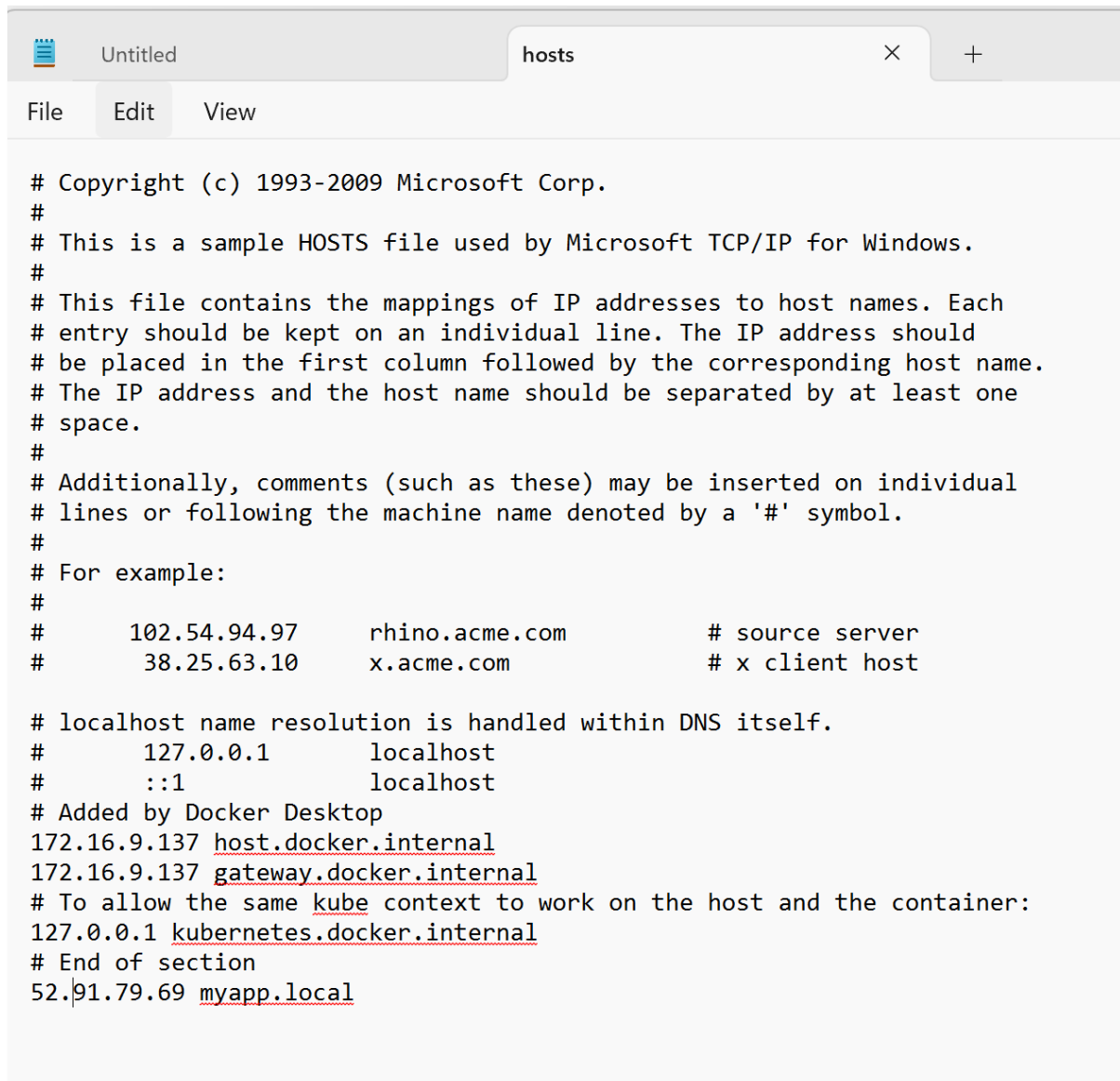
1. At the bottom of the file, add:

<Your EC2 Public IP> myapp.local

Replace <Your EC2 Public IP> with the public IP you copied.

(Eg: 52.91.79.69 myapp.local)

2. Save the file and close Notepad.



```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com          # source server
#       38.25.63.10       x.acme.com              # x client host

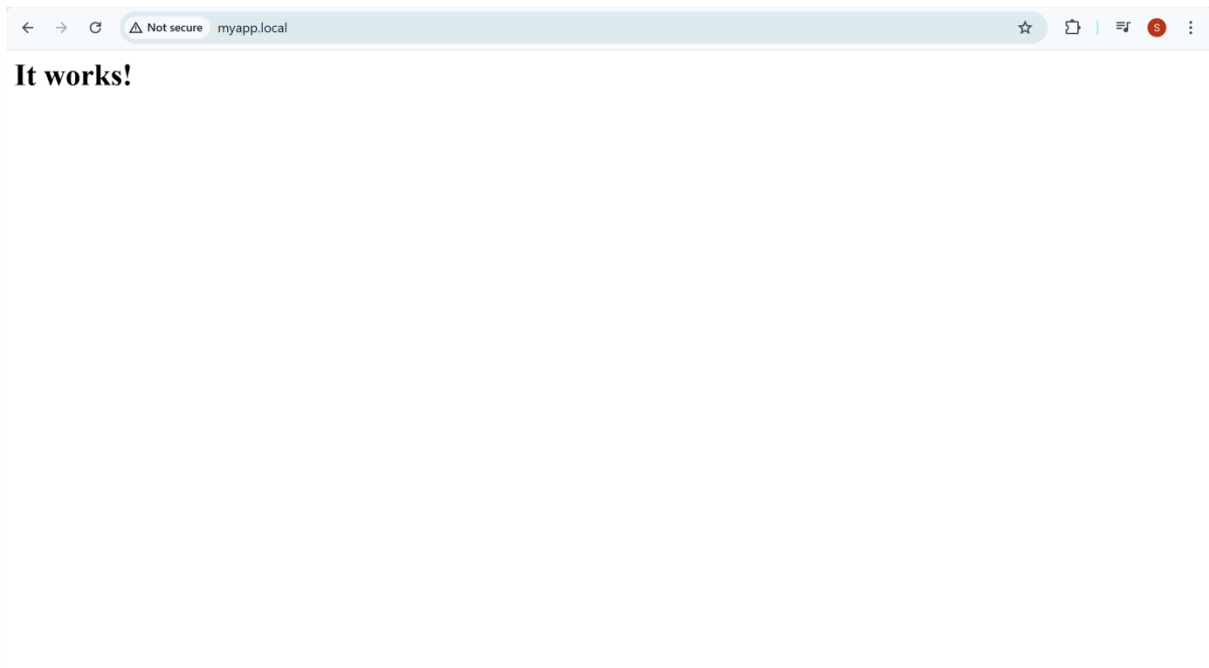
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
# Added by Docker Desktop
172.16.9.137 host.docker.internal
172.16.9.137 gateway.docker.internal
# To allow the same kube context to work on the host and the container:
127.0.0.1 kubernetes.docker.internal
# End of section
52.91.79.69 myapp.local
```

## Step 12:

Open your **web browser**.

Type `myapp.local` in the address bar and press **Enter**.

You should see the Apache default page



## Outcome

By completing this PoC of configuring DNS for your application using AWS Route 53 and EC2, you will:

1. Launch and configure an EC2 instance with a web server (e.g., Apache or Nginx).
2. Deploy a sample web application on the EC2 instance and ensure it is accessible via the instance's public IP.
3. Create a hosted zone in AWS Route 53 for DNS management.
4. Set up an A record in Route 53 to map your custom domain (e.g., myapp.local) to the EC2 instance's public IP.
4. Modify the local hosts file on your system to resolve the custom domain name locally for testing.
5. Successfully access your web application using the custom domain name in a browser.

