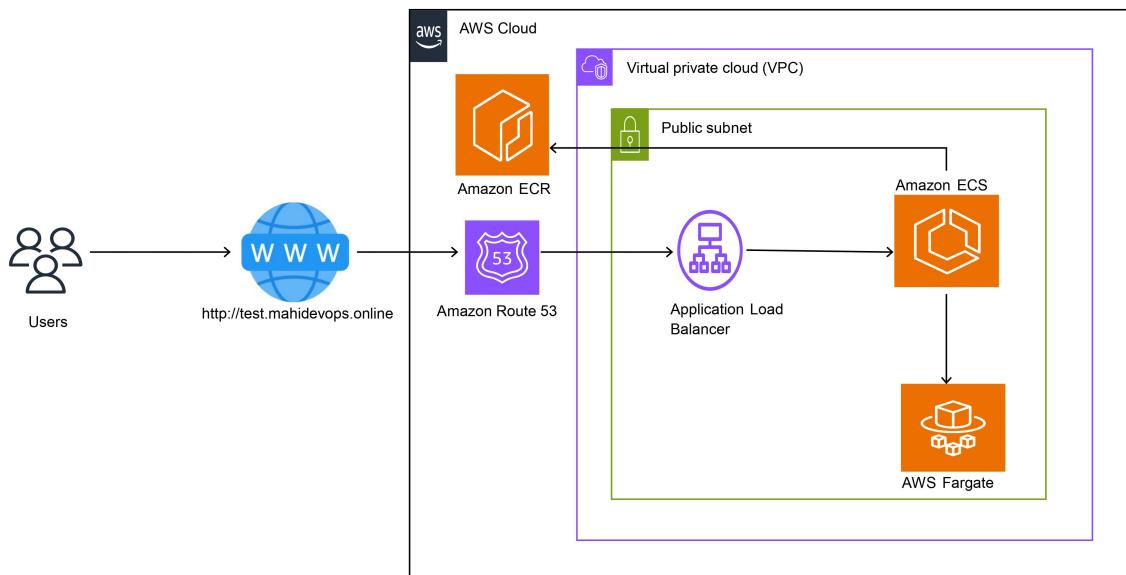


Seamlessly Integrating ECS with Application Load Balancer, Route 53 and GoDaddy



By
Mahendran Selvakumar
<https://devopstronaut.com/>



1. Create Application Load Balancer for ECS

Log in to the AWS Management Console and navigate to the "EC2" service

The screenshot shows the AWS EC2 service dashboard. On the left, a navigation menu includes options like Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network interfaces, and Load Balancing. The main area displays 'Resources' with counts for Instances (running), Auto Scaling Groups, Dedicated Hosts, Elastic IPs, Instances, Key pairs, Load balancers, Placement groups, Security groups, and Volumes. A 'Launch instance' button is present. To the right, there's a section for 'EC2 Free Tier' which says '1 EC2 free tier offers in use'. It also shows storage space on EBS at 29.44 GB remaining. Below that is a 'Service health' section with a link to the AWS Health Dashboard.

Click on "Load Balancers" and then click "Create load balancer"

The screenshot shows the 'Load balancers' page under the EC2 service. The left sidebar has the same navigation as the previous dashboard. The main area shows a table with columns for Name, DNS name, State, VPC ID, Availability Zones, and Type. A message indicates 'No load balancers' and 'You don't have any load balancers in eu-north-1'. At the bottom, there is a 'Create load balancer' button. A modal window titled '0 load balancers selected' is open, with the instruction 'Select a load balancer above.'

Under "Application Load Balancer", click "Create"

AWS Services Search [Option+S]

	Application Load Balancer <small>Info</small>	Network Load Balancer <small>Info</small>	Gateway Load Balancer <small>Info</small>
	<p>Choose an Application Load Balancer when you need a flexible feature set for your applications with HTTP and HTTPS traffic. Operating at the request level, Application Load Balancers provide advanced routing and visibility features targeted at application architectures, including microservices and containers.</p> <p>Create</p>	<p>Choose a Network Load Balancer when you need ultra-high performance, TLS offloading at scale, centralized certificate deployment, support for UDP, and static IP addresses for your applications. Operating at the connection level, Network Load Balancers are capable of handling millions of requests per second securely while maintaining ultra-low latencies.</p> <p>Create</p>	<p>Choose a Gateway Load Balancer when you need to deploy and manage a fleet of third-party virtual appliances that support GENEVE. These appliances enable you to improve security, compliance, and policy controls.</p> <p>Create</p>

Provide the Load Balancer name, select the scheme as "internet-facing", and set the Load Balancer IP address type to "IPv4"



Create Application Load Balancer Info

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and containers, based on request attributes. When the load balancer receives a connection request, it evaluates the listener rules in priority order to determine which rule to apply, and if applicable, it selects a target from the target group for the rule action.

► How Application Load Balancers work

Basic configuration

Load balancer name

Name must be unique within your AWS account and can't be changed after the load balancer is created.

`devopstronaut-alb`

A maximum of 32 alphanumeric characters including hyphens are allowed, but the name must not begin or end with a hyphen.

Scheme Info

Scheme can't be changed after the load balancer is created.

Internet-facing

An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. [Learn more](#)

Internal

An internal load balancer routes requests from clients to targets using private IP addresses. Compatible with the **IPv4** and **Dualstack** IP address types.

Load balancer IP address type Info

Select the front-end IP address type to assign to the load balancer. The VPC and subnets mapped to this load balancer must include the selected IP address types. Public IPv4 addresses have an additional cost.

IPv4

Includes only IPv4 addresses.

Dualstack

Includes IPv4 and IPv6 addresses.

Dualstack without public IPv4

Includes a public IPv6 address, and private IPv4 and IPv6 addresses. Compatible with **internet-facing** load balancers only.

Select the VPC and Availability Zones under "Network mapping"

Network mapping Info

The load balancer routes traffic to targets in the selected subnets, and in accordance with your IP address settings.

VPC Info

The load balancer will exist and scale within the selected VPC. The selected VPC is also where the load balancer targets must be hosted unless routing to Lambda or on-premises targets, or if using VPC peering. To confirm the VPC for your targets, view [target groups](#). For a new VPC, [create a VPC](#).

-
vpc-02aa3080a2b7a0b7
IPv4 VPC CIDR: 172.31.0.0/16



Mappings Info

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

Availability Zones

eu-north-1a (eun1-az1)

Subnet

subnet-0c7727afb8ff0c730
IPv4 subnet CIDR: 172.31.16.0/20

IPv4 address
Assigned by AWS

eu-north-1b (eun1-az2)

Subnet

subnet-071184dc52011c698
IPv4 subnet CIDR: 172.31.32.0/20

IPv4 address
Assigned by AWS

eu-north-1c (eun1-az3)

Subnet

subnet-0f4e64ce0a813bf21
IPv4 subnet CIDR: 172.31.0.0/20

IPv4 address
Assigned by AWS



Select the security groups and the target group. If a target group is not available, click "Create target group"

The screenshot shows the AWS Load Balancer configuration interface. In the 'Security groups' section, a single security group 'default' is selected. In the 'Listeners and routing' section, a listener for port 80 is configured to forward traffic to a target group. A 'Create target group' link is visible.

Select "IP addresses" as the target type and provide the target group name

The screenshot shows the 'Create target group' wizard, Step 1: Specify group details. It asks to choose a target type. The 'IP addresses' option is selected, highlighted with a blue border. Other options like 'Instances', 'Lambda function', and 'Application Load Balancer' are shown with their respective descriptions. A 'Target group name' field contains 'devopstronaut-tg'.



Select the protocol as "HTTP" and port as "80", set the IP address type to "IPv4", choose the VPC, and then click "Next"

Protocol : Port

Choose a protocol for your target group that corresponds to the Load Balancer type that will route traffic to it. Some protocols now include anomaly detection for the targets and you can set mitigation options once your target group is created. This choice cannot be changed after creation

HTTP 80

IP address type

Only targets with the indicated IP address type can be registered to this target group.

IPv4

IPv6

VPC

Select the VPC that hosts the load balancer. Only VPCs that support the IP address type selected above are available in this list. On the Register targets page, you can register IP addresses from this VPC, or from private IP addresses located outside of this load balancer's VPC (such as a peered VPC, EC2-Classic, or on-premises targets that are reachable over Direct Connect or VPN).

-
vpc-02aa3080a2b7a0b77
IPv4 VPC CIDR: 172.31.0.0/16

Protocol version

HTTP1
Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2.

HTTP2
Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available.

gRPC
Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

The associated load balancer periodically sends requests, per the settings below, to the registered targets to test their status.

Health check protocol

HTTP

Health check path

Use the default path of "/" to perform health checks on the root, or specify a custom path if preferred.

/
Up to 1024 characters allowed.

► Advanced health check settings

Attributes

ⓘ Certain default attributes will be applied to your target group. You can view and edit them after creating the target group.

Tags - optional

Consider adding tags to your target group. Tags enable you to categorize your AWS resources so you can more easily manage them.

Click “Create Target group”



EC2 > Target groups > Create target group

Step 1
Specify group details

Step 2
Register targets

IP addresses

Step 1: Choose a network

You can add IP addresses from the VPC selected for your target group or from outside the VPC. Note that you can assemble a mix of targets from multiple network sources by returning to this step and choosing another network.

Network: vpc-02a598a257ab677 (IPv4 VPC CIDR: 172.31.0.0/16)

Step 2: Specify IPs and define ports

You can manually enter IP addresses from the selected network.

Enter an IPv4 address from a VPC subnet: 172.31.0.0

Add IPv4 address

You can add up to 4 more IP addresses.

Ports: Port for routing to this target: 80
80-80553 (separate multiple ports with commas)
Include as pending below

Review targets

Step 3: Review IP targets to include in your group

Confirms the IP targets to include in your target group. Add more IP targets by repeating steps 1 and 2 on this page. You can also register additional targets after your target group is created.

Targets (0)

Remove IPv4 address

Health status

IP address

Port

Zone

No IP addresses included yet.
Specify IP addresses above and add to list.

0 pending

Cancel Previous Create target group

Now, refresh the target group list and choose the desired target group

Listeners and routing Info

A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80

Protocol: HTTP Port: 80 Default action: Forward to: Select a target group Info

Create target

Listener tags - optional

Consider adding tags to your listener. Tags enable you to categorize your AWS resources so you can more easily manage them.

Add listener tag

You can add up to 50 more tags.

Add listener

► Load balancer tags - optional

Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

Optimize with service integrations - optional

Optimize your load balancing architecture by integrating AWS services with this load balancer at launch. You can also add these and other services after your load balancer is created by reviewing the load balancer's "Integrations" tab.

AWS Web Application Firewall (WAF) Info Additional charges apply
Optimizes: Security

Include WAF security protections behind the load balancer
Associates a pre-defined web ACL that includes the AWS-recommended security protections. Alternatively, you can associate any of your existing WAF web ACLs for custom protections.

AWS Global Accelerator Info Additional charges apply
Optimizes: Performance, Availability, Security

Create an accelerator
An accelerator will be created in your account. The accelerator provides 2 global static IPs that act as a fixed entry point to your load balancer.



Click “Create Load Balancer”

▶ **Load balancer tags - optional**
Consider adding tags to your load balancer. Tags enable you to categorize your AWS resources so you can more easily manage them. The 'Key' is required, but 'Value' is optional. For example, you can have Key = production-webserver, or Key = webserver, and Value = production.

Optimize with service integrations - optional
Optimize your load balancing architecture by integrating AWS services with this load balancer at launch. You can also add these and other services after your load balancer is created by reviewing the load balancer's "Integrations" tab.

AWS Web Application Firewall (WAF) Info Optimizes: Security	Additional charges apply
<input type="checkbox"/> Include WAF security protections behind the load balancer Associates a pre-defined web ACL that includes the AWS-recommended security protections. Alternatively, you can associate any of your existing WAF web ACLs for custom protections.	
AWS Global Accelerator Info Optimizes: Performance, Availability, Security	Additional charges apply
<input type="checkbox"/> Create an accelerator An accelerator will be created in your account. The accelerator provides 2 global static IPs that act as a fixed entry point to your load balancer.	

Review
Review the load balancer configurations and make changes if needed. After you finish reviewing the configurations, choose **Create load balancer**.

Summary Review and confirm your configurations. Estimate cost			
Basic configuration Edit devopstronaut-alb <ul style="list-style-type: none">Internet-facingIPv4	Security groups Edit <ul style="list-style-type: none">default sg-086bbc46375ed734e	Network mapping Edit <ul style="list-style-type: none">VPC vpc-02aa3080a2b7a0b77<ul style="list-style-type: none">eu-north-1a subnet-0c7727afb8ff0c730eu-north-1b subnet-071184dc52011c698eu-north-1c subnet-0f4e64ce0a813bf21	Listeners and routing Edit <ul style="list-style-type: none">HTTP:80 defaults to <i>Target group not defined</i>
Service integrations Edit AWS WAF: <i>None</i> AWS Global Accelerator: <i>None</i>	Tags Edit <i>None</i>		
Attributes <div style="border: 1px solid #ccc; padding: 5px;"><p><i>ⓘ Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.</i></p></div>			
Creation workflow and status			
<p>▶ Server-side tasks and status After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.</p>			
Cancel Create load balancer			



2. Create ECR Repository for ECS Container

Go to Amazon Elastic Container Registry and click "Create repository"

Containers

Amazon Elastic Container Registry

Share and deploy container software, publicly or privately

Amazon Elastic Container Registry (ECR) is a fully managed container registry that makes it easy to store, manage, share and deploy your container images and artifacts anywhere.

Pricing (US)

Select "Private" and provide the repository name

Amazon ECR > Private registry > Repositories > Create repository

Create repository

General settings

Visibility settings | [Info](#)
Choose the visibility setting for the repository.

Private
Access is managed by IAM and repository policy permissions.

Public
Publicly visible and accessible for image pulls.

Repository name
Provide a concise name. A developer should be able to identify the repository contents by the name.

851725583489.dkr.ecr.eu-north-1.amazonaws.com/

13 out of 256 characters maximum (2 minimum). The name must start with a letter and can only contain lowercase letters, numbers, hyphens, underscores, periods and forward slashes.

Tag immutability | [Info](#)
Enable tag immutability to prevent image tags from being overwritten by subsequent image pushes using the same tag. Disable tag immutability to allow image tags to be overwritten.

Disabled

ⓘ Once a repository has been created, the visibility setting of the repository can't be changed.



Click "Create repository"

Image scan settings

Deprecation warning
The ScanOnPush configuration at the repository level has been deprecated in favour of registry-level scan filters.

Scan on push
Enable scan on push to have each image automatically scanned after being pushed to a repository. If disabled, each image scan must be manually started to get scan results.
 Disabled

Encryption settings

KMS encryption
You can use AWS Key Management Service (KMS) (KMS) to encrypt images stored in this repository instead of using the default encryption settings.
 Disabled

i The KMS encryption settings cannot be changed or disabled after the repository has been created.

Create repository

3. Create an IAM user with ECR permissions

Go to IAM and click "Create user"

Identity and Access Management (IAM)

Users (1) Info
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group:	Last activity	MFA	Password age	Console
ansibledemouser	/	0	-	-	-	-

Create user

Provide a username



Specify user details

User details

User name

mahi

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . @ _ - (hyphen)

Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.

ⓘ If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel

Next

Add the user to the admin group. Here, you can also restrict access with a custom policy

Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

Permissions options

Add user to group

Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

Copy permissions

Copy all group memberships, attached managed policies, and inline policies from an existing user.

Attach policies directly

Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

User groups (1/1)

[Create group](#)

< 1 >

Group name

▲ | Users

▼ | Attached policies

▼ | Created

[adminaccess](#)

0

[AdministratorAccess](#)

2024-07-14 (16 days ago)

► Set permissions boundary - optional

Cancel

[Previous](#)

Next

Click "Create user"



Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
mahi	None	No

Permissions summary

Name	Type	Used as
adminaccess	Group	Permissions group

Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#)

[Previous](#)

[Create user](#)

Go to the new user and create an Access key for AWS CLI

IAM > Users > mahi

mahi [Info](#) [Delete](#)

Summary

ARN arn:aws:iam::851725583489:user/mahi	Console access Disabled	Access key 1 Create access key
Created July 31, 2024, 00:28 (UTC+01:00)	Last console sign-in -	

[Permissions](#) [Groups \(1\)](#) [Tags](#) [Security credentials](#) [Access Advisor](#)

Console sign-in [Enable console access](#)

Console sign-in link https://851725583489.sigin.aws.amazon.com/console	Console password Not enabled
---	---------------------------------

Multi-factor authentication (MFA) (0) [Remove](#) [Resync](#) [Assign MFA device](#)

Type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			
Assign MFA device			

Access keys (0) [Create access key](#)

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

Select "Command line interface (CLI)"



Access key best practices & alternatives Info

Avoid using long-term credentials like access keys to improve your security. Consider the following use cases and alternatives.

Use case

Command Line Interface (CLI)

You plan to use this access key to enable the AWS CLI to access your AWS account.

Local code

You plan to use this access key to enable application code in a local development environment to access your AWS account.

Application running on an AWS compute service

You plan to use this access key to enable application code running on an AWS compute service like Amazon EC2, Amazon ECS, or AWS Lambda to access your AWS account.

Third-party service

You plan to use this access key to enable access for a third-party application or service that monitors or manages your AWS resources.

Application running outside AWS

You plan to use this access key to authenticate workloads running in your data center or other infrastructure outside of AWS that needs to access your AWS resources.

Other

Your use case is not listed here.



Alternatives recommended

- Use [AWS CloudShell](#), a browser-based CLI, to run commands. [Learn more](#)
- Use the [AWS CLI V2](#) and enable authentication through a user in IAM Identity Center. [Learn more](#)

Confirmation

I understand the above recommendation and want to proceed to create an access key.

Cancel

Next

Enter a description for the access key and click “create access key”

Set description tag - optional Info

The description for this access key will be attached to this user as a tag and shown alongside the access key.

Description tag value

Describe the purpose of this access key and where it will be used. A good description will help you rotate this access key confidently later.

Access key for ECR

Maximum 256 characters. Allowed characters are letters, numbers, spaces representable in UTF-8, and: _ : / = + - @

Cancel

Previous

Create access key

Copy the access key and secret key, as the secret key value will not be visible again



Retrieve access keys Info

Access key

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Access key	Secret access key
AKIA4MTWNASATFXBN35N	***** Show

Access key best practices

- Never store your access key in plain text, in a code repository, or in code.
- Disable or delete access key when no longer needed.
- Enable least-privilege permissions.
- Rotate access keys regularly.

For more details about managing access keys, see the [best practices for managing AWS access keys](#).

[Download .csv file](#)[Done](#)

To verify if AWS CLI is installed and available on your system, you can run the following command in your terminal or command prompt. If AWS CLI is installed, this command will display the version information. If it is not installed, you'll receive an error message indicating that the command is not recognized

```
mahendranelvakumar@Mahendrals-MBP ~ % which aws
/usr/local/bin/aws
mahendranelvakumar@Mahendrals-MBP ~ % aws --version
aws-cli/2.17.20 Python/3.11.9 Darwin/23.2.0 exe/x86_64
mahendranelvakumar@Mahendrals-MBP ~ %
```

To configure AWS CLI with your access credentials

```
mahendranelvakumar@Mahendrals-MBP ~ % aws configure
AWS Access Key ID [None]: AKIA4MTWNASATFXBN35N
AWS Secret Access Key [None]: EN4VXD5xRVmkeMTAxsF0PxGJkhqr87gGzcsYNPZi
Default region name [None]: eu-north-1
Default output format [None]:
mahendranelvakumar@Mahendrals-MBP ~ %
```

You'll be prompted to enter the following details:

- AWS Access Key ID: Enter your access key.
- AWS Secret Access Key: Enter your secret key.
- Default region name: Enter your preferred AWS region (e.g., us-west-2).



- Default output format: Enter your preferred output format (e.g., Json, text, or yaml).

Verify the configuration

```
mahendranelvakumar@Mahendrans-MBP ~ % aws sts get-caller-identity
{
    "UserId": "AIDA4MTWNASA3FRJ52CGR",
    "Account": "851725583489",
    "Arn": "arn:aws:iam::851725583489:user/mahi"
}
mahendranelvakumar@Mahendrans-MBP ~ %
```

4. Build the Docker image and push it to ECR

Create a Dockerfile to build a Docker image

```
↳ Dockerfile > ...
1  # Use the official Ubuntu image as a base
2  FROM ubuntu:20.04
3
4  # Set the timezone environment variable (replace 'Area/City' with the desired timezone, e.g., 'America/New_York')
5  ENV TZ=Europe
6
7  # Set the timezone
8  RUN ln -snf /usr/share/zoneinfo/$TZ /etc/localtime && echo $TZ > /etc/timezone
9
10 # Install Apache and tzdata, then clean up unnecessary files
11 RUN apt update && \
12     apt install -y apache2 tzdata && \
13     apt clean && \
14     rm -rf /var/lib/apt/lists/*
15
16 # Set environment variables for Apache
17 ENV APACHE_RUN_USER=www-data
18 ENV APACHE_RUN_GROUP=www-data
19 ENV APACHE_LOG_DIR=/var/log/apache2
20 ENV APACHE_RUN_DIR=/var/www/html
21
22 # Add a custom index.html
23 RUN echo 'Hello, Devopstronaut Family!' > /var/www/html/index.html
24
25
26
27 # Expose port 80 for Apache
28 EXPOSE 80
29
30 # Add a health check to monitor the container's health
31 HEALTHCHECK --interval=30s --timeout=10s --start-period=5s --retries=3 \
32     CMD curl -f http://localhost/ || exit 1
33
34 # Start Apache in the foreground
35 ENTRYPOINT ["apache2ctl", "-D", "FOREGROUND"]
```

Build docker image using this command (**docker build -t devopstronaut .**)



```
mahendranelvakumar@Mahendrans-MBP Docker % docker build --platform linux/amd64 -t devopstronaut .
[+] Building 51.6s (8/8) FINISHED
=> [internal] load build definition from Dockerfile
=> transferring dockerfile: 1.05kB
=> [internal] load metadata for docker.io/library/ubuntu:20.04
=> [internal] load .dockerignore
=> transferring context: 2B
=> CACHED [1/4] FROM docker.io/library/ubuntu:20.04@sha256:0b897358ff6624825fb50d20ffb605ab0eaea77ced0adb8c6a4b756513dec6fc
=> [2/4] RUN ln -snf /usr/share/zoneinfo/Europe /etc/localtime && echo Europe > /etc/timezone
=> [3/4] RUN apt update && apt install -y apache2 tzdata && apt clean && rm -rf /var/lib/apt/lists/*
=> [4/4] RUN echo 'Hello, Devopstronaut Family' > /var/www/html/index.html
=> exporting to image
=> exporting layers
=> => writing image sha256:cb0f5c642be53d725333d9de36ba372715f904851c72bb045c237157dbe0a6b0
=> => naming to docker.io/library/devopstronaut

View build details: docker-desktop://dashboard/build/desktop-linux/desktop-linux/nb0ivgb5729tq9ceoutqzkwz3

What's next:
  View a summary of image vulnerabilities and recommendations → docker scout quickview
```

Retrieve an authentication token and authenticate your Docker client to your registry. Use the AWS CLI

```
aws ecr get-login-password --region eu-north-1 | docker login --username AWS --password-stdin 851725583489.dkr.ecr.eu-north-1.amazonaws.com
```

```
mahendranelvakumar@Mahendrans-MBP Docker % aws ecr get-login-password --region eu-north-1 | docker login --username AWS --password-stdin 851725583489.dkr.ecr.eu-north-1.amazonaws.com
Login Succeeded
mahendranelvakumar@Mahendrans-MBP Docker %
```

Tag your image so you can push the image to this repository

```
docker tag devopstronaut:latest 851725583489.dkr.ecr.eu-north-1.amazonaws.com/devopstronaut:latest
```

```
mahendranelvakumar@Mahendrans-MBP Docker % docker tag devopstronaut:latest 851725583489.dkr.ecr.eu-north-1.amazonaws.com/devopstronaut:latest
mahendranelvakumar@Mahendrans-MBP Docker % docker push 851725583489.dkr.ecr.eu-north-1.amazonaws.com/devopstronaut:latest
The push refers to repository [851725583489.dkr.ecr.eu-north-1.amazonaws.com/devopstronaut]
2f61c1b9a272: Pushed
7dc8fa8ac06a: Pushing [=====>] 96.08MB/146.7MB
373fa0b680e0: Pushed
a8c68591d421: Pushing [=====>] 15.76MB/65.66MB
```

Run the following command to push this image to your newly created AWS repository

```
docker push 851725583489.dkr.ecr.eu-north-1.amazonaws.com/devopstronaut:latest
```

```
mahendranelvakumar@Mahendrans-MBP Docker % docker push 851725583489.dkr.ecr.eu-north-1.amazonaws.com/devopstronaut:latest
The push refers to repository [851725583489.dkr.ecr.eu-north-1.amazonaws.com/devopstronaut]
2f61c1b9a272: Pushed
7dc8fa8ac06a: Pushed
373fa0b680e0: Pushed
a8c68591d421: Pushed
latest: digest: sha256:3c300b8612412605a64ffae9d9c359355072ea99313704a600524c89b4af6917 size: 1155
mahendranelvakumar@Mahendrans-MBP Docker %
```

Verify that the docker image has been pushed



Amazon ECR > Private registry > Repositories > devopstronaut

devopstronaut

[View push commands](#)

Images (1)

[Delete](#) [Details](#) [Scan](#)

<input type="checkbox"/>	Image tag	Artifact type	Pushed at	Size (MB)	Image URI	Digest
<input type="checkbox"/>	latest	Image	31 July 2024, 01:46:41 (UTC+01)	88.53	Copy URI	sha256:3c300b86124126...

5.Create ECS Cluster

Go to AWS ECS and click “Create Cluster”

Amazon Elastic Container Service > Clusters

Clusters (0) [Info](#)

[Create cluster](#)

[Search clusters](#)

< 1 > [@](#)

Cluster | Services | Tasks | Container instances | CloudWatch monitoring

No clusters

No clusters to display

Enter a cluster name and choose "AWS Fargate" so that the cluster is automatically configured for AWS Fargate



Cluster configuration

Cluster name

Cluster name must be 1 to 255 characters. Valid characters are a-z, A-Z, 0-9, hyphens (-), and underscores (_).

Default namespace - *optional*

Select the namespace to specify a group of services that make up your application. You can overwrite this value at the service level.

 X

▼ Infrastructure Info Serverless

Your cluster is automatically configured for AWS Fargate (serverless) with two capacity providers. Add Amazon EC2 instances.

AWS Fargate (serverless)
Pay as you go. Use if you have tiny, batch or burst workloads or for zero maintenance overhead. The cluster has Fargate and Fargate Spot capacity providers by default.

Amazon EC2 instances
Manual configurations. Use for large workloads with consistent resource demands.

i External instances using **ECS Anywhere** can be registered after cluster creation is complete.

► Monitoring - *optional* Info

Container Insights is turned off by default. To change the default behaviour, use the CloudWatch Container Insights account setting. When you use Container Insights, there is a cost associated with it.

► Encryption - *new, optional*

Choose the KMS keys used by tasks running in this cluster to encrypt your storage.

► Tags - *optional* Info

Tags help you to identify and organise your clusters.

Cancel Create

The Cluster has been created successfully

cluster devopstronautcluster has been created successfully. View cluster X

Amazon Elastic Container Service > Clusters

Clusters (1) Info Create cluster

Cluster	Services	Tasks	Container instances	CloudWatch monitoring	Capacity provider strategy
devopstronautcluster	0	No tasks running	0 EC2	Default	No default found



Create Task definition

Specify the task definition family and set the launch type to "AWS Fargate"

Amazon Elastic Container Service > Create new task definition

Create new task definition Info

Task definition configuration

Task definition family Info
Specify a unique task definition family name.

Up to 255 letters (uppercase and lowercase), numbers, hyphens, and underscores are allowed.

▼ Infrastructure requirements
Specify the infrastructure requirements for the task definition.

Launch type Info
Selection of the launch type will change task definition parameters.
 AWS Fargate
Serverless compute for containers.
 Amazon EC2 instances
Self-managed infrastructure using Amazon EC2 instances.

OS, Architecture, Network mode
Network mode is used for tasks and is dependent on the compute type selected.
Operating system/Architecture Info

Network mode Info

Task size Info
Specify the amount of CPU and memory to reserve for your task.
CPU
Memory

▼ Task roles - conditional

Task role Info
A task IAM role allows containers in the task to make API requests to AWS services. You can create a task IAM role from the [IAM console](#).

Enter the container name, provide the ECR image URI, and specify the port name



▼ Container – 1 [Info](#)

Container details
Specify a name, container image and whether the container should be marked as essential. Each task definition must have at least one essential container.

Name	Image URI	Essential container
mycontainer	851725583489.dkr.ecr.eu-north-1.amazonaws.com	<input checked="" type="checkbox"/> Yes

Up to 255 letters (uppercase and lowercase), numbers, hyphens, underscores, colons, periods, forward slashes, and number signs are allowed.

Private registry [Info](#)
Store credentials in Secrets Manager, and then use the credentials to reference images in private registries.

Private registry authentication

Port mappings [Info](#)
Add port mappings to allow the container to access ports on the host to send or receive traffic. For port name, a default will be assigned if left blank.

Container port	Protocol	Port name	App protocol
80	TCP	httpd	HTTP

[Add port mapping](#)

Read-only root file system [Info](#)
When this parameter is turned on, the container is given read-only access to its root file system.

Read only

Resource allocation limits - conditional [Info](#)
Container-level CPU, GPU and memory limits are different from task-level values. They define how many resources are allocated for the container. If the container attempts to exceed the memory specified by the hard limit, the container is terminated.

CPU 1 in vCPU	GPU 1	Memory hard limit 3 in GB	Memory soft limit 1 in GB
---------------------	----------	---------------------------------	---------------------------------

▼ Environment variables - optional

Environment variables [Info](#)

Add individually
Add a key-value pair to specify an environment variable.

You can verify the created task by checking the container name



Amazon Elastic Container Service > Task definitions > devopstask > Revision 1 > Containers

devopstask:1

Deploy Actions Create new revision

Overview Info

ARN arn:aws:ecs:eu-north-1:851725583489:task-definition/devopstask:1	Status ACTIVE	Time created 31 July 2024 at 02:16 (UTC+1:00)	App environment FARGATE
Task role -	Task execution role ecsTaskExecutionRole	Operating system/Architecture Linux/X86_64	Network mode awsvpc

Containers JSON Task placement Volumes (0) Requires attributes Tags

Task size

Task CPU 1024 units (1 vCPU)	Task memory 3072 MiB (3 GB)
Task CPU maximum allocation for containers	
CPU (unit) 0 100 200 300 400 500 600 700 800 900 1000	Memory (MiB) 0 200 400 600 800 1000 1200 1400 1600 1800 2000 2200 2400 2600 2800 3000
█ mycontainer Shared task CPU	█ mycontainer Shared task memory

Containers Info

Container name	Image	Private registry	Essential	CPU	Memory hard/soft limit
mycontainer	851725583489.dkr.ecr.eu-north-1.amazonaws.com	-	Yes	0	-/-

Create ECS Service

Go back to the "Deploy" section and select "Create service"

Task definition successfully created
devopstask:1 has been successfully created. You can use this task definition to deploy a service or run a task.

View task definition

Amazon Elastic Container Service > Task definitions > devopstask

devopstask (1/1) Info

Filter status Active

Task definition: revision
 devopstask:1

Deploy Actions Create service Update service Run task Status ACTIVE

Choose the existing cluster and select compute option as “capacity provider”



Create Info

Environment

AWS Fargate

Existing cluster

devopstronautcluster

▼ Compute configuration (advanced)

Compute options Info

To ensure task distribution across your compute types, use appropriate compute options.

Capacity provider strategy
Specify a launch strategy to distribute your tasks across one or more capacity providers.

Launch type
Launch tasks directly without the use of a capacity provider strategy.

Capacity provider strategy Info

Select either your cluster default capacity provider strategy or select the customised option to configure a different strategy.

Use cluster default
No default capacity provider strategy configured for this cluster.

Use custom (Advanced)

Capacity provider	Base <small>Info</small>	Weight <small>Info</small>
FARGATE <input type="button" value="▼"/>	0 <input type="text"/>	1 <input type="text"/>

Add capacity provider

Platform version Info

Specify the platform version on which to run your service.

LATEST

Provide the Service name and specify the desired tasks to “1”



Deployment configuration

Application type [Info](#)

Specify what type of application you want to run.

Service

Launch a group of tasks handling a long-running computing work that can be stopped and restarted. For example, a web application.

Task

Launch a standalone task that runs and terminates. For example, a batch job.

Task application type is not applicable when launching a service.

Task definition

Select an existing task definition. To create a new task definition, go to [Task definitions](#).

Specify the revision manually

Manually input the revision instead of choosing from the 100 most recent revisions for the selected task definition family.

Family

Revision

devopstask

1

Service name

Assign a unique name for this service.

devopsservice

Service type [Info](#)

Specify the service type that the service scheduler will follow.

Replica

Place and maintain a desired number of tasks across your cluster.

Daemon

Place and maintain one copy of your task on each container instance.

Desired tasks

Specify the number of tasks to launch.

1

► Deployment options

► Deployment failure detection [Info](#)

In the Networking section, choose the VPC, subnet, and security group



▼ Networking

VPC | [Info](#)

Choose the Virtual Private Cloud to use.

vpc-02aa3080a2b7a0b77

default



Subnets

Choose the subnets within the VPC that the task scheduler should consider for placement.

[Choose subnets](#)



[Clear current selection](#)

subnet-0f4e64ce0a813bf21 X

eu-north-1c 172.31.0.0/20

subnet-071184dc52011c698 X

eu-north-1b 172.31.32.0/20

subnet-0c7727afb8ff0c730 X

eu-north-1a 172.31.16.0/20

Security group | [Info](#)

Choose an existing security group or create a new security group.

Use an existing security group

Create a new security group

Security group name

Choose an existing security group.

[Choose security groups](#)



sg-086bbc46373ed734e X

default

Public IP | [Info](#)

Choose whether to auto-assign a public IP to the task's elastic network interface (ENI).

Turned on

In the Load Balancing section, select "Application Load Balancer," choose "Existing load balancer," and select the created load balancer



▼ Load balancing - optional

Configure load balancing using Amazon Elastic Load Balancing to distribute traffic evenly across the healthy tasks in your service.

Load balancer type Info

Configure a load balancer to distribute incoming traffic across the tasks running in your service.

Application Load Balancer



Container

The container and port to load balance the incoming traffic to

mycontainer 80:80



Host port:Container port

Application Load Balancer

Specify whether to create a new load balancer or choose an existing one.

- Create a new load balancer
- Use an existing load balancer

Load balancer

Select the load balancer you wish to use to distribute incoming traffic across the tasks running in your service.

devopstronaut-alb



devopstronaut-alb
devopstronaut-alb-271571893.eu-north-1.elb.amazonaws.com

internet-facing



seconds

In the Load Balancing section, choose "Existing listener," select "Existing target group," and then choose the created target group



Listener | Info

Specify the port and protocol that the load balancer will listen for connection requests on.

Create new listener

Listener

Use an existing listener

80:HTTP



Listener rules for 80:HTTP (1)

Traffic received by the listener is routed according to its rules. Rules are evaluated in priority order, from the lowest value to the highest value. The default rule is evaluated last.

< 1 >

Evaluation order



Rule path



Target group



default

/

[devopstronaut-tg](#)

Target group | Info

Specify whether to create a new target group or choose an existing one that the load balancer will use to route requests to the tasks in your service.

Create new target group

Target group name

Use an existing target group

devopstronaut-tg



devopstronaut-tg



HTTP 80

Health check protocol

HTTP

It will take more time to create the service

devopservice deployment is in progress. It takes a few minutes.

View in CloudFormation

Amazon Elastic Container Service > Clusters > [devopstronautcluster](#) > Services

[devopstronautcluster](#)

[G](#) [Update cluster](#) [Delete cluster](#)

Cluster overview			
ARN	arn:aws:ecs:eu-north-1:851725583499:cluster/devopstronautcluster	Status	Active
CloudWatch monitoring	<input type="radio"/> Default	Registered container instances	-
Services		Tasks	
Draining	-	Pending	Running
Encryption			
Managed storage	Fargate ephemeral storage		

Verify the task status after the service has been created



Amazon Elastic Container Service > Clusters > devopstronautcluster > Services > devops > Tasks

devops [Info](#)

Health and metrics [Tasks](#) Logs Deployments Events Configuration and networking Tags

Tasks (1/1)

Task	Last status	Desired state	Task def...	Health status	Started at	Container instan...	Launch type	Pla...
22c29c033ac64087ad573c6911e7c9e7	Running	Running	devopstask:4	Unknown	1 minute ago	-	FARGATE	1.4

Containers for task 22c29c033ac64087ad573c6911e7c9e7

Containers (1)

Container name	Container runtime ID	Image URI	Image Digest	Status	Health status
mycontainer	22c29c033ac6408...	851725583489.dkr.ecr.eu-north-1.a...	sha256:7a29aba7e182e7884...	Running	Unknown

Go to Load Balancers in the EC2 console and select the created Application Load Balancer

Dedicated Hosts
Capacity Reservations

Images AMIs AMI Catalog

Elastic Block Store Volumes Snapshots Lifecycle Manager

Network & Security Security Groups Elastic IPs Placement Groups Key Pairs Network Interfaces

Load Balancing [Load Balancers](#) Target Groups Trust Stores [New](#)

Auto Scaling Auto Scaling Groups

EC2 > Load balancers

Load balancers (1)

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
devopstronaut-alb	devopstronaut-alb-27157...	Active	vpc-02aa3080a2b7a0...	3 Availability Zones	application	August 4, 2024, 09:22:40

Load balancer:

Copy the DNS name



EC2 > Load balancers > devopstronaut-alb

devopstronaut-alb

[C](#) Actions ▾

▼ Details

Load balancer type Application	Status Active	VPC vpc-02aa3080a2b7a0b77	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone Z23TAZ6LKFMNIO	Availability Zones subnet-0f4e64ce0a813bf21 eu-north-1c (eu-n1-az3) subnet-071184dc52011c698 eu-north-1b (eu-n1-az2) subnet-0c7727afb8ff0c730 eu-north-1a (eu-n1-az1)	Date created August 4, 2024, 00:24 (UTC+01:00)
Load balancer ARN arnaws:elasticloadbalancing:eu-north-1:851725583489:loadbalancer/app/devopstronaut-alb/863b9c1885724abb		DNS name Info devopstronaut-alb-271571893.eu-north-1.elb.amazonaws.com (A Record)	

[Listeners and rules](#) [Network mapping](#) [Resource map - new](#) [Security](#) [Monitoring](#) [Integrations](#) [Attributes](#) [Tags](#)

Listeners and rules (1) [Info](#)
A listener checks for connection requests on its configured protocol and port. Traffic received by the listener is routed according to the default action and any additional rules.

<input type="checkbox"/> Protocol:Port	Default action	Rules	ARN	Security policy	Default SSL/TLS certificate	mTLS
<input type="checkbox"/> HTTP:80	Forward to target group <ul style="list-style-type: none">• devopstronaut-tg: 1 (100%)• Target group stickiness: Off	1 rule	ARN	Not applicable	Not applicable	Not applicable

Paste the URL in the browser and verify that the application is functioning correctly

← → C △ Not Secure devopstronaut-alb-271571893.eu-north-1.elb.amazonaws.com

Hello, Devopstronaut Family

6.Create Route 53 Zone

Go to Route 53 and click "Create hosted zone"



aws Services Search [Option+S] Global ▾ Mahi ▾

Route 53 X Route 53 > Dashboard

Route 53 Dashboard Info

DNS management
A hosted zone tells Route 53 how to respond to DNS queries for a domain such as example.com.

Traffic management
A visual tool that lets you easily create policies for multiple endpoints in complex configurations.

Availability monitoring
Health checks monitor your applications and web resources, and direct DNS queries to healthy resources.

Domain registration
A domain is the name, such as example.com, that your users use to access your application.

Create hosted zone **Create policy**

Create health check **Register domain**

Dashboard Domains

Provide the domain name, choose "Public Hosted Zone," and click "Create hosted zone"

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. 0/256

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.

Cancel **Create hosted zone**



Now, a hosted zone has been created for the mahidevops.online domain

The screenshot shows the AWS Route 53 Hosted Zone Details page for the domain "mahidevops.online". A green banner at the top indicates that the hosted zone was successfully created. Below the banner, the page displays the "Hosted zone details" for "mahidevops.online". Under the "Records" tab, there are two entries:

Record name	Type	Value/Route traffic to	TTL	Health	Evaluate	R.
mahidevops.online	NS	Simple ns-407.awsdns-50.com. ns-555.awsdns-05.net. ns-1718.awsdns-22.co.uk. ns-1311.awsdns-35.org.	172800	-	-	-
mahidevops.online	SOA	Simple ns-407.awsdns-50.com. awsd...	900	-	-	-

7. Register the domain mahidevops. online in a domain manager such as GoDaddy

Log in to your GoDaddy account

The screenshot shows the GoDaddy homepage. At the top, there is a search bar with the placeholder "Search using your business name or desired domain name" and a "Find a domain" button. To the right of the search bar, there is a "Set up a fr" button. The main content area features a question "Which business do you want to work on, Mahendran?". Below this question are two cards: one for "DevOpstronaut" and one for "mahidevops.online".

DevOpstronaut
devopstronaut.com
Website, Domain

mahidevops.online
mahidevops.online
Website, Domain

Select the domain and click “Manage DNS”



The screenshot shows the GoDaddy Domain dashboard for the domain `mahidevops.online`. The main area displays domain renewal details: Auto-renew is set to OFF, it expires on December 4, 2024, and the renewal cost is £39.04 per year. A yellow callout box encourages users to secure their domain with Domain Protection, stating it keeps the domain safe against unauthorized access and prevents honest mistakes like accidental expiration. Buttons for "Forward Domain", "Manage DNS", and "Domain Settings" are present. On the left, a sidebar lists other services: Website, Email, Store, Appointments, and Social.

Go to the DNS settings, select "Nameservers," and click "Change Nameservers"

The screenshot shows the GoDaddy DNS settings page for the domain `mahidevops.online`. The "Nameservers" tab is selected. It lists two nameservers: `ns69.domaincontrol.com` and `ns70.domaincontrol.com`. A "Change Nameservers" button is located at the top right of the nameserver list. Other tabs include "DNS Records", "Forwarding", "Premium DNS", "Hostnames", "DNSSEC", and "Crypto V".

Copy the nameserver details from the AWS Route 53 hosted zone (`mahidevops.online`) and paste them into the appropriate fields in GoDaddy. After entering the nameservers, make sure to save the changes



See what's new | Help Center



Edit nameservers

Choose nameservers for mahidevops.online

- GoDaddy Nameservers (recommended)
- I'll use my own nameservers

ns-407.awsdns-50.com



ns-555.awsdns-05.net



ns-1718.awsdns-22.co.uk



ns-1311.awsdns-35.org

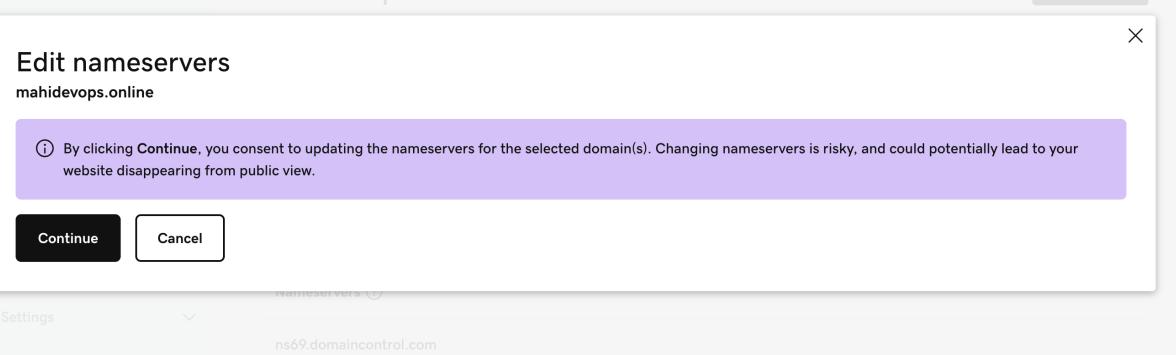


[+ Add Nameserver](#)

Save

Cancel

Click "Continue"



After changing the nameservers, we are encountering the following message



< [Domain Portfolio](#)

mahidevops.online

Overview DNS Products

DNS Records Forwarding Nameservers Premium DNS Hostnames DS Records

DNS records define how your domain behaves, like showing your website content and delivering your email.

[Add New Record](#)

Filters Actions



We can't display your DNS information because your nameservers aren't managed by us.

8.create a CNAME record in Route 53

Go to Route 53, select the hosted zone, and click “Create record”

Route 53 > Hosted zones > mahidevops.online

Public mahidevops.online [Info](#)

Delete zone Test record Configure query logging

Hosted zone details [Edit hosted zone](#)

Records (2) [Info](#)

Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

<input type="checkbox"/> Record name	Type	Routing policy	Alias	Value/Route traffic to	TTL (s...)	Health ...	Evaluat...	R...
mahidevops.online	NS	Simple	No	ns-407.awsdns-50.com. ns-555.awsdns-05.net. ns-1718.awsdns-22.co.uk. ns-1311.awsdns-35.org.	172800	-	-	-
mahidevops.online	SOA	Simple	No	ns-407.awsdns-50.com. awsd...	900	-	-	-

Provide the record name as `test` , enter the DNS name, and select the record type as “CNAME”



Services Search [Option+S]

Route 53 > Hosted zones > mahidevops.online > Create record

Create record Info

Quick create record Switch to wizard

Record 1 Delete

Record name Info .mahidevops.online
Keep blank to create a record for the root domain.

Alias

Value Info
Enter multiple values on separate lines.

TTL (seconds) Info 1m 1h 1d Simple routing
Recommended values: 60 to 172800 (two days)

Routing policy Info

Add another record

Create records Create Cancel

View existing records
The following table lists the existing records in mahidevops.online.

The CNAME record has been created

Record for mahidevops.online was successfully created.
Route 53 propagates your changes to all of the Route 53 authoritative DNS servers within 60 seconds. Use "View status" button to check propagation status.

Route 53 > Hosted zones > mahidevops.online

Public mahidevops.online Info Delete zone Test record Configure query logging

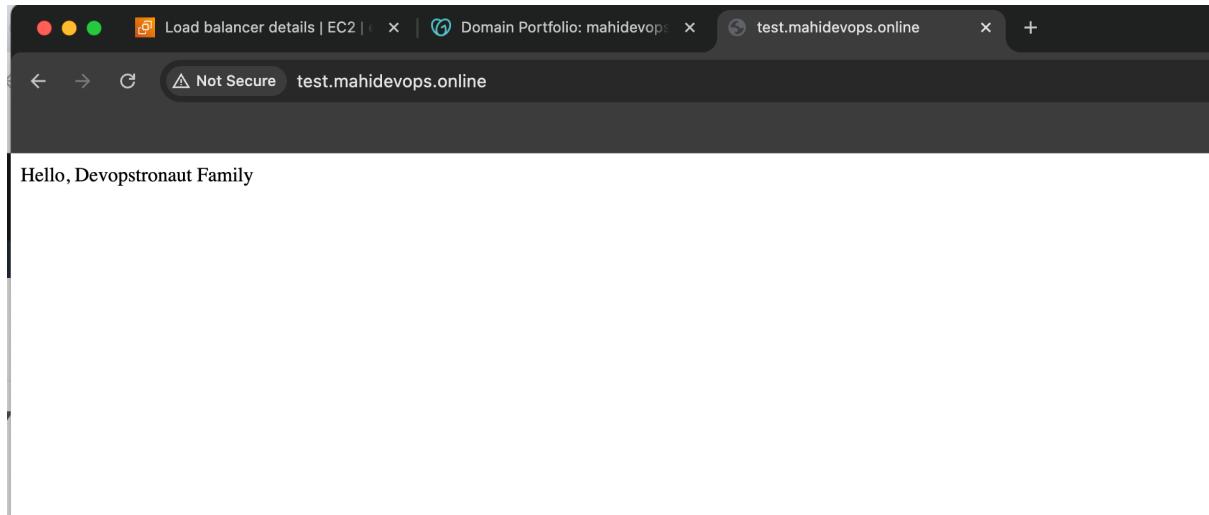
Hosted zone details Edit hosted zone

Records (3) Info
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

<input type="checkbox"/> Record name	Type	Routing policy	Alias	Value/Route traffic to	TTL (s...)	Health ...	Evalu...	R...
<input type="checkbox"/> mahidevops.online	NS	Simple	-	No ns-407.awsdns-50.com. ns-555.awsdns-05.net. ns-1718.awsdns-22.co.uk. ns-1311.awsdns-35.org.	172800	-	-	-
<input type="checkbox"/> mahidevops.online	SOA	Simple	-	No ns-407.awsdns-50.com. awsd...	900	-	-	-
<input type="checkbox"/> test.mahidevops.online	CNAME	Simple	-	No devopstronaut-alb-2715718...	300	-	-	-



Enter the URL `test.mahidevops.online` into your browser, and you should now be able to access the Apache website hosted on AWS ECS



Keep Learning, Keep Deploying!!!

Feel free to reach out to me, if you have any other queries or suggestions

Stay connected on Linkedin <https://www.linkedin.com/in/mahendran-selvakumar-36444a77/>