

Travel Memory Application Deployment

- **Instance Configuration**

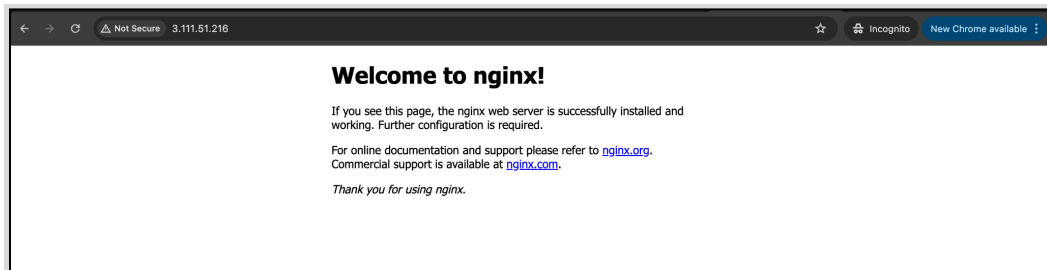
1. Update the package management tool (apt)

```
sudo apt update
```

```
Sudo apt-get update
```

2. Install the nginx server

```
sudo apt install nginx
```



3. Install the nodejs

```
curl -sL https://deb.nodesource.com/setup_18.x -o/tmp/nodesource_setup.sh
```

```
sudo bash /tmp/nodesource_setup.sh
```

```
sudo apt install nodejs
```

- **Backend Configuration**

1. Clone the "TravelMemory" project from git.

```
git clone https://github.com/UnpredictablePrashant/TravelMemory
```

2. Navigate to the Backend directory of the project and create .env file

```
cd TravelMemory/backend
```

```
sudo nano .env
```

3. Add the URI and PORT details in .env file and save it.

```
MONGO_URI='mongodb+srv://Yash:<password>@cluster0.swmtw8d.mongodb.net/?retryWrites=true&w=majority&appName=Cluster0'
```

```
PORT=3000
```

4. Install the npm libraries and run the backend.

```
npm install
```

```
node index.js
```

5. Backend started running at port 3001.

```
ubuntu@ip-172-31-41-164:~/TravelMemory/backend$ sudo nano .env
ubuntu@ip-172-31-41-164:~/TravelMemory/backend$ node index.js
Server started at http://localhost:3000
```

6. Edit Security group rules to allow port 3000 for public access.



- **Frontend Configurations**

1. Navigate to the src/frontend Directory in TravelMemory app

```
cd TravelMemory/frontend/src
```

2. Open the url.js file and provide the backend url.

```
http://<ip address>:3000
```

Note:- replace ip address with your instance ip address

```
export const baseUrl = "http://13.208.164.76:3000"
```

3. Edit Security group rules to allow port 3001 for public access of the website.

sgr-06da55f838f61d44	Custom TCP	TCP	3001	Custom	Q		Delete
						0.0.0.0/0 X	

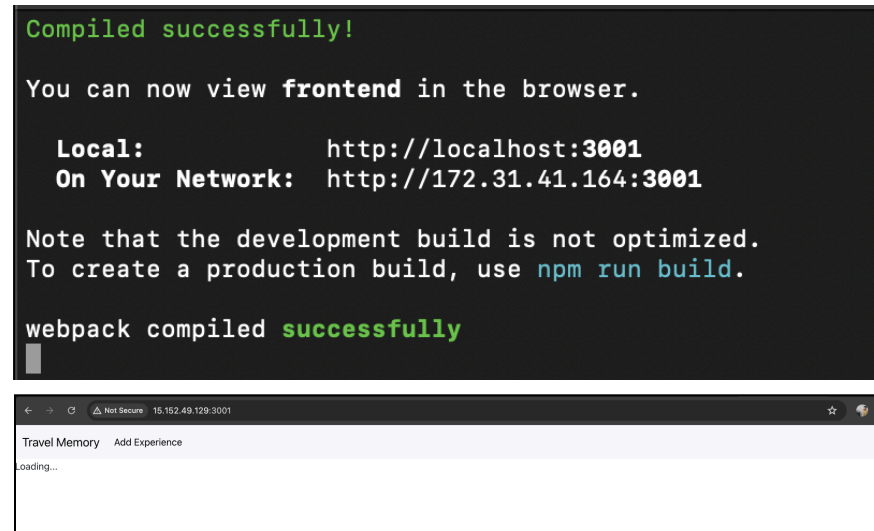
4. Install the npm libraries and run the Frontend.

```
cd ..
```

```
npm install
```

```
npm start
```

5. Frontend started at port 3000



- **Configuring the path forwarding**

1. Navigate to sites-available path in nginx and add the proxy pass details in the default named file.

```
sudo nano /etc/nginx/sites-available/default
```

```
server {
    listen 80 default_server;
    listen [::]:80 default_server;
    server_name _;
    location / {
        #try_files $uri $uri/ =404;
        proxy_pass http://localhost:3001;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection "upgrade";
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
    }
}
```

2. Delete the default file in sites-enabled and create a soft link of default file in sites-available.

```
sudo rm -rf /etc/sites-enabled/default
```

```
sudo ln -s /etc/nginx/sites-available/default /etc/sites-enabled/default
```

- **Full Application Working**

1. Open the port 3001 of your app and click on Add Experience and fill the form.

Travel Memory Add Experience

Trip Name
Goa

Trip Date
01/07/2024

Name of Hotels
Goa Gloters

Trip Type
Leisure

Total Cost
100000

Places Visited
Goa Beaches

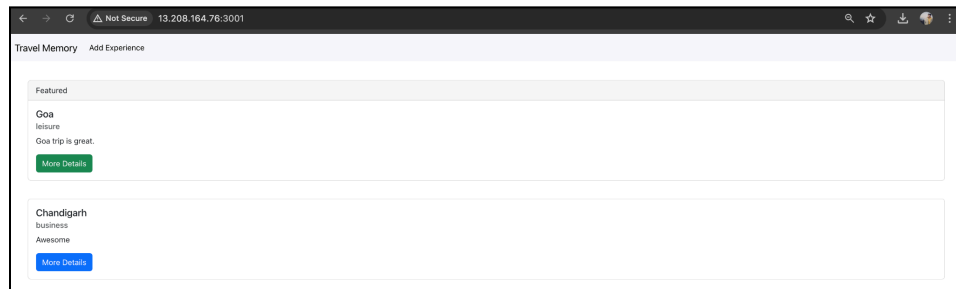
Featured Trip?
☒ True
☐ False

Image Link
http://image.com

Short Description
Goa trip is great.

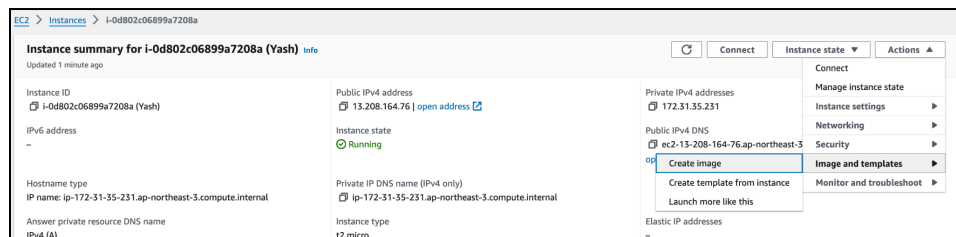
Experience
Awesome trip. Having lots of fun!

2. Navigate to the Home Page of your App and you can see a card created for your trip.



- **Load Balancer**

1. Create the AMI image of the running Instance.



2. Provide Image name and keep everything as default.

EC2 > AMIs > ami-08a345345a2692f3c			
Image summary for ami-08a345345a2692f3c			
<div> <div>EC2 Image Builder</div> <div>Actions</div> <div>Launch Instance from AMI</div> </div>			
AMI ID ami-08a345345a2692f3c	Image type machine	Platform details Linux/UNIX	Root device type EBS
AMI name Yashimg	Owner account ID 381491974700	Architecture x86_64	Usage operation RunInstances
Root device name /dev/sda1	Status Available	Source 381491974700/Yashimg	Virtualization type hvm
Boot mode uefi-preferred	State reason -	Creation date Mon Jul 08 2024 20:38:18 GMT+0530 (India Standard Time)	Kernel ID -
Description -	Product codes -	RAM disk ID -	Deprecation time -
Last launched time -	Block devices /dev/sda1=snap-00721b4c0aec7861a:8:true:gp3 /dev/sdb=ephemeral0 /dev/sdc=ephemeral1	Deregistration protection Disabled	

3. Create a new Application Load Balancer

Services

Search

[Option+5]

Load balancer types

Application Load Balancer

Info

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.

Create

Network Load Balancer

Info

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.

Create

Gateway Load Balancer

Info

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.

Create

Classic Load Balancer - previous generation

4. Provide a unique name and select the configurations as per below Screenshots.

Basic configuration

Load balancer name

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

Yash-LB

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 type of IP addresses that your subnets use. 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.

Network mapping Info

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

VPC Info

Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

-

vpc-0743d29cc89dc4d9e

IPv4 VPC CIDR: 172.31.0.0/16

↻

Mappings Info

Select at least one Availability Zone and one subnet for each zone. We recommend selecting at least two Availability Zones. 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.

☒ **ap-northeast-3a (apne3-az3)**

Subnet

subnet-039dba4ef0be873f5

IPv4 address

Assigned by AWS

☐ **ap-northeast-3b (apne3-az1)**

☐ **ap-northeast-3c (apne3-az2)**

Security groups Info

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

Security groups

Select up to 5 security groups

↻

↻

launch-wizard-yash-1

sg-08e8414ffa6ba8142

VPC: vpc-0743d29cc89dc4d9e

✕

Security groups Info

A security group is a set of firewall rules that control the traffic to your load balancer. Select an existing security group, or you can [create a new security group](#).

Security groups

Select up to 5 security groups

↻

↻

launch-wizard-yash-1

sg-08e8414ffa6ba8142

VPC: vpc-0743d29cc89dc4d9e

✕

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

Remove

Protocol

HTTP

Port

80

1-65535

Default action Info

Forward to

Select a target group

↻

↻

[Create target group](#)

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

- Select create new Target Group and choose Instance type and provide a unique name and click on next.

Specify group details

Your load balancer routes requests to the targets in a target group and performs health checks on the targets.

Basic configuration

Settings in this section can't be changed after the target group is created.

Choose a target type

☒ **Instances**

- Supports load balancing to instances within a specific VPC.
- Facilitates the use of [Amazon EC2 Auto Scaling](#) to manage and scale your EC2 capacity.

☐ **IP addresses**

- Supports load balancing to VPC and on-premises resources.
- Facilitates routing to multiple IP addresses and network interfaces on the same instance.
- Offers flexibility with microservice based architectures, simplifying inter-application communication.
- Supports IPv6 targets, enabling end-to-end IPv6 communication, and IPv4-to-IPv6 NAT.

☐ **Lambda function**

- Facilitates routing to a single Lambda function.
- Accessible to Application Load Balancers only.

☐ **Application Load Balancer**

- Offers the flexibility for a Network Load Balancer to accept and route TCP requests within a specific VPC.
- Facilitates using static IP addresses and PrivateLink with an Application Load Balancer.

Target group name

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

- Select the instance in Register targets and click on “include as pending below” then click on create target group.

Register targets

This is an optional step to create a target group. However, to ensure that your load balancer routes traffic to this target group you must register your targets.

Available instances (1)

Filter instances

Instance ID	Name	State	Security groups	Zone	Private IPv4 address
I-0d802c06899a7208a	Yash	Running	launch-wizard-yash-1	ap-northeast-3a	172.31.35.231

0 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.

1-65535 (separate multiple ports with commas)

Include as pending below

1 selection is now pending below. Include more or register targets when ready.

Review targets

Targets (1)

Filter targets

Show only pending

Remove all pending

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID	Launch time
I-0d802c06899a7208a	Yash	80	Running	launch-wizard-yash-1	ap-northeast-3a	172.31.35.231	subnet-039dba4ef0be873f5	July 8, 2024, 19:40 (UTC)

- Select the Target group you created in listeners and routing then click on create load balancer.

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 Remove

Protocol

Port

Default action

Info

HTTP

: 80

Forward to

Select a target group

1-65535

Create target

Q

Yash-TG

Target type: Instance, IPv4

HTTP

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

8. Load Balancer successfully created.

[EC2](#) > [Load balancers](#) > Yash-LB

Yash-LB Actions ▼

▼ Details

Load balancer type

Application

Status

Provisioning

VPC

vpc-0743d29cc89dc499e

Load balancer IP address type

IPv4

Scheme

Internet-facing

Hosted zone

ZSLKXXYW11ES

Availability Zones

subnet-039db4ef0be873f5 ap-northeast-3a (apne3-az3)

Date created

July 8, 2024, 21:05 (UTC+05:30)

Load balancer ARN

arn:aws:elasticloadbalancing:ap-northeast-3:381491974700:loadbalancer/app/Yash-LB/998be271841c5639

DNS name info

Yash-LB-1135237520.ap-northeast-3.elb.amazonaws.com (A Record)

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

Listeners and rules (1) [Info](#) Manage rules ▼ Manage listener ▼ Add listener

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	<div>Forward to target group</div> <ul style="list-style-type: none"> Yash-TG 1 (100%) Target group stickiness: Off 	1 rule	ARN	Not applicable	Not applicable	Not applicable

• Configuring Domain Setup

1. Created a Cname record and added the DNS name from load balancer in content as shown below.

DNS management for mrjunket.in DNS Setup: Full [Import and Export](#) [Dashboard Display Settings](#)

Review, add, and edit DNS records. Edits will go into effect once saved.

▼ Add filter Search + Add record

Type ▲	Name	Content	Proxy status	TTL	Actions
CNAME	react	yashbm-lb-1657885131.ap-northe...	DNS only	Auto	Edit

2. Open the react.mrjunket.in and you will see the application working.

Travel Memory Add Experience

Featured

Goa

backpacking

Goa is awesome

More Details

Featured

Goa

backpacking

Goa is awesome

More Details

- **Adding SSL Certificate to Load Balancer**

1. Go to ACM (Amazon ACM) and request a new public certificate. Puth the Domain names as below and rest leave everything default.

AWS Certificate Manager > Certificates > Request certificate > Request public certificate

Request public certificate

Domain names
Provide one or more domain names for your certificate.

Fully qualified domain name [Info](#)

mrjunket.in [Remove](#)

www.mrjunket.in [Remove](#)

[Add another name to this certificate](#)

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

Validation method [Info](#)
Select a method for validating domain ownership.

☒ **DNS validation - recommended**
Choose this option if you are authorized to modify the DNS configuration for the domains in your certificate request.

☐ **Email validation**
Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.

2. Open the certificate issued to you and copy the cname record key value pair to cloudflare.

DNS management for **mrjunket.in**

Review, add, and edit DNS records. Edits will go into effect once saved.

DNS Setup: Full ⓘ [Import and Export](#) ▼ [Dashboard Display Settings](#)

Search DNS Records

[Add filter](#) [Search](#) [Add record](#)

Type ▲	Name	Content	Proxy status	TTL	Actions
CNAME	_840946536bd61a7c090...	_4a1ec087856c319b775470cf39...	DNS only	Auto	Edit ▶
CNAME	_56f2d9701bfd9d495bd5...	_a708adff5d41752e16d499510a4...	DNS only	Auto	Edit ▶
A	mrjunket.in	15.168.8.247	DNS only	Auto	Edit ▶
CNAME	www	mrjunket.in	DNS only	Auto	Edit ▶

AWS Certificate Manager > Certificates > 94f49e2e-96f3-4d1e-b795-7beaf01cc6e0

94f49e2e-96f3-4d1e-b795-7beaf01cc6e0 [Delete](#)

Certificate status

Identifier: 94f49e2e-96f3-4d1e-b795-7beaf01cc6e0 Status: ✔ Issued

ARN: arn:aws:acm:ap-northeast-3:515210271098:certificate/94f49e2e-96f3-4d1e-b795-7beaf01cc6e0

Type: Amazon Issued

Domains (2) [Create records in Route 53](#) [Export to CSV](#)

Domain	Status	Renewal status	Type	CNAME name	CNAME value
mrjunket.in	✔ Success	-	CNAME	_56f2d9701bfd9d495bd5e54d446cdc7e.mrjunket.in.	_a708adff5d41752e16d499510a46156a.sdgjtdhzhz.acm-validations.aws.
www.mrjunket.in	✔ Success	-	CNAME	_840946536bd61a7c0903835cf8d641e7.www.mrjunket.in.	_4a1ec087856c319b775470cf393741df.sdgjtdhzhz.acm-validations.aws.

3. You can see status as success. Then navigate to load balancer and click on add listener.

EC2 > Load balancers > Yash-LB

Yash-LB

[Refresh](#) [Actions](#)

Details

Load balancer type	Status	VPC	IP address type
Application	Provisioning	vpc-e654388f	IPv4
Scheme	Hosted zone	Availability Zones	Date created
Internet-facing	ZSLXEXYW11E5	subnet-188d5455 ap-northeast-3a (apne3-az3)	May 29, 2024, 20:08 (UTC+05:30)

Load balancer ARN	DNS name
arn:aws:elasticloadbalancing:ap-northeast-3:515210271098:loadbalancer/app/Yash-LB/1c4856880b18985f	Yash-LB-203147769.ap-northeast-3.elb.amazonaws.com (A Record)

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

Listeners and rules (1) [Info](#)
[Refresh](#) [Manage rules](#) [Manage listener](#) [Add listener](#)

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"> Yash-TG 1 (100%) Group-level stickiness: Off 	1 rule	ARN	Not applicable	Not applicable	Not applicable

4. Select Https in listener configuration and the target group which you created.

Listener details: HTTPS:443

A listener checks for connection requests using the protocol and port that you configure. The default action and any additional rules that you create determine how the Application Load Balancer routes requests to its registered targets.

Listener configuration

The listener will be identified by the protocol and port.

Protocol Used for connections from clients to the load balancer. HTTPS	Port The port on which the load balancer is listening for connections. <input type="text" value="443"/> 1-65535
---	---

Default actions [Info](#)

The default action is used if no other rules apply. Choose the default action for traffic on this listener.

Authentication [Info](#)

☐ Use OpenID or Amazon Cognito
 Include authentication using either OpenID Connect (OIDC) or Amazon Cognito.

Routing actions

☒ Forward to target groups
 ☐ Redirect to URL
 ☐ Return fixed response

Forward to target group [Info](#)

Choose a target group and specify routing weight or [Create target group](#).

Target group	Weight	Percent
Yash-TG Target type: Instance, IPv4	<input type="text" value="1"/> 0-999	100%

[Add target group](#)

You can add up to 4 more target groups.

5. Attach the certificate you created in the listener setting.

Secure listener settings [Info](#)

Security policy [Info](#)

Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration called a security policy to manage SSL connections with clients. [Compare security policies](#)

Security category

Policy name

All security policies

ELBSecurityPolicy-TLS13-1-2-2021-06 (recommended)

Default SSL/TLS server certificate

The certificate used if a client connects without SNI protocol, or if there are no matching certificates. You can source this certificate from AWS Certificate Manager (ACM), Amazon Identity and Access Management (IAM), or import a certificate. This certificate will automatically be added to your listener certificate list.

Certificate source

☒ From ACM

☐ From IAM

☐ Import certificate

Certificate (from ACM)

The selected certificate will be applied as the default SSL/TLS server certificate for this load balancer's secure listeners.

Select a certificate

↻

[Request new ACM certificate](#)

Client certificate handling [Info](#)

Client certificates are used to make authenticated requests to remote servers. [Learn more](#)

☐ Mutual authentication (mTLS)

Mutual TLS (Transport Layer Security) authentication offers two-way peer authentication. It adds a layer of security over TLS and allows your services to verify the client that's making the connection.

6. Navigate to your domain and you can see a secure connection over https.

- Travel Memory Application Architecture

