



PROJECT

## AWS – DEPLOY HIGHLY AVAILABLE, SCALABLE, FAULT TOLERANT AND RESILIENT WEB APPLICATION & INTEGRATE MANAGED RDS DATABASE

(NETWORKING & CONTENT DELIVERY)

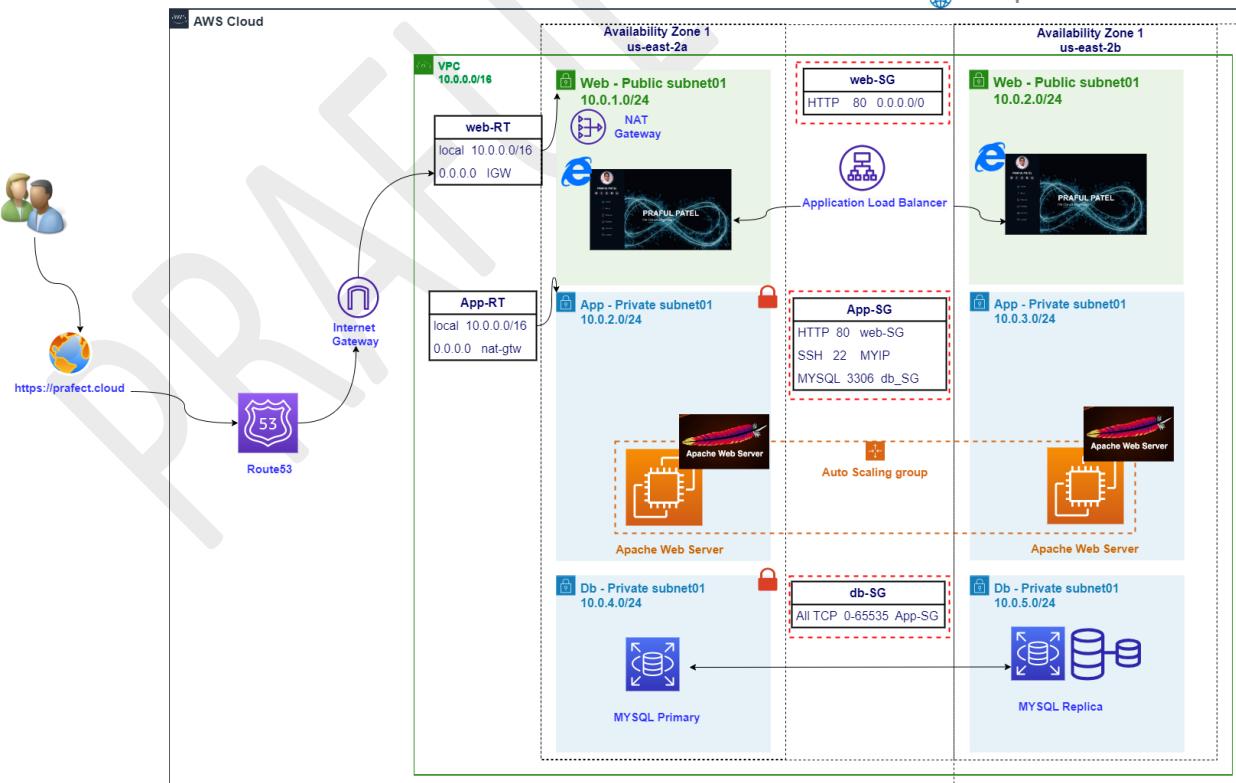
By: PRAFUL PATEL

HIGHLY AVAILABLE THREE TIER WEB APPLICATION

Prefect.cloud

Way To Go, Cloud Is Future!

Designed By: PRAFUL PATEL

<https://github.com/prafulpatel16>[www.praefect.cloud](http://www.praefect.cloud)



➤ **Project:**

An IT services provider company called **PRAFECT.CLOUD**, is engaged into providing software development solutions. Currently, they have a requirement to deploy on-premises to cloud migrated application on aws has to build and provision on AWS platform with managed relational database.

They are going to launch a personal portfolio web application on aws cloud platform. It assumes that more than 10000 users may access their web application to view the portfolio web application. The business users have an expectation of having a web application up and running all the time without any delay or single point of failure on the servers. The systems should be capable enough to handle the load and traffic in all circumstances and requires to scale up when the traffic or load crosses the certain threshold  $>40\%$  on each individual servers, and it should also be scaled in when the load reaches below to the specified cpu  $>40\%$  threshold.

➤ **Project Description:**

Web Servers: apache web server

Application source code: php/html web application

This project demonstrates an experience of web application deployment through using aws EC2 machines which can scale out and scale in using elastic load balancer, auto scaling and target group services.

➤ **Solution:**

This project needs to be deployed on highly available environment where web application should be scale out and scale in as per the traffic and load on the web servers. The web application should be always up and running always without any single point of failure. It needs to use aws service using application load balancer, auto scaling, target groups and launch template through which it can be made the web application always scale out and scale in as per the needs. There will be two public servers(EC2 machines) will be running initially which will be placed behind an application load balancer and it should be scaled out when certain cpu load  $>=40\%$  reaches to any of the web server machines, where it should be scaled out using auto scaling group and target group should be configured. VPC services should consist more than public subnet that web application machine should be placed behind a public server, and behind private server the DB instance should be placed.

For Web server perspective, this server should be running on apache web servers and the application source code of php/html packages should be installed and configured.

For networking and security perspective, web application server will have to be accessed and allowed publicly available so internet gateway needs to be provisioned and assigned to the public ip.

For security concerns and avoiding cyber threats it has to configure some security group and assign and appropriate routes and rules based on requirement. Also web serve should be allowed to access from SSH at port 22 for system administration perspective, and it should allow to be accessible at custom TCP: Port 8080 from everywhere.

For DB server perspective, this needs to be behind a private subnet so it should not allow from external world so certain settings like publicly available should be disabled. Also it has to strictly define some rules from security groups so that no one can access and abuse the db server. DB credentials should be defined while provisioning a db server and pass through safe mechanism.

OS and application packages requirements are provided separately which needs to be provisioned and be ready before go on live session.

➤ **Project Cost Estimation:**

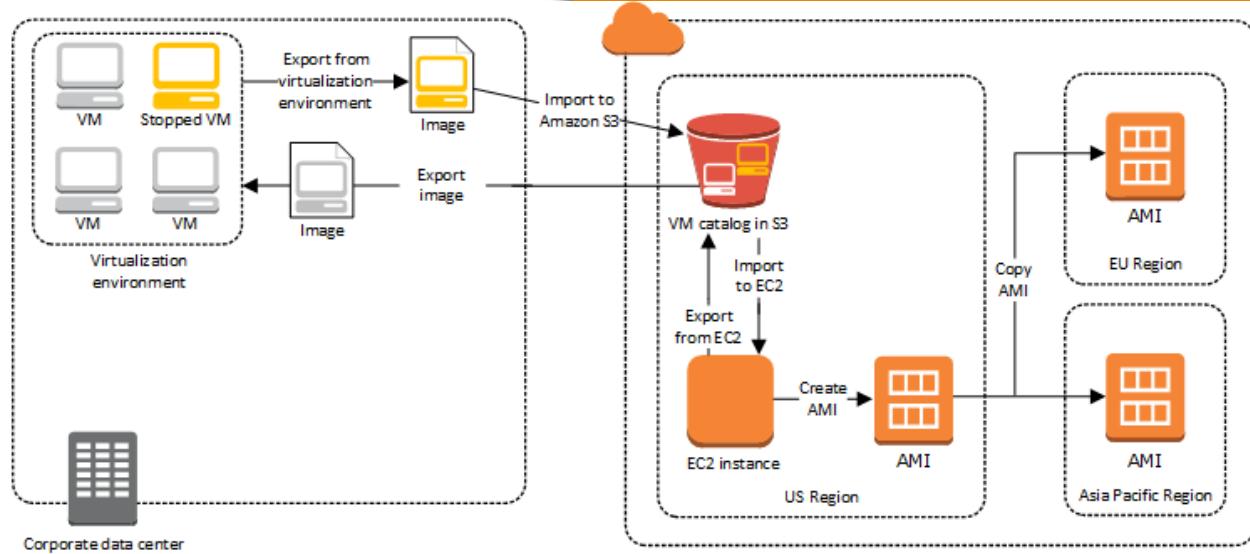
(Note: This cost is Not any actual cost, it's just an estimation based on high level requirement. Price may be vary based on adding and removing services based on requirement.)

➤ **Strategy**

○ **On-Premise to AWS Migration**

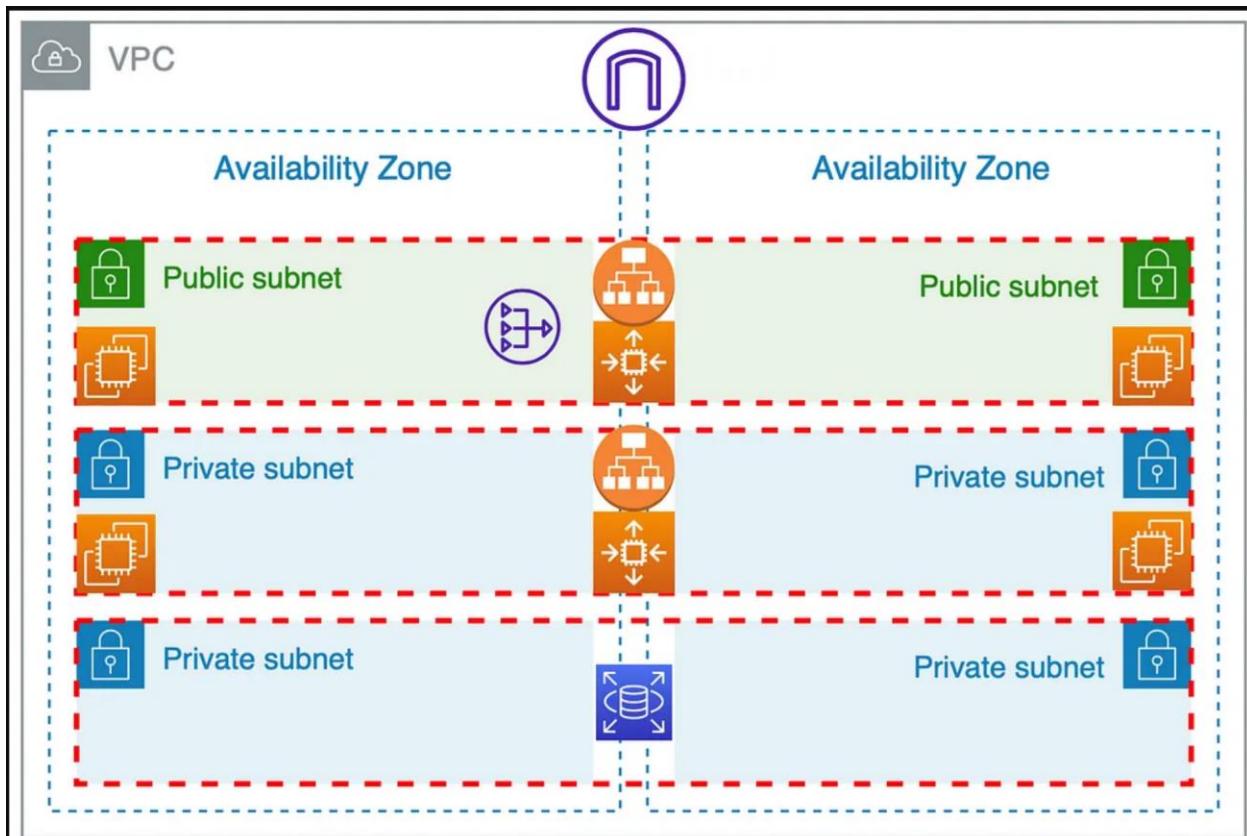
There are seven common migration strategies when moving applications to the cloud, including:

- Retain – keeping applications running as is and revisiting the migration at a later stage
- Retire – decommissioning applications that are no longer required
- Repurchase – switching from existing applications to a software-as-a-service (SaaS) solution
- **Rehost – moving applications as is (lift and shift), without making any changes to take advantage of cloud capabilities**
- Relocate – moving applications as is, but at a hypervisor level
- Replatform – moving applications as is, but introduce capabilities that take advantage of cloud-native features
- Refactor – re-architect the application to take full advantage of cloud-native features

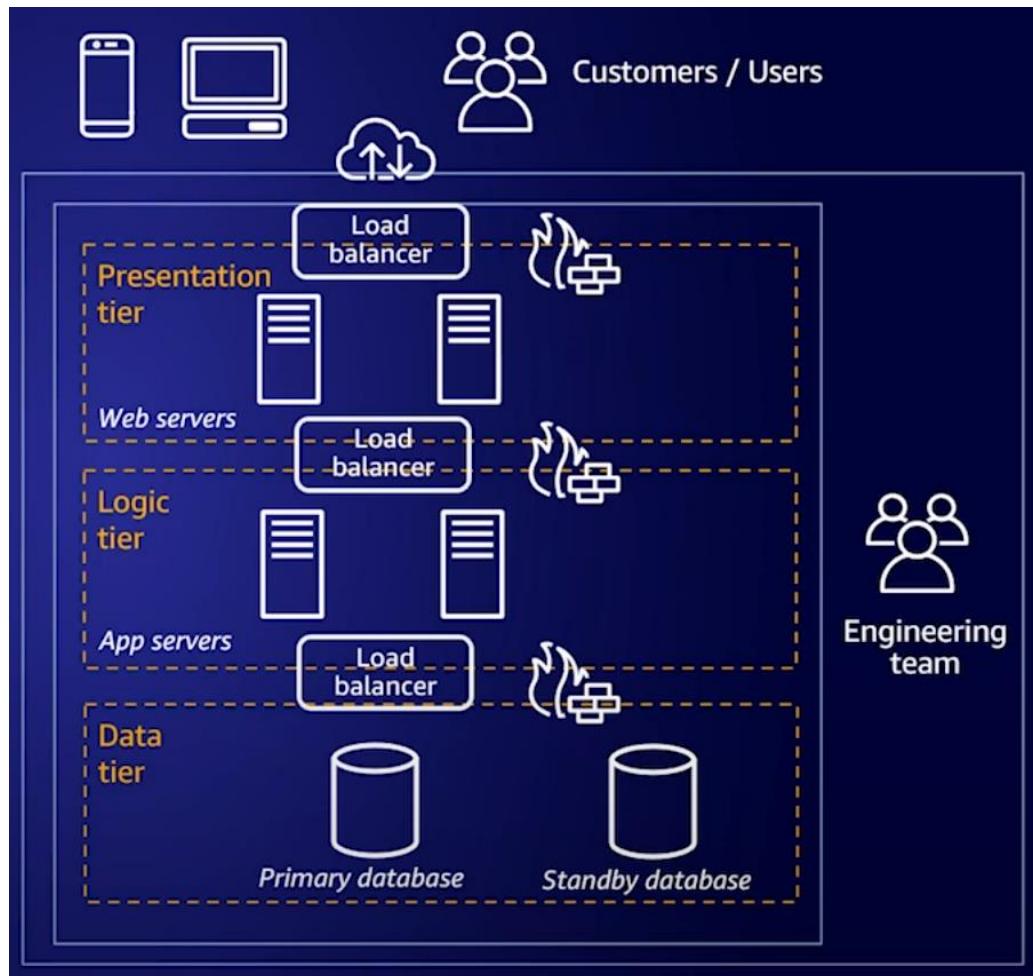


- **Re-platform and modernize the web application on AWS Cloud**

The solution is comprised of the following components:



### 3 – Tier application – components



#### ► What is load balancing ?

Load balancing is the method of distributing network traffic equally across a pool of resources that support an application. Modern applications must process millions of users simultaneously and return the correct text, videos, images, and other data to each user in a fast and reliable manner. To handle such high volumes of traffic, most applications have many resource servers with duplicate data between them. A load balancer is a device that sits between the user and the server group and acts as an invisible facilitator, ensuring that all resource servers are used equally.

#### ► Benefits of load balancing:

- **Application availability**
  - Runs application servers without any downtime
  - Automatic disaster recovery to backup sites
  - Performs health checks and prevents downtime
- **Application Scalability**

- Prevents traffic bottlenecks at any one server
- Predicts application traffic so that you can add or remove different servers, if needed
- Adds redundancy to your system so that you can scale with confidence

- **Application Scalability**

- Monitor traffic and block malicious content
- Automatically redirect attack traffic to multiple backend servers to minimize impact
- Route traffic through a group of network firewalls for additional security

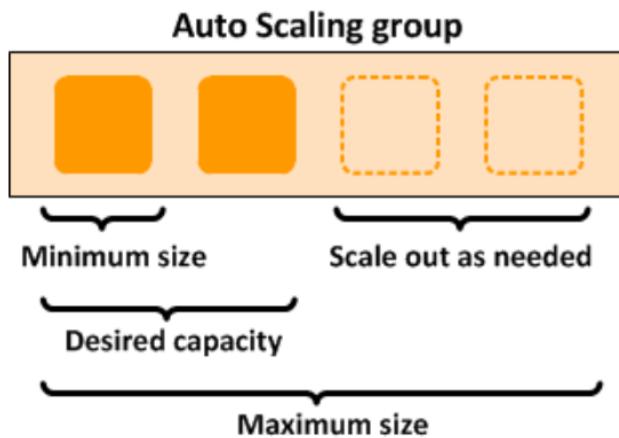
- **Application Performance**

- Distribute the load evenly between server to improve app performance
- Redirect client requests to geographically closer server to reduce latency
- Ensure the reliability and performance of physical and virtual computing resources

### ► **What is Auto Scaling ?**

Amazon EC2 Auto Scaling helps you ensure that you have the correct number of Amazon EC2 instances available to handle the load for your application.

You create collections of EC2 instances, called *Auto Scaling groups*. You can specify the minimum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes below this size. You can specify the maximum number of instances in each Auto Scaling group, and Amazon EC2 Auto Scaling ensures that your group never goes above this size. If you specify the desired capacity, either when you create the group or at any time thereafter, Amazon EC2 Auto Scaling ensures that your group has this many instances. If you specify scaling policies, then Amazon EC2 Auto Scaling can launch or terminate instances as demand on your application increases or decreases.

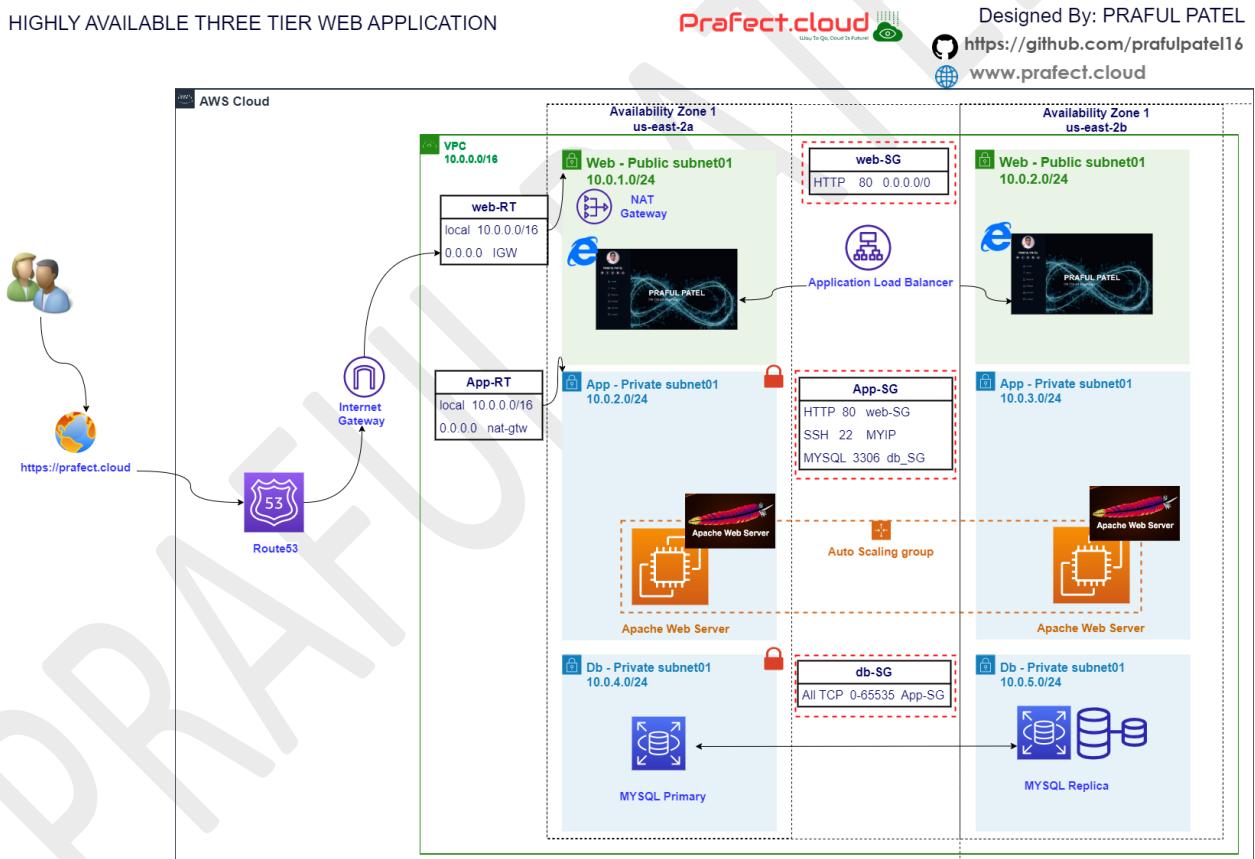


❖ **Challenges or Improvement Tasks to be implemented:**

- ▶ Challenge 1: Reproduce core components – 3tier app
  - ✓ Solution 1: Core components
    - Compute & storage: web and app servers
    - Database – primary & standby
    - Network – connectivity, load balancers, DNS
- ▶ Challenge 2: Serve to local customers, later global expansion
  - ✓ Solution 2: Core components
    - Regions
    - Availability zones
    - VPCs
- ▶ Challenge 3: Don't over provision resources
  - ✓ Solution 3: Select suitable Type of Workload resources
    - Instances
      - EC2
    - Containers
      - AWS ECS
      - AWS EKS
      - AWS Fargate
    - Serverless
      - AWS Lambda
- ▶ Challenge 4: Handle peak days / times
  - ✓ Solution 4: Auto scaling
    - Capacity groups
    - Scale tiers independently
    - Predefined, predictive, smart scaling

- Managed service

- ▶ Reduce outages
- ✓ Solution 5: Reduce planned and unplanned outages
  - Availability and managed services
  - Automatically failover between AZs
  - High availability with load balancing
    - Application Load balancer
    - Network Load balancer
    - Gateway Load balancer
  - Supports health checks
  - EC2 auto scaling



- ▶ The solution is comprised of the following components:
  - A VPC across two Availability Zones
  - Two public web subnets, two private app subnets, and two private DB subnets
  - An Internet Gateway attached to the VPC
    - A public route table routing internet traffic to the Internet Gateway
    - Two private route tables routing traffic internally within the VPC
  - A frontend web server application Elastic Load Balancing that routes traffic to the Apache Web Servers

- An Auto Scaling group that launches additional Apache Web Servers based on defined scaling policies. Each instance of the web server is based on a launch template, which defines the same configuration for each new web server.
- A hosted zone in Amazon Route 53 with a domain name that routes to the frontend web server Elastic Load Balancing
- An Auto Scaling group that launches additional Apache Web Application Servers based on defined scaling policies. Each instance of the Apache Web Application server is based on a launch template, which defines the same configuration and software components for each new application server
- A MySQL Amazon Relational Database Service (Amazon RDS) Multi-AZ deployment for MySQL RDS to store the contact management and role access tables

➤ **Tools & Technologies covered:**

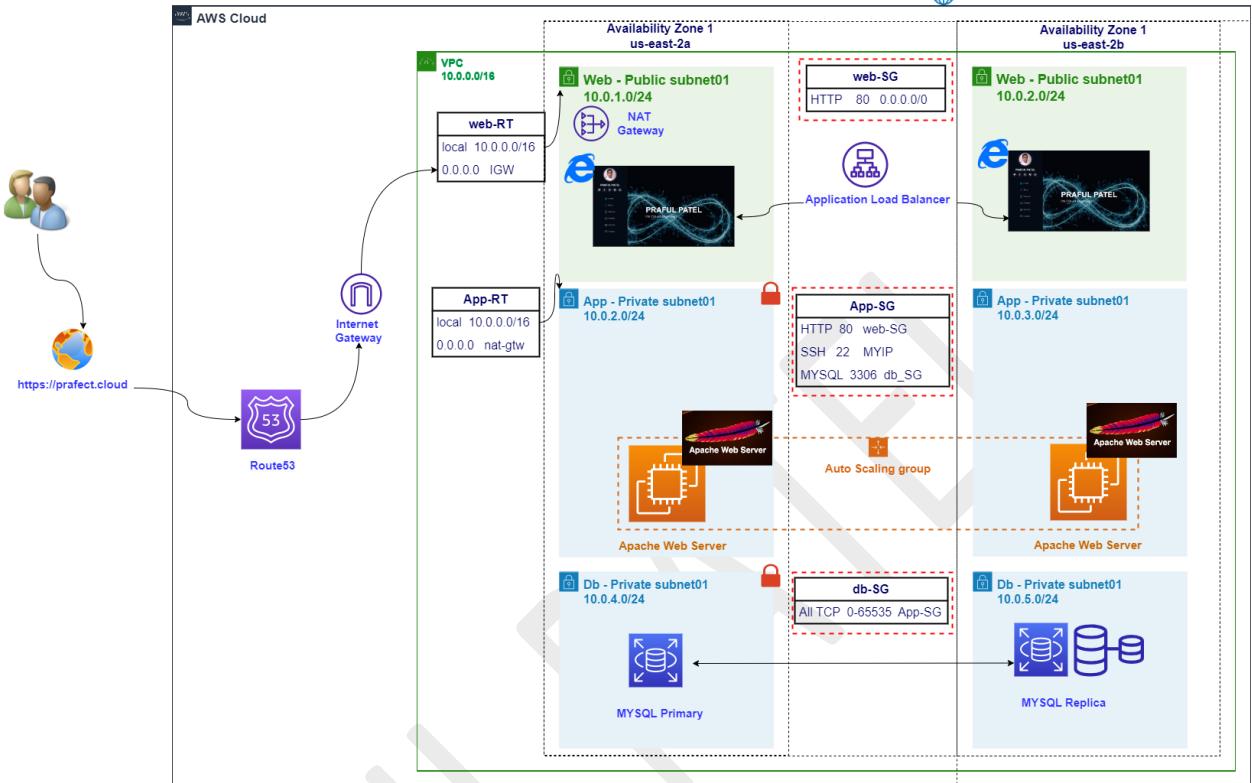
1. AWS cloud
2. VPC
  - Subnets
  - Internet Gateway
  - NAT Gateway
  - Route tables
  - Security Groups
3. EC2 Machine
4. Application Load balancer
5. Auto scaling
6. Launch template
7. RDS Database - MySQL
8. MobaXterm SSH client

## ➤ Architectural Diagram:

HIGHLY AVAILABLE THREE TIER WEB APPLICATION

PraFect.cloud 

Designed By: PRAFUL PATEL  
<https://github.com/prafulpatel16>  
[www.prafect.cloud](http://www.prafect.cloud)



This High availability project will be completed following implementation phases.

## ➤ Project implementation Phases:

- Phase 1: Deploy networking infrastructure
- Phase 2: Deploy Launch Template
- Phase 3: Create elastic load balancer, auto scaling group, target group
- Phase 4: Verify that web application is accessible
- Phase 5: Test horizontal scaling, high availability of web application
- Phase 6: Deploy RDS DB managed MySQL instance

## ➤ Implementation:

### ❖ Phase 1: Deploy networking components.

#### 1. Create vpc

1. Name: prafect-vpc
2. CIDR: 10.0.0.0/16

#### 2. Create web Subnets

1. Name: web-public01
  1. Availability zone: us-east-2a
  2. CIDR: 10.0.1.0/24
2. Name: web-public02
  1. Availability zone: us-east-2b

2. CIDR: 10.0.2.0/24

### 3. Create app Subnets

1. Name: app-private01
  1. Availability zone: us-east-2a
  2. CIDR: 10.0.3.0/24
2. Name: app-private02
  1. Availability zone: us-east-2b
  2. CIDR: 10.0.4.0/24

### 4. Create db Subnets

1. Name: db-private01
  1. Availability zone: us-east-2a
  2. CIDR: 10.0.5.0/24
2. Name: db-private02
  1. Availability zone: us-east-2b
  2. CIDR: 10.0.6.0/24

### 5. Create Internet Gateway

1. Name: web-igw
2. Attach to VPC: prafect-vpc

### 6. Create NAT Gateway

1. Name: prafect-NAT
2. Subnet: web-public01
3. Connectivity: Public
4. Elastic Ip: Allocate Elastic IP

### 7. Create Route table – web-RT

1. Name: Web-RT
2. Select the VPC: prarect-vpc
3. Subnet Associations
  1. Select – web-public01
  2. Select – web-public02
4. Routes – Add internet gateway as route from 0.0.0.0/0
  1. Destination: 0.0.0.0/0
  2. Target: Select internet gateway: web-igw

### 8. Create Route table – App-RT

1. Name: App-RT
2. Select the VPC: prafect-vpc
3. Subnet Associations
  1. Select – app-private01
  2. Select – app-private02
4. Routes – Add NAT 0.0.0.0/0
  1. Destination: 0.0.0.0/0
  2. Target: Select NAT gateway

### 9. Create security Groups

#### 1. Create one security group for web traffic

1. Name: web-SG
2. VPC: prafect-vpc
3. Inbound rule:
  1. Type: HTTP
  2. Protocol: TCP

3. Port Range: 80
4. Source: 0.0.0.0/0

## 2. Create second security group for App traffic

1. Name: app-SG
2. VPC: prafec-vpc
3. Inbound rule 1:
  1. Type: HTTP
  2. Protocol: TCP
  3. Port Range: 80
  4. Source: anywhere : web-SG
4. Inbound rule 2:
  1. Type: MYSQL/Aurora
  2. Protocol: TCP
  3. Port Range: 3306
  4. Source: anywhere : db-SG
5. Inbound rule 3:
  1. Type: SSH (if need to access app instance by admin)
  2. Protocol: TCP
  3. Port Range: 22
  4. Source: anywhere : MYIP

## 3. Create third security group for db traffic

1. Name: db-SG
2. VPC: prafec-vpc
3. Inbound rule 1:
  1. Type: ALL TCP
  2. Protocol: TCP
  3. Port Range: 0-65635
  4. Source: anywhere : app-SG

### ❖ Phase 2: Deploy Launch Template

1. Create Launch Template: instances
2. Target Group name: app-TG
  1. Protocol: TCP
  2. Port: 80
  3. VPC: prafec-vpc
3. Health checks
  1. Health check protocol: HTTP
4. Advanced health check
  1. Port: Traffic port
  2. Healthy threshold: 3
  3. Unhealthy threshold: 3
  4. Timeout: 4
  5. Interval: 10 seconds

### ❖ Phase 3: Deploy Target Group

5. Choose target group: instances

6. Target Group name: app-TG
  1. Protocol: TCP
  2. Port: 80
  3. VPC: prefect-vpc
7. Health checks
  1. Health check protocol: HTTP
8. Advanced health check
  1. Port: Traffic port
  2. Healthy threshold: 3
  3. Unhealthy threshold: 3
  4. Timeout: 4
  5. Interval: 10 seconds

❖ **Phase 4: Deploy Application Load Balancer**

9. Create Launch template
10. Create Application Load Balancer
  1. Name: web-ALB
  2. Scheme: internet-facing
  3. Ip address: ipv4
  4. Network mapping:
    1. Select VPC: web-vpc
    2. Mappings: select: us-east-1a, us-east1b
    3. Security Groups: select: web-ALB-SG
    4. Listener:
      1. HTTP:80
      2. Default action: Target Group

❖ **Phase 5: Deploy Auto Scaling Group**

11. Name: web-ASG
12. Launch template: web-template
13. Network:
  1. VPC: web-vpc
  2. Availability Zones: us-east-1a, us-east-1b
  3. Load Balancing: Attach to and existing load balancer
  4. Choose Target Group: web-TG
  5. Health Check: ELB: 300 seconds
  6. Group Size:
    1. Units
    2. Desired Capacity: 2
    3. Minimum Capacity: 2
    4. Maximum Capacity:4
  7. Scaling Policies:
    1. Name: Target Tracking Policy
    2. Metric Type: Average CPU Utilization
    3. Target Value: 50
    4. Warm up: 300 seconds

❖ **Phase 6: Verify that web application is accessible**

- 1. Go to application load balancer

- 2. Access the ALB DNS and access the web application

#### ❖ **Phase 7: Deploy RDS DB managed MYSQL instance**

- **Create DB instance group**

- Go to Subnet groups
- Create DB subnet group
  - Name: db-subnetgroup
  - Vpc: prefect-vpc
  - Add subnets:
    - Availability Zone: us-east-2a, us-east-2b
    - Subnets: db-private01, db-private02
  - Create

- **Create DB instance – MYSQL**

- **Create database**
- Standard create
- Engine options: MySQL
- Engine version: 5.7.39
- Template: Dev/Test
- Availability: Single DB Instance
- Settings:
  - DB instance: mysql
  - Credentials: master username: admin
    - Password: Passw0rd!
- Connectivity:
  - VPC: prefect-vpc
  - DBsubnet group: dbsubnet
  - Public class: No
- Existing SG group: db-SG
- Database Authentication: Password authentication

➤ **Pre-requisite:**

- 1) AWS Free Tier
- 2) Web Application source code
- 3) Webserver installation script file
- 4) SSH Client

➤ **Implementation in an Action:**

Create VPC

CIDR: 10.0.0.0/16

VPC settings

Resources to create [Info](#)  
Create only the VPC resource or the VPC and other networking resources.

VPC only 1  VPC and more

Name tag - optional  
Creates a tag with a key of 'Name' and a value that you specify.

prefect-vpc 2

IPv4 CIDR block [Info](#)  
 IPv4 CIDR manual input 3  
 IPAM-allocated IPv4 CIDR block

IPv4 CIDR  10.0.0.0/16 4

IPv6 CIDR block [Info](#)  
 No IPv6 CIDR block  
 IPAM-allocated IPv6 CIDR block  
 Amazon-provided IPv6 CIDR block  
 IPv6 CIDR owned by me

Tenancy [Info](#)  
 Default 5

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional
<input type="text"/> Name	<input type="text"/> prefect-vpc <span>6</span>

[Add new tag](#)  
You can add 49 more tags.

[Cancel](#) [Create VPC](#)

Create Web-public subnets

1. Create Subnets

1. Name: web-public01
  1. Availability zone: us-east-2a
  2. CIDR: 10.0.1.0/24
2. Name: web-public02
  1. Availability zone: us-east-2b
  2. CIDR: 10.0.2.0/24

[VPC](#) [Route 53](#) [EC2](#) [S3](#) [CloudFront](#) [Certificate Manager](#) [CloudWatch](#) [Simple Notification Service](#) [AWS FIS](#) [IAM](#)

**Subnet 1 of 2**

**Subnet name**  
Create a tag with a key of 'Name' and a value that you specify.

1.

The name can be up to 256 characters long.

**Availability Zone** [Info](#)  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

2.

**IPv4 CIDR block** [Info](#)

3.

**Tags - optional**

Key	Value - optional
<input type="text" value="Name"/>	<input type="text" value="web-public01"/>

[Add new tag](#)

You can add 49 more tags.

[Remove](#)

**Subnet 2 of 2**

**Subnet name**  
Create a tag with a key of 'Name' and a value that you specify.

4.

The name can be up to 256 characters long.

**Availability Zone** [Info](#)  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

5.

**IPv4 CIDR block** [Info](#)

6.

**Tags - optional**

Key	Value - optional
-----	------------------

[VPC dashboard](#) [Route 53](#) [EC2](#) [S3](#) [CloudFront](#) [Certificate Manager](#) [CloudWatch](#) [Simple Notification Service](#) [AWS FIS](#) [IAM](#)

You have successfully created 2 subnets: subnet-08ac1353d5fa03389, subnet-063a9789f581f151d

**Subnets (2) [Info](#)**

<input type="checkbox"/>	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 a
<input type="checkbox"/>	web-public02	subnet-063a9789f581f151d	Available	vpc-024a44812f7630f8a   pra...	10.0.2.0/24	-	251
<input type="checkbox"/>	web-public01	subnet-08ac1353d5fa03389	Available	vpc-024a44812f7630f8a   pra...	10.0.1.0/24	-	251

## Create App-private subnets

### 1. Create Subnets

1. Name: app-private01
  1. Availability zone: us-east-2a
  2. CIDR: 10.0.2.0/24
2. Name: app-private02
  1. Availability zone: us-east-2b
  2. CIDR: 10.0.3.0/24

**Create subnet** [Info](#)

**VPC**

**VPC ID**  
Create subnets in this VPC.  
vpc-024a44812f7630f8a (prefect-vpc) 1

**Associated VPC CIDRs**  
IPv4 CIDRs  
10.0.0.0/16

**Subnet settings**  
Specify the CIDR blocks and Availability Zone for the subnet.

**Subnet 1 of 2**

**Subnet name**  
Create a tag with a key of 'Name' and a value that you specify.  
app-private01 2  
The name can be up to 256 characters long.

**Availability Zone** [Info](#)  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.  
US East (Ohio) / us-east-2a 3

**IPv4 CIDR block** [Info](#)  
Q 10.0.3.0/24 4

**Tags - optional**  
Key Value - optional  
Q Name X Q app-private01 X Remove  
Add new tag  
You can add 49 more tags.

**Subnet 2 of 2**

**Subnet name**  
Create a tag with a key of 'Name' and a value that you specify.  
app-private02 1  
The name can be up to 256 characters long.

**Availability Zone** [Info](#)  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.  
US East (Ohio) / us-east-2b 2

**IPv4 CIDR block** [Info](#)  
Q 10.0.4.0/24 3

**Tags - optional**  
Key Value - optional  
Q Name X Q app-private02 X Remove  
Add new tag  
You can add 49 more tags.

**Remove**  
**Add new subnet**

4 **Create subnet**

**VPC dashboard** X

**EC2 Global View** New

**Filter by VPC:** Select a VPC

**Virtual private cloud**

**Your VPCs**

**Subnets**

Route tables  
Internet gateways  
Egress-only internet gateways  
DHCP option sets

**Subnets (2) [Info](#)**

**Subnet ID:** subnet-050cdc2ef3b68f4e6 X **Subnet ID:** subnet-06c007c74f2f7740f X **Clear filters**

	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 a
<span style="border: 1px solid red; border-radius: 50%; padding: 2px;">1</span>	app-private02	subnet-06c007c74f2f7740f	<span style="color: green;">Available</span>	vpc-024a44812f7630f8a   pra...	10.0.4.0/24	-	251
<span style="border: 1px solid red; border-radius: 50%; padding: 2px;">2</span>	app-private01	subnet-050cdc2ef3b68f4e6	<span style="color: green;">Available</span>	vpc-024a44812f7630f8a   pra...	10.0.3.0/24	-	251

## Create Data-private subnets

### 1. Create Subnets

#### 1. Name: data-private01

1. Availability zone: us-east-2a
2. CIDR: 10.0.5.0/24

#### 2. Name: data-private02

1. Availability zone: us-east-2b
2. CIDR: 10.0.6.0/24

VPC > Subnets > Create subnet

Create subnet [Info](#)

**VPC**

VPC ID  
Create subnets in this VPC.  
vpc-024a44812f7630f8a (prefect-vpc) 1

Associated VPC CIDRs  
IPv4 CIDRs  
10.0.0.0/16

**Subnet settings**  
Specify the CIDR blocks and Availability Zone for the subnet.

**Subnet 1 of 1**

Subnet name  
Create a tag with a key of 'Name' and a value that you specify.  
data-private01 2  
The name can be up to 256 characters long.

Availability Zone [Info](#)  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.  
US East (Ohio) / us-east-2a 3

IPv4 CIDR block [Info](#)  
Q 10.0.5.0/24 4

▼ Tags - optional  
Key Value - optional  
Q Name X Q data-private01 X Remove  
Add new tag

**Subnet 2 of 2**

Subnet name  
Create a tag with a key of 'Name' and a value that you specify.  
data-private02 1  
The name can be up to 256 characters long.

Availability Zone [Info](#)  
Choose the zone in which your subnet will reside, or let Amazon choose one for you.  
US East (Ohio) / us-east-2b 2

IPv4 CIDR block [Info](#)  
Q 10.0.6.0/24 3

▼ Tags - optional  
Key Value - optional  
Q Name X Q data-private02 X Remove  
Add new tag  
You can add 49 more tags.  
Remove  
Add new subnet

4 Create subnet

All subnets created successfully

	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 a...
<input type="checkbox"/>	app-private01	subnet-050cdc2ef5b68f4e6	Available	vpc-024a44812f7630f8a   pr...	10.0.3.0/24	-	251
<input type="checkbox"/>	app-private02	subnet-06c007c74f2f7740f	Available	vpc-024a44812f7630f8a   pr...	10.0.4.0/24	-	251
<input type="checkbox"/>	data-private01	subnet-0e897818fc46ee889	Available	vpc-024a44812f7630f8a   pr...	10.0.5.0/24	-	251
<input type="checkbox"/>	data-private02	subnet-07f990de50647510a	Available	vpc-024a44812f7630f8a   pr...	10.0.6.0/24	-	251
<input type="checkbox"/>	web-public01	subnet-08ac1353d5fa03389	Available	vpc-024a44812f7630f8a   pr...	10.0.1.0/24	-	251
<input type="checkbox"/>	web-public02	subnet-063a9789f581f151d	Available	vpc-024a44812f7630f8a   pr...	10.0.2.0/24	-	251

## Create Internet Gateway

1. Create Internet Gateway
  1. Name: web-igw
  2. Attach to VPC: web-vpc

Internet gateways (1/1) <small>Info</small>					
<input type="checkbox"/> <small>Filter internet gateways</small>					
<input checked="" type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner
<input checked="" type="checkbox"/>	-	igw-05bb23de610aca27f	Attached	vpc-05f3e3d6d1ff2c3fb	914141388779

Internet gateway settings

Name tag  
Creates a tag with a key of 'Name' and a value that you specify.

web-IGW

Tags - optional

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key: Name, Value - optional: web-IGW

Add new tag

2

Create Internet gateway

The screenshot shows the AWS VPC Internet Gateways page. A new internet gateway, 'igw-023bc1ddebab1a1be', has been created. The 'Attach to a VPC' button is highlighted with a red arrow.

The screenshot shows the 'Attach to VPC' dialog box. The VPC dropdown menu is open, showing 'vpc-024a44812f7630f8a - prefect-vpc'. The 'Attach internet gateway' button is highlighted with a red arrow.

The screenshot shows the AWS VPC Internet Gateways page. The internet gateway 'igw-023bc1ddebab1a1be' is successfully attached to the VPC 'vpc-024a44812f7630f8a | prefect-vpc'. The 'Attached' status is highlighted with a green box.

## Create Route Tables

### 1. Create Web Route table

1. Name: Web-RT
2. Select the VPC: web-vpc
3. Subnet Associations
  1. Select – web-public01
  2. Select – web-public02
4. Routes – Add internet gateway as route from 0.0.0.0/0
  1. Destination: 0.0.0.0/0
  2. Target: Select internet gateway: web-igw

EC2 VPC CloudWatch Simple Notification Service Route 53 CloudFront AWS FIS IAM

VPC > Route tables > Create route table

### Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

**Route table settings**

Name - optional  
Create a tag with a key of 'Name' and a value that you specify.  
web-RT 1

VPC  
The VPC to use for this route table.  
vpc-0f032fa0af9e6357f (web-vpc) 2

**Tags**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key Value - optional  
Name web-RT 3 Remove

Add new tag You can add 49 more tags.

Cancel Create route table

## Web subnet association

EC2 VPC CloudWatch Simple Notification Service Route 53 CloudFront AWS FIS IAM

New VPC Experience Tell us what you think

VPC dashboard EC2 Global View New

Filter by VPC: Select a VPC

**Virtual private cloud**  
Your VPCs  
Subnets  
**Route tables**  
Internet gateways  
Egress-only internet gateways  
Carrier gateways  
DHCP option sets  
Elastic IPs  
Managed prefix lists  
Endpoints  
Endpoint services  
NAT gateways  
Peering connections

**Security**  
Network ACLs  
Security groups

**Network Analysis**  
Reachability Analyzer  
Network Access Analyzer

Route table rtb-0b71c662fc25fb83e | web-RT was created successfully.

VPC > Route tables > rtb-0b71c662fc25fb83e / web-RT

Actions

You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer

**Details** Info

Route table ID rtb-0b71c662fc25fb83e	Main No	Explicit subnet associations —	Edge associations —
VPC vpc-0f032fa0af9e6357f   web-vpc	Owner ID 914141388779		

Routes Subnet associations Edge associations Route propagation Tags

**Explicit subnet associations (0)** Edit subnet associations

Subnet ID IPv4 CIDR IPv6 CIDR

No subnet associations  
You do not have any subnet associations.

**Subnets without explicit associations (2)** Edit subnet associations

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

VPC Route 53 EC2 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

VPC dashboard EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud Your VPCs Subnets **Route tables** Internet gateways Egress-only internet gateways DHCP option sets Elastic IPs Managed prefix lists Endpoints Endpoint services NAT gateways Peering connections

Security Network ACLs Security groups

Network Analysis Reachability Analyzer Network Access Analyzer

DNS firewall Rule groups Domain lists

Network Firewall

Details Info

Route table ID: rtb-031013f268408fdee Main: No Owner ID: vpc-024a44812f7630f8a | prafect-vpc

Explicit subnet associations: - Edge associations: -

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (0) Find subnet association Edit subnet associations

No subnet associations You do not have any subnet associations.

Subnets without explicit associations (6) Find subnet association Edit subnet associations

Name Subnet ID IPv4 CIDR IPv6 CIDR

data-private01	subnet-0e897818fc46ee889	10.0.5.0/24	-
web-public02	subnet-063a9789f581f151d	10.0.2.0/24	-
app-private02	subnet-06c007c74f2f7740f	10.0.4.0/24	-
app-private01	subnet-050cdc2ef3b68f4e6	10.0.3.0/24	-
web-public01	subnet-08ac1355d5fa03389	10.0.1.0/24	-
data-private02	subnet-07f790de306475104	10.0.6.0/24	-

VPC Route 53 EC2 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

VPC > Route tables > rtb-031013f268408fdee > Edit subnet associations

### Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/6) Filter subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
data-private01	subnet-0e897818fc46ee889	10.0.5.0/24	-	Main (rtb-042d02a2a4ea6a8c0)
<input checked="" type="checkbox"/> web-public02	subnet-063a9789f581f151d	10.0.2.0/24	-	Main (rtb-042d02a2a4ea6a8c0)
<input type="checkbox"/> app-private02	subnet-06c007c74f2f7740f	10.0.4.0/24	-	Main (rtb-042d02a2a4ea6a8c0)
<input type="checkbox"/> app-private01	subnet-050cdc2ef3b68f4e6	10.0.3.0/24	-	Main (rtb-042d02a2a4ea6a8c0)
<input checked="" type="checkbox"/> web-public01	subnet-08ac1355d5fa03389	10.0.1.0/24	-	Main (rtb-042d02a2a4ea6a8c0)
<input type="checkbox"/> data-private02	subnet-07f790de306475104	10.0.6.0/24	-	Main (rtb-042d02a2a4ea6a8c0)

Selected subnets

subnet-063a9789f581f151d / web-public02   subnet-08ac1355d5fa03389 / web-public01  

Cancel Save associations

3

Web Subnets associated successfully

You have successfully updated subnet associations for rtb-031013f268408fdee / web-RT.

VPC > Route tables > rtb-031013f268408fdee / web-RT

Actions ▾ Run Reachability Analyzer X

Details Info

Route table ID rtb-031013f268408fdee	Main No	Explicit subnet associations 2 subnets	Edge associations -
VPC vpc-024a44812f7630f8a   prefect-vpc	Owner ID 914141388779		

Routes Subnet associations Edge associations Route propagation Tags

Explicit subnet associations (2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
web-public02	subnet-063a9789f581f151d	10.0.2.0/24	-
web-public01	subnet-08ac1353d5fa03389	10.0.1.0/24	-

Subnets without explicit associations (4)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
data-private01	subnet-0e897818fc46ee889	10.0.5.0/24	-
app-private02	subnet-06c007c74f2f7740f	10.0.4.0/24	-
app-private01	subnet-050cdc2ef3b68f4e6	10.0.3.0/24	-
data-private02	subnet-07f790de306475104	10.0.6.0/24	-

## Add Route to Internet Gateway

Web-subnet needs to have internet connectivity so need to add route from internet gateway  
Add Internet gateway as route

VPC dashboard X EC2 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

VPC > Route tables > rtb-031013f268408fdee

rtb-031013f268408fdee / web-RT

Actions ▾ Run Reachability Analyzer X

Details Info

Route table ID rtb-031013f268408fdee	Main No	Explicit subnet associations 2 subnets	Edge associations -
VPC vpc-024a44812f7630f8a   prefect-vpc	Owner ID 914141388779		

1 Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

VPC > Route tables > rtb-031013f268408fdee > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

Add route 1

Cancel Preview Save changes

Destination: 0.0.0.0/0

Target: Internet gateway

Destination: 10.0.0.0/16

Target: local

Status: Active

Propagated: No

Target dropdown options (visible): Carrier Gateway, Core Network, Egress Only Internet Gateway, Gateway Load Balancer Endpoint, Instance, Internet Gateway, local, NAT Gateway, Network Interface, Outpost Local Gateway, Peering Connection, Transit Gateway, Virtual Private Gateway

Buttons: Cancel, Preview, Save changes (with red circle 2)

Destination: 10.0.0.0/0

Target: igw-023bc1ddebab1a1be (web-igw)

Status: Active

Propagated: No

Target dropdown options (visible): local, Internet Gateway, igw-, local, Internet Gateway

Buttons: Cancel, Preview, Save changes (with red circle 2)

Updated routes for rtb-031013f268408fdee / web-RT successfully

rtb-031013f268408fdee / web-RT

Details Info

Route table ID: rtb-031013f268408fdee

Main: No

Owner ID: 914141388779

Explicit subnet associations: 2 subnets

Edge associations: -

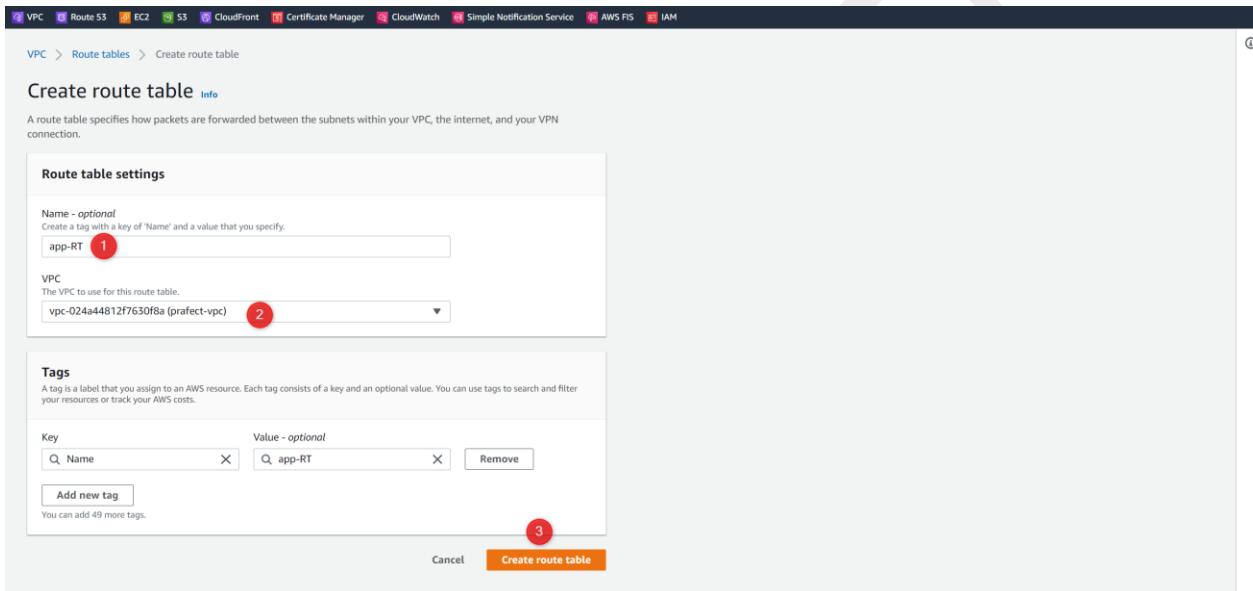
Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-023bc1ddebab1a1be	Active	No
10.0.0.0/16	local	Active	No

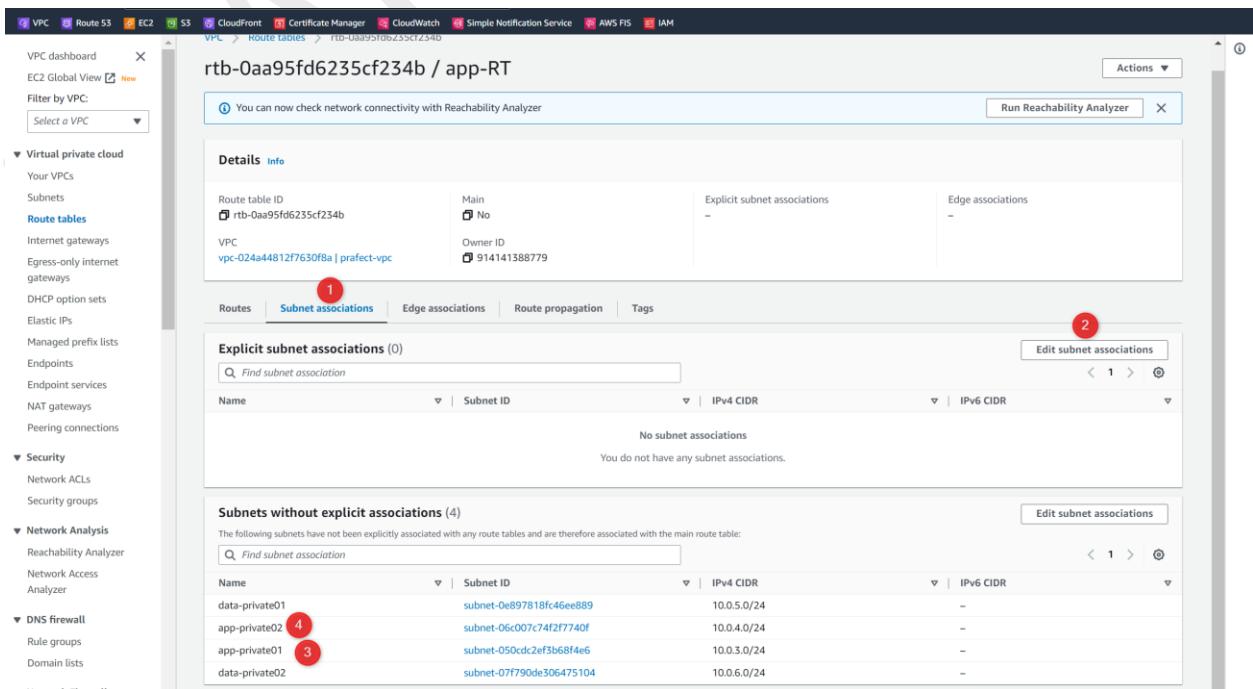
Buttons: Run Reachability Analyzer, Edit routes

## 1. Create App Route table

1. Name: App-RT
2. Select the VPC: web-vpc
3. Subnet Associations
  1. Select – app-private01
  2. Select – web-private02
4. Routes – Add internet gateway as route from 0.0.0.0/0
  1. Destination: 0.0.0.0/0
  2. Target: Select internet gateway: web-igw



## App subnet association



VPC > Route tables > rtb-0aa95fd6235cf234b > Edit subnet associations

**Edit subnet associations**

Change which subnets are associated with this route table.

**Available subnets (2/6)**

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
data-private01	subnet-0e897818fc46ee889	10.0.5.0/24	-	Main (rtb-042d02a2a4ea6a8c0)
web-public02	subnet-063a9789f581f151d	10.0.2.0/24	-	rtb-031013f268408fdee / web-RT
<b>app-private02</b> <span style="color: red;">2</span>	subnet-06c007c74f2f7740f	10.0.4.0/24	-	Main (rtb-042d02a2a4ea6a8c0)
<b>app-private01</b> <span style="color: red;">1</span>	subnet-050cdc2ef3b68f4e6	10.0.3.0/24	-	Main (rtb-042d02a2a4ea6a8c0)
web-public01	subnet-08ac1353d5fa03389	10.0.1.0/24	-	rtb-031013f268408fdee / web-RT
data-private02	subnet-07f790de506475104	10.0.6.0/24	-	Main (rtb-042d02a2a4ea6a8c0)

**Selected subnets**

subnet-050cdc2ef3b68f4e6 / app-private01 X subnet-06c007c74f2f7740f / app-private02 X

3 Cancel Save associations

App Subnets associated successfully

VPC dashboard > Route tables > rtb-0aa95fd6235cf234b / app-RT

You have successfully updated subnet associations for rtb-0aa95fd6235cf234b / app-RT.

rtb-0aa95fd6235cf234b / app-RT

Details Info

Route table ID	Main	Explicit subnet associations	Edge associations
rtb-0aa95fd6235cf234b	No	2 subnets	-
VPC	Owner ID		
vpc-024a44812f7630f8a   prefect-vpc	914141388779		

Actions ▼

Run Reachability Analyzer X

Subnet associations Edit subnet associations

Subnet associations (2)

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
app-private02	subnet-06c007c74f2f7740f	10.0.4.0/24	-
app-private01	subnet-050cdc2ef3b68f4e6	10.0.3.0/24	-

Explicit subnet associations (2) Edit subnet associations

Subnets without explicit associations (2)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
data-private01	subnet-0e897818fc46ee889	10.0.5.0/24	-
data-private02	subnet-07f790de506475104	10.0.6.0/24	-

## 1. Create Security Groups

### 1. Create one security group for web public subnets

1. Name: web-SG
2. VPC: prefect-vpc
3. Inbound rule:
  1. Type: HTTP
  2. Protocol: TCP
  3. Port Range: 80
  4. Source: anywhere : 0.0.0.0/0

**Create security group**

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

**Basic details**

Security group name: **web-SG** (1)

Description: **Allows internet access to web subnets** (2)

VPC: **vpc-024a44812f7630f8a** (3)

**Inbound rules**

Type: **HTTP** (4)

Protocol: **TCP**

Port range: **80**

Source: **Anywhere (0.0.0.0/0)** (5)

Description - optional:  (6)

**Outbound rules**

Type: **All traffic**

Protocol: **All**

Port range: **All**

Destination: **Custom**

Description - optional:

**sg-01ff419fd0cd6fe91 - web-SG**

**Details**

Security group name: <b>web-SG</b>	Security group ID: <b>sg-01ff419fd0cd6fe91</b>	Description: <b>Allows internet access to web subnets</b>	VPC ID: <b>vpc-024a44812f7630f8a</b>
Owner: <b>914141388779</b>	Inbound rules count: <b>1 Permission entry</b>	Outbound rules count: <b>1 Permission entry</b>	

**Inbound rules (1/1)**

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
-	sgr-068cd11e9be8232...	IPv4	HTTP	TCP	80	0.0.0.0/0

## 1. Create second security group for app private subnets

1. Name: app-SG
2. VPC: prefect-vpc
3. Inbound rule 1:
  1. Type: Custom TCP
  2. Protocol: TCP
  3. Port Range: custom
  4. Source: Security group ref : web-SG

**Create security group** Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group

**Basic details**

Security group name Info **app-SG** **1**  
Name cannot be edited after creation.

Description Info Allow inbound traffic from web-SG only **2**

VPC Info **vpc-024a44812f7630f8a** **3**

**Inbound rules** Info

Type	Protocol	Port range	Source
Custom TCP	TCP	0	Custom

**Add rule**

**Outbound rules** Info

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	0.0.0.0/0

**sg-05955a1727b715e72 - app-SG**

**Details**

Security group name: app-SG | Security group ID: sg-05955a1727b715e72 | Description: Allow inbound traffic from web-SG only | VPC ID: vpc-024a44812f7630f8a

Owner: 914141388779 | Inbound rules count: 1 Permission entry | Outbound rules count: 1 Permission entry

**Inbound rules** **Outbound rules** **Tags**

**Inbound rules (1/1)**

Name	Security group rule...	IP version	Type	Protocol	Port ra...	Source
sgr-03637bf40ec168a64	-	-	Custom TCP	TCP	0	sg-01ff419fd0cd6fe91 / web-SG

1. Create second security group for app private subnets
  1. Name: db-SG
  2. VPC: prefect-vpc
  3. Inbound rule 1:
    1. Type: Custom TCP
    2. Protocol: TCP
    3. Port Range: custom
    4. Source: Security group ref : app-SG

Basic details

Security group name: db-SG (1)

Description: Allow traffic from app-SG only (2)

VPC: vpc-024a44812f7630f8a (3)

Inbound rules

Type: Custom TCP (4)

Protocol: TCP

Port range: 0

Source: app-SG (5)

Outbound rules

Type: All traffic

Destination: 0.0.0.0/0 (6)

VPC Route 53 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

Security group (sg-07b9a1eda87c5b837 | db-SG) was created successfully

Details

Virtual private cloud

Your VPCs Subnets Route tables Internet gateways Egress-only internet gateways DHCP option sets Elastic IPs Managed prefix lists Endpoints Endpoint services NAT gateways Peering connections

Security groups

Network ACLs

Security groups

Network Analysis

Reachability Analyzer Network Access Analyzer

DNS firewall

sg-07b9a1eda87c5b837 - db-SG

Actions

Details

Security group name	sg-07b9a1eda87c5b837	Description	VPC ID
Owner	914141388779	Inbound rules count	Allow traffic from app-SG only
		1 Permission entry	vpc-024a44812f7630f8a
		Outbound rules count	1 Permission entry
		1 Permission entry	

Inbound rules Outbound rules Tags

You can now check network connectivity with Reachability Analyzer

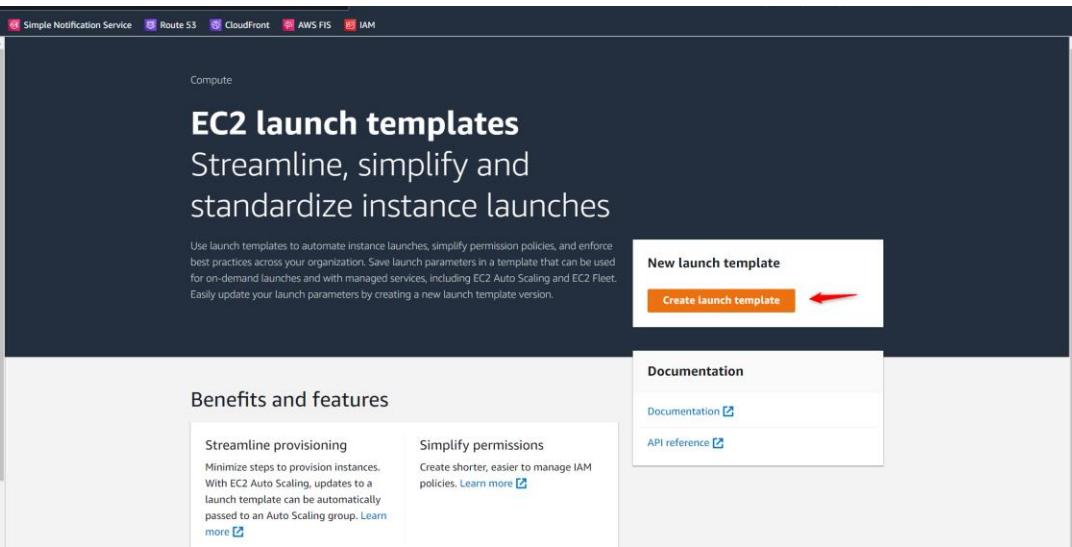
Run Reachability Analyzer

Inbound rules (1/1)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
-	sgr-0ebdde1f2b2d3e125	-	Custom TCP	TCP	0	sg-05955a1727b715e72 / app-SG

## ❖ Phase 2: Create Launch Template

14. Choose target group: instances
15. Target Group name: web-TG
  1. Protocol: TCP
  2. Port: 80
  3. VPC: web-vpc



The screenshot shows the AWS EC2 Launch Templates page. The main heading is "EC2 launch templates" with the subtext "Streamline, simplify and standardize instance launches". Below this, there's a section titled "Benefits and features" with two items: "Streamline provisioning" and "Simplify permissions". A callout box highlights the "Create Launch template" button. To the right, there's a "Documentation" sidebar with links to "Documentation" and "API reference".

**Create launch template**

Creating a launch template allows you to create a saved instance configuration that can be reused, shared and launched at a later time. Templates can have multiple versions.

**Launch template name and description**

**Launch template name - required** **1**  
prefect-template

Must be unique to this account. Max 128 chars. No spaces or special characters like ' ', ' ', '@'.

**Template version description** **2**  
v1

Max 255 chars

**Auto Scaling guidance** [Info](#)  
Select this if you intend to use this template with EC2 Auto Scaling

Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

**Launch template contents**  
Specify the details of your launch template below. Leaving a field blank will result in the field not being included in the launch template.

**Application and OS Images (Amazon Machine Image)** [Info](#)  
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Quick Start

Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below.

Search our full catalog including 1000s of application and OS images

Quick Start

Don't include in launch template

Amazon Linux

macOS

Ubuntu

Windows

aws

Mac

ubuntu

Microsoft

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type [2](#)

Free tier eligible

Canonical, Ubuntu, 18.04 LTS, amd64 bionic image build on 2023-01-31

Architecture AMI ID

64-bit (x86) ami-03a5defb0190cef7

Verified provider

Description

Canonical, Ubuntu, 18.04 LTS, amd64 bionic image build on 2023-01-31

Architecture AMI ID

64-bit (x86) ami-03a5defb0190cef7

Verified provider

Summary

Software Image (AMI)

Canonical, Ubuntu, 18.04 LTS, ... [read more](#)

ami-03a5defb0190cef7

Virtual server type (instance type)

t2.micro

Firewall (security group)

-

Storage (volumes)

1 volume(s) - 8 GiB

**Free tier** in your first year includes 750 hours of t2.micro (or 16 micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GiB of snapshots, and 100 GiB of bandwidth to the internet.

Cancel [Create launch template](#)

Instance type [Info](#)

Manually select instance type [3](#)

Select an instance type that meets your computing, memory, networking, or storage needs.

Specify instance type attributes

Specify instance attributes that match your compute requirements.

Simple

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0116 USD per Hour

On-Demand SUSE pricing: 0.0116 USD per Hour

On-Demand Windows pricing: 0.0162 USD per Hour

On-Demand RHEL pricing: 0.0716 USD per Hour

Free tier eligible [4](#)

Compare instance types

Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

## Create key pair

Route 53 EC2 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

Key pair (login) [Info](#)  
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name  [Create new key pair](#)

Network settings [Info](#)

Subnet [Info](#)  
Don't include in launch template [Create new subnet](#)

When you specify a subnet, a network interface is automatically added to your template.

Firewall (security groups) [Info](#)  
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Select existing security group [Create security group](#)

Common security groups [Info](#)  
Select security groups [Compare security group rules](#)

app-SG [Info](#) [Edit](#) [Remove](#)  
app-SG (arn:aws:ec2:us-east-1:123456789012:security-group/app-SG) [VPC](#) [Edit](#) [Remove](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces.

Advanced network configuration

Network interface 1

Device index [Info](#)  [Remove](#)

Network interface [Info](#)  [Description](#) [Info](#)

Subnet: [Info](#)  
Don't include in launch template [Select security groups](#) [Show all selected \(1\)](#)

Primary IP: [Info](#) [Secondary IP](#) [IPv4 Prefixes](#) [IPv6 Prefixes](#)

Auto-assign public IP: [Info](#)  include in launch tem... [Remove](#)

IPv4 Prefixes [Info](#) [IPv6 Prefixes](#) [Delete on termination](#) [Info](#)

IPv6 Prefixes [Info](#) [Delete on termination](#) [Info](#)

The selected instance type does not support IPv6 prefixes.

Elastic Fabric Adapter [Info](#)  Enable [Edit](#)  
EFA is only compatible with certain instance types.

Network card index [Info](#) [Don't include in launch tem...](#)

The selected instance type does not support IPv6 prefixes.

Summary

Software Image (AMI) [Info](#)  
Canonical, Ubuntu, 18.04 LTS, ... [Read more](#)  
ami-03ad5efb0190ef07

Virtual server type (instance type) [Info](#)  
t2.micro

Firewall (security group) [Info](#)  
app-SG

Storage (volumes) [Info](#)  
1 volume(s) 8 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 100 snapshots, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. [X](#)

[Cancel](#) [Create launch template](#)

The screenshot shows the AWS Lambda 'Create Launch Template' wizard. The current step is 'Summary'.

**Software Image (AMI)**  
Canonical, Ubuntu, 18.04 LTS, ... [read more](#)  
ami-03a5defeb0190cef

**Virtual server type (instance type)**  
t2.micro

**Firewall (security group)**  
app-SG

**Storage (volumes)**  
1 volume(s) - 8 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 30 GiB of EBS storage, 2 million I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet. X

**Cancel** **Create launch template**

**Metadata accessible** [Info](#)  
Don't include in launch template

**Metadata version** [Info](#)  
Don't include in launch template

**Metadata response hop limit** [Info](#)  
Don't include in launch template

**Allow tags in metadata** [Info](#)  
Don't include in launch template

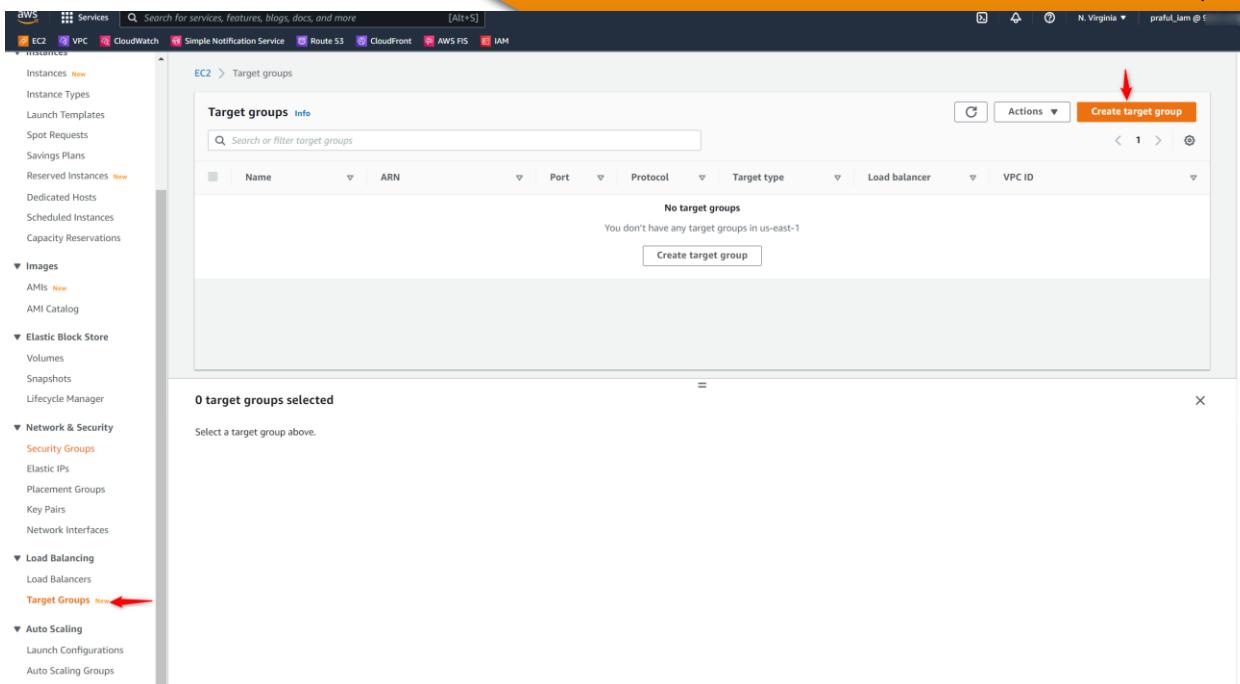
**User data - optional** [Info](#)  
Enter user data in the field.

```
#!/bin/bash
# Purpose: Install apache webserver and copy praful's portfolio web application
from github to apache webserver
# Author: Praful Patel
# Date & Time: SEP 24, 2022
# -----
sudo apt update
sudo apt install -y apache2
sudo ufw allow 'apache full'
sudo apt install software-properties-common
sudo add-apt-repository ppa:ondrej/php
sudo apt install git
sudo apt update
sudo apt install -y php7.4
sudo apt install php7.4-common php7.4-mysql php7.4-xml php7.4-xmlrpc php7.4-curl php7.4-gd php7.4-imagick php7.4-cli php7.4-dev php7.4-imap php7.4-mbstring php7.4-opcache php7.4-soap php7.4-zip php7.4-intl -y
sudo apt update
sudo apt install mysql-client-core-8.0
sudo git clone https://github.com/prafulpatel16/php-html-projects.git
sudo cp -r php-html-projects/Portfolio1_emp/* /var/www/html/
sudo systemctl start apache2
```

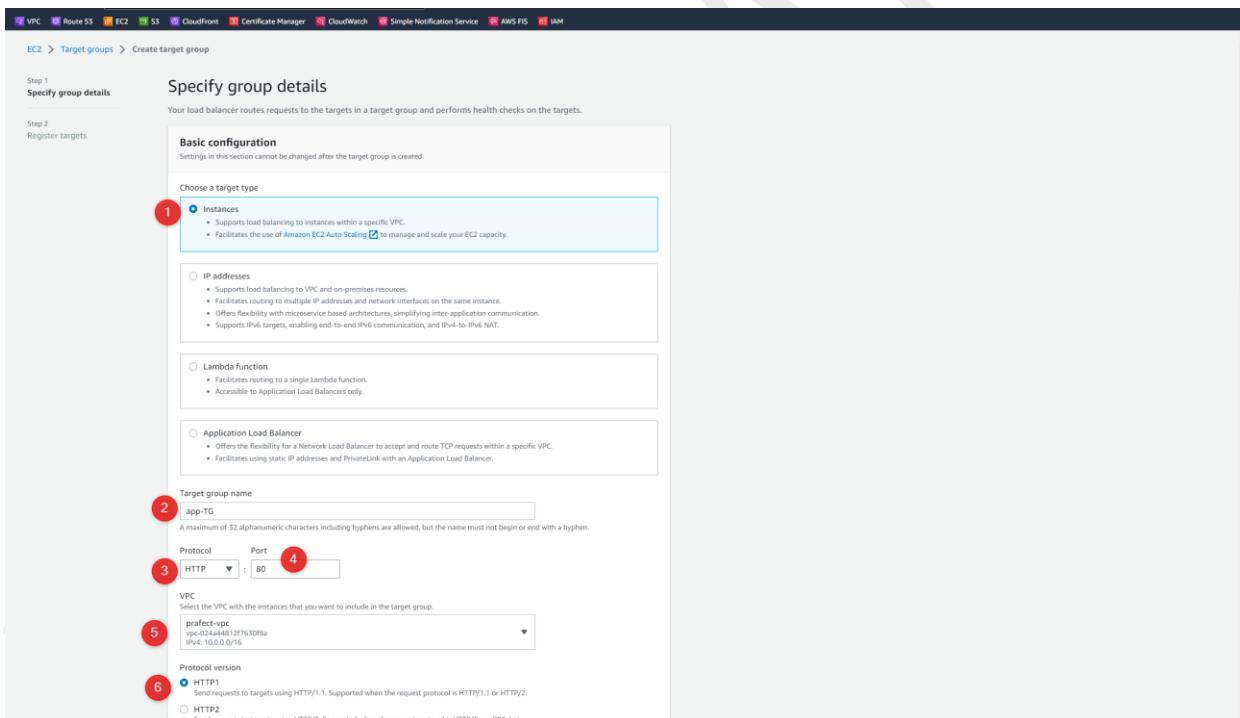
Launch template ID	Launch template name	Default version	Latest version
lt-0c88746db53cdd2f3	prefect-template	1	1

## ❖ Phase 2: Create Target Group

16. Choose target group: instances
17. Target Group name: app-TG
  1. Protocol: TCP
  2. Port: 80
  3. VPC: web-vpc
18. Health checks
  1. Health check protocol: HTTP
19. Advanced health check
  1. Port: Traffic port
  2. Healthy threshold: 3
  3. Unhealthy threshold: 3
  4. Timeout: 4
  5. Interval: 10 seconds



The screenshot shows the AWS EC2 Target groups page. The left sidebar includes sections for Instances, Images, Network & Security, Load Balancing, and Auto Scaling. The 'Target Groups' section is highlighted with a red arrow. The main content area shows a table with columns: Name, ARN, Port, Protocol, Target type, Load balancer, and VPC ID. A message indicates 'No target groups' and 'You don't have any target groups in us-east-1'. A 'Create target group' button is located at the bottom right of the table area.



The screenshot shows the 'Specify group details' step of the 'Create target group' wizard. The 'Basic configuration' section is displayed. Step 1: Specify group details. Step 2: Register targets. The 'Choose a target type' section shows 'Instances' selected (circled 1). The 'Target group name' field contains 'app-TG' (circled 2). The 'Protocol' dropdown is set to 'HTTP' (circled 3) and the 'Port' dropdown is set to '80' (circled 4). The 'VPC' section shows 'prefect-vpc' selected from a dropdown (circled 5). The 'Protocol version' section shows 'HTTP1' selected (circled 6).

EC2 VPC CloudWatch Simple Notification Service Route 53 CloudFront AWS FMS IAM

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** **1**

Health check path:  
Use the default path of "/" to ping the host, or specify a custom path if preferred.  
**/**

Up to 1024 characters allowed.

**Advanced health check settings**

Port:  
The port the load balancer uses when performing health checks on targets. The default is the port on which each target receives traffic from the load balancer, but you can specify a different port.

Traffic port

Override

Healthy threshold:  
The number of consecutive health check successes required before considering a target healthy.  
**5** **2**

Unhealthy threshold:  
The number of consecutive health check failures required before considering a target unhealthy.  
**2** **3**

Timeout:  
The amount of time, in seconds, during which no response means a failed health check.  
**5** **4**  
seconds  
2-100

Interval:  
The approximate amount of time between health checks of an individual target.  
**30** **5**  
seconds  
5-300

Success codes:  
The HTTP codes to use when checking for a successful response from a target. You can specify multiple values (for example, "200,202") or a range of values (for example, "200-299").  
**200** **6**

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

Cancel **Next** **7**

EC2 VPC CloudWatch Simple Notification Service Route 53 CloudFront AWS FMS IAM

EC2 > Target groups > Create target group

Step 1: Specify group details

**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.

Step 2: Register targets

**Available instances (0)**

Filter resources by property or value

Instance ID	Name	State	Security groups	Zone	Subnet ID
No Available instances					

0 selected

Ports for the selected instances  
Ports for routing traffic to the selected instances.  
80  
1-65535 (separate multiple ports with commas)

**Include as pending below**

**Review targets**

Targets (0)

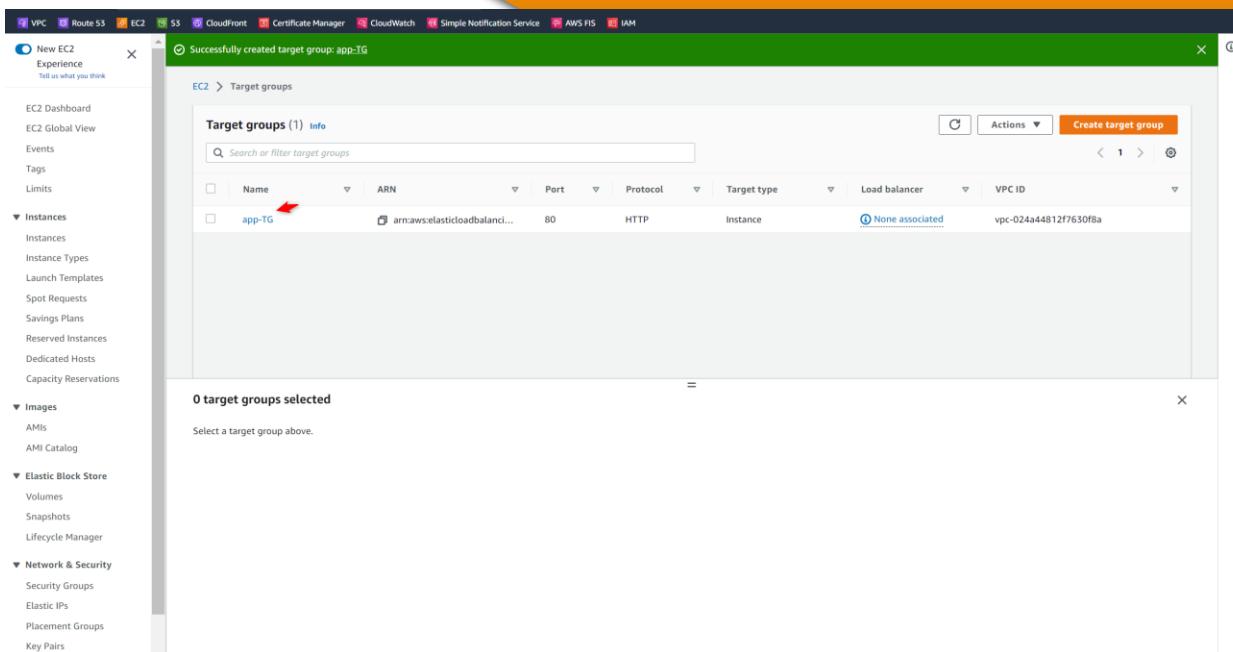
Remove Health status Instance ID Name Port State Security groups Zone Subnet ID

No instances added yet

Specify instances above, or leave the group empty if you prefer to add targets later.

0 pending

Cancel Previous **Create target group**



Successfully created target group: app-TG

EC2 > Target groups

Target groups (1) **Info**

Search or filter target groups

Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
app-TG	arn:aws:elasticloadbalancing:us-east-2:123456789012:targetgroup/app-TG/5678901234567890	80	HTTP	Instance	None associated	vpc-024a44812f7630f8a

0 target groups selected

Select a target group above.

#### ❖ Phase 4: Deploy Application Load Balancer

20. Create Launch template
21. Create Application Load Balancer
  1. Name: prefect-ALB
  2. Scheme: internet-facing
  3. IP address: ipv4
  4. Network mapping:
    1. Select VPC: prefect-vpc
    2. Mappings: select: us-east-2a, us-east2b
    3. Security Groups: select: web-SG
    4. Listener:
      1. HTTP:80
      2. Default action: Target Group

EC2 VPC CloudWatch Simple Notification Service Route 53 CloudFront AWS FIS IAM

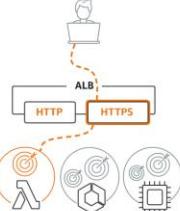
EC2 > Load balancers > Select load balancer type

A complete feature-by-feature comparison along with detailed highlights is also available. [Learn more](#)

### Select load balancer type

Load balancer types

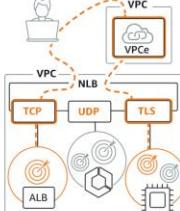
**Application Load Balancer** [Info](#)



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](#) 1

**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](#)

VPC Route 53 EC2 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

EC2 > Load balancers > 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.

### Create Application Load Balancer [Info](#)

▶ How Elastic Load balancing works

#### Basic configuration

Load balancer name

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

1

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

Scheme [Info](#)

Scheme cannot be changed after the load balancer is created.

2 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.

IP address type [Info](#)

Select the type of IP addresses that your subnets use.

3 IPv4

Recommended for internal load balancers.

Dualstack

Includes IPv4 and IPv6 addresses.

#### 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. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#)

4

**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. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups [\[2\]](#)

web-vpc  
vpc-0f032fa0af9b6557f  
IPv4: 10.0.0.0/16

**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.

**us-east-1a**

Subnet  
subnet-05d667e65d7d4214 1 web-subnet01 [\[3\]](#)

IPv4 settings  
Assigned by AWS

**us-east-1b**

Subnet  
subnet-01224earfb85af2836 2 web-subnet02 [\[4\]](#)

IPv4 settings  
Assigned by AWS

**Security groups** [Info](#)  
A security group is a set of firewall rules that control the traffic to your load balancer.

**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. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups [\[2\]](#)

prefect-vpc  
vpc-024a48137f650f9a 1

**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.

**us-east-2a (use2-az1)** 2

Subnet  
subnet-08ac1553d5fa03589 3 web-public01 [\[5\]](#)

IPv4 settings  
Assigned by AWS

**us-east-2b (use2-az2)**

Subnet  
subnet-063a9789f581f151d 4 web-public02 [\[6\]](#)

IPv4 settings  
Assigned by AWS

**Security groups** [Info](#)  
A security group is a set of firewall rules that control the traffic to your load balancer.

**Security groups**  
Select up to 5 security groups  
Create new security group [\[5\]](#)

web-SG sg-01f419d0ddcfe9f1 X  
VPC vpc-024a48137f650f9a

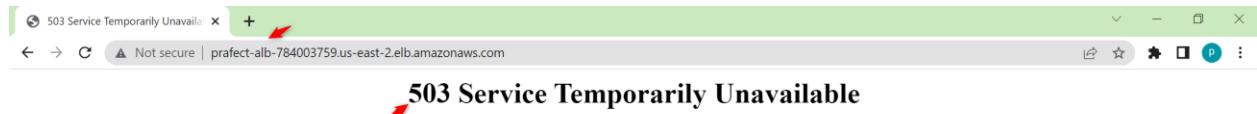
Load balancer created successfully

Verify that ALB URL is accessible

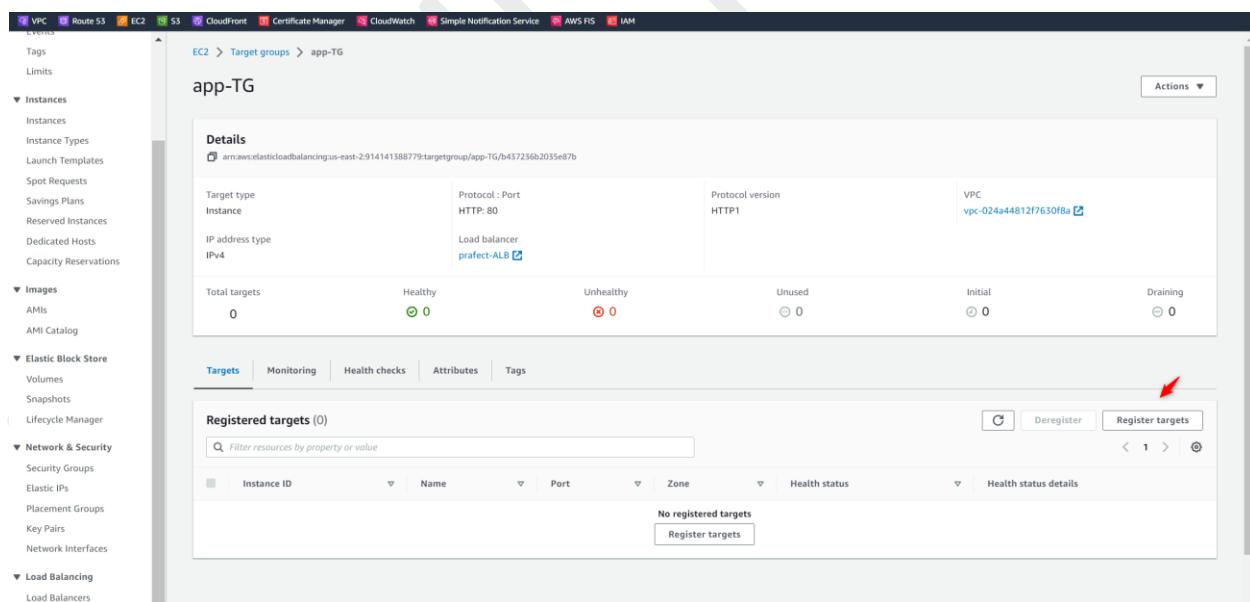
Copy ALB DNS

prefect-ALB-784003759.us-east-2.elb.amazonaws.com

Open Browser and access the url



Go to Target Group



## ❖ Phase 5: Deploy Auto Scaling Group

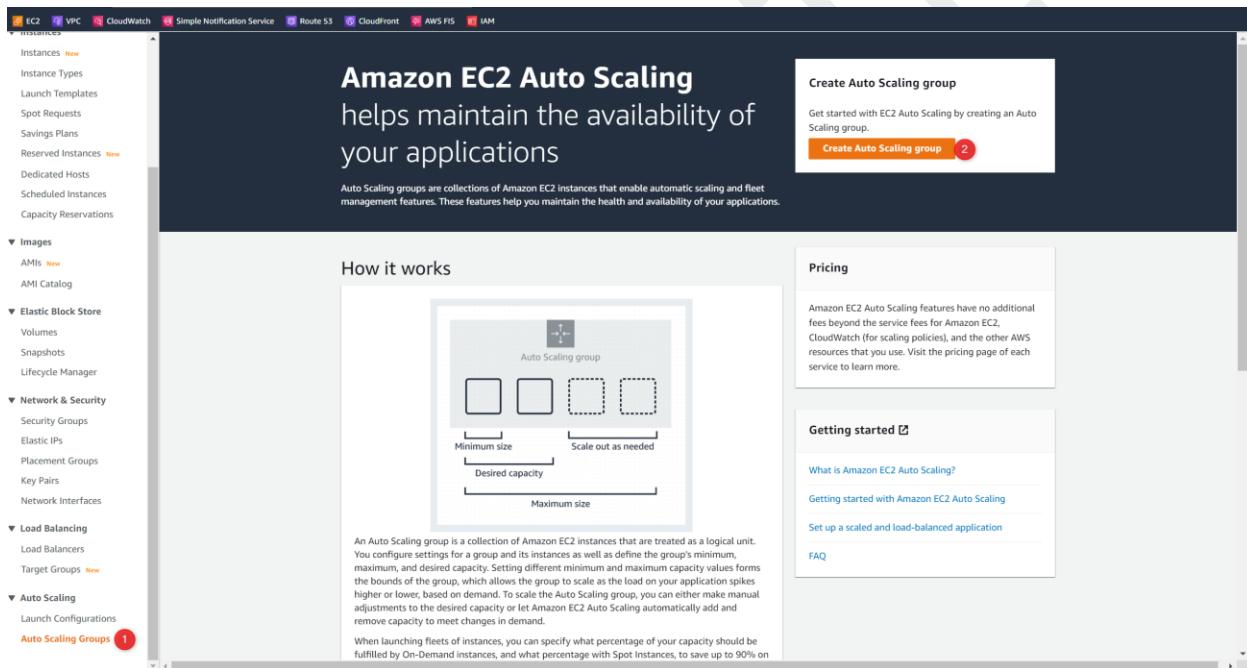
22. Name: prefect-ASG

23. Launch template: prefect-template, version: 1

24. Network:

1. VPC: prefect-vpc
2. Availability Zones: us-east-2a, us-east-2b
3. Load Balancing: Attach to and existing load balancer

4. Choose Target Group: app-TG
5. Health Check: ELB: 300 seconds
6. Group Size:
  1. Units
  2. Desired Capacity: 2
  3. Minimum Capacity: 2
  4. Maximum Capacity: 4
7. Scaling Policies:
  1. Name: Target Tracking Policy
  2. Metric Type: Average CPU Utilization
  3. Target Value: 50
  4. Warm up: 300 seconds



VPC Route 53 EC2 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1 Choose launch template or configuration

Step 2 Choose instance launch options

Step 3 - optional Configure advanced options

Step 4 - optional Configure group size and scaling policies

Step 5 - optional Add notifications

Step 6 - optional Add tags

Step 7 Review

### Choose launch template or configuration Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

**Name**

Auto Scaling group name  
Enter a name to identify the group.  
prefect-ASG 1

Must be unique to this account in the current Region and no more than 255 characters.

**Launch template Info** Switch to launch configuration

Launch template  
Choose a launch template that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

prefect-template 2

Create a launch template [x]

Version  
Default (1) 3 [x] [c]

Create a launch template version [x]

Description	Launch template	Instance type
v1	prefect-template <span style="border: 1px solid red; border-radius: 50%; padding: 2px;">2</span> lt-0c88746db53cd2f3	t2.micro
AMI ID	ami-03a5def6b0190cef7	Security groups -
Key pair name	prefect-key	Security group IDs sg-05955a1727b715e72 <span style="border: 1px solid red; border-radius: 50%; padding: 2px;">2</span>

**Additional details**

Storage (volumes)  
-

Date created  
Thu Mar 02 2023 16:49:33 GMT-

VPC Route 53 EC2 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

Choose launch template or configuration

Step 2 Choose instance launch options

Step 3 - optional Configure advanced options

Step 4 - optional Configure group size and scaling policies

Step 5 - optional Add notifications

Step 6 - optional Add tags

Step 7 Review

### Choose instance launch options Info

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase options.

**Network Info**

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

**VPC**  
Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-02444812f7630f8a (prefect-vpc) 1 [x] [c]

10.0.0.0/16

Create a VPC [x]

**Availability Zones and subnets**  
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets [x]

us-east-2a | subnet-050cdc2ef3b68f4e6 (app-private01) 2 [x]  
10.0.3.0/24

us-east-2b | subnet-06c007c74f2f7740f (app-private02) 3 [x]  
10.0.4.0/24

Create a subnet [x]

**Instance type requirements Info** Override launch template

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

Launch template	Version	Description
prefect-template <span style="border: 1px solid red; border-radius: 50%; padding: 2px;">2</span> lt-0c88746db53cd2f3	Default	v1

Instance type  
t2.micro

Cancel Skip to review Previous Next 4

Step 1  
Choose launch template or configuration

Step 2  
Choose instance launch options

Step 3 - optional  
Configure advanced options

Step 4 - optional  
Configure group size and scaling policies

Step 5 - optional  
Add notifications

Step 6 - optional  
Add tags

Step 7  
Review

### Configure advanced options - optional

Choose a load balancer to distribute incoming traffic for your application across instances to make it more reliable and easily scalable. You can also set options that give you more control over health check replacements and monitoring.

#### Load balancing - optional

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

No load balancer  
Traffic to your Auto Scaling group will not be fronted by a load balancer.

Attach to an existing load balancer  
Choose from your existing load balancers.

Attach to a new load balancer  
Quickly create a basic load balancer to attach to your Auto Scaling group.

#### Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

Choose from your load balancer target groups  
This option allows you to attach Application, Network, or Gateway Load Balancers.

Choose from Classic Load Balancers

#### Existing load balancer target groups

Only instance target groups that belong to the same VPC as your Auto Scaling group are available for selection.

Select target groups

app-TG HTTP  Application Load Balancer: prefect-ALB  3

### Health checks - optional

Health check type Info  
EC2 Auto Scaling automatically replaces instances that fail health checks. If you enabled load balancing, you can enable ELB health checks in addition to the EC2 health checks that are always enabled.

EC2  ELB 4

Health check grace period  
The amount of time until EC2 Auto Scaling performs the first health check on new instances after they are put into service.

300 seconds

### Additional settings - optional

Monitoring Info

Step 1 - optional  
Configure advanced options

Step 2 - optional  
Configure group size and scaling policies

Step 3 - optional  
Add notifications

Step 4 - optional  
Add tags

Step 5 - optional  
Review

### Group size - optional

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

Desired capacity  1

Minimum capacity  2

Maximum capacity  3

### Scaling policies - optional

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. Info

Target tracking scaling policy  
Choose a desired outcome and leave it to the scaling policy to add and remove capacity as needed to achieve that outcome.

None

Scaling policy name  5

Metric type  6

Target value  7

Instances to warm up  8  
seconds warm up before including in metric

Disable scale in to create only a scale-out policy

### Instance scale-in protection - optional

Instance scale-in protection  
If protect from scale in is enabled, newly launched instances will be protected from scale in by default.

Enable instance scale-in protection

Auto Scale your Amazon EC2 Instances Ahead of Demand  
Explore how the new predictive scaling policy of EC2 Auto Scaling helps you improve availability for your applications. [Learn More](#)

**prefect-ASG, 1 Scaling policy created successfully**

[EC2](#) > Auto Scaling groups

### Auto Scaling groups (1) Info

Search your Auto Scaling groups

Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
<a href="#">prefect-ASG</a>	<a href="#">prefect-template</a>   Version Default	0	<input type="button" value="Updating capacity..."/>	2	2	4	us-east-2a, us-east-2b

Go to EC2 section and observe the EC2 servers

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Instances (2) Info

Find instance by attribute or tag (case-sensitive)

Instance state = running

Clear Filters

Instance state

Instance type

Status check

Alarm status

Availability Zone

Public IPv4 DNS

Public IPv4 ...

Elastic IP

1 i-080d2f2d5fb36138f Running @Q t2.micro Initializing No alarms + us-east-2a - - -

2 i-0a2769ad11b080fa1 Running @Q t2.micro Initializing No alarms + us-east-2b - - -

Select an instance

Go to ALB and copy DNS

Events

Tags

Limits

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 IP

Placement Groups

Key Pairs

Network Interfaces

Load Balancing

Load Balancers

Target Groups

EC2 > Load balancers

Load balancers (1/1)

Filter by property or value

Name

DNS name

State

VPC ID

Availability Zones

Type

Date created

Instance ID

prefect-ALB

prefect-ALB-784003759.us-east-2.elb.amazonaws.com

Active

vpc-024a44812f7630f8a

2 Availability Zones

application

March 2, 2023, 16:59 (UTC-06:00)

Load balancer: prefect-ALB

Details

arn:aws:elasticloadbalancing:us-east-2:914141388779:loadbalancer/app/prefect-ALB/fbde1ec1176bdcb2

Load balancer type: Application

DNS name: prefect-ALB-784003759.us-east-2.elb.amazonaws.com (A Record)

Status: Active

VPC: vpc-024a44812f7630f8a

IP address type: IPv4

Scheme: Internet-facing

Availability Zones: subnet-08ac1353d5fa03389 (us-east-2a (use2-a1))

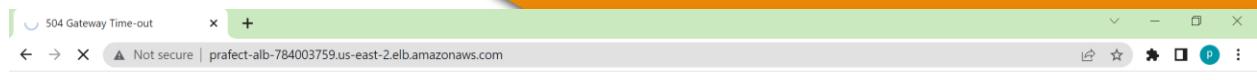
Hosted zone: Z3ADJGX6KTTL2

subnet-063a9789f581f151d (us-east-2b (use2-a2))

Date created: March 2, 2023, 16:59 (UTC-06:00)

Access Web Application from Browser

url: [iPortfolio Bootstrap Template - Index \(web-alb-577355044.us-east-1.elb.amazonaws.com\)](http://Portfolio Bootstrap Template - Index (web-alb-577355044.us-east-1.elb.amazonaws.com))



## 504 Gateway Time-out

Go to Targets

Verify if Target web instance are Healthy

If it's unhealthy check, route table or security groups that appropriate rules are allowed.

Instance ID	Name	Port	Zone	Health status	Health status details
i-0a2769ad11b080fa1		80	us-east-2b	unhealthy	Request timed out
i-080d2f2d5fb36138f		80	us-east-2a	unhealthy	Request timed out

Create NAT Gateway

**Create NAT gateway** Info

A highly available, managed Network Address Translation (NAT) service that instances in private subnets can use to connect to services in other VPCs, on-premises networks, or the internet.

**NAT gateway settings**

**Name - optional**  
Create a tag with a key of 'Name' and a value that you specify.

1

The name can be up to 256 characters long.

**Subnet**  
Select a subnet in which to create the NAT gateway.

2

**Connectivity type**  
Select a connectivity type for the NAT gateway.

Public 3

Private

**Elastic IP allocation ID** Info  
Assign an Elastic IP address to the NAT gateway.

4

**Additional settings** Info

**Tags**  
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

NAT Gateway created

**NAT gateways (1/1)** Info

**Name** 1 **NAT gateway ID** 2 **Connectivity...** 3 **State** 4 **State message** 5 **Primary public I...** 6 **Primary priv...**

Name	NAT gateway ID	Connectivity...	State	State message	Primary public I...	Primary priv...
prefect-NAT	nat-03a9026de10327a1a	Public	Available	-	52.14.221.131	10.0.1.123

**nat-03a9026de10327a1a / prefect-NAT**

**Details** Secondary IPv4 addresses Monitoring Tags

**Details**

NAT gateway ID <input type="text" value="nat-03a9026de10327a1a"/>	Connectivity type Public	State <input checked="" type="radio"/> Available	State message -
NAT gateway ARN <input type="text" value="arn:aws:ec2:us-east-2:914141388779:natgateway/nat-03a9026de10327a1a"/>	Primary public IPv4 address <input type="text" value="52.14.221.131"/>	Primary private IPv4 address <input type="text" value="10.0.1.123"/>	Primary network interface ID <input type="text" value="eni-0229dae5472c7545b"/>
VPC <input type="text" value="vpc-024a44812f7630f8a / prefect-vpc"/>	Subnet <input type="text" value="subnet-08ac1353d5fa03389 / web-public01"/>	Created <input type="text" value="Thursday, March 2, 2023 at 18:52:02 CST"/>	Deleted -

Add route to application private route table: APP-RT route table

VPC dashboard New

EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud

- Your VPCs
- Subnets
- Route tables**
- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways

Route tables (4) Info

Name	Route table ID	Explicit subnet associations	Edge associations	Main	VPC
—	rtb-02501b4d7593da6e5	—	—	Yes	vpc-05f5e3d6d1ff2c3fb
—	rtb-042d02a2a4ea6a8c0	—	—	Yes	vpc-024a44812f7630f8a   prefect-vpc
app-RT	rtb-0aa95fd6235cf234b	2 subnets	—	No	vpc-024a44812f7630f8a   prefect-vpc
web-RT	rtb-031013f268408fdee	2 subnets	—	No	vpc-024a44812f7630f8a   prefect-vpc

Select a route table

VPC dashboard New

EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud

- Your VPCs
- Subnets
- Route tables**
- Internet gateways
- Egress-only internet gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- Endpoints
- Endpoint services
- NAT gateways
- Peering connections
- Security
- Network ACLs
- Security groups
- Network Analysis
- Reachability Analyzer

rtb-0aa95fd6235cf234b / app-RT

You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer

Details Info

Route table ID <a href="#">rtb-0aa95fd6235cf234b</a>	Main <input checked="" type="checkbox"/> No	Explicit subnet associations <a href="#">2 subnets</a>	Edge associations —
VPC <a href="#">vpc-024a44812f7630f8a   prefect-vpc</a>	Owner ID <a href="#">914141388779</a>		

Routes Subnet associations Edge associations Route propagation Tags

**Routes (2)**

Destination	Target	Status	Propagated
10.0.0.0/16	local	<span style="color: green;">Active</span>	No

Edit routes

## Edit Route – Add NAT gateway

Destination: 0.0.0.0/0

Target: NAT Gateway

VPC New

Route tables New

rtb-0aa95fd6235cf234b Edit routes

**Edit routes**

Destination	Target	Status	Propagated
10.0.0.0/16	local	<span style="color: green;">Active</span>	No
<span style="background-color: #f0f0f0;">[REDACTED]</span>	<span style="background-color: #f0f0f0;">[REDACTED]</span>	<span style="background-color: #f0f0f0;">[REDACTED]</span>	<span style="background-color: #f0f0f0;">[REDACTED]</span>
<span style="border: 1px solid #ccc; padding: 2px;">Q 0.0.0.0/0</span> <span style="color: red;">1</span>	<span style="border: 1px solid #ccc; padding: 2px;">Q nat-<span style="color: red;">2</span></span>	<span style="color: red;">3</span>	<span style="color: red;">3</span>
<span style="border: 1px solid #ccc; padding: 2px;">nat-03a9026de10327a1a (prefect-NAT)</span> <span style="border: 1px solid #ccc; padding: 2px;">nat-03a9026de10327a1a (prefect-NAT)</span>			

Add route

Cancel Preview Save changes

VPC dashboard X

EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud

Your VPCs

Subnets

**Route tables**

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Network ACLs

Security groups

Actions ▼

Run Reachability Analyzer X

**rtb-0aa95fd6235cf234b / app-RT**

i You can now check network connectivity with Reachability Analyzer

**Details** Info

Route table ID <a href="#">rtb-0aa95fd6235cf234b</a>	Main <span style="color: #0070C0;">No</span>	Explicit subnet associations <a href="#">2 subnets</a>	Edge associations -
VPC <a href="#">vpc-024a44812f7630f8a   prefect-vpc</a>	Owner ID <a href="#">914141388779</a>		

**Routes** Subnet associations Edge associations Route propagation Tags

**Routes (2)**

Destination	Target	Status	Propagated
0.0.0.0/0	<a href="#">nat-03a9026de10327a1a</a>	<span style="color: green;">Active</span>	No
10.0.0.0/16	local	<span style="color: green;">Active</span>	No

Edit routes

Now go back to TARGET Group

Verify now that Targets are healthy

New EC2 Experience X

Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

**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

Actions ▼

app-TG

**Details**

i arn:aws:elasticloadbalancing:us-east-2:914141388779:targetgroup/app-TG/b437236b2035e87b

Target type Instance	Protocol : Port HTTP: 80	Protocol version HTTP1	VPC <a href="#">vpc-024a44812f7630f8a</a>
IP address type IPv4	Load balancer <a href="#">prefect-ALB</a>		
Total targets 3	Healthy <span style="color: green;">2</span>	Unhealthy <span style="color: red;">0</span>	Unused <span style="color: grey;">0</span>
	Initial <span style="color: grey;">0</span>	Draining <span style="color: grey;">1</span>	

**Distribution of targets by Availability Zone (AZ)**

Select values in this table to see corresponding filters applied to the Registered targets table below.

**Targets** Monitoring Health checks Attributes Tags

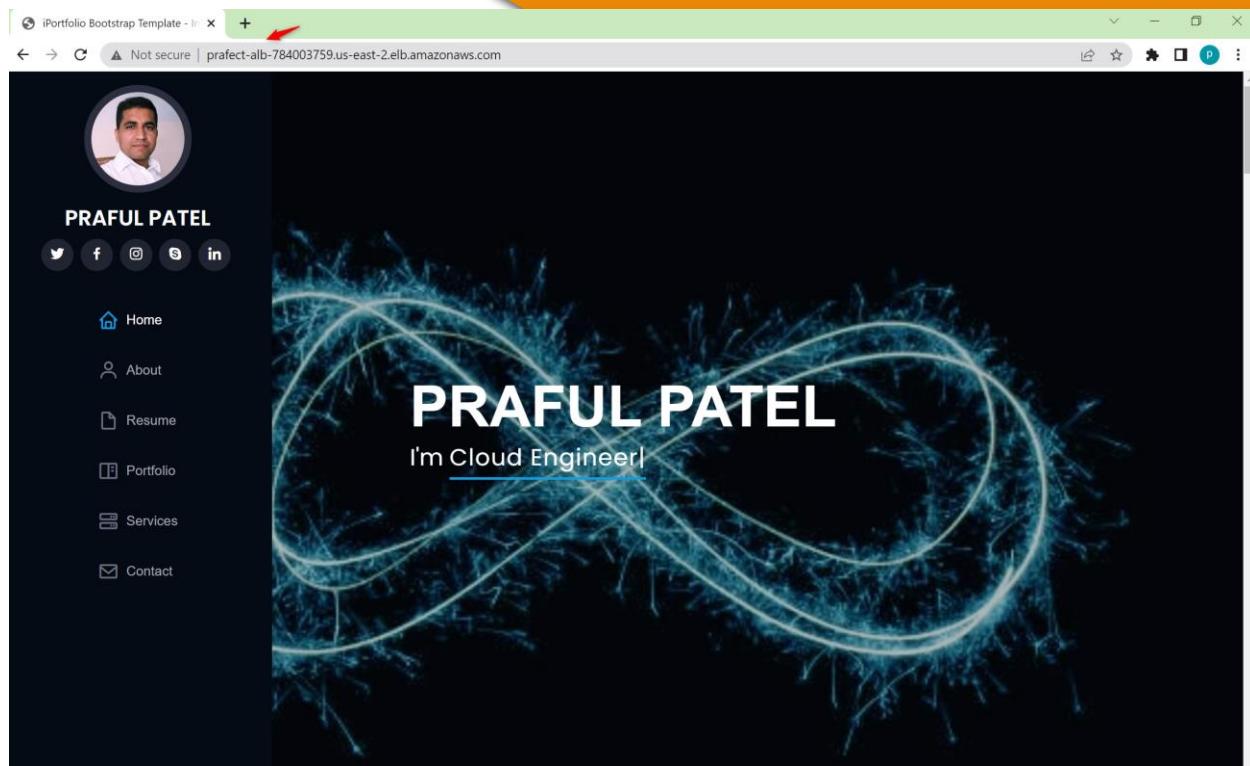
**Registered targets (3)**

<span style="color: #0070C0;">Filter resources by property or value</span>	<span style="color: #0070C0;">C</span>	<span style="color: #0070C0;">Deregister</span>	<span style="color: #0070C0;">Register targets</span>		
Instance ID	Name	Port	Zone	Health status	Health status details
<a href="#">i-01517ec55cb9bc9e5</a>		80	us-east-2b	<span style="color: green;">healthy</span>	<span style="color: green;">healthy</span>
<a href="#">i-0af69caf015bb833f</a>		80	us-east-2a	<span style="color: green;">healthy</span>	<span style="color: green;">healthy</span>

Verify web application is accessible from browser

ALB URL:

[prefect-ALB-784003759.us-east-2.elb.amazonaws.com](http://prefect-ALB-784003759.us-east-2.elb.amazonaws.com)



Note:

If web application source code is in Private APP subnet then while creating Launch template enable public ip in order to access the server from SSH

In order to download the packages and install the web server into private APP subnet following configuration is needed.

NAT Gateway : Launch nat gateway into Web-public subnet

App-RT : Add NAT gateway route to APP-Route table

## RDS Database creation

## Create MYSQL Database

## 1. Create DB Subnet Group

Amazon RDS X

VPC Route 53 EC2 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

RDS > Subnet groups > Create DB subnet group

### Create DB subnet group

To create a new subnet group, give it a name and a description, and choose an existing VPC. You will then be able to add subnets related to that VPC.

#### Subnet group details

**Name**  
You won't be able to modify the name after your subnet group has been created.  
 1

Must contain from 1 to 255 characters. Alphanumeric characters, spaces, hyphens, underscores, and periods are allowed.

**Description**

**VPC**  
Choose a VPC identifier that corresponds to the subnets you want to use for your DB subnet group. You won't be able to choose a different VPC identifier after your subnet group has been created.  
 2

**Add subnets**

**Availability Zones**  
Choose the Availability Zones that include the subnets you want to add.  
 3

**Subnets**  
Choose the subnets that you want to add. The list includes the subnets in the selected Availability Zones.  
 4

5

6

Feedback Language

Automated backups  
Reserved instances  
Proxies

**Subnet groups**  
Parameter groups  
Option groups  
Custom engine versions

Events  
Event subscriptions

Recommendations (0)  
Certificate update

Feedback Language

Automated backups  
Reserved instances  
Proxies

**Subnet groups**  
Parameter groups  
Option groups  
Custom engine versions

Events  
Event subscriptions

Recommendations (0)  
Certificate update

© 2023, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preference](#)

Amazon RDS X

VPC Route 53 EC2 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

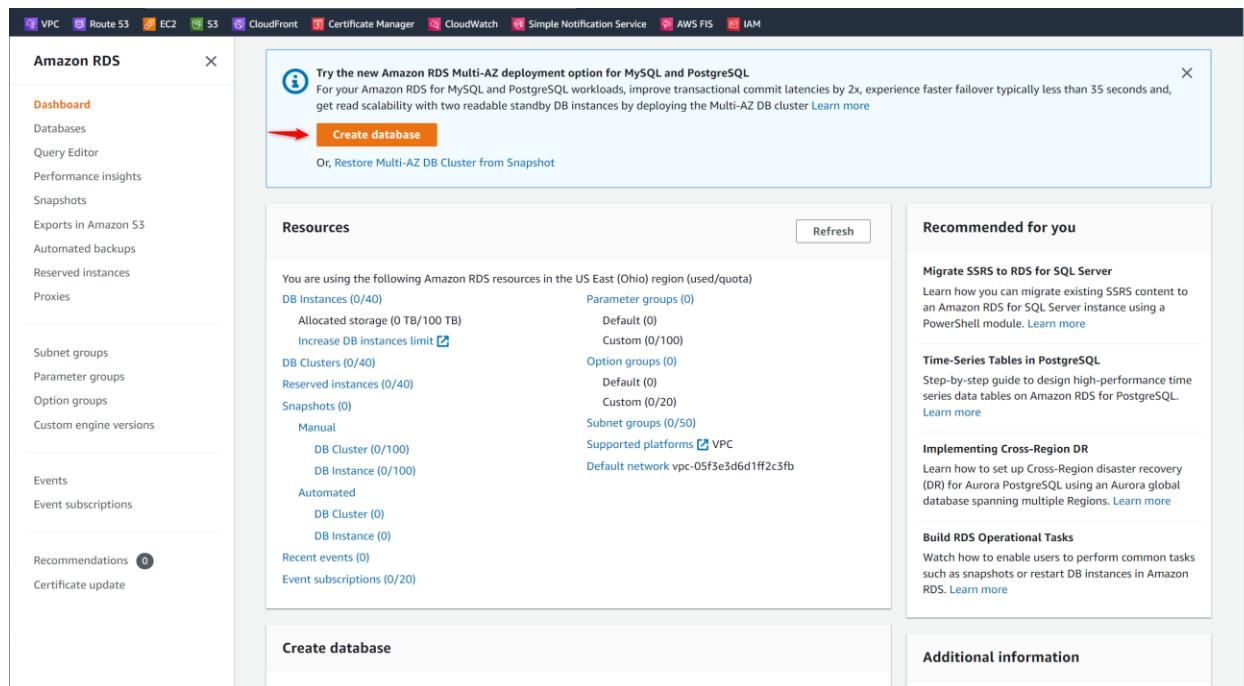
Successfully created db-subnetGroup. View subnet group

RDS > Subnet groups

### Subnet groups (2)

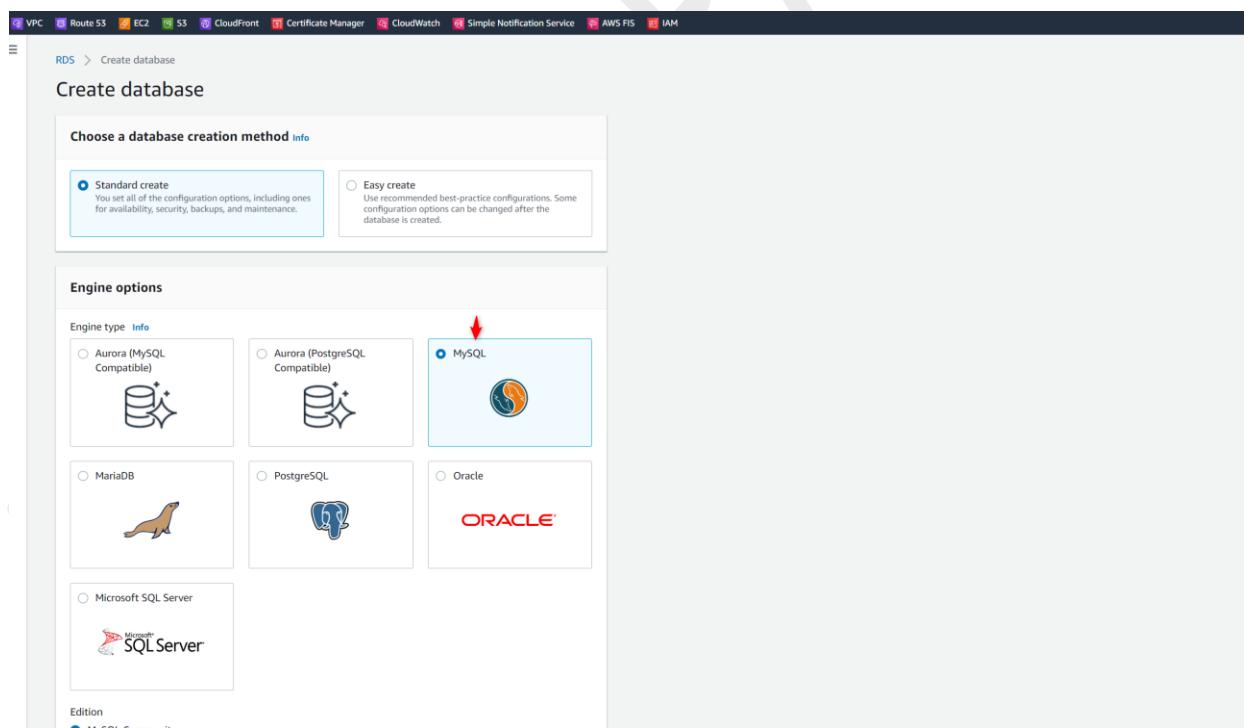
<input type="checkbox"/>	Name	Description	Status	VPC
<input type="checkbox"/>	db-subnetgroup	mysql db subnet group	<span style="color: green;">Complete</span>	vpc-024a44812f7650f8a

## 2. Create Database



The screenshot shows the Amazon RDS Dashboard. On the left, a sidebar lists various RDS features: Dashboard, Databases, Query Editor, Performance insights, Snapshots, Exports in Amazon S3, Automated backups, Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, Events, Event subscriptions, Recommendations (0), and Certificate update. The main content area has a heading 'Try the new Amazon RDS Multi-AZ deployment option for MySQL and PostgreSQL'. It includes a callout with a red arrow pointing to a 'Create database' button. Below this, there are sections for 'Resources' (DB Instances, DB Clusters, Snapshots, Automations, Events, and Event Subscriptions) and 'Recommended for you' (links to Migrate SSRS to RDS for SQL Server, Time-Series Tables in PostgreSQL, Implementing Cross-Region DR, and Build RDS Operational Tasks). At the bottom, there is an 'Additional information' section.

### Select MySQL



The screenshot shows the 'Create database' wizard. The first step, 'Choose a database creation method', has 'Standard create' selected. The second step, 'Engine options', shows a grid of database engines: Aurora (MySQL Compatible), Aurora (PostgreSQL Compatible), MySQL (selected), MariaDB, PostgreSQL, Oracle, and Microsoft SQL Server. A red arrow points to the 'MySQL' option. Below the engines, there is an 'Edition' section with a 'MySQL Community' link.

Db instance name: mysql

User: admin

Password: Passw0rd!

**Instance configuration**  
The DB instance configuration options below are limited to those supported by the engine that you selected above.

**DB instance class** [Info](#)  
 Standard classes (includes m classes)  
 Memory optimized classes (includes r and x classes)  
 **Burstable classes (includes t classes)**

**db.t3.micro**  
2 vCPUs 1 GiB RAM Network: 2,085 Mbps 1

**Include previous generation classes**

**Storage**

**Storage type** [Info](#) 2  
General Purpose SSD (gp2)  
Baseline performance determined by volume size

**Allocated storage** [Info](#) 3 GiB  
The minimum value is 20 GiB and the maximum value is 6,144 GiB

**Storage autoscaling** [Info](#)  
Provides dynamic scaling support for your database's storage based on your application's needs.

**Enable storage autoscaling**  
Enabling this feature will allow the storage to increase after the specified threshold is exceeded.

**Maximum storage threshold** [Info](#)  
Charges will apply when your database autoscales to the specified threshold  
1000 GiB  
The minimum value is 22 GiB and the maximum value is 6,144 GiB

### Dbsubnet group: select db-subnetGroup

**Connectivity** [Info](#)

**Compute resource**  
Choose whether to set up a connection to a compute resource for this database. Setting up a connection will automatically change connectivity settings so that the compute resource can connect to this database.

1  **Don't connect to an EC2 compute resource**  
Don't set up a connection to a compute resource for this database. You can manually set up a connection to a compute resource later.

**Connect to an EC2 compute resource**  
Set up a connection to an EC2 compute resource for this database.

**Virtual private cloud (VPC)** [Info](#)  
Choose the VPC. The VPC defines the virtual networking environment for this DB instance.

2 **prefect-vpc (vpc-024a44812f7630f8a)**  
Only VPCs with a corresponding DB subnet group are listed.

3 After a database is created, you can't change its VPC.

**DB subnet group** [Info](#)  
Choose the DB subnet group. The DB subnet group defines which subnets and IP ranges the DB instance can use in the VPC that you selected.

3 **Create new DB Subnet Group**

**Public access** [Info](#)

**Yes**  
RDS assigns a public IP address to the database. Amazon EC2 instances and other resources outside of the VPC can connect to your database. Resources inside the VPC can also connect to the database. Choose one or more VPC security groups that specify which resources can connect to the database.

4  **No**  
RDS doesn't assign a public IP address to the database. Only Amazon EC2 instances and other resources inside the VPC can connect to your database. Choose one or more VPC security groups that specify which resources can connect to the database.

**VPC security group (firewall)** [Info](#)  
Choose one or more VPC security groups to allow access to your database. Make sure that the security group rules allow the appropriate incoming traffic.

5  **Choose existing**  
Choose existing VPC security groups

6 **Existing VPC security groups**  
Choose one or more options  
db-SG X

VPC Route 53 EC2 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

**Availability Zone** [Info](#) 1  
us-east-2a

**RDS Proxy**  
RDS Proxy is a fully managed, highly available database proxy that improves application scalability, resiliency, and security.  
 [Create an RDS Proxy](#) [Info](#)  
RDS automatically creates an IAM role and a Secrets Manager secret for the proxy. RDS Proxy has additional costs. For more information, see [Amazon RDS Proxy pricing](#).

**Certificate authority - optional** [Info](#)  
Using a server certificate provides an extra layer of security by validating that the connection is being made to an Amazon database. It does so by checking the server certificate that is automatically installed on all databases that you provision.  
 rds-ca-2019 (default) 2  
If you don't select a certificate authority, RDS chooses one for you.

[Additional configuration](#)

**Database authentication**

**Database authentication options** [Info](#) 3  
 [Password authentication](#)  
Authenticates using database passwords.  
 [Password and IAM database authentication](#)  
Authenticates using the database password and user credentials through AWS IAM users and roles.  
 [Password and Kerberos authentication](#)  
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

**Monitoring**

**Monitoring**  
 [Enable Enhanced monitoring](#)  
Enabling Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU.

**Monitoring**  
 [Password and Kerberos authentication](#)  
Choose a directory in which you want to allow authorized users to authenticate with this DB instance using Kerberos Authentication.

**Monitoring**  
 [Enable Enhanced monitoring](#)  
Enabling Enhanced monitoring metrics are useful when you want to see how different processes or threads use the CPU.

**Additional configuration**  
Database options, encryption turned on, backup turned on, backtrack turned off, maintenance, CloudWatch Logs, delete protection turned off.

**Estimated monthly costs**

The Amazon RDS Free Tier is available to you for 12 months. Each calendar month, the free tier will allow you to use the Amazon RDS resources listed below for free.

- 750 hrs of Amazon RDS in a Single-AZ db.t2.micro, db.t3.micro or db.t4g.micro Instance.
- 20 GB of General Purpose Storage (SSD).
- 20 GB for automated backup storage and any user-initiated DB Snapshots.

[Learn more about AWS Free Tier](#)

When your free usage expires or if your application use exceeds the free usage tiers, you simply pay standard, pay-as-you-go service rates as described in the [Amazon RDS Pricing page](#).

**Important** You are responsible for ensuring that you have all of the necessary rights for any third-party products or services that you use with AWS services.

[Cancel](#) [Create database](#)



Mysql Database instance created

VPC Route 53 EC2 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

**Amazon RDS**

- Dashboard
- Databases**
- Query Editor
- Performance insights
- Snapshots
- Exports in Amazon S3
- Automated backups
- Reserved instances
- Proxies
- Subnet groups
- Parameter groups
- Option groups
- Custom engine versions
- Events
- Event subscriptions

**RDS > Databases**

Consider creating a Blue/Green Deployment to minimize downtime during upgrades  
You may want to consider using Amazon RDS Blue/Green Deployments and minimize your downtime during upgrades. A Blue/Green Deployment provides a staging environment for changes to production databases. [RDS User Guide](#) [Aurora User Guide](#)

**Databases**

Group resources  Modify Actions

Filter by databases

DB identifier	Role	Engine	Region & AZ	Size	Status	Actions	CPU	Current
mysql1	Instance	MySQL Community	us-east-2a	db.t3.micro	<span>Available</span>	<input type="button" value="Modify"/>	3.10%	

VPC Route 53 EC2 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

**Amazon RDS**

- Dashboard
- Databases**
- Query Editor
- Performance insights
- Snapshots
- Exports in Amazon S3
- Automated backups
- Reserved instances
- Proxies
- Subnet groups
- Parameter groups
- Option groups
- Custom engine versions
- Events
- Event subscriptions
- Recommendations 0
- Certificate update

**RDS > Databases > mysql1**

**mysql1**

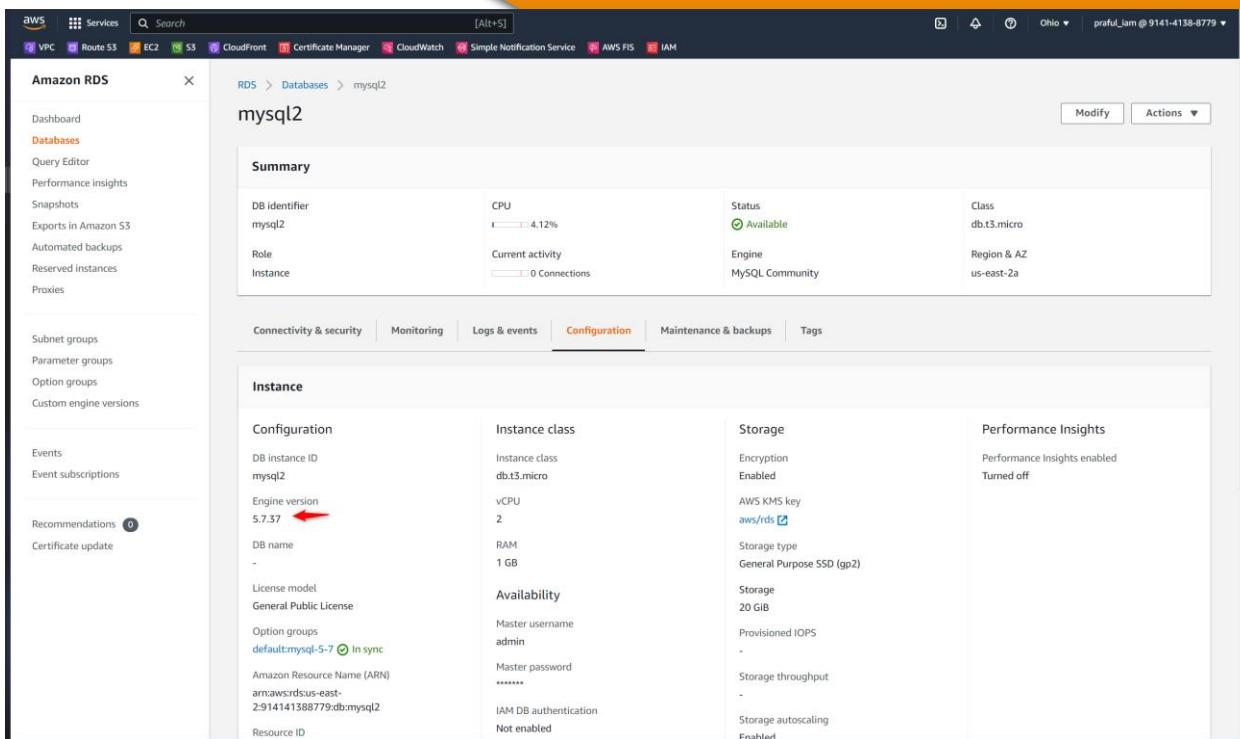
**Summary**

DB identifier	CPU	Status	Class
mysql1	3.10%	<span>Available</span>	db.t3.micro
Role	Current activity	Engine	Region & AZ
Instance	0 Connections	MySQL Community	us-east-2a

**Connectivity & security**

**Connectivity & security**

<b>Endpoint &amp; port</b>	<b>Networking</b>	<b>Security</b>
Endpoint <a href="#">mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com</a>	Availability Zone us-east-2a	VPC security groups <a href="#">db-SG (sg-07b9a1eda87c5b837)</a> <span>Active</span>
Port 3306	VPC <a href="#">prefect-vpc (vpc-024a44812f7630f8a)</a>	Publicly accessible No
	Subnet group <a href="#">db-subnetgroup</a>	Certificate authority <a href="#">Info</a> <a href="#">rds-ca-2019</a>
	Subnets <a href="#">subnet-07f790de506475104</a> <a href="#">subnet-0e897818fc46ee889</a>	Certificate authority date August 22, 2024, 11:08 (UTC-06:00)
	Network type IPv4	DB instance certificate expiration date August 22, 2024, 11:08 (UTC-06:00)



The screenshot shows the AWS RDS console for a MySQL database named 'mysql2'. The 'Configuration' tab is selected. A red arrow points to the 'Engine version' field, which displays '5.7.37'. The 'Instance' table provides detailed information about the database instance, including its class (db.t3.micro), storage (General Purpose SSD (gp2)), and performance insights status (Turned off).

Webserver to database connection parameters:

Need to update the parameters



The screenshot shows a GitHub commit for a file named 'db.php'. The commit message is 'new project folder emp1 added'. The commit was made by 'prafulpatel16' on February 25, 2022. The file contains 11 lines of code, with the first four lines highlighted and circled in red. The code is as follows:

```

1 <?php
2 $servername='mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com';
3 $username='admin';
4 $password='admin123456';
5 $dbname = "contacts";
6 $conn=mysqli_connect($servername,$username,$password,"$dbname");
7 if(!$conn){
8     die('Could not Connect MySQL Server: ' .mysqli_error());
9 }
10 ?>

```

New DB connection parameters:

Servername: mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com

Username: admin

Password: Passw0rd!

Dbname: contacts

Go to web source code file: db.php

Parameter updated to web file

main → php-html-projects / iPortfoliov1\_emp / forms / db.php / < Jump to ↻

prafulpatel16 updated db.php

1 contributor

11 lines (10 sloc) | 316 Bytes

```

1  <?php
2  $servername='mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com';
3  $username='admin';
4  $password='Passw0rd!';
5  $dbname = "contacts";
6  $conn=mysqli_connect($servername,$username,$password,$dbname);
7  if(!$conn){
8      die('Could not Connect MySQL Server:' .mysqli_error());
9  }
10 ?>

```

Raw Blame ⌂ ⌂ ⌂

Give feedback

Create or modify the Launch template

Update Security Group

VPC Route 53 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

Select a VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoints

Endpoint services

NAT gateways

Peering connections

Security

Network ACLs

Security groups

Security Groups (5) Info

Filter security groups

Actions Export security groups to CSV Create security group

sg-0d4e27bb4b706d83c default vpc-05f3e3d6d1ff2c3fb default VPC security gr... 914141388779 1 Permission entry

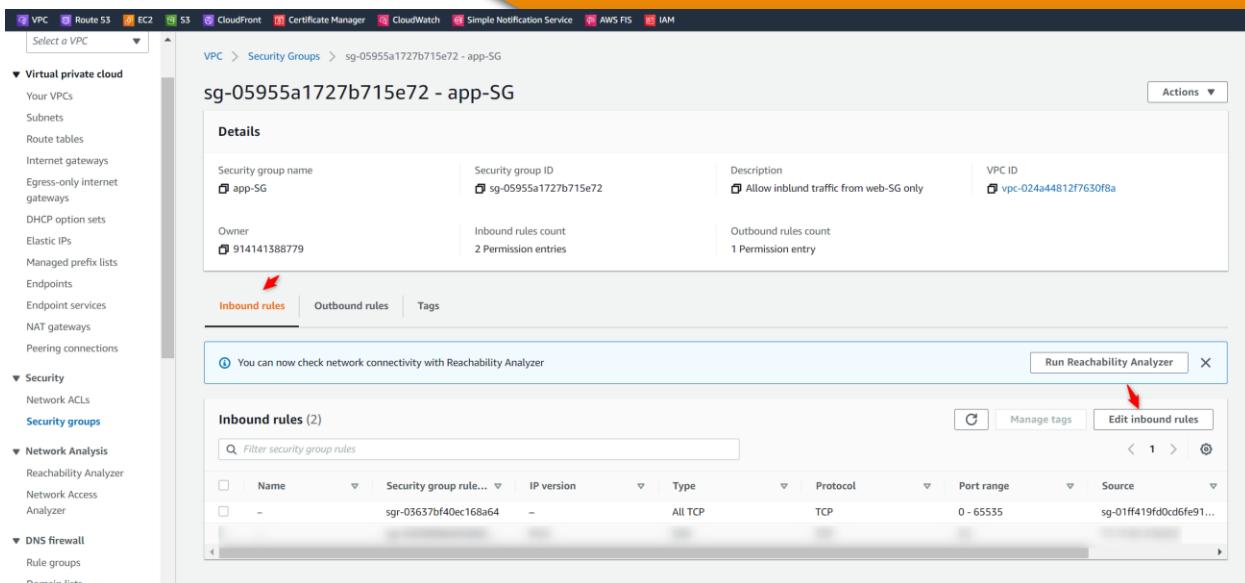
sg-0e968fce6f058c4fd default vpc-024a44812f7630f8a default VPC security gr... 914141388779 1 Permission entry

sg-05955a1727b715e72 app-SG vpc-024a44812f7630f8a Allow inbnd traffic fr... 914141388779 2 Permission entries

sg-07b9a1eda87c5b837 db-SG vpc-024a44812f7630f8a Allow traffic from app-... 914141388779 1 Permission entry

sg-01ff419fd0cd6fe91 web-SG vpc-024a44812f7630f8a Allows internet access ... 914141388779 2 Permission entries

Edit inbound rules:



Virtual private cloud

Security group name: app-SG

Security group ID: sg-05955a1727b715e72

Description: Allow inbound traffic from web-SG only

Owner: 914141388779

Inbound rules count: 2 Permission entries

Outbound rules count: 1 Permission entry

Inbound rules (2)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
-	sgr-03637bf40ec168a64	-	All TCP	TCP	0 - 65535	sg-01ff419fd0cd6fe91...

Run Reachability Analyzer

Edit inbound rules

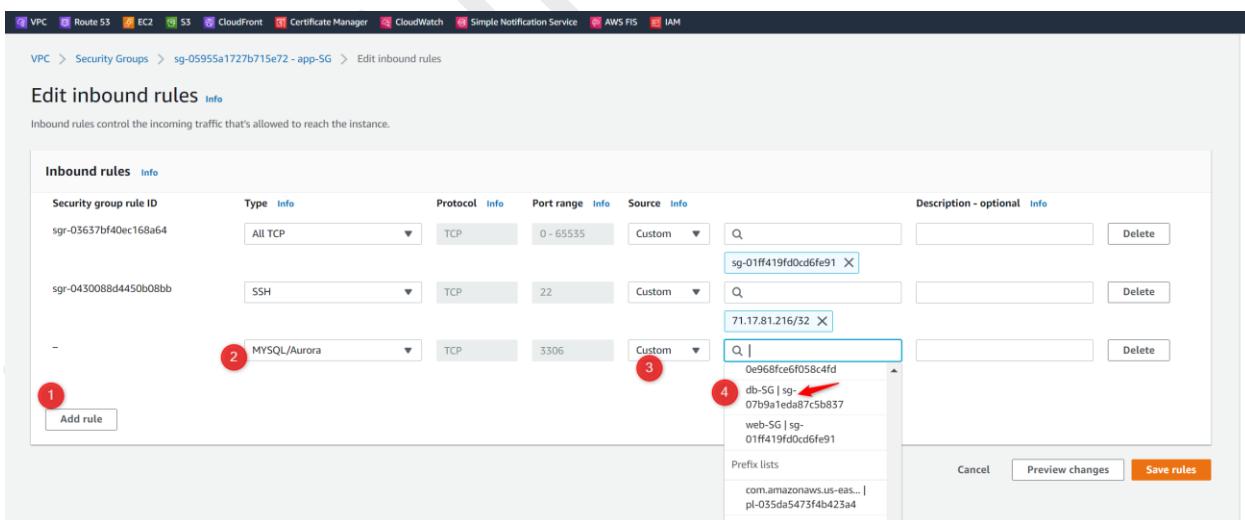
Add rule

Type: MySQL/Aurora

Protocol: TCP

Port range: 3306

Source : custom: db\_SG



Inbound rules

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type	Protocol	Port range	Source	Description - optional
sgr-03637bf40ec168a64	All TCP	TCP	0 - 65535	Custom	sg-01ff419fd0cd6fe91
sgr-0450088d4450b08bb	SSH	TCP	22	Custom	71.17.81.216/32
-	MySQL/Aurora	TCP	3306	Custom	0e968fce6f058c4fd db-SG   sg-07b9a1ed87c5b837 web-SG   sg-01ff419fd0cd6fe91

Add rule

MySQL/Aurora

Custom

0e968fce6f058c4fd  
db-SG | sg-07b9a1ed87c5b837  
web-SG | sg-01ff419fd0cd6fe91

Prefix lists

Cancel Preview changes Save rules

VPC Route 53 EC2 S3 CloudFront Certificate Manager CloudWatch Simple Notification Service AWS FIS IAM

VPC dashboard EC2 Global View New

Filter by VPC: Select a VPC

Virtual private cloud Your VPCs Subnets Route tables Internet gateways Egress-only internet gateways DHCP option sets Elastic IPs Managed prefix lists Endpoints Endpoint services NAT gateways Peering connections

Inbound security group rules successfully modified on security group (sg-05955a1727b715e72 | app-SG)

Details

VPC > Security Groups > sg-05955a1727b715e72 - app-SG Actions

## sg-05955a1727b715e72 - app-SG

Details		
Security group name	Security group ID	Description
app-SG	sg-05955a1727b715e72	Allow inbound traffic from web-SG only
Owner	Inbound rules count	Outbound rules count
914141388779	3 Permission entries	1 Permission entry

Inbound rules Outbound rules Tags

ⓘ You can now check network connectivity with Reachability Analyzer Run Reachability Analyzer

### Inbound rules (3)

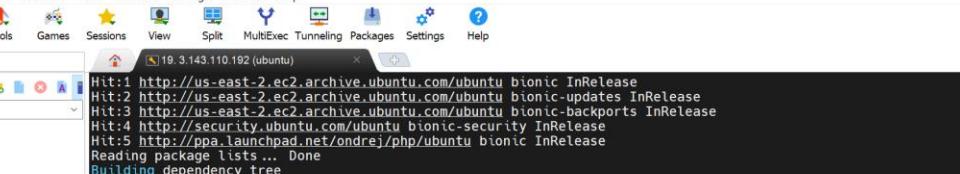
Filter security group rules

Name	Security group rule type	IP version	Type	Protocol	Port range	Source
-	sgr-03637bf40ec168a64	-	All TCP	TCP	0 - 65535	sg-01ff419fd0cd6fe91 / web-SG
-	sgr-04d95afafdfc5862193	-	MySQL/Aurora	TCP	3306	sg-07b9a1edab7c5b837 / db-SG

Access rds db instance from one of web server

3.143.110.192

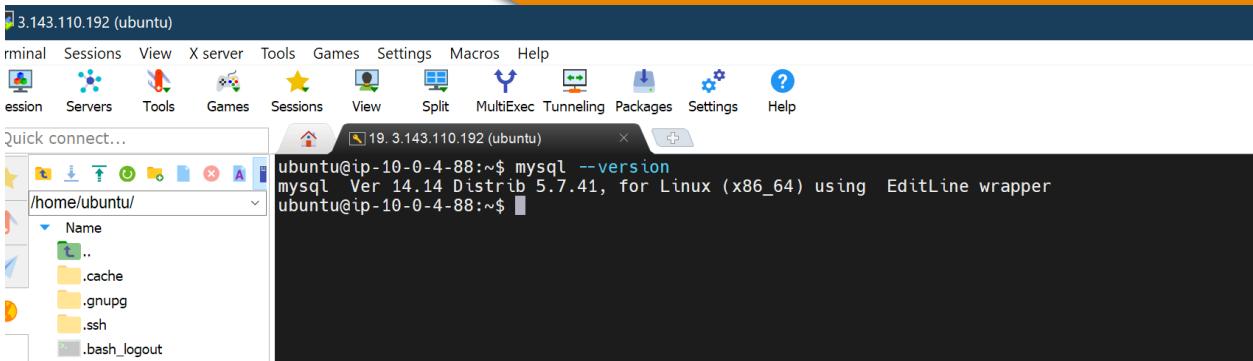
Install **sudo apt-get install mysql-server mysql-client**



```
Hit:1 http://us-east-2.ec2.archive.ubuntu.com/ubuntu bionic InRelease
Hit:2 http://us-east-2.ec2.archive.ubuntu.com/ubuntu bionic-updates InRelease
Hit:3 http://us-east-2.ec2.archive.ubuntu.com/ubuntu bionic-backports InRelease
Hit:4 http://security.ubuntu.com/ubuntu bionic-security InRelease
Hit:5 http://ppa.launchpad.net/ondrej/php/ubuntu bionic InRelease
Reading package lists... Done
Building dependency tree
Reading state information... Done
36 packages can be upgraded. Run 'apt list --upgradable' to see them.
ubuntu@ip-10-0-4-88:~$ sudo apt-get install mysql-server mysql-client
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libaio1 liblbcgi-fast-perl liblbcgi-pm-perl libencode-locale-perl libevent-core-2.1-6 libfcgi-perl libhtml-parser-perl
  libhtml-tmplset-perl liblhttp-template-perl liblhttp-date-perl liblhttp-message-perl libio-html-perl liblwp-mediatypes-perl
  liburi-perl mysql-client 5.7 mysql-client-core 5.7 mysql-common mysql-server 5.7 mysql-server-core 5.7
Suggested packages:
  libdata-dump-perl libipc-sharedcache-perl libwww-perl mailx tinyca
The following NEW packages will be installed:
  libaio1 liblbcgi-fast-perl liblbcgi-pm-perl libencode-locale-perl libevent-core-2.1-6 libfcgi-perl libhtml-parser-perl
  libhtml-tmplset-perl liblhttp-template-perl liblhttp-date-perl liblhttp-message-perl libio-html-perl liblwp-mediatypes-perl
  liburi-perl mysql-client mysql-client-core 5.7 mysql-common mysql-server mysql-server 5.7
  mysql-server-core 5.7
0 upgraded, 21 newly installed, 0 to remove and 36 not upgraded.
Need to get 20.1 MB of archives.
After this operation, 157 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://us-east-2.ec2.archive.ubuntu.com/ubuntu/bionic/main amd64 mysql-common all 5.8+1.0.4 [7308 B]
Get:2 http://us-east-2.ec2.archive.ubuntu.com/ubuntu/bionic-updates/main amd64 libaio1 amd64 0.3.110-Subuntu0.1 [6476 B]
Get:3 http://us-east-2.ec2.archive.ubuntu.com/ubuntu/bionic-updates/main amd64 mysql-client-core 5.7 amd64 5.7.41-0ubuntu0.18.0.1 [6758 KB]
```

Verify that mysql is installed

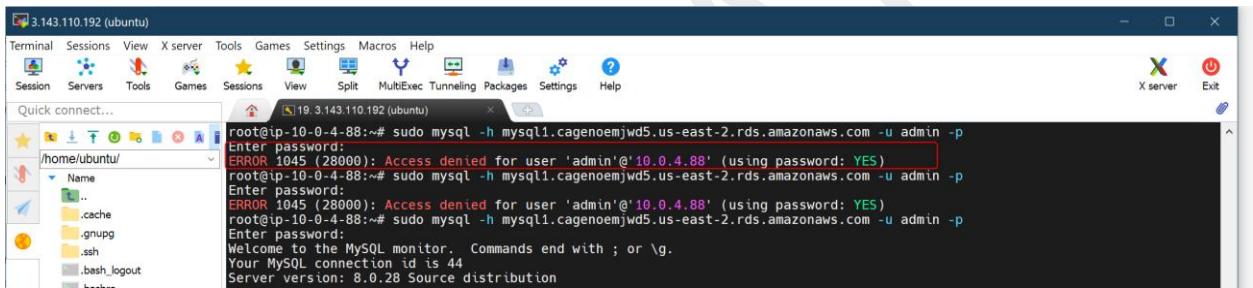
Mysql --version



Access RDS mysql db instance

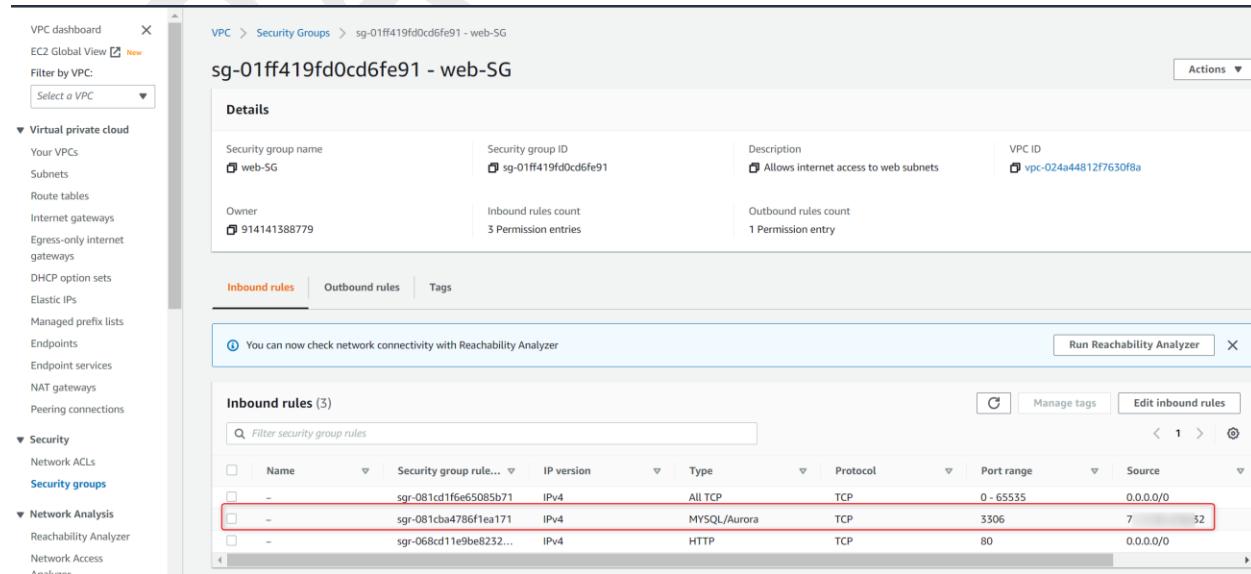
**sudo mysql -u admin -p -h mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com**

Error: accessing mysql database



Note: if getting this error accessing RDS database

**Solution: Go to web-SG, Add MY IP as source for MYSQL/Aurora 3306**



Successfully established mysql rds instance

```
sudo mysql -u admin -p -h mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com
```

```
root@ip-10-0-4-88:~# sudo mysql -h mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com -u admin -p
Enter password:
ERROR 1045 (28000): Access denied for user 'admin'@'10.0.4.88' (using password: YES)
root@ip-10-0-4-88:~# sudo mysql -h mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com -u admin -p
Enter password:
ERROR 1045 (28000): Access denied for user 'admin'@'10.0.4.88' (using password: YES)
root@ip-10-0-4-88:~# sudo mysql -h mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com -u admin -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 44
Server version: 8.0.28 Source distribution

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
4 rows in set (0.00 sec)

mysql>
```

### Create a New Database

```
mysql> create database contacts;
```

Verify that database 'contacts' is created

```
root@ip-10-0-4-88:~# sudo mysql -h mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com -u admin -p
Enter password:
Welcome to the MySQL monitor. Commands end with ; or \g.
Your MySQL connection id is 44
Server version: 8.0.28 Source distribution

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
4 rows in set (0.00 sec)

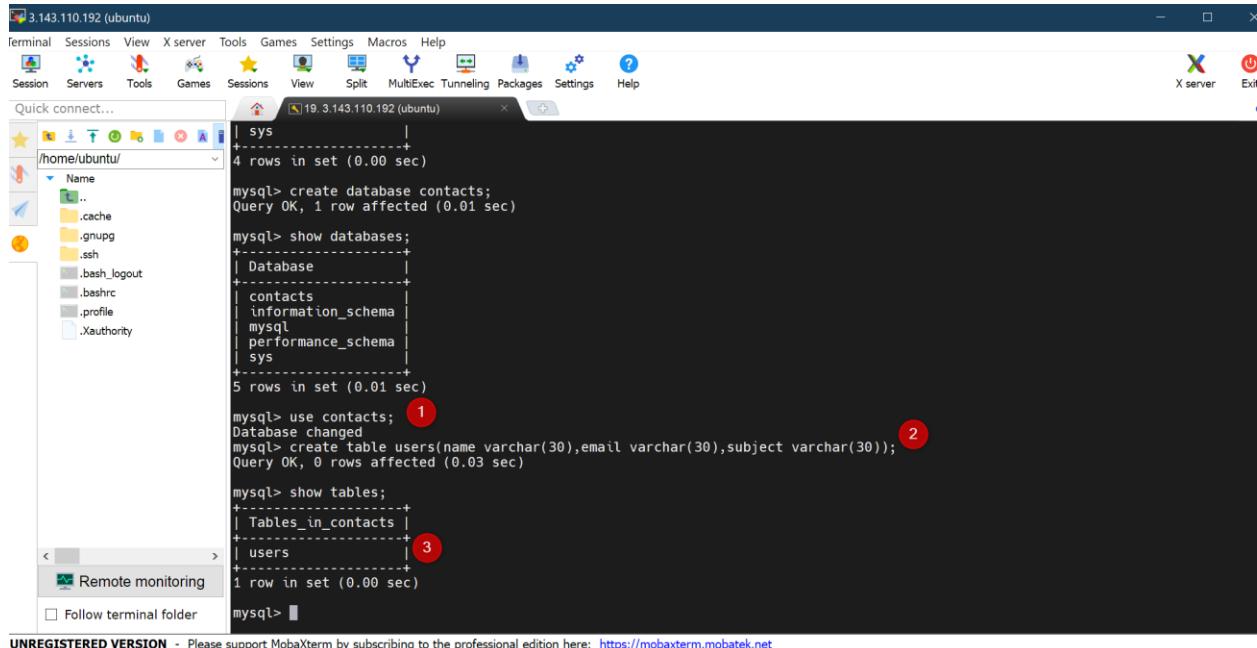
mysql> create database contacts; 1
Query OK, 1 row affected (0.01 sec)

mysql> show databases; 2
+-----+
| Database |
+-----+
| contacts 3 |
| information_schema |
| mysql |
| performance_schema |
| sys |
+-----+
5 rows in set (0.01 sec)

mysql>
```

► Create a tables inside database 'Contacts'

- ▶ `mysql> use contacts;`
- ▶ `mysql> create table users(name varchar(30),email varchar(30),subject varchar(30));`
- ▶ **6.Verify that table 'user's is created**
- ▶ `mysql> show tables;`



```

3.143.110.192 (ubuntu)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect... 19.3.143.110.192 (ubuntu) X server Exit
| sys
+-----+
| 4 rows in set (0.00 sec)

mysql> create database contacts;
Query OK, 1 row affected (0.01 sec)

mysql> show databases;
+-----+
| Database
+-----+
| contacts
| information_schema
| mysql
| performance_schema
| sys
+-----+
5 rows in set (0.01 sec)

mysql> use contacts; 1
Database changed

mysql> create table users(name varchar(30),email varchar(30),subject varchar(30));
Query OK, 0 rows affected (0.03 sec)

mysql> show tables;
+-----+
| Tables_in_contacts
+-----+
| users
+-----+
1 row in set (0.00 sec)

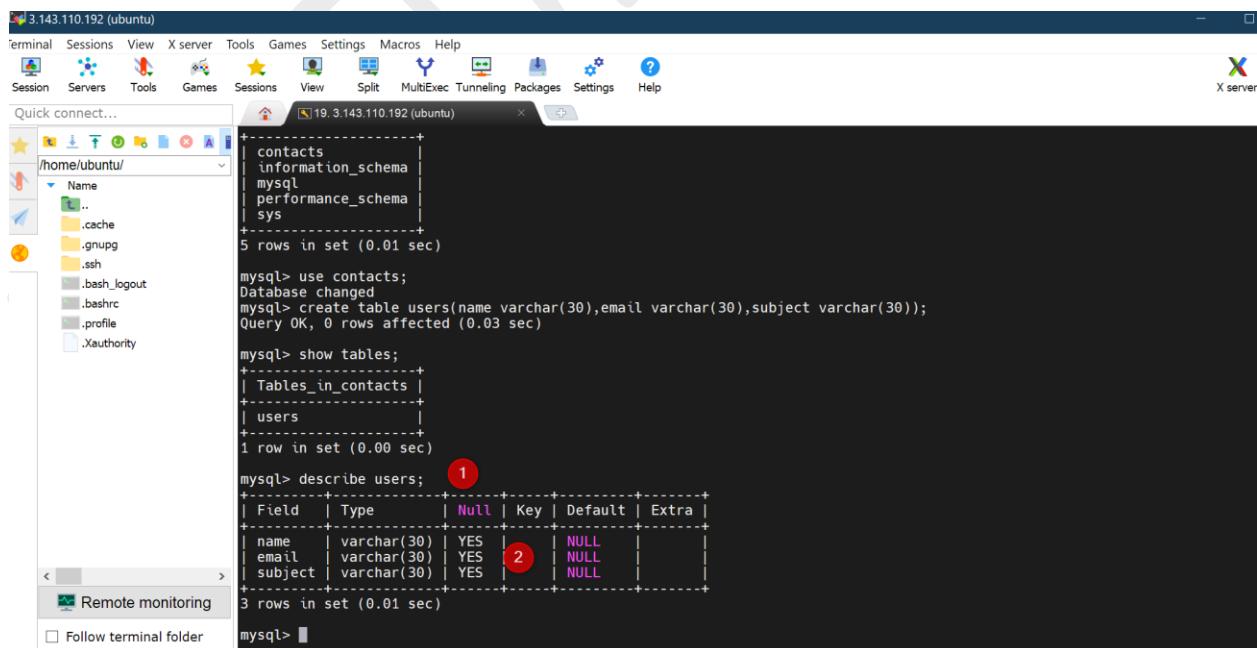
mysql> 2

```

UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: <https://mobaxterm.mobatek.net>

**Describe table and check if the fields are exist**

`mysql>Describe users;`



```

3.143.110.192 (ubuntu)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect... 19.3.143.110.192 (ubuntu) X server
+-----+
| contacts
| information_schema
| mysql
| performance_schema
| sys
+-----+
5 rows in set (0.01 sec)

mysql> use contacts;
Database changed

mysql> create table users(name varchar(30),email varchar(30),subject varchar(30));
Query OK, 0 rows affected (0.03 sec)

mysql> show tables;
+-----+
| Tables_in_contacts
+-----+
| users
+-----+
1 row in set (0.00 sec)

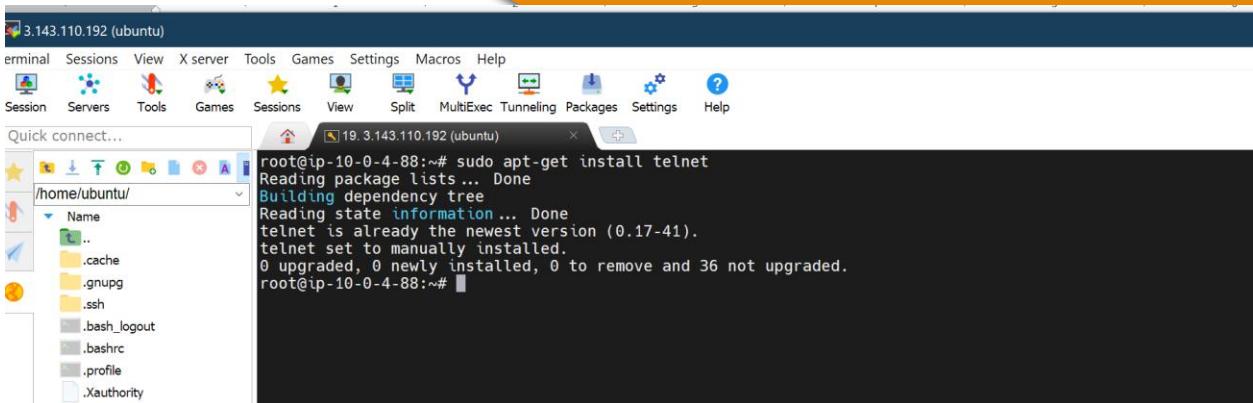
mysql> 1
describe users;
+-----+
| Field | Type | Null | Key | Default | Extra |
+-----+
| name  | varchar(30) | YES | 2 | NULL | |
| email | varchar(30) | YES | | NULL | |
| subject | varchar(30) | YES | | NULL | |
+-----+
3 rows in set (0.01 sec)

mysql> 3

```

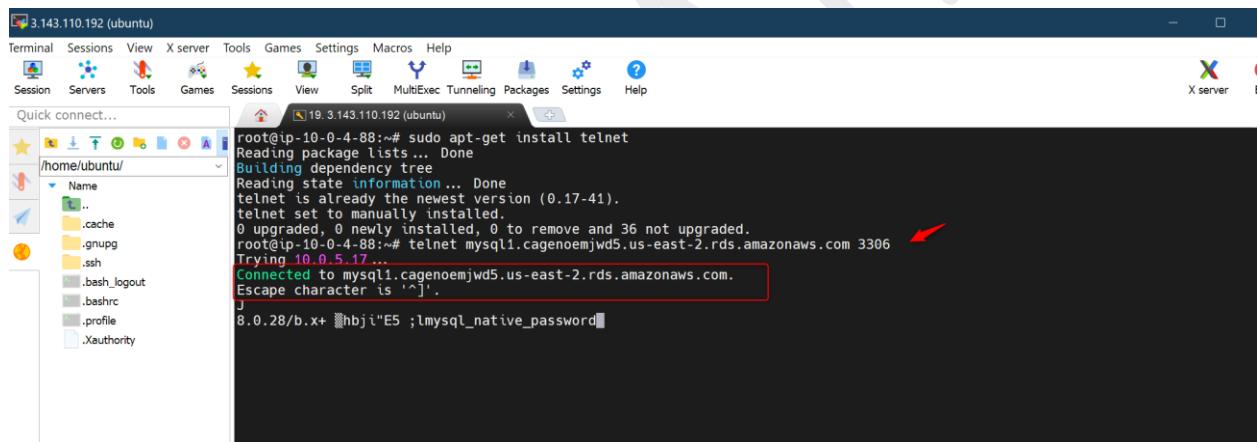
**Install Telnet utility & check DB Connection**

- ▶ `Sudo apt-get install telnet`



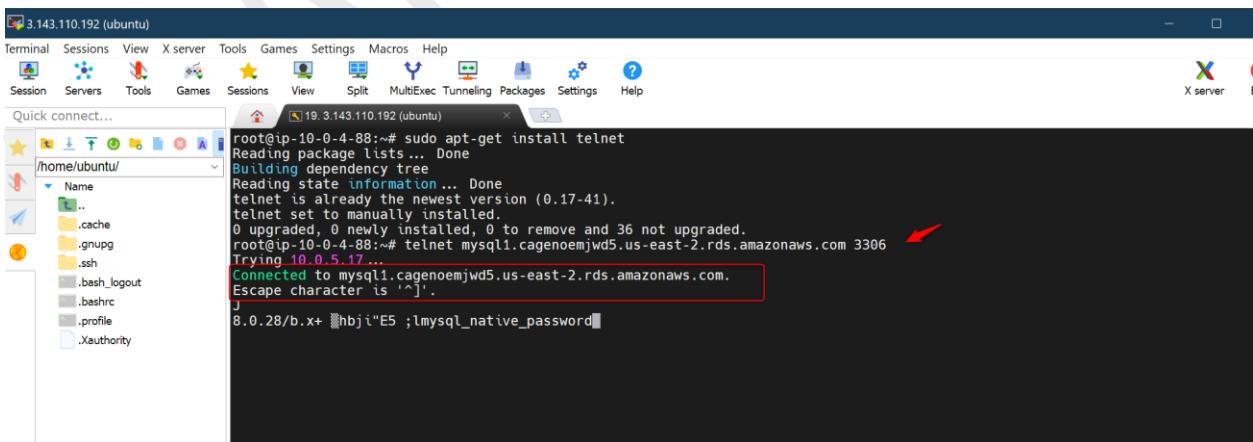
```
root@ip-10-0-4-88:~# sudo apt-get install telnet
Reading package lists... Done
Building dependency tree
Reading state information... Done
telnet is already the newest version (0.17-41).
telnet set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 36 not upgraded.
root@ip-10-0-4-88:~#
```

- ▶ Test RDS DB connection from Web to DB
- ▶ Telnet <RDS MySQL Endpoint> <MySQL port>
- ▶ telnet mysql2021.cnliikk0jg8xf.ca-central-1.rds.amazonaws.com 3306
- ▶



```
root@ip-10-0-4-88:~# sudo apt-get install telnet
Reading package lists... Done
Building dependency tree
Reading state information... Done
telnet is already the newest version (0.17-41).
telnet set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 36 not upgraded.
root@ip-10-0-4-88:~# telnet mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com 3306
Trying 10.0.5.17...
Connected to mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com.
Escape character is '^'.
J
8.0.28/b.x+ 8hbji"E5 ;lmysql_native_password
```

- ▶ If connection is successfully established between both the VPC's then it show's like



```
root@ip-10-0-4-88:~# sudo apt-get install telnet
Reading package lists... Done
Building dependency tree
Reading state information... Done
telnet is already the newest version (0.17-41).
telnet set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 36 not upgraded.
root@ip-10-0-4-88:~# telnet mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com 3306
Trying 10.0.5.17...
Connected to mysql1.cagenoemjwd5.us-east-2.rds.amazonaws.com.
Escape character is '^'.
J
8.0.28/b.x+ 8hbji"E5 ;lmysql_native_password
```

Let's insert data to the database from web application

← → ⌛ Not secure | prefect-alb-784003759.us-east-2.elb.amazonaws.com

**PRAFUL PATEL**

[Home](#) [About](#) [Resume](#) [Portfolio](#) [Services](#) [Contact](#)

**Location:** Regina, CANADA

**Email:** praful.patel@gmail.com

**Call:** +1 5589 55928 55

**Contact Form**

Please fill this form and submit to add employee record to the database.

**Name**  1

**Email**  2

**Subject**  3

**Submit** 4

New record successfully added

prefect-alb-784003759.us-east-2.elb.amazonaws.com/insert.php

← ⌛ Not secure | 18.191.135.225 | prefect-alb-784003759.us-east-2.elb.amazonaws.com/forms/insert.php

New record has been added successfully !

Not secure | prefect-alb-784003759.us-east-2.elb.amazonaws.com

**PRAFUL PATEL**

[Home](#) [About](#) [Resume](#) [Portfolio](#) [Services](#) [Contact](#)

**Contact**

Magnam dolores commodi suscipit. Necessitatibus eius consequatur ex aliquid fuga eum quidem. Sit sint consectetur velit. Quisquam quos quisquam cupiditate. Et nimpedit suscipit alias ea. Quia fugiat sit in iste officiis commodi quidem hic quas.

**Location:** Regina, CANADA

**Email:** praful.patel@gmail.com

**Call:** +1 5589 55928 55



Designed by [BootstrapMade](#)

**Contact Form**

Please fill this form and submit to add employee record to the database.

**Name**  \*

**Email**

**Subject**

**Submit**

Not secure | prefect-alb-784003759.us-east-2.elb.amazonaws.com/forms/insert.php

New record has been added successfully !

Verify from the backend database that data has successfully added from the web application

```

18.191.135.225 (ubuntu)
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
Quick connect...
23.18.191.135.225 (ubuntu)
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> show databases; 1
+-----+
| Database |
+-----+
| information_schema |
| contacts |
| innodb |
| mysql |
| performance_schema |
| sys |
+-----+
6 rows in set (0.00 sec)

mysql> use contacts; 2
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> select * from users; 3
+-----+-----+-----+
| name | email | subject |
+-----+-----+-----+
| Praful | praful1611@outlook.com | test |
| Alex | alex@gmail.com | this is just test |
+-----+-----+-----+
2 rows in set (0.00 sec)

mysql> 4

```

Remote monitoring

Follow terminal folder

## ❖ Improvements Tasks:

- ▶ Reduce security incidents
  - identity and access management
  - Firewalls(web application, network) and DDOS protection
  - Create & manage cryptographic key
  - Manage secrets, API keys, credentials
  - Security assessment for EC2 instances
  - Threat Detection
  - Manage security Alerts
  - Configure security controls for individual AWS services
- ▶ Reduce deployment time & maintenance
  - Automate provisioning
  - Observability of AWS resources
  - Track user action & API usage on AWS
  - Evaluate configuration of AWS resources
  - Centralize operations:
    - Automate actions with runbooks
    - Manage & patch instances
    - Schedule & govern changes



Congratulations!!!! 🎉

► **Clean up project resources:**

- ✓ EC2 instances
- ✓ Volumes
- ✓ Application Load balancer
- ✓ Auto scaling group
- ✓ NAT Gateway
- ✓ Elastic IP
- ✓ RDS DB instance
- ✓ RDS snapshots

PRAFUL PATEL