

Project: EC2 based Web Server & Configure Apache on an EC2 instance

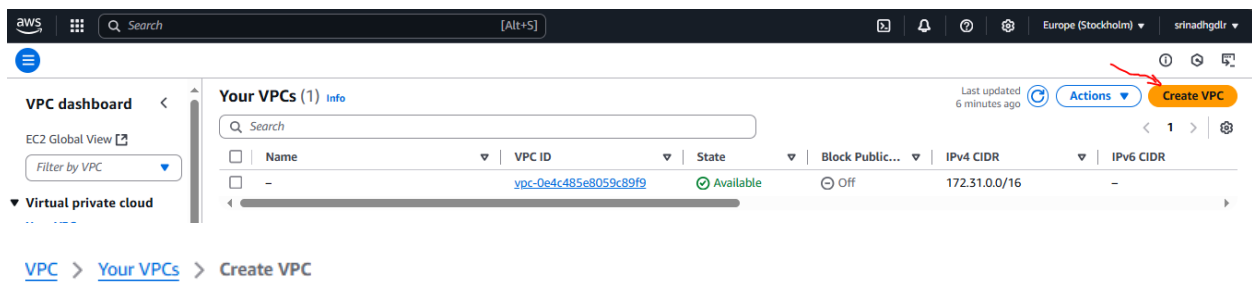
In this project, I will deploy a web server using Amazon EC2.

I will launch an EC2 instance, install Apache and configure it to serve a basic website.

Steps to Set Up an EC2 based Web Server

Step 1: Create VPC

1. Open the AWS Management Console.
2. Navigate to VPC under the Networking & Content Delivery section.
3. Click Create VPC and provide the necessary details in VPC settings:
 - Resources to create: VPC only
 - IPv4 CIDR block: Choose a CIDR block like 10.0.0.0/16
 - Name: myvpc
 - Tenancy: Default is usually fine.
4. Click Create VPC



Create VPC [Info](#)

A VPC is an isolated portion of the AWS Cloud populated by AWS objects, such as Amazon EC2 instances.

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

☒ VPC only

☐ VPC and more

Name tag - optional

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

myvpc

IPv4 CIDR block [Info](#)

☒ IPv4 CIDR manual input

☐ IPAM-allocated IPv4 CIDR block

IPv4 CIDR

10.0.0.0/16

CIDR block size must be between /16 and /28.

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

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

Q Name X

Value - optional

Q myvpc X Remove tag

Add tag

You can add 49 more tags

Cancel Preview code Create VPC

1.1 Create Subnet

A public subnet needs to be created to allow internet traffic.

1. In the VPC Dashboard, click on Subnets on the left side, and then click on Create subnet.

2. Choose the VPC you just created - myvpc

3. Enter the following details:

- Subnet Name: publicsubnet.
- Availability Zone: Select an AZ in your region (eu-north-1a).
- IPv4 CIDR block: Choose a CIDR block like 10.0.1.0/24.

4. Click Create.

aws [Search] [Alt+S] Europe (Stockholm) srinadhgdir

VPC dashboard < EC2 Global View Filter by VPC

Virtual private cloud Your VPCs Subnets

Subnets (3) [Info](#)

Find resources by attribute or tag

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
-	subnet-0bf2a4813162c839f	Available	vpc-0e4c485e8059c89f9	Off	172.31.0.0/24
-	subnet-0605a164679239de5	Available	vpc-0e4c485e8059c89f9	Off	172.31.16.0/24
-	subnet-0d6bcbf7f7550a82e	Available	vpc-0e4c485e8059c89f9	Off	172.31.32.0/24

Actions Create subnet

VPC > Subnets > Create subnet

Create subnet [Info](#)

VPC

VPC ID

Create subnets in this VPC.

vpc-0207cbce3c6f02a1d (myvpc)

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

VPC > Subnets > Create subnet

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.
publicsubnet

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
Europe (Stockholm) / eu-north-1a

IPv4 VPC CIDR block Info
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.
10.0.0.0/16

IPv4 subnet CIDR block
10.0.1.0/24 256 IPs

Tags - optional
Key: Name Value: optional: publicsubnet
Add new tag Remove Add new subnet

Cancel Create subnet

VPC dashboard <
EC2 Global View
Filter by VPC
▼
▼ Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways

Subnets (1) Info
Find resources by attribute or tag
Subnet ID: subnet-06a5cf72b342a191c Clear filters
1 > ⚙️

<input type="checkbox"/>	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR	
<input type="checkbox"/>	publicsubnet	subnet-06a5cf72b342a191c	Available	vpc-0207cbce3c6f02a1d myvpc	Off	10.0.1.0/24	-

1.2 Create an Internet gateways and attach to VPC

An Internet Gateway (IGW) is required to allow communication between the VPC and the internet.

1. In the VPC Dashboard, click on Internet Gateways.
2. Click Create Internet Gateway.
3. Provide a name: IGW
4. Click Create Internet gateway
5. Attach to VPC

Once created, select the newly created IGW and click Attach to VPC. Choose your VPC and click Attach.

VPC dashboard <
EC2 Global View
Filter by VPC
▼
▼ Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet

Internet gateways (1) Info
Search
1 > ⚙️

<input type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner
<input type="checkbox"/>	-	igw-0e1d520842dab8b2f	Attached	vpc-0e4c485e8059c89f9	284514300790

Create internet gateway Info

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

Name tag

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

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

Q Name

X

Value - optional

Q IGW

X

Remove

Add new tag

You can add 49 more tags.

Cancel

Create internet gateway

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

igw-018c440449b1acf84 / IGW

Actions

Details Info

Internet gateway ID

igw-018c440449b1acf84

State

Detached

VPC ID

-

Owner

28451430079

Tags

Search tags

Key

Value

Name

IGW

Manage tags

< 1 > ⚙

Attach to VPC

Detach from VPC

Manage tags

Delete

Attach to VPC (igw-018c440449b1acf84) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

Q vpc-0207cbce3c6f02a1d

Use: "vpc-0207cbce3c6f02a1d"

vpc-0207cbce3c6f02a1d - myvpc

Cancel

Attach internet gateway

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

igw-018c440449b1acf84 / IGW

Actions

Details Info

Internet gateway ID

igw-018c440449b1acf84

State

Attached

VPC ID

vpc-0207cbce3c6f02a1d | myvpc

Owner

284514300790

Tags

Search tags

Key

Value

Name

IGW

Manage tags

< 1 > ⚙

1.3 Create Route tables

1. In the VPC Dashboard, click on Route tables under the left navigation menu.
2. Click Create Route tables.
3. Name: public-route-table
4. Select your VPC from the drop-down list -myvpc
5. Click Create route table

VPC dashboard < EC2 Global View Filter by VPC

Virtual private cloud

- Your VPCs
- Subnets
- Route tables**
- Internet gateways

Route tables (1) info Last updated 20 minutes ago **Actions** **Create route table**

Find resources by attribute or tag

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
<input type="checkbox"/>	-	rtb-08a770e5bcb321169	-	-	Yes	vpc-0e4c485e8059c89f9

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.

VPC
The VPC to use for this route table.

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** **Remove**

Add new tag
You can add 49 more tags.

Cancel **Create route table**

VPC > Route tables > rtb-04510bf8d651b2d03

rtb-04510bf8d651b2d03 / public-route-table **Actions**

Details info

Route table ID rtb-04510bf8d651b2d03	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-0207cbce3c6f02a1d myvpc	Owner ID 284514300790		

Routes | Subnet associations | Edge associations | Route propagation | Tags

Routes (1) Filter routes **Both** **Edit routes**

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

1.4 Edit the Route Table to Add a Route to the Internet Gateway

To enable internet access for the subnet, you need to add a route in the route table.

1. In the Route Tables section, select the route table: public-route-table
2. Under the Routes tab, click Edit routes.
3. Click Add route:
 - Destination: 0.0.0.0/0 (This means all traffic).
 - Target: Select Internet Gateway and then select your Internet Gateway: IGW
4. Click Save changes.

VPC > Route tables > rtb-04510bf8d651b2d03

rtb-04510bf8d651b2d03 / public-route-table

Details

Route table ID: rtb-04510bf8d651b2d03

VPC: vpc-0207cbce3c6f02a1d | myvpc

Main: No

Owner ID: 284514300790

Explicit subnet associations: -

Edge associations: -

Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

VPC > Route tables > rtb-04510bf8d651b2d03 > Edit routes

Edit routes

Destination: 10.0.0.0/16

Target: local

Status: Active

Propagated: No

Add route

Cancel Preview Save changes

VPC > Route tables > rtb-04510bf8d651b2d03 > Edit routes

Edit routes

Destination: 10.0.0.0/16

Target: local

Status: Active

Propagated: No

Add route

Remove

Cancel Preview Save changes

1.5 Associate the Route Table with the Public Subnet

1. In the Route Tables section, select the route table: public-route-table
2. Under the Subnet Associations tab, click Edit subnet associations.
3. Select the Public Subnet: public-subnet
4. Click Save associations.

VPC dashboard < EC2 Global View Filter by VPC ▾

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

▼ Security
Network ACLs
Security groups

▼ PrivateLink and Lattice

rtb-04510bf8d651b2d03 / public-route-table Actions ▾

Details info

Route table ID rtb-04510bf8d651b2d03	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-0207cbce3c6f02a1d myvpc	Owner ID 284514300790		

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

Explicit subnet associations (0) Edit subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
No subnet associations You do not have any subnet associations.			

Subnets without explicit associations (1) 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 tables > rtb-04510bf8d651b2d03 > Edit subnet associations

Edit subnet associations
Change which subnets are associated with this route table.

Available subnets (1/1)

<input checked="" type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	publicsubnet	subnet-06a5cf72b342a191c	10.0.1.0/24	-	Main (rtb-0ba6320bf350d307a)

Selected subnets

subnet-06a5cf72b342a191c / publicsubnet ✕

Cancel Save associations

VPC > Route tables > rtb-04510bf8d651b2d03

VPC dashboard < EC2 Global View Filter by VPC ▾

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

rtb-04510bf8d651b2d03 / public-route-table Actions ▾

Details info

Route table ID rtb-04510bf8d651b2d03	Main No	Explicit subnet associations subnet-06a5cf72b342a191c / publicsubnet	Edge associations -
VPC vpc-0207cbce3c6f02a1d myvpc	Owner ID 284514300790		

Routes Subnet associations Edge associations Route propagation Tags

Routes (2) Both ▾ Edit routes

Destination	Target	Status	Propagated
0.0.0.0/0	igw-018c440449b1acfb4	Active	No
10.0.0.0/16	local	Active	No

1.6 Create Security groups

Using AWS Security Groups

For AWS EC2 instances, the primary firewall configuration is done through Security Groups.

To allow HTTP traffic:

1. Open the AWS Management Console.
2. Navigate to EC2 > Security Groups.
3. Find the security group attached to your EC2 instance.
4. Click on Inbound rules and then Edit inbound rules.
5. Add a new rule:
 - Type: HTTP
 - Protocol: TCP
 - Port Range: 80
 - Source: 0.0.0.0/0 (allow all IPs) or specify a specific IP range if needed.

This will allow HTTP traffic through your instance's firewall Security Group at the AWS level.

VPC dashboard < **Security Groups (2)** Info

EC2 Global View Filter by VPC

▼ **Virtual private cloud**

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

▼ **Security**

- Network ACLs
- Security groups**

Find resources by attribute or tag

Actions Export security groups to CSV **Create security group**

<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description
<input type="checkbox"/>	-	sg-05851d1375f0a36a3	default	vpc-0207cbce3c6f02a1d	default VPC se
<input type="checkbox"/>	-	sg-0f23f0888d10c342f	default	vpc-0e4c485e8059c89f9	default VPC se

VPC > Security Groups > Create security group

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

mySG

Name cannot be edited after creation.

Description

Allow SSH and http

VPC

vpc-0207cbce3c6f02a1d (myvpc)

Inbound rules

This security group has no inbound rules.

Add rule

VPC > Security Groups > Create security group

Inbound rules

Type	Protocol	Port range	Source	Description - optional
SSH	TCP	22	Anywhere... 0.0.0.0/0	
HTTP	TCP	80	Anywhere... 0.0.0.0/0	

Add rule

Outbound rules

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

Add rule

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.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Create security group

VPC > Security Groups > sg-01c08d157563f6e26 - mySG

VPC dashboard

EC2 Global View

Filter by VPC

Virtual private cloud

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

Security

- Network ACLs
- Security groups

sg-01c08d157563f6e26 - mySG

Actions

Details

Security group name mySG	Security group ID sg-01c08d157563f6e26	Description Allow SSH and http	VPC ID vpc-0207cbce3c6f02a1d
Owner 284514300790	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules

Outbound rules

Sharing - new

VPC associations - new

Tags

Inbound rules (2)

Manage tags Edit inbound rules

Search

	Name	Security group rule ID	IP version	Type	Protocol	Port range
<input type="checkbox"/>	-	sgr-03ea6fde31726a084	IPv4	SSH	TCP	22
<input type="checkbox"/>	-	sgr-06b25b4932b1a88eb	IPv4	HTTP	TCP	80

Step 2: Launch an EC2 Instance

- Go to the AWS Management Console → EC2.
- Click Launch Instance.
- Configure the instance:
 - Name: MyWebserver
 - AMI: Choose Amazon Linux 2
 - Instance Type: t3.micro (Free Tier eligible)
 - Key Pair: Create a new key pair or use an existing one. (mykeypair)
 - Security Group: Choose the existing Security Group: mySG
- Click Launch Instance.

aws

Search

[Alt+S]

Europe (Stockholm)

srinadgdir

EC2 > Instances > Launch an instance

Launch an instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags

Name

MyWebserver

Add additional tags

Application and OS Images (Amazon Machine Image)

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

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Linux

Debian

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Summary

Number of instances 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0c2e61fdc5495691

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

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

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier...

Cancel Launch instance Preview code

Instance type

Info | Get advice

Instance type

t3.micro Free tier eligible

Family: t3 2 vCPU 1 GiB Memory Current generation: true

On-Demand Ubuntu Pro base pricing: 0.0143 USD per Hour

On-Demand RHEL base pricing: 0.0396 USD per Hour

On-Demand Linux base pricing: 0.0108 USD per Hour

On-Demand SUSE base pricing: 0.0108 USD per Hour

On-Demand Windows base pricing: 0.02 USD per Hour

All generations

Compare instance types

Additional costs apply for AMIs with pre-installed software

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 - required

mykeypair

Create new key pair

Summary

Number of instances 1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0c2e61fdc5495691

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

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

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where t2.micro isn't available) when used with free tier...

▼ Network settings Info

VPC - required Info

vpc-0207cbce3c6f02a1d (myvpc)
10.0.0.0/16

↻

Subnet Info

subnet-06a5cf72b342a191c
VPC: vpc-0207cbce3c6f02a1d Owner: 284514300790 Availability Zone: eu-north-1a
Zone type: Availability Zone IP addresses available: 251 CIDR: 10.0.1.0/24

publicsubnet
↻ Create new subnet

Auto-assign public IP Info

Enable

Additional charges apply when outside of free tier allowance

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.

Create security group

Select existing security group

Common security groups Info

Select security groups

mySG sg-01c08d157563f6e26
VPC: vpc-0207cbce3c6f02a1d

Compare security group rules

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

► Advanced network configuration

▼ Configure storage Info Advanced

1x 8 GIB gp3 Root volume, 3000 IOPS, Not encrypted

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

Click refresh to view backup information

The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems Edit

► Advanced details Info

Software Image (AMI)
Amazon Linux 2023 AMI 2023.6.2...read more
ami-0c2e61fdbc5495691

Virtual server type (instance type)
t3.micro

Firewall (security group)
mySG

Storage (volumes)
1 volume(s) - 8 GIB

Free tier: In your first year of opening an AWS account, you get 750 hours per month of t2.micro instance usage (or t3.micro where

Cancel Launch instance Preview code

- Create Key pair as below and save it some location, we have to use this to connect EC2 instance

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

mykeypair

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair

Private key file format

☐ .pem
For use with OpenSSH

☒ .ppk
For use with PuTTY

⚠ When prompted, store the private key in a secure and accessible location on your computer. You will need it later to connect to your instance. [Learn more](#)

Cancel

Create key pair

EC2 > Instances > Launch an instance

Success
Successfully initiated launch of instance (i-0a4d6653f6e0c3a36)

Launch log

Manage detailed monitoring

Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.

Manage detailed monitoring

Create Load Balancer

Create a application, network gateway or classic Elastic Load Balancer

Create Load Balancer

Create AWS budget

AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.

Create AWS budget

Manage CloudWatch alarms

Create or update Amazon CloudWatch alarms for the instance.

Manage CloudWatch alarms

View all instances

Step 3: Connect to the EC2 Instance

Open a terminal in MacOS and Linux laptop and run:

```
ssh -i your-key.pem ec2-user@your-EC2-instance-public-ip
```

```
(login as ec2-user)
```

or

Open putty in windows laptop and connect EC2 instance public IPV4 address

Get the ip 51.20.63.231 from EC2 instance details

Here we need to upload keypair into putty and login as ec2-user into EC2 server

```
ec2-user@ip-10-0-1-220:~  
login as: ec2-user  
Authenticating with public key "mykeypair"  
  
#_      _____  
~\####   Amazon Linux 2023  
~~\#####\  
~~ \###|  
~~  \#/    https://aws.amazon.com/linux/amazon-linux-2023  
~~   V~' '->  
~~~~  
~~ . _.  
~~ / /  
~~ /m/'
```

[ec2-user@ip-10-0-1-220 ~]\$

Step 4: Install Apache

For Apache (httpd), run below commands in EC2 server

Update the package repository:

```
sudo yum update -y # Amazon Linux
```

#Install Apache:

```
sudo yum install httpd -y # Amazon Linux
```

#Start and enable Apache:

```
sudo systemctl start httpd # Amazon Linux
```

```
sudo systemctl enable httpd # Amazon Linux
```

```
[ec2-user@ip-10-0-1-220 ~]$ hostname
ip-10-0-1-220.eu-north-1.compute.internal
[ec2-user@ip-10-0-1-220 ~]$ date
Wed Mar 26 20:24:03 UTC 2025
[ec2-user@ip-10-0-1-220 ~]$
[ec2-user@ip-10-0-1-220 ~]$
[ec2-user@ip-10-0-1-220 ~]$ sudo yum update -y
sudo yum install httpd -y
sudo systemctl start httpd
sudo systemctl enable httpd
Amazon Linux 2023 Kernel Livepatch repository
115 kB/s | 15 kB    00:00
=====
WARNING:
  A newer release of "Amazon Linux" is available.

Available Versions:

  Version 2023.6.20250317:
    Run the following command to upgrade to 2023.6.20250317:

      dnf upgrade --releasever=2023.6.20250317

  Release notes:
    https://docs.aws.amazon.com/linux/al2023/release-notes/relnotes-2023.6.20250317.html
=====
Dependencies resolved.
Nothing to do.
Complete!
Last metadata expiration check: 0:00:01 ago on Wed Mar 26 20:27:35 2025.
Dependencies resolved.
```

Package	Architecture	Version	Repository	Size
Installing:				
httpd	x86_64	2.4.62-1.amzn2023	amazonlinux	48 k
Installing dependencies:				
apr	x86_64	1.7.5-1.amzn2023.0.4	amazonlinux	129 k
apr-util	x86_64	1.6.3-1.amzn2023.0.1	amazonlinux	98 k
generic-logos-httpd	noarch	18.0.0-12.amzn2023.0.3	amazonlinux	19 k
httpd-core	x86_64	2.4.62-1.amzn2023	amazonlinux	1.4 M
httpd-filesystem	noarch	2.4.62-1.amzn2023	amazonlinux	14 k
httpd-tools	x86_64	2.4.62-1.amzn2023	amazonlinux	81 k
libbrotli	x86_64	1.0.9-4.amzn2023.0.2	amazonlinux	315 k
mailcap	noarch	2.1.49-3.amzn2023.0.3	amazonlinux	33 k
Installing weak dependencies:				
apr-util-openssl	x86_64	1.6.3-1.amzn2023.0.1	amazonlinux	17 k
mod_http2	x86_64	2.0.27-1.amzn2023.0.3	amazonlinux	166 k
mod_lua	x86_64	2.4.62-1.amzn2023	amazonlinux	61 k
Transaction Summary				
Install 12 Packages				
Total download size: 2.3 M				
Installed size: 6.9 M				
Downloading Packages:				
(1/12): apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64.rpm			460 kB/s 17 kB	00:00
(2/12): apr-util-1.6.3-1.amzn2023.0.1.x86_64.rpm			2.1 MB/s 98 kB	00:00
(3/12): apr-1.7.5-1.amzn2023.0.4.x86_64.rpm			2.4 MB/s 129 kB	00:00
(4/12): generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch.rpm			974 kB/s 19 kB	00:00
(5/12): httpd-2.4.62-1.amzn2023.x86_64.rpm			2.4 MB/s 48 kB	00:00
(6/12): httpd-filesystem-2.4.62-1.amzn2023.noarch.rpm			791 kB/s 14 kB	00:00
(7/12): httpd-tools-2.4.62-1.amzn2023.x86_64.rpm			3.6 MB/s 81 kB	00:00
(8/12): httpd-core-2.4.62-1.amzn2023.x86_64.rpm			27 MB/s 1.4 MB	00:00
(9/12): mailcap-2.1.49-3.amzn2023.0.3.noarch.rpm			1.7 MB/s 33 kB	00:00
(10/12): libbrotli-1.0.9-4.amzn2023.0.2.x86_64.rpm			8.0 MB/s 315 kB	00:00
(11/12): mod_http2-2.0.27-1.amzn2023.0.3.x86_64.rpm			7.2 MB/s 166 kB	00:00
(12/12): mod_lua-2.4.62-1.amzn2023.x86_64.rpm			2.9 MB/s 61 kB	00:00
Total				14 MB/s 2.3 MB 00:00

Total				14 MB/s 2.3 MB 00:00
Running transaction check				
Transaction check succeeded.				
Running transaction test				
Transaction test succeeded.				
Running transaction				
Preparing	:			1/1
Installing	:	apr-1.7.5-1.amzn2023.0.4.x86_64		1/12
Installing	:	apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64		2/12
Installing	:	apr-util-1.6.3-1.amzn2023.0.1.x86_64		3/12
Installing	:	mailcap-2.1.49-3.amzn2023.0.3.noarch		4/12
Installing	:	httpd-tools-2.4.62-1.amzn2023.x86_64		5/12
Installing	:	libbrotli-1.0.9-4.amzn2023.0.2.x86_64		6/12
Running scriptlet:	:	httpd-filesystem-2.4.62-1.amzn2023.noarch		7/12
Installing	:	httpd-filesystem-2.4.62-1.amzn2023.noarch		7/12
Installing	:	httpd-core-2.4.62-1.amzn2023.x86_64		8/12
Installing	:	mod_http2-2.0.27-1.amzn2023.0.3.x86_64		9/12
Installing	:	mod_lua-2.4.62-1.amzn2023.x86_64		10/12
Installing	:	generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch		11/12
Installing	:	httpd-2.4.62-1.amzn2023.x86_64		12/12
Running scriptlet:	:	httpd-2.4.62-1.amzn2023.x86_64		12/12
Verifying	:	apr-1.7.5-1.amzn2023.0.4.x86_64		1/12
Verifying	:	apr-util-1.6.3-1.amzn2023.0.1.x86_64		2/12
Verifying	:	apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64		3/12
Verifying	:	generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch		4/12
Verifying	:	httpd-2.4.62-1.amzn2023.x86_64		5/12
Verifying	:	httpd-core-2.4.62-1.amzn2023.x86_64		6/12
Verifying	:	httpd-filesystem-2.4.62-1.amzn2023.noarch		7/12
Verifying	:	httpd-tools-2.4.62-1.amzn2023.x86_64		8/12
Verifying	:	libbrotli-1.0.9-4.amzn2023.0.2.x86_64		9/12
Verifying	:	mailcap-2.1.49-3.amzn2023.0.3.noarch		10/12
Verifying	:	mod_http2-2.0.27-1.amzn2023.0.3.x86_64		11/12
Verifying	:	mod_lua-2.4.62-1.amzn2023.x86_64		12/12
=====				
WARNING:				

```

WARNING:
  A newer release of "Amazon Linux" is available.

Available Versions:

Version 2023.6.20250317:
  Run the following command to upgrade to 2023.6.20250317:

    dnf upgrade --releasever=2023.6.20250317

Release notes:
  https://docs.aws.amazon.com/linux/al2023/release-notes/relnotes-2023.6.20250317.html
=====

Installed:
apr-1.7.5-1.amzn2023.0.4.x86_64          apr-util-1.6.3-1.amzn2023.0.1.x86_64          apr-util-openssl-1.6.3-1.amzn2023.0.1.x86_64
generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch  httpd-2.4.62-1.amzn2023.x86_64          httpd-core-2.4.62-1.amzn2023.x86_64
httpdfilesystem-2.4.62-1.amzn2023.noarch          httpd-tools-2.4.62-1.amzn2023.x86_64          libbrotli-1.0.9-4.amzn2023.0.2.x86_64
mailcap-2.1.49-3.amzn2023.0.3.noarch              mod_http2-2.0.27-1.amzn2023.0.3.x86_64          mod_lua-2.4.62-1.amzn2023.x86_64

Complete!
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[ec2-user@ip-10-0-1-220 ~]$
[ec2-user@ip-10-0-1-220 ~]$

```

Verify installation:

sudo systemctl status httpd # Amazon Linux

```

[ec2-user@ip-10-0-1-220 ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Wed 2025-03-26 20:27:39 UTC; 14min ago
     Docs: man:httpd.service(8)
  Main PID: 3639 (httpd)
    Status: "Total requests: 2; Idle/Busy workers 100/0;Requests/sec: 0.00233; Bytes served/sec: 1 B/sec"
    Tasks: 177 (limit: 1058)
   Memory: 13.6M
      CPU: 864ms
   CGroup: /system.slice/httpd.service
           └─3639 /usr/sbin/httpd -DFOREGROUND
             └─3744 /usr/sbin/httpd -DFOREGROUND
               └─3746 /usr/sbin/httpd -DFOREGROUND
                 └─3747 /usr/sbin/httpd -DFOREGROUND
                   └─3748 /usr/sbin/httpd -DFOREGROUND

Mar 26 20:27:39 ip-10-0-1-220.eu-north-1.compute.internal systemd[1]: Starting httpd.service - The Apache HTTP Server...
Mar 26 20:27:39 ip-10-0-1-220.eu-north-1.compute.internal systemd[1]: Started httpd.service - The Apache HTTP Server.
Mar 26 20:27:39 ip-10-0-1-220.eu-north-1.compute.internal httpd[3639]: Server configured, listening on: port 80
[ec2-user@ip-10-0-1-220 ~]$

```

Step 5: Deploy a Web Page

Edit the default index file:

Run below command in EC2 server

echo "<h1>Welcome to My Web Server</h1>" | sudo tee /var/www/html/index.html > /dev/null

```

[ec2-user@ip-10-0-1-220 ~]$ echo "<h1>Welcome to My Web Server</h1>" | sudo tee /var/www/html/index.html > /dev/null
[ec2-user@ip-10-0-1-220 ~]$
[ec2-user@ip-10-0-1-220 ~]$

```

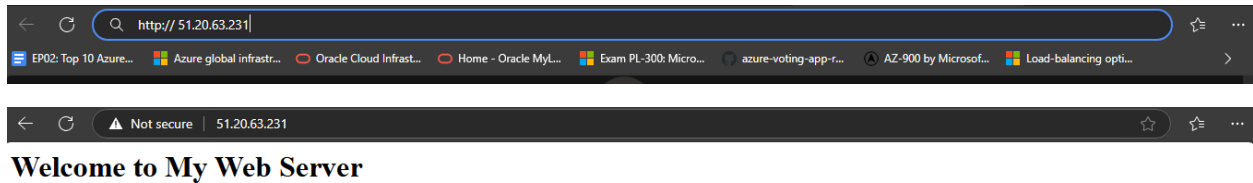
Step 6: Access the Web Server

Open a browser and go to:

`http://EC2-instance-public-ip`

Here it is: `http://51.20.63.231`

"I should see "Welcome to My Web Server"



Step 7: Configure Auto Start (Optional)

Ensure the web server starts on reboot:

`sudo systemctl enable httpd # Apache`

```
[ec2-user@ip-10-0-1-220 ~]$  
[ec2-user@ip-10-0-1-220 ~]$ sudo systemctl enable httpd  
[ec2-user@ip-10-0-1-220 ~]$
```

Conclusion

I have successfully deployed an EC2 based web server running Apache. This setup is commonly used for hosting websites, web applications, or acting as a reverse proxy.