

# How does AWS WAF Protect?

## INTRODUCTION

AWS WAF protects your web applications from common web exploits

It is a web application firewall service that lets you monitor web requests forwarded to an Amazon API Gateway API, an Amazon CloudFront distribution, or an Application Load Balancer.

You can protect those resources based on conditions you specify, such as the IP addresses from which the requests originate.

It comes under → Security, Identity, and Compliance Services

## OBJECTIVE

We will understand the importance of AWS WAF by implementing it to block my laptop or any IP address from accessing EC2 instances (accessed via Load balancer).

The uses of AWS WAF are boundless. It can be used to set up other rules like CAPTCHA, Count, and Challenge and enable CloudWatch metrics.

## PREREQUISITES

**AWS Account:** You need an AWS account to access and use AWS WAF. If you do not have an account, you can sign up for one on the AWS website.

**Web Application:** AWS WAF is designed to protect web applications deployed on AWS services such as Amazon CloudFront, Application Load Balancer, or Amazon API Gateway. Therefore, you should have a web application deployed on these services or plan to deploy one.

**AWS Management Console or AWS CLI:** You can manage AWS WAF either through the AWS Management Console, which provides a web-based interface, or by using the AWS Command Line Interface (CLI). Ensure that you have access to either of these tools to configure and manage AWS WAF.

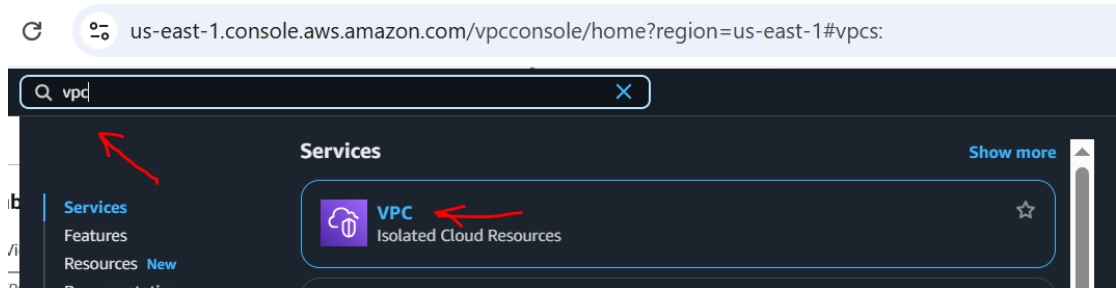
**Basic Understanding of Web Application Security:** While AWS WAF simplifies the process of protecting your web applications, it is beneficial to have a basic understanding of common web application security vulnerabilities and best practices. This knowledge helps create effective rules and configure AWS WAF to suit your application's needs.

By meeting these prerequisites, you can effectively leverage the benefits of AWS WAF to enhance the security of your web applications in the AWS ecosystem.

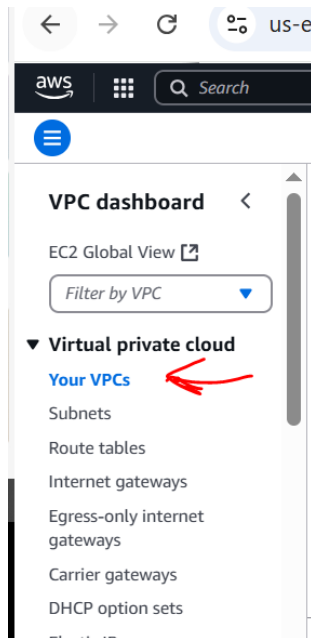
## IMPLEMENTATION STEPS

### 1. Create VPC

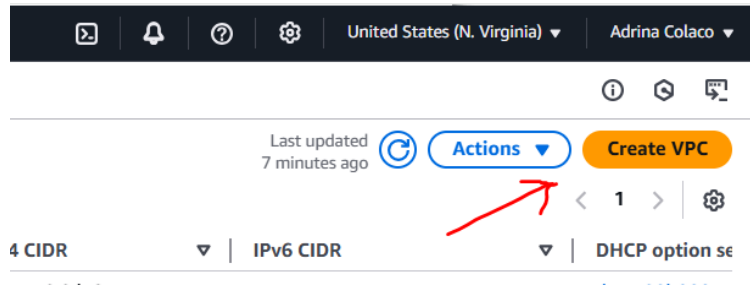
- a. Type “VPC” in the search bar and click on “VPC” in the search results



- b. Go to “Your VPC” on the left panel.



- c. Click on “Create VPC” on the right corner.



- d. Enter the highlighted details in the Launch an instance page and click on “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.

test-vpc

**IPv4 CIDR block** [Info](#)  
☒ IPv4 CIDR manual input  
☐ IPAM-allocated IPv4 CIDR block

**IPv4 CIDR**  
12.0.0.0/16  
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.

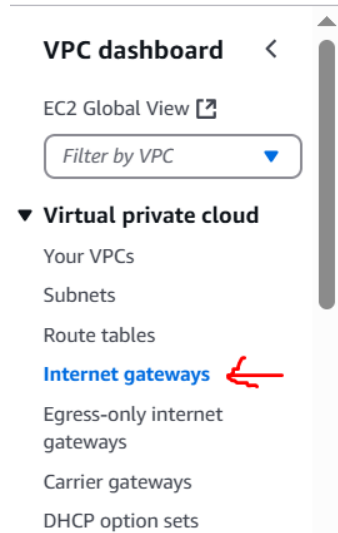
Key	Value - optional	
Q Name	Q test-vpc	Remove tag
<a href="#">Add tag</a>		

You can add 49 more tags

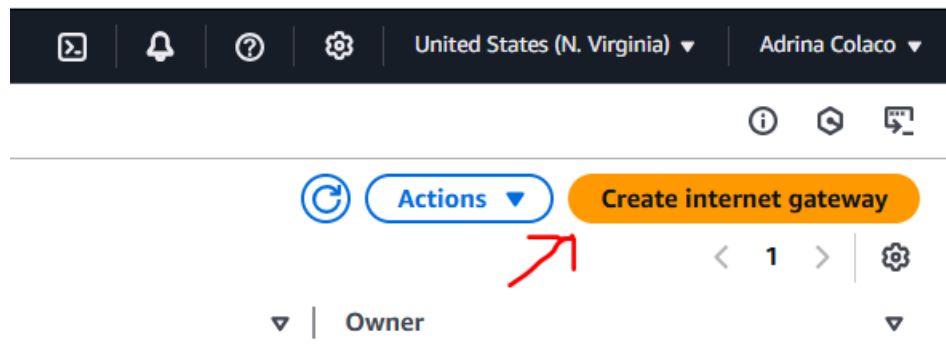
Cancel [Preview code](#) [Create VPC](#)

## 2. Create Internet Gateway

- a. Click on “Internet Gateways” in the left panel.



- b. Click on “Create internet gateway”



- c. Enter the details in highlighted fields and click on “Create internet gateway”.

**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.

**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	Value - optional
<input type="text" value="Q, Name"/>	<input type="text" value="Q, igw-test"/>

[Add new tag](#) [Remove](#)

You can add 49 more tags.

[Cancel](#) [Create internet gateway](#)

- d. Goto “Actions” and click on “Attach to VPC”

igw-0d64845c4e6d7b1ec / igw-test

**Details** [Info](#)

Internet gateway ID igw-0d64845c4e6d7b1ec	State Detached	VPC ID -	Owner 311141542113
--	-------------------	-------------	-----------------------

**Tags**

Search tags

Key	Value
Name	igw-test

**Actions**

- Attach to VPC
- Detach from VPC
- Manage tags
- Delete

**Manage tags**

< 1 > ⚙

- e. Select the respective VPC and click on “Attach internet gateway”.

**Attach to VPC (igw-0d64845c4e6d7b1ec)** [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-01f63a55063cdef6f

Use: "vpc-01f63a55063cdef6f"

vpc-01f63a55063cdef6f -test-vpc

**Cancel** **Attach internet gateway**

### 3. Create Public Subnet

- a. Go to “Subnets” on the left panel.

**VPC dashboard** <

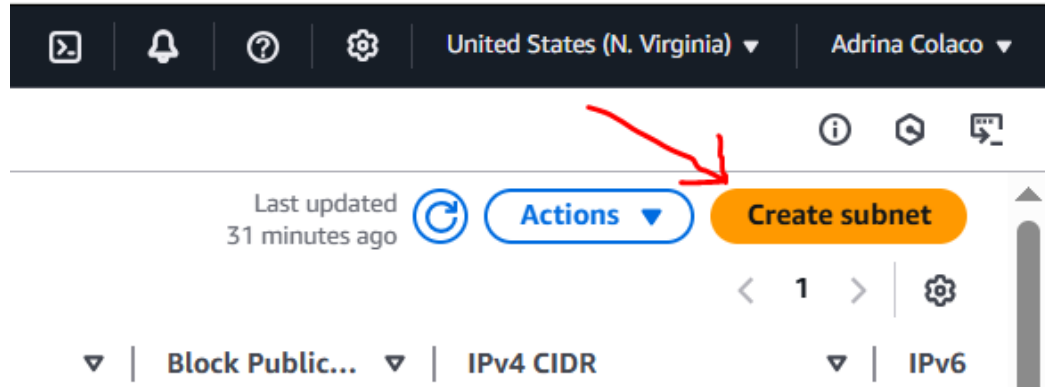
EC2 Global View [↗](#)

Filter by VPC ▼

▼ **Virtual private cloud**

- Your VPCs
- Subnets** ←
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways

- b. Click on “Create subnet”



- c. Create two subnets in 2 different availability zones and fill out the highlighted fields.

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

**VPC**

**VPC ID**  
Create subnets in this VPC.

vpc-01f63a55063cdef6f (test-vpc)

**Associated VPC CIDRs**

**IPv4 CIDRs**  
12.0.0.0/16

#### Details of first Subnet

**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.

test-public-subnet-1a

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.

United States (N. Virginia) / us-east-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.

12.0.0.0/16

**IPv4 subnet CIDR block**

12.0.1.0/24 256 IPs

**Tags - optional**

Key	Value - optional
Name	test-public-subnet-1a

[Add new tag](#)

You can add 49 more tags.

[Remove](#)

Add details of the second subnet by clicking on the “Add new subnet” button. Enter details as highlighted below and click on “Create subnet”.

**Subnet 2 of 2**

**Subnet name**  
Create a tag with a key of 'Name' and a value that you specify.  
test-public-subnet-1b  
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.  
United States (N. Virginia) / us-east-1b

**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.  
12.0.0.0/16

**IPv4 subnet CIDR block**  
12.0.2.0/24 256 IPs

▼ **Tags - optional**

Key	Value - optional	
Q Name	test-public-subnet-1b	Remove

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

[Remove](#)

[Add new subnet](#)

[Cancel](#) [Create subnet](#)

d. Subnets will be created.

**Subnets (2)** [Info](#) Last updated less than a minute ago [Actions](#) [Create](#)

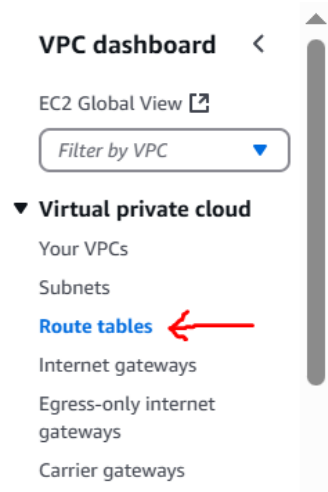
Find resources by attribute or tag

Subnet ID : subnet-01523b3f16ca2fbc0 Subnet ID : subnet-023cdb9640b08ad39 [Clear filters](#)

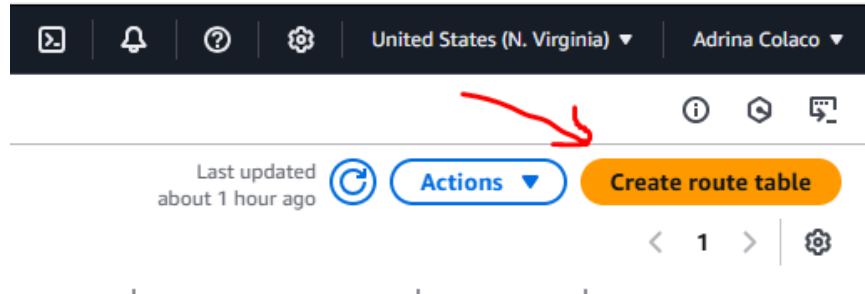
<input type="checkbox"/>	Name	Subnet ID	State	VPC	Block Public...
<input type="checkbox"/>	test-public-subnet-1a	subnet-01523b3f16ca2fbc0	Available	vpc-01f63a55063cdef6f   test-vpc	Off
<input type="checkbox"/>	test-public-subnet-1b	subnet-023cdb9640b08ad39	Available	vpc-01f63a55063cdef6f   test-vpc	Off

## 4. Create Route table

a. Go to "Route tables" in the left panel.



b. Click on the "Create route table" button in the right corner.



- c. Enter details into the highlighted fields and click on the “Create route table” button.

**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**

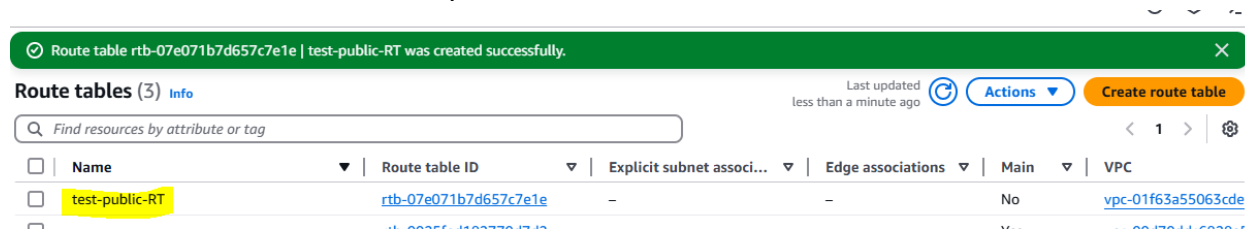
**Value - optional**  
 [Remove](#)

[Add new tag](#)

You can add 49 more tags.

[Cancel](#) [Create route table](#)

- d. The route table will be successfully created.



- e. Associate Subnets to the Route table by clicking on “Edit subnet associations”.



Route tables (1/3) Info Last updated 6 minutes ago Actions Create route table

Find resources by attribute or tag

	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
<input checked="" type="checkbox"/>	test-public-RT	<a href="#">rtb-07e071b7d657c7e1e</a>	-	-	No	<a href="#">vpc-01f63a55063cde</a>
<input type="checkbox"/>	-	<a href="#">rtb-0025fed182770d7d2</a>	-	-	Yes	<a href="#">vpc-00d70ddc6828a</a>
<input type="checkbox"/>	-	<a href="#">rtb-0247bf3e6c355591d</a>	-	-	Yes	<a href="#">vpc-01f63a55063cde</a>

rtb-07e071b7d657c7e1e / test-public-RT

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

Explicit subnet associations (0) Edit subnet associations

Find subnet association

Name	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:

Find subnet association

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
test-public-subnet-1a	<a href="#">subnet-01523b3f16ca2fbc0</a>	12.0.1.0/24	-
test-public-subnet-1b	<a href="#">subnet-023cdb9640b08ad39</a>	12.0.2.0/24	-

f. Check mark on both the subnets and click on “Save associations”

#### Edit subnet associations

Change which subnets are associated with this route table.

Available subnets (2/2) Filter subnet associations 1

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input checked="" type="checkbox"/>	test-public-subnet-1a	<a href="#">subnet-01523b3f16ca2fbc0</a>	12.0.1.0/24	-	Main (rtb-0247bf3e6c355591d)
<input checked="" type="checkbox"/>	test-public-subnet-1b	<a href="#">subnet-023cdb9640b08ad39</a>	12.0.2.0/24	-	Main (rtb-0247bf3e6c355591d)

Selected subnets

[subnet-01523b3f16ca2fbc0 / test-public-subnet-1a](#) [subnet-023cdb9640b08ad39 / test-public-subnet-1b](#)

Cancel Save associations

Subnets associated with the Route table.

You have successfully updated subnet associations for rtb-07e071b7d657c7e1e / test-public-RT.

Route tables (1/3) Info

Last updated about 1 hour ago

Actions

Create route table

Find resources by attribute or tag

<input checked="" type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
<input checked="" type="checkbox"/>	test-public-RT	rtb-07e071b7d657c7e1e	2 subnets	-	No	vpc-01f63a55063cde
<input type="checkbox"/>	-	rtb-0025fed182770d7d2	-	-	Yes	vpc-00d70ddc6828a5
<input type="checkbox"/>	-	rtb-0247bf3e6c355591d	-	-	Yes	vpc-01f63a55063cde

rtb-07e071b7d657c7e1e / test-public-RT

DetailsRoutesSubnet associationsEdge associationsRoute propagationTags

Explicit subnet associations (2)

Find subnet association

Edit subnet associations

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
test-public-subnet-1a	subnet-01523b3f16ca2fbc0	12.0.1.0/24	-
test-public-subnet-1b	subnet-023cdb9640b08ad39	12.0.2.0/24	-

g. Edit the Routes to provide internet access to the Route table.

Route tables (1/3) Info

Last updated about 1 hour ago

Actions

Create route table

Find resources by attribute or tag

<input checked="" type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
<input checked="" type="checkbox"/>	test-public-RT	rtb-07e071b7d657c7e1e	2 subnets	-	No	vpc-01f63a55063cde
<input type="checkbox"/>	-	rtb-0025fed182770d7d2	-	-	Yes	vpc-00d70ddc6828a5
<input type="checkbox"/>	-	rtb-0247bf3e6c355591d	-	-	Yes	vpc-01f63a55063cde

rtb-07e071b7d657c7e1e / test-public-RT

DetailsRoutesSubnet associationsEdge associationsRoute propagationTags

Routes (1)

Filter routes

Both

Edit routes

Destination	Target	Status	Propagated
12.0.0.0/16	local	Active	No

h. Click on “Add route” and add the highlighted fields. Click on “Save changes”.

Edit routes

Destination

12.0.0.0/16

Target

local

local

Internet Gateway

igw-0d64845c4e6d7b1ec

Use: "igw-0d64845c4e6d7b1ec"

igw-0d64845c4e6d7b1ec (igw-test)

Status

Active

-

Propagated

No

No

Add route

Remove

Cancel

Preview

Save changes

- i. Routes should be updated and active.

rtb-07e071b7d657c7e1e / test-public-RT

Actions

**Details** Info

**Route table ID**  
rtb-07e071b7d657c7e1e

**VPC**  
vpc-01f63a55063cdef6f

**Main**  
No

**Owner ID**  
311141542113

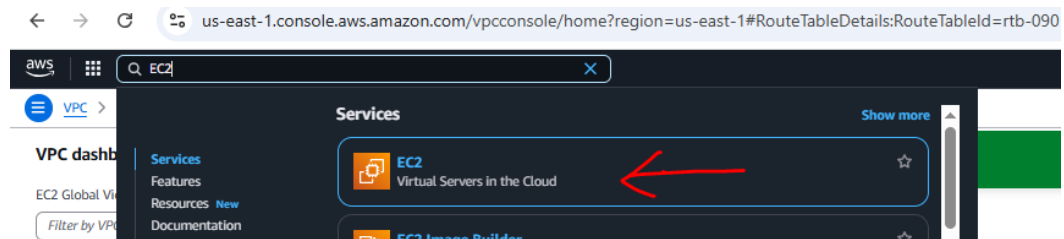
**Explicit subnet associations**  
2 subnets

**Edge associations**  
-

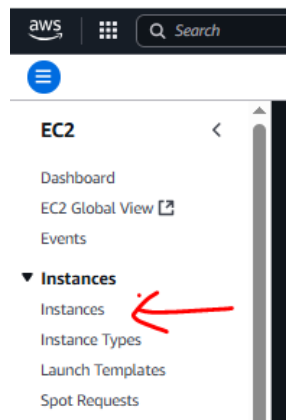
**Routes** Subnet associations Edge associations Route propagation Tags**Routes (2)** Both Edit routes

## 5. Create an “EC2” instance.

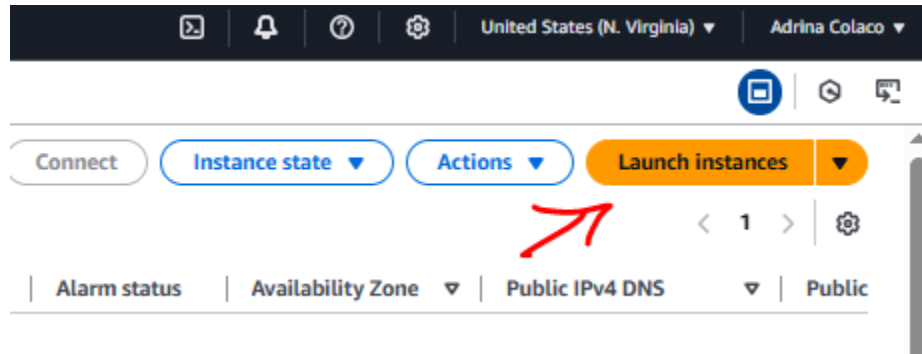
- a. The goal is to create two different EC2 instances belonging to the 2 respective subnets that we created earlier.
- b. Type “EC2” in the search bar and click on “EC2” in the search results.



- c. Goto “Instances” on the left panel.



- d. Click on “Launch instance” on the right corner.



- e. Enter the highlighted details in the Launch an instance page.

## Launch an instance [Info](#)

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 [Info](#)

Name

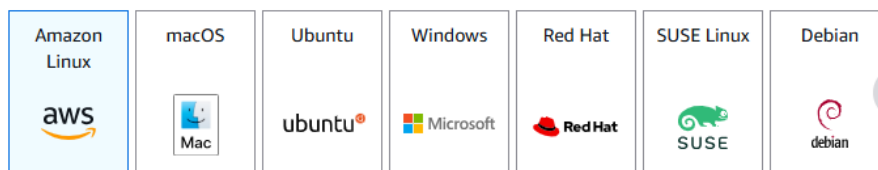
[Add additional tags](#)

### ▼ 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

Recents

Quick Start



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

### Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-00a929b66ed6e0de6 (64-bit (x86), uefi-preferred) / ami-05f417c208be02d4d (64-bit (Arm), uefi)

Virtualization: hvm    ENA enabled: true    Root device type: ebs

Free tier eligible

#### Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.7.20250331.0 x86\_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Publish Date	Username
64-bit (x86)	uefi-preferred	ami-00a929b66ed6e0de6	2025-03-29	ec2-user

Verified provider

### Instance type

t2.micro

Family: t2    1 vCPU    1 GiB Memory    Current generation: true

On-Demand Windows base pricing: 0.0162 USD per Hour

On-Demand Ubuntu Pro base pricing: 0.0134 USD per Hour

On-Demand SUSE base pricing: 0.0116 USD per Hour

On-Demand RHEL base pricing: 0.026 USD per Hour    On-Demand Linux base pricing: 0.0116 USD per Hour

Free tier eligible

☐ All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

f. Create a new Key Pair

### Key pair (login)

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*

Select

Create new key pair

g. Enter the highlighted fields and click on "Create key pair"

**Create key pair** ✕

**Key pair name**  
Key pairs allow you to connect to your instance securely.

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**

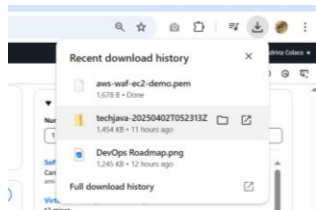
☒ **.pem**  
For use with OpenSSH

☐ **.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](#)

- h. The key pair will automatically be downloaded to your “Downloads” folder.



- i. The key pair will also attach to the EC2.

▼ **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**

[Create new key pair](#)

- j. Network setting:

- i. Edit and change the highlighted fields

1. VPC
2. Subnet (Select the respective subnet for each EC2 instance; we are creating 2 EC2 instances)
3. Change Auto-assign public IP to “Enable”

**▼ Network settings** [Info](#)

**VPC - required** | [Info](#)

vpc-0b08eefdf29412f43 (test-vpc)  
12.0.0.0/16

**Subnet** | [Info](#)

subnet-07a580b6685598764 test-public-subnet-1a  
VPC: vpc-0b08eefdf29412f43 Owner: 311141542113 Availability Zone: us-east-1a  
Zone type: Availability Zone IP addresses available: 251 CIDR: 12.0.1.0/24

**Auto-assign public IP** | [Info](#)

Enable

Additional charges apply when outside of free tier allowance

- ii. Create a Security Group and add the HTTP security group rule as highlighted below.

**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

**Security group name - required**

launch-wizard-3

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and \_-./!@#%&\*~:;[]^\_`{|}~

**Description - required** | [Info](#)

launch-wizard-3 created 2025-04-02T16:21:37.583Z

**Inbound Security Group Rules**

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0) [Remove](#)

<b>Type</b>   <a href="#">Info</a>	<b>Protocol</b>   <a href="#">Info</a>	<b>Port range</b>   <a href="#">Info</a>
ssh	TCP	22
<b>Source type</b>   <a href="#">Info</a>	<b>Source</b>   <a href="#">Info</a>	<b>Description - optional</b>   <a href="#">Info</a>
Anywhere	<input type="text" value="0.0.0.0/0"/> <a href="#">Add CIDR, prefix list or security group</a>	e.g. SSH for admin desktop

▼ Security group rule 2 (TCP, 80, 0.0.0.0/0) [Remove](#)

<b>Type</b>   <a href="#">Info</a>	<b>Protocol</b>   <a href="#">Info</a>	<b>Port range</b>   <a href="#">Info</a>
HTTP	TCP	80
<b>Source type</b>   <a href="#">Info</a>	<b>Source</b>   <a href="#">Info</a>	<b>Description - optional</b>   <a href="#">Info</a>
Anywhere	<input type="text" value="0.0.0.0/0"/> <a href="#">Add CIDR, prefix list or security group</a>	e.g. SSH for admin desktop

⚠ Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Add security group rule](#)

- k. Leave “Configure storage” and “Advanced details” as is.

▼ **Configure storage** [Info](#)

Advanced

1x  GiB  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

The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance

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

- l. Click on “Launch instance”. You will see the screen below.

Launch an instance | EC2 | us-east-1

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances:

aws  [Alt+S]

EC2 > Instances > Launch an instance

Launching instance

Creating security group rules

33%

Details

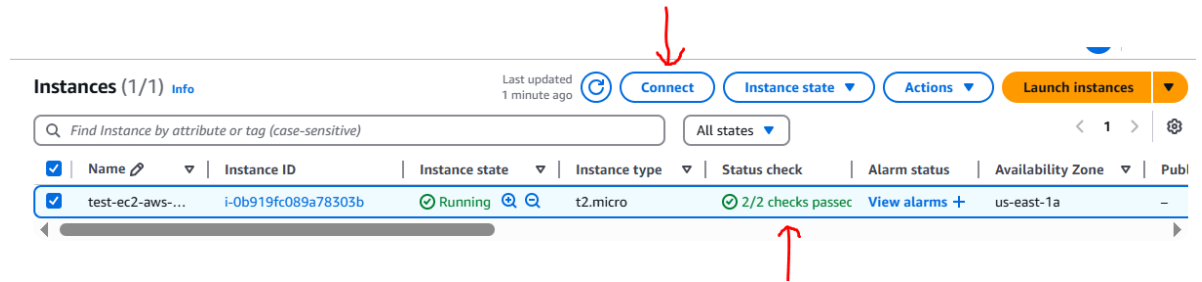
Please wait while we launch your instance.  
Do not close your browser while this is loading.

## 6. Installation of HTTPD service on EC2.

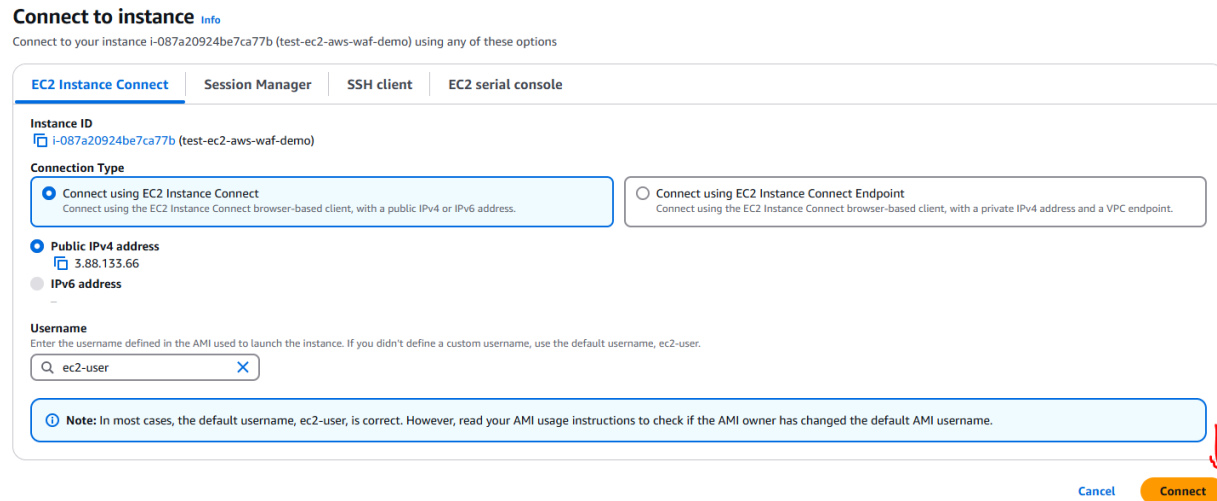
- a. Connect to the EC2 instance.



- b. Click on the check mark next to the EC2 instance. Make sure the Status Check is **GREEN**. Click on the “Connect” button.

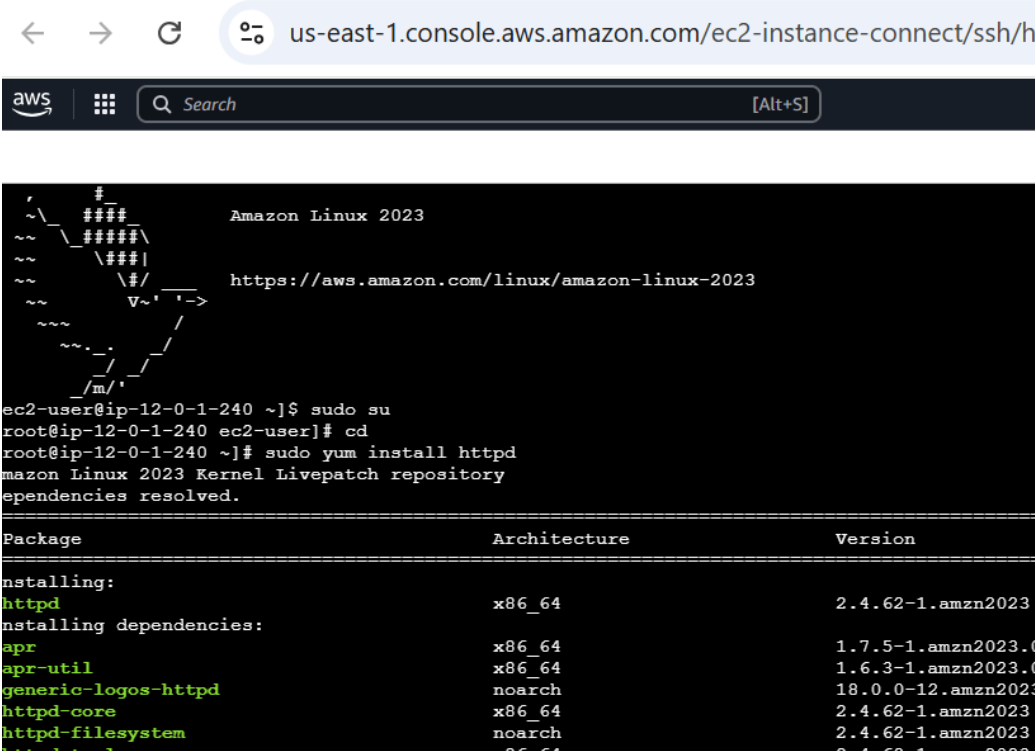


- c. Connect to the EC2 instance by clicking on “Connect.”



- d. Install, start, and enable the HTTPD service on EC2 using the below commands(One at a time).
- ```
sudo yum install httpd -y  
sudo systemctl enable httpd  
sudo systemctl status httpd  
sudo systemctl start httpd
```

sudo systemctl status httpd



The screenshot shows a terminal window within the AWS Management Console. The URL bar at the top indicates the session is connected to an EC2 instance via SSH. The terminal output shows the user logging in as 'ec2-user' on an 'ip-12-0-1-240' instance. They run 'sudo su' to become root, then 'cd' to move to the root directory. Next, they run 'sudo yum install httpd', which resolves dependencies. A table of packages to be installed is displayed:

| Package                  | Architecture | Version              |
|--------------------------|--------------|----------------------|
| Installing:              |              |                      |
| httpd                    | x86_64       | 2.4.62-1.amzn2023.0  |
| Installing dependencies: |              |                      |
| apr                      | x86_64       | 1.7.5-1.amzn2023.0   |
| apr-util                 | x86_64       | 1.6.3-1.amzn2023.0   |
| generic-logos-httpd      | noarch       | 18.0.0-12.amzn2023.0 |
| httpd-core               | x86_64       | 2.4.62-1.amzn2023.0  |
| httpd-filesystem         | noarch       | 2.4.62-1.amzn2023.0  |
| httpd-tools              | x86_64       | 2.4.62-1.amzn2023.0  |

- e. Create "index.html" in /var/www/html folder
  - i. Write the below command in the command CLI.  
cd /var/www/html  
Vim index.html

Write the bash code below in index.html and save it by pressing [ESC] → :wq  
[Press enter]

Replace Linux Server 1 with Linux Server 2 in the below code while creating this file on the second EC2 instance.

```
<!DOCTYPE html>
<html>
<body>

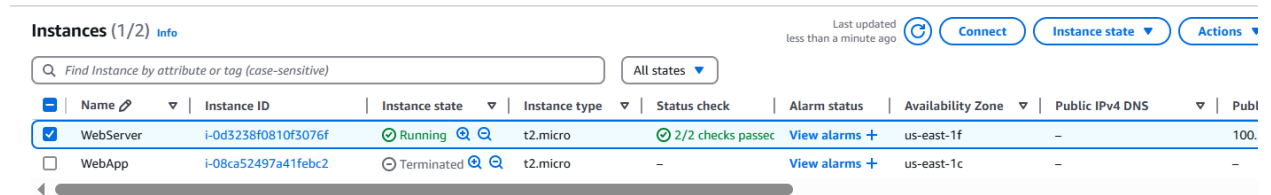
<h1>Hello World!</h1>
<p>You have reached Linux Server 1.</p>

</body>
</html>
```

## 7. Testing of EC2 instance

Copy the Public IPv4 address from the EC2 and place it in the browser to check if the website is displaying.

Use **http://**<IP address>



Instances (1/2) Info									
Last updated less than a minute ago									
Find Instance by attribute or tag (case-sensitive)									
All states									
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 address
<input checked="" type="checkbox"/>	WebServer	i-0d3238f0810f3076f	Running	t2.micro	2/2 checks passed	View alarms +	us-east-1f	-	100.28.128.34
<input type="checkbox"/>	WebApp	i-08ca52497a41febc2	Terminated	t2.micro	-	View alarms +	us-east-1c	-	-

### i-0d3238f0810f3076f (WebServer)

Details Status and alarms Monitoring Security Networking Storage Tags

#### Instance summary Info

Instance ID  
i-0d3238f0810f3076f

IPv6 address  
-

Public IPv4 address

100.28.128.34 | open address

Instance state

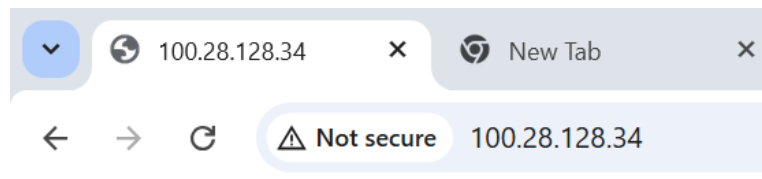
Running

Private IPv4 addresses

12.0.1.132

Public IPv4 DNS

-

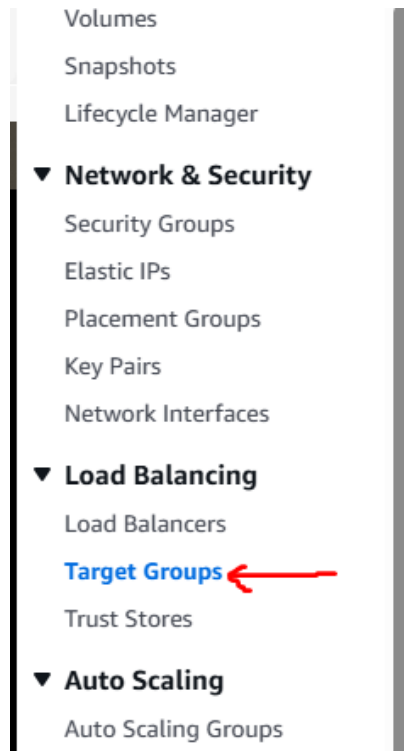


# Hello World!

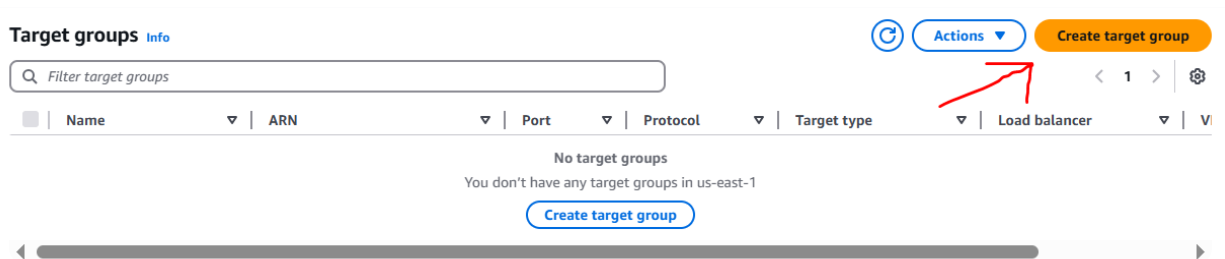
You have reached Linux Server 1.

## 8. Target Group

- a. Go to “Target groups” in the left pane.



- b. Click on “Create target group”



c. Enter details in the highlighted fields.

### Specify group details

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

#### Basic configuration

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

##### Choose a target type

☒ Instances

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

☐ IP addresses

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

☐ Lambda function

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

☐ Application Load Balancer

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

#### Target group name

tg-ec2-instances

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

#### Protocol : Port

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

HTTP

80

1-65535

#### IP address type

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

☒ IPv4

Each instance has a default network interface (eth0) that is assigned the primary private IPv4 address. The instance's primary private IPv4 address is the one that will be applied to the target.

☐ IPv6

Each instance you register must have an assigned primary IPv6 address. This is configured on the instance's default network interface (eth0). [Learn more](#)

#### VPC

Select the VPC with the instances that you want to include in the target group. Only VPCs that support the IP address type selected above are available in this list.

my-vpc

vpc-03ad40e7bb181aaf9  
IPv4 VPC CIDR: 12.0.0.0/16

#### Protocol version

☒ HTTP1

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

☐ HTTP2

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

☐ gRPC

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

### Health checks

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

**Health check protocol**

HTTP

**Health check path**

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

/

Up to 1024 characters allowed.

► **Advanced health check settings**

### Attributes

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

► **Tags - optional**

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

Cancel

Next

- d. Click on the checkbox, select the instance ID, and click “Include as pending below”.
- Then click on “Create target group.”

### Register targets

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

#### Available instances (1/1)

Filter instances

<input checked="" type="checkbox"/>	Instance ID	Name	State	Security groups	Zone
<input checked="" type="checkbox"/>	i-0d3238f0810f3076f	WebServer	Running	launch-wizard-4	us-east-1

1 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 (1)

Filter targets

Show only pending

Remove all pending

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID
i-0d3238f0810f3076f	WebServer	80	Running	launch-wizard-4	us-east-1f	12.0.1.132	subnet-0b0c2fd0150


1 pending


Cancel Previous Create target group






- e. Target group will be created.

**tg-ec2-instances** Actions ▾

**Details**


 [arn:aws:elasticloadbalancing:us-east-1:311141542113:targetgroup/tg-ec2-instances/4e958c423021205c](#)

<b>Target type</b> Instance	<b>Protocol : Port</b> HTTP: 80	<b>Protocol version</b> HTTP1	<b>VPC</b> <a href="#">vpc-03ad40e7bb181aaf9</a> 
<b>IP address type</b> IPv4	<b>Load balancer</b> <a href="#">None associated</a>		








1 Total targets	 0 Healthy 0 Anomalous	 0 Unhealthy	 1 Unused	 0 Initial	 0 Draining
--------------------	---------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------

► **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 (1)** [Info](#) [Anomaly mitigation: Not applicable](#)  Deregister Register targets

Target groups route requests to individual registered targets using the protocol and port number specified. Health checks are performed on all registered targets according to the target group's health check settings. Anomaly detection is automatically applied to HTTP/HTTPS target groups with at least 3 healthy targets.

 Instance ID	 Name	 Port	 Zone	 Health status	 Health status details	 Admini
-----------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------

## 9. Load balancer


- a. Click on “Load Balancers” on the left panel.

Placement Groups

Key Pairs

Network Interfaces

▼ **Load Balancing**

**Load Balancers** 

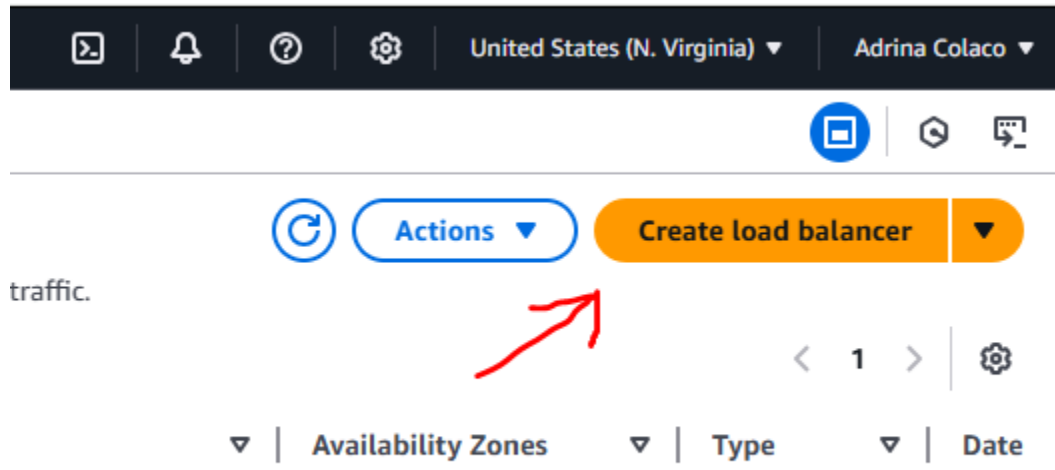
Target Groups

Trust Stores

▼ **Auto Scaling**

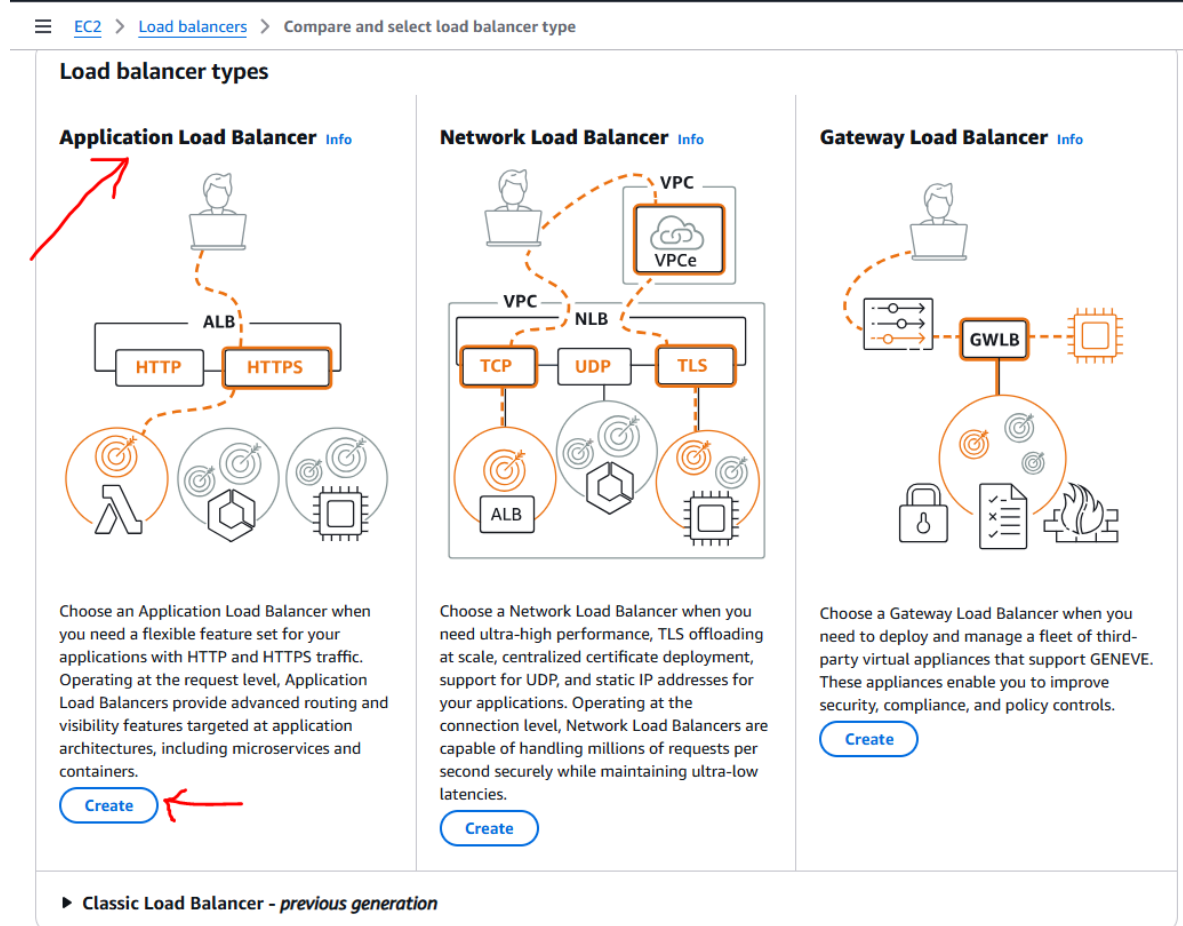
Auto Scaling Groups

- b. Click on “Create load balancer”



us-east-1

- c. Click on “Application Load Balancer”



- d. Enter details into the highlighted fields. Select the relevant VPC and at least two subnets.



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

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

### ► How Application Load Balancers work

#### Basic configuration

##### Load balancer name

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

lb-waf-demo

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

##### Scheme [Info](#)

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

##### ☒ Internet-facing

- Serves Internet-facing traffic.
- Has public IP addresses.
- DNS name is publicly resolvable.
- Requires a public subnet.

##### ☐ Internal

- Serves internal traffic.
- Has private IP addresses.
- DNS name is publicly resolvable.
- Compatible with the IPv4 and Dualstack IP address types.

##### Load balancer IP address type [Info](#)

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

##### ☒ IPv4

Includes only IPv4 addresses.

##### ☐ Dualstack

Includes IPv4 and IPv6 addresses.

##### ☐ Dualstack without public IPv4

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

#### Network mapping [Info](#)

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

##### VPC [Info](#)

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

my-vpc

vpc-03ad40e7bb181aa9  
IPv4 VPC CIDR: 12.0.0.0/16



##### IP pools - new [Info](#)

You can optionally choose to configure an IPAM pool as the preferred source for your load balancers IP addresses. Create or view [Pools in Amazon VPC IP Address Manager console](#).

##### ☐ Use IPAM pool for public IPv4 addresses

The IPAM pool you choose will be the preferred source of public IPv4 addresses. If the pool is depleted IPv4 addresses will be assigned by AWS.

##### Availability Zones and subnets [Info](#)

Select at least two Availability Zones and a subnet for each zone. A load balancer node will be placed in each selected zone and will automatically scale in response to traffic. The load balancer routes traffic to targets in the selected Availability Zones only.

##### ☒ us-east-1d (use1-az1)

###### Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-0d5c1eef5f4a55284

IPv4 subnet CIDR: 12.0.2.0/24

Public-Subnet



The selected subnet does not have a route to an internet gateway. This means that your load balancer will not receive internet traffic. You can proceed with this selection; however, for internet traffic to reach your load balancer, you must update the subnet's route table in the [VPC console](#).

##### ☒ us-east-1f (use1-az5)

###### Subnet

Only CIDR blocks corresponding to the load balancer IP address type are used. At least 8 available IP addresses are required for your load balancer to scale efficiently.

subnet-0b0c2fd01505ebbc7

IPv4 subnet CIDR: 12.0.1.0/24

Public-Subnet

- e. Create a security group for the load balancer and add the respective SSH and HTTP Inbound rules and click on “Create security group”.

#### 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, complete the fields below.

**Basic details**

**Security group name** [Info](#)  
  
Name cannot be edited after creation.

**Description** [Info](#)

**VPC** [Info](#)

**Inbound rules** [Info](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
SSH	TCP	22	Any... <input type="text" value="0.0.0.0/0"/>	<input type="text"/>	<a href="#">Delete</a>
HTTP	TCP	80	Any... <input type="text" value="0.0.0.0/0"/>	<input type="text"/>	<a href="#">Delete</a>

[Add rule](#)

**Outbound rules** [Info](#)

Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Destination <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
All traffic	All	All	Cust... <input type="text" value="0.0.0.0/0"/>	<input type="text"/>	<a href="#">Delete</a>

[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](#)

- f. Attach the security group to the load balancer.

**Security groups** [Info](#)

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

**Security groups**

default  
sg-00e4cf816bd525ec VPC: vpc-03ad40e7bb181aaf9

secgrp-aws-waf-demo-ssh-http  
sg-06ddf4f704a7c2c9d VPC: vpc-03ad40e7bb181aaf9

## g. Listeners and routing (Important)

**Listeners and routing** [Info](#)  
A listener is a process that checks for connection requests using the port and protocol you configure. The rules that you define for a listener determine how the load balancer routes requests to its registered targets.

▼ Listener HTTP:80

Protocol

Port

HTTP

:

80

1-65535

Default action

Forward to

tg-ec2-instances

HTTP

Target type: Instance, IPv4

Create target group

Remove

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

Add listener tag

You can add up to 50 more tags.

Add listener

## h. The rest of the details stay the same. Click on “Create load balancer”.

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

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

**Amazon CloudFront + AWS Web Application Firewall (WAF)** [new](#) [info](#)  
Optimizes: Performance, Availability, Security  
☐ Apply application layer acceleration and security protections - *in front of the load balancer*  
Automatically configures and creates a CloudFront distribution with the basic recommended AWS WAF security protections, and associates it to your load balancer. [Additional charges apply](#)

**Benefits and considerations**

**AWS Web Application Firewall (WAF)** [info](#)  
Optimizes: Security  
☐ Apply application layer security protections - *in front of targets*  
Your choice of either a pre-defined security configuration with basic recommended AWS WAF security protections, or associate any of your existing WAF configurations for custom protections. [Additional charges apply](#)

**Benefits and considerations**

**AWS Global Accelerator** [info](#)  
Optimizes: Performance, Availability  
☐ Apply global load balancing across multiple regions  
Creates an accelerator in your account with two global static IPs that act as a fixed entry point to your load balancer. If you do not need global static IPs or traffic management across multiple regions, select Amazon CloudFront. [Additional charges apply](#)

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

**Summary**  
Review and confirm your configurations. [Estimate cost](#)

**Basic configuration** [Edit](#)  
Name: lb-waf-demo  
Scheme: Internet-facing  
IP address type: IPv4

**Network mapping** [Edit](#)  
VPC: vpc-03ad40e7bb181aaf9  
Public IPv4 IPAM pool: -  
Availability Zones and subnets: -

**Service integrations** [Edit](#)  
Amazon CloudFront + AWS Web Application Firewall (WAF): -  
AWS WAF: -  
AWS Global Accelerator: -

**Security groups** [Edit](#)  
default  
sg-00e4c6f816bd525ec  
secgrp-aws-waf-demo-ssh-http  
sg-06d9f4f704a7c2c9d

**Listeners and routing** [Edit](#)  
HTTP:80 | Target group: tg-ec2-instances

**Tags** [Edit](#)  
-

**Attributes**  

Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.

**Creation workflow and status**

**Server-side tasks and status**  
After completing and submitting the above steps, all server-side tasks and their statuses become available for monitoring.

Cancel

Create load balancer

- i. Load Balancer created.

**Successfully created load balancer: lb-waf-demo**  
It might take a few minutes for your load balancer to fully set up and route traffic. Targets will also take a few minutes to complete the registration process and pass initial health checks.

**lb-waf-demo** **Actions**

**▼ Details**

<b>Load balancer type</b> Application	<b>Status</b> Provisioning	<b>VPC</b> <a href="#">vpc-03ad40e7bb181aaf9</a>	<b>Load balancer IP address type</b> IPv4
<b>Scheme</b> Internet-facing	<b>Hosted zone</b> Z35SXDOTRQ7X7K	<b>Availability Zones</b> <a href="#">subnet-0d5c1eef5f4a55284</a> us-east-1d (use1-az1) <a href="#">subnet-0b0c2fd01505ebbc7</a> us-east-1f (use1-az5)	<b>Date created</b> April 4, 2025, 17:48 (UTC+05:30)
<b>Load balancer ARN</b> <a href="#">arn:aws:elasticloadbalancing:us-east-1:311141542113:loadbalancer/app/lb-waf-demo/e494e938079ce4b7</a>		<b>DNS name Info</b> <a href="#">lb-waf-demo-1628904794.us-east-1.elb.amazonaws.com</a> (A Record)	

## 10. Evaluate the load balancer DNS.

- a. Copy the DNS name and open it in a browser(Use HTTP)

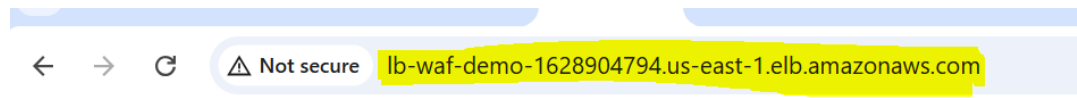
**Successfully created load balancer: lb-waf-demo**  
It might take a few minutes for your load balancer to fully set up and route traffic. Targets will also take a few minutes to complete the registration process and pass initial health checks.

**lb-waf-demo** **Actions**

**▼ Details**

<b>Load balancer type</b> Application	<b>Status</b> Provisioning	<b>VPC</b> <a href="#">vpc-03ad40e7bb181aaf9</a>	<b>Load balancer IP address type</b> IPv4
<b>Scheme</b> Internet-facing	<b>Hosted zone</b> Z35SXDOTRQ7X7K	<b>Availability Zones</b> <a href="#">subnet-0d5c1eef5f4a55284</a> us-east-1d (use1-az1) <a href="#">subnet-0b0c2fd01505ebbc7</a> us-east-1f (use1-az5)	<b>Date created</b> April 4, 2025, 17:48 (UTC+05:30)
<b>Load balancer ARN</b> <a href="#">arn:aws:elasticloadbalancing:us-east-1:311141542113:loadbalancer/app/lb-waf-demo/e494e938079ce4b7</a>		<b>DNS name Info</b> <a href="#">lb-waf-demo-1628904794.us-east-1.elb.amazonaws.com</a> (A Record)	

- b. The web browser should show a result from one of the EC2s like below screenshot.

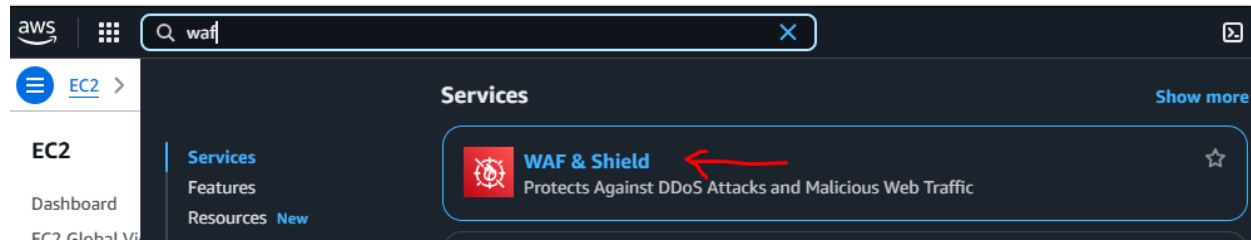


# Hello World!

You have reached **Linux Server 1.**

## 11. AWS WAF

- a. Type WAF in the search bar.



- b. Make sure you select the correct region.

**Web ACL details**

**Resource type**  
Choose the type of resource to associate with this web ACL. Changing this setting will reset the page.

☐ Global resources (CloudFront Distributions and AWS Amplify Applications)

☒ Regional resources (Application Load Balancers, Amazon API Gateway REST APIs, Amazon App Runner services, AWS AppSync APIs, Amazon Cognito user pools and AWS Verified Access Instances)

**Region**  
Choose the AWS Region to create this web ACL in. Changing this setting will reset the page.

US East (N. Virginia) ▼

**Name**

waf-demo

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and \_ (underscore).

**Description - optional**

The description can have 1-256 characters.

**CloudWatch metric name**

waf-demo

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and \_ (underscore).

- c. Attach Load Balancer by clicking on “Add AWS resources”

**Associated AWS resources - optional (0)**

Remove

Add AWS resources

<

1

>

⚙

Name	Resource type	Region
<div>No items</div> <div>No items to display</div>		

Cancel

Next

Add AWS resources

×

Resource type

Select the resource type and then select the resource you want to associate with this web ACL.

☒ Application Load Balancer

☐ Amazon API Gateway REST API

☐ Amazon App Runner service

☐ AWS AppSync API

☐ Amazon Cognito user pool

☐ AWS Verified Access

Resources (1)

⌂

Select the resource you want to associate with the web ACL.

<

1

>

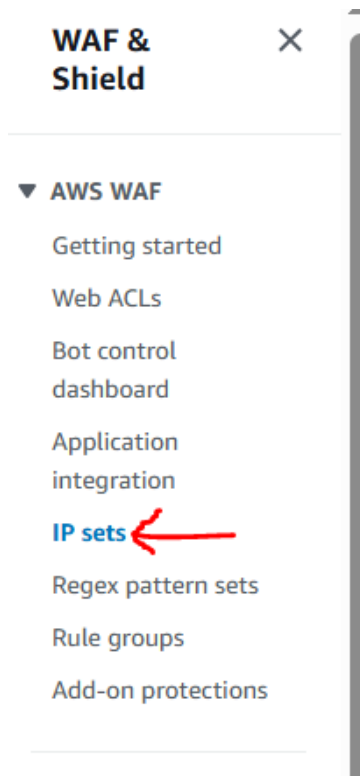
⚙

<input checked="" type="checkbox"/>	Name
<input checked="" type="checkbox"/>	lb-waf-demo

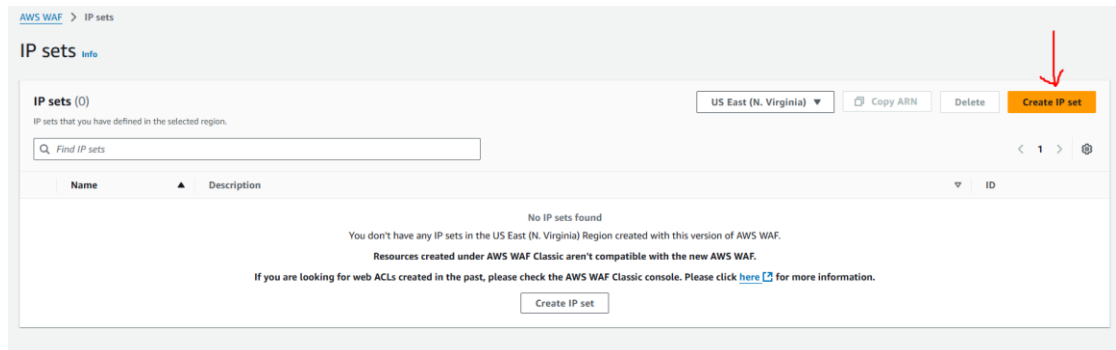
Cancel

Add

d. Next step is to add rules, but before doing this create IP sets.  
Go to left panel and open IP sets in a **new TAB**



- e. Click on the “Create IP set” button.



- f. Add the IP you want to BLOCK. Do not forget to add the range as highlighted. Click on “Create IP set”.

## Create IP set [Info](#)

An IP set is a collection of IP addresses.

### IP set details

#### IP set name

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and \_ (underscore).

#### Description - *optional*

The description can have 1-256 characters.

#### Region

Choose the AWS region to create this IP set in.

#### IP version

☒ IPv4☐ IPv6

#### IP addresses



Enter one IP address per line in CIDR format.

[Cancel](#)[Create IP set](#)

- g. Time to add rules.  
Go back to the Add rules and rule groups page.  
Click on “add rules” drop down.



Select “Add my own rules and rule groups”

## Add rules and rule groups [Info](#)

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

**Rules (0)**

EditDeleteAdd rules ▲

Add managed rule groups

Add my own rules and rule groups

<input type="checkbox"/>	Name	Capacity	...
No rules. You don't have any rules added.			

h. Enter the highlighted details. Click on “add rule”.

## Add my own rules and rule groups [Info](#)

### Rule type

#### Rule type

☒ **IP set**

Use IP sets to identify a specific list of IP addresses.

☐ **Rule builder**

Use a custom rule to inspect for patterns including query strings, headers, countries, and rate limit violations.

☐ **Rule group**

Use a rule group to combine rules into a single logical set.

### Rule

#### Name

BlockmyLaptop

### IP set

#### IP set

MyLaptopIP

#### IP address to use as the originating address

When a request comes through a CDN or other proxy network, the source IP address identifies the proxy and the original IP address is sent in a header. Use caution with the option, IP address in header, because headers can be handled inconsistently by proxies and they can be modified to bypass inspection.

☒ **Source IP address**

☐ IP address in header

#### Action

Choose an action to take when a request originates from one of the IP addresses in this IP set.

☐ Allow

☒ **Block**

☐ Count

☐ CAPTCHA customize [↗](#)

☐ Challenge

► Custom response - optional

Cancel

Add rule

- i. Check the newly created rule. Click on “Next”.

## Add rules and rule groups Info

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (1/1)

EditDeleteAdd rules ▼

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

<input checked="" type="checkbox"/>	Name	Capacity	Action
<input checked="" type="checkbox"/>	BlockmyLaptop	1	Block

### Web ACL capacity units (WCUs) used by your web ACL

The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.

The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs. [AWS WAF Pricing](#)

1/5000 WCUs

### Default web ACL action for requests that don't match any rules

Default action

☒ Allow

☐ Block

► Custom request - *optional*

### Token domain list - *optional*

Enable the use of tokens across multiple protected applications by entering the application domains here. Tokens are used by the Challenge and CAPTCHA rule actions, the application integration SDKs, and the ATP and Bot Control managed rule groups. [Learn more](#)

Add token domain

You can add 10 more domains

CancelPreviousNext

- j. Set rule priority. Click on “Next”

## Set rule priority [Info](#)

### Rules (1/1)

[▲ Move up](#)[▼ Move down](#)

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

	Name	Capacity	Action
<input checked="" type="radio"/>	BlockmyLaptop	1	Block

[Cancel](#)[Previous](#)[Next](#)

- k. Leave “Configure metrics” as is.

## Configure metrics [Info](#)

### Amazon CloudWatch metrics

CloudWatch metrics allow you to monitor web requests, web ACLs, and rules.

Rules

CloudWatch metric name

☒ BlockmyLaptop

BlockmyLaptop

### Request sampling options

If you disable request sampling, you can't view requests that match your web ACL rules.

Options

- ☒ Enable sampled requests  
☐ Disable sampled requests  
☐ Enable sampled requests with exclusions

[Cancel](#)[Previous](#)[Next](#)

- l. Leave “Review and create web ACL” as is and click on “Create web ACL”

# Review and create web ACL [Info](#)

## Step 1: Describe web ACL and associate it to AWS resources

Edit step 1

Web ACL details

Name	Scope
waf-demo	REGIONAL
Description	Region
	us-east-1
CloudWatch metric name	
waf-demo	

## Steps 2 and 3: Add rules and set rule priority

Edit steps 2 and 3


Rules (1)

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

Name	Capacity	Action
BlockmyLaptop	1	Block

Web ACL capacity units (WCUs) used by your web ACL

The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.

The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs. [AWS WAF Pricing](#) 

1/5000 WCUs

Default web ACL action for requests that don't match any rules

Action	Custom request headers
Allow	-

Token domain list (0)

Name
No items No items to display

Step 4: Configure metrics

Edit step 4

Amazon CloudWatch metrics (1)

Rules	CloudWatch metric name
BlockmyLaptop	BlockmyLaptop

Sampled requests

Sampled requests for web ACL default actions

Enabled

Cancel

Previous

Create web ACL

m. Web ACL should be successfully created.

Success

You successfully created the web ACL waf-demo.

[AWS WAF](#) > Web ACLs

Web ACLs [Info](#)

Web ACLs (1)

US East (N. Virginia) Delete Create web ACL

Web ACLs that you have defined in the selected region.

Find web ACLs

Name	Description	ARN	ID
waf-demo	-	arn:aws:wafv2:us-east-1:311141542113:regional/w...	68f8e2ea-b39c-4817-be26-609c20d8f5df

## 12. Evaluate the load balancer DNS again.

- a. Copy the DNS name and open it in a browser(Use HTTP)

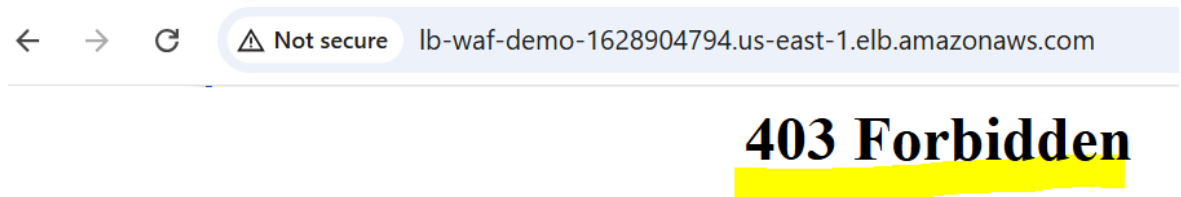
✔ Successfully created load balancer: **lb-waf-demo**  
It might take a few minutes for your load balancer to fully set up and route traffic. Targets will also take a few minutes to complete the registration process and pass initial health checks.

**lb-waf-demo** Actions

▼ Details

Load balancer type Application	Status ⏸ Provisioning	VPC <a href="#">vpc-03ad40e7bb181aaf9</a>	Load balancer IP address type IPv4
Scheme Internet-facing	Hosted zone Z35SXDOTRQ7X7K	Availability Zones <a href="#">subnet-0d5c1eef5f4a55284</a> us-east-1d (use1-az1) <a href="#">subnet-0b0c2fd01505ebbc7</a> us-east-1f (use1-az5)	Date created April 4, 2025, 17:48 (UTC+05:30)
Load balancer ARN <a href="#">arn:aws:elasticloadbalancing:us-east-1:311141542113:loadbalancer/app/lb-waf-demo/e494e938079ce4b7</a>		DNS name info <a href="#">lb-waf-demo-1628904794.us-east-1.elb.amazonaws.com</a> (A Record)	

- b. The web browser should show “403 Forbidden” error like the screenshot below.



## 13. WAF Testing Complete.

- a. Similarly, you can allow IP addresses, set up CAPTCHA, calculate the count of requests or set up challenges in the rules.

## 14. Try it yourself!

Change the rule in WAF to CAPTCHA and see what happens.

## AWS SERVICES USED

- AWS VPC
- AWS EC2
- AWS WAF