

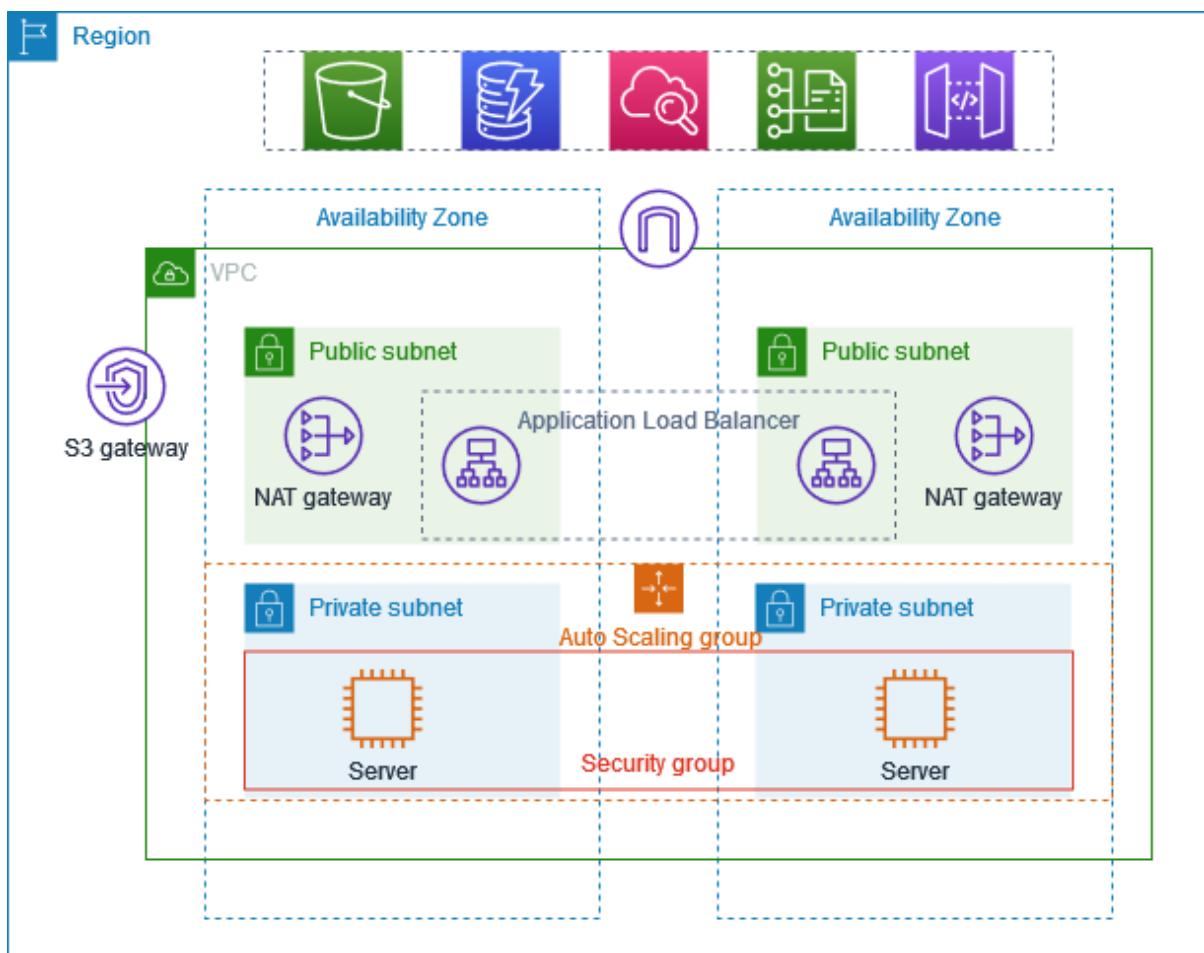
Secure VPC Architecture with Public and Private Subnets for Production Environment

Overview :

This project's overview is depicted in the diagram below. The setup revolves around a Virtual Private Cloud (VPC) featuring both public and private subnets, thoughtfully distributed across two Availability Zones to ensure reliability.

Within each public subnet, there's a NAT gateway to facilitate outbound internet connectivity and a load balancer node for effective traffic distribution.

On the other hand, the project's servers reside in the private subnets. Their deployment and termination are automated through an Auto Scaling group, allowing them to dynamically adapt to workload changes. These servers play a pivotal role in receiving traffic from the load balancer and can access the internet through the NAT gateway when necessary



Steps :

Step 1 :

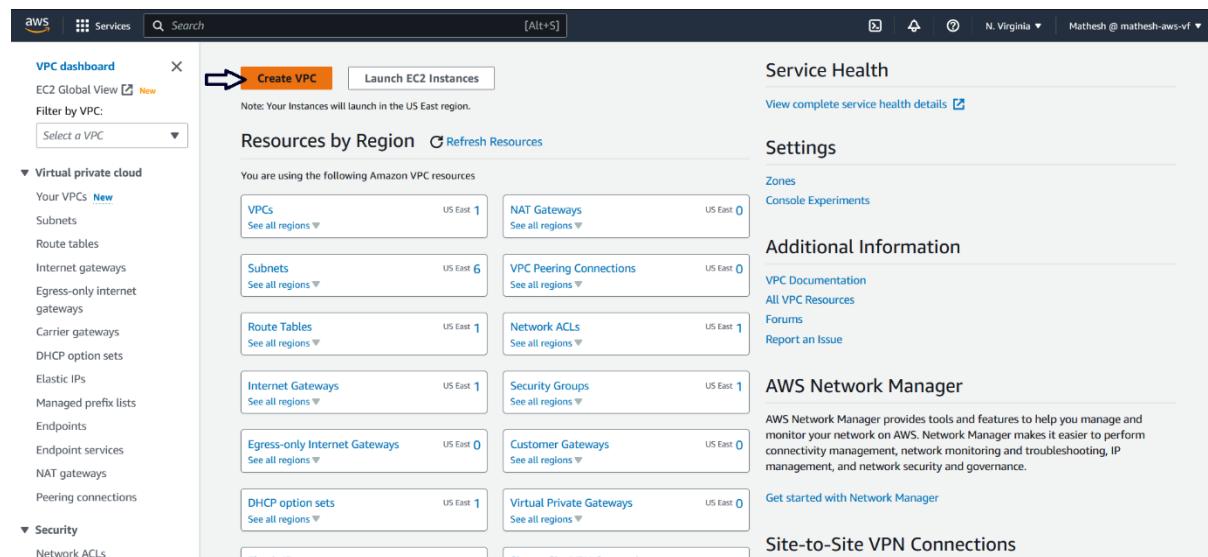
Create the VPC :

1. Open the Amazon VPC console by visiting <https://console.aws.amazon.com/vpc/>.
2. On the dashboard, click on "Create VPC."
3. Under "Resources to create," select "VPC and more."

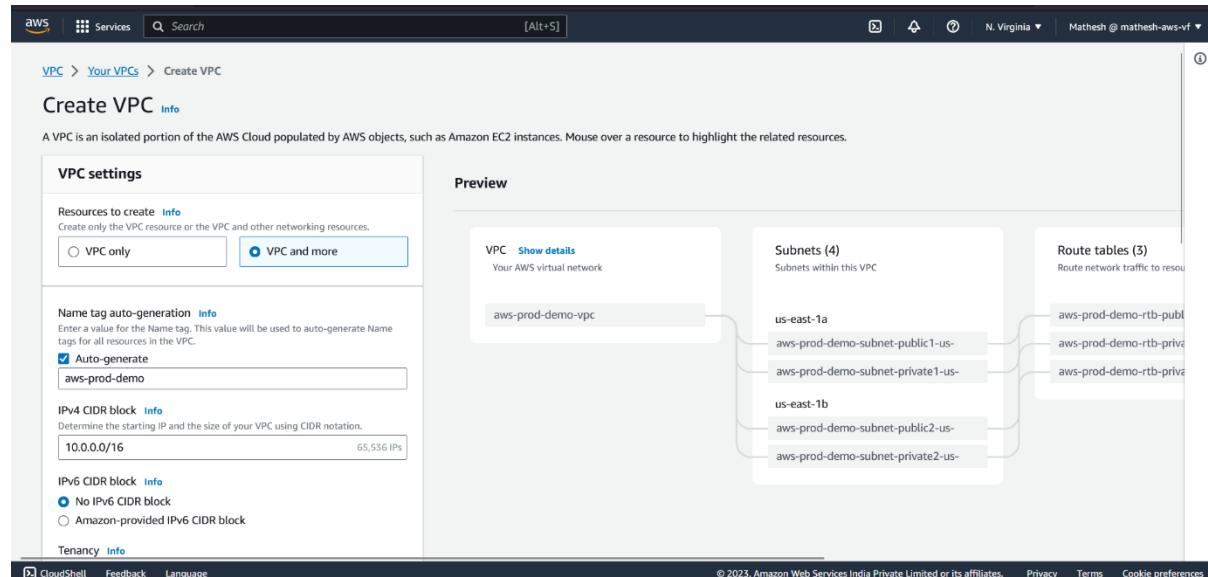
4. Configure the VPC:
 - a. Provide a name for the VPC in the "Name tag auto-generation" field.
 - b. For the IPv4 CIDR block, leave it as default suggestion.

5. Configure the subnets:
 - a. Set the "Number of Availability Zones" to 2 for increased resiliency across multiple Availability Zones.
 - b. Specify the "Number of public subnets" as 2.
 - c. Specify the "Number of private subnets" as 2.
 - d. For NAT gateways, choose "1 per AZ" to enhance resiliency.
 - e. For VPC endpoints, you can choose "None".
 - f. Regarding DNS options, clear the checkbox for "Enable DNS hostnames."

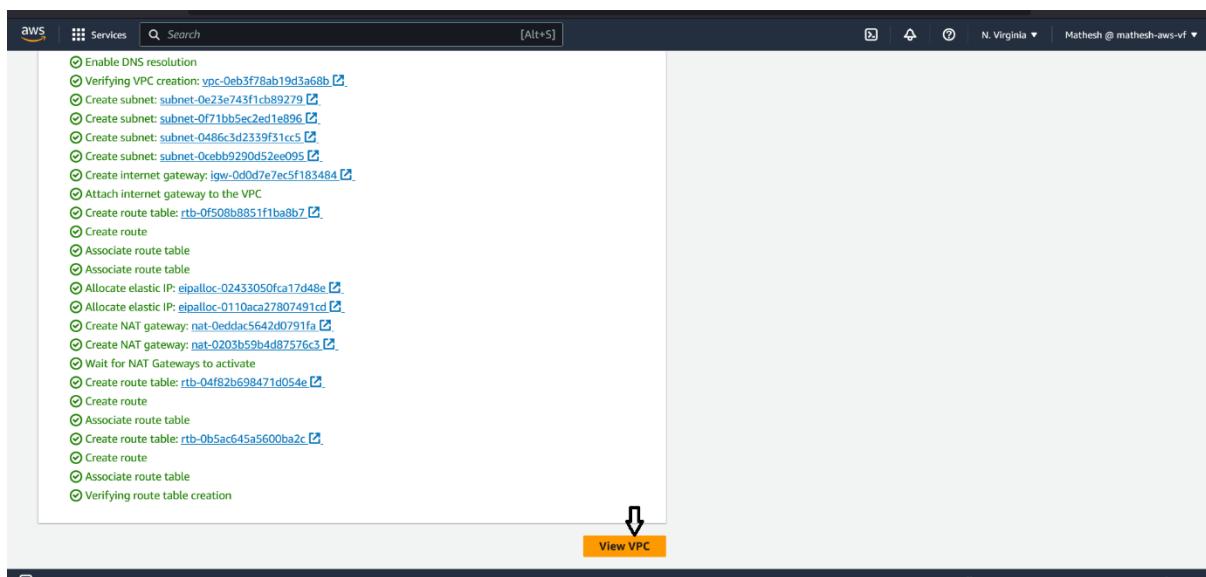
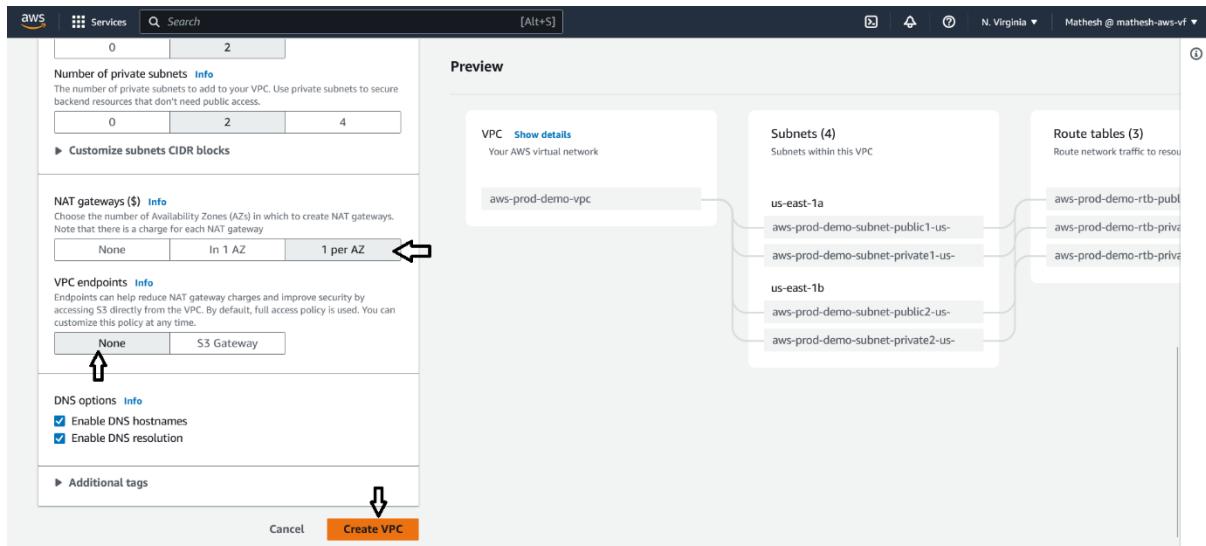
Once you've configured all the settings, click "Create VPC."



The screenshot shows the AWS VPC dashboard. On the left, there's a sidebar with various VPC-related options like Subnets, Route tables, Internet gateways, and Security. The main area has a heading 'Resources by Region' with several boxes showing counts for different services: VPCs (1), Subnets (6), Route Tables (1), Internet Gateways (1), DHCP option sets (1), and Network ACLs (1). To the right, there are sections for Service Health, Settings (with Zones and Console Experiments), Additional Information (with links to documentation and forums), and AWS Network Manager (with a brief description and a 'Get started with Network Manager' link). At the bottom, there's a 'Site-to-Site VPN Connections' section.



The screenshot shows the 'Create VPC' configuration page. In the 'VPC settings' tab, under 'Resources to create', 'VPC and more' is selected. Under 'Name tag auto-generation', 'Auto-generate' is checked, and the name 'aws-prod-demo' is entered. Under 'IPv4 CIDR block', the range '10.0.0.0/16' is specified, which results in '65,536 IPs'. Under 'IPv6 CIDR block', 'No IPv6 CIDR block' is selected. Under 'Tenancy', both options are available. On the right, there's a 'Preview' section showing a hierarchical tree of resources: a VPC named 'aws-prod-demo-vpc' containing four subnets ('us-east-1a' and 'us-east-1b') each with two route tables ('aws-prod-demo-rtb-public' and 'aws-prod-demo-rtb-private'). The footer includes links for CloudShell, Feedback, Language, and cookie preferences.



6. Now you can see you are successfully Created VPC .

Step 2:

Creating the Auto Scaling Group :

Amazon EC2 Auto Scaling
helps maintain the availability of your applications

Auto Scaling groups are collections of Amazon EC2 instances that enable automatic scaling and fleet management features. These features help you maintain the health and availability of your applications.

How it works

Pricing

Amazon EC2 Auto Scaling features have no additional fees beyond the service fees for Amazon EC2, CloudWatch (for scaling policies), and the other AWS resources that you use. Visit the pricing page of each service to learn more.

Getting started

Create Auto Scaling group

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group.

Name

Auto Scaling group name
Enter a name to identify the group.
Must be unique to this account in the current Region and no more than 255 characters.

Launch template

For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.

Create a launch template

<https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#CreateTemplate:autoScalingGuidance=True>

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
aws-prod-template
Must be unique to this account. Max 128 chars. No spaces or special characters like '%', "'", '@'.

Template version description
Demo Prod Template
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

Summary

- Software Image (AMI)**
- Virtual server type (instance type)**
- Firewall (security group)**
- Storage (volumes)**

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 IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Create launch template

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) - required

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 Enterprise Server

Browse more AMIs

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

ami-053b0d53c279acc90 (64-bit (x86)) / ami-0a0e3eebcccc6cd0 (64-bit (Arm))

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

Free tier eligible

Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-05-16

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Summary

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...[read more](#)
ami-053b0d53c279acc90

Virtual server type (instance type)
-

Firewall (security group)
-

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

① 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 GiB of snapshots, and 100 GiB of bandwidth to the internet.

Cancel Create launch template

Instance type

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 SUSE base pricing: 0.0116 USD per Hour

On-Demand RHEL base pricing: 0.0116 USD per Hour

On-Demand Linux base pricing: 0.0116 USD per Hour

Additional costs apply for AMIs with pre-installed software

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: Don't include in launch template

Create new key pair

Network settings

Subnet info

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Summary

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...[read more](#)
ami-053b0d53c279acc90

Virtual server type (instance type)
t2.micro

Firewall (security group)
-

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

① 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 GiB of snapshots, and 100 GiB of bandwidth to the internet.

Cancel Create launch template

Instance type

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 SUSE base pricing: 0.0116 USD per Hour

On-Demand RHEL base pricing: 0.0116 USD per Hour

On-Demand Linux base pricing: 0.0116 USD per Hour

Additional costs apply for AMIs with pre-installed software

Create key pair

Key pair name: aws demo

Key pairs allow you to connect to your instance securely.

Key pair type: RSA

RSA RSA encrypted private and public key pair

ED25519 ED25519 encrypted private and public key pair

Private key file format: .pem

.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](#)

Create key pair

- Now you have to choose the Key-pair you created.

aws Services Search [Alt+S]

Network settings

Subnet Info
Don't include in launch 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

Security group name - required
aws-prod-sg
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
Allow SSH Access

VPC - required
vpc-0ebf78ab19d3a68b (aws-prod-demo-vpc) 10.0.0.0/16

Inbound Security Group Rules
No security group rules are currently included in this template. Add a new rule to include it in the launch template.

Summary

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...[read more](#)
ami-053b0d53c279acc90

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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 IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Inbound Security Group Rules

Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type	Protocol	Port range
ssh	TCP	22

Source type Custom e.g. SSH for admin desktop
0.0.0.0/0

Security group rule 2 (TCP, 8000, 0.0.0.0/0)

Type	Protocol	Port range
Custom TCP	TCP	8000

Source type Custom e.g. SSH for admin desktop
0.0.0.0/0

⚠️ 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.

Summary

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...[read more](#)
ami-053b0d53c279acc90

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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 IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

EBS Volumes

Volume 1 (AMI Root) (8 GiB, EBS, General purpose SSD (gp2))
AMI Volumes are not included in the template unless modified

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

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

Resource tags
No resource tags are currently included in this template. Add a resource tag to include it in the launch template.

You can add up to 50 more tags.

Advanced details

Summary

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...[read more](#)
ami-053b0d53c279acc90

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

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 IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS Auto Scaling Groups 'Create Auto Scaling group' wizard. The current step is 'Step 1: Choose launch template'. On the left, a sidebar lists steps from 1 to 7. Step 1 is 'Choose launch template', which is highlighted in blue. The main content area is titled 'Choose launch template' with a 'Info' link. It instructs the user to specify a launch template for common settings across EC2 instances. A 'Name' input field contains 'aws-prod-asg'. Below it, a note states: 'For accounts created after May 31, 2023, the EC2 console only supports creating Auto Scaling groups with launch templates. Creating Auto Scaling groups with launch configurations is not recommended but still available via the CLI and API until December 31, 2023.' A 'Launch template' dropdown menu shows 'aws-prod-template'.

2. Scroll Down and then Click "Next".

The screenshot shows the AWS Auto Scaling Groups 'Create Auto Scaling group' wizard. The current step is 'Step 2: Choose instance launch options'. The sidebar shows steps 2 through 7. Step 2 is 'Choose instance launch options', which is highlighted in blue. The main content area is titled 'Network' with an 'Info' link. It explains that multiple Availability Zones can be used to balance instances. A 'VPC' dropdown menu shows 'vpc-0eb3f78ab19d3a68b (aws-prod-demo-vpc)'. Below it, 'Availability Zones and subnets' are listed: 'us-east-1a | subnet-0486c3d2339f31cc5 (aws-prod-demo-subnet-private1-us-east-1a)' and 'us-east-1b | subnet-0cebb9290d52ee095 (aws-prod-demo-subnet-private2-us-east-1b)'. A 'Create a subnet' button is visible at the bottom of the subnet list.

3. Scroll Down and then Click "Next".

The screenshot shows the AWS Auto Scaling 'Create Auto Scaling group' wizard at Step 3: Configure advanced options - optional. The left sidebar lists steps 1 through 7. The main content area has two sections:

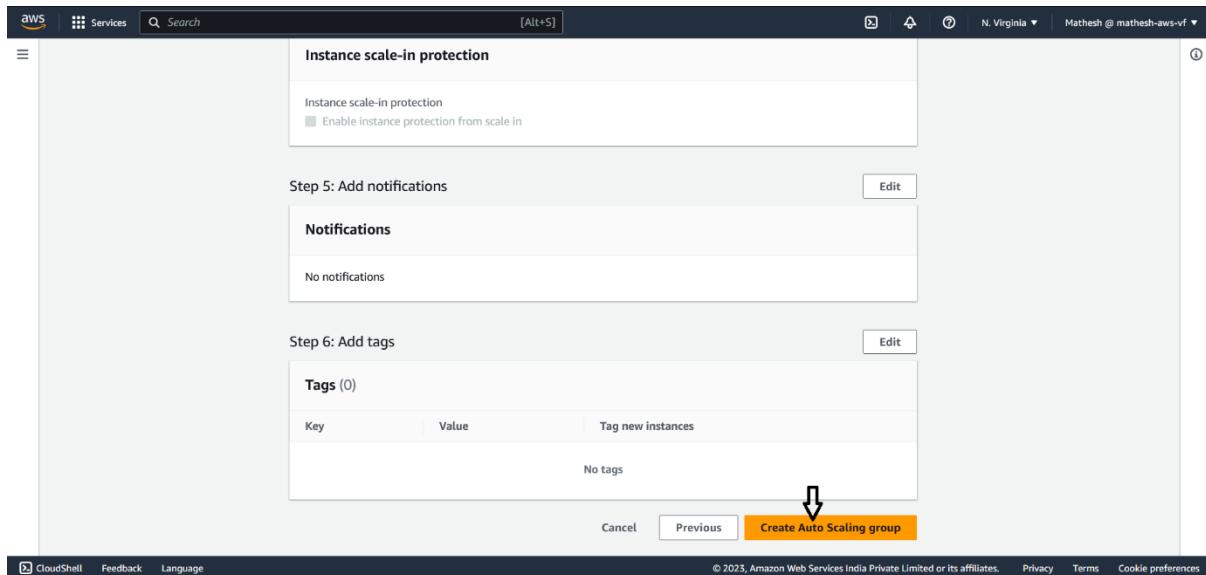
- Load balancing**: A section titled "Configure advanced options - optional" with the sub-section "Load balancing". It contains three options:
 - No load balancer: Traffic to your Auto Scaling group will not be fronted by a load balancer.
 - Attach to an existing load balancer: Choose from your existing load balancers.
 - Attach to a new load balancer: Quickly create a basic load balancer to attach to your Auto Scaling group.
- VPC Lattice integration options**: A section titled "Configure advanced options - optional" with the sub-section "VPC Lattice integration options". It contains two options:
 - No VPC Lattice service: VPC Lattice will not manage your Auto Scaling group's
 - Attach to VPC Lattice service: Incoming requests associated with specified VPC Lattice

4. Scroll Down and then Click "Next".

The screenshot shows the AWS Auto Scaling 'Create Auto Scaling group' wizard at Step 4: Configure advanced options. The left sidebar lists steps 1 through 7. The main content area has two sections:

- Group size - optional**: A section titled "Configure advanced options - optional" with the sub-section "Group size - optional". It contains three input fields for capacity:
 - Desired capacity: 2
 - Minimum capacity: 1
 - Maximum capacity: 4
- Scaling policies - optional**: A section titled "Configure advanced options - optional" with the sub-section "Scaling policies - optional". It contains two options:
 - 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

5. Scroll Down and then Click "Skip to Review".

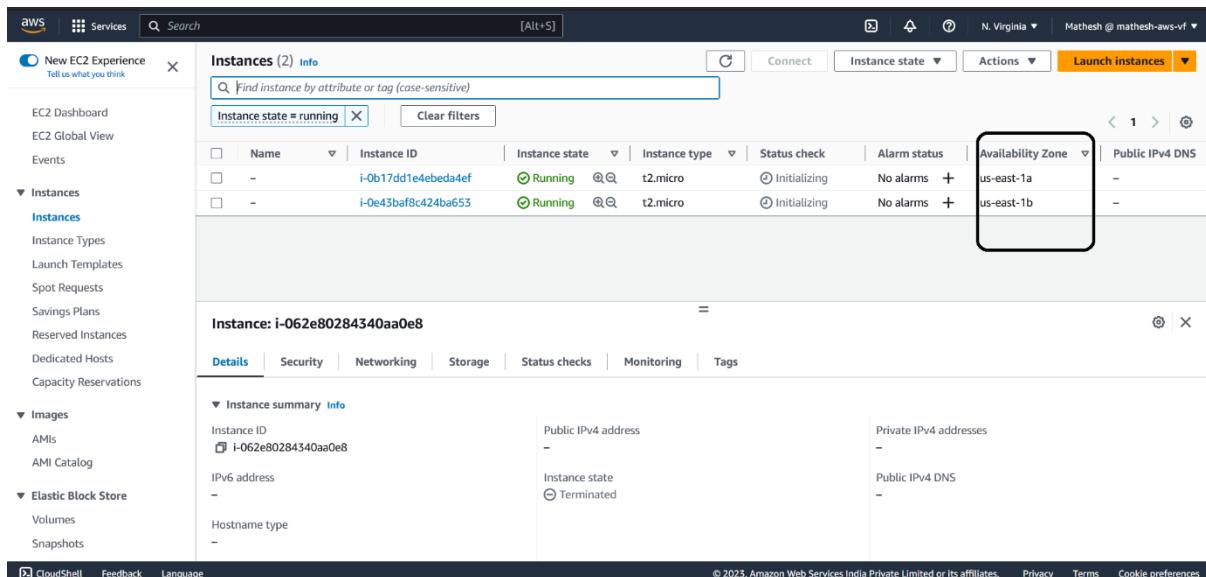


6. Now you are Successfully Created Auto Scaling Group.
 7. Open the AWS Management Console.
 8. Navigate to the EC2 console by clicking on "Services" in the top-left corner, then selecting "EC2" under the "Compute" section.
 9. In the EC2 dashboard, you'll find the "Instances" link on the left-hand navigation pane. Click on "Instances."
 10. Here, you should see the list of EC2 instances associated with your account. Look for the instances created by your Auto Scaling Group.
- Since you mentioned that the Auto Scaling Group launched instances in different AZs, you can check the "Availability Zone" column to verify that these instances are indeed distributed across multiple AZs.

Step 3 :

Creating the Bastion Host :

1. Launch Instance as Specified below .



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: Bastion_host

Application and OS Images (Amazon Machine Image)

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

Recents Quick Start

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...read more
ami-053b0d53c279acc90

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

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. [Learn More](#)

Cancel Launch instance Review commands

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Instance type

64-bit (x86) ami-053b0d53c279acc90 Verified provider

Key pair (login)

Key pair name - required aws demo

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...read more
ami-053b0d53c279acc90

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

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. [Learn More](#)

Cancel Launch instance Review commands

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Network settings

VPC - required

vpc-0eb3f78ab19d3a68b (aws-prod-demo-vpc) 10.0.0.0/16

Subnet

subnet-0f71b5ec2ed1e896 aws-prod-demo-subnet-public2-us-east-1b VPC: vpc-0eb3f78ab19d3a68b Owner: 804937851364 Availability Zone: us-east-1b IP addresses available: 4090 CIDR: 10.0.16.0/20

Auto-assign public IP

Enable

Firewall (security groups)

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-1

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

launch-wizard-1 created 2023-09-07T15:09:57.668Z

Inbound Security Group Rules

Software Image (AMI)

Canonical, Ubuntu, 22.04 LTS, ...read more
ami-053b0d53c279acc90

Virtual server type (instance type)

t2.micro

Firewall (security group)

New security group

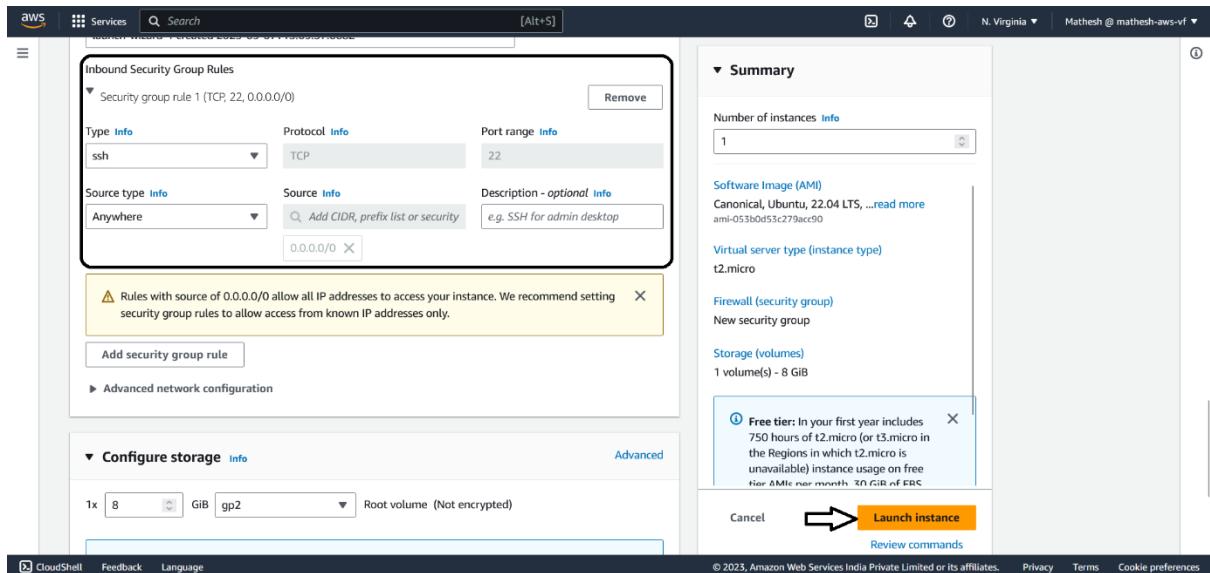
Storage (volumes)

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. [Learn More](#)

Cancel Launch instance Review commands

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences



Step 4:

SSH into Private Instance

1. SSH into the Bastion Host Instance: To SSH into the private instances, we first need to connect to our Bastion host instance. From there, we'll be able to SSH into the private instance.
2. Ensure the PEM File is Present on the Bastion Host: Additionally, make sure that the PEM file is present on the Bastion host. Without it, you won't be able to SSH into the private instance from the Bastion host.
3. Open a Terminal: Open a terminal window on your local machine.
4. Execute the Following Commands: a. If your PEM file is named something like <aws demo.pem>, you must remove spaces in the filename. Please rename the file to something like <aws_demo.pem>. b. Copy the PEM file to the Bastion host using the scp command. Replace <pem file location> with the local and remote file paths, and <bastion host public IP> with the Bastion host's public IP address. Example:


```
scp -i /Users/mathesh/Downloads/aws_demo.pem /Users/mathesh/Downloads/aws_demo.pem ubuntu@34.229.240.123:/home/ubuntu
```

 c. The above command will copy the PEM file from your computer to the Bastion host. Once the file is successfully copied, move on to the next step. d. SSH into the Bastion host using the following command:


```
ssh -i aws_demo.pem ubuntu@34.229.240.123
```

 e. After SSHing into the Bastion host, use the ls command to check if the aws_demo.pem file is present. If it's not there, double-check your previous commands. f. Now, you can SSH into the private instance using the following command, replacing <private IP> with the private instance's IP address:


```
ssh -i aws_demo.pem ubuntu@<private IP>
```

 g. We will deploy our application on one of the private instances to test the load balancer. h. After successfully SSHing into the private instance, create an HTML file using the Vim text editor:

```
vim demo.html
```

i. This will open the Vim editor. Copy and paste any HTML content you like into the editor. j. For example:

```
<!DOCTYPE html>  
  
<html>  
  
<head>  
  
<title>Page Title</title>  
  
</head>  
  
<body>  
  
<h1>This is an AWS Demo Production</h1>  
  
</body>  
  
</html>
```

k. After pasting the content, save the file by pressing 'Esc' to exit insert mode and then entering :w to save. l. Finally, start a Python HTTP server on port 8000 to deploy your application on the private instance:

```
python3 -m http.server 8000
```

Now, your application is deployed on the private instance on port 8000.

Note :

We intentionally deployed the application on only one instance to check if the Load Balancer will distribute 50% of the traffic to one instance (which will receive a response) and 50% to another instance (which will not receive a response).

Step 4 :

Creating the Load Balancer :

1. Access the EC2 Terminal.
2. Follow the steps outlined below.

Screenshot of the AWS Management Console showing the Load Balancers page under the EC2 service. The sidebar on the left shows various AWS services like Images, Elastic Block Store, Network & Security, and Load Balancing. The main pane displays a table with no load balancers listed, and a message stating "No load balancers". A "Create load balancer" button is visible at the top right.

Screenshot of the AWS Management Console showing the comparison between Application Load Balancer (ALB), Network Load Balancer (NLB), and Gateway Load Balancer (GWLB). Each section includes a diagram and a brief description:

- Application Load Balancer (ALB):** Handles HTTP and HTTPS traffic, operating at the request level. It routes traffic to multiple targets (Amazon EC2 instances, microservices, containers) based on advanced routing and visibility features.
- Network Load Balancer (NLB):** Handles TCP, UDP, and TLS traffic, operating at the connection level. It is designed for ultra-high performance, TLS offloading, centralized certificate deployment, and static IP addresses.
- Gateway Load Balancer (GWLB):** Handles traffic for third-party virtual appliances supporting GENEVE. It improves security, compliance, and policy controls.

A "Create" button is located at the bottom of each section, and a note at the bottom indicates "Classic Load Balancer - previous generation".

Screenshot of the AWS Management Console showing the "Create Application Load Balancer" wizard. The first step, "Basic configuration", is displayed. It includes fields for:

- Load balancer name:** "aws-prod-all" (highlighted with a red box).
- Scheme:** "Internet-facing" (radio button selected).
- IP address type:** "Public" (radio button selected).

The "How Elastic Load Balancing works" section is also visible above the configuration form.

IP address type **Info**
 Select the type of IP addresses that your subnets use.

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

aws-prod-demo-vpc
 vpc-0eb3f78ab19d3a68b
 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 (use1-az4)

Subnet
 subnet-0e23e743f1cb89279 aws-prod-demo-subnet-public1-us-east-1a

IPv4 address

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 (use1-az4)

Subnet
 subnet-0e23e743f1cb89279 aws-prod-demo-subnet-public1-us-east-1a

IPv4 address
 Assigned by AWS

us-east-1b (use1-az6)

Subnet
 subnet-0f71bb5ec2ed1e896 aws-prod-demo-subnet-public2-us-east-1b

IPv4 address
 Assigned by AWS

CloudShell **Feedback** **Language**

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

Security groups
 Select up to 5 security groups

aws-prod-sg
 sg-0307215e2b24ec234 VPC: vpc-0eb3f78ab19d3a68b

Select a Security Group With SSH access Port 22 , HTTP access Port 80 , Custom TCP access Port 8000 or Create a new Security group with the mentioned access.

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	Default action
HTTP	: 80	Forward to Select a target group
1-65535		

Create target group [\[?\]](#)

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

Screenshot of the AWS CloudFront console showing the "Specify group details" step for creating a target group. The "Basic configuration" section is visible, and the "Choose a target type" section shows "Instances" selected.

Specify group details

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

Step 1: Specify group details

Step 2: Register 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.

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS CloudFront console showing the "Create target group" step. The "Target group name" is set to "aws-prod-tg". The "Protocol" dropdown is set to "HTTP" and "Port" is set to "8000". A callout bubble points to the "Define Port 8000" link.

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

aws-prod-tg

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

Protocol

Protocol: Port

HTTP : 8000 Define Port 8000

1-65535

VPC

Select the VPC with the instances that you want to include in the target group.

aws-prod-demo-vpc
vpc-0eb3f78a19d3a68b
IPv4: 10.0.0.0/16

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.

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS CloudFront console showing the "Create target group" step. The "Health check protocol" is set to "HTTP". The "Health check path" is set to "/". The "Attributes" section contains a note about default attributes. The "Tags - optional" section is present. A large orange "Next" button is at the bottom right.

Health check protocol

HTTP

Health check path

Use the default path of "/" to ping 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

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

EC2 > Target groups > Create target group

Step 1
Specify group details

Step 2
Register targets

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.

Instance ID	Name	State	Security groups	Zone
i-0b17dd1e4ebeda4ef		Running	aws-prod-sg	us-east-1a
i-0e43baf8c424ba653		Running	aws-prod-sg	us-east-1b
i-of9bf711b9cc2da54	Bastion_host	Running	launch-wizard-1	us-east-1b

Available instances (2/3)

2 selected

Ports for the selected instances
Ports for routing traffic to the selected instances.
8000
1-65535 (separate multiple ports with commas)

Select two private instances and Click Include as pending below

Include as pending below

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Services Search [Alt+S]

Ports for the selected instances
Ports for routing traffic to the selected instances.
8000
1-65535 (separate multiple ports with commas)

Include as pending below

2 selections are now pending below. Include more or register targets when ready.

Review targets

Targets (2)

Show only pending Remove all pending

Remove	Health status	Instance ID	Name	Port	State	Security groups	Zone	Subnet ID
X	Pending	i-0b17dd1e4ebeda4ef		8000	Running	aws-prod-sg	us-east-1a	subnet-0486c3d2:8000
X	Pending	i-0e43baf8c424ba653		8000	Running	aws-prod-sg	us-east-1b	subnet-0cebb929c:8000

2 pending

Create target group

CloudShell Feedback Language

© 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Services Search [Alt+S]

Listener HTTP:80

Protocol Port : 80 Default action Info
Forward to aws-prod-tg Target type: Instance, IPv4
Create target group

Listener tags - optional
Add listener tag
Add listener

Add-on services - optional
AWS Global Accelerator Info
Create an accelerator to get static IP addresses and improve the performance and availability of your applications. Additional charges apply

Summary
Review and confirm your configurations. Estimate cost

Basic configuration Edit aws-prod-alb <ul style="list-style-type: none">Internet-facingIPV4	Security groups Edit <ul style="list-style-type: none">aws-prod-sg sg-0307215e2b24ec234	Network mapping Edit VPC vpc-0eb3f78ab19d3a68b aws-prod-vpn <ul style="list-style-type: none">us-east-1a subnet-0e23e743f1cb89279 aws-prod-demo-subnet-public1-us-east-1aus-east-1b subnet-0f71bb5ec2ed1e896 aws-prod-demo-subnet-public2-us-east-1b	Listeners and routing Edit <ul style="list-style-type: none">HTTP:80 defaults to aws-prod-tg
Add-on services Edit None		Tags Edit None	
Attributes <p> Certain default attributes will be applied to your load balancer. You can view and edit them after creating the load balancer.</p>			

[Create load balancer](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

Successfully created load balancer: aws-prod-alb
Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic. Targets will also take a few minutes to complete the registration process and pass initial health checks.

[EC2](#) > [Load balancers](#) > [aws-prod-alb](#) > Create Application Load Balancer

Create Application Load Balancer

Suggested next steps

- Review, customize, or configure attributes for your load balancer and listeners using the **Description** and **Listeners** tabs within [aws-prod-alb](#).
- Discover other services that you can integrate with your load balancer. Visit the **Integrated services** tab within [aws-prod-alb](#).

[View load balancer](#)

CloudShell Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences

New EC2 Experience [Tell us what you think](#)

Load balancers (1)
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

Name	DNS name	State	VPC ID	Availability Zones	Type	Date created
aws-prod-alb	aws-prod-alb-125533229...	Active	vpc-0eb3f78ab19d3a68b	2 Availability Zones	application	September 10, 2023 10:41

[Actions](#) [Create load balancer](#)

0 load balancers selected
Select a load balancer above.

[Copy the DNS and paste it in any browser.](#)



Now We Successfully deployed Application securely in Private instance , We can access it through Internet using Load Balancer Securely .