

1. Create one VPC in N. Virginia region.

Go to n virginia region and select vpc create vpc.

The image shows two screenshots from the AWS Management Console. The top screenshot is the 'Create VPC' wizard in the 'United States (N. Virginia)' region. It shows the 'VPC settings' section with the following configurations: 'Resources to create' set to 'VPC only', 'Name tag' set to 'my-vpc', 'IPv4 CIDR block' set to '10.0.0.0/16' (manual input), and 'IPv6 CIDR block' set to 'No IPv6 CIDR block'. The bottom screenshot is the 'VPC dashboard' for the VPC 'vpc-0c51898d0fd83685e / my-vpc'. It shows a 'Details' section with the following information: VPC ID 'vpc-0c51898d0fd83685e', State 'Available', DNS resolution 'Enabled', Main network ACL 'acl-01ad49fd9f13dd150', IPv6 CIDR 'Network border group', Tenancy 'default', Default VPC 'No', Network Address Usage metrics 'Disabled', Block Public Access 'Off', DHCP option set 'dopt-00c6903fa1073ba46', IPv4 CIDR '10.0.0.0/16', Route 53 Resolver DNS Firewall rule groups '-', DNS hostnames 'Disabled', Main route table 'rtb-0167a738f71797291', IPv6 pool '-', and Owner ID '235351028455'. The 'Resource map' section shows a VPC, 2 Subnets, 3 Route tables, and Network Connections.

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.

my-vpc

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

IPv4 CIDR
10.0.0.0/16
CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)
☒ No IPv6 CIDR block
☐ IPAM-allocated IPv6 CIDR block
☐ Amazon-provided IPv6 CIDR block

VPC dashboard [vpc-0c51898d0fd83685e](#)

Virtual private cloud

- Your VPCs
- Subnets
- Route tables
- Internet gateways
- Egress-only internet gateways
- Carrier gateways
- DHCP option sets
- Elastic IPs
- Managed prefix lists
- NAT gateways
- Peering connections
- Route servers [New](#)

Security

vpc-0c51898d0fd83685e / my-vpc [Action](#)

Details [Info](#)

VPC ID vpc-0c51898d0fd83685e	State Available	Block Public Access Off	DNS hostnames Disabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-00c6903fa1073ba46	Main route table rtb-0167a738f71797291
Main network ACL acl-01ad49fd9f13dd150	Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool -
IPv6 CIDR (Network border group) -	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 235351028455

Resource map [Info](#) [Show all details](#)

Resource map

- VPC
Your AWS virtual network
- Subnets (2)
Subnets within this VPC
- Route tables (3)
Route network traffic to resources
- Network Connections
Connections to other VPCs

2. Create two subnets: one public subnet and one private subnet.

Go to subnets and create subnet and select vpc and give the cidr range for subnet.

aws

Search

[Alt+S]

VPC

Subnets

Create subnet

VPC ID

Create subnets in this VPC.

vpc-0c51898d0fd83685e (my-vpc)

Associated VPC CIDRs

IPv4 CIDRs

10.0.0.0/16

Subnet settings

Specify the CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name

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

pub-subnet

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.

No preference

CloudShell

Feedback

© 2025, Amazon

Create public subnet and select created vpc and give subnet name and cidr range .

aws

Search

[Alt+S]

VPC

Subnets

VPC dashboard

AWS Global View

Filter by VPC

Virtual private cloud

Your VPCs

Subnets

Route tables

Internet gateways

Egress-only internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

NAT gateways

Peering connections

Route servers

Security

Subnets (1/2)

Info

Last updated 18 minutes ago

Actions

Find subnets by attribute or tag

	Name	Subnet ID	State	VPC	Block Public...
<input type="checkbox"/>	pri-subnet	subnet-0e32deb8085ee322d	Available	vpc-0c51898d0fd83685e my-...	Off
<input checked="" type="checkbox"/>	pub-subnet	subnet-04e9b2feb7e22f4b3	Available	vpc-0c51898d0fd83685e my-...	Off

subnet-04e9b2feb7e22f4b3 / pub-subnet

Details

Flow logs

Route table

Network ACL

CIDR reservations

Sharing

Tags

Details

Subnet ID

subnet-04e9b2feb7e22f4b3

Subnet ARN

arn:aws:ec2:us-east-1:235351028455:subnet/subnet-04e9b2feb7e22f4b3

State

Available

Block Public Access

Off

IPv4 CIDR

10.0.0.0/20

Available IPv4 addresses

4091

IPv6 CIDR

-

IPv6 CIDR association ID

-

Availability Zone

us-east-1a

Network border group

-

VPC

vpc-0c51898d0fd83685e | mv-vpc

Route table

rtb-0ae8874bb25115589 | publi

VPC dashboard > Subnets

Subnets (1/2) Info

Find subnets by attribute or tag

Name	Subnet ID	State	VPC	Block Public...
<input checked="" type="checkbox"/> pri-subnet	subnet-0e32deb8085ee322d	Available	vpc-0c51898d0fd83685e my-...	Off
<input type="checkbox"/> pub-subnet	subnet-04e9b2feb7e22f4b3	Available	vpc-0c51898d0fd83685e my-...	Off

subnets-0e32deb8085ee322d / pri-subnet

Details | Flow logs | Route table | Network ACL | CIDR reservations | Sharing | Tags

Details

Subnet ID subnet-0e32deb8085ee322d	Subnet ARN arn:aws:ec2:us-east-1:23535102845:subnet/subnet-0e32deb8085ee322d	State Available	Block Public Access Off
IPv4 CIDR 10.0.16.0/20	Available IPv4 addresses 4091	IPv6 CIDR -	IPv6 CIDR association ID -

3. Attach an IGW to the VPC.

Go to internet gateways and create internet gateway and attach to vpc.

VPC dashboard > Internet gateways > 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.

my-internet-gateway

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**

Q Name X Q my-internet-gateway X Remove

Add new tag

You can add 49 more tags.

Cancel Create internet gateway

VPC dashboard > Internet gateways > igw-061e0cce444b0dc00

igw-061e0cce444b0dc00 / my-vpc-gateway

Details Info

Internet gateway ID igw-061e0cce444b0dc00	State Attached	VPC ID vpc-0c51898d0fd83685e my-vpc	Owner 23535102845
---	---------------------------------------	---	---

Tags

Search tags

Key	Value
Name	my-vpc-gateway

Manage tags

4. Create one public route table (RT) and one private route table.

Go to route table and create route table and give name and select vpc.

☰ VPC > Route tables > Create route table

Create route table Info

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

Route table settings

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

VPC
The VPC to use for this route table.

vpc-0c51898d0fd83685e (my-vpc) ▼

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**

You can add 49 more tags.

☰ VPC > Route tables > rtb-0ae8874bb25115589

rtb-0ae8874bb25115589 / public-routetable

VPC dashboard <
AWS Global View
 ▼

Virtual private cloud ▼
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Route servers [New](#)

Details Info

Route table ID rtb-0ae8874bb25115589	Main No	Explicit subnet associations subnet-04e9b2feb7e22f4b3 / pub-subnet	Edge associations -
VPC vpc-0c51898d0fd83685e my-vpc	Owner ID 235351028455		

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

Routes (2) ▼

Destination	Target	Status	Propagated	Route Origin
0.0.0.0/0	igw-061e0cce444b0dc00	Active	No	Create Route
10.0.0.0/16	local	Active	No	Create Route Tab

Create private route table and give name and select vpc.

aws [Alt+S] United States (N. Virginia) Account ID: 2353-5102-8455 root

VPC > Route tables > Create route table

Create route table [Info](#)

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

Route table settings

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

VPC
The VPC to use for this route table.

vpc-0c51898d0fd83685e (my-vpc)

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](#)

aws [Alt+S] United States (N. Virginia) Account ID: 2353-5102-8455 root

VPC > Route tables > rtb-0b41bd3f28020f417

rtb-0b41bd3f28020f417 / private-routetable [Actions](#)

VPC dashboard

[AWS Global View](#)

[Filter by VPC](#)

Virtual private cloud

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

Details [Info](#)

Route table ID rtb-0b41bd3f28020f417	Main No	Explicit subnet associations subnet-0e32deb8085ee322d / pri-subnet	Edge associations -
VPC vpc-0c51898d0fd83685e my-vpc	Owner ID 235351028455		

[Routes](#) | [Subnet associations](#) | [Edge associations](#) | [Route propagation](#) | [Tags](#)

Routes (1)

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	Active	No	Create Route Table

[Both](#) [Edit routes](#)

5. Deploy a NAT gateway in the public subnet and attach the NAT gateway to the private subnet.

Go to nat gateways and create nat gateway and select public subnet and allocate elastic ip.

☰ [VPC](#) > [NAT gateways](#) > Create NAT gateway

✔ Elastic IP address 52.206.43.157 (eipalloc-0ea1ec4217bb98d45) allocated.

Create NAT gateway [Info](#)

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

NAT gateway settings

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

my-nat-gateway

The name can be up to 256 characters long.

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

subnet-04e9b2feb7e22f4b3 (pub-subnet) ▼

Connectivity type
Select a connectivity type for the NAT gateway.

☒ Public
☐ Private

Elastic IP allocation ID [Info](#)
Assign an Elastic IP address to the NAT gateway.

eipalloc-0ea1ec4217bb98d45 ▼ [Allocate Elastic IP](#)

Go to route tables and go to private route table and edit routes and add nat gateway.

aws ☰ Search [Alt+S] United States (N. Virginia) Account ID: 2353-5102-8455 root

☰ [VPC](#) > [Route tables](#) > [rtb-0b41bd3f28020f417](#) > Edit routes

Edit routes

Destination	Target	Status	Propagated	Route Origin
10.0.0.0/16	local	✔ Active	No	CreateRouteTable
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="NAT Gateway"/>	-	No	CreateRoute

[Add route](#)

[Cancel](#) [Preview](#) [Save changes](#)

6.Create two instances, one in the public subnet and one in the private subnet.

Go to instance and create instance give instance name and give the key pair

aws [Search] [Alt+S] United States (N. Virginia)

EC2 > Instances > Launch an instance

It seems like you may be new to launching instances in EC2. Take a walkthrough to learn about EC2, how to launch instances and about best practices

[Take a walkthrough](#) [Do not show me this message again.](#)

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

public-instance [Add additional tags](#)

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

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

[Recents](#) [Quick Start](#)

Summary

Number of instances [Info](#)

1

[Software Image \(AMI\)](#)
Amazon Linux 2023 AMI 2023.9.2...[read more](#)
ami-052064a798f08f0d3

[Virtual server type \(instance type\)](#)
t3.micro

[Firewall \(security group\)](#)
New security group

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

[Cancel](#)

In network settings select your vpc and select public subnet and select existing security group or create new security group.

EC2 > Instances > Launch an instance

red [Create new key pair](#)

Network settings [Info](#)

VPC - required [Info](#)

vpc-0c51898d0fd83685e (my-vpc) [10.0.0.0/16](#)

Subnet [Info](#)

subnet-04e9b2feb7e22f4b3 pub-subnet [Create new subnet](#)

VPC: vpc-0c51898d0fd83685e Owner: 235351028455
Availability Zone: us-east-1a (use1-az6) Zone type: Availability Zone
IP addresses available: 4090 CIDR: 10.0.0.0/20

Auto-assign public IP [Info](#)

Enable

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:

Summary

Number of instances

1

[Software Image](#)
Amazon Linux
ami-052064a798f08f0d3

[Virtual server type](#)
t3.micro

[Firewall \(security group\)](#)
New security group

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

[Cancel](#)

Repeat the same process for private instance. In network settings give the private subnet.

Key pair name - *required*

red [Create new key pair](#)

▼ **Network settings** [Info](#)

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

vpc-0c51898d0fd83685e (my-vpc) 10.0.0.0/16 [Create new VPC](#)

Subnet | [Info](#)

subnet-0e32deb8085ee322d pri-subnet [Create new subnet](#)

VPC: vpc-0c51898d0fd83685e Owner: 235351028455
Availability Zone: us-east-1a (use 1-az6) Zone type: Availability Zone
IP addresses available: 4091 CIDR: 10.0.16.0/20

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

Disable

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 4

EC2 > Instances

Instances (2/2) [Info](#)

Last updated less than a minute ago [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

Find Instance by attribute or tag (case-sensitive) All states

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input checked="" type="checkbox"/>	public-instance	i-0a3cf5850b7332622	Running	t3.micro	3/3 checks passed	View alarms	us-east-1a	-
<input checked="" type="checkbox"/>	private-instance	i-0095bbdc6ca4e921e	Initializing	t3.micro	Initializing	View alarms	us-east-1a	-

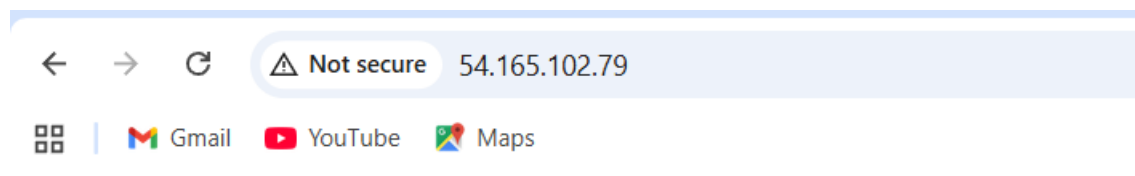
2 instances selected

[Monitoring](#)

7. Deploy Apache server on both EC2 instances with a sample index.html file.

Connect to public instance.

Open with public ip in your browser.



It works!

Login with the public ip from that login with the private instance for that there is no public ip so,we use public instance ip as bastion server.

```
MUJJU SK@DESKTOP-LU541U4 MINGW64 ~/Downloads
$ ssh -i red.pem ec2-user@54.165.102.79

_#-
~\##### Amazon Linux 2023
~~\#####
~~\###|
~~\#/ https://aws.amazon.com/linux/amazon-linux-2023
~~V'-'->
~~~~
~~~.-.-
~~~\_/
~~~/m/'

Last login: Wed Oct 8 15:13:39 2025 from 103.143.169.218
[ec2-user@ip-10-0-7-172 ~]$ sudo su -
Last login: Wed Oct 8 15:13:48 UTC 2025 on pts/1
[root@ip-10-0-7-172 ~]# ssh -i red.pem ec-2 user@10.0.20.86
Warning: Identity file red.pem not accessible: No such file or directory.
ssh: Could not resolve hostname ec-2: Name or service not known
[root@ip-10-0-7-172 ~]# ssh -i red.pem ec2-user@10.0.20.86
Warning: Identity file red.pem not accessible: No such file or directory.
The authenticity of host '10.0.20.86 (10.0.20.86)' can't be established.
ED25519 key fingerprint is SHA256:eKoLd6VlvzbwyE306wscXsvO27Af9DSFa0ZGy9SZC1E.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.20.86' (ED25519) to the list of known hosts.
ec2-user@10.0.20.86: Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
[root@ip-10-0-7-172 ~]#
```

```
[root@ip-10-0-7-172 ~]# yum install httpd -y
Last metadata expiration check: 0:22:01 ago on Wed Oct  8 15:14:19 2025.
Package httpd-2.4.65-1.amzn2023.0.1.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
Complete!
[root@ip-10-0-7-172 ~]# sudo systemctl start httpd
[root@ip-10-0-7-172 ~]# sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
   Active: active (running) since Wed 2025-10-08 15:15:29 UTC; 21min ago
     Docs: man:httpd.service(8)
  Main PID: 27057 (httpd)
    Status: "Total requests: 2; Idle/Busy workers 100/0; Requests/sec: 0.00156; Bytes served/sec: 1 B/sec"
    Tasks: 230 (limit: 1053)
   Memory: 16.6M
      CPU: 1.567s
   CGroup: /system.slice/httpd.service
           └─27057 /usr/sbin/httpd -DFOREGROUND
             └─27084 /usr/sbin/httpd -DFOREGROUND
               └─27088 /usr/sbin/httpd -DFOREGROUND
                 └─27089 /usr/sbin/httpd -DFOREGROUND
                   └─27091 /usr/sbin/httpd -DFOREGROUND
                     └─27507 /usr/sbin/httpd -DFOREGROUND

Oct 08 15:15:29 ip-10-0-7-172.ec2.internal systemd[1]: Starting httpd.service - The Apache HTTP Server...
Oct 08 15:15:29 ip-10-0-7-172.ec2.internal systemd[1]: Started httpd.service - The Apache HTTP Server.
Oct 08 15:15:29 ip-10-0-7-172.ec2.internal httpd[27057]: Server configured, listening on: port 80
[root@ip-10-0-7-172 ~]#
```

8. Create one application load balancer and attach it to both EC2 instances.

Go to load balancers and select application load balancer and create load balancer.

[Alt+S]

[EC2](#) > [Load balancers](#) > Compare and select load balancer type

Compare and select load balancer type

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

Load balancer types

Application Load Balancer [Info](#)

Network Load Balancer [Info](#)

Gateway Load Balancer [Info](#)

Give the name and select vpc,select internet facing and select ipv4.

EC2 > Load balancers > Create Application Load Balancer

Create Application Load Balancer

The Application Load Balancer distributes incoming HTTP and HTTPS traffic across multiple targets such as Amazon EC2 instances, microservices, and c 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

► 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.

application-loadbalancer

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

Scheme

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

☒ Internet-facing

- Serves internet-facing traffic.
- Has public IP addresses.
- DNS name resolves to public IPs.
- Requires a public subnet.

☐ Internal

- Serves internal traffic.
- Has private IP addresses.
- DNS name resolves to private IPs.
- Compatible with the IPv4 and Dualstack IP address types.

Load balancer IP address type

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 IP

☒ IPv4

Select security groups and listners port 80.

EC2 > Load balancers > Create Application Load Balancer

Security groups

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

default

sg-0880f310383562b69 VPC: vpc-06cf45eaab13624fe

Listeners and routing

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 I

▼ Listener HTTP:80

Protocol

HTTP

Port

80

Default action

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

Create target group to redirect to target group which we placed.

Go to ec2 and select target groups and create.

EC2 > Target groups > Create target group

Step 1

Create target group

Step 2

Register targets

Create target group

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

target groups > Create target group

Target group name

us-east1

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

Protocol

Protocol for load balancer-to-target communication. Can't be modified after creation.

HTTP

Port

Port number where targets receive traffic. Can be overridden for individual targets during registration.

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.

vpc-06cf45eaab13624fe (default)

172.31.0.0/16

(default)

Create VPC

aws

Search

[Alt+S]

United

EC2 > Target groups > Create target group

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.

Select the both instances and click create.

EC2 > Target groups > Create target group

Step 1

Create target group

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.

Available instances (2/2)

Filter instances

<input checked="" type="checkbox"/>	Instance ID	Name	State	Security groups
<input checked="" type="checkbox"/>	i-0b1c306f0271cf8bc	private-instance	Running	default
<input checked="" type="checkbox"/>	i-089f2e7536df47667	public-instance	Running	default

2 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

EC2 > Load balancers > application-loadbalancer

EC2

Dashboard

EC2 Global View

Events

Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Successfully created load balancer: application-loadbalancer

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.

application-loadbalancer

Details

Load balancer type

Application

Scheme

Internet-facing

Status

Provisioning

Hosted zone

Z355XDOTRQ7X7K

VPC

vpc-06cf45eaab13624fe

Availability Zones

subnet-04f12a817188fcadc us-east-1b (use1-az1)

subnet-0a192382de0e2bf6a us-east-1a (use1-az6)

Load balancer IP address type

IPv4

Date created

October 9, 2025, 12:35 (UTC+)

Load balancer ARN

arn:aws:elasticloadbalancing:us-east-1:235351028455:loadbalancer/app/application-loadbalancer/bfa35c7473e0bf9e

DNS name info

application-loadbalancer-1181816658.us-east-1.elb.amazonaws.com (A F

Listeners and rules

Network mapping

Resource map

Security

Monitoring

Integrations

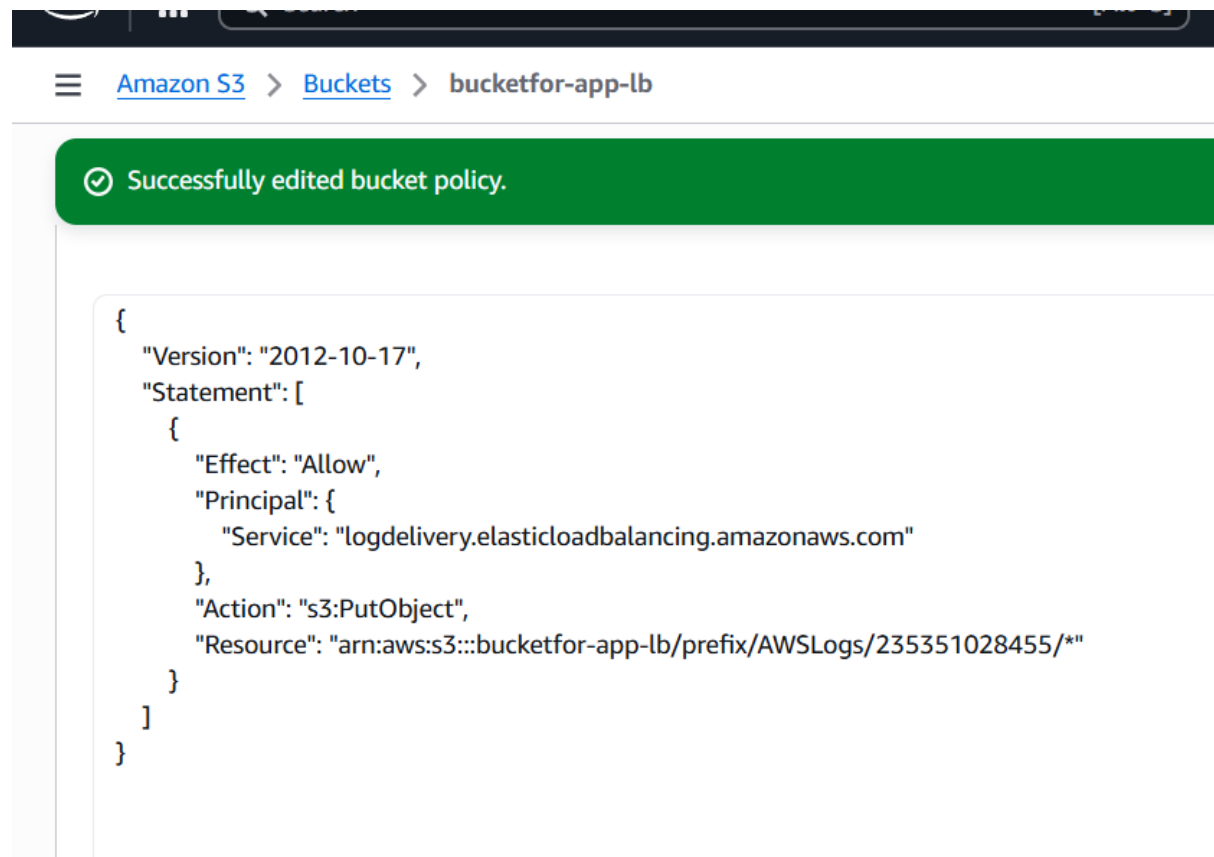
Attributes

Capacity

T

9.Store application load balancer logs in S3.

Go to s3 bucket and create a bucket and go to that bucket and add permissions add the policy.



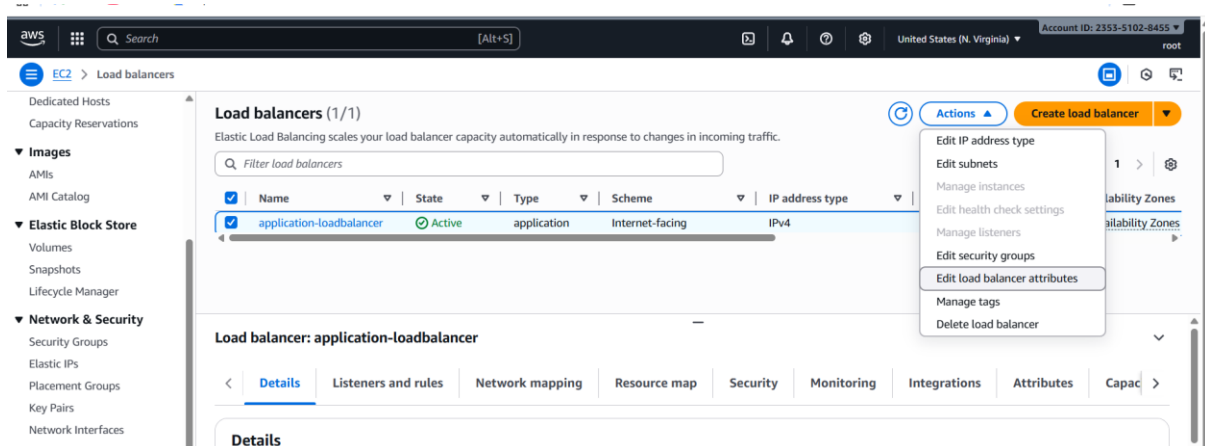
```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"  
      },  
      "Action": "s3:PutObject",  
      "Resource": "arn:aws:s3:::bucketfor-app-lb/prefix/AWSLogs/235351028455/*"  
    }  
  ]  
}
```

```

    },
    "Action": "s3:PutObject",
    "Resource": "arn:aws:s3:::bucketfor-app-
lb/prefix/AWSLogs/235351028455/*"
  }
]
}

```

Go to load balancers and edit the load balancer attribute.



Go to monitoring and select access logs and choose your bucket.

aws

Search [Alt+S]

EC2 > Load balancers > application-loadbalancer > Edit load balancer attributes

☒ **Disable - Default**
Zonal shift will not be available to the load balancer.

☐ **Enable**
Zonal shift will be available to the load balancer.

Protection

☐ **Deletion protection**
To prevent your load balancer from being deleted accidentally, turn on deletion protection. If you turn on deletion protection, you must

Monitoring

☒ **Access logs**
Access logs deliver detailed logs of all requests made to your Elastic Load Balancer. Choose an existing S3 location. If you don't specify a

S3 URI

Q s3://bucketfor-app-lb|

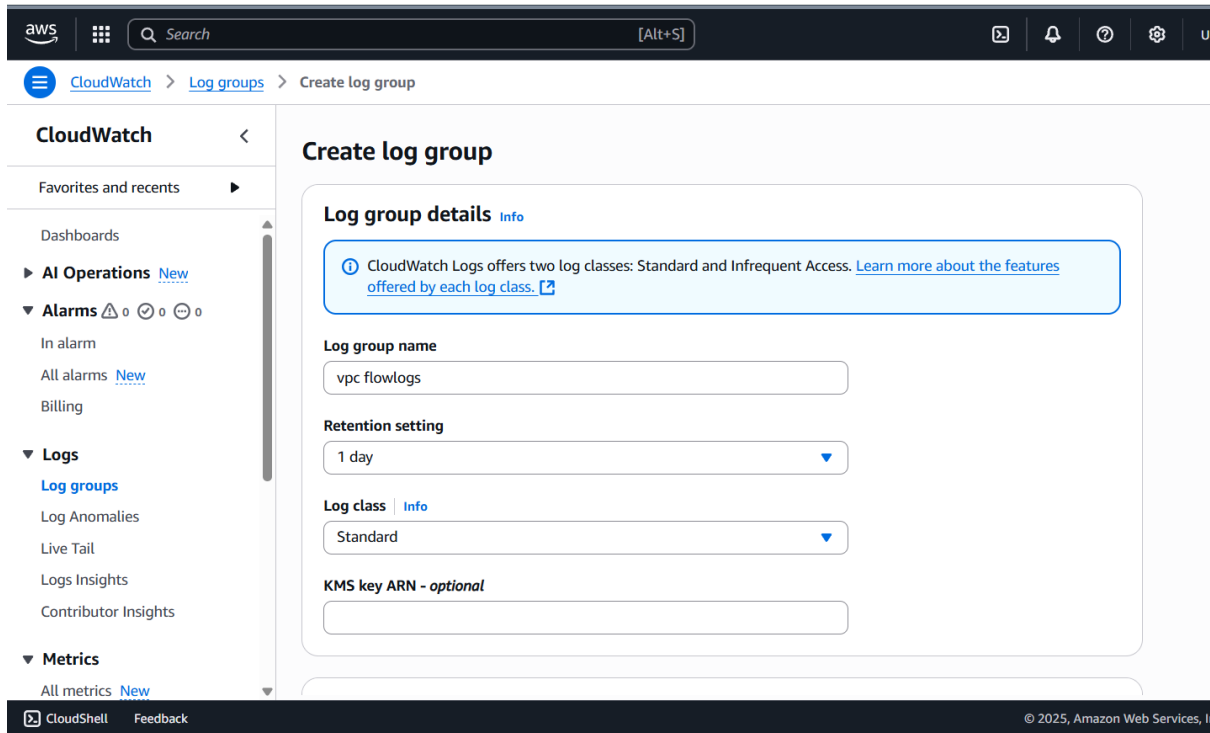
Format: s3://bucket/prefix

☐ **Connection logs**
Connection logs deliver detailed logs of all connections made to your Elastic Load Balancer. Choose an existing S3 location. If you don't s

Then the flowlogs are stored in the bucket.

10.Store the VPC flow logs in a CloudWatch log group.

Go to cloud watch and select flowlog groups and create flowlogs



Go to vpc and select flowlogs and create flowlogs.

aws

Search

[Alt+S]

VPC

>

Your VPCs

>

Create flow logs

Flow log settings

Name - optional

flowlogs-01

Filter
The type of traffic to capture (accepted traffic only, rejected traffic only, or all traffic).

☐ Accept

☐ Reject

☒ All

Maximum aggregation interval | [Info](#)
The maximum interval of time during which a flow of packets is captured and aggregated into a flow log record.

☒ 10 minutes

☐ 1 minute

Destination
The destination to which to publish the flow log data.

☒ Send to CloudWatch Logs

☐ Send to an Amazon S3 bucket

☐ Send to Amazon Data Firehose in the same account

☐ Send to Amazon Data Firehose in a different account

Use: logs

logs

aws

Search

[Alt+S]

United States (N. Virginia)

Account ID: 2353-5102-8455

root

CloudWatch

>

Log groups

CloudWatch

<

Favorites and recents

>

Dashboards

>

AI Operations

New

Alarms

<

>

<

>

In alarm

All alarms

New

Billing

Logs

>

Log groups

Log Anomalies

Live Tail

Logs Insights

The following log group(s) have been deleted:

logs

Log groups (1)

By default, we only load up to 10000 log groups.

Filter log groups or try pattern search

Exact match

<

1

>

<input type="checkbox"/>	Log group	<input type="checkbox"/>	Log class	<input type="checkbox"/>	Anomaly d...	<input type="checkbox"/>	Data pr...	<input type="checkbox"/>	Sensitiv...	<input type="checkbox"/>	Retention	<input type="checkbox"/>	Metric fi...
<input type="checkbox"/>	logs		Standard	Configure	-	-	-	-	-	-	Never expire	-	-

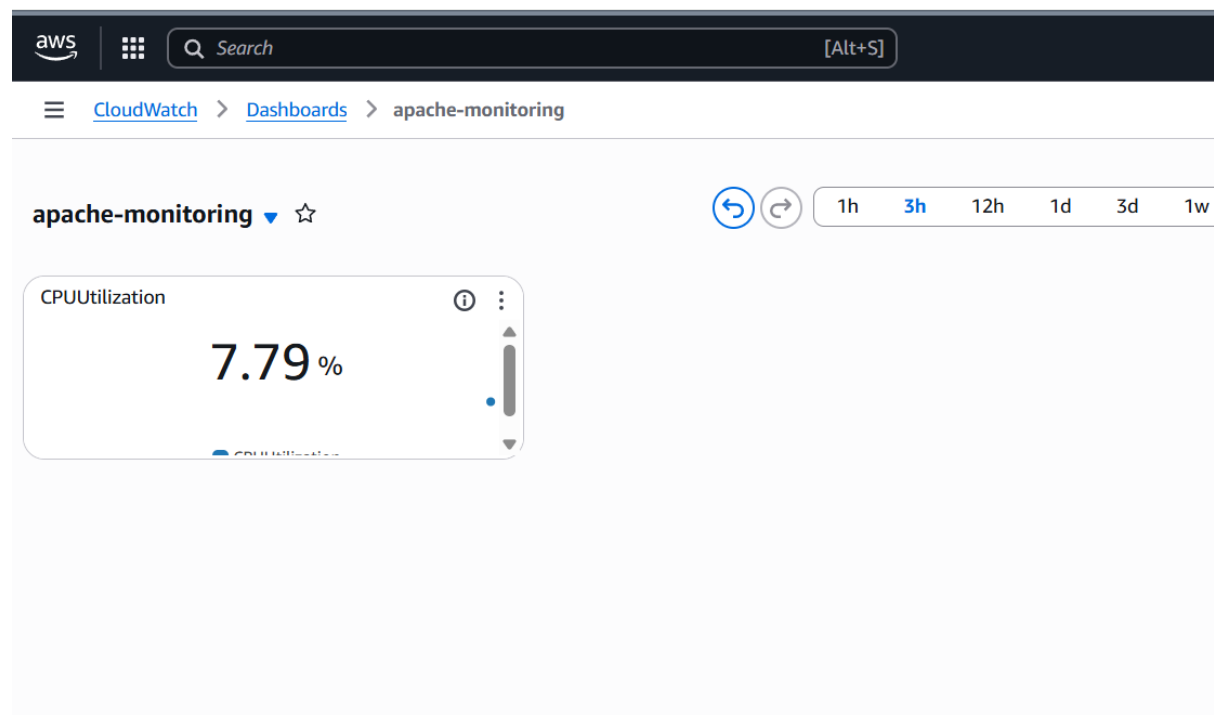
11.Create monitoring dashboards to monitor CPU utilization and to monitor the Apache service.

Launch a instance and install apache in that.

```
[root@ip-172-31-83-40 ~]# yum install httpd
Last metadata expiration check: 0:00:17 ago on Thu Oct  9 09:43:54 2025.
Dependencies resolved.
=====
Package                                Architecture                Version
=====
Installing:
httpd                                  x86_64                       2.4.65-1.amzn2023.0.1
Installing dependencies:
apr                                    x86_64                       1.7.5-1.amzn2023.0.4
apr-util                              x86_64                       1.6.3-1.amzn2023.0.1
generic-logos-httpd                  noarch                       18.0.0-12.amzn2023.0.3
httpd-core                           x86_64                       2.4.65-1.amzn2023.0.1
httpd-filesystem                     noarch                       2.4.65-1.amzn2023.0.1
httpd-tools                           x86_64                       2.4.65-1.amzn2023.0.1
libbrotli                             x86_64                       1.0.9-4.amzn2023.0.2
mailcap                              noarch                       2.1.49-3.amzn2023.0.3
Installing weak dependencies:
apr-util-openssl                     x86_64                       1.6.3-1.amzn2023.0.1
mod_http2                             x86_64                       2.0.27-1.amzn2023.0.3
mod_lua                               x86_64                       2.4.65-1.amzn2023.0.1
=====
```

Go to cloudwatch and create a dashboard.

Select the metrics as number,ec2,copy the instance id and paste there and select apache service cpu utilization.



12.If CPU utilization is more than 70%, then it should trigger auto scaling and launch new instance.

Go to templates launch create template

aws

Search

[Alt+S]

Search results

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 have multiple versions.

Launch template name and description

Launch template name - *required*

my-template

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

Template version description

v1

Max 255 chars

Auto Scaling guidance

[Info](#)

Select this if you intend to use this template with EC2 Auto Scaling

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

► Template tags

► Source template

Launch template contents

aws

Search

[Alt+S]

United States (N. Virginia)

Search results

Instance type

t3.micro

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

Free tier eligible

On-Demand Ubuntu Pro base pricing: 0.0139 USD per Hour

On-Demand SUSE base pricing: 0.0104 USD per Hour

On-Demand RHEL base pricing: 0.0392 USD per Hour

On-Demand Linux base pricing: 0.0104 USD per Hour

On-Demand Windows base pricing: 0.0196 USD per Hour

Additional costs apply for AMIs with pre-installed software

▼

All generations

Compare instance types

Key pair (login)

[Info](#)

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

Key pair name

red

Create new key pair

Network settings

[Info](#)

Subnet

Don't include in launch template

Create new subnet

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

Availability Zone

Don't include in launch template

Enable additional zones

Summary

[Software Image \(AMI\)](#)

Amazon Linux 2023 kernel-6.1 A...[read](#)

ami-052064a798f08f0d3

[Virtual server type \(instance type\)](#)

t3.micro

[Firewall \(security group\)](#)

default

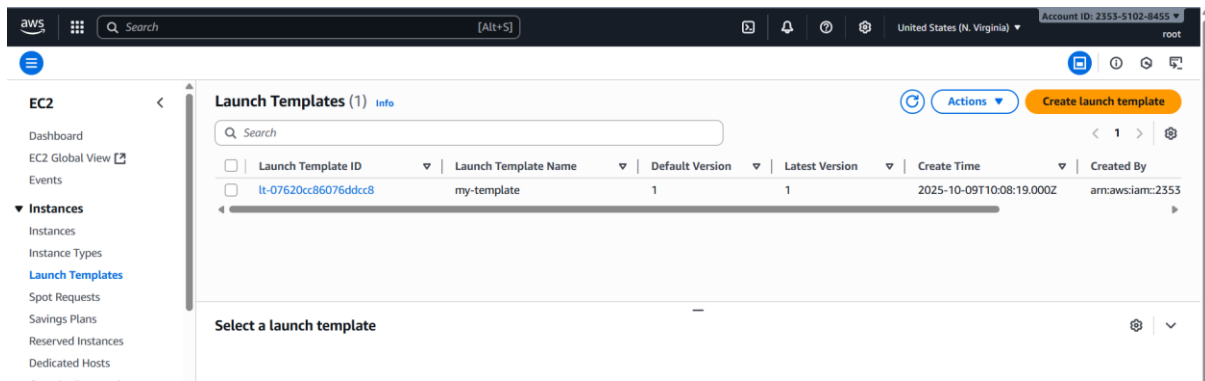
[Storage \(volumes\)](#)

1 volume(s) - 8 GiB

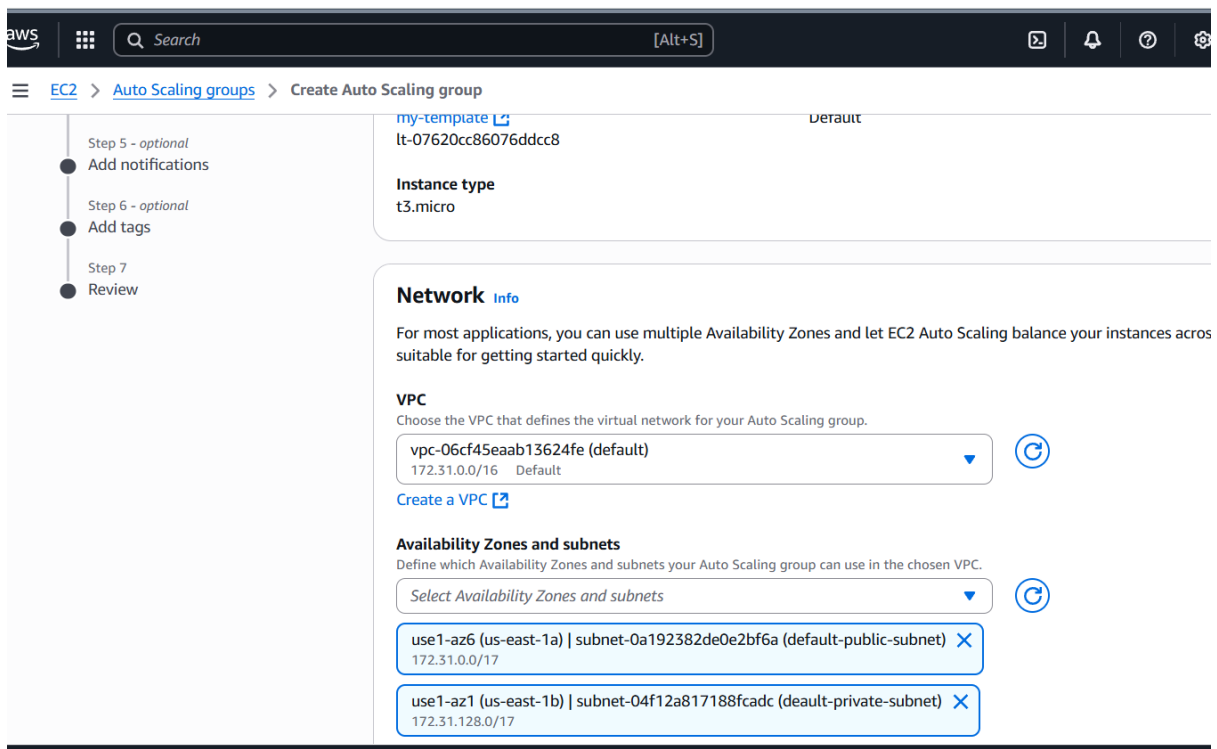
Cancel

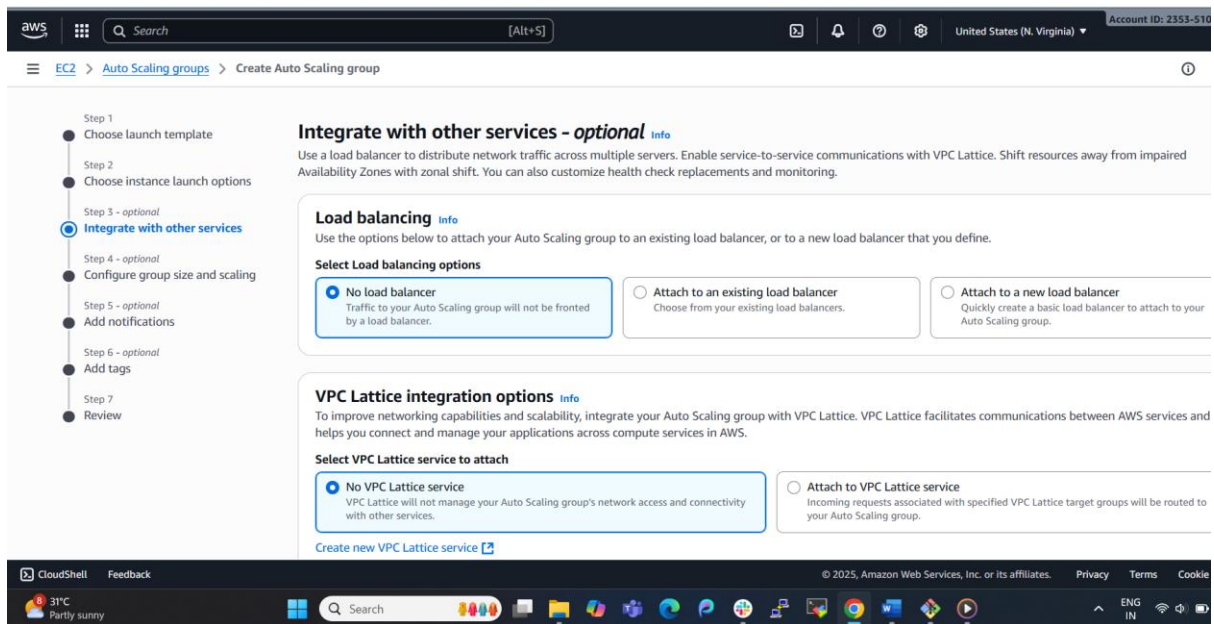
CloudShell Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.



Go to auto scaling groups and create auto scaling groups.
Give the name and select subnets, and give the security groups.





Two instances were created.

