

# ASG

## 1. Create one VPC in N. Virginia region.

- Open aws console

- Navigate to vpc

a39d7c4a4792149d

You successfully created vpc-0a39d7c4a4792149d / ASG-task-vpc

### vpc-0a39d7c4a4792149d / ASG-task-vpc

#### Details Info

VPC ID  
vpc-0a39d7c4a4792149d

DNS resolution  
Enabled

Main network ACL  
acl-014491767cc904a00

IPv6 CIDR (Network border group)  
-

State  
Available

Tenancy  
default

Default VPC  
No

Network Address Usage metrics  
Disabled

Block Public Access  
Off

DHCP option set  
dopt-05c5f706803d0d90e

IPv4 CIDR  
10.0.0.0/24

Route 53 Resolver DNS Firewall rule  
groups  
-

DNS hostnames  
Disabled

Main route table  
rtb-0004078bd986192aa

IPv6 pool  
-

Owner ID  
414691912691

#### Resource map

CIDRs

Flow logs

Tags

Integrations

#### Resource map Info

•

VPC

Subnets (0)

Route tables (1)

## 1.

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

- In vpc
- One public subnet
- One private subnet

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

You have successfully created 2 subnets: subnet-08e25989ee6c2a873, subnet-07c7d65419aad7e70

Last updated 4 minutes ago Actions Create subnet

Subnets (2) Info

Find subnets by attribute or tag

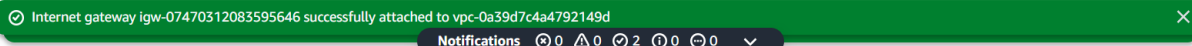
Subnet ID : subnet-08e25989ee6c2a873 Subnet ID : subnet-07c7d65419aad7e70 Clear filters

<input type="checkbox"/>	Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
<input type="checkbox"/>	asg-private	subnet-07c7d65419aad7e70	Available	vpc-0a39d7c4a4792149d   ASG...	Off	10.0.0.128/25
<input type="checkbox"/>	asg-public	subnet-08e25989ee6c2a873	Available	vpc-0a39d7c4a4792149d   ASG...	Off	10.0.0.0/25

Select a subnet


### 3 . Attach an IGW to the VPC.


- Create a internetgate way and attach it to VPC




**igw-07470312083595646 / ASG-IGW** Actions

**Details** Info

Internet gateway ID  
 igw-07470312083595646


State  
 Attached

VPC ID  
[vpc-0a39d7c4a4792149d](#) | ASG-task-vpc


Owner  
 414691912691

**Tags (1)**

Key	Value
-----	-------

Manage tags < 1 > 

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



**Route tables (4)** Info Last updated less than a minute ago Actions

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
<input type="checkbox"/>	-	<a href="#">rtb-0bb7c59c17d3274aa</a>	-	-	Yes	<a href="#">vpc-0dc28</a>
<input type="checkbox"/>	-	<a href="#">rtb-0004078bd986192aa</a>	-	-	Yes	<a href="#">vpc-0a39d</a>
<input type="checkbox"/>	asg-public-rt	<a href="#">rtb-0c8cdb8d7c33aa5d6</a>	<a href="#">subnet-08e25989ee6c2a...</a>	-	No	<a href="#">vpc-0a39d</a>
<input type="checkbox"/>	asg-private-rt	<a href="#">rtb-0b77eab20a0e583fa</a>	-	-	No	<a href="#">vpc-0a39d</a>

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

- NAT gateway created in public subnet while creating
-

nat-0edf3fff2e85a9bc5

✔ NAT gateway nat-0edf3fff2e85a9bc5 | asg-nat was created successfully.

### nat-0edf3fff2e85a9bc5 / asg-nat

[Details](#)

<b>NAT gateway ID</b> nat-0edf3fff2e85a9bc5	<b>Connectivity type</b> Public	<b>State</b> ⏸ Pending	<b>State message</b> <a href="#">Info</a> -
<b>NAT gateway ARN</b> arn:aws:ec2:us-east-1:414691912691:natgateway/nat-0edf3fff2e85a9bc5	<b>Primary public IPv4 address</b> -	<b>Primary private IPv4 address</b> -	<b>Primary network interface ID</b> -
<b>VPC</b> vpc-0a39d7c4a4792149d / ASG-task-vpc	<b>Subnet</b> subnet-07c7d65419aad7e70 / asg-private	<b>Created</b> 📅 Tuesday, November 4, 2025 at 11:44:40 GMT+5:30	<b>Deleted</b> -

[Secondary IPv4 addresses](#) | [Monitoring](#) | [Tags](#)

#### Secondary IPv4 addresses

🔍 Search

Private IPv4 address | Network interface ID | Status | Failure message

- Attaching NAT to private subnet in private route table
- Add private subnet to private route table and edit route sand add NAT gateway

✔ You have successfully updated subnet associations for rtb-0b77eab20a0e583fa / asg-private-rt.

### rtb-0b77eab20a0e583fa / asg-private-rt

[Details](#) [Info](#)

<b>Route table ID</b> rtb-0b77eab20a0e583fa	<b>Main</b> 📌 No	<b>Explicit subnet associations</b> subnet-07c7d65419aad7e70 / asg-private	<b>Edge associatio</b> -
<b>VPC</b> vpc-0a39d7c4a4792149d   ASG-task-vpc	<b>Owner ID</b> 414691912691		

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

#### Routes (2)

🔍 Filter routes

Destination	Target	Status	Propagated	Route i
0.0.0.0/0	nat-0edf3fff2e85a9bc5	✔ Active	No	Create
10.0.0.0/24	local	✔ Active	No	Create

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

- Navigate ec2 and edit network setting add vpc and public subnet and security groups

## ▼ Network settings [Info](#)

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

vpc-0a39d7c4a4792149d (ASG-task-vpc)  
10.0.0.0/24



### Subnet [Info](#)

subnet-08e25989ee6c2a873  
VPC: vpc-0a39d7c4a4792149d Owner: 414691912691  
Availability Zone: us-east-1a (use1-az4) Zone type: Availability Zone  
IP addresses available: 123 CIDR: 10.0.0.0/25

asg-public



[Create new subnet](#)

### 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

### Common security groups [Info](#)

Select security groups

default sg-07f90e1219dc5b3ad ✕  
VPC: vpc-0a39d7c4a4792149d



[Compare security group rules](#)

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

- Second instance private
- Select vpc
- Select private subnet and default security groups

## ▼ Network settings [Info](#)

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

vpc-0a39d7c4a4792149d (ASG-task-vpc)  
10.0.0.0/24



### Subnet [Info](#)

subnet-07c7d65419aad7e70  
VPC: vpc-0a39d7c4a4792149d Owner: 414691912691  
Availability Zone: us-east-1a (use1-az4) Zone type: Availability Zone  
IP addresses available: 122 CIDR: 10.0.0.128/25

asg-private



[Create new subnet](#)

### 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

### Common security groups [Info](#)

Select security groups

default sg-07f90e1219dc5b3ad ✕  
VPC: vpc-0a39d7c4a4792149d



[Compare security gr](#)

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

- Public instance and private instance

<input type="checkbox"/>	asg-public	i-0345700c9381ead39	⏸ Stopped	🔍 🔍	t3.micro	-	<a href="#">View alarms +</a>	us-east-1a
<input type="checkbox"/>	asg-private	i-05fd47955fca46195	🟢 Running	🔍 🔍	t3.micro	🕒 Initializing	<a href="#">View alarms +</a>	us-east-1a

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

- Using jump server,
- Access to public subnet instance
- Next, give chmod 400 (pem.key name)
- Now do ssh , using private instance ssh paste it in the same terminal

```
[ec2-user@ip-10-0-0-114 ~]$ ssh -i "all-key.pem" ec2-user@10.0.0.197
The authenticity of host '10.0.0.197 (10.0.0.197)' can't be established
ED25519 key fingerprint is SHA256:a5gy+SRDTxcyUU98HilDXctbDKQNIQPTYha/n
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.0.197' (ED25519) to the list of known hosts

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

[ec2-user@ip-10-0-0-197 ~]$ exit
Logout
```

- 
- Install httpd
- Sudo yum install httpd -y

Installed:

```
apr-1.7.5-1.amzn2023.0.4.x86_64
apr-util-1.6.3-1.amzn2023.0.2.x86_64
apr-util-ldap-1.6.3-1.amzn2023.0.2.x86_64
apr-util-openssl-1.6.3-1.amzn2023.0.2.x86_64
generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch
httpd-2.4.65-1.amzn2023.0.2.x86_64
httpd-core-2.4.65-1.amzn2023.0.2.x86_64
httpd-filesystem-2.4.65-1.amzn2023.0.2.noarch
httpd-tools-2.4.65-1.amzn2023.0.2.x86_64
libbrotli-1.0.9-4.amzn2023.0.2.x86_64
mailcap-2.1.49-3.amzn2023.0.3.noarch
mod_http2-2.0.27-1.amzn2023.0.3.x86_64
mod_lua-2.4.65-1.amzn2023.0.2.x86_64
```

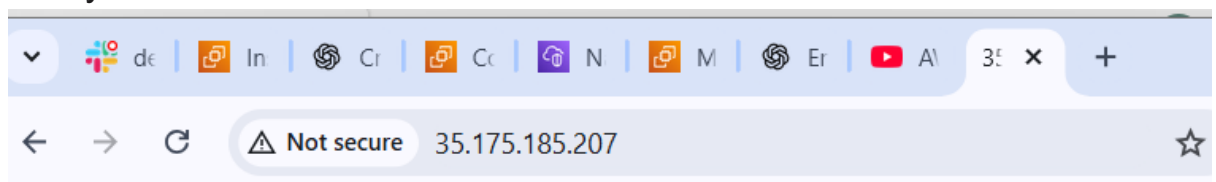
Complete!

- Creating simple webpage
- `echo "<h1>This is the PUBLIC Apache Server (Jump Server)</h1>" | sudo tee /var/www/html/index.html`

Complete!

```
[ec2-user@ip-10-0-0-197 ~]$ sudo systemctl start httpd
sudo systemctl enable httpd
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service
→ /usr/lib/systemd/system/httpd.service.
[ec2-user@ip-10-0-0-197 ~]$ cd /var/www/html/index.html
-bash: cd: /var/www/html/index.html: No such file or directory
[ec2-user@ip-10-0-0-197 ~]$ echo "<h1>This is the PUBLIC Apache Server
(Jump Server)</h1>" | sudo tee /var/www/html/index.html
<h1>This is the PUBLIC Apache Server (Jump Server)</h1>
[ec2-user@ip-10-0-0-197 ~]$ curl localhost
<h1>This is the PUBLIC Apache Server (Jump Server)</h1>
[ec2-user@ip-10-0-0-197 ~]$
```

- 
- Verify



Amazon Linux 2023

<https://aws.amazon.com/linux/amazon-linux-2023>

```
[ec2-user@ip-10-0-0-197 ~]$
```

- ```
Package httpd-2.4.65-1.amzn2023.0.2.x86_64 is already installed.
Dependencies resolved.
Nothing to do.
● Complete!
```

- ```
[ec2-user@ip-10-0-0-197 ~]$ curl http://35.175.185.207
<h1>Apache on Jump Server</h1>
[ec2-user@ip-10-0-0-197 ~]$
```

- Open aws console
- Navigate to ec2 > target groups
- Give name, select target as instance
- Select vpc of existing subnets
- Select public subnet and private subnet

- Now navigate to load balancer
- Create new
- Select application load balancer

aws [Search] [Alt+S] United States (N. Virginia) Account ID: 4146-9191-339

EC2 > Target groups > Create target group

Step 1 Create target group  
Step 2 **Register targets**  
Step 3 Review and create

### 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	Zone
<input checked="" type="checkbox"/>	i-01f12a13e564aefbb	autosacding-private	Running	default	us-east-1a
<input checked="" type="checkbox"/>	i-0bc2cb72c8ca6f030	autoscaling-ec2	Running	default	us-east-1a

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](#)

Select internet facing in scheme

EC2 > Load balancers > Create Application Load Balancer

### 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 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 | 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

- Click include as pending below



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

target group

80

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)

Filter targets

Show only pending

Remove all pending

Instance ID	Name	Port	State	Security groups	Zone	Private IPv4 address	Subnet ID
<a href="#">i-01f12a13e564aefbb</a>	autosacling-private	80	Running	default	us-east-1a	10.0.3.19	subnet-0a56bacc97
<a href="#">i-0bc2cb72c8ca6f030</a>	autoscaling-ec2	80	Running	default	us-east-1a	10.0.1.87	subnet-0e890e6d48

2 pending

Cancel

Previous

Next

- Target created successfully
- Now , create a application nload balancer
- Navigasge to load balancer in ec2
- Select vpc and 2 subnet s from different availability zone

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](#).

vpc-0ad3c0b33fec285e (autoscaling)  
10.0.0.0/16

#### IP pools [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 the [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 b.

☒ us-east-1a (use1-az4)

##### 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-0e890e6d482e183aa  
IPv4 subnet CIDR: 10.0.1.0/24

☒ us-east-1b (use1-az6)

##### 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-01e8c875b370cd0aa  
IPv4 subnet CIDR: 10.0.2.0/24

▼ Listener HTTP:80

Protocol

HTTP

Port

80

1-65535

Default action [Info](#)

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

Routing action

☒ Forward to target groups☐ Redirect to URL☐ Return fixed responseForward to target group [Info](#)Choose a target group and specify routing weight or [create target group](#).

Target group

asg

Target type: Instance, IPv4 | Target stickiness: Off

HTTP



Weight

1

0-999

Percent

100%

[+ Add target group](#)

You can add up to 4 more target groups.

Target group stickiness [Info](#)

Enables the load balancer to bind a user's session to a specific target group. To use stickiness the client must support cookies. If you want to bind a user's session to a specific target, turn on the Target

autoscaling-alb



Successfully created load balancer: autoscaling-alb

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.



Introducing URL rewrite for Application Load Balancer

Modify host headers and URL paths of incoming requests before they reach your targets. To get started, add a rule to your listener and configure a transform. [Learn more](#)

autoscaling-alb



Actions ▼

▼ Details

Load balancer type

Status

VPC

Load balancer IP address type

● Everything is healthy

asg

Actions ▼

Details

[arn:aws:elasticloadbalancing:us-east-1:414691912691:targetgroup/asg/2ec37f88654679a3](#)

Target type

Instance

Protocol : Port

HTTP: 80

Protocol version

HTTP1

VPC

[vpc-0ad3c0b33fecd285e](#)

IP address type

IPv4

Load balancer

[autoscaling-alb](#)

2

Total targets

2

Healthy

0

Unhealthy

0

Unused

0

Initial

0

Draining

0 Anomalous

► Distribution of targets by Availability Zone (AZ)

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

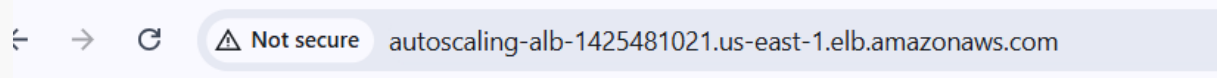
● Copy dns name from load balancer

.7K	<b>VPC</b> <a href="#">vpc-0ad3c0b33fec285e</a>	<b>Load balancer IP address type</b> IPv4
	<b>Availability Zones</b> <a href="#">subnet-0e890e6d482e183aa</a> us-east-1a (use1-az4) <a href="#">subnet-01e8c875b370cd0aa</a> us-east-1b (use1-az6)	<b>Date created</b> November 4, 2025, 17:02 (UTC+05:30)
loadbalancer/app/a	<b>DNS name</b> <a href="#">Info</a> <a href="#">autoscaling-alb-1425481021.us-east-1.elb.amazonaws.com</a> (A Record)	

✓ DNS name copied

Resource map
Security
Monitoring
Integrations
Attributes
Ca >

- Paste in local browser



## Apache on Public Instance

- 
- It is on load balancer
- 9 . Store application load balancer logs in S3.
- Navigate to s3 bucket
- Create a bucket enable block all ip
- Open bucket and click permission
- Edit and give script

✓ Successfully edited bucket policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSApplicationLoadBalancerAccessLogs",
      "Effect": "Allow",
      "Principal": {
        "Service": "logdelivery.elasticloadbalancing.amazonaws.com"
      },
      "Action": "s3:PutObject",
      "Resource": "arn:aws:s3:::asg-autoscaling/AWSLogs/414691912691/*"
    }
  ]
}
```

- 
- Now navigate to , ec2 > load balancer,
- Edit attributes
- Click access logs
- Click s3 bucket add existing bucket
- Can monitoring logs in > load balancer > below the attributes

aws EC2 > Load balancers > autoscaling-alb

- ▼ **Images**
  - AMIs
  - AMI Catalog
- ▼ **Elastic Block Store**
  - Volumes
  - Snapshots
  - Lifecycle Manager
- ▼ **Network & Security**
  - Security Groups
  - Elastic IPs
  - Placement Groups
  - Key Pairs
  - Network Interfaces
- ▼ **Load Balancing**
  - Load Balancers
  - Target Groups
  - Trust Stores
- ▼ **Auto Scaling**

**Preserve host header**  
Off

**Availability Zone routing configuration**

**Cross-zone load balancing**  
On

**Protection**

**Deletion protection**  
Off

**Monitoring**

**Access logs**  
S3 location: [asg-autoscaling](#)

- Can find the logs in s3 buckets

**asg-autoscaling** [Info](#)

**Objects** | Metadata | Properties | Permissions | Metrics | Management | Access Points

**Objects (1)**

[Refresh](#) [Copy S3 URI](#) [Copy URL](#) [Download](#) [Open](#) [Delete](#) [Actions](#) [Create folder](#)

[Upload](#)

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For o your objects, you'll need to explicitly grant them permissions. [Learn more](#)

<input type="checkbox"/>	Name	Type	Last modified	Size	Storage
<input type="checkbox"/>	<a href="#">AWSLogs/</a>	Folder	-	-	-

- 10 . Store the VPC flow logs in a CloudWatch log group.
- Navigate to vpc
- Select vpc
- Below find flow logs
- And create and add , destination and time

## Flow log settings

### Name - optional

autoscaling-flow-logs

### 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

- 
- Navigate to cloud watch and create a log group
- And return back to vpc and refresh you can see cloudwatch log group
- Select log group
- Select new role
- And then create

512ec5c0b9daa913

✓ Successfully created flow log for the following resource:  
vpc-0ad3c0b33fecd285e

## fl-0512ec5c0b9daa913 / autoscaling-flow-logs

Active

### Details

<b>Flow Log ID</b> fl-0512ec5c0b9daa913	<b>Destination Type</b> cloud-watch-logs	<b>Traffic Type</b> All	<b>File Format</b> -
<b>Name</b> autoscaling-flow-logs	<b>Destination Name</b> <a href="#">autoscaling-logs</a>	<b>Max Aggregation Interval</b> 10 minutes	<b>Hive Compatible Partitions</b> -
<b>State</b> Active	<b>IAM Role</b> <a href="#">arn:aws:iam::414691912691:role/service-role/VPCFlowLogs-Cloudwatch-1762258515835</a>	<b>Log Format</b> Default	<b>Partition Logs</b> -
<b>Creation Time</b> Tuesday, November 4, 2025 at 17:50:27 GMT+5:30	<b>Cross Account IAM Role</b> -		

- 
- Cerify in cloud watch

autoscaling-logs > eni-004a17a04063e9efb-all

Log group "autoscaling-logs" has been created.

You can use the filter bar below to search for and match terms, phrases, or values in your log events. [Learn more about filter patterns](#)

Filter events - press enter to search

1m 1h Local timezone Display

Timestamp	Message
2025-11-04T17:51:37.000+05:30	2 414691912691 eni-004a17a04063e9efb 204.76.203.219 10.0.1.179 51840 82 6 1 40 1762258897 1762258926 REJECT OK
2025-11-04T17:51:37.000+05:30	2 414691912691 eni-004a17a04063e9efb 45.173.27.9 10.0.1.179 30967 443 6 1 52 1762258897 1762258926 REJECT OK
2025-11-04T17:51:37.000+05:30	2 414691912691 eni-004a17a04063e9efb 45.173.27.59 10.0.1.179 3588 443 6 1 52 1762258897 1762258926 REJECT OK
2025-11-04T17:51:37.000+05:30	2 414691912691 eni-004a17a04063e9efb 10.0.1.87 10.0.1.179 80 12300 6 5 570 1762258897 1762258926 ACCEPT OK
2025-11-04T17:51:37.000+05:30	2 414691912691 eni-004a17a04063e9efb 45.173.24.144 10.0.1.179 7990 443 6 1 52 1762258897 1762258926 REJECT OK
2025-11-04T17:51:37.000+05:30	2 414691912691 eni-004a17a04063e9efb 45.173.26.40 10.0.1.179 29348 443 6 1 52 1762258897 1762258926 REJECT OK
2025-11-04T17:51:37.000+05:30	2 414691912691 eni-004a17a04063e9efb 167.94.146.43 10.0.1.179 29618 48719 6 1 60 1762258897 1762258926 REJECT ...
2025-11-04T17:51:37.000+05:30	2 414691912691 eni-004a17a04063e9efb 45.173.26.220 10.0.1.179 40691 443 6 1 52 1762258897 1762258926 REJECT OK
2025-11-04T17:51:37.000+05:30	2 414691912691 eni-004a17a04063e9efb 45.173.27.104 10.0.1.179 19105 443 6 1 52 1762258897 1762258926 REJECT OK
2025-11-04T17:51:37.000+05:30	2 414691912691 eni-004a17a04063e9efb 45.173.25.238 10.0.1.179 11193 443 6 1 52 1762258897 1762258926 REJECT OK

No newer events at this moment. Auto retry paused. [Resume](#)

[Back to top](#)

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

- Cloud watch
- Create new dashboard
- Add ec2 in metrics
- Pre instance select cpu utilization add
- Add instance id in graphed metrics

1h 3h 12h 1d

0.26 %

CPUUtilization

Options Source

Instance • InstanceId: i-0bc2c

**Edit details**

To apply values to all graphed metrics, click on

AccountId Region

414691912691 us-east-1

Namespace Metric name

AWS/EC2 CPUUtilization

InstanceId

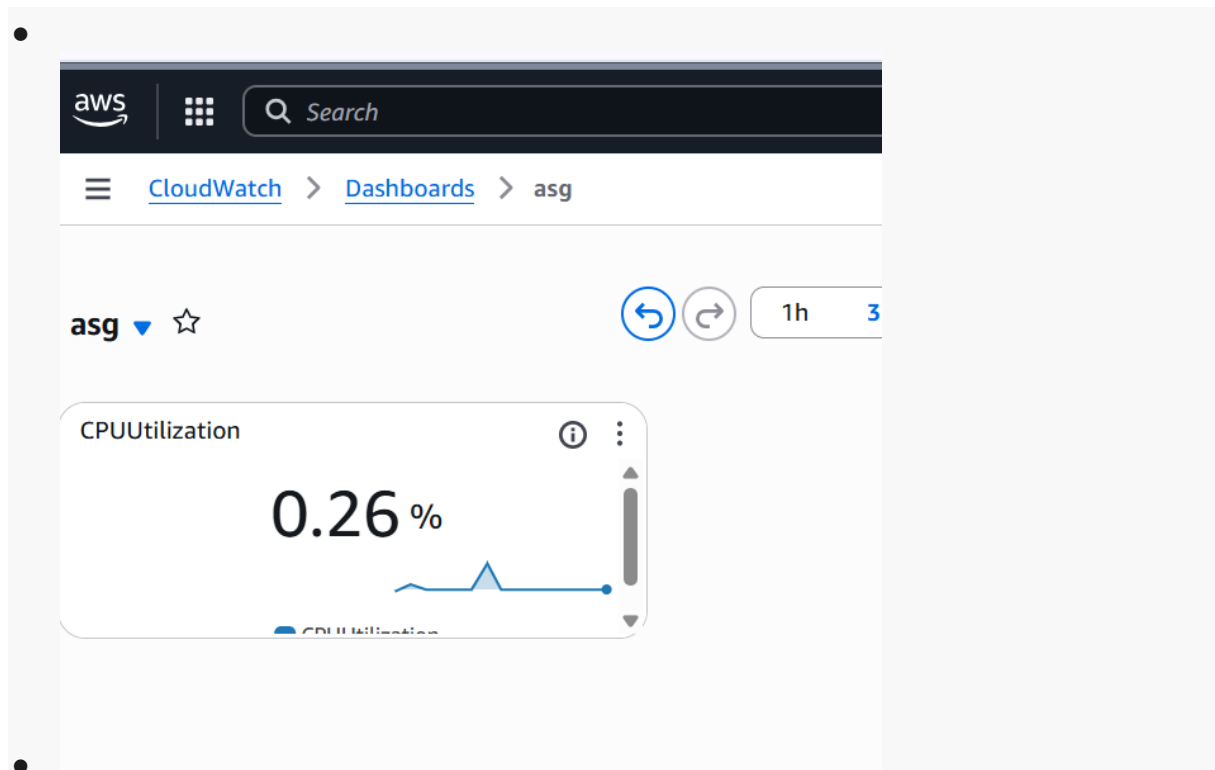
i-0bc2cb72c8ca6f030

Cancel Update

Show all actions (6)

Cancel Create widget

- Created a dashboard for instance

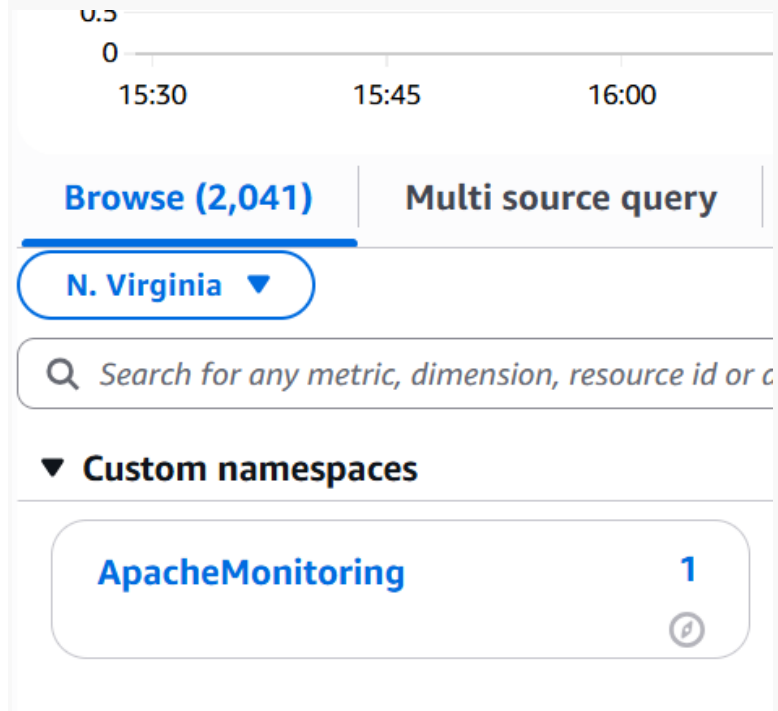


- 
- Monitor apache is running or not
- Open cli check aws is configured or not
- Now create file and add script for monitor apache running or not
  - `#!/bin/bash`
  - 
  - `# Check Apache (httpd) status`
  - `status=$(systemctl is-active httpd)`
  - 
  - `if [ "$status" == "active" ]; then`
  - `metric_value=1`
  - `else`
  - `metric_value=0`
  - `fi`
  - 
  - `# Push the metric to CloudWatch`
  - `aws cloudwatch put-metric-data \`
  - `--metric-name ApacheServiceStatus \`
  - `--namespace "ApacheMonitoring" \`
  - `--value $metric_value \`
  - `--region us-east-1`
  - Install corntab and edit it
  - By `sudo corntab -e`
  - Add `* /5 * * * *`



- Run this command in CLI to create a custom namespace in GUI

```
aws cloudwatch put-metric-data \
  --metric-name ApacheServiceStatus \
  --namespace "ApacheMonitoring" \
  --value 1 \
  --region us-east-1
```

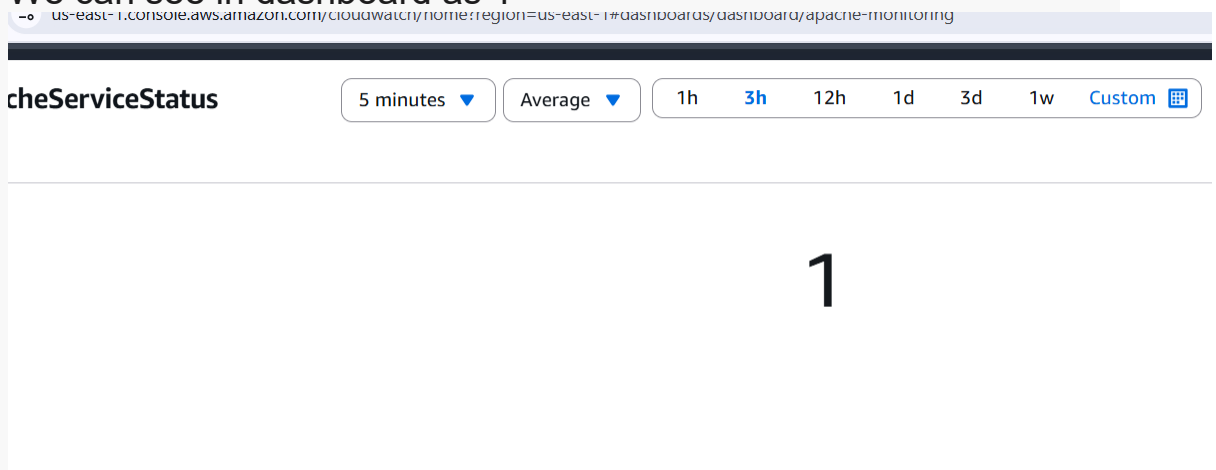


- As apache running in cli
-

```
[ec2-user@ip-10-0-1-87 ~]$ aws cloudwatch put-metric-data \
--metric-name ApacheServiceStatus \
--namespace "ApacheMonitoring" \
--value 1 \
--region us-east-1
[ec2-user@ip-10-0-1-87 ~]$ sudo systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset:
   Active: active (running) since Tue 2025-11-04 11:46:20 UTC; 1h 15min ago
     Docs: man:httpd.service(8)
  Main PID: 25951 (httpd)
    Status: "Total requests: 332; Idle/Busy workers 100/0;Requests/sec: 0.05
    Tasks: 177 (limit: 1053)
   Memory: 16.2M
      CPU: 4.273s
   CGroup: /system.slice/httpd.service
           └─25951 /usr/sbin/httpd -DFOREGROUND
             └─25952 /usr/sbin/httpd -DFOREGROUND
               └─25954 /usr/sbin/httpd -DFOREGROUND
                 └─25955 /usr/sbin/httpd -DFOREGROUND
                   └─25956 /usr/sbin/httpd -DFOREGROUND

Nov 04 11:46:20 ip-10-0-1-87.ec2.internal systemd[1]: Starting httpd.service
Nov 04 11:46:20 ip-10-0-1-87.ec2.internal systemd[1]: Started httpd.service
Nov 04 11:46:20 ip-10-0-1-87.ec2.internal httpd[25951]: Server configured, 1b
lines 1-19/19 (END)
```

- We can see in dashboard as 1



- 12. If CPU utilization is more than 70%, then it should trigger auto scaling and launch new instance.
- Open aws console
- Navigate to launch template
- Give configuration as needed for autoscaling

## ▼ Network settings [Info](#)

### Subnet [Info](#)

subnet-0e890e6d482e183aa Public-1A-k  
 VPC: vpc-0ad3c0b33fec285e Owner: 414691912691  
 Availability Zone: us-east-1a (use1-az4) Zone type: Availability Zone  
 IP addresses available: 248 CIDR: 10.0.1.0/24

[Create new subnet](#)

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

### Availability Zone [Info](#)

us-east-1a use1-az4

[Enable additional zones](#)

### Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Select existing security group

☐ Create security group

### Common security groups [Info](#)

Select security groups

default sg-0afe7e3379e26dce8  
 VPC: vpc-0ad3c0b33fec285e

[Compare security group rules](#)

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

- Now navigagte autoscaling and create new
- Add launch template to this
- Add vpc and 2 subnets atleast

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling select the default subnets are suitable for getting started quickly.

### VPC

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

vpc-0ad3c0b33fec285e (autoscaling)  
 10.0.0.0/16

[Create a VPC](#)

### Availability Zones and subnets

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

Select Availability Zones and subnets

use1-az4 (us-east-1a) | subnet-0e890e6d482e183aa (Public-1A-k)  
 10.0.1.0/24

use1-az6 (us-east-1b) | subnet-01e8c875b370cd0aa (public-av-1b-k)  
 10.0.2.0/24

[Create a subnet](#)

### Availability Zone distribution - new

Auto Scaling automatically balances instances across Availability Zones. If launch failures occur in a zone

- 
- Add existing load balancer
-

EC2 > Auto Scaling groups > Create Auto Scaling group

Configure group size and scaling

Step 5 - optional

Add notifications

Step 6 - optional

Add tags

Step 7

Review

Select load balancing 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.

Attach to an existing load balancer

Select the load balancers to attach

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

☐ Choose from Classic Load Balancers

Existing load balancer target groups

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

Select target groups

asg | HTTP  
Application Load Balancer: autoscaling-alb

VPC Lattice integration options [Info](#)

roups > Create Auto Scaling group

1

Scaling [Info](#)

You can resize your Auto Scaling group manually or automatically to meet changes in demand.

Scaling limits

Set limits on how much your desired capacity can be increased or decreased.

Min desired capacity

1

Equal or less than desired capacity

Max desired capacity

1

Equal or greater than desired capacity

Automatic scaling - optional

Choose whether to use a target tracking policy [Info](#)

You can set up other metric-based scaling policies and scheduled scaling after creating your Auto Scaling group.

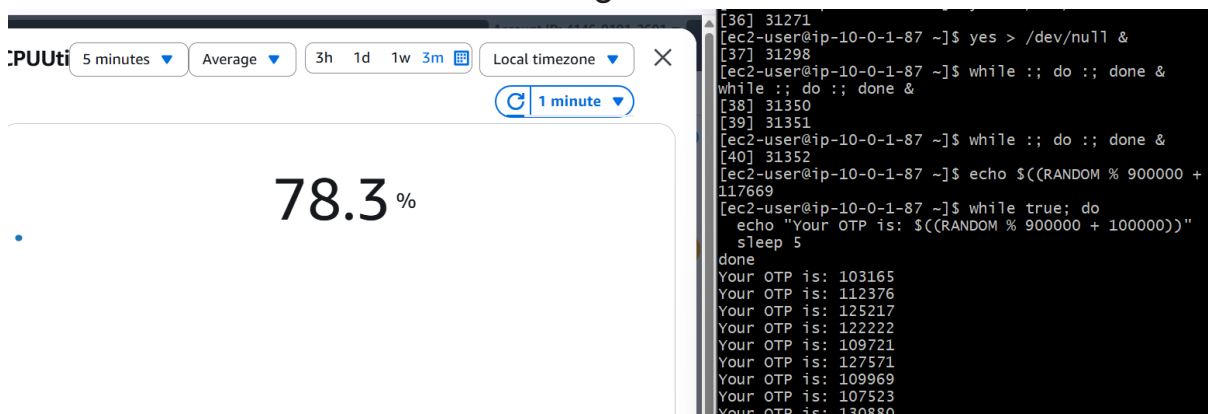
☐ No scaling policies  
Your Auto Scaling group will remain at its initial size and will not dynamically resize to meet demand.

☒ Target tracking scaling policy  
Choose a CloudWatch metric and target value and let the the desired capacity in proportion to the metric's value.

Scaling policy name

Target Tracking Policy

Load increased in monitor is working



So new instance launched automatically as its cpu usage increased above 50%

Instances (3) [Info](#)

Last updated less than a minute ago

Refresh

Connect

Instance state

Actions

Launch instances

Find Instance by attribute or tag (case-sensitive)

Running

< 1 >

Settings

<input type="checkbox"/>	Name <a href="#">🔗</a>	Instance ID	Instance state <a href="#">📄</a>	Instance type <a href="#">📄</a>	Status check	Alarm status	Availability Zone
<input type="checkbox"/>	autoscaling-ec2	<a href="#">i-0bc2cb72c8ca6f030</a>	<div>Running</div> <div><a href="#">📄</a> <a href="#">🔍</a></div>	t3.micro	<div>3/3 checks passed</div>	<a href="#">View alarms</a> <a href="#">+</a>	us-east-1a
<input type="checkbox"/>	autosacding-pr...	<a href="#">i-01f12a13e564aefbb</a>	<div>Running</div> <div><a href="#">📄</a> <a href="#">🔍</a></div>	t3.micro	<div>3/3 checks passed</div>	<a href="#">View alarms</a> <a href="#">+</a>	us-east-1a
<input type="checkbox"/>		<a href="#">i-058024f967ab29267</a>	<div>Running</div> <div><a href="#">📄</a> <a href="#">🔍</a></div>	t2.micro	<div>2/2 checks passed</div>	<a href="#">View alarms</a> <a href="#">+</a>	us-east-1a