7/29/2022

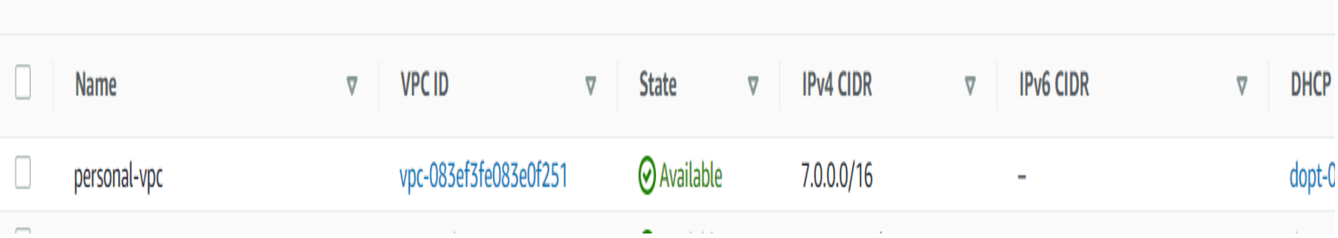
Project-01

Configure more than one webserver with proper load balancing, auto scaling and SSL configuration.

Sumit Mishra
SIC: 190310286

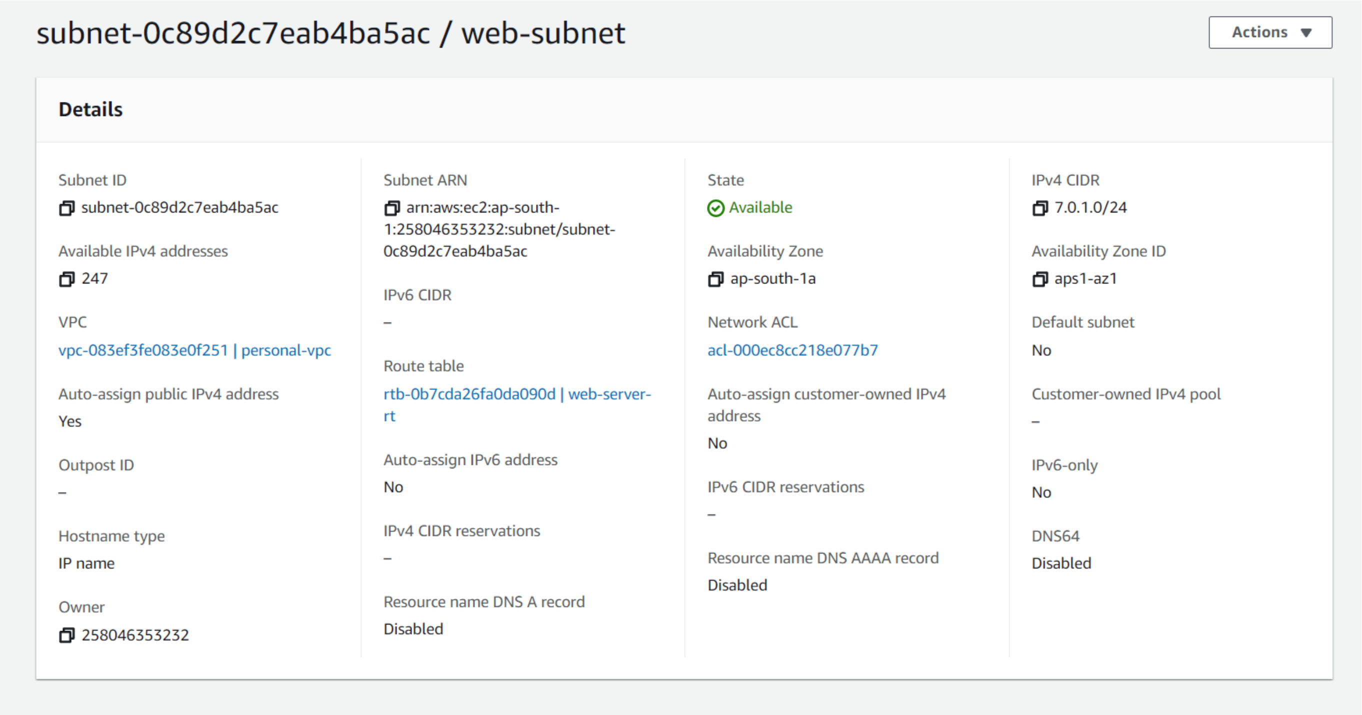
1. Creating and configuring a VPC.

1. Create a VPC



☐	Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP
☐	personal-vpc	vpc-083ef3fe083e0f251	✓ Available	7.0.0.0/16	-	dopt-0

2. Create a subnet inside the VPC to host servers.



subnet-0c89d2c7eab4ba5ac / web-subnet

Details

Subnet ID
subnet-0c89d2c7eab4ba5ac

Available IPv4 addresses
247

VPC
vpc-083ef3fe083e0f251 | personal-vpc

Auto-assign public IPv4 address
Yes

Outpost ID
–

Hostname type
IP name

Owner
258046353232

Subnet ARN
arn:aws:ec2:ap-south-1:258046353232:subnet/subnet-0c89d2c7eab4ba5ac

IPv6 CIDR
–

Route table
rtb-0b7cda26fa0da090d | web-server-rt

Auto-assign IPv6 address
No

IPv4 CIDR reservations
–

Resource name DNS A record
Disabled

State
✓ Available

Availability Zone
ap-south-1a

Network ACL
acl-000ec8cc218e077b7

Auto-assign customer-owned IPv4 address
No

IPv6 CIDR reservations
–

Resource name DNS AAAA record
Disabled

IPv4 CIDR
7.0.1.0/24

Availability Zone ID
aps1-az1

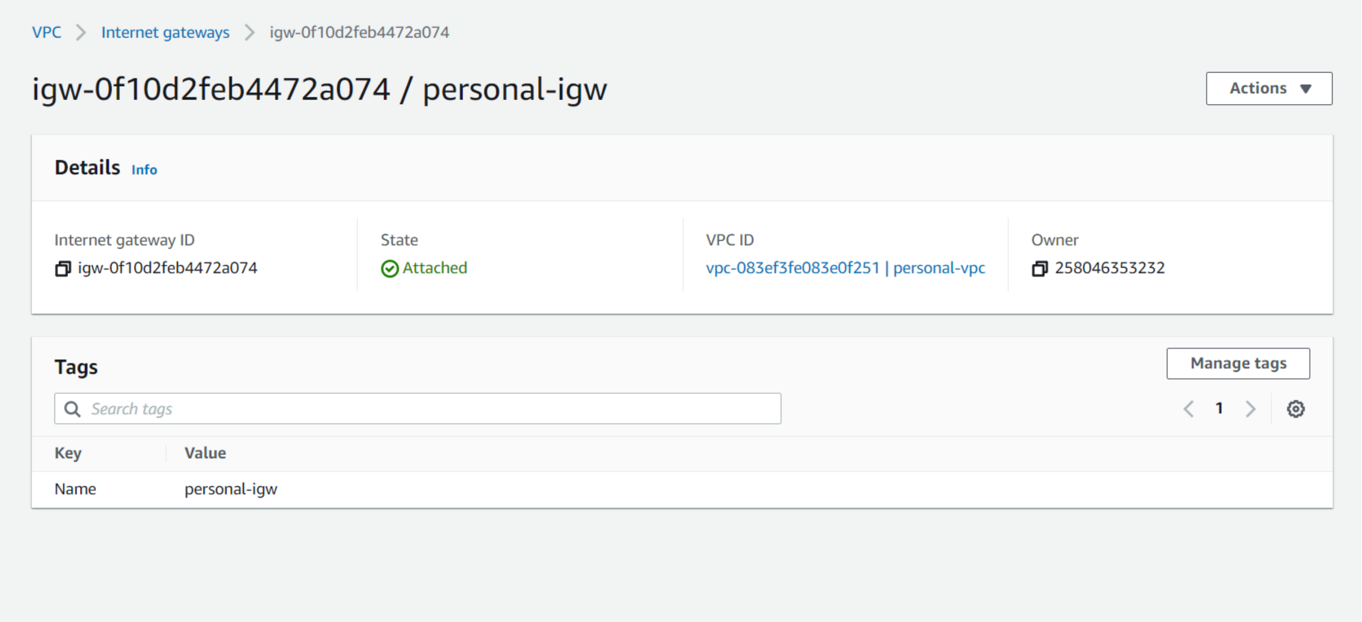
Default subnet
No

Customer-owned IPv4 pool
–

IPv6-only
No

DNS64
Disabled

3. Created an Internet Gateway for the servers to access the internet through it.



VPC > Internet gateways > igw-0f10d2feb4472a074

igw-0f10d2feb4472a074 / personal-igw

Details Info

Internet gateway ID
igw-0f10d2feb4472a074

State
✓ Attached

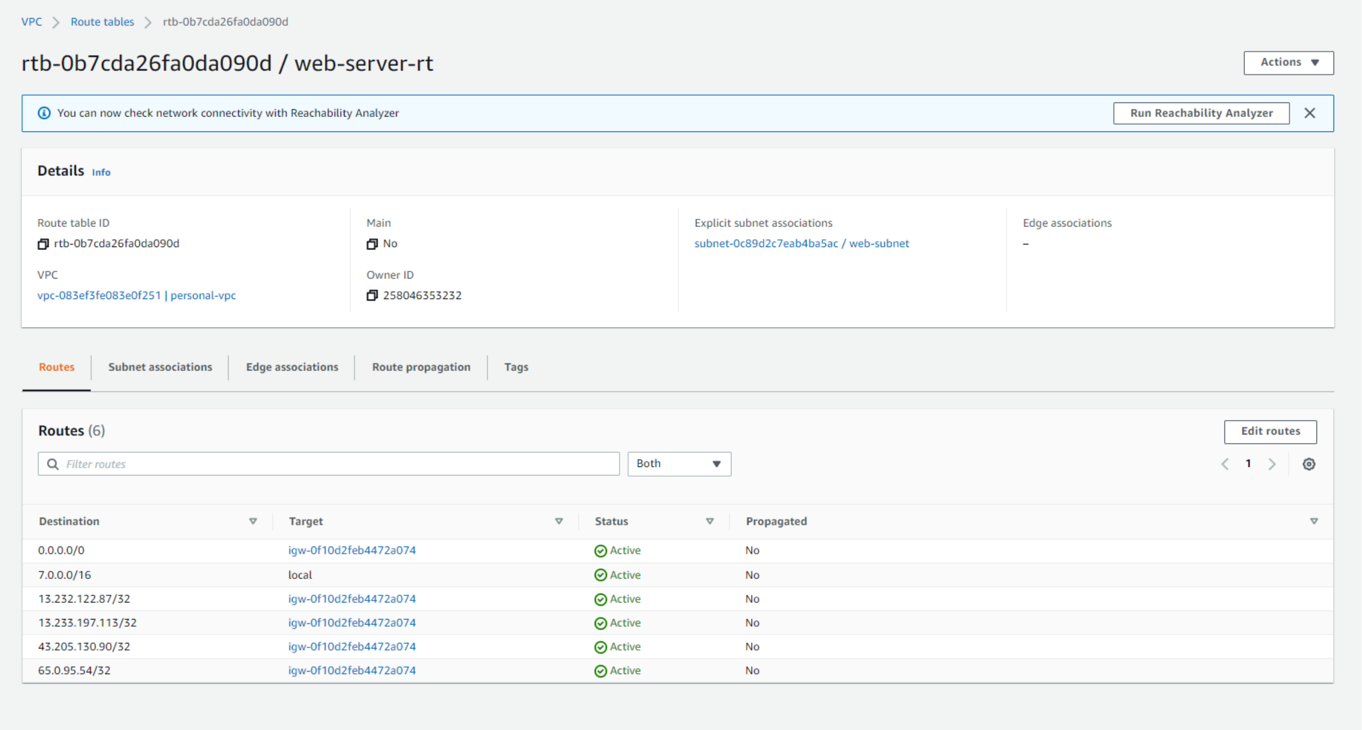
VPC ID
vpc-083ef3fe083e0f251 | personal-vpc

Owner
258046353232

Tags

Key	Value
Name	personal-igw

4. Created and configured the route table for the subnet created.



rtb-0b7cda26fa0da090d / web-server-rt

You can now check network connectivity with Reachability Analyzer

Details Info

Route table ID: rtb-0b7cda26fa0da090d

VPC: vpc-083ef3fe083e0f251 | personal-vpc

Main: No

Owner ID: 258046353232

Explicit subnet associations: subnet-0c89d2c7eab4ba5ac / web-subnet

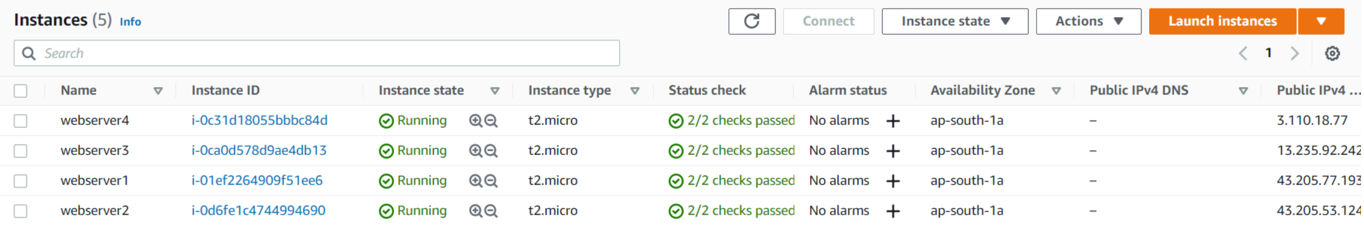
Edge associations: –

Routes (6)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0f10d2feb4472a074	Active	No
7.0.0.0/16	local	Active	No
13.232.122.87/32	igw-0f10d2feb4472a074	Active	No
13.233.197.113/32	igw-0f10d2feb4472a074	Active	No
43.205.130.90/32	igw-0f10d2feb4472a074	Active	No
65.0.95.54/32	igw-0f10d2feb4472a074	Active	No

2. Configuring Web servers, domain, hosting.

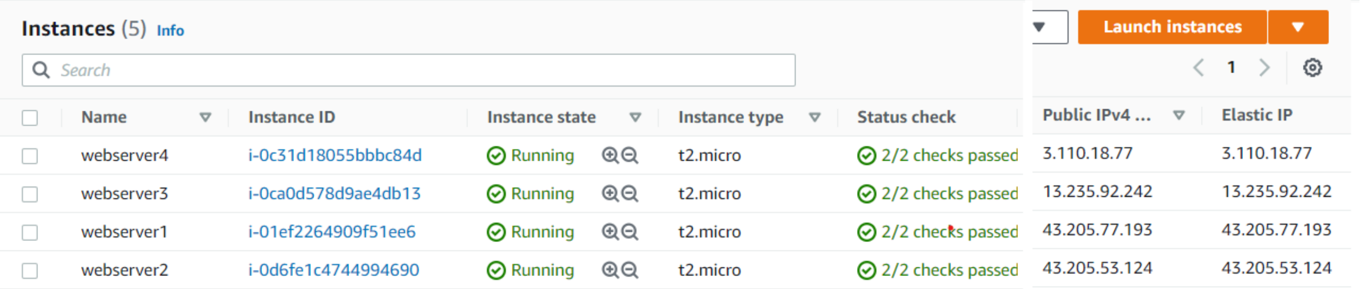
1. Launching 4 EC2 instances with Linux AMI.



Instances (5) Info

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
□	webserver4	i-0c31d18055bbbc84d	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	–	3.110.18.77
□	webserver3	i-0ca0d578d9ae4db13	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	–	13.235.92.242
□	webserver1	i-01ef2264909f51ee6	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	–	43.205.77.193
□	webserver2	i-0d6fe1c4744994690	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	–	43.205.53.124

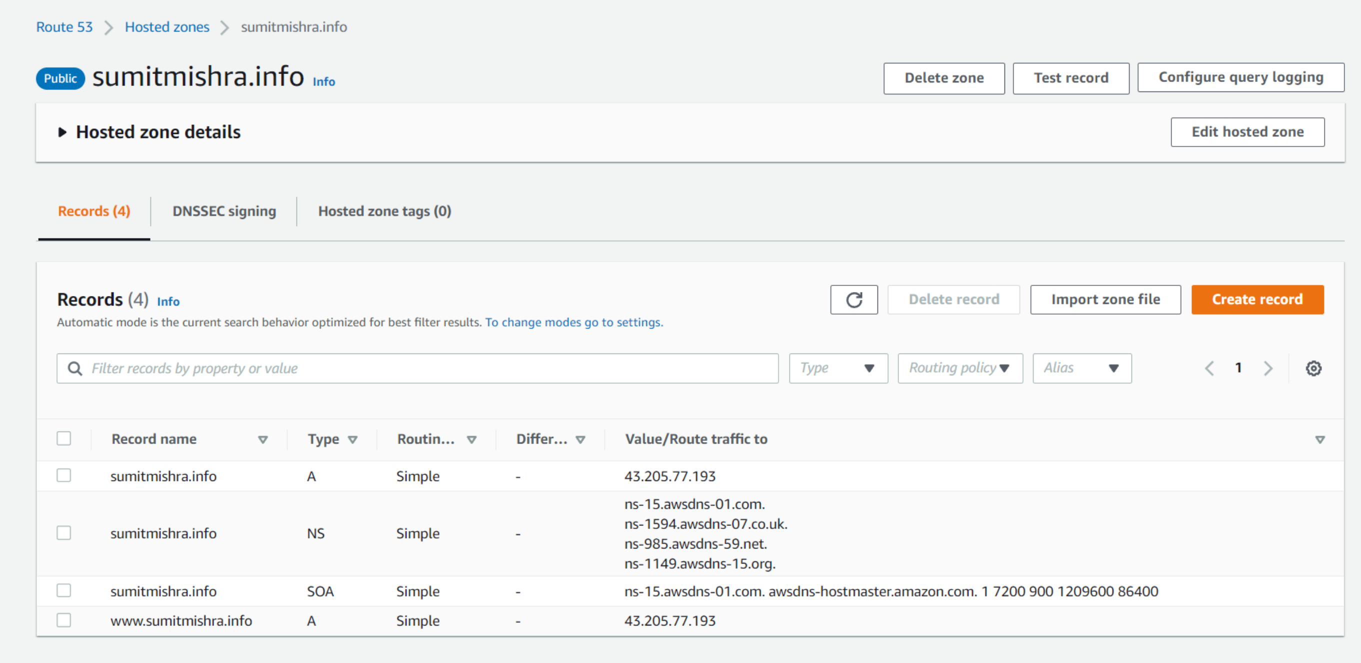
2. Assigning Elastic IP addresses to all the four servers.



Instances (5) Info

□	Name	Instance ID	Instance state	Instance type	Status check	Public IPv4 ...	Elastic IP
□	webserver4	i-0c31d18055bbbc84d	Running	t2.micro	2/2 checks passed	3.110.18.77	3.110.18.77
□	webserver3	i-0ca0d578d9ae4db13	Running	t2.micro	2/2 checks passed	13.235.92.242	13.235.92.242
□	webserver1	i-01ef2264909f51ee6	Running	t2.micro	2/2 checks passed	43.205.77.193	43.205.77.193
□	webserver2	i-0d6fe1c4744994690	Running	t2.micro	2/2 checks passed	43.205.53.124	43.205.53.124

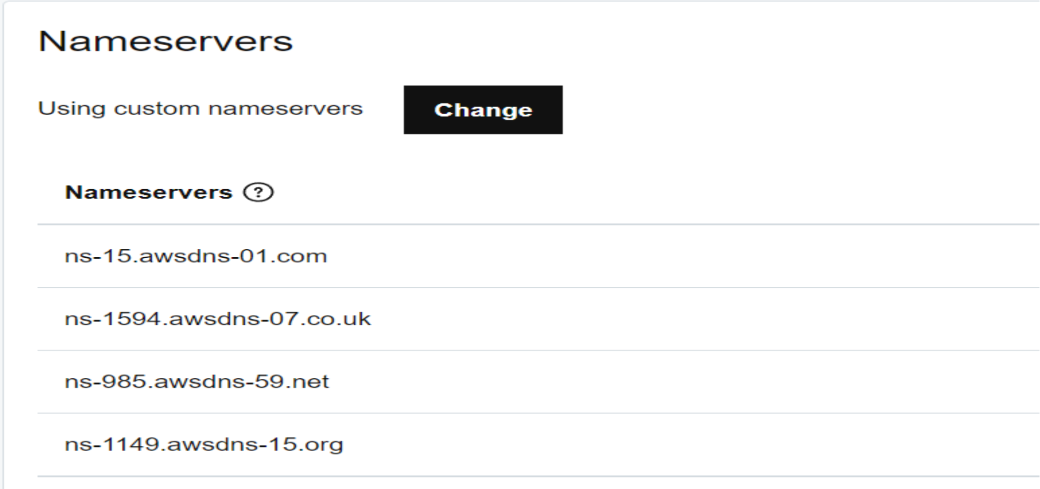
3. Creating a Hosted zone in AWS Route 53 and adding hosting records for root domain(sumitmishra.info) and sub-domain(www.sumitmishra.info).



Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.

□	Record name	Type	Routin...	Differ...	Value/Route traffic to
□	sumitmishra.info	A	Simple	-	43.205.77.193
□	sumitmishra.info	NS	Simple	-	ns-15.awsdns-01.com. ns-1594.awsdns-07.co.uk. ns-985.awsdns-59.net. ns-1149.awsdns-15.org.
□	sumitmishra.info	SOA	Simple	-	ns-15.awsdns-01.com. awsdns-hostmaster.amazon.com. 1 7200 900 1209600 86400
□	www.sumitmishra.info	A	Simple	-	43.205.77.193

4. Replacing Nameservers in GoDaddy Domain (sumitmishra.info) with AWS Route 53 Nameservers.



Using custom nameservers

Nameservers

ns-15.awsdns-01.com

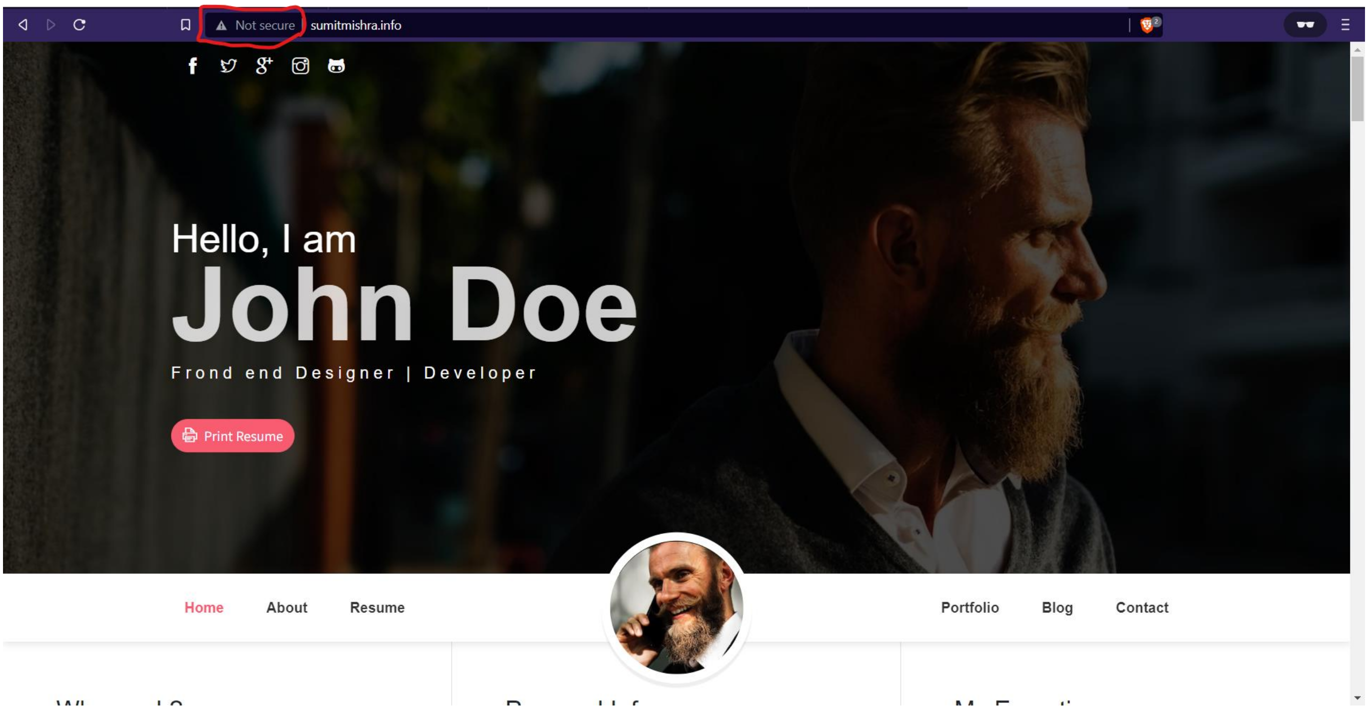
ns-1594.awsdns-07.co.uk

ns-985.awsdns-59.net

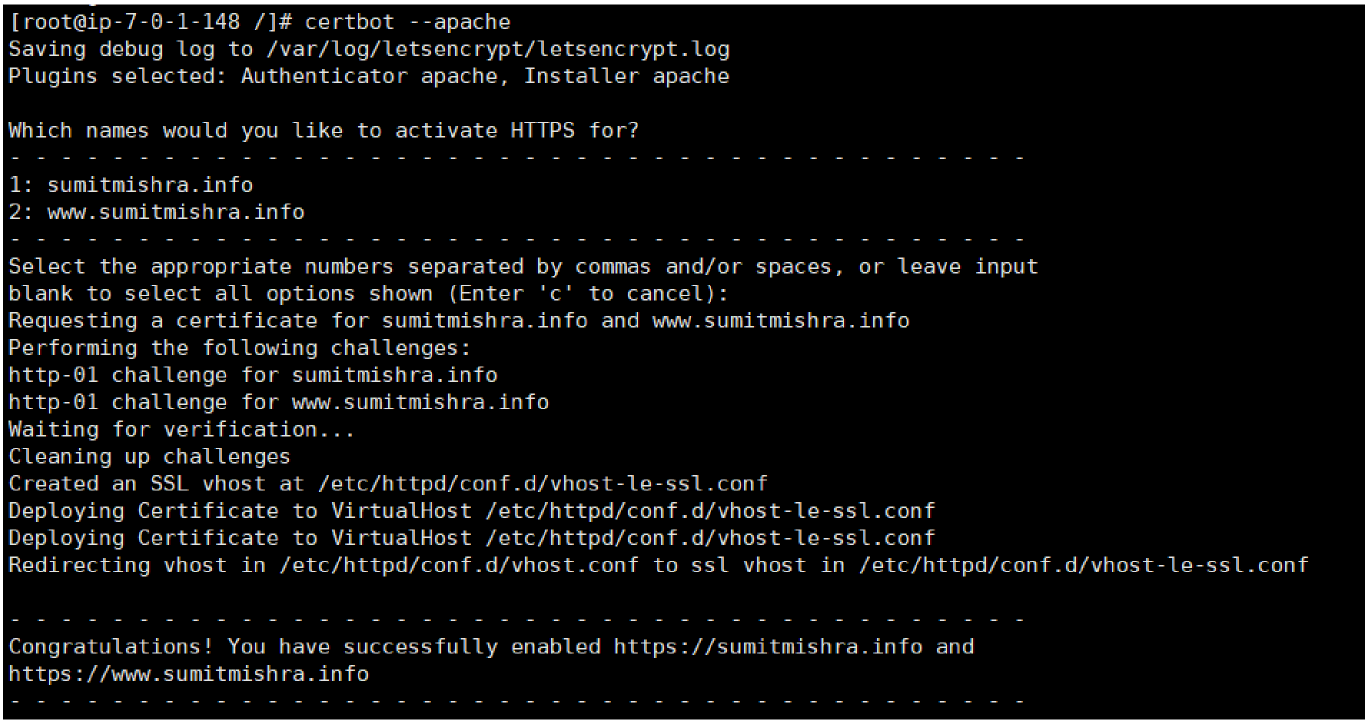
ns-1149.awsdns-15.org

3. Configuring SSL/TLS certificate for a webserver using let us encrypt Apache certbot.

1. Opening the website hosted in webserver one without SSL/TLS certificate we get the not secured warning in the left most side of URL bar.



2. Now configuring the SSL certificate through let’s encrypt using ssh client.

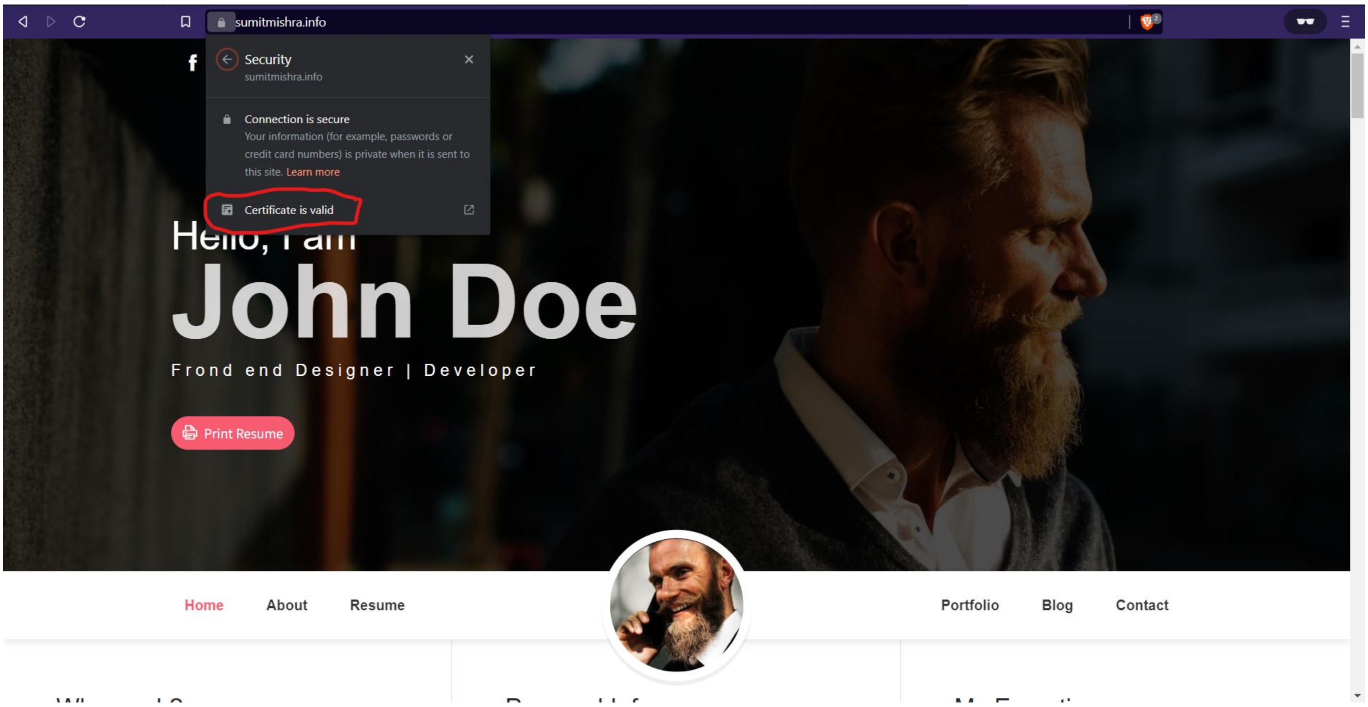


```
[root@ip-7-0-1-148 /]# certbot --apache
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache

Which names would you like to activate HTTPS for?
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
1: sumitmishra.info
2: www.sumitmishra.info
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel):
Requesting a certificate for sumitmishra.info and www.sumitmishra.info
Performing the following challenges:
http-01 challenge for sumitmishra.info
http-01 challenge for www.sumitmishra.info
Waiting for verification...
Cleaning up challenges
Created an SSL vhost at /etc/httpd/conf.d/vhost-le-ssl.conf
Deploying Certificate to VirtualHost /etc/httpd/conf.d/vhost-le-ssl.conf
Deploying Certificate to VirtualHost /etc/httpd/conf.d/vhost-le-ssl.conf
Redirecting vhost in /etc/httpd/conf.d/vhost.conf to ssl vhost in /etc/httpd/conf.d/vhost-le-ssl.conf

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
Congratulations! You have successfully enabled https://sumitmishra.info and
https://www.sumitmishra.info
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

3. Now again hitting the URL sumitmishra.info and www.sumitmishra.info to see that the website shows secured in the leftmost area of the URL bar, this means that SSL certificate has been enabled.



sumitmishra.info

Security
sumitmishra.info

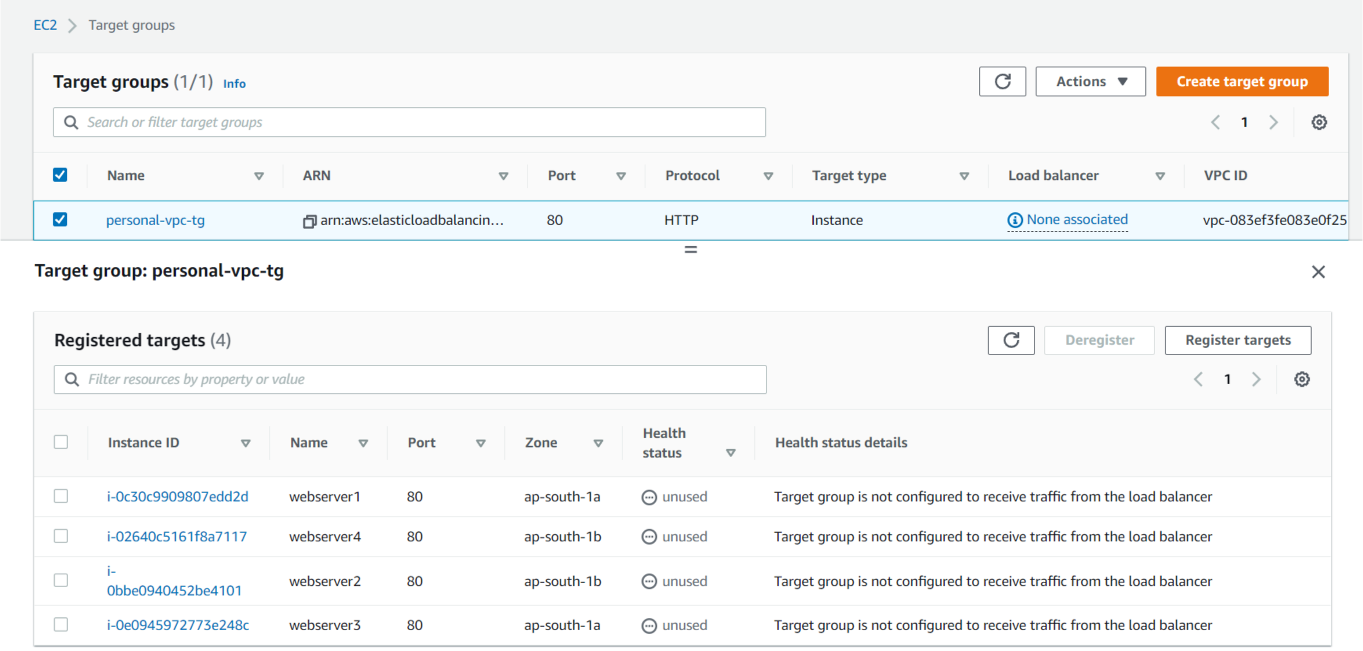
Connection is secure
Your information (for example, passwords or credit card numbers) is private when it is sent to this site. Learn more

Certificate is valid

Hello, I am
John Doe
Frond end Designer | Developer

4. Creating a target group using the four servers and configuring load balancing along with SSL certificate using let’s encrypt for the load balancer.

1. Creating a target group.



EC2 > Target groups

Target groups (1/1) Info

Actions
Create target group
Search or filter target groups

☑	Name	ARN	Port	Protocol	Target type	Load balancer	VPC ID
☑	personal-vpc-tg	arn:aws:elasticloadbalancin...	80	HTTP	Instance	None associated	vpc-083ef3fe083e0f25

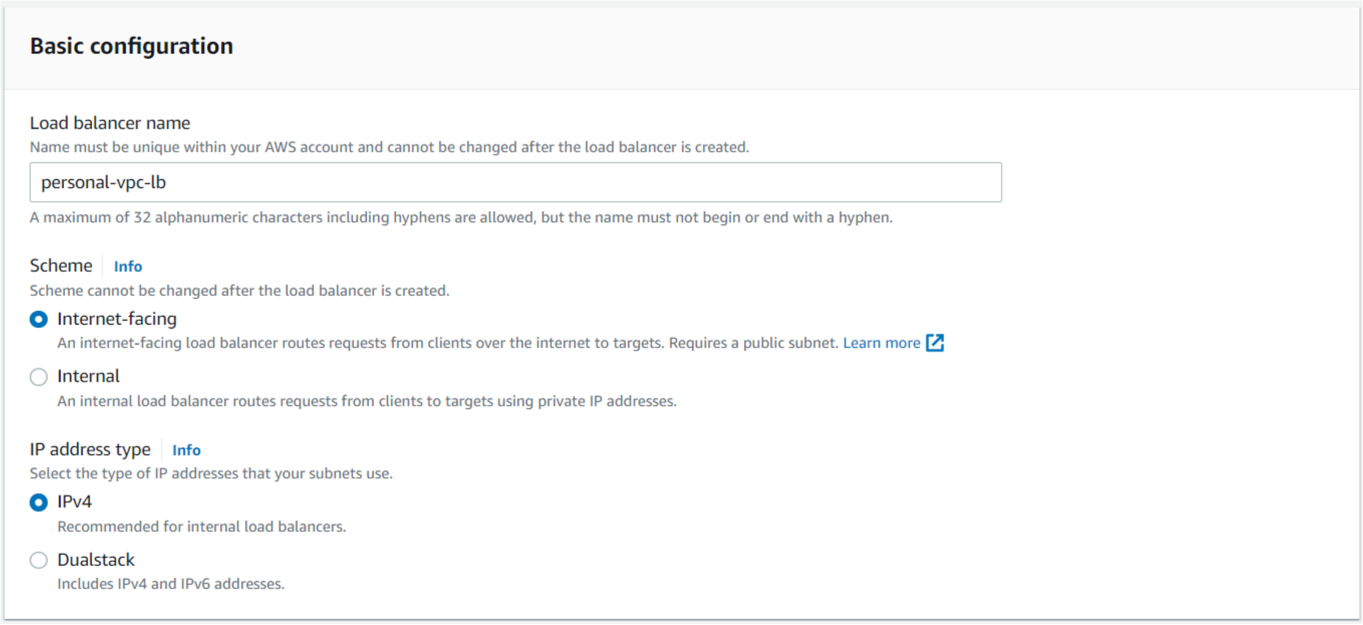
Target group: personal-vpc-tg

Registered targets (4)

Deregister
Register targets
Filter resources by property or value

□	Instance ID	Name	Port	Zone	Health status	Health status details
□	i-0c30c9909807edd2d	webserver1	80	ap-south-1a	unused	Target group is not configured to receive traffic from the load balancer
□	i-02640c5161f8a7117	webserver4	80	ap-south-1b	unused	Target group is not configured to receive traffic from the load balancer
□	i-0bbe0940452be4101	webserver2	80	ap-south-1b	unused	Target group is not configured to receive traffic from the load balancer
□	i-0e0945972773e248c	webserver3	80	ap-south-1a	unused	Target group is not configured to receive traffic from the load balancer

2. Creating a load balancer.



Basic configuration

Load balancer name

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

personal-vpc-lb

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

Scheme | Info

Scheme cannot be changed after the load balancer is created.

● Internet-facing
An internet-facing load balancer routes requests from clients over the internet to targets. Requires a public subnet. Learn more

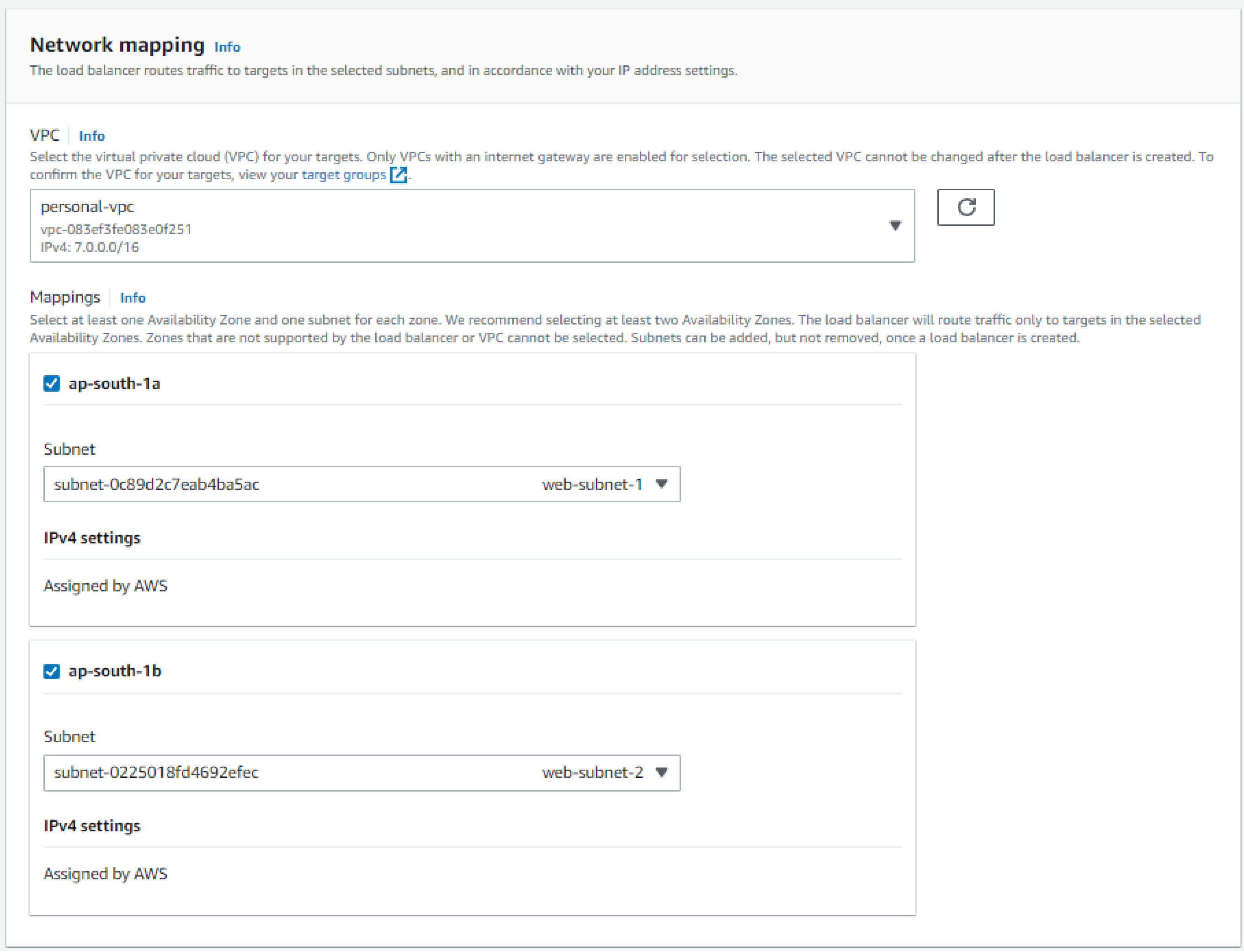
○ Internal
An internal load balancer routes requests from clients to targets using private IP addresses.

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. Only VPCs with an internet gateway are enabled for selection. The selected VPC cannot be changed after the load balancer is created. To confirm the VPC for your targets, view your target groups.

personal-vpc
vpc-083ef3fe083e0f251
IPv4: 7.0.0.0/16

Mappings | Info

Select at least one Availability Zone and one subnet for each zone. We recommend selecting at least two Availability Zones. The load balancer will route traffic only to targets in the selected Availability Zones. Zones that are not supported by the load balancer or VPC cannot be selected. Subnets can be added, but not removed, once a load balancer is created.

☑ **ap-south-1a**

Subnet

subnet-0c89d2c7eab4ba5ac web-subnet-1

IPv4 settings

Assigned by AWS

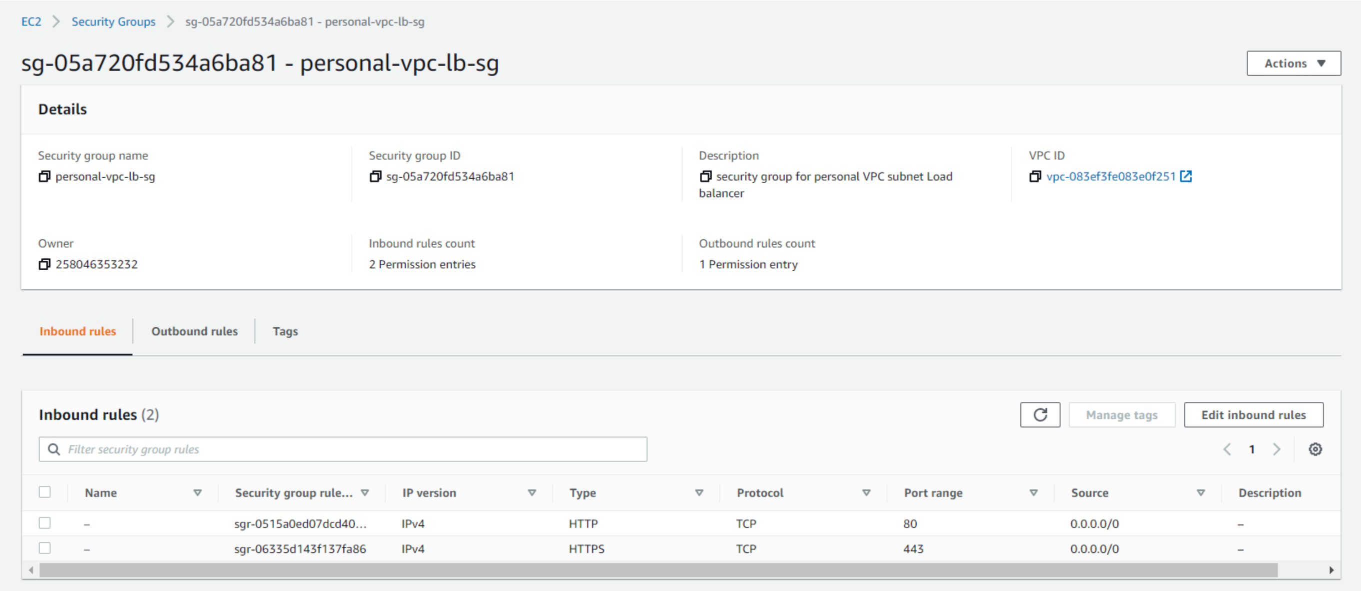
☑ **ap-south-1b**

Subnet

subnet-0225018fd4692efec web-subnet-2

IPv4 settings

Assigned by AWS



EC2 > Security Groups > sg-05a720fd534a6ba81 - personal-vpc-lb-sg

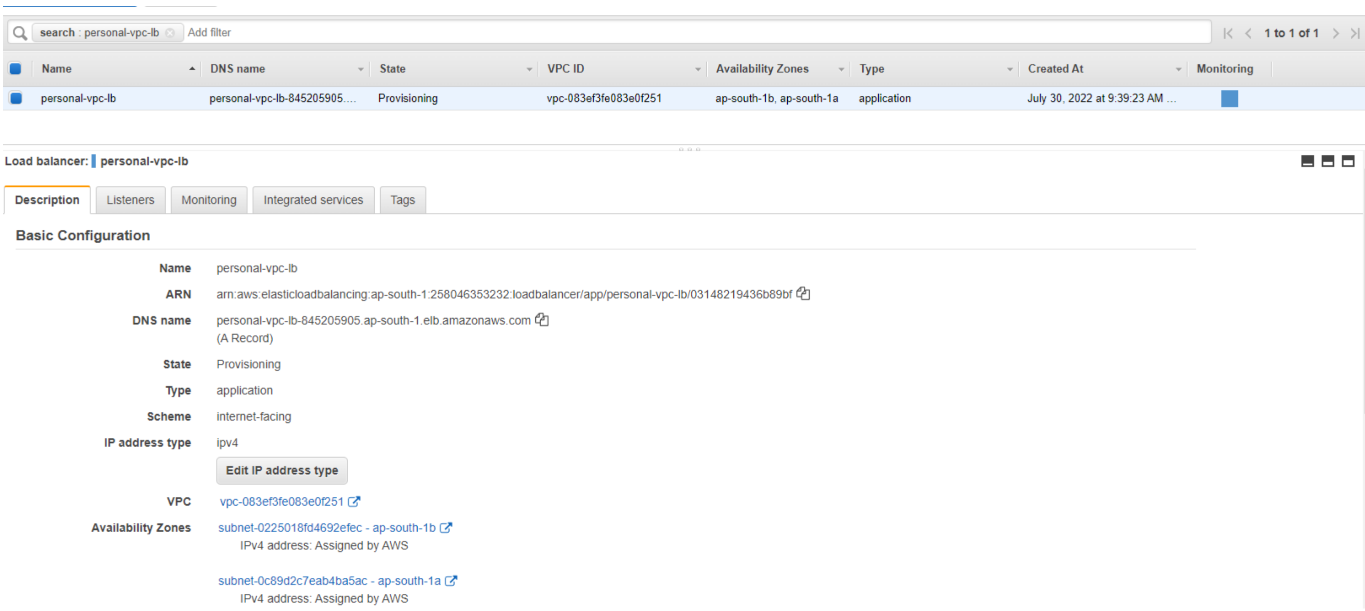
sg-05a720fd534a6ba81 - personal-vpc-lb-sg

Details

Security group name personal-vpc-lb-sg	Security group ID sg-05a720fd534a6ba81	Description security group for personal VPC subnet Load balancer	VPC ID vpc-083ef3fe083e0f251
Owner 258046353232	Inbound rules count 2 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules (2)

□	Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
□	–	sgr-0515a0ed07dcd40...	IPv4	HTTP	TCP	80	0.0.0.0/0	–
□	–	sgr-06335d143f137fa86	IPv4	HTTPS	TCP	443	0.0.0.0/0	–



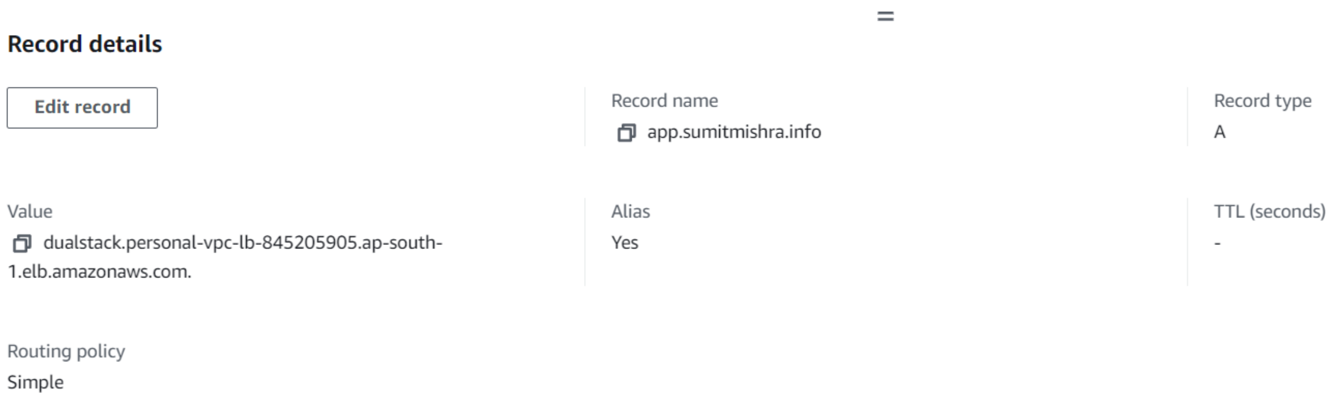
■	Name	DNS name	State	VPC ID	Availability Zones	Type	Created At	Monitoring
■	personal-vpc-lb	personal-vpc-lb-845205905....	Provisioning	vpc-083ef3fe083e0f251	ap-south-1b, ap-south-1a	application	July 30, 2022 at 9:39:23 AM ...	■

Load balancer: personal-vpc-lb

Basic Configuration

Name	personal-vpc-lb
ARN	arn:aws:elasticloadbalancing:ap-south-1:258046353232:loadbalancer/app/personal-vpc-lb/03148219436b89bf
DNS name	personal-vpc-lb-845205905.ap-south-1.elb.amazonaws.com (A Record)
State	Provisioning
Type	application
Scheme	internet-facing
IP address type	ipv4 Edit IP address type
VPC	vpc-083ef3fe083e0f251
Availability Zones	subnet-0225018fd4692efec - ap-south-1b IPv4 address: Assigned by AWS subnet-0c89d2c7eab4ba5ac - ap-south-1a IPv4 address: Assigned by AWS

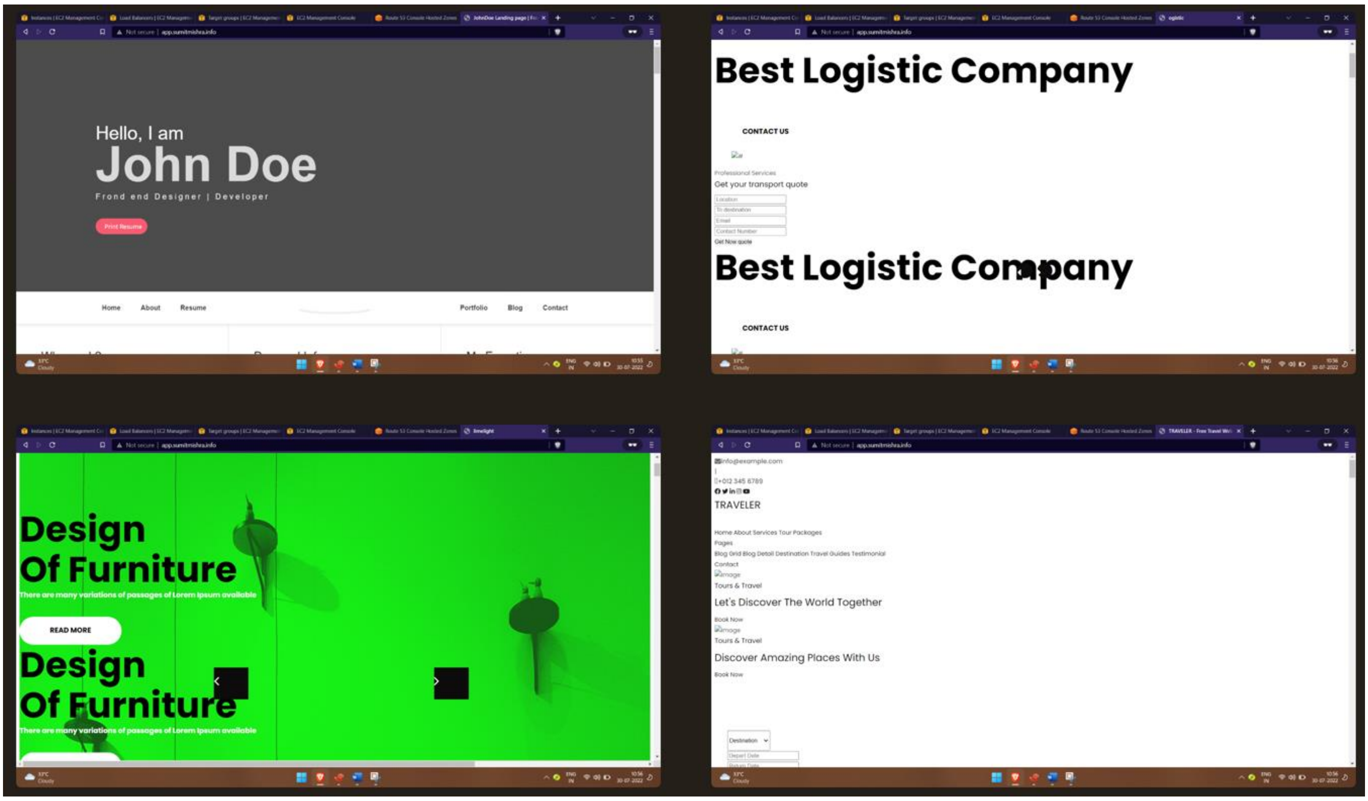
3. Creating a new sub-domain and associating the load balancer's DNS to that domain name.



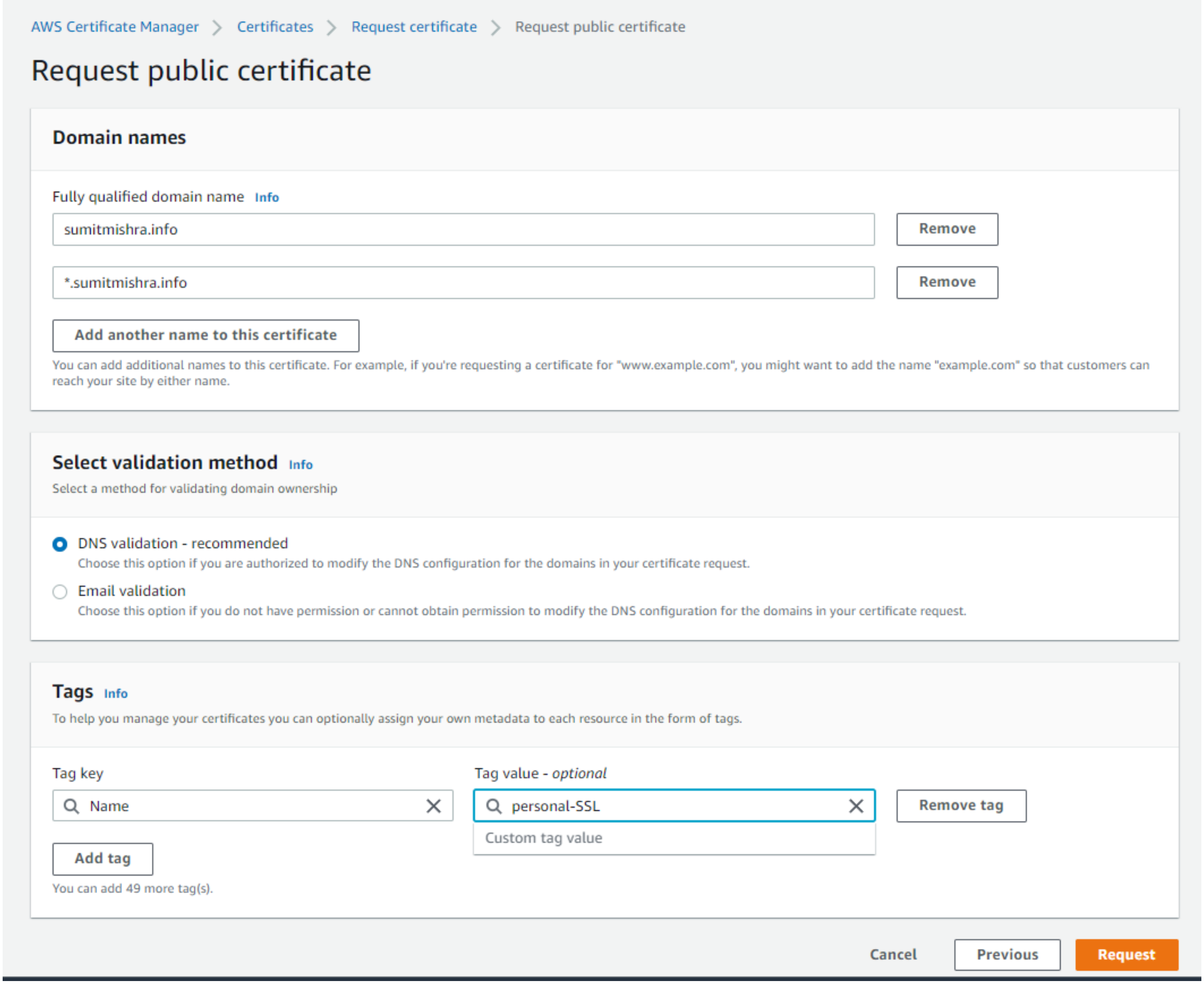
Record details

	Record name app.sumitmishra.info	Record type A
Value dualstack.personal-vpc-lb-845205905.ap-south-1.elb.amazonaws.com.	Alias Yes	TTL (seconds) -
Routing policy Simple		

4. Server is distributing the traffic, but SSL certificate has not been configured.



5. SSL configuration using AWS Certificate Manager.
    a. Request a certificate.



AWS Certificate Manager > Certificates > Request certificate > Request public certificate

Request public certificate

Domain names

Fully qualified domain name Info

sumitmishra.info Remove

*.sumitmishra.info Remove

Add another name to this certificate

You can add additional names to this certificate. For example, if you're requesting a certificate for "www.example.com", you might want to add the name "example.com" so that customers can reach your site by either name.

Select validation method Info

Select a method for validating domain ownership

● DNS validation - recommended
Choose this option if you are authorized to modify the DNS configuration for the domains in your certificate request.

○ Email validation
Choose this option if you do not have permission or cannot obtain permission to modify the DNS configuration for the domains in your certificate request.

Tags Info

To help you manage your certificates you can optionally assign your own metadata to each resource in the form of tags.

Tag key: Name

Tag value - *optional*: personal-SSL

Custom tag value

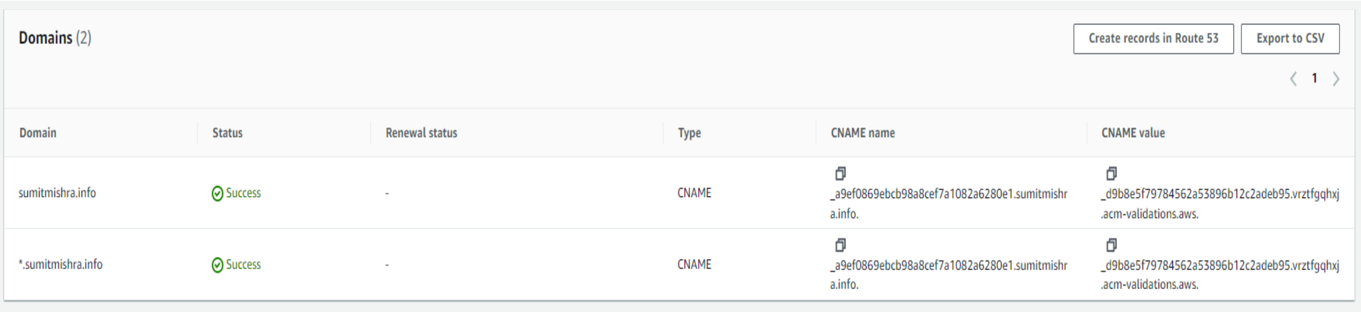
Remove tag

Add tag

You can add 49 more tag(s).

Cancel Previous Request

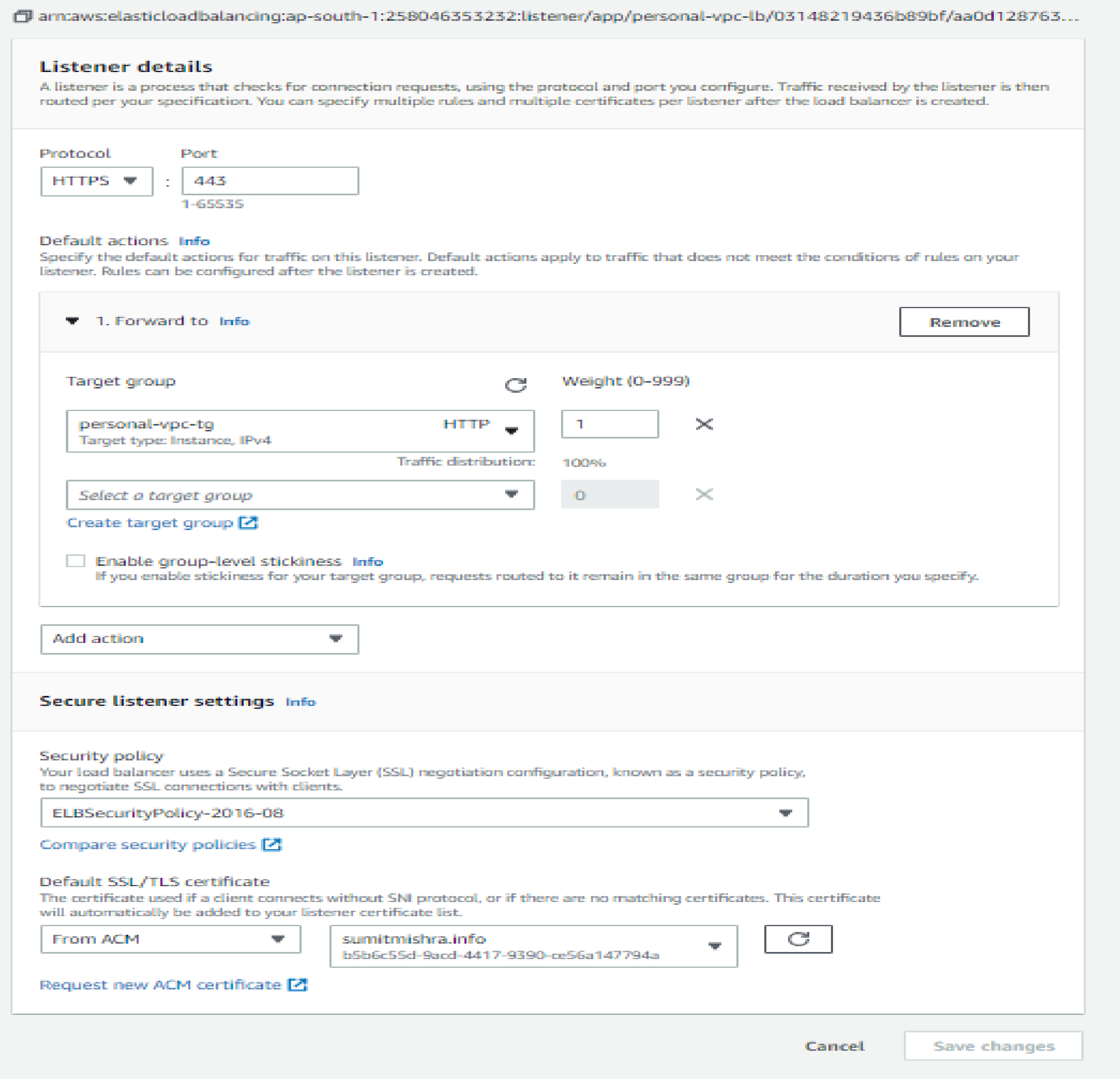
    b. After requesting, add the records to the route 53 table.



Domains (2)

Domain	Status	Renewal status	Type	CNAME name	CNAME value
sumitmishra.info	Success	-	CNAME	_a9ef0869ebcb98a8cef7a1082a6280e1.sumitmishra.info.	_d9b8e5f79784562a53896b12c2adeb95.vrztfgqhxj.acm-validations.aws.
*.sumitmishra.info	Success	-	CNAME	_a9ef0869ebcb98a8cef7a1082a6280e1.sumitmishra.info.	_d9b8e5f79784562a53896b12c2adeb95.vrztfgqhxj.acm-validations.aws.

c. After certificate has been issued, go to load balancer -> listener -> add new listener -> select https and forward it to target group created and select the certificate as the created one.



arn:aws:elasticloadbalancing:ap-south-1:258046353232:listener/app/personal-vpc-lb/03148219436b89bf/aa0d128763...

Listener details

A listener is a process that checks for connection requests, using the protocol and port you configure. Traffic received by the listener is then routed per your specification. You can specify multiple rules and multiple certificates per listener after the load balancer is created.

Protocol: HTTPS : Port: 443

1-65535

Default actions Info

Specify the default actions for traffic on this listener. Default actions apply to traffic that does not meet the conditions of rules on your listener. Rules can be configured after the listener is created.

1. Forward to Info

Target group: personal-vpc-tg HTTP
Target type: Instance, IPv4

Weight (0-999): 1

Traffic distribution: 100%

Select a target group — 0

□ Enable group-level stickiness Info

If you enable stickiness for your target group, requests routed to it remain in the same group for the duration you specify.

Secure listener settings Info

Security policy

Your load balancer uses a Secure Socket Layer (SSL) negotiation configuration, known as a security policy, to negotiate SSL connections with clients.

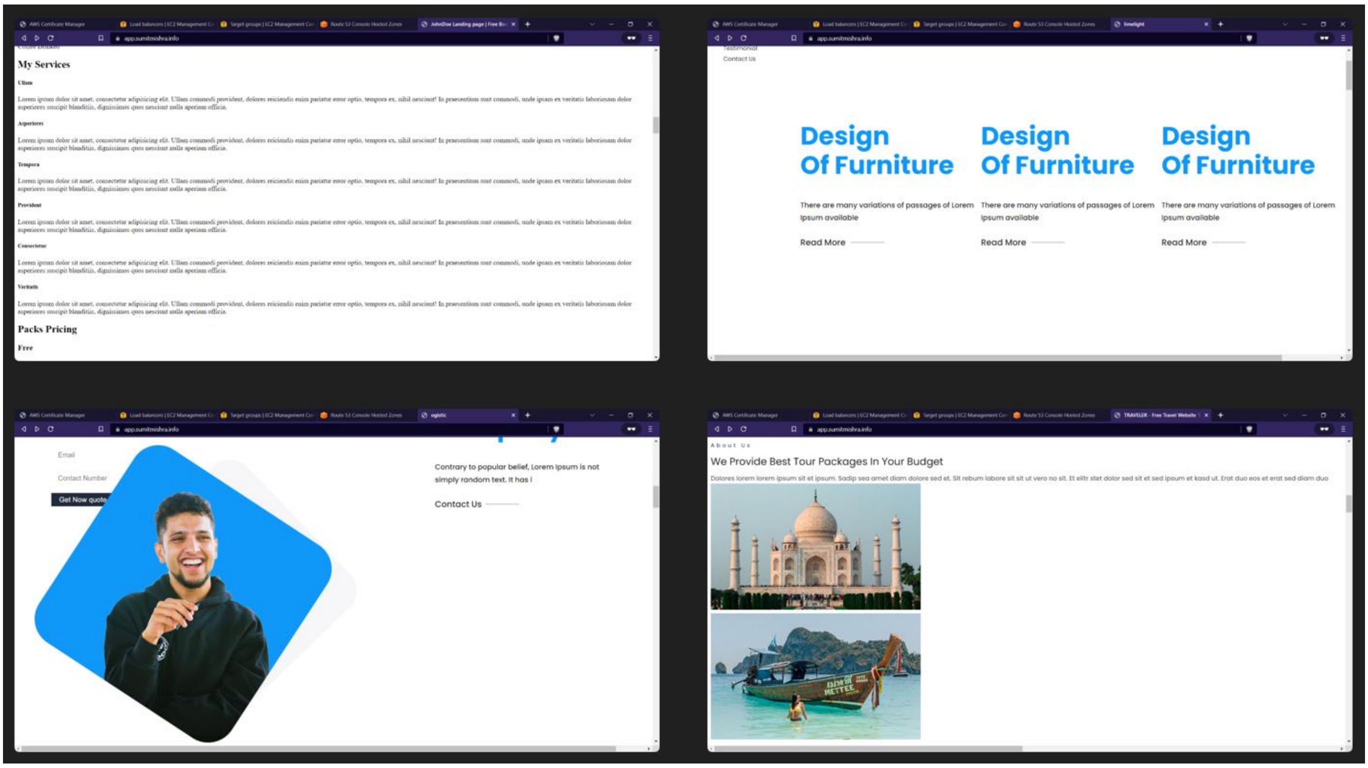
ELBSecurityPolicy-2016-08

Default SSL/TLS certificate

The certificate used if a client connects without SNI protocol, or if there are no matching certificates. This certificate will automatically be added to your listener certificate list.

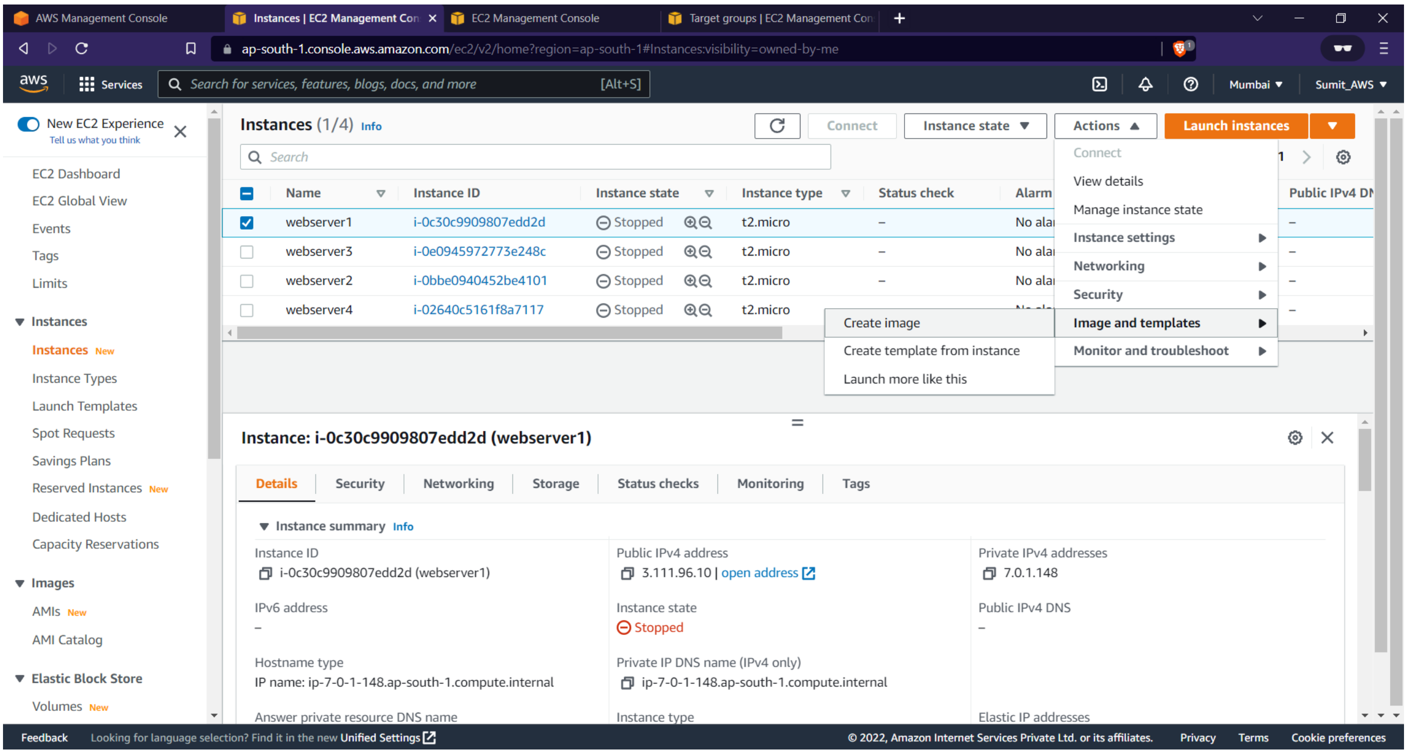
From ACM — sumitmishra.info
b5b6c55d-9acd-4417-9390-ce56a147794a

6. SSL has been successfully enabled if we hit the URL with https://app.sumitmishra.info and load is balanced between the backend web servers.


app.sumitmishra.info
My Services
Packs Pricing
Free
Design Of Furniture
Design Of Furniture
Design Of Furniture
There are many variations of passages of Lorem Ipsum available
Read More
Get Now quote
Contrary to popular belief, Lorem Ipsum is not simply random text. It has i
Contact Us
About Us
We Provide Best Tour Packages In Your Budget

5. Configuring auto scaling to an instance.

1. Create an Image of webserver1 EC2 instance.



Instances (1/4) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm	Public IPv4 DN
☑	webserver1	i-0c30c9909807edd2d	⊖ Stopped	t2.micro	–	No alar	–
□	webserver3	i-0e0945972773e248c	⊖ Stopped	t2.micro	–	No alar	–
□	webserver2	i-0bbe0940452be4101	⊖ Stopped	t2.micro	–	No alar	–
□	webserver4	i-02640c5161f8a7117	⊖ Stopped	t2.micro			–

Instance: i-0c30c9909807edd2d (webserver1)

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Instance summary Info

Instance ID: i-0c30c9909807edd2d (webserver1)

Public IPv4 address: 3.111.96.10 | open address

Private IPv4 addresses: 7.0.1.148

IPv6 address: –

Instance state: Stopped

Public IPv4 DNS: –

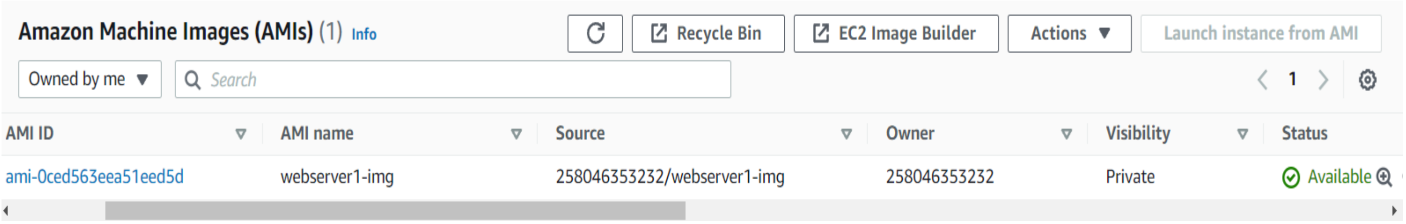
Hostname type: IP name: ip-7-0-1-148.ap-south-1.compute.internal

Private IP DNS name (IPv4 only): ip-7-0-1-148.ap-south-1.compute.internal

Answer private resource DNS name

Instance type

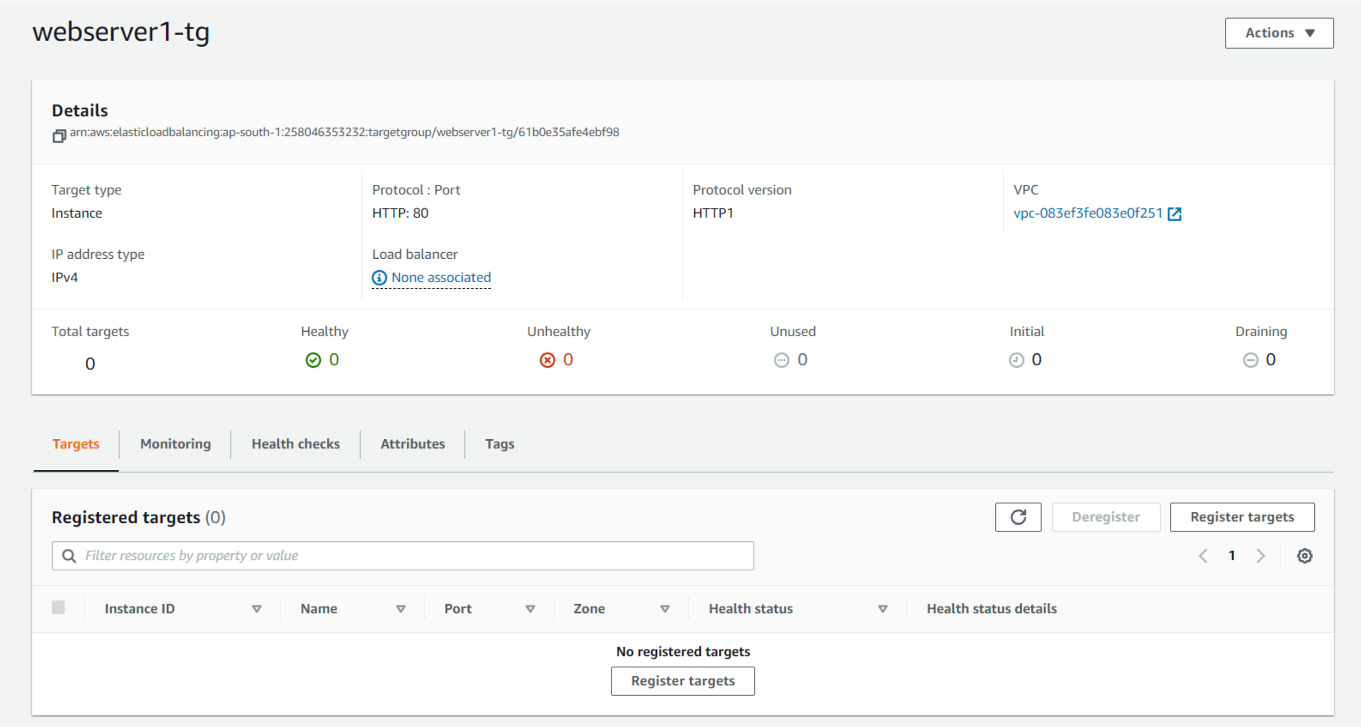
Elastic IP addresses



Amazon Machine Images (AMIs) (1) Info

AMI ID	AMI name	Source	Owner	Visibility	Status
ami-0ced563eea51eed5d	webserver1-img	258046353232/webserver1-img	258046353232	Private	✓ Available

2. Create a new Load balancer “webserver1-lb” specifically for that server and assign a new configured target group for the “webserver1-tg” not having any instance attached to it.



webserver1-tg

Details

arn:aws:elasticloadbalancing:ap-south-1:258046353232:targetgroup/webserver1-tg/61b0e35afe4ebf98

Target type: Instance

Protocol : Port: HTTP: 80

Protocol version: HTTP1

VPC: vpc-083ef3fe083e0f251

IP address type: IPv4

Load balancer: None associated

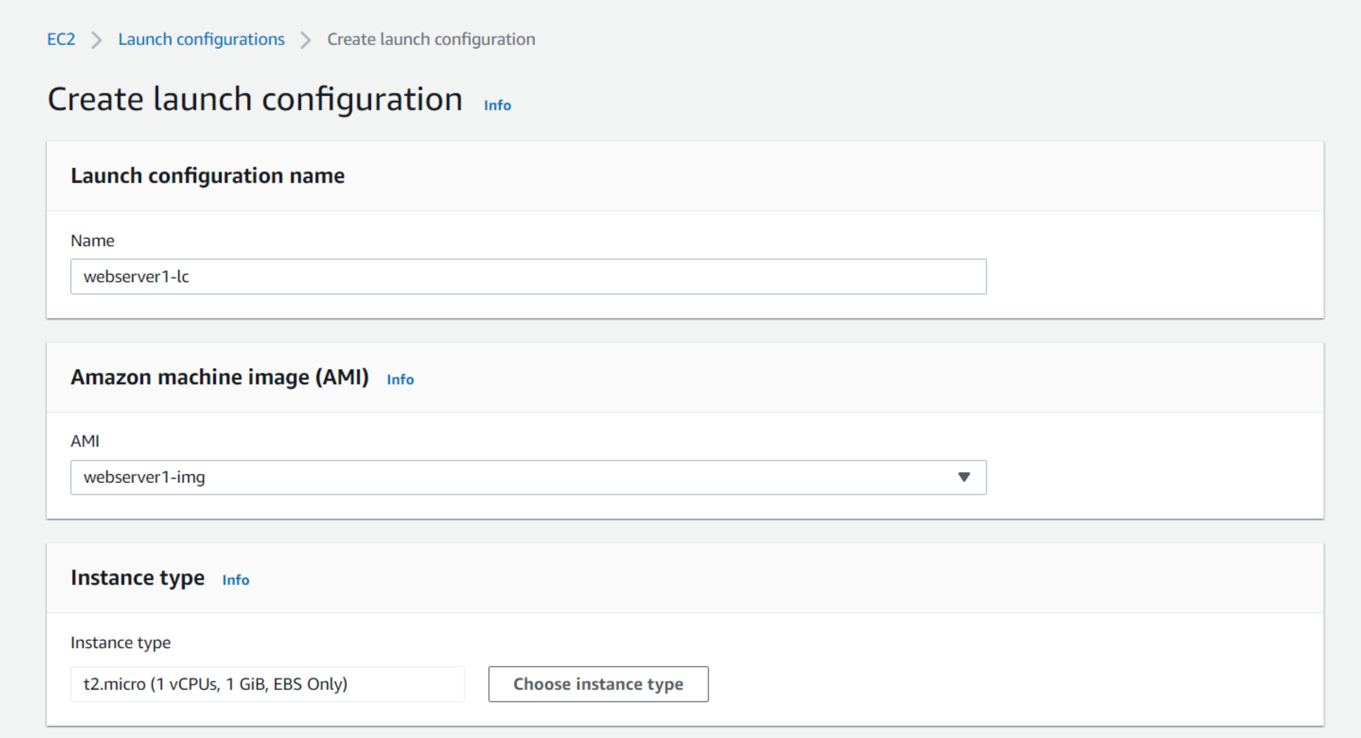
Total targets	Healthy	Unhealthy	Unused	Initial	Draining
0	0	0	0	0	0

Registered targets (0)

Instance ID	Name	Port	Zone	Health status	Health status details

No registered targets

3. Now, created a new launch configuration using image of the “webserver1” instance and also checking on the option of detailed monitoring using AWS cloudwatch.



Create launch configuration

Launch configuration name

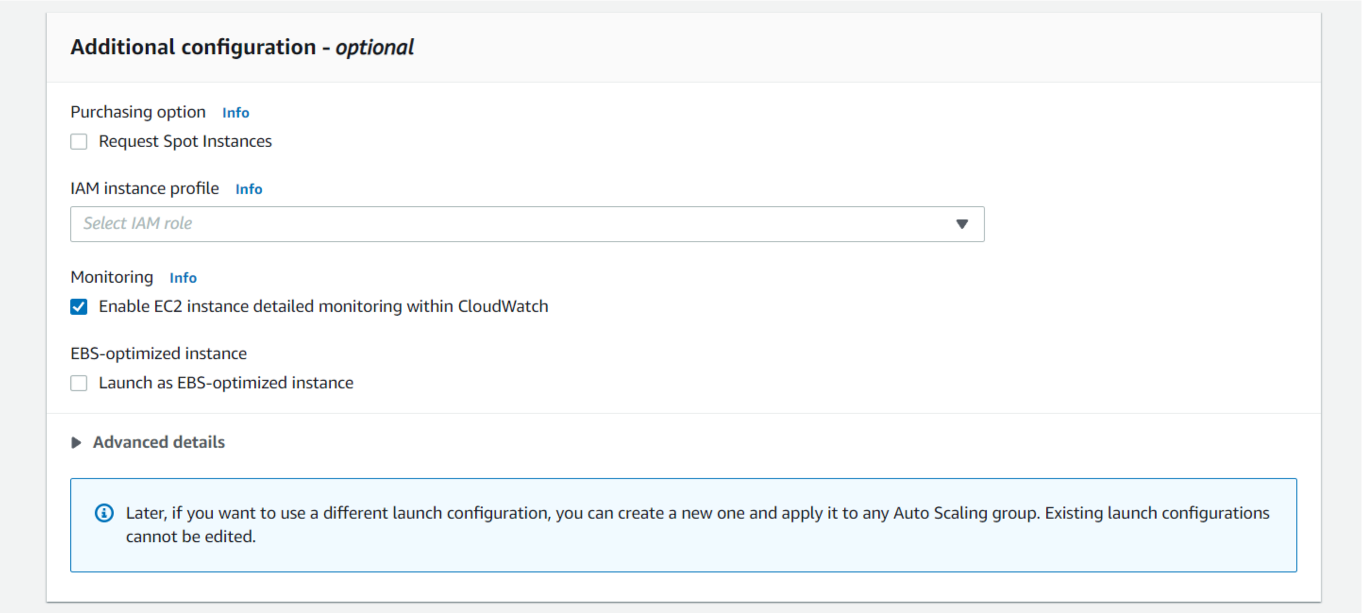
Name: webserver1-lc

Amazon machine image (AMI)

AMI: webserver1-img

Instance type

Instance type: t2.micro (1 vCPUs, 1 GiB, EBS Only)



Additional configuration - *optional*

Purchasing option Info

□ Request Spot Instances

IAM instance profile Info

Select IAM role ▼

Monitoring Info

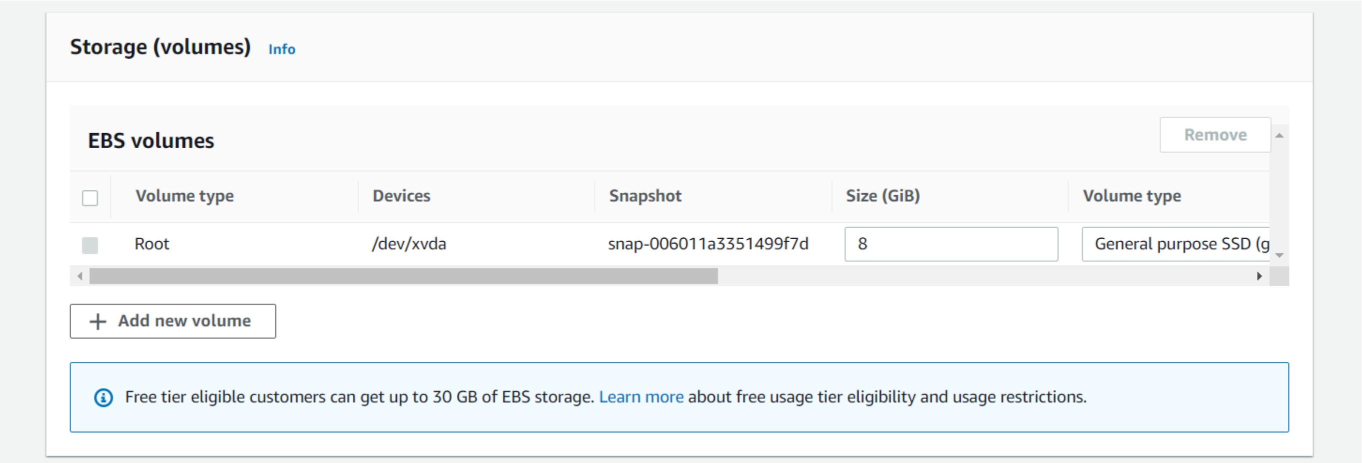
☑ Enable EC2 instance detailed monitoring within CloudWatch

EBS-optimized instance

□ Launch as EBS-optimized instance

▶ Advanced details

ⓘ Later, if you want to use a different launch configuration, you can create a new one and apply it to any Auto Scaling group. Existing launch configurations cannot be edited.

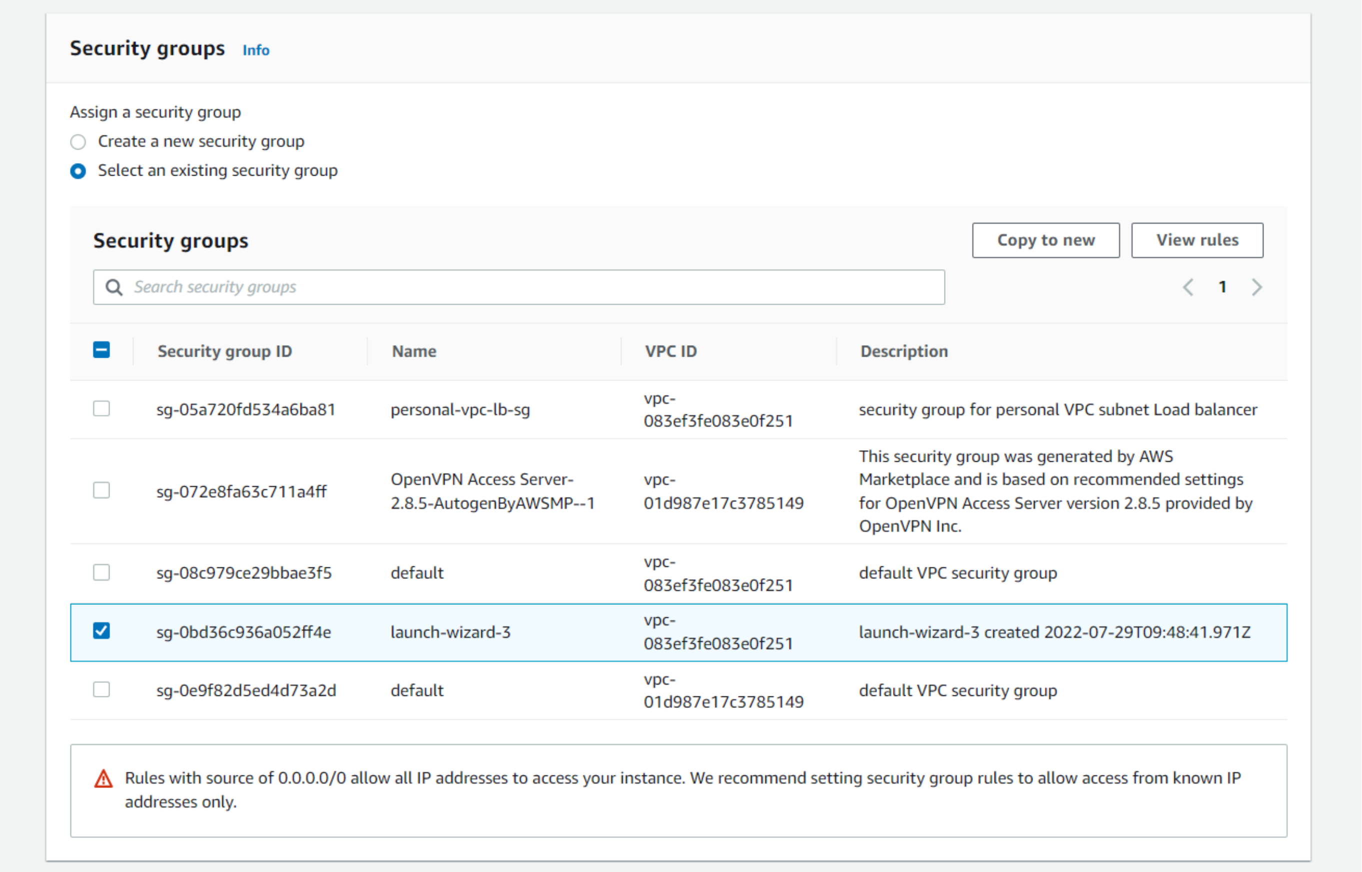


Storage (volumes) Info

EBS volumes

□	Volume type	Devices	Snapshot	Size (GiB)	Volume type
□	Root	/dev/xvda	snap-006011a3351499f7d	8	General purpose SSD (g

ⓘ Free tier eligible customers can get up to 30 GB of EBS storage. Learn more about free usage tier eligibility and usage restrictions.



Security groups Info

Assign a security group

○ Create a new security group

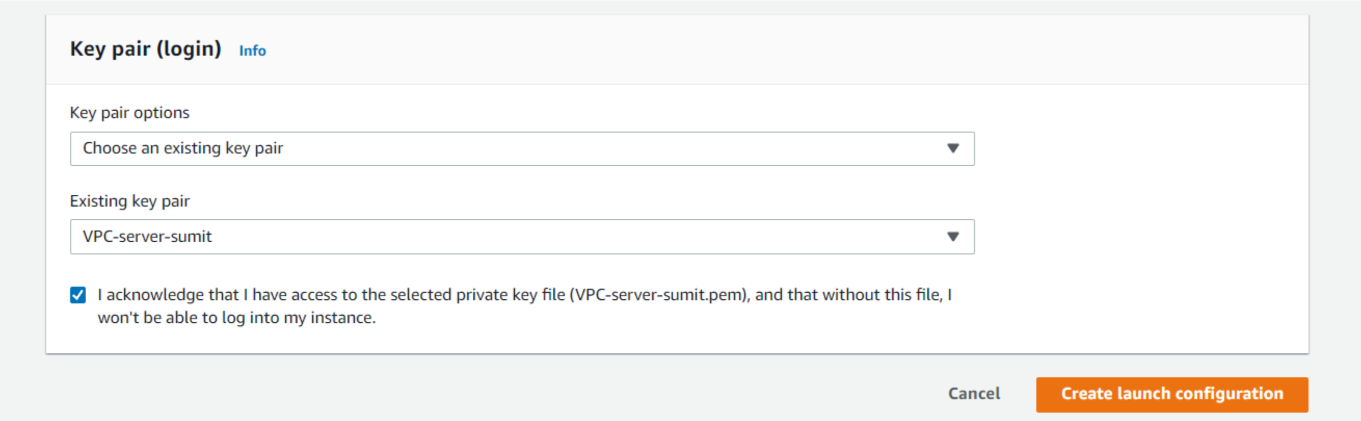
● Select an existing security group

Security groups

☐	Security group ID	Name	VPC ID	Description
□	sg-05a720fd534a6ba81	personal-vpc-lb-sg	vpc-083ef3fe083e0f251	security group for personal VPC subnet Load balancer
□	sg-072e8fa63c711a4ff	OpenVPN Access Server-2.8.5-AutogenByAWSMP--1	vpc-01d987e17c3785149	This security group was generated by AWS Marketplace and is based on recommended settings for OpenVPN Access Server version 2.8.5 provided by OpenVPN Inc.
□	sg-08c979ce29bbae3f5	default	vpc-083ef3fe083e0f251	default VPC security group
☑	sg-0bd36c936a052ff4e	launch-wizard-3	vpc-083ef3fe083e0f251	launch-wizard-3 created 2022-07-29T09:48:41.971Z
□	sg-0e9f82d5ed4d73a2d	default	vpc-01d987e17c3785149	default VPC security group

⚠ 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.

Sumit Mishra
190310286



Key pair (login) Info

Key pair options

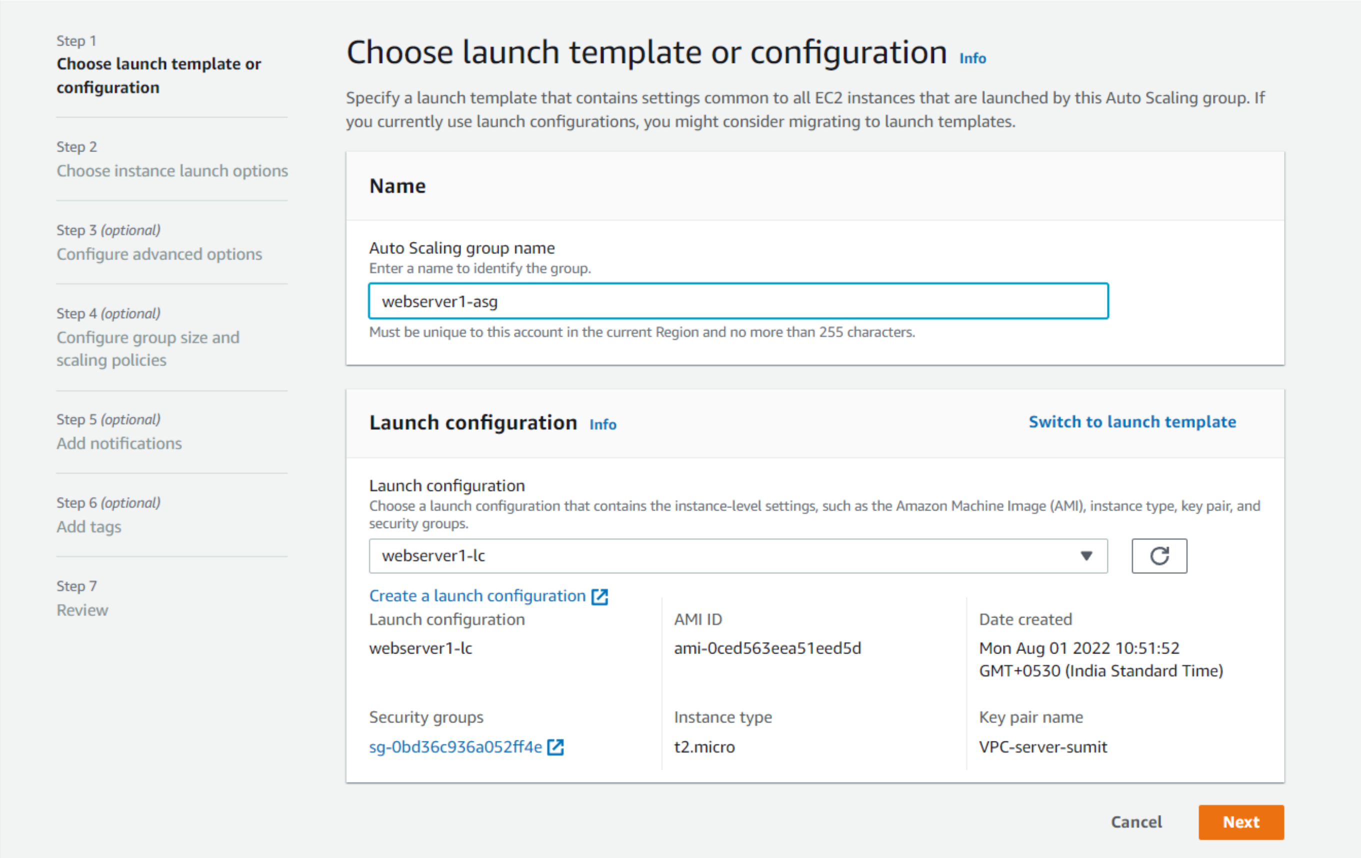
Choose an existing key pair

Existing key pair

VPC-server-sumit

☑ I acknowledge that I have access to the selected private key file (VPC-server-sumit.pem), and that without this file, I won't be able to log into my instance.

4. Created an auto scaling group using launch dynamic configuration by providing the created launch configuration.



Step 1
Choose launch template or configuration
Step 2
Choose instance launch options
Step 3 (optional)
Configure advanced options
Step 4 (optional)
Configure group size and scaling policies
Step 5 (optional)
Add notifications
Step 6 (optional)
Add tags
Step 7
Review

Choose launch template or configuration Info

Specify a launch template that contains settings common to all EC2 instances that are launched by this Auto Scaling group. If you currently use launch configurations, you might consider migrating to launch templates.

Name

Auto Scaling group name
Enter a name to identify the group.

webserver1-asg

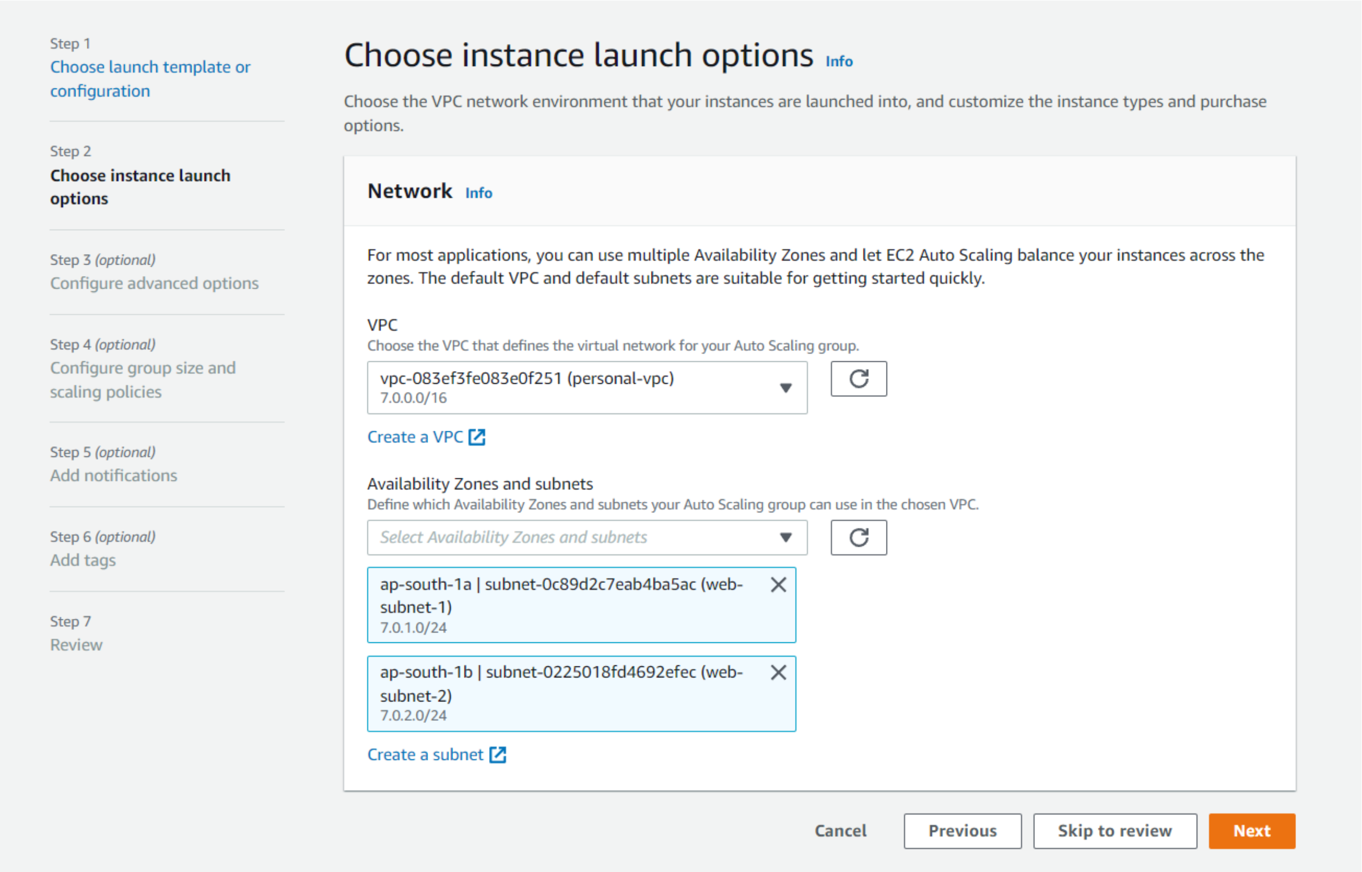
Must be unique to this account in the current Region and no more than 255 characters.

Launch configuration Info

Launch configuration
Choose a launch configuration that contains the instance-level settings, such as the Amazon Machine Image (AMI), instance type, key pair, and security groups.

webserver1-lc

Launch configuration	AMI ID	Date created
webserver1-lc	ami-0ced563eea51eed5d	Mon Aug 01 2022 10:51:52 GMT+0530 (India Standard Time)
Security groups	Instance type	Key pair name
sg-0bd36c936a052ff4e	t2.micro	VPC-server-sumit



Step 1
Choose launch template or configuration
Step 2
Choose instance launch options
Step 3 *(optional)*
Configure advanced options
Step 4 *(optional)*
Configure group size and scaling policies
Step 5 *(optional)*
Add notifications
Step 6 *(optional)*
Add tags
Step 7
Review

Choose instance launch options Info

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase options.

Network Info

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC
Choose the VPC that defines the virtual network for your Auto Scaling group.
vpc-083ef3fe083e0f251 (personal-vpc)
7.0.0.0/16

Create a VPC

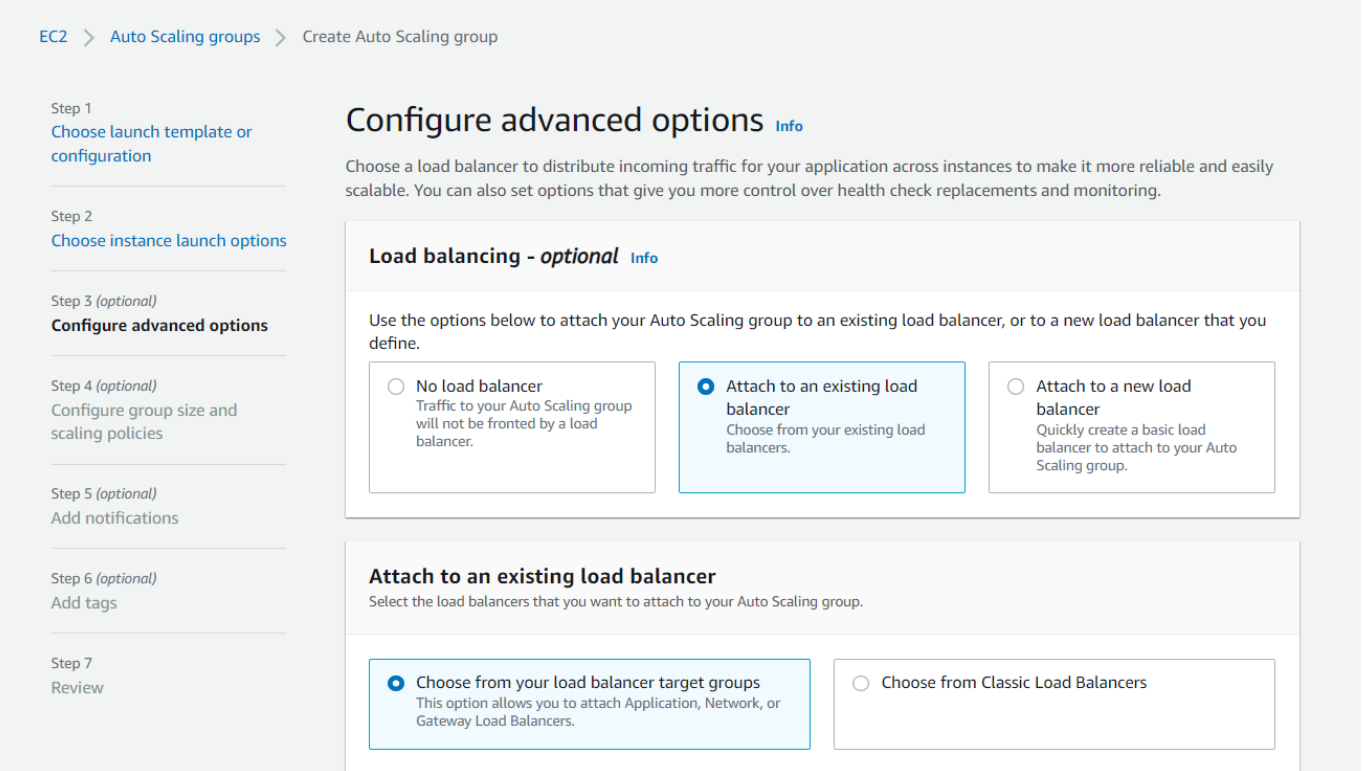
Availability Zones and subnets
Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.
Select Availability Zones and subnets

ap-south-1a | subnet-0c89d2c7eab4ba5ac (web-subnet-1)
7.0.1.0/24

ap-south-1b | subnet-0225018fd4692efec (web-subnet-2)
7.0.2.0/24

Create a subnet

Cancel
Previous
Skip to review
Next



EC2 > Auto Scaling groups > Create Auto Scaling group
Step 1
Choose launch template or configuration
Step 2
Choose instance launch options
Step 3 *(optional)*
Configure advanced options
Step 4 *(optional)*
Configure group size and scaling policies
Step 5 *(optional)*
Add notifications
Step 6 *(optional)*
Add tags
Step 7
Review

Configure advanced options Info

Choose a load balancer to distribute incoming traffic for your application across instances to make it more reliable and easily scalable. You can also set options that give you more control over health check replacements and monitoring.

Load balancing - *optional* Info

Use the options below to attach your Auto Scaling group to an existing load balancer, or to a new load balancer that you define.

○ 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.

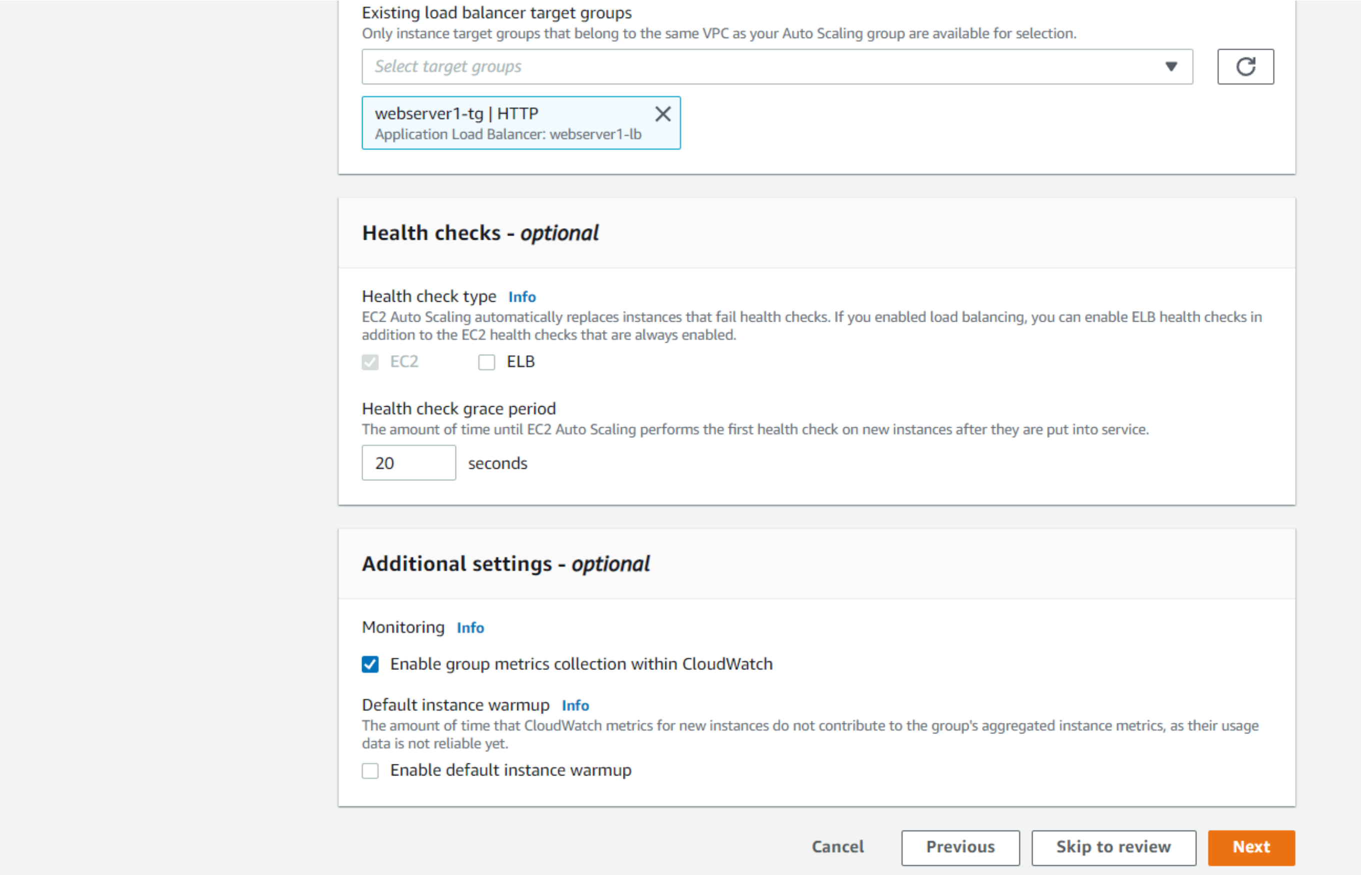
○ Attach to a new load balancer
Quickly create a basic load balancer to attach to your Auto Scaling group.

Attach to an existing load balancer

Select the load balancers that you want to attach to your Auto Scaling group.

● 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 ▼

webserver1-tg | HTTP ✕
Application Load Balancer: webserver1-lb

Health checks - *optional*

Health check type **Info**

EC2 Auto Scaling automatically replaces instances that fail health checks. If you enabled load balancing, you can enable ELB health checks in addition to the EC2 health checks that are always enabled.

☑ EC2 □ ELB

Health check grace period

The amount of time until EC2 Auto Scaling performs the first health check on new instances after they are put into service.

20 seconds

Additional settings - *optional*

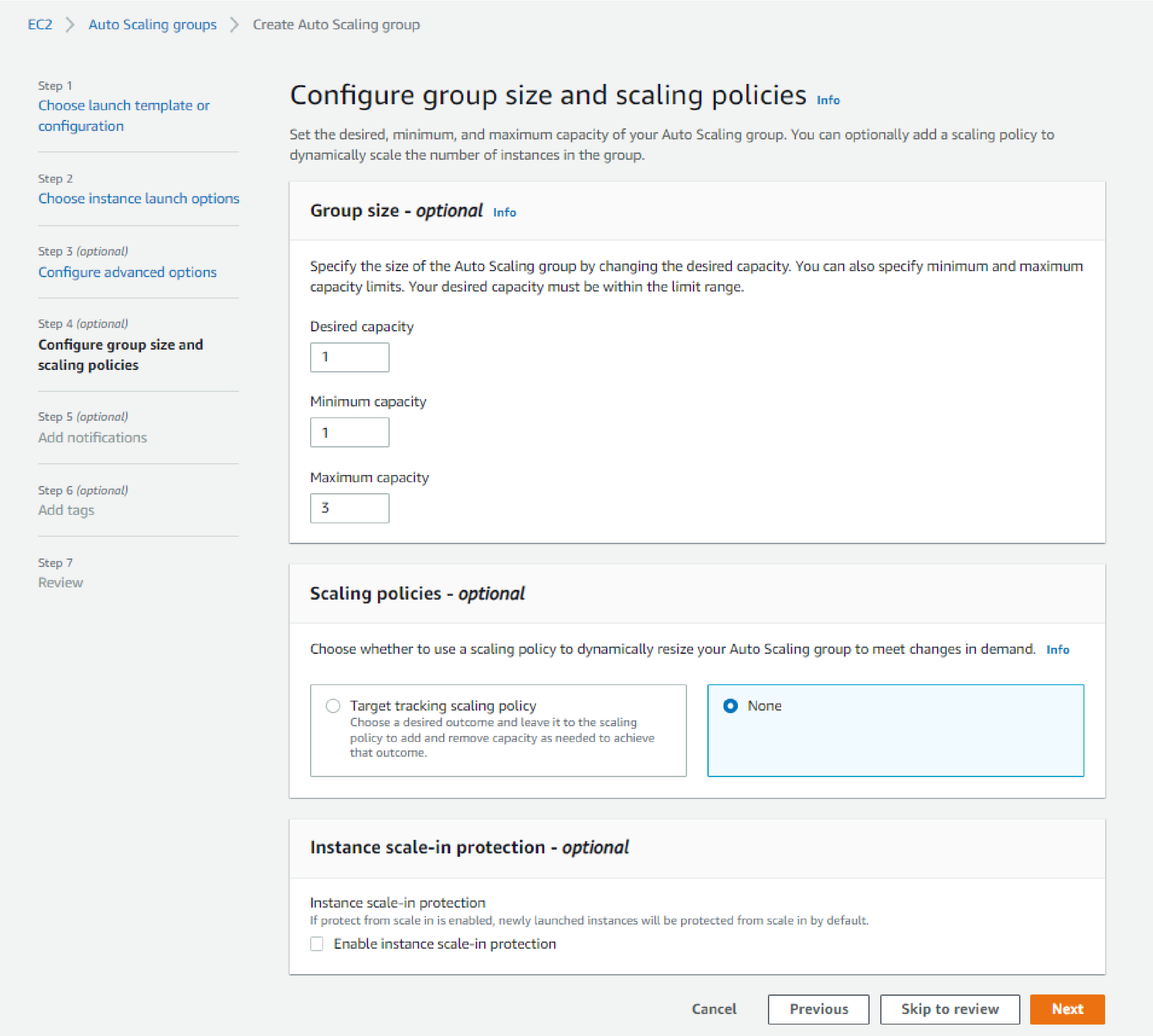
Monitoring **Info**

☑ Enable group metrics collection within CloudWatch

Default instance warmup **Info**

The amount of time that CloudWatch metrics for new instances do not contribute to the group's aggregated instance metrics, as their usage data is not reliable yet.

□ Enable default instance warmup



Step 1
Choose launch template or configuration

Step 2
Choose instance launch options

Step 3 *(optional)*
Configure advanced options

Step 4 *(optional)*
Configure group size and scaling policies

Step 5 *(optional)*
Add notifications

Step 6 *(optional)*
Add tags

Step 7
Review

Configure group size and scaling policies Info

Set the desired, minimum, and maximum capacity of your Auto Scaling group. You can optionally add a scaling policy to dynamically scale the number of instances in the group.

Group size - *optional* Info

Specify the size of the Auto Scaling group by changing the desired capacity. You can also specify minimum and maximum capacity limits. Your desired capacity must be within the limit range.

Desired capacity
1

Minimum capacity
1

Maximum capacity
3

Scaling policies - *optional*

Choose whether to use a scaling policy to dynamically resize your Auto Scaling group to meet changes in demand. **Info**

○ 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

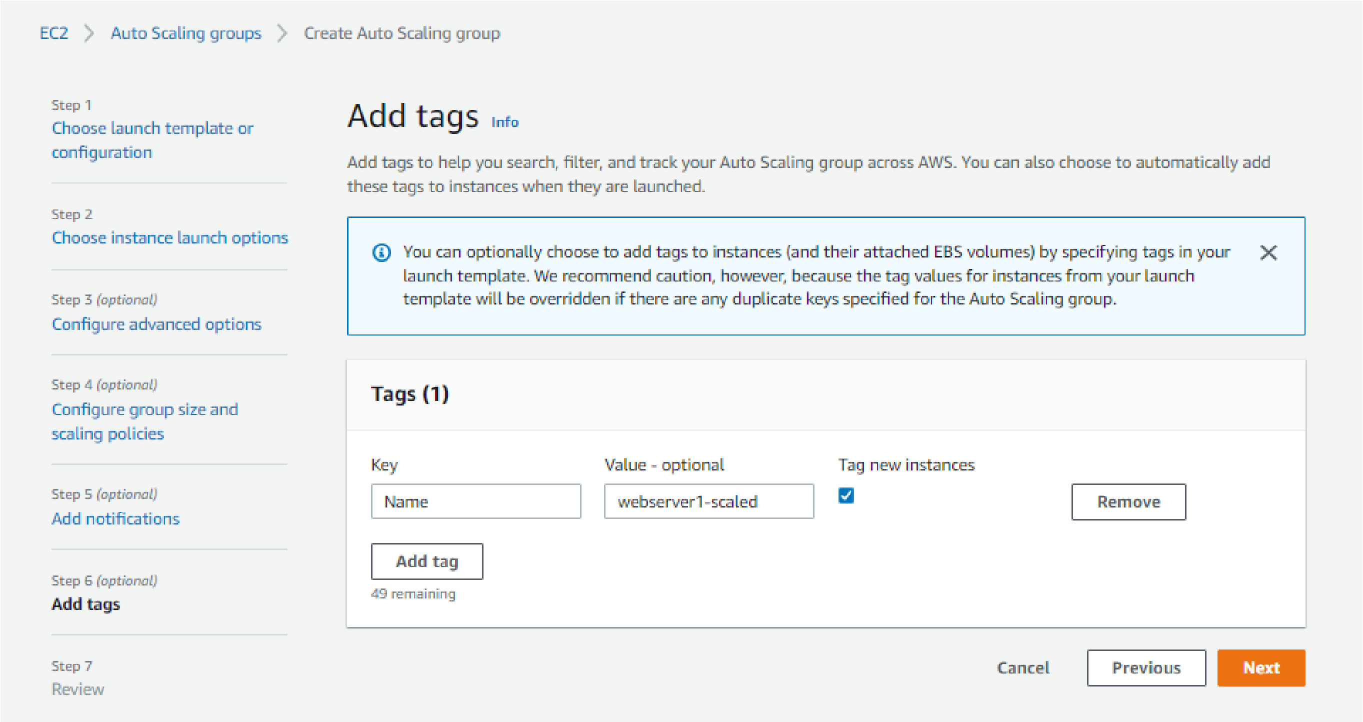
Instance scale-in protection - *optional*

Instance scale-in protection

If protect from scale in is enabled, newly launched instances will be protected from scale in by default.

□ Enable instance scale-in protection

Sumit Mishra
190310286



EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template or configuration

Step 2
Choose instance launch options

Step 3 *(optional)*
Configure advanced options

Step 4 *(optional)*
Configure group size and scaling policies

Step 5 *(optional)*
Add notifications

Step 6 *(optional)*
Add tags

Step 7
Review

Add tags Info

Add tags to help you search, filter, and track your Auto Scaling group across AWS. You can also choose to automatically add these tags to instances when they are launched.

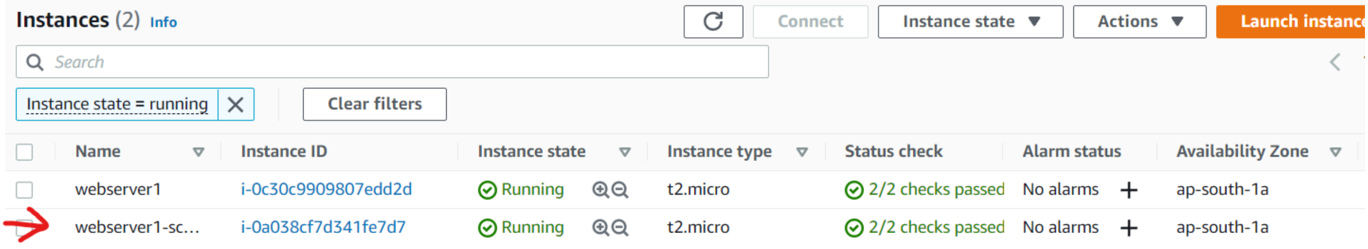
You can optionally choose to add tags to instances (and their attached EBS volumes) by specifying tags in your launch template. We recommend caution, however, because the tag values for instances from your launch template will be overridden if there are any duplicate keys specified for the Auto Scaling group.

Tags (1)

Key	Value - optional	Tag new instances	
Name	webserver1-scaled	☑	Remove

Add tag
49 remaining

When auto scaling group will be created then by default an instance using the image created will be launched in the backend.

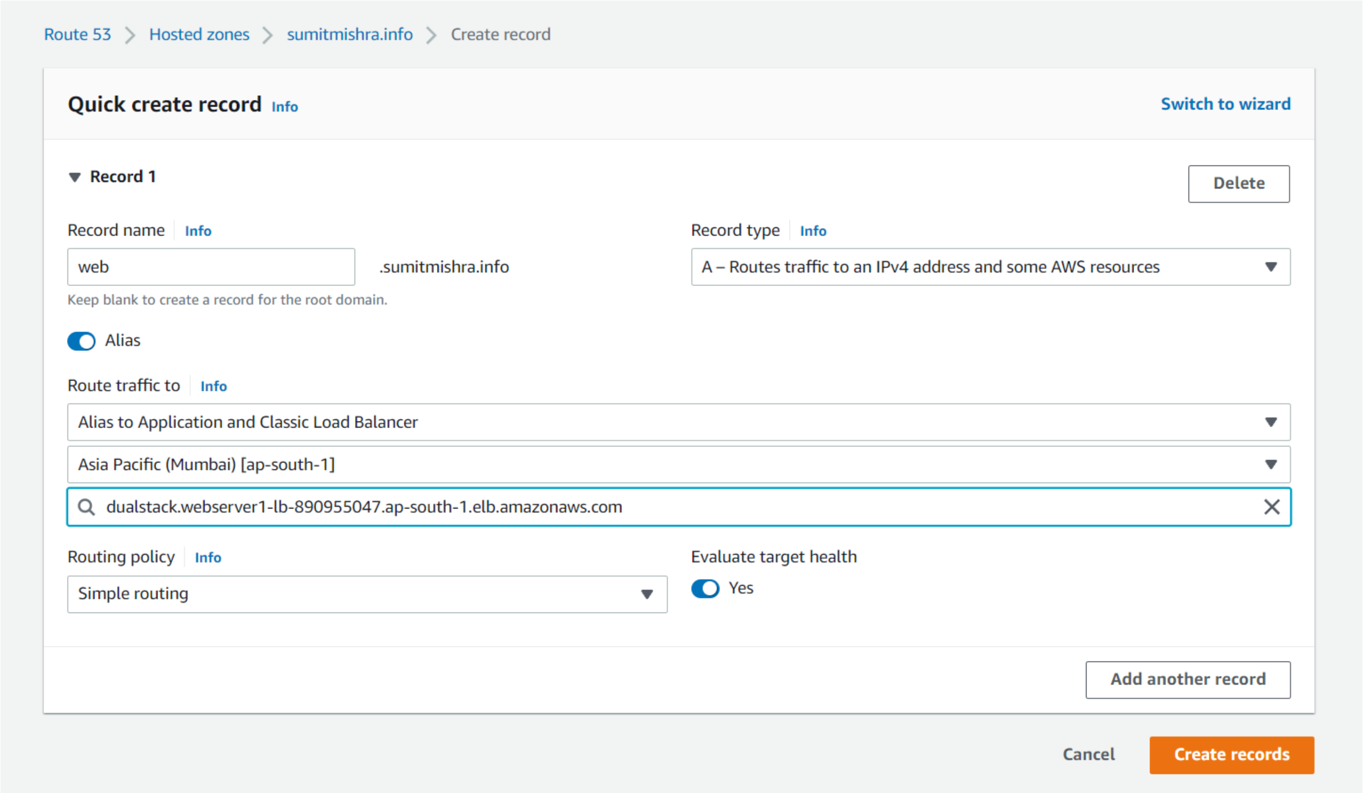


Instances (2) Info

Instance state = running ✕ Clear filters

□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone
□	webserver1	i-0c30c9909807edd2d	✓ Running	t2.micro	✓ 2/2 checks passed	No alarms +	ap-south-1a
□	webserver1-sc...	i-0a038cf7d341fe7d7	✓ Running	t2.micro	✓ 2/2 checks passed	No alarms +	ap-south-1a

5. Added a record in route table of my domain for the web server load balancer.



Route 53 > Hosted zones > sumitmishra.info > Create record

Quick create record Info

▼ **Record 1**

Record name Info: web .sumitmishra.info
Keep blank to create a record for the root domain.

Record type Info: A – Routes traffic to an IPv4 address and some AWS resources

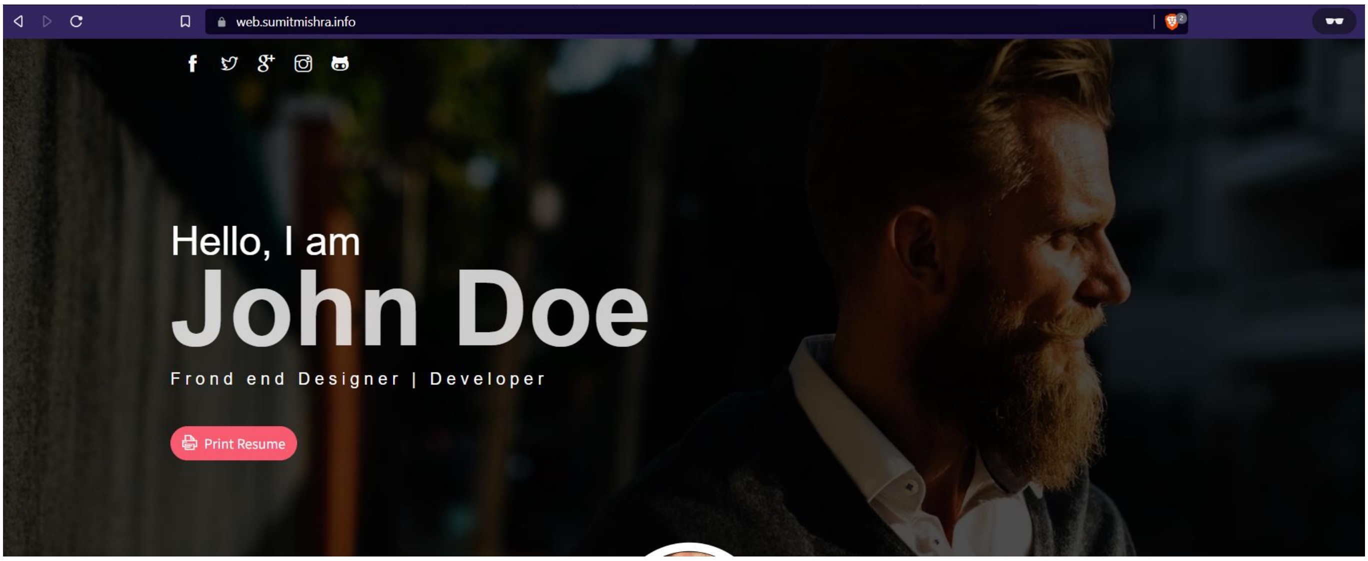
● Alias

Route traffic to Info
Alias to Application and Classic Load Balancer
Asia Pacific (Mumbai) [ap-south-1]
dualstack.webserver1-lb-890955047.ap-south-1.elb.amazonaws.com

Routing policy Info: Simple routing

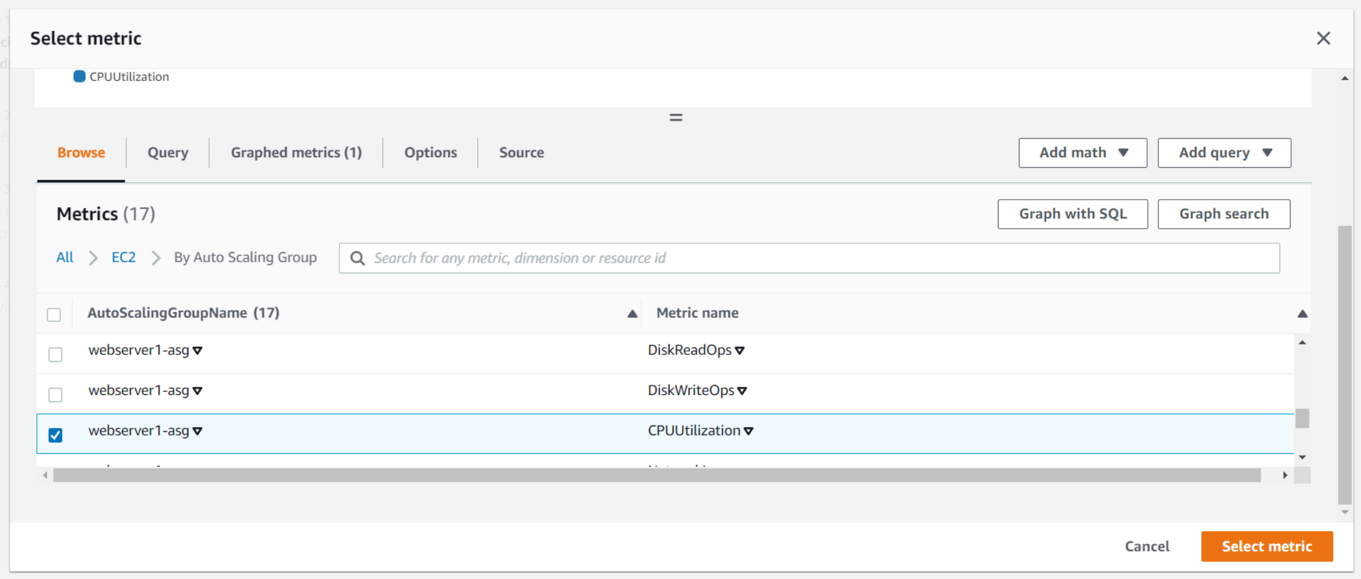
Evaluate target health: ● Yes

6. Then I created an SSL certificate for the webserver using AWS certificate manager in the same way as I did for "personal-vpc-lb" (metioned earlier).



As we can see here the SSL certificate is enabled for https://web.sumitmishra.info .

7. Created two Cloud watch alarms using the auto scaling group I just created named as “webserver1-asg” one for scaling out and another for scaling in.

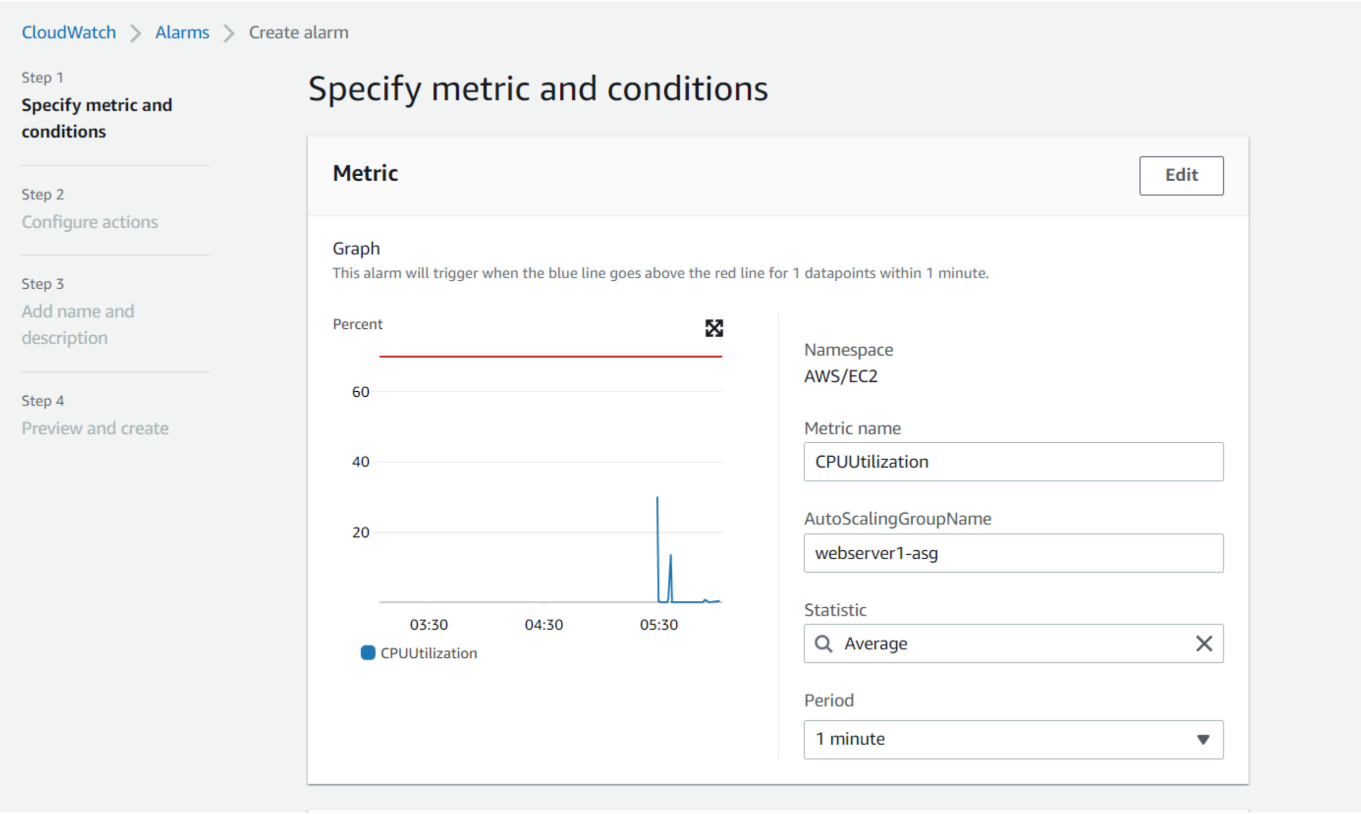


Metrics (17)

All > EC2 > By Auto Scaling Group

Search for any metric, dimension or resource id

	AutoScalingGroupName (17)	Metric name
□	webserver1-asg	DiskReadOps
□	webserver1-asg	DiskWriteOps
☑	webserver1-asg	CPUUtilization



Specify metric and conditions

Metric

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.

Namespace
AWS/EC2

Metric name
CPUUtilization

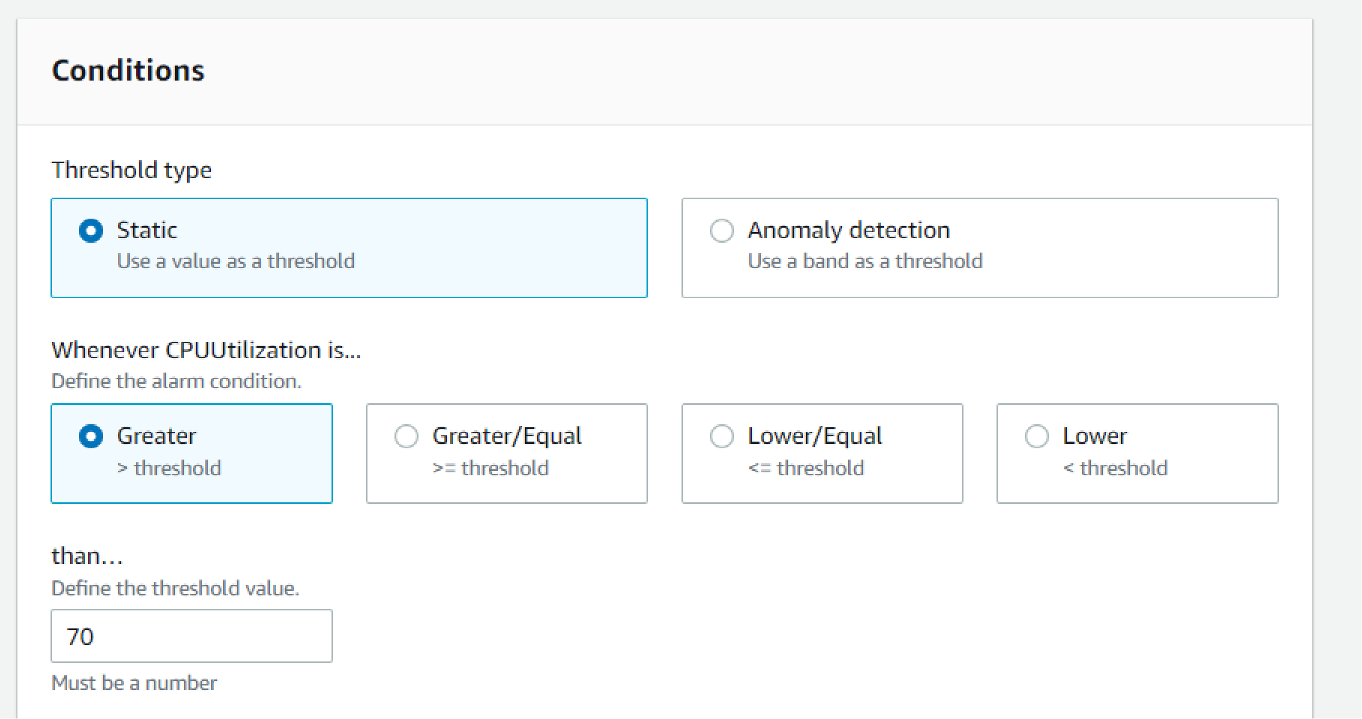
AutoScalingGroupName
webserver1-asg

Statistic
Average

Period
1 minute

Sumit Mishra
190310286

For scale-out



Conditions

Threshold type

● Static
Use a value as a threshold

○ Anomaly detection
Use a band as a threshold

Whenever CPUUtilization is...
Define the alarm condition.

● Greater
> threshold

○ Greater/Equal
>= threshold

○ Lower/Equal
<= threshold

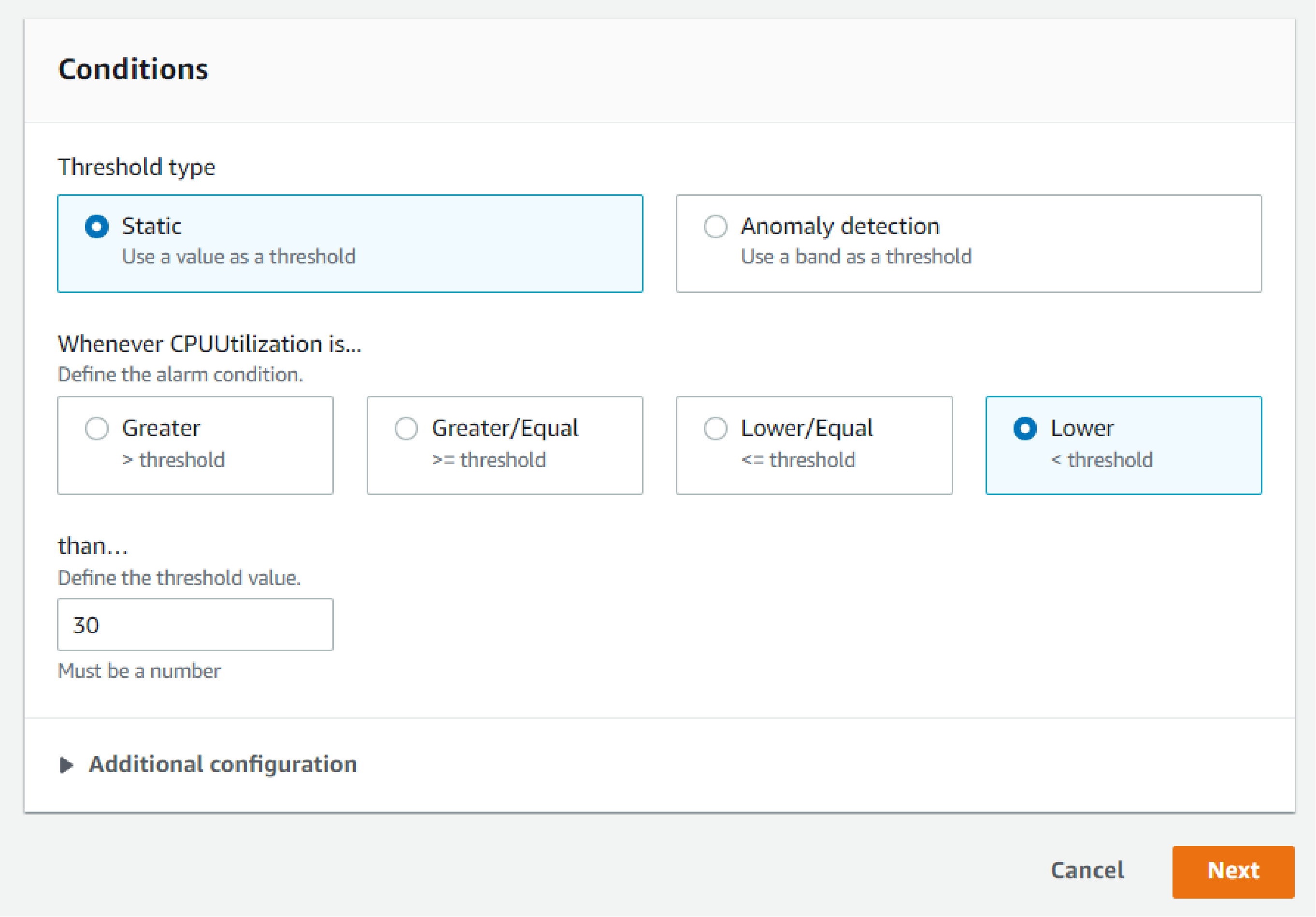
○ Lower
< threshold

than...
Define the threshold value.

70

Must be a number

For scale in



Conditions

Threshold type

● Static
Use a value as a threshold

○ Anomaly detection
Use a band as a threshold

Whenever CPUUtilization is...
Define the alarm condition.

○ Greater
> threshold

○ Greater/Equal
>= threshold

○ Lower/Equal
<= threshold

● Lower
< threshold

than...
Define the threshold value.

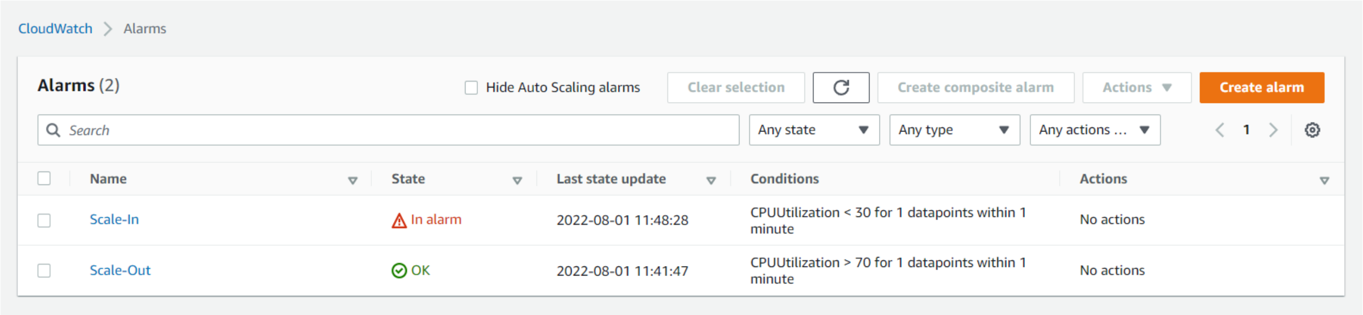
30

Must be a number

▶ Additional configuration

Alarms created :

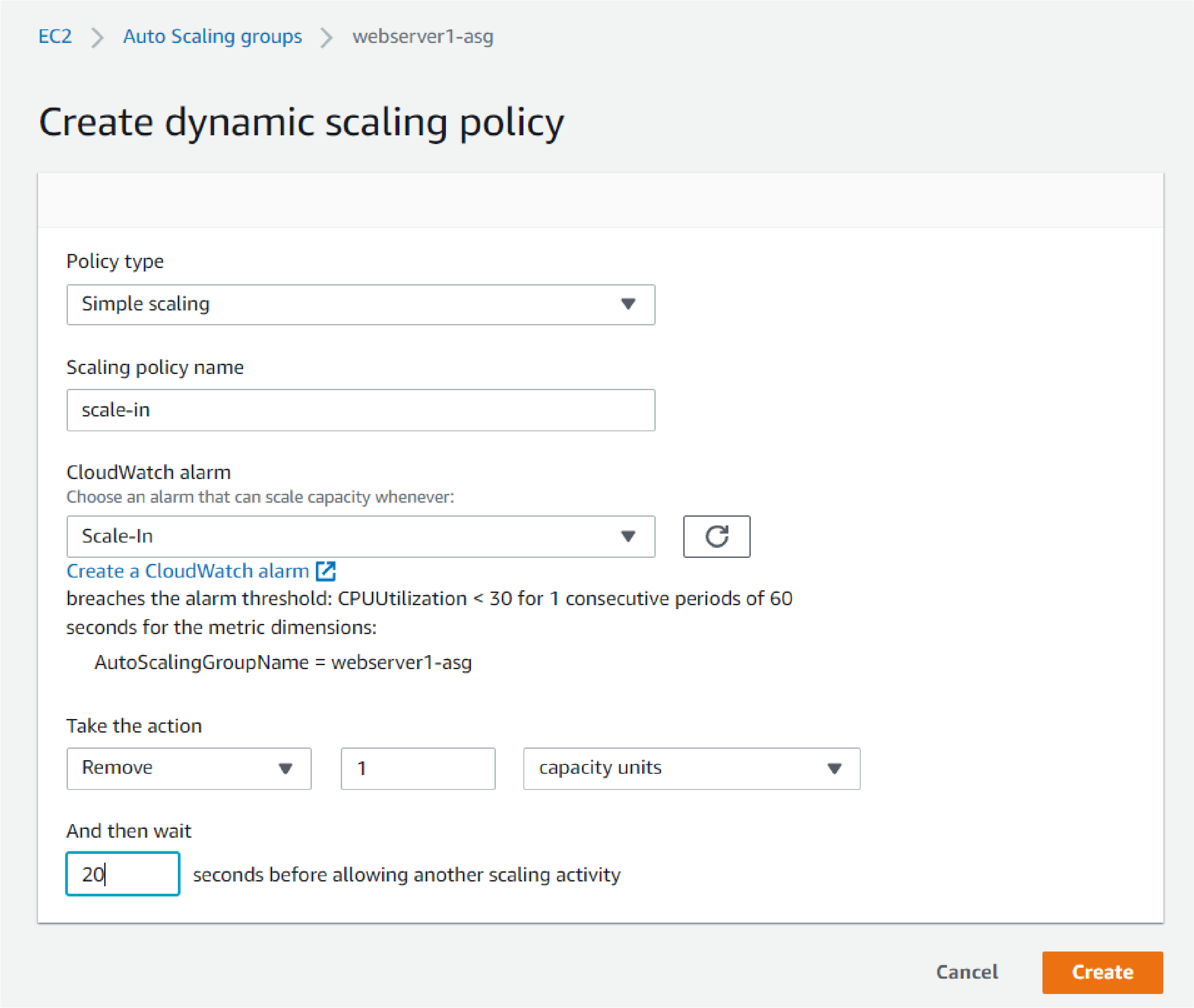
Sumit Mishra
190310286



□	Name	State	Last state update	Conditions	Actions
□	Scale-In	⚠ In alarm	2022-08-01 11:48:28	CPUUtilization < 30 for 1 datapoints within 1 minute	No actions
□	Scale-Out	✓ OK	2022-08-01 11:41:47	CPUUtilization > 70 for 1 datapoints within 1 minute	No actions

8. Then I created two dynamic scaling policies for scaling in and scaling out operation, and attached the alarms to respective scaling policies.

For scale-in:


EC2 > Auto Scaling groups > webserver1-asg

Create dynamic scaling policy

Policy type: Simple scaling

Scaling policy name: scale-in

CloudWatch alarm
Choose an alarm that can scale capacity whenever:
Scale-In

Create a CloudWatch alarm

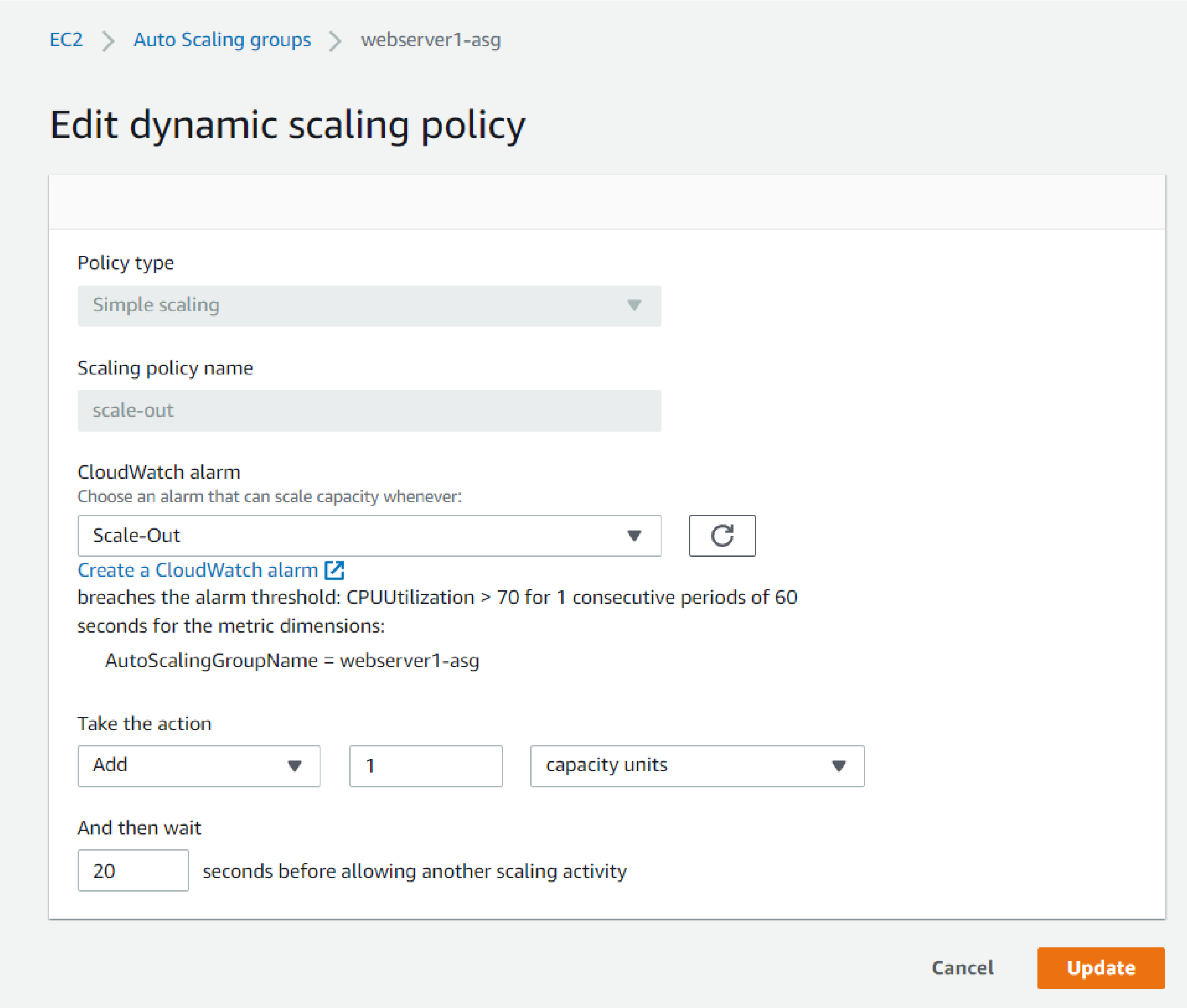
breaches the alarm threshold: CPUUtilization < 30 for 1 consecutive periods of 60 seconds for the metric dimensions:

AutoScalingGroupName = webserver1-asg

Take the action: Remove 1 capacity units

And then wait 20 seconds before allowing another scaling activity

For scale-out :



Edit dynamic scaling policy

Policy type

Simple scaling

Scaling policy name

scale-out

CloudWatch alarm

Choose an alarm that can scale capacity whenever:

Scale-Out

Create a CloudWatch alarm

breaches the alarm threshold: CPUUtilization > 70 for 1 consecutive periods of 60 seconds for the metric dimensions:

AutoScalingGroupName = webserver1-asg

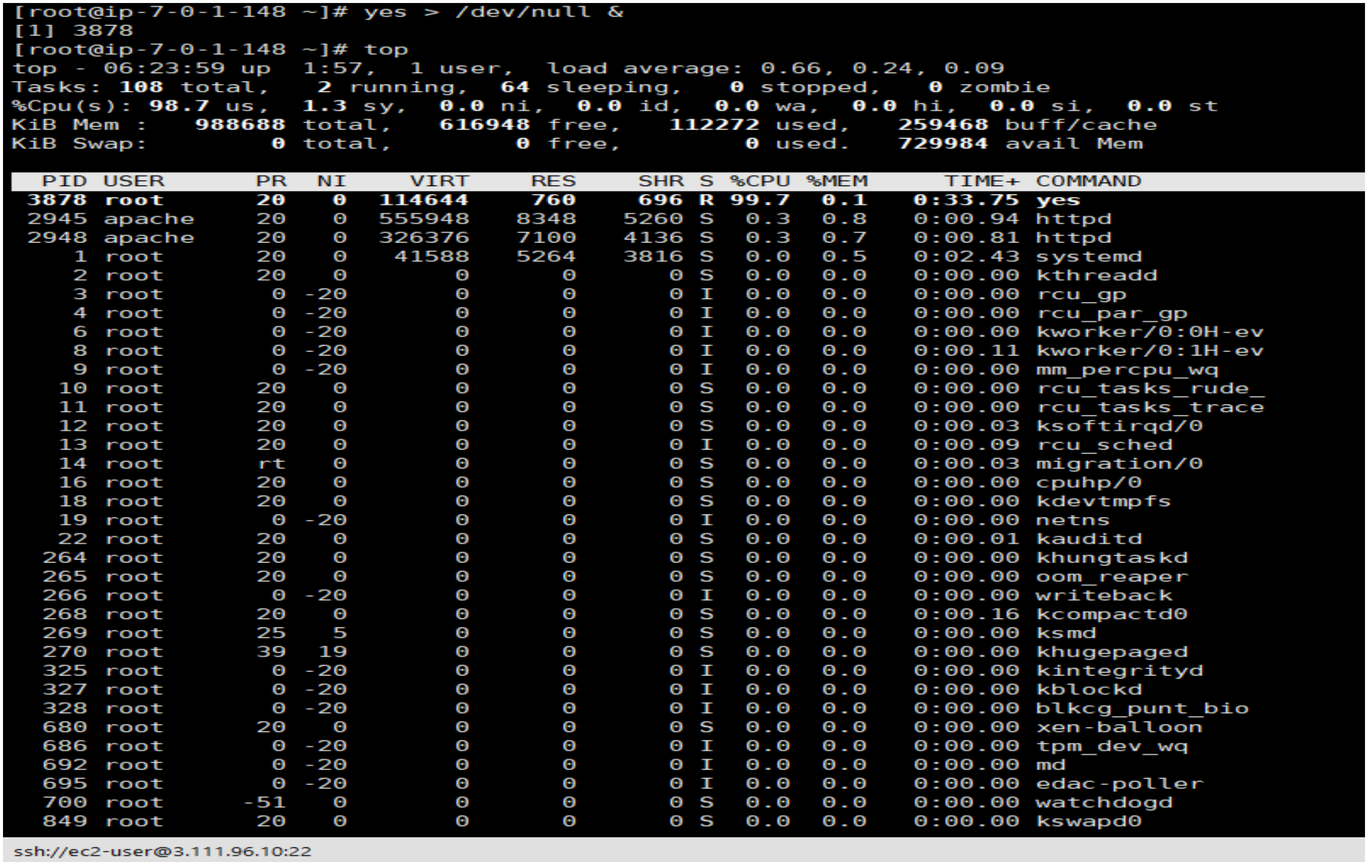
Take the action

Add | 1 | capacity units

And then wait

20 seconds before allowing another scaling activity

9. Then I increased the CPU utilization to 99% by typing the command “yes /dev/null &” then I typed “top” to see the utilization table.

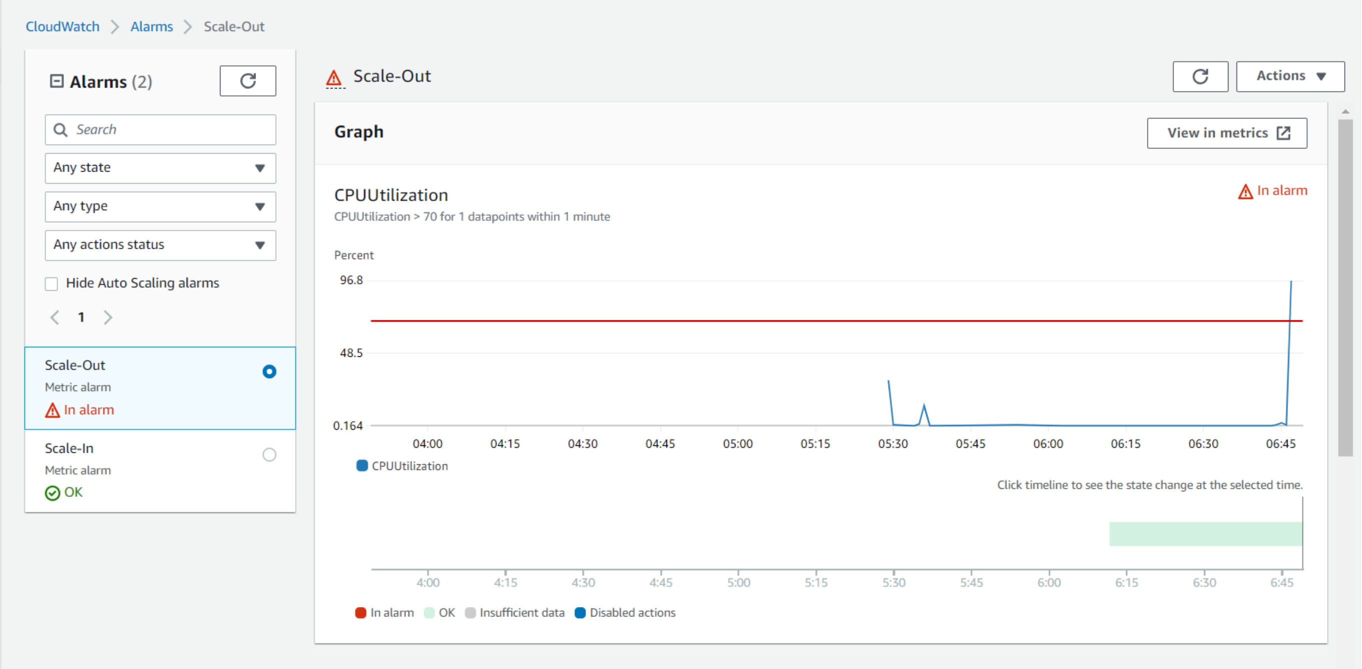


```
[root@ip-7-0-1-148 ~]# yes > /dev/null &
[1] 3878
[root@ip-7-0-1-148 ~]# top
top - 06:23:59 up  1:57,  1 user,  load average: 0.66, 0.24, 0.09
Tasks: 108 total,   2 running,  64 sleeping,   0 stopped,   0 zombie
%Cpu(s): 98.7 us,  1.3 sy,  0.0 ni,  0.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :   988688 total,   616948 free,   112272 used,   259468 buff/cache
KiB Swap:        0 total,        0 free,        0 used.   729984 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
 3878 root      20   0  114644    760    696 R 99.7  0.1   0:33.75 yes
 2945 apache    20   0  555948   8348   5260 S  0.3  0.8   0:00.94 httpd
 2948 apache    20   0  326376   7100   4136 S  0.3  0.7   0:00.81 httpd
    1 root      20   0   41588   5264   3816 S  0.0  0.5   0:02.43 systemd
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kthreadd
    3 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 rcu_par_gp
    6 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 kworker/0:0H-ev
    8 root       0 -20       0      0      0 I  0.0  0.0   0:00.11 kworker/0:1H-ev
    9 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 mm_percpu_wq
   10 root      20   0       0      0      0 S  0.0  0.0   0:00.00 rcu_tasks_rude_
   11 root      20   0       0      0      0 S  0.0  0.0   0:00.00 rcu_tasks_trace
   12 root      20   0       0      0      0 S  0.0  0.0   0:00.03 ksoftirqd/0
   13 root      20   0       0      0      0 I  0.0  0.0   0:00.09 rcu_sched
   14 root      rt   0       0      0      0 S  0.0  0.0   0:00.03 migration/0
   16 root      20   0       0      0      0 S  0.0  0.0   0:00.00 cpuhp/0
   18 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kdevtmpfs
   19 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 netns
   22 root      20   0       0      0      0 S  0.0  0.0   0:00.01 kauditd
  264 root      20   0       0      0      0 S  0.0  0.0   0:00.00 khungtaskd
  265 root      20   0       0      0      0 S  0.0  0.0   0:00.00 oom_reaper
  266 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 writeback
  268 root      20   0       0      0      0 S  0.0  0.0   0:00.16 kcompactd0
  269 root      25   5       0      0      0 S  0.0  0.0   0:00.00 ksmd
  270 root      39  19       0      0      0 S  0.0  0.0   0:00.00 khugepaged
  325 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 kintegrityd
  327 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 kblockd
  328 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 blkcg_punt_bio
  680 root      20   0       0      0      0 S  0.0  0.0   0:00.00 xen-balloon
  686 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 tpm_dev_wq
  692 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 md
  695 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 edac-poller
  700 root     -51   0       0      0      0 S  0.0  0.0   0:00.00 watchdogd
  849 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kswapd0
```

ssh://ec2-user@3.111.96.10:22

Here, we can see that CPU utilization percentage is 99.7% and scale-out alarm is triggered.



CloudWatch > Alarms > Scale-Out

Alarms (2)

Scale-Out
Metric alarm
In alarm

Scale-In
Metric alarm
OK

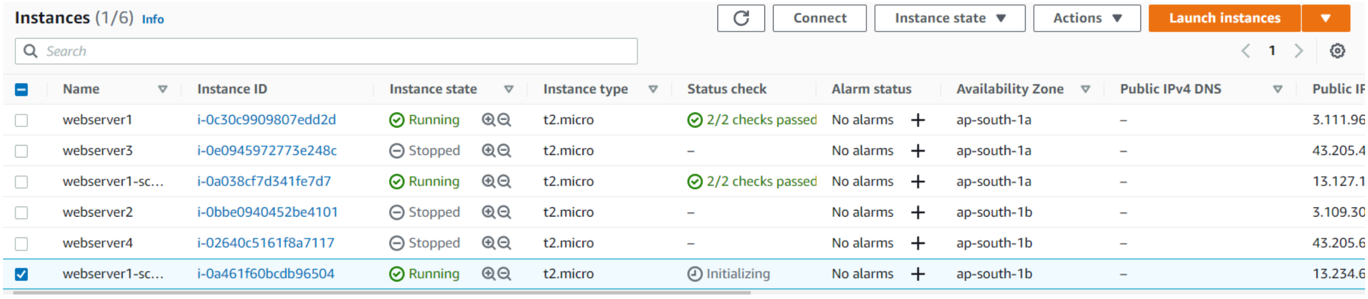
Scale-Out

Graph

CPUUtilization
CPUUtilization > 70 for 1 datapoints within 1 minute

Click timeline to see the state change at the selected time.

10. In the backend, servers started to deploy automatically to manage the traffic of CPU.

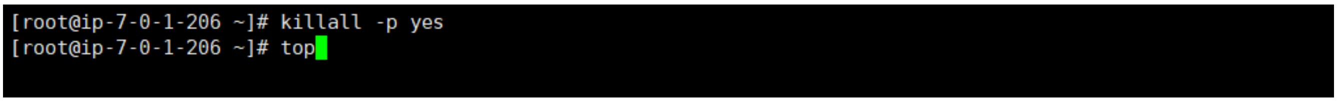


Instances (1/6) Info

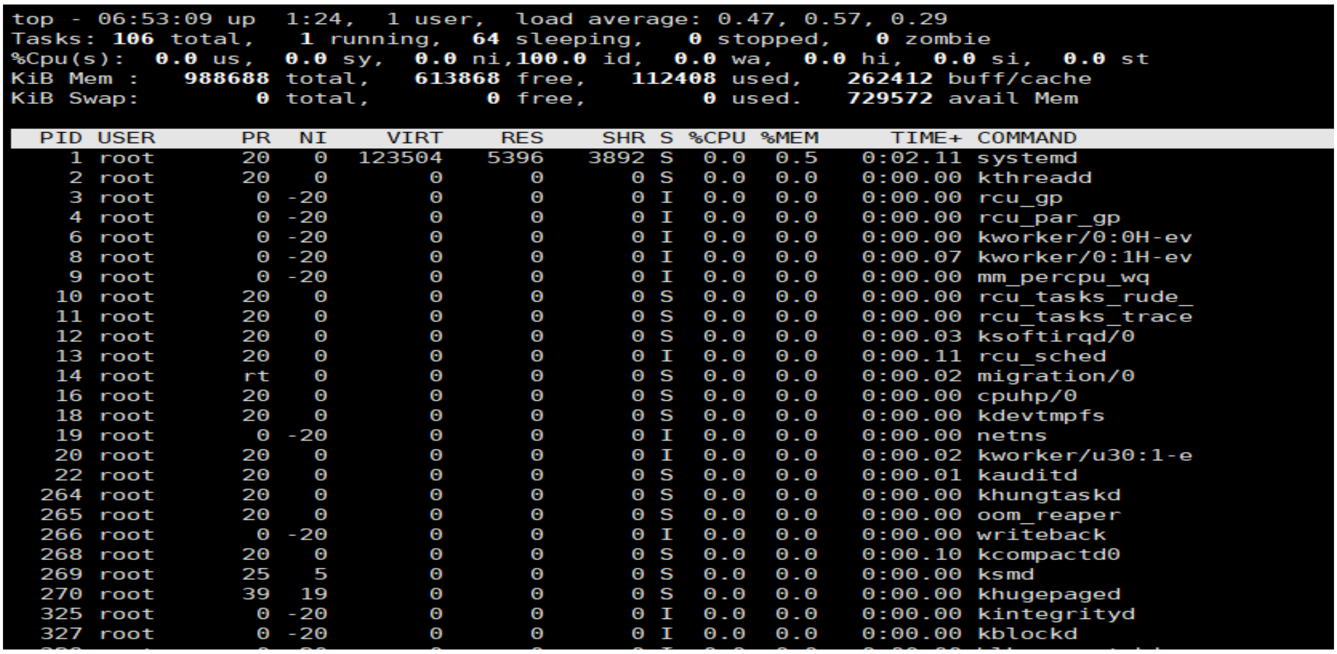
	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IP
□	webserver1	i-0c30c9909807edd2d	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	–	3.111.96
□	webserver3	i-0e0945972773e248c	Stopped	t2.micro	–	No alarms	ap-south-1a	–	43.205.4
□	webserver1-sc...	i-0a038cf7d341fe7d7	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	–	13.127.1
□	webserver2	i-0bbe0940452be4101	Stopped	t2.micro	–	No alarms	ap-south-1b	–	3.109.30
□	webserver4	i-02640c5161f8a7117	Stopped	t2.micro	–	No alarms	ap-south-1b	–	43.205.6
☑	webserver1-sc...	i-0a461f60bcdb96504	Running	t2.micro	Initializing	No alarms	ap-south-1b	–	13.234.6

11. After that I decreased the CPU utilization of the server using the command “killall -p yes”. Then used “top” command to get the metrics.

We can see that CPU utilization has dropped close to 0%.



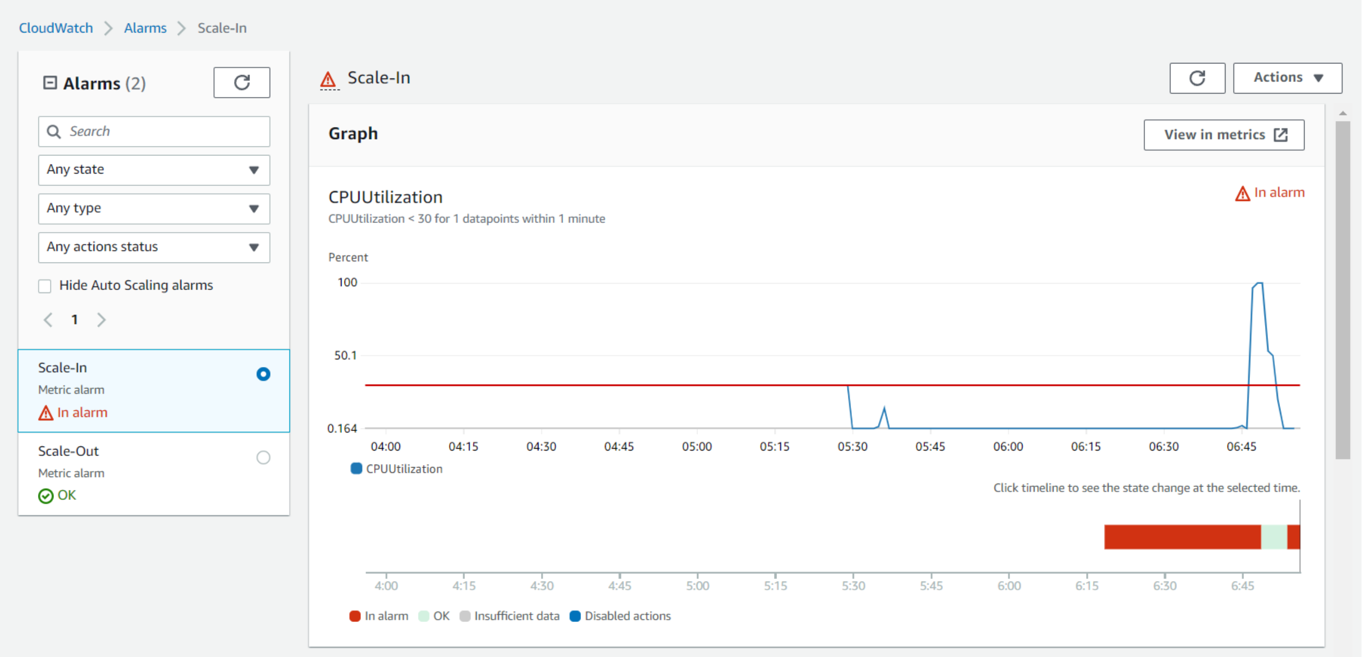
```
[root@ip-7-0-1-206 ~]# killall -p yes
[root@ip-7-0-1-206 ~]# top
```



```
top - 06:53:09 up  1:24,  1 user,  load average: 0.47, 0.57, 0.29
Tasks: 106 total,   1 running,  64 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :   988688 total,   613868 free,   112408 used,   262412 buff/cache
KiB Swap:        0 total,        0 free,        0 used.   729572 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S %CPU %MEM     TIME+ COMMAND
    1 root      20   0  123504   5396   3892 S  0.0  0.5   0:02.11 systemd
    2 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kthreadd
    3 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 rcu_gp
    4 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 rcu_par_gp
    6 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 kworker/0:0H-ev
    8 root       0 -20       0      0      0 I  0.0  0.0   0:00.07 kworker/0:1H-ev
    9 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 mm_percpu_wq
   10 root      20   0       0      0      0 S  0.0  0.0   0:00.00 rcu_tasks_rude_
   11 root      20   0       0      0      0 S  0.0  0.0   0:00.00 rcu_tasks_trace
   12 root      20   0       0      0      0 S  0.0  0.0   0:00.03 ksoftirqd/0
   13 root      20   0       0      0      0 I  0.0  0.0   0:00.11 rcu_sched
   14 root      rt   0       0      0      0 S  0.0  0.0   0:00.02 migration/0
   16 root      20   0       0      0      0 S  0.0  0.0   0:00.00 cpuhp/0
   18 root      20   0       0      0      0 S  0.0  0.0   0:00.00 kdevtmpfs
   19 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 netns
   20 root      20   0       0      0      0 I  0.0  0.0   0:00.02 kworker/u30:1-e
   22 root      20   0       0      0      0 S  0.0  0.0   0:00.01 kauditd
  264 root      20   0       0      0      0 S  0.0  0.0   0:00.00 khungtaskd
  265 root      20   0       0      0      0 S  0.0  0.0   0:00.00 oom_reaper
  266 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 writeback
  268 root      20   0       0      0      0 S  0.0  0.0   0:00.10 kcompactd0
  269 root      25   5       0      0      0 S  0.0  0.0   0:00.00 ksmd
  270 root      39  19       0      0      0 S  0.0  0.0   0:00.00 khugepaged
  325 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 kintegrityd
  327 root       0 -20       0      0      0 I  0.0  0.0   0:00.00 kblockd
```

We can see that the scale in alarm has been triggered in the alarm section.



CloudWatch > Alarms > Scale-In

Alarms (2)

Search

Any state

Any type

Any actions status

□ Hide Auto Scaling alarms

Scale-In
Metric alarm
In alarm

Scale-Out
Metric alarm
OK

Scale-In

Graph

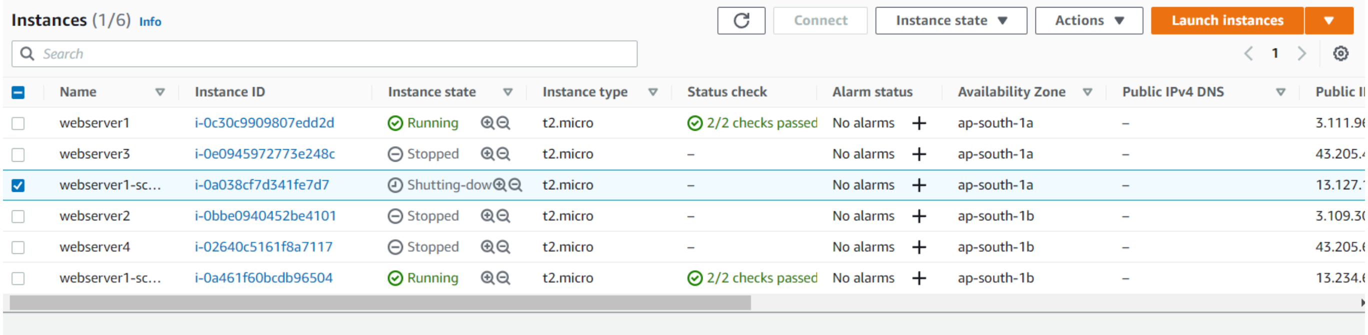
CPUUtilization

CPUUtilization < 30 for 1 datapoints within 1 minute

In alarm

Click timeline to see the state change at the selected time.

12. In the backend, the allocated servers started to terminate.



Instances (1/6) Info

☐	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public I
☐	webserver1	i-0c30c9909807edd2d	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1a	–	3.111.9
☐	webserver3	i-0e0945972773e248c	Stopped	t2.micro	–	No alarms	ap-south-1a	–	43.205.
☑	webserver1-sc...	i-0a038cf7d341fe7d7	Shutting-dow	t2.micro	–	No alarms	ap-south-1a	–	13.127.
☐	webserver2	i-0bbe0940452be4101	Stopped	t2.micro	–	No alarms	ap-south-1b	–	3.109.3
☐	webserver4	i-02640c5161f8a7117	Stopped	t2.micro	–	No alarms	ap-south-1b	–	43.205.
☐	webserver1-sc...	i-0a461f60bcdb96504	Running	t2.micro	2/2 checks passed	No alarms	ap-south-1b	–	13.234.

Sumit Mishra
190310286