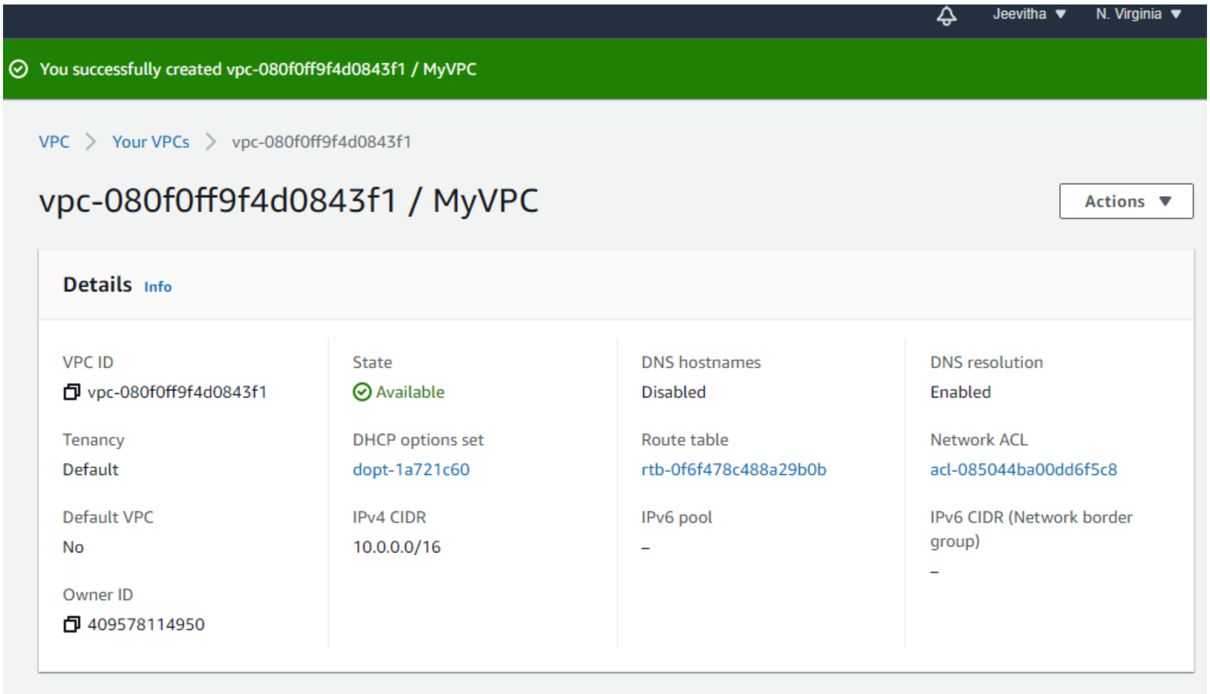
Assessment Project

Deploying a Highly Available Web Application

and Bastion Host in AWS

Task 1: Create a VPC with a private subnet and a public subnet.

1) Create a VPC with a IP of **10.0.0.0/16.**



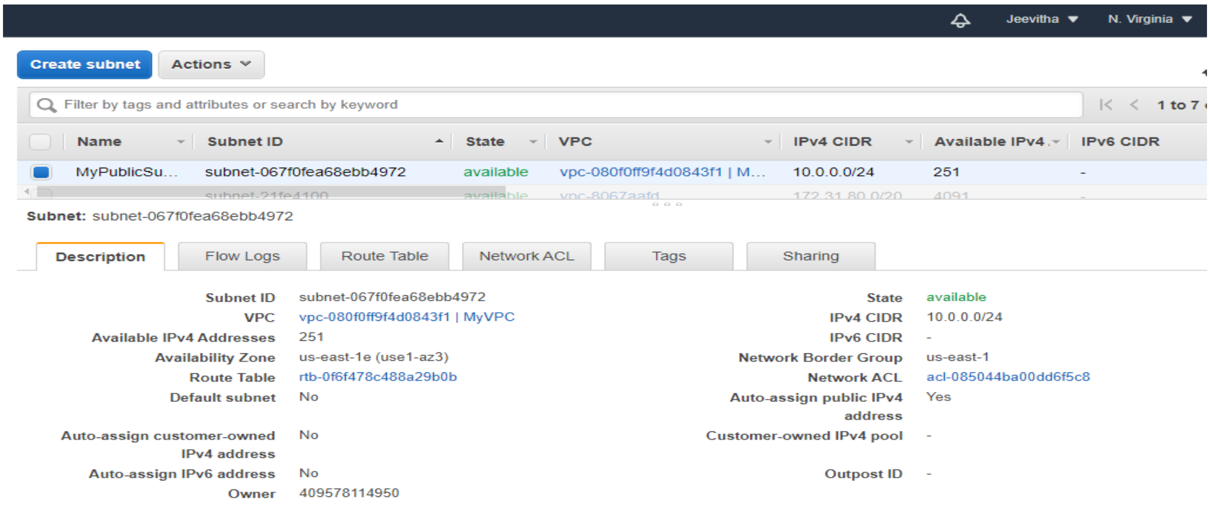
You successfully created vpc-080f0ff9f4d0843f1 / MyVPC

vpc-080f0ff9f4d0843f1 / MyVPC

Details

VPC ID vpc-080f0ff9f4d0843f1	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP options set dopt-1a721c60	Route table rtb-0f6f478c488a29b0b	Network ACL acl-085044ba00dd6f5c8
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool –	IPv6 CIDR (Network border group) –
Owner ID 409578114950			

2) Create Public subnet with range of **10.0.0.0/24** and **enable** the **Auto-assign IPv4 address**.

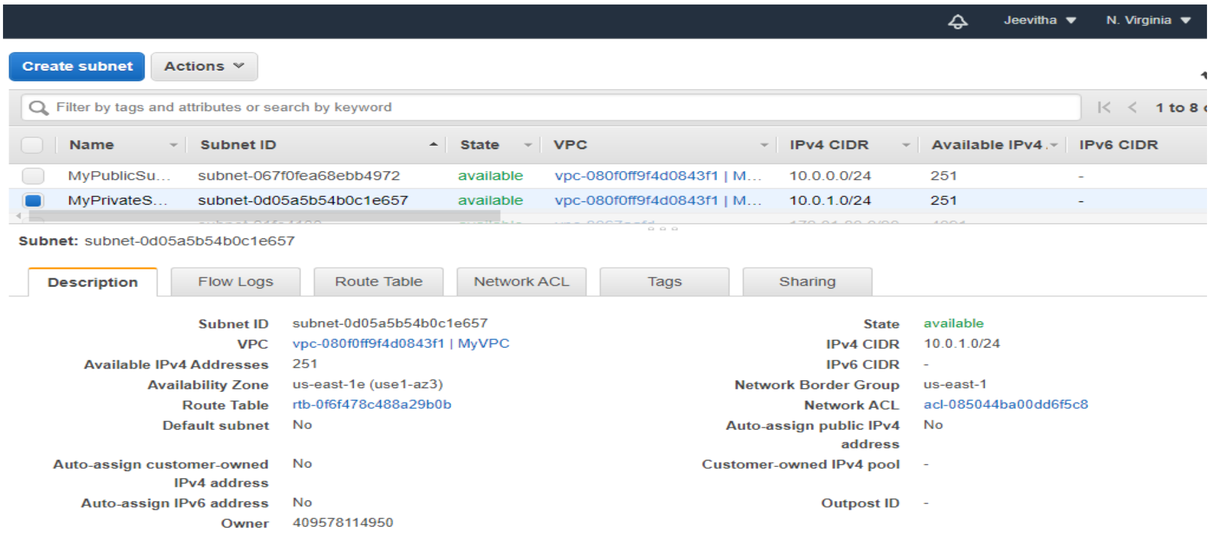


	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
■	MyPublicSu...	subnet-067f0fea68ebb4972	available	vpc-080f0ff9f4d0843f1 | M...	10.0.0.0/24	251	-
□		subnet-21fe4100	available	vpc-8067aafd	172.31.80.0/20	4091	-

Subnet: subnet-067f0fea68ebb4972

Subnet ID	subnet-067f0fea68ebb4972	State	available
VPC	vpc-080f0ff9f4d0843f1 | MyVPC	IPv4 CIDR	10.0.0.0/24
Available IPv4 Addresses	251	IPv6 CIDR	-
Availability Zone	us-east-1e (use1-az3)	Network Border Group	us-east-1
Route Table	rtb-0f6f478c488a29b0b	Network ACL	acl-085044ba00dd6f5c8
Default subnet	No	Auto-assign public IPv4 address	Yes
Auto-assign customer-owned IPv4 address	No	Customer-owned IPv4 pool	-
Auto-assign IPv6 address	No	Outpost ID	-
Owner	409578114950		

3) Create Private subnet with range of **10.0.1.0/24.**



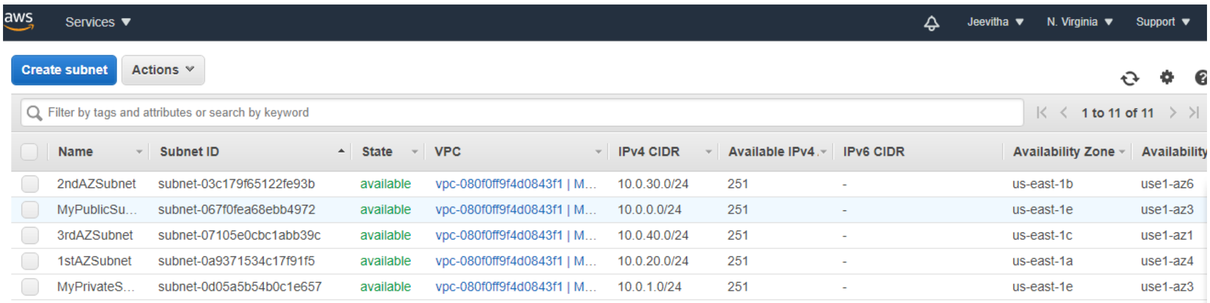
	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR
□	MyPublicSu...	subnet-067f0fea68ebb4972	available	vpc-080f0ff9f4d0843f1 | M...	10.0.0.0/24	251	-
■	MyPrivateS...	subnet-0d05a5b54b0c1e657	available	vpc-080f0ff9f4d0843f1 | M...	10.0.1.0/24	251	-

Subnet: subnet-0d05a5b54b0c1e657

Subnet ID subnet-0d05a5b54b0c1e657
VPC vpc-080f0ff9f4d0843f1 | MyVPC
Available IPv4 Addresses 251
Availability Zone us-east-1e (use1-az3)
Route Table rtb-0f6f478c488a29b0b
Default subnet No
Auto-assign customer-owned IPv4 address No
Auto-assign IPv6 address No
Owner 409578114950

State available
IPv4 CIDR 10.0.1.0/24
IPv6 CIDR -
Network Border Group us-east-1
Network ACL acl-085044ba00dd6f5c8
Auto-assign public IPv4 address No
Customer-owned IPv4 pool -
Outpost ID -

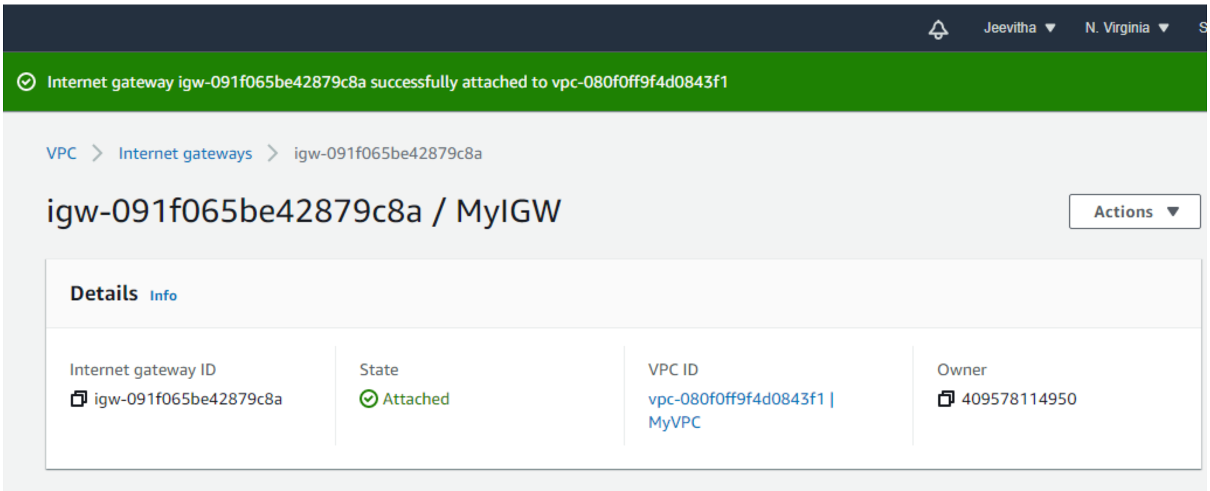
4) Create **3 more Public subnets** in **different AZ** with the range of **10.0.20.0/24, 10.0.30.0/24** and **10.0.40.0/24** and **enable auto assign ipv4 for these subnets.**



	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability
□	2ndAZSubnet	subnet-03c179f65122fe93b	available	vpc-080f0ff9f4d0843f1 | M...	10.0.30.0/24	251	-	us-east-1b	use1-az6
□	MyPublicSu...	subnet-067f0fea68ebb4972	available	vpc-080f0ff9f4d0843f1 | M...	10.0.0.0/24	251	-	us-east-1e	use1-az3
□	3rdAZSubnet	subnet-07105e0cbc1abb39c	available	vpc-080f0ff9f4d0843f1 | M...	10.0.40.0/24	251	-	us-east-1c	use1-az1
□	1stAZSubnet	subnet-0a9371534c17f91f5	available	vpc-080f0ff9f4d0843f1 | M...	10.0.20.0/24	251	-	us-east-1a	use1-az4
□	MyPrivateS...	subnet-0d05a5b54b0c1e657	available	vpc-080f0ff9f4d0843f1 | M...	10.0.1.0/24	251	-	us-east-1e	use1-az3

Task 2: Create a IGW and associate with the public subnet.

1) Create **Internet gateway** and **attached to the VPC.**



Internet gateway igw-091f065be42879c8a successfully attached to vpc-080f0ff9f4d0843f1

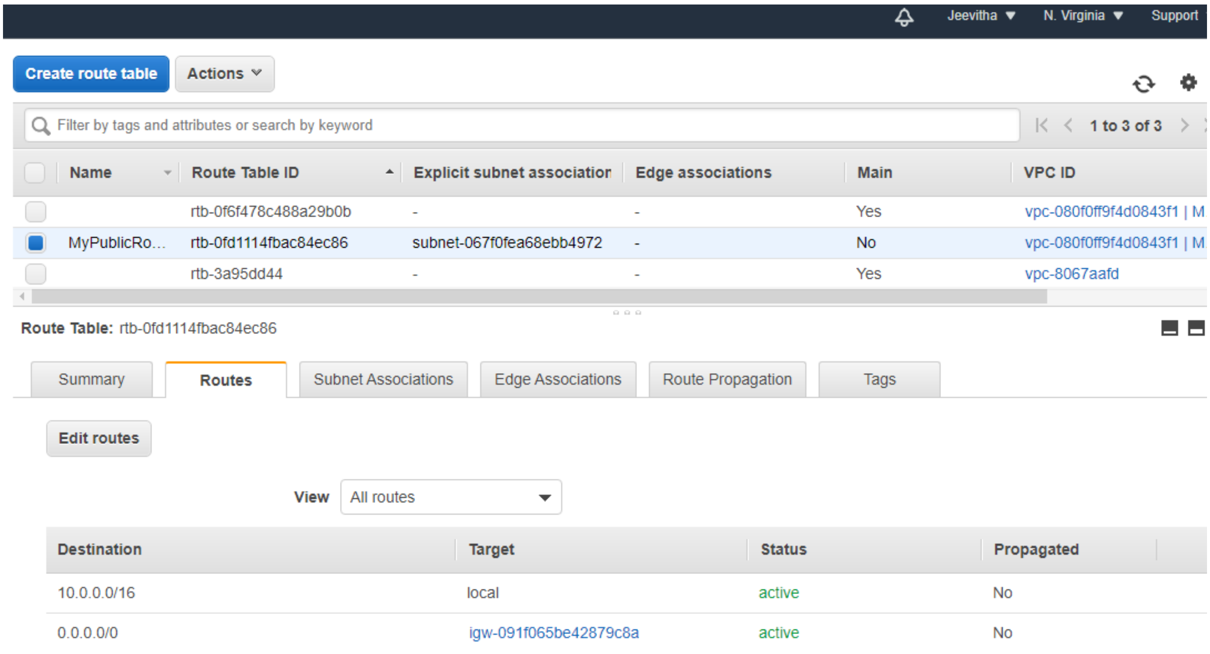
igw-091f065be42879c8a / MyIGW

Details Info

Internet gateway ID	State	VPC ID	Owner
igw-091f065be42879c8a	✓ Attached	vpc-080f0ff9f4d0843f1 | MyVPC	409578114950

Task 3: Create Public Route Table and associated with IGW.

1) Create **Public Route Table** and click to **edit routes**. Add routes to **0.0.0.0/0** with **IGW.**



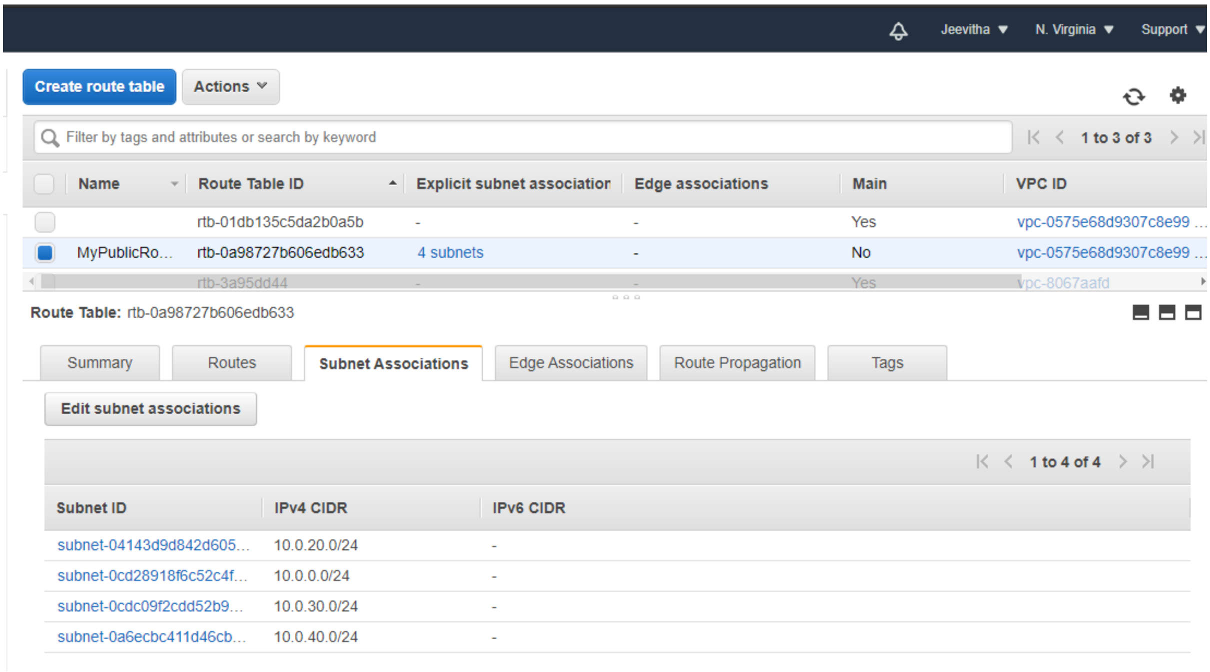
□	Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
□		rtb-0f6f478c488a29b0b	-	-	Yes	vpc-080f0ff9f4d0843f1 | M
☑	MyPublicRo...	rtb-0fd1114fbac84ec86	subnet-067f0fea68ebb4972	-	No	vpc-080f0ff9f4d0843f1 | M
□		rtb-3a95dd44	-	-	Yes	vpc-8067aafd

Route Table: rtb-0fd1114fbac84ec86

View All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-091f065be42879c8a	active	No

2) **Edit** the **Subnet Association** and add **all public subnets**.



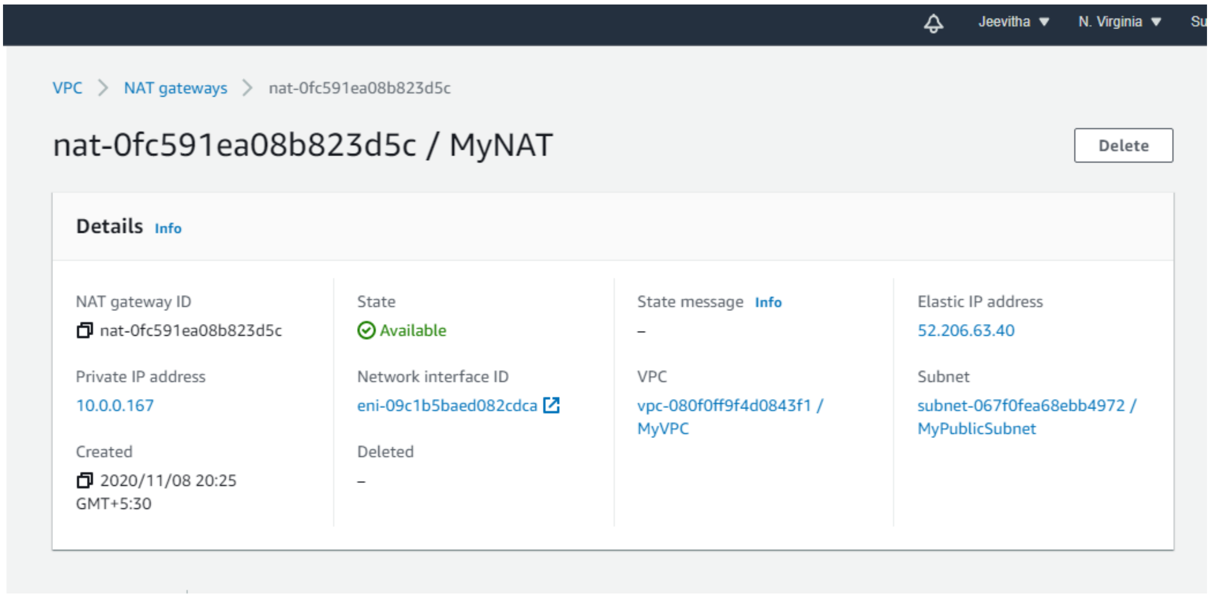
□	Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
□		rtb-01db135c5da2b0a5b	-	-	Yes	vpc-0575e68d9307c8e99 ...
☑	MyPublicRo...	rtb-0a98727b606edb633	4 subnets	-	No	vpc-0575e68d9307c8e99 ...
□		rtb-3a95dd44	-	-	Yes	vpc-8067aafd

Route Table: rtb-0a98727b606edb633

Subnet ID	IPv4 CIDR	IPv6 CIDR
subnet-04143d9d842d605...	10.0.20.0/24	-
subnet-0cd28918f6c52c4f...	10.0.0.0/24	-
subnet-0cdc09f2cdd52b9...	10.0.30.0/24	-
subnet-0a6ecbc411d46cb...	10.0.40.0/24	-

Task 4: Create NAT Gateway and allocate Elastic IP.

1) **Create NAT Gateway** with **Elastic IP.**



VPC > NAT gateways > nat-0fc591ea08b823d5c

nat-0fc591ea08b823d5c / MyNAT

Details Info

NAT gateway ID: nat-0fc591ea08b823d5c

State: ✓ Available

State message Info: –

Elastic IP address: 52.206.63.40

Private IP address: 10.0.0.167

Network interface ID: eni-09c1b5baed082cdca

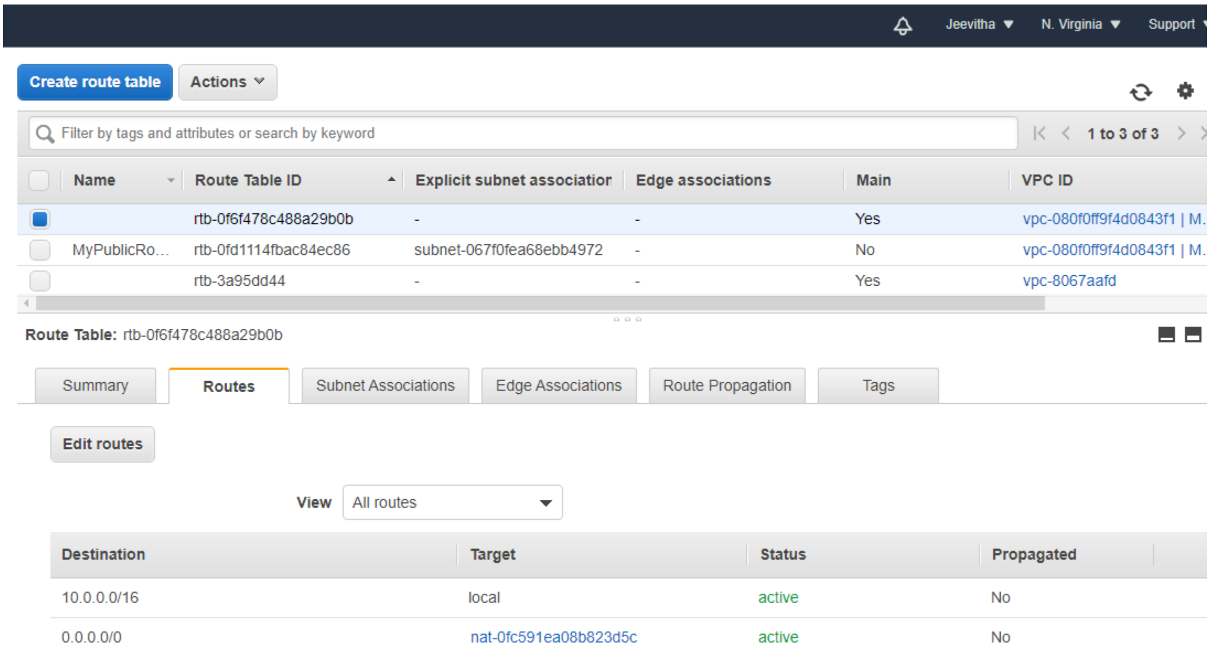
VPC: vpc-080f0ff9f4d0843f1 / MyVPC

Subnet: subnet-067f0fea68ebb4972 / MyPublicSubnet

Created: 2020/11/08 20:25 GMT+5:30

Deleted: –

2) **Attach NAT Gateway** with **0.0.0.0/0** in Route Table which has **MyVPC ID without name**.



	Name	Route Table ID	Explicit subnet associatior	Edge associations	Main	VPC ID
■		rtb-0f6f478c488a29b0b	-	-	Yes	vpc-080f0ff9f4d0843f1 | M.
□	MyPublicRo...	rtb-0fd1114fbac84ec86	subnet-067f0fea68ebb4972	-	No	vpc-080f0ff9f4d0843f1 | M.
□		rtb-3a95dd44	-	-	Yes	vpc-8067aafd

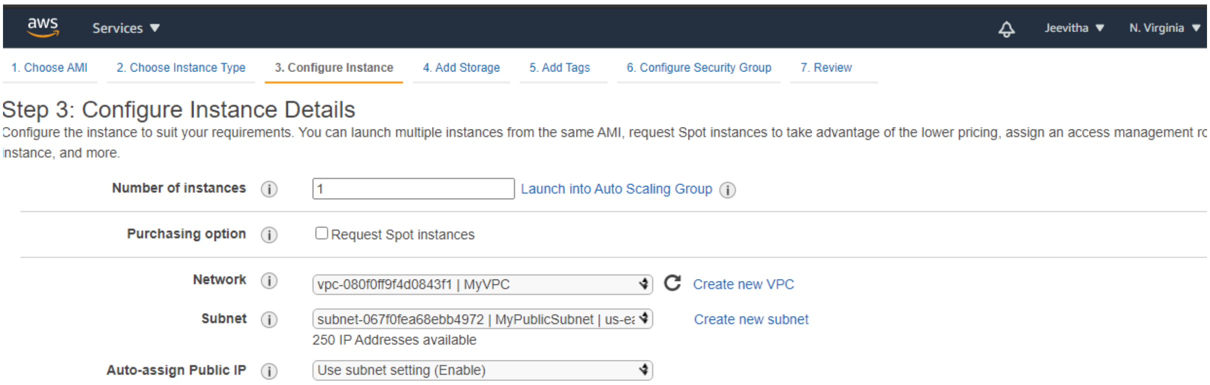
Route Table: rtb-0f6f478c488a29b0b

View: All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	nat-0fc591ea08b823d5c	active	No

Task 5: Create Bastion Host in Public Subnet with configured security group.

1) Create Linux instance for **Bastion Host** in **MyVPC Public subnet.**



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management rc
nstance, and more.

Number of instances: 1 — Launch into Auto Scaling Group

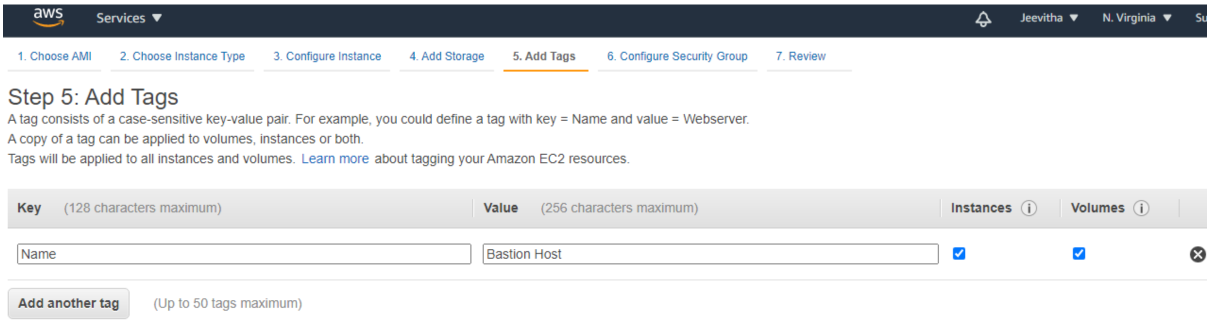
Purchasing option: □ Request Spot instances

Network: vpc-080f0ff9f4d0843f1 | MyVPC — Create new VPC

Subnet: subnet-067f0fea68ebb4972 | MyPublicSubnet | us-ea — Create new subnet
250 IP Addresses available

Auto-assign Public IP: Use subnet setting (Enable)

2) Add **Tags** then **Key** as **Name** and **Value** as **Bastion Host**.



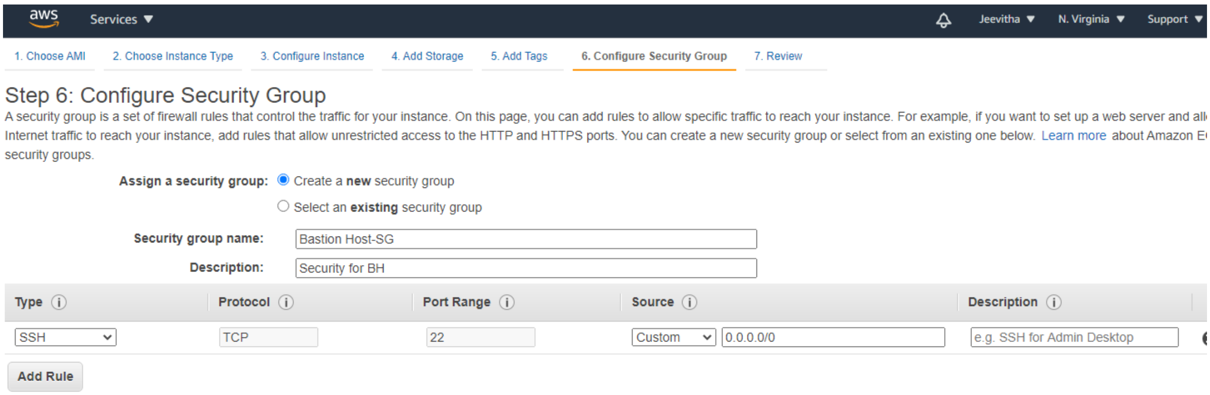
Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Name	Bastion Host	☑	☑

(Up to 50 tags maximum)

3) **Configure Security Group Name** as **Bastion Host-SG** and **Description as Security as BH.** Remaining as Deafault**.**



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and all
Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon E
security groups.

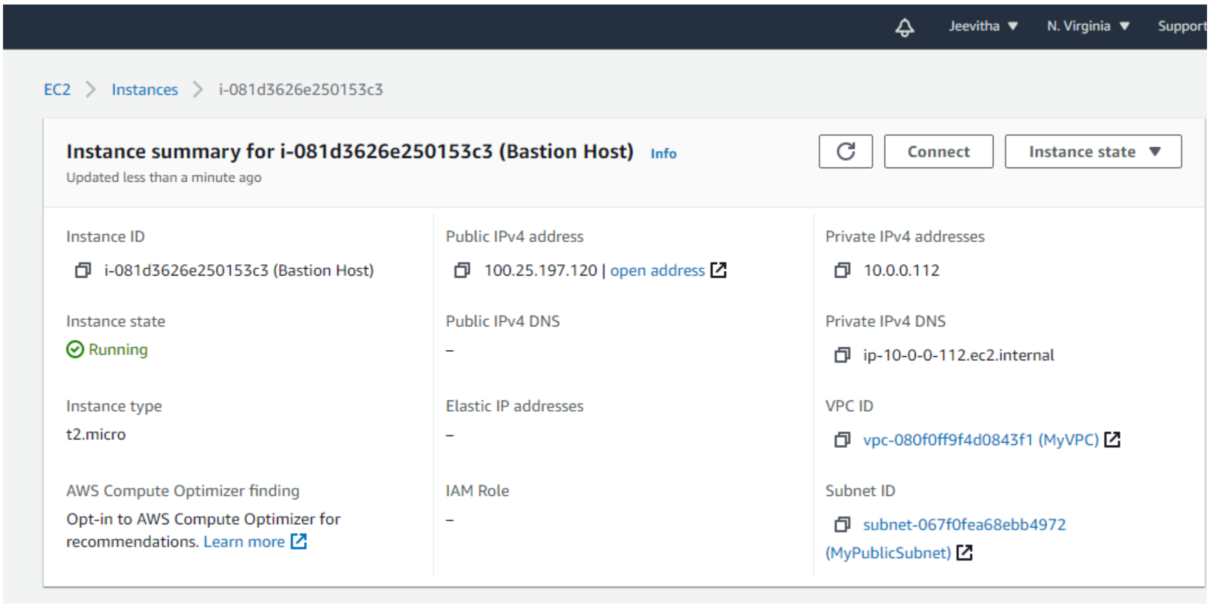
Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: Bastion Host-SG

Description: Security for BH

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

4) **Review and Launch** the Instance**.**



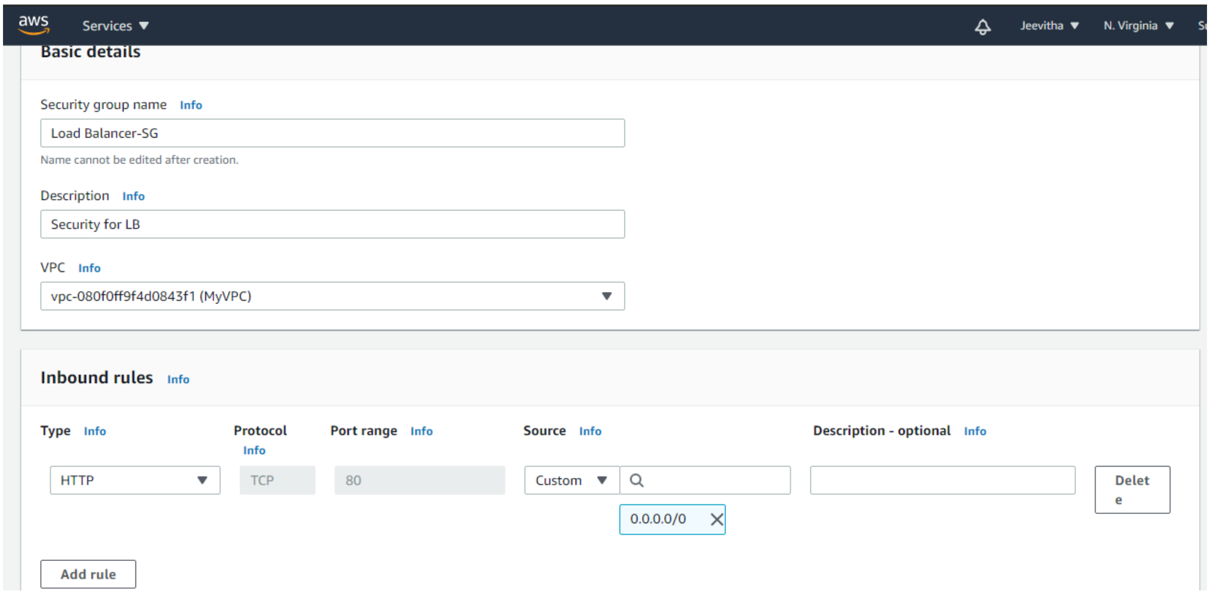
Instance summary for i-081d3626e250153c3 (Bastion Host) Info

Updated less than a minute ago

Instance ID i-081d3626e250153c3 (Bastion Host)	Public IPv4 address 100.25.197.120 | open address	Private IPv4 addresses 10.0.0.112
Instance state Running	Public IPv4 DNS –	Private IPv4 DNS ip-10-0-0-112.ec2.internal
Instance type t2.micro	Elastic IP addresses –	VPC ID vpc-080f0ff9f4d0843f1 (MyVPC)
AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. Learn more	IAM Role –	Subnet ID subnet-067f0fea68ebb4972 (MyPublicSubnet)

Task 5: Create security group for Load Balancer.

1) **Name LoadBalancer-SG** and **Description** as **Seurity for LB.** Add **inbound rule as HTTP wirh 0.0.0.0/0.**



Basic details

Security group name Info

Load Balancer-SG

Name cannot be edited after creation.

Description Info

Security for LB

VPC Info

vpc-080f0ff9f4d0843f1 (MyVPC)

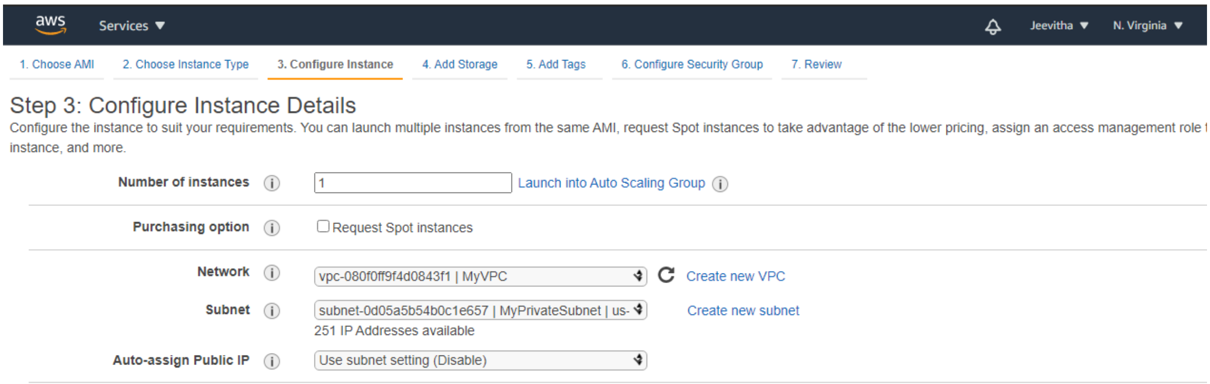
Inbound rules Info

Type	Protocol	Port range	Source	Description - optional	
HTTP	TCP	80	Custom 0.0.0.0/0		Delete

Task 6: Create WebServers in Private Subnet with configured security group.

1) Create Linux instance for **webservers** in **MyVPC Private subnet.**

   Webserver1:



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role t instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

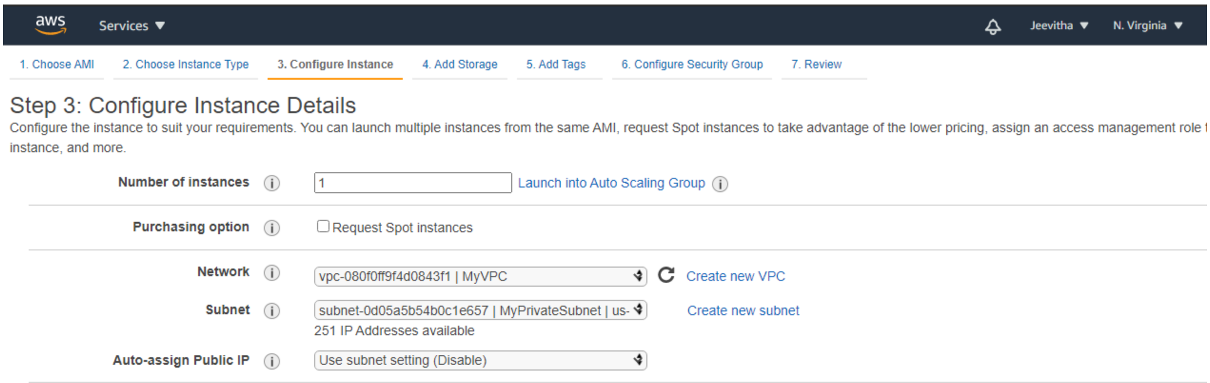
Purchasing option: □ Request Spot instances

Network: vpc-080f0ff9f4d0843f1 | MyVPC Create new VPC

Subnet: subnet-0d05a5b54b0c1e657 | MyPrivateSubnet | us- Create new subnet
251 IP Addresses available

Auto-assign Public IP: Use subnet setting (Disable)

   Webserver2:



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role t instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

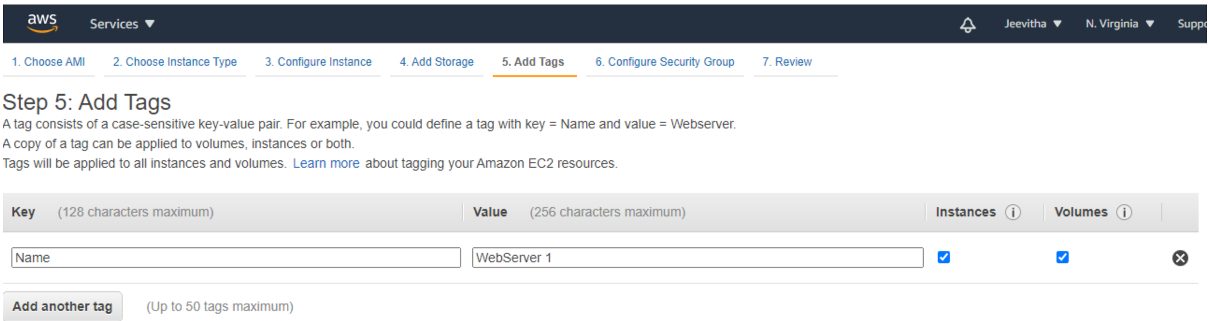
Network: vpc-080f0ff9f4d0843f1 | MyVPC Create new VPC

Subnet: subnet-0d05a5b54b0c1e657 | MyPrivateSubnet | us- Create new subnet
251 IP Addresses available

Auto-assign Public IP: Use subnet setting (Disable)

2) Add **Tags** then give **Key** as **Name** and **Value** as **Webserver1/2**.

   Webserver1:



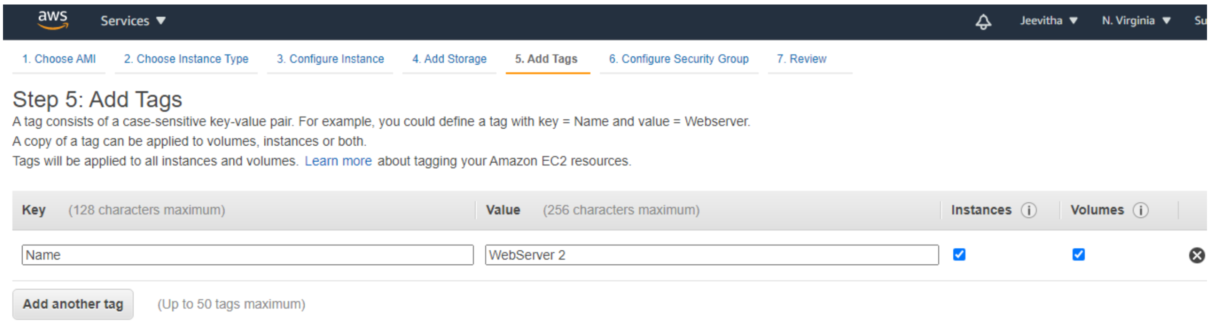
Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Name	WebServer 1	☑	☑

Add another tag (Up to 50 tags maximum)

Webserver2:



Step 5: Add Tags

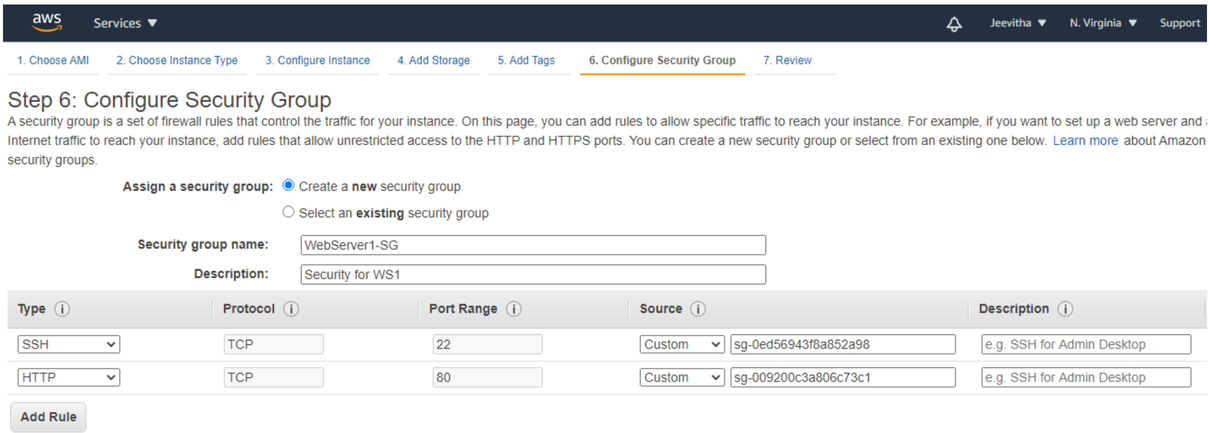
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. Learn more about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes	
Name	WebServer 2	☑	☑	⊗

(Up to 50 tags maximum)

3) **Configure Security Group Name** as **Webserver-SG** and **Description as Security as WS.** For **SSH** select **Bastion Host-SG** and for **HTTP** select as **LoadBalancer-SG.**

Webserver1:



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon security groups.

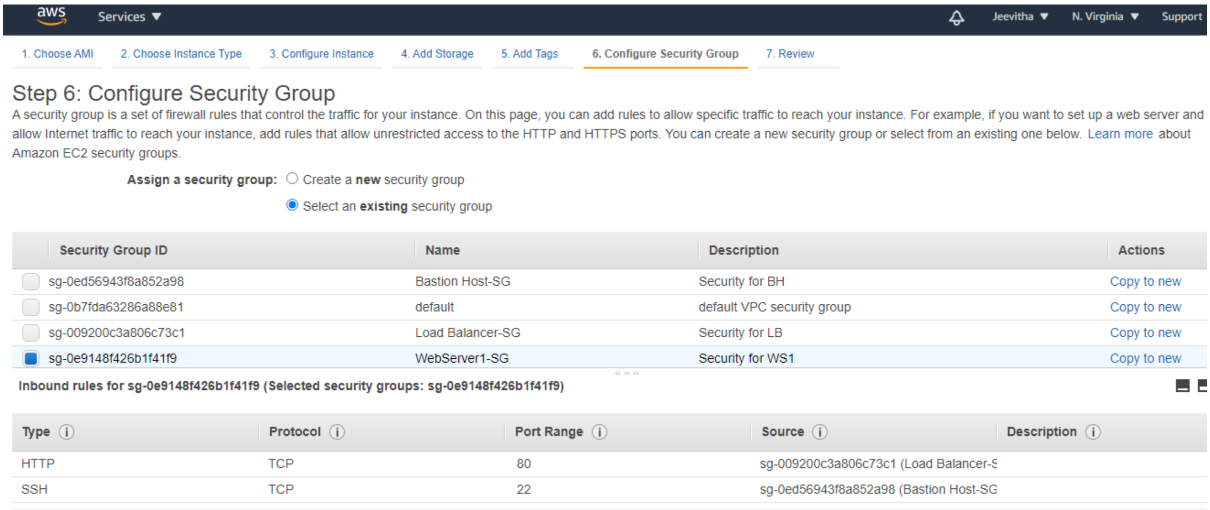
Assign a security group: ● Create a **new** security group
○ Select an **existing** security group

Security group name: WebServer1-SG

Description: Security for WS1

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	Custom	sg-0ed56943f8a852a98	e.g. SSH for Admin Desktop
HTTP	TCP	80	Custom	sg-009200c3a806c73c1	e.g. SSH for Admin Desktop

Webserver2: Select an Existing SG of Webserver-SG.



Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. Learn more about Amazon EC2 security groups.

Assign a security group: ○ Create a **new** security group
● Select an **existing** security group

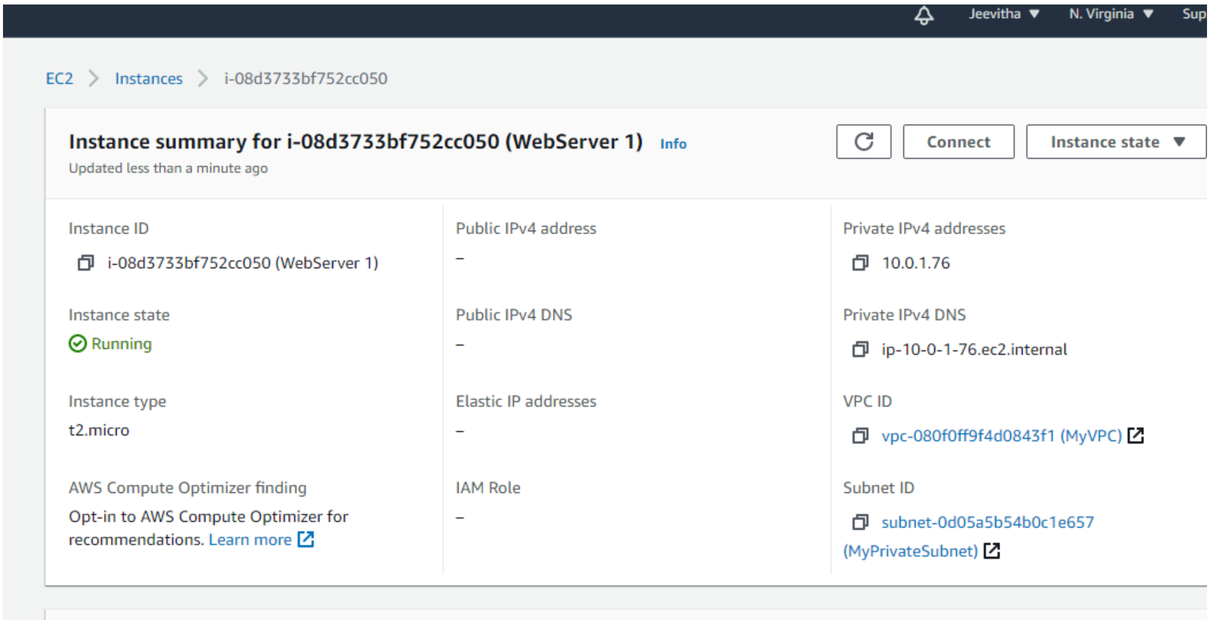
	Security Group ID	Name	Description	Actions
□	sg-0ed56943f8a852a98	Bastion Host-SG	Security for BH	Copy to new
□	sg-0b7fda63286a88e81	default	default VPC security group	Copy to new
□	sg-009200c3a806c73c1	Load Balancer-SG	Security for LB	Copy to new
■	sg-0e9148f426b1f41f9	WebServer1-SG	Security for WS1	Copy to new

Inbound rules for sg-0e9148f426b1f41f9 (Selected security groups: sg-0e9148f426b1f41f9)

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	sg-009200c3a806c73c1 (Load Balancer-S	
SSH	TCP	22	sg-0ed56943f8a852a98 (Bastion Host-SG	

4) **Review and Lauch** the instance.

Webserver1:



EC2 > Instances > i-08d3733bf752cc050

Instance summary for i-08d3733bf752cc050 (WebServer 1) Info

Updated less than a minute ago

Instance ID: i-08d3733bf752cc050 (WebServer 1)

Public IPv4 address: –

Private IPv4 addresses: 10.0.1.76

Instance state: Running

Public IPv4 DNS: –

Private IPv4 DNS: ip-10-0-1-76.ec2.internal

Instance type: t2.micro

Elastic IP addresses: –

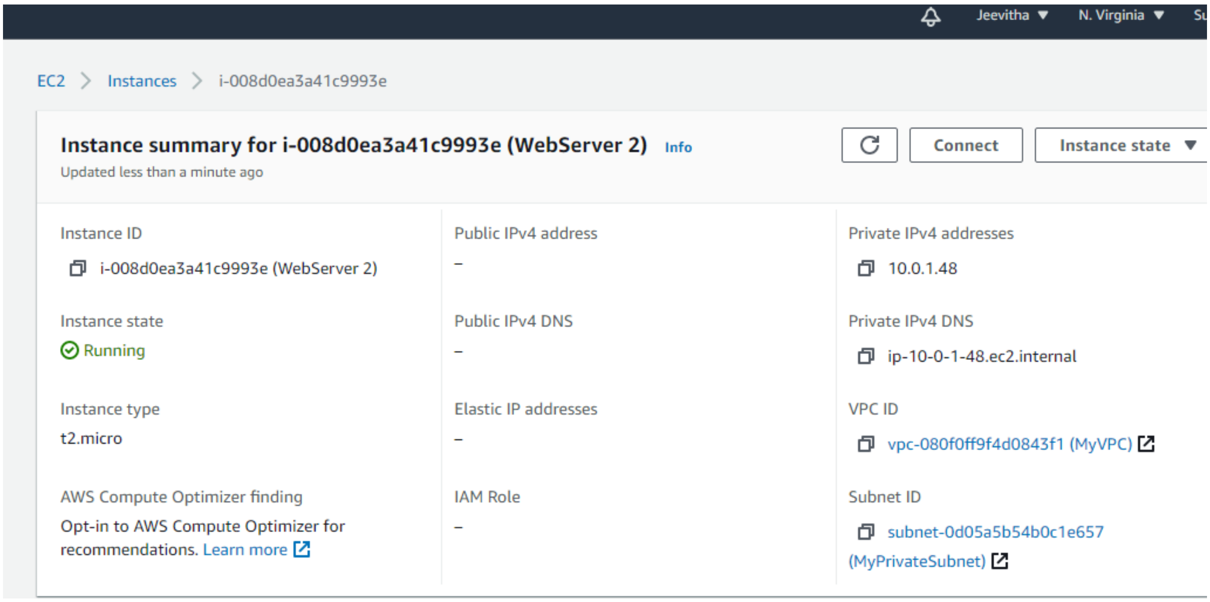
VPC ID: vpc-080f0ff9f4d0843f1 (MyVPC)

AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. Learn more

IAM Role: –

Subnet ID: subnet-0d05a5b54b0c1e657 (MyPrivateSubnet)

Webserver2:



EC2 > Instances > i-008d0ea3a41c9993e

Instance summary for i-008d0ea3a41c9993e (WebServer 2) Info

Updated less than a minute ago

Instance ID: i-008d0ea3a41c9993e (WebServer 2)

Public IPv4 address: –

Private IPv4 addresses: 10.0.1.48

Instance state: Running

Public IPv4 DNS: –

Private IPv4 DNS: ip-10-0-1-48.ec2.internal

Instance type: t2.micro

Elastic IP addresses: –

VPC ID: vpc-080f0ff9f4d0843f1 (MyVPC)

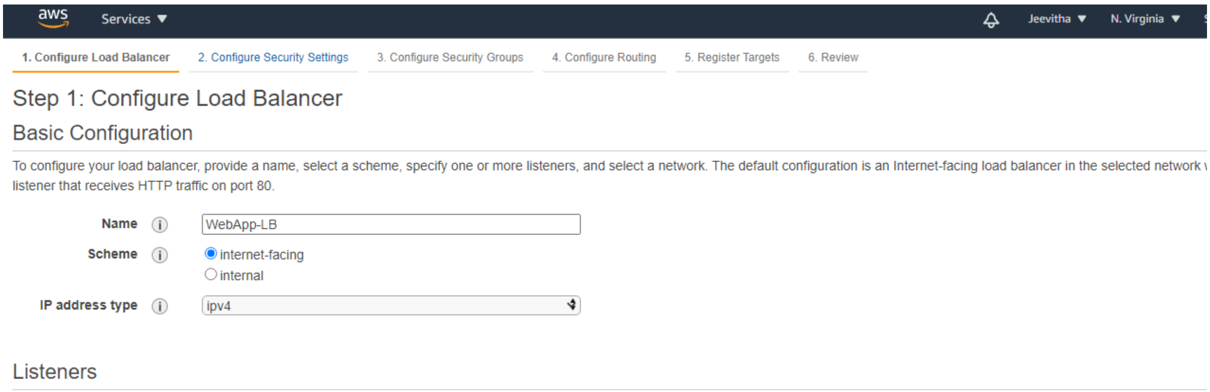
AWS Compute Optimizer finding: Opt-in to AWS Compute Optimizer for recommendations. Learn more

IAM Role: –

Subnet ID: subnet-0d05a5b54b0c1e657 (MyPrivateSubnet)

Task 7: Create LoadBalancer for Webservers.

1) Name as WebApp-LB. Select MyVPC and also select all public subnets.


aws
Services ▼
Jeevitha ▼
N. Virginia ▼
1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review

Step 1: Configure Load Balancer

Basic Configuration

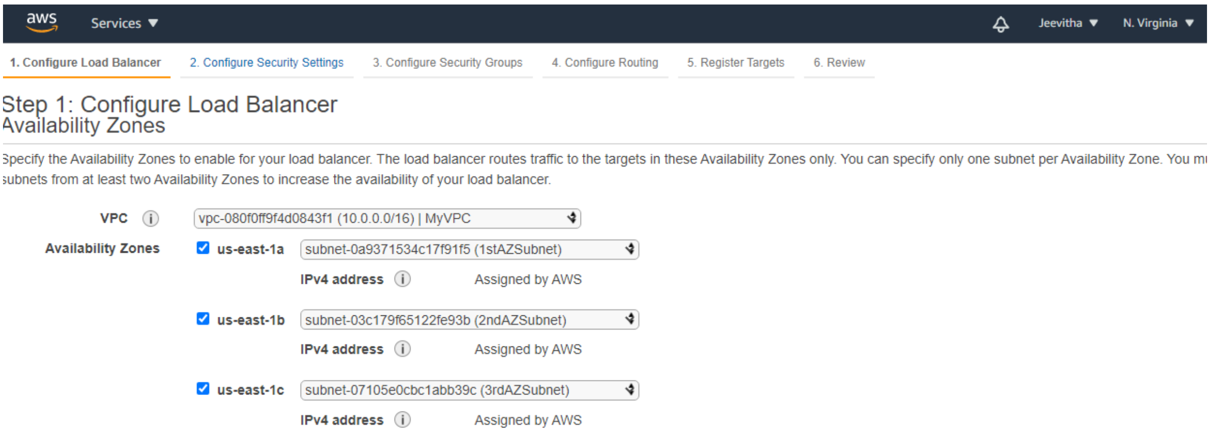
To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network listener that receives HTTP traffic on port 80.

Name: WebApp-LB

Scheme: ● internet-facing ○ internal

IP address type: ipv4

Listeners


aws
Services ▼
Jeevitha ▼
N. Virginia ▼
1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review

Step 1: Configure Load Balancer

Availability Zones

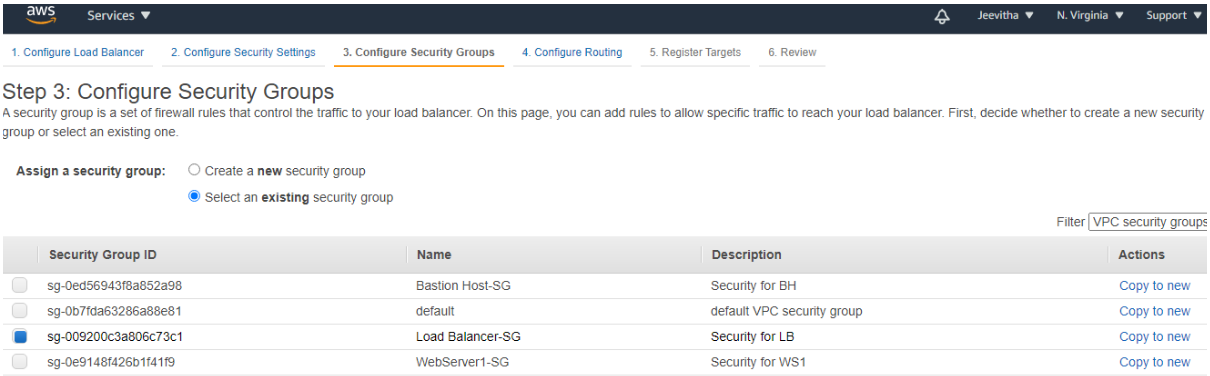
Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You m subnets from at least two Availability Zones to increase the availability of your load balancer.

VPC: vpc-080f0ff9f4d0843f1 (10.0.0.0/16) | MyVPC

Availability Zones:

- ☑ us-east-1a: subnet-0a9371534c17f91f5 (1stAZSubnet) — IPv4 address: Assigned by AWS
- ☑ us-east-1b: subnet-03c179f65122fe93b (2ndAZSubnet) — IPv4 address: Assigned by AWS
- ☑ us-east-1c: subnet-07105e0cbc1abb39c (3rdAZSubnet) — IPv4 address: Assigned by AWS

2) Select security group as **LoadBalancer-SG.**



Step 3: Configure Security Groups

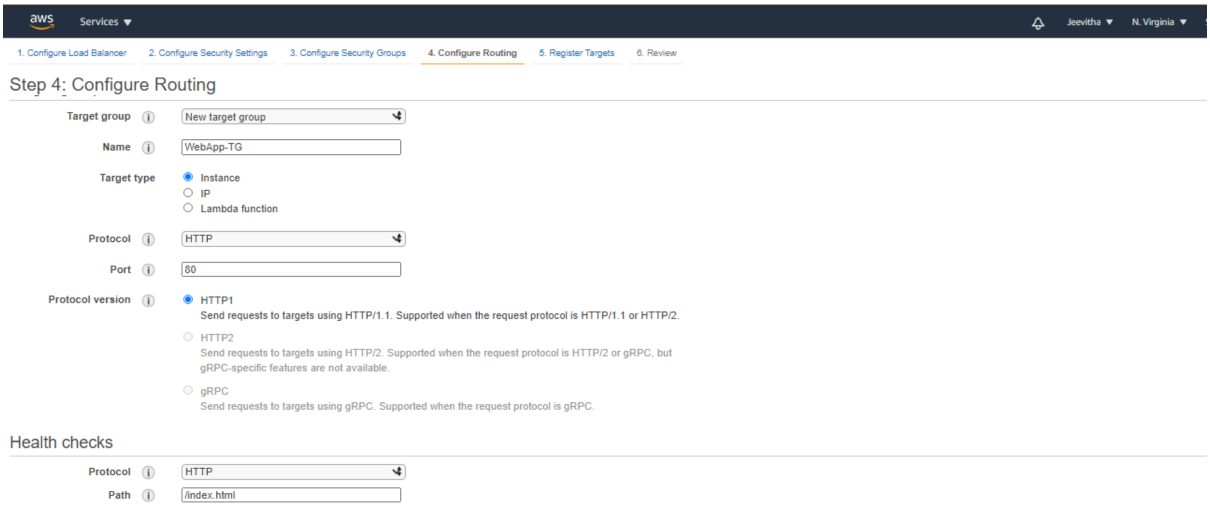
A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. First, decide whether to create a new security group or select an existing one.

Assign a security group: ○ Create a **new** security group ● Select an **existing** security group

Filter: VPC security groups

	Security Group ID	Name	Description	Actions
☐	sg-0ed56943f8a852a98	Bastion Host-SG	Security for BH	Copy to new
☐	sg-0b7fda63286a88e81	default	default VPC security group	Copy to new
☑	sg-009200c3a806c73c1	Load Balancer-SG	Security for LB	Copy to new
☐	sg-0e9148f426b1f41f9	WebServer1-SG	Security for WS1	Copy to new

3) Name as WebApp-TG and give path as index.html.


aws
Services ▼
Jeevitha ▼
N. Virginia ▼
1. Configure Load Balancer
2. Configure Security Settings
3. Configure Security Groups
4. Configure Routing
5. Register Targets
6. Review

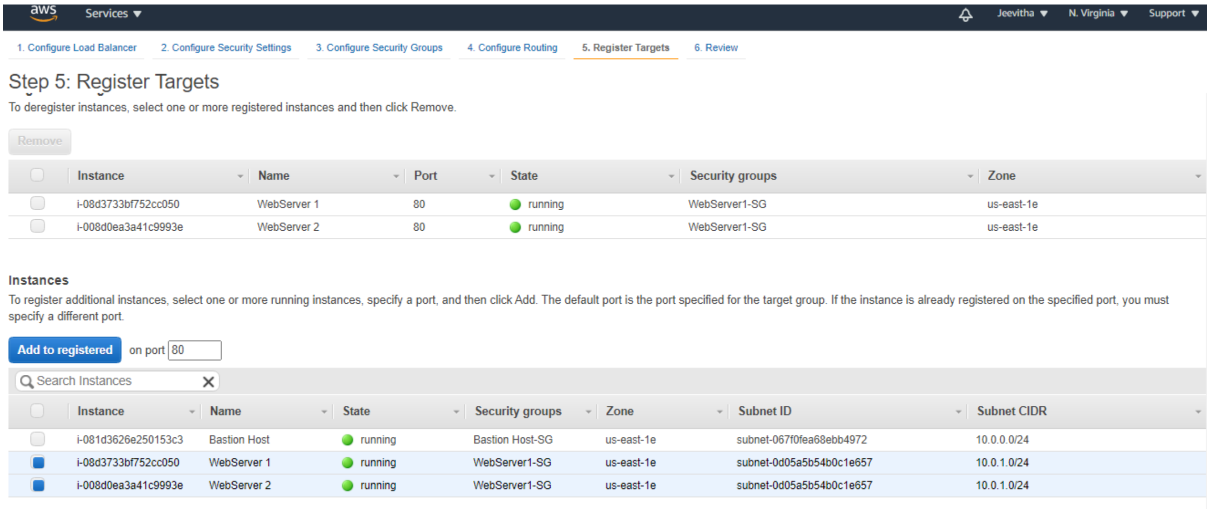
Step 4: Configure Routing

Target group	New target group
Name	WebApp-TG
Target type	● Instance ○ IP ○ Lambda function
Protocol	HTTP
Port	80
Protocol version	● HTTP1 Send requests to targets using HTTP/1.1. Supported when the request protocol is HTTP/1.1 or HTTP/2. ○ HTTP2 Send requests to targets using HTTP/2. Supported when the request protocol is HTTP/2 or gRPC, but gRPC-specific features are not available. ○ gRPC Send requests to targets using gRPC. Supported when the request protocol is gRPC.

Health checks

Protocol	HTTP
Path	/index.html

4) Register the Targets as WebServers1 and 2 and then create.



Step 5: Register Targets

To deregister instances, select one or more registered instances and then click Remove.

□	Instance	Name	Port	State	Security groups	Zone
□	i-08d3733bf752cc050	WebServer 1	80	● running	WebServer1-SG	us-east-1e
□	i-008d0ea3a41c9993e	WebServer 2	80	● running	WebServer1-SG	us-east-1e

Instances

To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

Add to registered on port 80

Search Instances

□	Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
□	i-081d3626e250153c3	Bastion Host	● running	Bastion Host-SG	us-east-1e	subnet-067f0fea68ebb4972	10.0.0.0/24
☑	i-08d3733bf752cc050	WebServer 1	● running	WebServer1-SG	us-east-1e	subnet-0d05a5b54b0c1e657	10.0.1.0/24
☑	i-008d0ea3a41c9993e	WebServer 2	● running	WebServer1-SG	us-east-1e	subnet-0d05a5b54b0c1e657	10.0.1.0/24

Task 5: Launch the Bastion Host and configure all web servers.

1. SSH into the Bastion server using the Bastion PEM key: **NVkey.pem**
2. To SSH into web servers via Bastion server, we need the web server key that we used to launch the privious web servers (web-serverkey).
3. Open the **web-serverkey** file on your local system and then **copy the text content**.
4. Navigate to the Bastion server and create a file named **web-serverkey.pem** using below command:

- **vi web-serverkey.pem**

5. Paste the content and save it by pressing **shift+colon followed by :wq!** and then enter to save your private key.
6. Make sure you have changed the **permission of the key file to 400**. You can change the permission using below command:

- **chmod 400 web-serverkey.pem**

7. Now **you can log into the web servers** using the private key copied to the bastion server with the help of below commands.

- **Note:** You **don't have a public IPs** for the web servers since we them in a private **subnet.**
- Syntax **: ssh -i web-serverkey.pem ec2-user@<**Web-server-1 private IP**>**
- Example: **ssh -i web-serverkey.pem ec2-user@172.31.101.237**

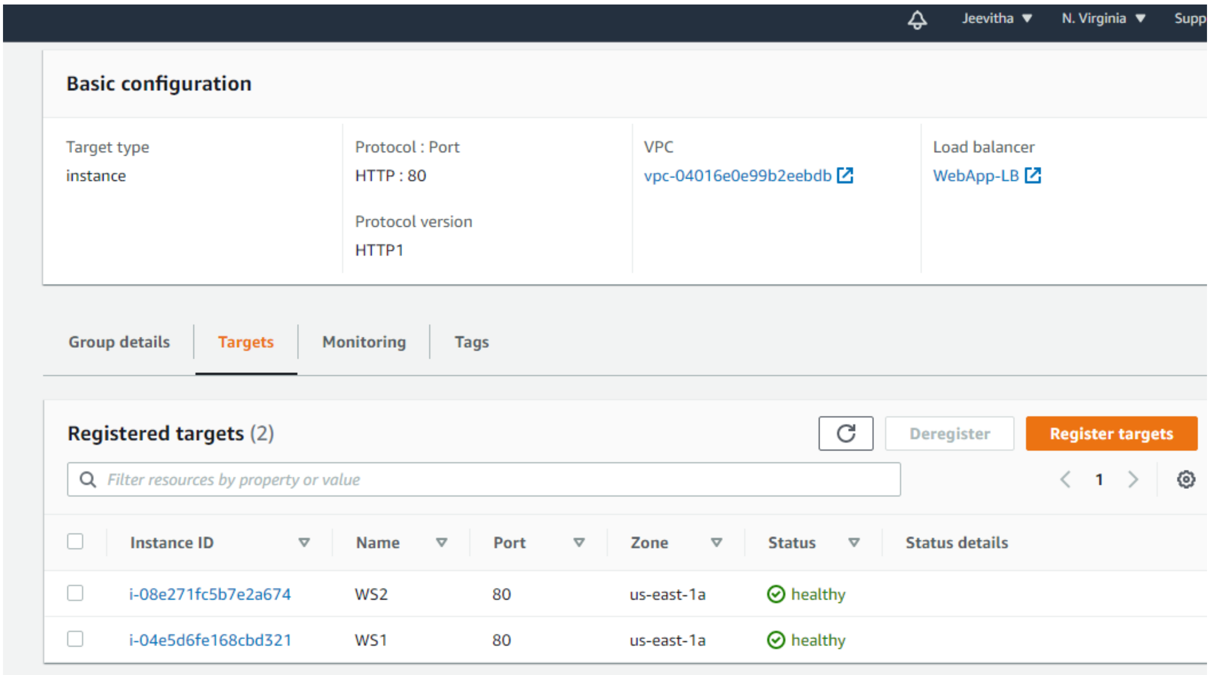
8. Now **install the apache service** using the below commands and **create a test index.html file,** which will be **used for a health check.**

- **Installing Apache:**
  - **sudo su**
  - **yum update -y**
  - yum install httpd -y
  - systemctl start httpd
  - systemctl enable httpd
  - cd /var/www/html
- **Creating the example homepage :**
  - **echo " REQUEST HANDLING BY SERVER 1" > index.html**
- **?Exit from webserver to Bastion server**
  - **?**To come out of 2nd instance, type **exit** command for coming out of root user, and **exit** command again for coming out of the instance.

9. Repeat steps 7 & 8 for web server 2 **with its respective private IP** , making sure to change the content of index.html to "**REQUEST HANDLING BY SERVER 2"**
10. To come out of 1st instance, type **exit** command for coming out of root user, and **exit** command again for coming out of the instance.

Task 8: Checking the health of the load balancer.

1) Initially checks the status of targets which shown as healthy.



Basic configuration

Target type: instance

Protocol : Port: HTTP : 80

Protocol version: HTTP1

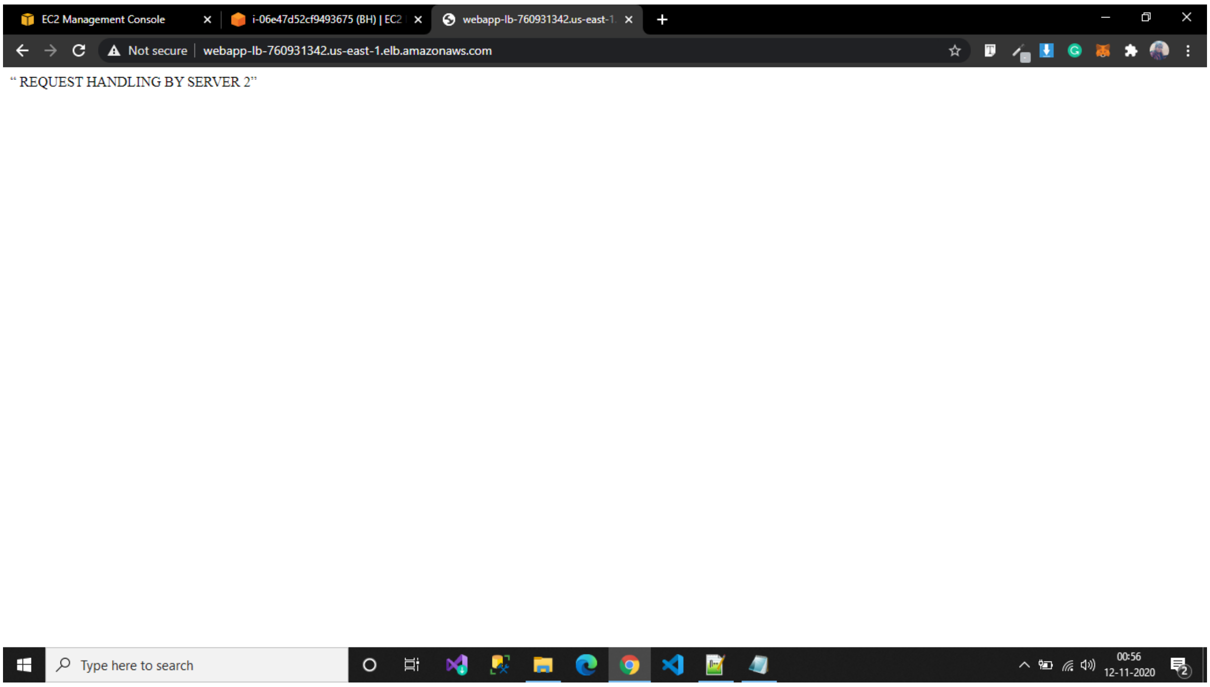
VPC: vpc-04016e0e99b2eebdb

Load balancer: WebApp-LB

Registered targets (2)

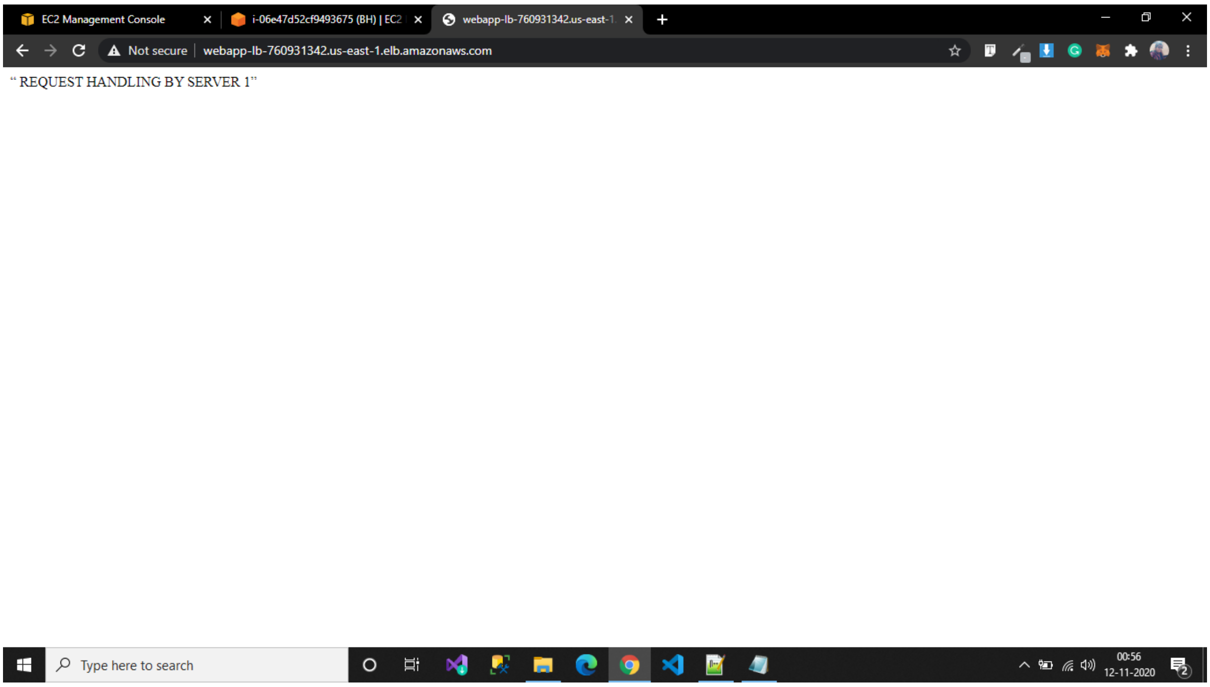
	Instance ID	Name	Port	Zone	Status	Status details
□	i-08e271fc5b7e2a674	WS2	80	us-east-1a	✓ healthy	
□	i-04e5d6fe168cbd321	WS1	80	us-east-1a	✓ healthy	

2) Now navigate to and select the load balancer that you created earlier. Click on, copy and paste it into the browser.


EC2 Management Console
i-06e47d52cf9493675 (BH) | EC2
webapp-lb-760931342.us-east-1
Not secure
webapp-lb-760931342.us-east-1.elb.amazonaws.com
Type here to search
00:56
12-11-2020

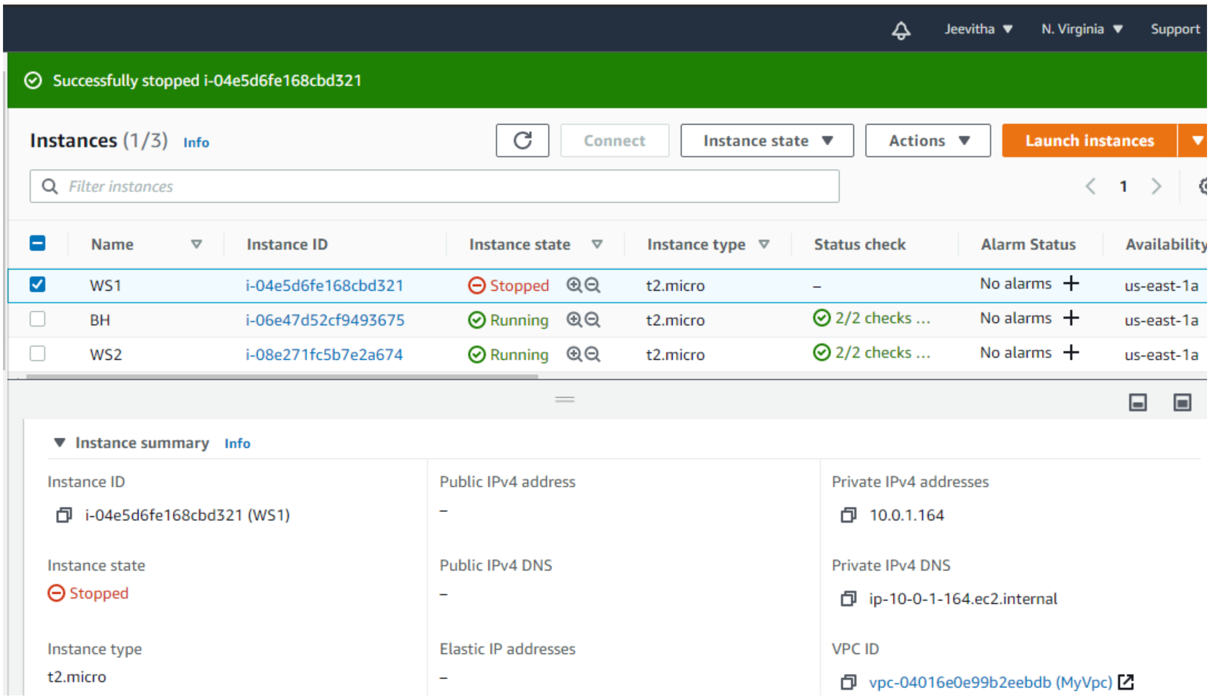
" REQUEST HANDLING BY SERVER 2"

After refreshing…


EC2 Management Console
i-06e47d52cf9493675 (BH) | EC2
webapp-lb-760931342.us-east-1
Not secure
webapp-lb-760931342.us-east-1.elb.amazonaws.com
Type here to search
00:56
12-11-2020

“ REQUEST HANDLING BY SERVER 1”

3) Navigate to the EC2 dashboard and select Web-server-1. Click on, select and then click on stop.



Successfully stopped i-04e5d6fe168cbd321

Instances (1/3) Info

	Name	Instance ID	Instance state	Instance type	Status check	Alarm Status	Availability
☑	WS1	i-04e5d6fe168cbd321	Stopped	t2.micro	–	No alarms +	us-east-1a
□	BH	i-06e47d52cf9493675	Running	t2.micro	2/2 checks ...	No alarms +	us-east-1a
□	WS2	i-08e271fc5b7e2a674	Running	t2.micro	2/2 checks ...	No alarms +	us-east-1a

▼ Instance summary Info

Instance ID
i-04e5d6fe168cbd321 (WS1)

Public IPv4 address
–

Private IPv4 addresses
10.0.1.164

Instance state
Stopped

Public IPv4 DNS
–

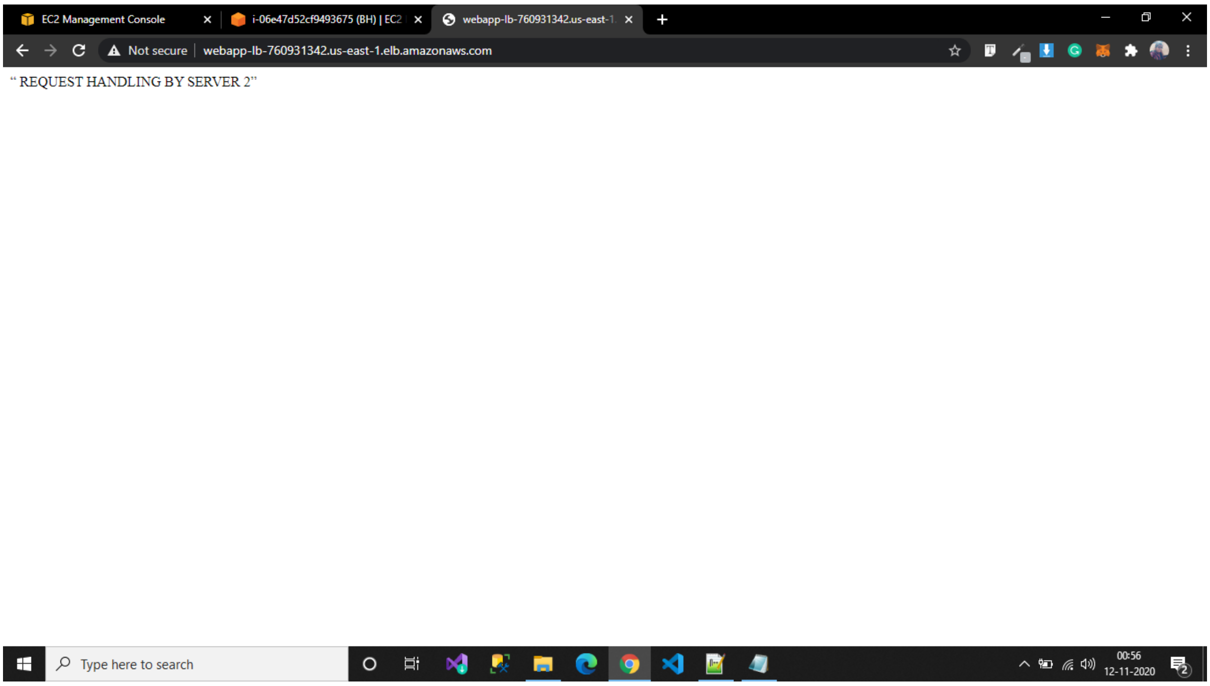
Private IPv4 DNS
ip-10-0-1-164.ec2.internal

Instance type
t2.micro

Elastic IP addresses
–

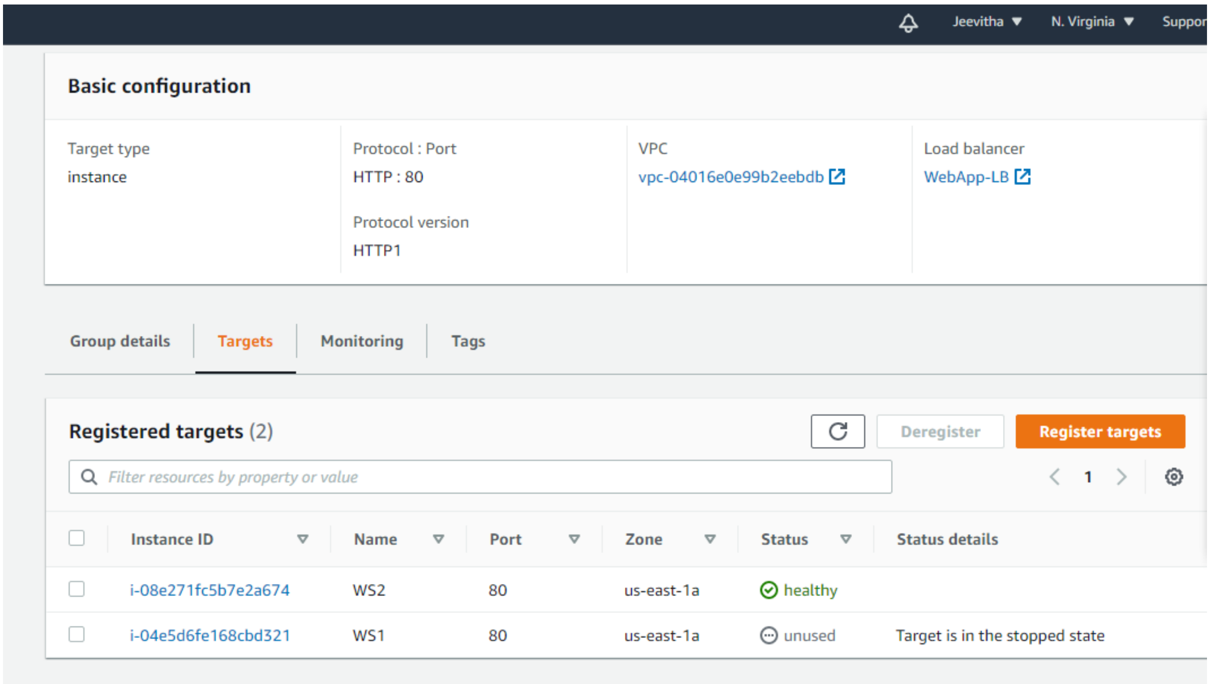
VPC ID
vpc-04016e0e99b2eebdb (MyVpc)

Now navigate to and select the load balancer that you created earlier. Click on, copy and paste it into the browser.


EC2 Management Console
i-06e47d52cf9493675 (BH) | EC2
webapp-lb-760931342.us-east-1.
Not secure
webapp-lb-760931342.us-east-1.elb.amazonaws.com
Type here to search
00:56
12-11-2020

“ REQUEST HANDLING BY SERVER 2”

Targets shown as **Unused in WS1.**



Basic configuration

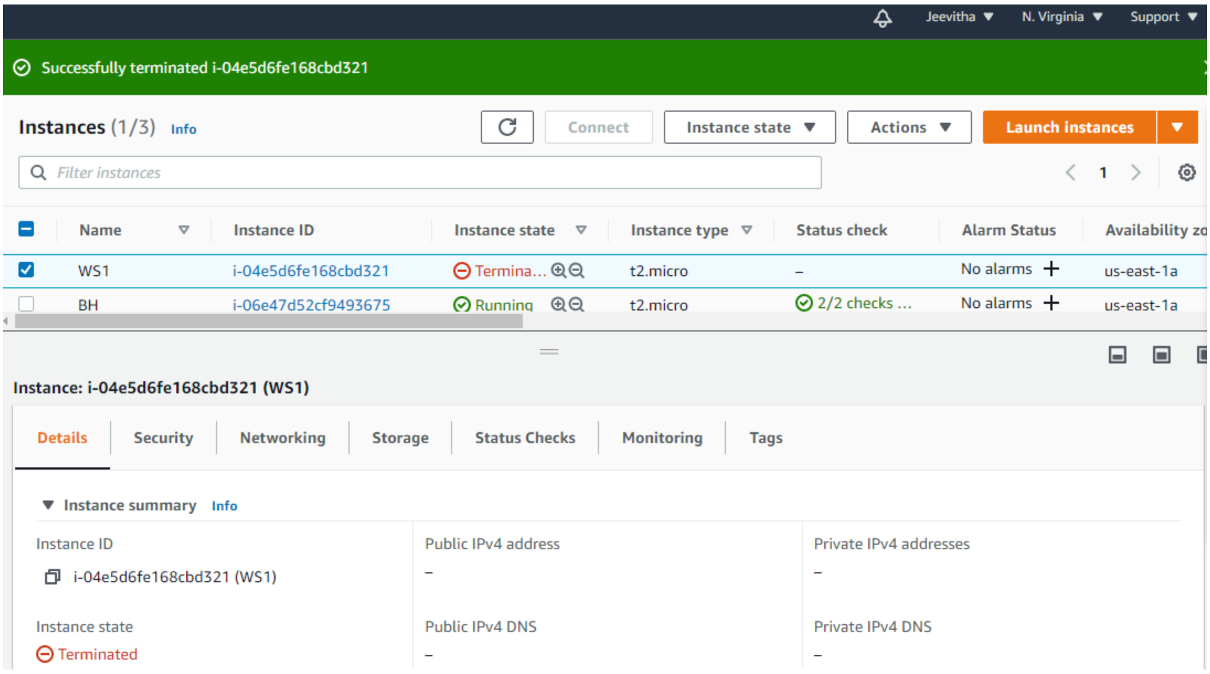
Target type	Protocol : Port	VPC	Load balancer
instance	HTTP : 80	vpc-04016e0e99b2eebdb	WebApp-LB

Protocol version
HTTP1

Registered targets (2)

□	Instance ID	Name	Port	Zone	Status	Status details
□	i-08e271fc5b7e2a674	WS2	80	us-east-1a	✓ healthy	
□	i-04e5d6fe168cbd321	WS1	80	us-east-1a	⋯ unused	Target is in the stopped state

4) Navigate to the EC2 dashboard and select Web-server-1. Click on, select and then click on Terminated.



Successfully terminated i-04e5d6fe168cbd321

Instances (1/3) Info

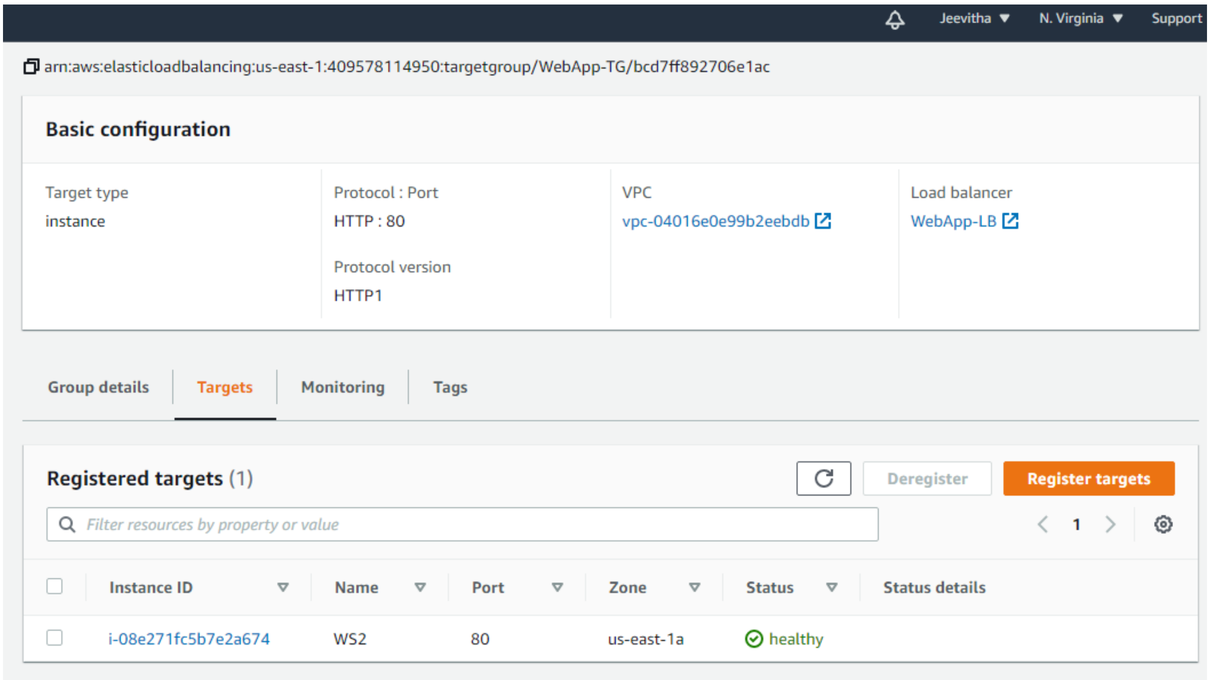
☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm Status	Availability zo
☑	WS1	i-04e5d6fe168cbd321	Termina...	t2.micro	–	No alarms +	us-east-1a
□	BH	i-06e47d52cf9493675	Running	t2.micro	2/2 checks ...	No alarms +	us-east-1a

Instance: i-04e5d6fe168cbd321 (WS1)

▼ Instance summary Info

Instance ID i-04e5d6fe168cbd321 (WS1)	Public IPv4 address –	Private IPv4 addresses –
Instance state Terminated	Public IPv4 DNS –	Private IPv4 DNS –

It didn`t show the WS1.



arn:aws:elasticloadbalancing:us-east-1:409578114950:targetgroup/WebApp-TG/bcd7ff892706e1ac

Basic configuration

Target type instance	Protocol : Port HTTP : 80 Protocol version HTTP1	VPC vpc-04016e0e99b2eebdb	Load balancer WebApp-LB

Registered targets (1)

□	Instance ID	Name	Port	Zone	Status	Status details
□	i-08e271fc5b7e2a674	WS2	80	us-east-1a	healthy	