

An **Internet Gateway** is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in your VPC and the Internet. It therefore imposes no availability risks or bandwidth constraints on your network traffic.

An Internet gateway serves two purposes: to provide a target in your VPC route tables for Internet-routable traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses. An Internet gateway supports IPv4 and IPv6 traffic.

A **Route Table** contains a set of rules, called **routes** that are used to determine where network traffic is directed.

Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

Creating VPC:

- ❖ Go to VPC Dashboard from AWS main Dashboard as shown below, and click on Start VPC Wizard

The screenshot shows the AWS VPC Dashboard. On the left sidebar, there are several navigation options: Services, Resource Groups, VPC Dashboard, Filter by VPC (set to None), Virtual Private Cloud, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, Security, and Network ACLs. In the center, there's a large "Resources" section with a "Start VPC Wizard" button and a "Launch EC2 Instances" button. Below these are sections for "Your VPCs" (listing 1 VPC, 0 Egress-only Internet Gateways, 1 Route Table, 0 Elastic IPs, 0 Endpoints, 5 Security Groups, 0 VPN Connections, and 0 Customer Gateways), "Internet Gateways" (listing 0 Internet Gateways, 3 Subnets, 1 Network ACL, 0 VPC Peering Connections, 0 Nat Gateways, 0 Running Instances, 0 Virtual Private Gateways, and 0 Customer Gateways), and "VPN Connections". To the right, there's a "Service Health" section showing "Current Status" for Amazon VPC - US West (Oregon) and Amazon EC2 - US West (Oregon), both marked as "Service is operating normally". There's also a "View complete service health details" link. Below that is an "Additional Information" section with links to "VPC Documentation", "All VPC Resources", "Forums", and "Report an Issue".

- ❖ You will a VPC configuration page, select VPC with a single Public subnet and click on select

Visualpath Training & Consulting.

Flat no: 205, Nilgiri Block, Aditya Enclave, Ameerpet, Hyderabad, Phone No: +91-970 445 5959, 961 824 5689 E-Mail ID : online.visualpath@gmail.com, Website : www.visualpath.in.

Step 1: Select a VPC Configuration

VPC with a Single Public Subnet

Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.

Creates:

A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.

Select

Amazon Virtual Private Cloud

Cancel and Exit

- ❖ Specify the IPV4 CIDR block range for subnet, provide a name for vpc and click on create vpc.

Step 2: VPC with a Single Public Subnet

IPv4 CIDR block: 17.24.0.0/16 (65531 IP addresses available)

IPv6 CIDR block: No IPv6 CIDR Block Amazon provided IPv6 CIDR block

VPC name: myvpc

Public subnet's IPv4 CIDR: 17.24.0.0/24 (251 IP addresses available)

Availability Zone: No Preference

Subnet name: Public subnet

You can add more subnets after AWS creates the VPC.

Service endpoints

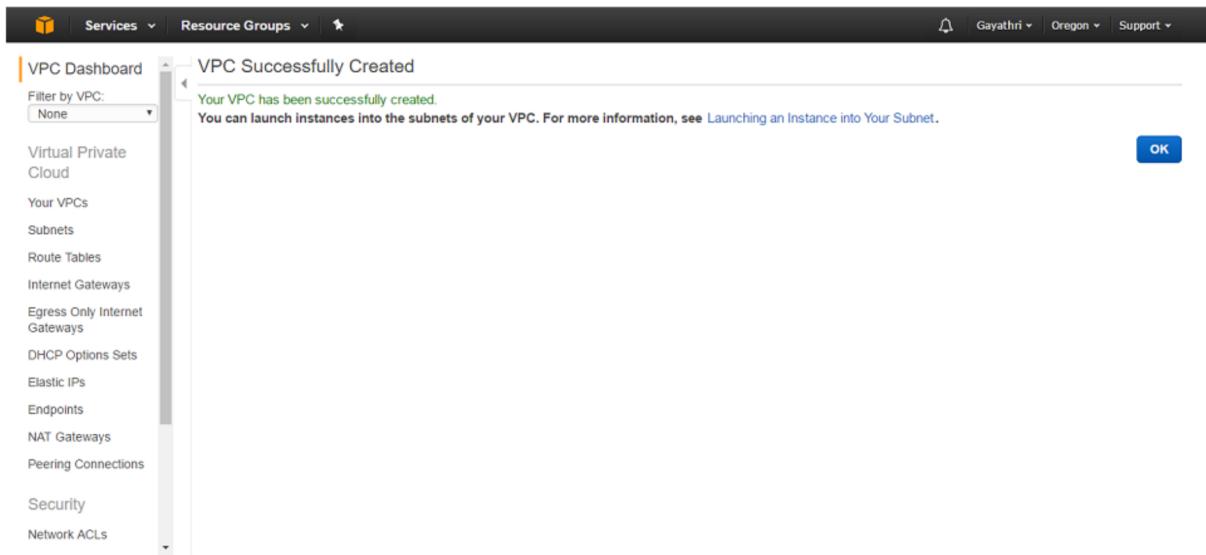
Add Endpoint

Enable DNS hostnames: Yes No

Hardware tenancy: Default

Create VPC

- ❖ Your vpc is successfully created and is available to attach it to instances.



- ❖ It takes few minutes come to available state. Once it is available select the vpc and click on actions to attach it to the instance.

Create VPC Actions

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table	Network ACL	Tenancy
vpc-802f2e7	available	172.31.0.0/16			dopt-bc4e14d8	rtb-ecc3a58b	acl-f7932890	Default
myvpc	available	17.24.0.0/16			dopt-bc4e14d8	rtb-b0630dd6	acl-822f84e4	Default

vpc-ac9a74ca | myvpc

Summary Flow Logs Tags

VPC ID: vpc-ac9a74ca | myvpc
State: available
IPv4 CIDR: 17.24.0.0/16
IPv6 CIDR:
DHCP options set: dopt-bc4e14d8
Route table: rtb-b0630dd6

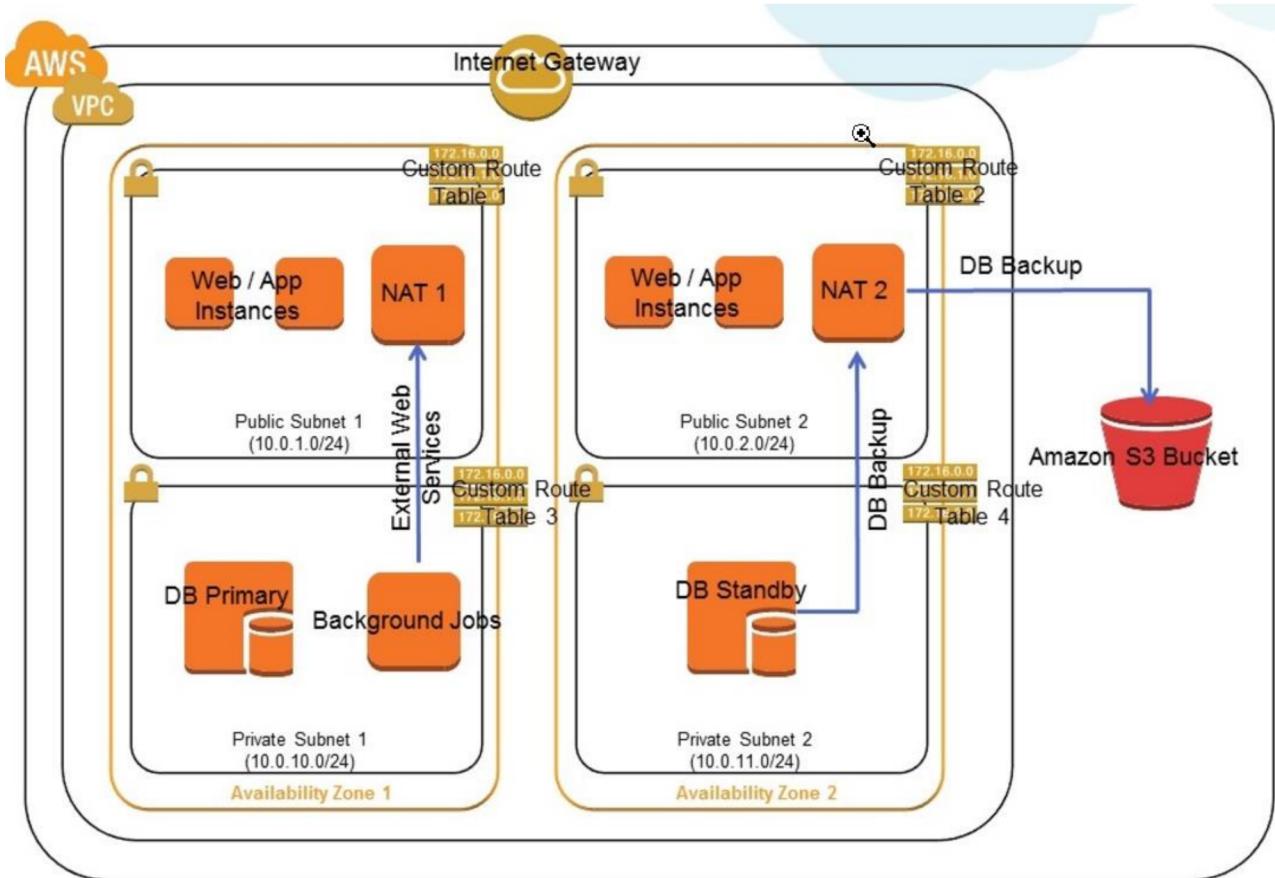
Network ACL: acl-822f84e4
Tenancy: Default
DNS resolution: yes
DNS hostnames: yes
ClassicLink DNS Support: no

In the summary tab of vpc you can see the complete details of vpc.

Visualpath Training & Consulting.

Flat no: 205, Nilgiri Block, Aditya Enclave, Ameerpet, Hyderabad, Phone No: - +91-970 445 5959, 961 824 5689 E-Mail ID : online.visualpath@gmail.com, Website : www.visualpath.in.

11. Creating Highly Available VPC



Highly available VPC spans over multiple zones. Even if one zone goes down our services spanned over the other zone will be still serving the user traffic. If you see from above diagram we have web, DB and backend services in two zones. While creating Ec2 instance we can decide now on which subnet our instance to create. So, for example we will create web01 in one subnet (located in zone 1a) and web02(located in zone 1b) in other subnet. So, if zone 1a goes down we still have web02 serving user traffic from zone 1b.

We are going to create HA VPC manually and not with the wizard.

❖ **Creating VPC:** Go to VPC from AWS main Dashboard.

The screenshot shows the AWS VPC Management console. The left navigation pane includes options like VPC Dashboard, Your VPCs, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, Security, Network ACLs, Security Groups, VPN Connections, Customer Gateways, Virtual Private Gateways, and VPN Connections. The main content area displays a table with one row for the VPC 'vpc-139e387a'. The table columns include Name, VPC ID, State, IPv4 CIDR, IPv6 CIDR, DHCP options set, Route table, Network ACL, Tenancy, and Default VPC. The VPC is marked as 'available' with an IPv4 CIDR of 172.31.0.0/16, associated with route table rtb-5dad1334 and network ACL aci-e51fa28c, and is set as the 'Default VPC'.

- ❖ Click on your VPCs on left side of navigation pane and Click on Create VPC.
 ❖ Create CIDR block /16 and private IP range of your choice as shown below

The screenshot shows the 'Create VPC' dialog box. It contains the following fields:
 - Name tag: ImranHANet
 - IPv4 CIDR block*: 172.20.0.0/16
 - IPv6 CIDR block*: No IPv6 CIDR Block Amazon provided IPv6 CIDR block
 - Tenancy: Default
 At the bottom are 'Cancel' and 'Yes, Create' buttons.

- ❖ Go to Subnets and Click on create Subnets.
- ❖ Create first public subnet from same VPC range with /24 CIDR block.
- ❖ Select the Availability Zone as us-east-2a.

Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag	ImranHAPubNet1
VPC	vpc-1b79c472 ImranHANet
VPC CIDRs	
CIDR	Status
172.20.0.0/16	associated
Availability Zone	
us-east-2a	
IPv4 CIDR block	
172.20.1.0/24	

Cancel **Yes, Create**

- ❖ Create second public subnet from same VPC range with /24 CIDR block.
- ❖ Select the Availability Zone as us-east-2b.

Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag	ImranHAPubNet2
VPC	vpc-1b79c472 ImranHANet
VPC CIDRs	
CIDR	Status
172.20.0.0/16	associated
Availability Zone	
us-east-2b	
IPv4 CIDR block	
172.20.2.0/24	

Cancel **Yes, Create**

- ❖ Create First PRIVATE subnet from same VPC range with /24 CIDR block.
- ❖ Select the Availability Zone as us-east-2a.

Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag	ImranHAPrivateNet1
VPC	vpc-1b79c472 ImranHANet
VPC CIDRs	
CIDR	Status
172.20.0.0/16	associated
Availability Zone	
us-east-2a	
IPv4 CIDR block	
172.20.3.0/24	

Cancel **Yes, Create**

Visualpath Training & Consulting.

Flat no: 205, Nilgiri Block, Aditya Enclave, Ameerpet, Hyderabad, Phone No: - +91-970 445 5959, 961 824 5689 E-Mail ID : online.visualpath@gmail.com, Website : www.visualpath.in.

- ❖ Create Second PRIVATE subnet from same VPC range with /24 CIDR block.
- ❖ Select the Availability Zone as us-east-2b.

Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag	ImranHAPrivNet2
VPC	vpc-1b79c472 ImranHANet
VPC CIDRs	CIDR Status Status Reason
172.20.0.0/16	associated

Availability Zone: us-east-2b

IPv4 CIDR block: 172.20.4.0/24

Cancel **Yes, Create**

- ❖ Verify all your subnet settings.

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Route Table	Network ACL	Default Subnet
ImranHAPubNet1	subnet-6975f700	available	vpc-1b79c472 ImranHANet	172.20.1.0/24	251		us-east-2a	rtb-78c14511	aci-0fad1666	No
ImranHAPubNet2	subnet-a913c7d2	available	vpc-1b79c472 ImranHANet	172.20.2.0/24	251		us-east-2b	rtb-78c14511	aci-0fad1666	No
ImranHAPrivNet1	subnet-5675f73f	available	vpc-1b79c472 ImranHANet	172.20.3.0/24	251		us-east-2a	rtb-78c14511	aci-0fad1666	No
ImranHAPrivNet2	subnet-631cc818	available	vpc-1b79c472 ImranHANet	172.20.4.0/24	251		us-east-2b	rtb-78c14511	aci-0fad1666	No

- ❖ Go to Internet Gateway to Create Internet Gateway to map to Public subnet.

VPC Dashboard

Filter by VPC: None

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

Create Internet Gateway Delete Attach to VPC Detach from VPC

Search Internet Gateways and X

Name	ID	State	VPC
igw-8e12cbe7	attached	vpc-138e387a	

- ❖ Provide the name for Internet Gateway. Click on Create

Create Internet Gateway

An Internet gateway is a virtual router that connects a VPC to the Internet.

Name tag	ImranHAIGW
----------	------------

Cancel **Yes, Create**

❖ Attach IGW to your VPC:

Select Internet Gateway you created, choose the VPC to be attached and click on click on Attach to VPC.

The screenshot shows the AWS VPC Management console. On the left, there's a navigation pane with various options like VPC Dashboard, Virtual Private Cloud, Subnets, Route Tables, Internet Gateways, Egress Only Internet Gateways, DHCP Options Sets, Elastic IPs, Endpoints, NAT Gateways, Peering Connections, Security, Network ACLs, and Security Groups. In the center, there's a table showing two Internet Gateways: 'igw-5ad27733' (ImranHAGW) which is 'detached', and 'igw-8e12cbe7' which is 'attached'. A modal dialog box titled 'Attach to VPC' is open over the table. It contains the instruction 'Attach an Internet gateway to a VPC to enable communication with the Internet.' Below this, there's a dropdown menu labeled 'VPC' with the value 'vpc-1b79c472 | ImranHANet'. At the bottom of the dialog are 'Cancel' and 'Yes, Attach' buttons. The status bar at the bottom of the page includes links for Feedback, English, Privacy Policy, and Terms of Use.

❖ Create NAT Gateway to Map to your Private subnets.

❖ You also need an Elastic IP (EIP) to assign to your NAT Gateway.

❖ Go to NAT Gateway navigation pane and click on create NAT Gateway

The screenshot shows the AWS VPC Management console. The navigation pane on the left is identical to the previous screenshot. In the center, there's a message stating 'You do not have any NAT gateways in this region.' Below this, it says 'Choose the Create NAT gateway button to create your first NAT gateway.' A large blue button labeled 'Create a NAT Gateway' is prominently displayed. The status bar at the bottom includes links for Feedback, English, Privacy Policy, and Terms of Use.

Visualpath Training & Consulting.

Flat no: 205, Nilgiri Block, Aditya Enclave, Ameerpet, Hyderabad, Phone No: - +91-970 445 5959, 961 824 5689 E-Mail ID : online.visualpath@gmail.com, Website : www.visualpath.in.

- ❖ Select any of the PUBLIC subnet that we created earlier, Create New EIP and assign to Gateway.

Create a NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. [Learn more](#)

Subnet*	VPC
subnet-73d6501a	vpc-138e387a
subnet-63be7618	vpc-138e387a
subnet-6975f700 ImranHAPubNet1	vpc-1b79c472 ImranHANet
subnet-b023c0fd	vpc-138e387a
subnet-5675f73f ImranHAPrivNet1	vpc-1b79c472 ImranHANet
subnet-631cc818 ImranHAPrivNet2	vpc-1b79c472 ImranHANet
subnet-a913c7d2 ImranHAPubNet2	vpc-1b79c472 ImranHANet

- ❖ Once done click on create NAT Gateway

Create a NAT Gateway

Create a NAT gateway and assign it an Elastic IP address. [Learn more](#)

Subnet*	subnet-6975f700	
Elastic IP Allocation ID*	eipalloc-9251f1fb	Create New EIP
Allocation ID	Elastic IP Address	
eipalloc-9251f1fb	52.14.164.255	

[Cancel](#) [Create a NAT Gateway](#)

Create a NAT Gateway

✓ Your NAT gateway has been created.

Note: In order to use your NAT gateway, ensure that you edit your route tables to include a route with a target of 'nat-082ee4212351084fc'.

[Find out more.](#)

[View NAT Gateways](#) [Edit Route Tables](#)

- ❖ NAT Gateway is successfully created as shown below.

❖ Go to Route Table to create route tables for subnets.

- ❖ Click on create Route Table and Give a name, Click on create.
- ❖ We need two route tables, one for Public subnet & one for Private Subnet.

Create Route Table

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

Name tag	<input type="text" value="XXXXXXXXXXXX"/>	
VPC	<input type="text" value="XXXXXXXXXXXXXXet"/>	

Visualpath Training & Consulting.

Flat no: 205, Nilgiri Block, Aditya Enclave, Ameerpet, Hyderabad, Phone No: - +91-970 445 5959, 961 824 5689 E-Mail ID : online.visualpath@gmail.com, Website : www.visualpath.in.

Create Route Table

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

Name tag i

VPC i

Cancel Yes, Create

❖ Add Route Table rule on HAPubRT to route to IGW that we created and save.

The screenshot shows the AWS VPC Management console. In the top navigation bar, there are tabs for EC2 Management, CloudWatch Metrics, CloudWatch Logs, and VPC Management. The VPC Management tab is active. Below the navigation, there are dropdown menus for Services and Resource Groups. The main content area is titled "Create Route Table". A search bar at the top says "Search Route Tables and their..." followed by a close button. Below the search bar is a table with columns: Name, Route Table ID, Explicitly Associated, Main, and VPC. The table contains four rows:

Name	Route Table ID	Explicitly Associated	Main	VPC
ImranHAPubRT	rtb-2fc34746	0 Subnets	No	vpc-1b79c472 ImranHANet
ImranHAPrivateRT	rtb-0dc34764	0 Subnets	No	vpc-1b79c472 ImranHANet
	rtb-7bc14511	0 Subnets	Yes	vpc-1b79c472 ImranHANet
	rtb-5dad1334	0 Subnets	Yes	vpc-138e387a

Below the table, a message says "1 to 4 of 4 Route Tables". At the bottom of the "Create Route Table" section, there are buttons for "Cancel" and "Save". The "Save" button is highlighted in blue. To the right of the "Save" button, there are three small icons: a magnifying glass, a gear, and a question mark.

❖ Associate HAPubRT to Public subnets and save.

VPC Dashboard

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Name	Route Table ID	Explicitly Associated	Main	VPC
ImranHAPubRT	rtb-2fc34746	0 Subnets	No	vpc-1b79c472 ImranHANet
ImranHAPrivRT	rtb-0dc34764	0 Subnets	No	vpc-1b79c472 ImranHANet
	rtb-78c14511	0 Subnets	Yes	vpc-1b79c472 ImranHANet
	rtb-5dad1334	0 Subnets	Yes	vpc-138e387a

rtb-2fc34746 | ImranHAPubRT

Summary Routes Subnet Associations Route Propagation Tags

Associate Subnet IPv4 CIDR IPv6 CIDR Current Route Table

Associate	Subnet	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input checked="" type="checkbox"/>	subnet-6975f700 ImranHAPubNet1	172.20.1.0/24	-	Main
<input checked="" type="checkbox"/>	subnet-a913c7d2 ImranHAPubNet2	172.20.2.0/24	-	Main
<input type="checkbox"/>	subnet-5675f73f ImranHAPrivNet1	172.20.3.0/24	-	Main
<input type="checkbox"/>	subnet-631cc818 ImranHAPrivNet2	172.20.4.0/24	-	Main

Cancel Save

Feedback English © 2008–2017 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

❖ Add Route Table rule on HAPrivRT to route to NAT GW and save.

VPC Dashboard

Virtual Private Cloud

Your VPCs

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Name	Route Table ID	Explicitly Associated	Main	VPC
rtb-78c14511	0 Subnets	Yes	vpc-1b79c472 ImranHANet	
ImranHAPubRT	rtb-2fc34746	2 Subnets	No	vpc-1b79c472 ImranHANet
ImranHAPrivRT	rtb-0dc34764	0 Subnets	No	vpc-1b79c472 ImranHANet
	rtb-5dad1334	0 Subnets	Yes	vpc-138e387a

rtb-0dc34764 | ImranHAPrivRT

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save

View: All rules

Destination	Target	Status	Propagated	Remove
172.20.0.0/16	local	Active	No	
0.0.0.0/0	nat-082ee4212351084fc		No	

Add another route

Feedback English © 2008–2017 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

❖ Associate HAPrivRT to PRIVATE subnets and save.

Visualpath Training & Consulting.

Flat no: 205, Nilgiri Block, Aditya Enclave, Ameerpet, Hyderabad, Phone No: - +91-970 445 5959, 961 824 5689 E-Mail ID : online.visualpath@gmail.com, Website : www.visualpath.in.

VPC Dashboard

Virtual Private Cloud

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create Route Table Delete Route Table Set As Main Table

Search Route Tables and their X

Name	Route Table ID	Explicitly Associated	Main	VPC
rtb-78c14511	0 Subnets	Yes	vpc-1b79c472 ImranHANet	
ImranHAPubRT	rtb-2fc34746	2 Subnets	No	vpc-1b79c472 ImranHANet
ImranHAPrivateRT	rtb-0dc34764	0 Subnets	No	vpc-1b79c472 ImranHANet
	rtb-5dad1334	0 Subnets	Yes	vpc-138e387a

rtb-0dc34764 | ImranHAPrivateRT

Summary Routes Subnet Associations Route Propagation Tags

Associate Subnet IPv4 CIDR IPv6 CIDR Current Route Table

subnet-6975f700 | ImranHAPubNet1 172.20.1.0/24 rtb-2fc34746 | ImranHAPubRT

subnet-a913c7d2 | ImranHAPubNet2 172.20.2.0/24 rtb-2fc34746 | ImranHAPubRT

subnet-5675f73f | ImranHAPrivateNet1 172.20.3.0/24 Main

subnet-631cc818 | ImranHAPrivateNet2 172.20.4.0/24 Main

Feedback English

© 2008–2017 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

❖ Go to your Subnets and verify every subnet.

VPC Dashboard

Virtual Private Cloud

Subnets

Route Tables

Internet Gateways

Egress Only Internet Gateways

DHCP Options Sets

Elastic IPs

Endpoints

NAT Gateways

Peering Connections

Security

Network ACLs

Security Groups

VPN Connections

Customer Gateways

Virtual Private Gateways

VPN Connections

Create Subnet Subnet Actions

Search Subnets and their proj X

Subnet ID	Subnet Name	State	VPC	IPv4 CIDR	IPv6 CIDR	Availability Zone	Route Table	Network ACL	Flow Logs	Tags
subnet-a913c7d2	ImranHAPubNet2	available	vpc-1b79c472 ImranHANet	172.20.2.0/24	251	us-east-2b	rtb-2fc34746 Imra...	aci-0fad1666	No	
subnet-6975f700	ImranHAPubNet1	available	vpc-1b79c472 ImranHANet	172.20.1.0/24	250	us-east-2a	rtb-2fc34746 Imra...	aci-0fad1666	No	
subnet-631cc818	ImranHAPrivateNet2	available	vpc-1b79c472 ImranHANet	172.20.4.0/24	251	us-east-2b	rtb-0dc34764 Imr...	aci-0fad1666	No	
subnet-5675f73f	ImranHAPrivateNet1	available	vpc-1b79c472 ImranHANet	172.20.3.0/24	251	us-east-2a	rtb-0dc34764 Imr...	aci-0fad1666	No	
subnet-73d9501a		available	vpc-138e387a	172.31.0.0/20	4091	us-east-2a	rtb-5dad1334	aci-e51fa28c	Yes	
subnet-63be7618		available	vpc-138e387a	172.31.16.0/20	4091	us-east-2b	rtb-5dad1334	aci-e51fa28c	Yes	
subnet-b023c0fd		available	vpc-138e387a	172.31.32.0/20	4091	us-east-2c	rtb-5dad1334	aci-e51fa28c	Yes	

subnet-631cc818 | ImranHAPrivateNet2

Summary Route Table Network ACL Flow Logs Tags

Edit Route Table: rtb-0dc34764 | ImranHAPrivateRT

Destination Target

172.20.0.0/16 local

0.0.0.0 nat-082ee4212351084c

Feedback English

© 2008–2017 Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

You can attach this VPC to EC2 instances with public subnet and private subnet. If you want to connect to the private subnet instance first you need to connect to the public subnet instance.

Visualpath Training & Consulting.

Flat no: 205, Nilgiri Block, Aditya Enclave, Ameerpet, Hyderabad, Phone No: +91-970 445 5959, 961 824 5689 E-Mail ID : online.visualpath@gmail.com, Website : www.visualpath.in.

12. Elastic Load Balancer

Elastic Load Balancing distributes incoming application traffic across multiple EC2 instances, in multiple Availability Zones. This increases the fault tolerance of your applications. A load balancer accepts incoming traffic from clients and routes requests to its registered EC2 instances in one or more Availability Zones. The load balancer also monitors the health of its registered instances and ensures that it routes traffic only to healthy instances. When the load balancer detects an unhealthy instance, it stops routing traffic to that instance, and then resumes routing traffic to that instance when it detects that the instance is healthy again.

Elastic Load Balancing supports two types of load balancers: Application Load Balancers and Classic Load Balancers. There is a key difference between the way you configure these load balancers. With a Classic Load Balancer, you register instances with the load balancer. With an Application Load Balancer, you register the instances as targets in a target group, and route traffic to a target group.

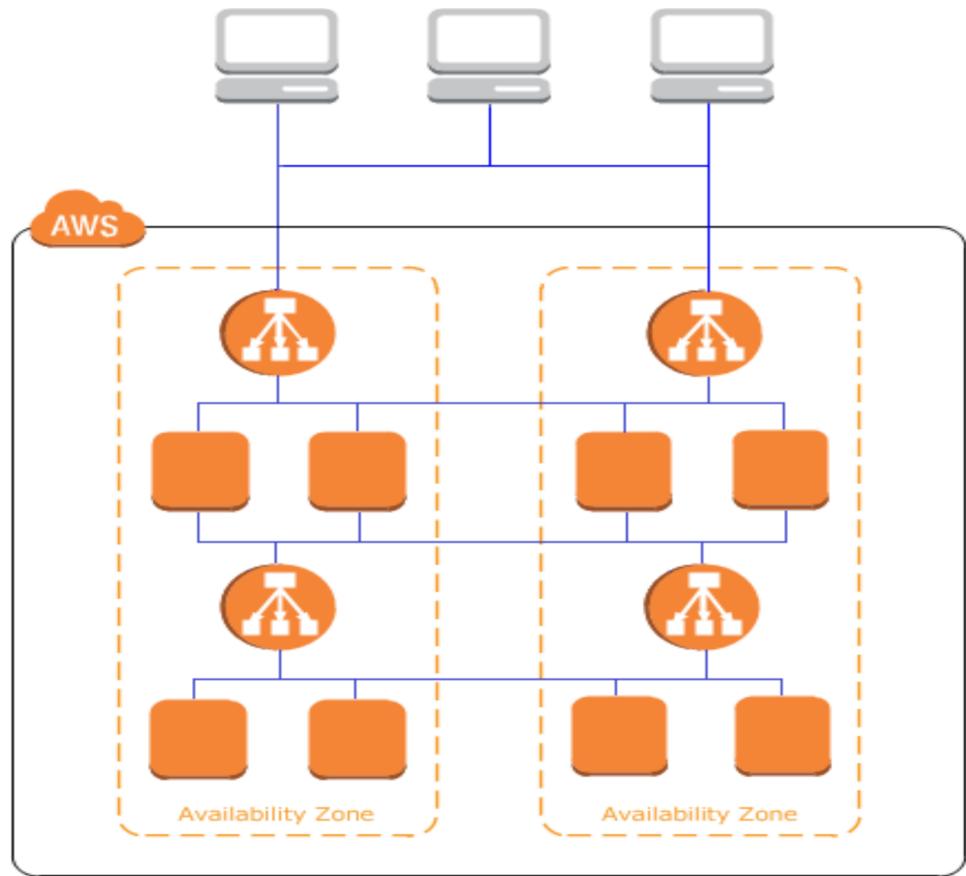
When you create a load balancer, you must choose whether to make it an internal load balancer or an Internet-facing load balancer. Note that when you create a Classic Load Balancer in EC2-Classic, it must be an Internet-facing load balancer. The nodes of an Internet-facing load balancer have public IP addresses. The DNS name of an Internet facing load balancer is publicly resolvable to the public IP addresses of the nodes. Therefore, Internet facing load balancers can route requests from clients over the Internet.

The nodes of an internal load balancer have only private IP addresses. The DNS name of an internal load balancer is publicly resolvable to the private IP addresses of the nodes. Therefore, internal load balancers can only route requests from clients with access to the VPC for the load balancer.

Note: Both Internet-facing and internal load balancers route requests to your instances using private IP addresses. Therefore, your instances do not need public IP addresses to receive requests from an internal or an Internet-facing load balancer.

If your application has multiple tiers, for example web servers that must be connected to the Internet and database servers that are only connected to the web servers, you can design an architecture that uses both internal and Internet-facing load balancers. Create an Internet-facing load balancer and register the web servers with it. Create an internal load balancer and register the database servers with it.

The web servers receive requests from the Internet-facing load balancer and send requests for the database servers to the internal load balancer. The database servers receive requests from the internal load balancer.



Creating Elastic Load Balancer:

Prerequisites:

- Choose any two Availability Zones you will use for your EC2 instances. Verify that your virtual private cloud (VPC) has at least one public subnet in each of these Availability Zones.
- Launch at least one EC2 instance in each Availability Zone.
- Ensure that the security group for your EC2 instances allows HTTP access on port 80. To test the web server, copy the DNS name of the instance and verify whether browser displays the default page of the web server or not.

The below screenshot shows the instance created named elbtestproj-web1, it has a public IP address but this IP is dynamic and changes after every reboot of the instance. We need to assign an Elastic IP to this instance which is static and does not change.

The screenshot shows the AWS EC2 Management Console. The left sidebar includes links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Spot Requests, Reserved Instances, Dedicated Hosts, AMIs, Bundle Tasks, Elastic Block Store, Volumes, Snapshots, Network & Security, Security Groups, Elastic IPs (selected), Placement Groups, Key Pairs, Network Interfaces, Load Balancing, Load Balancers, and Target Groups. The main content area displays a table of instances. A specific instance, 'elbtestproj-web1', is selected. Below the table, there's a detailed view of the instance with tabs for Description, Status Checks, Monitoring, Tags, and Usage Instructions. The instance details shown are: Instance ID i-0e240d9ab028759f1, Public DNS: ec2-54-241-145-82.us-west-1.compute.amazonaws.com, Instance state: running, and IPv4 Public IP: 54.241.145.82.

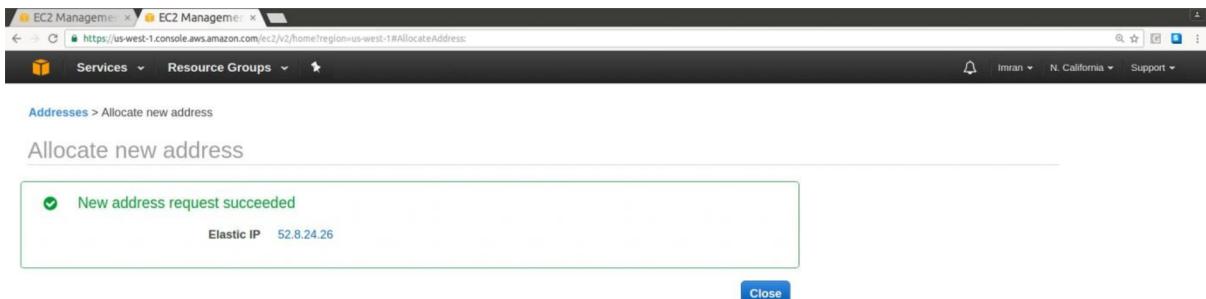
Elastic IP: An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. An Elastic IP address is associated with your AWS account. With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.

Assigning Elastic IP:

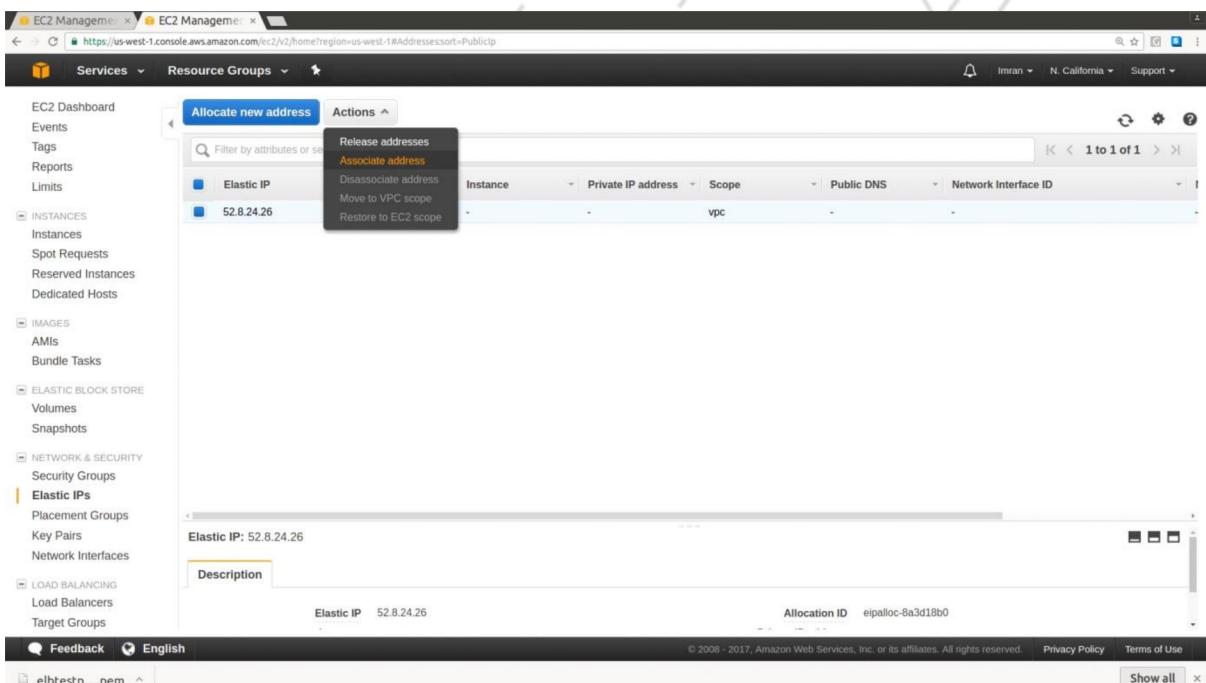
Navigate to the Elastic IPs tab on the EC2 Dashboard and click on allocate new address.

The screenshot shows the AWS EC2 Management Console. The left sidebar includes links for EC2 Dashboard, Events, Tags, Reports, Limits, Instances, AMIs, Elastic Block Store, Network & Security, and Load Balancing. The 'Elastic IPs' link under Network & Security is selected. The main content area shows a message: 'You do not have any Addresses in this region'. Below this message is a button labeled 'Allocate new address'.

❖ You will get a message 'New address request succeeded'



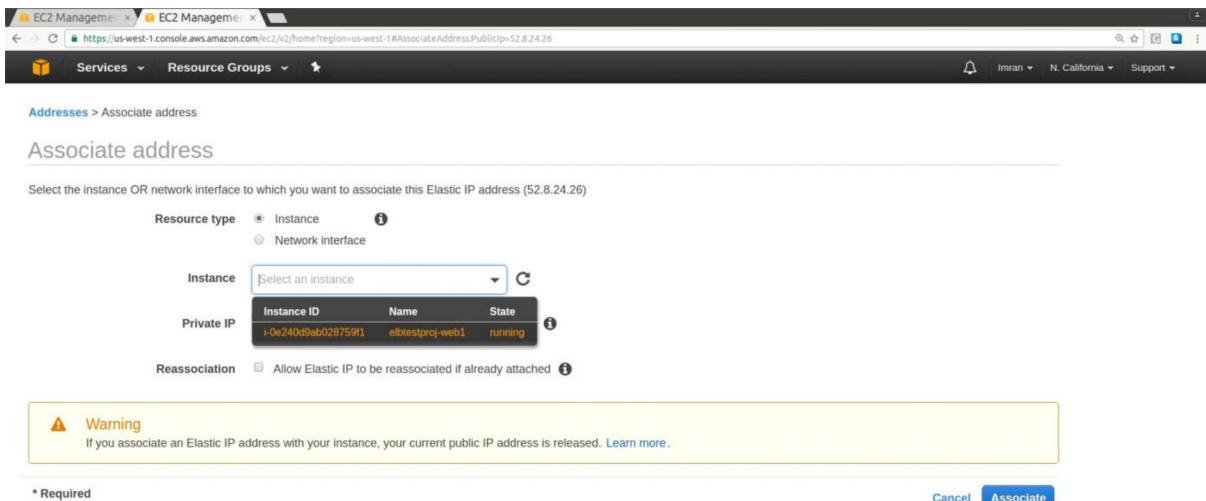
❖ Click on actions and select Associate address



❖ Provide the instance id and click on associate. Then your instance will be allocated with this elastic IP.

Visualpath Training & Consulting.

Flat no: 205, Nilgiri Block, Aditya Enclave, Ameerpet, Hyderabad, Phone No: +91-970 445 5959, 961 824 5689 E-Mail ID : online.visualpath@gmail.com, Website : www.visualpath.in.



Login to the instance by using public IP

```
imran@DevOps:~/keys$ ssh -i elbtestproj-nocalifornia.pem centos@52.8.24.26
^C
imran@DevOps:~/keys$ ssh -i elbtestproj-nocalifornia.pem centos@52.8.24.26
The authenticity of host '52.8.24.26 (52.8.24.26)' can't be established.
RSA key fingerprint is SHA256:5UigbWQvFCVNTynq2oJgMCeL+n3ewbnG3AArnU6PaQo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '52.8.24.26' (RSA) to the list of known hosts.
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
cccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccccc
Permissions 0664 for 'elbtestproj-nocalifornia.pem' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "elbtestproj-nocalifornia.pem": bad permissions
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
imran@DevOps:~/keys$ chmod 400 elbtestproj-nocalifornia.pem
imran@DevOps:~/keys$ ssh -i elbtestproj-nocalifornia.pem centos@52.8.24.26
[centos@ip-172-31-4-195 ~]$ sudo -i
[root@ip-172-31-4-195 ~]#
```

Install apache service by using below command

```
# yum install httpd
```

Start apache service

```
# service httpd start
```

Enable apache service

```
# chkconfig httpd on
```

Stop & Disable firewall

```
# service iptables stop
```

```
# chkconfig iptables off
```

Create a test webpage for apache using html.

```
cd /var/www/html/
```

```
vi index.html
```

Visualpath Training & Consulting.

Flat no: 205, Nilgiri Block, Aditya Enclave, Ameerpet, Hyderabad, Phone No: +91-970 445 5959, 961 824 5689 E-Mail ID : online.visualpath@gmail.com, Website : www.visualpath.in.

```

<html>
<head>
<body>
    <h1>This is a test webpage.</h1>
</body>
</head>
</html>

```

Test the webpage

Enter the ec2 inst public IP in browser.

<http://52.8.24.26>

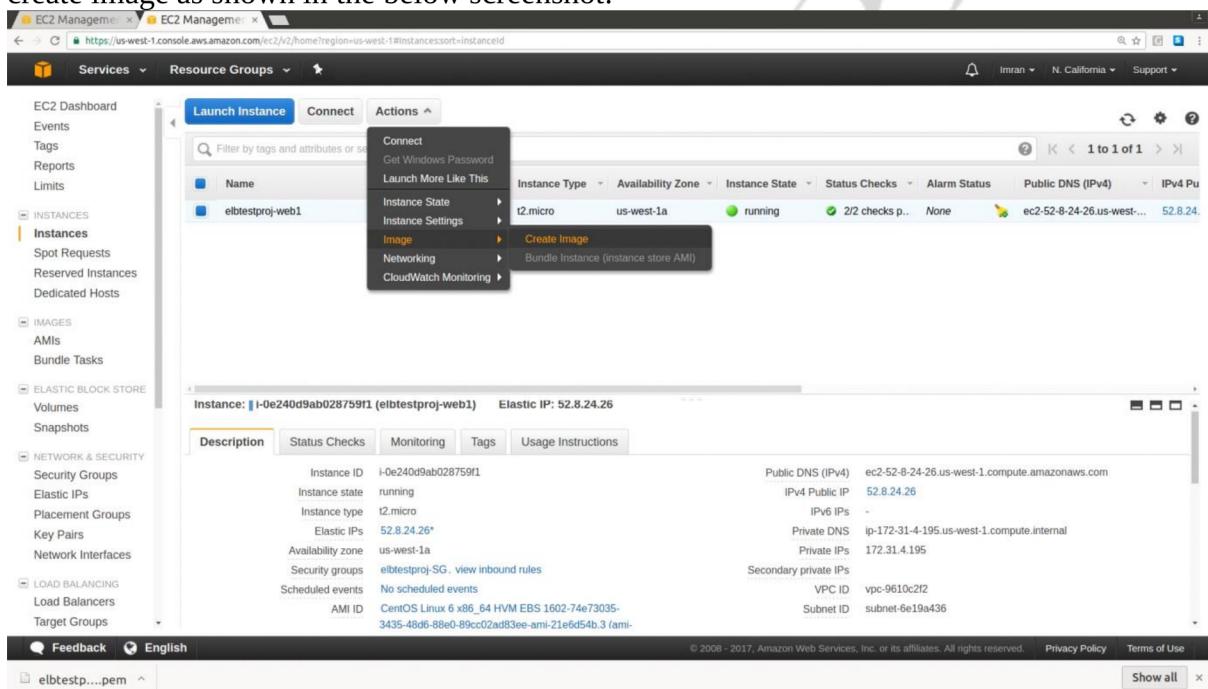
AWS AMI: An Amazon Machine Image (AMI) is a special type of virtual appliance that is used to create a virtual machine within the Amazon Elastic Compute Cloud ("EC2"). It serves as the basic unit of deployment for services delivered using EC2.

AMI Creation

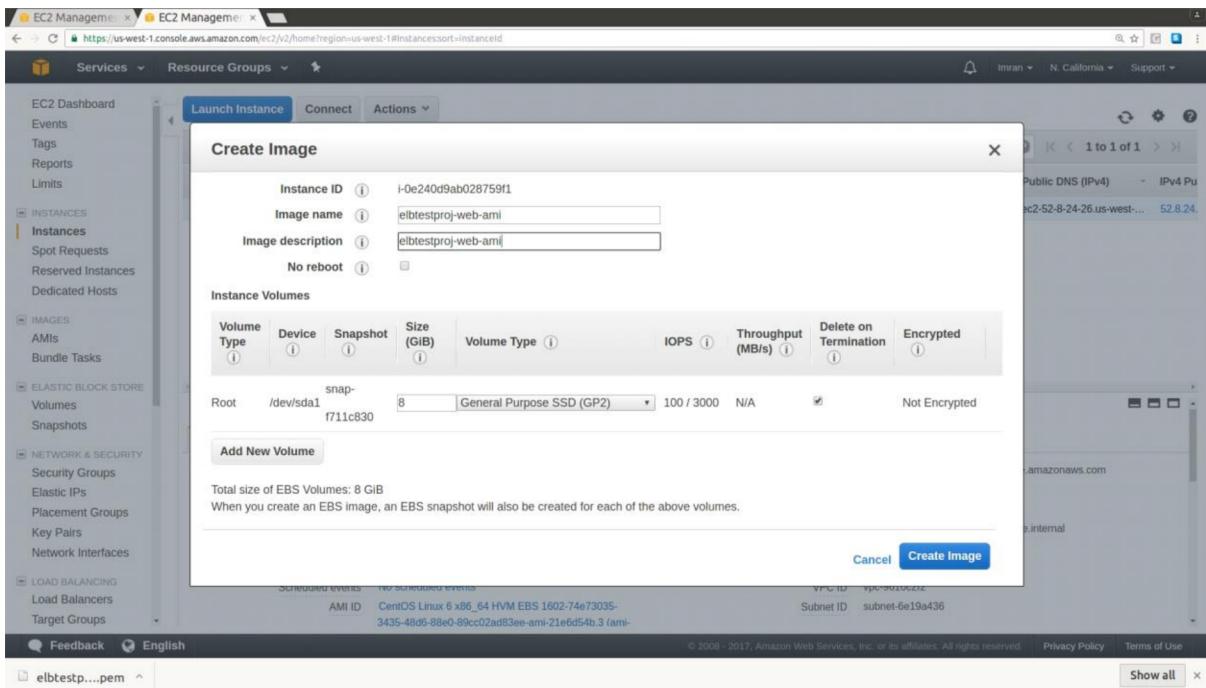
Create AMI of the instance which we will use to spin web02 instance.

Web02 instance is exactly similar to web01, so instead to creating new instance from scratch and setting up apache, we can create an AMI (image) of web01 instance and can spin as many as web instances we want.

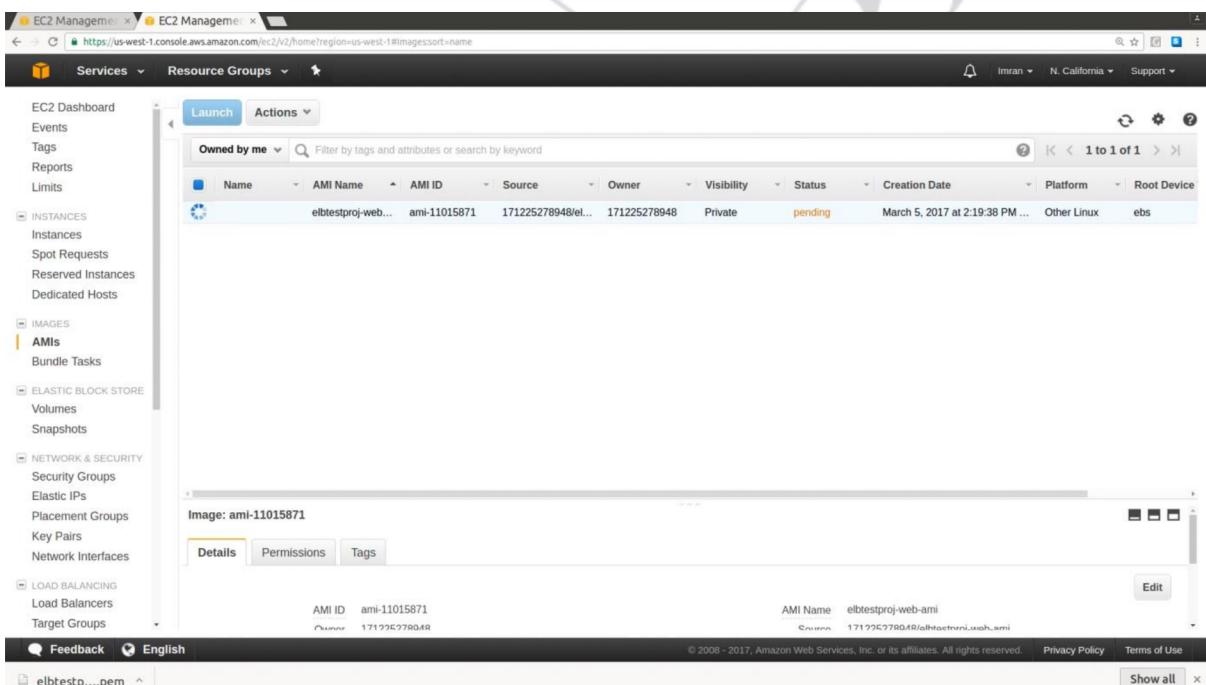
Select the instance in which we have to create an image. Click on actions, select image and click on create image as shown in the below screenshot:



- ❖ You will get a create image dialog box as shown below. Give proper name and description for image and click on create image.



- ❖ It takes few minutes to create an image which you can see on AMIs navigation pane



Create web02 instance from elbtestproj-web-ami.

Click on Launch instance --> My AMI --> Select your AMI --> Follow the wizard and create the instance similar to web01.

Tag Name: elbtestproj-web02

Security: Select existing security group --> elbtestproj-SG

Select an existing key pair --> <same key used for web01>

Assign Elastic IP

Visualpath Training & Consulting.

Flat no: 205, Nilgiri Block, Aditya Enclave, Ameerpet, Hyderabad, Phone No: - +91-970 445 5959, 961 824 5689 E-Mail ID : online.visualpath@gmail.com, Website : www.visualpath.in.