LAB: Create a VPC with Subnets and Routing and an IG/NAT Gateway

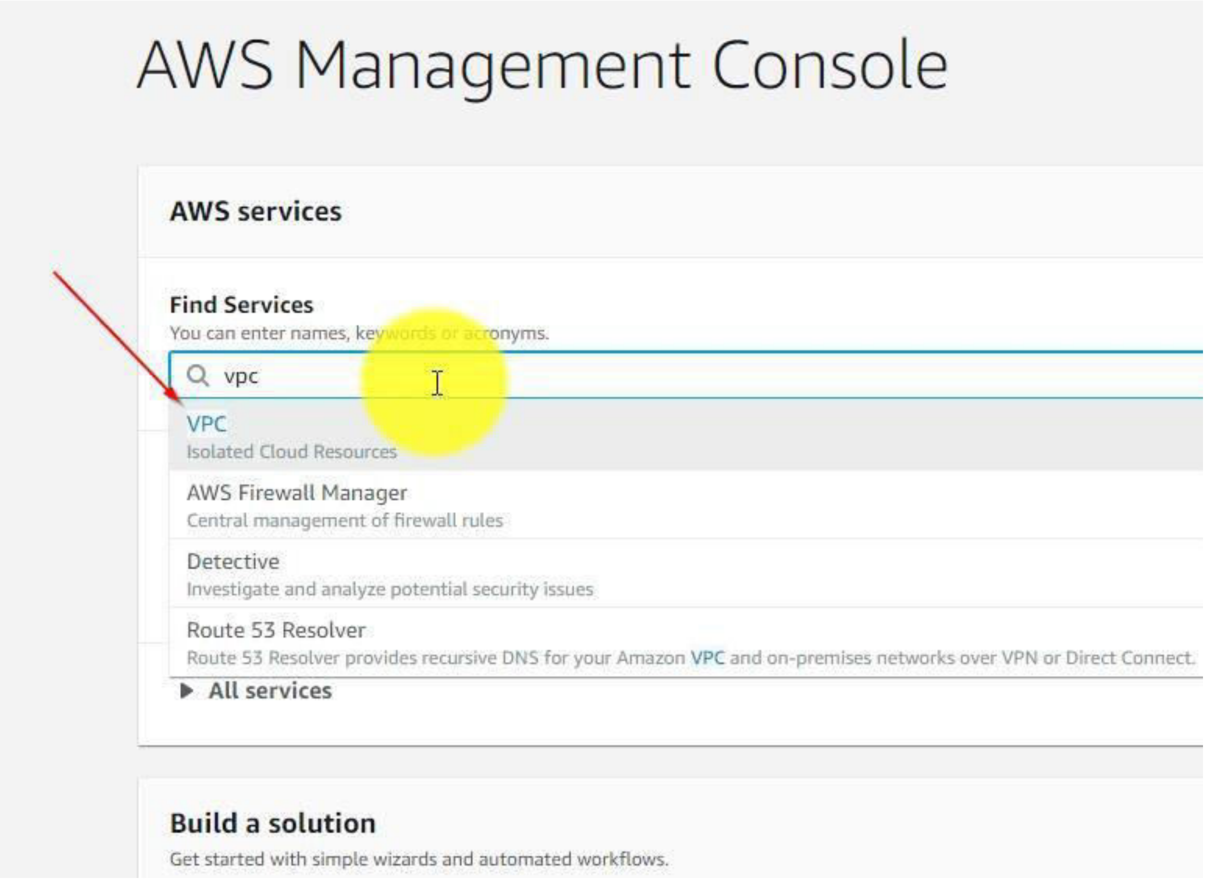
You need:

- An AWS Account

Duration of the Lab: 30 Minutes.

Difficulty: medium

Open the VPC Dashboard



AWS Management Console

AWS services

Find Services

You can enter names, keywords or acronyms.

vpc

VPC
Isolated Cloud Resources

AWS Firewall Manager
Central management of firewall rules

Detective
Investigate and analyze potential security issues

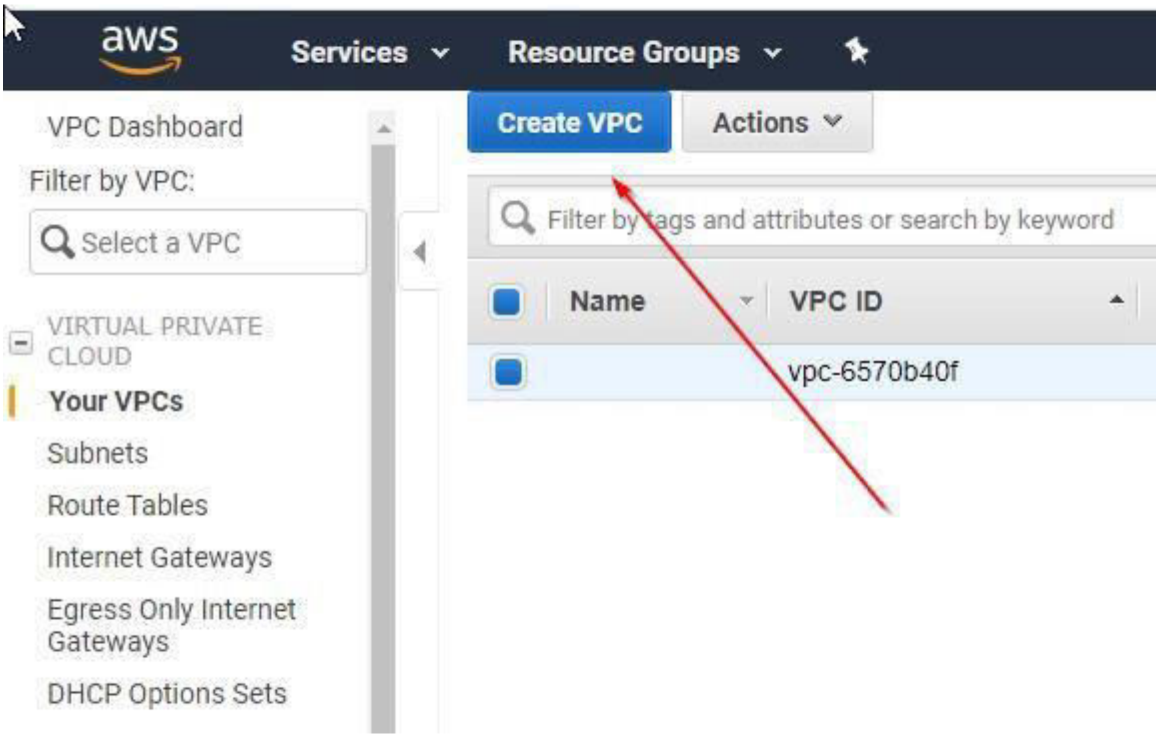
Route 53 Resolver
Route 53 Resolver provides recursive DNS for your Amazon VPC and on-premises networks over VPN or Direct Connect.

▶ All services

Build a solution

Get started with simple wizards and automated workflows.

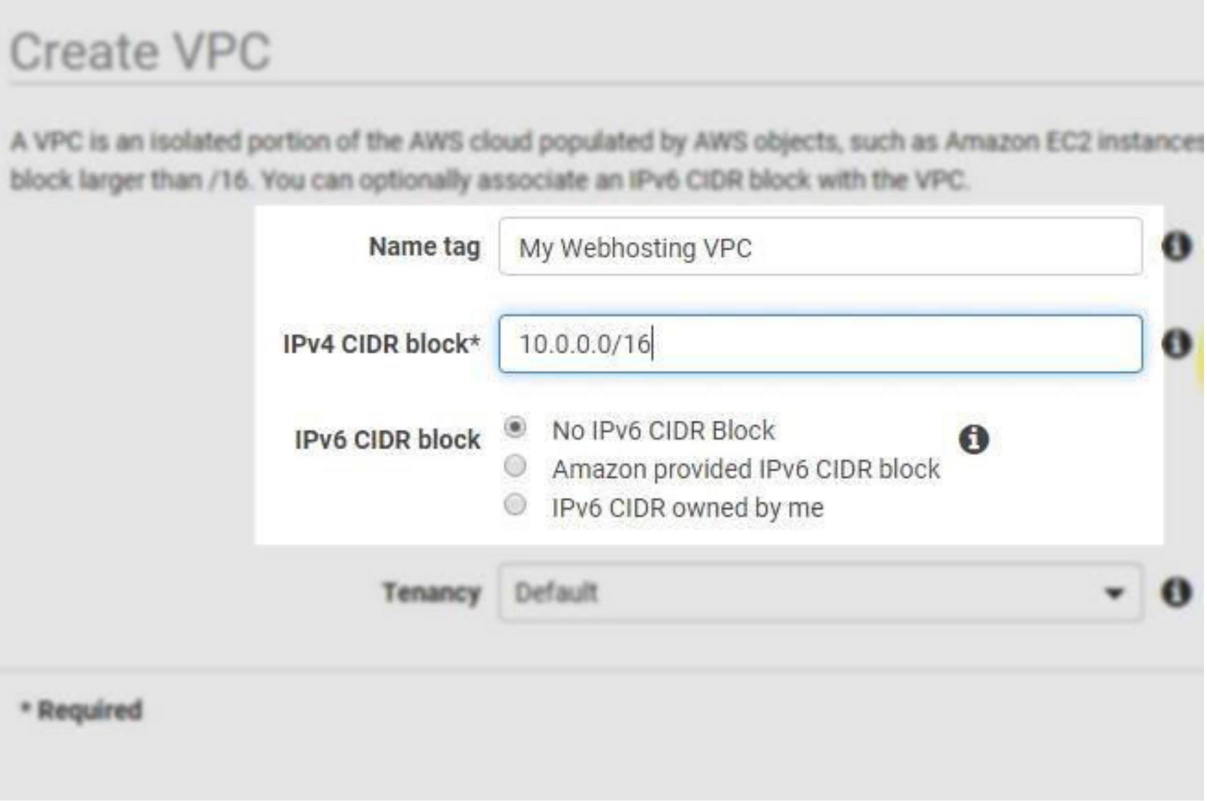
Create a new VPC



Name	VPC ID
	vpc-6570b40f

Enter a Name and a CIDR Block, for example 10.0.0.0/16.

This CIDR Block will give you 10.0.X.X IPs, which corresponds to a Class B Network with 65536 IP Addresses (256*256).



Create VPC

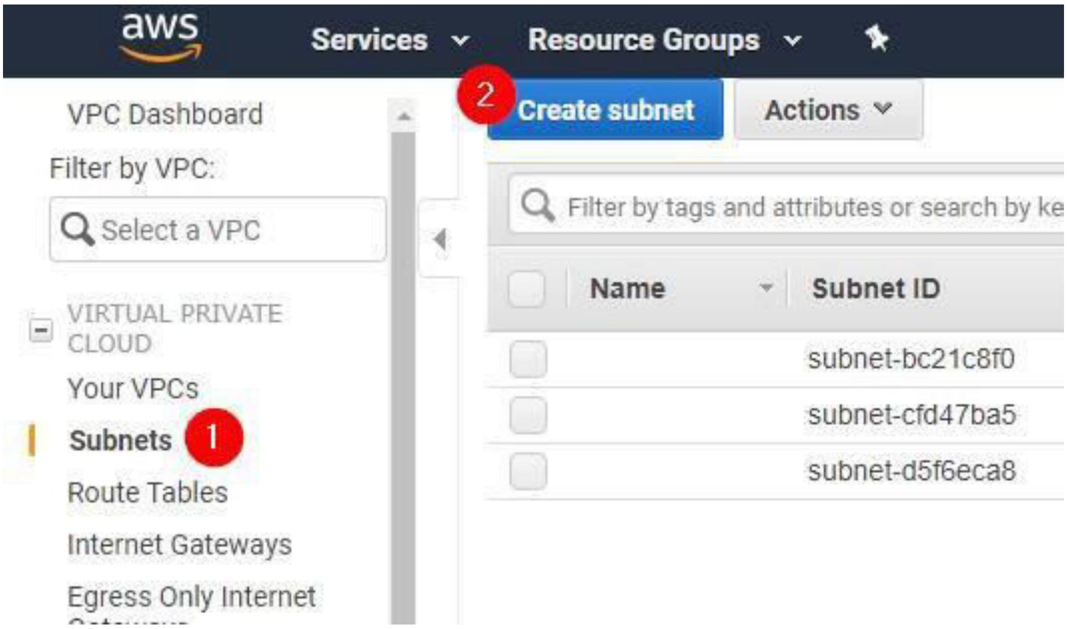
A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances block larger than /16. You can optionally associate an IPv6 CIDR block with the VPC.

Name tag	My Webhosting VPC
IPv4 CIDR block*	10.0.0.0/16
IPv6 CIDR block	● No IPv6 CIDR Block ○ Amazon provided IPv6 CIDR block ○ IPv6 CIDR owned by me
Tenancy	Default

* Required

Create Subnets

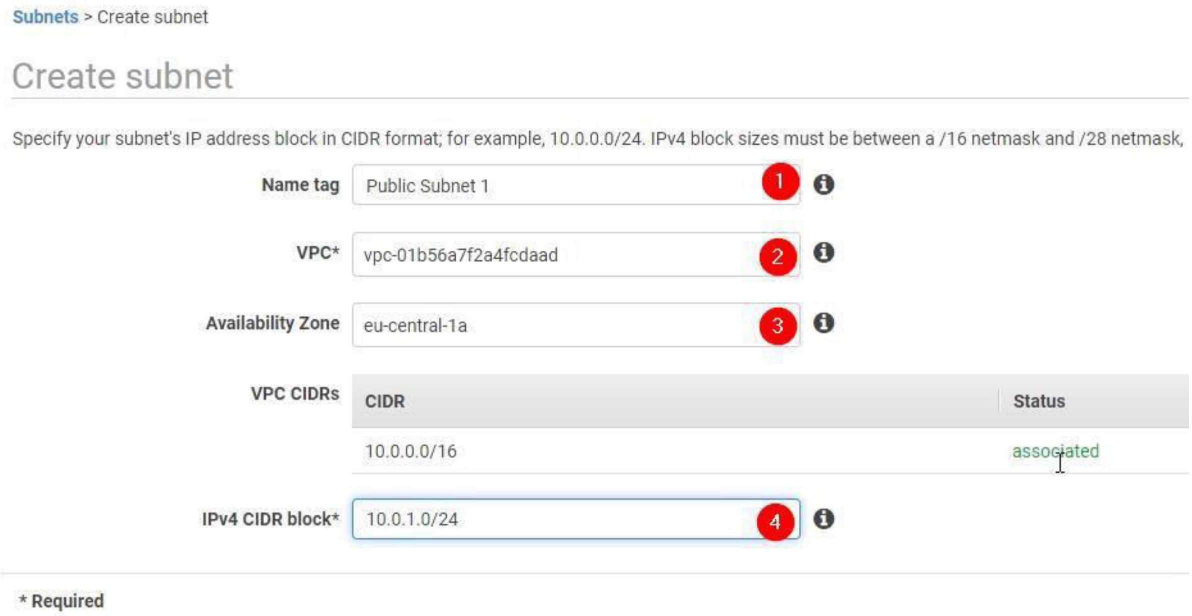
Create three Subnets:



	Name	Subnet ID
□		subnet-bc21c8f0
□		subnet-cfd47ba5
□		subnet-d5f6eca8

Create three subnets:

1) Public/Private Subnet 1 and 2
2) Select the VPC you created earlier
3) Select two different AZ for the public subnets and a single one for your private subnet
4) For the public subnets set 10.0.1.0/24 and 10.0.2.0/24 as the CIDR Block, for the private one set 10.0.10.0/24 as the CIDR Block. This gives you 256 IP Addresses in the Subnets, corresponding to a Class C network.



Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask,

Name tag: Public Subnet 1 (1)

VPC*: vpc-01b56a7f2a4fcdaad (2)

Availability Zone: eu-central-1a (3)

VPC CIDRs:

CIDR	Status
10.0.0.0/16	associated

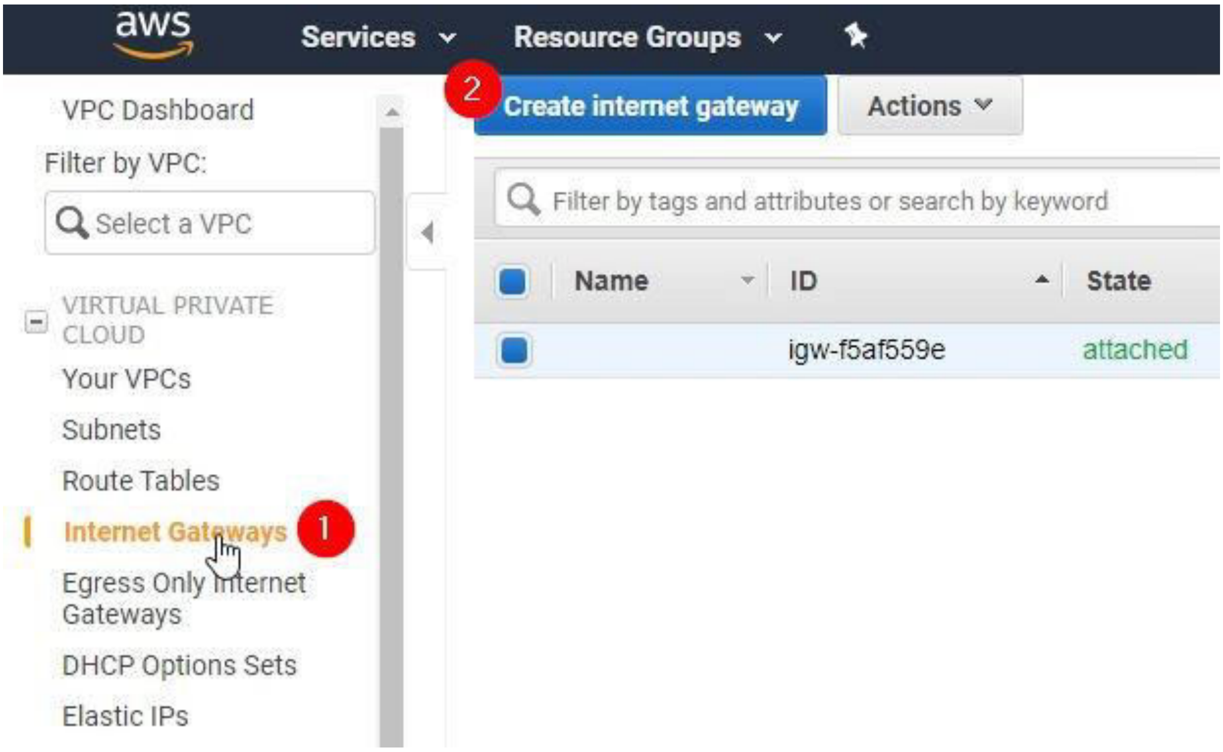
IPv4 CIDR block*: 10.0.1.0/24 (4)

* Required

QUESTION: Is this is a High Availability Setup? Why yes, why not?

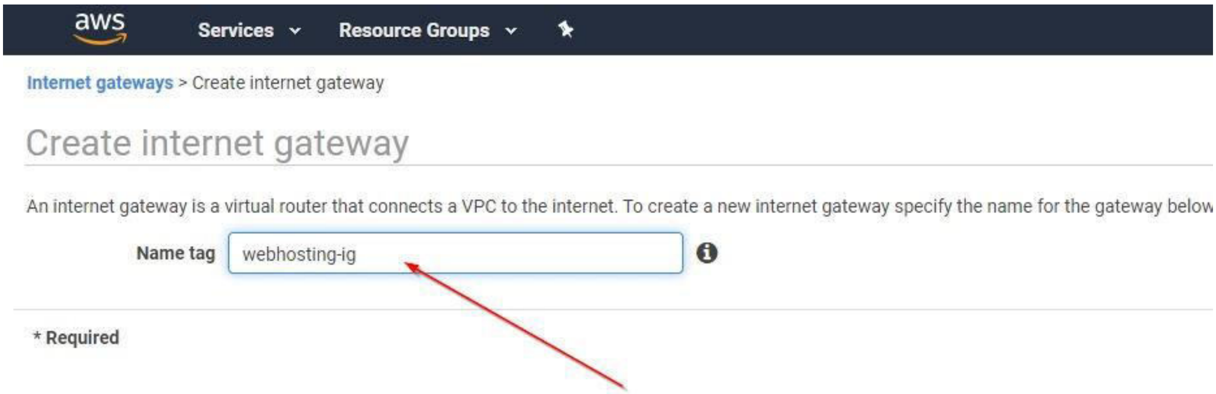
Create Internet Gateway

Open the Internet Gateway section of the VPC Dashboard and create an internet Gateway:



Name	ID	State
	igw-f5af559e	attached

Give it a name:



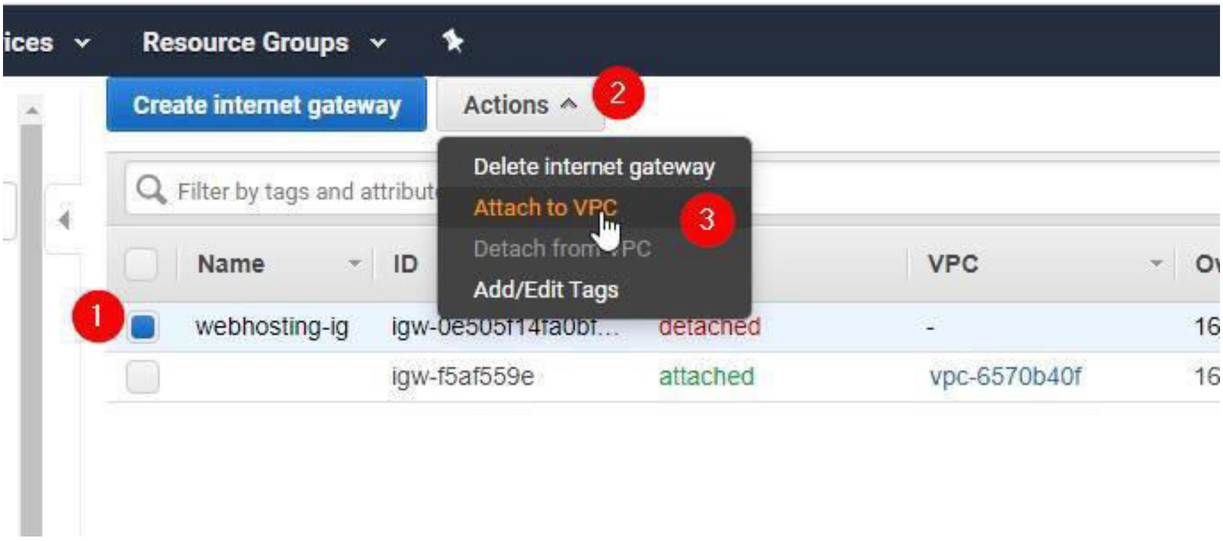
Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below

Name tag: webhosting-ig

* Required

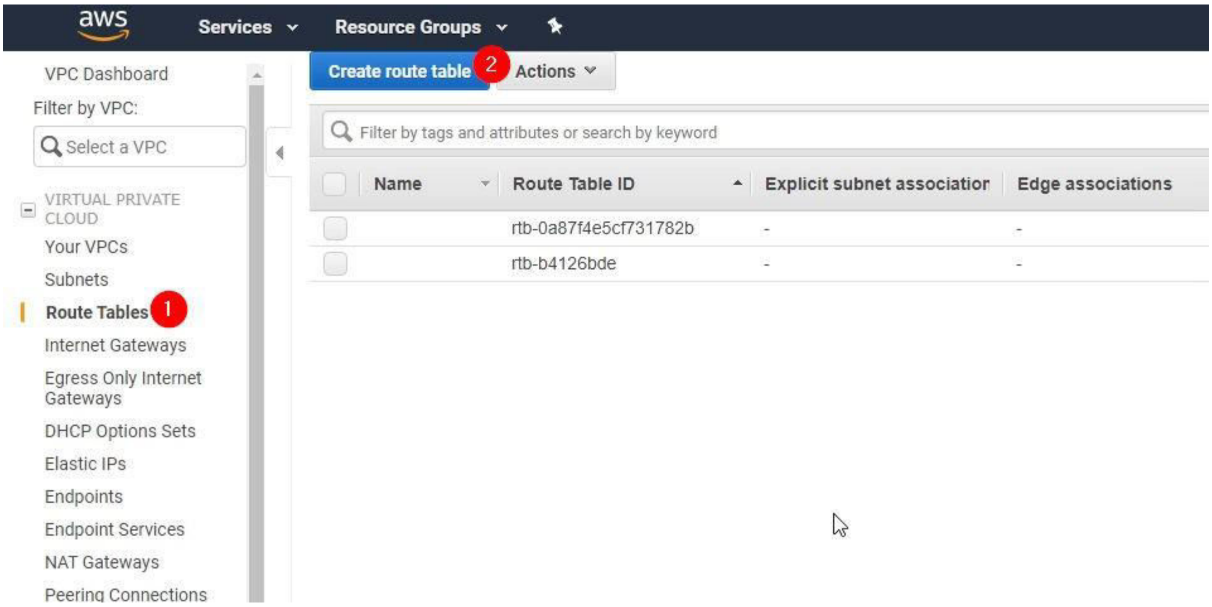
Then attach it to your VPC:



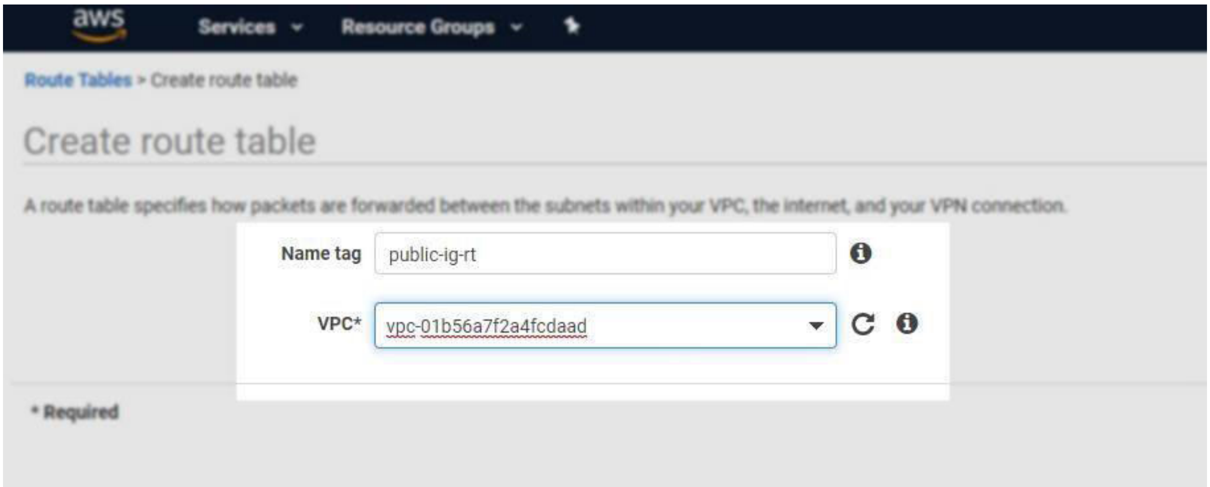
	Name	ID		VPC	Ov
☑	webhosting-ig	igw-0e505f14fa0bf…	detached	-	16
□		igw-f5af559e	attached	vpc-6570b40f	16

Create a Route Table

To route traffic from your public subnet to the Internet Gateway you have to create a new Route table:



	Name	Route Table ID	Explicit subnet associatior	Edge associations
□		rtb-0a87f4e5cf731782b	-	-
□		rtb-b4126bde	-	-



Route Tables > Create route table

Create route table

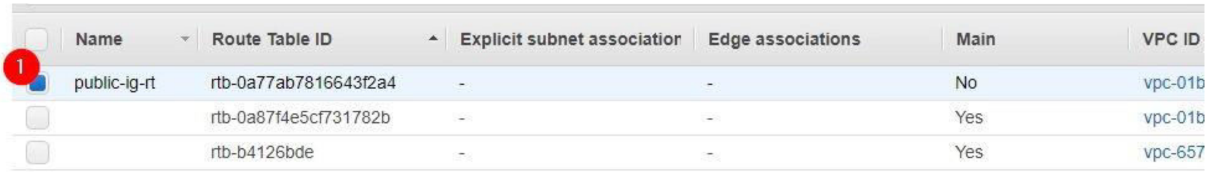
A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag: public-ig-rt

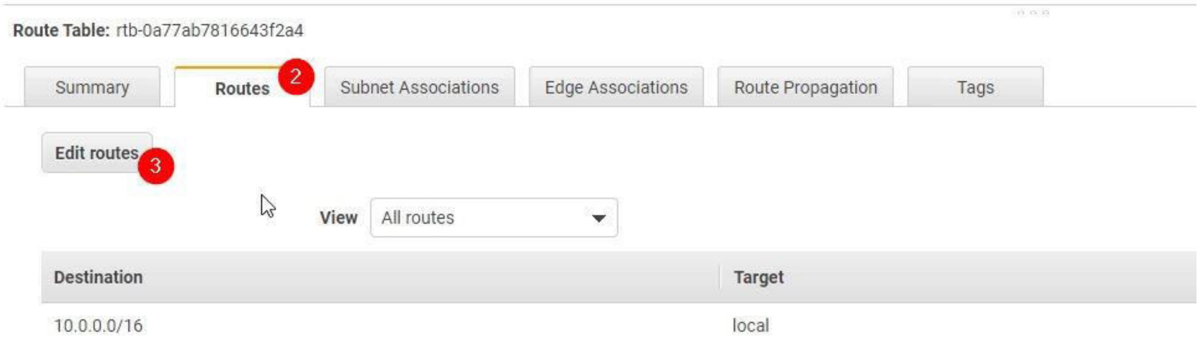
VPC*: vpc-01b56a7f2a4fcdaad

* Required

Edit the new Route Table:



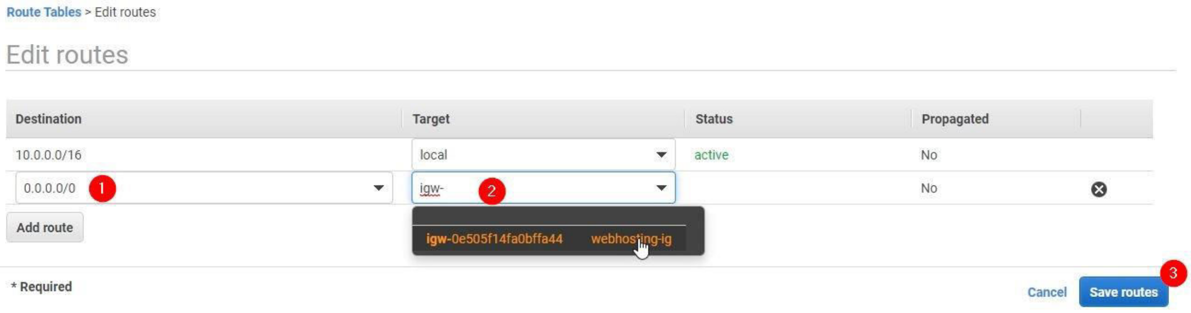
□	Name	Route Table ID	Explicit subnet associatior	Edge associations	Main	VPC ID
☑	public-ig-rt	rtb-0a77ab7816643f2a4	-	-	No	vpc-01b
□		rtb-0a87f4e5cf731782b	-	-	Yes	vpc-01b
□		rtb-b4126bde	-	-	Yes	vpc-657



Route Table: rtb-0a77ab7816643f2a4

Destination	Target
10.0.0.0/16	local

Select 0.0.0.0/0 for the destination and the newly created Internet Gateway for the Target:



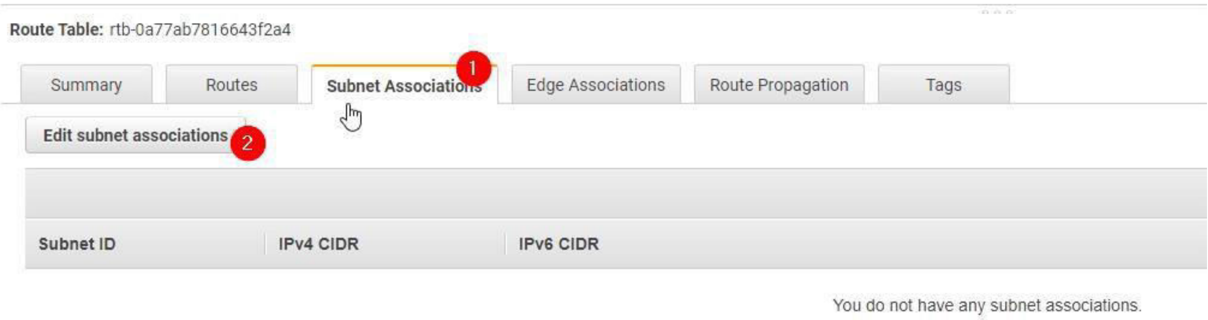
Route Tables > Edit routes

Edit routes

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

igw-0e505f14fa0bffa44 webhosting-ig

Associate the right subnet with the new route table:

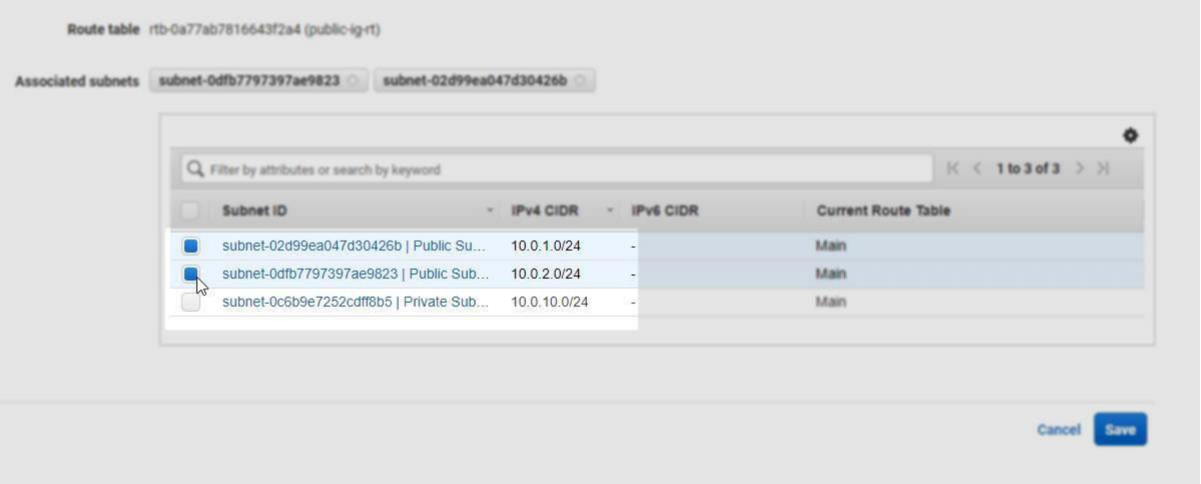


Route Table: rtb-0a77ab7816643f2a4

Subnet ID	IPv4 CIDR	IPv6 CIDR

You do not have any subnet associations.

Select the public subnets:



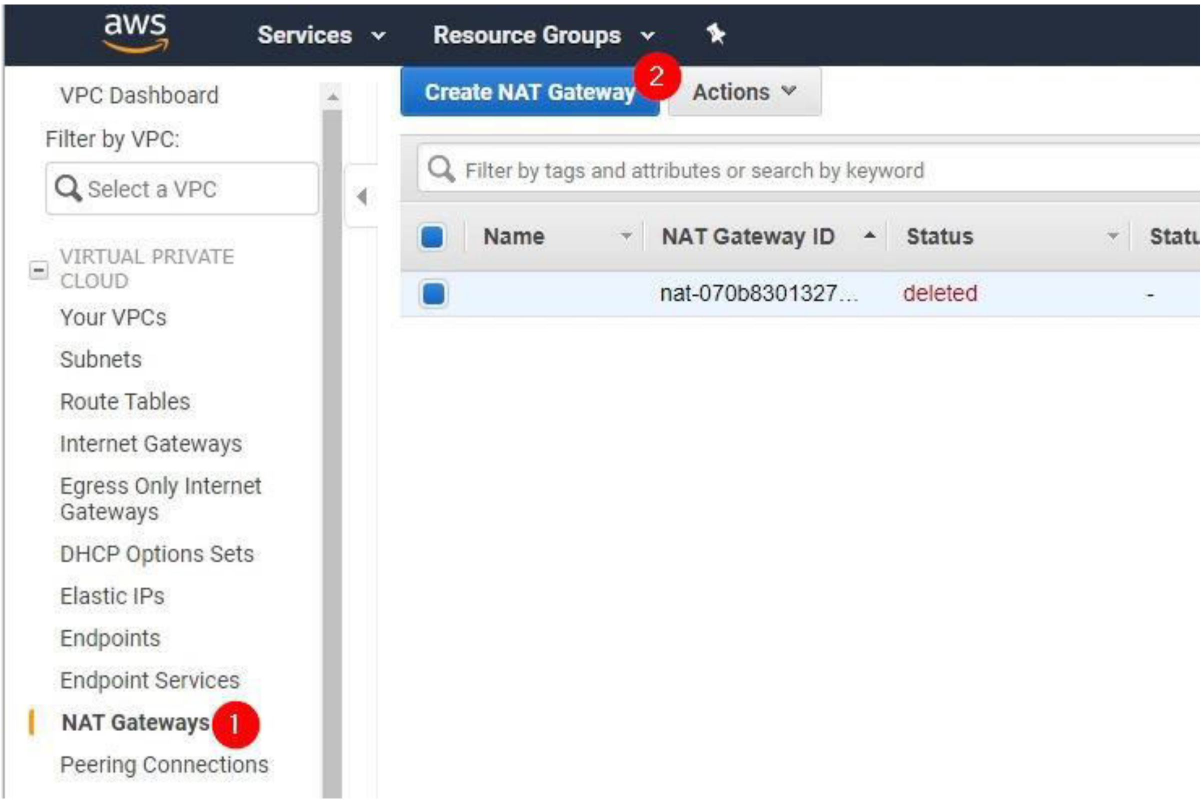
Route table rtb-0a77ab7816643f2a4 (public-ig-rt)

Associated subnets subnet-0dfb7797397ae9823 subnet-02d99ea047d30426b

☐	Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
☑	subnet-02d99ea047d30426b | Public Su...	10.0.1.0/24	-	Main
☑	subnet-0dfb7797397ae9823 | Public Sub...	10.0.2.0/24	-	Main
☐	subnet-0c6b9e7252cdff8b5 | Private Sub...	10.0.10.0/24	-	Main

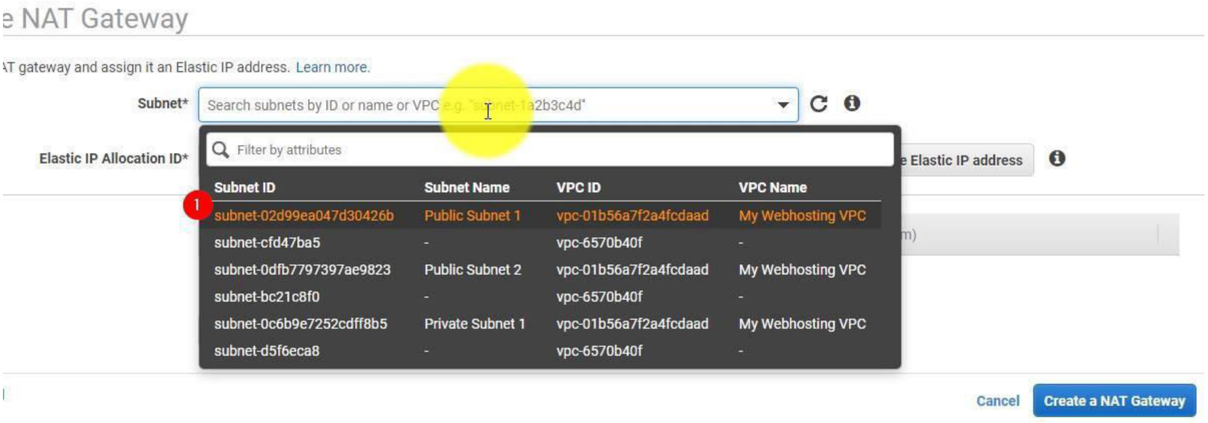
Create a NAT Gateway

For your private subnet to get internet accessibility create a NAT Gateway:



☑	Name	NAT Gateway ID	Status	Statu
☑		nat-070b8301327...	deleted	-

You need to place your subnet in a *public* subnet, because the NAT Gateway needs internet access:



e NAT Gateway

AT gateway and assign it an Elastic IP address. Learn more.

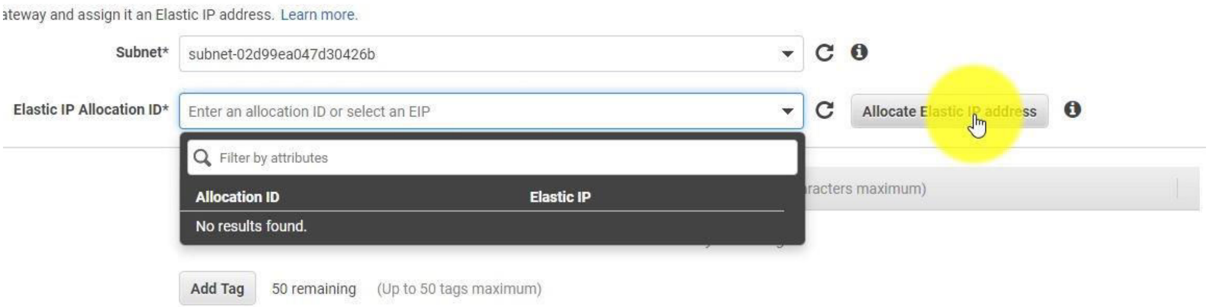
Subnet* Search subnets by ID or name or VPC e.g. "subnet-1a2b3c4d"

Elastic IP Allocation ID*

Filter by attributes

Subnet ID	Subnet Name	VPC ID	VPC Name
subnet-02d99ea047d30426b	Public Subnet 1	vpc-01b56a7f2a4fcdaad	My Webhosting VPC
subnet-cfd47ba5	-	vpc-6570b40f	-
subnet-0dfb7797397ae9823	Public Subnet 2	vpc-01b56a7f2a4fcdaad	My Webhosting VPC
subnet-bc21c8f0	-	vpc-6570b40f	-
subnet-0c6b9e7252cdff8b5	Private Subnet 1	vpc-01b56a7f2a4fcdaad	My Webhosting VPC
subnet-d5f6eca8	-	vpc-6570b40f	-

Allocate a new Elastic IP Address:



ateway and assign it an Elastic IP address. Learn more.

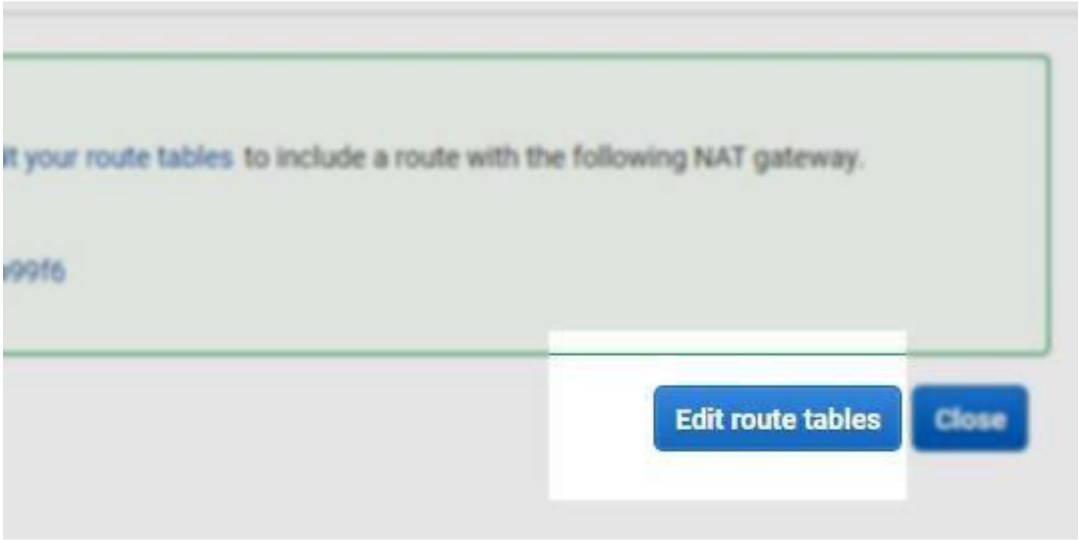
Subnet* subnet-02d99ea047d30426b

Elastic IP Allocation ID* Enter an allocation ID or select an EIP

Filter by attributes

Allocation ID	Elastic IP
No results found.	

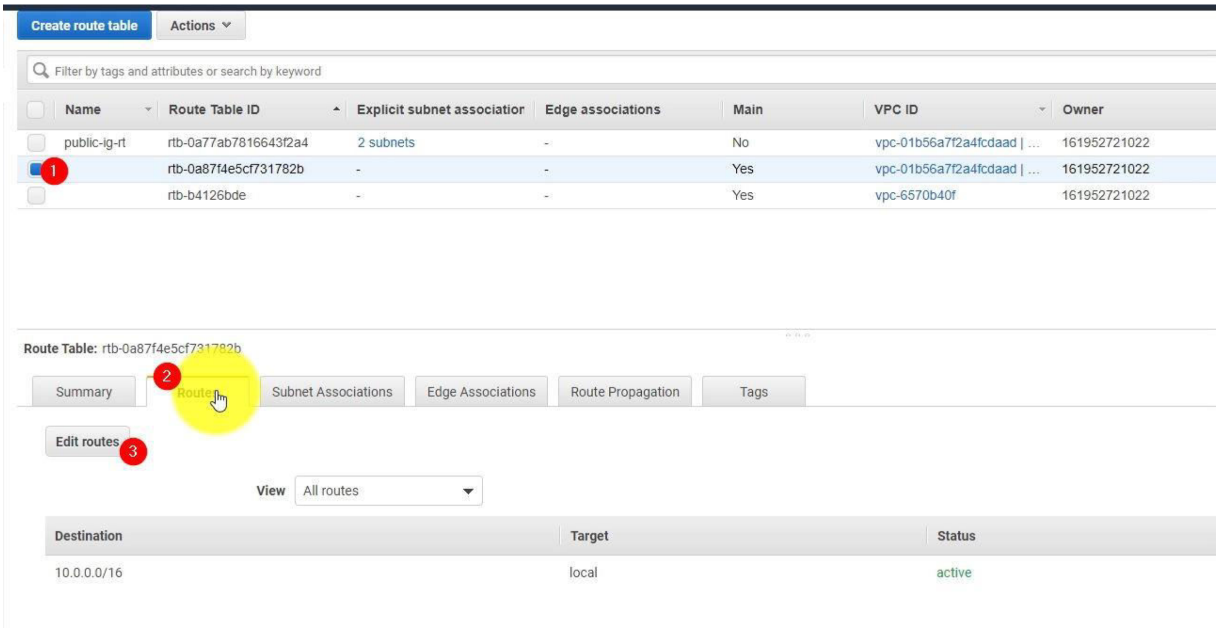
Edit the Route Tables:



it your route tables to include a route with the following NAT gateway.

99f6

Edit the Main Route Table for your new VPC:

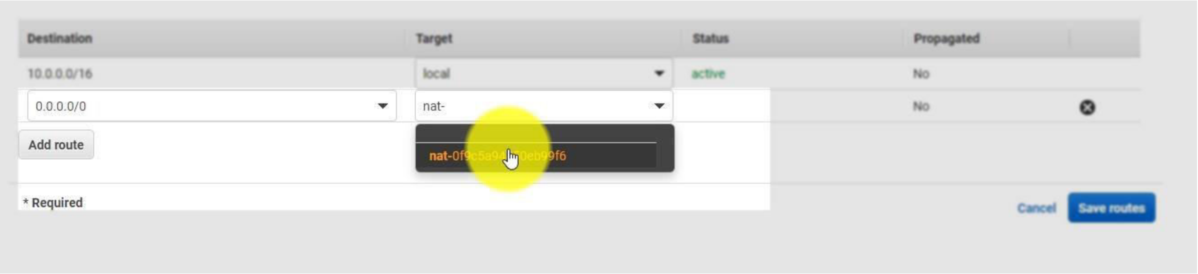


Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID	Owner
public-ig-rt	rtb-0a77ab7816643f2a4	2 subnets	-	No	vpc-01b56a7f2a4fcdaad | ...	161952721022
	rtb-0a87f4e5cf731782b	-	-	Yes	vpc-01b56a7f2a4fcdaad | ...	161952721022
	rtb-b4126bde	-	-	Yes	vpc-6570b40f	161952721022

Route Table: rtb-0a87f4e5cf731782b

Destination	Target	Status
10.0.0.0/16	local	active

Select the traffic destination 0.0.0.0/0 with the NAT Gateway as your target:

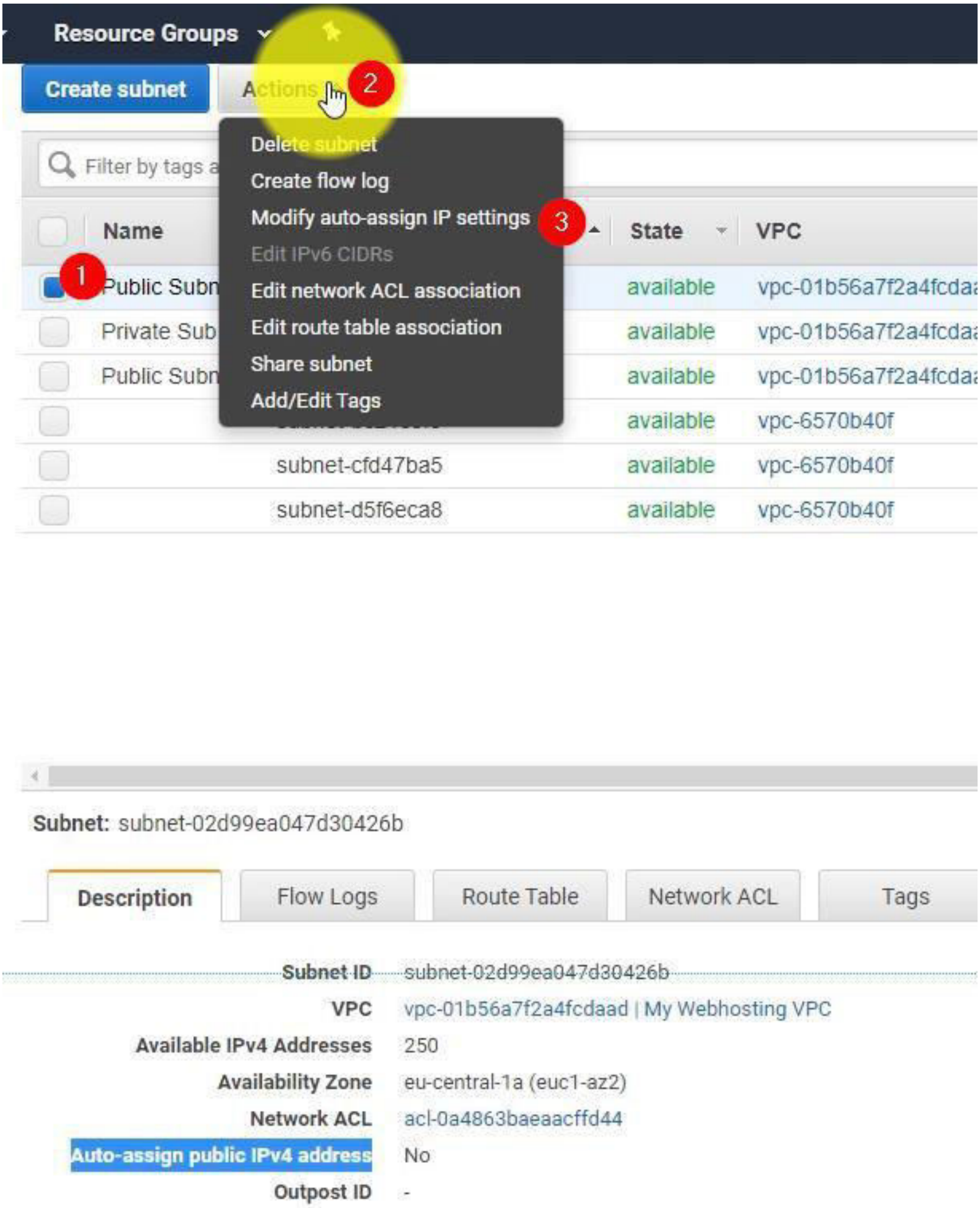


Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	nat-		No

* Required

Auto-Assign a Public IP in public Subnets

Modify *both* public subnets and activate that IP Addresses are automatically assigned:



Name		State	VPC
Public Subn		available	vpc-01b56a7f2a4fcdaa
Private Sub		available	vpc-01b56a7f2a4fcdaa
Public Subn		available	vpc-01b56a7f2a4fcdaa
		available	vpc-6570b40f
	subnet-cfd47ba5	available	vpc-6570b40f
	subnet-d5f6eca8	available	vpc-6570b40f

Subnet: subnet-02d99ea047d30426b

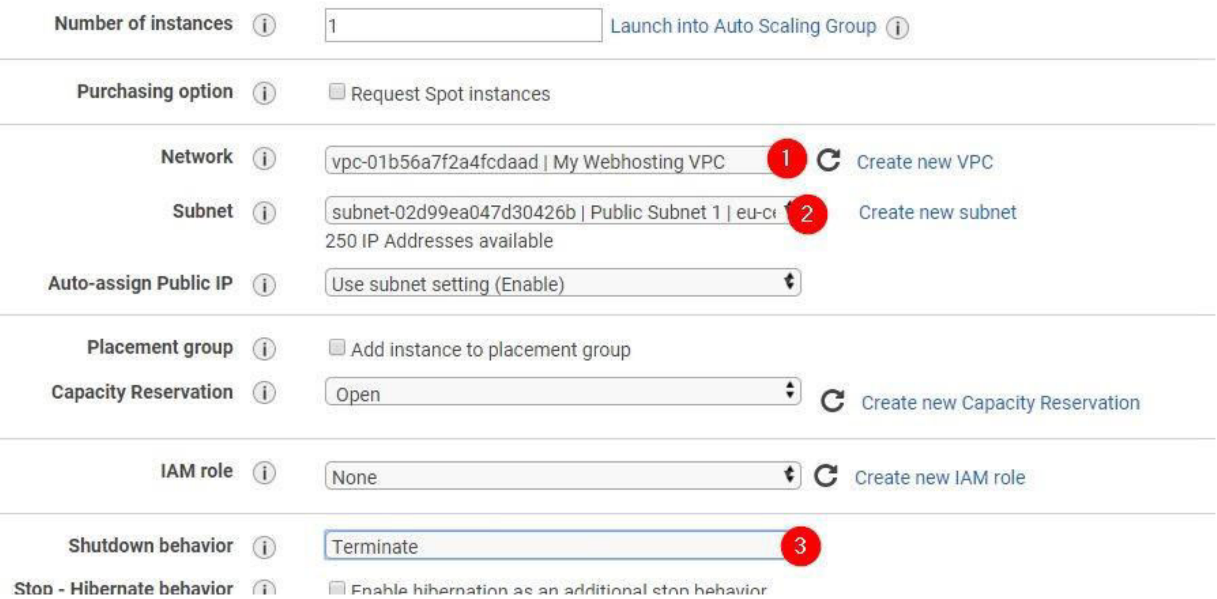
Subnet ID	subnet-02d99ea047d30426b
VPC	vpc-01b56a7f2a4fcdaad | My Webhosting VPC
Available IPv4 Addresses	250
Availability Zone	eu-central-1a (euc1-az2)
Network ACL	acl-0a4863baeaacffd44
Auto-assign public IPv4 address	No
Outpost ID	-

Launch a Bastion Host Architecture

Head over to the EC2 Dashboard and launch two instances. One in the Private Subnet and one in the public subnet with user-data.

1. Select the Amazon Linux 2 AMI
2. Select the t2.micro

Select the new VPC (1) and the public subnet for one instance, and the private subnet for another instance (2). Also select that instances should terminate on shutdown (3):



Number of instances: 1 — Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-01b56a7f2a4fcdaad | My Webhosting VPC — Create new VPC

Subnet: subnet-02d99ea047d30426b | Public Subnet 1 | eu-c — Create new subnet
250 IP Addresses available

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

Placement group: □ Add instance to placement group

Capacity Reservation: Open — Create new Capacity Reservation

IAM role: None — Create new IAM role

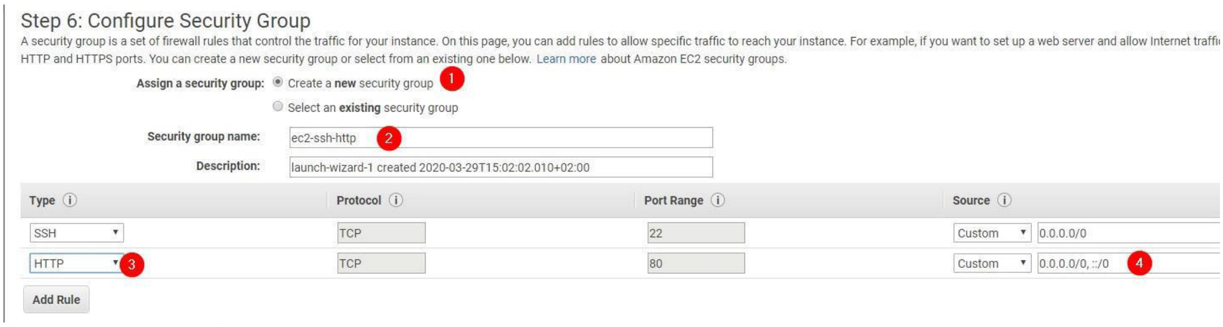
Shutdown behavior: Terminate

Stop - Hibernate behavior: □ Enable hibernation as an additional stop behavior

As User-Data enter the following (for both instances):

```
#!/bin/bash
yum update -y
amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
yum install -y httpd mariadb-server
systemctl start httpd
systemctl enable httpd
usermod -a -G apache ec2-user
chown -R ec2-user:apache /var/www
chmod 2775 /var/www
find /var/www -type d -exec chmod 2775 {} \;
find /var/www -type f -exec chmod 0664 {} \;
echo "<?php phpinfo(); ?>" > /var/www/html/phpinfo.php
echo "hello apache" > /var/www/html/index.html
```

For the first instance add a new security Group which allows HTTP Access from anywhere:



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 traffi 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 1
○ Select an **existing** security group

Security group name: ec2-ssh-http 2

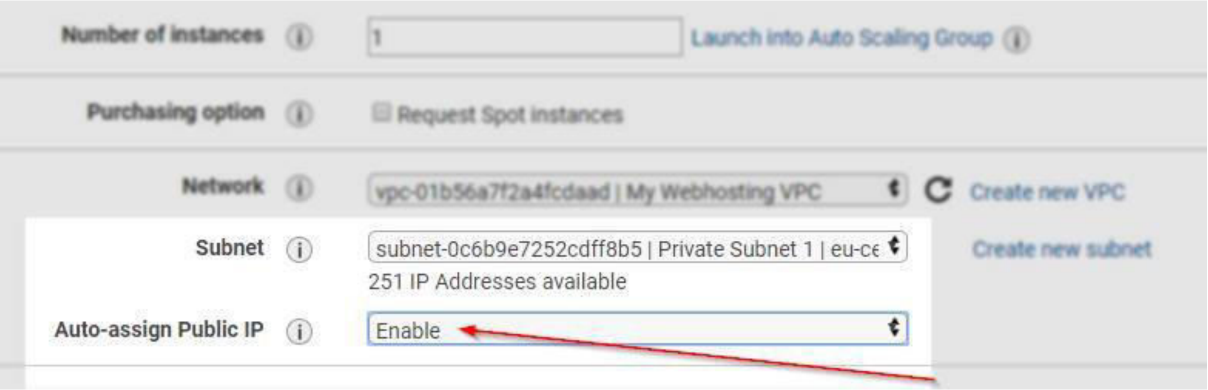
Description: launch-wizard-1 created 2020-03-29T15:02:02.010+02:00

Type	Protocol	Port Range	Source
SSH	TCP	22	Custom 0.0.0.0/0
HTTP 3	TCP	80	Custom 0.0.0.0/0, ::/0 4

Then launch the instance.

Launch the instance in the private subnet

For the second instance, do exactly the same as for the public instance, just launch it into the private subnet, but still enable public IP address:



Number of instances: 1

Purchasing option: □ Request Spot instances

Network: vpc-01b56a7f2a4fcdaad | My Webhosting VPC

Subnet: subnet-0c6b9e7252cdff8b5 | Private Subnet 1 | eu-ce
251 IP Addresses available

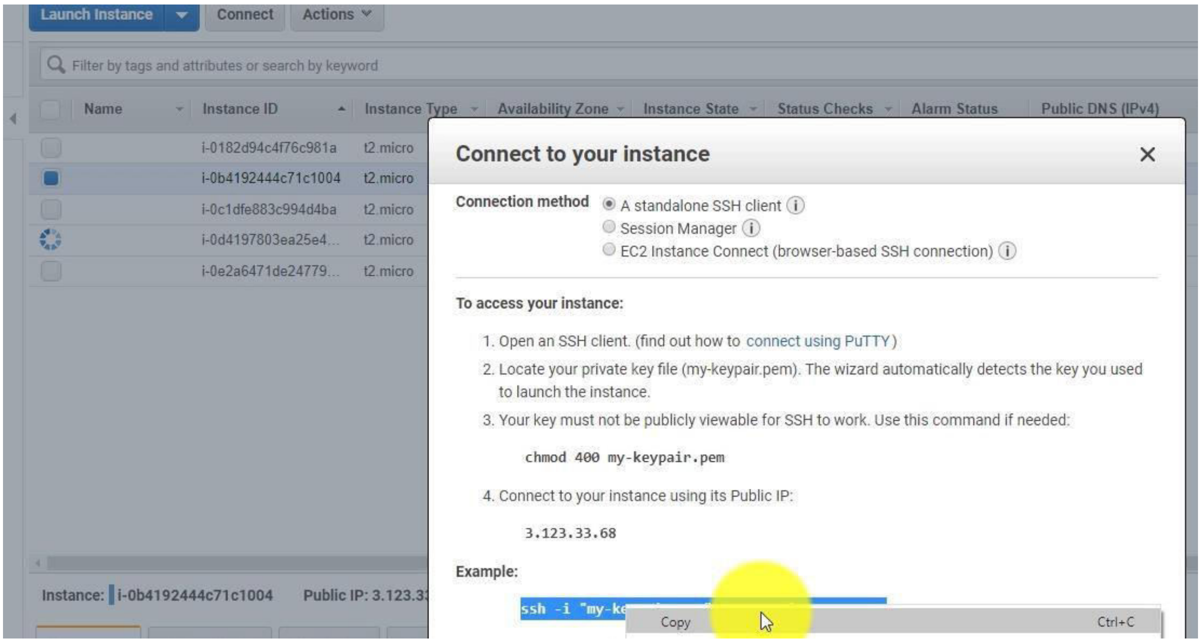
Auto-assign Public IP: Enable

Add the same user-data, select the same Security group we created for the previous instance.

Then launch the instance.

Access Instance in Public Subnet

SSH Into the Instance in the public subnet:



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
	i-0182d94c4f76c981a	t2.micro					
	i-0b4192444c71c1004	t2.micro					
	i-0c1dfe883c994d4ba	t2.micro					
	i-0d4197803ea25e4...	t2.micro					
	i-0e2a6471de24779...	t2.micro					

Instance: i-0b4192444c71c1004 Public IP: 3.123.3

Connect to your instance

Connection method ● A standalone SSH client
○ Session Manager
○ EC2 Instance Connect (browser-based SSH connection)

To access your instance:

1. Open an SSH client. (find out how to connect using PuTTY)
2. Locate your private key file (my-keypair.pem). The wizard automatically detects the key you used to launch the instance.
3. Your key must not be publicly viewable for SSH to work. Use this command if needed:

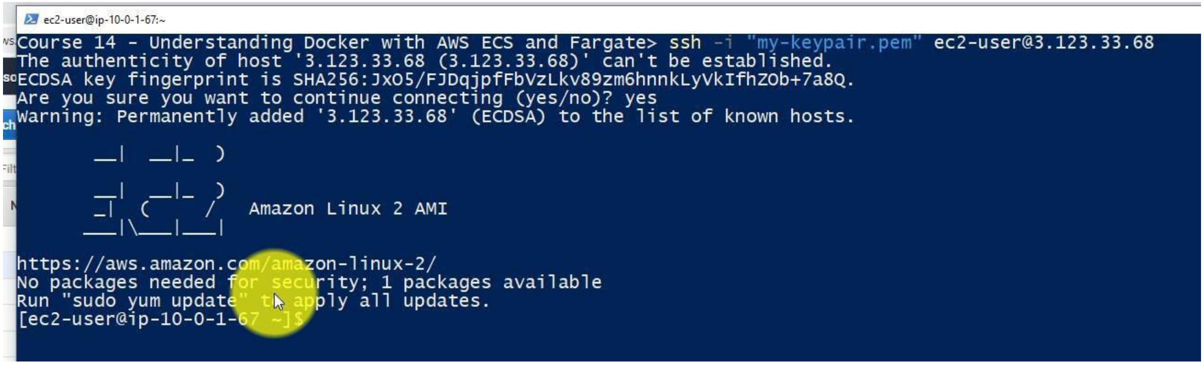
```
chmod 400 my-keypair.pem
```

4. Connect to your instance using its Public IP:

```
3.123.33.68
```

Example:

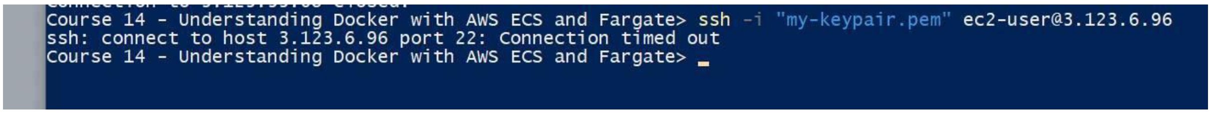
```
ssh -i "my-ke
```



```
ec2-user@ip-10-0-1-67:~
Course 14 - Understanding Docker with AWS ECS and Fargate> ssh -i "my-keypair.pem" ec2-user@3.123.33.68
The authenticity of host '3.123.33.68 (3.123.33.68)' can't be established.
ECDSA key fingerprint is SHA256:Jx05/FJDqjpfFbVzLkv89zm6hnnkLyVkIfhZOb+7a8Q.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '3.123.33.68' (ECDSA) to the list of known hosts.

       __|  __|_  )

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
No packages needed for security; 1 packages available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-10-0-1-67 ~]$
```

Try to Access into the EC2 Instance in the private Subnet

Observe a connection timeout when you try and connect to the instance in the private subnet:

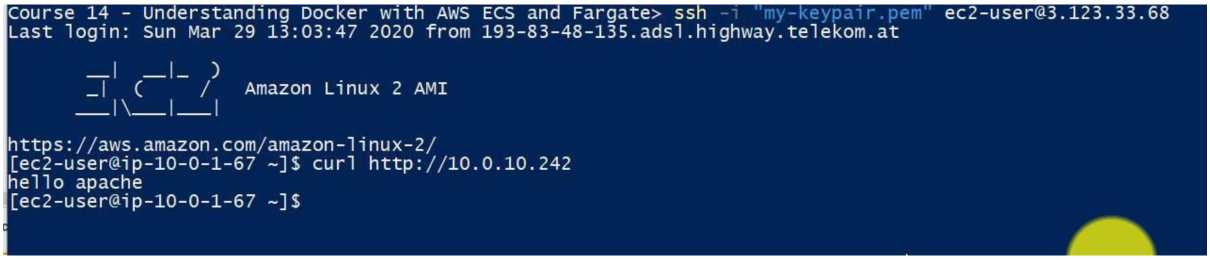


```
Course 14 - Understanding Docker with AWS ECS and Fargate> ssh -i "my-keypair.pem" ec2-user@3.123.6.96
ssh: connect to host 3.123.6.96 port 22: Connection timed out
Course 14 - Understanding Docker with AWS ECS and Fargate> _
```

Access the private instance via the bastion host

Our Instance in the public subnet acts as a bastion host. SSH into the public instance and then from there connect to the private instance:

1. SSH Into the instance in the public subnet
2. Curl from there to the private IPv4 Address of the instance in the private subnet
3. You should see the output from Apache.
4. That means you can connect via the bastion host



```
Course 14 - Understanding Docker with AWS ECS and Fargate> ssh -i "my-keypair.pem" ec2-user@3.123.33.68
Last login: Sun Mar 29 13:03:47 2020 from 193-83-48-135.adsl.highway.telekom.at

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-10-0-1-67 ~]$ curl http://10.0.10.242
hello apache
[ec2-user@ip-10-0-1-67 ~]$
```

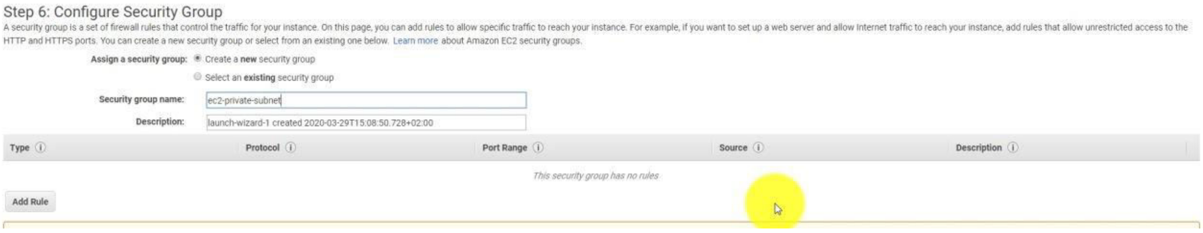
You can safely terminate your instances now to save Free-Tier credits.

Use a Load Balancer to connect to Instances in private Subnets

Launch a private EC2 Instance

Launch again an EC2 Instance with the same AMI, same Instance type as before, same User-Data.

For the security group, create a new security group and remove *all* rules:



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 name: ec2-private-subnet

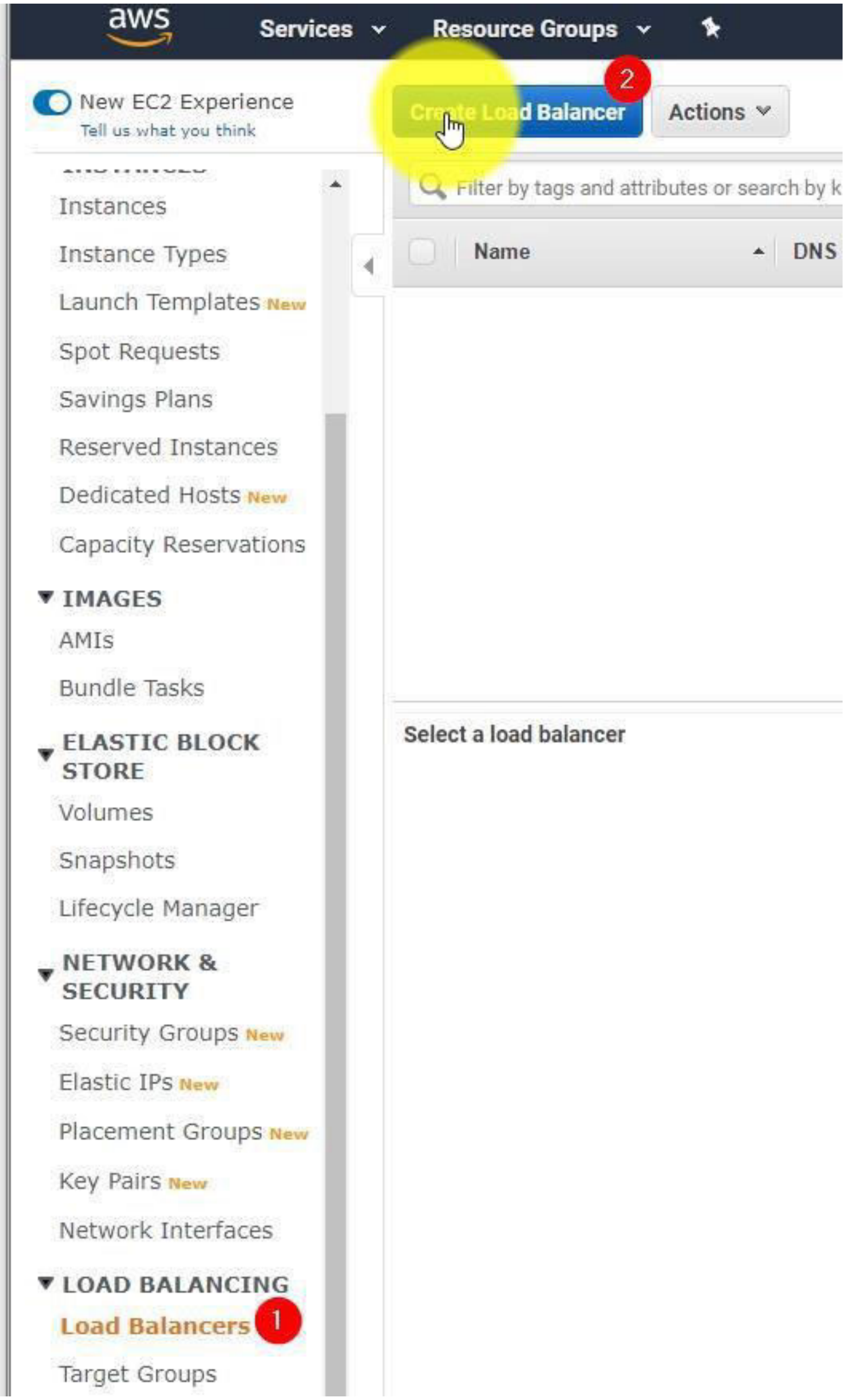
Description: launch-wizard-1 created 2020-03-29T15:08:50.728+02:00

Type	Protocol	Port Range	Source	Description
		This security group has no rules		

Then launch your instance.

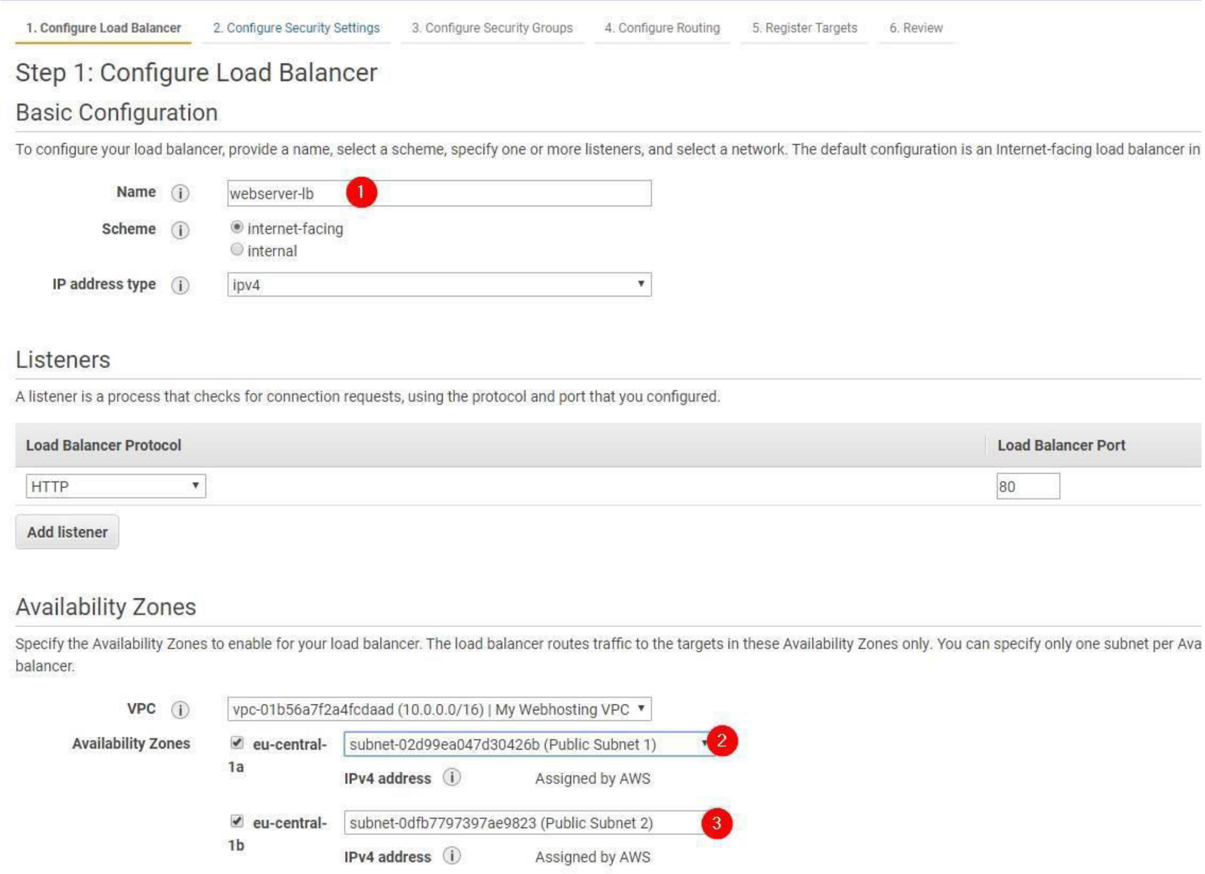
Create an Application Load Balancer

In the EC2 Dashboard select Load Balancer and hit “Create Load Balancer”



Select a load balancer

Select an Application Load Balancer. Give the Load Balancer a name (1) and place it into your two *public* subnets (2) and (3):



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

Name: webserver-lb (1)

Scheme: ● internet-facing ○ internal

IP address type: ipv4

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port
HTTP	80

Add listener

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 Ava balancer.

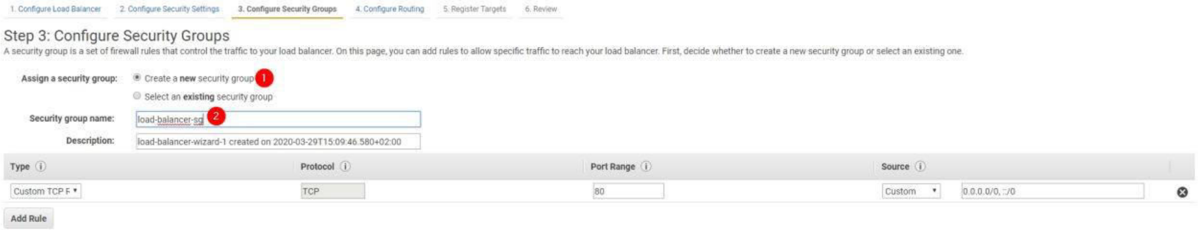
VPC: vpc-01b56a7f2a4fcdaad (10.0.0.0/16) | My Webhosting VPC

Availability Zones:

☑ eu-central-1a: subnet-02d99ea047d30426b (Public Subnet 1) (2)
IPv4 address: Assigned by AWS

☑ eu-central-1b: subnet-0dfb7797397ae9823 (Public Subnet 2) (3)
IPv4 address: Assigned by AWS

Attach a new Security Group to the Load Balancer:



1. Configure Load Balancer | 2. Configure Security Settings | 3. Configure Security Groups | 4. Configure Routing | 5. Register Targets | 6. Review

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 (1) ○ Select an **existing** security group

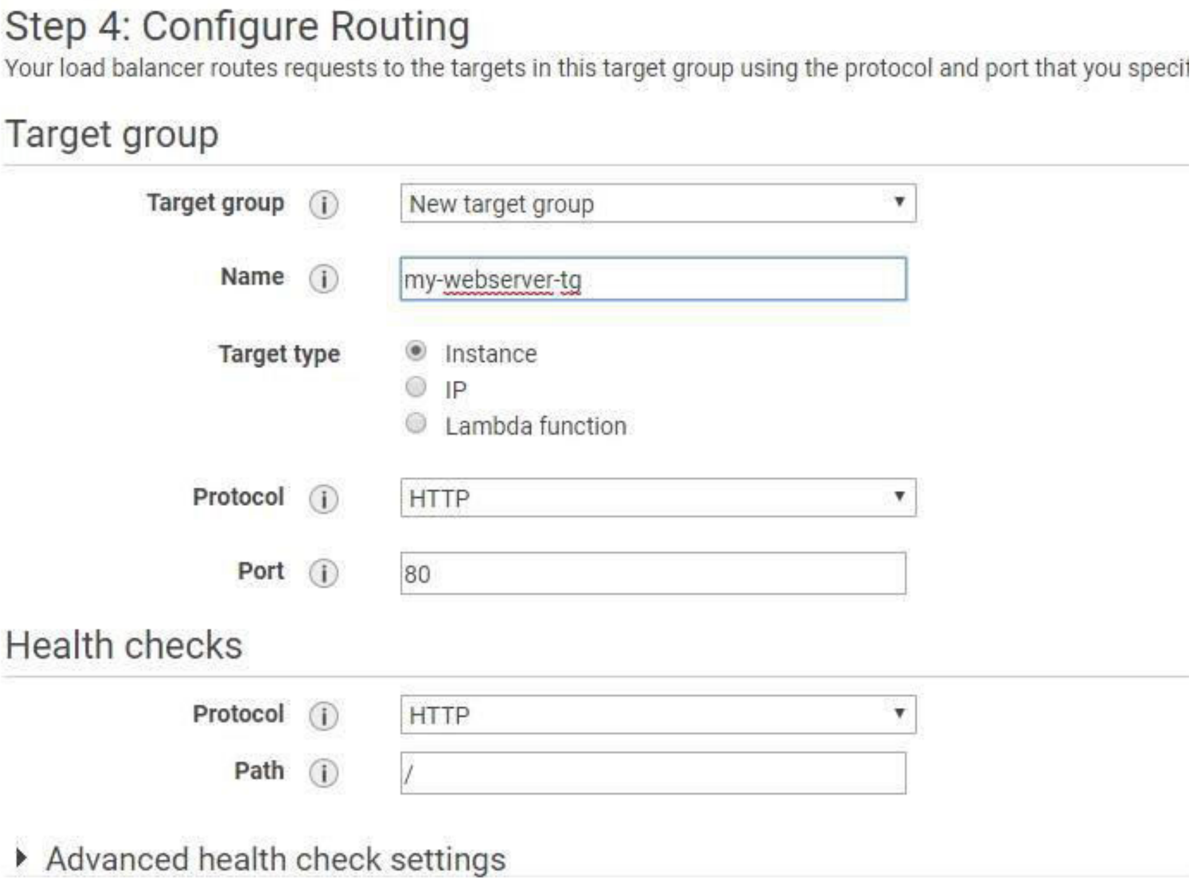
Security group name: load-balancer-sg (2)

Description: load-balancer-wizard-1 created on 2020-03-29T15:09:46.580+02:00

Type	Protocol	Port Range	Source	
Custom TCP F	TCP	80	Custom	0.0.0.0/0, ::/0

Add Rule

Create a new Target Group for the Load Balancer:



Step 4: Configure Routing

Your load balancer routes requests to the targets in this target group using the protocol and port that you specif

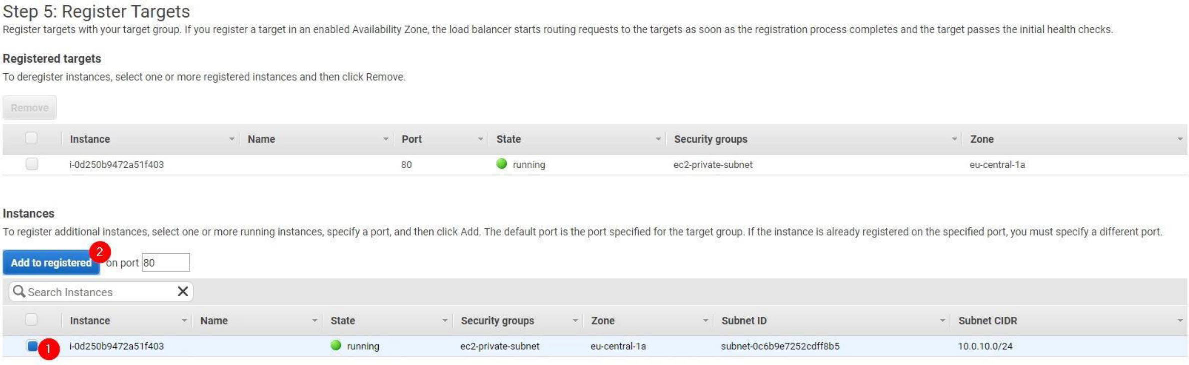
Target group

Target group	New target group
Name	my-webserver-tg
Target type	● Instance ○ IP ○ Lambda function
Protocol	HTTP
Port	80

Health checks

Protocol	HTTP
Path	/

Register your Instance in your private subnet into the Target Group:



Step 5: Register Targets

Register targets with your target group. If you register a target in an enabled Availability Zone, the load balancer starts routing requests to the targets as soon as the registration process completes and the target passes the initial health checks.

Registered targets

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

□	Instance	Name	Port	State	Security groups	Zone
□	i-0d250b9472a51f403		80	● running	ec2-private-subnet	eu-central-1a

Instances

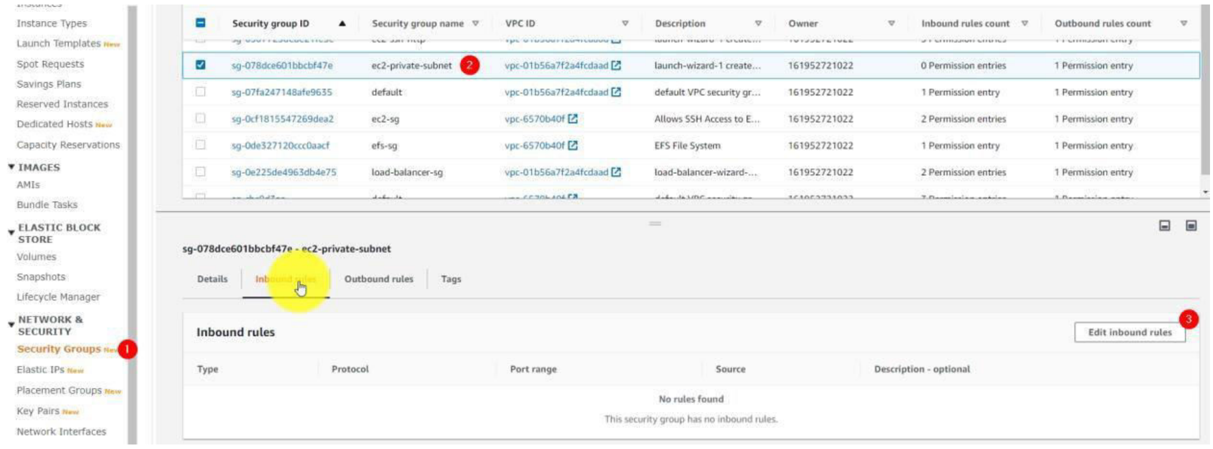
To register additional instances, select one or more running instances, specify a port, and then click Add. The default port is the port specified for the target group. If the instance is already registered on the specified port, you must specify a different port.

□	Instance	Name	State	Security groups	Zone	Subnet ID	Subnet CIDR
☑ 1	i-0d250b9472a51f403		● running	ec2-private-subnet	eu-central-1a	subnet-0c6b9e7252cdff8b5	10.0.10.0/24

Then create the Load Balancer.

Allow Load-Balancer Traffic in the Security Group

In the ec2-instance security group edit the inbound rules to allow Traffic from the Load Balancer to the EC2 Intance:



	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
☑	sg-078dce601bbcbf47e	ec2-private-subnet	vpc-01b56a7f2a4fcdaad	launch-wizard-1 create...	161952721022	0 Permission entries	1 Permission entry
□	sg-07fa247148afe9635	default	vpc-01b56a7f2a4fcdaad	default VPC security gr...	161952721022	1 Permission entry	1 Permission entry
□	sg-0cf1815547269dea2	ec2-sg	vpc-6570b40f	Allows SSH Access to E...	161952721022	2 Permission entries	1 Permission entry
□	sg-0de327120ccc0aacf	efs-sg	vpc-6570b40f	EFS File System	161952721022	1 Permission entry	1 Permission entry
□	sg-0e225de4963db4e75	load-balancer-sg	vpc-01b56a7f2a4fcdaad	load-balancer-wizard-...	161952721022	2 Permission entries	1 Permission entry

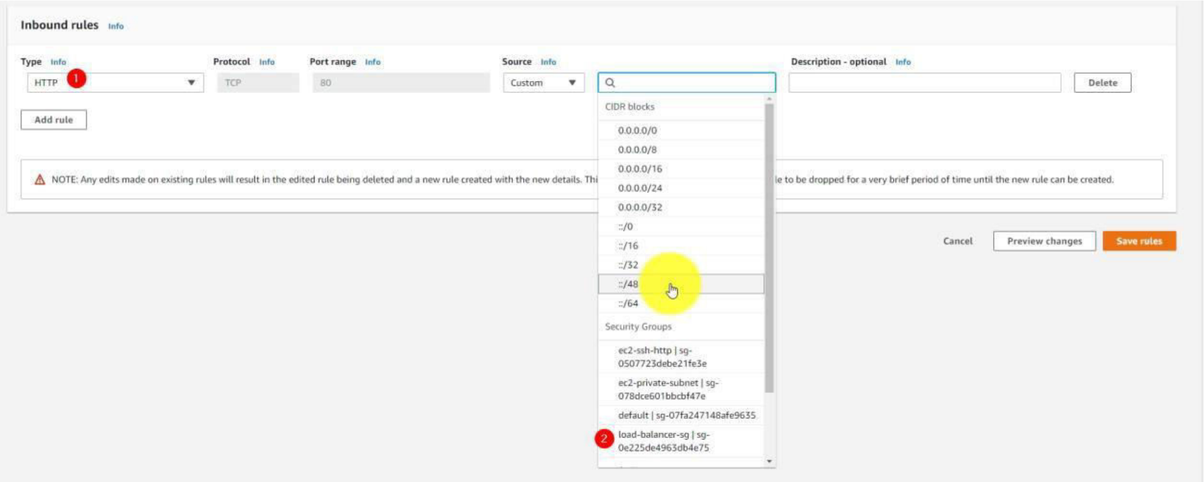
sg-078dce601bbcbf47e - ec2-private-subnet

Inbound rules

Type	Protocol	Port range	Source	Description - optional

No rules found

This security group has no inbound rules.


Inbound rules Info

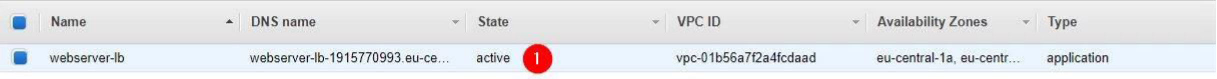
Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Custom	

1
Delete
Add rule
CIDR blocks
0.0.0.0/0
0.0.0.0/8
0.0.0.0/16
0.0.0.0/24
0.0.0.0/32
::/0
::/16
::/32
::/48
::/64
Security Groups
ec2-ssh-http | sg-0507723debe21fe3e
ec2-private-subnet | sg-078dce601bbcbf47e
default | sg-07fa247148afe9635
2
load-balancer-sg | sg-0e225de4963db4e75
Cancel
Preview changes
Save rules

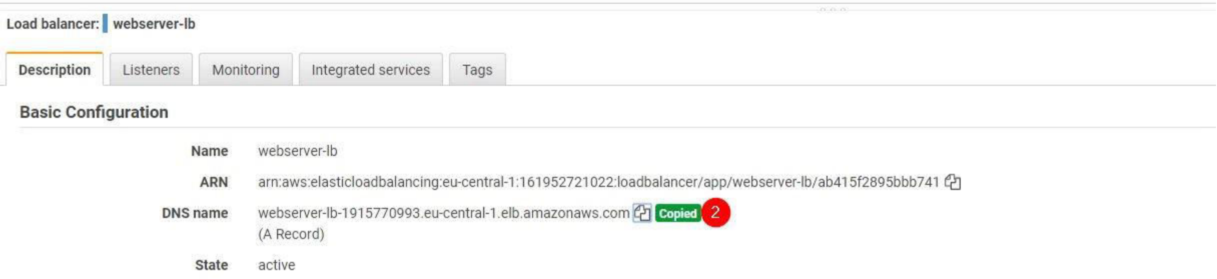
NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. Thi … le to be dropped for a very brief period of time until the new rule can be created.

Test the Load Balancer

Wait until the load balancer is active, then copy the DNS Name and open the url in a new Tab:



	Name	DNS name	State	VPC ID	Availability Zones	Type
■	webserver-lb	webserver-lb-1915770993.eu-ce...	active 1	vpc-01b56a7f2a4fcdaad	eu-central-1a, eu-centr...	application


Load balancer: webserver-lb

Basic Configuration

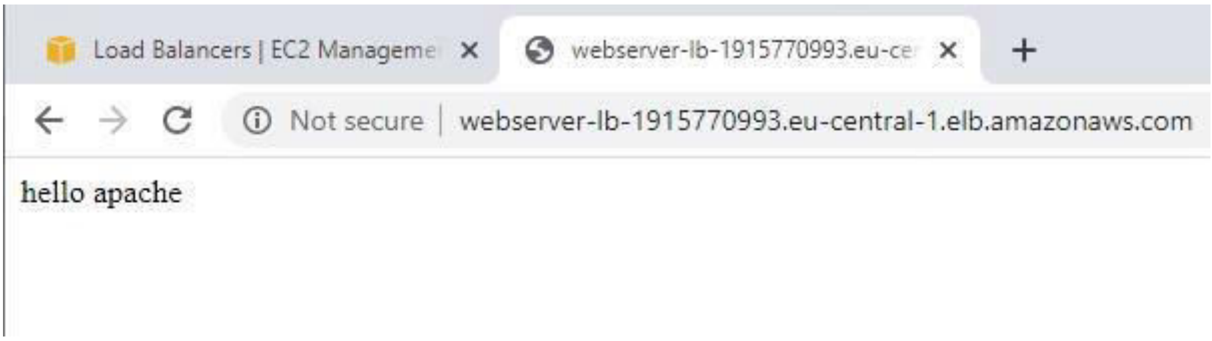
Name webserver-lb

ARN arn:aws:elasticloadbalancing:eu-central-1:161952721022:loadbalancer/app/webserver-lb/ab415f2895bbb741

DNS name webserver-lb-1915770993.eu-central-1.elb.amazonaws.com Copied 2
(A Record)

State active

You should see the hello apache string:



Load Balancers | EC2 Manageme
webserver-lb-1915770993.eu-ce
Not secure
webserver-lb-1915770993.eu-central-1.elb.amazonaws.com

hello apache

Clean Up

Tear down everything again:

1. Terminate the EC2 Instance
2. Delete the Load Balancer
3. Remove the Target Group
4. Delete the NAT Gateway
5. Disassociate the Elastic IP
6. Then Release the Elastic IP
7. Disassociate the Public Subnets from the Custom Route Table
8. Delete the Custom Route Table
9. Detach the Internet Gateway from the VPC
10. Delete the Internet Gateway
11. Delete the three Subnets from your VPC
12. Delete the VPC
13.