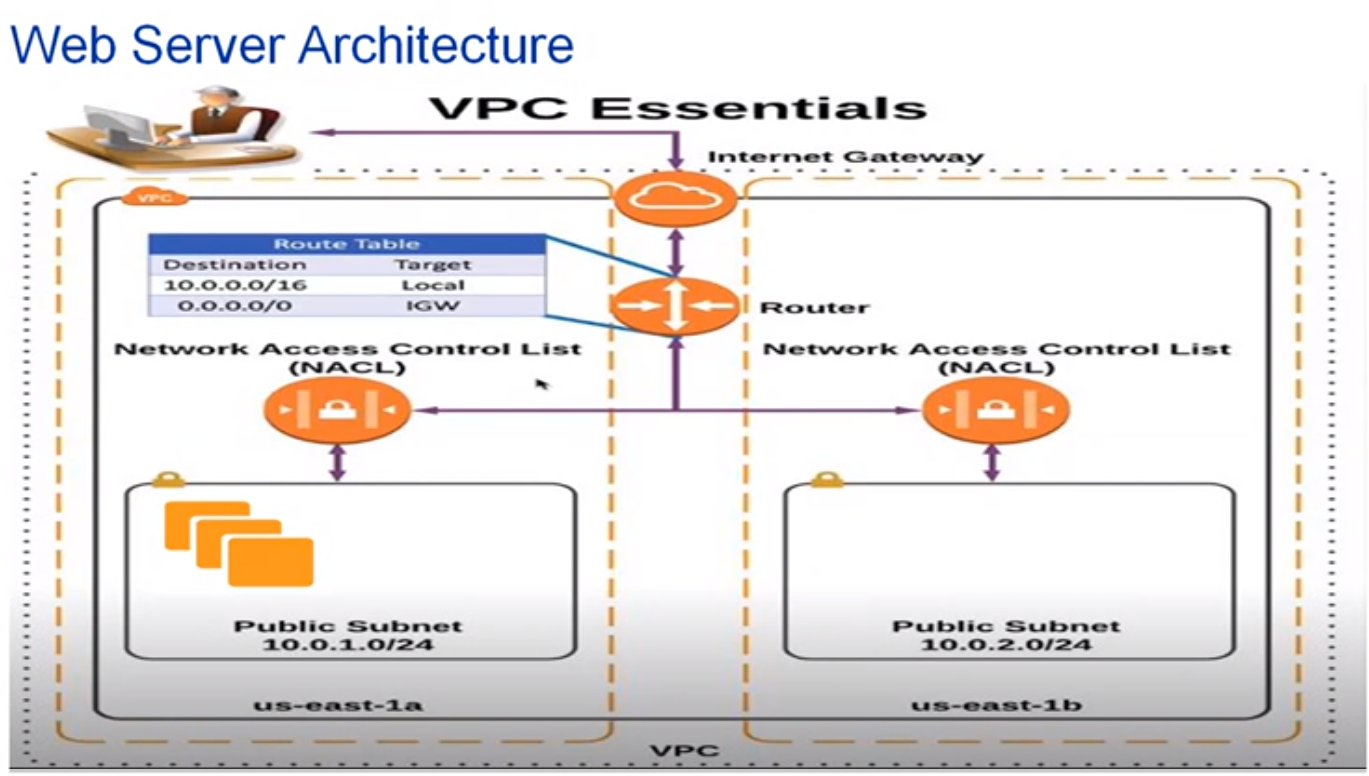
# Hands-on – 1

# AWS-lab-hands-on-practice

You will be able to create a various infrastructure components that will be used to **build Web server** within the AWS Cloud Environment.



Web site->has different infrastructure layer-> It shows how server can be access by application user.

* All firewall, router etc can be replaced with virtual components.
* VPC-Configure of VPC is important for component inside the it to communicate with each other and with internet.
* Internet Gateway Point – It is vpc access point to internet
* Router – Responsible for define routes from different resource to internet gateway. It created while creating VPC.
* -Availability Zone are collection of data centers which present under a region to ensure high availability of application whenever there is outage in one specific data center.
* NACL(Network Access Control List)- Created in availability Zone. It is first layer of defece for our resources applied at subnet level.

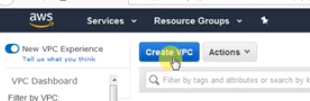
They are stateless and they need to have inbound and outbound rule to complete the access pattern.

* Subnet – Forms a vpc ip address range which is responsible for hosting your resource.

It can be public or private depending on whether they access to internet or not. Public subnet come back to DMZ within a traditional data center which exposes the organization to external world

Phase 1: Create VPC

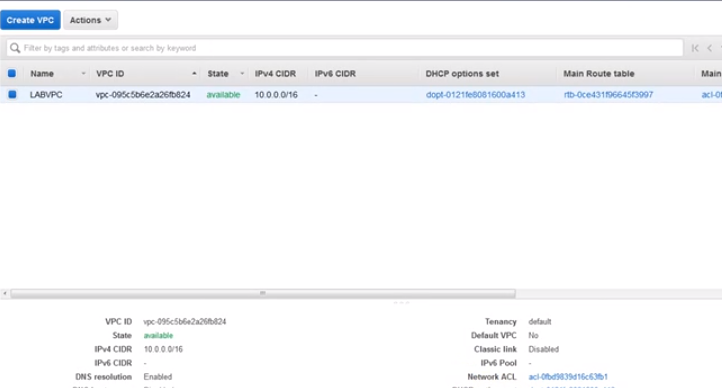
* + Select VPC from dashboard-> Create VPC



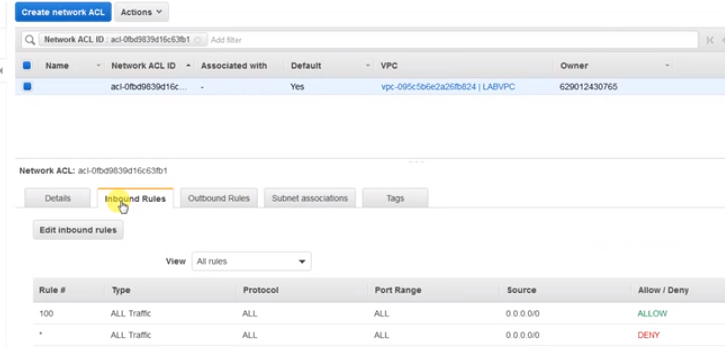
Step 2:Enter vpc details: Name, CIDR block details (IP address range) -10.0.0.0/16

16 is CIDR mask- > specify no, of ip address (32-16=16) so 16 then 2raise to 16 =65536 ipaddress

CIDR : Classless Inter-Domain Routing



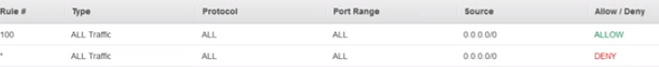
Step 3: Explore VPC- click on NACL



In above inbound rule says allow any traffic from any source. NACL works on first match basis and it evaluates from lowest rule to highest rule.

Observe this

**NACL:**



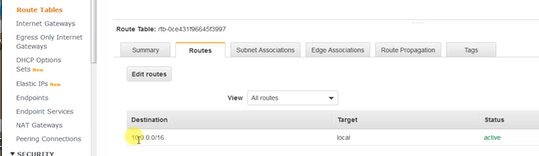
First rule that matches the specified protocol or the port ranges however \* Rule # deny so as allow comes before Deny so it will be applicable.

**Route Table:**

<https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Route_Tables.html>

Whenever a [node](https://en.wikipedia.org/wiki/Node_(networking)) needs to send data to another node on a network, it must first know *where* to send it. If the node cannot directly connect to the destination node, it has to send it via other nodes along a route to the destination node. Each node needs to keep track of which way to deliver various packages of data, and for this it uses a routing table. A routing table is a database that keeps track of paths, like a map, and uses these to determine which way to forward traffic. A routing table is a data file in RAM that is used to store route information about directly connected and remote networks. Nodes can also share the contents of their routing table with other nodes.

1. Click on Route table from left pane and click on Route tab



We have one local route within local vpc. The target is mentioned as **loca**l which means that if one resource in one subnet and another in one subnet both can communicate with each other.

Step 4: Create Internet Gateway

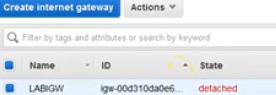
<https://docs.aws.amazon.com/vpc/latest/userguide/VPC_Internet_Gateway.html>

1. Click on Internet Gateway from left pane.
2. Enter Internet Gateway name LABGW



Close.

It shows status as detached.



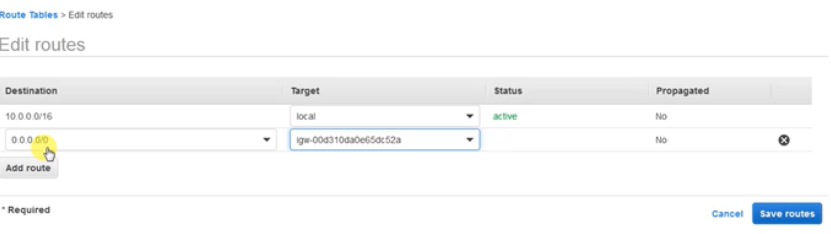
1. Attach it to VPC -> Click on Action ->Attach -> Select VPC +Attach



Step 5: Setup Route to allow the internet access to all of the resource, subnet and all.

Let do that

1. Click on Edit Routes
2. Using this we will internet access for our resource

sud

0.0.0.0 /0 means all traffic which is not distinct locally within vpc will routed through internet gateway.

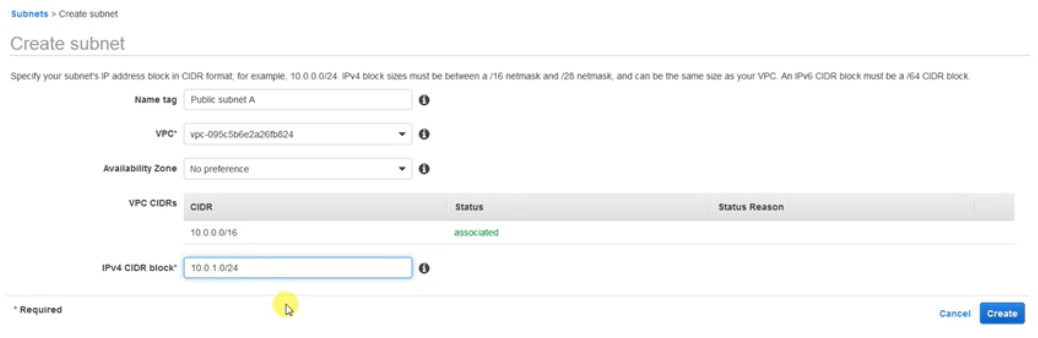
Step 6: Setup Subnet A

We will create subnet each availability zone.

1. Click on Subnet + Click on Create subnet

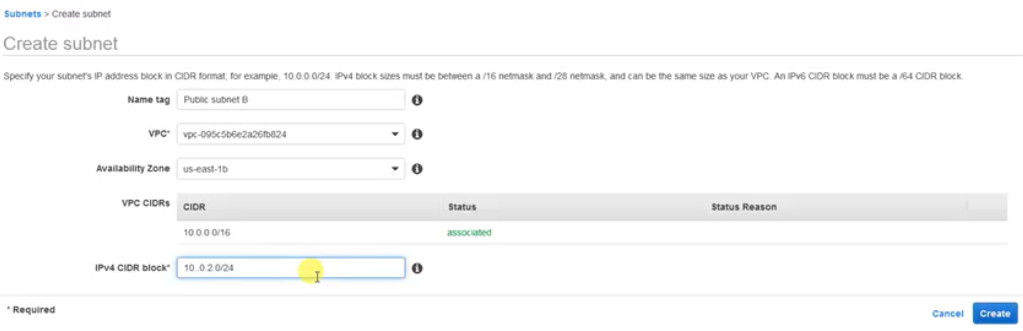


1. Enter details



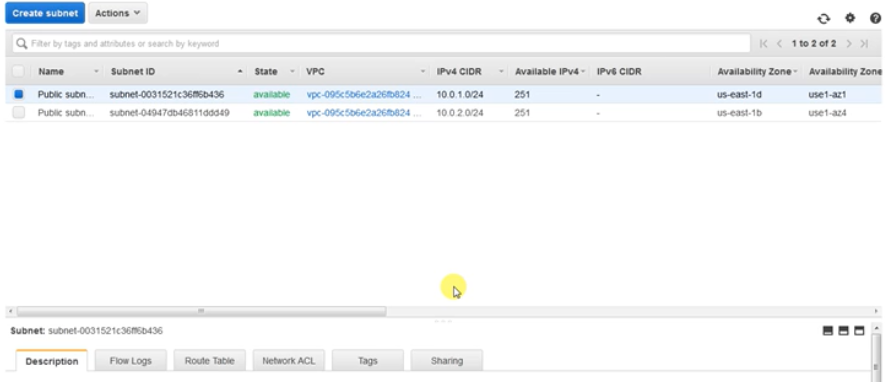
Total available ip range for 10.0.1.0/24 means total available ip address would 32-24=8 and 2 raise 8 means 256.

Step 7: Create another subnet B and another availability zone

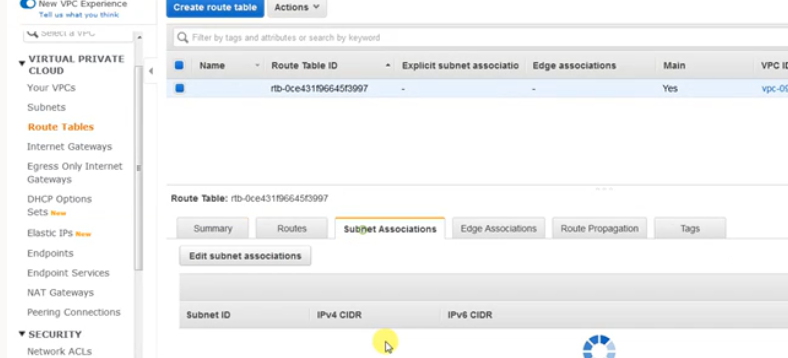




Step 8: Make the subnet as public by associating the subnets with route table

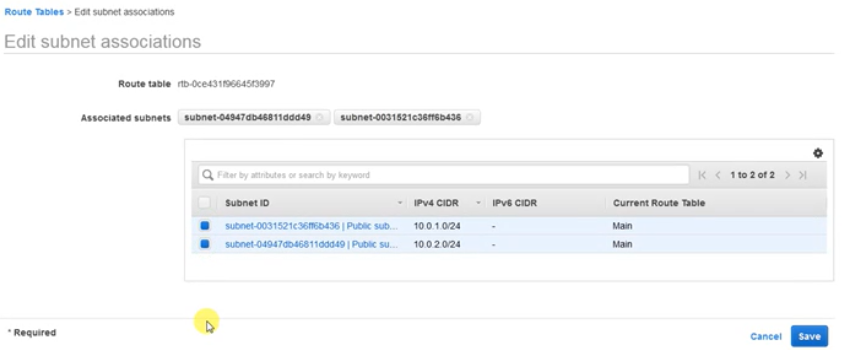


Step 8: Click on Route link on left pane and click on SUBNET Association

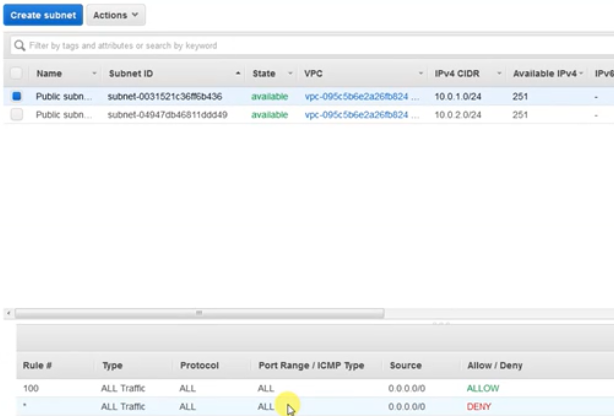


Step 9: Click on Edit subnet associations

1. Select both subnets

+Save

Step 10: Click on subnet list and review the NACL list for both the subnet. Currently it is same.

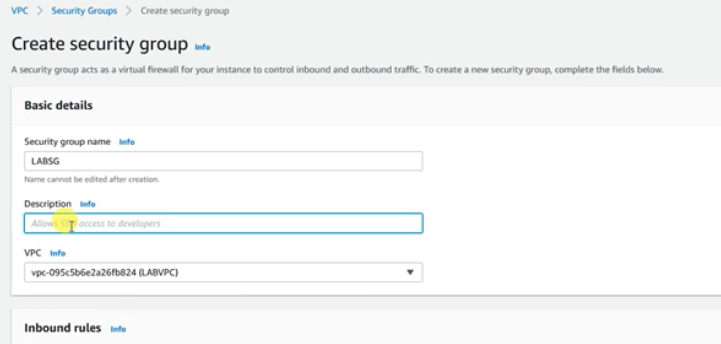


Step 11: Create Security Group

Another layer of defense is Security group which is specific for particular resource such db, ec2, web server etc.

Note: Security Groups are STATEFULL.

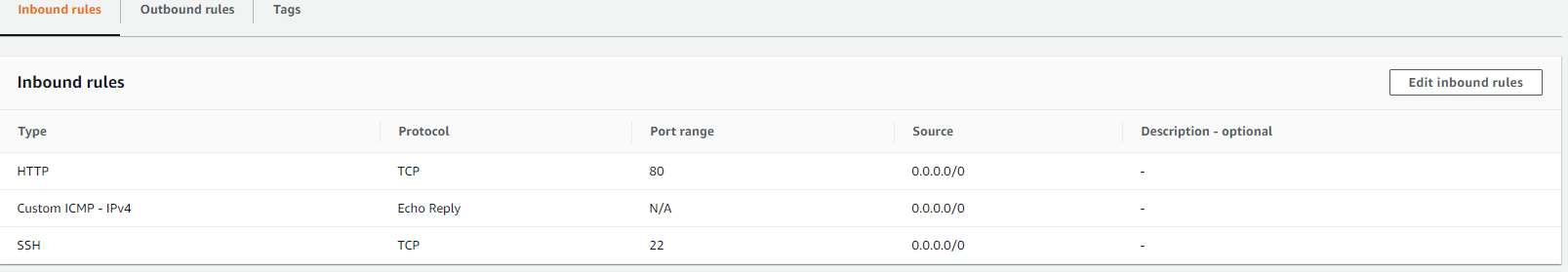
1. Click on Security group from left pane.
2. Enter SG name:



1. Add inbound rule –
   * 1. **HTTP**

Allow http traffic on port 80 from anywhere.

* + 1. Custom IPV4 rule is for **allows access from internet of an website url and http and select dns name.**



Phase 2: Create EC2 which would be a web server

Step 1: Go to EC2 -> click on running instance

Step 2: Select Launch instance

Step 3: Select

1. Linux 2 AMI
2. instance type -> t2-micro
3. Configure instance Details
   * 1. Select vpc that you have created)
     2. Map the ec2 instance with **public subnet A.**
     3. Make Auto Assign Public IP = Enable
     4. As you want the helloworld page on hit of url so you need to add script

In Advanced Details section -> in User Data add following script

#!/bin/bash

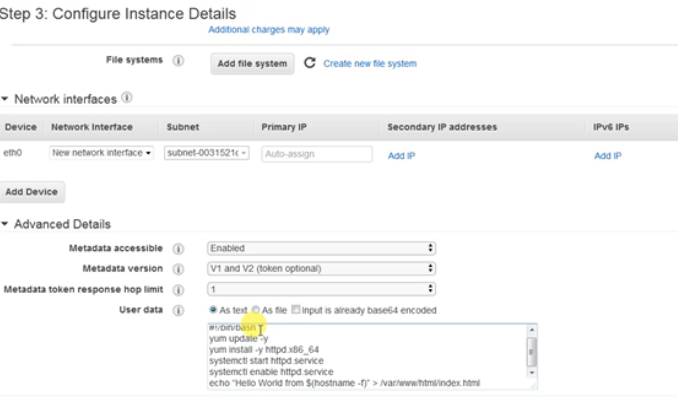
yum update -y

yum install -y httpd.x86\_64

systemctl start httpd.service

systemctl enable httpd.service

echo "Hello World from $(hostname -f) > /var/www/html/index.html



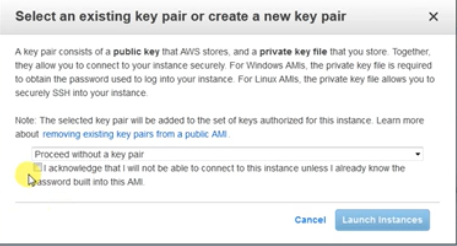
It will executed whenever instance is going to be created.

1. Select Security Group that we have create (http+icmp)
2. Review+Launch

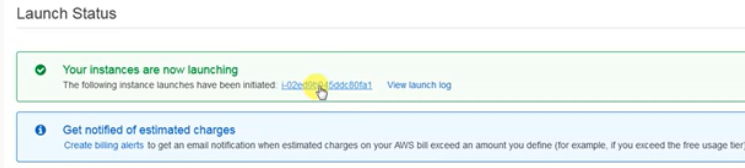
Step 4: download key pair

No need to select key pair because we are not going to login.

Select -> Proceed without key pair

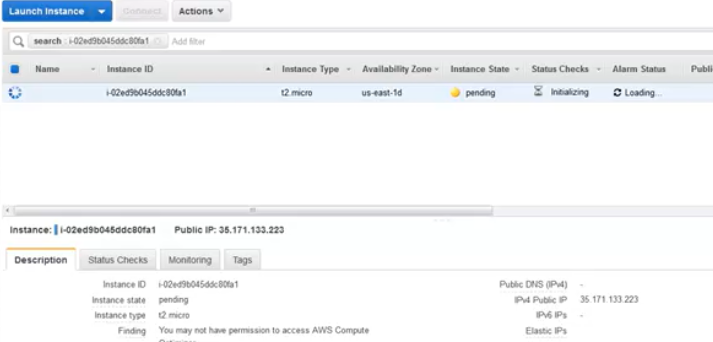


Launch instance



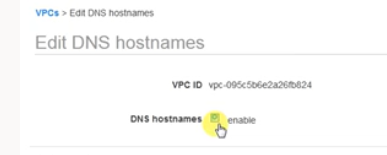
Step 5: Click on link given with the following instance have been initiated.

Setup 6: Currently Public DNS for ec2 will **not be enabled**. So you have to enable it by

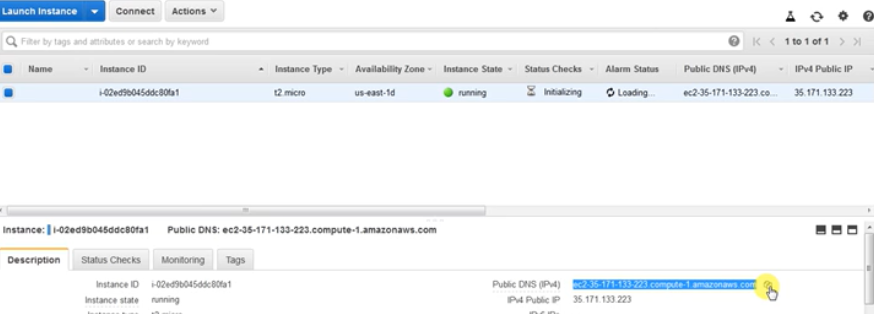


Step 7: Go to VPC -> Action->Select “Edit DNS Host Name”

Click on check box DNS Hostname: enable

 +Save

Step 8: Switch EC2 and check public dns ip :



Step 9” Click on Connect

You will get prompt

[ec2-user@ip-10-0-1-157 ~]$ sudo su

[root@ip-10-0-1-157 ec2-user]# yum update –y

[root@ip-10-0-1-157 ec2-user]# systemctl start httpd.service

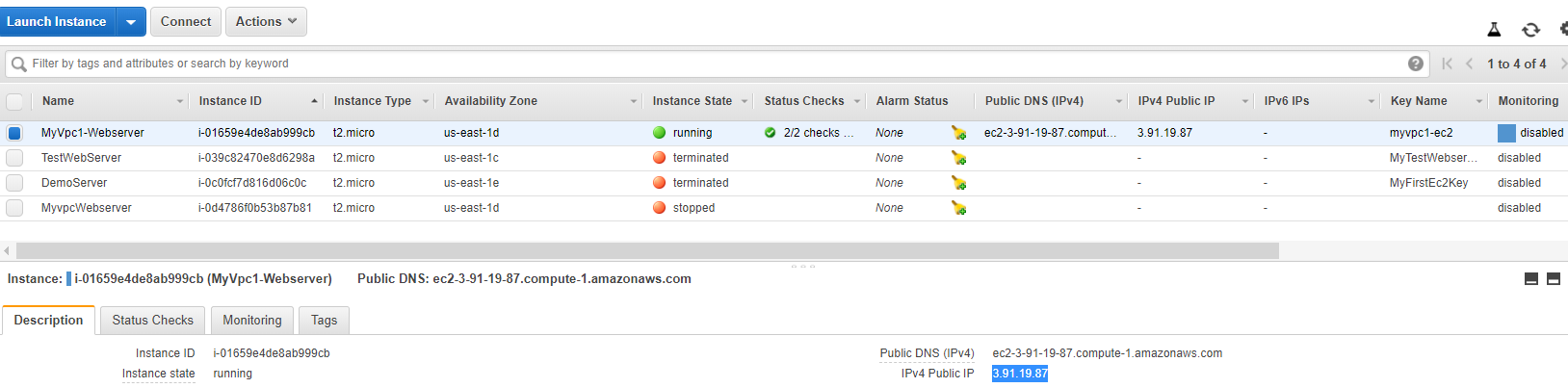
[root@ip-10-0-1-157 ec2-user]# systemctl enable httpd.service

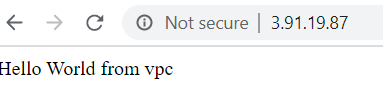
Switch to /var/www/html

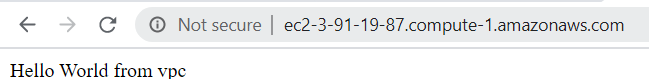
[root@ip-10-0-1-157 html]# echo "Hello World from vpc" >index.html

[root@ip-10-0-1-157 html]# cat index.html

Test Now:







Step 9: Wait for some time and then past dns url

