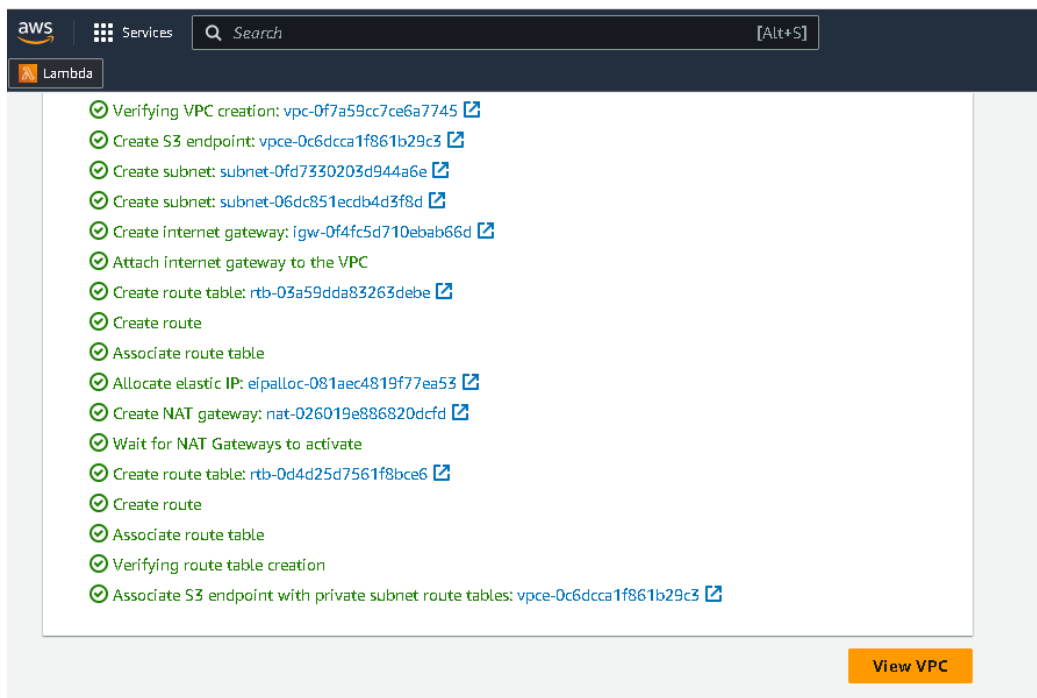
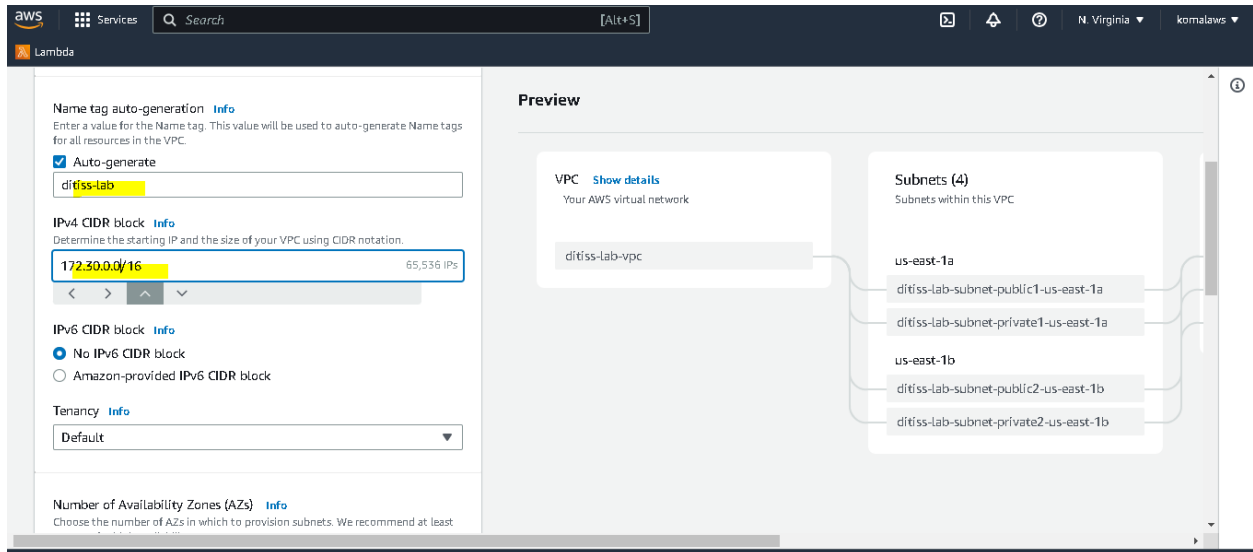


A **virtual private cloud (VPC)** is a secure, isolated private cloud hosted within a public cloud. VPC customers can run code, store data, host websites, and do anything else they could do in an ordinary private cloud, but the private cloud is hosted remotely by a public cloud provider.

## 1)create vpc



aws Services Search [Alt+S] N. Virginia kornalaws

Lambda

VPC dashboard X

EC2 Global View New

Filter by VPC:  
Select a VPC

▼ Virtual private cloud

Your VPCs New

Subnets

Route tables

Internet gateways

Egress-only Internet gateways

Carrier gateways

DHCP option sets

Elastic IPs

Managed prefix lists

Endpoint

VPC > Your VPCs > vpc-0f7a59cc7ce6a7745

vpc-0f7a59cc7ce6a7745 / ditiss-lab-vpc Actions

Details Info

VPC ID vpc-0f7a59cc7ce6a7745	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-03744a32e1df37e7e	Main route table rtb-0bdc04efce984ed94	Main network ACL acl-06cf1211cad8159b6
Default VPC No	IPv4 CIDR 172.30.0.0/16	IPv6 pool -	IPv6 CIDR (Network border group) -
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups -	Owner ID 423894482761	

Resource map New CIDRs Flow Logs Tags

Now our vpc is created go to instances

## 1) Make private instance

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name  
privatevpc Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Quick Start

▼ Summary

Number of instances Info  
1

Software Image (AMI)  
Debian 11 (20230515-1381)  
ami-01e5ff16fd6e8c542

Virtual server type (instance type)  
t2.micro

Firewall (security group)  
New security group

Storage (volumes)

Cancel Launch instance Review commands

Create .pem key for private, and allow ssh http and https for it

Key pair name  
Key pairs allow you to connect to your instance securely.

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type


☒ RSA  
RSA encrypted private and public key pair

☐ ED25519  
ED25519 encrypted private and public key pair

Private key file format

☒ .pem  
For use with OpenSSH

☐ .ppk  
For use with PuTTY

 When prompted, store the private key in a secure and accessible location on

[Cancel](#) [Create key pair](#)

Go to network settings don't provide public ip ,select vpc cloud name as ditiss private ,

▼ Network settings [Info](#)

VPC - required [Info](#)

172.30.0.0/16

Subnet [Info](#)

VPC: vpc-0f7a59cc7ce6a7745 Owner: 423894482761 Availability Zone: us-east-1a  
IP addresses available: 4091 CIDR: 172.30.128.0/20

Auto-assign public IP [Info](#)

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

Security group name - required

After instance is done make sure it has only private ip

EC2 > Instances > i-0f15156577c0280c8

**Instance summary for i-0f15156577c0280c8 (PRIVATE)** [Info](#) [Refresh](#) [Connect](#) [Instance state ▼](#) [Actions ▼](#)

Updated less than a minute ago

Instance ID i-0f15156577c0280c8 (PRIVATE)	Public IPv4 address -	Private IPv4 addresses 172.30.139.241
IPv6 address -	Instance state Running	Public IPv4 DNS -
Hostname type IP name: ip-172-30-139-241.ec2.internal	Private IP DNS name (IPv4 only) ip-172-30-139-241.ec2.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding Opt-in to AWS Compute Optimizer for recommendations. <a href="#">Learn more</a>
Auto-assigned IP address -	VPC ID vpc-0f7a59cc7ce6a7745 (ditiss-lab-vpc)	

Same for public (take instance ,allow only ssh,go to network settings select name of vpc for public ,mention public ip as enable and create .ppk key for public)

**Key pair name**  
Key pairs allow you to connect to your instance securely.

**PUBLICKEY**

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

**Key pair type**

☒ **RSA**  
RSA encrypted private and public key pair

☐ **ED25519**  
ED25519 encrypted private and public key pair

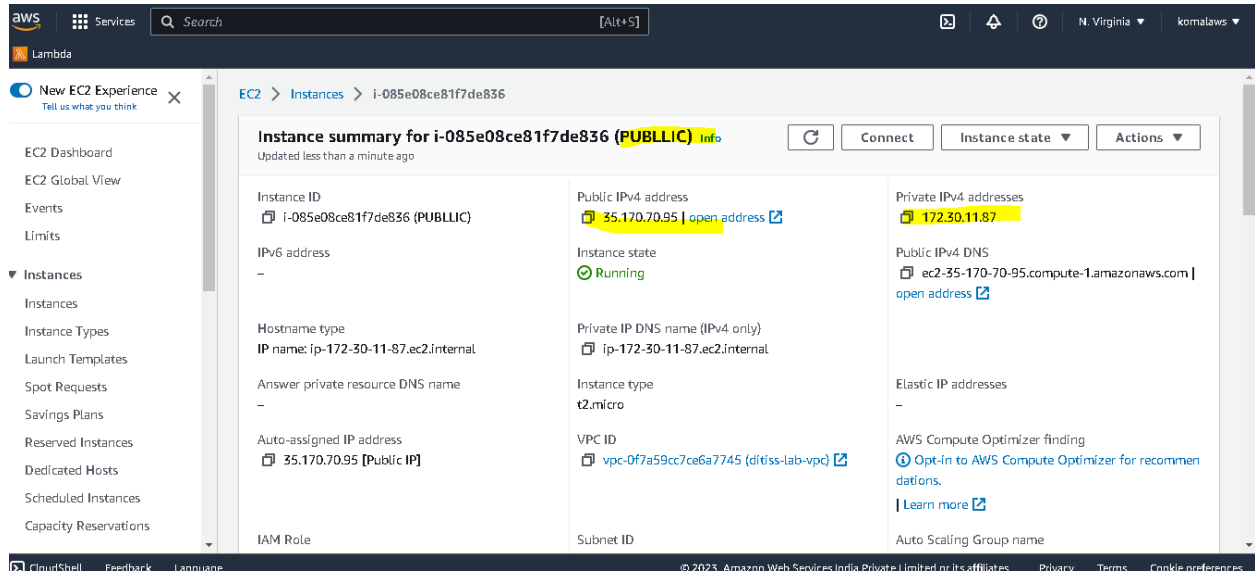
**Private key file format**

☐ **.pem**  
For use with OpenSSH

☒ **.ppk**  
For use with PuTTY

[Cancel](#) [Create key pair](#)

After instance is done make sure it has both public and private ips



After both the instances set then open the public instance machine by .ppk public key and

Make a nano file which contains (private .pem key of private instance )in it

**Nano key**

Give permissions to it as it private key secure it

**Chmod 400 key**

After this login to private mc by public mc

**Ssh -i key admin@(private instance machines ip)**

Now we are in private machine

**Sudo apt-get update**

**Sudo apt-get install apache2**

Edit default file of (index.html) private machine

**Sudo rm /var/www/html/index.html**

**Sudo nano /var/www/html/index.html**

Exit from private machine

Now we are in public machine

Access private mc from public

curl ip of private machine

and we will be able to see the default page of private machine

