Q) 1 . Describe VPC and Subnet. Mention its purpose and its significance in a cloud environment ANS –

Virtual Private Cloud (VPC) networks are global resources. It works similarly like network resources but it gives us control over the network. Each VPC network consists of one or more IP address range called subnets. This means we can provide how many the number of systems can be attached to a particular network. Subnets are regional resources and have IP address ranges associated with them. Subnets work similarly like local IP addresses or we can say that each subnet is associated with a particular system.

In the cloud, it gives us full control over security, resources, and connectivity which is one of the best features in the cloud environment.

Q) 2 . Describe CIDR address ANS –

CIDR (Classless Inter-Domain Routing or supernetting) addresses are made up of two sets of numbers: a prefix, which is the binary representation of the network address, and a suffix, which declares the total number of bits in the entire address ex 192.168.129.23/17 where 17 tells that we have only 17 bits to assign for assign to different systems and 32 - 17 = 15 bits (First 15 bits) in Ipv4 is fixed. The real notation of CIDR is $(2^8.2^8.2^8.2^8.2^8.2^8)$ i.e, Highest ip address in IPV4 can be 255.255.255.255. So we can say that in this example 192.168 is fixed and 129.23 can be vary.

Q) 2 . Create a customized network as depicted below using AWS academy canvas environment ANS –

Step 1 \rightarrow Open VPC \rightarrow Create new vpc \rightarrow select vpc and more \rightarrow Give (the name in Name tag auto-generation) sslabvpc-vpc \rightarrow type 10.0.0.0/16 in the IPV4 CIDR block \rightarrow Keep number of availability zone, number of public subnets and private subnets "1" \rightarrow In the Customized subnets CIDR blocks -- Change Public subnet CIDR block in us-east-1a to 10.0.0.0/24 and Change Private subnet CIDR block in us-east-1a to 10.0.1.0/24 \rightarrow Set NAT gateways(\$) as In 1 AZ \rightarrow Set VPC endpoints as none \rightarrow keep everything as it is \rightarrow Select Create VPC

■ YouTube X ⑤ NewTab X 🖪 Lab Exercis X 🔥 Exercise_5, X	🔥 Exercise_6, 🗙 🧰 Your VPCs 🗴 🔤 Learner Lal 🗴 🔞 VPC Mana	x Lab 2 - Bu x +
← → C 🖷 us-east-1.console.aws.amazon.com/vpc/home?region=us-	nast-1#CreateVpc:createMode=vpcWithResources	e ★ 🖈 🗖 🥙 E
christ Courses INterview 🔇 🛵 Color Name Finder 🖸 Top 50 I	Machine Le 🔛 SmartSimple - Can 📘 copy format - Goog 📋 Pytho	n 🔖 Challenges FindCo 🛄 Launch Meeting - Z »
aWS : Services Q Search	[Alt+S]	voclabs/user1555531=sandeep.sutradhar@mca.christuniversity.in ▼
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet. 0 1	Preview	• 0
Number of private subnets Info The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.	Introducing the new create VPC experience We've designed the new create VPC experience to make it easier to use. Now you can visualize the resources • New: Edit the name tap of influidual resources. Uncheck 'Nuto-generate' and set each name tap in the vi	
0 1 2	New: Edit the name tag or individual resources. Let us know what you think.	. Uncheck "Auto-generate" and set each name tag in the vi
▼ Customize subnets CIDR blocks		
Public subnet CIDR block in us-east-1a		
10.0.0.0/20 4,096 IPs	VPC Show details	Subnets (2) Subnets within this VPC
Private subnet CIDR block in us-east-1a	Your AWS virtual network	Subnets within this VPC
10.0.128.0/20 4,096 IPs	vpc	us-east-1a
		subnet-public1-us-east-1a
NAT gateways (5) Info Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway		subnet-private1-us-east-1a
None In 1 AZ 1 per AZ		•
Francis and a second of the se	2000)
Feedback Looking for language selection? Find it in the new Unified Settings 🖸	6 2022, Amazon Web S	Services, Inc. or its affiliates. Privacy Terms Cookie preferences
MUSICIPG ^		Show all X
₽ Type here to search O Ħ	C N O 0 E 0 M M	€ 26°C ^ // 1805 ENG 28-11-2022 F

Step 2 \rightarrow It will give the following options by default

Route tables

lab-rtb-public

lab-rtb-private1-us-east-1a

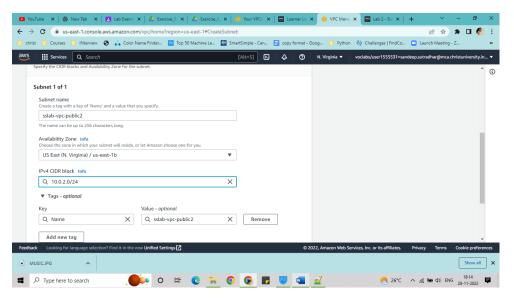
Network connections

lab-igw

lab-nat-public1-us-east-1a

Step 3 \rightarrow In left side of vpc dashboard \rightarrow Click Subnets \rightarrow Click Create subnet \rightarrow Select the VPC ID which we created sslabvpc -vpc \rightarrow Give Subnet name as sslab-subnet-public2 \rightarrow

Select the second Availability zone like us-east-1b \rightarrow in the IPV4 CIDR block give address as $10.0.2.0/24 \rightarrow$ Click create subnet



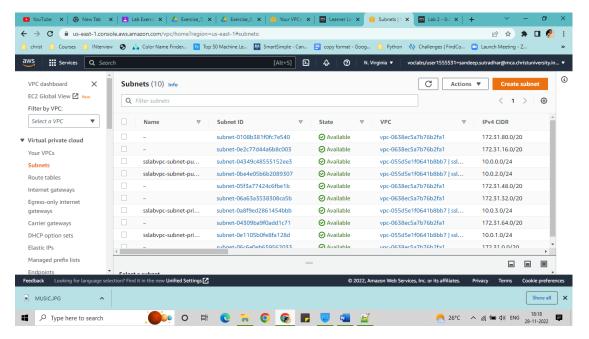
Step 4 \rightarrow Create 2nd private subnet similar to step 3 with

VPC ID: sslab-vpc

Subnet name: sslab-subnet-private2

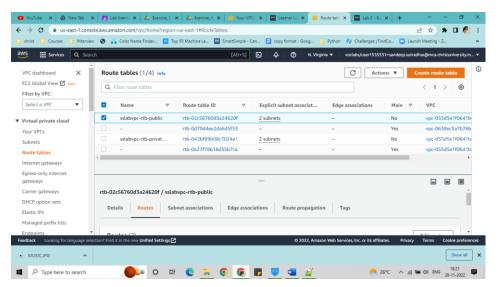
Availability Zone: us-east-1b

IPv4 CIDR block: 10.0.3.0/24 → Create subnet

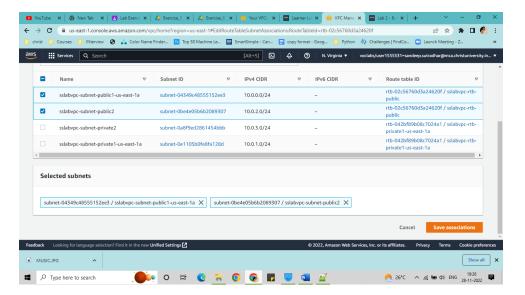


STEP 5 \rightarrow ROUTE TABLES:

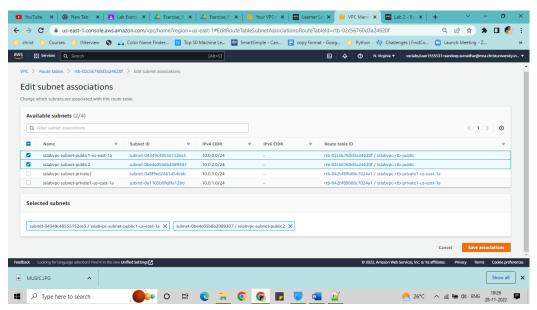
In the left side click Route tables \rightarrow Select the sslab-rtb-private1-us-east-1a route table \rightarrow down menu select Routes \rightarrow this will show the network address which is used to forward any packet to forward to the internet



Choose subnet association → Choose | Edit subnet associations | → select both the private networks → Choose | Save associations

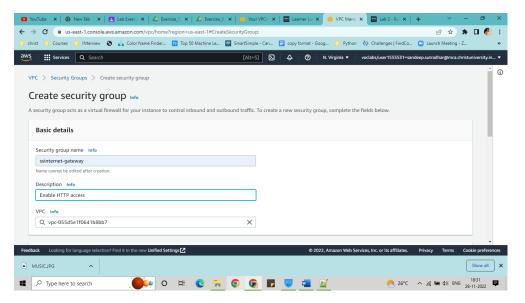


SIMILARLY do it for public subnet association

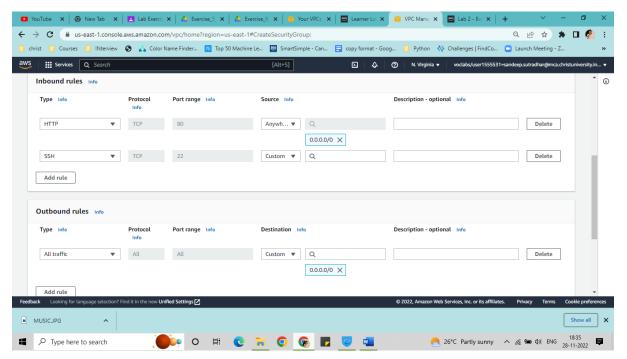


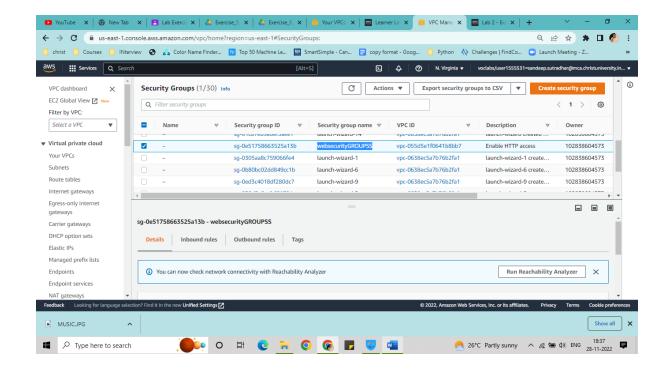
STEP 6 → Create a VPC Security Group:

In the left pane \rightarrow Under security select Security Groups \rightarrow Choose Create security group and then configure \rightarrow Security group name: WEBsecuritygroupss \rightarrow Description: Enable HTTP access \rightarrow in the VPC select the VPC we created and remove the selected one (continue...)



- → In the inbound rule pane choose Add rule → type HTTP and in the Source select Allow from anywhere IPV4 → Description: Permit web requests
- → ADD Rule and select ssh → Source select Allow from anywhere IPV4 → Leave everything as it is → select Create security group

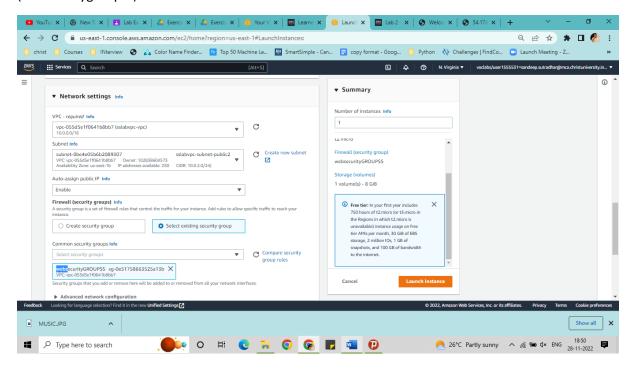




STEP 7 \rightarrow INSTANCE CREATE:

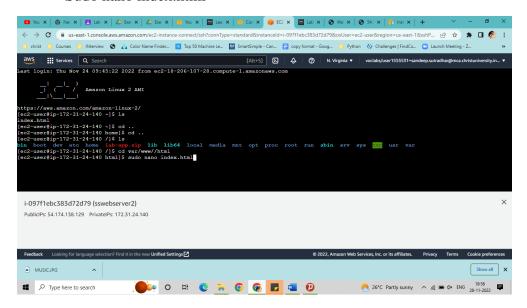
Go to EC2 INSTANCE \rightarrow create instance with name webserverss2 \rightarrow change accordingly \rightarrow In the network setting click on edit \rightarrow in the VPC select the vpc we created above (sslabvpc-vpc) \rightarrow select subnet as public subnet2 \rightarrow Enable the auto assign public IP \rightarrow In the firewall security groups select

Select existing security group → from the dropdown select the above created security group (websecirtygroupss) → Select Launch Instance →



Connect the instance → Write the following code

- Sudo yum update -y
- Sudo amazon-linux-extras install php 8.0 mariadb10.5
- Sudo yum install -y httpd
- Sudo systemctl start httpd
- Sudo systemctl enable httpd
- Cd ..
- Cd ..
- Cd var/www/html
- Sudo nano index.html



<!DOCTYPE html>

<html>

<body>

<h2>Alternative text</h2>

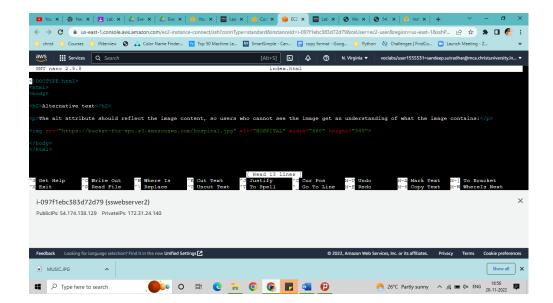
The alt attribute should reflect the image content, so users who cannot see the image get an understanding of what the image contains:

<img src="https://bucket-for-vpc.s3.amazonaws.com/hospital.jpg" alt="HOSPITAL"
width="460" height="345">

</body>

</html>

 $Ctrl + o enter \rightarrow ctrl + x enter$



OUTPUT:



Alternative text

The alt attribute should reflect the image content, so users who cannot see the image get an understanding of what the image contains:



