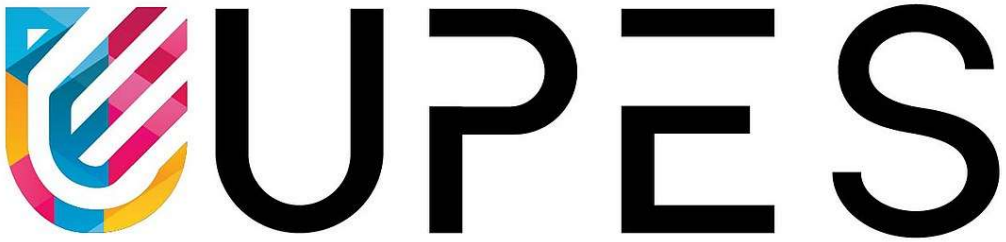


CLOUD SECURITY & MANAGEMENT LAB

Name: Harsh Ranjan

SAP ID: 500097019

Roll no: R2142211262

SUBMISSION TO:

Ms. Avita Katal

Experiment 3: Create a Virtual Private Cloud In AWS

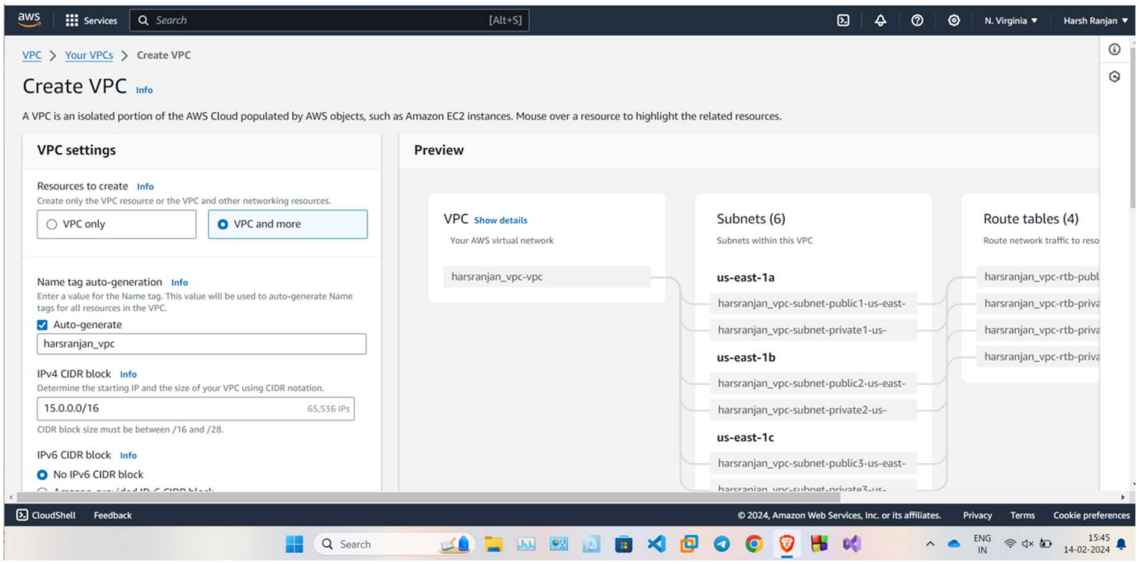
STEP 1: Sign in to the AWS Management Console:

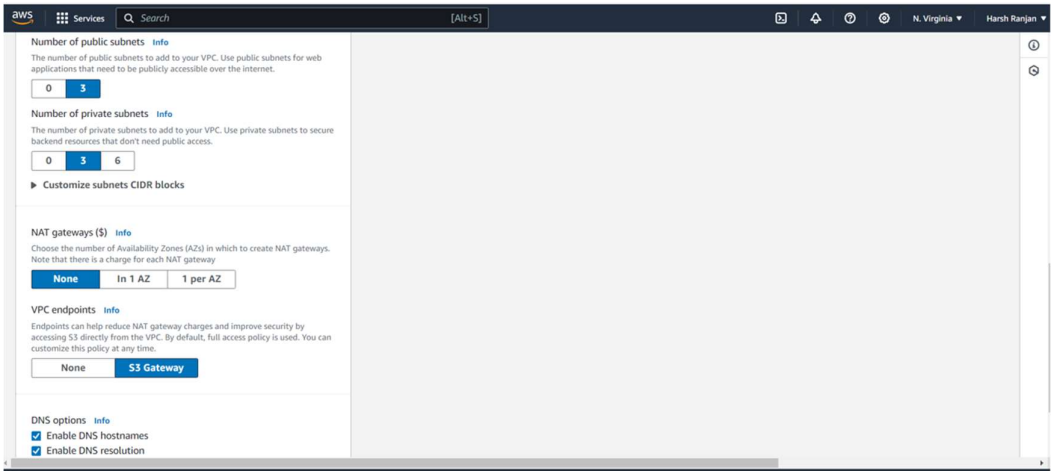
Go to the AWS Management Console and sign in to your AWS account.

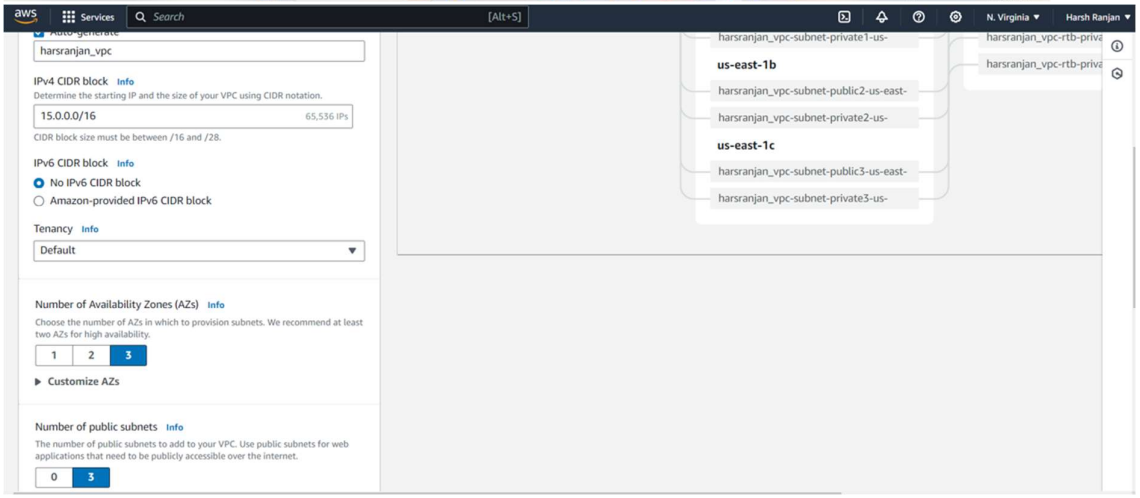
STEP 2: Open the VPC Dashboard: Navigate to the VPC dashboard by selecting "Services" from the top menu and then selecting "VPC" under the "Networking & Content Delivery" section.

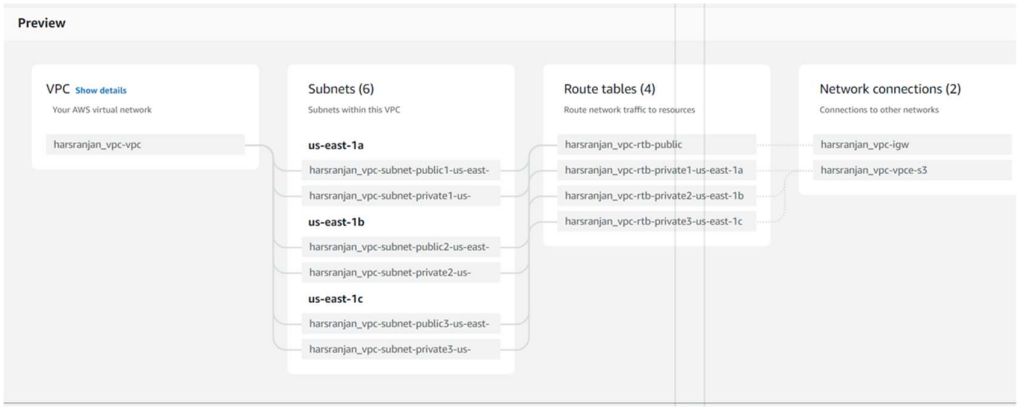
STEP 3: Create a VPC:

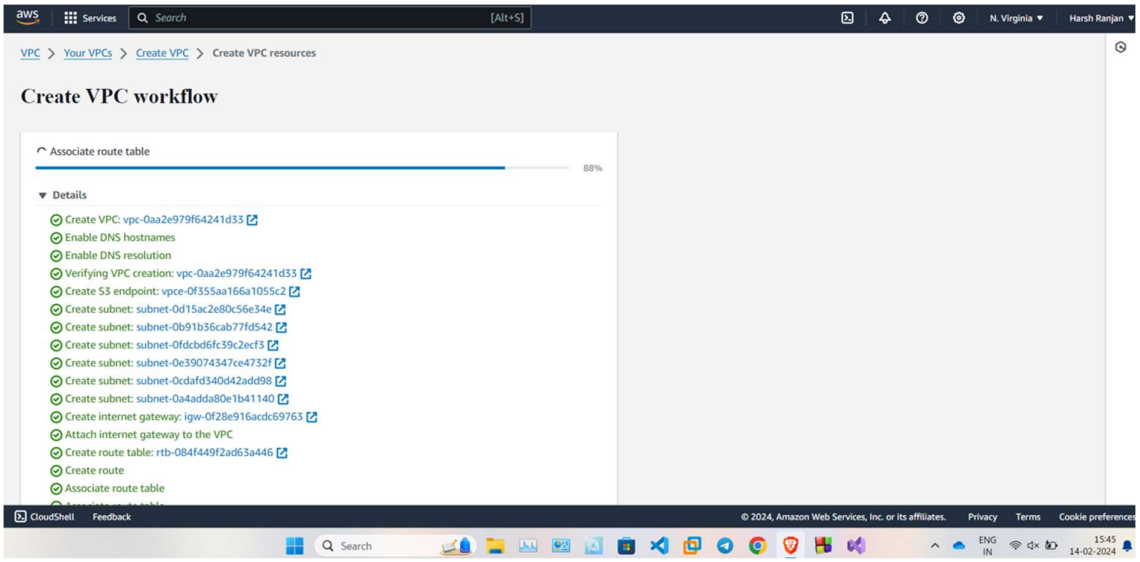
- Click on the "Create VPC" button.




Number of public subnets Info
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
3
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.
0
3
6
Customize subnets CIDR blocks
NAT gateways ($) Info
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway
None
In 1 AZ
1 per AZ
VPC endpoints Info
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.
None
S3 Gateway
DNS options Info
Enable DNS hostnames
Enable DNS resolution
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

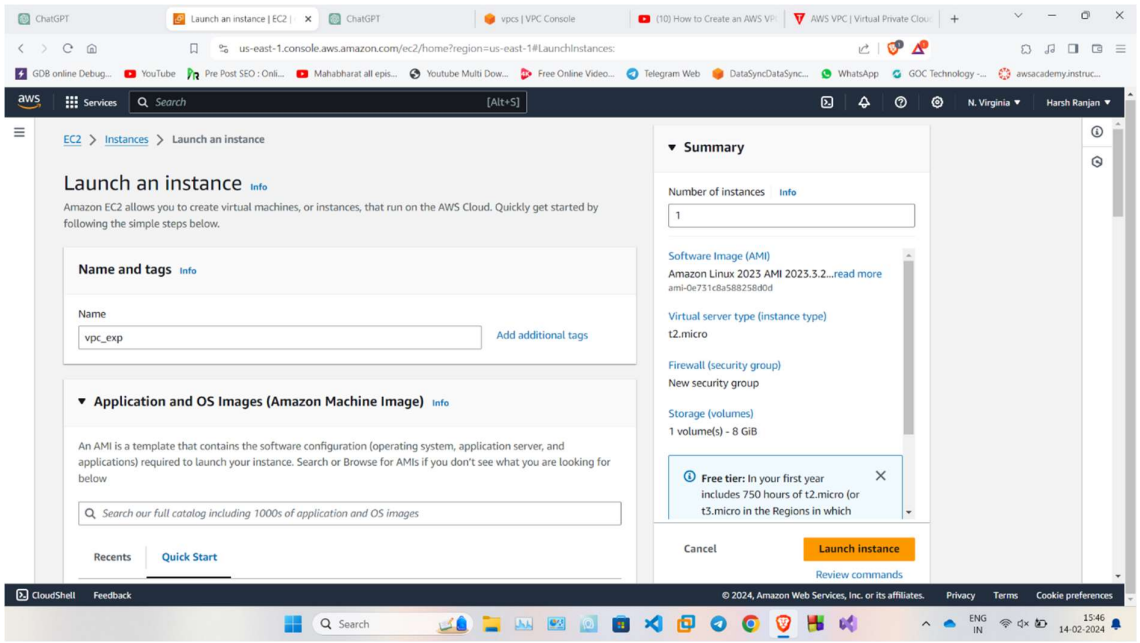

harsranjan_vpc
IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.
15.0.0.0/16
65,536 IPs
CIDR block size must be between /16 and /28.
IPv6 CIDR block Info
No IPv6 CIDR block
Amazon-provided IPv6 CIDR block
Tenancy Info
Default
Number of Availability Zones (AZs) Info
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.
1
2
3
Customize AZs
Number of public subnets Info
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
3
us-east-1b
harsranjan_vpc-subnet-public2-us-east-
harsranjan_vpc-subnet-private2-us-
us-east-1c
harsranjan_vpc-subnet-public3-us-east-
harsranjan_vpc-subnet-private3-us-

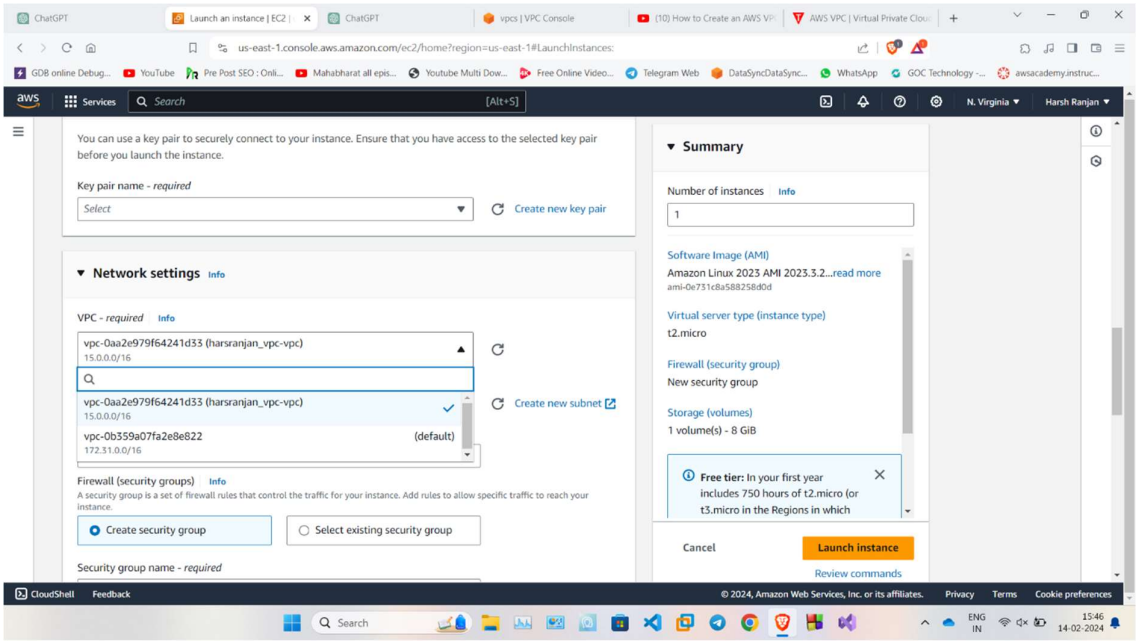

Preview
VPC Show details
Your AWS virtual network
harsranjan_vpc-vpc
Subnets (6)
Subnets within this VPC
us-east-1a
harsranjan_vpc-subnet-public1-us-east-
harsranjan_vpc-subnet-private1-us-
us-east-1b
harsranjan_vpc-subnet-public2-us-east-
harsranjan_vpc-subnet-private2-us-
us-east-1c
harsranjan_vpc-subnet-public3-us-east-
harsranjan_vpc-subnet-private3-us-
Route tables (4)
Route network traffic to resources
harsranjan_vpc-rtb-public
harsranjan_vpc-rtb-private1-us-east-1a
harsranjan_vpc-rtb-private2-us-east-1b
harsranjan_vpc-rtb-private3-us-east-1c
Network connections (2)
Connections to other networks
harsranjan_vpc-igw
harsranjan_vpc-vpce-s3

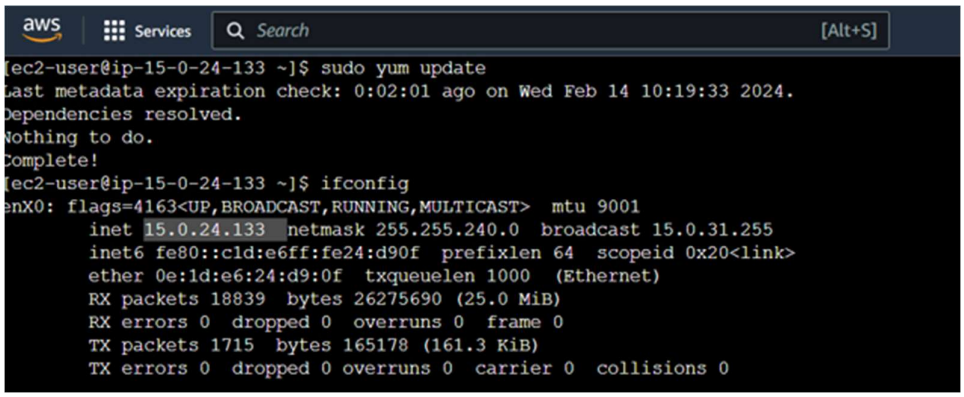


Using the VPC:

1. **Launch Resources**: Now that your VPC is set up, you can launch various AWS resources within it like EC2 instances, RDS instances, etc.
2. **Configure Networking**: When launching resources, you can select the VPC and subnet to deploy them into.







Q1: Why is VPC important in AWS?

ANSWER: A Virtual Private Cloud (VPC) is essential in AWS because it allows you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. This provides several benefits:

- Security: You can control access to your instances and resources using security groups and network access control lists (ACLs).
- Customization: You can customize your network configuration, including selecting your own IP address range, creating subnets, and configuring route tables and network gateways.

- Connectivity: VPC enables you to connect your AWS infrastructure to your corporate data center, other VPCs, and the internet securely.

Q2: What is the primary purpose of creating subnets within a VPC?

ANSWER: Subnets within a VPC allow you to segment your network into smaller, more manageable parts. The primary purposes of creating subnets include:

- Organizing resources: You can group similar resources together within a subnet for easier management and security configuration.
- Implementing network segregation: By placing resources in different subnets, you can control access between them using network ACLs and security groups.
- Supporting high availability: Subnets can be spread across multiple availability zones (AZs) within a region, enabling you to design highly available architectures for your applications.

Q3: Can a VPC span multiple AWS regions?

ANSWER: No, a VPC is confined to a single AWS region. However, you can establish connectivity between VPCs in different regions using inter-region VPC peering, AWS Transit Gateway, or VPN connections.

Q4: How does the concept of availability zone relate to VPC? Can resources in one AZ communicate with resources in another AZ within the same region?
ANSWER : Availability Zones (AZs) are distinct locations within an AWS region that are engineered to be isolated from failures in other AZs. When you create a VPC, you can choose to spread your subnets across multiple AZs within the same region to achieve fault tolerance and high availability. Resources in one AZ can communicate with resources in another AZ within the same region via internal network traffic without leaving the AWS backbone network.

Q5: How can internet connectivity be achieved within a VPC?

ANSWER: Internet connectivity within a VPC can be achieved by:

- Attaching an Internet Gateway (IGW) to the VPC.
- Configuring a public subnet and associating it with a route table that directs traffic destined for the internet to the IGW.

- Assigning public IP addresses or using Elastic IP addresses to instances in the public subnet.
- Ensuring that network ACLs and security groups allow inbound and outbound traffic as required.

Q6: What is the significance of a route table in a VPC?

ANSWER: A route table in a VPC controls the routing of network traffic within the VPC. It specifies the rules for directing traffic between subnets, to the internet via an internet gateway, or to other network destinations. Each subnet in a VPC must be associated with a route table, which determines how traffic is routed in and out of the subnet.

Q7: What is the difference between public, private, and elastic IP addresses?

ANSWER:

- Public IP address: A public IP address is an address that can be accessed over the internet. It is typically assigned to instances that need to communicate directly with the internet, such as web servers.
- Private IP address: A private IP address is used for communication within a private network, such as a VPC. These addresses are not routable over the internet and are typically used for internal communication between instances.
- Elastic IP address (EIP): An Elastic IP address is a static IPv4 address designed for dynamic cloud computing. It is associated with your AWS account rather than a specific instance, allowing you to quickly remap the address to another instance in case of instance failure or migration. EIPs are public IP addresses that can be dynamically allocated and released as needed.