Virtual Private Cloud

Introduction:

Virtual private cloud is logically isolated, customizable, and manageable virtual network.

Because of logical isolation of network resource security as well as network deployment is simplified.

Component of VPC are:

1. IP range in CIDR format
2. Subnets
3. Network ACL
4. Security group
5. Internet gateway (IGW)
6. Virtual private gateway (VGW)
7. Route tables

Components

Subnet

1. Subnet is a subrange of IP addresses in the VPC. We can launch AWS resources into the subnet.

   Public subnet → For resources that must be connected to internet.

   Private subnet → For resources that must remain isolated from internet.

Components

Internet gateway

2. Internet gateway allows communication between the resources in a VPC and the internet.
IGW serves following two purposes:

1. To provide route table that connects to the internet.
2. Perform network address translation.

Components

Route table

3. Route table associated with subnets must be configured before subnets access the IGW.

Route table contains set of rules , called routes, that are used to know where the traffic is directed.

Each subnet in VPC must be associated with route table because table controls routing for the subnet.

Components

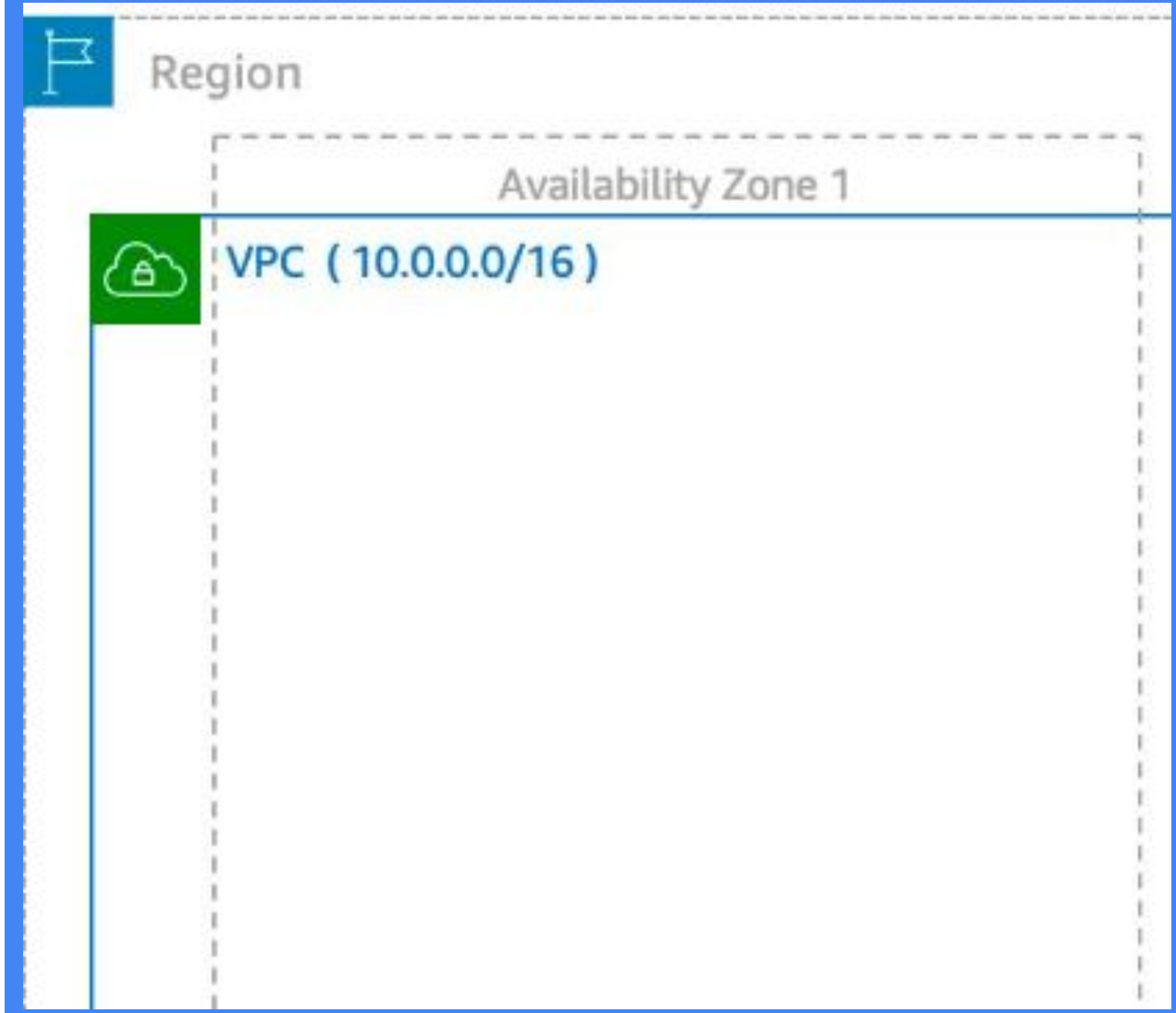
Security group

4. Security group act as a virtual firewall for instances to control inbound & outbound traffic.

If security group is not specified at the launch time then default security group is assigned for the VPC.

Requirements

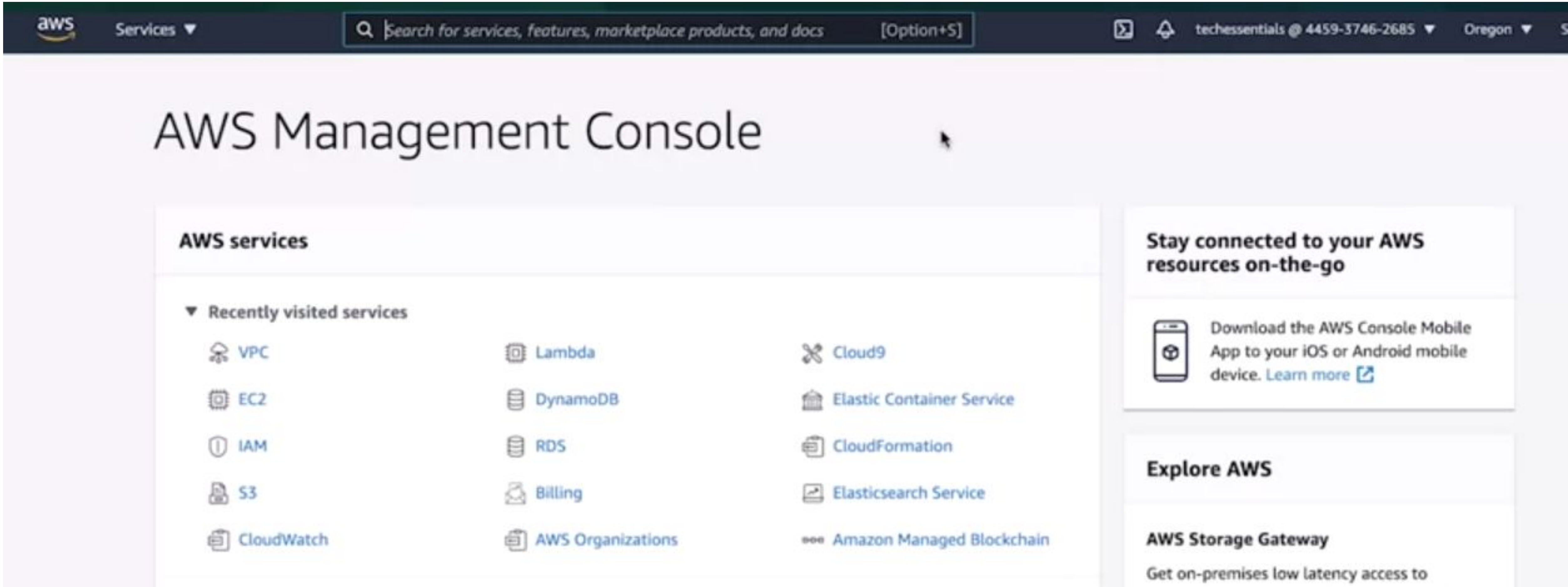
1. Name of the VPC
2. Region for the VPC
3. IP range (CIDR notation)



Steps to create VPC

Step 1:

Open AWS console and check for the correct region



aws
Services ▼
Search for services, features, marketplace products, and docs [Option+S]
techessentials @ 4459-3746-2685 ▼
Oregon ▼

AWS Management Console

AWS services

▼ Recently visited services

VPC	Lambda	Cloud9
EC2	DynamoDB	Elastic Container Service
IAM	RDS	CloudFormation
S3	Billing	Elasticsearch Service
CloudWatch	AWS Organizations	Amazon Managed Blockchain

Stay connected to your AWS resources on-the-go

Download the AWS Console Mobile App to your iOS or Android mobile device. Learn more

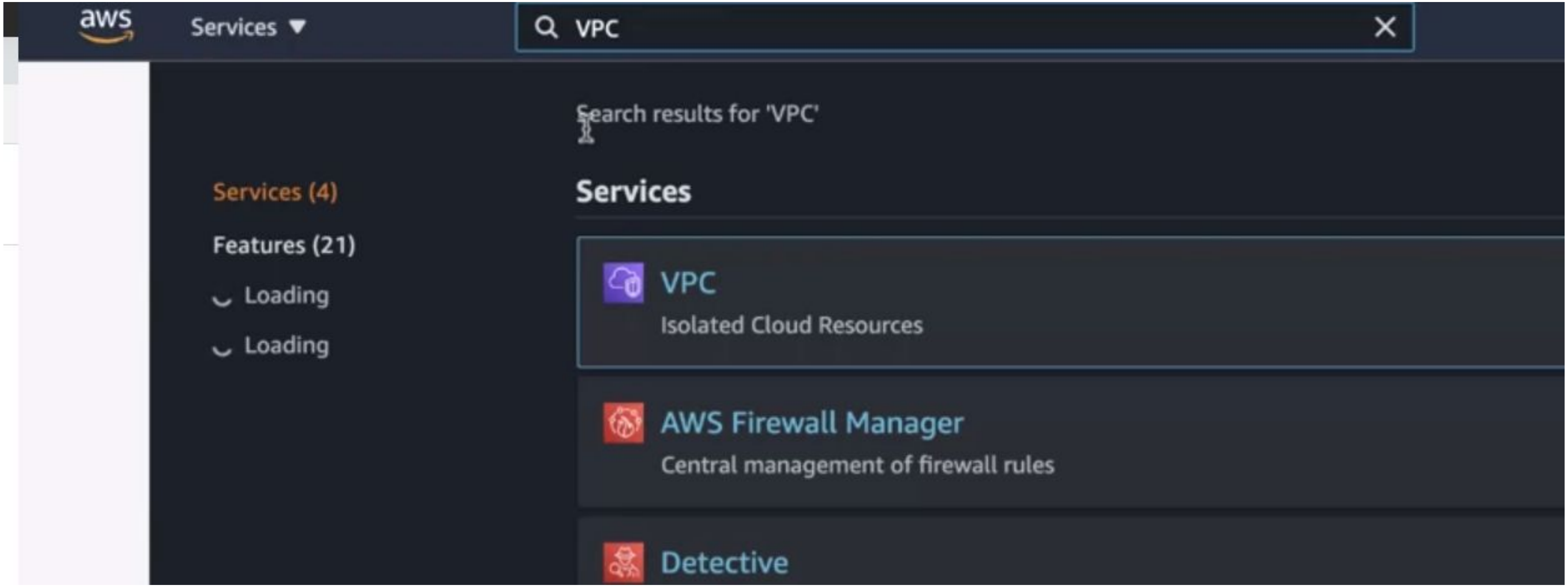
Explore AWS

AWS Storage Gateway

Get on-premises low latency access to

Step 2:

Search for service VPC in the search bar

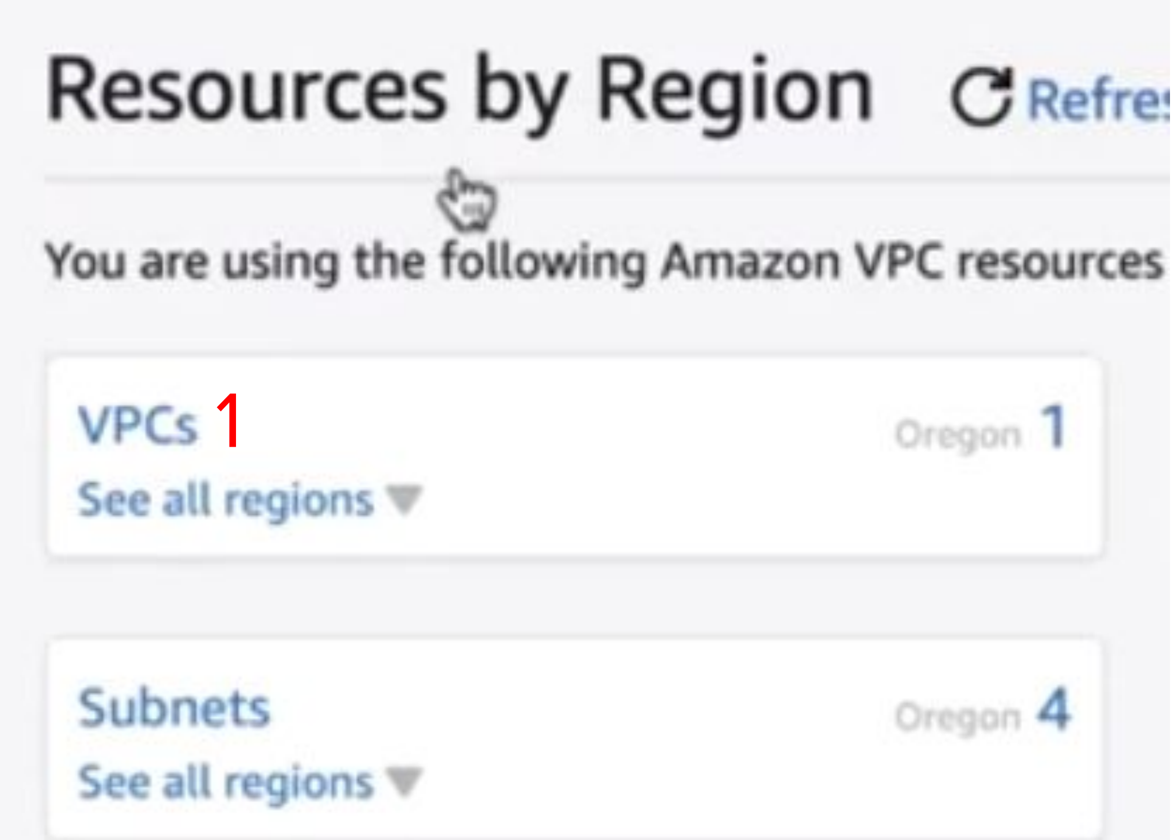


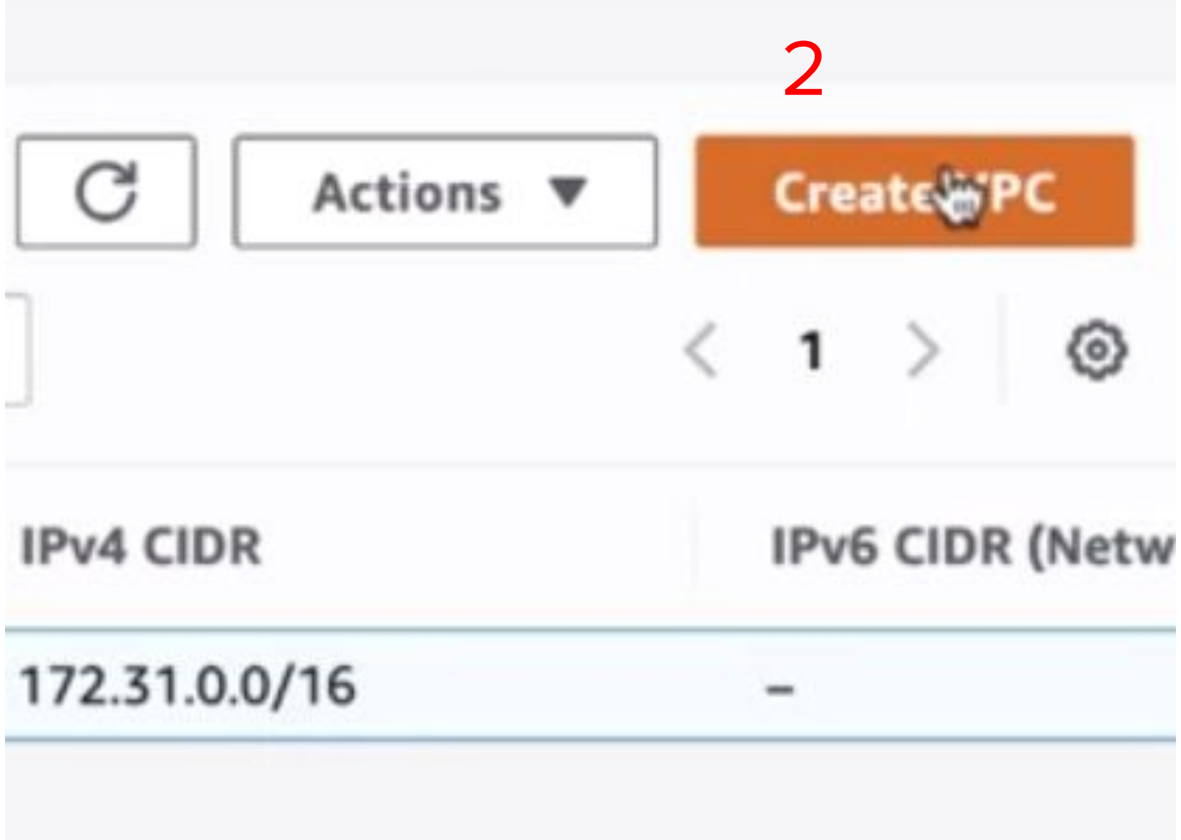
VPC

Search results for 'VPC'

Step 3:

At first click on VPC [1] and then Create VPC [2]

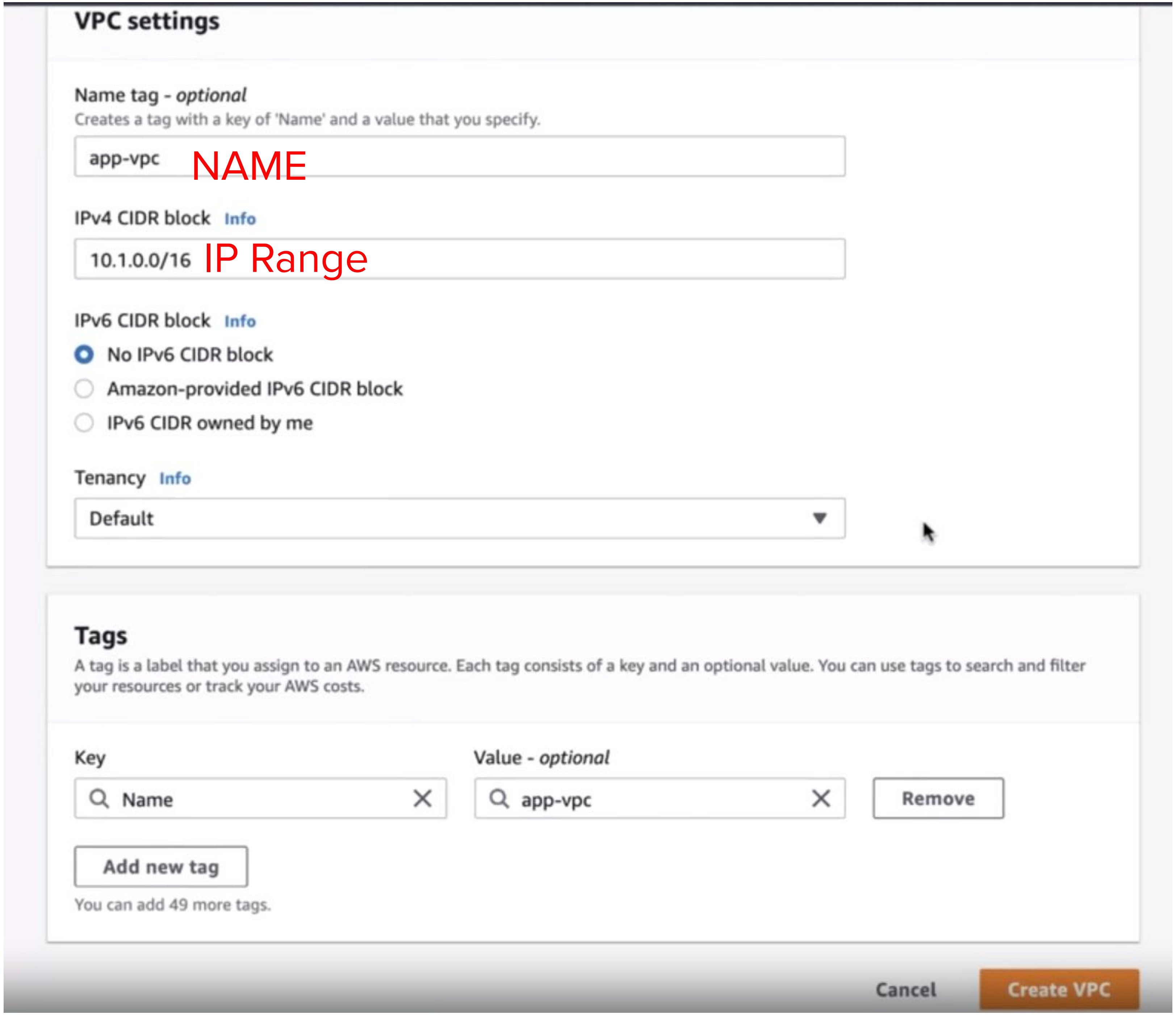




Step 4:

Then in VPC setting we set the name and insert IP range for the VPC.

Then we click create VPC.



VPC settings

Name tag - *optional*

Creates a tag with a key of 'Name' and a value that you specify.

app-vpc NAME

IPv4 CIDR block Info

10.1.0.0/16 IP Range

IPv6 CIDR block Info

● No IPv6 CIDR block

○ Amazon-provided IPv6 CIDR block

○ IPv6 CIDR owned by me

Tenancy Info

Default

Tags

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - *optional*	
Name	app-vpc	Remove

Add new tag

You can add 49 more tags.

Cancel Create VPC

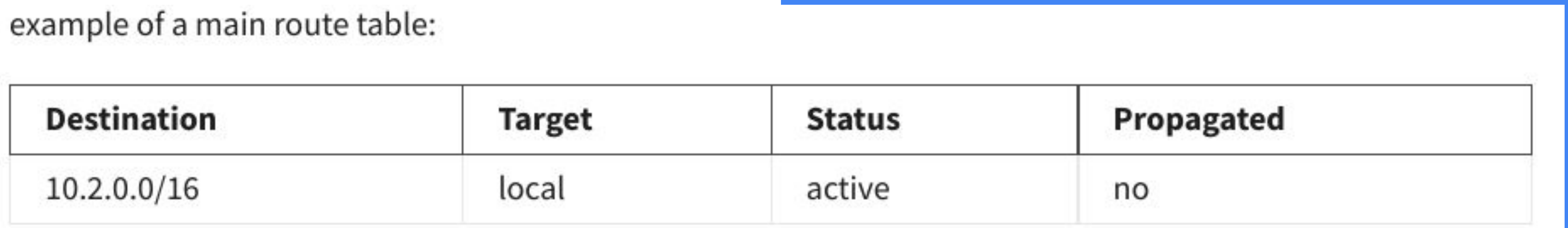
Route tables in VPC

Route table contains set of rules called routes which is used to determine where traffic is directed.

AWS creates route table when VPC is created.

Components of Route table:

1. The destination:
   It specifies the range of IP addresses where we want our traffic to go.
2. The target:
   It is the connection through which we send traffic.



example of a main route table:

Destination	Target	Status	Propagated
10.2.0.0/16	local	active	no

Conditions in Route table

1. Limitation of main route table
2. Introduction to custom route table

1. In case of multiple subnets if we want to direct traffic to specific subnet then it may not be possible.

2. If custom route table is created subnet uses it instead of main route table. In custom route table we can specify routing of traffic as our need.

Planning for VPC creation:

- VPC must be created in the nearest region to our service.
- Determining the number of VPC that we require:

    1. If workload is to be isolated different VPC required, for similar workload same VPC.
    2. If different environment are needed for workload then we must have different VPC.

- We must not have IP address conflicts while connecting the VPCs.

Traffic in a VPC:

- A VPC flow log records information about the traffic going to VPC and from VPC. It a monitors the network traffic, analyze network attacks, and determine whether security group and Access Control List(ACL) requires modification. VPC flow log must be used together with Log tank services(LTS). Log group and log stream must be created first before creating VPC flow log.