

## The image features a word cloud in the shape of the map of India. The words are arranged to fit the geographical outline. The most prominent words, shown in larger fonts, include "ATTACK", "DEFENSE", "LABS", "COURSES", "PENTESTER ACADEMY", "RED TEAM", "ACCESS POINT", "TOOL BOX", "TRAINING", "HACKER", "PATV", "WORLD-CLASS TRAINERS", "PENTESTING", "TEAM LABS", "ACADEMY", "POINT", "DEFENSE L", "ACCESS P", "WORLD-C", "TRAINING", "SPATV ACCESS", "PENTESTER ACADEN", "COURSES PENTESTER ACA", "PENTESTER ACADEMY ATTACK DEFENSE LABS", "TOOL BOX WORLD-CI", "TRAINING CO", "PENTESTER ACADEMY TOOL BOX", and "PENTESTING". The words "ATTACK" and "DEFENSE" are the largest and are colored red and dark blue respectively, while the others are in shades of gray. The background is white.

|             |   |
|-------------|---|
| <b>Name</b> | VPC Enumeration   |
| <b>URL</b>  | <a href="https://attackdefense.com/challengedetails?cid=2425">https://attackdefense.com/challengedetails?cid=2425</a> |
| <b>Type</b> | AWS Cloud Security : EC2  |

**Important Note:** This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

### Solution:

#### Console Based Enumeration

**Step 1:** Click on the lab link button to get access to the AWS lab credentials.

|                   |   |
|-------------------|---|
| Login URL         | <a href="https://276384657722.signin.aws.amazon.com/console">https://276384657722.signin.aws.amazon.com/console</a> |
| Region            | Asia Pacific (Singapore) ap-southeast-1   |
| Username          | student-i47blg8j8zcezmq0  |
| Password          | c8PZVRx3TMjralu61aC   |
| Access Key ID     | AKIAUAWOPGE5KDXBZHOM  |
| Secret Access Key | 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  |

**Step 2:** Sign in to the AWS console.



### Sign in as IAM user

Account ID (12 digits) or account alias

276384657722

IAM user name

student-i47blg8j8zcezmq0

Password

.....

☐ Remember this account

Sign in

[Sign in using root user email](#)

[Forgot password?](#)

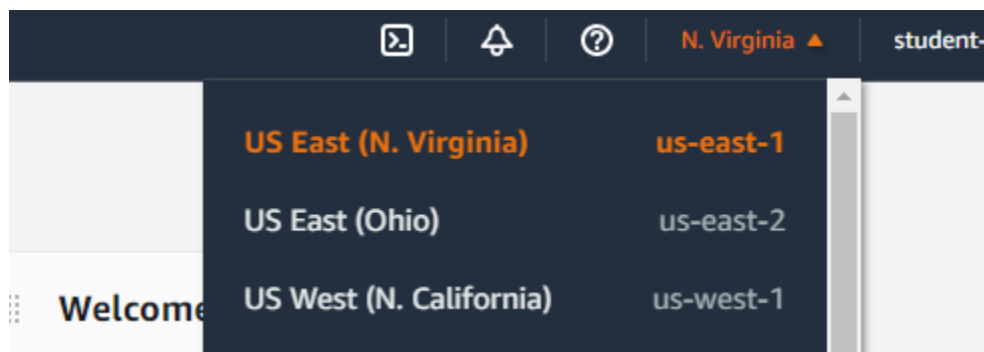
**AWS DeepRacer** offers online, in-person, and hybrid events for getting started with machine learning

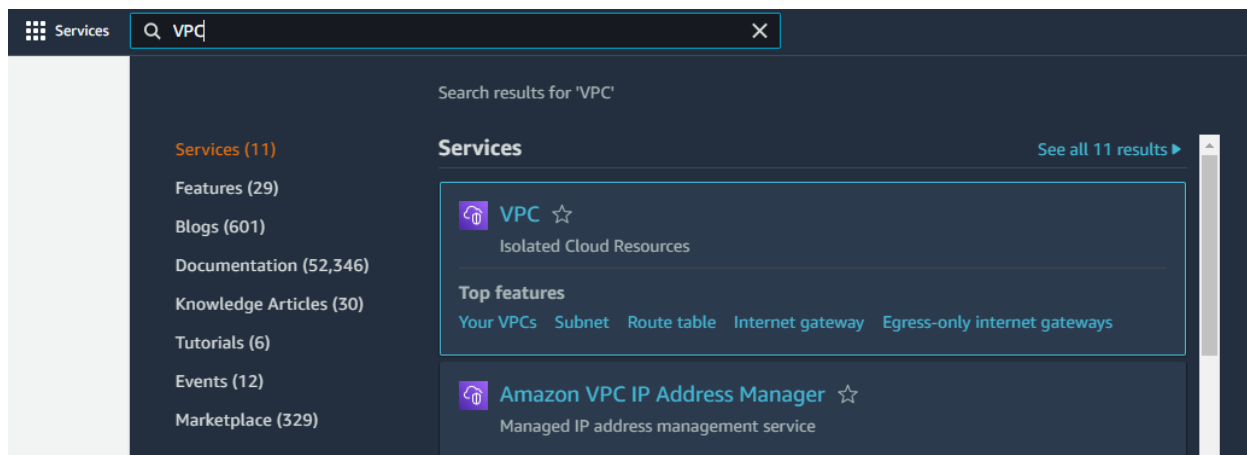


Learn more

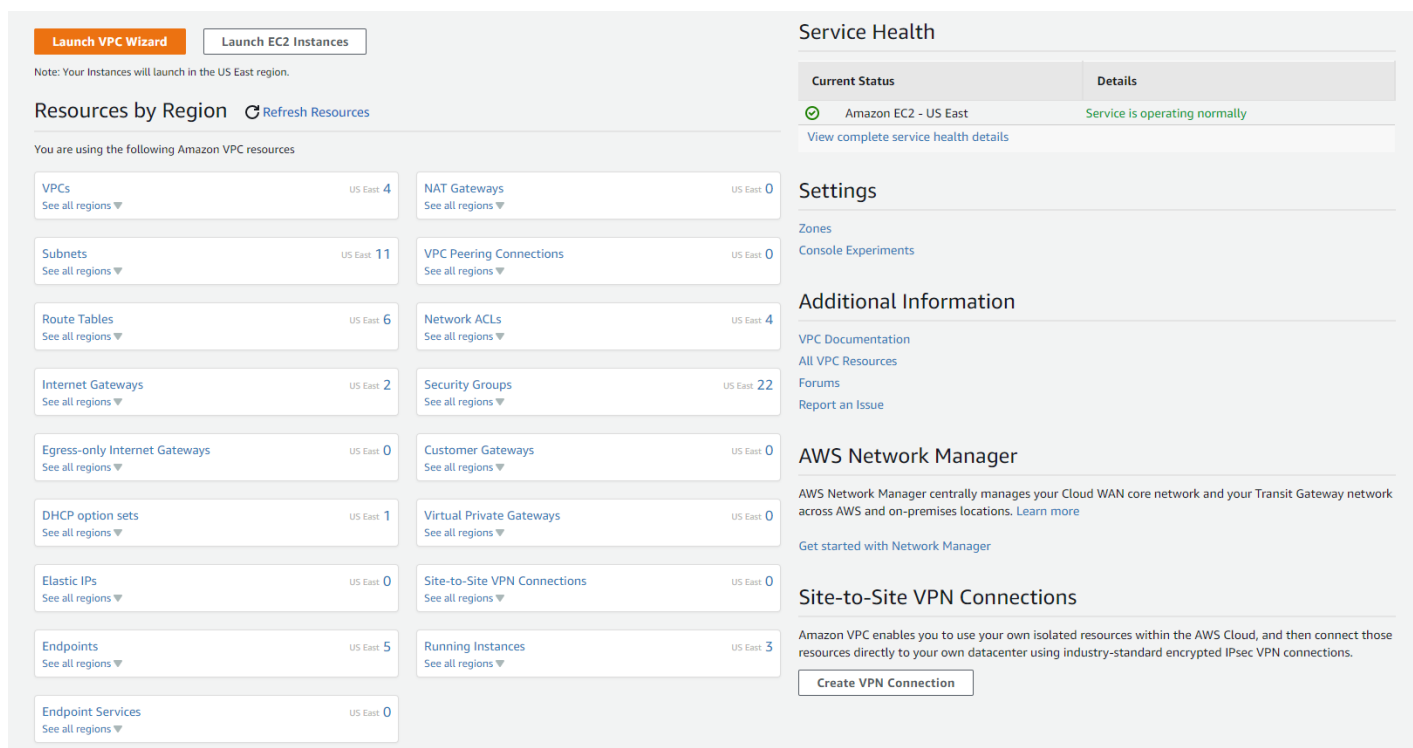
**Step 3:** Search for the VPC Dashboard and navigate to it.

**Note:** Change the region to “us-east-1”, if it is not selected by default.





**Step 4:** Navigate to the VPC from the dashboard by clicking “VPCs” under the resources by region.



**Step 5:** Under VPC is a list of the VPCs deployed in the account. Click on VPC id with the name “my-vpc”.

A virtual private cloud (VPC) is a virtual network dedicated to your AWS account. It is logically isolated from other virtual networks in the AWS Cloud. You can launch your AWS resources, such as Amazon EC2 instances, into your VPC. You can specify an IP address range for the VPC, add subnets, associate security groups, and configure route tables.

**Your VPCs (4)** [Info](#)

[Refresh](#) [Actions](#) [Create VPC](#)

| <input type="checkbox"/> | Name        | VPC ID                | State     | IPv4 CIDR     | IPv6 CIDR | DHCP options set | Main route table      | Ma   |
|--------------------------|-------------|-----------------------|-----------|---------------|-----------|------------------|-----------------------|------|
| <input type="checkbox"/> | private     | vpc-01c4ba0a5725adc37 | Available | 10.0.0.0/24   | –         | dopt-45fa603f    | rtb-06da0ab12f914f835 | acl- |
| <input type="checkbox"/> | vpc-network | vpc-0d414be05cf42ee48 | Available | 10.0.0.0/24   | –         | dopt-45fa603f    | rtb-052c09df0430a1e58 | acl- |
| <input type="checkbox"/> | Default VPC | vpc-cdf801b0          | Available | 172.31.0.0/16 | –         | dopt-45fa603f    | rtb-6446021a          | acl- |
| <input type="checkbox"/> | my-vpc      | vpc-0d6f49a7455240f28 | Available | 10.0.0.0/16   | –         | dopt-45fa603f    | rtb-09ad1b8d0794177b5 | acl- |

The details of the VPC deployed are mentioned here.

VPC > Your VPCs > vpc-0d6f49a7455240f28

### vpc-0d6f49a7455240f28 / my-vpc

**Details** [Info](#)

|   |                                   |   |   |
|---|-----------------------------------|---|---|
| VPC ID<br>vpc-0d6f49a7455240f28                 | State<br>Available                | DNS hostnames<br>Disabled                 | DNS resolution<br>Enabled                 |
| Tenancy<br>Default                              | DHCP options set<br>dopt-45fa603f | Main route table<br>rtb-09ad1b8d0794177b5 | Main network ACL<br>acl-0d853171f2241c203 |
| Default VPC<br>No                               | IPv4 CIDR<br>10.0.0.0/16          | IPv6 pool<br>–                            | IPv6 CIDR (Network border group)<br>–     |
| Route 53 Resolver DNS Firewall rule groups<br>– | Owner ID<br>276384657722          |   |   |

**CIDRs** [Flow logs](#) [Tags](#)

**CIDRs** [Info](#)

| Address type | CIDR        | Network Border Group | Pool | Status     |
|--------------|-------------|----------------------|------|------------|
| IPv4         | 10.0.0.0/16 | –                    | –    | Associated |

**Step 6:** Click on subnets to see the list of available subnets in this account.

Your VPCs  
**Subnets**  
Route Tables  
Internet Gateways

A subnet is a range of IP addresses in your VPC. You can launch AWS resources, such as EC2 instances, into a specific subnet. When you create a subnet, you specify the IPv4 CIDR block for the subnet, which is a subset of the VPC CIDR block. Each subnet must reside entirely within one Availability Zone and cannot span zones. By launching instances in separate Availability Zones, you can protect your applications from the failure of a single zone.

| Subnets (11) <a href="#">Info</a>           |             |                          |             |                                |                |  |
|---|-------------|--------------------------|-------------|--------------------------------|----------------|--|
| <input type="text" value="Filter subnets"/> |             |                          |             |                                |                |  |
| <input type="checkbox"/>                    | Name ▾      | Subnet ID ▾              | State ▾     | VPC ▾                          | IPv4 CIDR ▾    |  |
| <input type="checkbox"/>                    | My-Subnet-1 | subnet-0db023f337e57d0a  | ✓ Available | vpc-0d6f49a7455240f28   my...  | 10.0.1.0/24    |  |
| <input type="checkbox"/>                    | -           | subnet-8ca454bd          | ✓ Available | vpc-cdf801b0   Default VPC     | 172.31.48.0/20 |  |
| <input type="checkbox"/>                    | -           | subnet-bb18b09a          | ✓ Available | vpc-cdf801b0   Default VPC     | 172.31.80.0/20 |  |
| <input type="checkbox"/>                    | private-2   | subnet-0680e03de6c635bf1 | ✓ Available | vpc-01c4ba0a5725adc37   pri... | 10.0.0.128/26  |  |
| <input type="checkbox"/>                    | -           | subnet-e3ea97ae          | ✓ Available | vpc-cdf801b0   Default VPC     | 172.31.16.0/20 |  |
| <input type="checkbox"/>                    | -           | subnet-c3b11ca5          | ✓ Available | vpc-cdf801b0   Default VPC     | 172.31.0.0/20  |  |
| <input type="checkbox"/>                    | -           | subnet-2c59f773          | ✓ Available | vpc-cdf801b0   Default VPC     | 172.31.32.0/20 |  |
| <input type="checkbox"/>                    | private     | subnet-08ca6afa10392c0d9 | ✓ Available | vpc-01c4ba0a5725adc37   pri... | 10.0.0.0/26    |  |
| <input type="checkbox"/>                    | My-Subnet-2 | subnet-0117c0dfb9c3e60d4 | ✓ Available | vpc-0d6f49a7455240f28   my...  | 10.0.2.0/24    |  |
| <input type="checkbox"/>                    | subnet      | subnet-0f8eb1c3c34d6e36b | ✓ Available | vpc-0d414be05cf42ee48   vpc... | 10.0.0.128/25  |  |
| <input type="checkbox"/>                    | -           | subnet-658dea6b          | ✓ Available | vpc-cdf801b0   Default VPC     | 172.31.64.0/20 |  |

**Step 7:** Click on subnet id with the name “My-Subnet-1”.

The details of the subnet deployed are mentioned here.

VPC > Subnets > subnet-0db023f3337e57d0a

## subnet-0db023f3337e57d0a / My-Subnet-1

### Details

|                                       |  |  |   |
|---------------------------------------|--|--|---|
| Subnet ID<br>subnet-0db023f3337e57d0a | Subnet ARN<br>arn:aws:ec2:us-east-1:276384657722:subnet/subnet-0db023f3337e57d0a | State<br>Available   | IPv4 CIDR<br>10.0.1.0/24                      |
| Available IPv4 addresses<br>251       | IPv6 CIDR<br>-   | Availability Zone<br>us-east-1a                                | Availability Zone ID<br>use1-az4              |
| Network border group<br>us-east-1     | VPC<br>vpc-0d6f49a7455240f28   my-vpc  | Route table<br>rtb-0f482764c0f62290f   My-Public-Routing-Table | Network ACL<br>acl-0d853171f2241c203          |
| Default subnet<br>No                  | Auto-assign public IPv4 address<br>Yes   | Auto-assign IPv6 address<br>No                                 | Auto-assign customer-owned IPv4 address<br>No |
| Customer-owned IPv4 pool<br>-         | Outpost ID<br>-  | IPv4 CIDR reservations<br>-                                    | IPv6 CIDR reservations<br>-                   |
| IPv6-only<br>No                       | Hostname type<br>IP name   | Resource name DNS A record<br>Disabled                         | Resource name DNS AAAA record<br>Disabled     |
| DNS64<br>Disabled                     | Owner<br>276384657722  |  |   |

**Step 8:** Click on Network ACL and check the network access control list.

It is an optional layer of security for your VPC that acts as a firewall for controlling traffic in and out of one or more subnets. You might set up network ACLs with rules similar to your security groups in order to add an additional layer of security to your VPC.

Flow logs | Route table | **Network ACL** | CIDR reservations | Sharing | Tags

Network ACL: **acl-0d853171f2241c203** [Edit network ACL association](#)

#### Inbound rules (2)

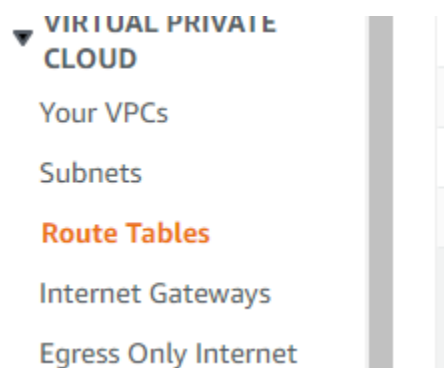
| Rule number | Type        | Protocol | Port range | Source    | Allow/Deny |
|-------------|-------------|----------|------------|-----------|------------|
| 100         | All traffic | All      | All        | 0.0.0.0/0 | Allow      |
| *           | All traffic | All      | All        | 0.0.0.0/0 | Deny       |

#### Outbound rules (2)

| Rule number | Type        | Protocol | Port range | Destination | Allow/Deny |
|-------------|-------------|----------|------------|-------------|------------|
| 100         | All traffic | All      | All        | 0.0.0.0/0   | Allow      |
| *           | All traffic | All      | All        | 0.0.0.0/0   | Deny       |



**Step 9:** Click on Route Tables to see the list of route tables available in the account.



A route table contains a set of rules, called routes, that determine where network traffic from your subnet or gateway is directed. Each subnet in your VPC must be associated with a route table, which controls the routing for the subnet (subnet route table). You can explicitly associate a subnet with a particular route table. Otherwise, the subnet is implicitly associated with the main route table. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same subnet route table.

| Route tables (6) <a href="#">Info</a>            |                       |                                       |  |                   |      |  |              |  |
|--|-----------------------|---------------------------------------|--|-------------------|------|--|--------------|--|
| <input type="text" value="Filter route tables"/> |                       |                                       |  |                   |      |  |              |  |
| <input type="checkbox"/>                         | Name                  | Route table ID                        | Explicit subnet associat...              | Edge associations | Main | VPC  | Owner ID     |  |
| <input type="checkbox"/>                         | -                     | <a href="#">rtb-06da0ab12f914f835</a> | -  | -                 | Yes  | <a href="#">vpc-01c4ba0a5725adc37</a>   pri... | 276384657722 |  |
| <input type="checkbox"/>                         | -                     | <a href="#">rtb-052c09df0430a1e58</a> | -  | -                 | Yes  | <a href="#">vpc-0d414be05cf42ee48</a>   vpc... | 276384657722 |  |
| <input type="checkbox"/>                         | -                     | <a href="#">rtb-09ad1b8d0794177b5</a> | -  | -                 | Yes  | <a href="#">vpc-0d6f49a7455240f28</a>   my...  | 276384657722 |  |
| <input type="checkbox"/>                         | Route Table           | <a href="#">rtb-0775b85bd5376d24d</a> | <a href="#">subnet-0f8eb1c3c34d6e...</a> | -                 | No   | <a href="#">vpc-0d414be05cf42ee48</a>   vpc... | 276384657722 |  |
| <input type="checkbox"/>                         | My-Public-Routing-... | <a href="#">rtb-0f482764c0f62290f</a> | <a href="#">2 subnets</a>                | -                 | No   | <a href="#">vpc-0d6f49a7455240f28</a>   my...  | 276384657722 |  |
| <input type="checkbox"/>                         | -                     | <a href="#">rtb-6446021a</a>          | -  | -                 | Yes  | <a href="#">vpc-cdf801b0</a>   Default VPC     | 276384657722 |  |


**Step 10:** Click on route table id with the name “My-Public-Routing-Table”.

Two routes are in this route table where one route has a target of local and the other one is associated with an internet gateway.



VPC > Route tables > rtb-0f482764c0f62290f

## rtb-0f482764c0f62290f / My-Public-Routing-Table

 You can now check network connectivity with Reachability Analyzer

### Details [Info](#)

|   |  |  |                        |
|---|--|--|------------------------|
| Route table ID<br> rtb-0f482764c0f62290f | Main<br> No               | Explicit subnet associations<br><u>2 subnets</u> | Edge associations<br>– |
| VPC<br><a href="#">vpc-0d6f49a7455240f28</a>   my-vpc   | Owner ID<br> 276384657722 |  |                        |

**Routes** | Subnet associations | Edge associations | Route propagation | Tags

### Routes (2)

 Filter routes

Both ▼


| Destination ▼ | Target ▼                             | Status ▼ | Propagated |
|---------------|--------------------------------------|----------|------------|
| 10.0.0.0/16   | local                                | ✓ Active | No         |
| 0.0.0.0/0     | <a href="#">igw-07afdebebf65c829</a> | ✓ Active | No         |

**Step 11:** Click on Subnet associations to get the explicit subnet associations.

Here we have two subnet associations in this route table.

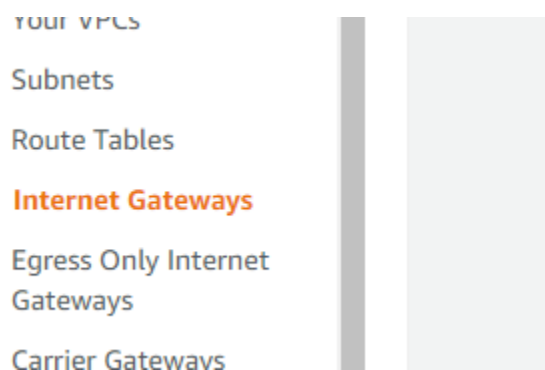
Routes | **Subnet associations** | Edge associations | Route propagation | Tags

### Explicit subnet associations (2)

 Find subnet association

| Subnet ID ▼  | IPv4 CIDR ▼ | IPv6 CIDR |
|--|-------------|-----------|
| <a href="#">subnet-0db023f3337e57d0a</a> / My-Subnet-1 | 10.0.1.0/24 | –         |
| <a href="#">subnet-0117c0dfb9c3e60d4</a> / My-Subnet-2 | 10.0.2.0/24 | –         |

**Step 12:** Click on Internet Gateways from the side panel.



An internet gateway enables resources (like EC2 instances) in your public subnets to connect to the internet if the resource has a public IPv4 address or an IPv6 address. Similarly, resources on the internet can initiate a connection to resources in your subnet using the public IPv4 address or IPv6 address.

It will list the available internet gateways in the account here.

| Internet gateways (2) <a href="#">Info</a>            |        |                                      |                       |  |              |  | <a href="#">Refresh</a> |
|---|--------|--------------------------------------|-----------------------|--|--------------|--|-------------------------|
| <input type="text" value="Filter internet gateways"/> |        |                                      |                       |  |              |  |                         |
| <input type="checkbox"/>                              | Name ▾ | Internet gateway ID ▾                | State ▾               | VPC ID ▾                                       | Owner        |  |                         |
| <input type="checkbox"/>                              | My-IGW | <a href="#">igw-07afdebebf65c829</a> | <span>Attached</span> | <a href="#">vpc-0d6f49a7455240f28   my-vpc</a> | 276384657722 |  |                         |
| <input type="checkbox"/>                              | -      | <a href="#">igw-8d4569f6</a>         | <span>Attached</span> | <a href="#">vpc-cdf801b0   Default VPC</a>     | 276384657722 |  |                         |

**Step 13:** Click on the internet gateway id with the name “My-IGW”.

The details associated with this internet gateway will be available here.

VPC > Internet gateways > igw-07afdebebf65c829

## igw-07afdebebf65c829 / My-IGW

### Details [Info](#)

|   |                   |  |                       |
|---|-------------------|--|-----------------------|
| Internet gateway ID<br>igw-07afdebebf65c829 | State<br>Attached | VPC ID<br>vpc-0d6f49a7455240f28   my-vpc | Owner<br>276384657722 |
|---|-------------------|--|-----------------------|

### Tags

| Key  | Value  |
|------|--------|
| Name | My-IGW |

### References:

1. AWS VPC documentation (<https://docs.aws.amazon.com/vpc/latest/userguide>)