

## CLOUD CONCEPTS

### (Virtual Private Cloud- VPC)

- VPC is virtual private cloud. Amazon provides a default VPC in every region. **Never delete default VPC** because VPC decides which type of traffic is allowed and blocked.

Think of a VPC as a virtual data centre in the cloud.

Every region in AWS has its own default VPC



- It provisions you isolate the section of AWS logically where you can launch AWS resources in a virtual network that you define.
  - ✓ Complete control over your virtual networking environment
  - ✓ Selection of your IP address range
  - ✓ Creation of subnets
  - ✓ Configuration of route table and networking gateways

Additionally, you can create a hardware Virtual Network (VPN) connection between your corporate datacentre and your VPC and leverage the AWS cloud as an extension of your corporate datacentre.

#### **Benefits:**

- **Easy to use**

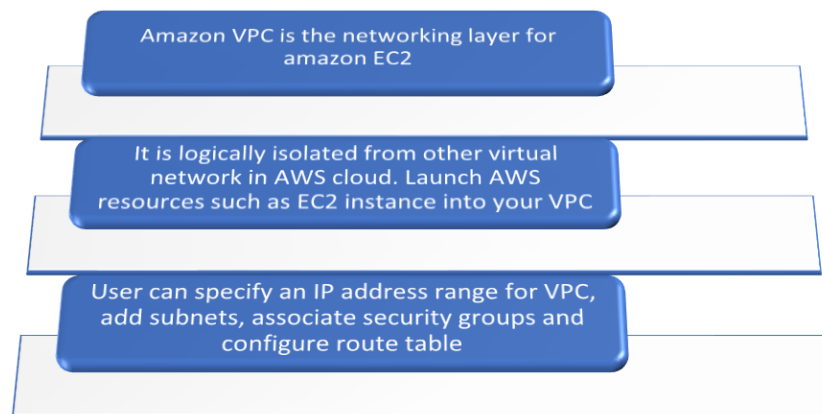
Ease of creating a VPC in very simple steps by selection network set-ups as per requirement. Define subnets, IP range, route tables, and security groups will be automatically created.

- **Pricing for Amazon VPC**

There's no additional storage care for using Amazon VPC. Pay the standard rates for the instance and other Amazon EC2 features that you use.

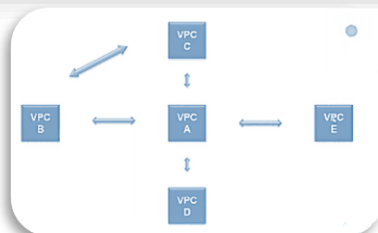
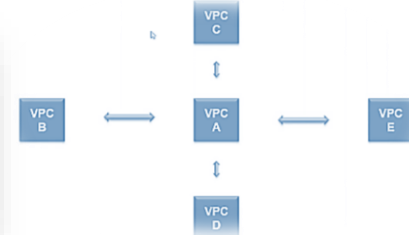
## Features:

- Create an Amazon VPC on AWS scalable infrastructure and specify its private IP address range from any range you choose.
- Expand VPC by adding secondary IP ranges.
- Divide VPC private IP address range into one or more public or private subnets to facilitate running applications and services in VPC.
- Control inbound and outbound access to and from individual subnets using network access control lists.
- Store data in Amazon S3 and set permissions such that the data can only be accessed from within Amazon VPC.
- Attach one or more Amazon Elastic IP address to any instance in VPC so it can be reached directly from the internet.
- Connect VPC with other VPCs and access resources in the other VPCs via private IP address using VPC peering.
- Enable EC2 instance in the EC2-classic platform to communicate with instance in a VPC using private IP address.
- Privately connect to other AWS services without using an internet gateway, NAT or firewall proxy through a VPC endpoint.
- Bridge VPC and onsite IT Infrastructure with an encrypted VPN connection.
- Privately connect to customized services or SaaS solution powered by AWS private link.
- User can use VPC flow logs to log information about network traffic going in and out of network interfaces in VPC.



- Say you have your database in your VPC, and you want to access it through the internet. For this an Internet Gateway is required (public internet access). NAT is used for private communication.
- Private address is mandatory.
- Communication of one VPC with other VPC through private IP address is **VPC Peering**. If one VPC is in one account and other VPC is in another account even then the communication is possible.

- Allow you to connect one VPC with another via a direct network route using private IP address.
- Instance behave as if they were on the same private network
- You can peer VPC's with other AWS accounts as well as with other VPCs in the same account.
- Peering is in a star configuration: i.e., 1 central VPC peer with 4 others. Not Transitive Peering!!!



- VPC Transitive Peering (Combine image no need for graphics just add arrow between VPC B and VPC C in second slide)

### Default VPC vs Custom VPC

- Default VPC is user friendly, allowing you to immediately deploy instance.
- All subnet in default VPC have a route out the internet.
- Each EC2 instance has both a public and private IP address.

### Key Concept | VPC and Subnet Sizing:

#### • VPC and Subnet Sizing for IPv4

While creating a VPC, must specify an IPv4 CIDR block for the VPC. The allowed block size is between a /16 netmask (65,536 IP address) and /28 netmask (16 IP address).

#### • Adding IPv4 CIDR Block to a VPC

Associate secondary IPv4 CIDR block with VPC. When CIDR block associate with VPC, a route is automatically added to VPC route tables to enable routing within the VPC.

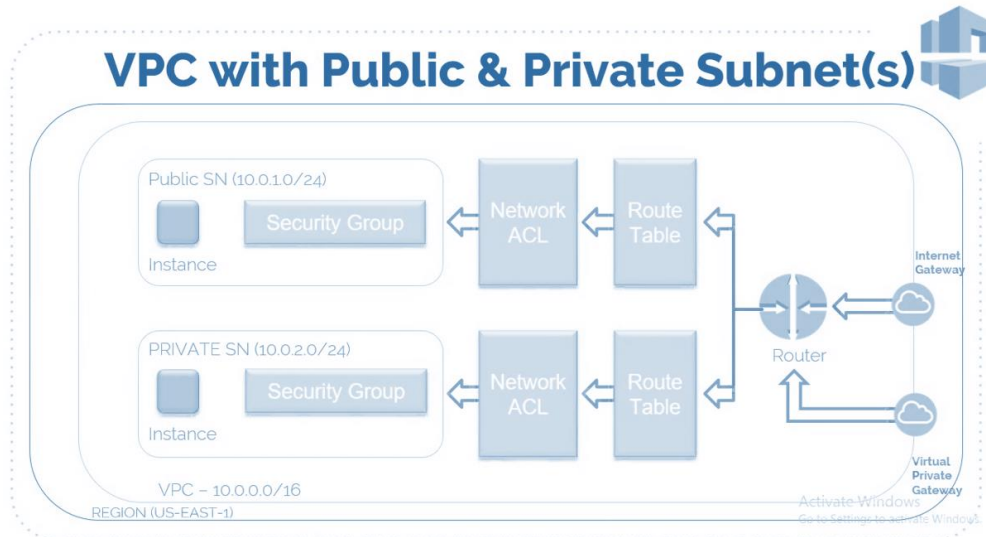
### IMPORTANT POINTS:

- Preferred by the enterprise.
- Scale automatically up to 10Gbps.
- No need to patch
- Not associated with security groups
- Automatically assigned a public in IP address
- Remember to update your route tables.
- No need to disable source/destination checks
- More secure than a NAT instance

### VPC Restrictions:

- 5 Elastic IP Address
- 5 Internet Gateway
- 5 VPCs per Region (Can be increased on request)
- 50 VPN connection per region
- 50 Customer Gateway per region
- 200 route tables per region
- 100 Security Group per VPC
- 50 Rules per Security group

- Think of a VPC as a logical datacenter in AWS.
- Consists of IGWs (or Virtual Private Gateway), Route tables, network access control lists, subnets, and security groups
- 1 subnet = 1 Availability Zone
- Security groups are stateful; Network access control lists are stateless.
- No transitive peering



- **Public subnet** = website for public access (traffic to/from internet in associated SG)
- **Private subnet** = data base for private access (traffic to/from internet is blocked in associated SG)
- Both subnets are in Availability Zone in a region. (One AZ = One Subnet)

#### STEPS:

1. Select a region selected and launch the VPC using specific IP range.
2. Define two gateways.
  - a. Internet gate way for public access
  - b. Virtual private gate way for private communication (*for DB*)
3. Setting up route tables. Any request received in sent to the route table. Route table will manage and decide the request to be forwarded to public or private subnet.

10.0.0.0 – 10.255.255.255 (10/8 prefix)  
 172.16.0.0 – 172.31.255.255 (172.16/12 prefix)  
 192.168.0.0 – 192.168.255.255 (192.168/16 prefix)

While creating the VPC AWS recommended specify CIDR block (of/16 or smaller) from the private IPv4 address ranges.

#### LAB (Custom VPC)

- Launch instance into a subnet of your choosing
- Assign custom IP address ranges in each subnet
- Configure route tables between subnets
- Create internet gateway and attach it to our VPC
- Much better security control over your AWS resources
- Instance Security groups
- Subnet network access control lists (ACLs)



1. First select any specific region. (Say Ohio or North Virginia)

*The number of AZ varies in different regions. No of AZs = No of subnets (more can be created)*

2. Search VPC. (Explore the options)

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with categories like 'VIRTUAL PRIVATE CLOUD' and 'SECURITY'. The main content area displays the 'Launch VPC Wizard' and 'Launch EC2 Instances' buttons. Below these, a note states: 'Note: Your Instances will launch in the US East (N. Virginia) region.' The 'Resources by Region' section shows a grid of VPC resources for the N. Virginia region, including VPCs (1), Subnets (6), Route Tables (1), Internet Gateways (1), Egress-only Internet Gateways (0), NAT Gateways (0), VPC Peering Connections (0), Network ACLs (1), Security Groups (3), and Customer Gateways (0). Each resource has a 'See all regions' link.

3. **[SKIP THIS STEP TO STEP 4]** Click on Launch VPC Configurations. You will see different options. You can select any of the options depending upon the requirement. (Say optn1: anything in public subnet is accessible or optn2: say Database is in private subnet and your website is in public subnet)

Step 1: Select a VPC Configuration

This screenshot shows the 'Select a VPC Configuration' step of the AWS VPC Wizard. On the left, there are four configuration options: 'VPC with a Single Public Subnet' (selected), 'VPC with Public and Private Subnets', 'VPC with Public and Private Subnets and Hardware VPN Access', and 'VPC with a Private Subnet Only and Hardware VPN Access'. The main area provides details for the selected configuration: 'Your instances run in a private, isolated section of the AWS cloud with direct access to the Internet. Network access control lists and security groups can be used to provide strict control over inbound and outbound network traffic to your instances.' It also states 'Creates: A /16 network with a /24 subnet. Public subnet instances use Elastic IPs or Public IPs to access the Internet.' An 'Important' note mentions Local Zones. A diagram on the right shows a 'Public Subnet' connected to 'Internet, S3, DynamoDB, SNS, SQS, etc.'. A 'Select' button is at the bottom right.

4. Click on “YOUR VPC” and check your running VPC --- Default VPC will be running which is connected to main route table. Never delete it.



Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR (Network Border Group)	DHCP options set
	vpc-efa62b92	available	172.31.0....	-	-	dopt-30a6884a

5. Click on Create VPC and set the name of the VPC and define the IPv4 address from the given ranges. Leave the other options default and create the VPC.
  - a. Default tenancy means shared hard drive is being used for VPC and dedicated tenancy means VPC will launch on underlying hypervisor.
  - b. Used IP address range can be 10.0.0.0/16
    - When you create a VPC, you must specify an IPv4 CIDR block for the VPC. The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses)
    - The IP addresses for your subnets are represented using Classless Inter-Domain Routing (CIDR) notation.
    - The CIDR block of a subnet can be the same as the CIDR block for the VPC (to create a single subnet in the VPC), or a subset of the CIDR block for the VPC (to create multiple subnets in the VPC). The allowed block size is between a /28 netmask and /16 netmask. If you create more than one subnet in a VPC, the CIDR blocks of the subnets cannot overlap. For example, if you create a VPC with CIDR block 10.0.0.0/24, it supports 256 IP addresses. You can break this CIDR block into two subnets, each supporting 128 IP addresses. One subnet uses CIDR block 10.0.0.0/25 (for addresses 10.0.0.0 - 10.0.0.127) and the other uses CIDR block 10.0.0.128/25 (for addresses 10.0.0.128 - 10.0.0.255).
  - c. In VPC 251 IP addresses available (5 are reserved). This is different from the subnetting we studied in which out of 256, available addresses are 254 [2 reserved].

The first four IP addresses and the last IP address in each subnet CIDR block are not available for your use, and they cannot be assigned to a resource, such as an EC2 instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

- 10.0.0.0: Network address.
- 10.0.0.1: Reserved by AWS for the VPC router.
- 10.0.0.2: Reserved by AWS. The IP address of the DNS server is the base of the VPC network range plus two. For VPCs with multiple CIDR blocks, the IP address of the DNS server is located in the primary CIDR. We also reserve the base of each subnet range plus two for all CIDR blocks in the VPC. For more information, see Amazon DNS server.
- 10.0.0.3: Reserved by AWS for future use.
- 10.0.0.255: Network broadcast address. We do not support broadcast in a VPC, therefore we reserve this address.

VPCs > Create VPC

## Create VPC

A VPC is an isolated portion of the AWS cloud populated by AWS objects, such as Amazon EC2 instances. You must specify an IPv4 address range for your VPC. Specify the IPv4 address range as a Classless Inter-Domain Routing (CIDR) block; for example, 10.0.0.0/16. You cannot specify an IPv4 CIDR block larger than /16. You can optionally associate an IPv6 CIDR block with the VPC.

Name tag

IPv4 CIDR block\*

IPv6 CIDR block ☒ No IPv6 CIDR Block ☐ Amazon provided IPv6 CIDR block ☐ IPv6 CIDR owned by me

Tenancy

\* Required

Cancel Create

Create VPC Actions

Filter by tags and attributes or search by keyword

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	IPv6 CIDR (Network Border Group)	DHCP options set
s_VPC	vpc-045514f27f5243384	available	10.0.0.0/16	-	-	dopt-30a6884a
	vpc-efa62b92	available	172.31.0.0/16	-	-	dopt-30a6884a

VPC: vpc-045514f27f5243384

Description CIDR Blocks Flow Logs Tags

VPC ID	vpc-045514f27f5243384	Tenancy	default
State	available	Default VPC	No
IPv4 CIDR	10.0.0.0/16	Classic link	Disabled
IPv6 CIDR	-	IPv6 CIDR (Network Border Group)	-
IPv6 Pool	-	DNS resolution	Enabled
Network ACL	acl-01e961498cc4c25e1	DNS hostnames	Disabled
DHCP options set	dopt-30a6884a	ClassicLink DNS Support	Disabled
Route table	rtb-03ad7aebf71c9d292	Owner	381424482865

- After creating the VPC now create subnet click subnet. You will find the available subnets associated with the default VPC. The number of subnets varies if your region is changed. Now click on create subnet.

Create subnet Actions

Filter by tags and attributes or search by keyword

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone
	subnet-0a443b2b	available	vpc-efa62b92	172.31.80.0/20	4091	-	us-east-1a
	subnet-30f5f57d	available	vpc-efa62b92	172.31.16.0/20	4091	-	us-east-1b
	subnet-7eb29970	available	vpc-efa62b92	172.31.64.0/20	4091	-	us-east-1c
	subnet-9d1b9fac	available	vpc-efa62b92	172.31.48.0/20	4091	-	us-east-1a
	subnet-de790481	available	vpc-efa62b92	172.31.32.0/20	4091	-	us-east-1b
	subnet-e9fa8b8f	available	vpc-efa62b92	172.31.0.0/20	4091	-	us-east-1c

- Set the name of the subnet custom. Select the VPC you created from the drop-down menu. Select the availability zone and make a new CIDR block for the subnet.
  - Assuming 10.0.0.0/16 as VPC CIDR BLOCK [say 256 subnets]
    - MAX 200 subnets per AZ are allowed in AWS VPC.
    - MAX 5 VPCs are allowed per region.
    - Subnets belong to one AZ and VPC can span more than one AZ.
  - First subnet 10.0.1.0/24 [251 IPs]
  - Second subnet 10.0.2.0/24 [251 IPs]
  - Third subnet 10.0.3.0/24 [251 IPs]
- Create three subnets in three different availability zones of a region. It must be done explicitly else Amazon will set up all the subnets in ONE AZ. (We are looking for high availability setup)

### Create subnet

Specify your subnet's IP address block in CIDR format, for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag

VPC\*

Availability Zone

No preference

VPC CIDRs

CIDR	Status	Status Reason
------	--------	---------------

IPv4 CIDR block\*

\* Required

Cancel

Create

Activate Windows

Subnets > Create subnet

### Create subnet

Specify your subnet's IP address block in CIDR format, for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag

10.0.1.0 - a

VPC\*

vpc-045514f27f5243384

Availability Zone

us-east-1a

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

IPv4 CIDR block\*

10.0.1.0/24

\* Required

Cancel

Create

Activate Windows

Subnets > Create subnet

### Create subnet

Specify your subnet's IP address block in CIDR format, for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag

10.0.2.0 - b

VPC\*

vpc-045514f27f5243384

Availability Zone

us-east-1b

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

IPv4 CIDR block\*

10.0.2.0/24

\* Required

Cancel

Create

Activate Windows



Subnets > Create subnet

## Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag  ⓘ

VPC\*  ⓘ

Availability Zone  ⓘ

VPC CIDRs

CIDR	Status	Status Reason
10.0.0.0/16	associated	

IPv4 CIDR block\*  ⓘ

\* Required

Cancel Create

Create subnet Actions ▾

Filter by tags and attributes or search by keyword

	Name ▾	Subnet ID	State ▾	VPC ▾	IPv4 CIDR ▾	Available IPv4 ▾	IPv6 CIDR	Av
<input type="checkbox"/>	10.0.1.0 - a	subnet-0590dd6df6db3b9d0	available	vpc-045514f27f5243384  ...	10.0.1.0/24	251	-	US-
<input type="checkbox"/>		subnet-0a443b2b	available	vpc-efa62b92	172.31.80.0/20	4091	-	US-
<input type="checkbox"/>	10.0.2.0 - b	subnet-0bd06cbb083f588	available	vpc-045514f27f5243384  ...	10.0.2.0/24	251	-	US-
<input type="checkbox"/>	10.0.3.0 - c	subnet-0d9a5af814805b9ab	available	vpc-045514f27f5243384  ...	10.0.3.0/24	251	-	US-
<input type="checkbox"/>		subnet-30f5f57d	available	vpc-efa62b92	172.31.16.0/20	4091	-	US-
<input type="checkbox"/>		subnet-7eb29970	available	vpc-efa62b92	172.31.64.0/20	4091	-	US-
<input type="checkbox"/>		subnet-9d1b9fac	available	vpc-efa62b92	172.31.48.0/20	4091	-	US-
<input type="checkbox"/>		subnet-de790481	available	vpc-efa62b92	172.31.32.0/20	4091	-	US-
<input type="checkbox"/>		subnet-e9fa8b8f	available	vpc-efa62b92	172.31.0.0/20	4091	-	US-

9. **All these subnets are private (we want our data to be private).** If any server is launched in an ec2 instances these servers cannot be accessed through public internet. It can only be accessed through load balancer.

10. Now launch a server using EC2 service in your VPC (custom VPC) and specify the subnet from the subnets you created.

### Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management instance, and more.

Number of instances ⓘ  Launch into Auto Scaling Group ⓘ

Purchasing option ⓘ ☐ Request Spot instances

Network ⓘ  ⓘ Create new VPC

Subnet ⓘ  ⓘ Create new subnet  
251 IP Addresses available

Auto-assign Public IP ⓘ  ⓘ

11. Attach IAM role S3 if you want your server (EC2) to communicate with S3. IAM role is defined whenever one service needs to communicate with another service.

E & OE

Handouts: Drakhshan Bokhat

Domain join directory ⓘ No directory ⓘ Create new directory

IAM role ⓘ None ⓘ Create new IAM role

Shutdown behavior ⓘ s3-Access

- To create the role. Click on create new role. Select EC2 as EC2 wants to communicate with S3 so attach the permission of S3. Set the names and tags and create the role.

### Roles

#### What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

**Additional resources:**

- [IAM Roles FAQ](#)
- [IAM Roles Documentation](#)
- [Tutorial: Setting Up Cross Account Access](#)
- [Common Scenarios for Roles](#)

[Create role](#)
[Delete role](#)

### Create role

1 2 3 4

#### Select type of trusted entity

**AWS service**  
EC2, Lambda and others

**Another AWS account**  
Belonging to you or 3rd party

**Web identity**  
Cognito or any OpenID provider

**SAML 2.0 federation**  
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

#### Choose a use case

**Common use cases**

**EC2**  
Allows EC2 instances to call AWS services on your behalf.

**Lambda**  
Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

<a href="#">API Gateway</a>	<a href="#">CodeBuild</a>	<a href="#">EMR Containers</a>	<a href="#">IoT SiteWise</a>	<a href="#">RDS</a>
<a href="#">AWS Backup</a>	<a href="#">CodeDeploy</a>	<a href="#">ElastiCache</a>	<a href="#">IoT Things Graph</a>	<a href="#">Redshift</a>

\* Required

[Cancel](#) [Next: Permissions](#)

## Create role

1 2 3 4

### ▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy



Filter policies ▼

Q s3

Showing 8 results

	Policy name ▼	Used as
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	None
<input checked="" type="checkbox"/>	AmazonS3FullAccess	None
<input type="checkbox"/>	AmazonS3OutpostsFullAccess	None
<input type="checkbox"/>	AmazonS3OutpostsReadOnlyAccess	None
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	None
<input type="checkbox"/>	IVSRecordToS3	None
<input type="checkbox"/>	QuickSightAccessForS3StorageManagementAnalyticsReadOnly	None

\* Required

Cancel

Previous

Next: Tags

Windows  
Go to Settings to activate Windows

## Create role

1 2 3 4

### Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
Name	S3-Access	✕
Add new key		

You can add 49 more tags.

## Create role

1 2 3 4

### Review

Provide the required information below and review this role before you create it.

Role name\*

EC2-S3-Access

Use alphanumeric and '+', '=', '@', '-', '\_' characters. Maximum 64 characters.

Role description

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+', '=', '@', '-', '\_' characters.

Trusted entities

AWS service: ec2.amazonaws.com

Policies

AmazonS3FullAccess

Permissions boundary

Permissions boundary is not set

E & OE

Handouts: Drakhshan Bokhat

13. Now attach the role. Keep the other values as default (tenancy = shared) and attach the security group. Please note that this SG resides in your custom VPC not in the region. **Review and Launch.**
14. Launch three instances in different AZs and install the Apache server (different servers index file for the difference) on them.

**Placement group** ⓘ
 ☐ Add instance to placement group

**Capacity Reservation** ⓘ
 

Open

---

**Domain join directory** ⓘ
 

No directory

↻ Create new directory

**IAM role** ⓘ
 

EC2-S3-Access

↻ Create new IAM role

---

**Shutdown behavior** ⓘ
 

Stop

---

**Monitoring** ⓘ
 ☐ Enable CloudWatch detailed monitoring  
 Additional charges apply.

**Tenancy** ⓘ
 

Shared - Run a shared hardware instance

Shared - Run a shared hardware instance  
 Dedicated - Run a Dedicated instance  
 Dedicated host **Launch this instance on a Dedicated host**

**Elastic Inference** ⓘ

---

**Credit specification** ⓘ
 ☐ Unlimited

---

1. Choose AMI
 2. Choose Instance Type
 3. Configure Instance
 4. Add Storage
 5. Add Tags
 6. Configure Security Group
 7. Review

### Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. A copy of a tag can be applied to volumes, instances or both. Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key	Value	Instances	Volumes	Network Interfaces
Name	first-server_in-VPC	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

**Add another tag** (1 in 50 tags maximum)

---

### Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

**Assign a security group:** ☒ Create a new security group  
☐ Select an existing security group

**Security group name:** vpc-ssg

**Description:** vpc-ssg

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

**Add Rule**

**Warning**

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Cancel
Previous
Review and Launch

first-server\_in-VPC    i-0f43f0fc3429ec38d    t2.micro    us-east-1a    pending    Initializing    None

---

Finding    Opt-in to AWS Compute Optimizer for recommendations. [Learn more](#)    Elastic IPs  
 Private DNS    ip-10-0-1-125.ec2.internal    Availability zone    us-east-1a  
 Private IPs    10.0.1.125    Security groups    vpc-ssg, view inbound rules, view outbound rules  
 Secondary private IPs    -    Scheduled events    -  
 VPC ID    vpc-045514f27f5243384 (aws VPC)    AMI ID    amzn2-ami-hvm-2.0.20210427.0-x86\_64

15. After creating subnets and launching the server in the subnet now create the route table. In route tables you will see two route tables. One is default and other is with your custom VPC. Both the route tables are private. Now click on create table click give name and select your custom VPC and tag if you want. Your route table is created.

- Each subnet can only be associated with one route table.

[Create route table](#) [Actions](#)

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
<input type="checkbox"/>		rtb-03ad7aebf71c9d292	-	-	Yes	vpc-045514f27f5243384
<input type="checkbox"/>		rtb-4aa6ae34	-	-	Yes	vpc-efa62b92

### Create route table

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Name tag

VPC\*

Key (128 characters maximum) Value (256 characters maximum)

This resource currently has no tags

[Add Tag](#) 50 remaining (Up to 50 tags maximum)

\* Required

[Cancel](#) [Create](#)

[Create route table](#) [Actions](#)

Filter by tags and attributes or search by keyword

<input type="checkbox"/>	Name	Route Table ID	Explicit subnet association	Edge associations	Main	VPC ID
<input checked="" type="checkbox"/>	rtb-internet	rtb-026d509f6d6c1eb70	-	-	No	vpc-045514f27f5243384
<input type="checkbox"/>		rtb-03ad7aebf71c9d292	-	-	Yes	vpc-045514f27f5243384
<input type="checkbox"/>		rtb-4aa6ae34	-	-	Yes	vpc-efa62b92

Route Table: rtb-026d509f6d6c1eb70



16. After creating the route table go to the subnet and select a subnet to associate the created route table with that subnet. Your subnet is linked with the default route table.

Create subnet

Actions

Filter by tags and attributes or search by keyword

1 to 9 of 9

	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Av.
<input checked="" type="checkbox"/>	10.0.1.0 - a	subnet-0590dd6df6db3b9d0	available	vpc-045514f27f5243384  ...	10.0.1.0/24	250	-	us-
<input type="checkbox"/>		subnet-0a443b2b	available	vpc-efa62b92	172.31.80.0/20	4091	-	us-
<input type="checkbox"/>	10.0.2.0 - b	subnet-0bd06cbb083f588	available	vpc-045514f27f5243384  ...	10.0.2.0/24	251	-	us-
<input type="checkbox"/>	10.0.3.0 - c	subnet-0d9a5af814805b9ab	available	vpc-045514f27f5243384  ...	10.0.3.0/24	251	-	us-
<input type="checkbox"/>		subnet-30f5f57d	available	vpc-efa62b92	172.31.16.0/20	4091	-	us-
<input type="checkbox"/>		subnet-7eb29970	available	vpc-efa62b92	172.31.64.0/20	4091	-	us-
<input type="checkbox"/>		subnet-9d1b9fac	available	vpc-efa62b92	172.31.48.0/20	4091	-	us-
<input type="checkbox"/>		subnet-de790481	available	vpc-efa62b92	172.31.32.0/20	4091	-	us-
<input type="checkbox"/>		subnet-0f6b88f	available	vpc-efa62b92	172.31.0.0/20	4091	-	us-

Create subnet

Actions

Filter by tags and attributes or search by keyword

1 to 9 of 9

	Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4
<input checked="" type="checkbox"/>	10.0.1.0 - a	subnet-0590dd6df6db3b9d0	available	vpc-045514f27f5243384  ...	10.0.1.0/24	250
<input type="checkbox"/>		subnet-0a443b2b	available	vpc-efa62b92	172.31.80.0/20	4091
<input type="checkbox"/>	10.0.2.0 - b	subnet-0bd06cbb083f588	available	vpc-045514f27f5243384  ...	10.0.2.0/24	251
<input type="checkbox"/>	10.0.3.0 - c	subnet-0d9a5af814805b9ab	available	vpc-045514f27f5243384  ...	10.0.3.0/24	251
<input type="checkbox"/>		subnet-30f5f57d	available	vpc-efa62b92	172.31.16.0/20	4091
<input type="checkbox"/>		subnet-7eb29970	available	vpc-efa62b92	172.31.64.0/20	4091

Subnet: subnet-0590dd6df6db3b9d0

Description

Flow Logs

Route Table

Network ACL

Tags

Sharing

Edit route table association

Route Table: rtb-03ad7aebf71c9d292

1 to 1 of 1

Destination	Target
-------------	--------

Subnets > Edit route table association

## Edit route table association

Subnet ID subnet-0590dd6df6db3b9d0

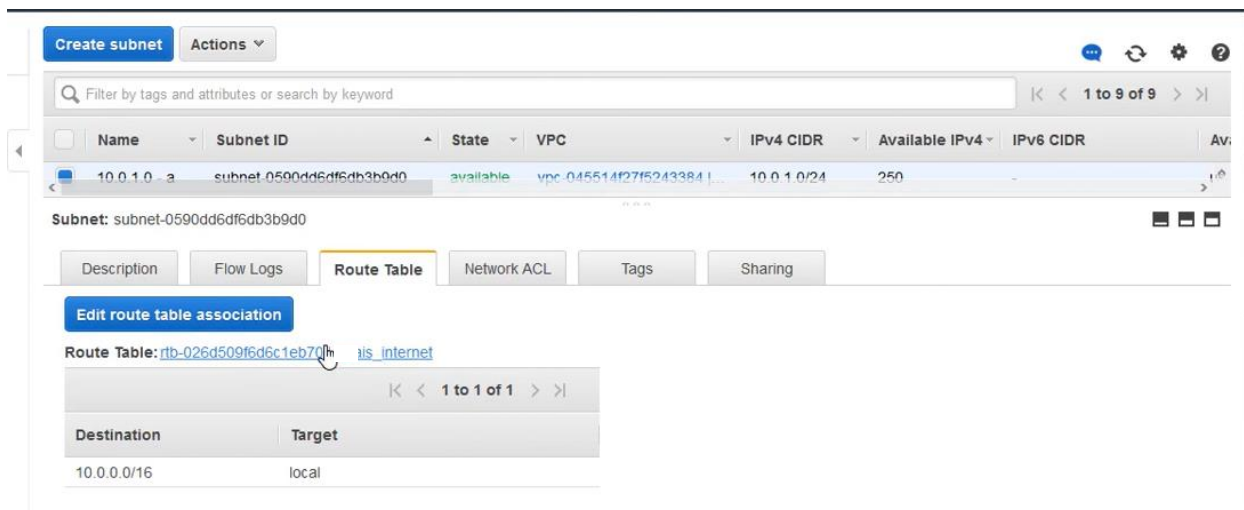
Route Table ID\* rtb-03ad7aebf71c9d292

Filter by attributes

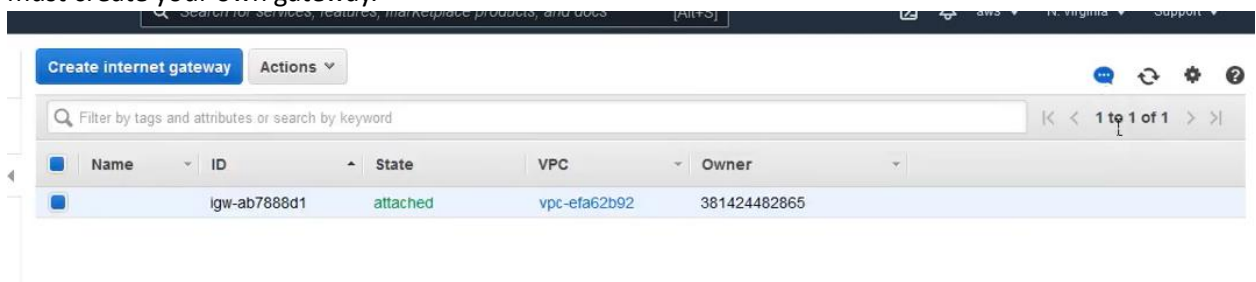
Route table ID	Route table name	VPC ID
rtb-03ad7aebf71c9d292		vpc-045514f27f5243384

E & OE

Handouts: Drakhshan Bokhat



17. Now create internet gateways. The default gateway associated with default VPC is there. You must create your own gateway.



18. Create the gateway and attach it with your custom VPC. This gateway is used for internet access for the public subnets.

[Internet gateways](#) > Create internet gateway

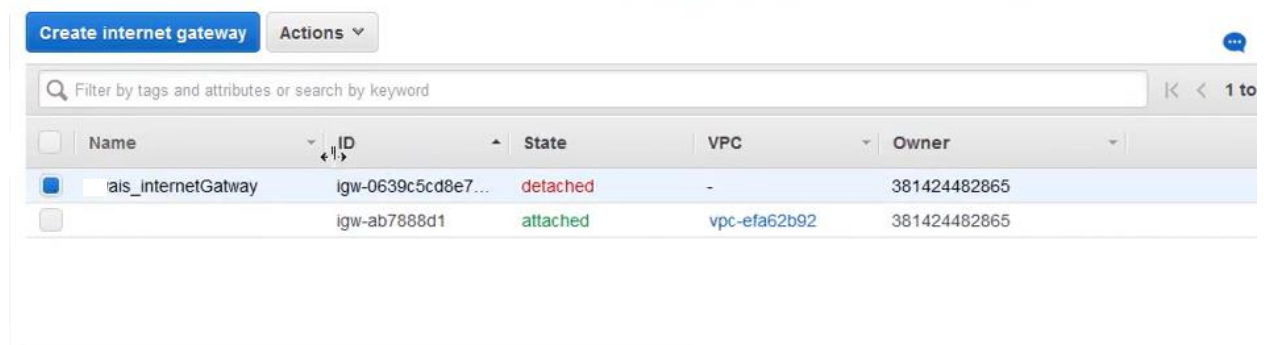
## Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Name tag

\* Required

[Cancel](#) [Create](#)



**Create internet gateway** **Actions**

Name	ID	State	VPC	Owner
ais_internetGateway	igw-0639c5cd8e7...	detached	-	381424482865
	igw-ab7888d1	attached	vpc-efa62b92	381424482865

[Internet gateways](#) > Attach to VPC

### Attach to VPC

Attach an internet gateway to a VPC to enable communication with the internet. Specify the VPC you would like to attach below.

VPC\*

**AWS Command Line**

VPC ID  Name

**Create internet gateway** **Actions**

Name	ID	State	VPC	Owner
ais_internetGateway	igw-0639c5cd8e7...	attached	vpc-045514f27f5...	381424482865
	igw-ab7888d1	attached	vpc-efa62b92	381424482865

19. Now enable the gateway and set the route in your route table. Go to route table select your custom route table and add the route. Attach your IGW and allow all the traffic from the internet.

**Create route table** **Actions**

Name	Route Table ID	Explicit subnet associatio	Edge associations	Main	VPC ID
ais_internet	rtb-026d509f6d6c1eb70	subnet-0590dd6df6db3b9d0	-	No	vpc-045514f27f5...
	rtb-03ad7aebf71c9d292	-	-	Yes	vpc-045514f27f5...
	rtb-4aa6ae34	-	-	Yes	vpc-efa62b92

**Route Table:** rtb-026d509f6d6c1eb70

**Summary** **Routes** Subnet Associations Edge Associations Route Propagation Tags

**Edit routes**

**View**

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No

Activate Windows

Route Tables > Edit routes

### Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No

Add route

\* Required

Cancel Save routes

Route Tables > Edit routes

### Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
			No

Add route

\* Required

Cancel Save routes

- Carrier Gateway
- Egress Only Internet Gateway
- Gateway Load Balancer
- Endpoint
- Instance
- Internet Gateway
- NAT Gateway
- Network Interface

Route Tables > Edit routes

### Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No

Destination must be a valid CIDR block or a prefix list.

0.0.0.0/0 igw-0639c5cd8e7c383f6 No

Add route

You must fix errors before saving.

\* Required

Cancel Save routes

20. (for public subnets) Click on route table and then go to associate subnets. Edit and associate the public subnets with the route table.

VPC > Route tables > rtb-075d460010dbd8954 > Edit subnet associations

## Edit subnet associations

Change which subnets are associated with this route table.

**Available subnets (3/6)**

< 1 > ⚙

<input type="checkbox"/>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/>	project-subnet-private1-us-east-2a	subnet-00555cf25dfbb075e	10.0.128.0/20	–	rtb-0163f0aa333301c49 / project-rtb-...
<input checked="" type="checkbox"/>	project-subnet-public2-us-east-2b	subnet-030282de943c1d7be	10.0.16.0/20	–	rtb-075d460010dbd8954 / project-rtb-...
<input type="checkbox"/>	project-subnet-private2-us-east-2b	subnet-07ba11c26569ebe54	10.0.144.0/20	–	rtb-07c33c74daf2347ea / project-rtb-...
<input type="checkbox"/>	project-subnet-private3-us-east-2c	subnet-07e814303a3c5184a	10.0.160.0/20	–	rtb-058fe29900faf5f1d / project-rtb-p...
<input checked="" type="checkbox"/>	project-subnet-public3-us-east-2c	subnet-0c810d268fe1d256e	10.0.32.0/20	–	rtb-075d460010dbd8954 / project-rtb-...
<input checked="" type="checkbox"/>	project-subnet-public1-us-east-2a	subnet-0c574ae8e466f25af	10.0.0.0/20	–	rtb-075d460010dbd8954 / project-rtb-...

**Selected subnets**

subnet-0c810d268fe1d256e / project-subnet-public3-us-east-2c ✕

subnet-030282de943c1d7be / project-subnet-public2-us-east-2b ✕

subnet-0c574ae8e466f25af / project-subnet-public1-us-east-2a ✕

21. Now create the NAT for the internet access in virtual machines in the private subnet, in public subnet and set the connectivity as public. Set the name and assign the elastic IP.

### NAT gateway settings

**Name - optional**  
Create a tag with a key of 'Name' and a value that you specify.

The name can be up to 256 characters long.

**Subnet**  
Select a subnet in which to create the NAT gateway.

subnet-0c574ae8e466f25af (project-subnet-public1-us-east-2a)

**Connectivity type**  
Select a connectivity type for the NAT gateway.

☒ Public  
☐ Private

**Elastic IP allocation ID** [Info](#)  
Assign an Elastic IP address to the NAT gateway.

▶ **Additional settings** [Info](#)

22. Now create a separate route table for NAT under the same VPC. Add the route and associate the private subnets to this route table.



### Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No
0.0.0.0/0	nat-01f167e6b4241ae14	-	No

[Add route](#)

[Cancel](#) [Preview](#) [Save changes](#)

### Edit subnet associations

Change which subnets are associated with this route table.

**Available subnets (2/4)**

Filter subnet associations

	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	Route table ID
<input type="checkbox"/>	PubSub1	subnet-01706bdc2496dcd2	10.0.1.0/24	-	rtb-04071552f8fc242db
<input checked="" type="checkbox"/>	PriSub1	subnet-09bba3d385fd5c156	10.0.3.0/24	-	Main (rtb-04071552f8fc242db)
<input type="checkbox"/>	PubSub2	subnet-0d0cb580a4ec1786b	10.0.2.0/24	-	rtb-04071552f8fc242db
<input checked="" type="checkbox"/>	PriSub2	subnet-0ded25715bf1bc0fe	10.0.4.0/24	-	Main (rtb-04071552f8fc242db)

**Selected subnets**

subnet-0ded25715bf1bc0fe / PriSub2    subnet-09bba3d385fd5c156 / PriSub1

23. Now create the ELB. Please note that ELB must be in your custom VPC. Add your instances work under your load balancer. The difference between the ELB in VPC and creating load balancer in EC2 is that in VPC we must add subnets. Since there is one subnet per AZ you must add the three AZ features.

#### VPC [Info](#)

Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

project-vpc  
vpc-062cdd7c3cd433c4a  
IPv4: 10.0.0.0/16

#### Mappings [Info](#)

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

- ☐ us-east-2a (use2-az1)
- ☐ us-east-2b (use2-az2)
- ☐ us-east-2c (use2-az3)

## VPC [Info](#)

Select the virtual private cloud (VPC) for your targets or you can [create a new VPC](#). Only VPCs with an internet gateway are enabled for selection. The selected VPC can't be changed after the load balancer is created. To confirm the VPC for your targets, view your [target groups](#).

project-vpc  
vpc-062cd7c3cd433c4a  
IPv4: 10.0.0.0/16



## Mappings [Info](#)

Select at least two Availability Zones and one subnet per zone. The load balancer routes traffic to targets in these Availability Zones only. Availability Zones that are not supported by the load balancer or the VPC are not available for selection.

### ☒ us-east-2a (use2-az1)

Subnet

subnet-00555cf25dfbb075e	project-subnet-private1-us-east-2a
subnet-00555cf25dfbb075e	project-subnet-private1-us-east-2a
subnet-0c574ae8e466f25af	project-subnet-public1-us-east-2a

You can proceed with this selection; however, for internet traffic to reach your load balancer, you must update the subnet's route table in the [VPC console](#).

IPv4 address

Assigned by AWS

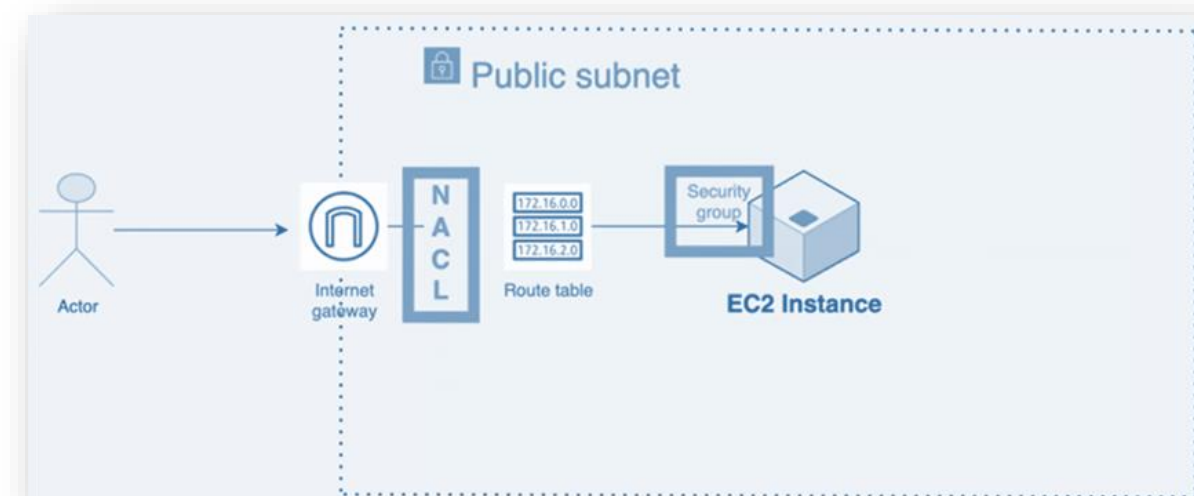
24. Instances (private) in VPC are not accessible through public IP so attach the elastic IPs with your instances. You must have elastic IPs created for that purpose. Now go to load balancer and access the load balancer through public DNS. Stop the instances to see the ELB in work in your VPC.

25. If you have your own DNS, you can use route 53 setup your DNS and redirect the traffic to load balancer.

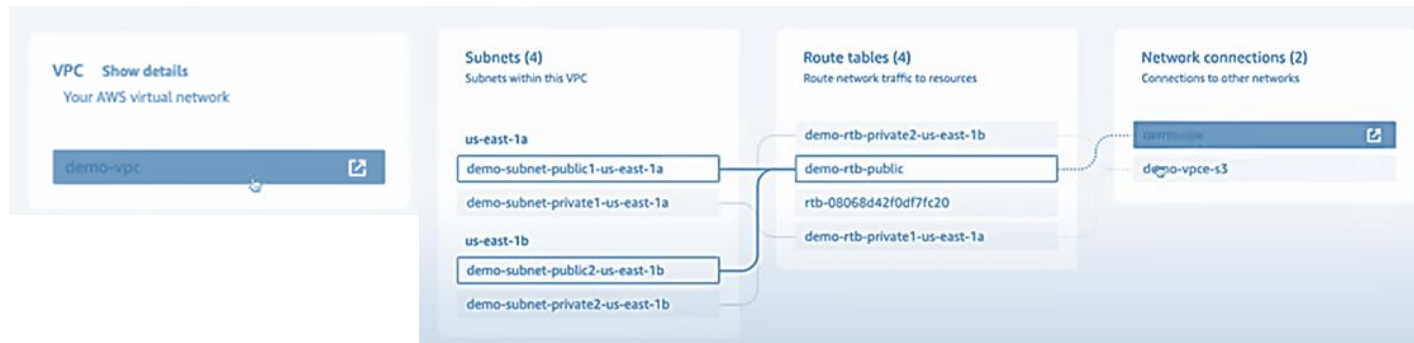
🌟 **AWS Route 53** translates URL names, such as [www.wordpress.com](#), into their corresponding numeric IP addresses.

## LAB TASK: WORKING OF Network Access Control List

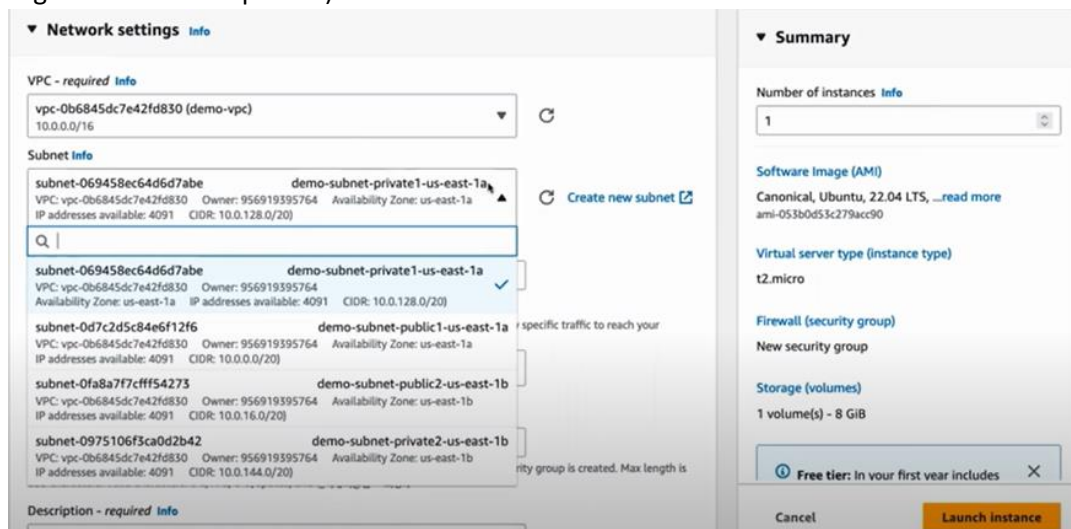
One of the tools in the AWS security toolkit for enabling defense-in-depth, is the Network Access Control List (NACL). A NACL is a security layer for your VPC, that acts as a firewall for controlling traffic in and out of one or more subnets



1. Create a VPC with more options.



2. Launch the server with (assign) public IP in public subnet of your custom VPC (one subnet = one AZ will be enough). (Recommended or default selection by Amazon will be private subnet to keep your organizational data private).



3. Install python application or Apache server though SSH.
  - a. Update the packages: `Sudo apt update`.
  - b. Check if python is installed: `Python3`
  - c. Install simple http server on python and access through port 8080: `python3 -m http.server 8080`
4. Try to access the application installed /running on your server though IP address and port number (on Browser of your system). [Format: `http://IP:port no`]
5. Not accessed? only SSH is allowed in SG attached to the instance? [Yes/No]
6. Now check NACL and check the inbound rules? All the traffic is allowed? [Yes/No]
7. NACL works at subnet level so its first level of security. Internet gateway will let the traffic enter the public subnet.
8. Change the SG rules and allow the traffic.
9. Refresh the page output will be shown.
10. Now restrict the traffic at NACL keeping SG rules allowing that type of traffic.
11. Try different rule numbers for different rules in NACL and check its pattern of execution.
12. Block specific IP addresses.