EE 542 – Laboratory Assignment #2: AWS Bring UP and Queuing

Instructor: Young H. Cho

Due date: September 3 at 11:59pm

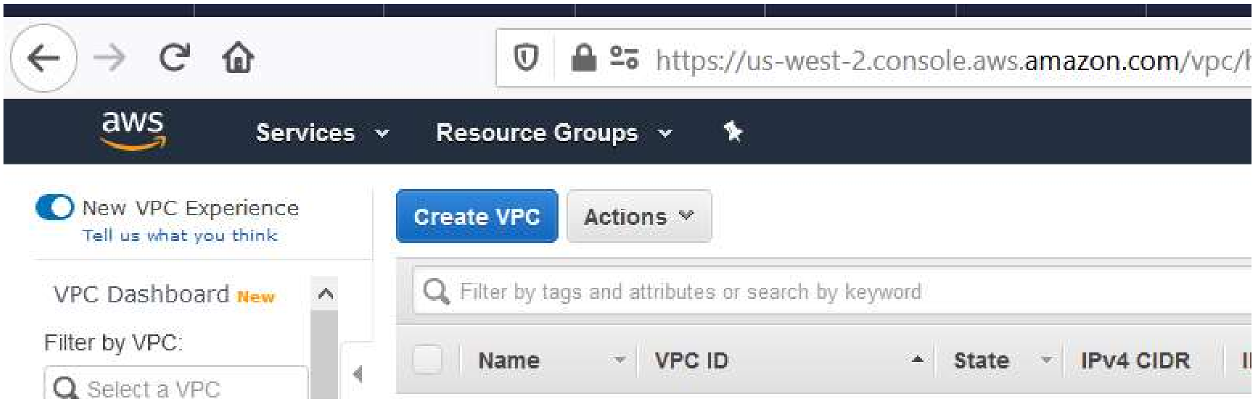
SETTING UP AWS

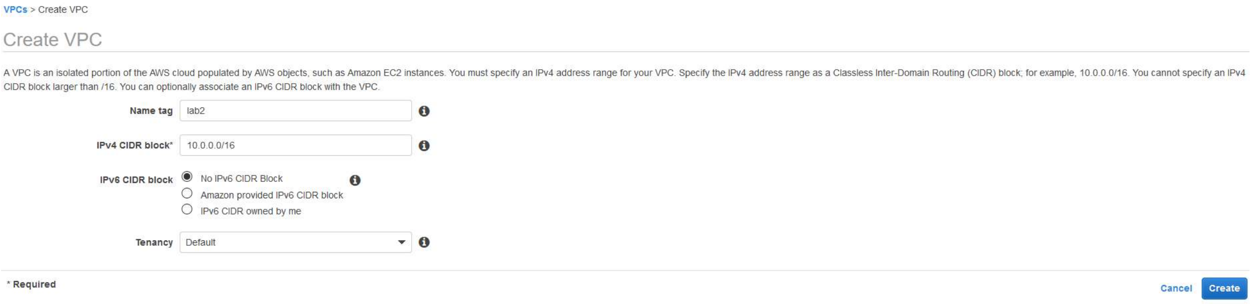
The first step is to set up AWS.

Log into AWS free tier account and select an AWS region of us-west-2(Oregon) and then go to VPC console tab by going to:

https://us-west-2.console.aws.amazon.com/vpc

Create a new VPC here in subnet 10.0.0.0/16 by selecting create VPC and configure as per below.




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: lab2

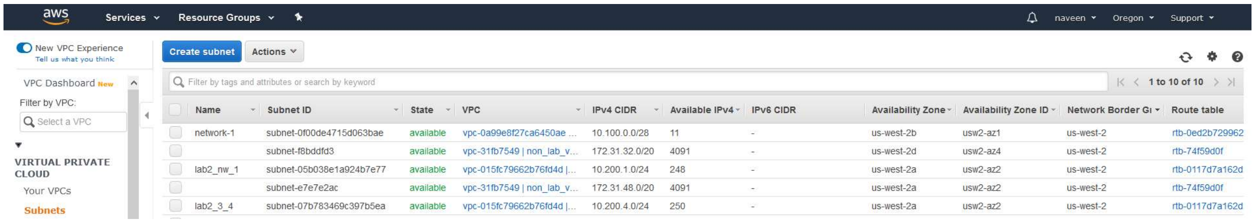
IPv4 CIDR block*: 10.0.0.0/16

IPv6 CIDR block: ● No IPv6 CIDR Block ○ Amazon provided IPv6 CIDR block ○ IPv6 CIDR owned by me

Tenancy: Default

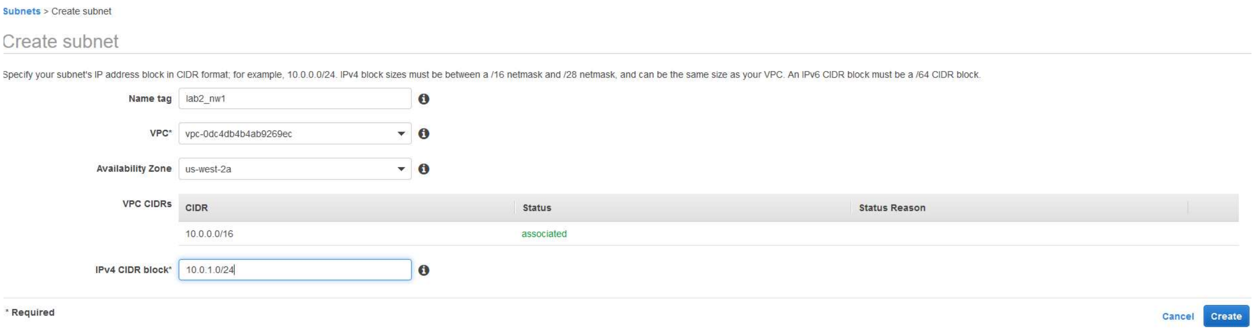
* Required

After this you need to create four subnets. One subnet is for client, other subnet for server and other two subnet are for public ip access over internet to client, server, router EC2 instance. Go to subnet tab in leftmost corner and select create subnet. Map this subnet to your newly created VPC. Create 4 subnet as per below configurations.



Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Availability Zone ID	Network Border Gı	Route table
network-1	subnet-0f00de4715d063bae	available	vpc-0a99e8f27ca6450ae ...	10.100.0.0/28	11	-	us-west-2b	usw2-az1	us-west-2	rtb-0ed2b729962
	subnet-f8bddfd3	available	vpc-31fb7549 | non_lab_v...	172.31.32.0/20	4091	-	us-west-2d	usw2-az4	us-west-2	rtb-74f59d0f
lab2_nw_1	subnet-05b038e1a924b7e77	available	vpc-015fc79662b76fd4d |...	10.200.1.0/24	248	-	us-west-2a	usw2-az2	us-west-2	rtb-0117d7a162d
	subnet-e7e7e2ac	available	vpc-31fb7549 | non_lab_v...	172.31.48.0/20	4091	-	us-west-2a	usw2-az2	us-west-2	rtb-74f59d0f
lab2_3_4	subnet-07b783469c397b5ea	available	vpc-015fc79662b76fd4d |...	10.200.4.0/24	250	-	us-west-2a	usw2-az2	us-west-2	rtb-0117d7a162d

Configurations:



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: lab2_nw1

VPC*: vpc-0dc4db4b4ab9269ec

Availability Zone: us-west-2a

VPC CIDRs

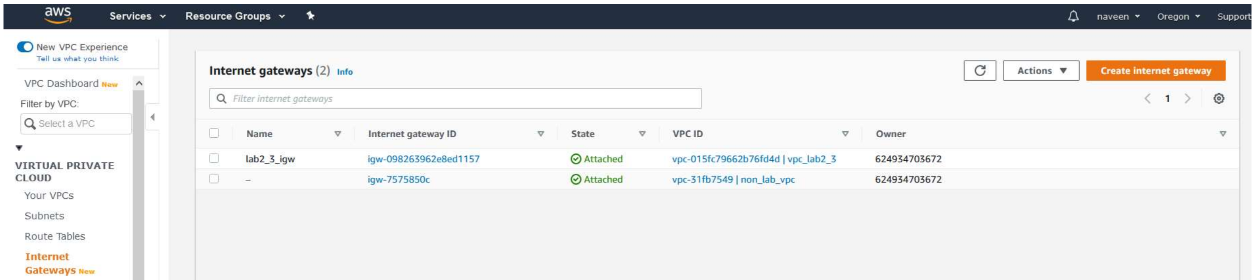
CIDR	Status	Status Reason
10.0.0.0/16	associated	

IPv4 CIDR block*: 10.0.1.0/24

* Required

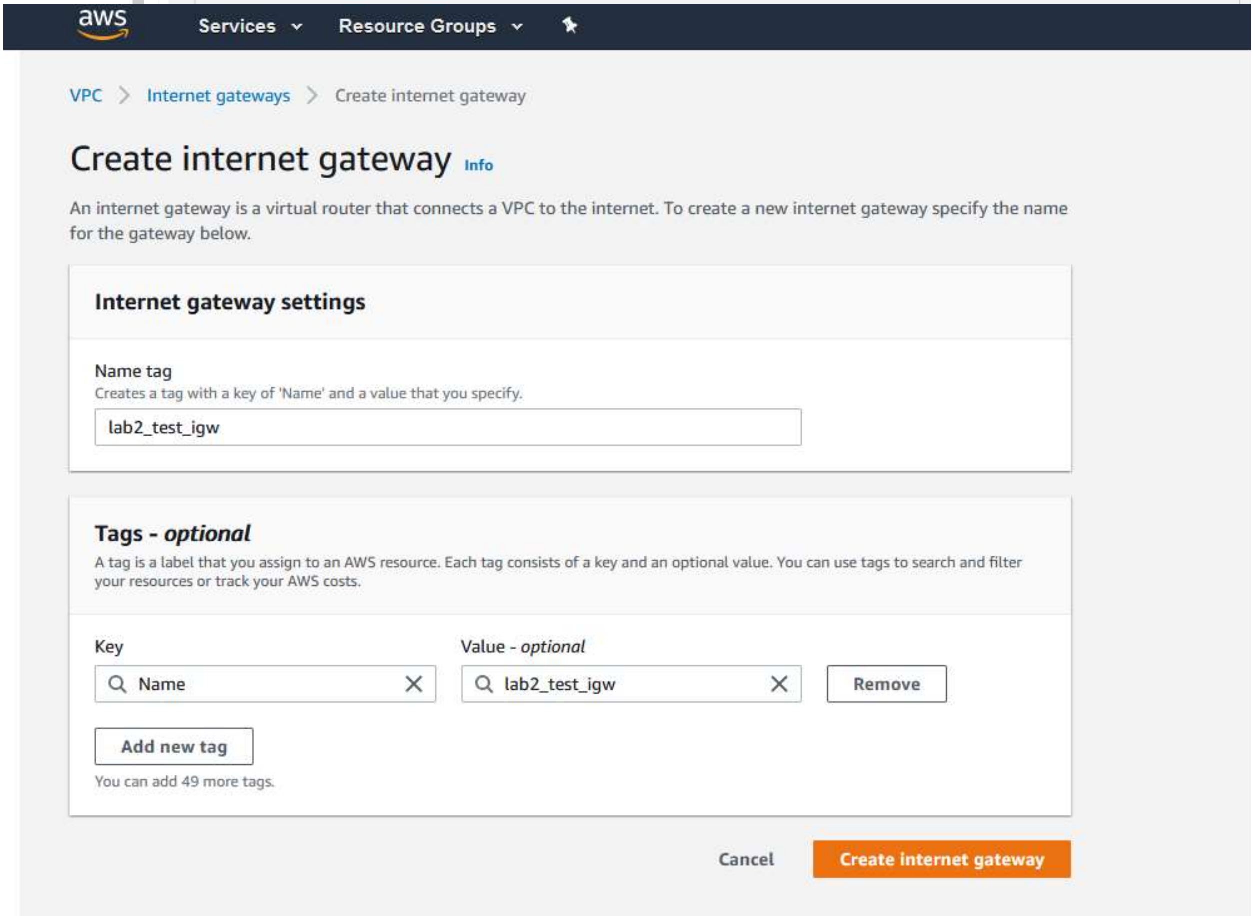
Repeat this for 10.0.2.0/24, 10.0.3.0/24, 10.0.4.0/24 subnets. Explore more about CIDR subnetting.

Now go to internet gateway tab on left most corner and create one. This is required so that the VPC network we created have access to the internet.



Internet gateways (2) Info

Name	Internet gateway ID	State	VPC ID	Owner
lab2_3_igw	igw-098263962e8ed1157	Attached	vpc-015fc79662b76fd4d | vpc_lab2_3	624934703672
–	igw-7575850c	Attached	vpc-31fb7549 | non_lab_vpc	624934703672



Create internet gateway Info

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.

Internet gateway settings

Name tag
Creates a tag with a key of 'Name' and a value that you specify.
lab2_test_igw

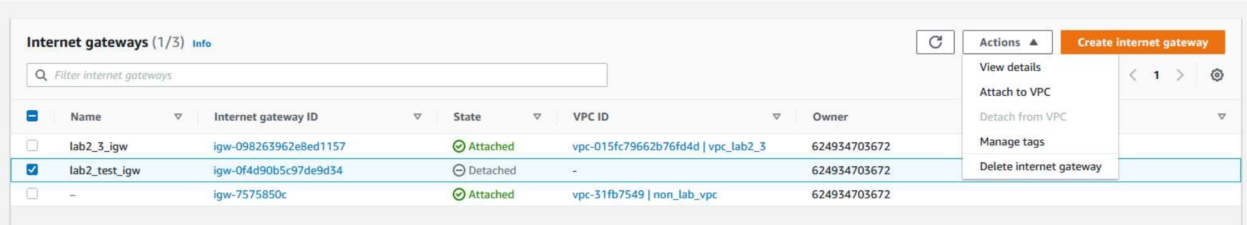
Tags - *optional*

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	lab2_test_igw

You can add 49 more tags.

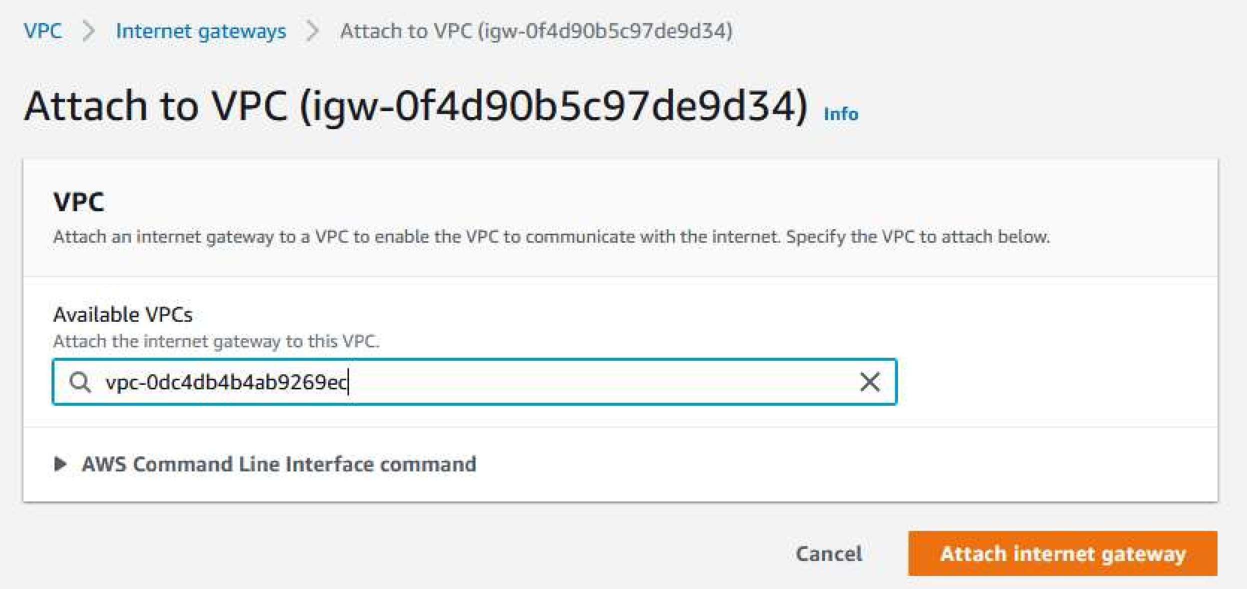
Now you need to attach this internet gateway to the corresponding VPC. Go back to Internet gateway tab and select the corresponding the IGW you created and select actions->attach to VPC.



Internet gateways (1/3) Info

	Name	Internet gateway ID	State	VPC ID	Owner
□	lab2_3_igw	igw-098263962e8ed1157	Attached	vpc-015fc79662b76fd4d | vpc_lab2_3	624934703672
☑	lab2_test_igw	igw-0f4d90b5c97de9d34	Detached	-	624934703672
□	–	igw-7575850c	Attached	vpc-31fb7549 | non_lab_vpc	624934703672

Select you VPC and then create it.



Attach to VPC (igw-0f4d90b5c97de9d34) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

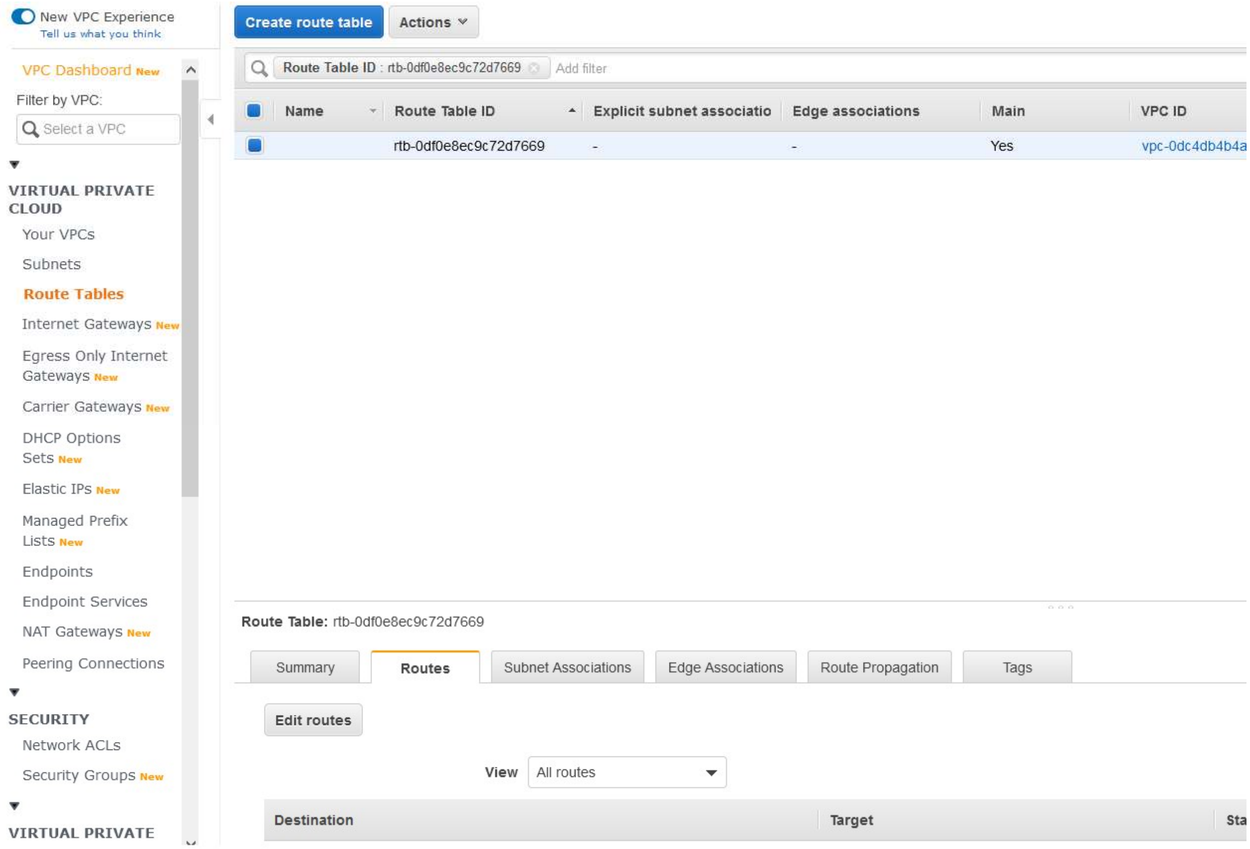
vpc-0dc4db4b4ab9269ec

▶ AWS Command Line Interface command

Now go to your VPC tab and select the vpc you have created. Explore more on dhcp option set, Main route table, and network ACL by going to below link:

- https://docs.aws.amazon.com/vpc/latest/userguide/working-with-vpcs.html
- https://docs.aws.amazon.com/appstream2/latest/developerguide/create-configure-new-vpc-with-private-public-subnets-nat.html
- https://docs.aws.amazon.com/vpc/latest/userguide/VPC_DHCP_Options.html
- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-nat-gateway.html
- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html
- https://medium.com/@mulupuru/your-comprehensive-guide-to-understanding-aws-data-transfer-costs-f5c8241d65ed

In the vpc tab, identify the main routing table the vpc is using and select that. Now configure a default route to point to the internet gateway we have created in the previous step. This is done fore internet access to all EC2 instance belonging to that VPC through the subnet.



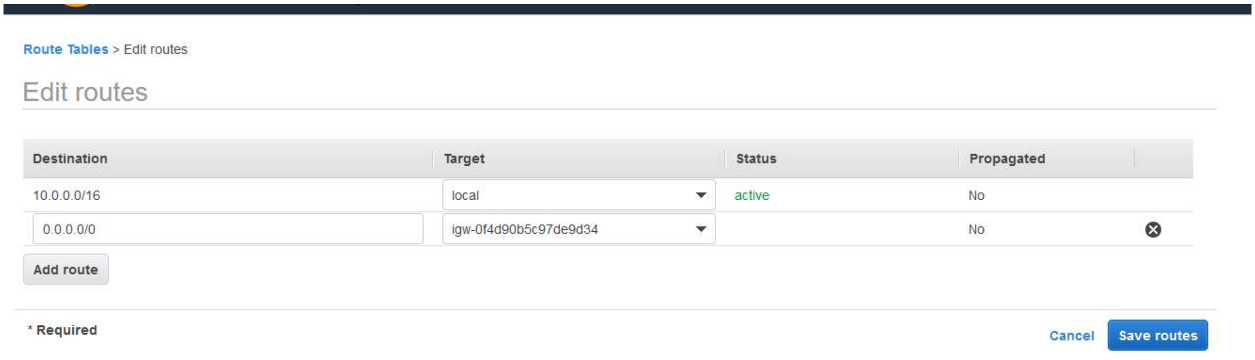
Route Table ID : rtb-0df0e8ec9c72d7669

Name	Route Table ID	Explicit subnet associatio	Edge associations	Main	VPC ID
	rtb-0df0e8ec9c72d7669	-	-	Yes	vpc-0dc4db4b4a

Route Table: rtb-0df0e8ec9c72d7669

Destination	Target	Sta

Click “edit routes” and add default routes with 0.0.0.0/0 and select “save routes”. Explore more on the different target visible under the drop-down selection and what each signifies. Now your VPC should have internet access.

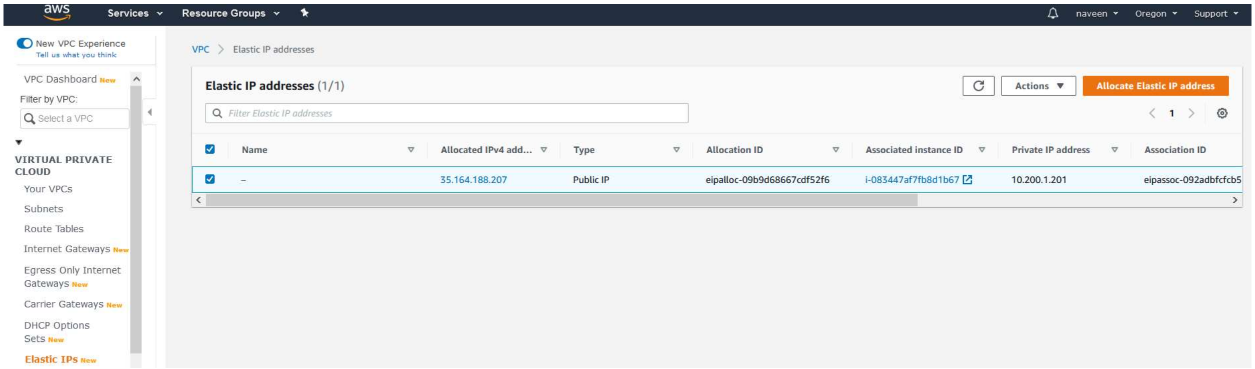


Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-0f4d90b5c97de9d34		No

* Required

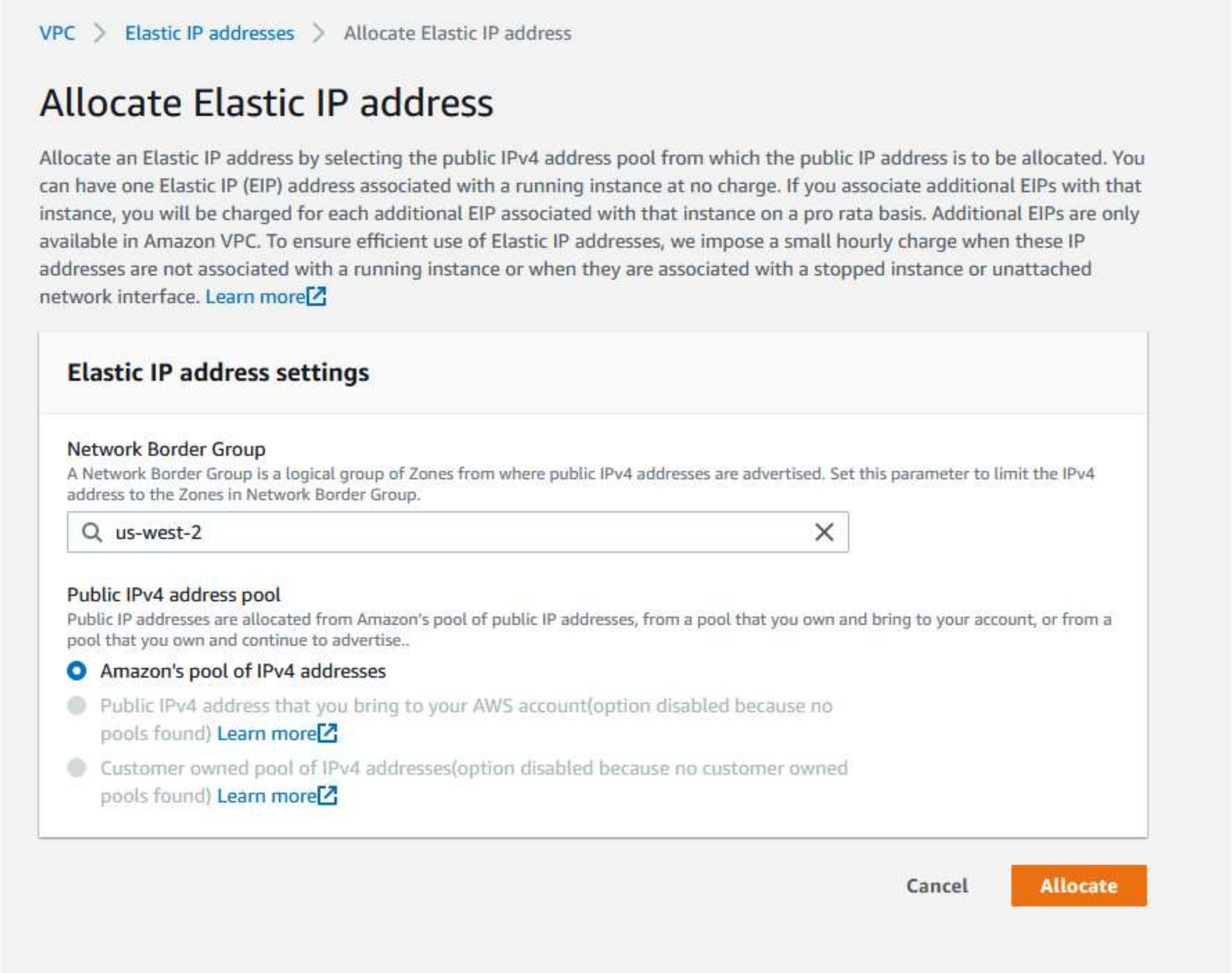
Now you need to create three “elastic IPs” for your three VM’s. Explore more on what elastic ip means. This would be your public ip reachable over internet through which you ssh. Make note that you would be billed for elastic ip usage if your ec2 instance is stopped and elastic ip is not associated with it. So, be mindfull of that. When stopping an ec2 instance, you should also disassociate the elastic ip and release the elastic ip back to the IP pool, since global ip’s are less. https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/elastic-ip-addresses-eip.html



Elastic IP addresses (1/1)

☑	Name	Allocated IPv4 add...	Type	Allocation ID	Associated instance ID	Private IP address	Association ID
☑	–	35.164.188.207	Public IP	eipalloc-09b9d68667cdf52f6	i-083447af7fb8d1b67	10.200.1.201	eipassoc-092adbfcfcb5

Select “allocate elastic ip address”. Select us-west-2 region and press allocate.



Allocate Elastic IP address

Allocate an Elastic IP address by selecting the public IPv4 address pool from which the public IP address is to be allocated. You can have one Elastic IP (EIP) address associated with a running instance at no charge. If you associate additional EIPs with that instance, you will be charged for each additional EIP associated with that instance on a pro rata basis. Additional EIPs are only available in Amazon VPC. To ensure efficient use of Elastic IP addresses, we impose a small hourly charge when these IP addresses are not associated with a running instance or when they are associated with a stopped instance or unattached network interface. Learn more

Elastic IP address settings

Network Border Group
A Network Border Group is a logical group of Zones from where public IPv4 addresses are advertised. Set this parameter to limit the IPv4 address to the Zones in Network Border Group.
us-west-2

Public IPv4 address pool
Public IP addresses are allocated from Amazon's pool of public IP addresses, from a pool that you own and bring to your account, or from a pool that you own and continue to advertise..
● Amazon's pool of IPv4 addresses
○ Public IPv4 address that you bring to your AWS account(option disabled because no pools found) Learn more
○ Customer owned pool of IPv4 addresses(option disabled because no customer owned pools found) Learn more

When you have instance created, you can attach it to your instance or n/w interface. We will be using n/w interface to attach the global ip. After attaching ip to your network interface, you cannot do any operations that would the change the interface characteristic such as changing IP or bringing down interface etc.
Question: How is amazon able to convert your public IP and reach your private IP on the interface?

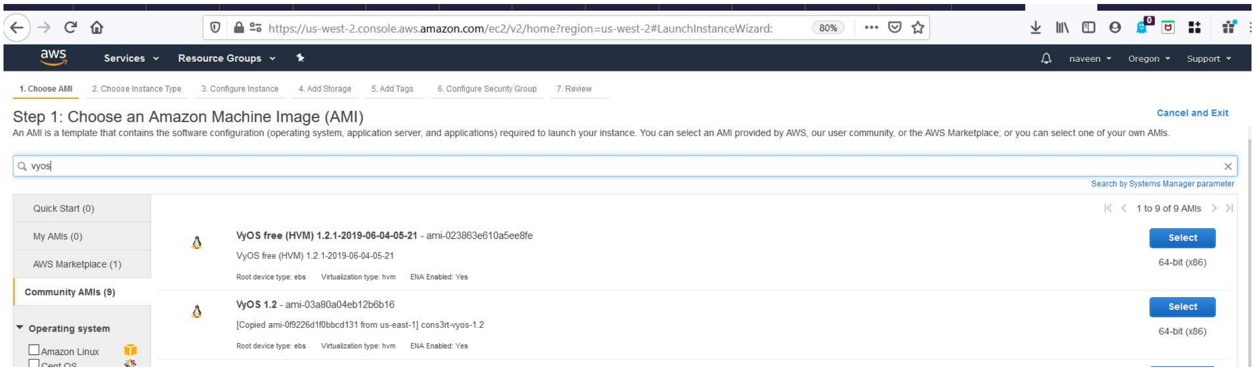
If you face network packet drops, make sure to look at network ACL list and security group of your instance. These both acts as firewall. Now we are done with networking part. Now we have to create EC2 instance.
EC2 instances are VMs which run over xen hypervisor in bare metal hardware

Research more on AWS IAM, how the permission is granted for different users etch and how to create new one from:
https://aws.amazon.com/iam/
https://docs.amazonaws.cn/en_us/IAM/latest/UserGuide/introduction.html

Go to your EC2 console tab by going to:
https://us-west-2.console.aws.amazon.com/ec2

Go to instances and select "launch instance".

1. First, we need to select OS image. For **vyos**, it should be selected from Community Ami's. Select **vyOS free (HVM) 1.2.1-2019-06-04-05-21** (ami-023863e610a5ee8fe) image. Explore more on what AMI means in AWS. With this way, you can install your own OS image on AWS servers.
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AMIs.html



Step 1: Choose an Amazon Machine Image (AMI)

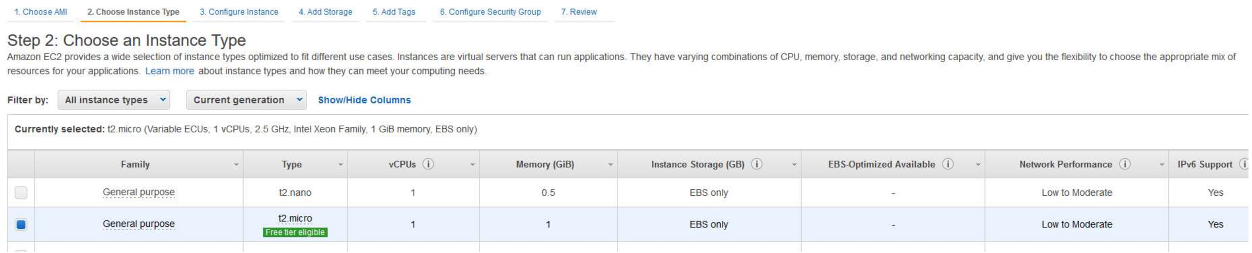
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

vyos

VyOS free (HVM) 1.2.1-2019-06-04-05-21 - ami-023863e610a5ee8fe
VyOS free (HVM) 1.2.1-2019-06-04-05-21
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
64-bit (x86)

VyOS 1.2 - ami-03a80a04eb12b6b16
[Copied ami-0f9226d1f0bbcd131 from us-east-1] cons3rt-vyos-1.2
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
64-bit (x86)

2. Then press select. In next window select **"t2.micro"** for your instance type. We have chosen this type because it's free under free tier limit. Here is where you will select the hardware configurations for your VM. Explore more on different type supported and its cost per hour.



Step 2: Choose an Instance Type

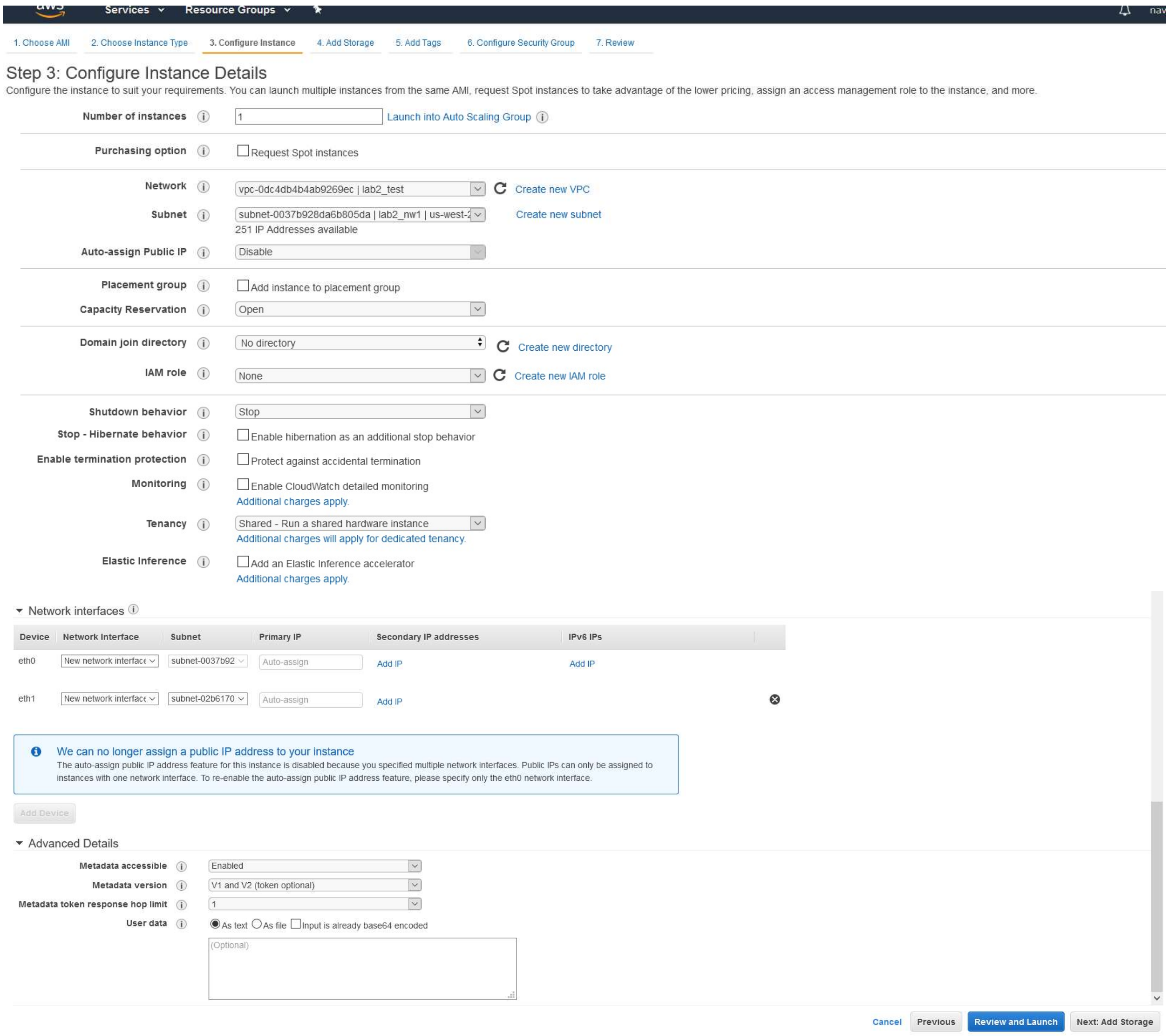
Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. Learn more about instance types and how they can meet your computing needs.

Filter by: All instance types | Current generation

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
☐	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes

3. select "next: configure instance details" on bottom right most corner and configure your instance details here. Here under network you have to select your newly created VPC in previous step. In subnet tab, select the subnet belonging to 16.0.1.0/24. Keep rest of the configuration same. Now in the "network interface" section, select "add device". This creates one more additional network adapter. You can assign static ip or get your ip from AWS DHCP server, which will be always running on VPC. Attach your newly created network adapter to 16.0.2.0/24 subnet. You can see a warning message that now public ip won't be assigned by AWS. This is why we need elastic IP to attach to one of these network adapters.



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

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 role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-0dc4db4b4ab9269ec | lab2_test — Create new VPC

Subnet: subnet-0037b928da6b805da | lab2_nw1 | us-west-2 — Create new subnet
251 IP Addresses available

Auto-assign Public IP: Disable

Placement group: □ Add instance to placement group

Capacity Reservation: Open

Domain join directory: No directory — Create new directory

IAM role: None — Create new IAM role

Shutdown behavior: Stop

Stop - Hibernate behavior: □ Enable hibernation as an additional stop behavior

Enable termination protection: □ Protect against accidental termination

Monitoring: □ Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

Elastic Inference: □ Add an Elastic Inference accelerator
Additional charges apply.

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-0037b92	Auto-assign	Add IP	Add IP
eth1	New network interface	subnet-02b6170	Auto-assign	Add IP	

We can no longer assign a public IP address to your instance
The auto-assign public IP address feature for this instance is disabled because you specified multiple network interfaces. Public IPs can only be assigned to instances with one network interface. To re-enable the auto-assign public IP address feature, please specify only the eth0 network interface.

Add Device

Advanced Details

Metadata accessible: Enabled

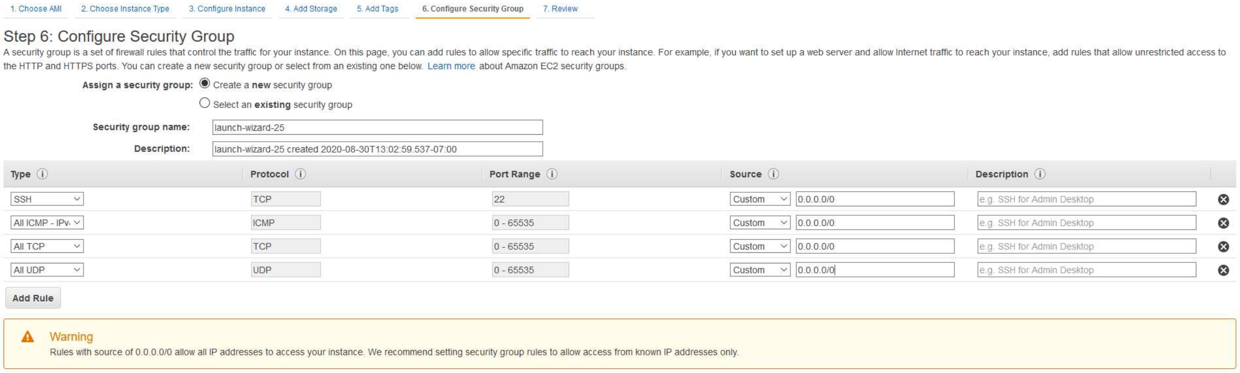
Metadata version: V1 and V2 (token optional)

Metadata token response hop limit: 1

User data: ● As text ○ As file □ Input is already base64 encoded
(Optional)

Cancel | Previous | Review and Launch | Next: Add Storage

4. Now select next, next and again select next to reach "configure security group". If you want to change storage configurations you can do in these respective tabs. In "Security group", You have to add firewall rules for your respective traffic to allow. By default, SSH is enabled. Configure in below way to allow ping, iperf and tcp, udp packet exchange.



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

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: launch-wizard-25

Description: launch-wizard-25 created 2020-08-30T13:02:59.537-07:00

Type	Protocol	Port Range	Source		Description
SSH	TCP	22	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
All ICMP - IPv4	ICMP	0 - 65535	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
All TCP	TCP	0 - 65535	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop
All UDP	UDP	0 - 65535	Custom	0.0.0.0/0	e.g. SSH for Admin Desktop

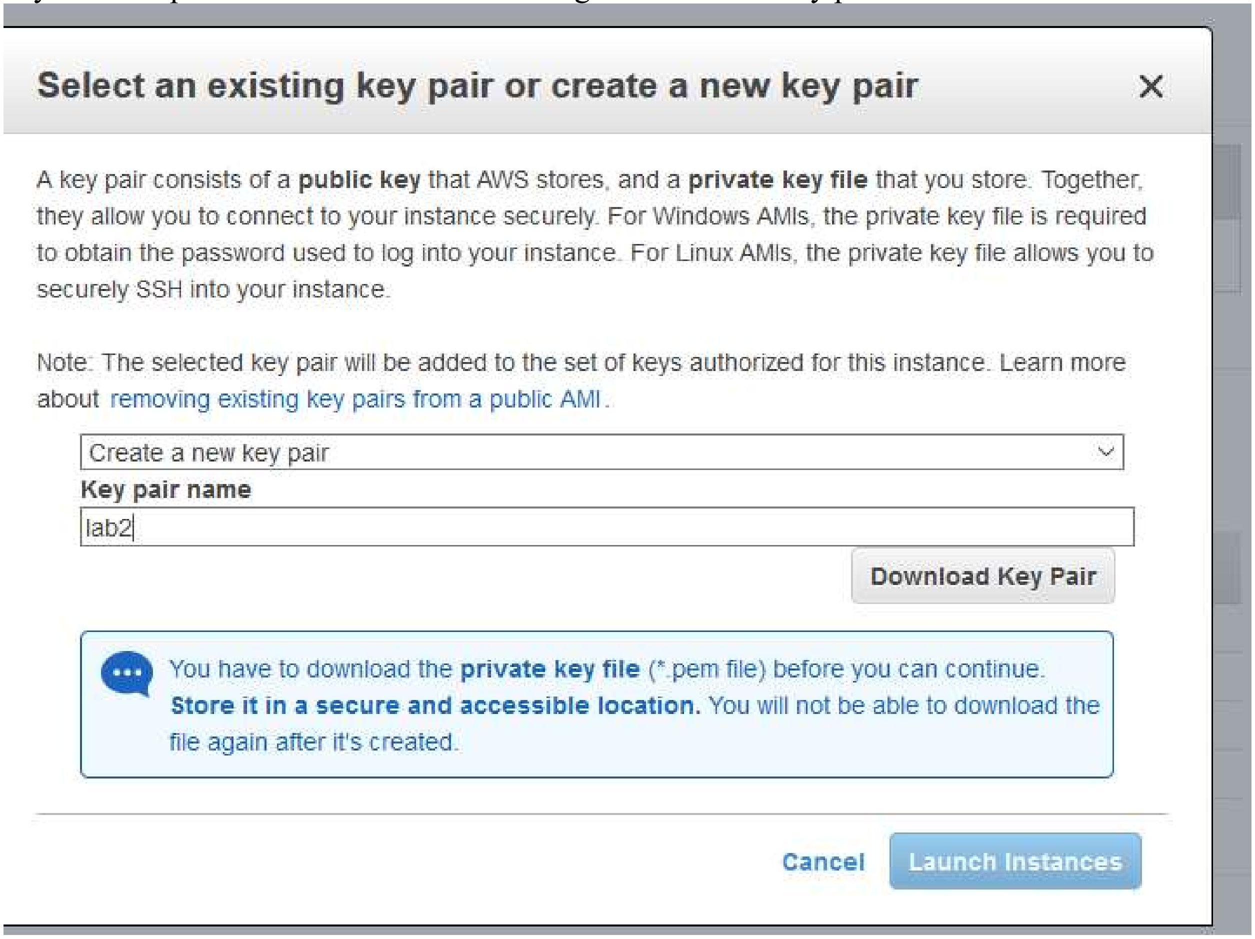
Add Rule

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.

5. Now press "review and launch" and then select "launch" to start your new VM which would be visible under your instance tab.

6. Here you would have to create ssh public, private key for logging into your ssh session. Give a name and download your key-pair. Never ever loss the private key as this key cannot be

regenerated again and you won’t be able to access instance again. You can use the same private key for multiple instances instead of choosing “create a new key pair”.



Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI.

Create a new key pair

Key pair name

lab2

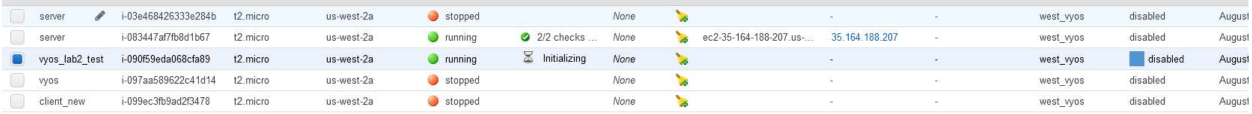
Download Key Pair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

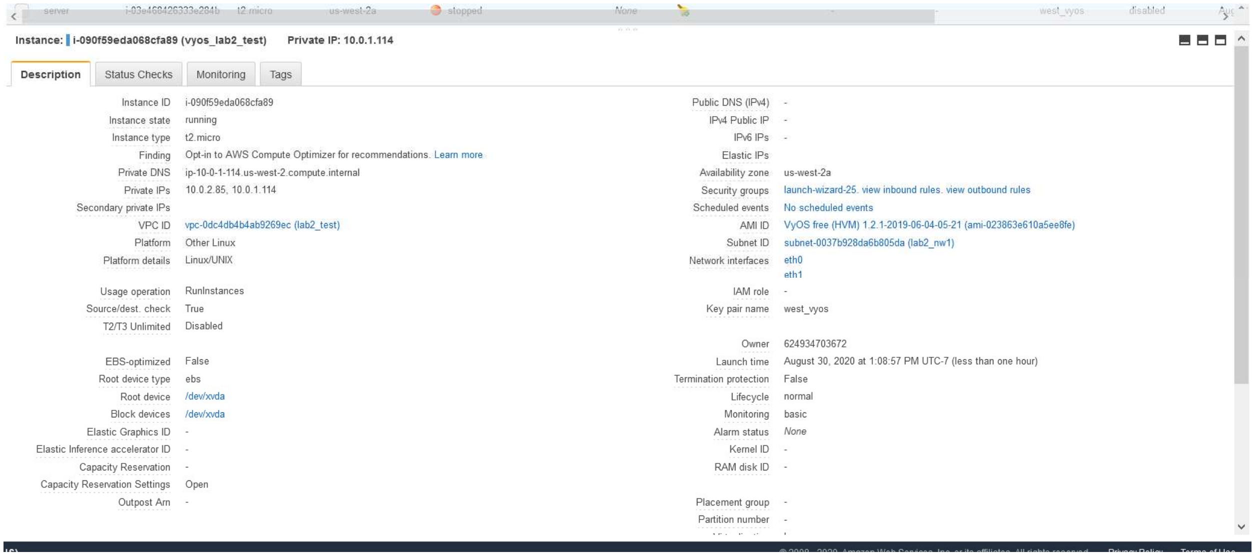
Cancel | Launch Instances

Explore more on ways to connect to your instance by going to below link: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstances.html

7. Give a name for your instance and observe what all configuration it shows by selecting your instance. From the description info you should be able to reach your VPC, security group, identify network interface adapter id etc.



☐	server	i-03e468426333e284b	t2.micro	us-west-2a	● stopped		None		-	-	west_vyos	disabled	August
☐	server	i-083447af7fb8d1b67	t2.micro	us-west-2a	● running	✓ 2/2 checks ...	None	ec2-35-164-188-207.us-...	35.164.188.207	-	west_vyos	disabled	August
■	vyos_lab2_test	i-090f59eda068cfa89	t2.micro	us-west-2a	● running	⌛ Initializing	None		-	-	west_vyos	disabled	August
☐	vyos	i-097aa589622c41d14	t2.micro	us-west-2a	● stopped		None		-	-	west_vyos	disabled	August
☐	client_new	i-099ec3fb9ad2f3478	t2.micro	us-west-2a	● stopped		None		-	-	west_vyos	disabled	August



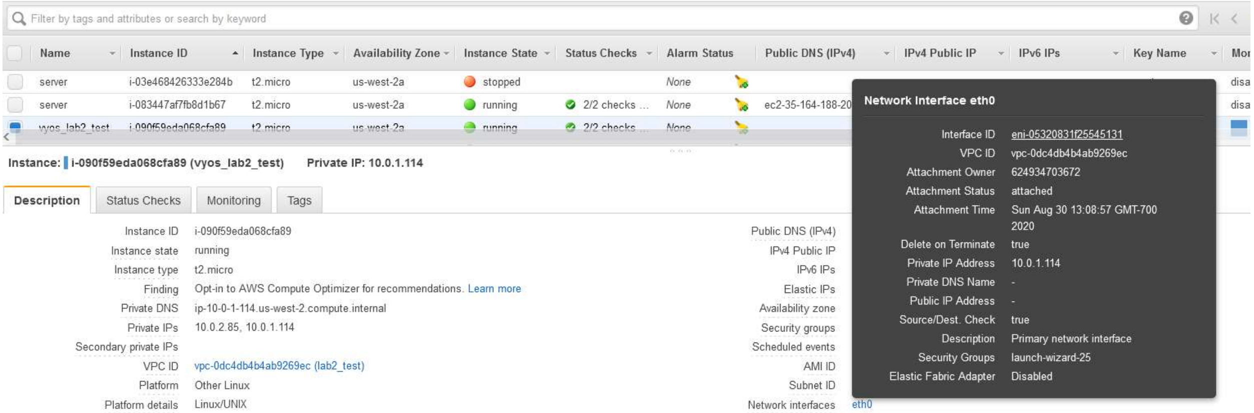
server i-03e468426333e284b t2.micro us-west-2a stopped None - - west_vyos disabled Aug

Instance: i-090f59eda068cfa89 (vyos_lab2_test) **Private IP:** 10.0.1.114

Description | Status Checks | Monitoring | Tags

Instance ID	i-090f59eda068cfa89	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	-
Instance type	t2.micro	IPv6 IPs	-
Finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more	Elastic IPs	
Private DNS	ip-10-0-1-114.us-west-2.compute.internal	Availability zone	us-west-2a
Private IPs	10.0.2.85, 10.0.1.114	Security groups	launch-wizard-25. view inbound rules. view outbound rules
Secondary private IPs		Scheduled events	No scheduled events
VPC ID	vpc-0dc4db4b4ab9269ec (lab2_test)	AMI ID	VyOS free (HVM) 1.2.1-2019-06-04-05-21 (ami-023863e610a5ee8fe)
Platform	Other Linux	Subnet ID	subnet-0037b928da6b805da (lab2_nw1)
Platform details	Linux/UNIX	Network interfaces	eth0 eth1
Usage operation	RunInstances	IAM role	-
Source/dest. check	True	Key pair name	west_vyos
T2/T3 Unlimited	Disabled		
		Owner	624934703672
EBS-optimized	False	Launch time	August 30, 2020 at 1:08:57 PM UTC-7 (less than one hour)
Root device type	ebs	Termination protection	False
Root device	/dev/xvda	Lifecycle	normal
Block devices	/dev/xvda	Monitoring	basic
Elastic Graphics ID	-	Alarm status	None
Elastic Inference accelerator ID	-	Kernel ID	-
Capacity Reservation	-	RAM disk ID	-
Capacity Reservation Settings	Open		
Outpost Arn	-	Placement group	-
		Partition number	-

8. Now we need to associate one of the elastic IP we created in previous steps to this instance. Go to VPC tab and then “elastic IP”. Associate this elastic IP with your network interface adapter of the EC2 instance.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs	Key Name	Mor
server	i-03e468426333e284b	t2.micro	us-west-2a	stopped		None					disa
server	i-083447af7fb8d1b67	t2.micro	us-west-2a	running	2/2 checks ...	None	ec2-35-164-188-20				disa
vyos_lab2_test	i-090f59eda068cfa89	t2.micro	us-west-2a	running	2/2 checks ...	None					

Network Interface eth0

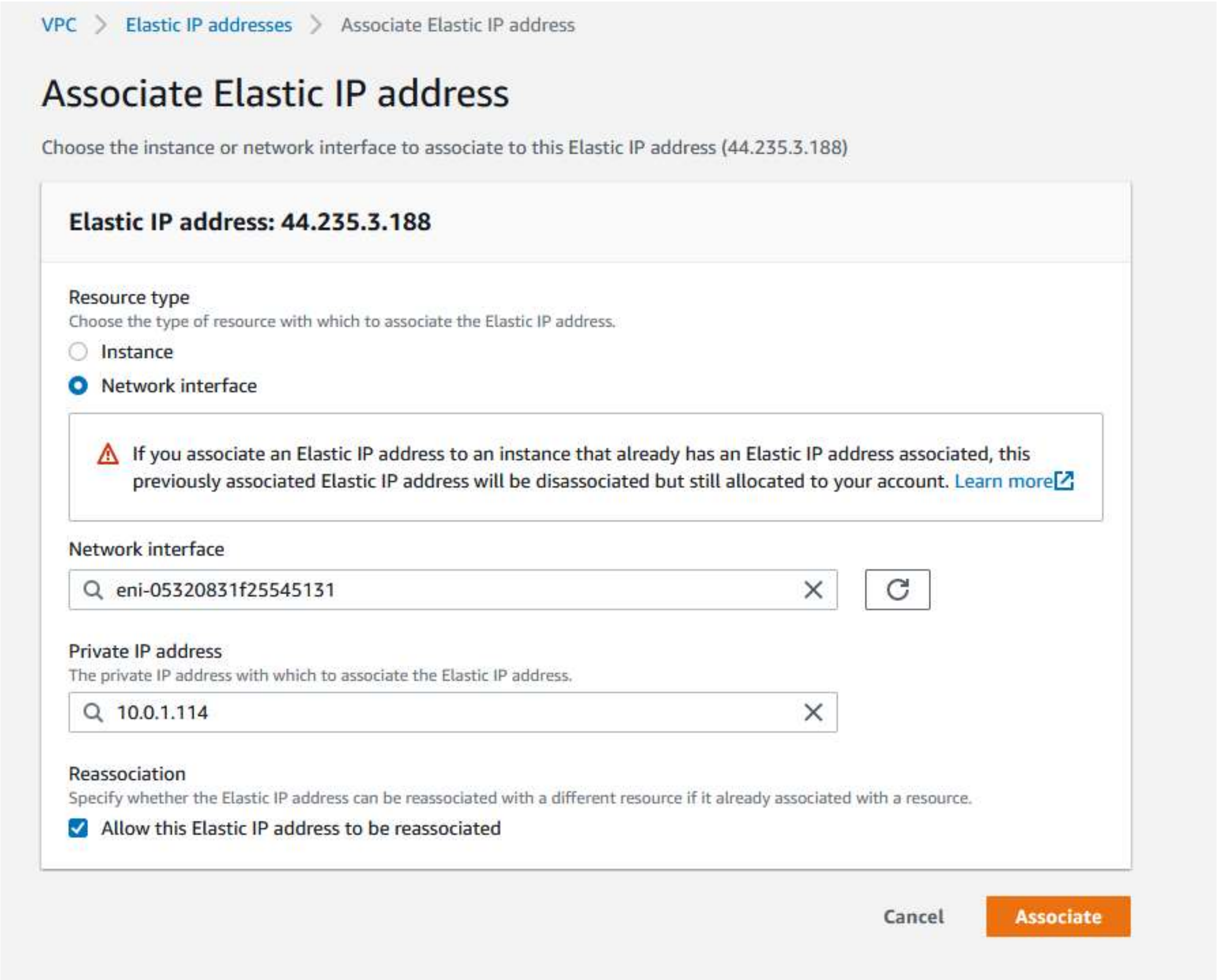
Interface ID	eni-05320831f25545131
VPC ID	vpc-0dc4db4b4ab9269ec
Attachment Owner	624934703672
Attachment Status	attached
Attachment Time	Sun Aug 30 13:08:57 GMT-700 2020
Delete on Terminate	true
Private IP Address	10.0.1.114
Private DNS Name	-
Public IP Address	-
Source/Dest. Check	true
Description	Primary network interface
Security Groups	launch-wizard-25
Elastic Fabric Adapter	Disabled

Instance: i-090f59eda068cfa89 (vyos_lab2_test) **Private IP:** 10.0.1.114

Description | Status Checks | Monitoring | Tags

Instance ID	i-090f59eda068cfa89	Public DNS (IPv4)	
Instance state	running	IPv4 Public IP	
Instance type	t2.micro	IPv6 IPs	
Finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more	Elastic IPs	
Private DNS	ip-10-0-1-114.us-west-2.compute.internal	Availability zone	
Private IPs	10.0.2.85, 10.0.1.114	Security groups	
Secondary private IPs		Scheduled events	
VPC ID	vpc-0dc4db4b4ab9269ec (lab2_test)	AMI ID	
Platform	Other Linux	Subnet ID	
Platform details	Linux/UNIX	Network interfaces	eth0

Get the network interface ip first and give that ip in the elastic IP tab. Select “allow the elastic IP to be re-associated” and then select associate. Check first whether you are able to ping this IP. Ig you are not able to ping then detach this IP from the instance and again re-associate with the next network adapter ID. This way, if you are not able to SSH session to interface issue, you can recover VM in this way.



VPC > Elastic IP addresses > Associate Elastic IP address

Associate Elastic IP address

Choose the instance or network interface to associate to this Elastic IP address (44.235.3.188)

Elastic IP address: 44.235.3.188

Resource type
Choose the type of resource with which to associate the Elastic IP address.
○ Instance
● Network interface

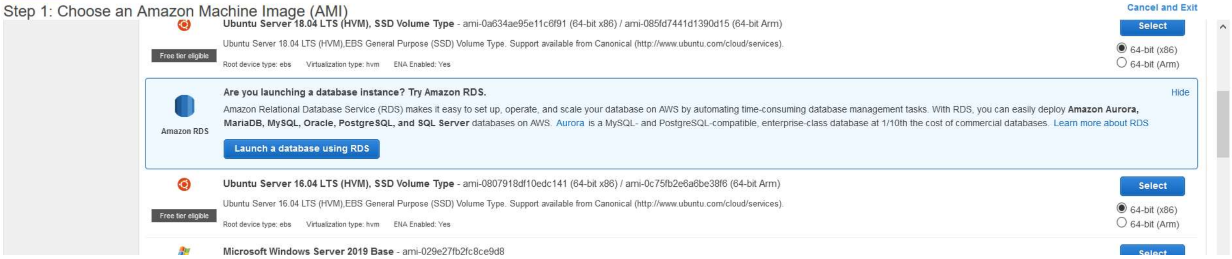
⚠ If you associate an Elastic IP address to an instance that already has an Elastic IP address associated, this previously associated Elastic IP address will be disassociated but still allocated to your account. Learn more

Network interface
eni-05320831f25545131

Private IP address
The private IP address with which to associate the Elastic IP address.
10.0.1.114

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.
☑ Allow this Elastic IP address to be reassociated

9. Now similarly create a client, server VM by using ubuntu “16.04” image. In the “configure instance details” tab you would have to accordingly choose one subnet which belongs to the vyos VM as done in LAB1 so that the router to client, router to server VM connectivity is established. All these VMs should be under same VPC. We choose the second interface for global elastic IP mapping to private IP for SSH connectivity so that we can play around with Linux commands on first network adapter interface eth0 under VM.



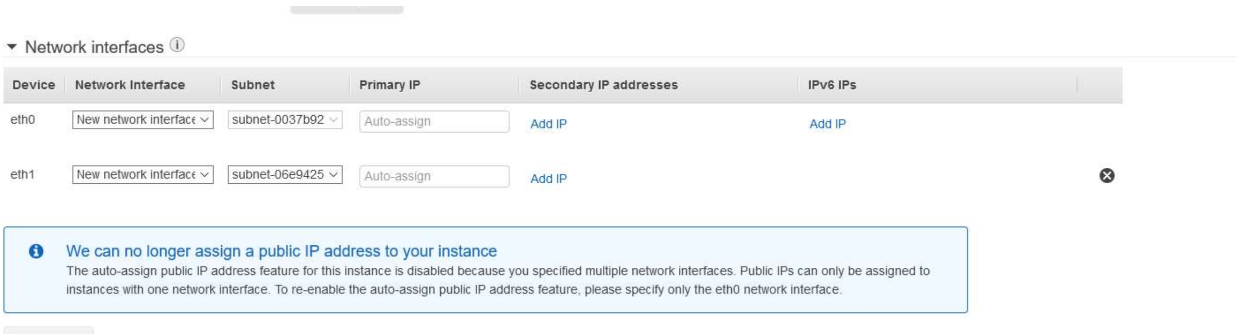
Step 1: Choose an Amazon Machine Image (AMI)

Ubuntu Server 18.04 LTS (HVM), SSD Volume Type - ami-0a634ae95e11c6f91 (64-bit x86) / ami-085fd7441d1390d15 (64-bit Arm)
Ubuntu Server 18.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
Free tier eligible
● 64-bit (x86)
○ 64-bit (Arm)

Are you launching a database instance? Try Amazon RDS.
Amazon Relational Database Service (RDS) makes it easy to set up, operate, and scale your database on AWS by automating time-consuming database management tasks. With RDS, you can easily deploy **Amazon Aurora, MariaDB, MySQL, Oracle, PostgreSQL, and SQL Server** databases on AWS. Aurora is a MySQL- and PostgreSQL-compatible, enterprise-class database at 1/10th the cost of commercial databases. Learn more about RDS

Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-0807918df10edc141 (64-bit x86) / ami-0c75fb2e6a6be38f6 (64-bit Arm)
Ubuntu Server 16.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
Root device type: ebs Virtualization type: hvm ENA Enabled: Yes
Free tier eligible
● 64-bit (x86)
○ 64-bit (Arm)

Microsoft Windows Server 2019 Base - ami-029e27fb2fc8ce9d8



▾ Network interfaces ⓘ

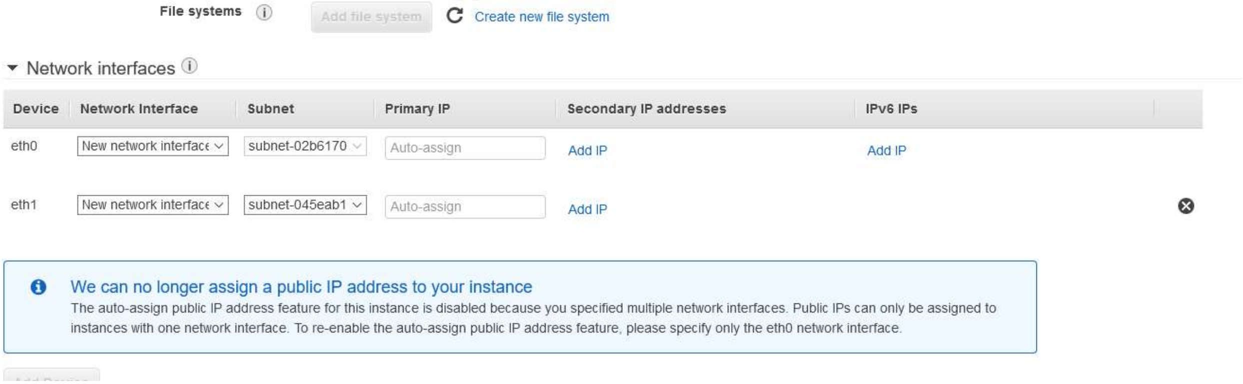
Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-0037b92	Auto-assign	Add IP	Add IP
eth1	New network interface	subnet-06e9425	Auto-assign	Add IP	

We can no longer assign a public IP address to your instance
The auto-assign public IP address feature for this instance is disabled because you specified multiple network interfaces. Public IPs can only be assigned to instances with one network interface. To re-enable the auto-assign public IP address feature, please specify only the eth0 network interface.

10. If you try to change any configuration of you elastic IP mapped network interface, your ssh would go down. So, don't do any configuration on that interface. This is why we created two n/w interface for client, server VM.

11. If you are not able to SSH, dissociate elastic IP from one network interface and connect to other. This could be due to that IP is not assigned for that network interface, since dhcp client would have to be manually started on the second interface eth1. So, it would be better to connect elastic IP to first interface always and after logging in and setting IP statically using ifconfig eth1 (static ip would be available from instance tab, you can even set these while you are in crating n/w interface tab when new instance is being created) and then change elastic IP mapping to this interface. Ensure that AWS private IP shown and the actual VM IP of that interface matches. (You can assign static IP in "Primary IP" tab).

12. Similarly, do the above steps for server VM, with subnet properly chosen for one n/w interface and other n/w interface mapped to last subnet where elastic IP would be matched.



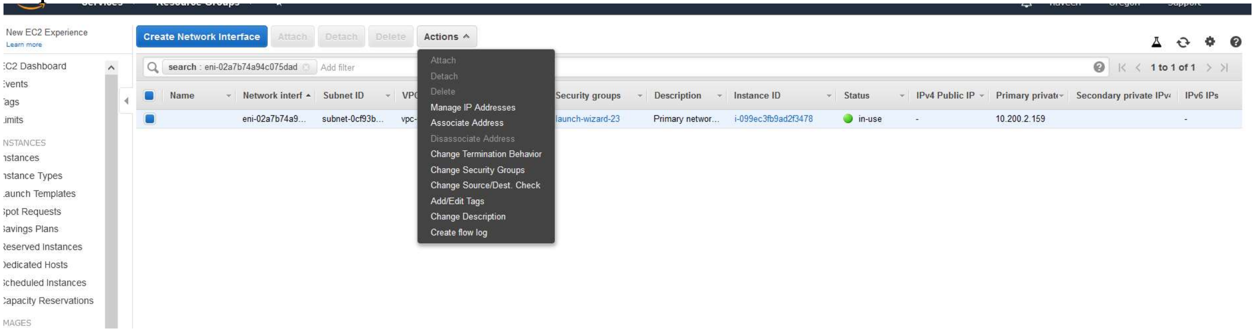
▾ Network interfaces ⓘ

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-02b6170	Auto-assign	Add IP	Add IP
eth1	New network interface	subnet-045eab1	Auto-assign	Add IP	

We can no longer assign a public IP address to your instance
The auto-assign public IP address feature for this instance is disabled because you specified multiple network interfaces. Public IPs can only be assigned to instances with one network interface. To re-enable the auto-assign public IP address feature, please specify only the eth0 network interface.

Now that we have created the topology, its time to login to all of your client, server, vyos VM through SSH. You will observe that there is no user/pass prompt here. This is because we are using certificate which employ asymmetric key cryptography for authentication.

13. Also, you would have to change network interface adapter setting of "Source/dest check" to allow traffic to pass over vyos router. Make this setting to Disable. What does this setting do? Explain.



search : eni-02a7b74a94c075dad

Name	Network interf	Subnet ID	VPC	Security groups	Description	Instance ID	Status	IPv4 Public IP	Primary private	Secondary private IPv	IPv6 IPs
	eni-02a7b74a9...	subnet-0cf93b...	vpc-	launch-wizard-23	Primary networ...	i-099ec3fb9ad2f3478	● in-use	-	10.200.2.159		-

14. Now you would have to change routing table of Client, Server VM to redirect the traffic to VYos VM as by default AWS set's a default route in all of the VM to redirect traffic to its default router. Explore how to do this with help of ip route commands. Ensure ping from client to server VM is passing through vyos VM with help of tcpdump listening on each interface. Explore more on tcpdump command from below:

```
https://opensource.com/article/18/10/introduction-tcpdump
```

15. Can you answer why SSH goes down if IP is changed on that interface?

16. What can be used in vyos Vm to start dhclient in Vyos VM?

17. If interface adapter is not visible in your instance you have to do:

```
 ifconfig <intf> up
```

18. Also check:

`/etc/network/interfaces.d/50-cloud-init.cfg`, for cloud override scripts.
This is how OS get's its IP automatically on AWS.

19. Next step is to install iperf, iperf3 on client, server VM. You would observe that VMs are not able to contact internet. Why is this? Explain. How can you correct it?

To solve it, look at /etc/resolvconf/resolv.conf.d/base file.

20. You would also have to do "sudo apt update". What does this command do?

MEASUREMENT WITH IPERF

1. Execute:

```
iperf3 -s on server VM and iperf3 -u -c <server IP> -b <bw> on
client VM
```

to test bandwidth of your connection over udp. Explore tcp throughput measurement also by using iperf. What is the max throughput and bandwidth you were able to achieve? Why if there is any difference in measurement between these two readings over same link?

2. Now set:

```
sudo tc qdisc add dev eth0 root netem delay 100ms.
```

on client, server VM and again do step 21. Were there any change in readings. If there is a change why is it?. (add -> when first time creating, change -> to update).

3. Now set:

```
sudo tc qdisc change dev eth0 root netem delay 0ms loss 10%
```

and take another measurement. What is your observation.

4. Run

```
dmesg -wH
```

in background to get kernel logs, for observing any kernel errors while you are executing the above commands and for hints to correct it. Also note the mtu of the interface and what is its significance on your readings. (you can change mtu using ifconfig and repeat iperf).

5. Execute:

```
sudo tc qdisc del dev eth1 root
```

for deleting the set configuration.

6. Execute:

```
        sudo tc qdisc add dev eth0 root tbf rate 100mbit latency 1ms burst
9015
```

Then run again step 21. What is your observations? What is the significance of the above command and how it effects performance?

7. Execute

```
sudo ethtool -s eth0 speed 10
```

Did you get any error and why is it not allowed in AWS? Explain.

8. Now delete all the above set configuration on interfaces on client, server VM and do the same steps on vyos VM on interface not mapped to elastic ip. Were you able to get the same observations as before in this configuration? Comment.

Refer below link for more understanding on queuing disciplines in Linux network stack.
https://tldp.org/HOWTO/Traffic-Control-HOWTO/overview.html
https://tldp.org/HOWTO/Traffic-Control-HOWTO/elements.html
https://tldp.org/HOWTO/Traffic-Control-HOWTO/components.html
https://tldp.org/HOWTO/Traffic-Control-HOWTO/classless-qdiscs.html

Make a brief report on your understanding of AWS and how it works along with the commands you have tried out and the issues you have debugged to make it work. Also explain the readings you have got from iperf in different scenarios by executing the above mentioned “tc” commands on Linux. Also, make sure to answer questions posed in the steps mentioned in the document and any errors you have faced which you have resolved.