COS20019 - Cloud Computing Architecture

Week 2: ACF Lab 2: Build a VPC and launch a Web Server

Author: Trac Duc Anh Luong - ID: 103488117

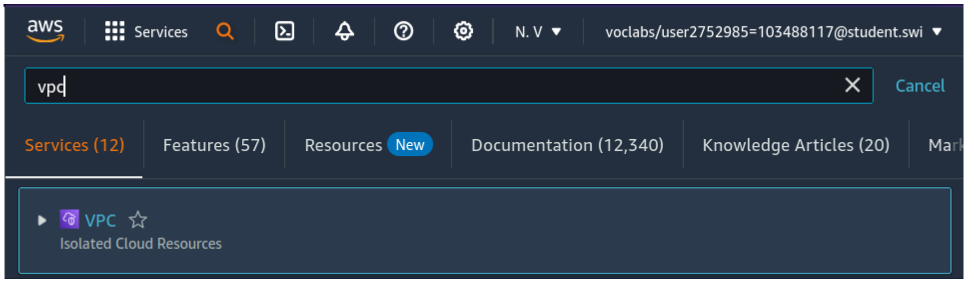
Due Date: 24/09/2023

Name: Trac Duc Anh Luong - ID: 103488117

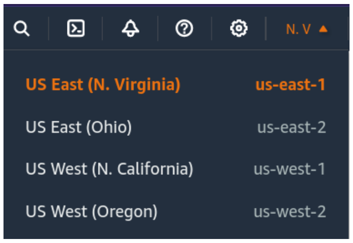
Task 1: Create Your VPC

In this task, you will use the *VPC and more* option in the VPC console to create multiple resources, including a *VPC*, an *Internet Gateway*, a *public subnet* and a *private subnet* in a single Availability Zone, two *route tables*, and a *NAT Gateway*.

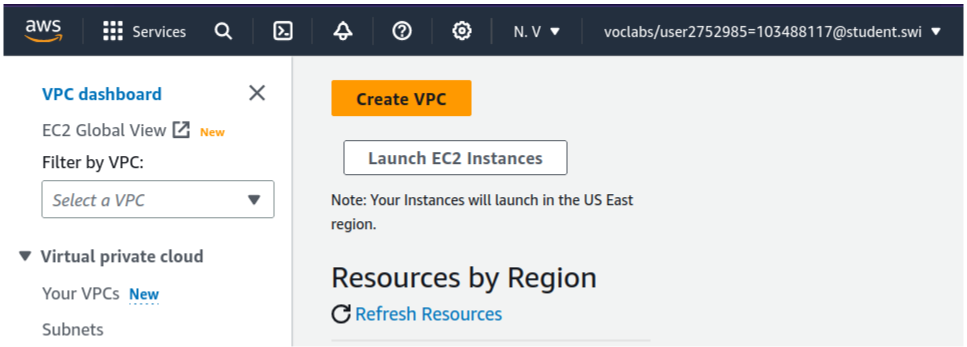
5. In the search box to the right of **Services**, search for and choose **VPC** to open the VPC console.



6. Begin creating a VPC.
   - In the top right of the screen, verify that **N. Virginia (us-east-1)** is the region.


N. V
US East (N. Virginia) us-east-1
US East (Ohio) us-east-2
US West (N. California) us-west-1
US West (Oregon) us-west-2

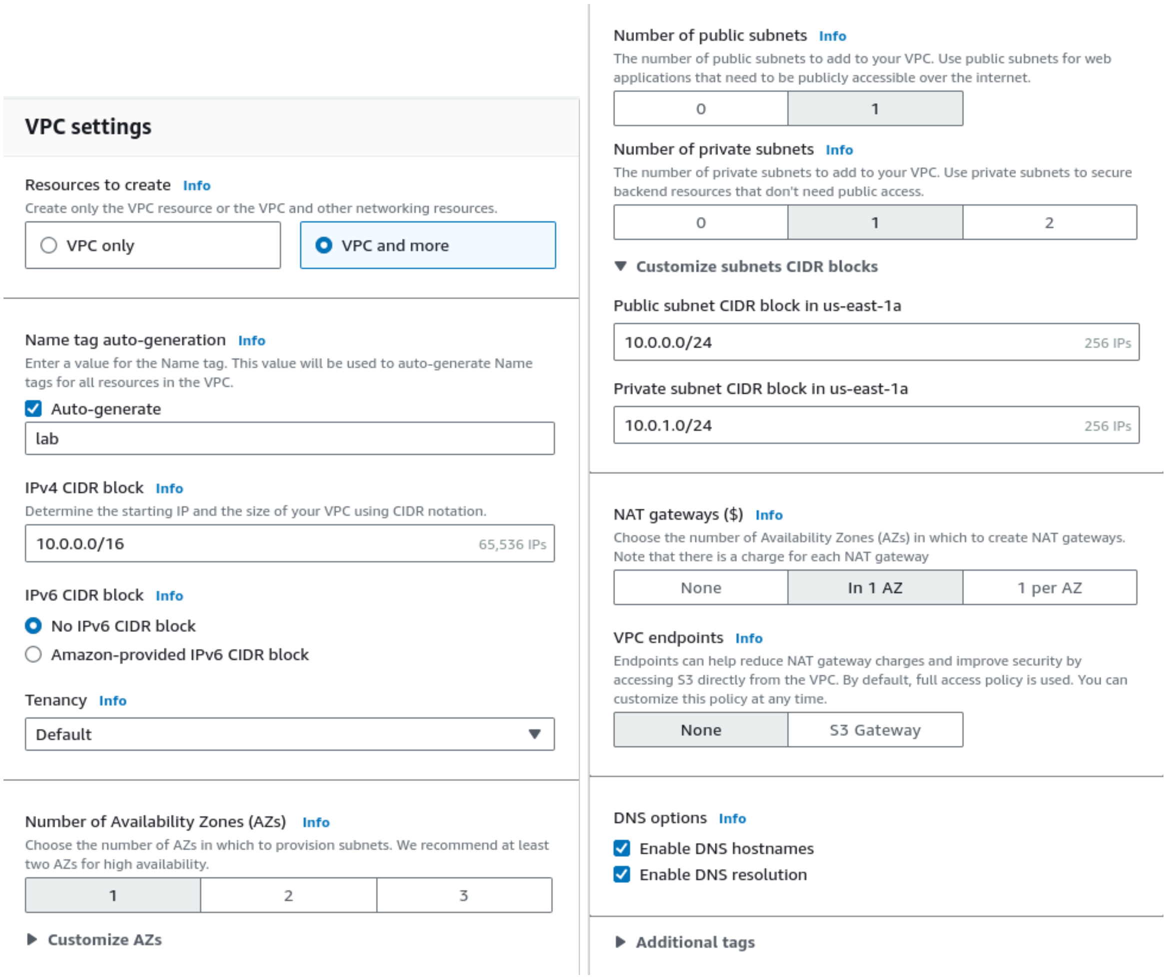
   - Choose the **VPC dashboard** link which is also towards the top left of the console.



   - Next, choose Create VPC.
     Note: If you do not see a button with that name, choose the Launch VPC Wizard button instead.

Name: Trac Duc Anh Luong - ID: 103488117

7. Configure the VPC details in the *VPC settings* panel on the left:
   - Choose **VPC and more**.
   - Under **Name tag auto-generation**, keep *Auto-generate* selected, however change the value from project to `lab`.
   - Keep the **IPv4 CIDR block** set to 10.0.0.0/16
   - For **Number of Availability Zones**, choose **1**.
   - For **Number of *public* subnets**, keep the **1** setting.
   - For **Number of *private* subnets**, keep the **1** setting.
   - Expand the **Customize subnets CIDR blocks** section
     - Change **Public subnet CIDR block in us-east-1a** to `10.0.0.0/24`
     - Change **Private subnet CIDR block in us-east-1a** to `10.0.1.0/24`
   - Set **NAT gateways** to **In 1 AZ**.
   - Set **VPC endpoints** to **None**.
   - Keep both **DNS hostnames** and **DNS resolution** *enabled*.



VPC settings

Resources to create Info
Create only the VPC resource or the VPC and other networking resources.

○ VPC only ● VPC and more

Name tag auto-generation Info
Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

☑ Auto-generate

lab

IPv4 CIDR block Info
Determine the starting IP and the size of your VPC using CIDR notation.

10.0.0.0/16 65,536 IPs

IPv6 CIDR block Info

● No IPv6 CIDR block
○ Amazon-provided IPv6 CIDR block

Tenancy Info

Default ▼

Number of Availability Zones (AZs) Info
Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

[✓ 1] 2 3

▶ Customize AZs

Number of public subnets Info
The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0 [✓ 1]

Number of private subnets Info
The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0 [✓ 1] 2

▼ Customize subnets CIDR blocks

Public subnet CIDR block in us-east-1a

10.0.0.0/24 256 IPs

Private subnet CIDR block in us-east-1a

10.0.1.0/24 256 IPs

NAT gateways ($) Info
Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None [✓ In 1 AZ] 1 per AZ

VPC endpoints Info
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

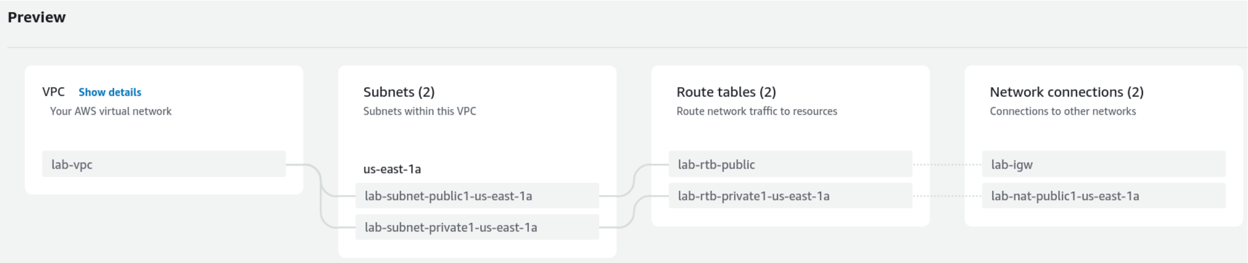
[✓ None] S3 Gateway

DNS options Info

☑ Enable DNS hostnames
☑ Enable DNS resolution

▶ Additional tags

8. In the *Preview* panel on the right, confirm the settings you have configured.
    - **VPC:** `lab-vpc`
    - **Subnets**:
        - us-east-1a
            - ***Public* subnet name:** `lab-subnet-public1-us-east-1a`
            - ***Private* subnet name:** `lab-subnet-private1-us-east-1a`
    - **Route tables**
        - `lab-rtb-public`
        - `lab-rtb-private1-us-east-1a`
    - **Network connections**
        - `lab-igw`
        - `lab-nat-public1-us-east-1a`



Preview

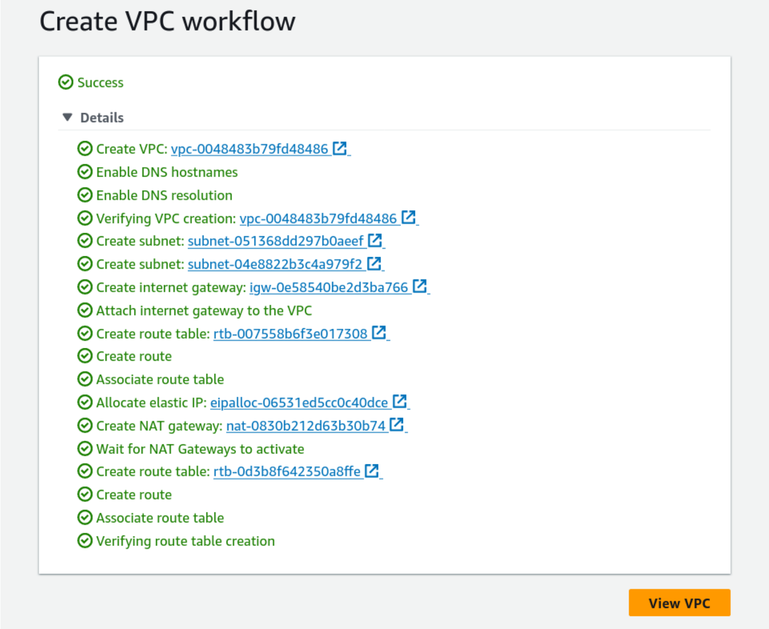
VPC Show details
Your AWS virtual network
lab-vpc

Subnets (2)
Subnets within this VPC
us-east-1a
lab-subnet-public1-us-east-1a
lab-subnet-private1-us-east-1a

Route tables (2)
Route network traffic to resources
lab-rtb-public
lab-rtb-private1-us-east-1a

Network connections (2)
Connections to other networks
lab-igw
lab-nat-public1-us-east-1a

9. At the bottom of the screen, choose Create VPC
   The VPC resources are created. The NAT Gateway will take a few minutes to activate.
   Please wait until *all* the resources are created before proceding to the next step.



Create VPC workflow

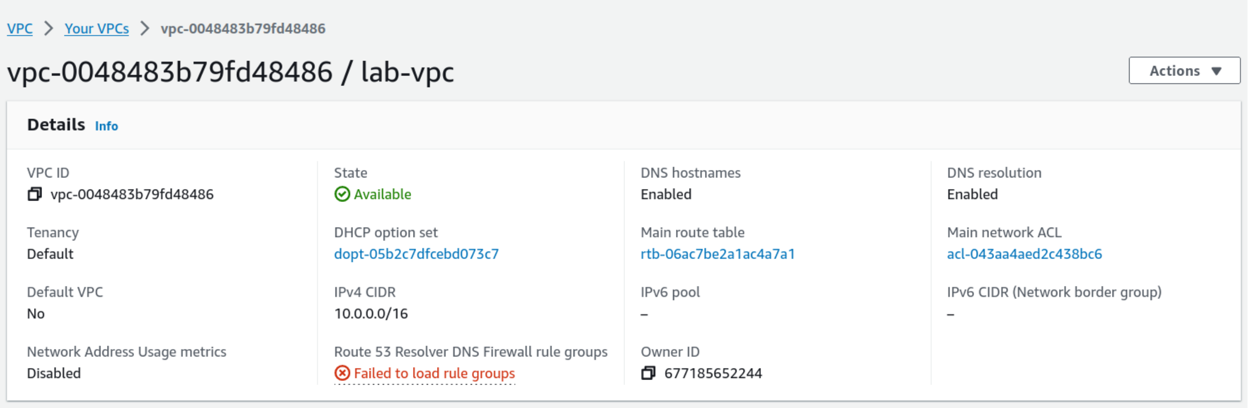
✓ Success

▼ Details

✓ Create VPC: vpc-0048483b79fd48486
✓ Enable DNS hostnames
✓ Enable DNS resolution
✓ Verifying VPC creation: vpc-0048483b79fd48486
✓ Create subnet: subnet-051368dd297b0aeef
✓ Create subnet: subnet-04e8822b3c4a979f2
✓ Create internet gateway: igw-0e58540be2d3ba766
✓ Attach internet gateway to the VPC
✓ Create route table: rtb-007558b6f3e017308
✓ Create route
✓ Associate route table
✓ Allocate elastic IP: eipalloc-06531ed5cc0c40dce
✓ Create NAT gateway: nat-0830b212d63b30b74
✓ Wait for NAT Gateways to activate
✓ Create route table: rtb-0d3b8f642350a8ffe
✓ Create route
✓ Associate route table
✓ Verifying route table creation

Name: Trac Duc Anh Luong - ID: 103488117

10. Once it is complete, choose View VPC



VPC > Your VPCs > vpc-0048483b79fd48486

vpc-0048483b79fd48486 / lab-vpc

Actions ▼

Details Info

VPC ID vpc-0048483b79fd48486	State Available	DNS hostnames Enabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-05b2c7dfcebd073c7	Main route table rtb-06ac7be2a1ac4a7a1	Main network ACL acl-043aa4aed2c438bc6
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool –	IPv6 CIDR (Network border group) –
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups Failed to load rule groups	Owner ID 677185652244	

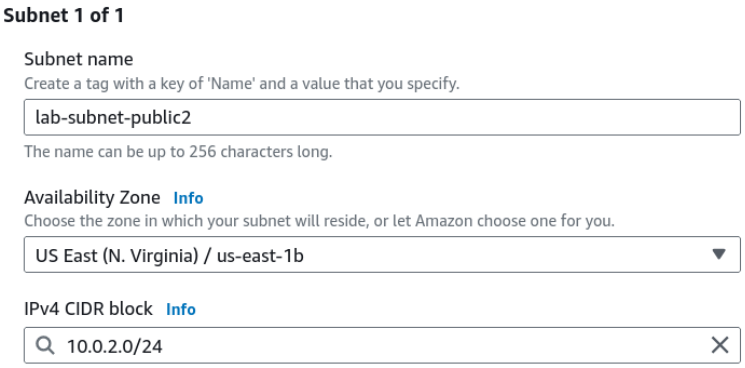
Task 2: Create Additional Subnets

In this task, you will create two additional subnets for the VPC in a second Availability Zone. Having subnets in multiple Availability Zones within a VPC is useful for deploying solutions that provide *High Availability*.

After creating a VPC as you have already done, you can still configure it further, for example, by adding more **subnets**. Each subnet you create resides entirely within one Availability Zone.

11. In the left navigation pane, choose **Subnets**.
    First, you will create a second *public* subnet.

12. Choose Create subnet then configure:
    - **VPC ID: lab-vpc** (select from the menu).
    - **Subnet name:** `lab-subnet-public2`
    - **Availability Zone:** Select the *second* Availability Zone (for example, us-east-1b)
    - **IPv4 CIDR block:** `10.0.2.0/24`



Subnet 1 of 1

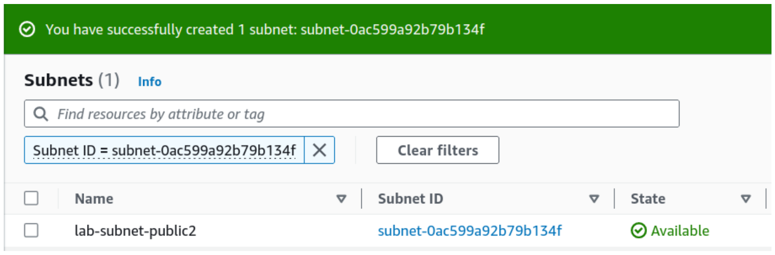
Subnet name
Create a tag with a key of 'Name' and a value that you specify.
lab-subnet-public2
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1b ▼

IPv4 CIDR block Info
10.0.2.0/24

The subnet will have all IP addresses starting with **10.0.2.x**.

13. Choose Create subnet
    The second *public* subnet was created. You will now create a second *private* subnet.



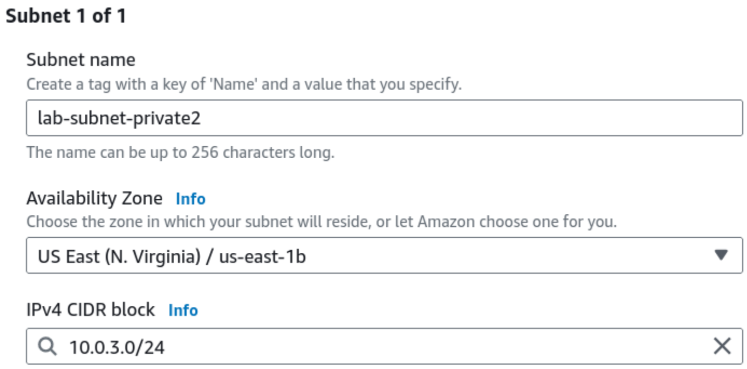
You have successfully created 1 subnet: subnet-0ac599a92b79b134f

Subnets (1) Info

Subnet ID = subnet-0ac599a92b79b134f

	Name	Subnet ID	State
□	lab-subnet-public2	subnet-0ac599a92b79b134f	Available

14. Choose Create subnet then configure:
    - **VPC ID:** `lab-vpc`
    - **Subnet name:** `lab-subnet-private2`
    - **Availability Zone:** Select the *second* Availability Zone (for example, us-east-1b)
    - **IPv4 CIDR block:** `10.0.3.0/24`

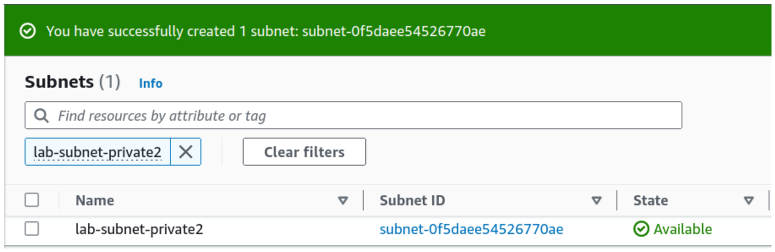


Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
lab-subnet-private2
The name can be up to 256 characters long.

Availability Zone Info
Choose the zone in which your subnet will reside, or let Amazon choose one for you.
US East (N. Virginia) / us-east-1b

IPv4 CIDR block Info
10.0.3.0/24



You have successfully created 1 subnet: subnet-0f5daee54526770ae

Subnets (1) Info

lab-subnet-private2

	Name	Subnet ID	State
□	lab-subnet-private2	subnet-0f5daee54526770ae	Available

The subnet will have all IP addresses starting with **10.0.3.x**.

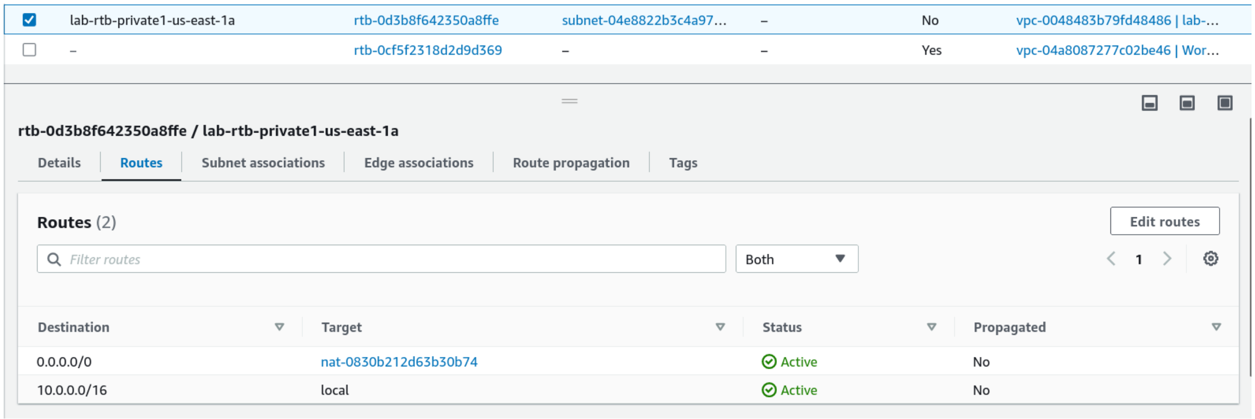
15. Choose Create subnet
    The second *private* subnet was created.
    You will now configure this new *private* subnet to route internet-bound traffic to the NAT Gateway so that resources in the second private subnet are able to connect to the Internet, while still keeping the resources private. This is done by configuring a *Route Table*.
    A *route table* contains a set of rules, called *routes*, that are used to determine where network traffic is directed. Each subnet in a VPC must be associated with a route table; the route table

controls routing for the subnet.

16. In the left navigation pane, choose **Route tables**.

17. Select the **lab-rtb-private1-us-east-1a** route table.

18. In the lower pane, choose the **Routes** tab.
    Note that **Destination 0.0.0.0/0** is set to **Target nat-xxxxxxxx**. This means that traffic destined for the internet (0.0.0.0/0) will be sent to the NAT Gateway. The NAT Gateway will then forward the traffic to the internet.
    This route table is therefore being used to route traffic from private subnets.



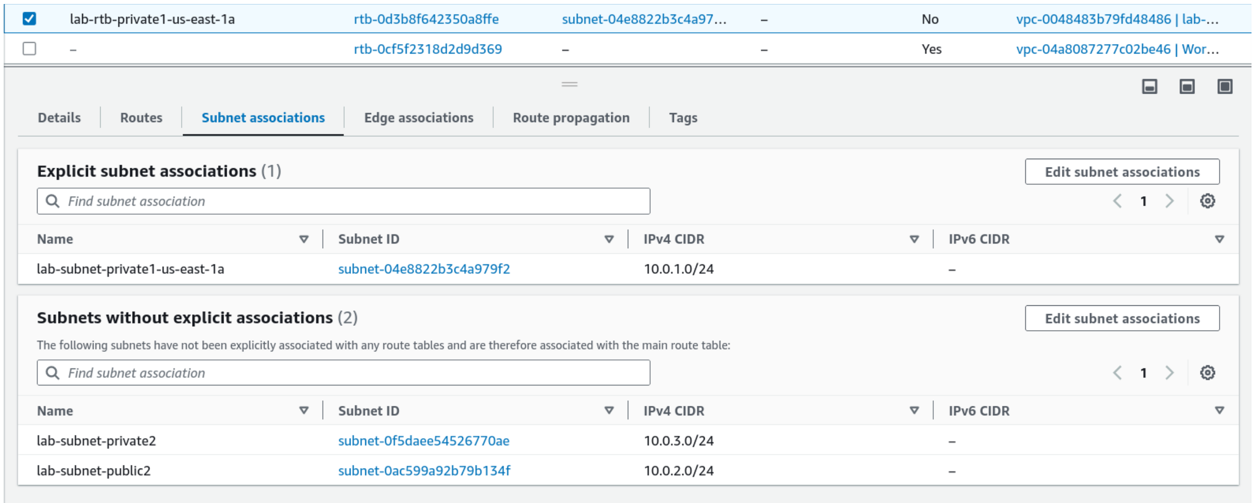
☑	lab-rtb-private1-us-east-1a	rtb-0d3b8f642350a8ffe	subnet-04e8822b3c4a97…	–	No	vpc-0048483b79fd48486 | lab-…
□	–	rtb-0cf5f2318d2d9d369	–	–	Yes	vpc-04a8087277c02be46 | Wor…

rtb-0d3b8f642350a8ffe / lab-rtb-private1-us-east-1a

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	nat-0830b212d63b30b74	✓ Active	No
10.0.0.0/16	local	✓ Active	No

19. Choose the **Subnet associations** tab.
    You created this route table in task 1 when you chose to create a VPC and multiple resources in the VPC. That action also created *lab-subnet-private-1* and associated that subnet with this route table.
    Now that you have created another private subnet, lab-subnet-private-2, you will associate this route table with that subnet as well.



☑	lab-rtb-private1-us-east-1a	rtb-0d3b8f642350a8ffe	subnet-04e8822b3c4a97…	–	No	vpc-0048483b79fd48486 | lab-…
□	–	rtb-0cf5f2318d2d9d369	–	–	Yes	vpc-04a8087277c02be46 | Wor…

Explicit subnet associations (1)

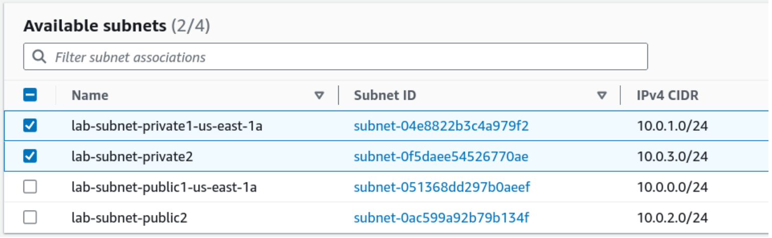
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
lab-subnet-private1-us-east-1a	subnet-04e8822b3c4a979f2	10.0.1.0/24	–

Subnets without explicit associations (2)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
lab-subnet-private2	subnet-0f5daee54526770ae	10.0.3.0/24	–
lab-subnet-public2	subnet-0ac599a92b79b134f	10.0.2.0/24	–

20. In the Explicit subnet associations panel, choose Edit subnet associations
21. Leave **lab-subnet-private1-us-east-1a** selected, but also select **lab-subnet-private2**.



Available subnets (2/4)

Filter subnet associations

☐	Name	Subnet ID	IPv4 CIDR
☑	lab-subnet-private1-us-east-1a	subnet-04e8822b3c4a979f2	10.0.1.0/24
☑	lab-subnet-private2	subnet-0f5daee54526770ae	10.0.3.0/24
☐	lab-subnet-public1-us-east-1a	subnet-051368dd297b0aeef	10.0.0.0/24
☐	lab-subnet-public2	subnet-0ac599a92b79b134f	10.0.2.0/24

22. Choose Save associations

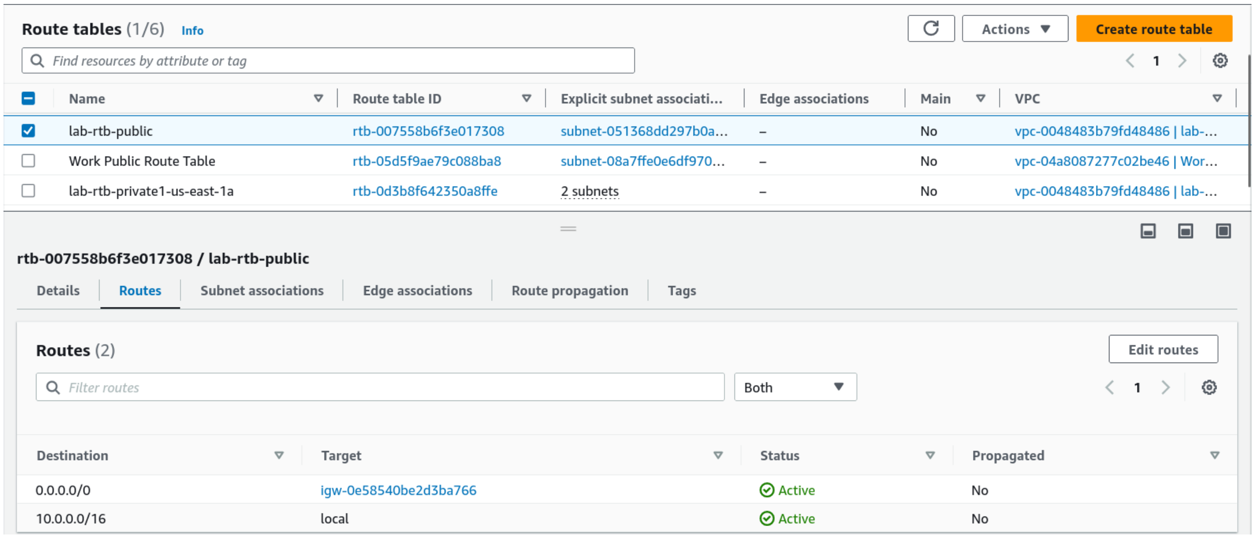
You will now configure the Route Table that is used by the Public Subnets.

23. Select the **lab-rtb-public** route table (and deselect any other subnets).

24. In the lower pane, choose the **Routes** tab.

Note that **Destination 0.0.0.0/0** is set to Target **igw-xxxxxxxx**, which is an Internet Gateway. This means that internet-bound traffic will be sent straight to the internet via this Internet Gateway.

You will now associate this route table to the second public subnet you created.



Route tables (1/6)

Find resources by attribute or tag

☐	Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC
☑	lab-rtb-public	rtb-007558b6f3e017308	subnet-051368dd297b0a...	–	No	vpc-0048483b79fd48486 | lab-...
☐	Work Public Route Table	rtb-05d5f9ae79c088ba8	subnet-08a7ffe0e6df970...	–	No	vpc-04a8087277c02be46 | Wor...
☐	lab-rtb-private1-us-east-1a	rtb-0d3b8f642350a8ffe	2 subnets	–	No	vpc-0048483b79fd48486 | lab-...

rtb-007558b6f3e017308 / lab-rtb-public

Routes (2)

Filter routes

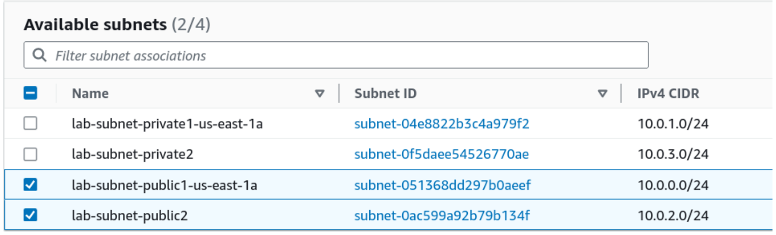
Both

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0e58540be2d3ba766	Active	No
10.0.0.0/16	local	Active	No

25. Choose the **Subnet associations** tab.

26. In the Explicit subnet associations area, choose Edit subnet associations

27. Leave **lab-subnet-public1-us-east-1a** selected, but also select **lab-subnet-public2**.



Available subnets (2/4)

Filter subnet associations

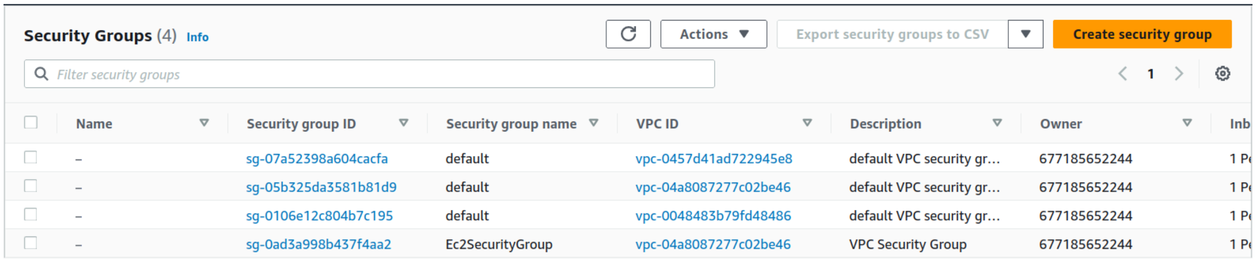
☐	Name	Subnet ID	IPv4 CIDR
☐	lab-subnet-private1-us-east-1a	subnet-04e8822b3c4a979f2	10.0.1.0/24
☐	lab-subnet-private2	subnet-0f5daee54526770ae	10.0.3.0/24
☑	lab-subnet-public1-us-east-1a	subnet-051368dd297b0aeef	10.0.0.0/24
☑	lab-subnet-public2	subnet-0ac599a92b79b134f	10.0.2.0/24

28. Choose Save associations
    Your VPC now has public and private subnets configured in two Availability Zones. The route tables you created in task 1 have also been updated to route network traffic for the two new subnets.

Task 3: Create a VPC Security Group

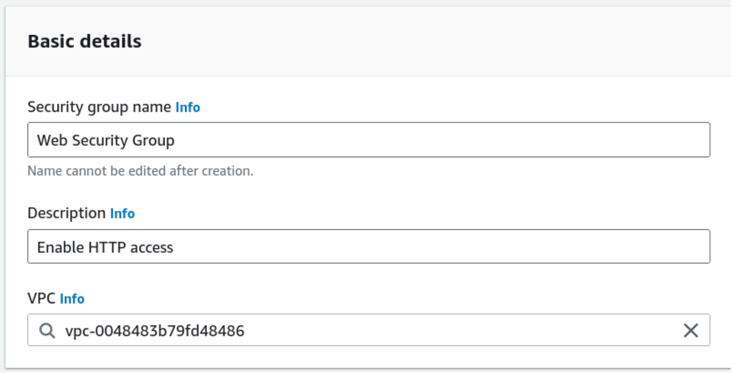
In this task, you will create a VPC security group, which acts as a virtual firewall. When you launch an instance, you associate one or more security groups with the instance. You can add rules to each security group that allow traffic to or from its associated instances.

29. In the left navigation pane, choose **Security groups**.



□	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inb
□	–	sg-07a52398a604cacfa	default	vpc-0457d41ad722945e8	default VPC security gr...	677185652244	1 P
□	–	sg-05b325da3581b81d9	default	vpc-04a8087277c02be46	default VPC security gr...	677185652244	1 P
□	–	sg-0106e12c804b7c195	default	vpc-0048483b79fd48486	default VPC security gr...	677185652244	1 P
□	–	sg-0ad3a998b437f4aa2	Ec2SecurityGroup	vpc-04a8087277c02be46	VPC Security Group	677185652244	1 P

30. Choose Create security group and then configure:
    - **Security group name:** `Web Security Group`
    - **Description:** `Enable HTTP access`
    - **VPC:** choose the X to remove the currently selected VPC, then from the drop down list choose **lab-vpc**



Basic details

Security group name Info
Web Security Group
Name cannot be edited after creation.

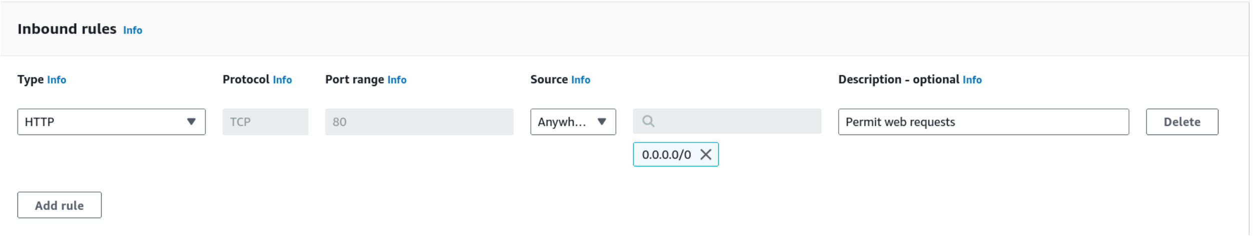
Description Info
Enable HTTP access

VPC Info
vpc-0048483b79fd48486

31. In the **Inbound rules** pane, choose Add rule

32. Configure the following settings:
    - **Type:** *HTTP*
    - **Source:** *Anywhere-IPv4*
    - **Description:** `Permit web requests`

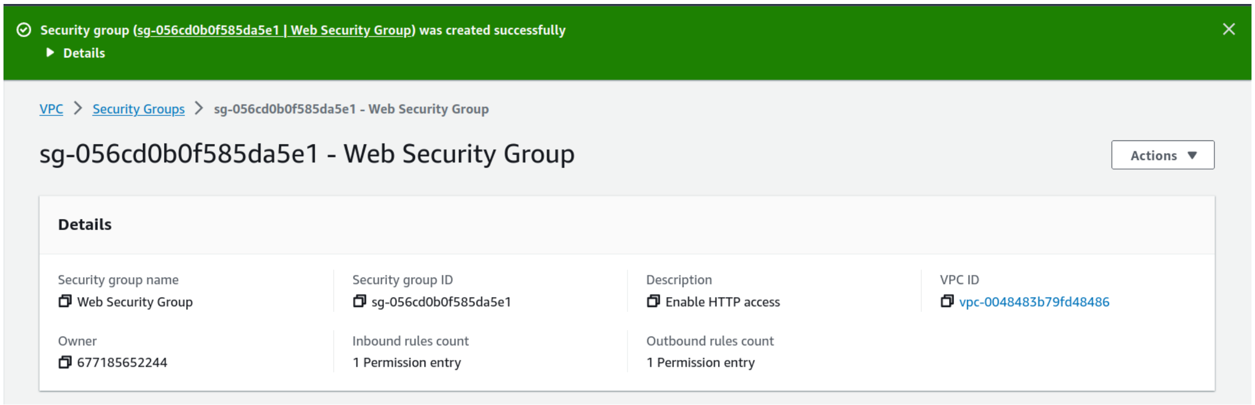
Name: Trac Duc Anh Luong - ID: 103488117



Inbound rules Info

Type	Protocol	Port range	Source		Description - optional
HTTP	TCP	80	Anywh...	0.0.0.0/0	Permit web requests

33. Scroll to the bottom of the page and choose Create security group
    You will use this security group in the next task when launching an Amazon EC2 instance.



Security group (sg-056cd0b0f585da5e1 | Web Security Group) was created successfully

Details
VPC > Security Groups > sg-056cd0b0f585da5e1 - Web Security Group
Actions

sg-056cd0b0f585da5e1 - Web Security Group

Details

Security group name: Web Security Group

Security group ID: sg-056cd0b0f585da5e1

Description: Enable HTTP access

VPC ID: vpc-0048483b79fd48486

Owner: 677185652244

Inbound rules count: 1 Permission entry

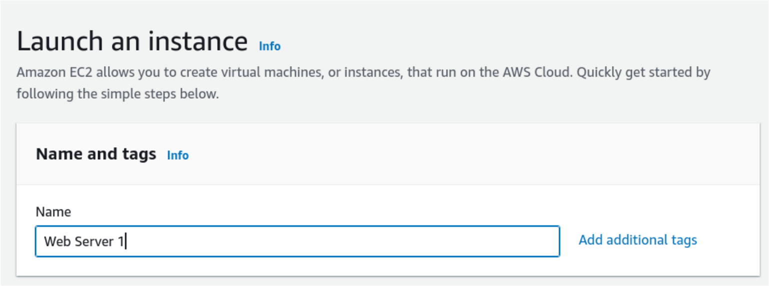
Outbound rules count: 1 Permission entry

Name: Trac Duc Anh Luong - ID: 103488117

Task 4: Launch a Web Server Instance

In this task, you will launch an Amazon EC2 instance into the new VPC. You will configure the instance to act as a web server.

34. In the search box to the right of **Services**, search for and choose **EC2** to open the EC2 console.
35. From the Launch instance menu choose **Launch instance**.
36. Name the instance:
    - Give it the name `Web Server 1`
      When you name your instance, AWS creates a tag and associates it with the instance. A tag is a key value pair. The key for this pair is ***Name***, and the value is the name you enter for your EC2 instance.



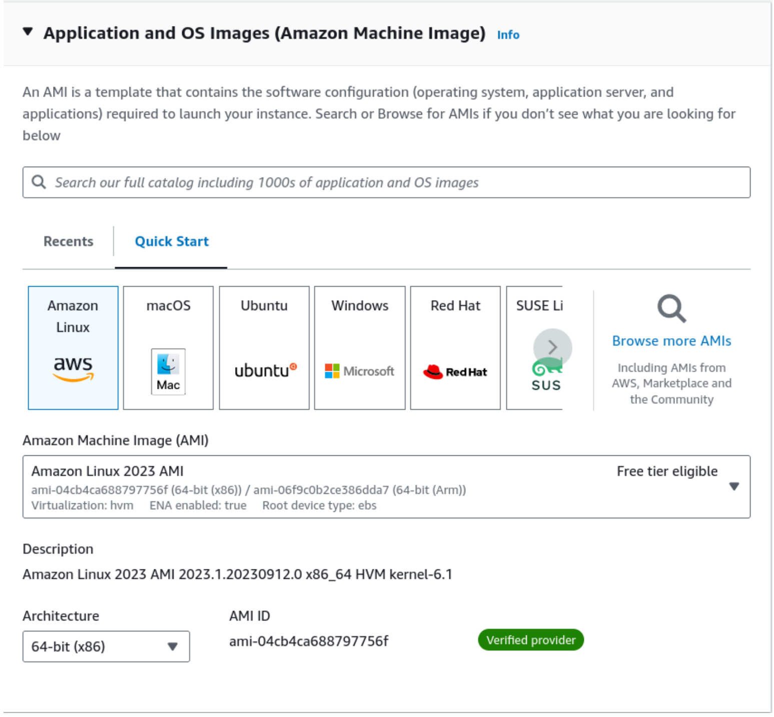
Launch an instance Info

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

Name and tags Info

Name: Web Server 1

37. Choose an AMI from which to create the instance:
    - In the list of available *Quick Start* AMIs, keep the default **Amazon Linux** selected.
    - Also keep the default **Amazon Linux 2023 AMI** selected.
      The type of *Amazon Machine Image (AMI)* you choose determines the Operating System that will run on the EC2 instance that you launch.



▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
aws
macOS
Mac
Ubuntu
ubuntu
Windows
Microsoft
Red Hat
Red Hat
SUSE Li
SUS
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI — Free tier eligible
ami-04cb4ca688797756f (64-bit (x86)) / ami-06f9c0b2ce386dda7 (64-bit (Arm))
Virtualization: hvm   ENA enabled: true   Root device type: ebs

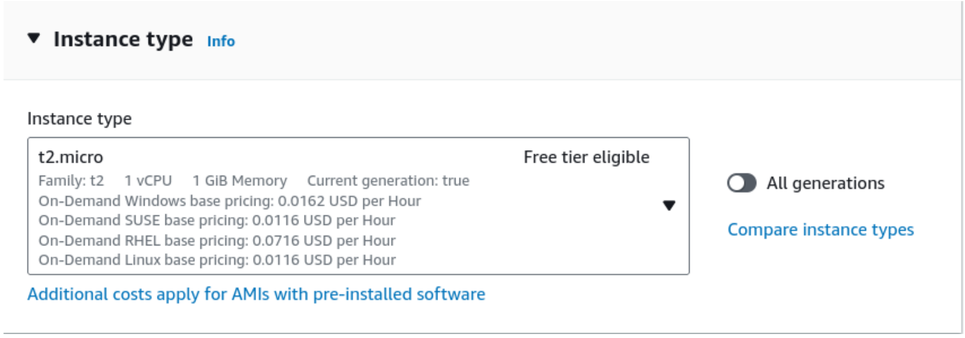
Description

Amazon Linux 2023 AMI 2023.1.20230912.0 x86_64 HVM kernel-6.1

Architecture: 64-bit (x86)

AMI ID: ami-04cb4ca688797756f

38. Choose an Instance type:
    - In the *Instance type* panel, keep the default **t2.micro** selected.
      The *Instance Type* defines the hardware resources assigned to the instance.

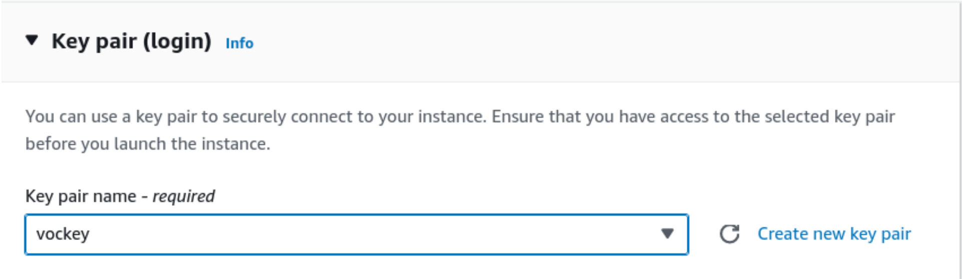


Instance type Info

Instance type

t2.micro Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

39. Select the key pair to associate with the instance:
    - From the **Key pair name** menu, select **vockey**.
      The vockey key pair you selected will allow you to connect to this instance via SSH after it has launched. Although you will not need to do that in this lab, it is still required to identify an existing key pair, or create a new one, when you launch an instance.



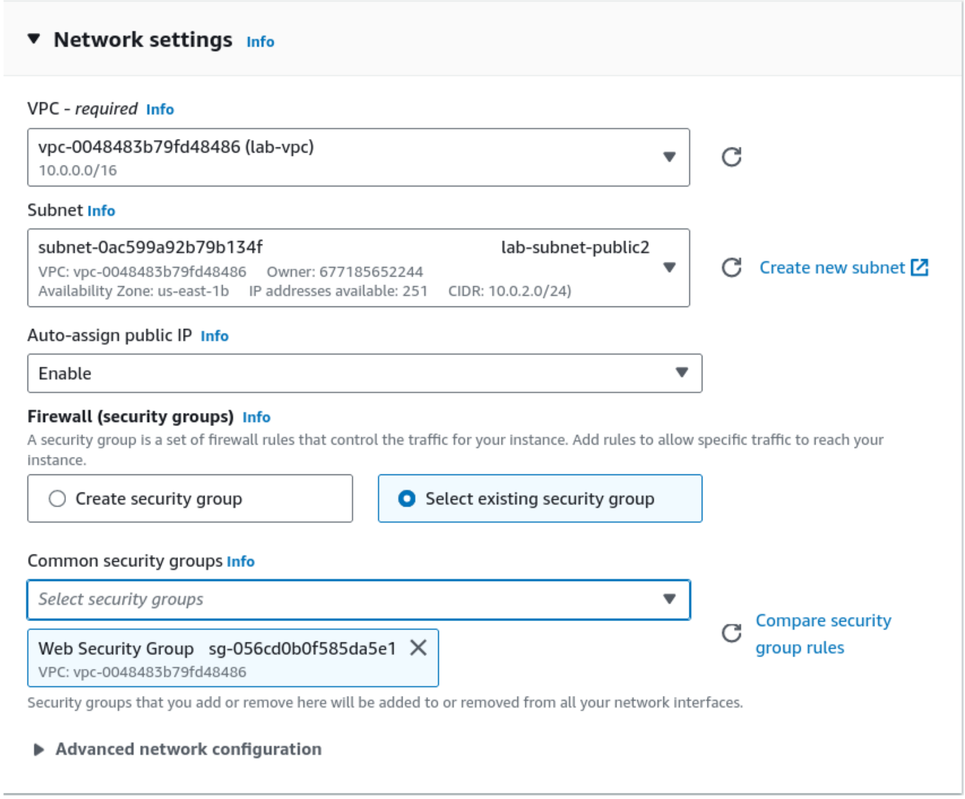
Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

vockey

40. Configure the Network settings:
    - Next to Network settings, choose **Edit**, then configure:
        - **Network:** *lab-vpc*
        - **Subnet:** *lab-subnet-public2* (*not* Private!)
        - **Auto-assign public IP:** *Enable*
    - Next, you will configure the instance to use the *Web Security Group* that you created earlier.
        - Under Firewall (security groups), choose **Select existing security group**.
        - For **Common security groups**, select **Web Security Group**.
          This security group will permit HTTP access to the instance.



▼ **Network settings** Info

VPC - *required* Info

vpc-0048483b79fd48486 (lab-vpc)
10.0.0.0/16

Subnet Info

subnet-0ac599a92b79b134f lab-subnet-public2
VPC: vpc-0048483b79fd48486 Owner: 677185652244
Availability Zone: us-east-1b IP addresses available: 251 CIDR: 10.0.2.0/24)

Create new subnet

Auto-assign public IP Info

Enable

Firewall (security groups) Info

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

○ Create security group ● Select existing security group

Common security groups Info

Select security groups

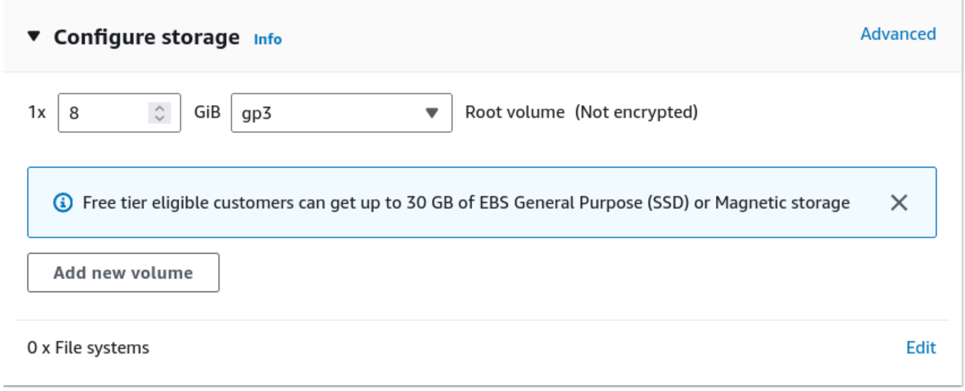
Web Security Group sg-056cd0b0f585da5e1
VPC: vpc-0048483b79fd48486

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

▶ **Advanced network configuration**

41. In the *Configure storage* section, keep the default settings.
    Note: The default settings specify that the *root volume* of the instance, which will host the Amazon Linux guest operating system that you specified earlier, will run on a general purpose SSD (*gp3*) hard drive that is 8 GiB in size. You could alternatively add more storage volumes, however that is not needed in this lab.



▼ **Configure storage** Info

Advanced

1x 8 GiB gp3 Root volume (Not encrypted)

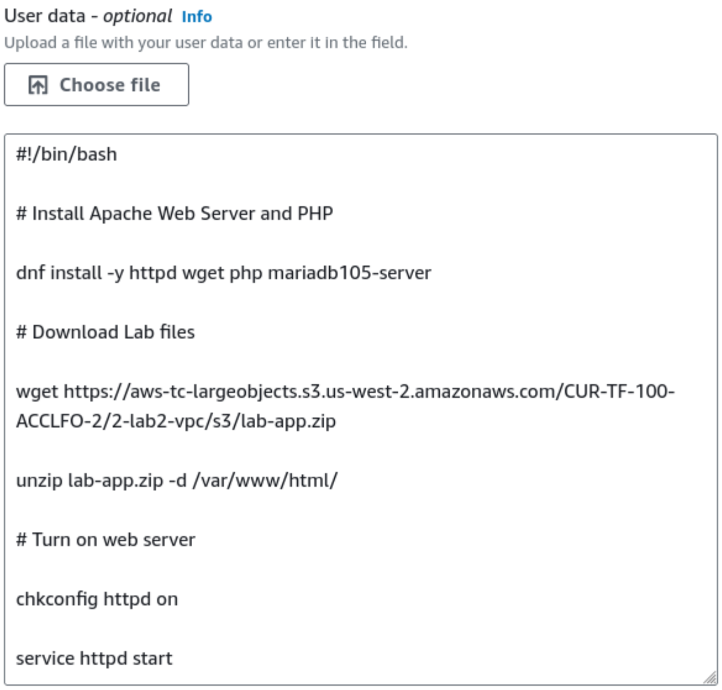
Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

Add new volume

0 x File systems

Edit

42. Configure a script to run on the instance when it launches:
    - Expand the **Advanced details** panel.
    - Scroll to the bottom of the page and then copy and paste the code shown below into the **User data** box:



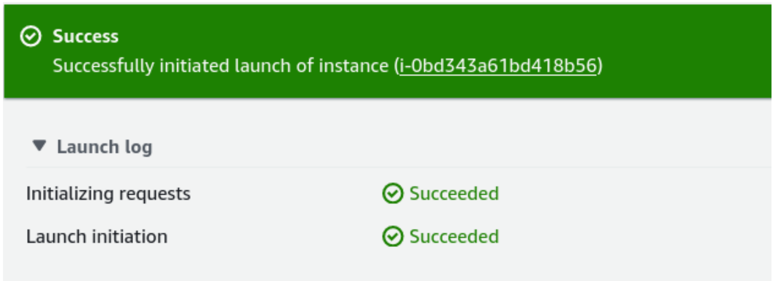
User data - *optional* Info

Upload a file with your user data or enter it in the field.

```
#!/bin/bash

# Install Apache Web Server and PHP

dnf install -y httpd wget php mariadb105-server

# Download Lab files

wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-100-ACCLFO-2/2-lab2-vpc/s3/lab-app.zip

unzip lab-app.zip -d /var/www/html/

# Turn on web server

chkconfig httpd on

service httpd start
```

- This script will run with root user permissions on the guest OS of the instance. It will run automatically when the instance launches for the first time. The script installs a web server, a database, and PHP libraries, and then it downloads and installs a PHP web application on the web server.

43. At the bottom of the **Summary** panel on the right side of the screen choose Launch instance You will see a Success message.



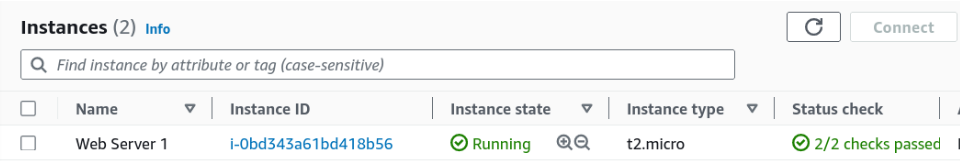
Success

Successfully initiated launch of instance (i-0bd343a61bd418b56)

Initializing requests	✓ Succeeded
Launch initiation	✓ Succeeded

44. Choose View all instances

45. Wait until **Web Server 1** shows *2/2 checks passed* in the **Status check** column.
 This may take a few minutes. Choose the refresh icon at the top of the page every 30 seconds or so to more quickly become aware of the latest status of the instance.
You will now connect to the web server running on the EC2 instance.



Instances (2) Info

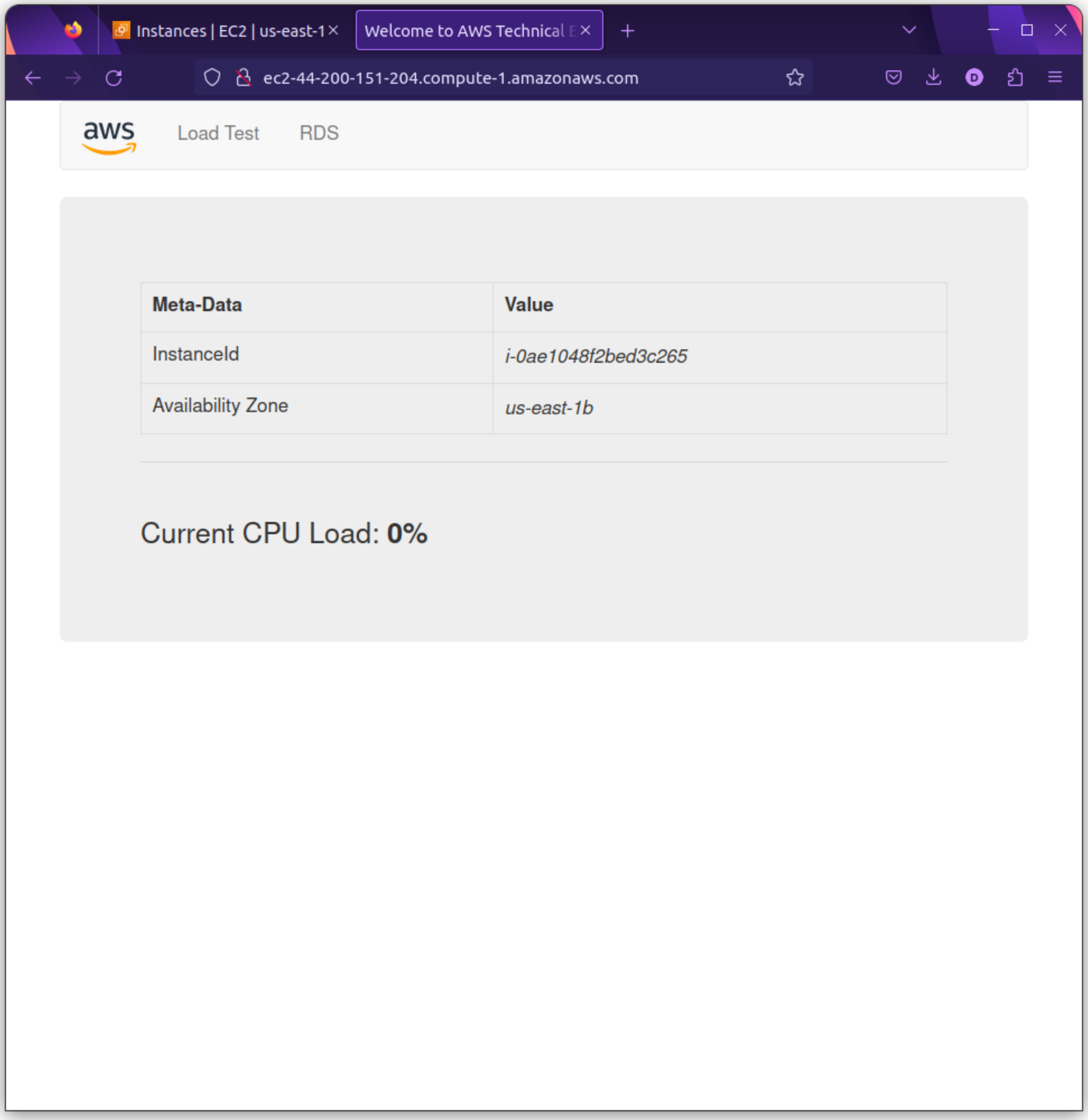
□	Name	Instance ID	Instance state	Instance type	Status check
□	Web Server 1	i-0bd343a61bd418b56	✓ Running	t2.micro	✓ 2/2 checks passed

Name: Trac Duc Anh Luong - ID: 103488117

46. Select **Web Server 1**.

47. Copy the **Public IPv4 DNS** value shown in the **Details** tab at the bottom of the page.

48. Open a new web browser tab, paste the **Public DNS** value and press Enter.
    You should see a web page displaying the AWS logo and instance meta-data values.


Instances | EC2 | us-east-1
Welcome to AWS Technical E
ec2-44-200-151-204.compute-1.amazonaws.com
aws
Load Test
RDS

Meta-Data	Value
InstanceId	*i-0ae1048f2bed3c265*
Availability Zone	*us-east-1b*

Current CPU Load: **0%**