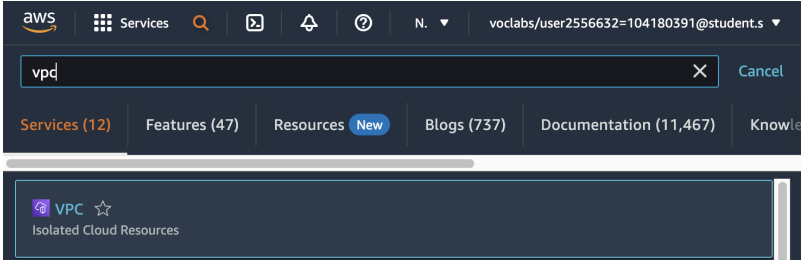
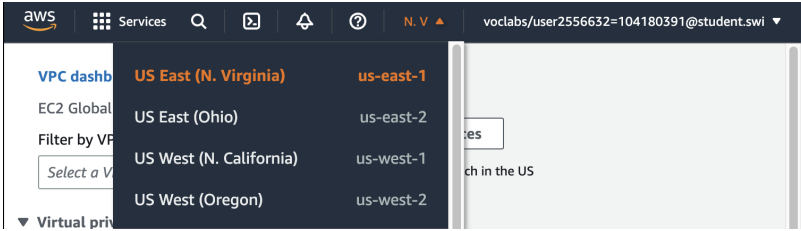
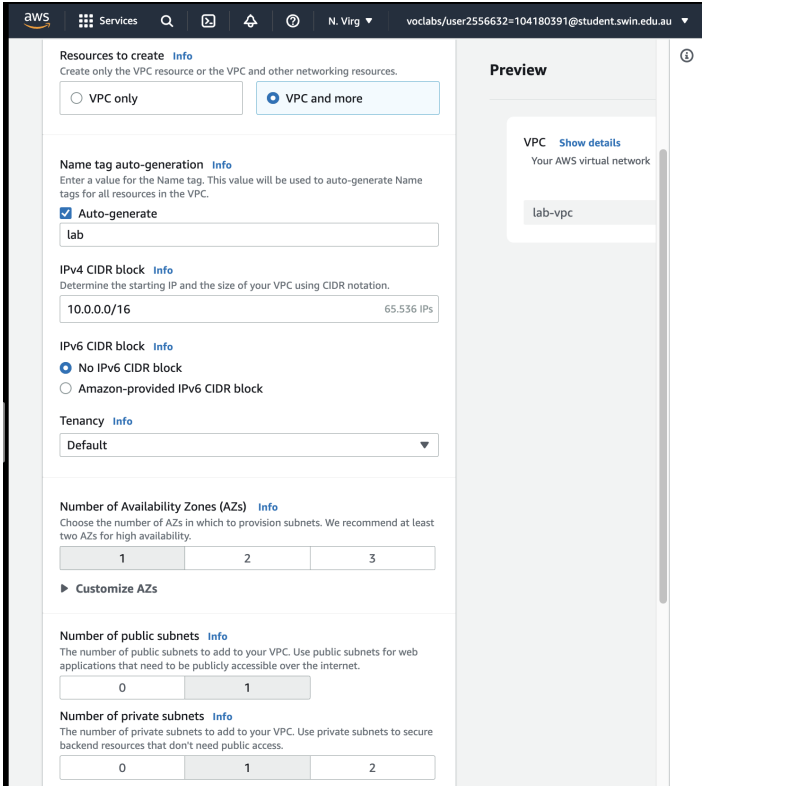



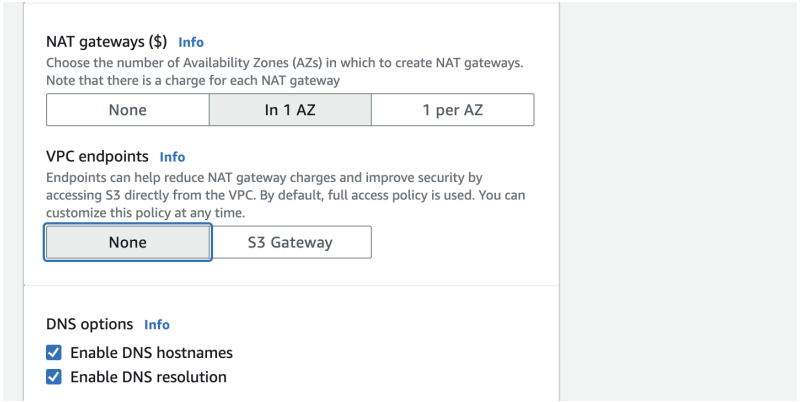
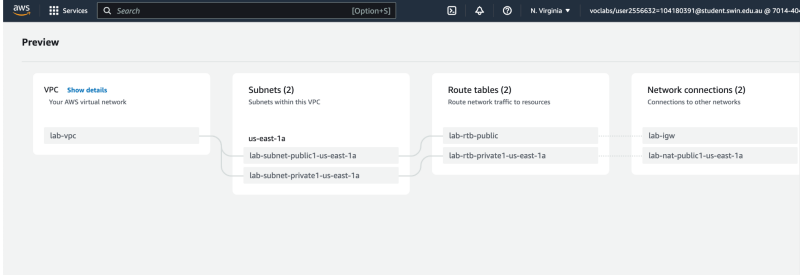


Week 3: ACF Lab 2: Build your VPC and Launch a Web Server

May 27, 2023

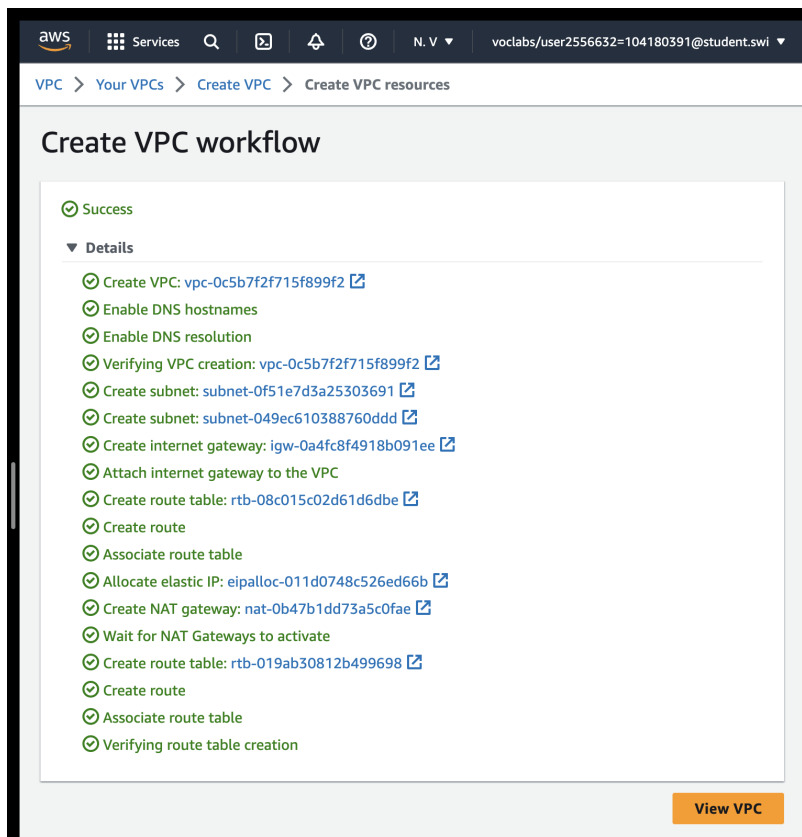
Luu Tuan Hoang
Student ID: 104180391

Step	Description	Screenshot
1	Open the VPC console to create a new VPC by searching in the search bar.	
2	Ensure that N. Virginia (us-east-1) is the region.	
3	Choose Create VPC to begin creating a new VPC	
4	Configure the VPC details in the VPC settings panel on the left: <ul style="list-style-type: none"> - 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 standard 1 setting. - For Number of private subnets, keep the standard 1 setting. 	

5	<p>Expand the Customize subnets CIDR blocks section</p> <ul style="list-style-type: none">- 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	
6	<ul style="list-style-type: none">- Set NAT gateways to In 1 AZ.- Set VPC endpoints to None.- Keep both DNS hostnames and DNS resolution enabled.	
7	<p>Preview panel of the VPC, choose Create VPC.</p>	

8

VPC successfully created.



aws Services 🔍 📄 🔔 ⓘ N. V ▼ voclabs/user2556632=104180391@student.swi ▼

VPC > Your VPCs > Create VPC > Create VPC resources

Create VPC workflow

✔ Success

▼ Details

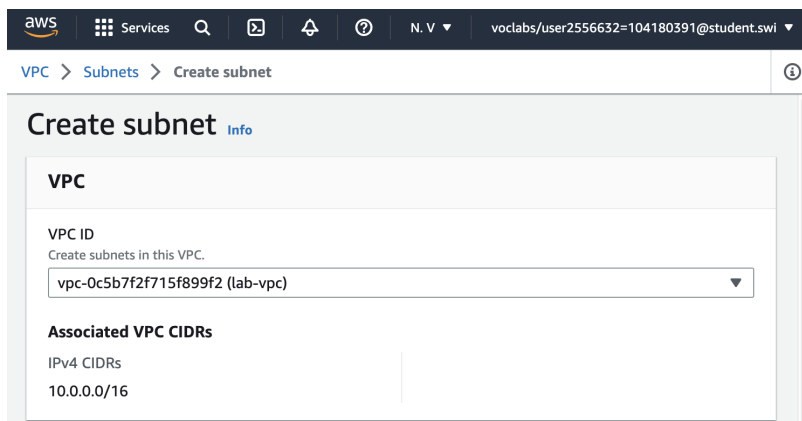
- ✔ Create VPC: [vpc-0c5b7f2f715f899f2](#)
- ✔ Enable DNS hostnames
- ✔ Enable DNS resolution
- ✔ Verifying VPC creation: [vpc-0c5b7f2f715f899f2](#)
- ✔ Create subnet: [subnet-0f51e7d3a25303691](#)
- ✔ Create subnet: [subnet-049ec610388760ddd](#)
- ✔ Create internet gateway: [igw-0a4fc8f4918b091ee](#)
- ✔ Attach internet gateway to the VPC
- ✔ Create route table: [rtb-08c015c02d61d6dbe](#)
- ✔ Create route
- ✔ Associate route table
- ✔ Allocate elastic IP: [eipalloc-011d0748c526ed66b](#)
- ✔ Create NAT gateway: [nat-0b47b1dd73a5c0fae](#)
- ✔ Wait for NAT Gateways to activate
- ✔ Create route table: [rtb-019ab30812b499698](#)
- ✔ Create route
- ✔ Associate route table
- ✔ Verifying route table creation

[View VPC](#)

9

In the left navigation pane, choose **Subnets**. Firstly, create a public subnet.

Choose Create subnet then configure: VPC ID: lab-vpc (select from the menu).



aws Services 🔍 📄 🔔 ⓘ N. V ▼ voclabs/user2556632=104180391@student.swi ▼

VPC > Subnets > Create subnet ⓘ

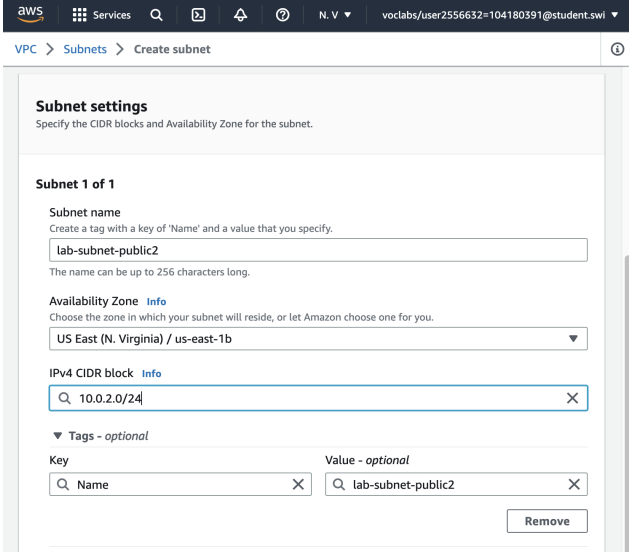
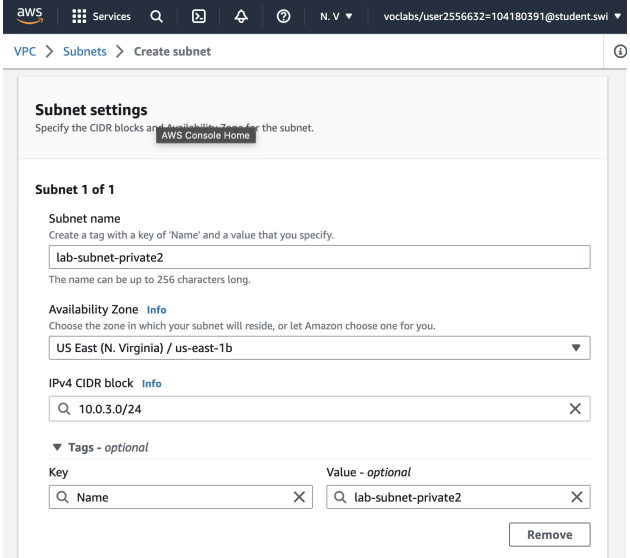
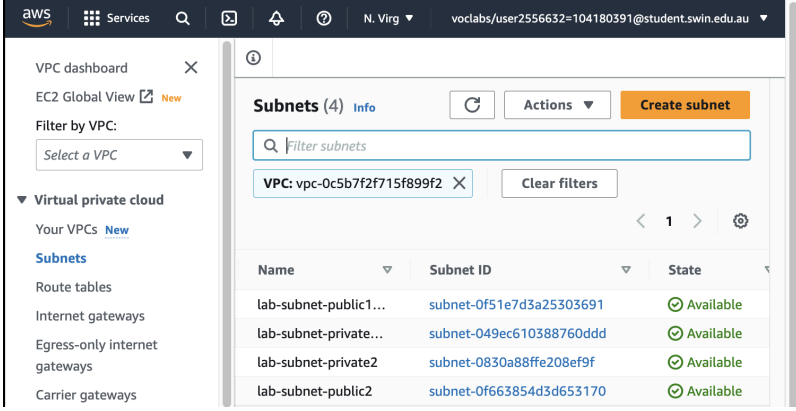
Create subnet Info

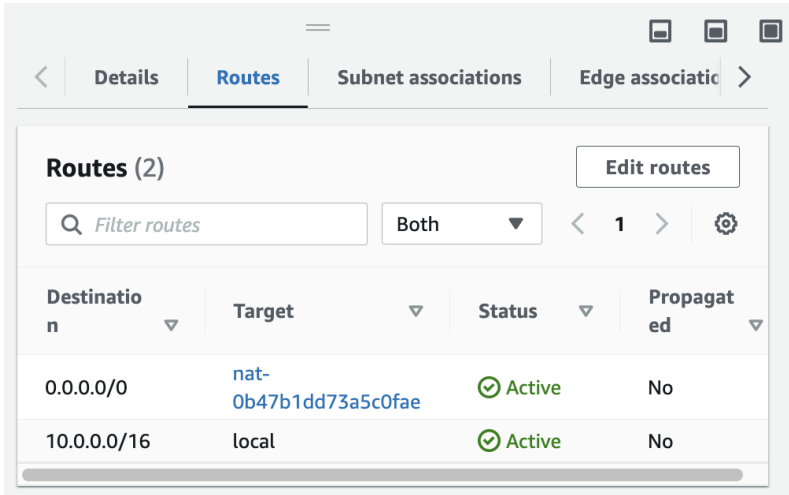
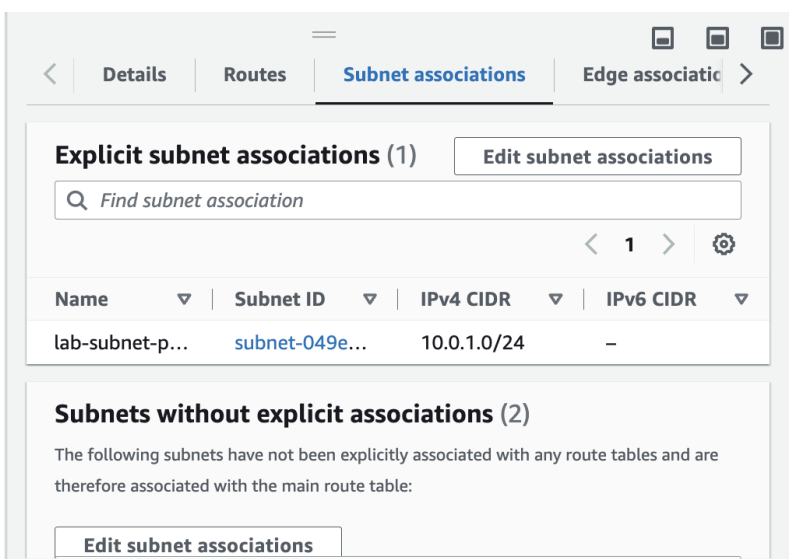
VPC

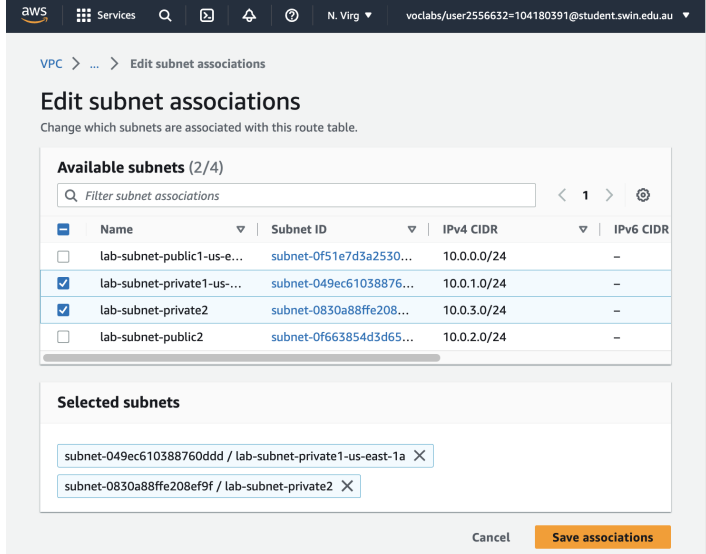
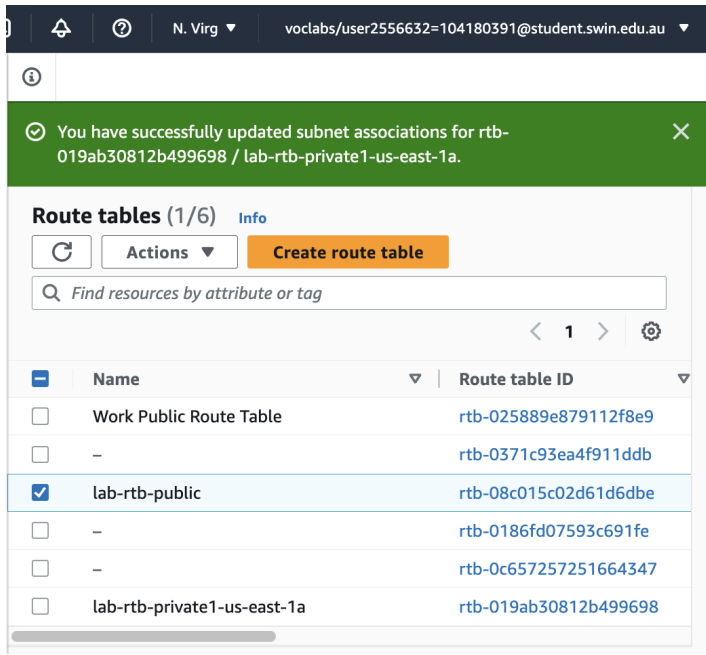
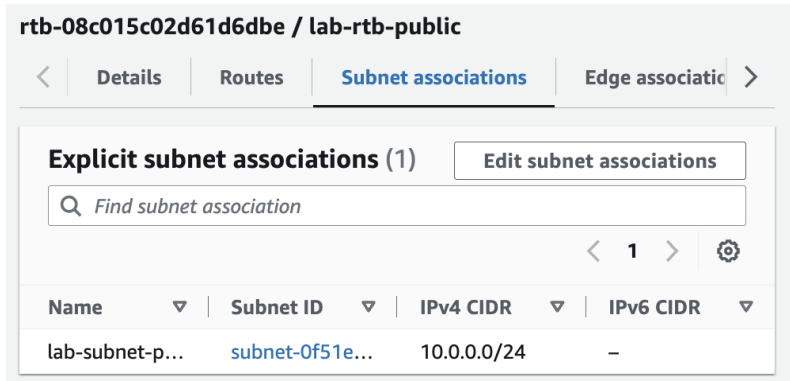
VPC ID
Create subnets in this VPC.
[vpc-0c5b7f2f715f899f2 \(lab-vpc\)](#) ▼

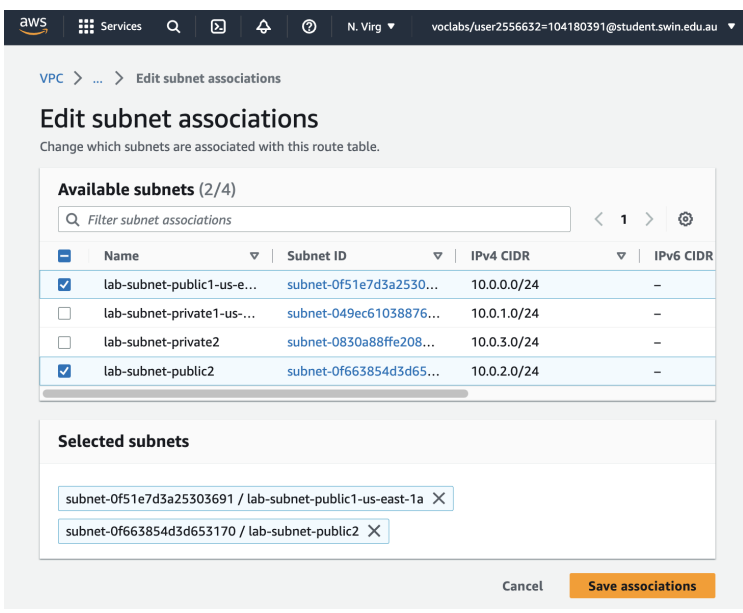
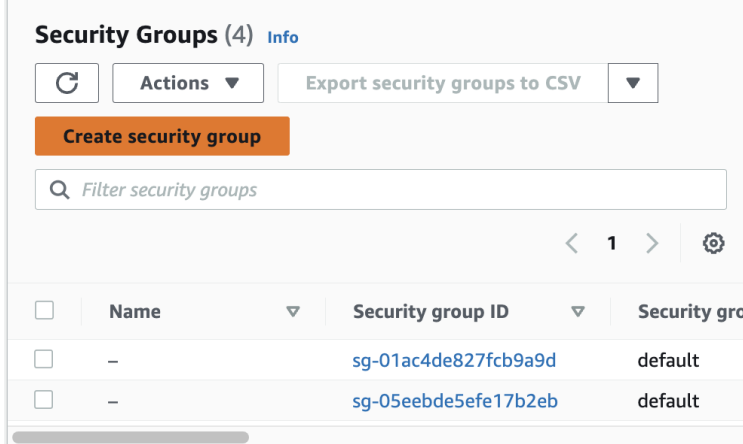
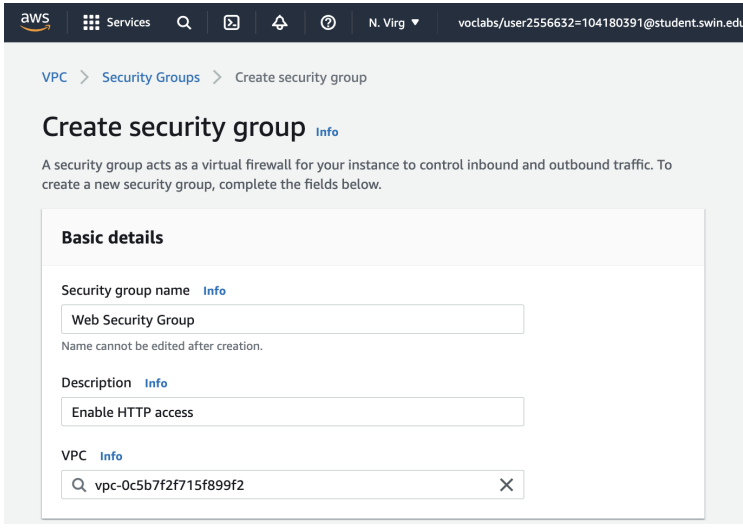
Associated VPC CIDRs

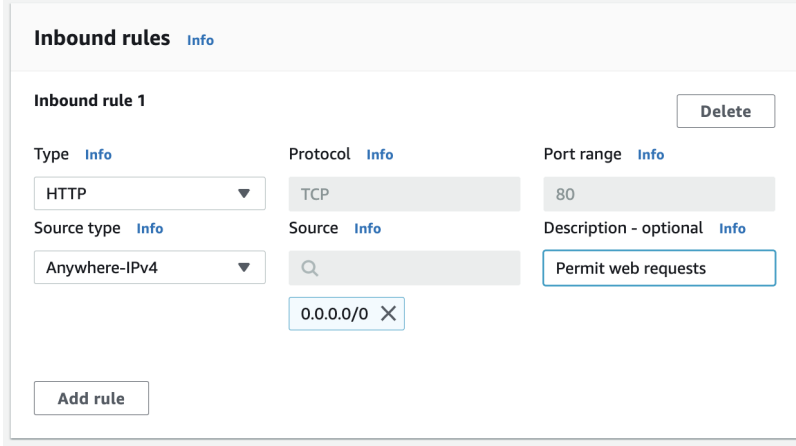
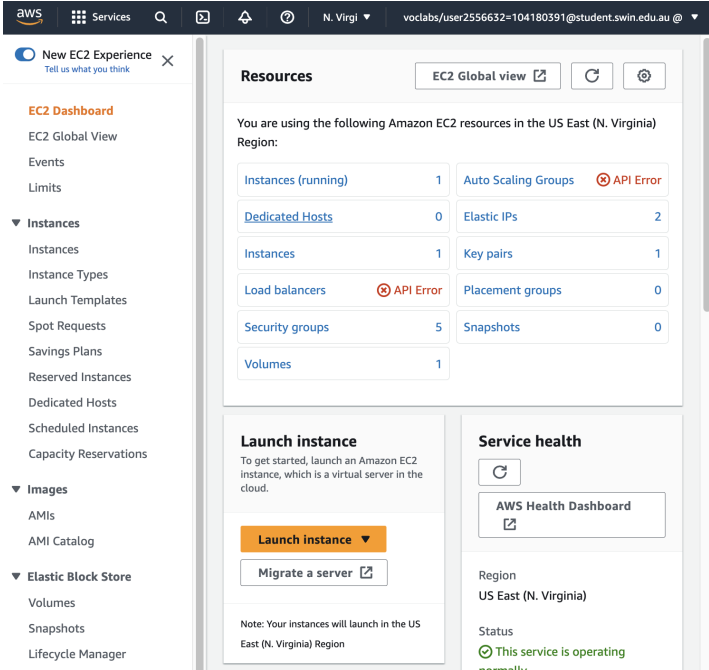
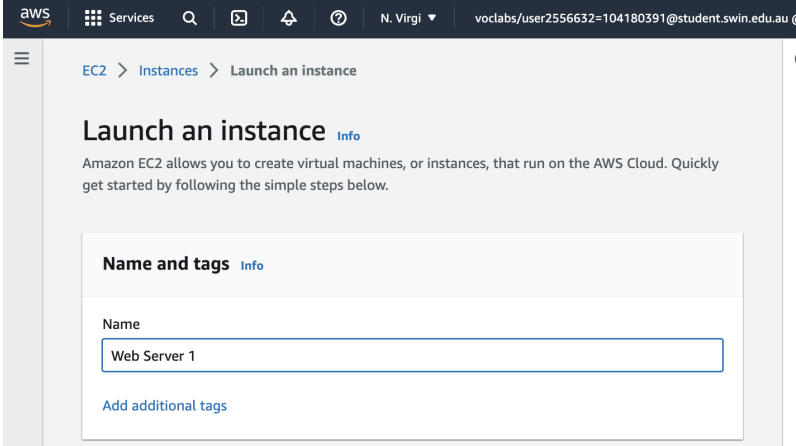
IPv4 CIDRs
10.0.0.0/16

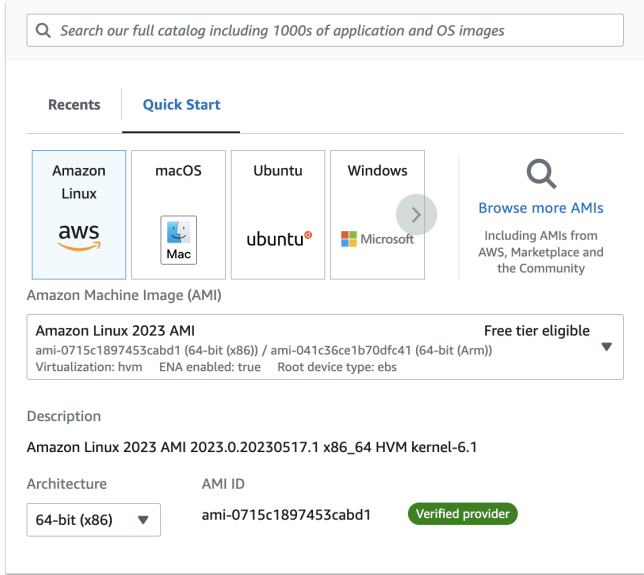
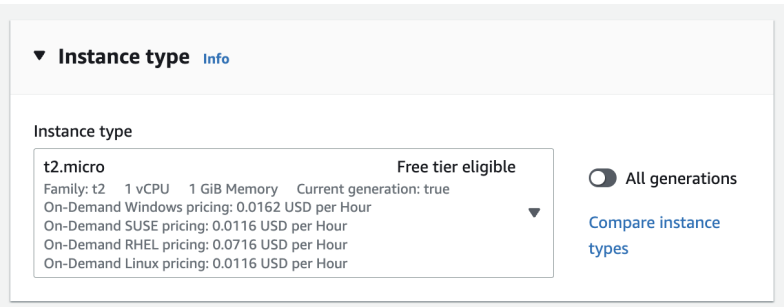
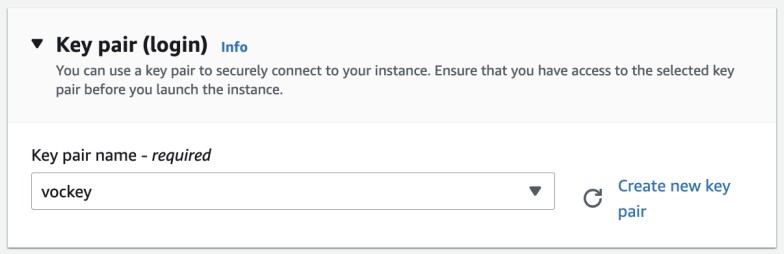
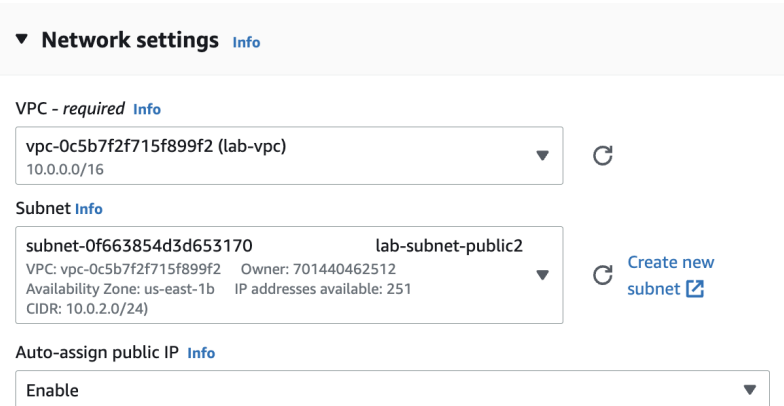
10	<ul style="list-style-type: none"> - Subnet name: lab-subnet-public2 - Availability Zone: Select the second Availability Zone (for example, us-east-1b) - IPv4 CIDR block: 10.0.2.0/24 - The subnet will have all IP addresses starting with 10.0.2.x. - Lastly, choose Create subnet. 	
11	<p>The second public subnet was created. Now, create a second private subnet.</p> <ul style="list-style-type: none"> - 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 - The subnet will have all IP addresses starting with 10.0.3.x. 	
12	<ul style="list-style-type: none"> - New private and public subnet is successfully created. - In the left navigation pane, choose Route tables. 	

13	<ul style="list-style-type: none">- Select the lab-rtb-private1-us-east-1a route table.- In the lower pane, choose the Routes tab.- This route table is therefore being used to route traffic from private subnets.	 <p>The screenshot shows the 'Routes' tab of the AWS Management Console. At the top, there are tabs for 'Details', 'Routes' (selected), 'Subnet associations', and 'Edge associations'. Below the tabs, there's a section titled 'Routes (2)' with an 'Edit routes' button. A search bar labeled 'Filter routes' and a dropdown menu set to 'Both' are present. Below this is a table with columns: Destination, Target, Status, and Propagated. The table contains two entries: one for destination 0.0.0.0/0 with target nat-0b47b1dd73a5c0fae, and another for 10.0.0.0/16 with target local. Both routes have a status of 'Active' (indicated by a green checkmark) and 'No' for propagation.</p> <table><tr><th>Destination</th><th>Target</th><th>Status</th><th>Propagated</th></tr><tr><td>0.0.0.0/0</td><td>nat-0b47b1dd73a5c0fae</td><td>Active</td><td>No</td></tr><tr><td>10.0.0.0/16</td><td>local</td><td>Active</td><td>No</td></tr></table>	Destination	Target	Status	Propagated	0.0.0.0/0	nat-0b47b1dd73a5c0fae	Active	No	10.0.0.0/16	local	Active	No
Destination	Target	Status	Propagated											
0.0.0.0/0	nat-0b47b1dd73a5c0fae	Active	No											
10.0.0.0/16	local	Active	No											
14	<ul style="list-style-type: none">- Choose the Subnet associations tab.- In the Explicit subnet associations panel, choose Edit subnet associations	 <p>The screenshot shows the 'Subnet associations' tab of the AWS Management Console. At the top, there are tabs for 'Details', 'Routes', 'Subnet associations' (selected), and 'Edge associations'. Below the tabs, there's a section titled 'Explicit subnet associations (1)' with an 'Edit subnet associations' button. A search bar labeled 'Find subnet association' is present. Below this is a table with columns: Name, Subnet ID, IPv4 CIDR, and IPv6 CIDR. The table contains one entry: 'lab-subnet-p...' with subnet ID 'subnet-049e...', IPv4 CIDR '10.0.1.0/24', and an empty IPv6 CIDR field. Below this table is a section titled 'Subnets without explicit associations (2)' with a message stating that the following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table. There is an 'Edit subnet associations' button at the bottom of this section.</p> <table><tr><th>Name</th><th>Subnet ID</th><th>IPv4 CIDR</th><th>IPv6 CIDR</th></tr><tr><td>lab-subnet-p...</td><td>subnet-049e...</td><td>10.0.1.0/24</td><td>-</td></tr></table>	Name	Subnet ID	IPv4 CIDR	IPv6 CIDR	lab-subnet-p...	subnet-049e...	10.0.1.0/24	-				
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR											
lab-subnet-p...	subnet-049e...	10.0.1.0/24	-											

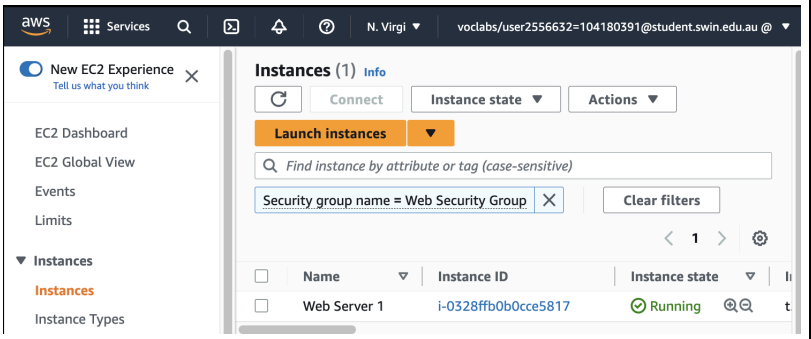
15	<ul style="list-style-type: none">- Leave lab-subnet-private1-us-east-1a selected, but also select lab-subnet-private2.- Choose Save associations	
16	Select the lab-rtb-public route table (and deselect any other subnets).	
17	<ul style="list-style-type: none">- Choose the Subnet associations tab.- In the Explicit subnet associations area, choose Edit subnet associations.	

18	<ul style="list-style-type: none"> - Leave lab-subnet-public1-us-east-1a selected, but also select lab-subnet-public2. - Choose Save associations - The VPC now has public and private subnets configured in two Availability Zones 	
19	<ul style="list-style-type: none"> - In the left navigation pane, choose Security groups. - Choose Create security group. 	
20	<p>Configuration:</p> <ul style="list-style-type: none"> - 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 	

21	<ul style="list-style-type: none"> - In the Inbound rules pane, choose Add rule - Configure the following settings: <ul style="list-style-type: none"> + Type: HTTP + Source: Anywhere-IPv4 + Description: Permit web requests - Choose Create security group 	
22	<ul style="list-style-type: none"> - In the search box to the right of Services, search for and choose EC2 to open the EC2 console. - Choose Launch instance. 	
23	Name the instance: Web Server 1	

24	<p>Choose an AMI from which to create the instance:</p> <ul style="list-style-type: none"> - In the list of available Quick Start AMIs, keep the default Amazon Linux selected. - Also keep the default Amazon Linux 2023 AMI selected. 	 <p>The screenshot shows the 'Quick Start' tab in the AWS IAM console. Under 'Amazon Machine Image (AMI)', the 'Amazon Linux 2023 AMI' is selected. The AMI ID is 'ami-0715c1897453cabd1' (64-bit (x86)) / 'ami-041c36ce1b70dfc41' (64-bit (Arm)). The description is 'Amazon Linux 2023 AMI 2023.0.20230517.1 x86_64 HVM kernel-6.1'. The architecture is '64-bit (x86)' and the AMI ID is 'ami-0715c1897453cabd1'. A 'Verified provider' badge is visible.</p>
25	<p>In the Instance type panel, keep the default t2.micro selected.</p>	 <p>The screenshot shows the 'Instance type' panel in the AWS IAM console. The 't2.micro' instance type is selected. The description is 'Family: t2 1 vCPU 1 GiB Memory Current generation: true'. The pricing is 'On-Demand Windows pricing: 0.0162 USD per Hour', 'On-Demand SUSE pricing: 0.0116 USD per Hour', 'On-Demand RHEL pricing: 0.0716 USD per Hour', and 'On-Demand Linux pricing: 0.0116 USD per Hour'. A 'Free tier eligible' badge is visible.</p>
26	<p>From the Key pair name menu, select vockey.</p>	 <p>The screenshot shows the 'Key pair (login)' panel in the AWS IAM console. The 'vockey' key pair is selected. The description is '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.' A 'Create new key pair' button is visible.</p>
27	<p>Next to Network settings, choose Edit, then configure:</p> <ul style="list-style-type: none"> - Network: lab-vpc - Subnet: lab-subnet-public2 (not Private!) - Auto-assign public IP: Enable 	 <p>The screenshot shows the 'Network settings' panel in the AWS IAM console. The 'VPC' is set to 'vpc-0c5b7f2f715f899f2 (lab-vpc)'. The 'Subnet' is set to 'subnet-0f663854d3d653170 lab-subnet-public2'. The 'Auto-assign public IP' is set to 'Enable'. A 'Create new subnet' button is visible.</p>

28	<p>Configure the instance to use the Web Security Group that was created earlier.</p> <ul style="list-style-type: none"> - Under Firewall (security groups), choose Select existing security group. - For Common security groups, select Web Security Group. 	<p>Firewall (security groups) Info</p> <p>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.</p> <p> <input type="radio"/> Create security group <input checked="" type="radio"/> Select existing security group </p> <p>Common security groups Info</p> <p>Select security groups ▼</p> <p>Web Security Group sg-0ec8d6afe18fedc15 × VPC: vpc-0c5b7f2f715f899f2</p> <p>Compare security group rules</p> <p>Security groups that you add or remove here will be added to or removed from all your network interfaces.</p> <p>► Advanced network configuration</p>
29	<p>In the Configure storage section, keep the default settings.</p>	<p>▼ Configure storage Info Advanced</p> <p>1x <input type="text" value="8"/> GiB <input type="text" value="gp3"/> ▼ Root volume (Not encrypted)</p> <p> <input checked="" type="checkbox"/> Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage × </p> <p><input type="button" value="Add new volume"/></p> <p>0 x File systems Edit</p>
30	<p>Configure a script to run on the instance when it launches:</p> <ul style="list-style-type: none"> - Expand the Advanced details panel. - Scroll to the bottom of the page and then copy and paste the script into the User data box. - Choose Launch instance 	<p>User data - <i>optional</i> Info</p> <p>Enter user data in the field.</p> <pre>#!/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</pre> <p><input type="checkbox"/> User data has already been base64 encoded</p> <p>► Summary</p> <p> <input type="button" value="Cancel"/> <input type="button" value="Launch instance"/> Review commands </p>

31	<ul style="list-style-type: none">- Choose View all instances- Wait until Web Server 1 shows 2/2 checks passed in the Status check column.- Copy the Public IPv4 DNS value into the browser..	
32	A web page displaying the AWS logo and instance meta-data values.	