

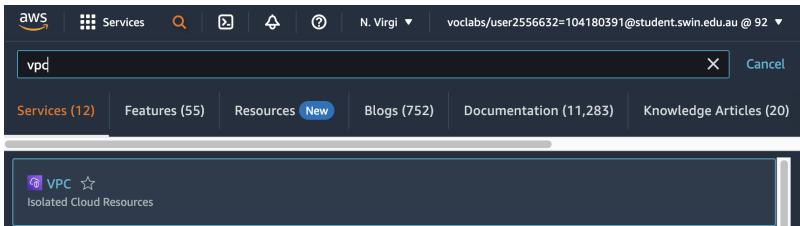
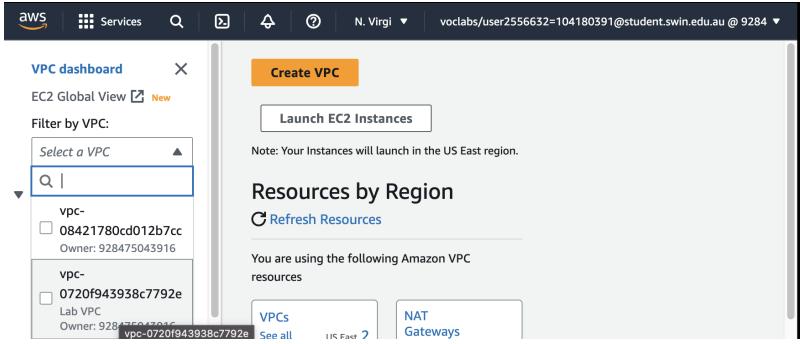
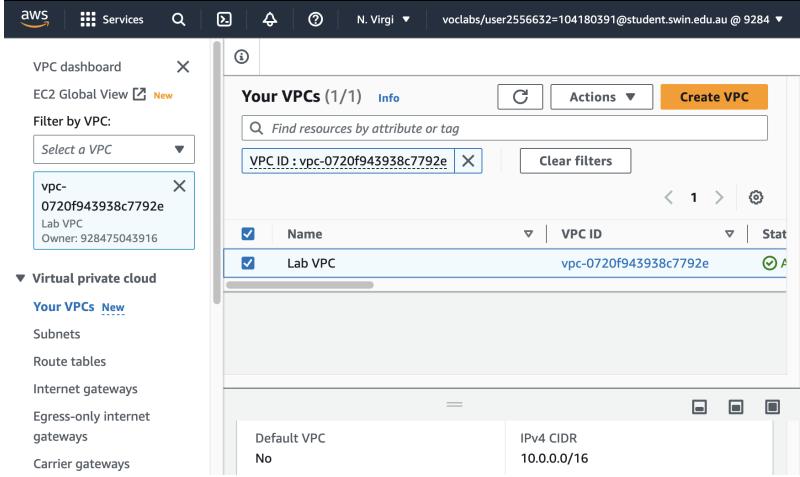


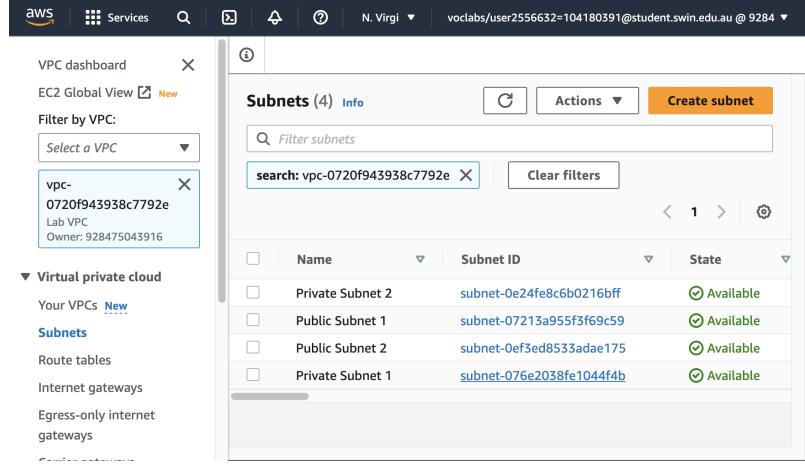
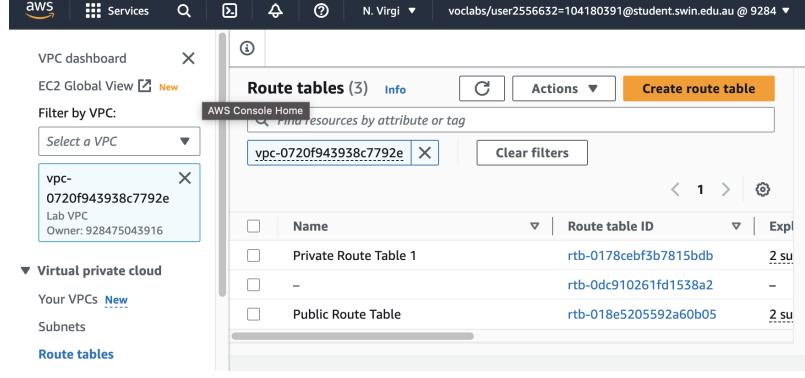
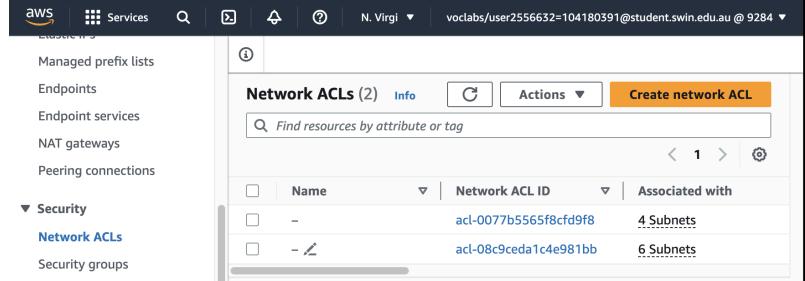
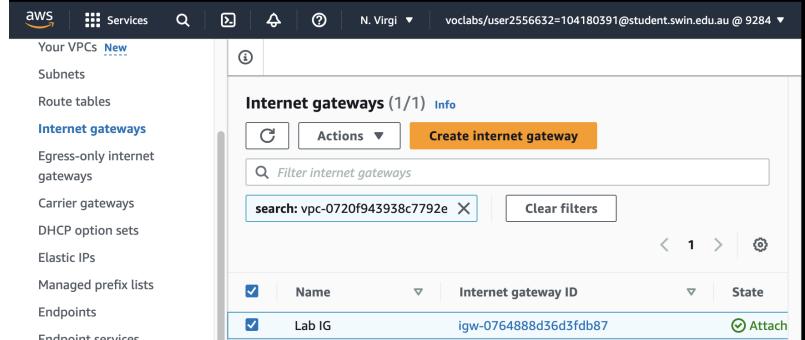
Module 9 Guided Lab - Creating a Highly Available Environment

July 1, 2023

Luu Tuan Hoang
Student ID: 104180391

Task 1: Inspecting your VPC

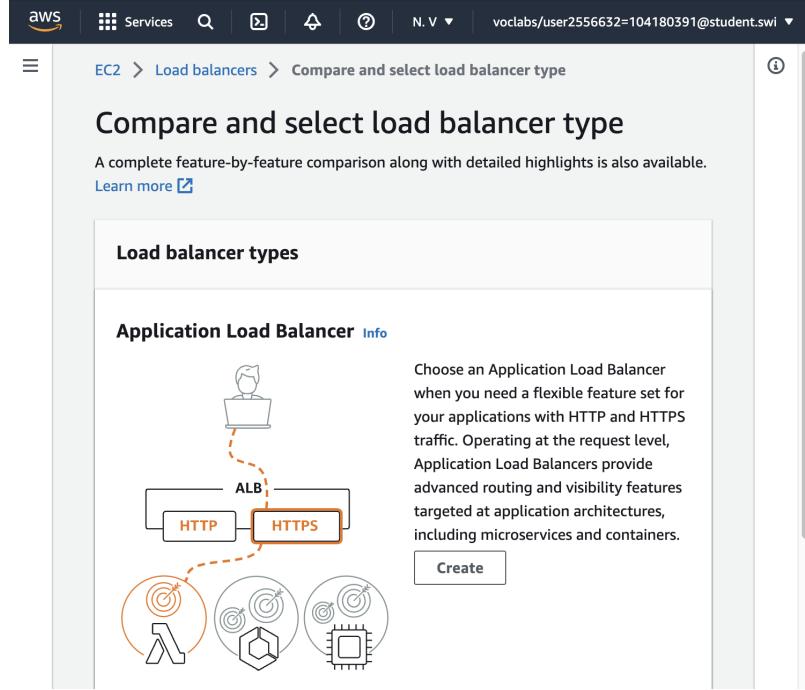
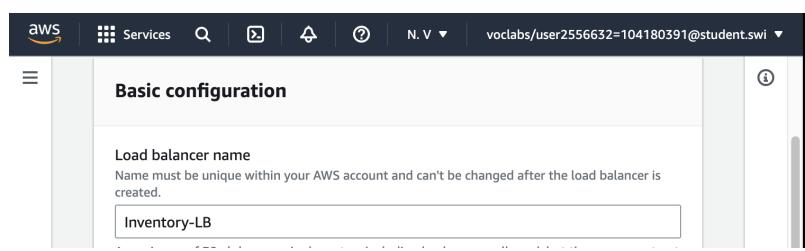
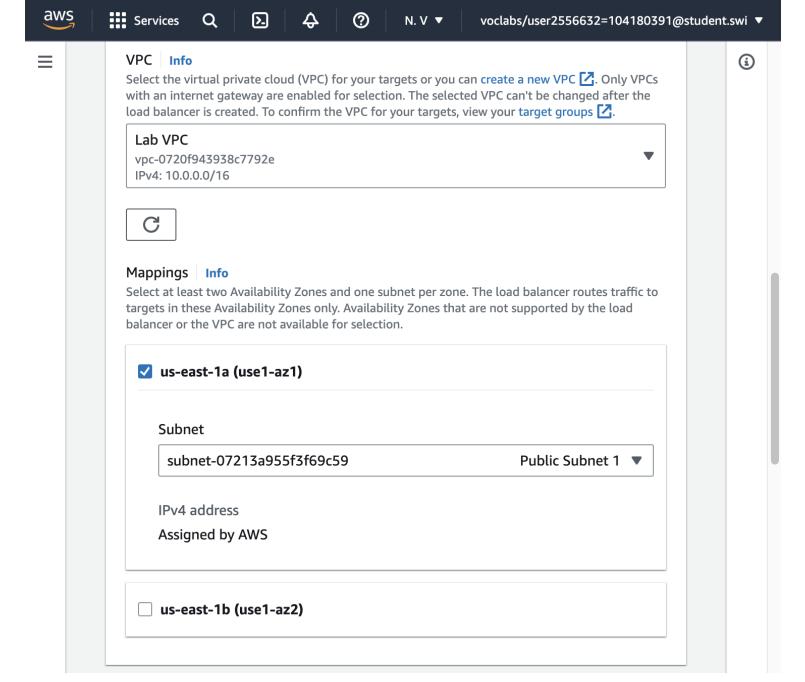
Step	Description	Screenshot
1	On the AWS Management Console, on the Services menu, choose VPC .	
2	In the left navigation pane, under Filter by VPC , choose the Select a VPC box and select Lab VPC .	
3	In the left navigation pane, choose Your VPCs . Information about the Lab VPC that was created can be accessed. Choose Lab VPC .	

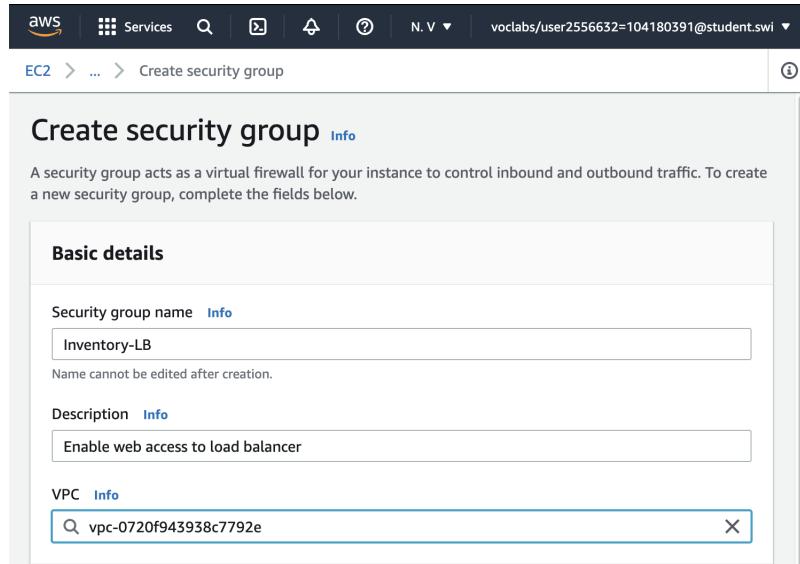
4	<p>In the left navigation pane, choose Subnets.</p> <p>Here, you can access information about Public Subnet 1.</p>	 <table border="1"> <thead> <tr> <th>Name</th> <th>Subnet ID</th> <th>State</th> </tr> </thead> <tbody> <tr> <td>Private Subnet 2</td> <td>subnet-0e24fe8c6b0216bff</td> <td>Available</td> </tr> <tr> <td>Public Subnet 1</td> <td>subnet-07213a955f3f69c59</td> <td>Available</td> </tr> <tr> <td>Public Subnet 2</td> <td>subnet-0ef3ed8533adae175</td> <td>Available</td> </tr> <tr> <td>Private Subnet 1</td> <td>subnet-076e2038fe1044f4b</td> <td>Available</td> </tr> </tbody> </table>	Name	Subnet ID	State	Private Subnet 2	subnet-0e24fe8c6b0216bff	Available	Public Subnet 1	subnet-07213a955f3f69c59	Available	Public Subnet 2	subnet-0ef3ed8533adae175	Available	Private Subnet 1	subnet-076e2038fe1044f4b	Available
Name	Subnet ID	State															
Private Subnet 2	subnet-0e24fe8c6b0216bff	Available															
Public Subnet 1	subnet-07213a955f3f69c59	Available															
Public Subnet 2	subnet-0ef3ed8533adae175	Available															
Private Subnet 1	subnet-076e2038fe1044f4b	Available															
5	<p>In the lower half of the page, choose the Route table tab.</p>	 <table border="1"> <thead> <tr> <th>Name</th> <th>Route table ID</th> <th>Associated with</th> </tr> </thead> <tbody> <tr> <td>Private Route Table 1</td> <td>rtb-0178cebf3b7815bdb</td> <td>2 subnets</td> </tr> <tr> <td>-</td> <td>rtb-0dc910261fd1538a2</td> <td>-</td> </tr> <tr> <td>Public Route Table</td> <td>rtb-018e5205592a60b05</td> <td>2 subnets</td> </tr> </tbody> </table>	Name	Route table ID	Associated with	Private Route Table 1	rtb-0178cebf3b7815bdb	2 subnets	-	rtb-0dc910261fd1538a2	-	Public Route Table	rtb-018e5205592a60b05	2 subnets			
Name	Route table ID	Associated with															
Private Route Table 1	rtb-0178cebf3b7815bdb	2 subnets															
-	rtb-0dc910261fd1538a2	-															
Public Route Table	rtb-018e5205592a60b05	2 subnets															
6	<p>Choose the Network ACL tab.</p>	 <table border="1"> <thead> <tr> <th>Name</th> <th>Network ACL ID</th> <th>Associated with</th> </tr> </thead> <tbody> <tr> <td>-</td> <td>acl-0077b5565f8fd9f8</td> <td>4 Subnets</td> </tr> <tr> <td>-</td> <td>acl-08c9ceda1c4e981bb</td> <td>6 Subnets</td> </tr> </tbody> </table>	Name	Network ACL ID	Associated with	-	acl-0077b5565f8fd9f8	4 Subnets	-	acl-08c9ceda1c4e981bb	6 Subnets						
Name	Network ACL ID	Associated with															
-	acl-0077b5565f8fd9f8	4 Subnets															
-	acl-08c9ceda1c4e981bb	6 Subnets															
7	<p>In the left navigation pane, choose Internet gateways.</p>	 <table border="1"> <thead> <tr> <th>Name</th> <th>Internet gateway ID</th> <th>Attached</th> </tr> </thead> <tbody> <tr> <td>Lab IG</td> <td>igw-0764888d36d3fdb87</td> <td>Attached</td> </tr> </tbody> </table>	Name	Internet gateway ID	Attached	Lab IG	igw-0764888d36d3fdb87	Attached									
Name	Internet gateway ID	Attached															
Lab IG	igw-0764888d36d3fdb87	Attached															

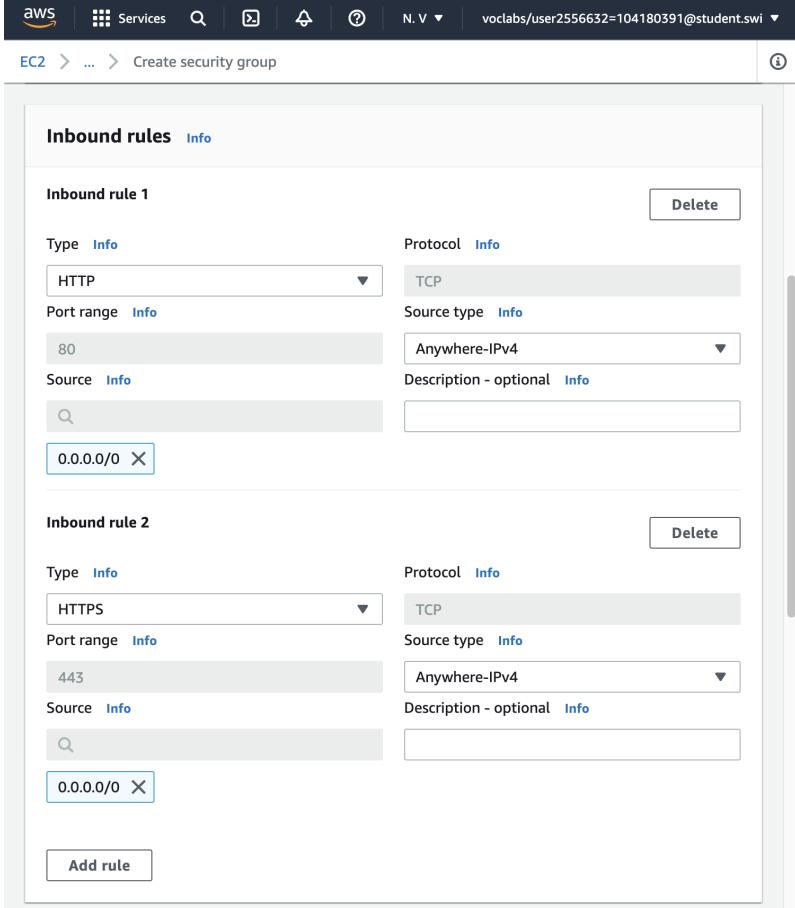
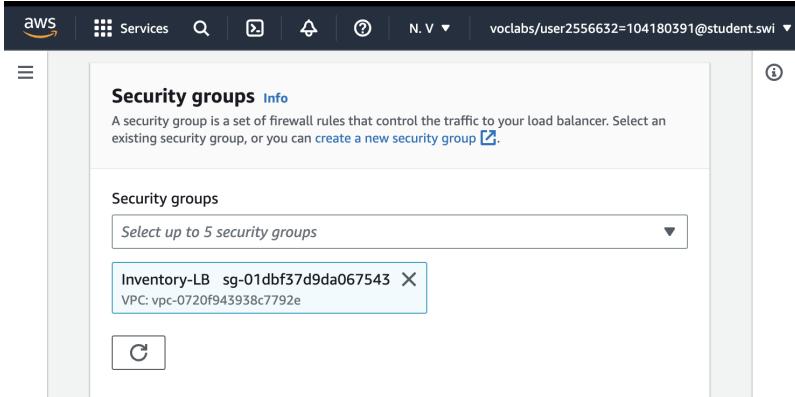
8	<p>In the left navigation pane, choose Security groups.</p> <p>Select Inventory-DB.</p> <p>This security group controls incoming traffic to the database.</p>	<table border="1"> <thead> <tr> <th>Name</th> <th>Security group ID</th> <th>Security group name</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Inventory-DB</td> <td>sg-068916f6841af5bb</td> <td>Inventory-DB</td> </tr> <tr> <td><input type="checkbox"/> Inventory-App</td> <td>sg-087ab7d1b26db2710</td> <td>Inventory-App</td> </tr> <tr> <td><input type="checkbox"/></td> <td>sg-086903dcbb90390ed</td> <td>default</td> </tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Name</th> <th>Security group rule...</th> <th>IP version</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> -</td> <td>sgr-017c911f453f673f1</td> <td>IPv4</td> </tr> </tbody> </table>	Name	Security group ID	Security group name	<input checked="" type="checkbox"/> Inventory-DB	sg-068916f6841af5bb	Inventory-DB	<input type="checkbox"/> Inventory-App	sg-087ab7d1b26db2710	Inventory-App	<input type="checkbox"/>	sg-086903dcbb90390ed	default	Name	Security group rule...	IP version	<input checked="" type="checkbox"/> -	sgr-017c911f453f673f1	IPv4
Name	Security group ID	Security group name																		
<input checked="" type="checkbox"/> Inventory-DB	sg-068916f6841af5bb	Inventory-DB																		
<input type="checkbox"/> Inventory-App	sg-087ab7d1b26db2710	Inventory-App																		
<input type="checkbox"/>	sg-086903dcbb90390ed	default																		
Name	Security group rule...	IP version																		
<input checked="" type="checkbox"/> -	sgr-017c911f453f673f1	IPv4																		

Task 2: Creating an Application Load Balancer

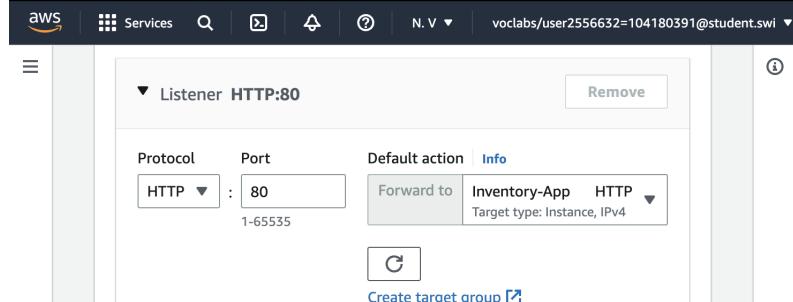
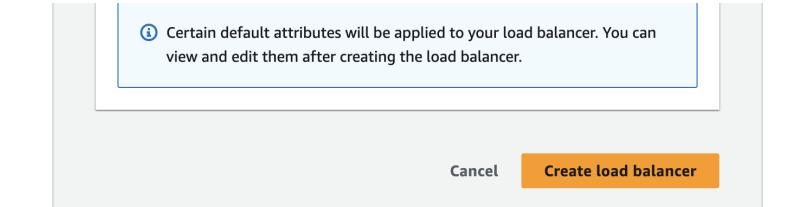
Step	Description	Screenshot
1	<p>On the Services menu, choose EC2.</p> <p>In the left navigation pane, choose Load Balancers.</p> <p>Choose Create load balancer</p>	

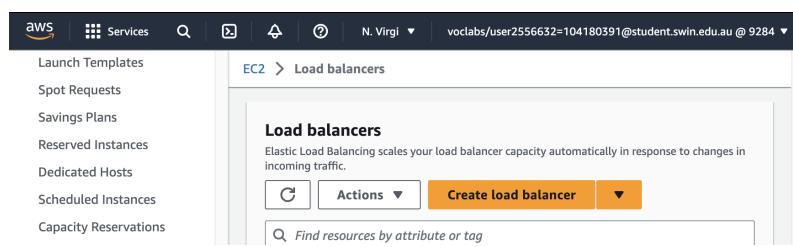
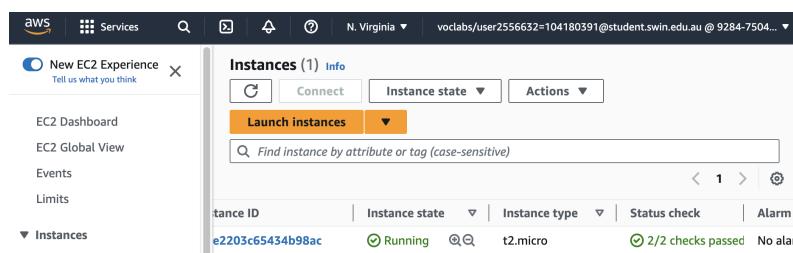
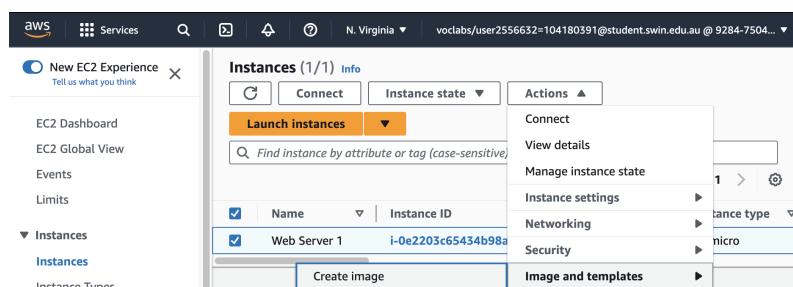
2	<p>Under Application Load Balancer, choose Create.</p>	
3	<p>For Load balancer name, enter: Inventory-LB</p>	
4	<p>Scroll down to the Network mapping section, then for VPC, select Lab VPC. Under Mappings, choose the first Availability Zone, then choose the Public Subnet that displays.</p>	

5	<p>Choose the second Availability Zone, then choose the Public Subnet that displays.</p>	
6	<p>In the Security groups section, select the Create a new security group hyperlink. This opens a new browser tab. Configure the new security group settings:</p> <ul style="list-style-type: none"> - Security group name: Inventory-LB - Description: Enable web access to load balancer - VPC: Remove the default VPC by choosing the X to the right of it. Then select Lab VPC. 	

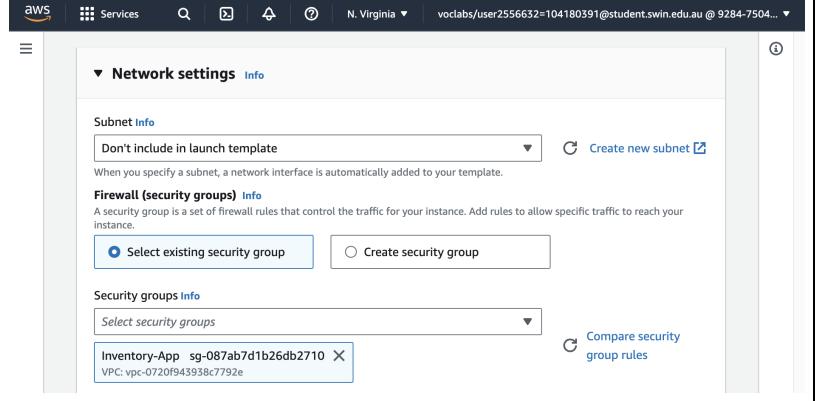
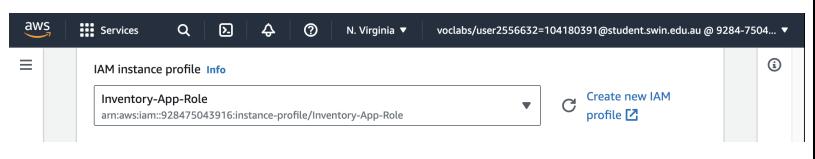
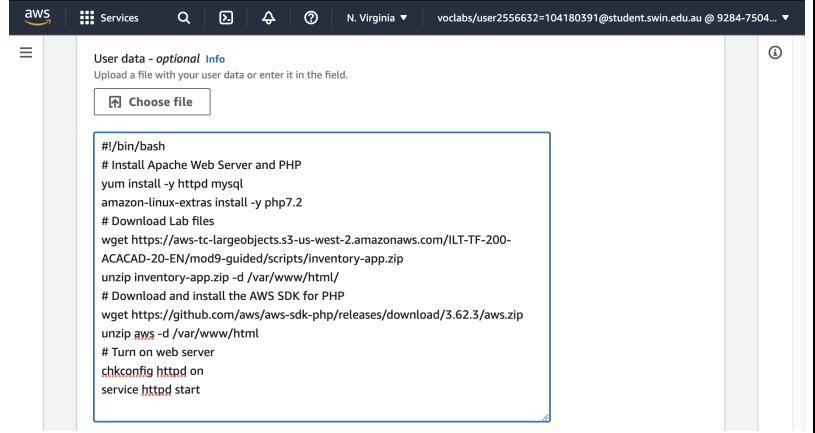
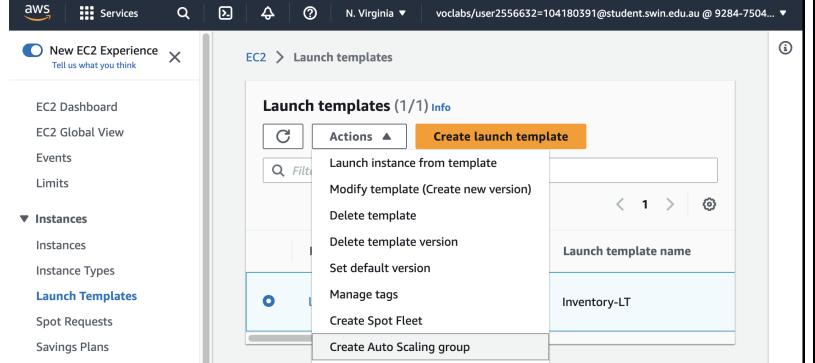
7	<p>Under Inbound rules, choose Add rule and configure as described:</p> <ul style="list-style-type: none"> - Type: HTTP - Source: Anywhere-IPv4 <p>Still under Inbound rules, choose Add rule again and configure:</p> <ul style="list-style-type: none"> - Type: HTTPS - Source: Anywhere-IPv4 <p>Choose Create security group.</p>	
8	<p>Assign the security group to the load balancer:</p> <ul style="list-style-type: none"> - Return to the browser tab where you are still configuring the load balancer. - In the Security groups area and choose the refresh icon. - For Security groups, select the Inventory-LB security group you just created. - Next, below the Security groups dropdown menu, select the X next to the default security group so that Inventory-LB is now the only security group chosen. 	

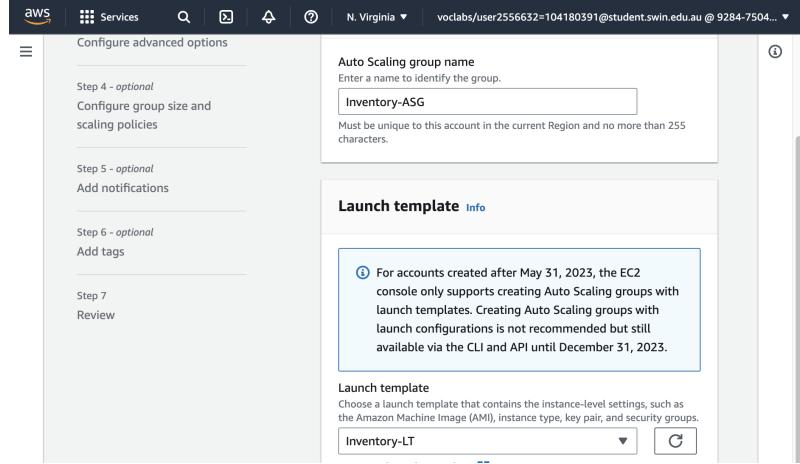
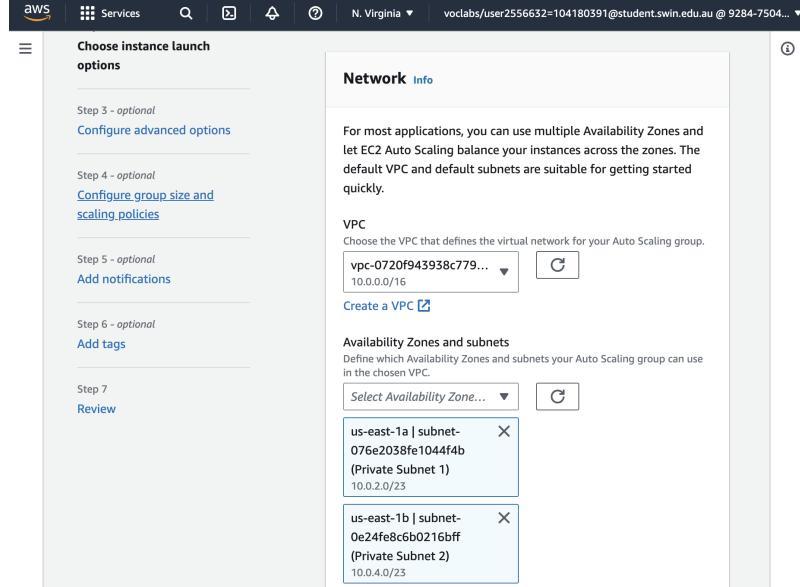
9	<p>In the Listeners and routing section, choose Create target group.</p> <p>A new browser tab will open.</p> <p>Configure the target group as described here:</p> <ul style="list-style-type: none"> - Choose a target type: Instances 	
10	<ul style="list-style-type: none"> - Target group name: Inventory-App - VPC: Ensure that Lab VPC is chosen. 	
11	<ul style="list-style-type: none"> - Healthy threshold: 2 - Interval: 10 (seconds) <p>Choose Next</p>	
12	<p>Choose Create target group</p>	

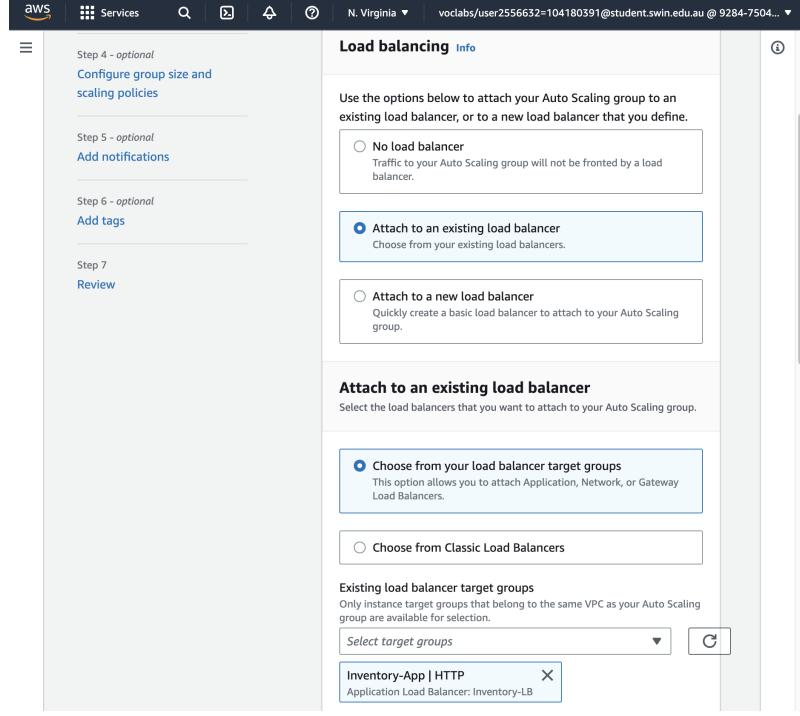
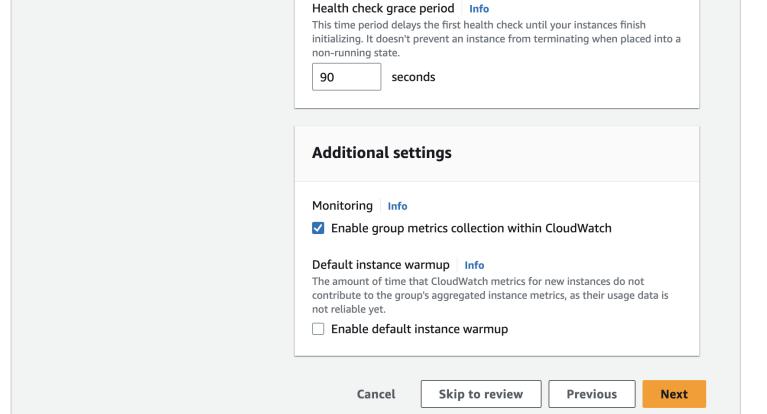
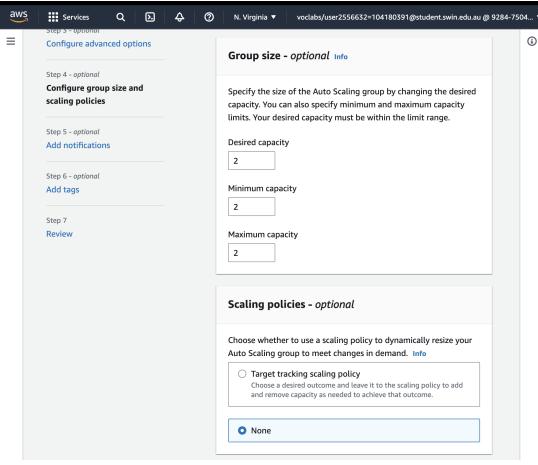
13	For the Listener HTTP:80 row, set the Default action to forward to the Inventory-App target group you just created.	
14	Scroll to the bottom of the page, and choose Create load balancer .	

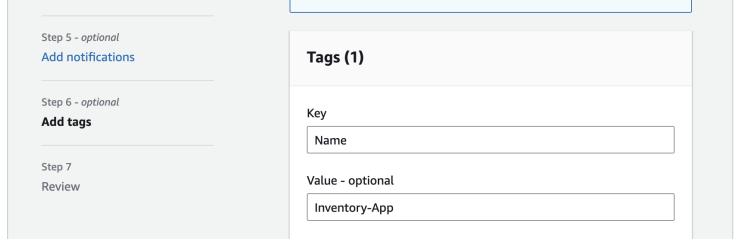
Step	Description	Screenshot
1	In the AWS Management Console, on the Services menu, choose EC2 .	
2	<p>In the left navigation pane, choose Instances.</p> <p>Wait until the Status check for Web Server 1 displays 2/2 checks passed</p> <p>Select Web Server 1.</p>	
3	In the Actions menu, choose Image and templates > Create image	

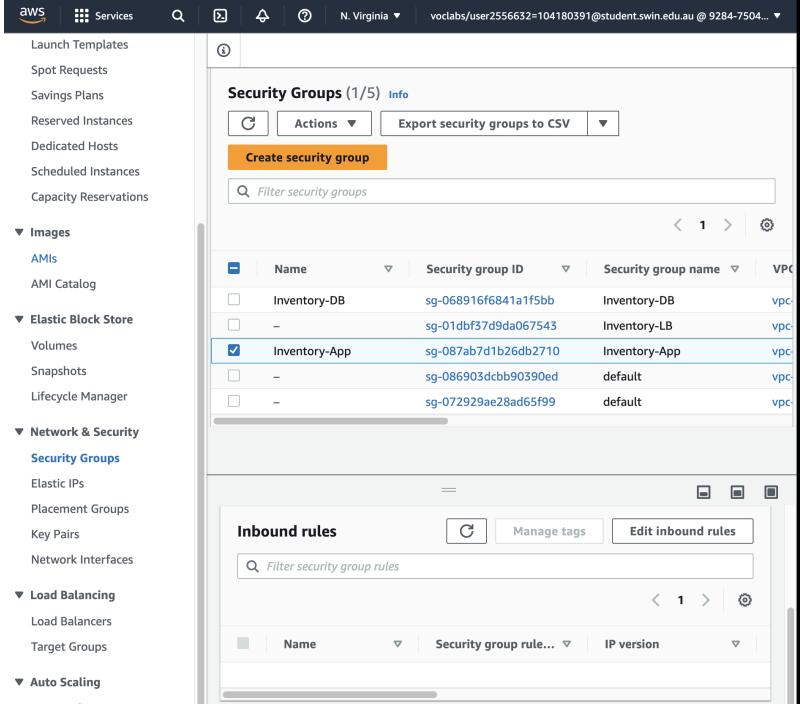
4	<p>Configure:</p> <ul style="list-style-type: none"> Image name: Web Server AMI Image description: Lab AMI for Web Server <p>Choose Create image</p>	
5	<p>In the left navigation pane, choose Launch Templates.</p> <p>Choose Create launch template</p> <p>Configure the launch template settings and create it:</p> <ul style="list-style-type: none"> Launch template name: Inventory-LT Under Auto Scaling guidance, select Provide guidance to help me set up a template that I can use with EC2 Auto Scaling 	
6	<ul style="list-style-type: none"> In the Application and OS Images (Amazon Machine Image) area, choose My AMIs. Amazon Machine Image (AMI): choose Web Server AMI 	
7	<ul style="list-style-type: none"> Instance type: choose t2.micro Key pair name: choose vockey 	

8	<ul style="list-style-type: none"> - Firewall (security groups): choose Select existing security group - Security groups: choose Inventory-App 	 <p>The screenshot shows the 'Network settings' section of the AWS Management Console. It includes fields for 'Subnet info' (set to 'Don't include in launch template'), 'Firewall (security groups)' (set to 'Select existing security group'), and 'Security groups info' (listing 'Inventory-App sg-087ab7d1b26db2710' and 'VPC: vpc-0f943938c7792e'). A 'Create new subnet' button is also visible.</p>
9	<ul style="list-style-type: none"> - IAM instance profile: choose Inventory-App-Role 	 <p>The screenshot shows the 'IAM instance profile' page. It displays the selected profile 'Inventory-App-Role arn:aws:iam::928475043916:instance-profile/Inventory-App-Role'. A 'Create new IAM profile' button is visible.</p>
10	<ul style="list-style-type: none"> - Scroll down to the Detailed CloudWatch monitoring setting. Select Enable 	 <p>The screenshot shows the 'Detailed CloudWatch monitoring' settings. The 'Enable' checkbox is checked, and a note 'Additional charges apply' is present.</p>
11	<ul style="list-style-type: none"> - Under User data, paste in the script below: <p>Choose Create launch template</p>	 <p>The screenshot shows the 'User data - optional' page. It contains a pre-filled shell script to download and install the inventory application:</p> <pre>#!/bin/bash # Install Apache Web Server and PHP yum install -y httpd mysql amazon-linux-extras install -y php7.2 # Download Lab files wget https://aws-tc-largeobjects.s3-us-west-2.amazonaws.com/ILT-TF-200-ACACAD-20-EN/mod9-guided/scripts/inventory-app.zip unzip inventory-app.zip -d /var/www/html/ # Download and install the AWS SDK for PHP wget https://github.com/aws/aws-sdk-php/releases/download/3.62.3/aws.zip unzip aws -d /var/www/html/ # Turn on web server chkconfig httpd on service httpd start</pre>
12	<p>From the Actions menu, choose Create Auto Scaling group</p>	 <p>The screenshot shows the 'Launch templates' page under the EC2 service. The 'Actions' menu is open, and the 'Create launch template' option is highlighted.</p>

13	<p>Configure the details in Step 1 (Choose launch template or configuration):</p> <ul style="list-style-type: none"> - Auto Scaling group name: Inventory-ASG (ASG stands for Auto Scaling group) - Launch template: confirm that the Inventory-LT template you just created is selected. 	
14	<p>Configure the details in Step 2 (Choose instance launch options):</p> <ul style="list-style-type: none"> - VPC: choose Lab VPC - Availability Zones and subnets: Choose Private Subnet 1 and then choose Private Subnet 2. - This will launch EC2 instances in private subnets across both Availability Zones. <p>Choose Next</p>	

15	<p>Configure the details in Step 3 (Configure advanced options):</p> <p>In the Load balancing panel:</p> <ul style="list-style-type: none"> - Choose Attach to an existing load balancer - Existing load balancer target groups: select Inventory-App. 	
16	<p>In the Health checks panel:</p> <ul style="list-style-type: none"> - Health check grace period: 90 seconds <p>In the Additional settings panel:</p> <ul style="list-style-type: none"> - Select Enable group metrics collection within CloudWatch <p>Choose Next</p>	
17	<p>Configure the details in Step 4 (Configure group size and scaling policies - optional):</p> <p>Under Group size, configure:</p> <ul style="list-style-type: none"> - Desired capacity: 2 - Minimum capacity: 2 - Maximum capacity: 2 <p>Under Scaling policies, choose None</p>	

18	<p>Choose Add tag and Configure the following:</p> <ul style="list-style-type: none"> - Key: Name - Value: Inventory-App 	
19	<p>At the bottom of the page, choose Create Auto Scaling group</p>	

Step	Description	Screenshot
1	<p>In the left navigation pane, choose Security Groups.</p> <p>Select Inventory-App.</p> <p>In the lower half of the page, choose the Inbound rules tab.</p> <p>Choose Edit inbound rules.</p>	

2	<p>On the Edit inbound rules page, choose Add rule and configure these settings:</p> <p>Type: HTTP</p> <p>Source:</p> <ul style="list-style-type: none"> - Choose the search box to the right of Custom - Delete the current contents - Enter sg - From the list that appears, select Inventory-LB - Description: Traffic from load balancer <p>Choose Save rules</p>																			
3	<p>In the Security groups list, choose Inventory-DB (and make sure that no other security groups are selected).</p> <p>Choose Edit inbound rules.</p>	<table border="1" data-bbox="780 1056 1566 1415"> <thead> <tr> <th>Name</th> <th>Security group ID</th> <th>Security group name</th> </tr> </thead> <tbody> <tr> <td>Inventory-DB</td> <td>sg-068916f6841a1f5bb</td> <td>Inventory-DB</td> </tr> <tr> <td>Inventory-App</td> <td>sg-087ab7d1b26db2710</td> <td>Inventory-App</td> </tr> <tr> <td>-</td> <td>sg-01dbf37d9da067543</td> <td>Inventory-LB</td> </tr> <tr> <td>-</td> <td>sg-086903dcbb90390ed</td> <td>default</td> </tr> <tr> <td>-</td> <td>sg-072929ae28ad65f99</td> <td>default</td> </tr> </tbody> </table>	Name	Security group ID	Security group name	Inventory-DB	sg-068916f6841a1f5bb	Inventory-DB	Inventory-App	sg-087ab7d1b26db2710	Inventory-App	-	sg-01dbf37d9da067543	Inventory-LB	-	sg-086903dcbb90390ed	default	-	sg-072929ae28ad65f99	default
Name	Security group ID	Security group name																		
Inventory-DB	sg-068916f6841a1f5bb	Inventory-DB																		
Inventory-App	sg-087ab7d1b26db2710	Inventory-App																		
-	sg-01dbf37d9da067543	Inventory-LB																		
-	sg-086903dcbb90390ed	default																		
-	sg-072929ae28ad65f99	default																		

4

- In the **Inbound rules** tab, choose **Edit inbound rules** and configure these settings:
- Delete the existing rule.
 - Choose **Add rule**.
 - For **Type**, choose **MYSQL/Aurora**
 - Choose the search box to the right of **Custom**
 - Enter **sg**
 - From the list that appears, select **Inventory-App**
 - **Description:** Traffic from application servers

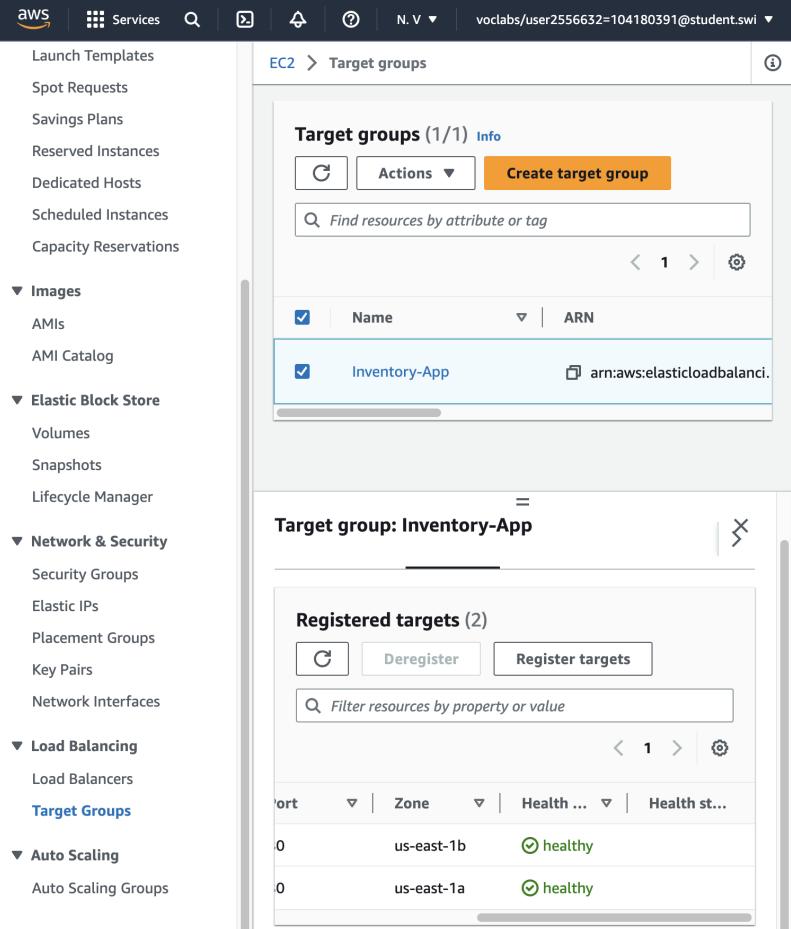
Choose **Save rules**

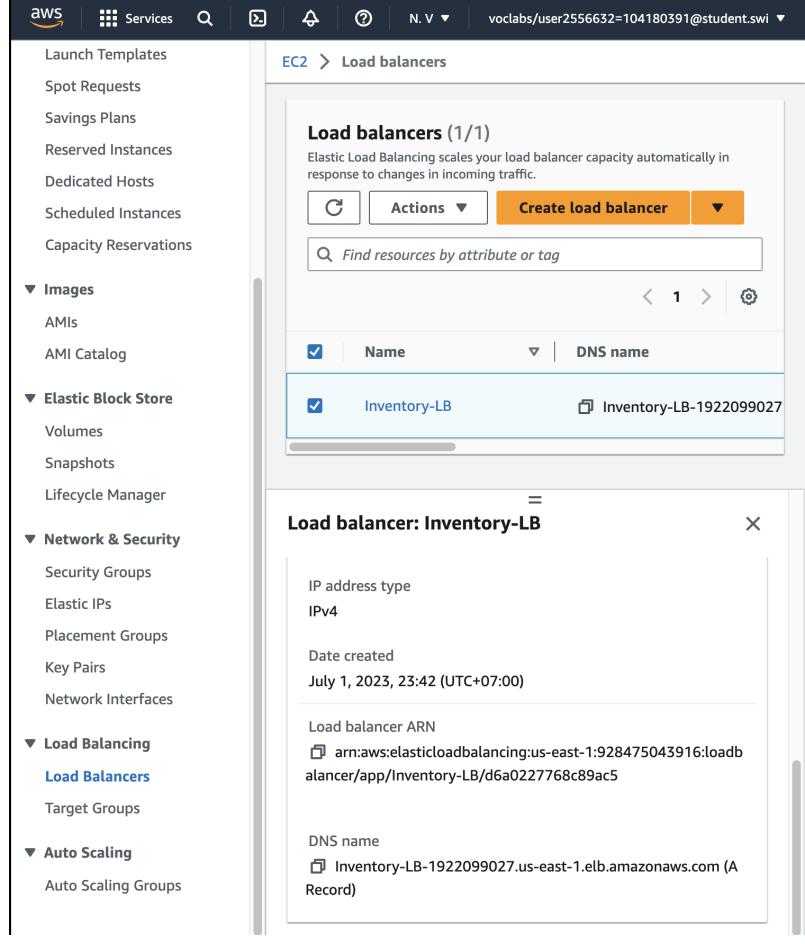
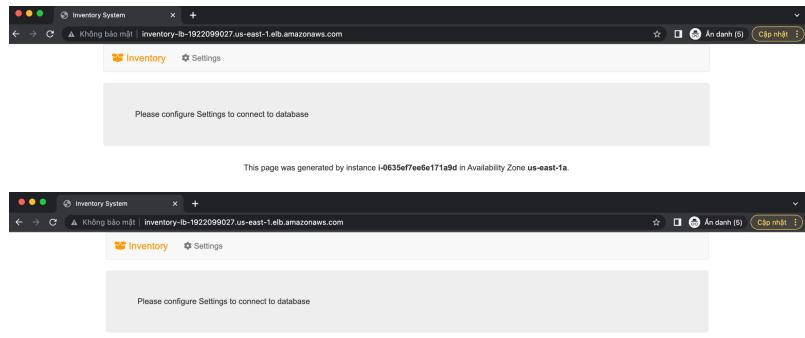
The screenshot shows the 'Edit inbound rules' configuration page in the AWS Management Console. The 'Inbound rule 1' section is displayed, showing the following details:

- Security group rule ID:** sg-087ab7d1b26db2710 (highlighted with a blue border)
- Type:** MYSQL/Aurora
- Port range:** 3306
- Protocol:** TCP
- Source type:** Custom
- Source:** A search bar containing 'sg' with a magnifying glass icon.
- Description - optional:** Traffic from application servers

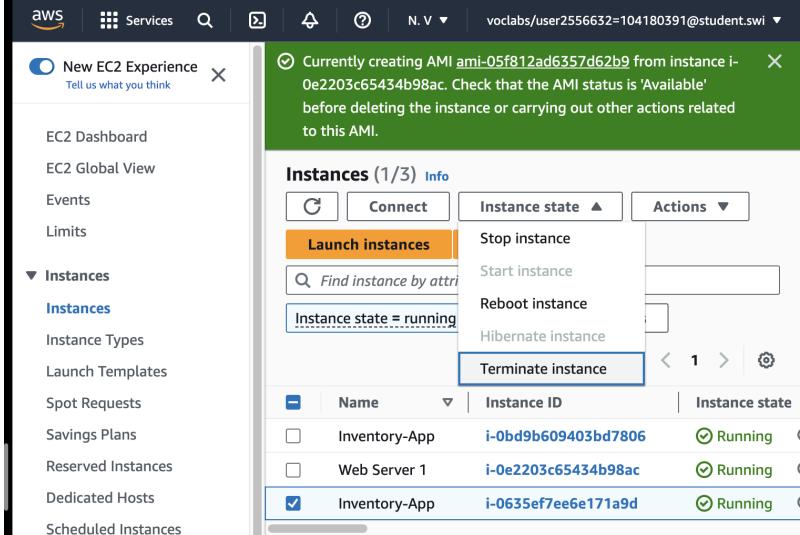
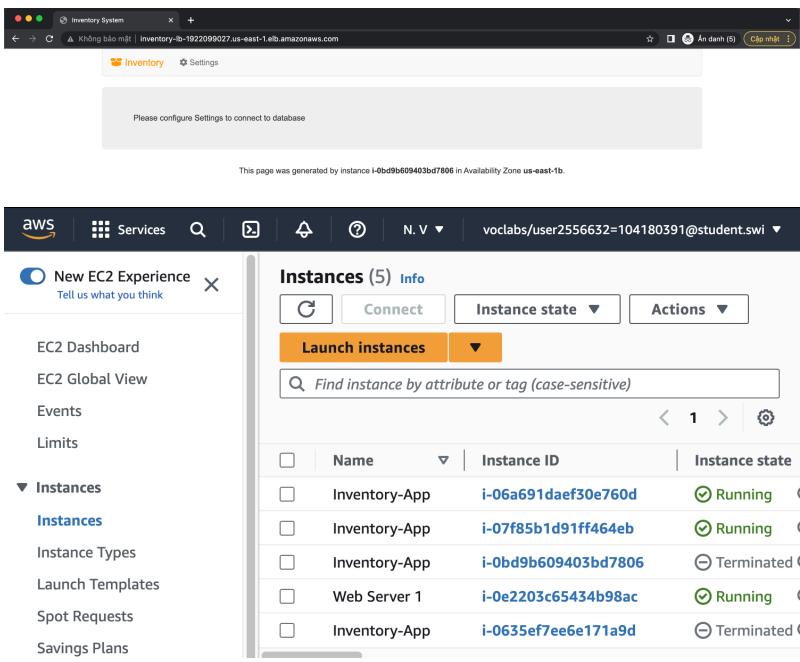
At the bottom of the form are three buttons: 'Cancel', 'Preview changes' (disabled), and 'Save rules' (highlighted with an orange border).

Task 5: Testing the application

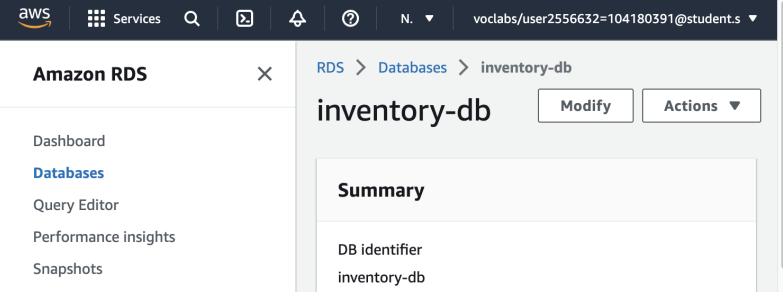
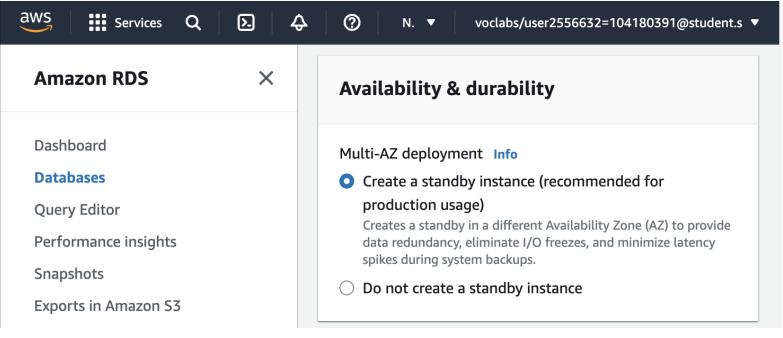
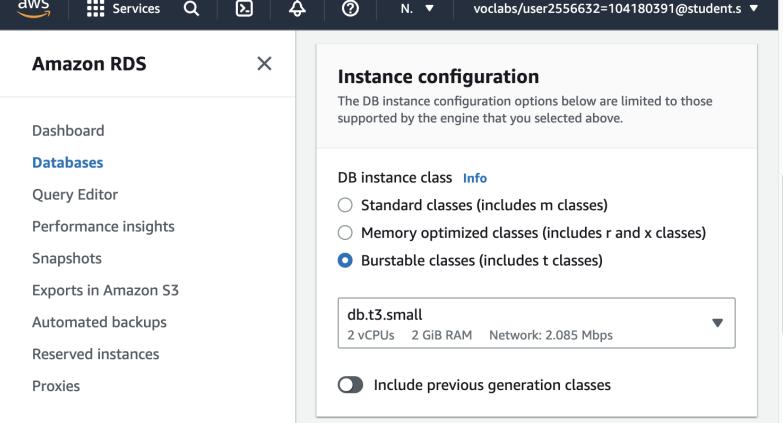
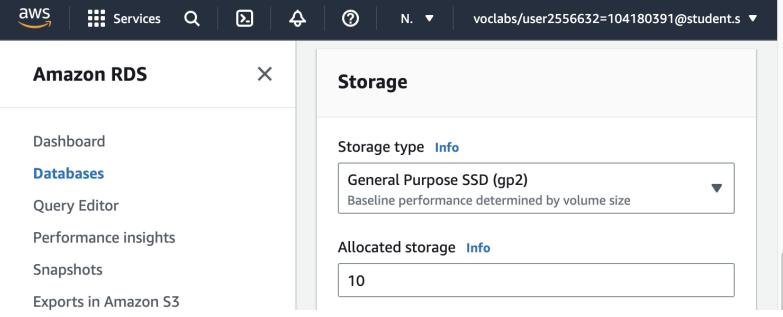
Step	Description	Screenshot									
1	<p>In the left navigation pane, choose Target Groups.</p> <p>Select Inventory-App.</p> <p>In the lower half of the page, choose the Targets tab.</p> <p>In the Registered targets area, occasionally choose the refresh icon until the Status for both instances appears as healthy.</p>	 <p>The screenshot shows the AWS EC2 Target Groups interface. On the left, a navigation pane lists various services like Launch Templates, Spot Requests, and Auto Scaling. The 'Target Groups' section is selected. In the main content area, the 'Target groups (1/1)' section shows one entry for 'Inventory-App'. Below it, the 'Target group: Inventory-App' section displays 'Registered targets (2)'. Two targets are listed: 'us-east-1b' and 'us-east-1a', both marked as 'healthy' with green checkmarks.</p> <table border="1"> <thead> <tr> <th>Port</th> <th>Zone</th> <th>Status</th> </tr> </thead> <tbody> <tr> <td>0</td> <td>us-east-1b</td> <td>healthy</td> </tr> <tr> <td>0</td> <td>us-east-1a</td> <td>healthy</td> </tr> </tbody> </table>	Port	Zone	Status	0	us-east-1b	healthy	0	us-east-1a	healthy
Port	Zone	Status									
0	us-east-1b	healthy									
0	us-east-1a	healthy									

2	<p>In the left navigation pane, choose Load Balancers and then choose Inventory-LB.</p> <p>In the Details tab in the lower half of the window, copy the DNS name to your clipboard.</p>	 <p>The screenshot shows the AWS EC2 Load Balancers console. The left sidebar lists services like Launch Templates, Spot Requests, Savings Plans, etc., with 'Load Balancers' under 'Load Balancing' expanded. Under 'Load Balancers', 'Inventory-LB' is selected. The main pane displays the 'Load balancers (1/1)' section with one entry for 'Inventory-LB'. Below it is the 'Load balancer: Inventory-LB' details panel, which includes fields for IP address type (IPv4), Date created (July 1, 2023, 23:42 (UTC+07:00)), Load balancer ARN (arn:aws:elasticloadbalancing:us-east-1:1928475043916:loadbalancer/app/Inventory-LB/d6a0227768c89ac5), and DNS name (Inventory-LB-1922099027.us-east-1.elb.amazonaws.com (A Record)).</p>
3	<p>Open a new web browser tab, paste the DNS name from your clipboard and press ENTER.</p> <p>The load balancer forwarded your request to one of the EC2 instances. The instance ID and Availability Zone are shown at the bottom of the webpage.</p> <p>Reload the page in your web browser. You should notice that the instance ID and Availability Zone sometimes toggles between the two instances.</p>	 <p>The screenshots show a web browser displaying the 'Inventory System' page. The top screenshot shows the page was generated by instance i-0635effe6e171a9d in Availability Zone us-east-1a. The bottom screenshot shows the page was generated by instance i-0bd9b609403bd7806 in Availability Zone us-east-1b. Both screenshots include a 'Please configure Settings to connect to database' message and a note at the bottom: 'This page was generated by instance i-0635effe6e171a9d in Availability Zone us-east-1a.' and 'This page was generated by instance i-0bd9b609403bd7806 in Availability Zone us-east-1b.'</p>

Task 6: Testing high availability

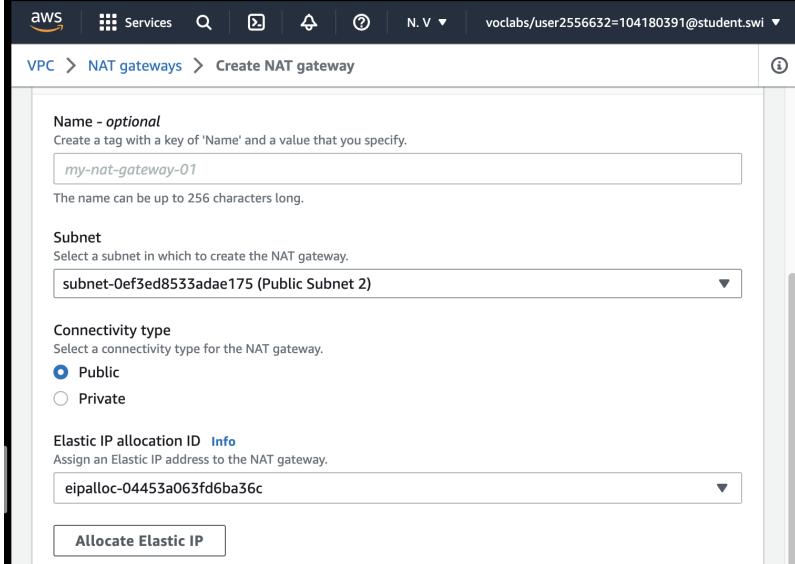
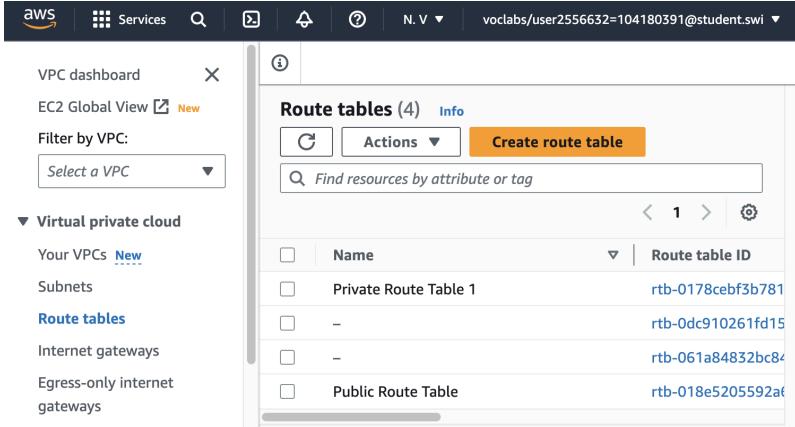
Step	Description	Screenshot
1	<p>In the left navigation pane, choose Instances.</p> <p>Select one of the Inventory-App instances.</p> <p>Choose Instance State > Terminate instance.</p> <p>Choose Terminate.</p>	 <p>The screenshot shows the AWS EC2 Instances page. A tooltip at the top right says: "Currently creating AMI ami-05f812ad6357d62b9 from instance i-0e2203c65434b98ac. Check that the AMI status is 'Available' before deleting the instance or carrying out other actions related to this AMI." Below the tooltip, the 'Instances (1/3) Info' section is visible. In the 'Actions' dropdown menu, the 'Terminate instance' option is highlighted with a blue box. The table below lists two instances: 'Inventory-App' (i-0bd9b609403bd7806, Running) and another 'Inventory-App' instance (i-0635ef7ee6e171a9d, Running).</p>
2	<p>Return to the web application tab in your web browser and reload the page several times.</p> <p>You should notice that the Availability Zone that is shown at the bottom of the page stays the same. Though an instance failed, your application remains available.</p> <p>After a few minutes, Amazon EC2 Auto Scaling will also notice the instance failure. It was configured to keep two instances running, so Amazon EC2 Auto Scaling will automatically launch a replacement instance.</p> <p>Return to the EC2 console tab where you have the instances list displayed. In the top-right area, choose the refresh icon every 30 seconds or so until a new EC2 instance appears.</p>	 <p>The screenshot shows the AWS EC2 Instances page after an instance has been terminated. The 'Instances (5) Info' section shows five instances listed: 'Inventory-App' (i-06a691daef30e760d, Running), 'Inventory-App' (i-07f85b1d91ff464eb, Running), 'Inventory-App' (i-0bd9b609403bd7806, Terminated), 'Web Server 1' (i-0e2203c65434b98ac, Running), and 'Inventory-App' (i-0635ef7ee6e171a9d, Terminated).</p>

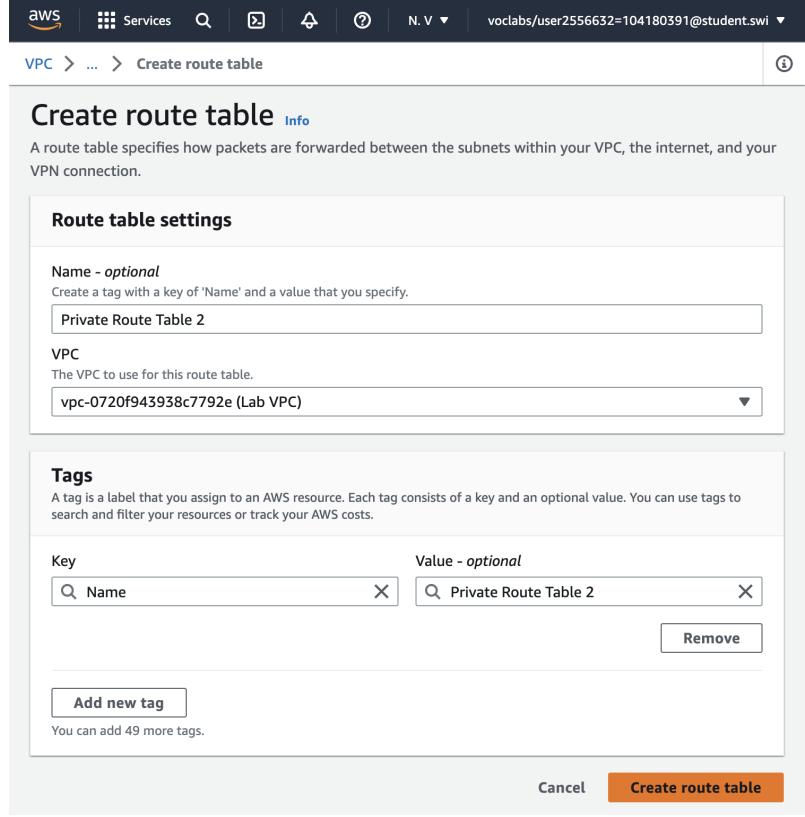
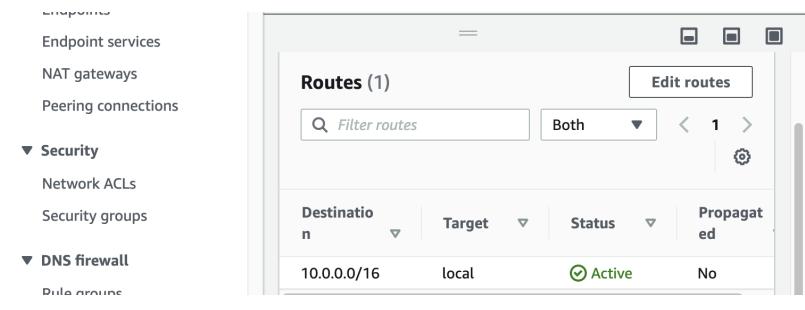
Optional task 1: Making the database highly available

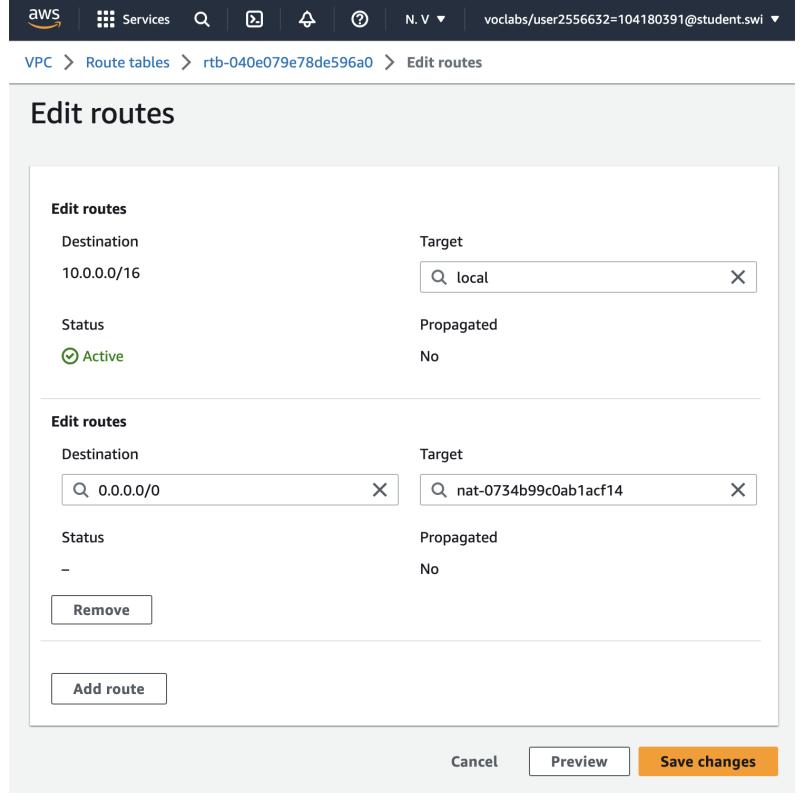
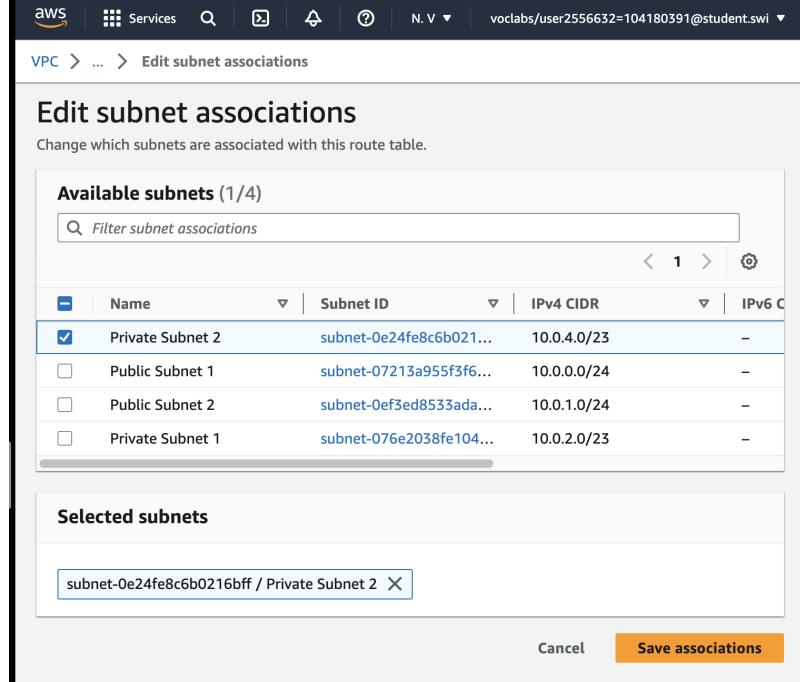
Step	Description	Screenshot
1	<p>On the Services menu, choose RDS.</p> <p>In the left navigation pane, choose Databases.</p> <p>Choose the link for the name of the inventory-db instance.</p> <p>Choose Modify</p>	
2	Scroll down to the Availability & durability section . For Multi-AZ deployment , select Create a standby instance .	
3	Scroll back up and for DB instance class , select db.t3.small .	
4	For Allocated storage , enter: 10	

5	<p>Under Schedule modifications, select Apply immediately.</p> <p>Choose Modify DB instance</p>	<p>The screenshot shows the 'Schedule modifications' section of the AWS RDS Modify DB instance wizard. It includes a list of other modification types like Reserved instances, Proxies, Subnet groups, Parameter groups, Option groups, Custom engine versions, Zero-ETL integrations, Events, Event subscriptions, Recommendations (4), and Certificate update. The 'Apply immediately' option is selected. A warning message states: 'Potential performance impact when converting to Multi-AZ. Your DB instance can experience a significant performance impact during and after converting to a Multi-AZ deployment. The impact is greater on DB instances with large amounts of storage and write-intensive workloads. We don't recommend this conversion on a production DB instance.' Buttons at the bottom include 'Cancel', 'Back', and a prominent orange 'Modify DB instance' button.</p>
---	--	--

Step	Description	Screenshot
1	<p>On the Services menu, choose VPC.</p> <p>In the left navigation pane, choose NAT gateways.</p>	<p>The screenshot shows the AWS VPC dashboard with the 'NAT gateways' section. It displays one entry: 'nat-021f47589be5e46a1'. There are buttons for 'Actions' and 'Create NAT gateway'.</p>

2	<p>Choose Create NAT gateway and configure these settings:</p> <ul style="list-style-type: none"> - Subnet: Public Subnet 2 - Choose Allocate Elastic IP - Choose Create NAT gateway 											
3	<p>In the left navigation pane, choose Route tables.</p>	 <table border="1" data-bbox="833 1058 1563 1248"> <thead> <tr> <th>Name</th> <th>Route table ID</th> </tr> </thead> <tbody> <tr> <td>Private Route Table 1</td> <td>rtb-0178cebf3b781</td> </tr> <tr> <td>-</td> <td>rtb-0dc910261fd15</td> </tr> <tr> <td>-</td> <td>rtb-061a84832bc84</td> </tr> <tr> <td>Public Route Table</td> <td>rtb-018e5205592a6</td> </tr> </tbody> </table>	Name	Route table ID	Private Route Table 1	rtb-0178cebf3b781	-	rtb-0dc910261fd15	-	rtb-061a84832bc84	Public Route Table	rtb-018e5205592a6
Name	Route table ID											
Private Route Table 1	rtb-0178cebf3b781											
-	rtb-0dc910261fd15											
-	rtb-061a84832bc84											
Public Route Table	rtb-018e5205592a6											

4	<p>Choose Create route table and configure these settings:</p> <ul style="list-style-type: none"> - Name: Private Route Table 2 - VPC: Lab VPC - Choose Create route table. 	 <p>The screenshot shows the 'Create route table' wizard. In the 'Route table settings' section, the name is set to 'Private Route Table 2' and the VPC is set to 'vpc-0720f943938c7792e (Lab VPC)'. In the 'Tags' section, there is one tag named 'Name' with the value 'Private Route Table 2'. The 'Create route table' button is highlighted in orange at the bottom.</p>								
5	<p>Choose Edit routes and then configure these settings</p>	 <p>The screenshot shows the 'Routes' table. There is one route entry listed:</p> <table border="1"> <thead> <tr> <th>Destination</th> <th>Target</th> <th>Status</th> <th>Propagated</th> </tr> </thead> <tbody> <tr> <td>10.0.0.0/16</td> <td>local</td> <td>Active</td> <td>No</td> </tr> </tbody> </table>	Destination	Target	Status	Propagated	10.0.0.0/16	local	Active	No
Destination	Target	Status	Propagated							
10.0.0.0/16	local	Active	No							

6	<p>Choose Add route</p> <ul style="list-style-type: none"> - Destination: 0.0.0.0/0 - Target: Select NAT Gateway, then select the nat- entry that is not the entry for _NATGateway1 - Choose Save changes 	 <p>The screenshot shows the 'Edit routes' section of the AWS VPC console. It displays two route entries. The first entry has a Destination of 10.0.0.0/16 and a Target of 'local'. The second entry has a Destination of 0.0.0.0/0 and a Target of 'nat-0734b99c0ab1acf14'. Both entries are marked as 'Propagated' and 'No' for 'Local'. There are 'Remove' and 'Add route' buttons at the bottom.</p>
7	<p>Choose the Subnet associations tab.</p> <p>Choose Edit subnet associations</p> <p>Select Private Subnet 2.</p> <p>Choose Save associations</p>	 <p>The screenshot shows the 'Edit subnet associations' section of the AWS VPC console. It lists available subnets and selected subnets. In the 'Available subnets' table, 'Private Subnet 2' is checked. In the 'Selected subnets' list, 'subnet-0e24fe8c6b0216bff / Private Subnet 2' is listed. There are 'Cancel' and 'Save associations' buttons at the bottom.</p>