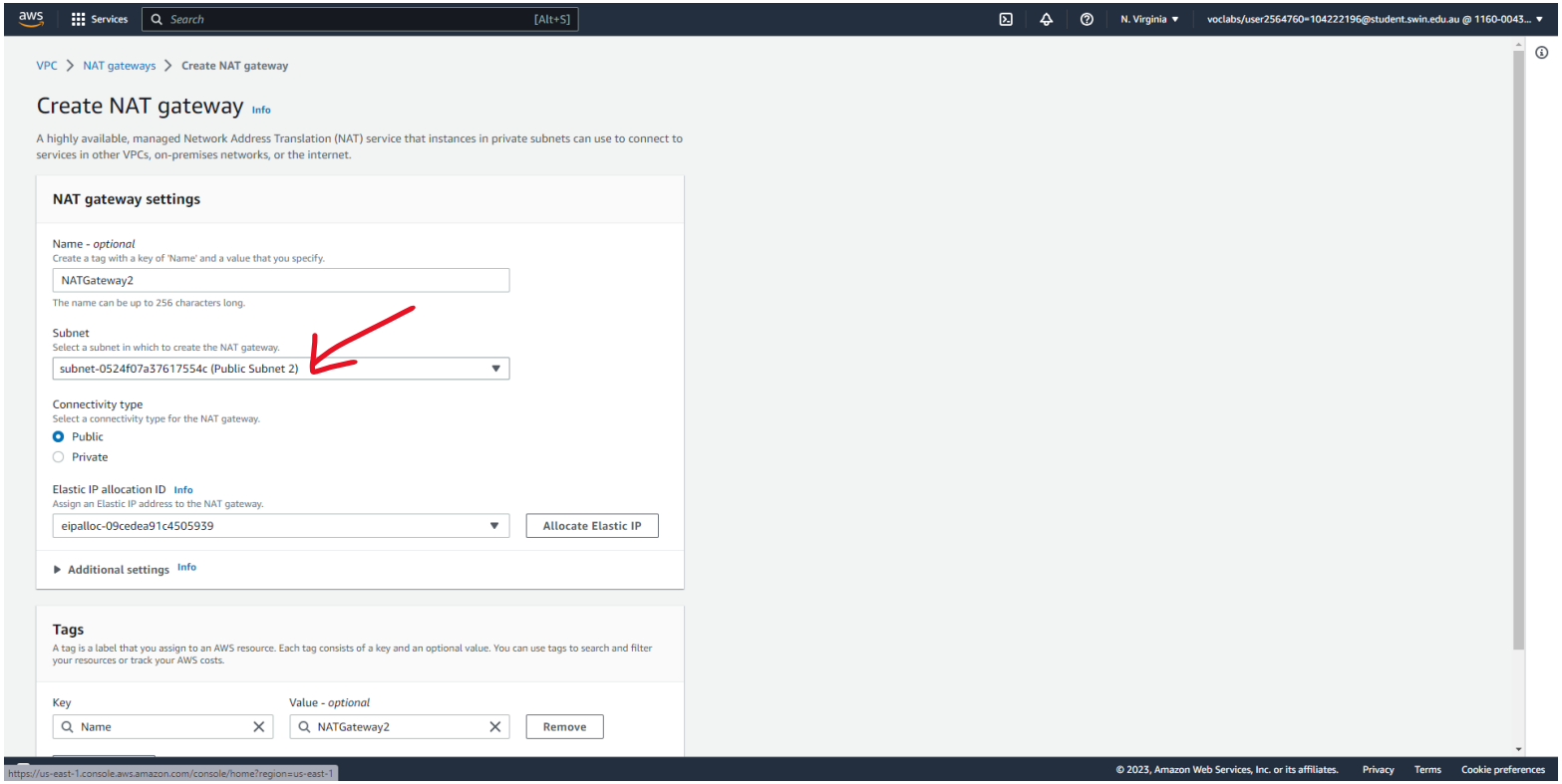
Ta Quang Tung – 104222196

COS20019 – Cloud Computing Architecture - Wk10: ACA Module 9 Challenge Lab - Creating a Scalable and Highly Available Environment for the Café

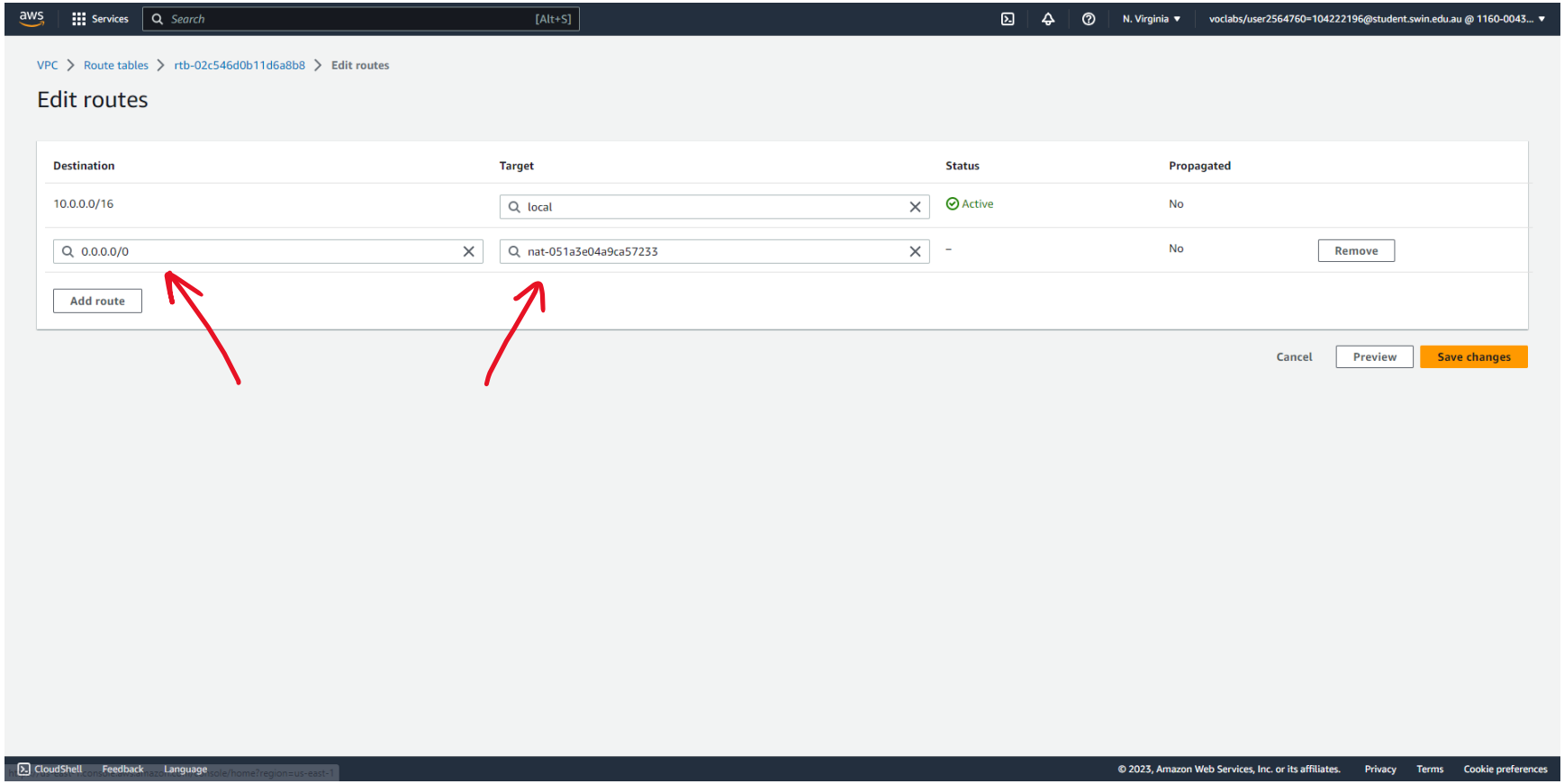
Task 1 - Inspecting your environment

The initial environment is explored on AWS and related questions are answered on Canvas.

Task 2 - Creating a NAT gateway for the second Availability Zone

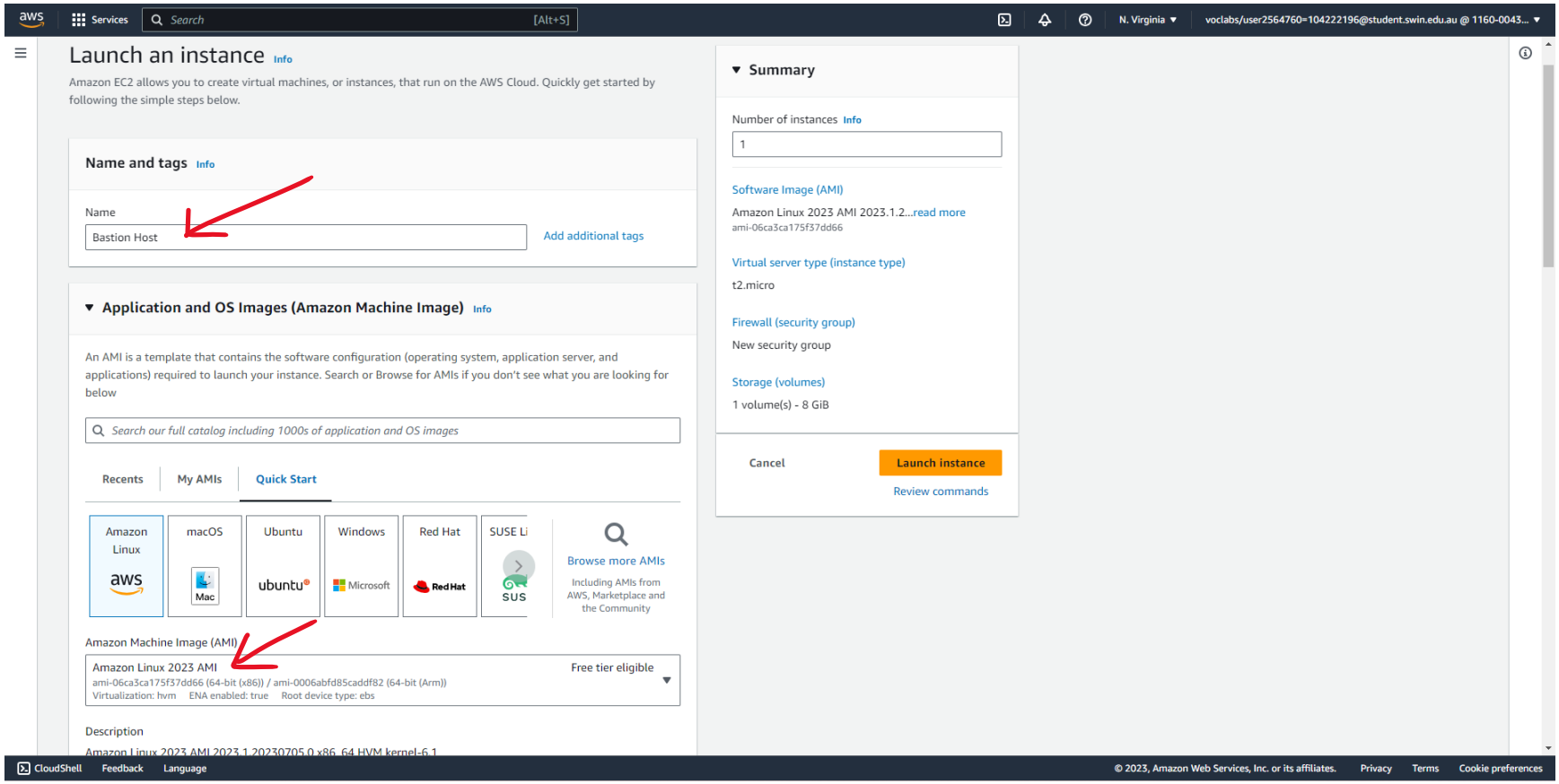


Create a NAT gateway in Public Subnet 2, which is in the second Availability Zone.

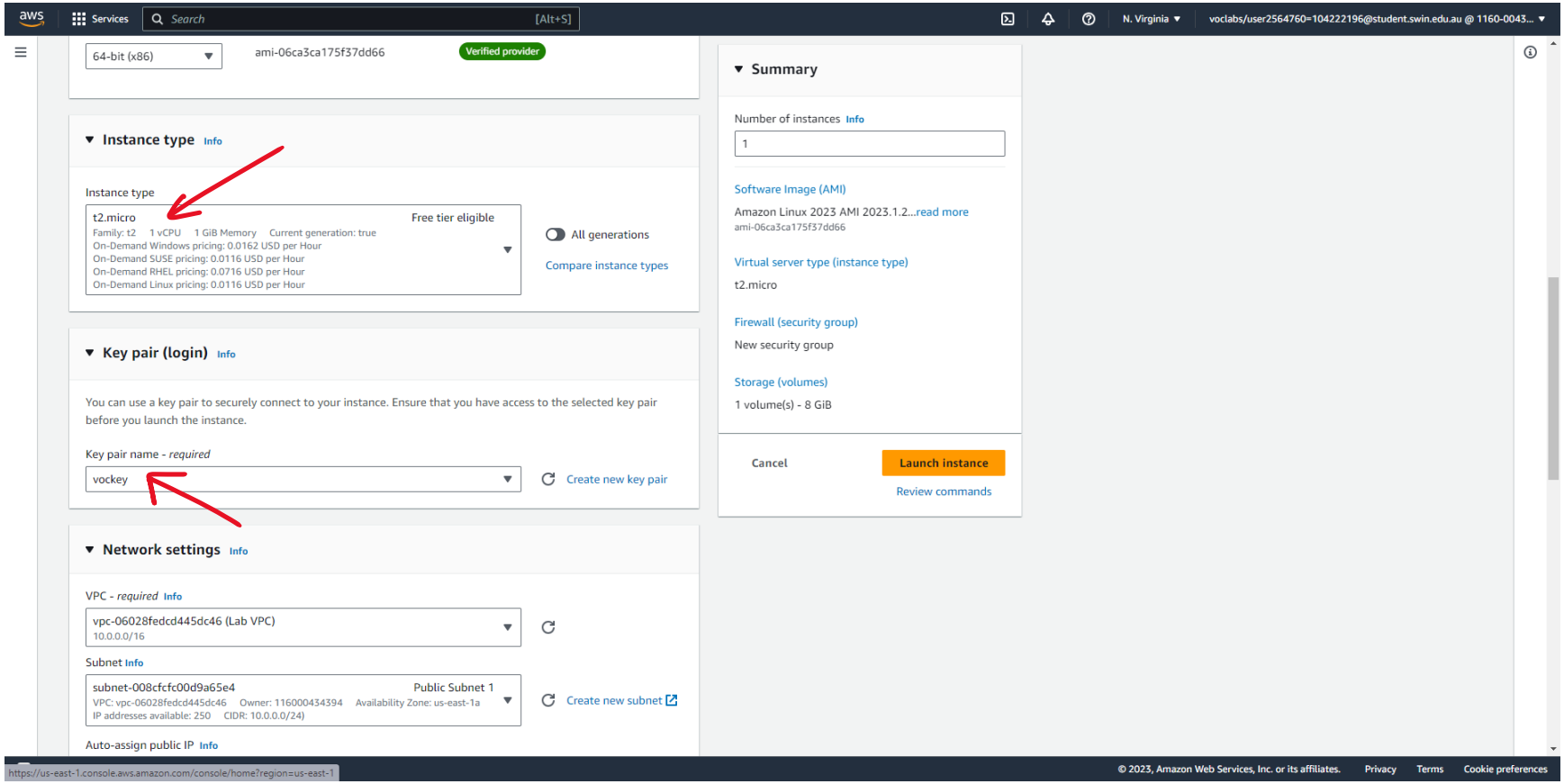


In the route table of Private Subnet 2, create a route that directs all Internet-bound traffic to the newly created NAT gateway.

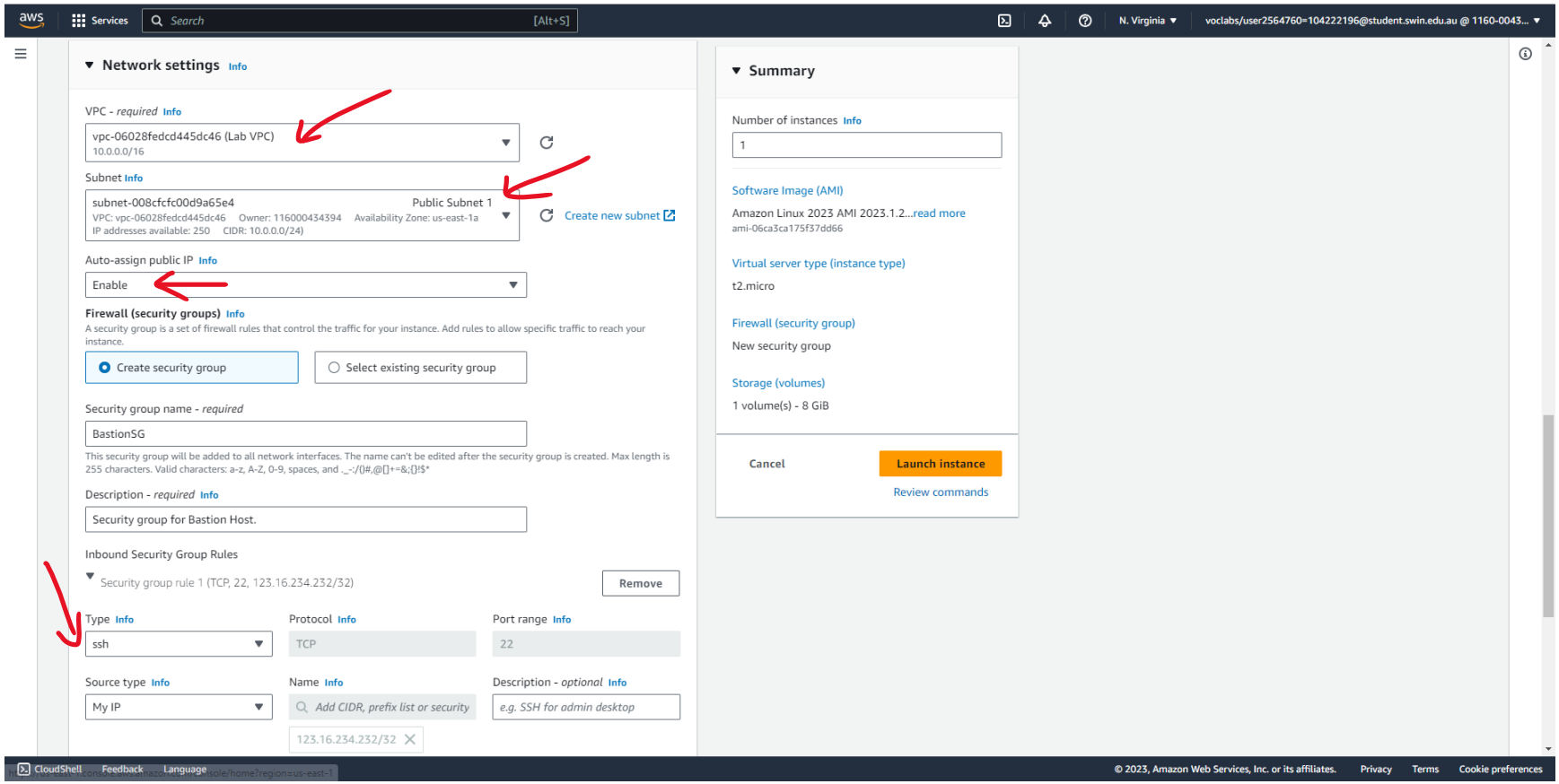
Task 3 - Creating a bastion host instance in a public subnet



Create a bastion host instance (part 1/3), specifying its name and AMI.

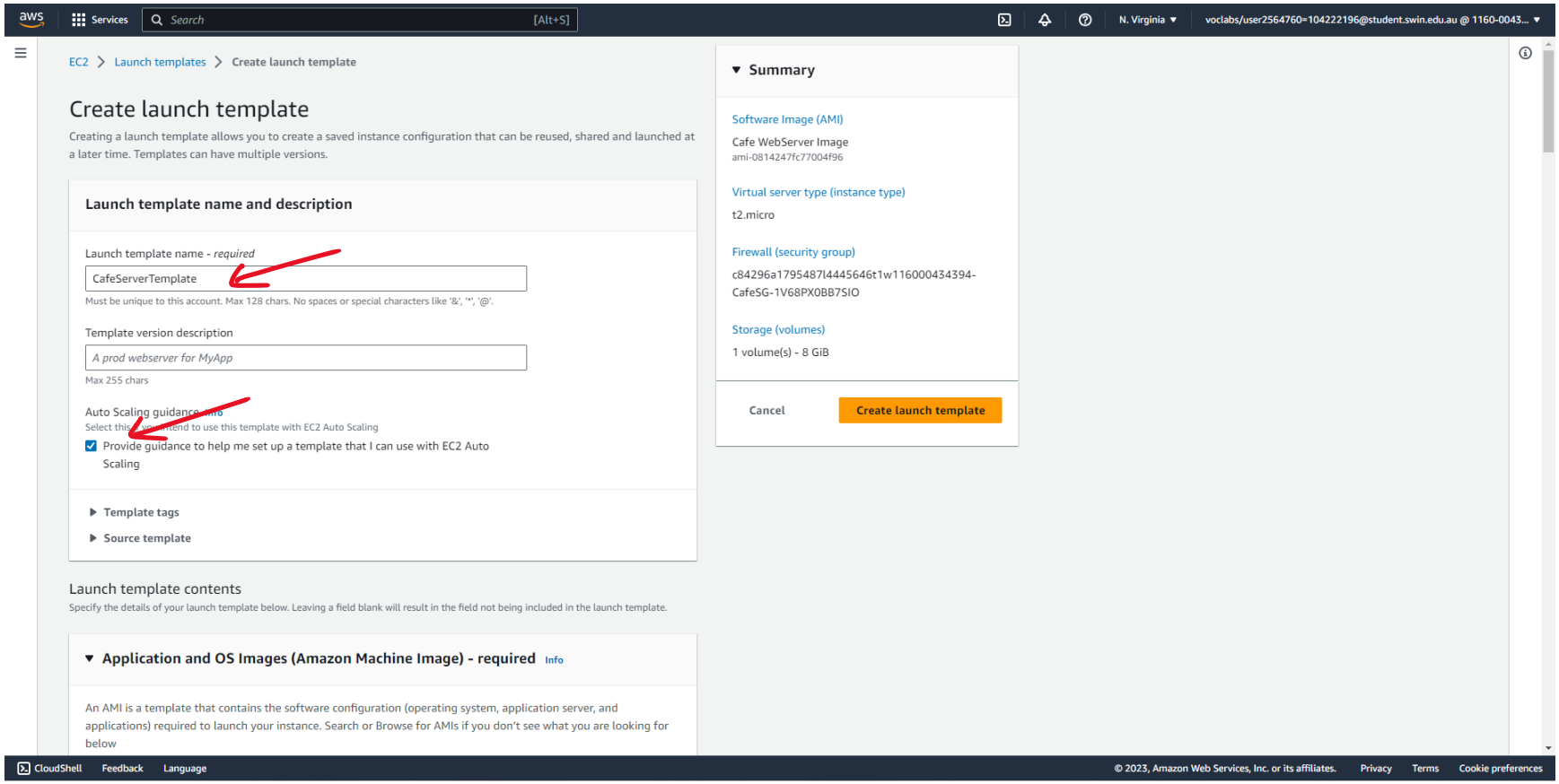


Create a bastion host instance (part 2/3), specifying its instance type and key pair.

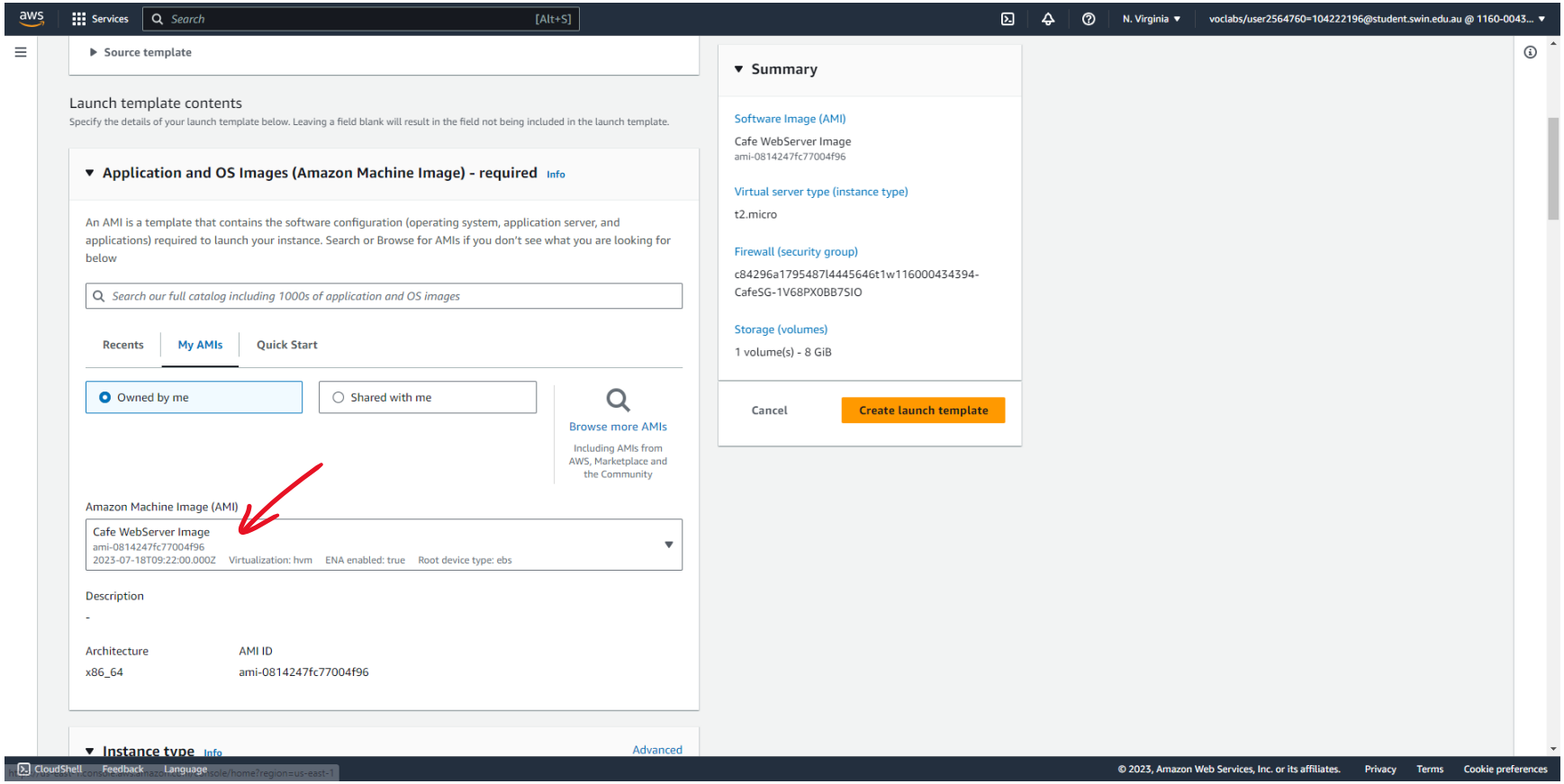


Create a bastion host instance (part 3/3), specifying its network settings such as VPC, subnet, IP, and security group. The security group allows only SSH traffic from “My IP”.

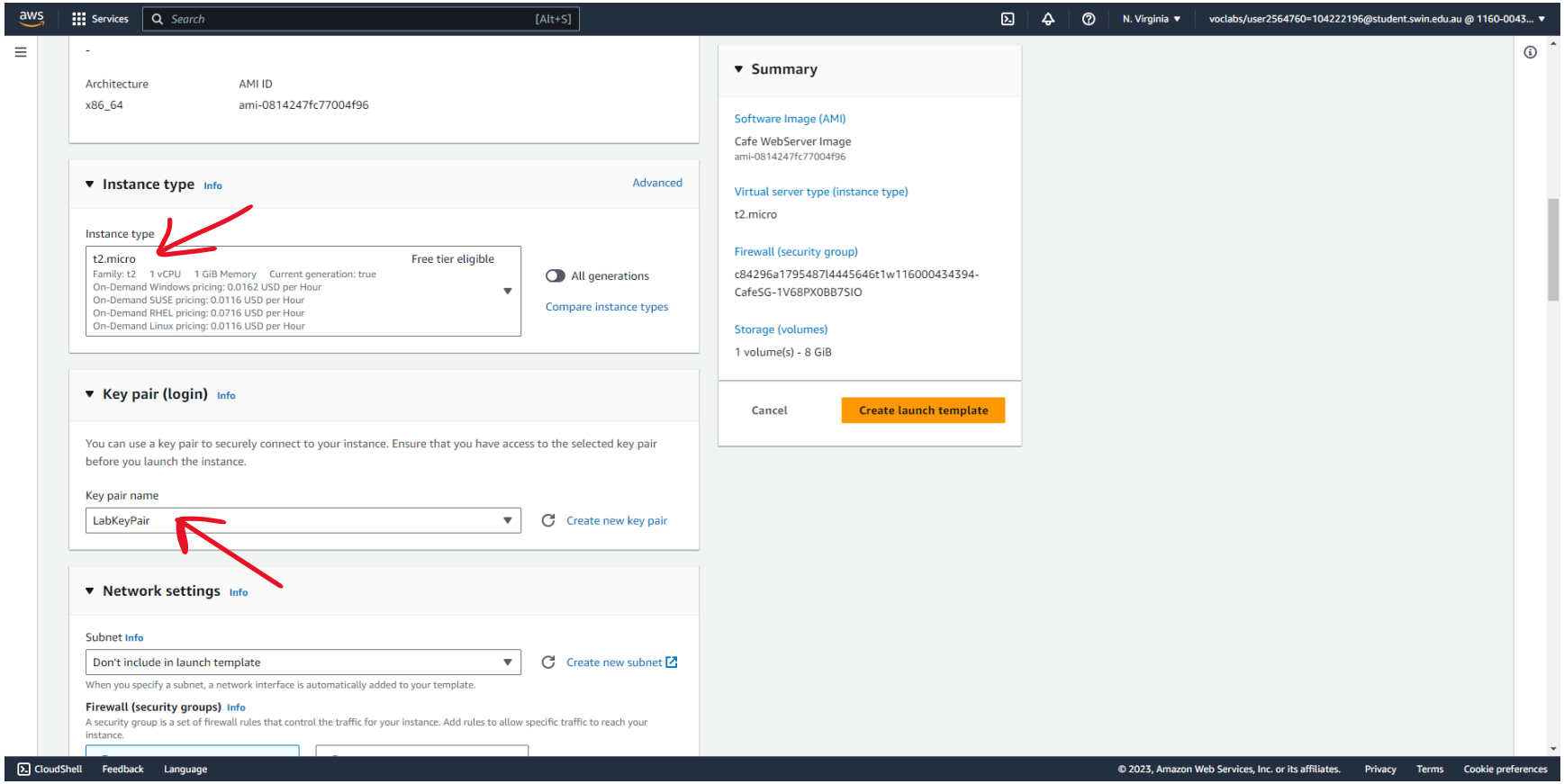
Task 4 - Creating a launch template



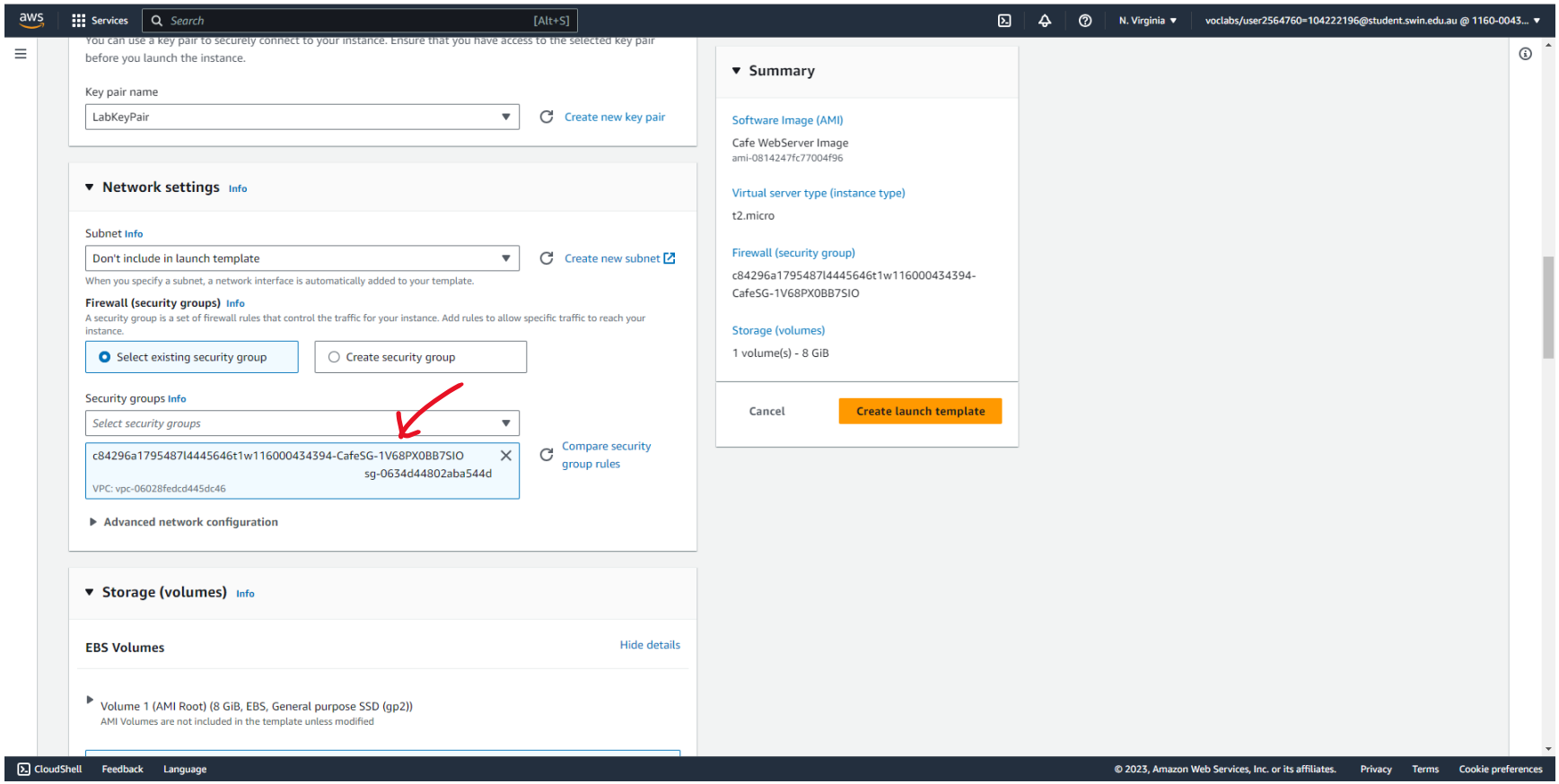
Create a launch template (part 1/5), specifying its name and enabling “provide guidance for ASG”.



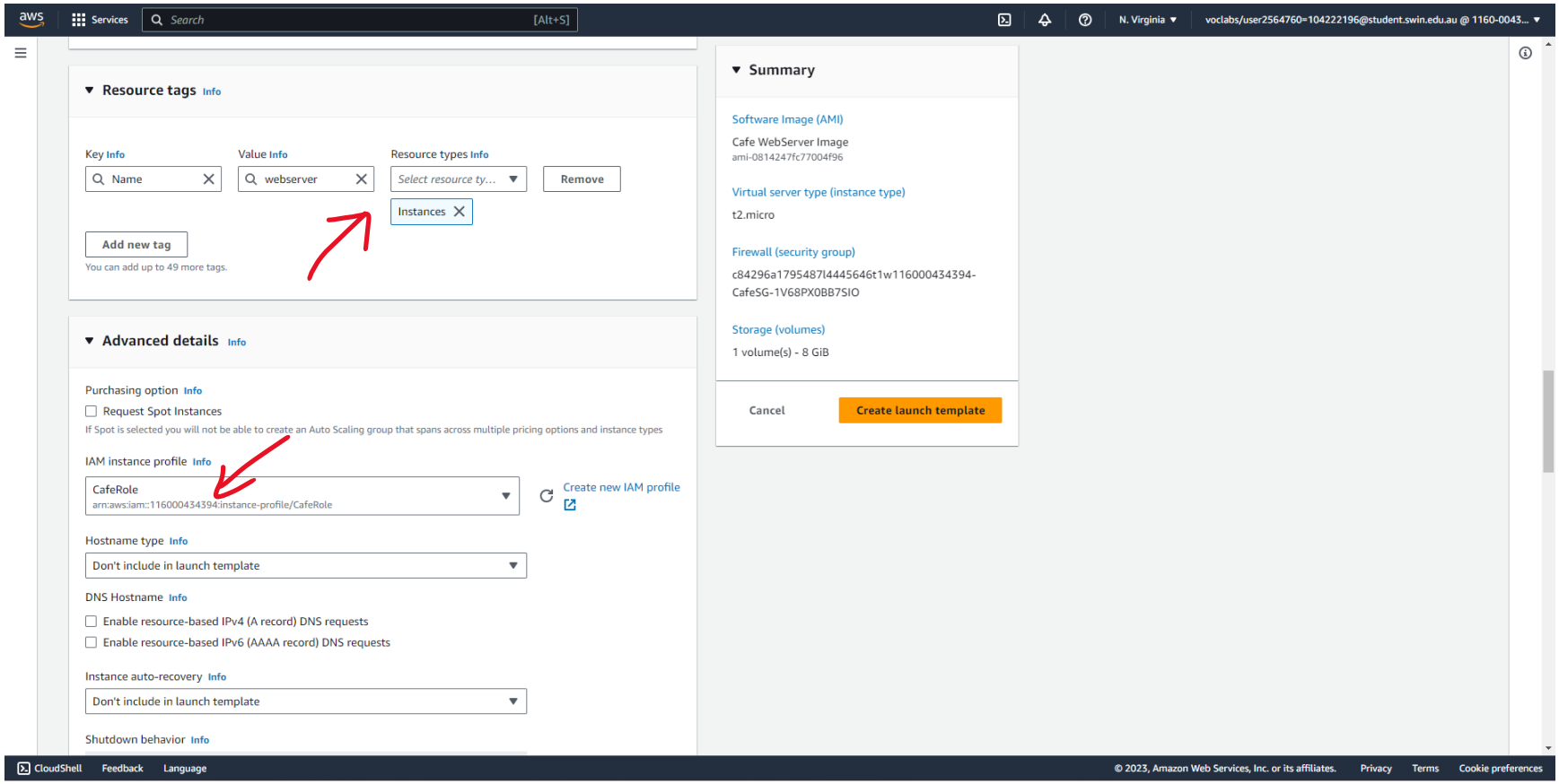
Create a launch template (part 2/5), specifying the correct Cafe WebServer Image AMI.



Create a launch template (part 3/5), specifying its instance type and key pair, which is a new key pair.

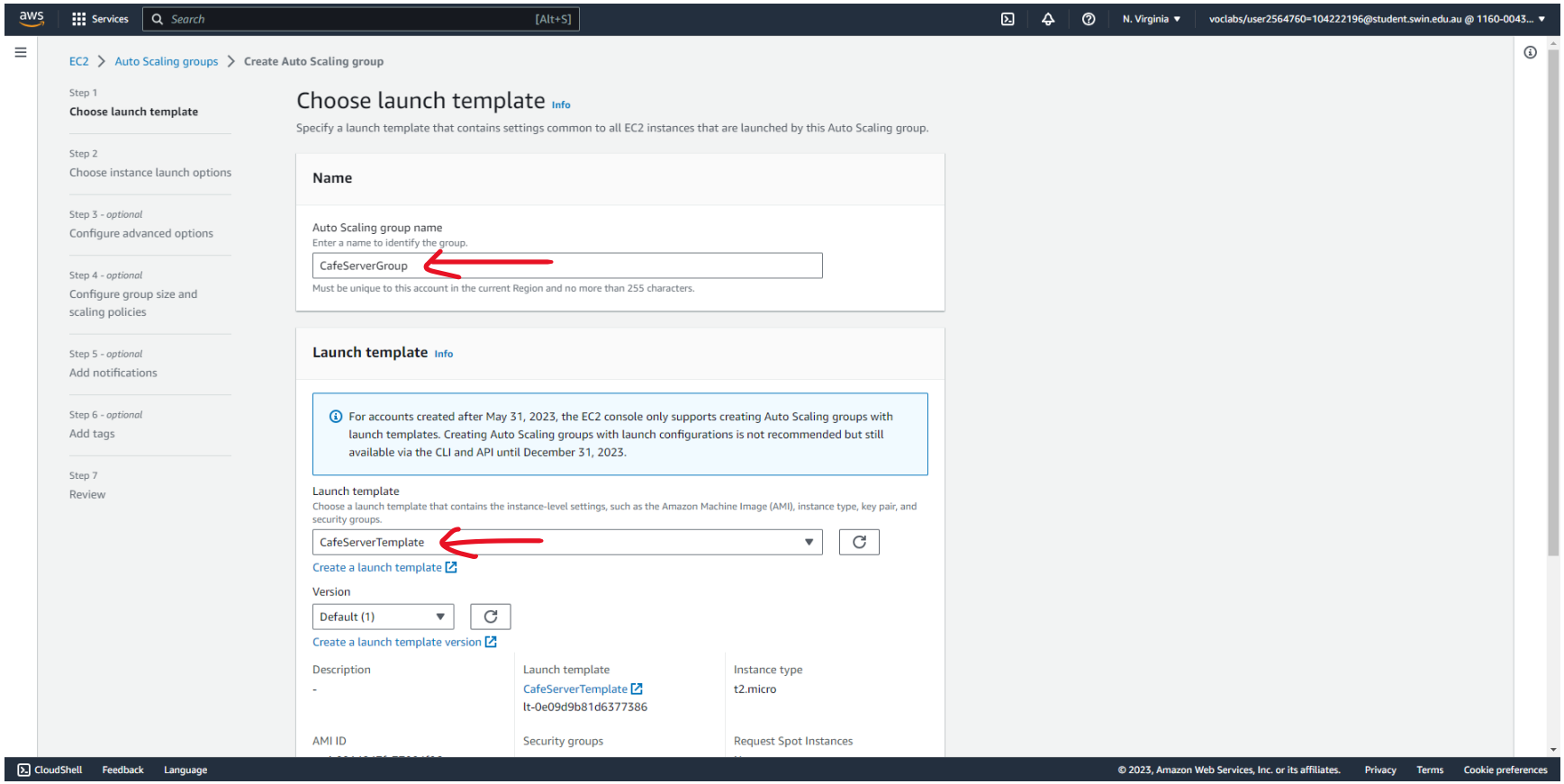


Create a launch template (part 4/5), specifying its security group.

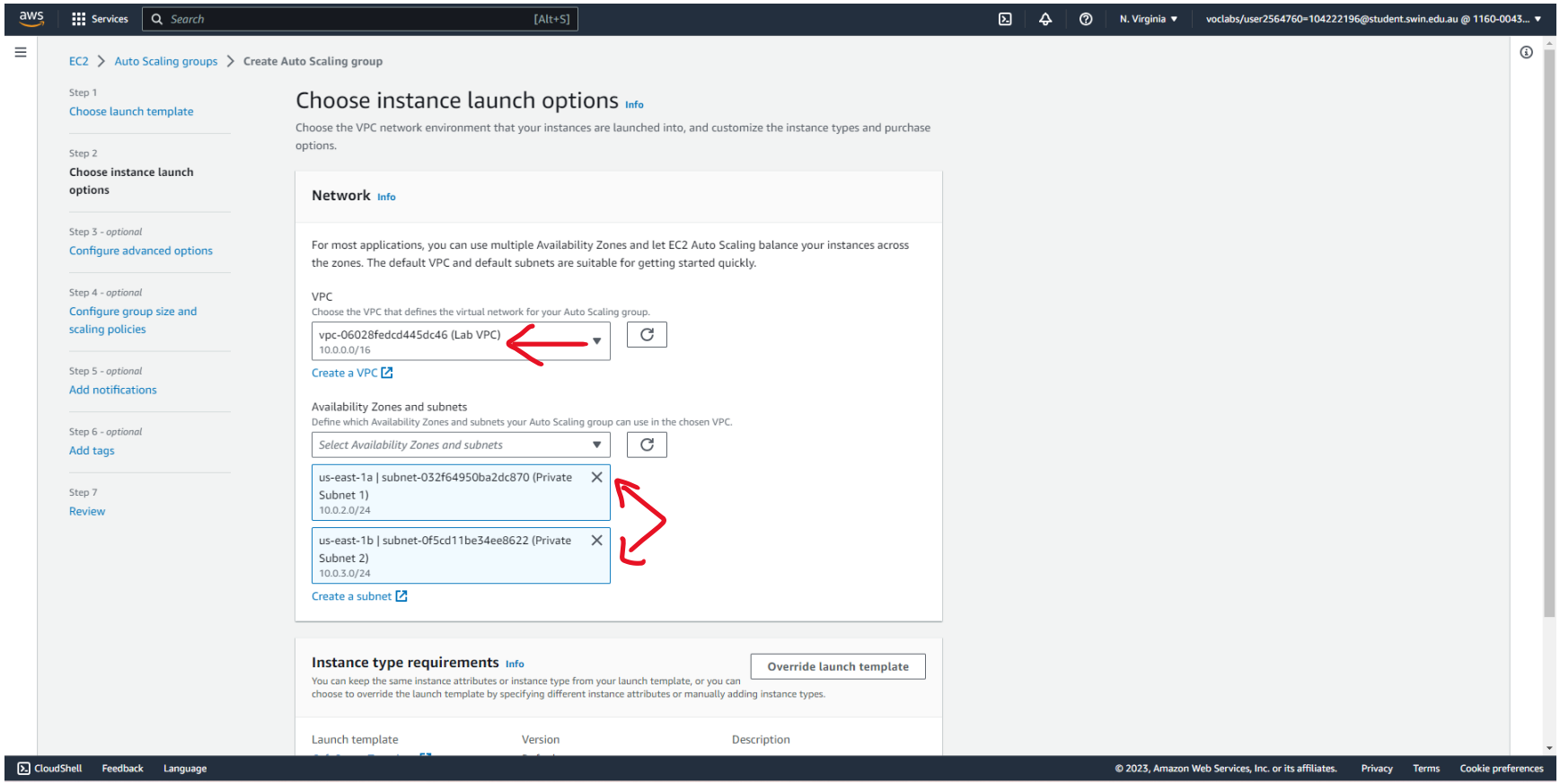


Create a launch template (part 5/5), specifying its resource tag and IAM role of CafeRole.

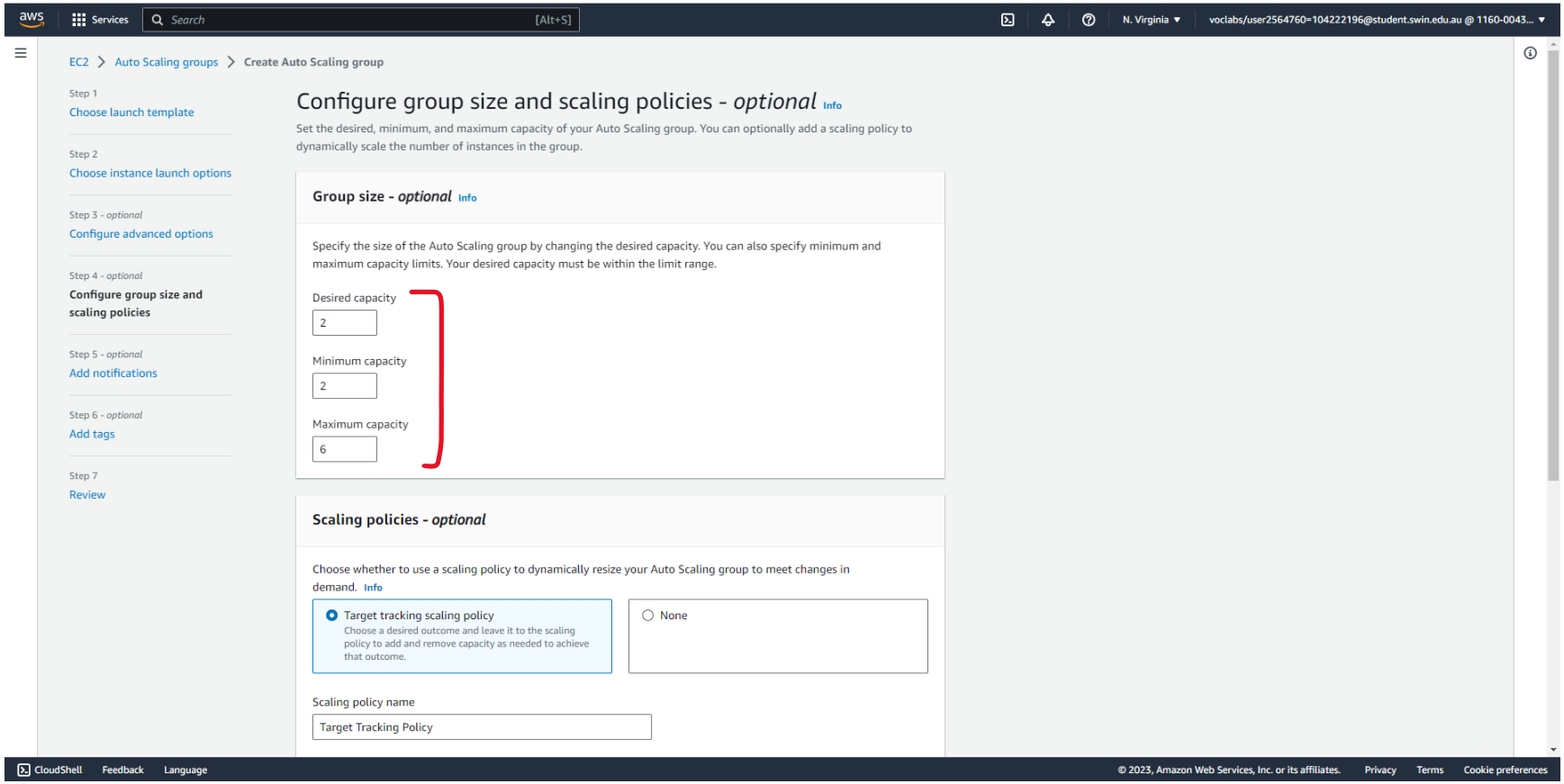
Task 5 - Creating an Auto Scaling group



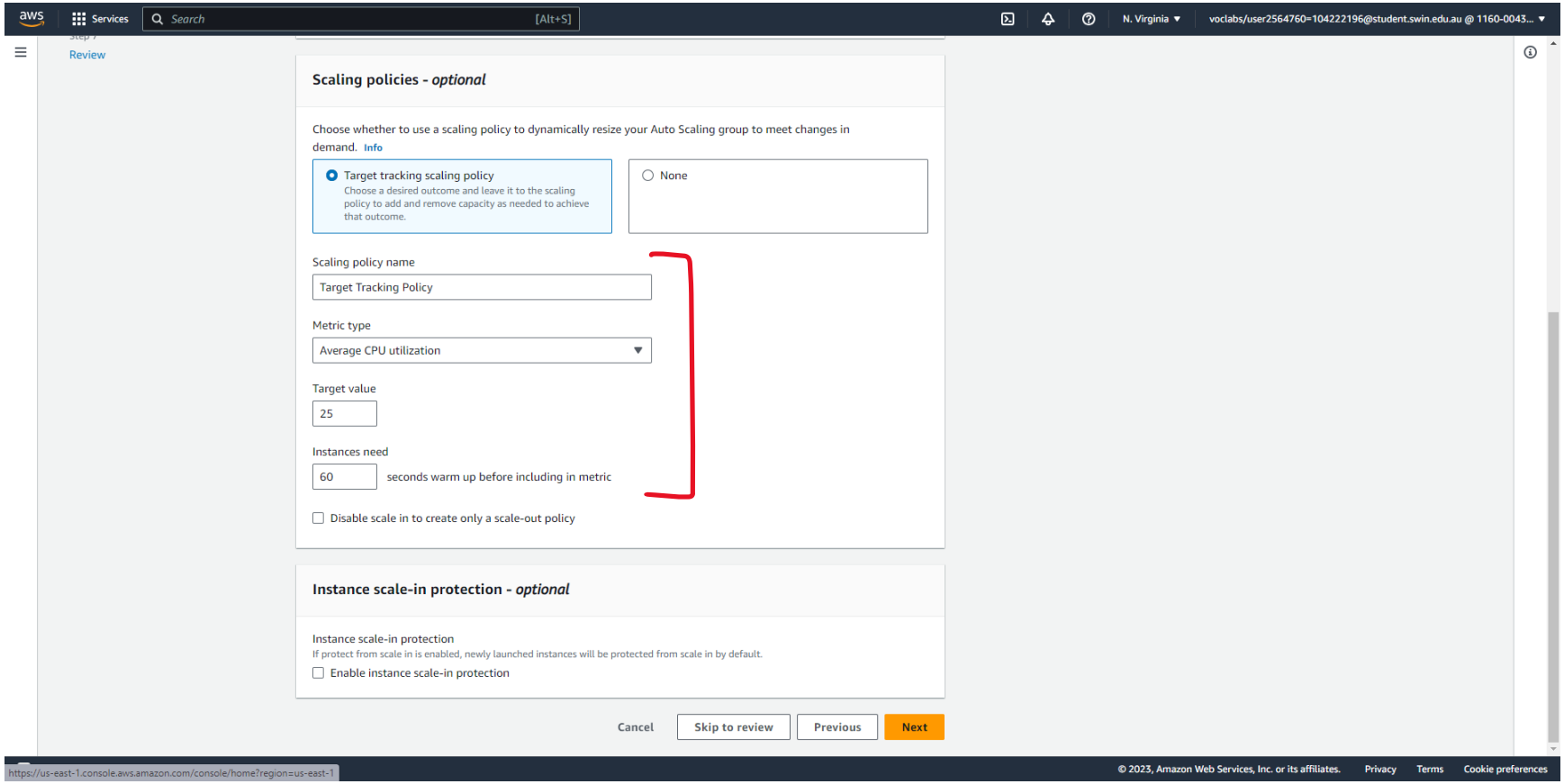
Create an auto-scaling group (part 1/4), specifying its name and launch template.



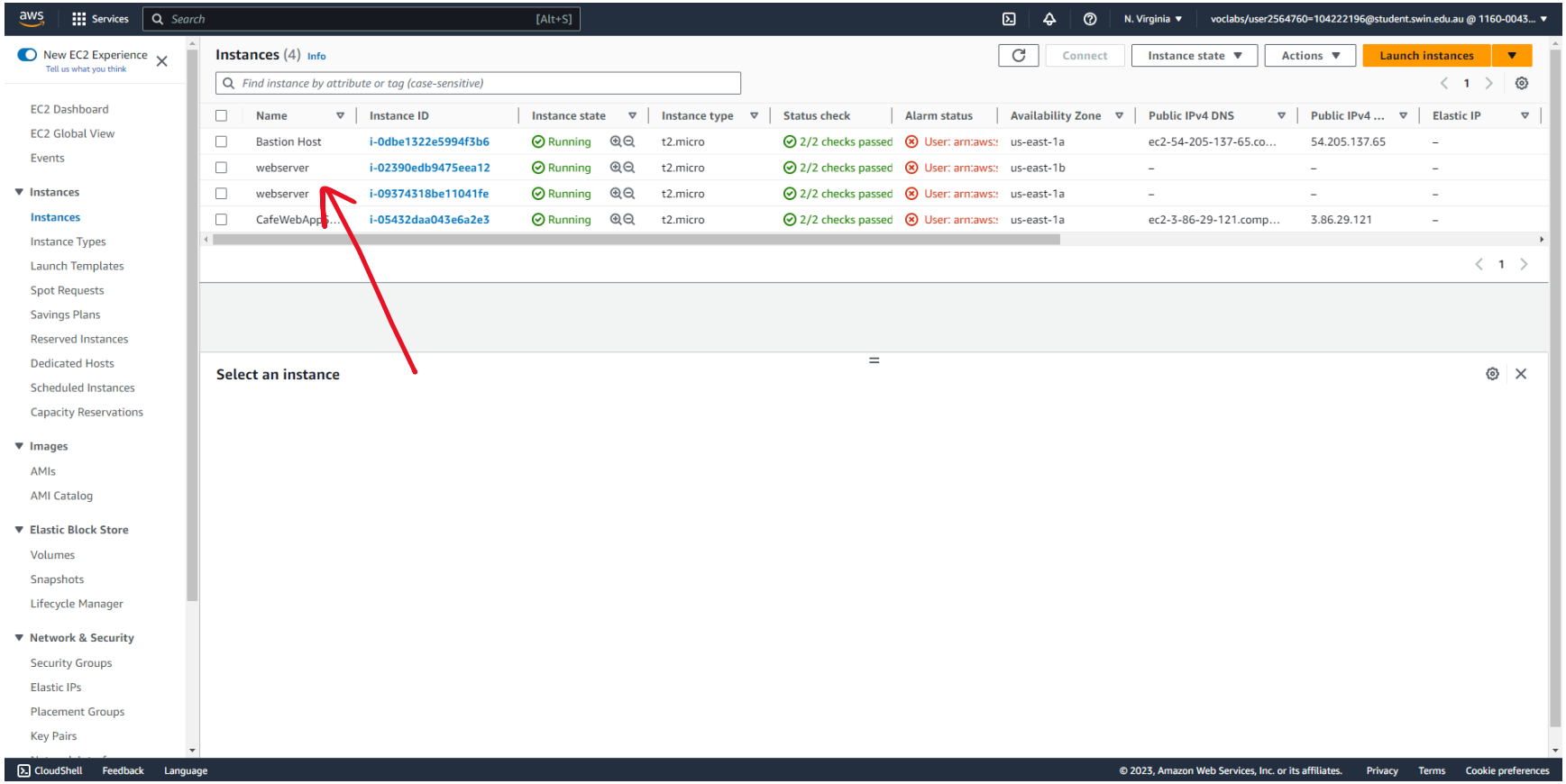
Create an auto-scaling group (part 2/4), specifying its VPC and subnets.



Create an auto-scaling group (part 3/4), specifying its group size.

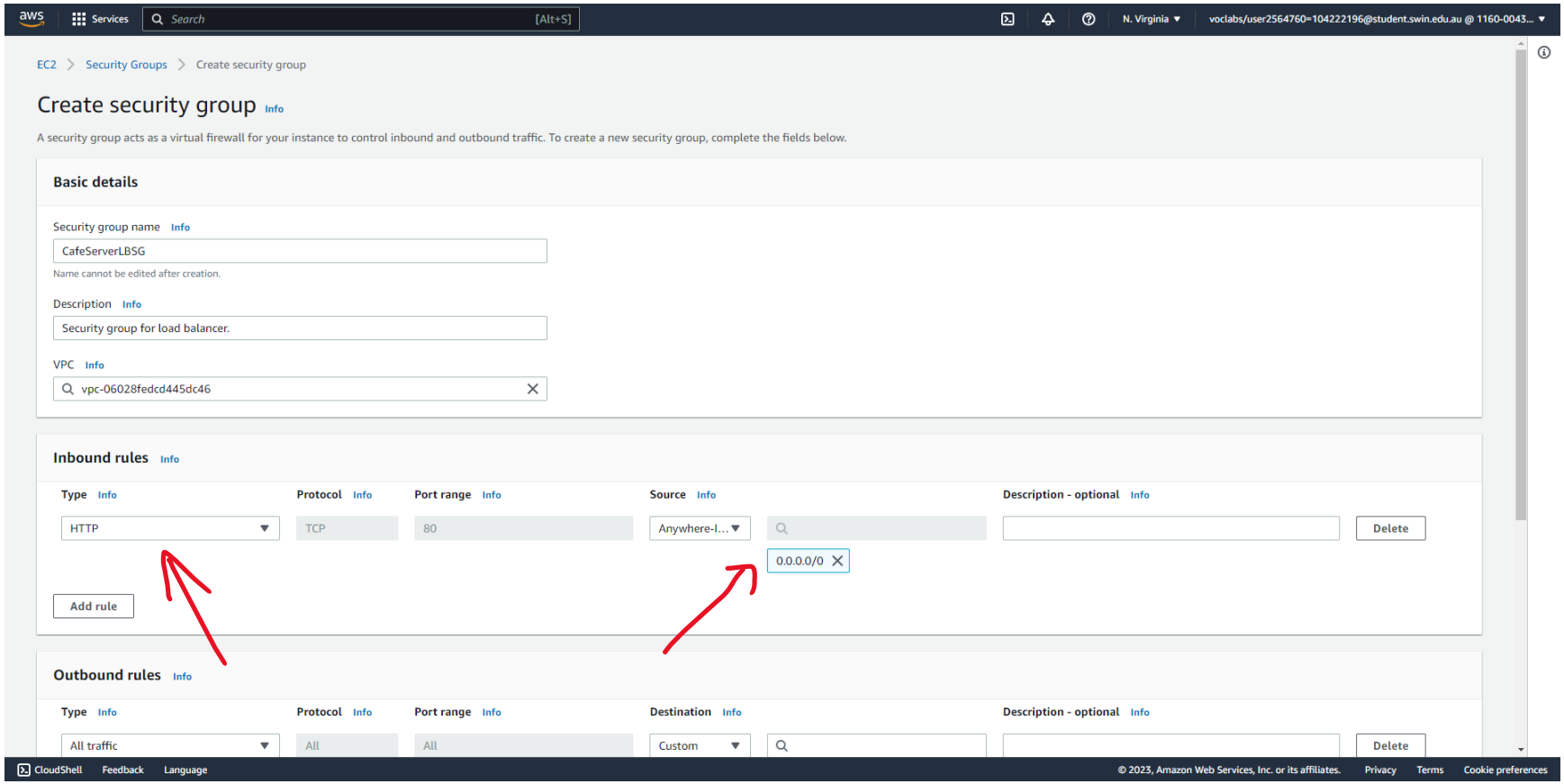


Create an auto-scaling group (part 4/4), specifying its scaling policy.

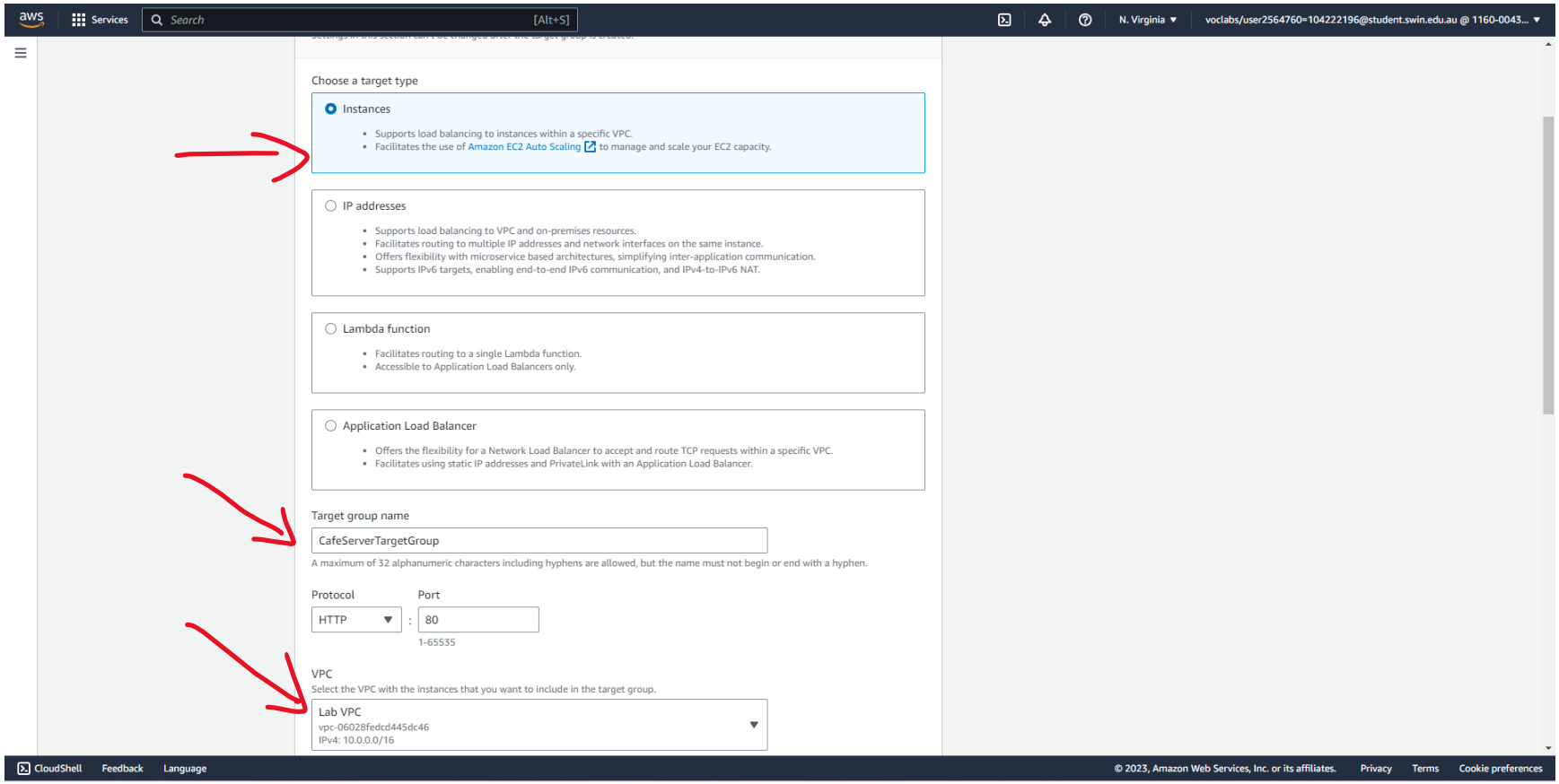


After the ASG has been successfully created, two instances are automatically created.

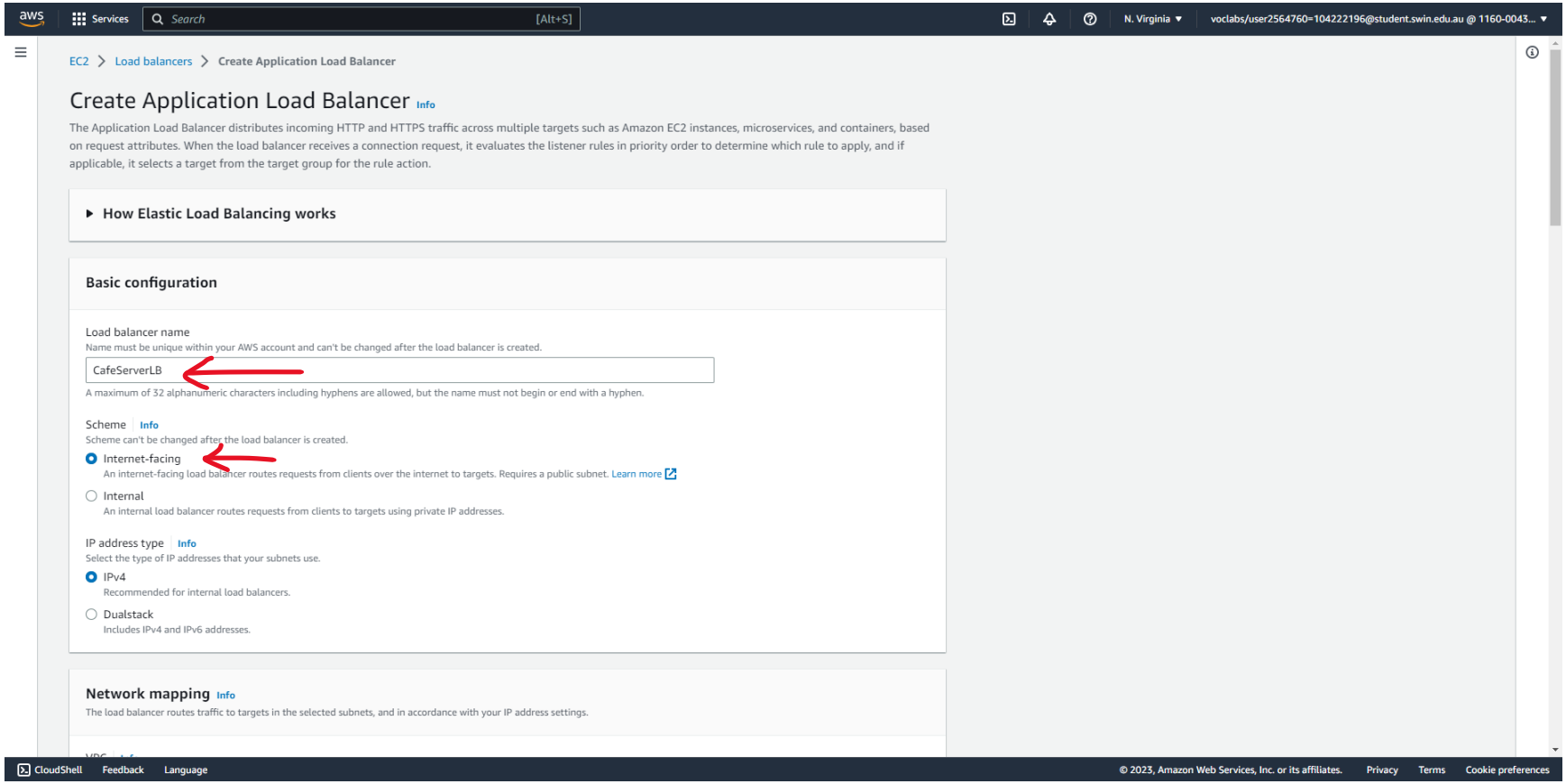
Task 6 - Creating a load balancer



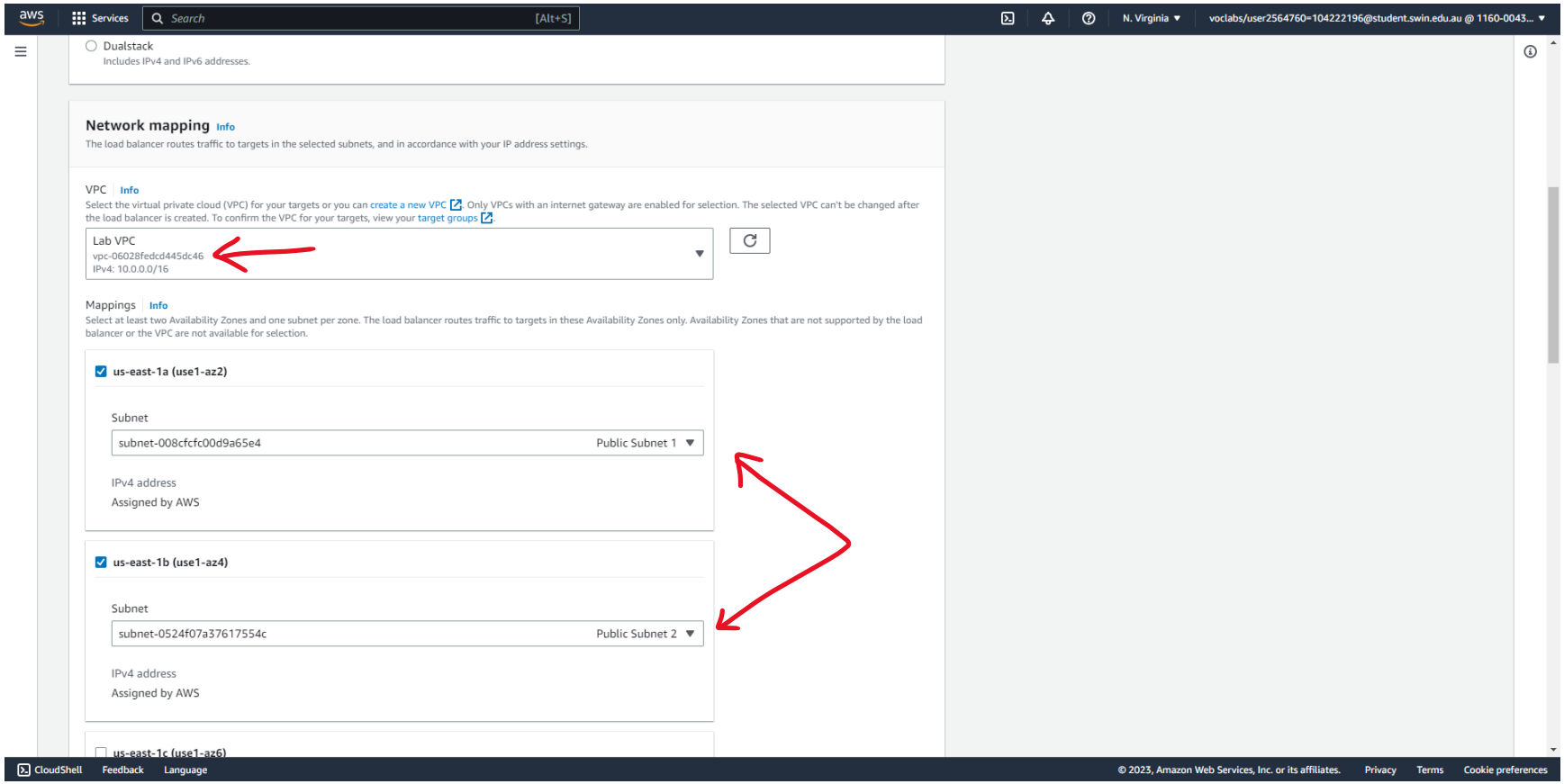
Create a security group for the load balancer that allows inbound HTTP traffic from anywhere.



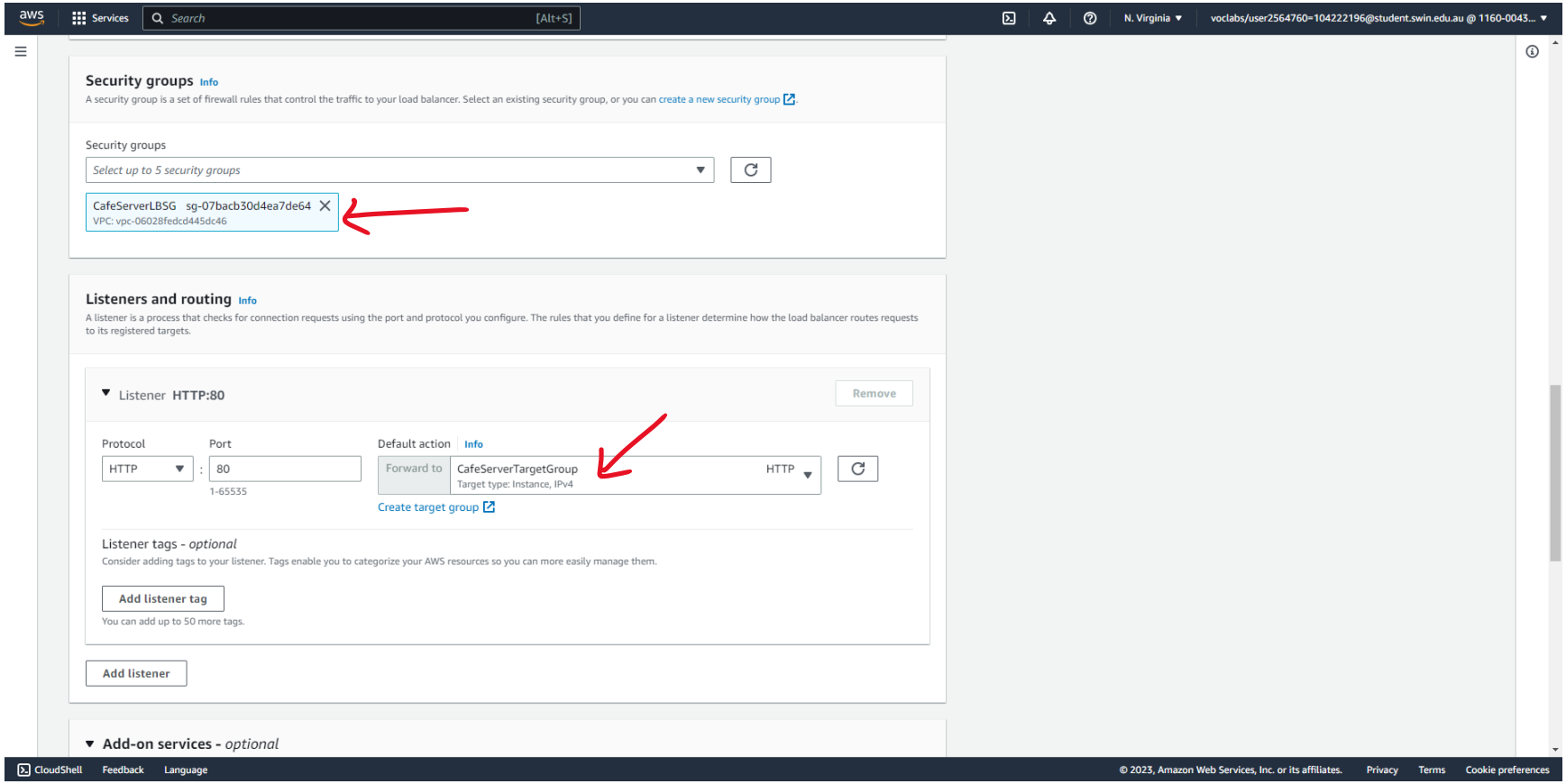
Create a target group for the load balancer in the Lab VPC.



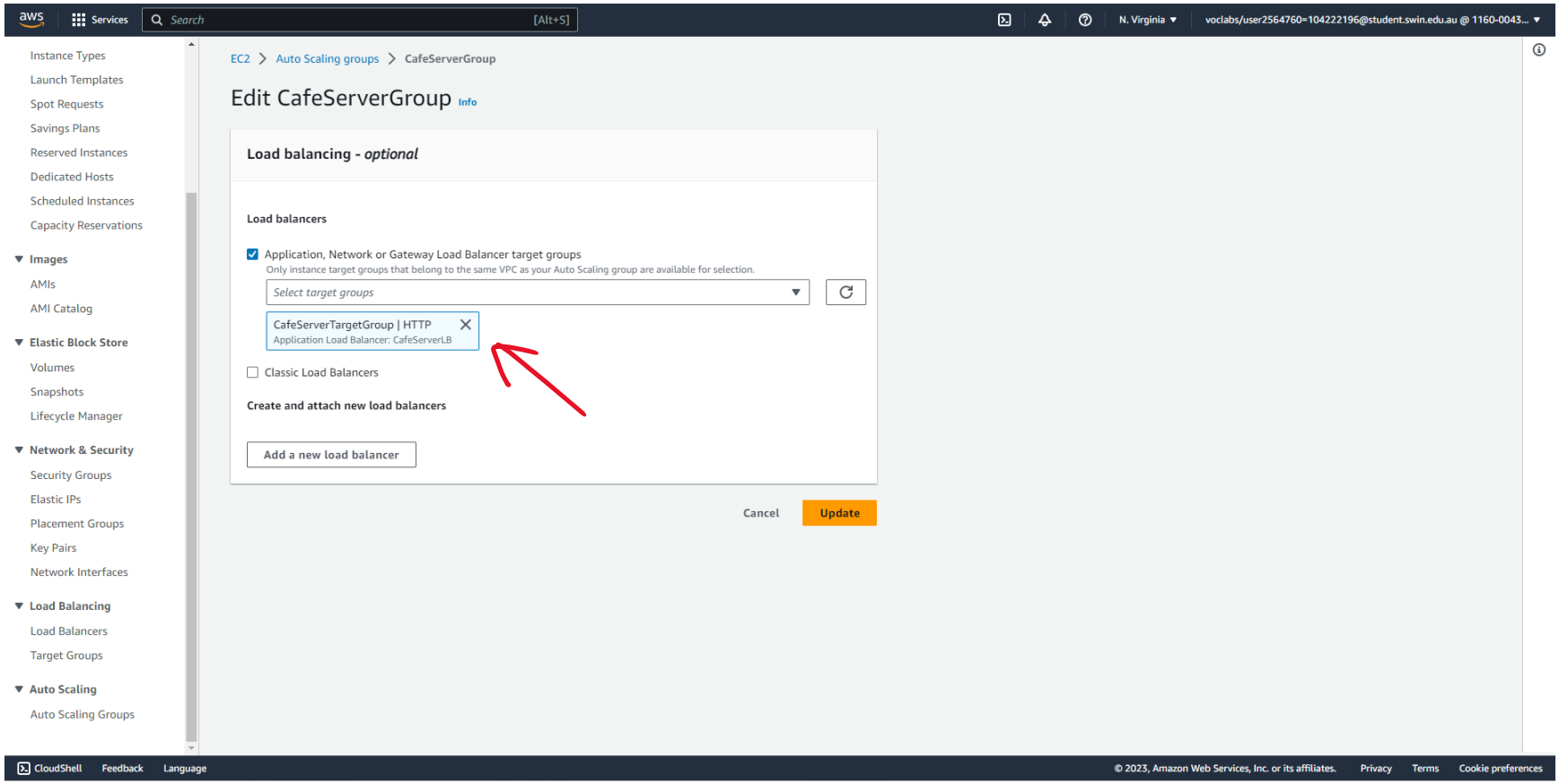
Create an Application Load Balancer (part 1/3), specifying its name and selecting the Internet-facing scheme.



Create an Application Load Balancer (part 2/3), specifying the Lab VPC and the two public subnets under network mapping.

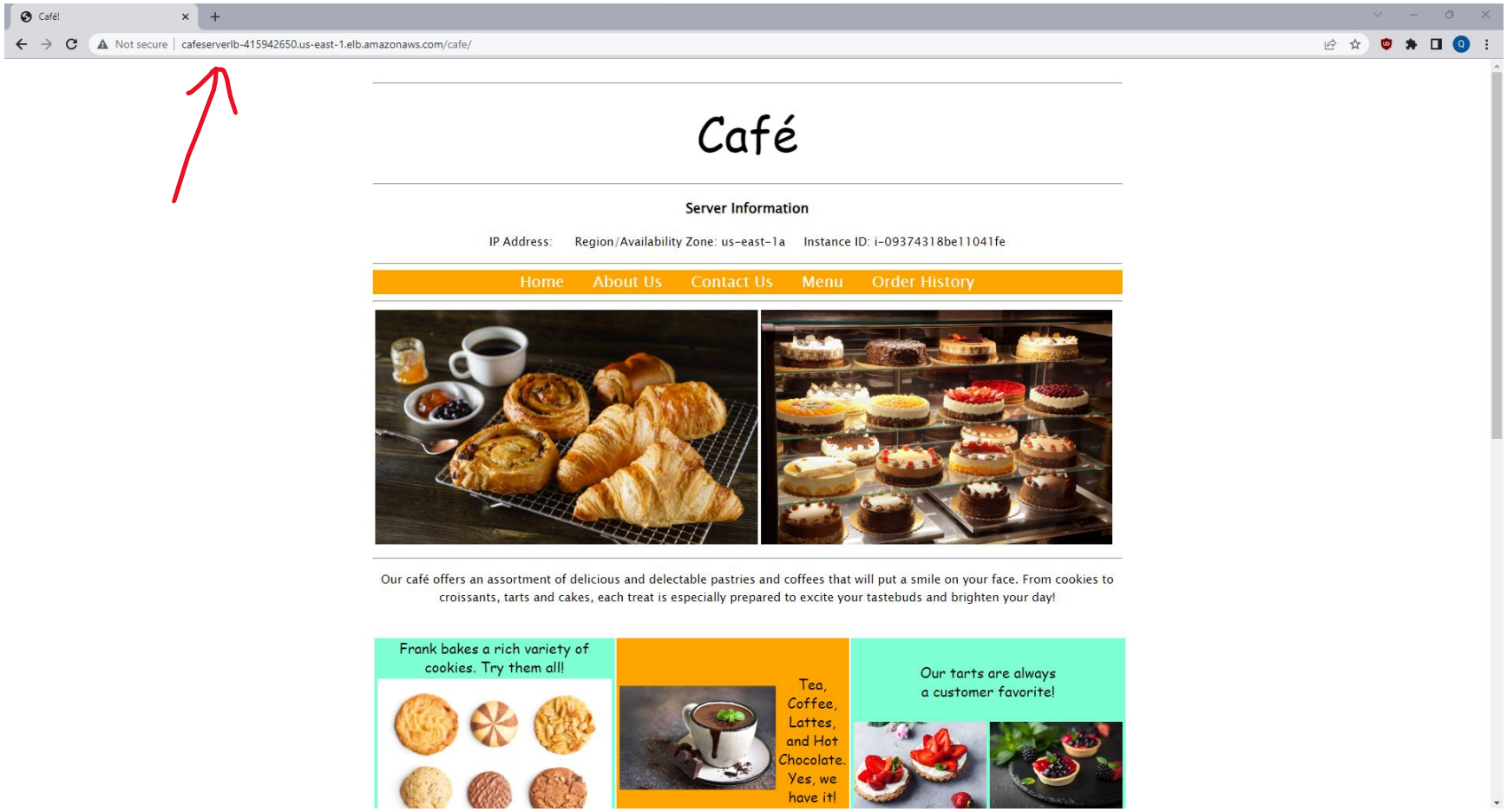


Create an Application Load Balancer (part 3/3), selecting the security group and target group created earlier.



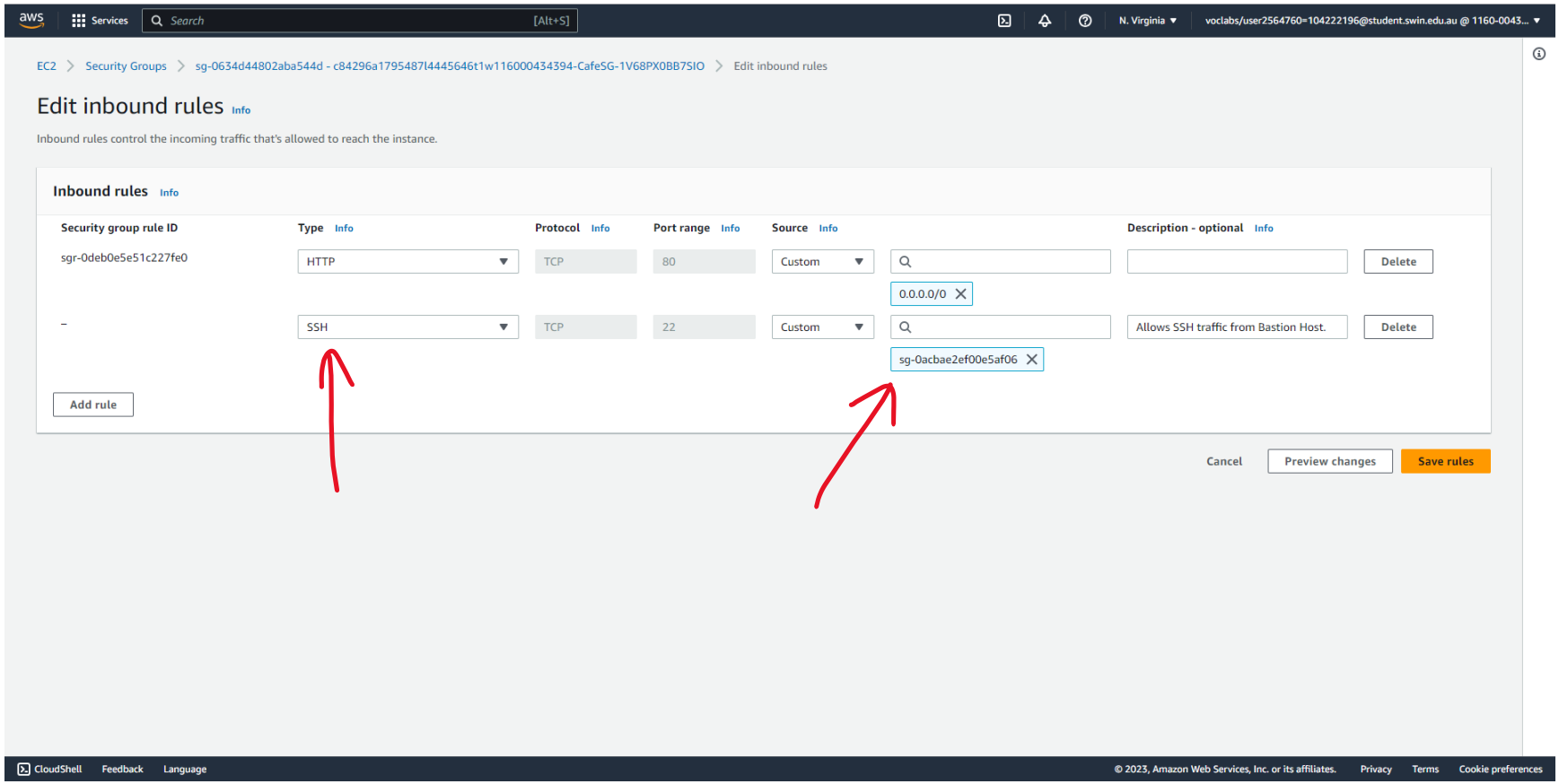
Attach the auto-scaling group to the load balancer by adding the target group.

Task 7 - Testing the web application

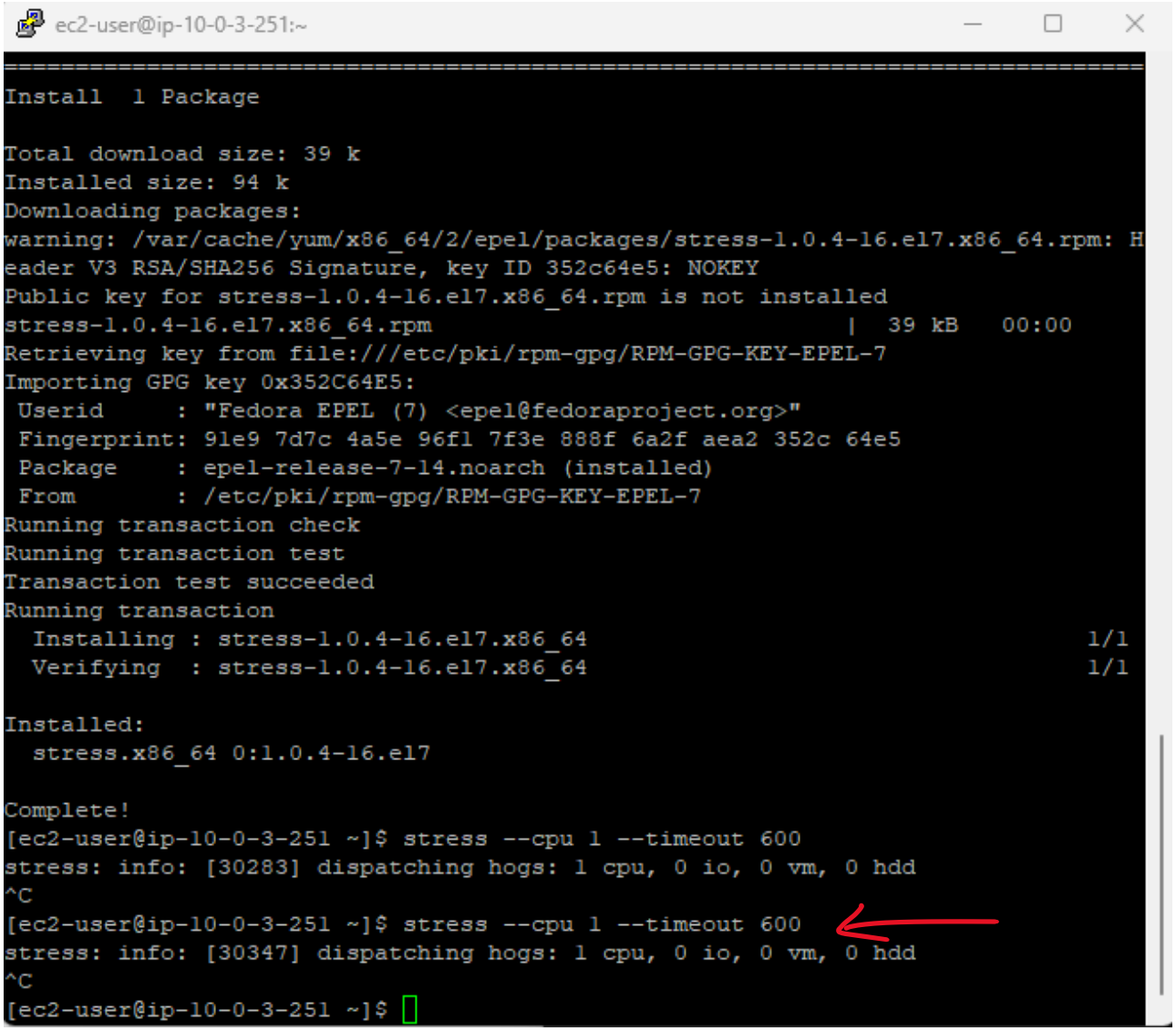


The webpage is now viewable through the load balancer DNS name.

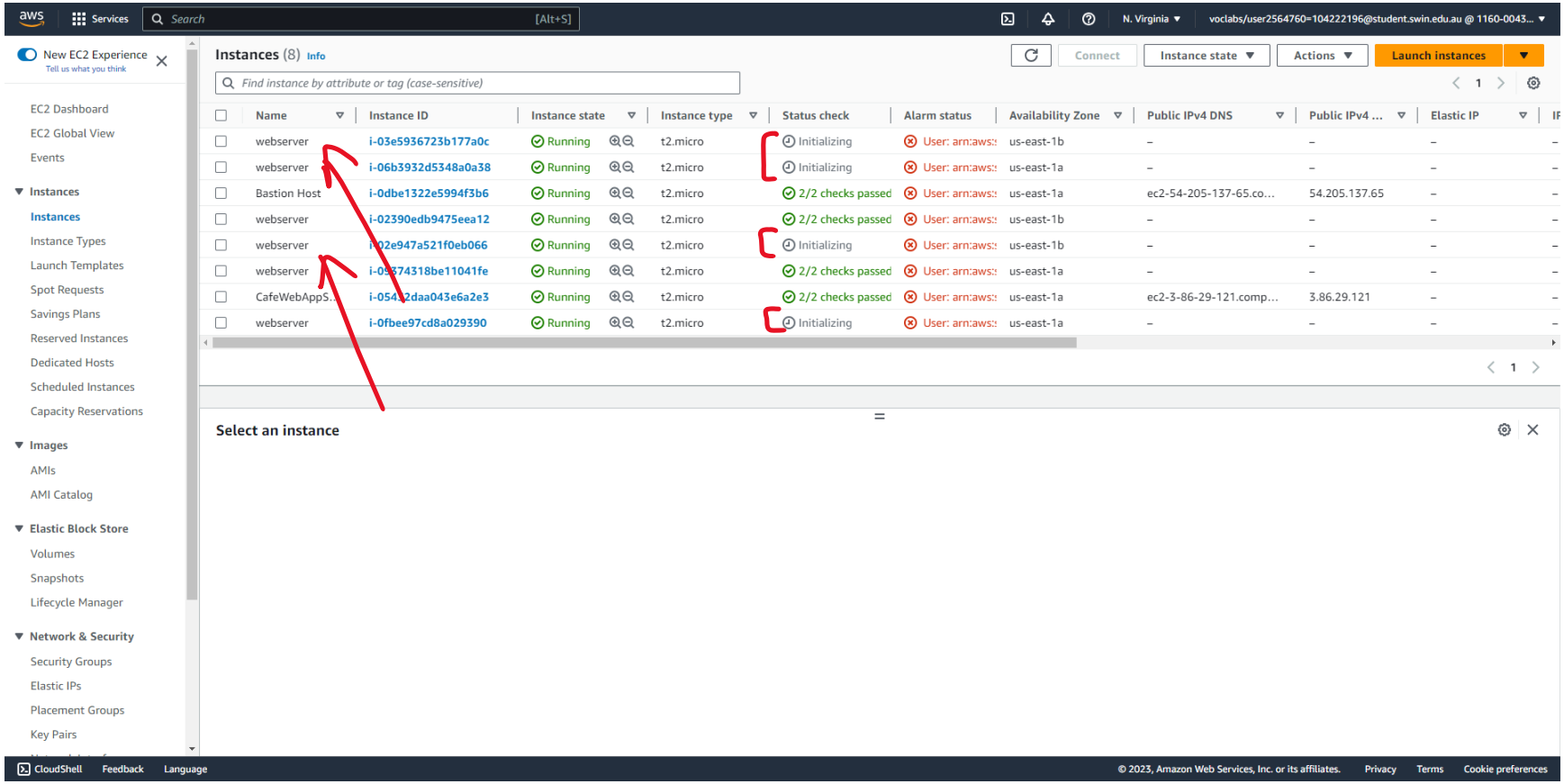
Task 8 - Testing automatic scaling under load



Add an additional rule to the security group used by the web server instances so they can be SSH-ed into by the bastion host.



After SSH-ing into the bastion host through through Putty, SSH into one of the private web servers (with agent-forwarding allowed) and run the code needed to increase the load on the web server.



Additional instances have been automatically launched by the ASG to accommodate the increased load on the web server.