IST 615 – Cloud Management

School of Information Studies, Syracuse University

Fall 2024

Lab - 2

Name of the Author: **Karan Shah**

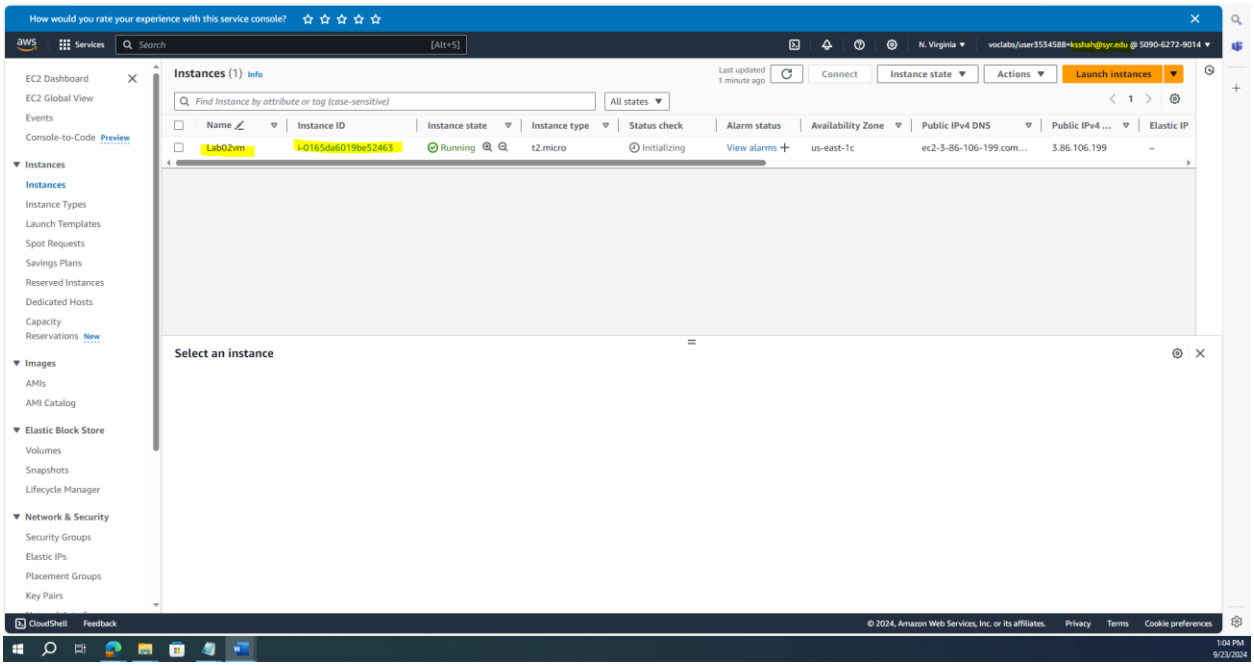
Assignment Due: 9/23/2024

Assignment Submitted: 9/24/2024

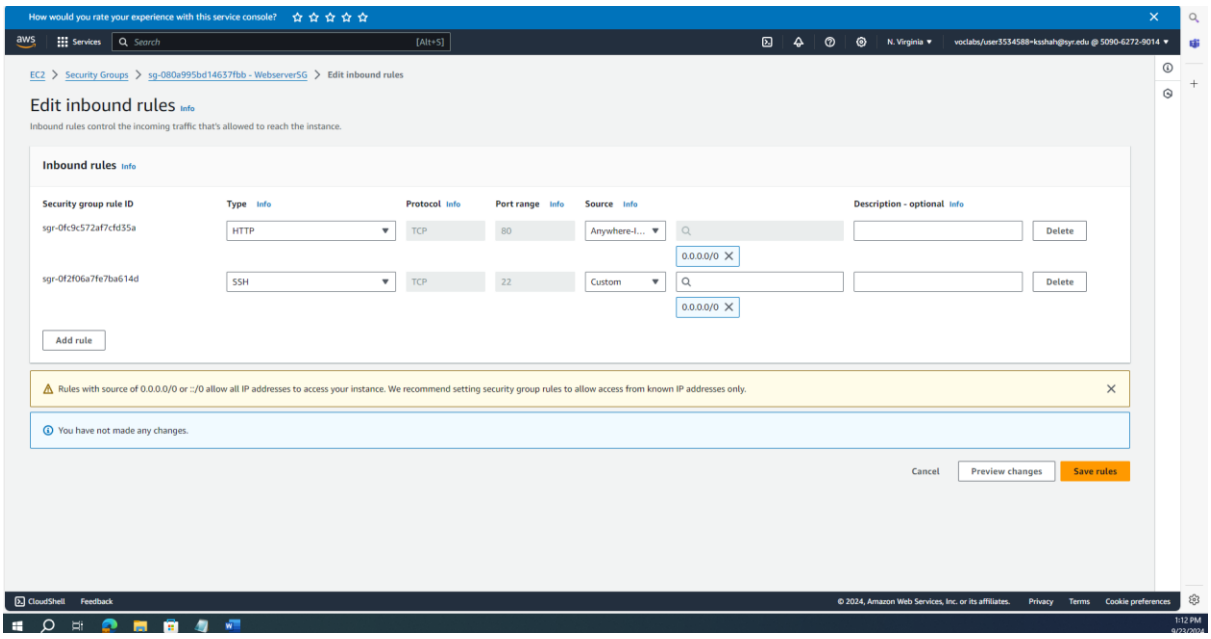
(The document has **6 pages** with the cover page)

Part 1 (70 points):

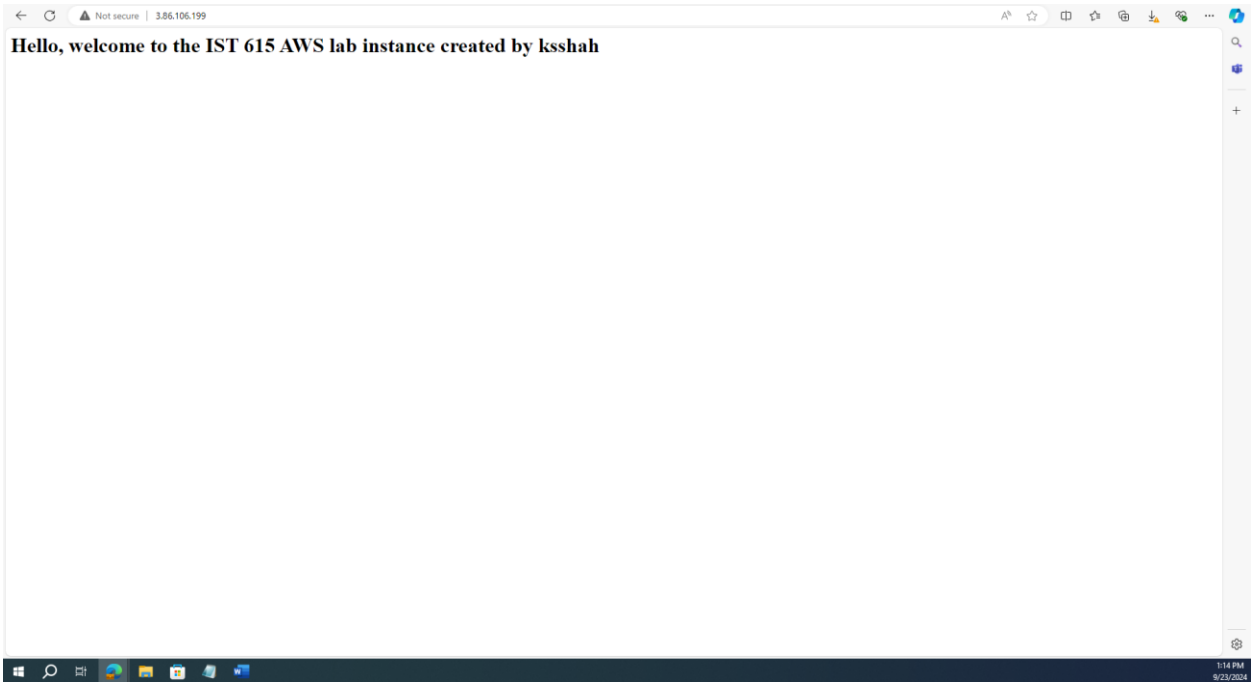
Include all the screenshots required throughout the lab guide. Provide a small description of what is being shown in each screenshot



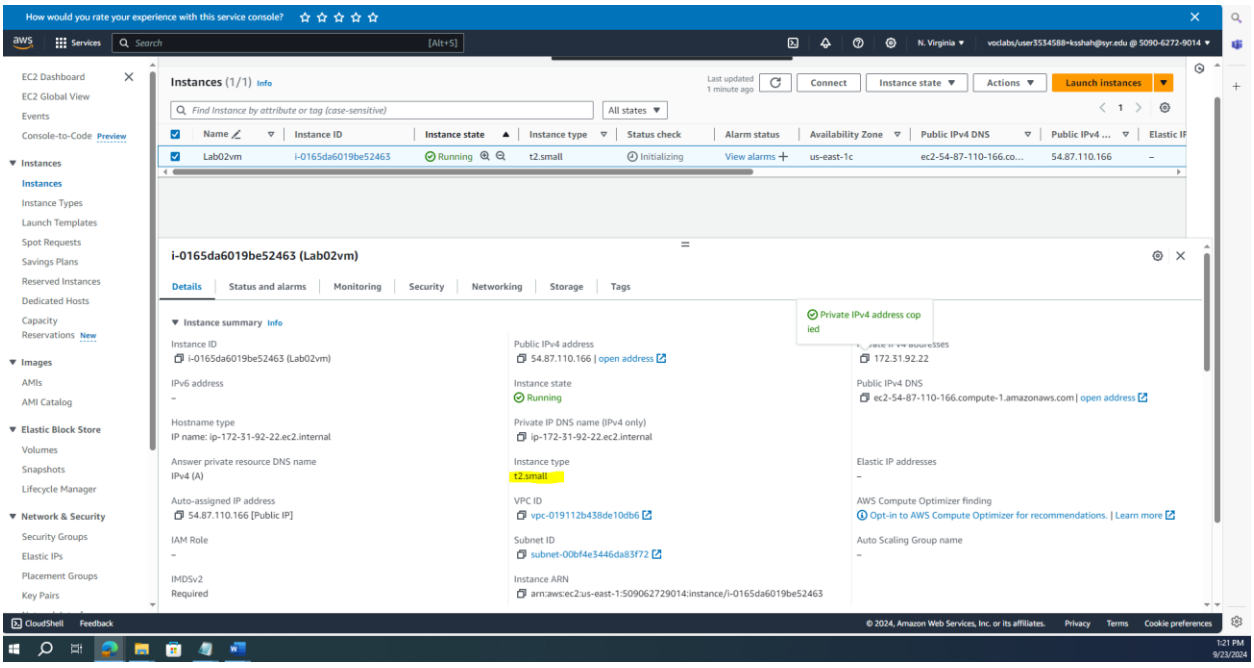
SCS01 - A screenshot from my browser that shows the new EC2 instance is now in my dashboard.



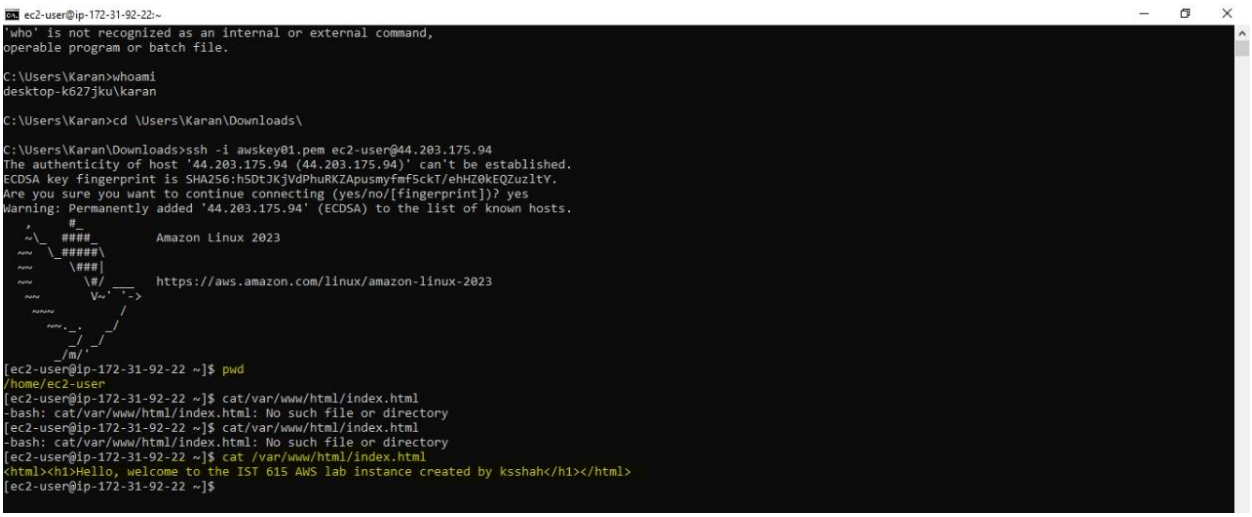
SCS02 - A screenshot from my browser showing that I have two inbound rules with the type set to HTTP and the source set to "Anywhere-IPv4" as selected in the dropdown.



SCS03 - The above screenshot is from my browser, showing a message that includes my netid and confirms that I have successfully launched a web server.



SCS04 - The screenshot above shows the resized EC2 instance (t2.small)



SCS05 - The screenshot shows the SSH session of my EC2 instance. It should display the output of the commands executed in steps 1 and 4, as highlighted in yellow.

Part 2 (30 points)

1. What is the purpose/use of the Amazon EC2 service?

Ans:

Amazon EC2 (Elastic Compute Cloud) is a web service that provides resizable compute capacity in the cloud. Its primary purpose is to enable users to deploy and manage virtual servers (known as instances) in a flexible and scalable manner. This service allows businesses to run applications without the need for physical hardware, facilitating quick scaling based on demand, optimizing costs, and improving availability. Users can choose different instance types, configure security, and manage various aspects of their virtual environments easily.

2. What is an Amazon Machine Image (AMI)?

Ans:

An Amazon Machine Image (AMI) is a pre-configured template used to create virtual machines (instances) in Amazon EC2. It serves as the foundational image that contains the operating system, application server, and applications necessary to launch an instance. AMIs allow users to quickly deploy environments with specific configurations, as they encapsulate all the required components, such as software, libraries, and settings.

3. What is the purpose of user data when creating an EC2 instance?

Ans:
User data in Amazon EC2 allows you to provide initial configuration information or scripts that can be executed automatically when the instance is launched. This feature is useful for automating instance configuration tasks at startup, such as installing software, applying updates, or configuring services.

When you specify user data while launching an instance, it can be a shell script, cloud-init directives, or other commands that run during the boot process. This functionality simplifies the process of configuring your instances and can help streamline deployment by ensuring each instance starts with the appropriate settings without needing manual intervention.

4. What do you use to control what types of traffic can access your Amazon EC2 instances?

Ans:
To control what types of traffic can access your Amazon EC2 instances, you use **security groups**. Security groups act as virtual firewalls that define inbound and outbound rules, specifying which traffic is allowed to or from the instances associated with that security group.

When you launch an EC2 instance, you can assign it one or more security groups. Each security group consists of rules that filter traffic based on specified criteria such as protocol (e.g., TCP, UDP), port range, and source or destination IP addresses.

5. Why would you want to resize an Amazon EC2 instance?

Ans:
You would want to resize an Amazon EC2 instance to handle increased traffic or resource demands as the company's web-based application grows. Resizing allows you to scale up to a more powerful instance for better performance or scale down to reduce costs when fewer resources are needed.

6. A security group works like a firewall because it contains a set of rules that filter traffic coming into and out of an Amazon EC2 instance. By default, all non-local traffic is blocked.

Ans:

By default, all non-local traffic is **blocked** in a security group. This means that unless you explicitly create inbound rules to allow traffic, all incoming traffic to your Amazon EC2 instance is denied. You can configure security groups to allow specific types of traffic, such as HTTP (port 80) or SSH (port 22), by adding inbound rules.