9/24/2024

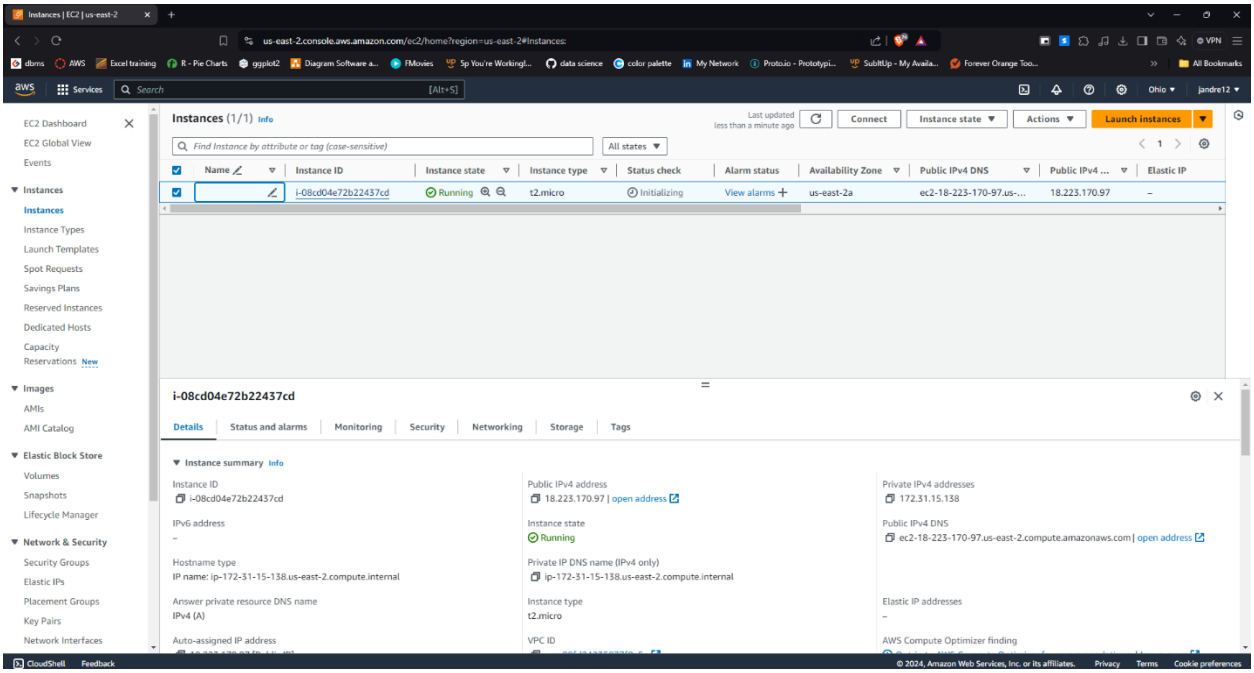
CLOUD MANAGEMENT

LAB #2 – VIRTUAL MACHINES IN AWS

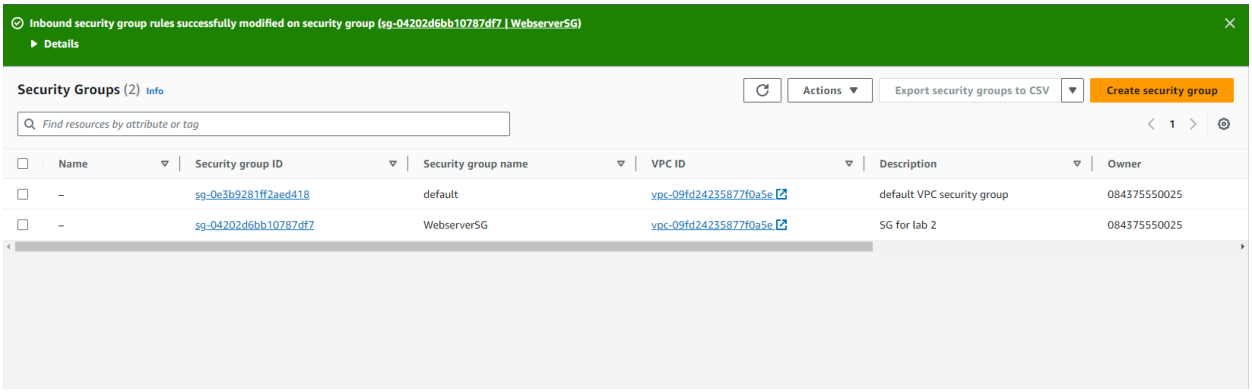
JOVITA ANDREWS - 522110149

Part 1(70 points):

SCS01 – AWS EC2 Dashboard: Shows the interface for launching and managing EC2 instances.



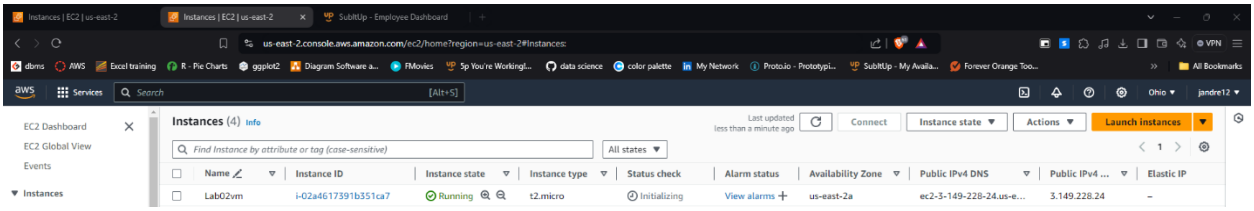
SCS02 – Capture of the browser that shows the two inbound rules.



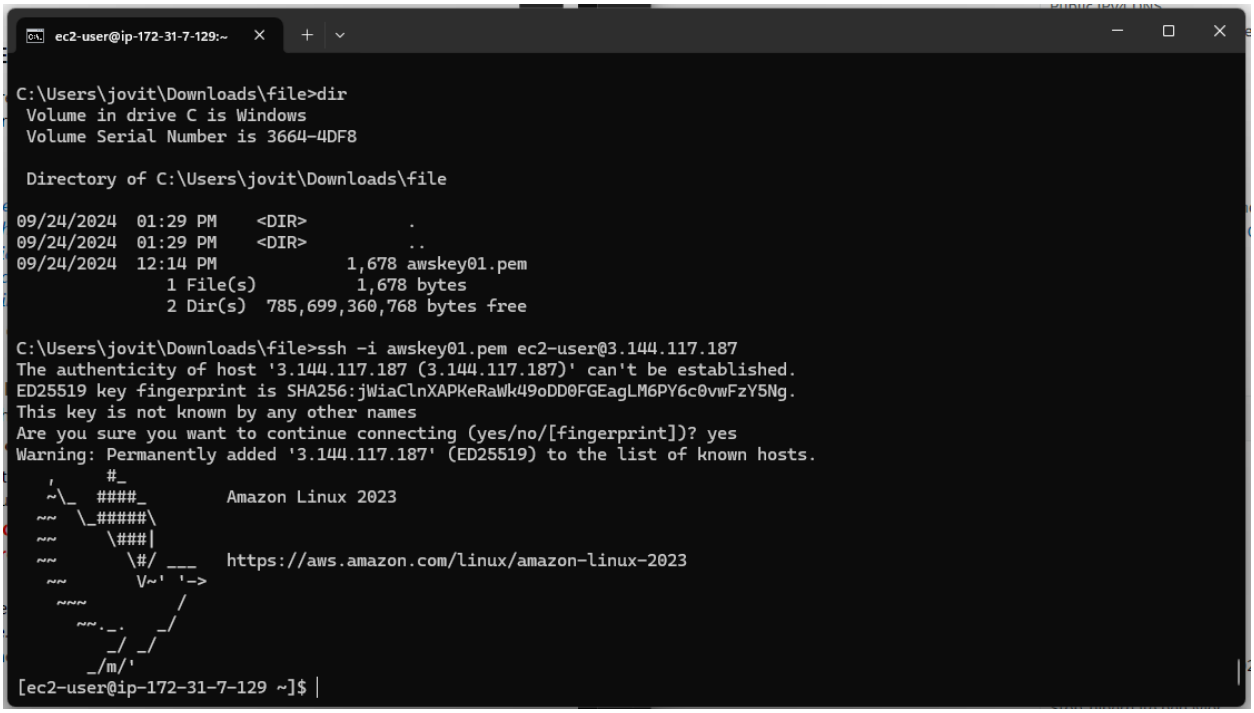
SCS03: Capture of the screenshot of your browser with the message that shows your NETID.

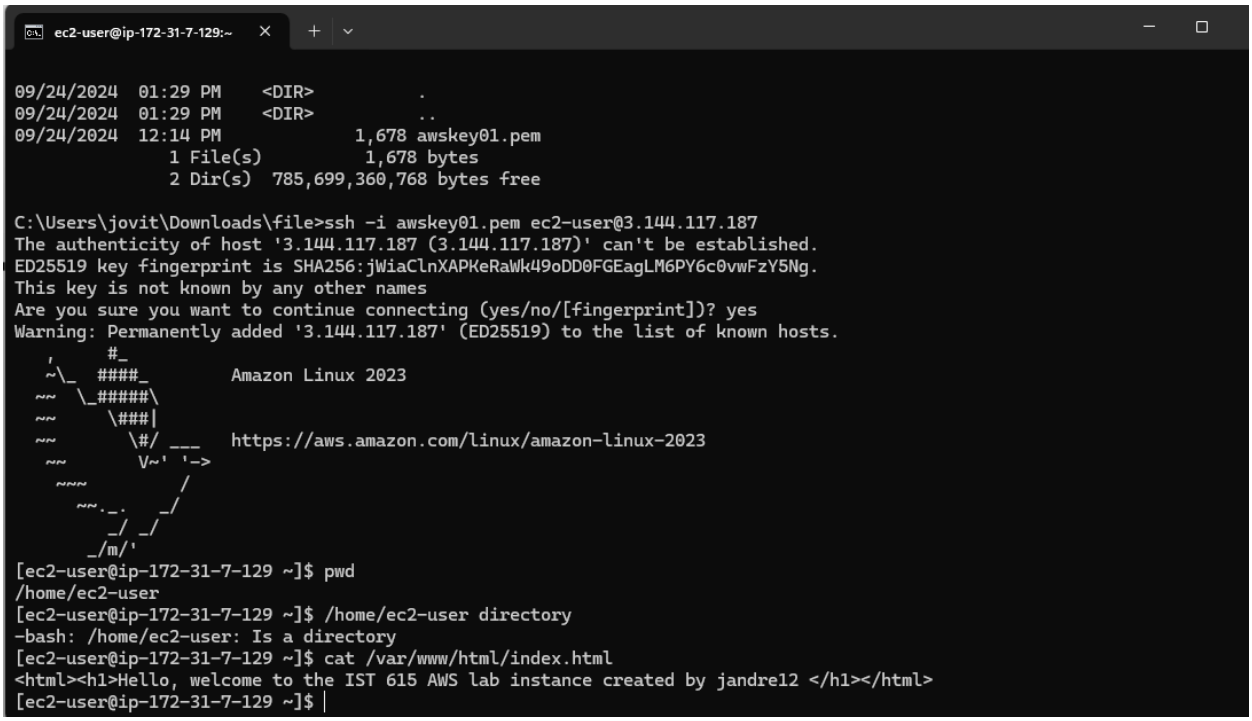
Hello, welcome to the IST 615 AWS lab instance created by jandre12

SCS04: Capture of a screenshot of the resized EC2 instance. This screenshot displays the configuration information related to the new instance type of the EC2 instance.



SCS05 – The SSH session to your EC2 instance.





Explanation:

SCS01 – AWS EC2 Dashboard: Shows the interface for launching and managing EC2 instances

In this screenshot, I captured the AWS EC2 Dashboard, where I manage all my EC2 instances. This is the main interface where I can:

- Launch and terminate EC2 instances: I can easily start or stop virtual machines (EC2 instances) whenever needed.
- View running instances: It gives me an overview of all my running instances and their statuses, whether they're running, stopped, or terminated.
- Instance management options: From this dashboard, I manage tasks like configuring security groups, resizing instances, attaching volumes, and monitoring the instance's performance.
- Instance details: I can see important details like the instance IDs, public DNS, instance types, and key pairs. This screenshot shows key components like the "Launch Instance" button, instance states (e.g., running, stopped), and performance metrics.

SCS02 – Capture of the browser that shows the two inbound rules

In this screenshot, I captured the security group settings for my EC2 instance, specifically showing the two inbound rules that control what kind of traffic can access the instance.

- Inbound rules: Here, I configured which types of traffic are allowed into my instance. For example, allowing SSH traffic on port 22 and HTTP traffic on port 80.
- Rule types: Each rule specifies the protocol (like TCP), the port range (22 for SSH or 80 for HTTP), and the source (such as an IP range or "Anywhere"). The screenshot clearly displays these two rules, highlighting how I allow SSH and HTTP traffic for my EC2 instance.

SCS03 – A screenshot of the browser with the message that shows the NetID

This screenshot captures a message displayed in the browser that shows my NetID.

- NetID: This is my unique identifier assigned by my institution, and it's often used for authentication purposes.
- Browser message: The screenshot shows a confirmation message or script output that includes my NetID, likely after completing a configuration step or accessing a specific resource. Here, I made sure the screenshot clearly shows the NetID message on the browser screen.

SCS04 – Capture of a screenshot of the resized EC2 instance. This screenshot displays the configuration information related to the new instance type of the EC2 instance

In this screenshot, I captured the results after resizing my EC2 instance:

- Resized instance type: It shows the new instance type I upgraded to (e.g., from t2.micro to t2.small) to accommodate the higher performance needs.
- Configuration details: The screenshot includes key details like memory, CPU resources, and the instance's status after the resizing operation (whether it's running or stopped).

- Cost implications: There may also be a notice about the cost changes due to the new instance type. This screenshot provides a detailed view of how the configuration of my EC2 instance changed after the resizing process.

SCS05 – The SSH session to your EC2 instance

This screenshot captures an active SSH session where I logged into my EC2 instance:

- SSH terminal: In the terminal window, you can see the session where I've successfully connected to the EC2 instance using SSH.
- Connection details: The screenshot shows the public IP address of the instance and the command prompt indicating I'm logged into the instance (e.g., user@instance).
- Commands executed: I've also included some commands I ran to verify the connection, such as checking the instance's status or viewing logs. This screenshot demonstrates that I've successfully connected to my EC2 instance using SSH and the correct key pair authentication.

These descriptions reflect my direct experience with each functionality, demonstrating how I managed and interacted with my EC2 instance through the AWS dashboard and SSH.

Part 2 (30 points):

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

Solution: Amazon EC2(Elastic Compute Cloud) provides scalable computing capacity in the AWS cloud. It allows users to launch virtual servers, called instances, to run applications, reducing the need to invest in hardware upfront.

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

Solution: An AMI is a template that defines the software configuration (operating system, application server, applications) required to launch an instance. It simplifies the process of setting up new EC2 instances by predefining all necessary components.

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

Solution: The user data is used for bootstrapping an EC2 instance by providing scripts that are executed when the instance is first launched. This allows for automatic configuration, such as installing software or setting up services. (eg: configuring Apache and creating a web page as in this lab)

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

Solution: Security groups are used to control the traffic allowed to access EC2 instances. These act as virtual firewalls by defining inbound and outbound rules, such as allowing traffic on specific ports (eg: HTTP on port 80)

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

Solution: Resizing an EC2 instance may be necessary when the current instance type is to providing sufficient computational resources for the workload. Upgrading to a more powerful instance type (like t2.micro to t2.small) can improve performance. Conversely, resizing to a smaller instance can save costs if the workload decreases.

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 _____. (Choose from the following options: Allowed, blocked, or neither)

Solution: Blocked.

By default, security groups block all inbound traffic unless explicitly allowed by the rules, while outbound traffic is allowed.