תשובות לשאלון האמריקאי:

AWS Exam - 4 Hours

**Instructions:**

* This exam consists of two sections: **Multiple Choice & Hands-on Questions (UI-Based)**.
* No AWS CLI is required; answer all questions based on AWS UI interactions and provide screenshots on completion.
* You may only use Google and not AI tools.
  + Terms that you are unfamiliar with, require you to google and answer.
* Time to complete: **3 Hours - 4 hours**

**Section 1: Multiple Choice Questions (MCQs)**

**1. AWS Core Services**

1. Which AWS service is used to store objects such as images, videos, and backups?  
     
   * A) EC2
   * B) RDS
   * C) S3
   * D) Lambda
2. What is the purpose of an AWS Availability Zone?  
     
   * A) It ensures high availability by distributing resources across multiple locations.
   * B) It acts as a data center located in different countries.
   * C) It is only used for networking and VPCs.
   * D) It is a security feature of AWS.
3. What is the default storage class for an S3 bucket when you create it?  
     
   * A) S3 Intelligent-Tiering
   * B) S3 Glacier
   * C) S3 Standard
   * D) S3 Infrequent Access (IA)

**2. IAM & Security**

1. What is the purpose of an IAM role?  
     
   * A) It is used to assign permissions to AWS services and users.
   * B) It is a dedicated user with full AWS access.
   * C) It replaces IAM users completely.
   * D) It is used only for temporary access.
2. In AWS IAM, what is the best practice for securing your root account?  
     
   * A) Keep it logged in at all times for easy access.
   * B) Use it only for creating IAM users and enable Multi-Factor Authentication (MFA).
   * C) Assign full administrator access to all IAM users.
   * D) Share credentials with your team for convenience.

**3. Networking and Connectivity**

1. What is the purpose of an Internet Gateway in AWS?  
     
   * A) To allow communication between instances within a VPC.
   * B) To provide internet access to resources in a private subnet.
   * C) To restrict public access to EC2 instances.
   * D) To encrypt data stored in S3.
2. What is the main difference between a Security Group and a Network ACL?  
     
   * A) Security Groups operate at the instance level, while NACLs operate at the subnet level.
   * B) NACLs provide fine-grained access control for IAM users.
   * C) Security Groups apply only to databases.
   * D) NACLs are only used for VPN connections.

**4. Storage & Databases**

1. Which AWS service provides a managed relational database service?  
     
   * A) DynamoDB
   * B) RDS
   * C) Redshift
   * D) S3
2. What happens if you delete an S3 bucket with objects inside it?  
     
   * A) The bucket is deleted, but the objects remain in AWS storage.
   * B) The bucket is deleted, and all objects inside it are permanently removed.
   * C) The bucket cannot be deleted unless it is empty.
   * D) The bucket is archived, and you can restore it later.

**5. AWS Billing & Pricing**

1. Which AWS pricing model allows you to pay only for the computing resources you use?

* A) Reserved Instances
* B) Spot Instances
* C) Pay-as-you-go
* D) Fixed-rate pricing

1. What tool in AWS helps users monitor their spending and set budget alerts?

* A) AWS Cost Explorer
* B) AWS Config
* C) AWS CloudTrail
* D) AWS Security Hub

**6. Research-based AWS Questions - using google only**

1. What are AWS Landing Zones, and how do they help with multi-account governance?

**AWS Landing Zones are a multi-account sandbox that serves as a starting point for organizations to quickly launch and deploy workloads and applications**. It's where you start your interaction with the cloud. You can have a couple of teams (not necessarily on the same account) meet together there and test a couple of strategies to deploy the site. Which database should we use? How many servers should we use? What kind of servers – t2.micro or t7xlarge? Those kind of questions. It helps with multi-account governance by allowing teams with different accounts to meet together in a safe neutral environment ("the sanbox") where they can discover that they can use the existing accounts more effectively, share ideas and approaches, and even come to the conclusion that they can use a single account (or not – that separation is a good thing).

1. Explain how AWS WAF protects web applications from common attacks.

**Web Application Firewall helps protect web applications by filtering and monitoring HTTP traffic between a web application and the internet. It typically protects web applications from attacks such as cross-site forgery, cross-site-scripting (XSS), file inclusion, and SQL injection, among others**. A classic example would be an instruction to the firewall to allow traffic only from a given ip (say xx.xx.xx.xx). This would make sense if for example you have a database server that is only supposed to communicate with its application server.

1. What is AWS Snowball, and when should it be used?

AWS snowball is a large data (peta-bytes) solution to move data in and out of the AWS cloud. Kind of like dropbox, according to the description. Formal definition :  **Snowball is a solution that uses secure appliances to transfer large amounts of data into and out of the AWS cloud. Using Snowball addresses common challenges with large-scale data transfers including high network costs, long transfer times, and security concerns**

1. What are the key differences between AWS Backup and manual snapshot backups?

Formal definition : **for an EC2 instance with limited storage and recovery options. An AWS EC2 backup is a more comprehensive and flexible copy of your cloud workloads, offering reliable protection and ensuring fast and consistent recovery**

In my words – consider an application running on a given EC2 instance. It's changing all the time – software being installed, data being changed in the RAM, data being changed on the hard-drive. You can freeze it in a given moment in time. That's a snapshot. It can be restored to that exact moment. However everything later on in time will be lost. AWS backup allows you to store deltas of change, to back up your hard-disk alone, to be restored on a different instance, and so on.

1. How does AWS Shield help mitigate DDoS attacks?

Formal definition : **AWS Shield is a managed distributed denial of service (DDoS) protection service that safeguards applications running on AWS. It provides dynamic detection and automatic inline mitigations that minimize application downtime and latency, so there is no need to engage AWS Support to benefit from DDoS protection.**

In my words – distributed denial of service is an attach where a couple of servers (say 100) simultaneously flood the server with requests. This overwhelms the resources of the server causing it to freeze/become really slow. It's as if instead of the usual 50 users using the system, there suddenly are 5000 users. However these attacks can be prepared for – for example if they come from the same 100 servers, they can automatically be blocked (even without a human intervention). That's what AWS shield software is all about.

1. Explain the differences between AWS Transit Gateway and VPC Peering.

 AWS VPC Peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. Instances in either VPC can communicate with each other as if they are within the same network. If more than two VPCs are used, a peering connection must be made within each pair. This means low cost since you need to pay only for data transfer. It also means No bandwidth limit, because both VPCs are inside amazon. On the other had if you connect just a few of these (say n=50) – it soon becomes a very complex to set up. AWS

Transit Gateway is a fully managed service that connects VPCs and On-Premises networks through a central hub without relying on numerous point-to-point connections or Transit VPC. So instead of connecting all the VPC's to each other, you have each of them connect to the gateway. Much easier to manage, much more uniformity. Very clear rules.

You can attach all your hybrid connectivity (VPN and Direct Connect connections) to a single Transit Gateway instance, consolidating and controlling your organization’s entire AWS routing configuration in one place.

1. What is AWS Step Functions, and how does it help with workflow automation?

Consider a warehouse where products are being stored and shipped. You would have one micro service taking in new cargo and supply and creating a report on them. Then another micro service based on this report will preform the daily inventory checks to order new supplies where needed. Then another micro service would deal with existing orders to customers , issue collection orders, and shipping instructions.

Each of these is a step to be done one after the other. All these together are called a workflow.

Formal definition – Step Functions is a visual workflow service that helps developers use AWS services to build distributed applications, automate processes, orchestrate microservices, and create data and machine learning (ML) pipelines

1. How does AWS Control Tower assist organizations in managing multiple AWS accounts?

Aws Control Tower helps manage multiple accounts, for uniformity. For example making sure that you don't have an account you forgot about that is spending money without you knowing it or without a cap limit. Or making sure your security guidelines are enforced across all your accounts.

1. What is the significance of AWS Outposts in hybrid cloud solutions?

Outposts servers provide compute and networking services that are ideal for low-latency, local data processing needs for on-premises locations such as retail stores, branch offices, healthcare provider locations, or factory floors.

For example a small computer or server is collecting data (not a lot at any given time). Should it choose to now analyze this data, the whole system would slow down significantly. Instead it connects to an AWS outpost service, runs the calculation over there, and receives the response. You pay only for usage, but you need the answer fast (low latency).

1. Explain the key use cases for AWS Elastic File System (EFS) compared to S3 and EBS.

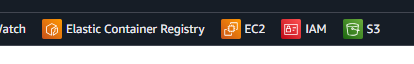
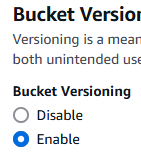
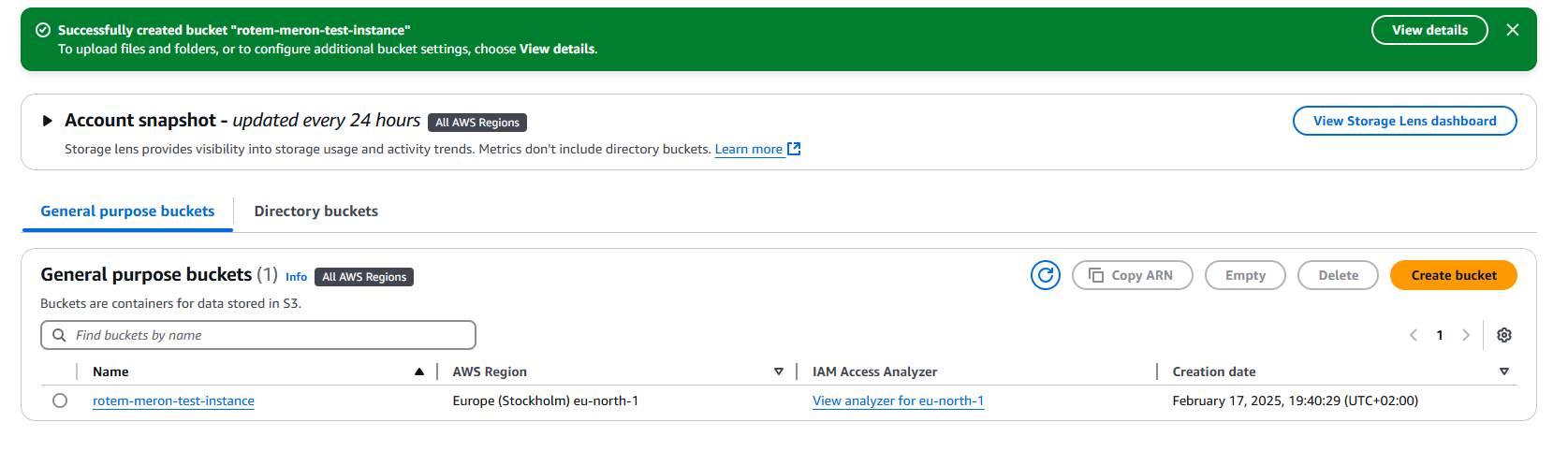
These are completely different things –

* S3 is a key value store (for any file actually). It is a storage facility accessible any where. It's designed as a mechanism to answer multiple requests of the file. Like a movie on Netflix that everyone wants to download at the same time.
* EBS is a device you can mount onto EC2. You have to have access to this EC2 instance to get to it. You can only access files on the EBS inside your EC2 instance. If you don't expose them to the outside – they cannot be accessed from outside. like your hard drive on your personal computer.
* EFS is a file system you can mount onto EC2, but it's replicated on different availability zones, so you can have the same instance of EFS connected to a couple of EC2s on different zones. Like a service hard-drive that can be shared across instances.

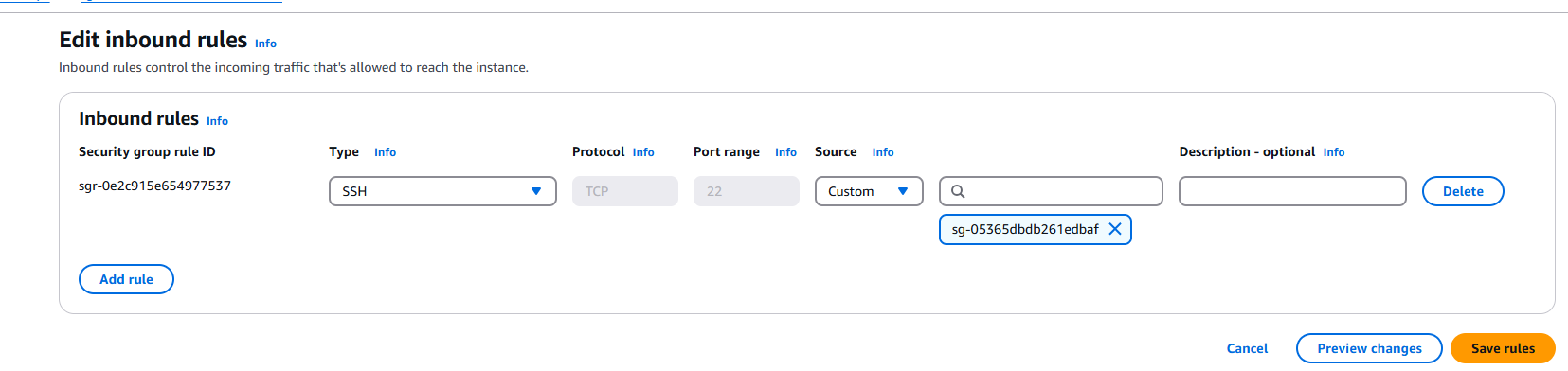
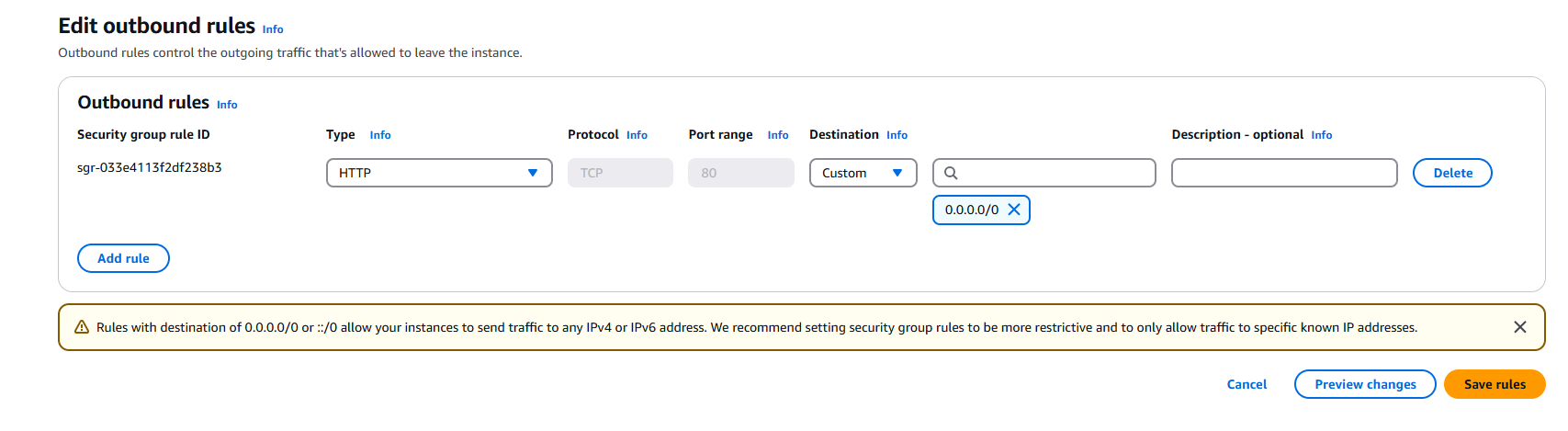
**Section 2: Hands-on UI-Based Questions**

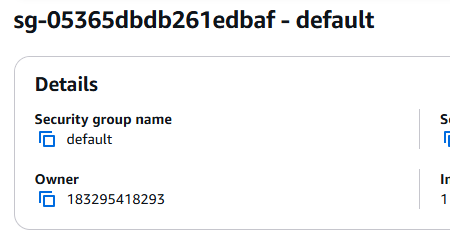
**1. S3 Bucket Configuration**

* Navigate to the AWS Management Console and create a new S3 bucket.
* Enable versioning and explain the steps you took.
* Set a policy to allow only your IAM user to upload objects.
* **Provide a screenshot on completion**

1. **log in to AWS. Select s3 from the menu bar (the green bucket)**
2. ****
3. **Click Create Bucket button **
4. **Bucket Name = rotem-meron-test-instance (leave ACL at default)**
5. **Select bucket versioning - enable**
6. **Add tags – Created =Rotem Meron**
7. **Name = rotem-meron-test-instance**
8. **Leave others as default**
9. **Final step : (screen**

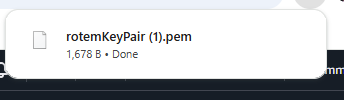
**2. Launch an EC2 Instance**

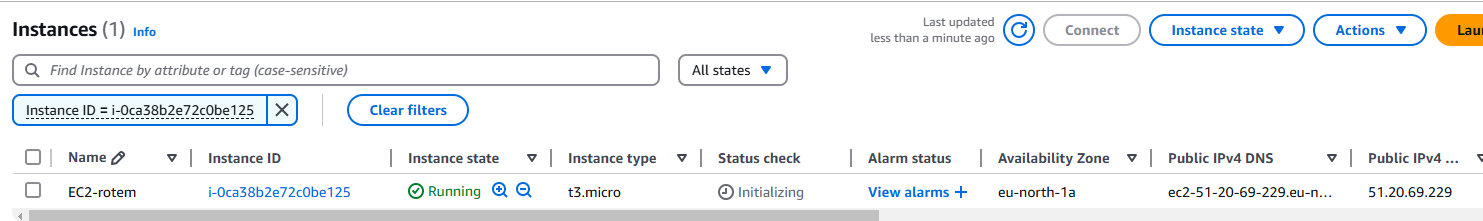
* Using the AWS UI, create a **t2.micro** EC2 instance.
* Attach a Security Group that allows inbound SSH (port 22) and HTTP (port 80) traffic.
* **Provide a screenshot on completion**
* Inbound : 
* Outbound (edit)



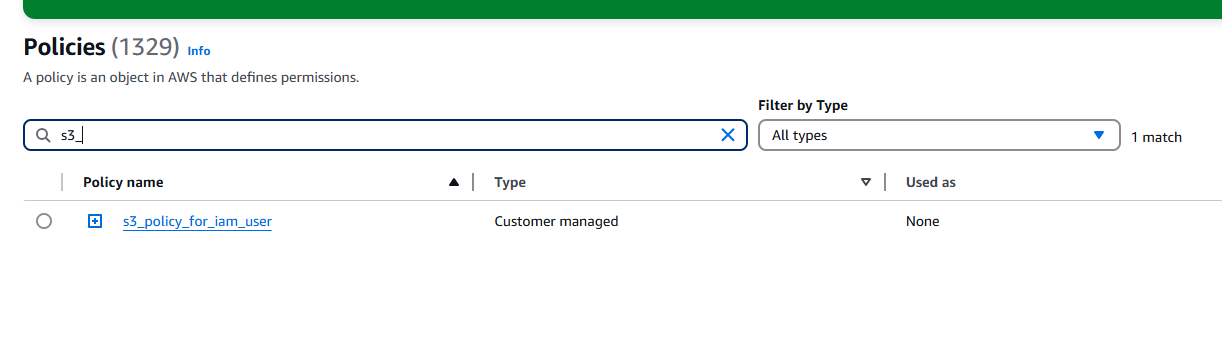
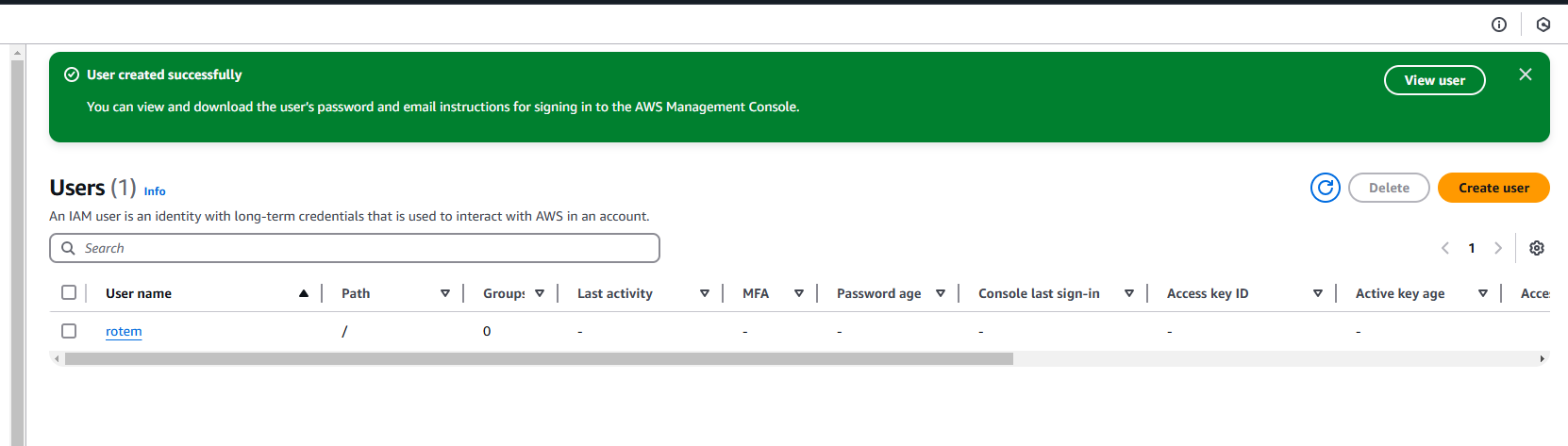
**EC2 :**

**Used t3.micro (that' s all the options I had on my free tier) – name EC2-Rotem**

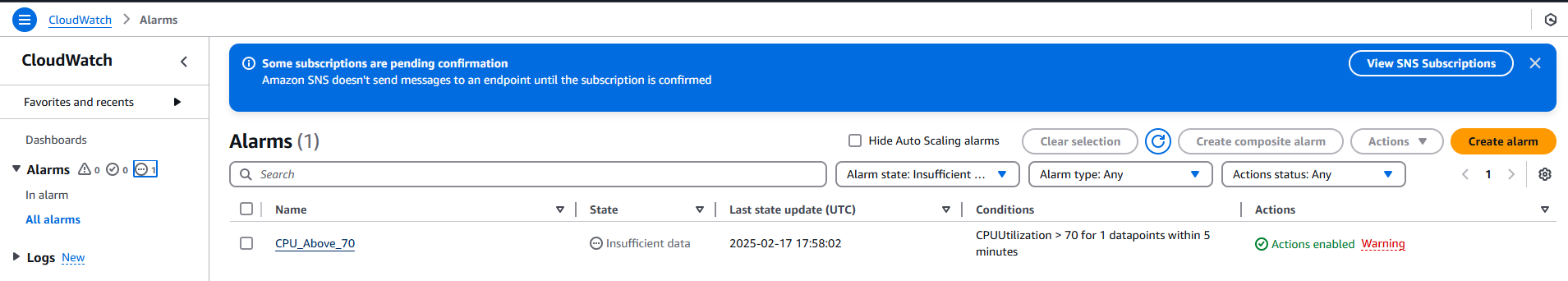
**Created keypair **

**Final result **

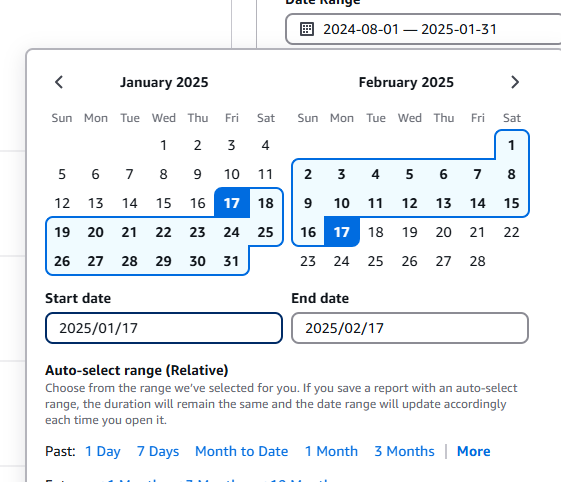
**3. Configure an IAM User with S3 Access**

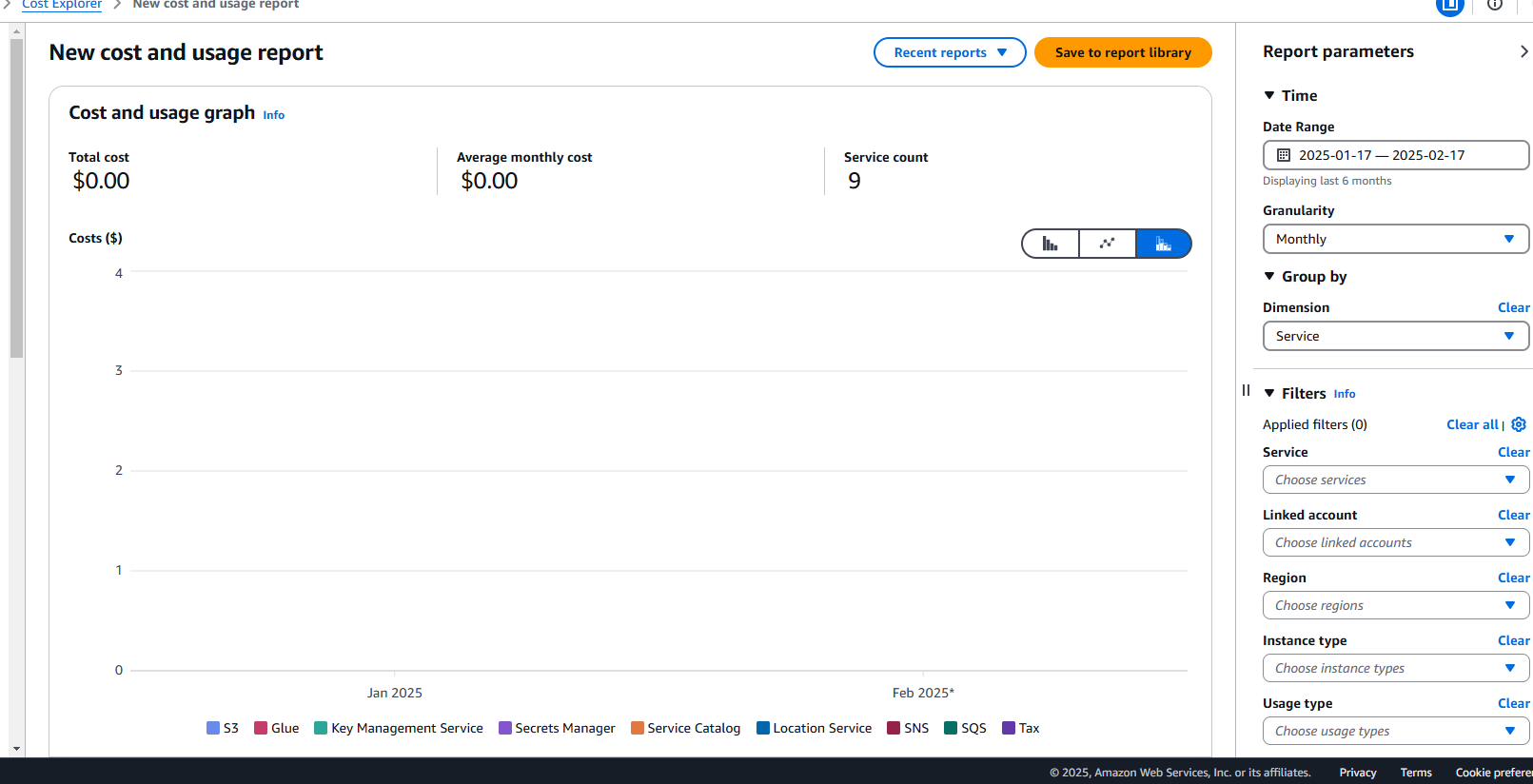
* Create a new IAM user with permissions to access only a specific S3 bucket.
* Group – s3users
* I didn't have an s3 specific bucket (because I already deleted – so I selected ARN = \*
* Policy\_name 
* **Provide a screenshot on completion**
* How would you verify that the user has the correct permissions?
* 

**4. Set Up a CloudWatch Alarm**

* Navigate to AWS CloudWatch and create an alarm to monitor CPU usage on an EC2 instance.
* Set the alarm to trigger if CPU utilization exceeds **70%** for **5 minutes**.
* Describe how you configured notifications for the alarm.
* Notification to email – rm13rotem@gmail.com
* **Provide a screenshot on completion**
* 

**5. Identify AWS Billing Costs**

* Navigate to AWS Cost Explorer and check the billing details for the past month.
* Limited time range 
* Explain the steps to analyze usage and forecast costs.
* **Provide a screenshot on completion**

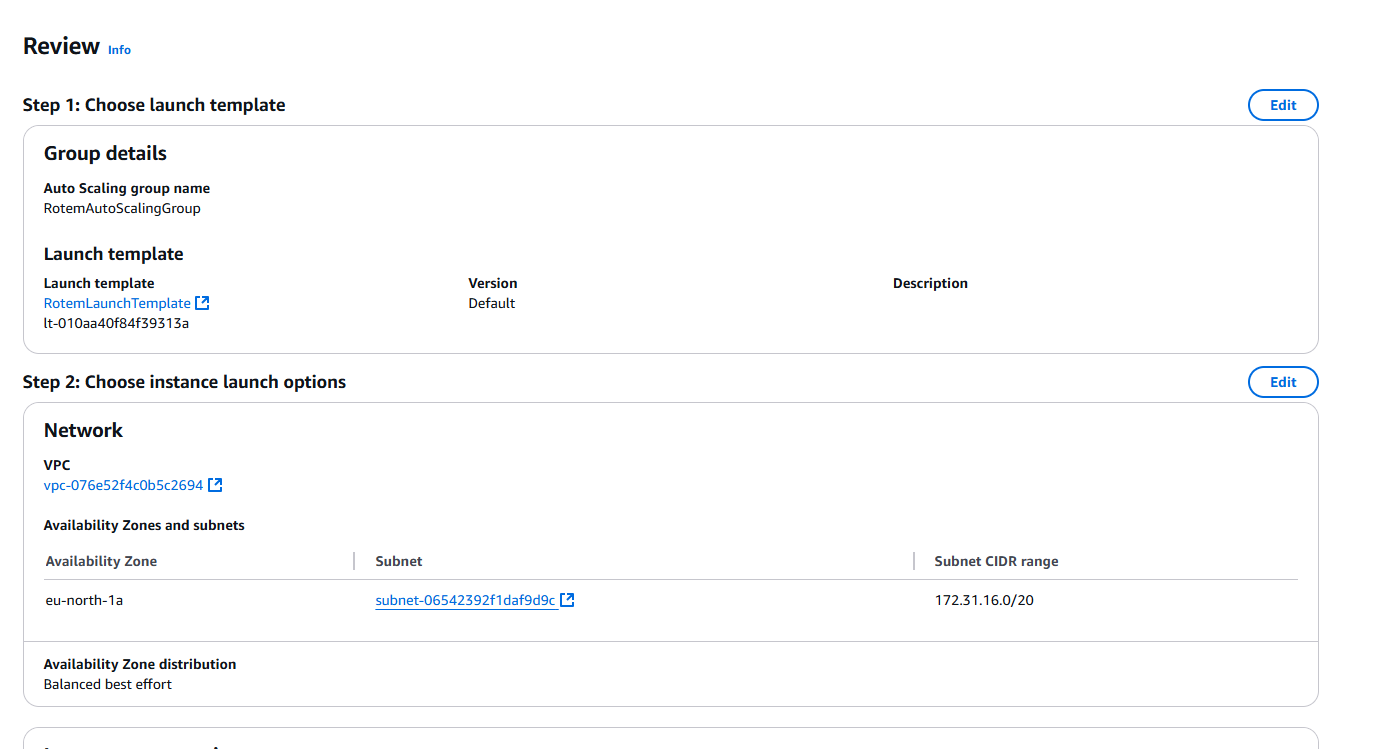
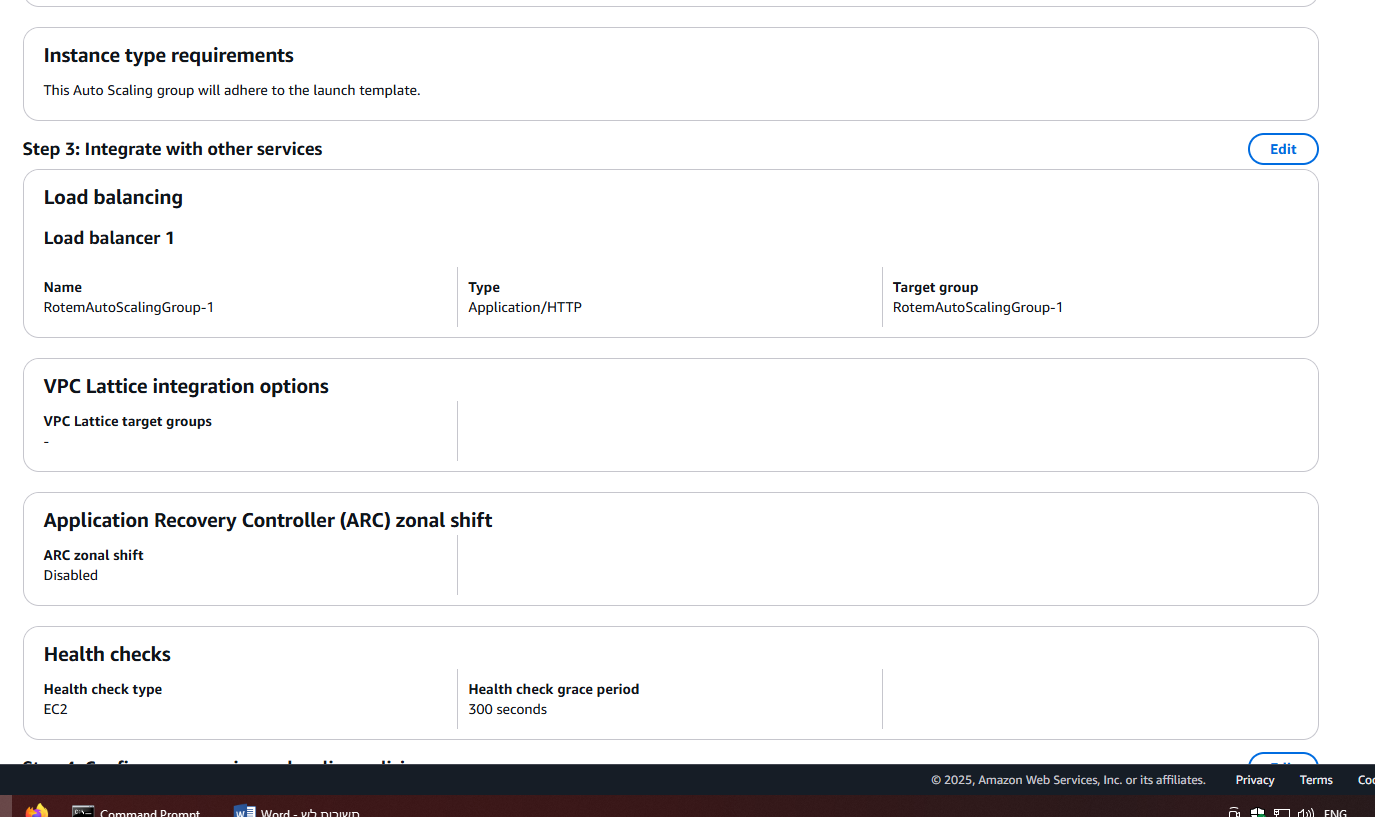


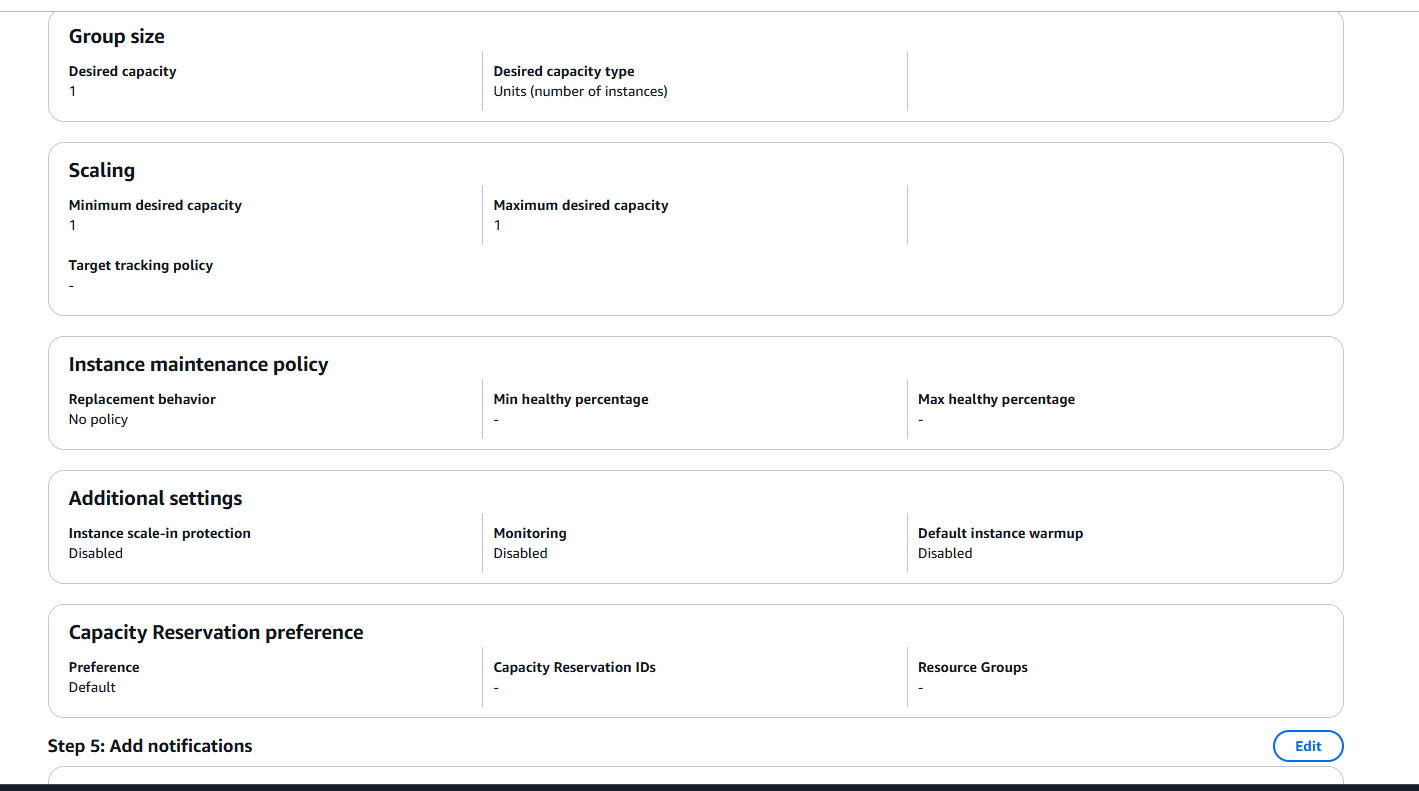
**Section 3: Hands-on advanced**

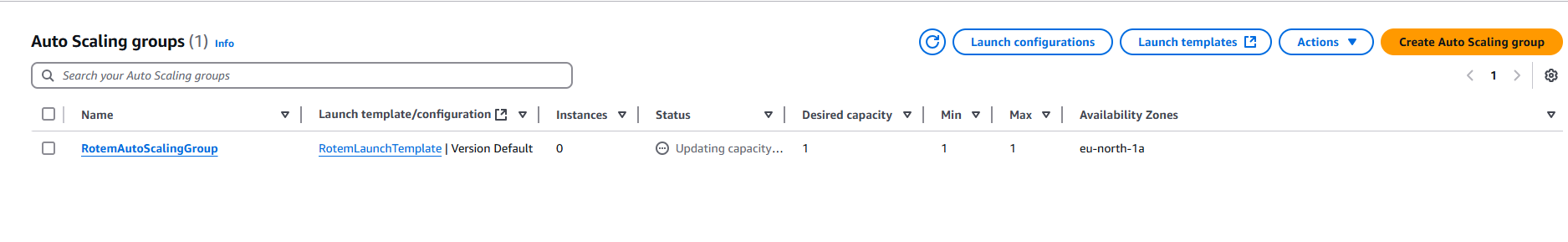
**Instructions:**

* **Perform the following tasks using the AWS UI.**
* **Provide screenshots as proof of completion.**
* **No AWS CLI is required; all actions must be performed using the AWS Management Console.**

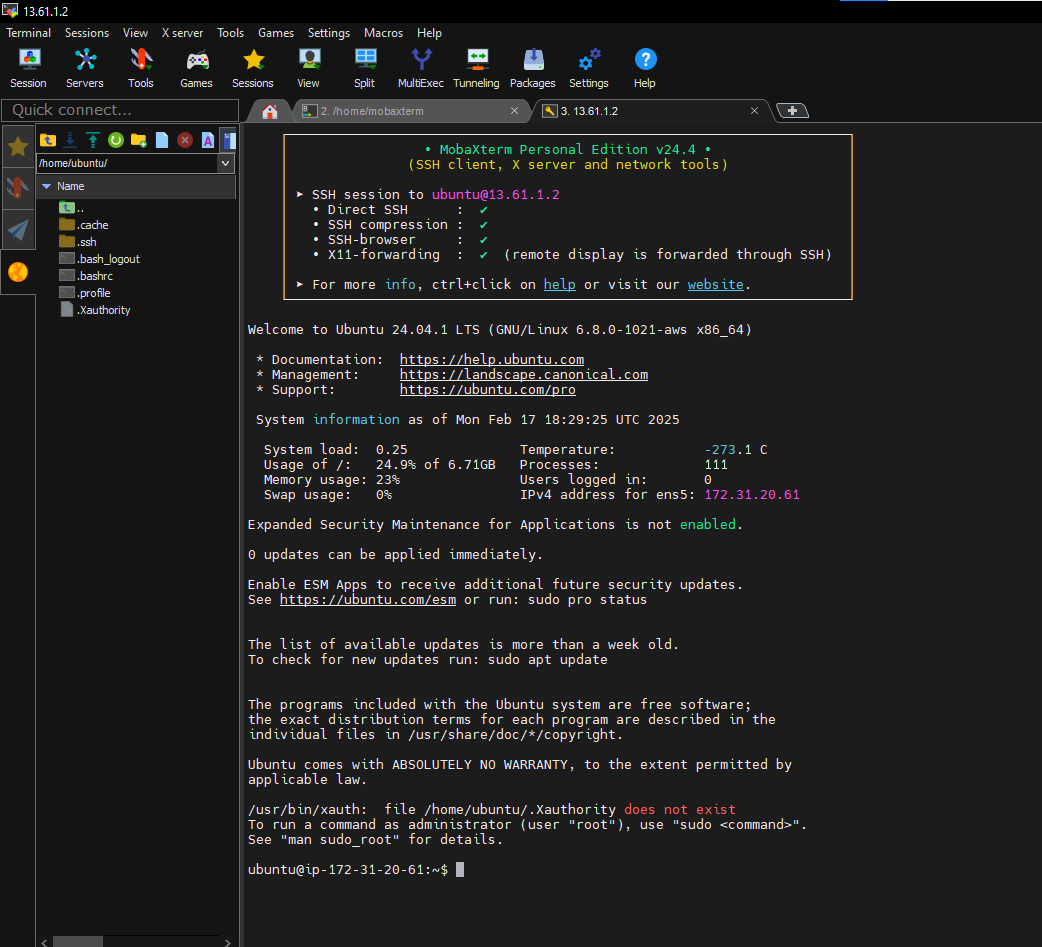
**1. Deploy an Auto Scaling Group with a Single EC2 Instance**

* Create an Auto Scaling Group with a t2.micro Amazon Linux 2 instance.
* **My create Launch Template only comes with t3.micro**
* Configure the Launch Template to include the following:
  + Amazon Linux 2 AMI.
  + Security Group that allows inbound SSH (port 22) and HTTP (port 80).
  + **Used my prevouisly configured security group**
* Set the desired capacity to 1 instance.
* Attach a Load Balancer to the Auto Scaling Group.
* Provide a screenshot of the Auto Scaling Group settings.
*  

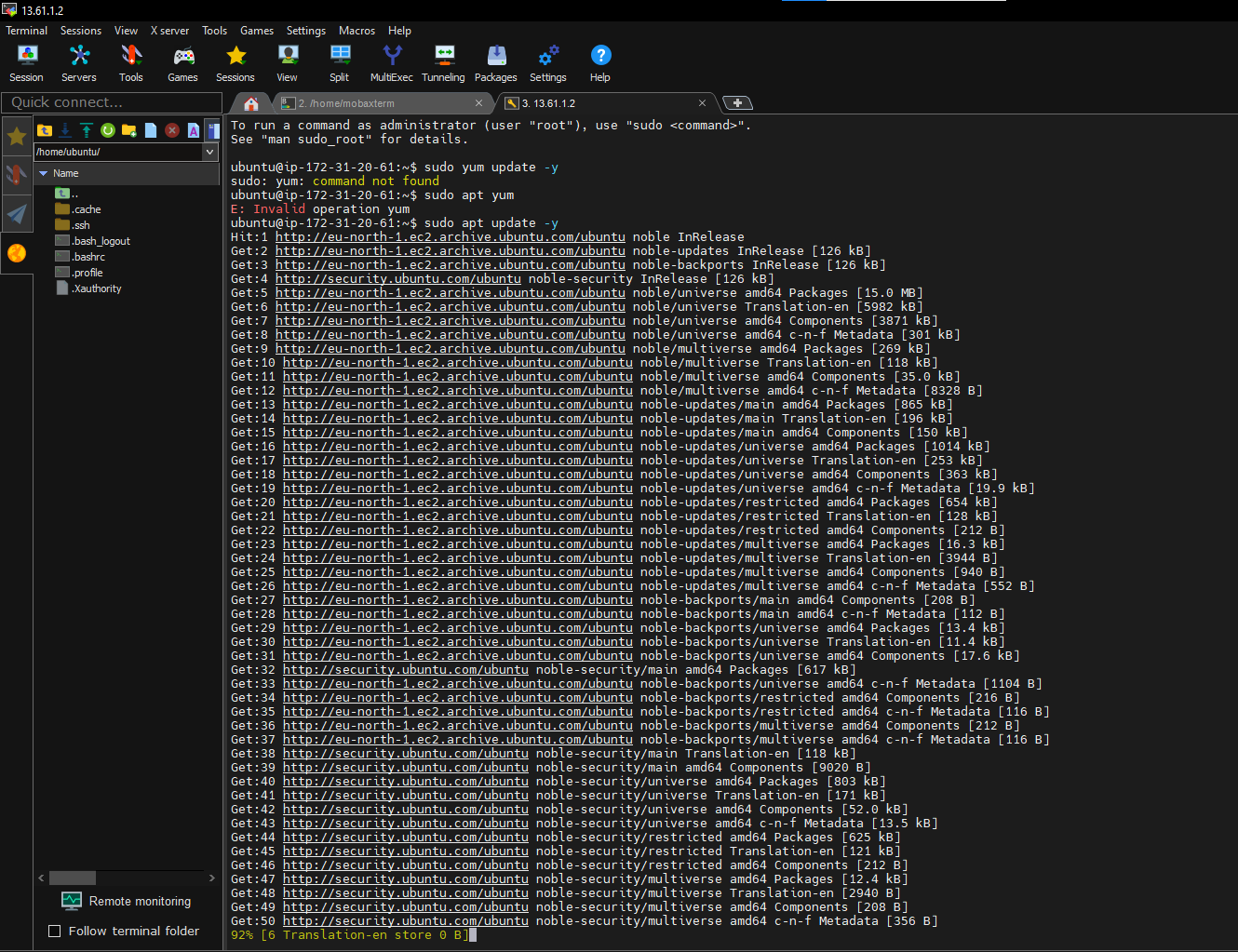
****

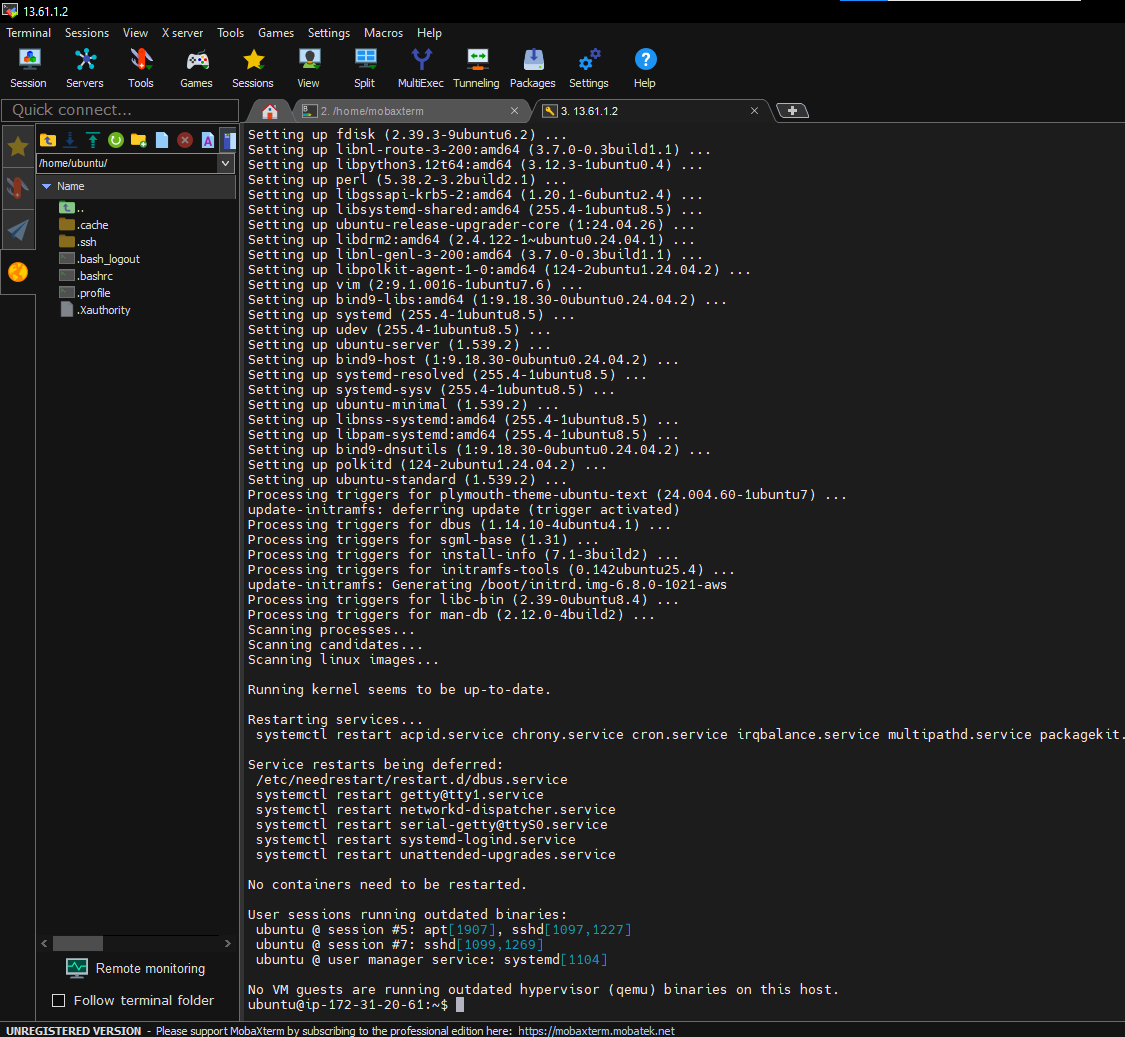
****

**2. Connect to the EC2 Instance and Install Nginx**

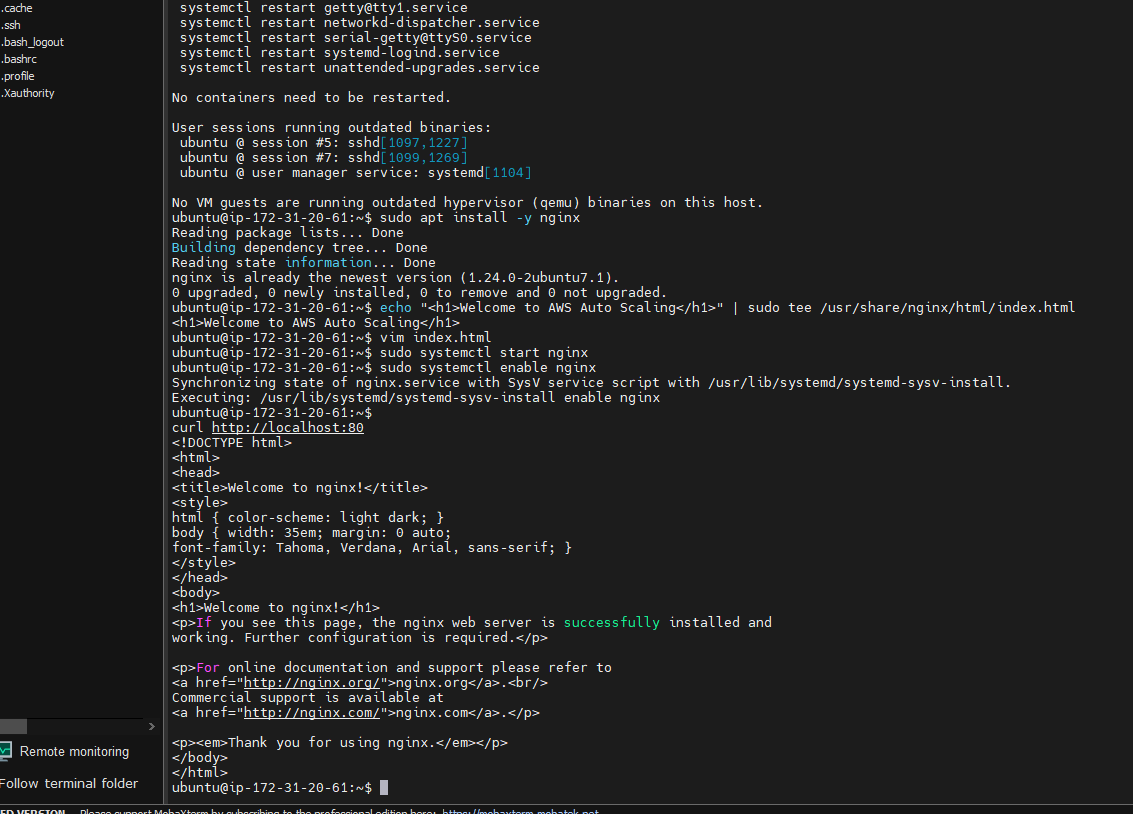
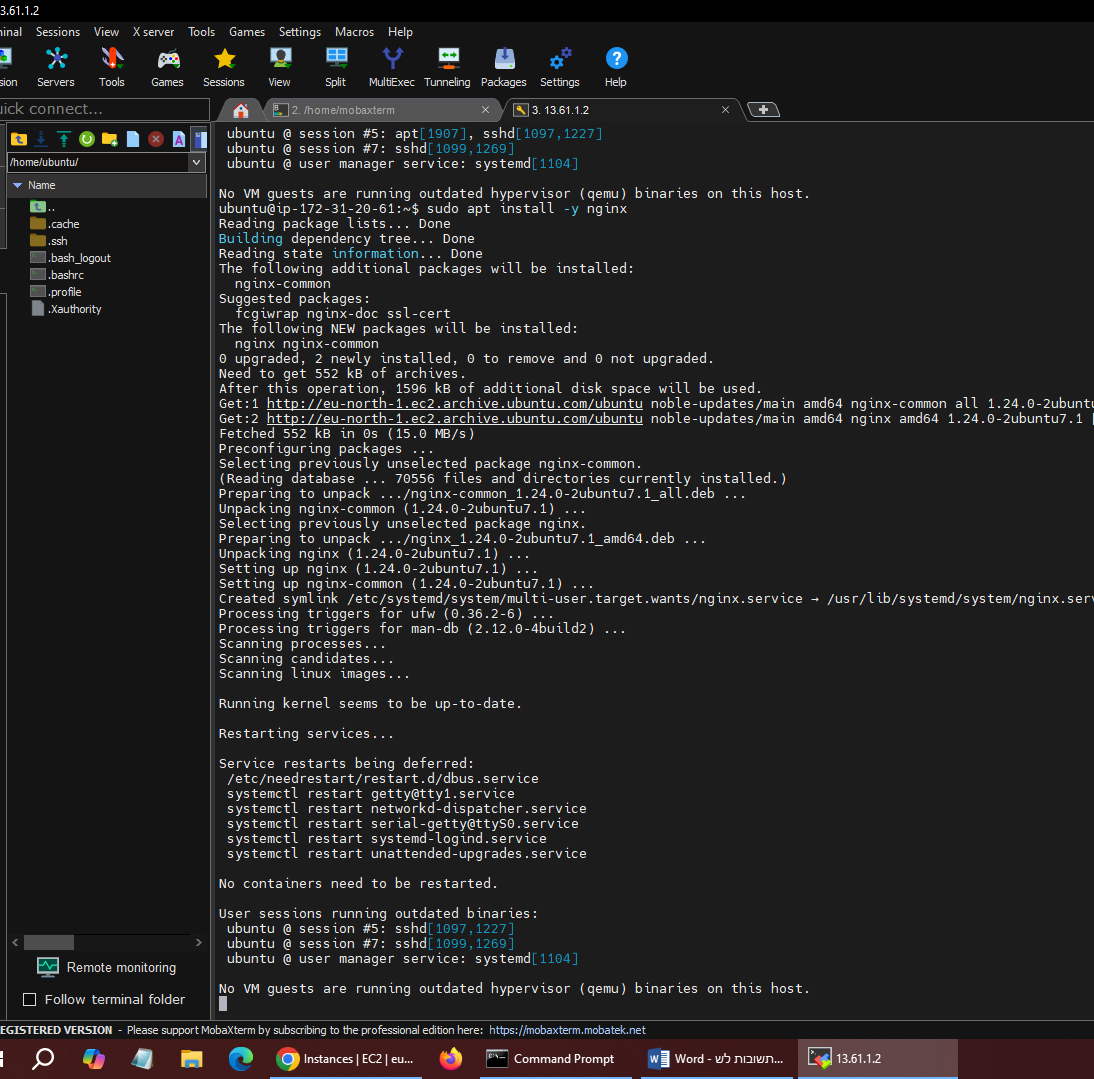
* Connect to the running EC2 instance via SSH.
* 13.61.1.2
* Username Ubuntu
* SSH login
* 

**Install Nginx and create a simple HTML welcome page - see commands to run below:  
sudo apt update –y**

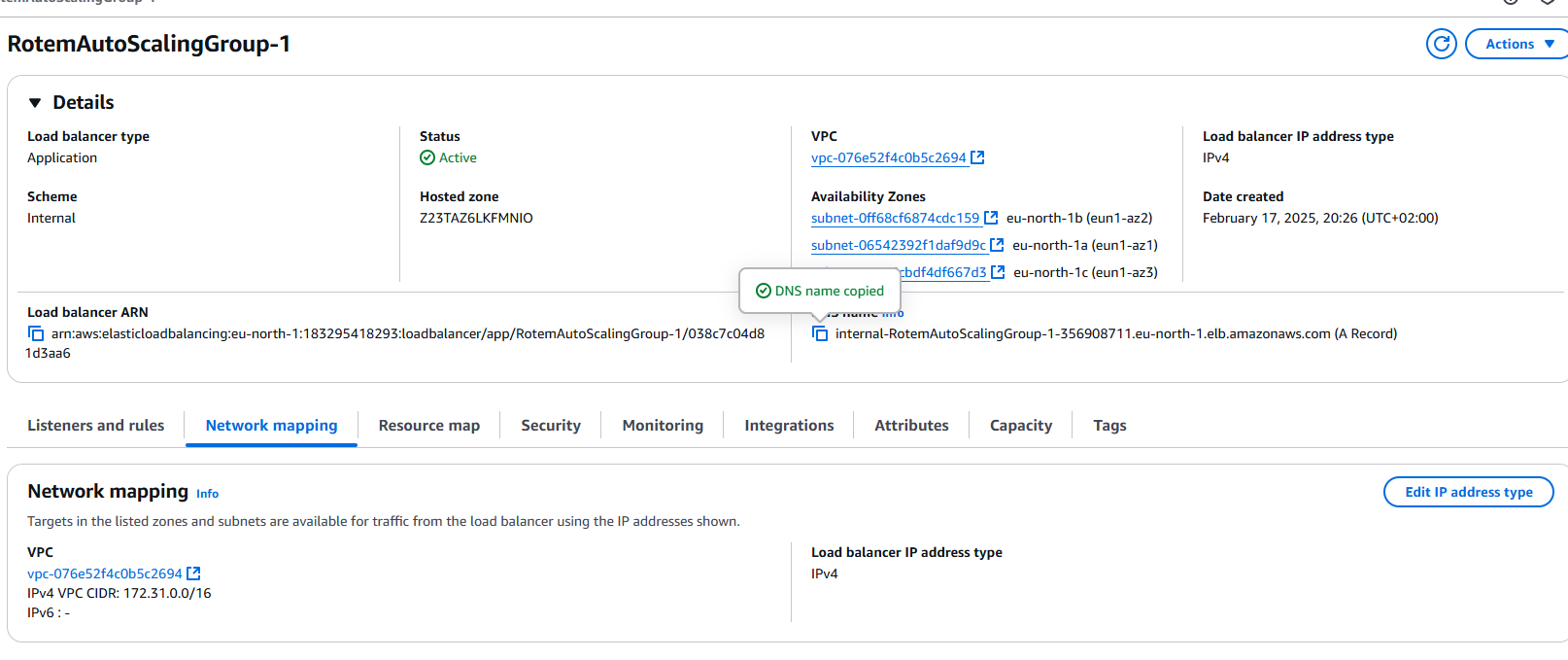
**Sudo apt upgrade** 

**s**

|  |
| --- |
| **sudo yum update -y sudo yum install -y nginx echo "<h1>Welcome to AWS Auto Scaling</h1>" | sudo tee /usr/share/nginx/html/index.html sudo systemctl start nginx sudo systemctl enable nginx**  **# Validate that it works by running:**  **curl** [**http://localhost:80**](http://localhost:80) |

* **Provide a screenshot of the running Nginx service on the instance and the output of the curl command**
* ****
* **Sudo apt –y nginx**
* ****

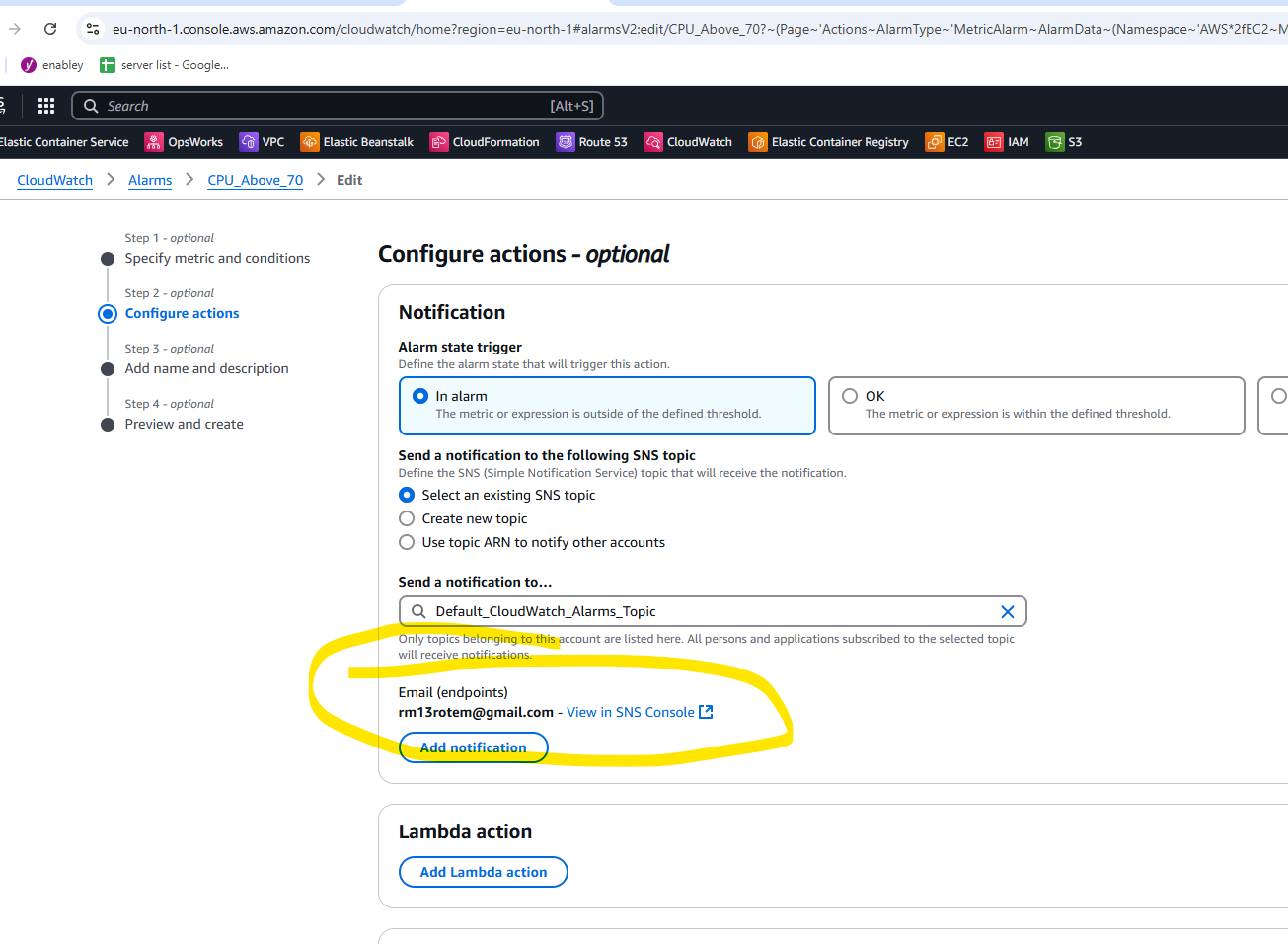
**3. Access the Web Page via the Load Balancer**

* Retrieve the Load Balancer DNS name.
* Open a web browser and access the Load Balancer URL.
* Take a screenshot showing the browser with the Load Balancer DNS and the welcome page.

**4. IAM User Setup for S3 Access**

* Create a new IAM user with permissions limited to accessing a specific S3 bucket.
* Provide a screenshot of the IAM policy attached to the user.
* Log in as the IAM user and verify access to the S3 bucket.
* Provide a screenshot showing the IAM user accessing the S3 bucket in the AWS Console.

**5. Create a CloudWatch Alarm for CPU Usage**

* Navigate to AWS CloudWatch and create an alarm for the EC2 instance.
* Set the alarm to trigger when CPU utilization exceeds 70% for 5 minutes.
* Configure notifications via email (SNS).
* Provide a screenshot of the CloudWatch alarm configuration.
* Same as before –
* 

**End of Exam**

**Send your answers and screenshots via email to your instructor.**