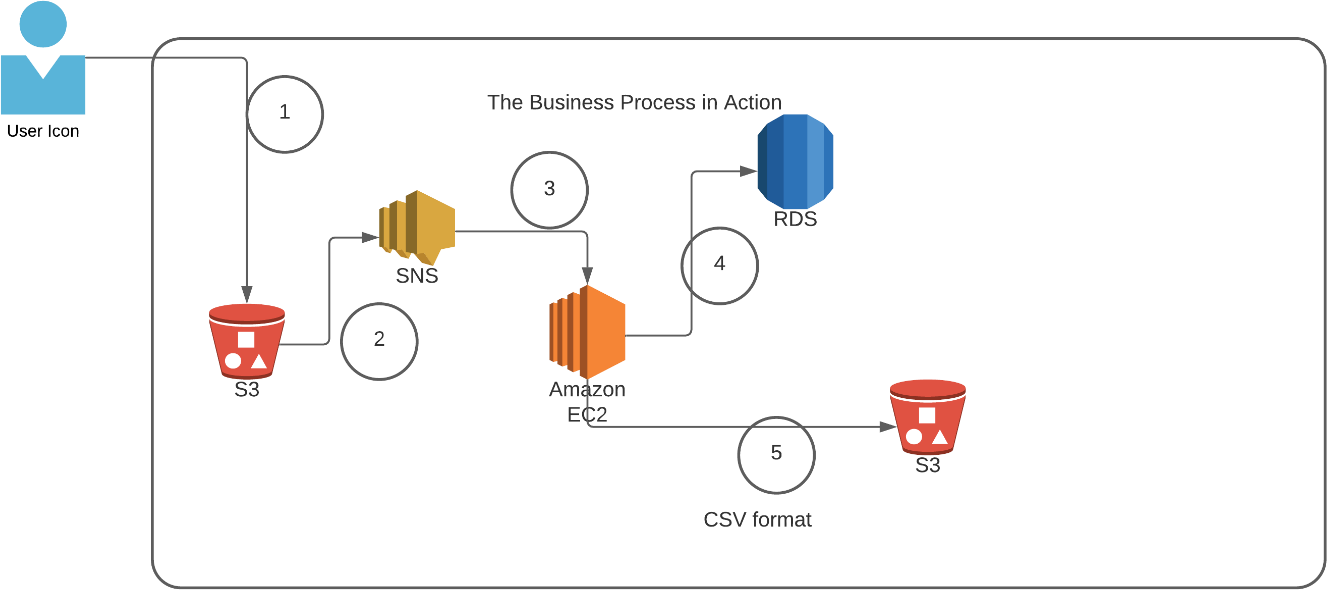
Lab Assignment - 2

|  |  |  |
| --- | --- | --- |
| **Declaration** |  | |
| Questions in this exercise are intentionally complex and could be convoluted or confusing. This is by design and to simulate real life situations where customers seldom give crystal clear requirements and ask unambiguous questions. | | |
| I have read the above statement and agree to these conditions | | |
| I AGREE | **Prasad Roundhal** | |
| <Enter your name above this line to indicate that you are in agreement> | |
|  | | |
| **Instructions** |  | |
| Every screenshot requested in this workbook is compulsory and carries 1 marks | | |
| Your AWS account ID must be clearly visible in every screenshot using the AWS console; missing id or using someone else's id is not permitted. Such cases will be considered as plagiarism and severe penalty will be imposed. | | |
| All screenshots must be in the order mentioned under "Expected Screenshots" for every step | | |
| DO NOT WAIT UNTIL THE LAST MINUTE. The program office will not extend the project submission deadline under any circumstances. | | |
| The file should be renamed in the format BATCH\_FIRSTNAME\_LASTNAME\_PROJECT1. For example: PGPCCMAY18\_VIJAY\_DWIVEDI\_PROJECT1.pdf | | |
|  | | |
| **Resource Clean Up** | |  |
| Cloud is always pay per use model and all resources/services that we consume are chargeable. Cleaning up when you’ve completed your lab or project is always necessary. This is true whether you’re doing a lab or implementing a project at your workplace. | | |
| After completing the lab, make sure to delete each resource created in reverse chronological order. | | |
| Each AWS Academy session lasts for 4 hours by default, although you can extend a session to run longer by pressing the start button to reset your session timer. At the end of each session, any resources you created in the account will be preserved. Some AWS resources, such as EC2 instances, may be automatically shut down, while other resources, such as RDS instances will be left running. | | |

**Architecture diagram**

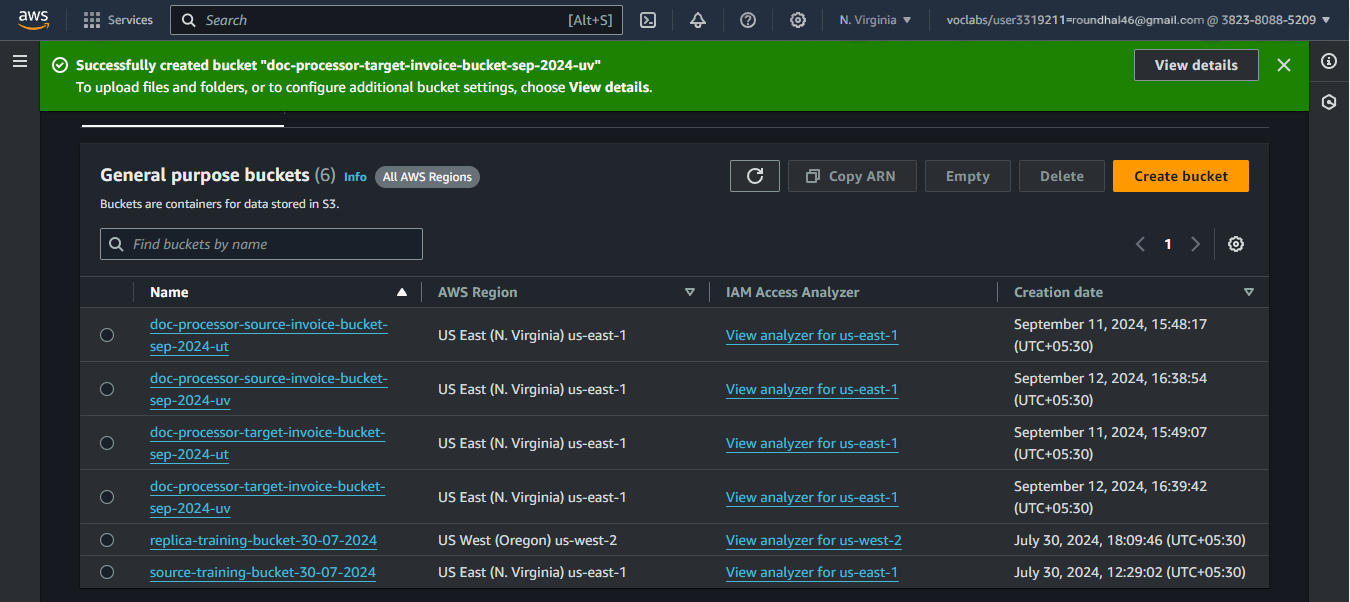


|  |  |
| --- | --- |
| **Architecture Implementation** | |
| 1 | The customer uploads the invoice data to S3 bucket in a text format as per their guidelines and policies. This bucket will have a policy to auto delete any content that is more than 1 day old (24 hours). |
| 2 | An event will trigger in the bucket that will place a message in SNS topic |
| 3 | A custom program running in EC2 will subscribe to the SNS topic and get the message placed by S3 event |
| 4 | The program will use S3 API to read from the bucket, parse the content of the file and create a CSV record and save the details in an RDS database |
| 5 | The program will use S3 API to write CSV record to destination S3 bucket as new S3 object. |

**Step 1: SNS and S3 topic creation**

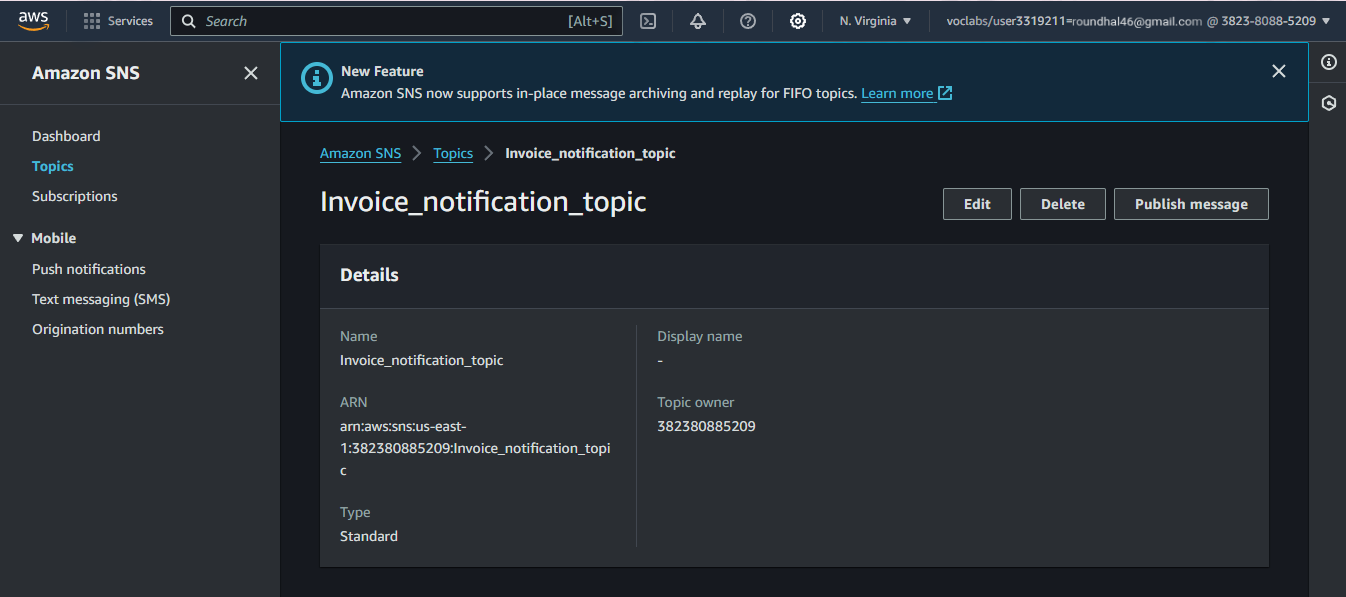
|  |  |
| --- | --- |
| Step number | a |
| Step name | Creation of Source and target buckets |
| Instructions | 1. Navigate to S3 using the Services button at the top of the screen 2. Select "Create Bucket" 3. Enter a source bucket name and use the default options for the rest of the fields 4. Click on "Create Bucket' 5. Repeat the above steps to create a target bucket |
| Expected screenshots | 1) Screen showing created S3 source and target buckets |

**Screenshot for a(1)**

****

|  |  |
| --- | --- |
| Step number | b |
| Step name | Creation of SNS subscription |
| Instructions | 1. Navigate to SNS -> Topics 2. Click on "Create Topic" 3. Enter the following fields Name : S3toEC2Topic   The other options can be ignored for now   1. Click on Create Topic |
| Expected screenshots | 1) Creation of SNS topic |

**Screenshot for b(1)**



****

|  |  |
| --- | --- |
| Step number | c |
| Step name | Modification of SNS Access Policy |

|  |  |
| --- | --- |
| Instructions | 1. Navigate to SNS -> Topics and select the topic created in the previous step 2. Note down the ARN shown in the topic details 3. Click on Edit and select "Access Policy". 4. Replace the text in the JSON editor with the following   {  "Version": "2012-10-17",  "Id": "example-ID", "Statement": [  {  "Sid": "example-statement-ID", "Effect": "Allow",  "Principal": {  "AWS":"\*"  },  "Action": [ "SNS:Publish"  ],  "Resource": "**SNS-topic-ARN**", "Condition": {  "ArnLike": { "aws:SourceArn": "arn:aws:s3:\*:\*:**bucket-name**" }, "StringEquals": { "aws:SourceAccount": "**bucket-owner-account-id**" }  }  }  ]  }   1. Replace the bold text with the SNS topic ARN, source bucket name and your AWS account ID respectively. 2. Click on Save Changes |
| Expected screenshots | 1) JSON Editor screen |

**Screenshot for c(1)**

****

|  |  |
| --- | --- |
| Step number | d |
| Step name | Configuring SNS notifications for S3 |
| Instructions | 1. Navigate to S3 and select the source bucket created in Step 1 (a) 2. Select Properties and scroll down to Event Notifications and select it 3. Select "Create Event Notification" 4. Fillup the details as follows Name : S3PutEvent   Select PUT from the list of radio buttons Destination : Select SNS Topic  SNS : Select S3ToEC2Topic   1. Save Changes |
| Expected screenshots | 1) Event Configuration Screen |

**Screenshot for d(1)**

****

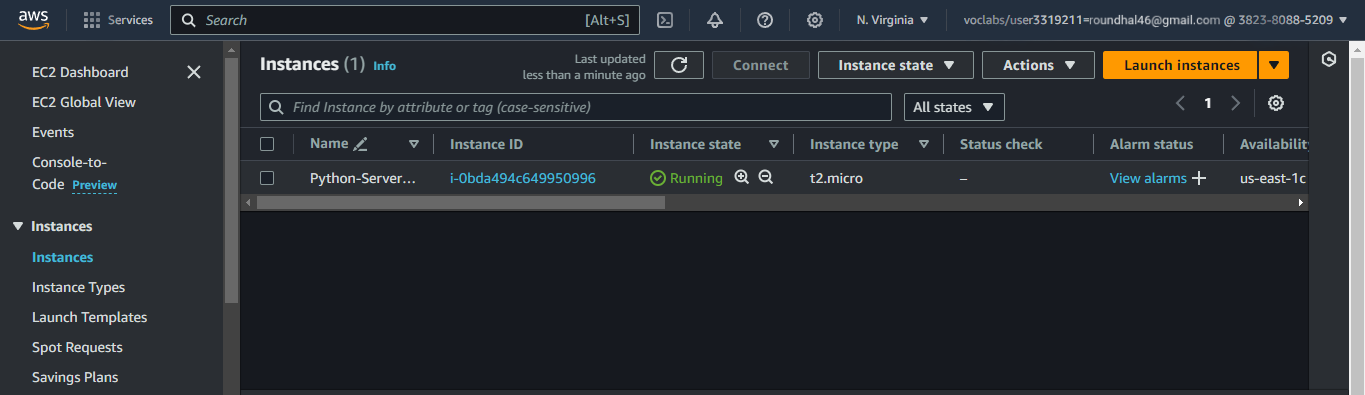
Step 2: Run the custom program in the EC2 instance

|  |  |
| --- | --- |
| Step number | a |
| Step name | Creation of the EC2 instance and RDS instance |
| Instructions | 1. Navigate to EC2 -> Instances 2. Create an EC2 instance with the following parameters   AMI : Amazon Linux 2  VPC : Default  Security group : Ports 22 and 8080 should be opened   1. Navigate to RDS 2. Create an RDS instance with the following parameters:   Engine type : MySql Template : Dev/Test  Set the username and password as required DB Instance class : Burstable  Instance type : t3.micro Public Access : Yes  VPC Security group : Create New ()  Under Additional Configuration, add an initial database name. Take note of this name as it will be required later.  Uncheck “Enable Enhanced Monitoring”  Ensure that the security group created by the RDS deployment has port 3306 open for all incoming connections from all sources. |
| Expected  screenshots | 1. List of instances after creation of EC2 instance 2. List of RDS instances |

**Screenshot for a(1)**

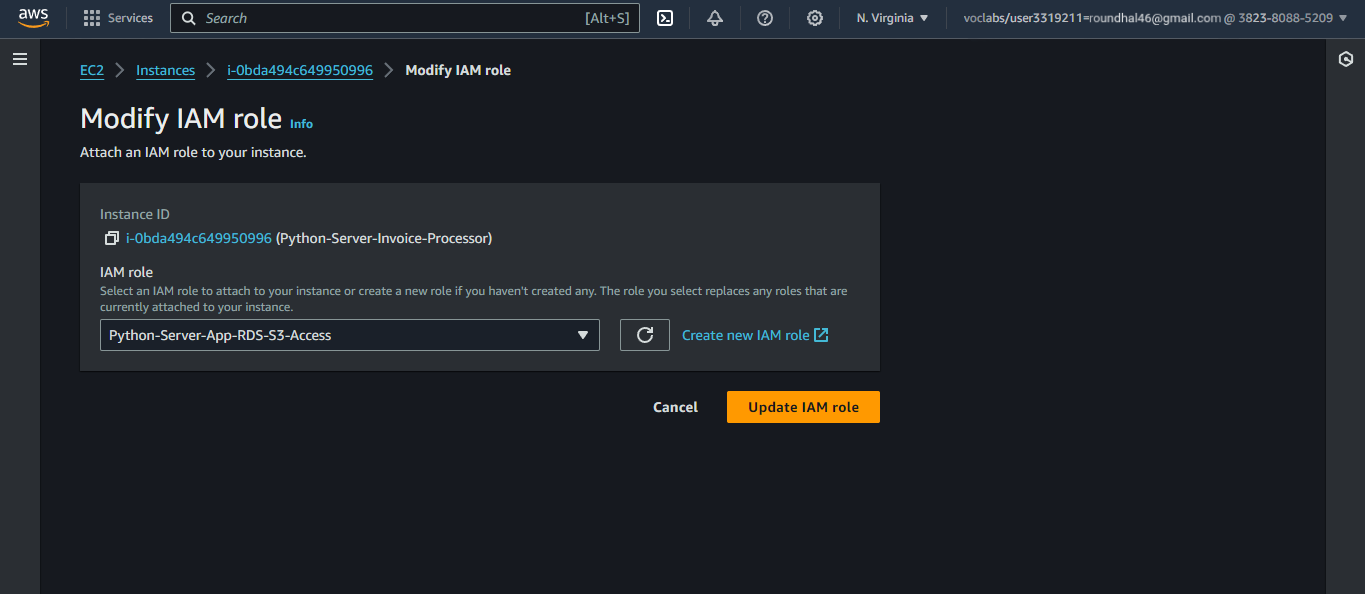
****

**Screenshot for a(2)**

****

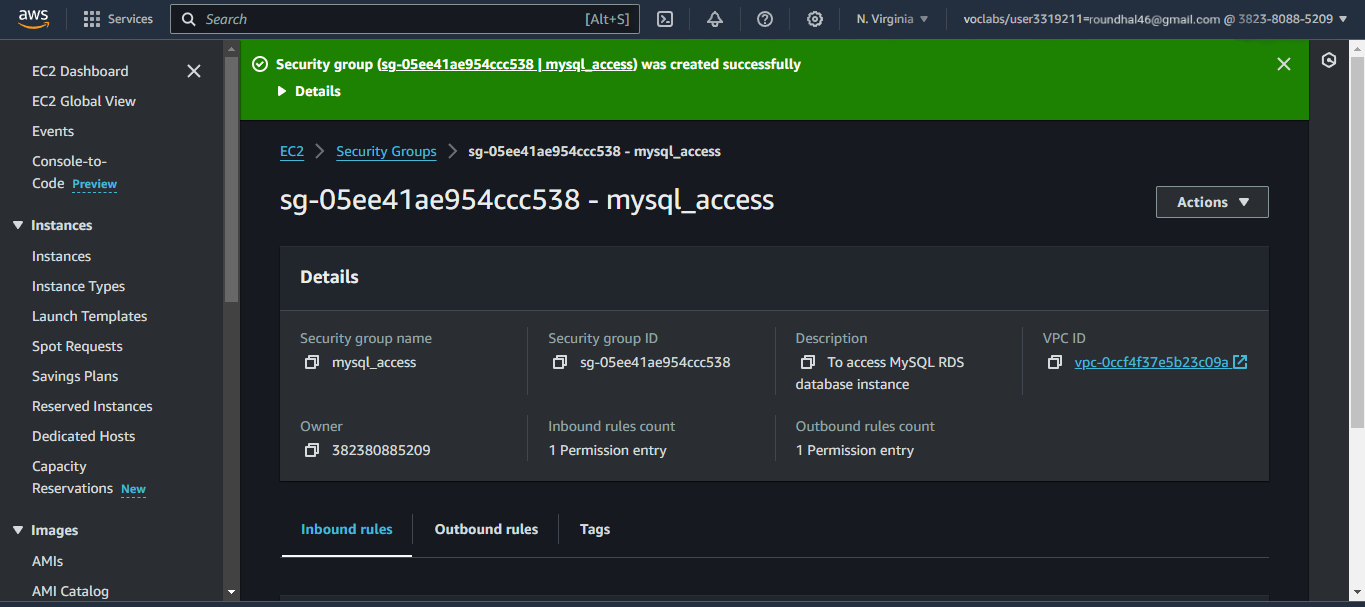
|  |  |
| --- | --- |
| Step number | B |
| Step name | Assignment of IAM role for EC2 instance |
| Instructions | 1. Navigate back to EC2- > Instances 2. Select the EC2 instance created in the previous step and select Actions-> Security -> Modify IAM role 3. Select the role LabInstanceProfile from the   dropdown and click on Save |
| Expected screenshots | 1) Modify IAM role screen |

**Screenshot for b(1)**

****

|  |  |  |
| --- | --- | --- |
| Step number | c |  |
| Step name | Configuration and Uploading of custom program |  |
| Instructi ons | 1. Download the file **docproc-new.zip** on your machine 2. Unzip the downloaded file 3. Enter the unzipped folder and open the file [views.py](http://views.py/) in the API folder using a text editor 4. In line number 19-24, modify the target   bucket name to the one created in Step 2  (a) and modify the hostname, username, password and database variables to the values set while creating the RDS database and save the file  5) Copy the folder docproc-new to the home folder of the EC2 instance created in Step 3(a) using scp. Use the command given below  *scp -i <pem> -r ./docproc-new ec2- user@<ip>:/home/ec2-user* |  |
| Expecte d screens hots | 1) Modifying of the [views.py](http://views.py/) file to point to  the target bucket | 2)Copying the folder to the  EC2 instance |

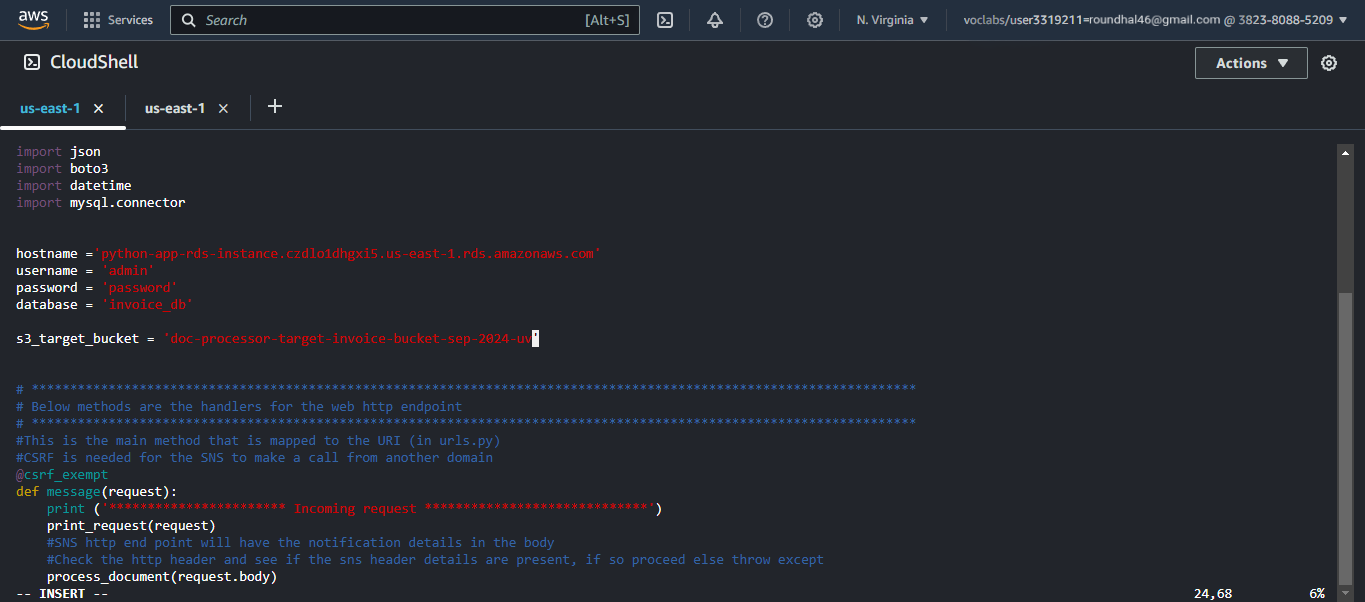
**Screenshot for c(1)** 

****

**Screenshot for c(2)**

**DETAILS:**

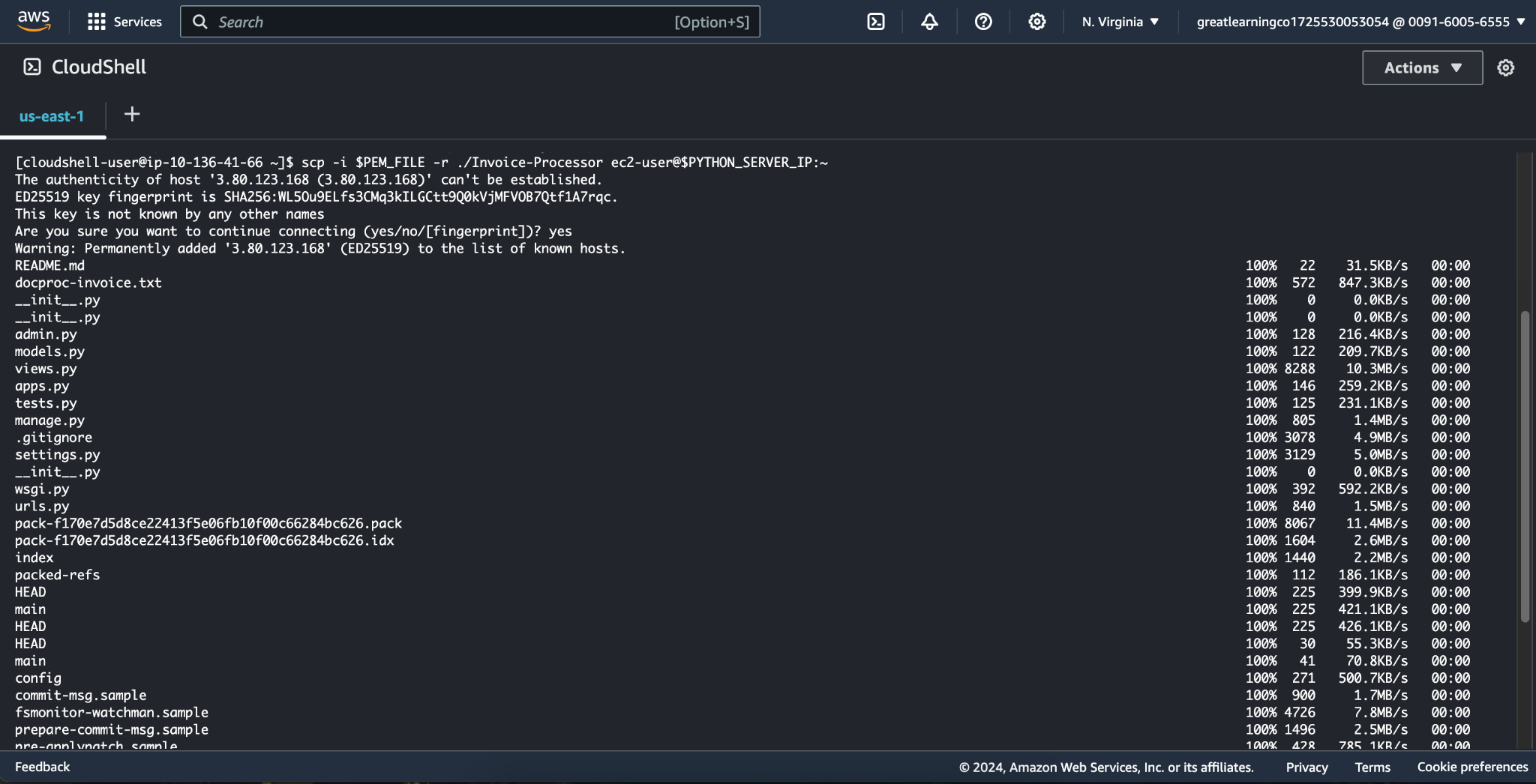
****

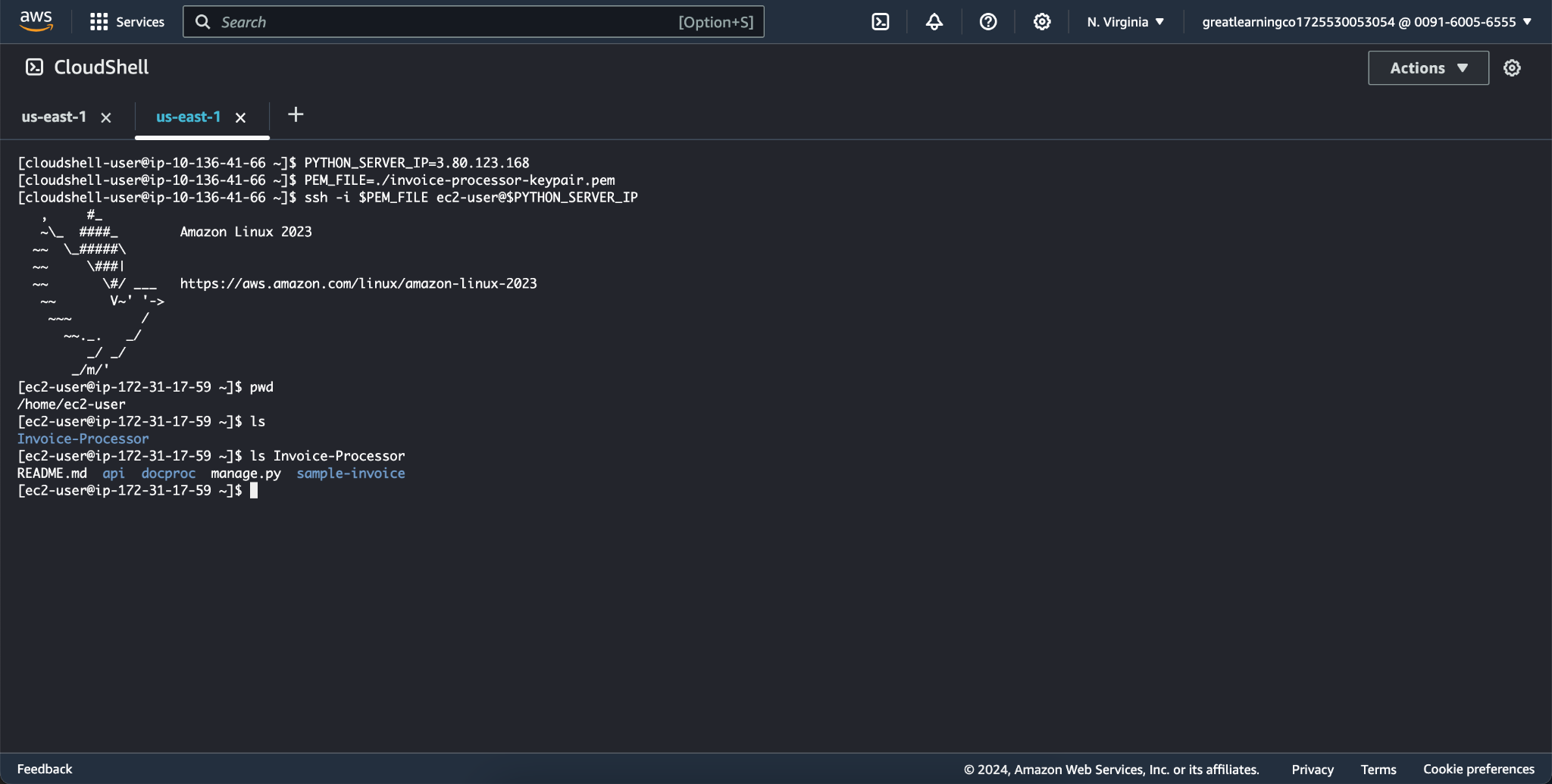
****

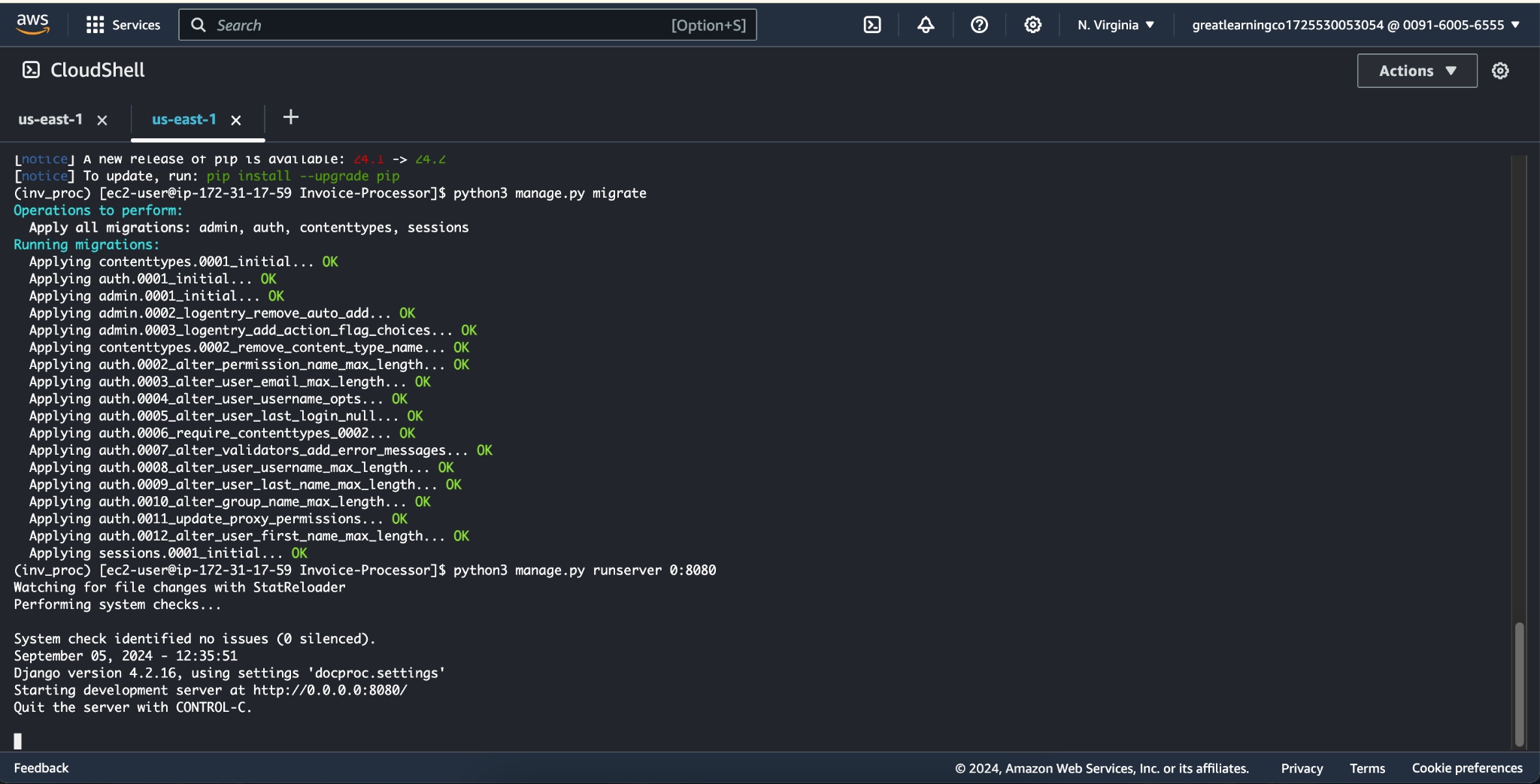
Step 3: Creation and Verification of SNS subscription and Generation of CSV file

|  |  |
| --- | --- |
| Step number | a |
| Step name | Starting the EC2 custom program |
| Instructions | 1. Log into the EC2 instance using SSH 2. Run the followng commands after successful SSH to start the server sudo cp -r docproc-new /opt   sudo chown ec2-user:ec2-user -R /opt cd /opt/docproc-new  sudo yum update  sudo yum install python-pip -y  python -m pip install --upgrade pip setuptools sudo pip install virtualenv  virtualenv ~/.virtualenvs/djangodev  source ~/.virtualenvs/djangodev/bin/activate pip install django  pip install boto3  pip install mysql-connector-python-rf python manage.py runserver 0:8080  **Keep this terminal window open throughout the rest of the exercise** |
| Expected screenshots | 1) Server in waiting state |

**Screenshot for a(1)**

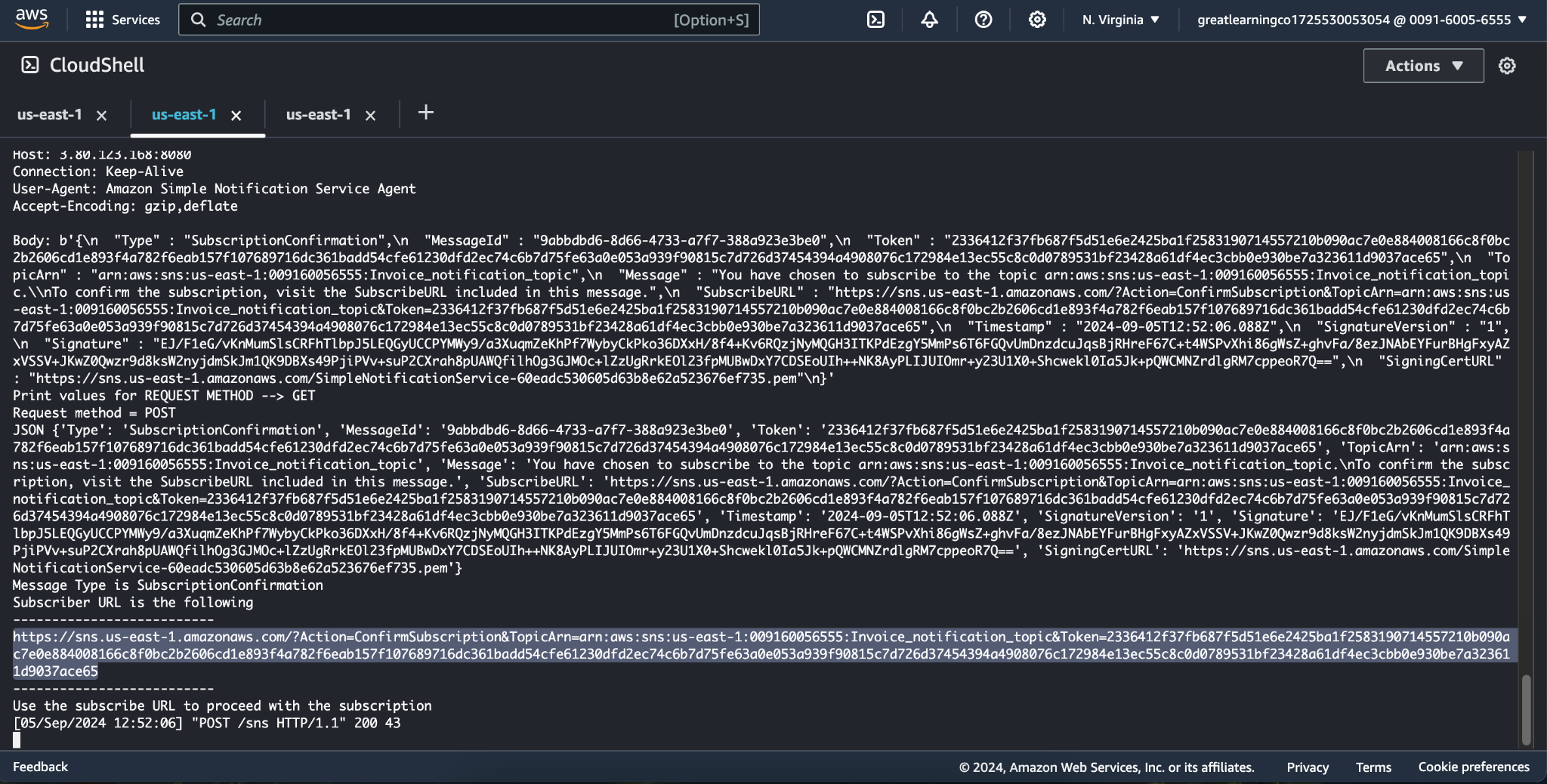
****

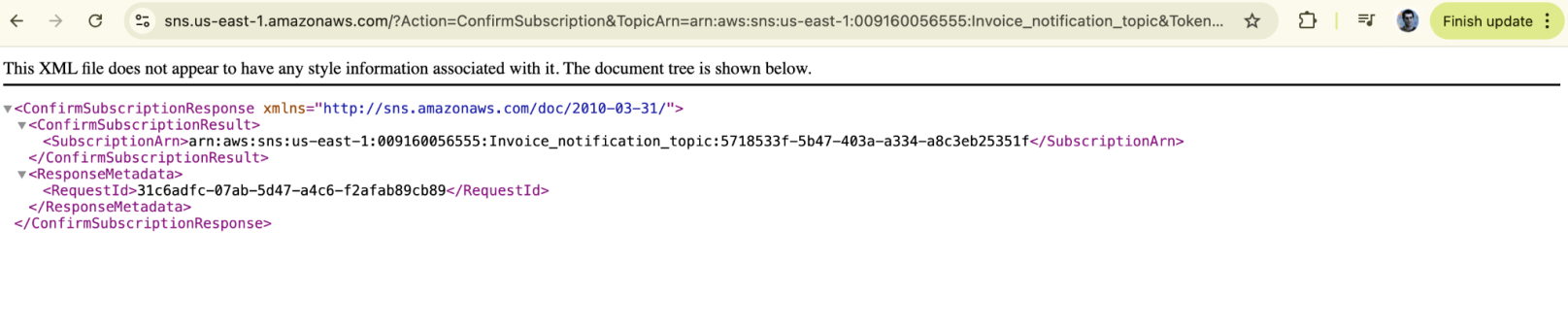
****

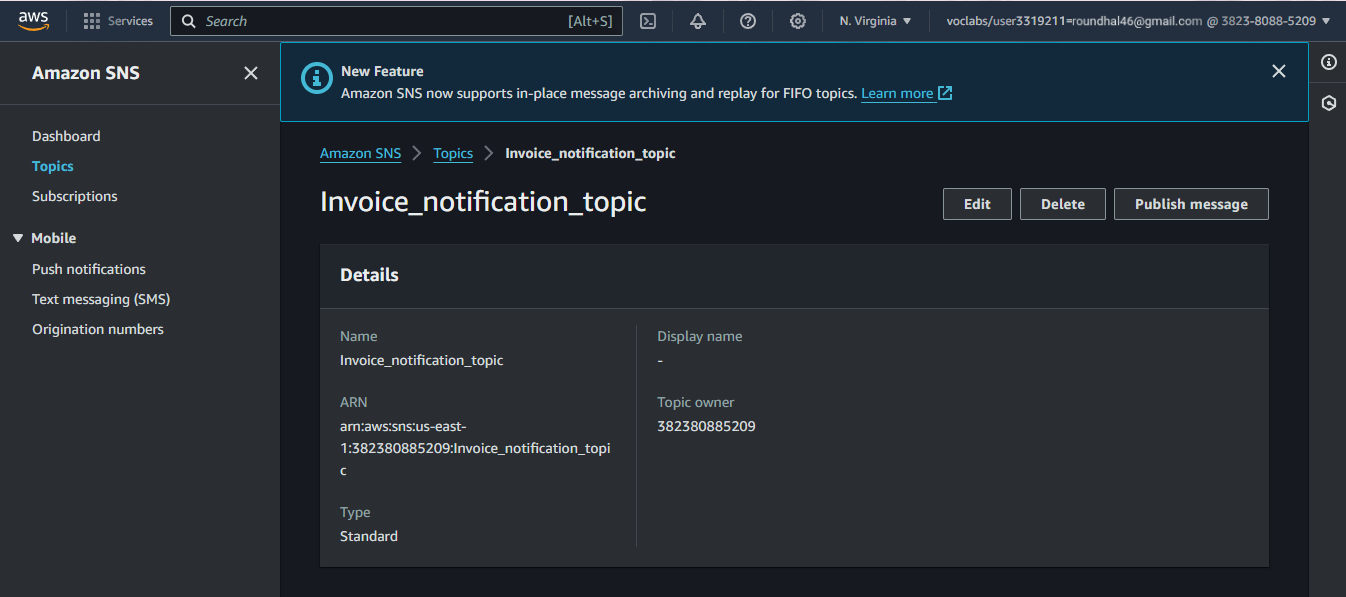
****

|  |  |
| --- | --- |
| Step number | b |
| Step name | Creation of  SNS  subscription |
| Instructions | 1. Navigate to SNS in the AWS Console and select the topic S3ToEC2Topic 2. Click on Create Subscription 3. Enter the following details Protocol : HTTP   Endpoint : http://<host>:8080/sns where <host> in the public IP of the EC2 instance Click on Create Subscription   1. In the EC2 terminal window, look for the field "SubscribeURL" and copy the entire link given   **Note: If a message is seen "ValueError: No JSON object could be decoded", it can be safely ignored**   1. Paste that link into a browser window to verify the SNS subscription (Ignore any   messages received in the web browser) |
| Expected screenshots | 1)  Subscription URL in EC2  terminal Window |

**Screenshot for b(1)**

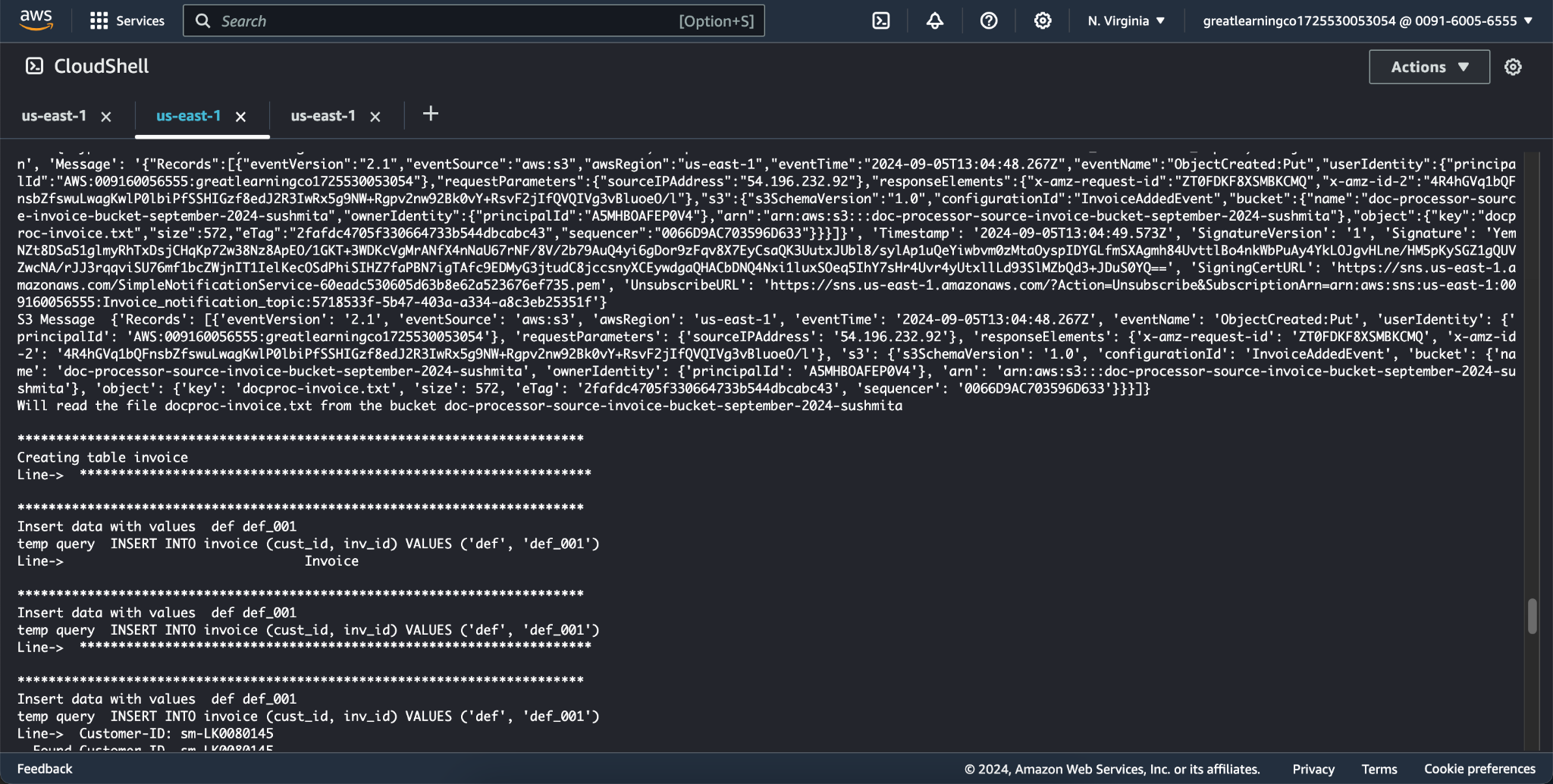
****

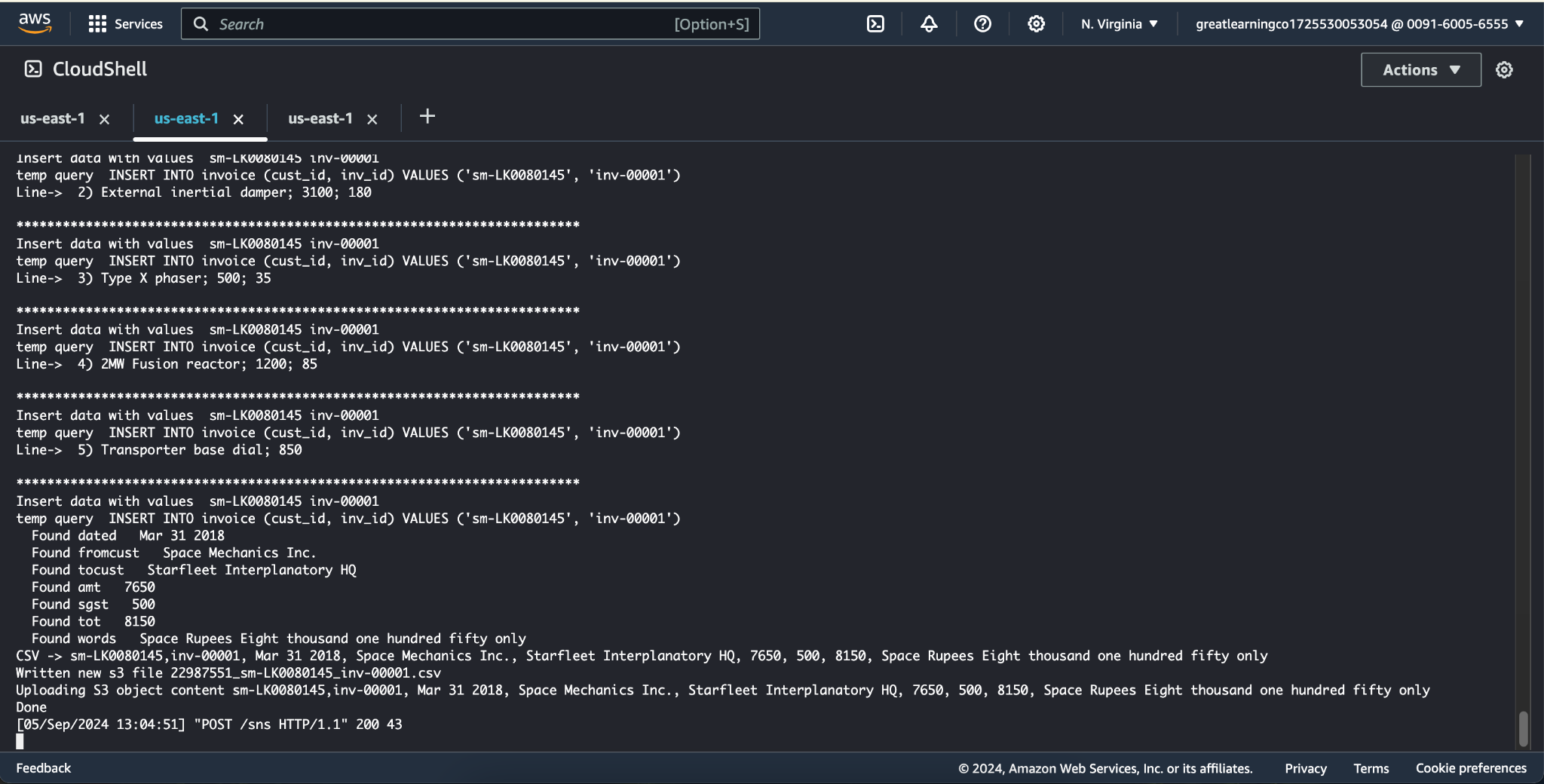
****

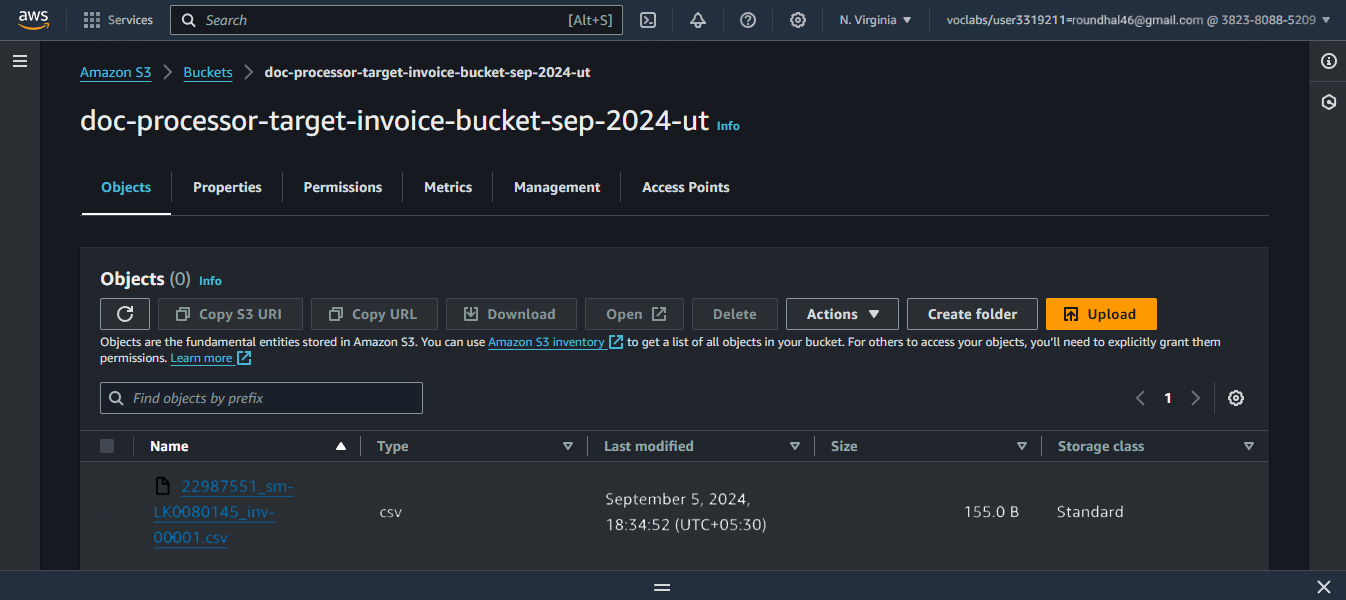
****

|  |  |
| --- | --- |
| Step number | c |
| Step name | Generation of CSV file |
| Instructions | 1. Download the file **docproc-invoice.txt** provided with this workbook 2. Navigate to S3 in the AWS Console 3. Upload the sample invoice file to the source S3 bucket using the default options 4. Verify that a CSV file is generated in the target S3 bucket. This may take a few minutes 5. (Optional) Login to the RDS instance using your preferred MySQL client and check the table created inside the specified database. |
| Expected screenshots | 1) Generated CSV file in the target S3 bucket |

**Screenshot for c(1)**

****

****

****

|  |  |
| --- | --- |
| **Answer the following questions** | |
| Q1 | Which of the following properties of an AWS resource is sufficient and necessary to uniquely identify it across all of AWS? |
|  | a) ARN |

****

|  |  |
| --- | --- |
|  | b) Region and ARN |
|  | c) ARN and Account number |
|  | d) Depends on the resource used |
|  | Enter your answer here  **A) ARN** |
| Q2 | Which of the following step numbers in Step 1 allowed S3 to publish to the SNS topic created? |
|  | a) 1(a) |
|  | b) 1(c) |
|  | c) 1(d) |
|  | d) 1(b) |
|  | Enter your answer here **B) 1(c)** |
| Q3 | Which port is being used by SNS to send the notification to the custom program? |
|  | a) 8081 |
|  | b) 80 |
|  | c) 8080 |
|  | d) 8065 |
|  | Enter your answer here **C) 8080** |
| Q4 | How many IAM roles can be attached to an EC2 instance at a time? |
|  | a) 2 |
|  | b) 3 |
|  | c) 1 |
|  | d) Depends on the policies required |
|  | Enter your answer here **C) 1** |

|  |  |
| --- | --- |
| Q5 | As a product manager, how would you describe the benefits of this architecture to  an client, as compared to an equivalent on-premises architecture? |

**Answer -** Benefits of Cloud-Based Architecture Compared to On-Premises Solutions

**1. Scalability and Flexibility**

**Cloud-Based**: With AWS, you can easily scale resources up or down based on your needs. If you have a sudden increase in invoice data, the system can handle it without manual intervention.

**On-Premises**: Scaling requires purchasing and installing additional hardware, which can be costly and time-consuming. Managing capacity for peak loads involves over-provisioning, leading to inefficiencies and wasted resources.

**2. Automatic Data Management**

**Cloud-Based**: The use of an S3 bucket with an auto-delete policy ensures that old data is automatically managed, reducing manual intervention and potential for errors. This helps in maintaining storage efficiency and compliance with data retention policies.

**On-Premises**: Managing data lifecycle manually can be labour-intensive.

**3. Event-Driven Architecture**

**Cloud-Based**: Integration with SNS allows for an event-driven approach where actions are triggered automatically based on data events (e.g., a new file upload).

**On-Premises**: Setting up an equivalent event-driven system on-premises would involve complex infrastructure and may require custom development for real-time processing, leading to higher costs and complexity.

**4. Managed Services and Reduced Maintenance**

**Cloud-Based**: AWS services like S3, SNS, and RDS are managed, meaning AWS handles the maintenance, updates, and scaling. This reduces the burden on your IT staff and ensures high availability and reliability.

**On-Premises**: Managing hardware, software, and updates in-house requires significant resources and expertise. Ensuring high availability and handling maintenance tasks can lead to increased operational costs and resource allocation.

**5. Cost Efficiency**

**Cloud-Based**: You benefit from a pay-as-you-go model where you only incur costs based on actual usage.

**On-Premises**: Requires significant upfront investment in hardware and software, along with ongoing costs for maintenance, upgrades, and energy consumption.

**6. Disaster Recovery and High Availability**

**Cloud-Based**: AWS provides built-in disaster recovery options and high availability across multiple regions and availability zones.

**On-Premises**: Implementing robust disaster recovery and high availability solutions on-premises can be complex and expensive, often requiring duplicate infrastructure and comprehensive backup strategies.

**7. Security and Compliance**

**Cloud-Based**: AWS offers a range of security features and compliance certifications that can be leveraged to protect your data. This includes encryption, access controls, and audit logs, which are managed and updated by AWS.

**On-Premises**: Ensuring security and compliance involves investing in specialised hardware, software, and skilled personnel to continuously manage and update security measures.