AWS-Cloud-Security-Project

In this project, I worked as a cloud security specialist at a Financial bank.

The company has locations throughout the country. The company provides checking and savings accounts, credit cards, loans, and investment products. All products require the use of personally identifiable information (PII), such as account numbers, contact information, and personal IDs. Your manager, the Director of IT, has tasked you to ensure the security of the company's resources in the AWS Cloud.

Key areas of the AWS infrastructure that need to be secured include S3 buckets, the network that hosts web servers, and keys that are used to encrypt data. Your manager also wants you to monitor and analyze access to these resources so that the bank can improve its security posture as changes and potential security incidents occur.

Your task within this project is to secure these AWS resources based on AWS best practices that are associated with the AWS Well-Architected Framework, the principle of least privilege, and internal company IT standards.

Throughout the project, you will test access to resources as two test users, Paulo and Mary, who are members of the Account Manager Group. In some cases, Paulo has more privileged access than Mary, to certain resources stored in the AWS account. You will compare his access to Mary's access. By comparing their access, you will be able to verify if specific resources have been secured by using mechanisms beyond AWS Identity and Access Management (IAM) policies.

In the AWS KMS phase of the project, you will use a test user named Sofia, who is a member of the Financial Advisor Group.

Solution requirements

This project is split into different phases, and each phase is designed to address one or more solution requirements. The solution must meet the following requirements:

- R1 - Design (phase 2)
- R2 - Optimize cost (phase 2)
- R3 - Restrict access (phases 1, 2, and 3)
- R4 - Enforce compliance (phases 3 and 4)
- R5 - Encrypt data (phase 3)

- R6 - Withstand penetration testing (phase 2)
- R7 - Monitor and log user activity (phases 1 and 4)

R8 - Generate alert and change management notifications (phase 4) In this project, you work as a cloud security specialist at AnyCompany Financial bank.

The company has locations throughout the country. The company provides checking and savings accounts, credit cards, loans, and investment products. All products require the use of personally identifiable information (PII), such as account numbers, contact information, and personal IDs. Your manager, the Director of IT, has tasked you to ensure the security of the company's resources in the AWS Cloud.

Key areas of the AWS infrastructure that need to be secured include S3 buckets, the network that hosts web servers, and keys that are used to encrypt data. Your manager also wants you to monitor and analyze access to these resources so that the bank can improve its security posture as changes and potential security incidents occur.

Your task within this project is to secure these AWS resources based on AWS best practices that are associated with the AWS Well-Architected Framework, the principle of least privilege, and internal company IT standards.

Throughout the project, you will test access to resources as two test users, Paulo and Mary, who are members of the Account Manager Group. In some cases, Paulo has more privileged access than Mary, to certain resources stored in the AWS account. You will compare his access to Mary's access. By comparing their access, you will be able to verify if specific resources have been secured by using mechanisms beyond AWS Identity and Access Management (IAM) policies.

In the AWS KMS phase of the project, you will use a test user named Sofia, who is a member of the Financial Advisor Group.

Solution requirements

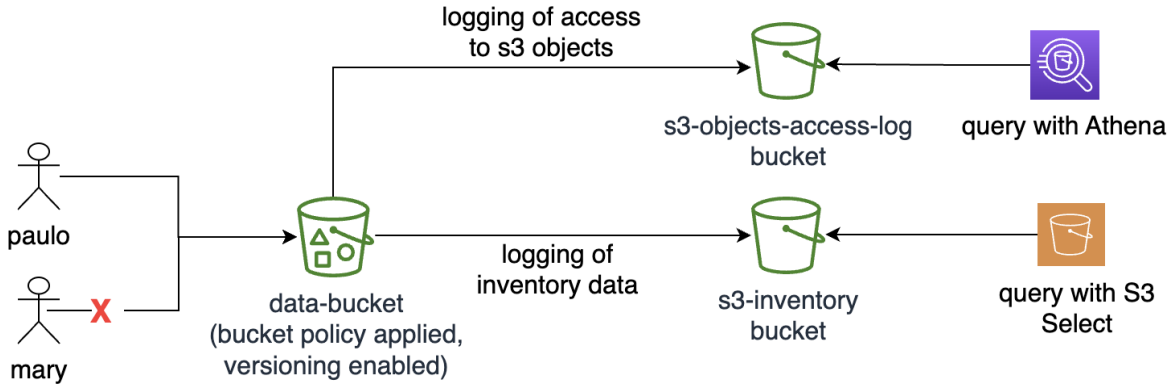
This project is split into different phases, and each phase is designed to address one or more solution requirements. The solution must meet the following requirements:

- R1 - Design (phase 2)
- R2 - Optimize cost (phase 2)
- R3 - Restrict access (phases 1, 2, and 3)

AWS-Cloud-Security-Project

- R4 - Enforce compliance (phases 3 and 4)
- R5 - Encrypt data (phase 3)
- R6 - Withstand penetration testing (phase 2)
- R7 - Monitor and log user activity (phases 1 and 4)
- R8 - Generate alert and change management notifications (phase 4)

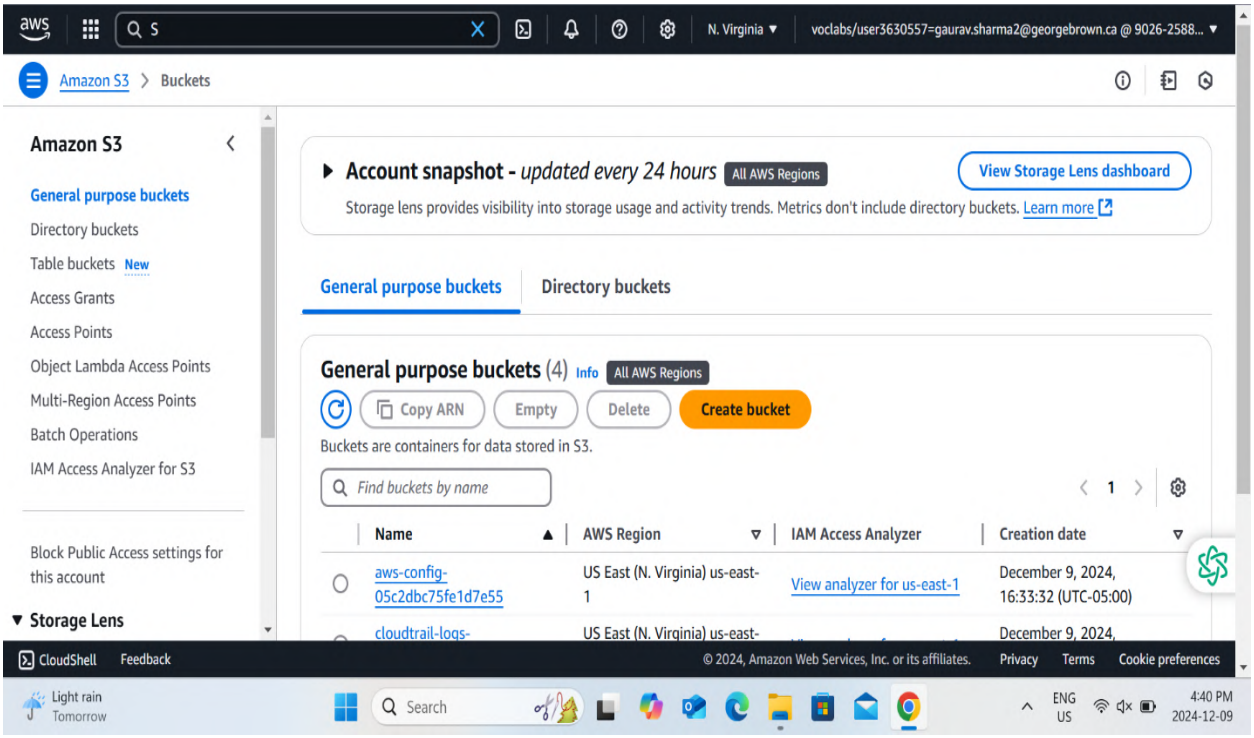
Cloud Security Builder: Securing and Monitoring Resources with AWS



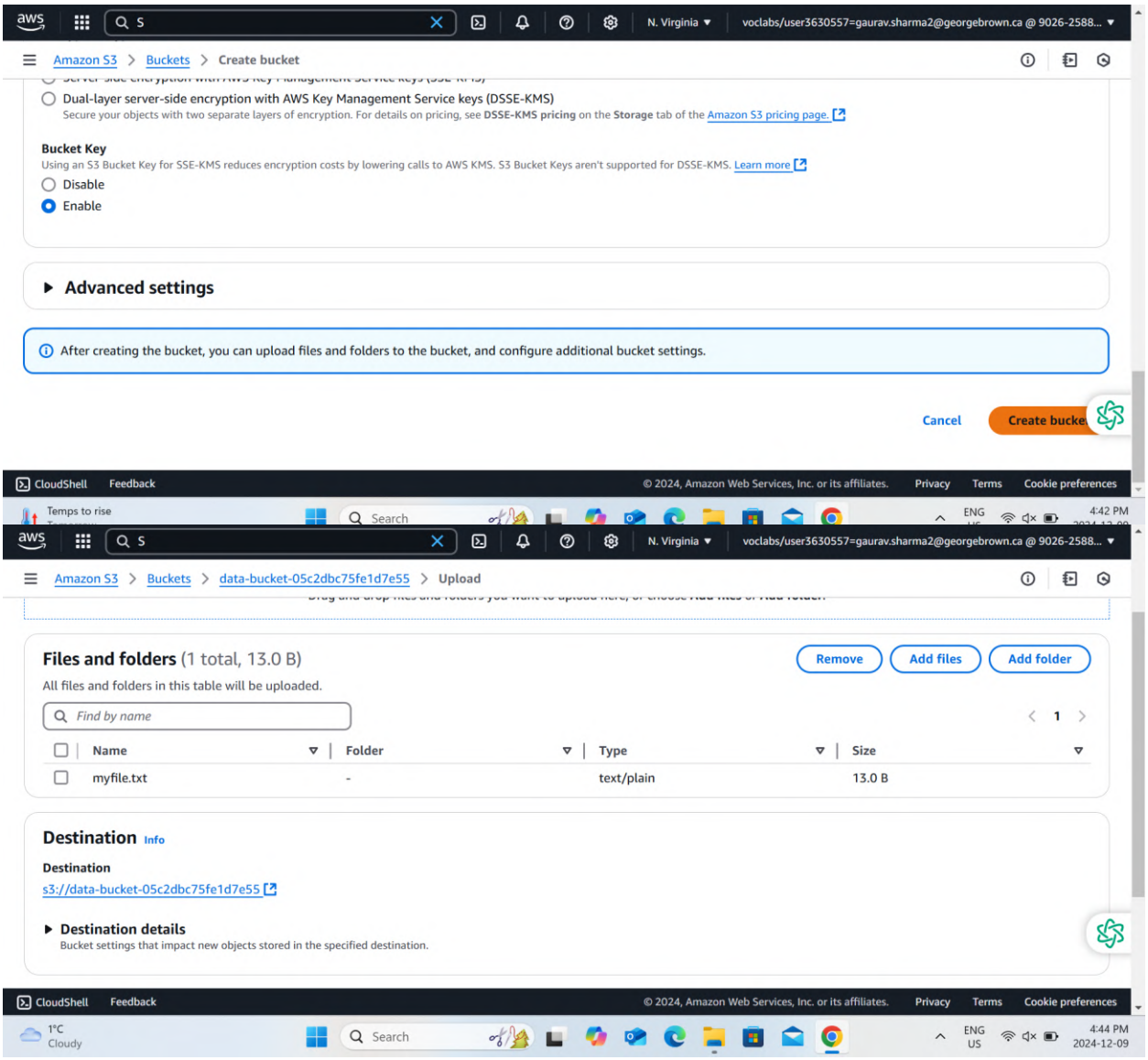
Phase 1: Securing data in Amazon S3

Task 1.1: Create a bucket, apply a bucket policy, and test access

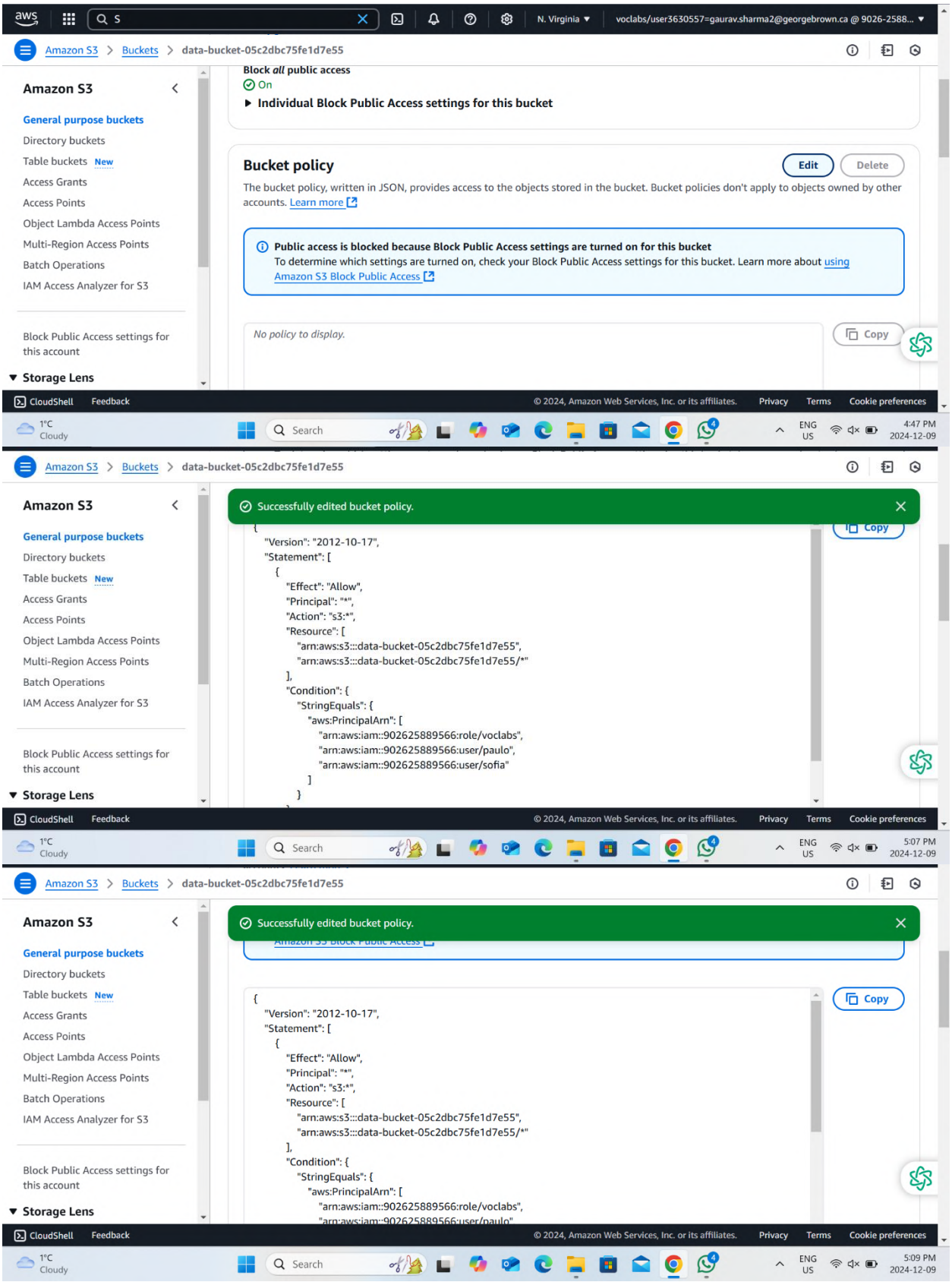
AWS-Cloud-Security-Project



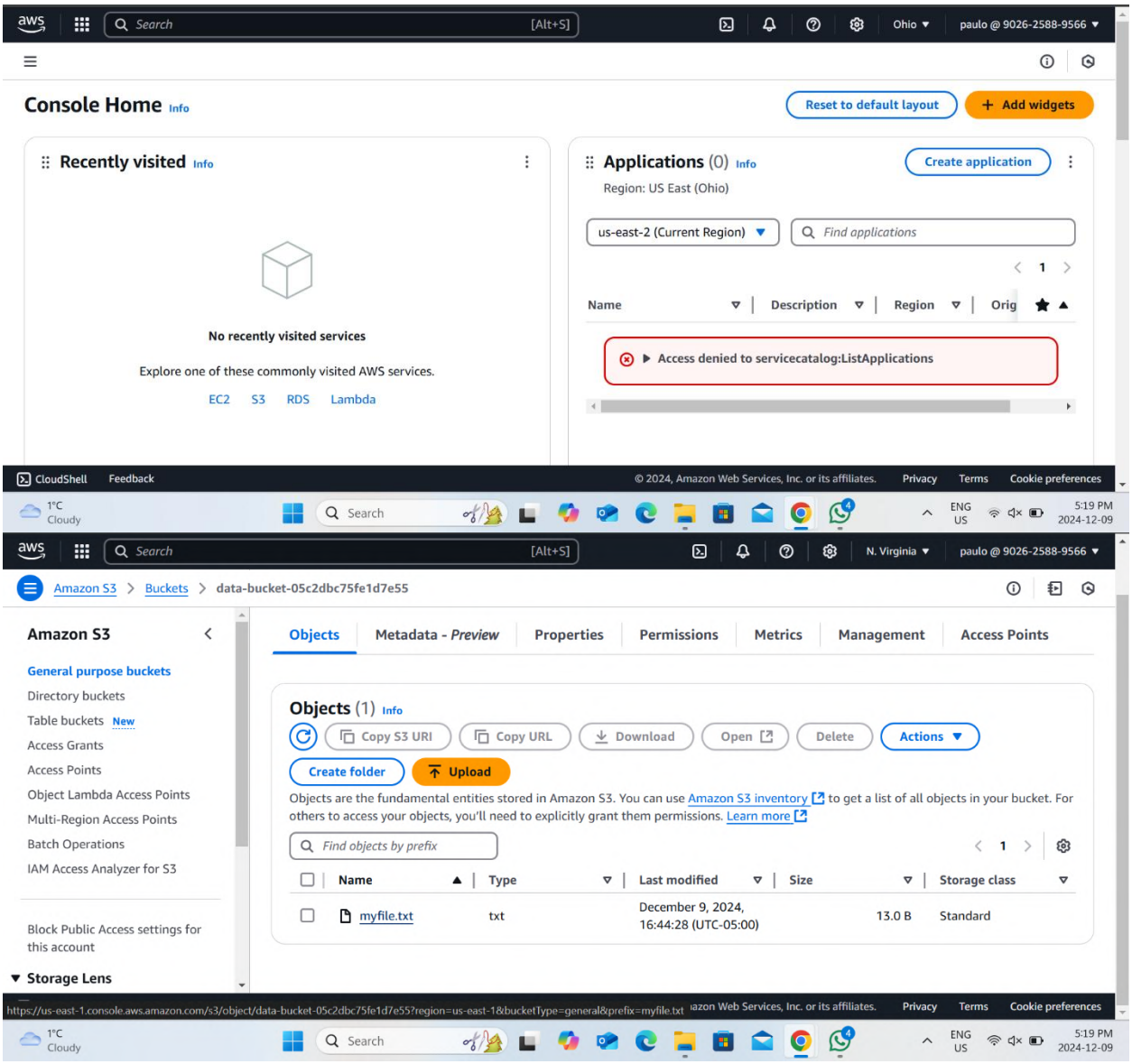
AWS-Cloud-Security-Project



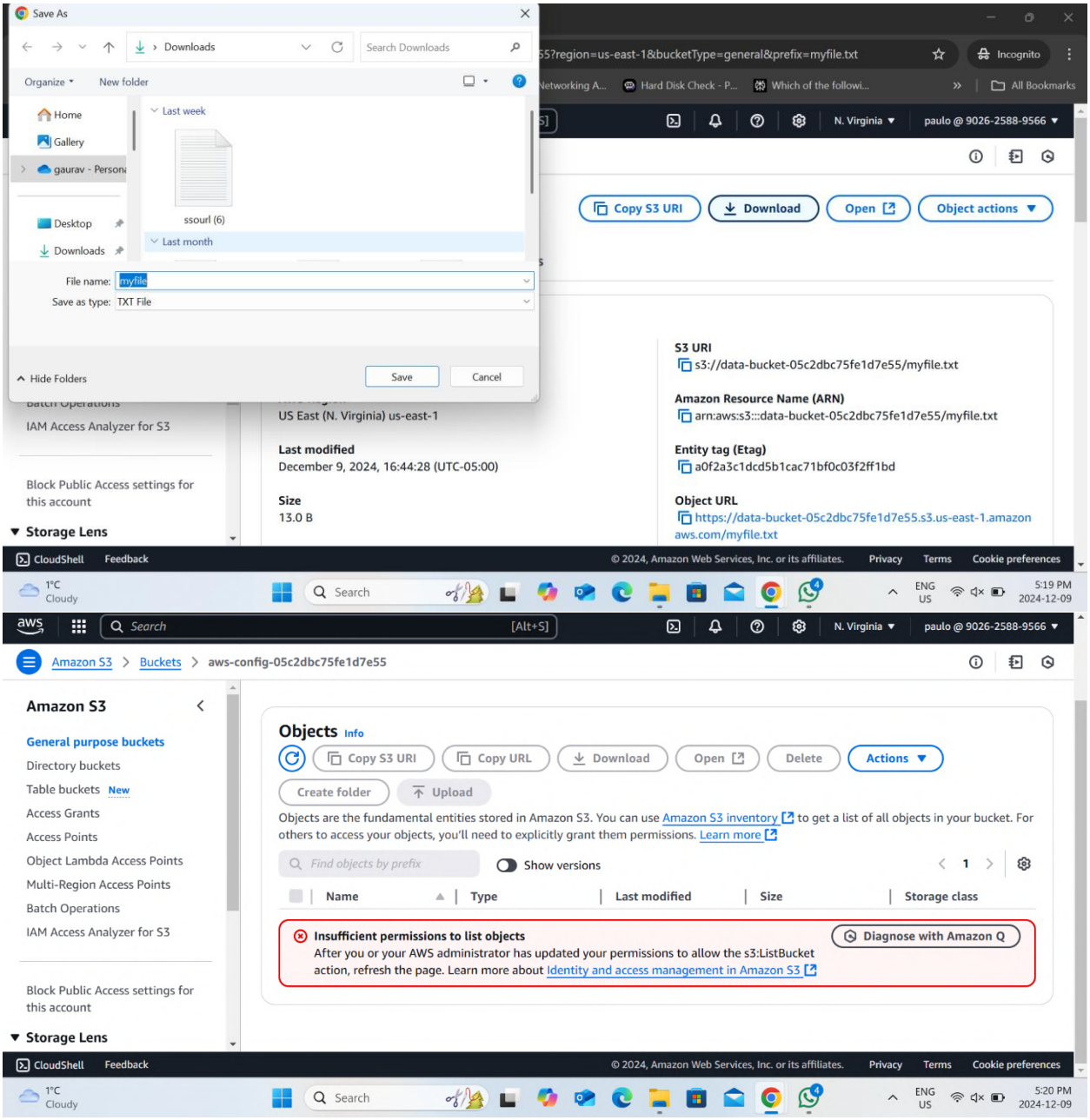
AWS-Cloud-Security-Project



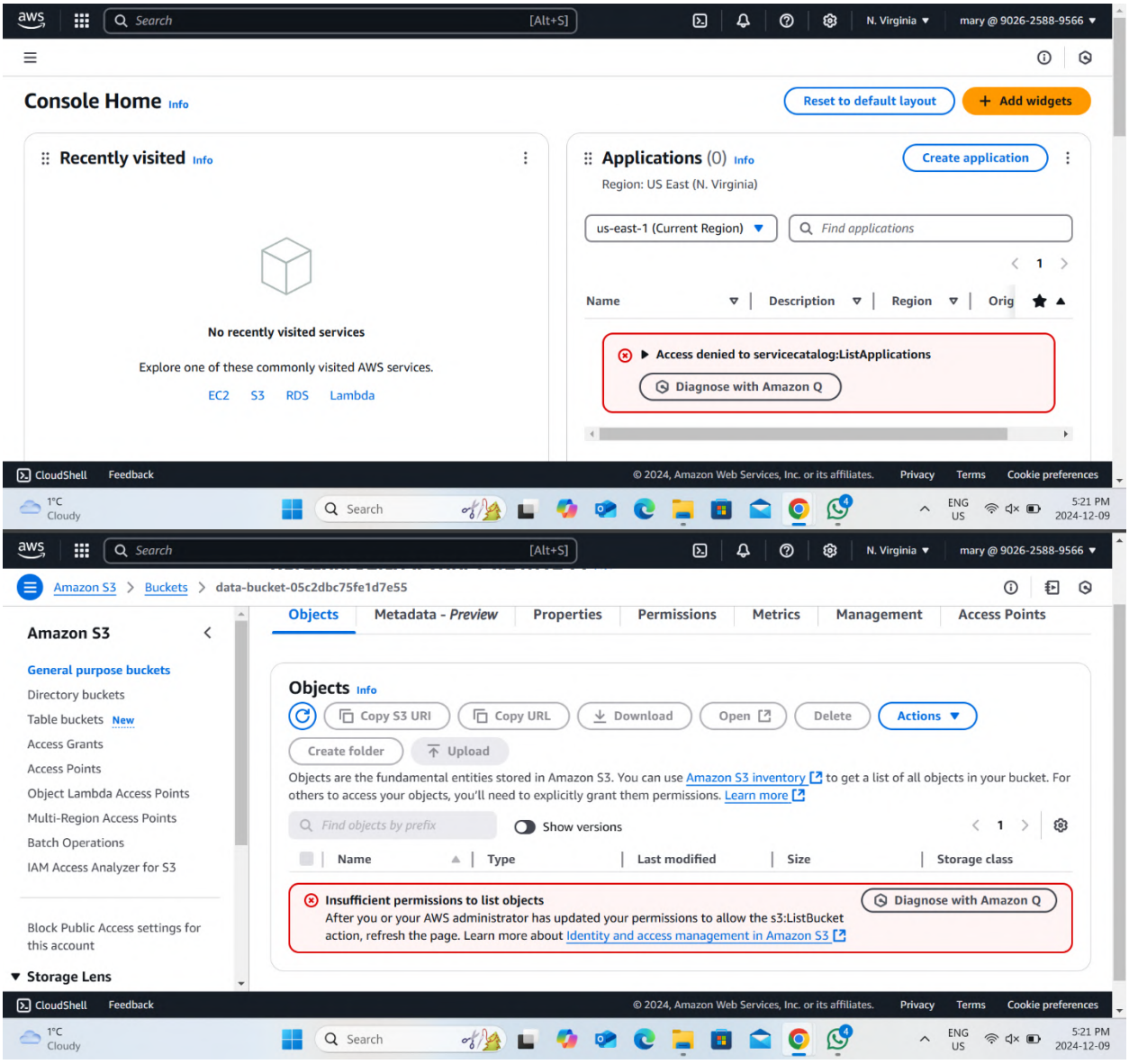
AWS-Cloud-Security-Project



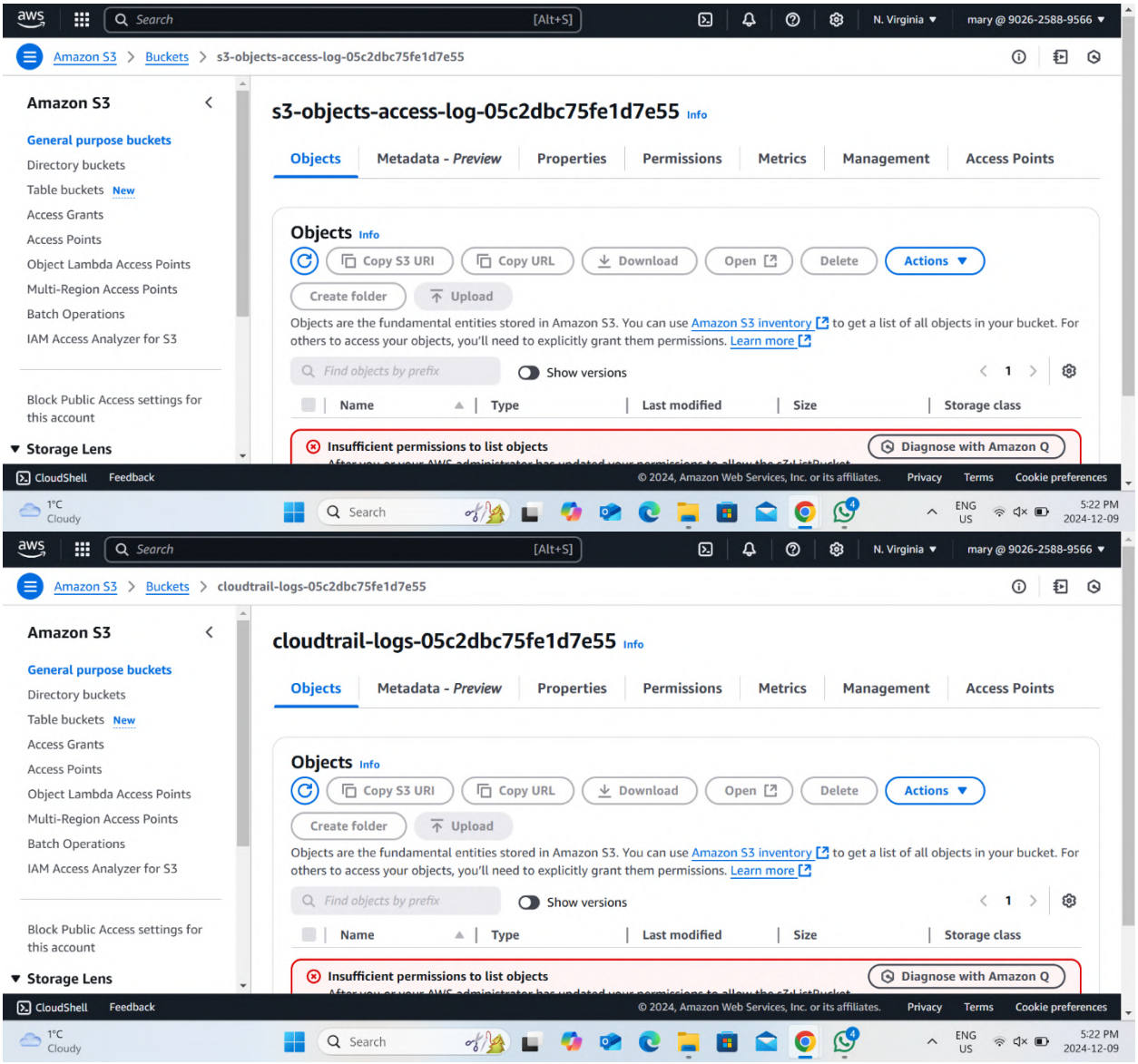
AWS-Cloud-Security-Project



AWS-Cloud-Security-Project

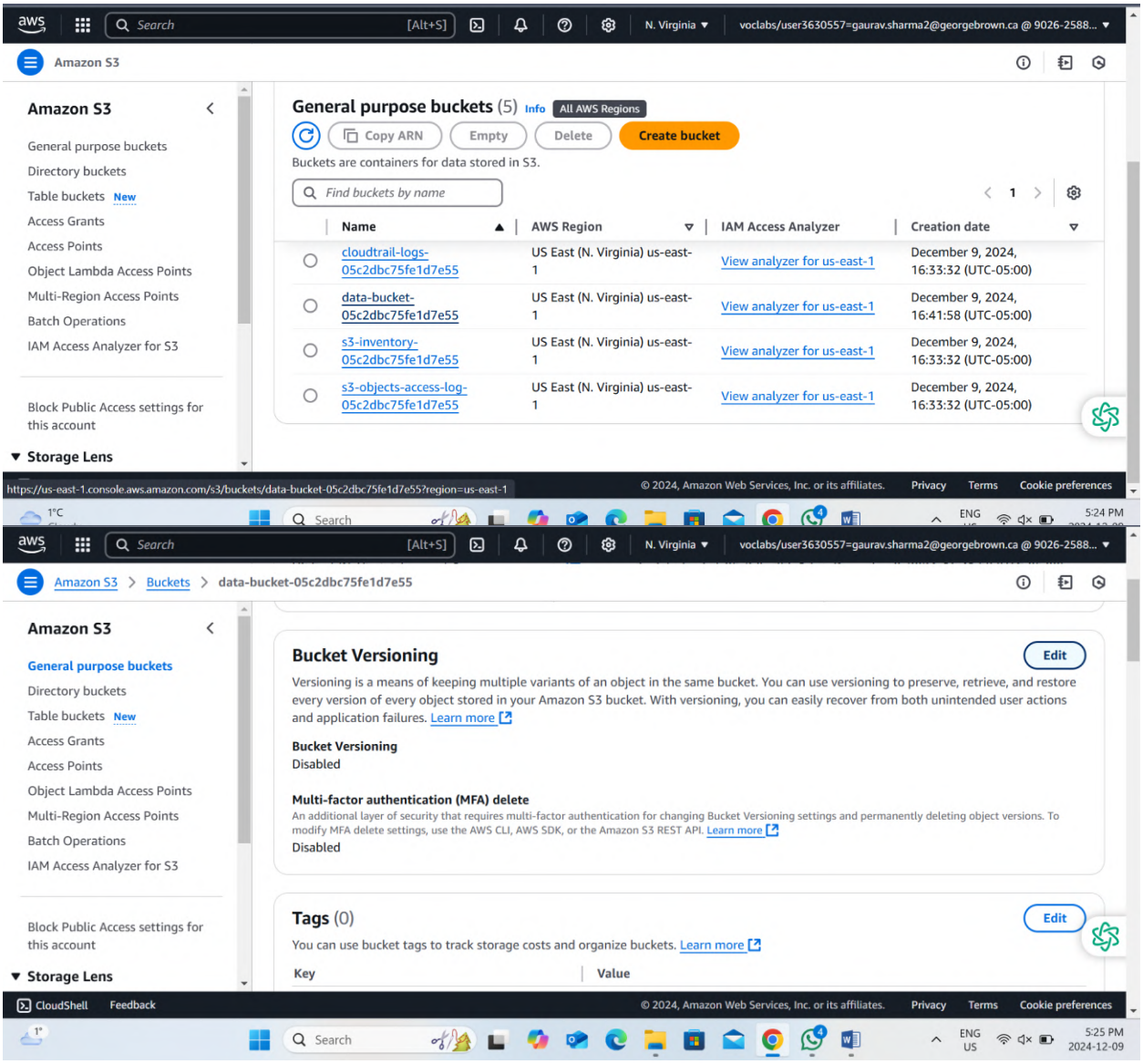


AWS-Cloud-Security-Project

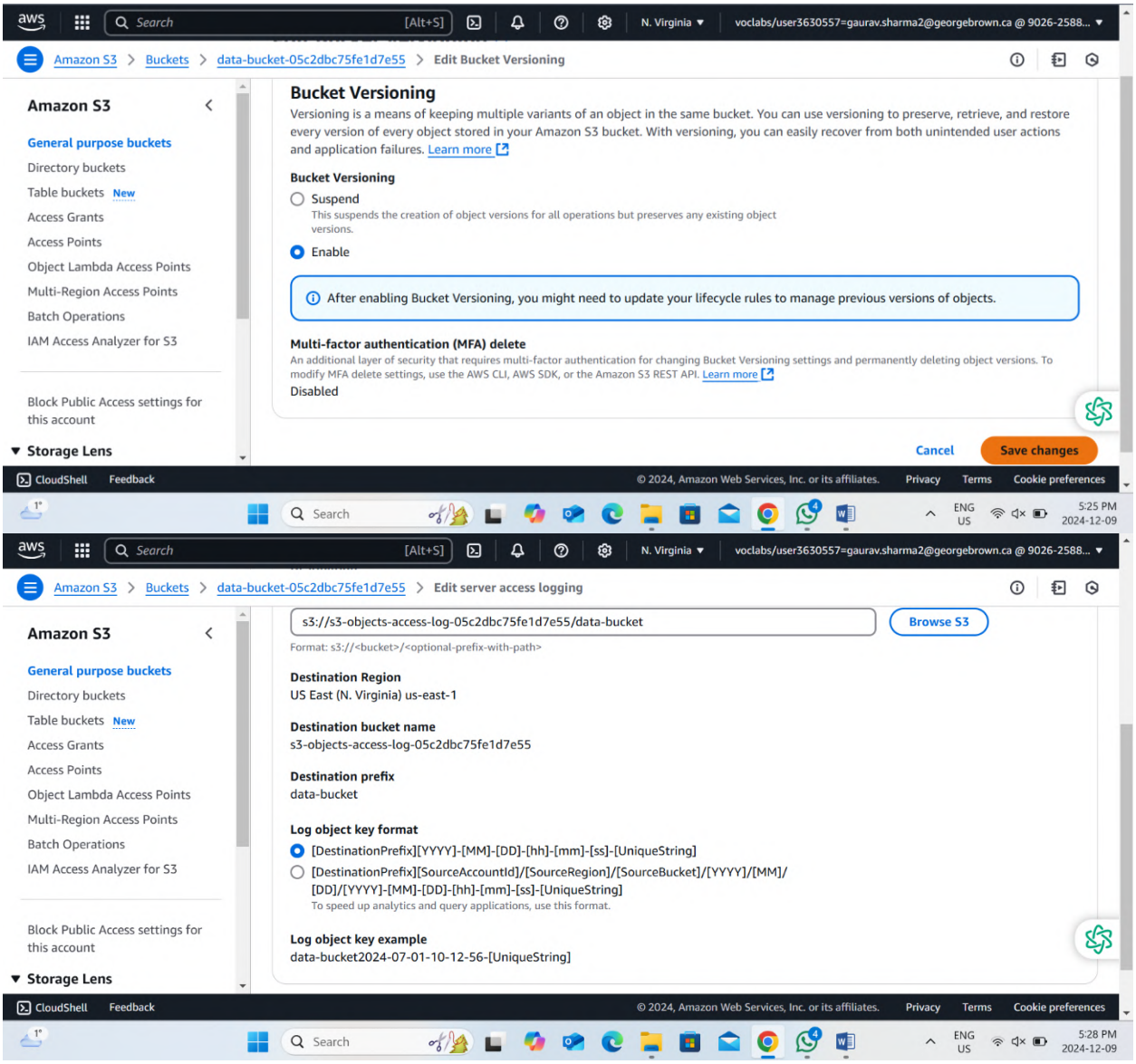


Task 1.2: Enable versioning and object-level logging on a bucket

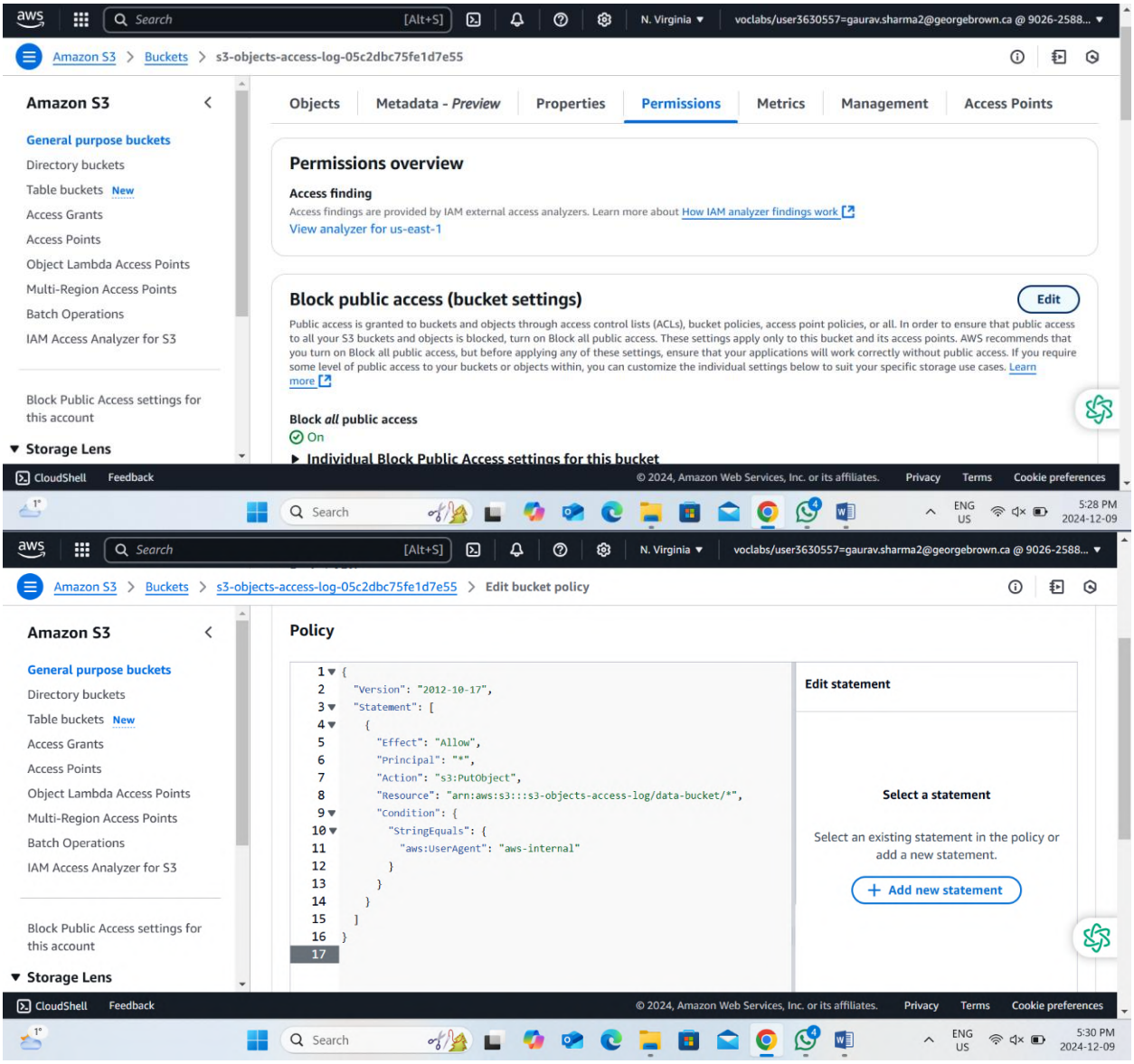
AWS-Cloud-Security-Project



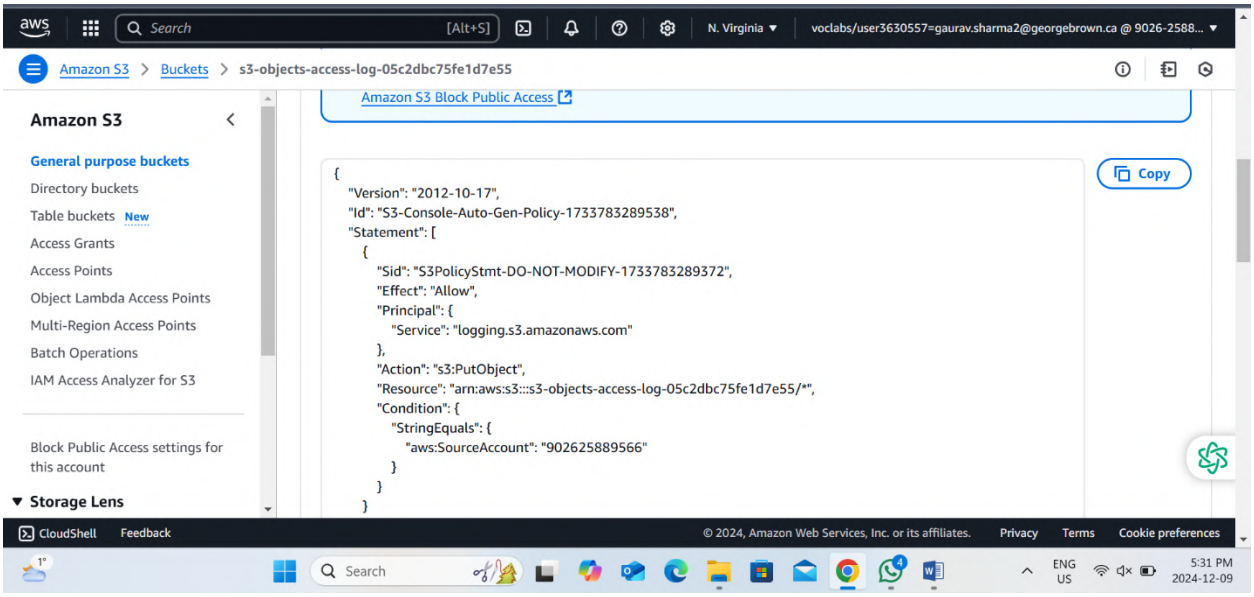
AWS-Cloud-Security-Project



AWS-Cloud-Security-Project

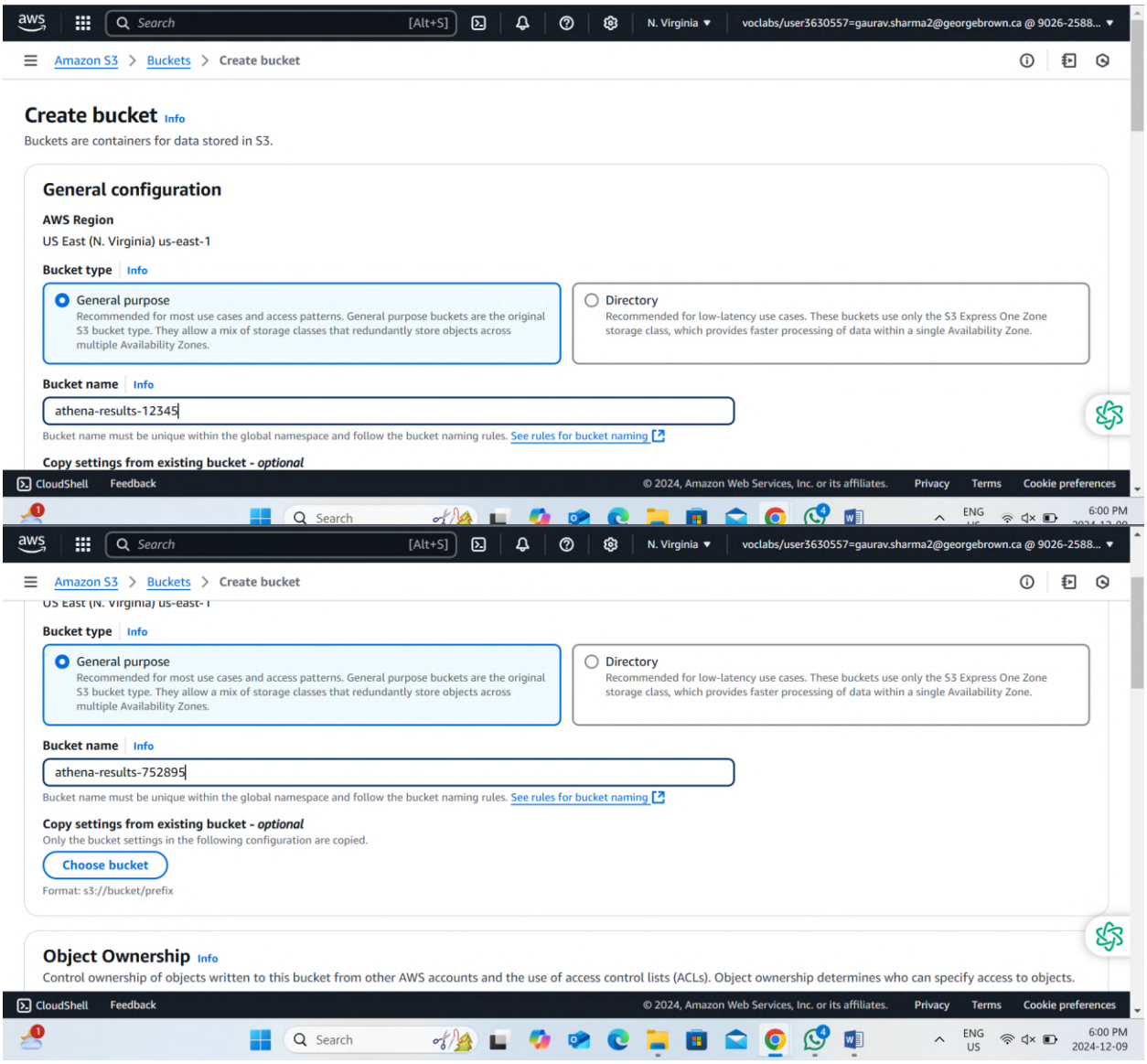


AWS-Cloud-Security-Project

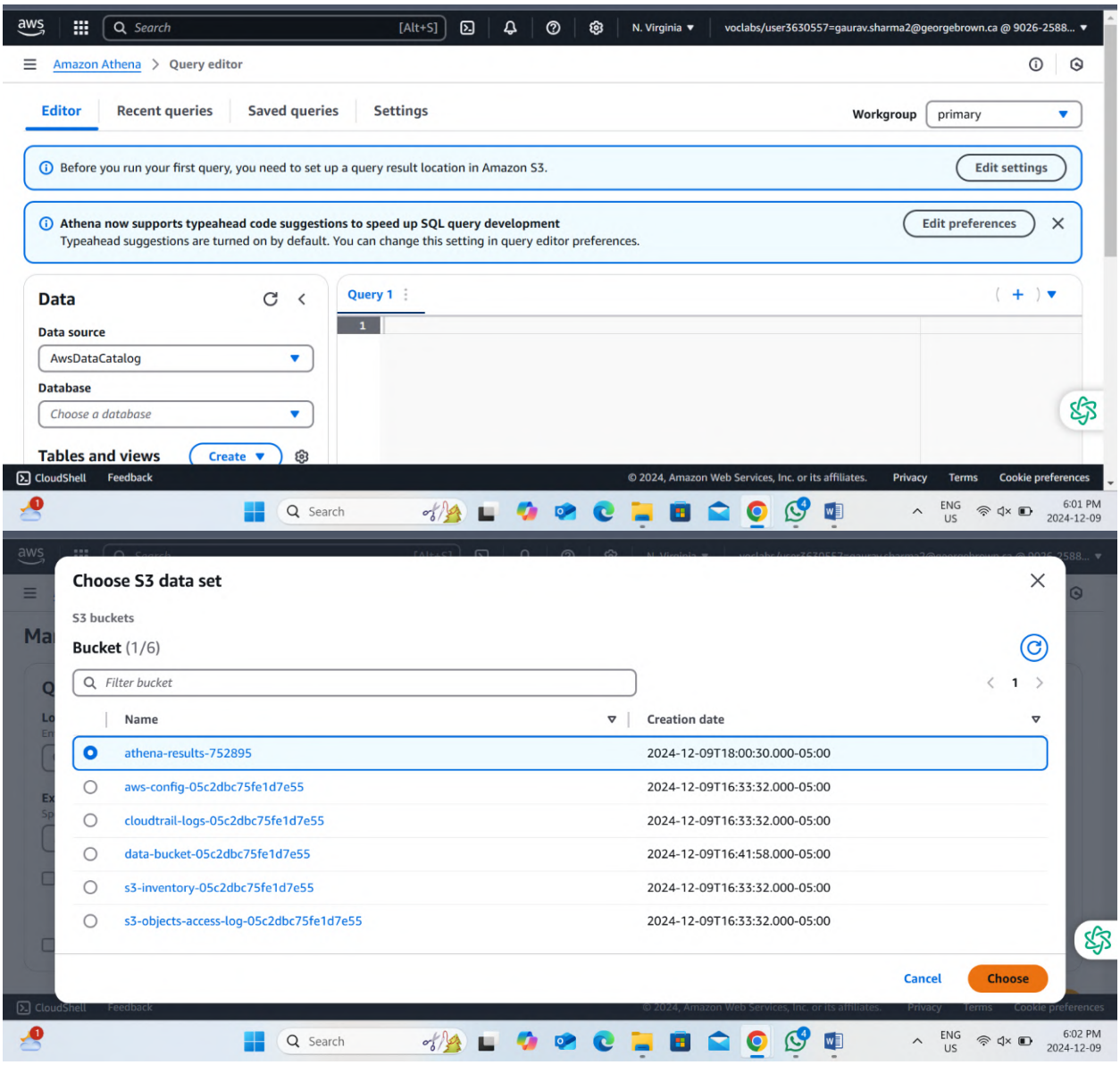


Task 1.3: Implement the S3 Inventory feature on a bucket

AWS-Cloud-Security-Project

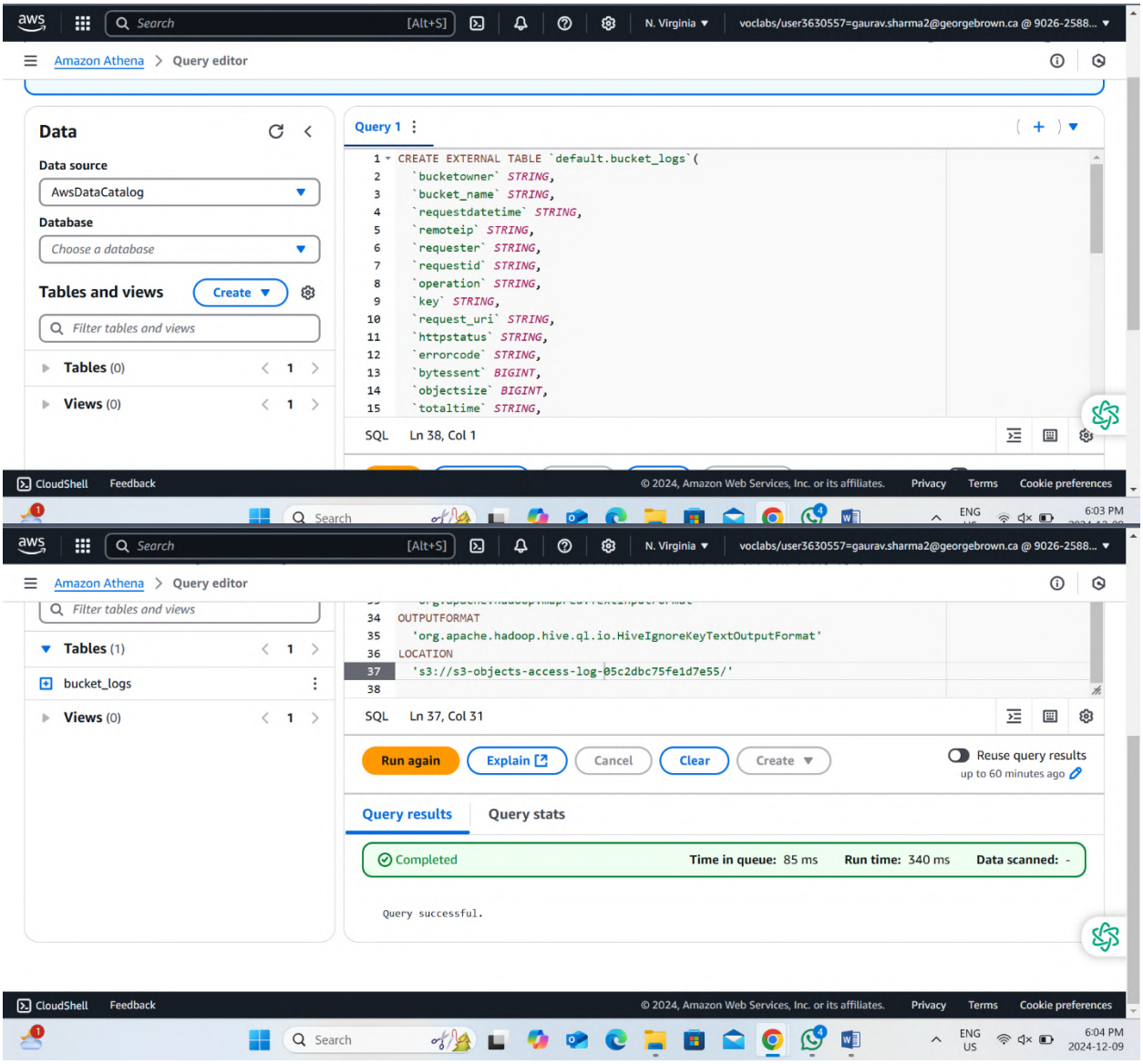


AWS-Cloud-Security-Project

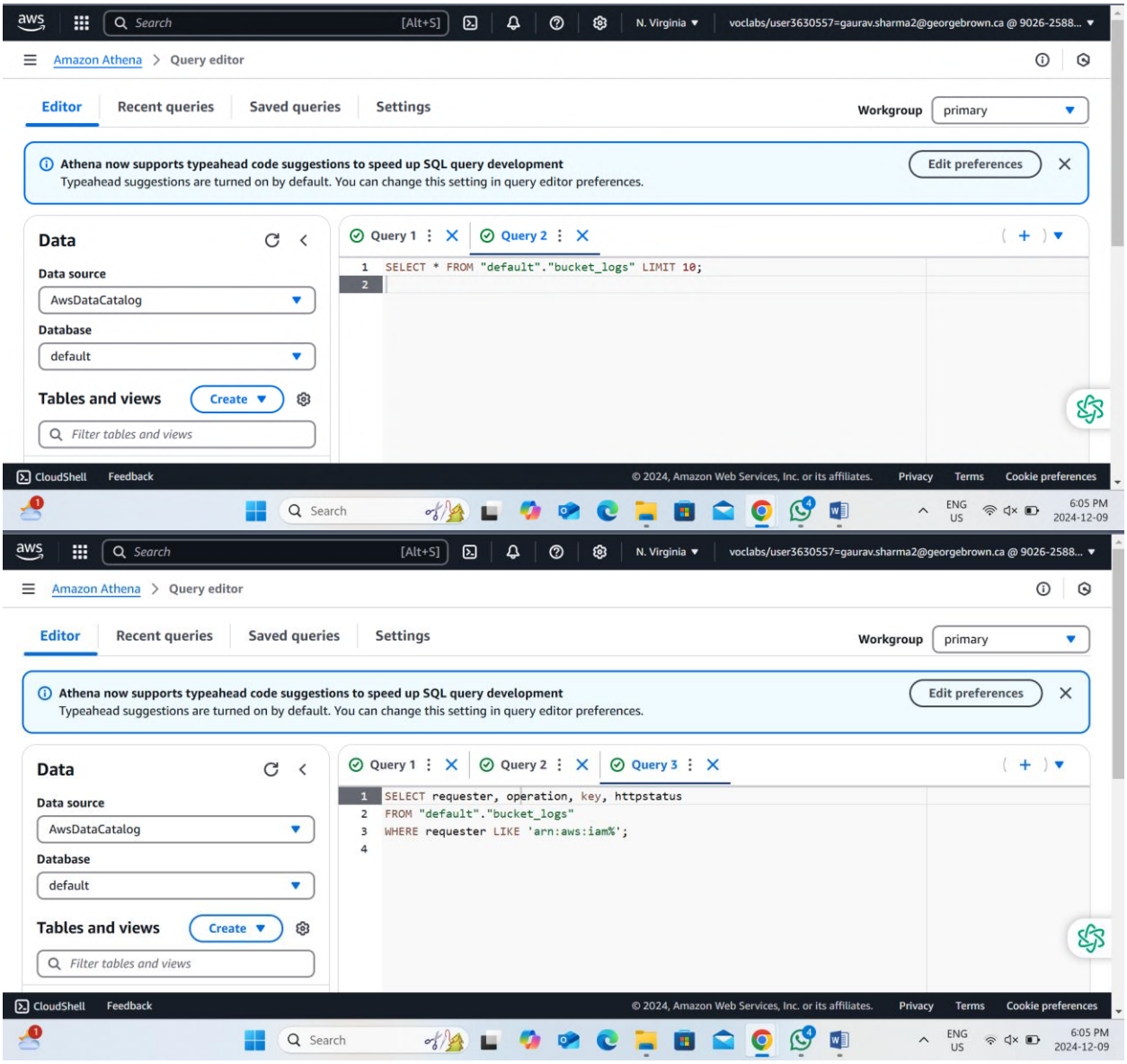


Task 1.4: Confirm that versioning works as intended

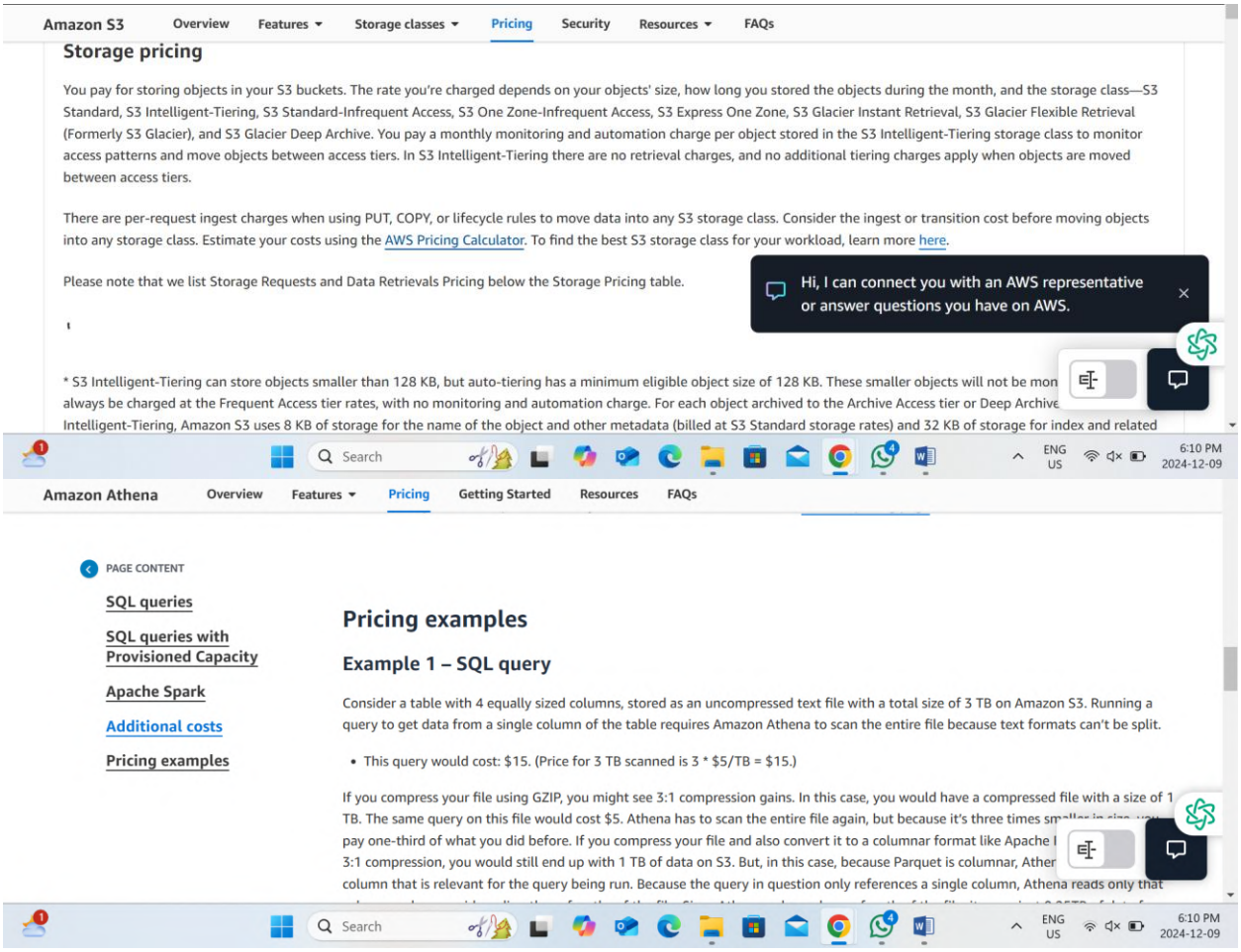
AWS-Cloud-Security-Project



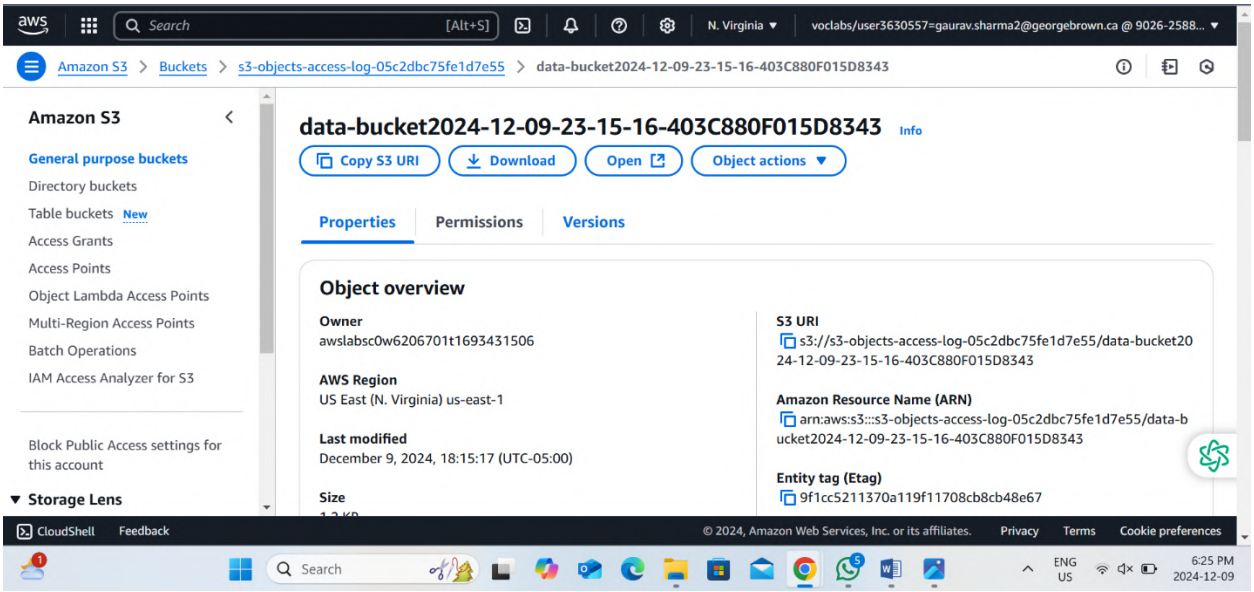
AWS-Cloud-Security-Project



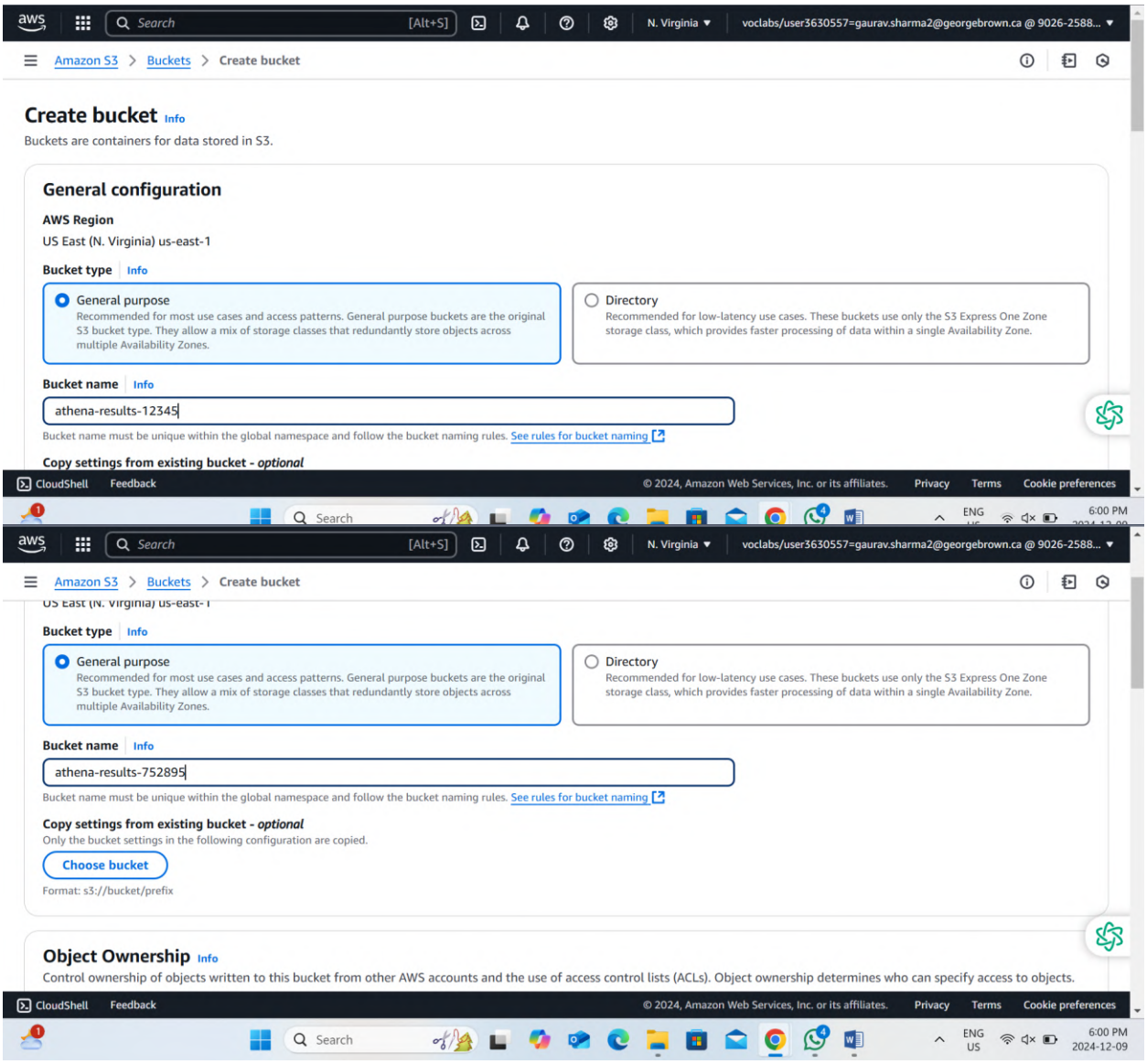
AWS-Cloud-Security-Project



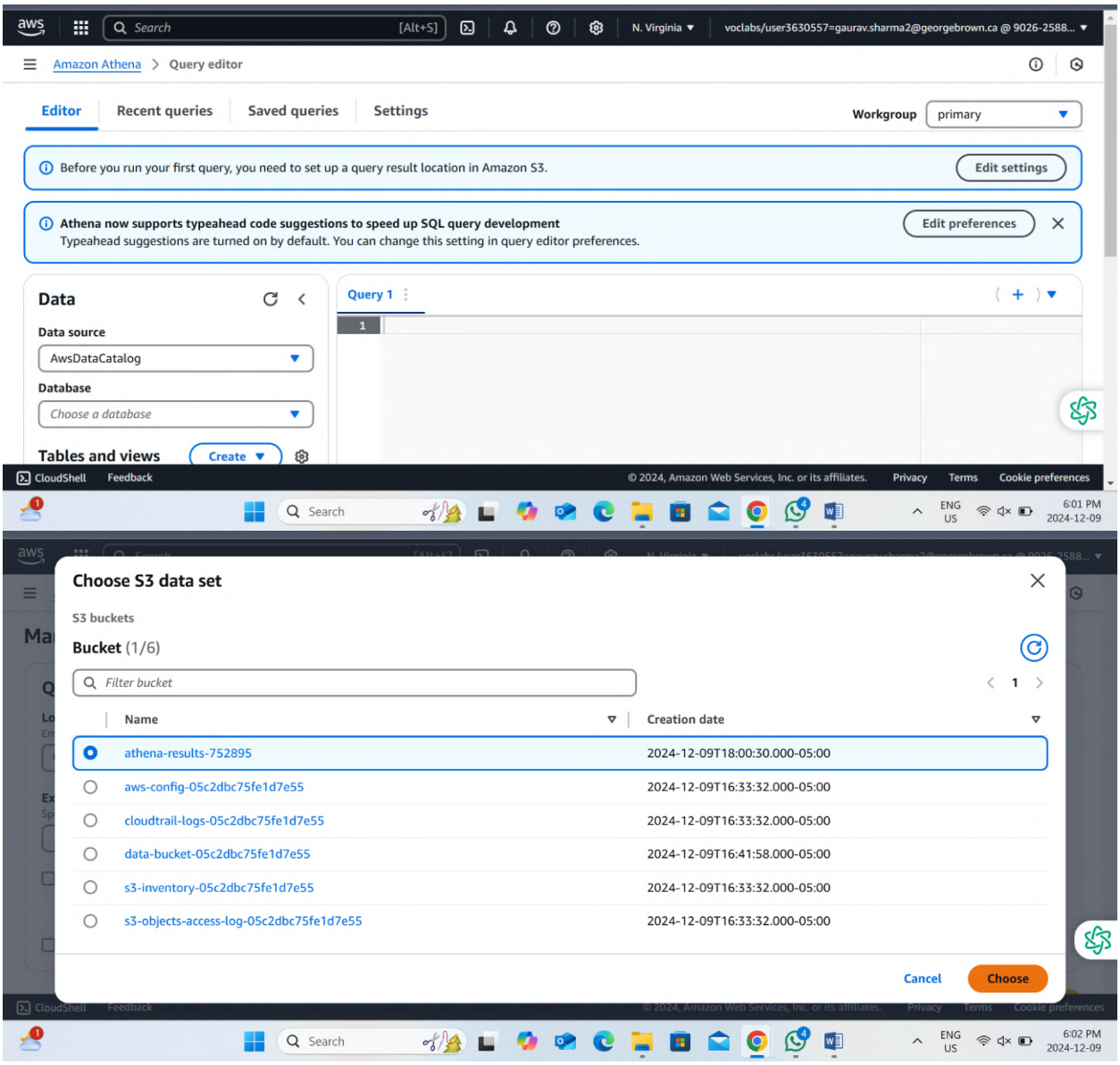
Task 1.5: Confirm object-level logging and query the access logs by using Athena



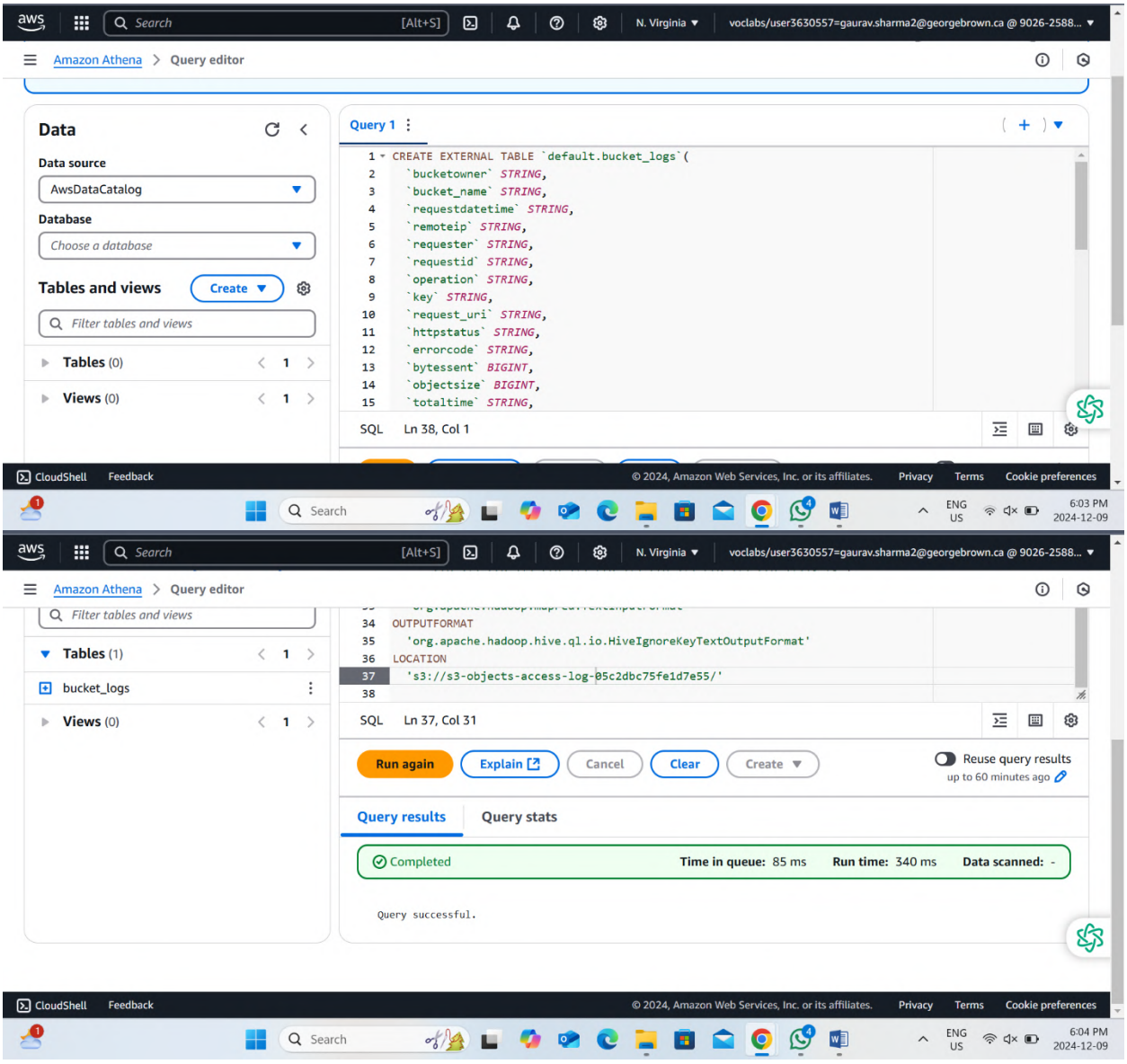
AWS-Cloud-Security-Project



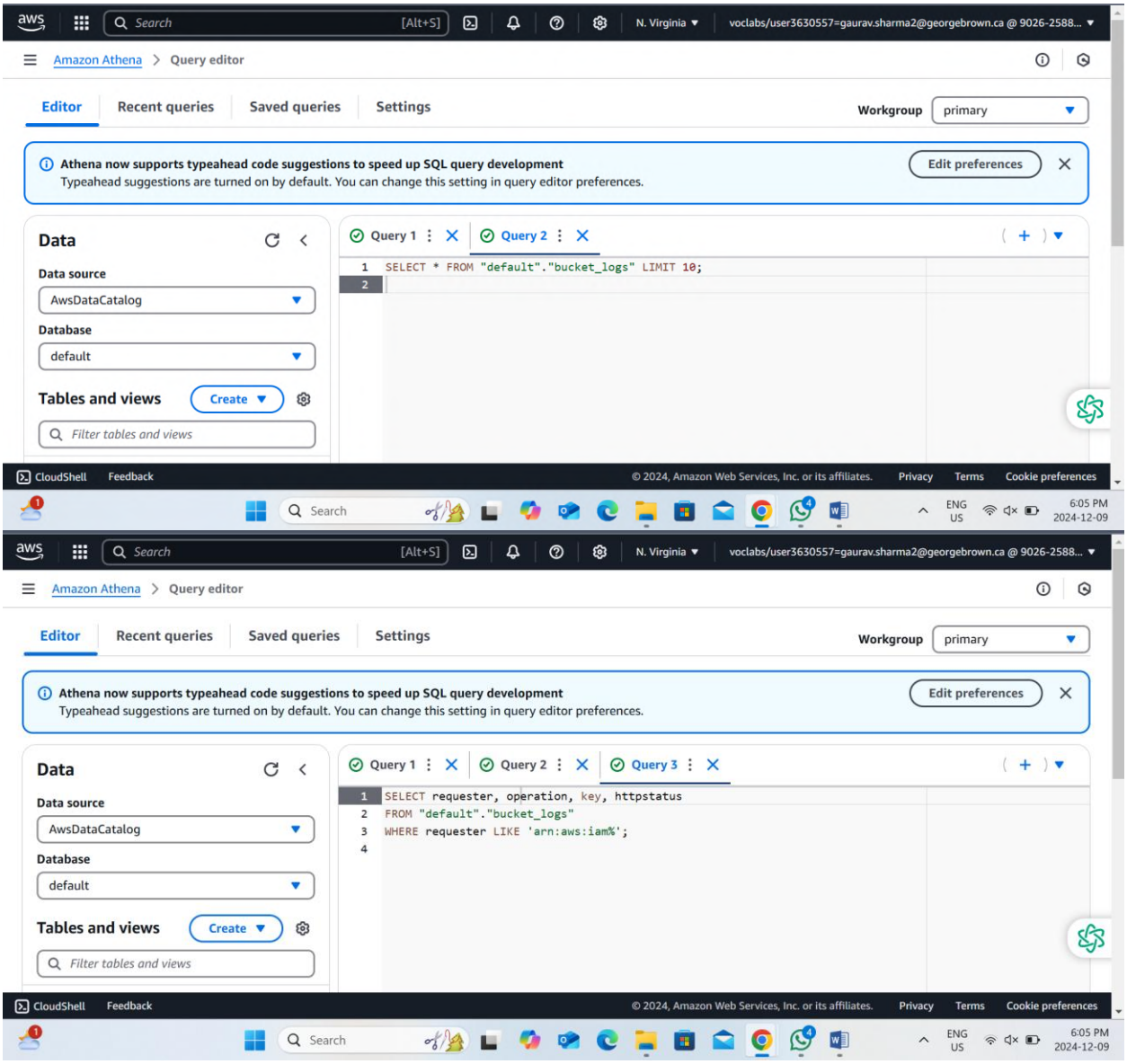
AWS-Cloud-Security-Project



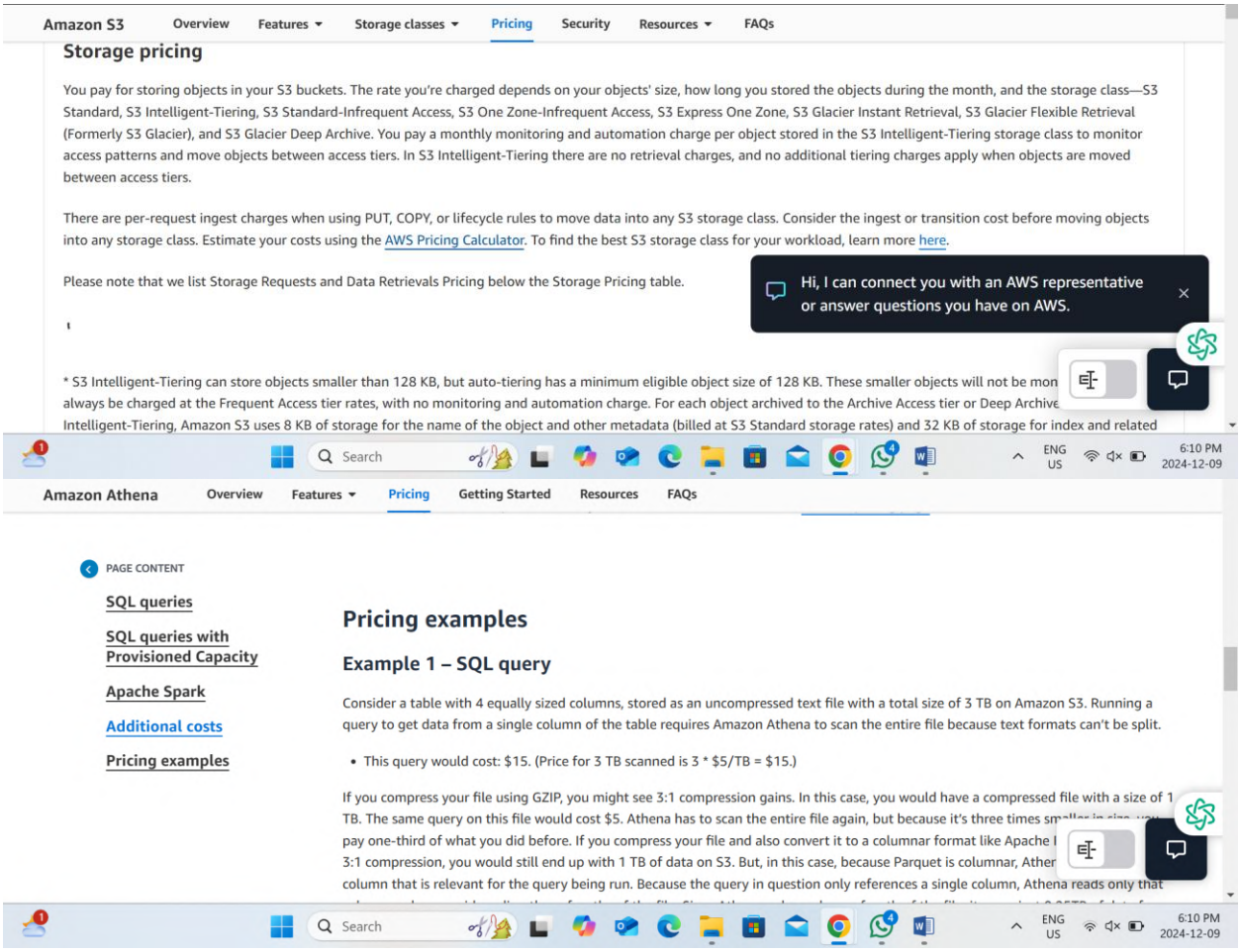
AWS-Cloud-Security-Project



AWS-Cloud-Security-Project



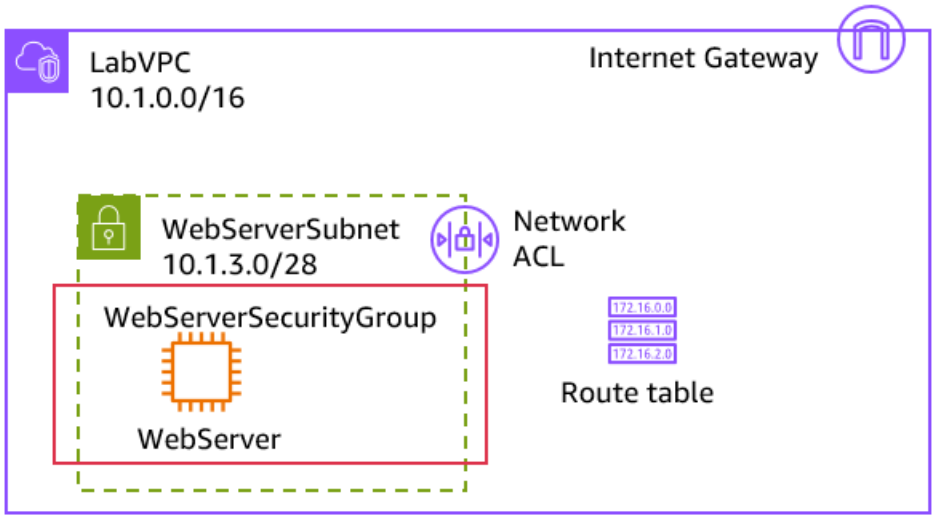
AWS-Cloud-Security-Project



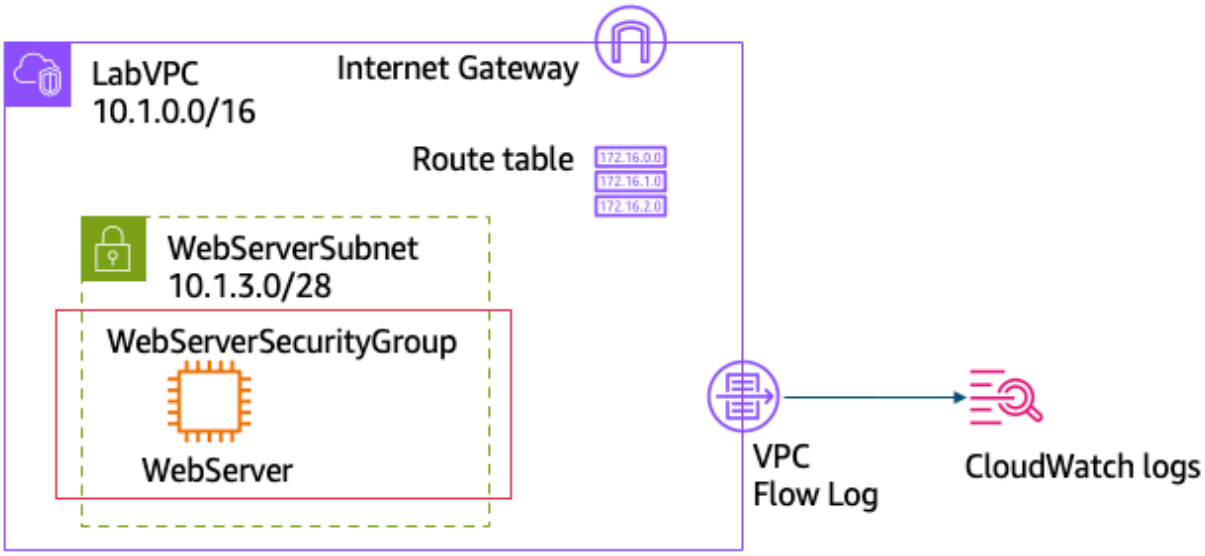
Phase 2: Securing VPCs

AWS-Cloud-Security-Project

Task 2.1: Review LabVPC and its associated resources

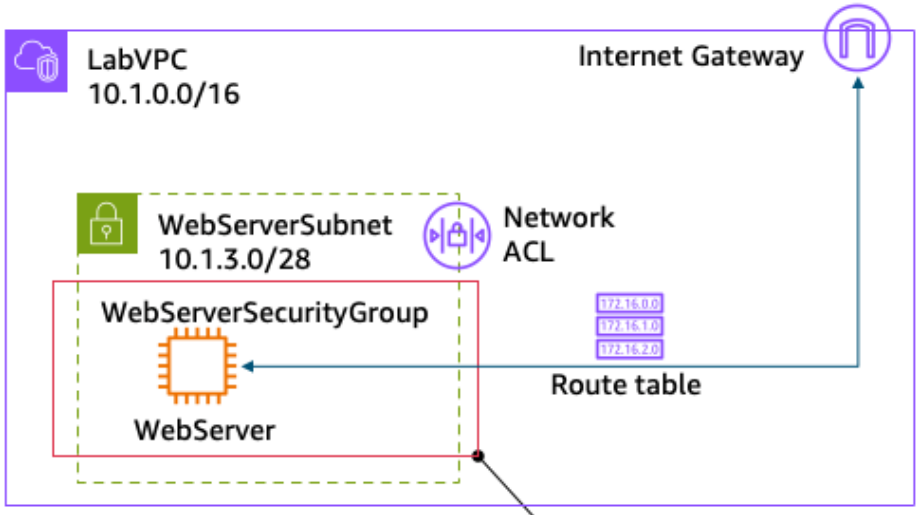


Task 2.2: Create a VPC flow log



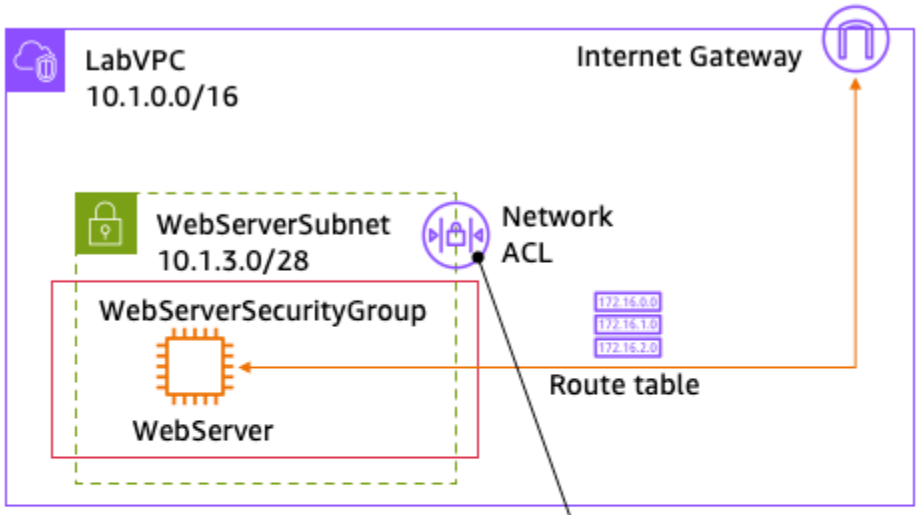
Task 2.3: Access the WebServer instance from the internet and review VPC flow logs in CloudWatch

Task 2.4: Configure route table and security group settings



Security Group (inbound)	
Type	**Source**
SSH (22)	18.206.107.24/29
HTTP (80)	0.0.0.0/0

Task 2.5: Secure the WebServerSubnet with a network ACL



NACL		
Rule number	**Type**	**Allow/Deny**
100	SSH (22)	Allow
90	HTTP (80)	Allow

AWS-Cloud-Security-Project

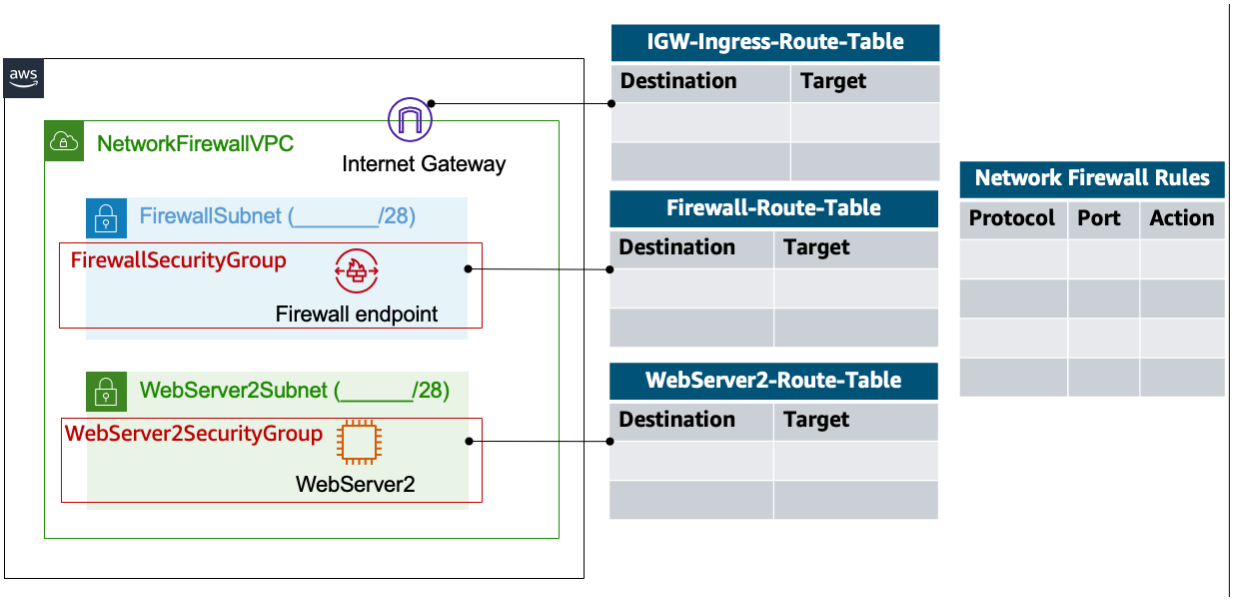
Task 2.6: Review NetworkFirewallVPC and its associated resources

Task 2.7: Create a network firewall

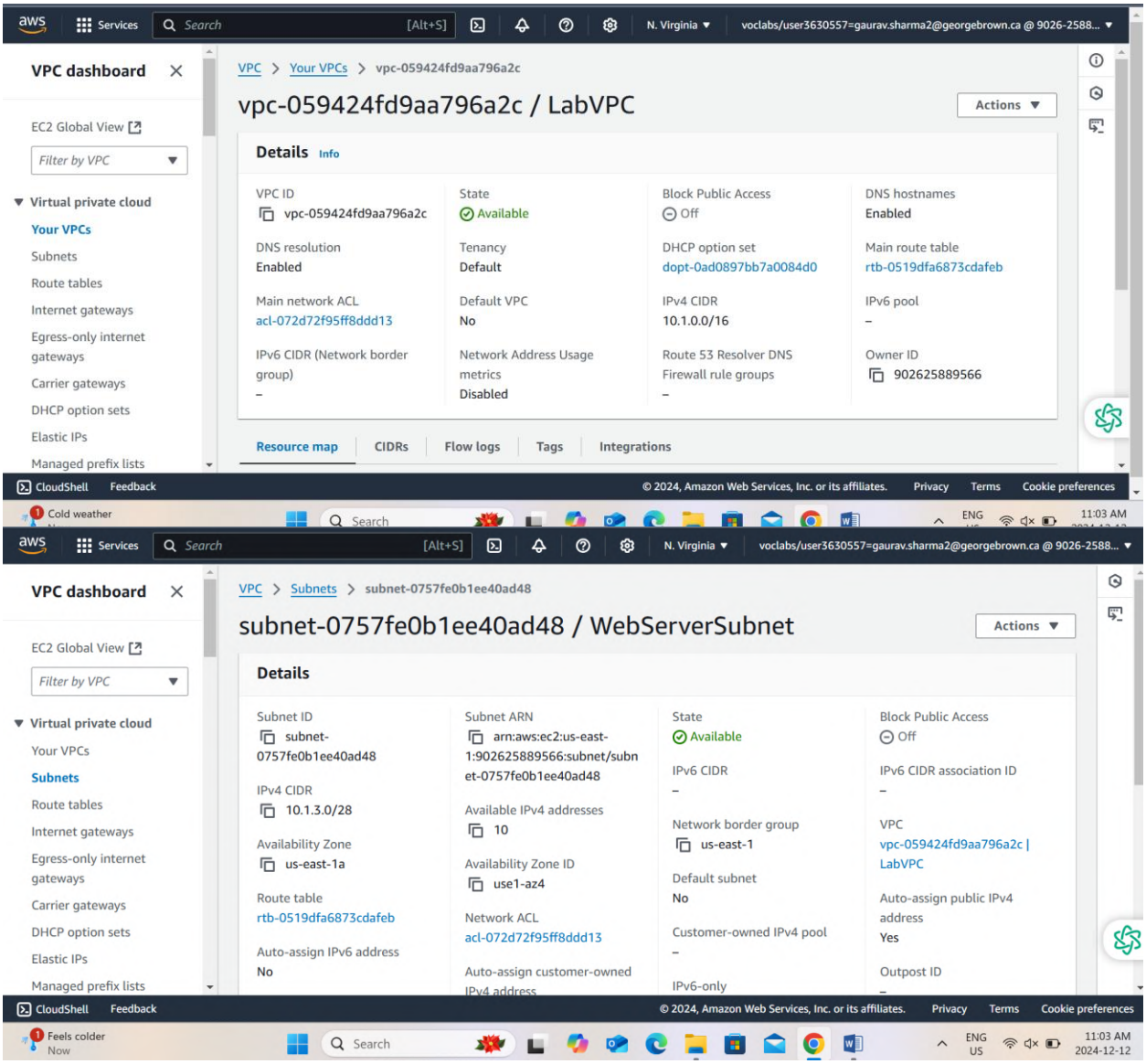
Task 2.8: Create route tables

Task 2.9: Configure logging for the network firewall

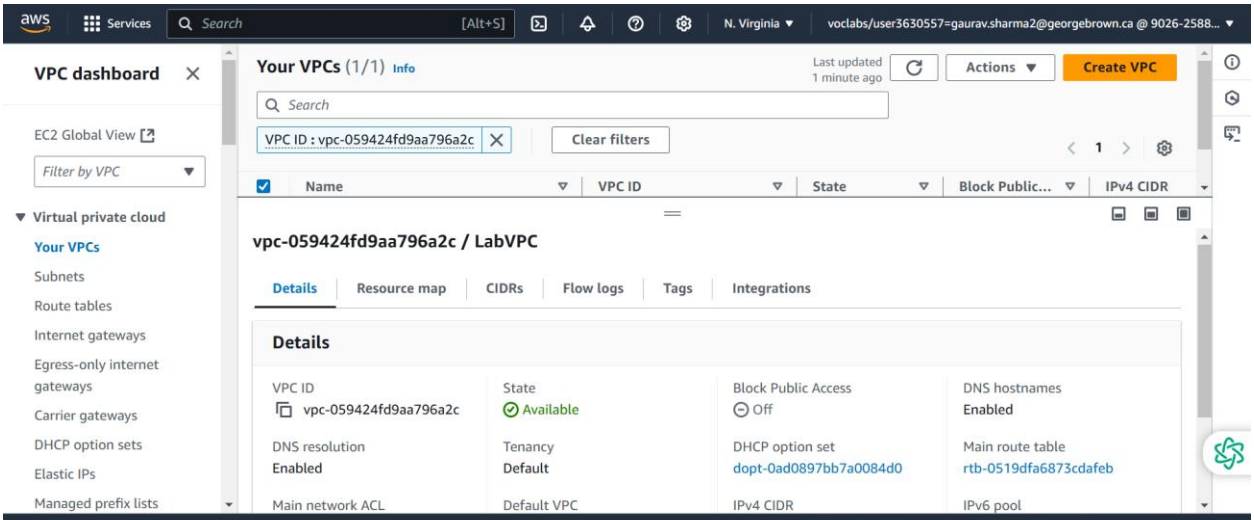
Task 2.10: Configure the firewall policy and test access

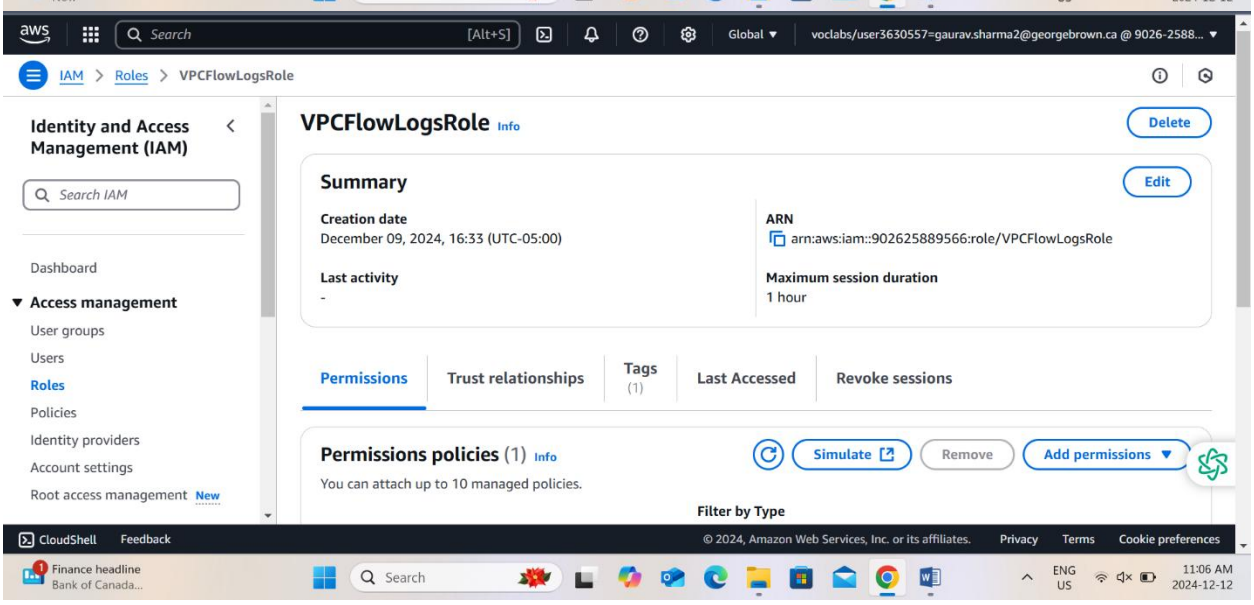


AWS-Cloud-Security-Project

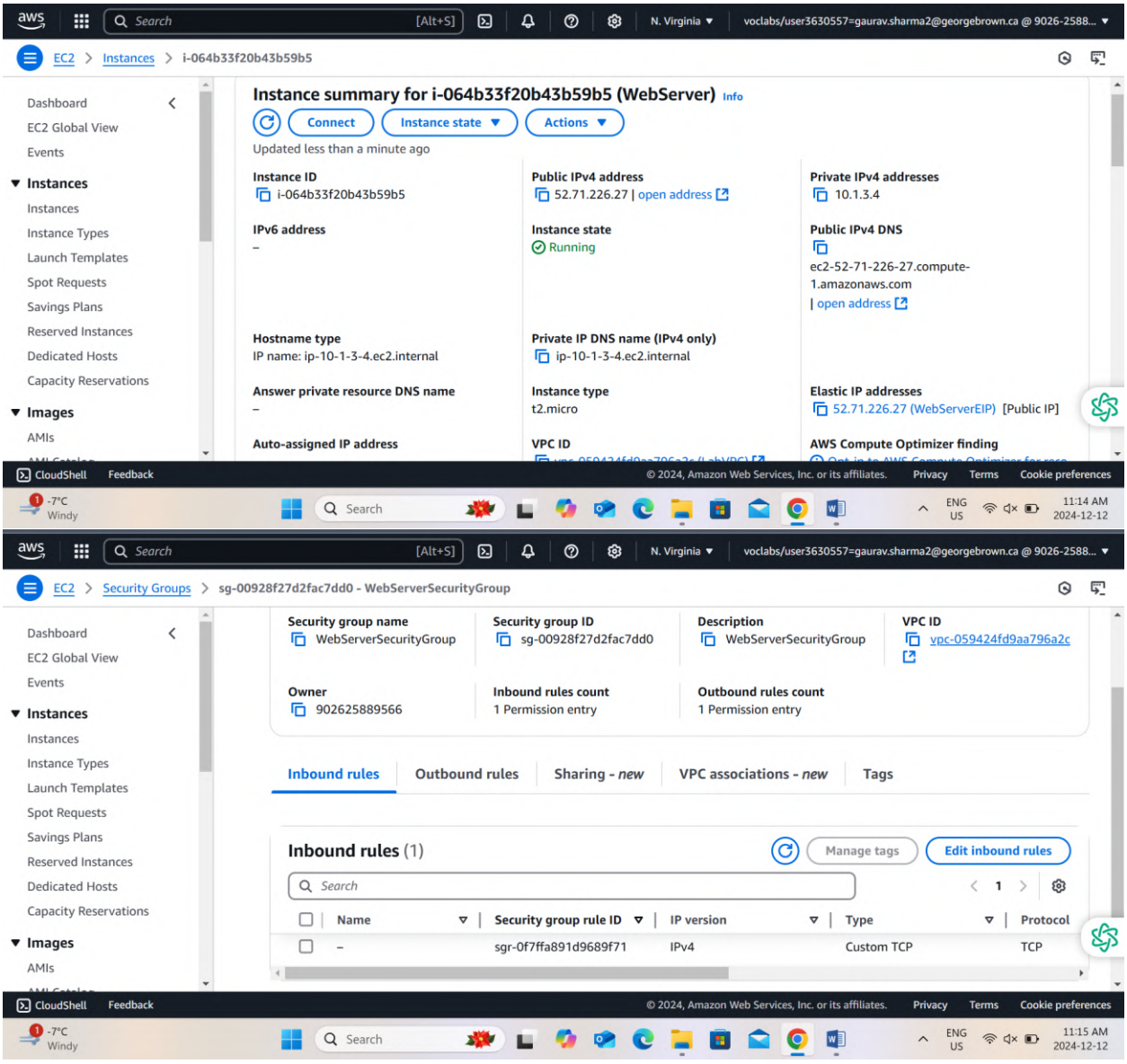


AWS-Cloud-Security-Project

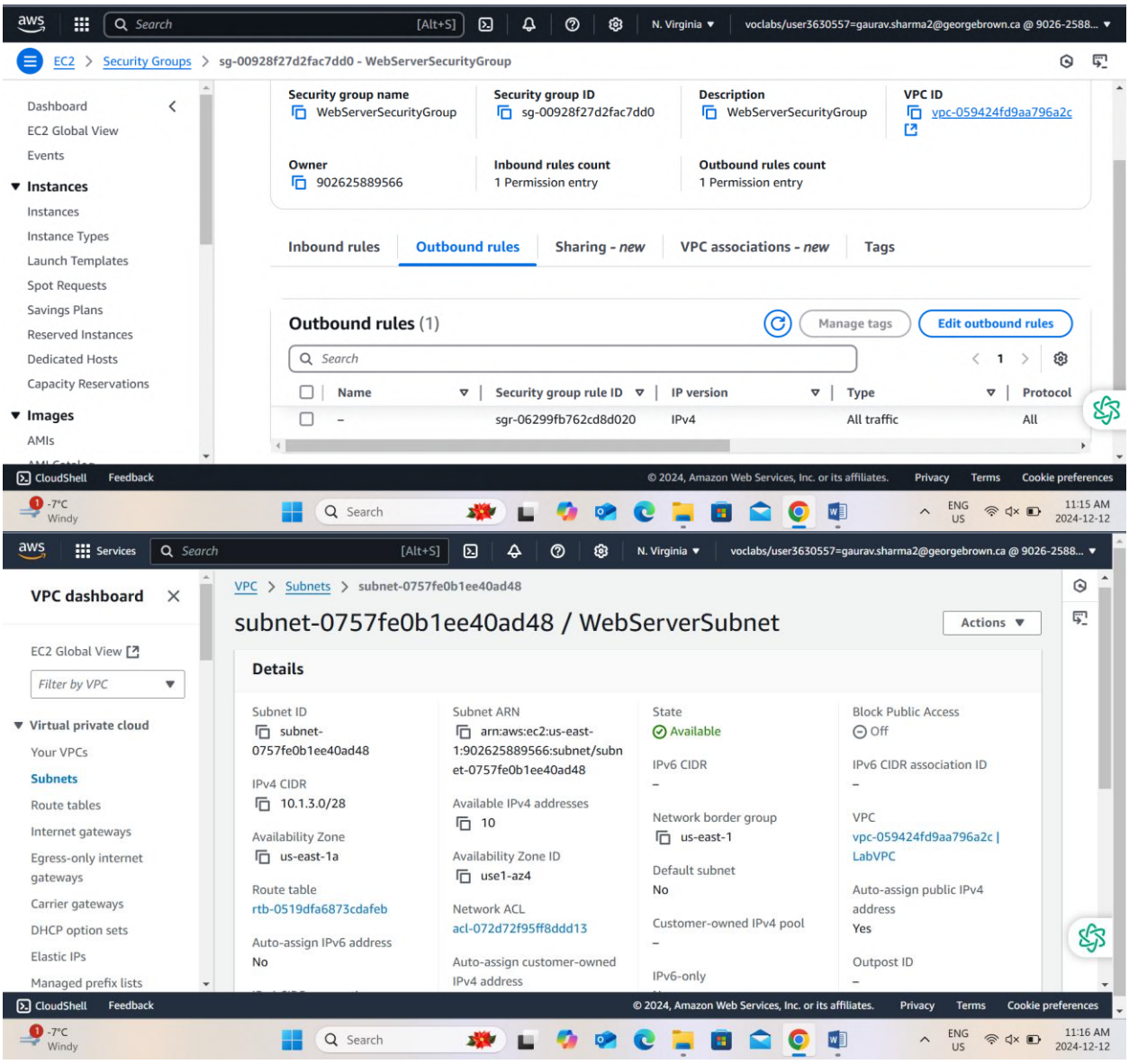




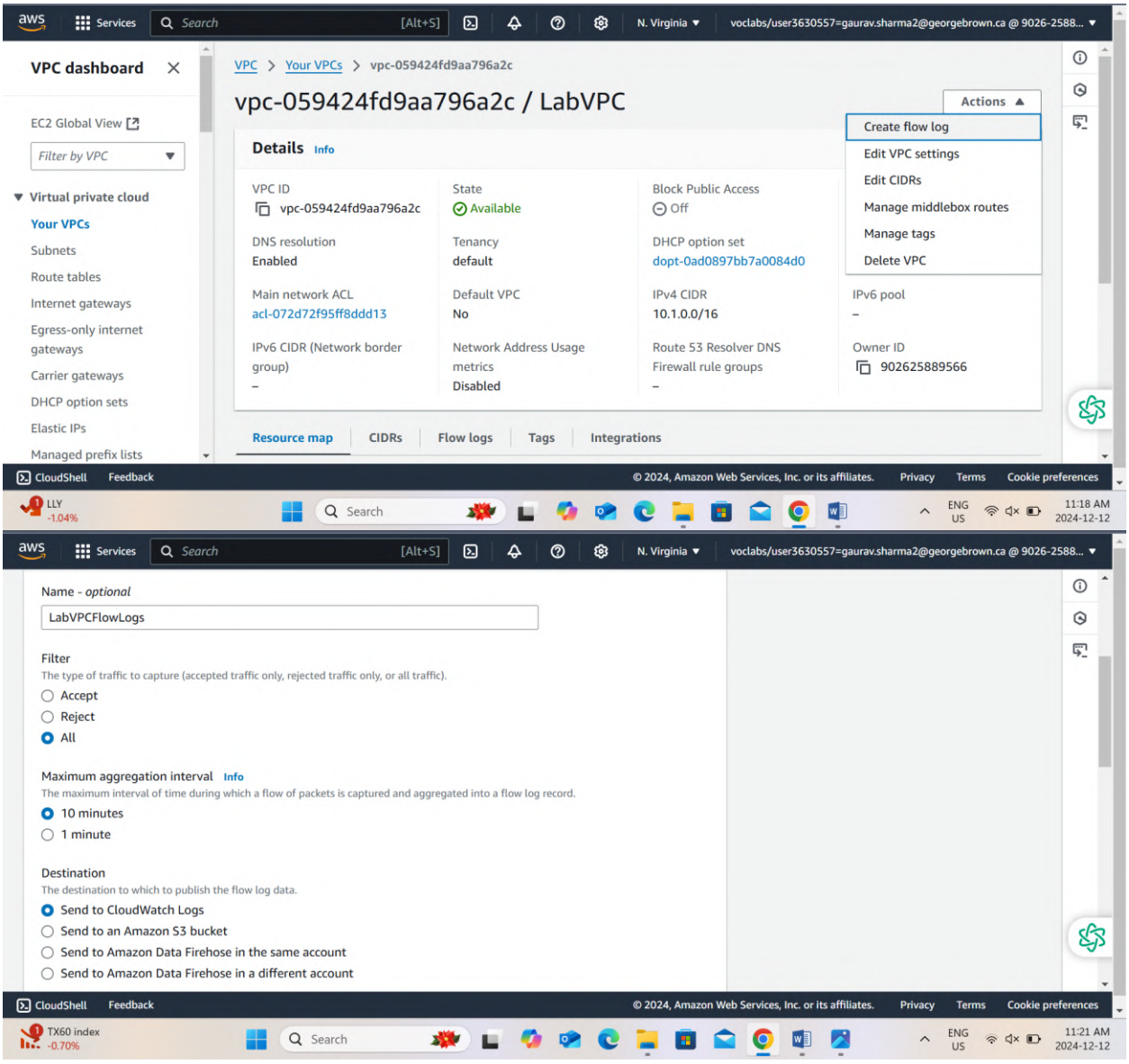
AWS-Cloud-Security-Project



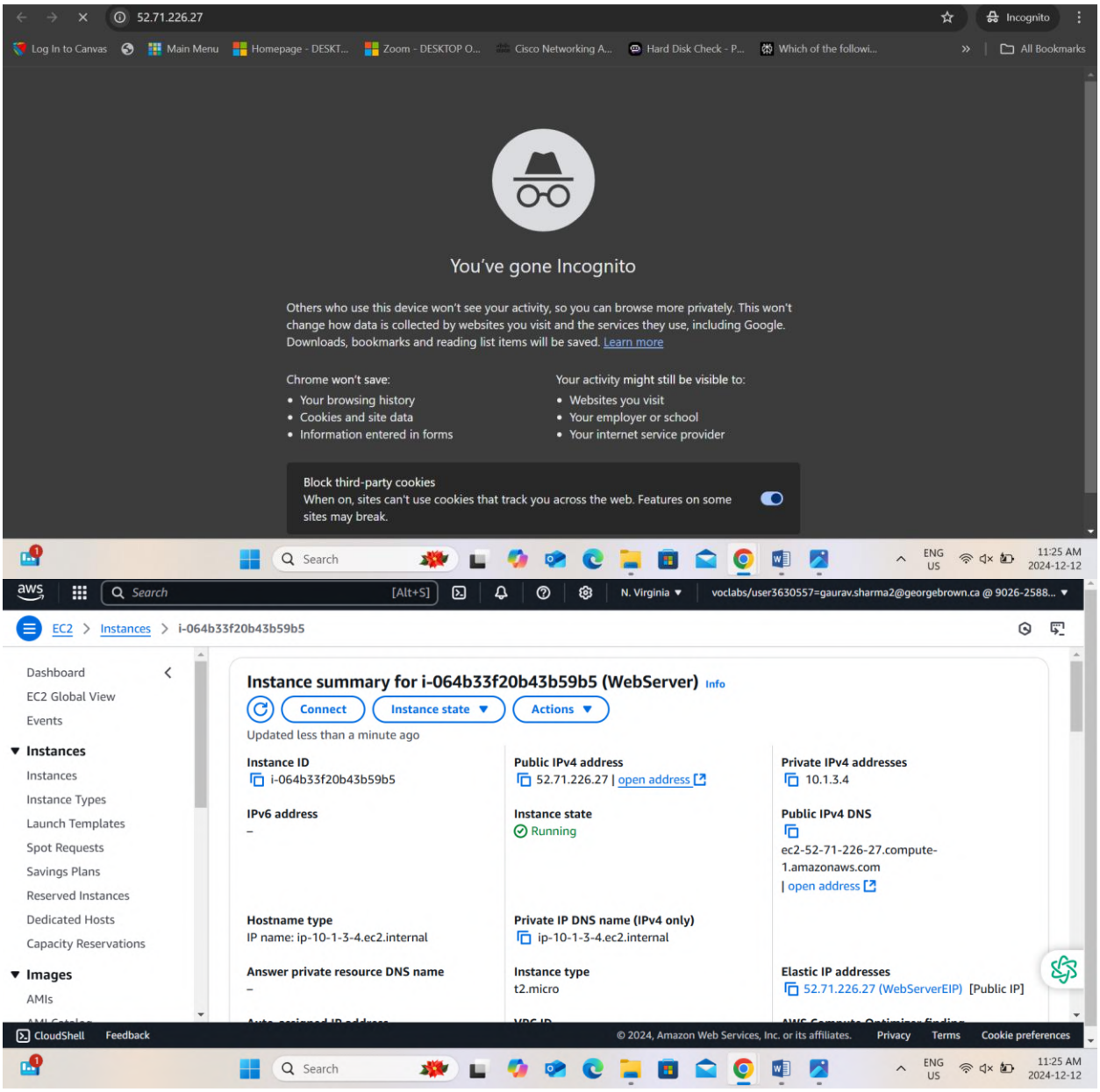
AWS-Cloud-Security-Project



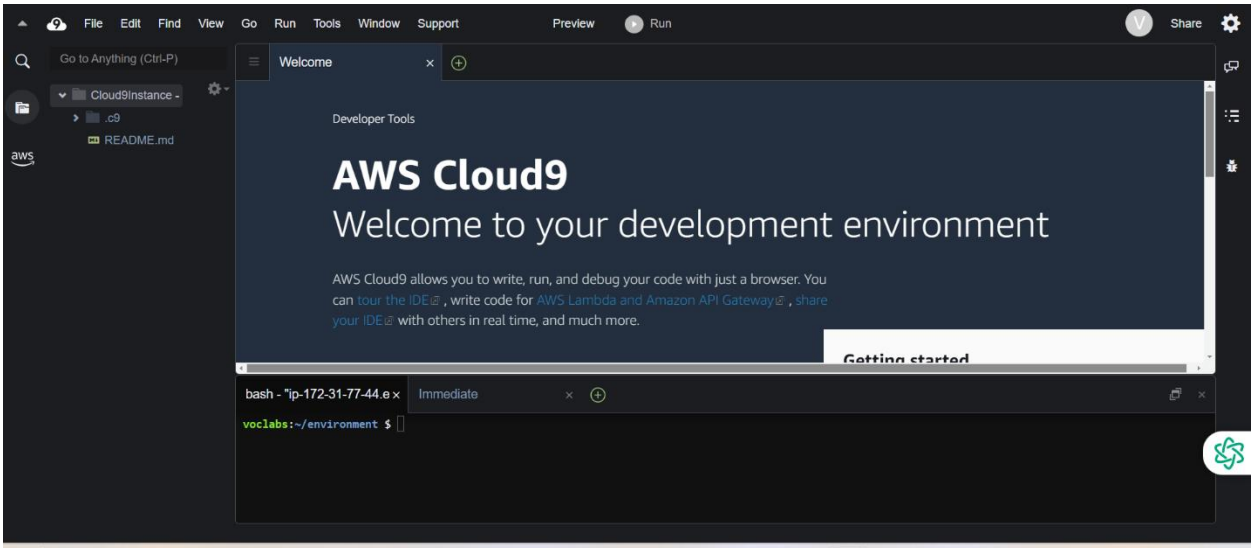
AWS-Cloud-Security-Project

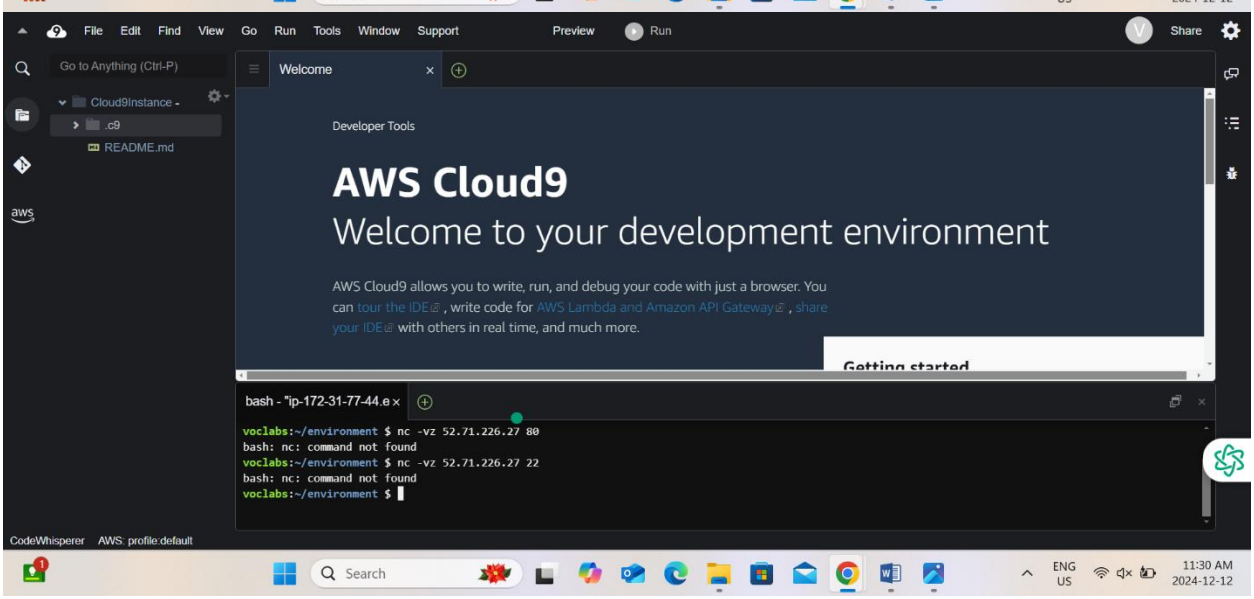


AWS-Cloud-Security-Project

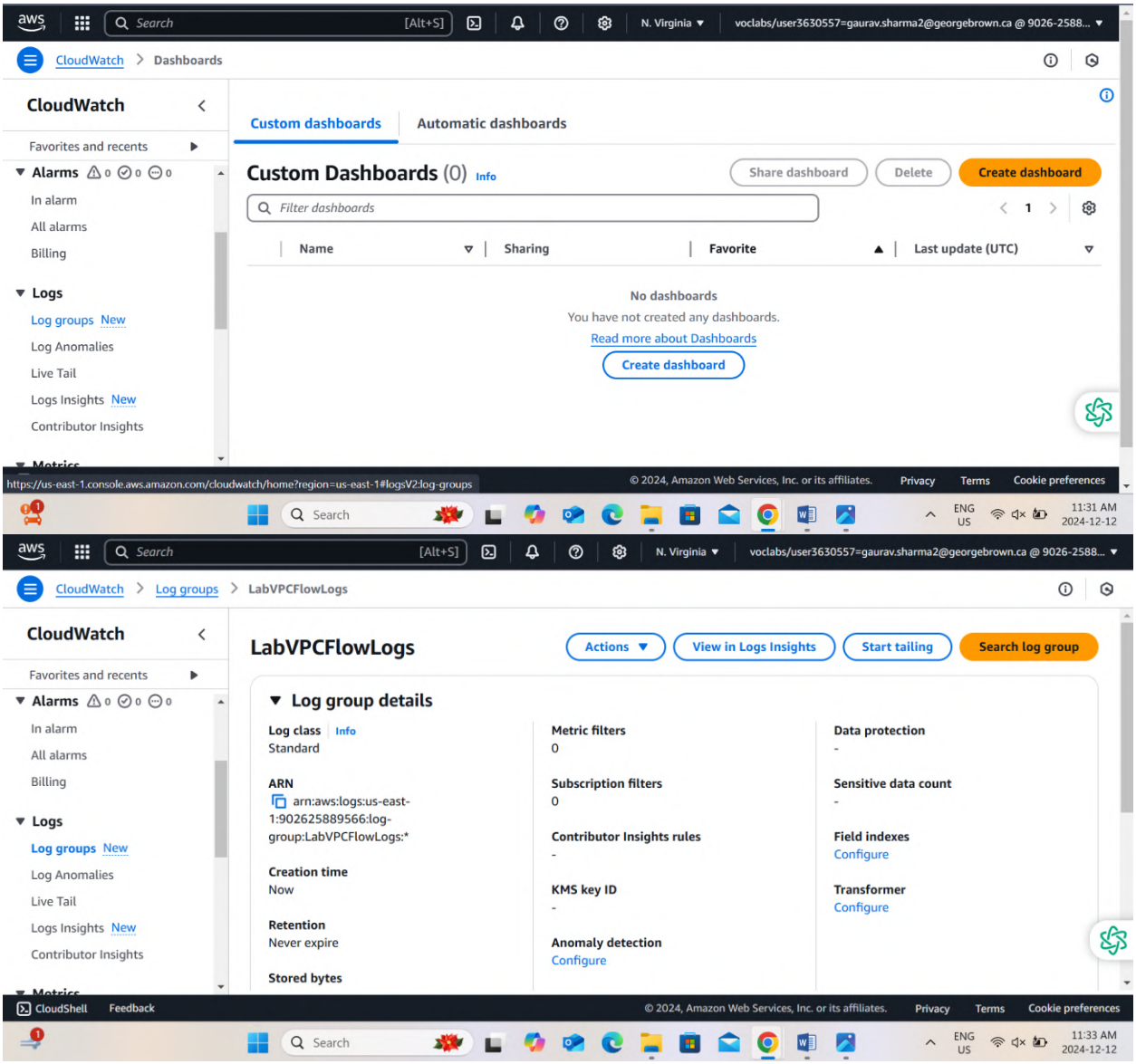


AWS-Cloud-Security-Project

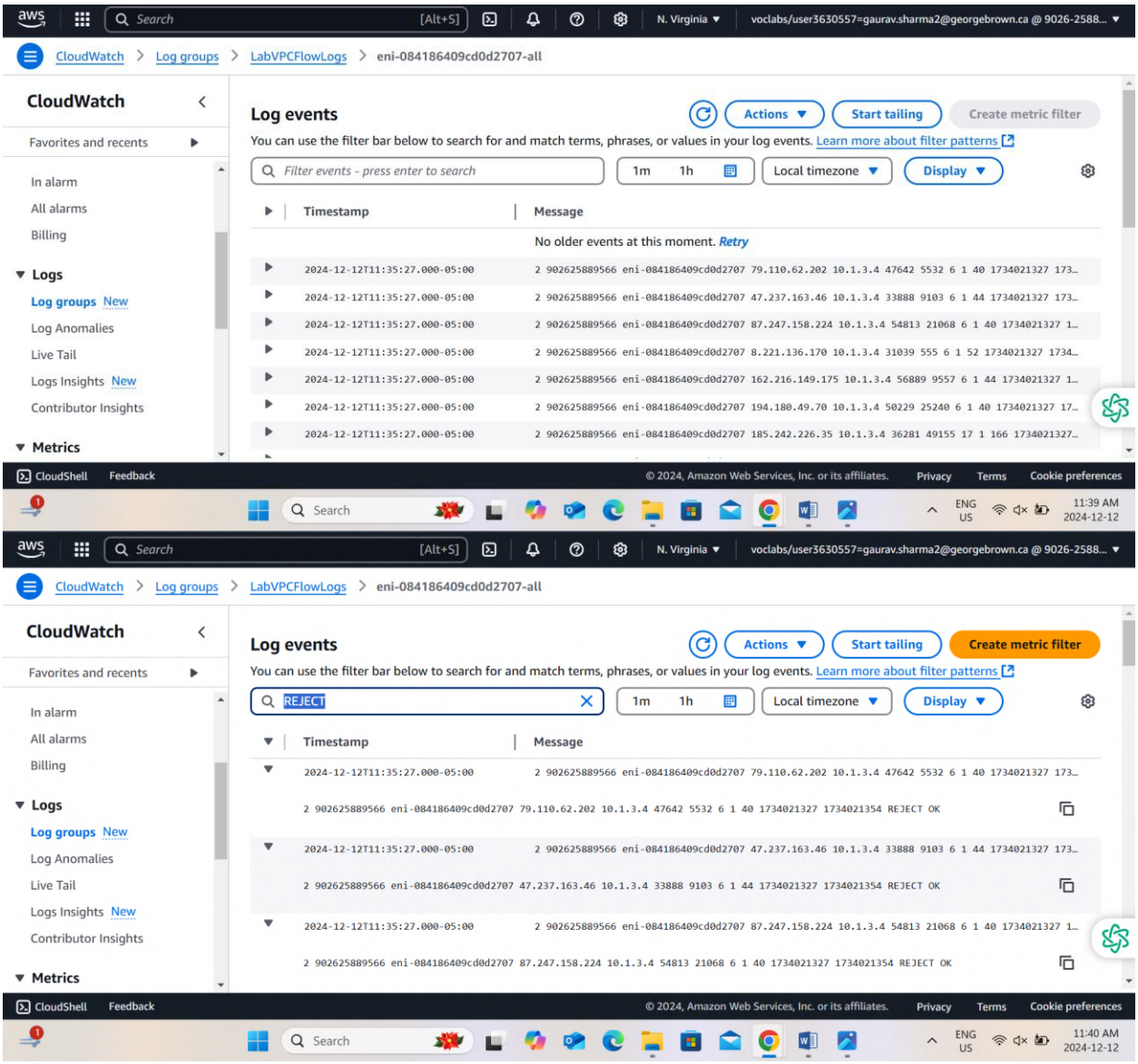




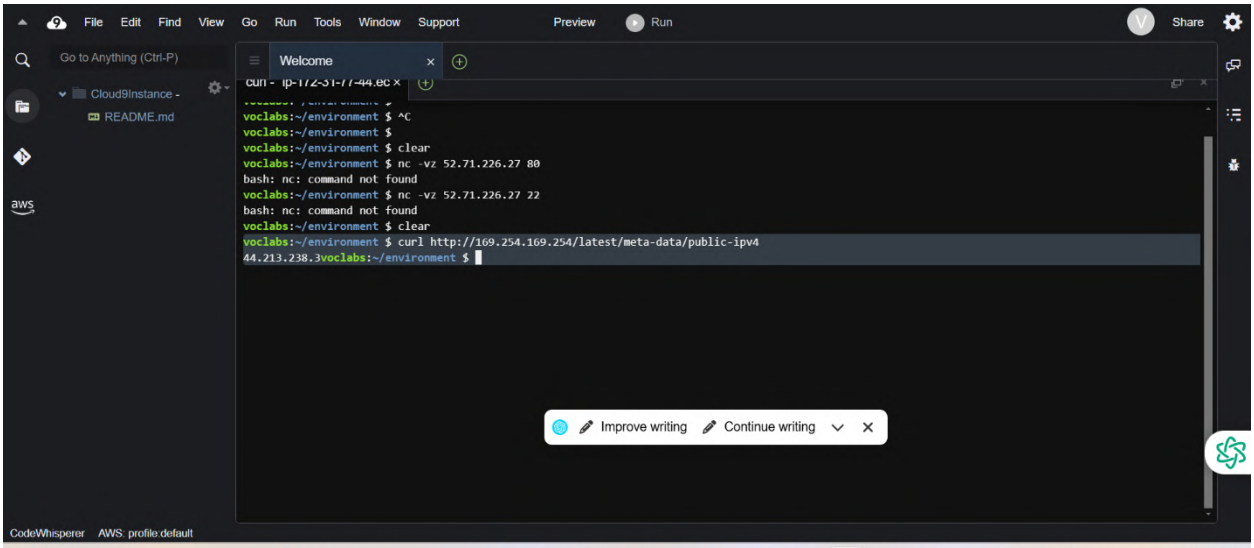
AWS-Cloud-Security-Project

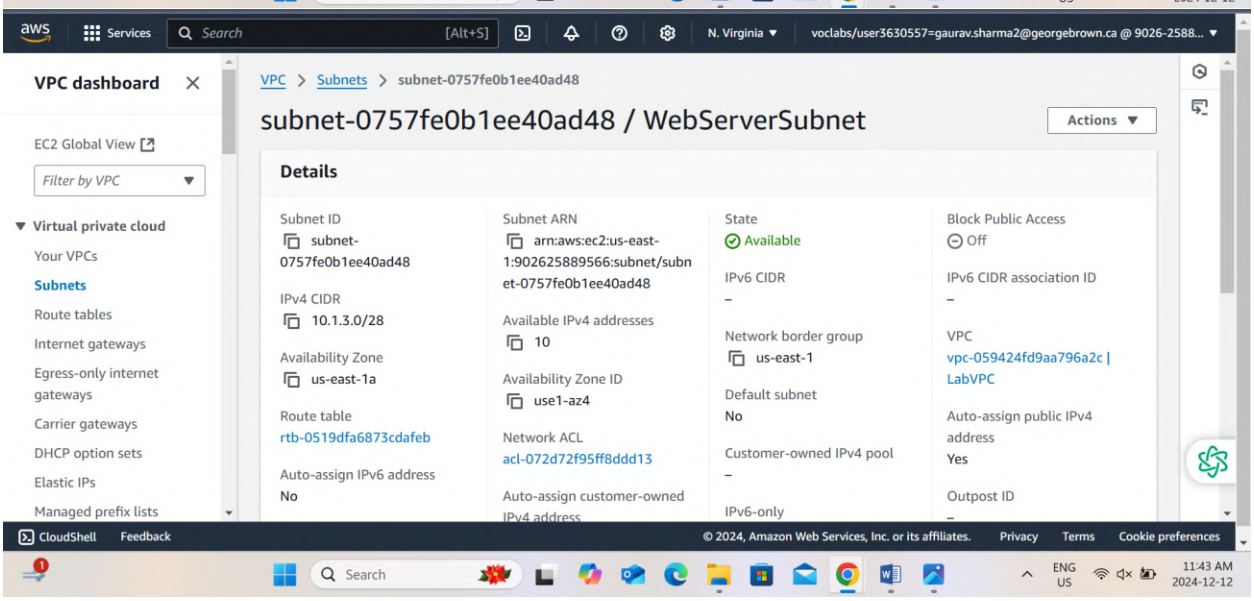


AWS-Cloud-Security-Project

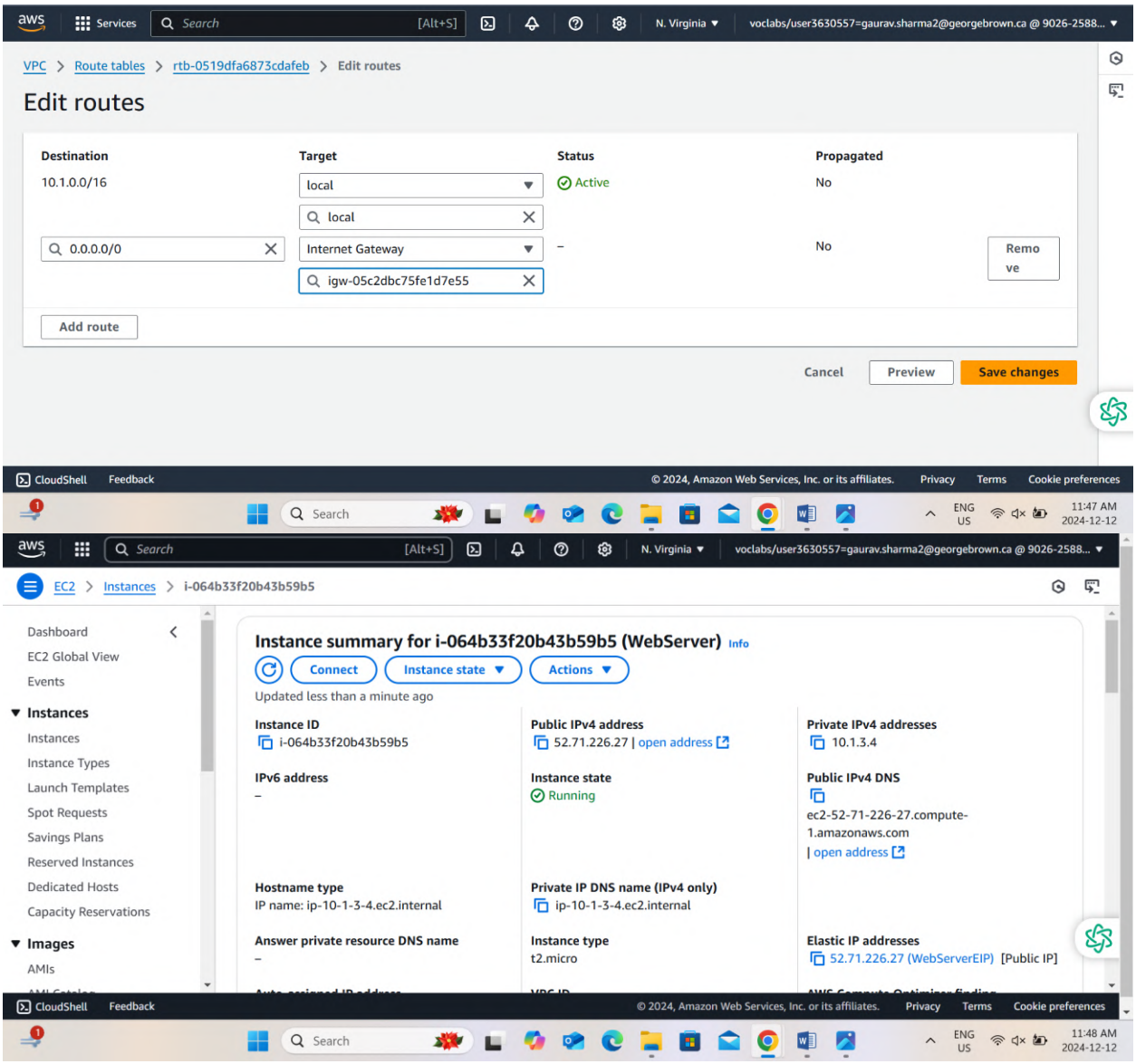


AWS-Cloud-Security-Project

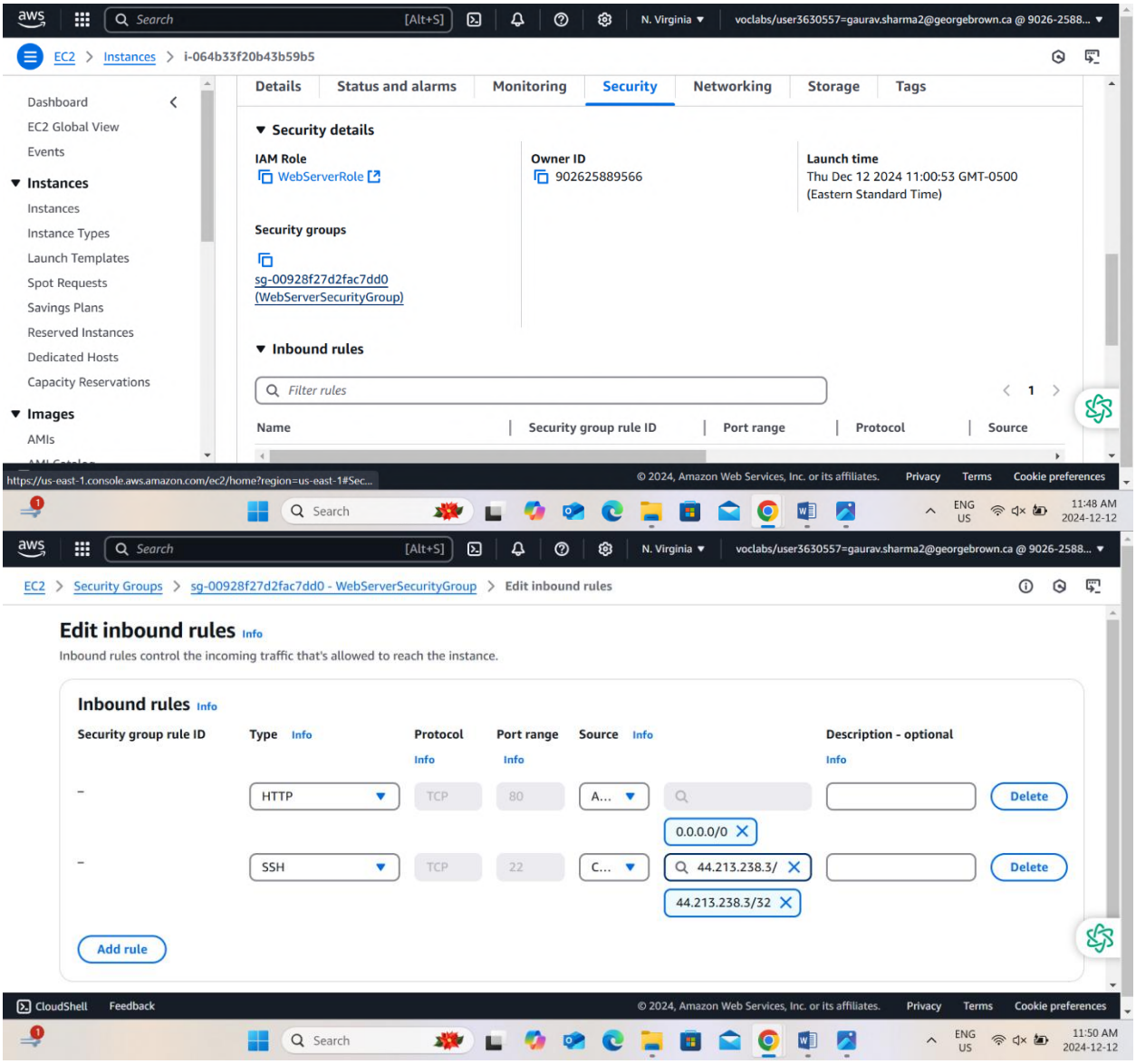




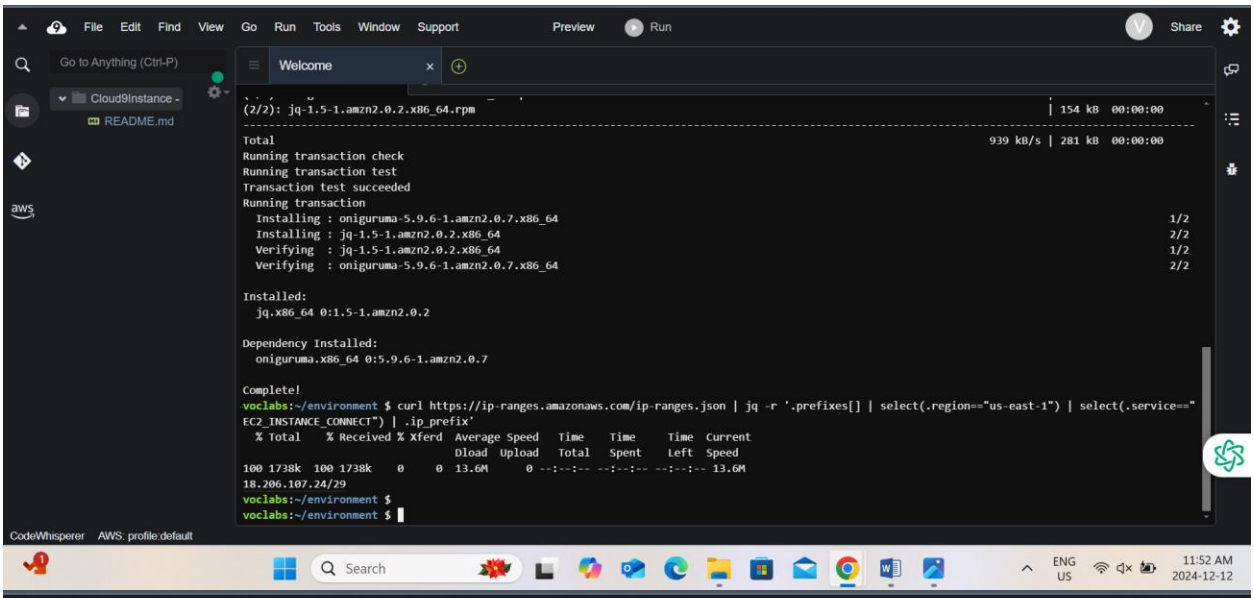
AWS-Cloud-Security-Project

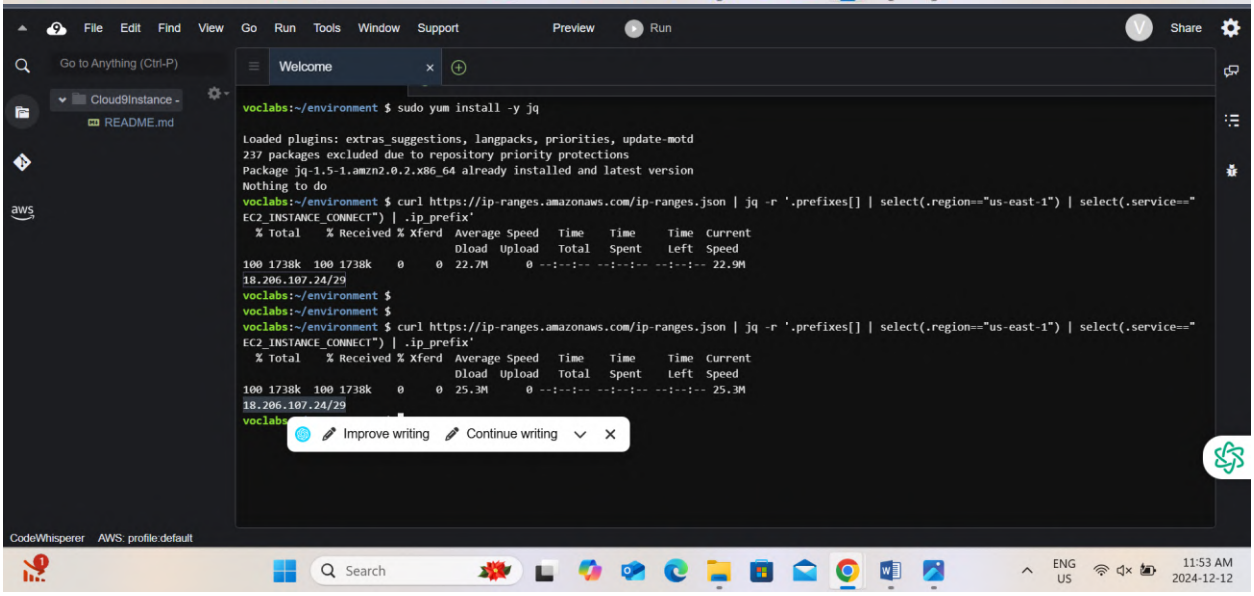


AWS-Cloud-Security-Project

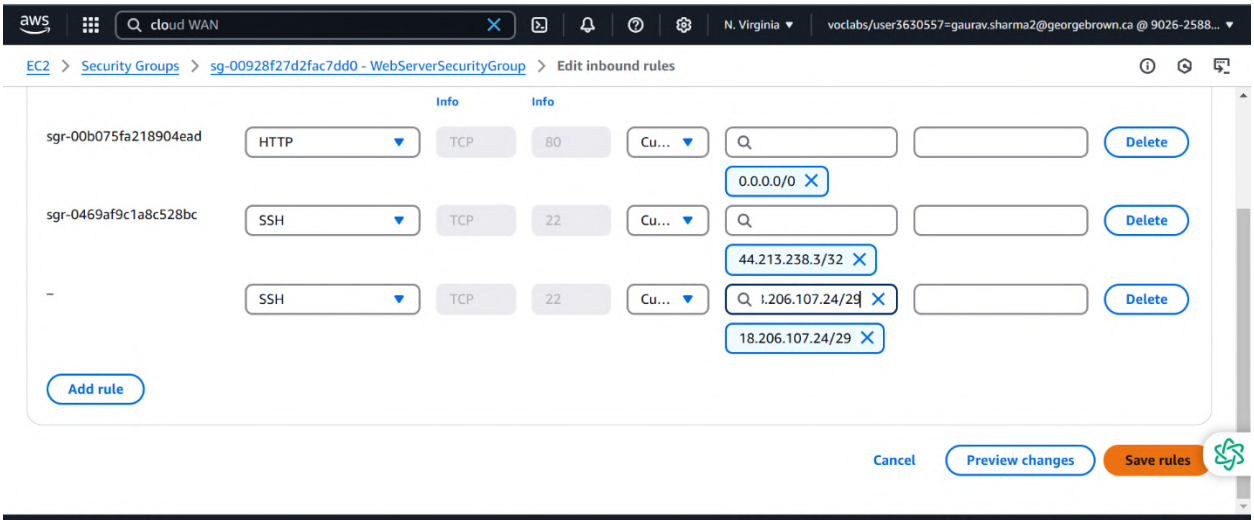


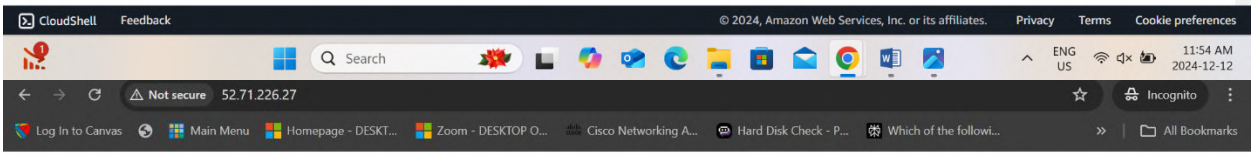
AWS-Cloud-Security-Project





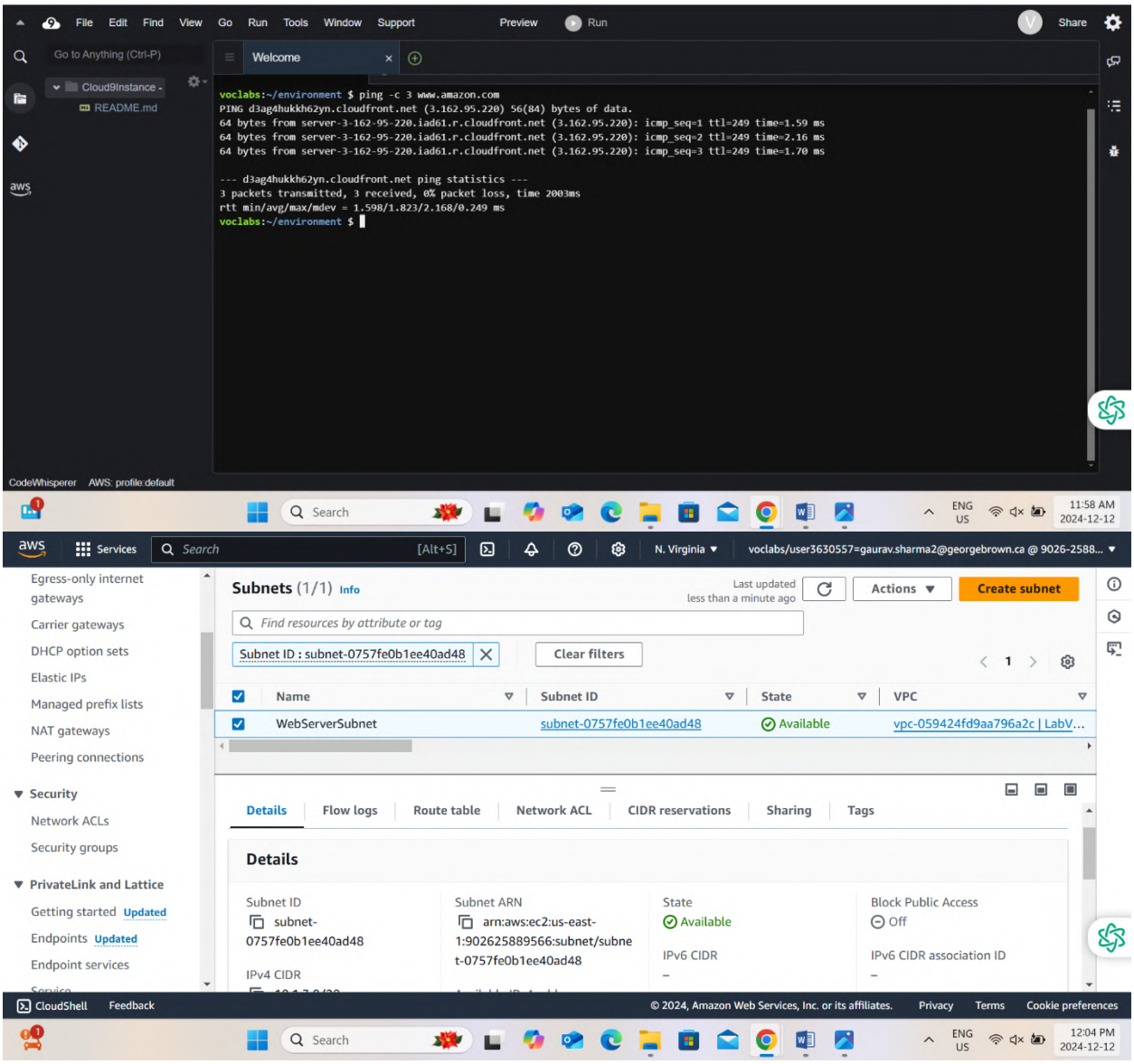
AWS-Cloud-Security-Project



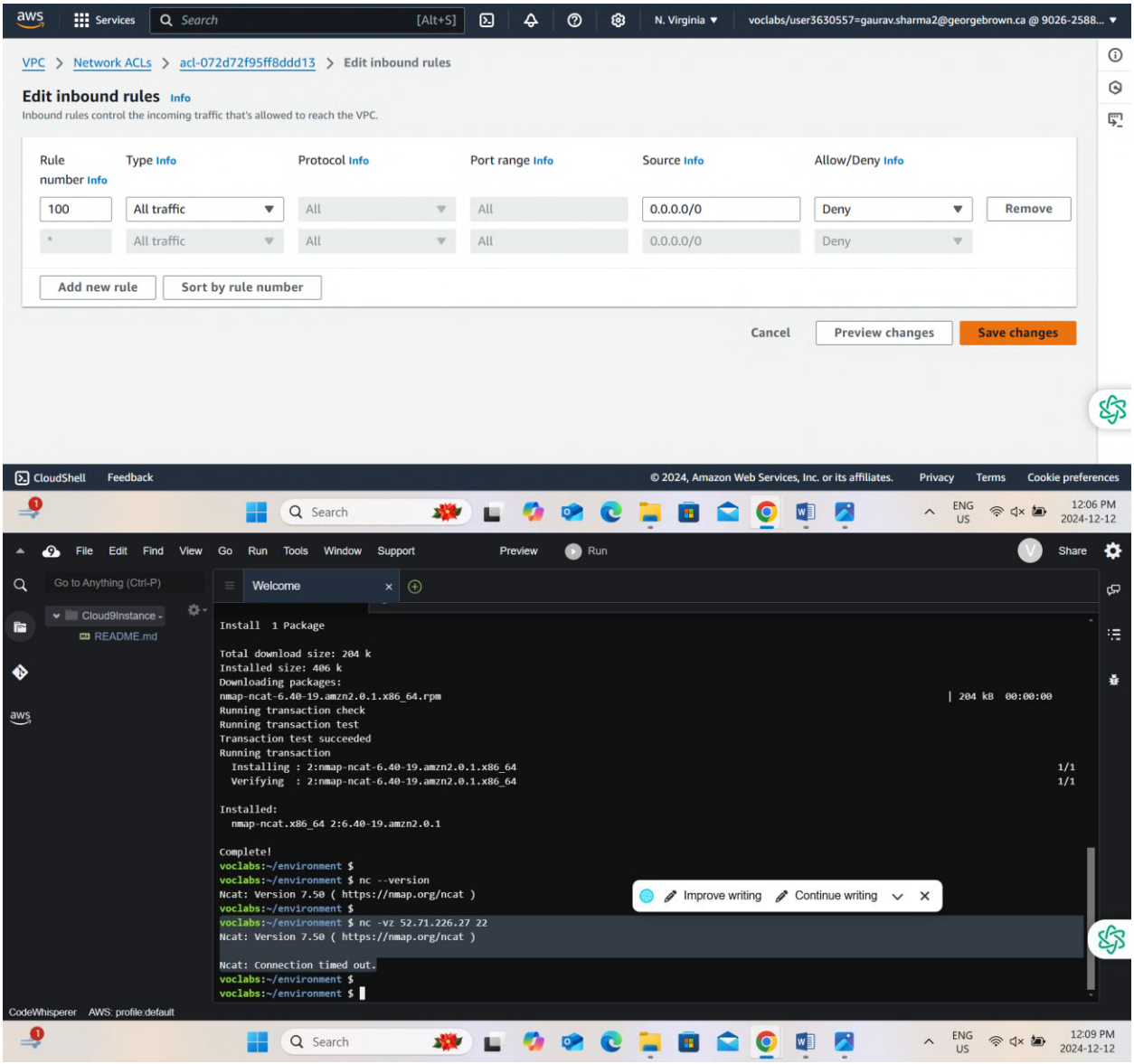


Hello world from WebServer!

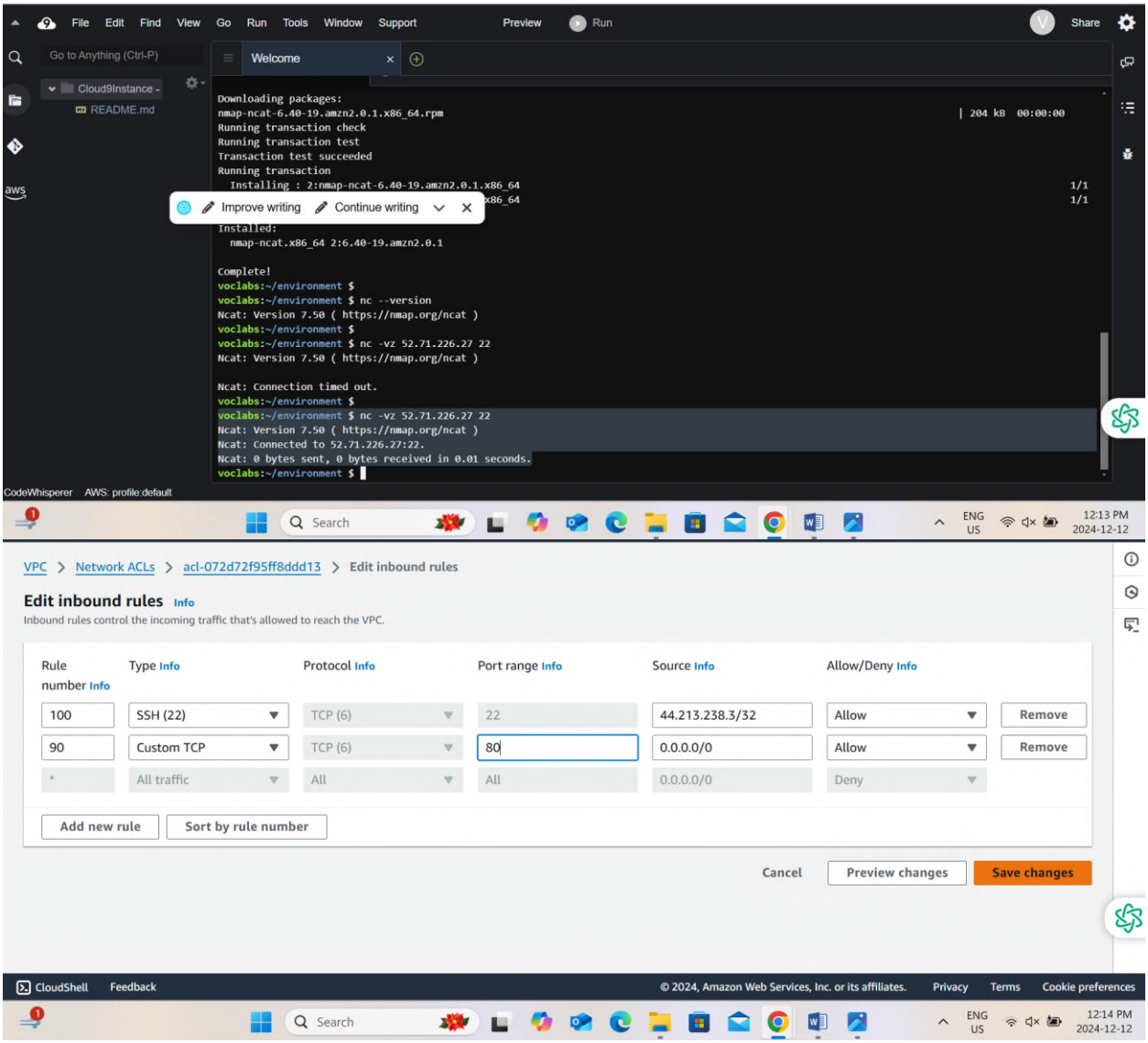
AWS-Cloud-Security-Project



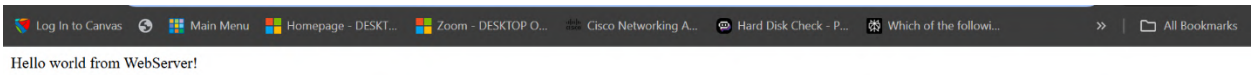
AWS-Cloud-Security-Project



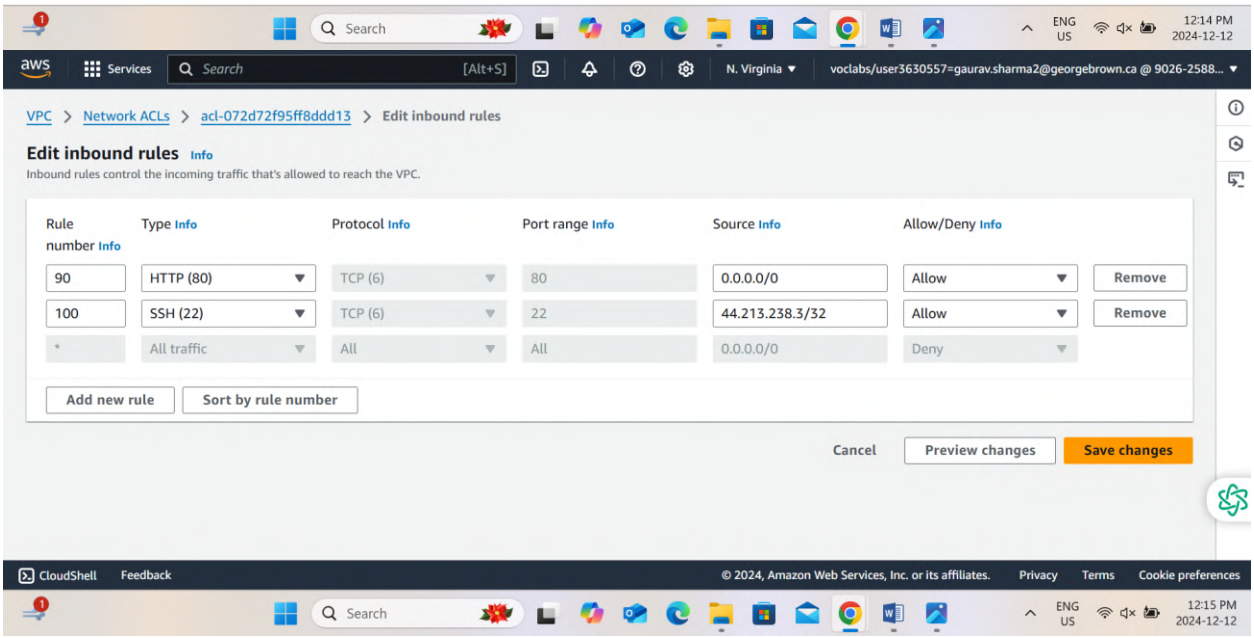
AWS-Cloud-Security-Project



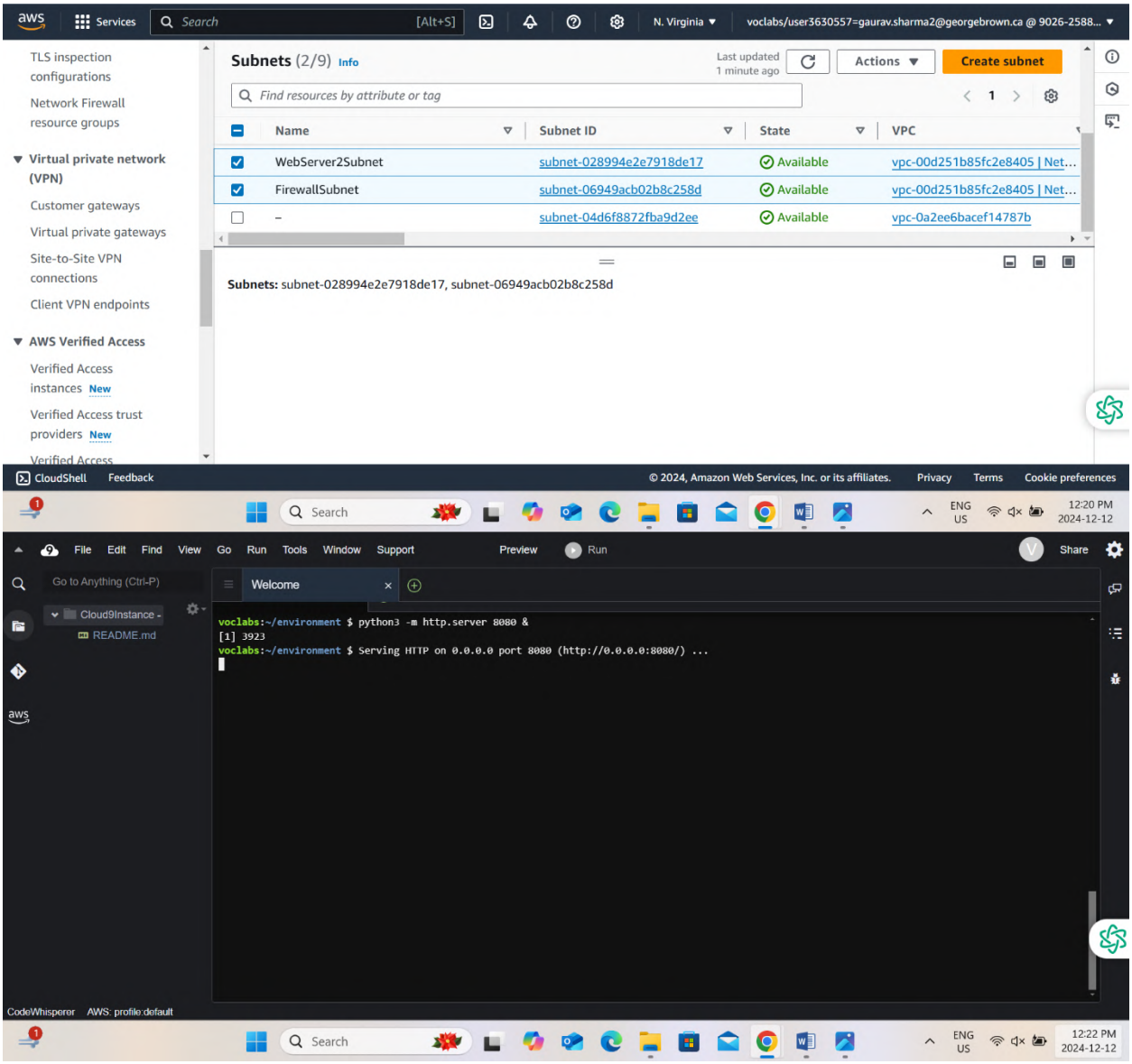
AWS-Cloud-Security-Project



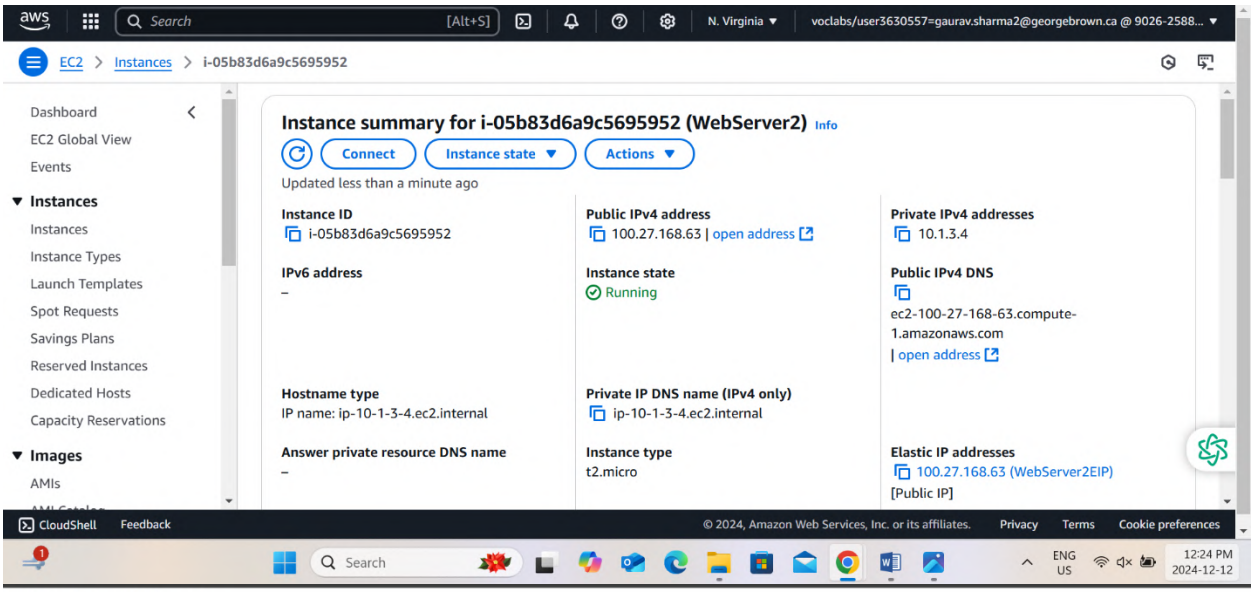
Hello world from WebServer!



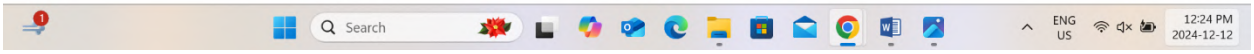
AWS-Cloud-Security-Project



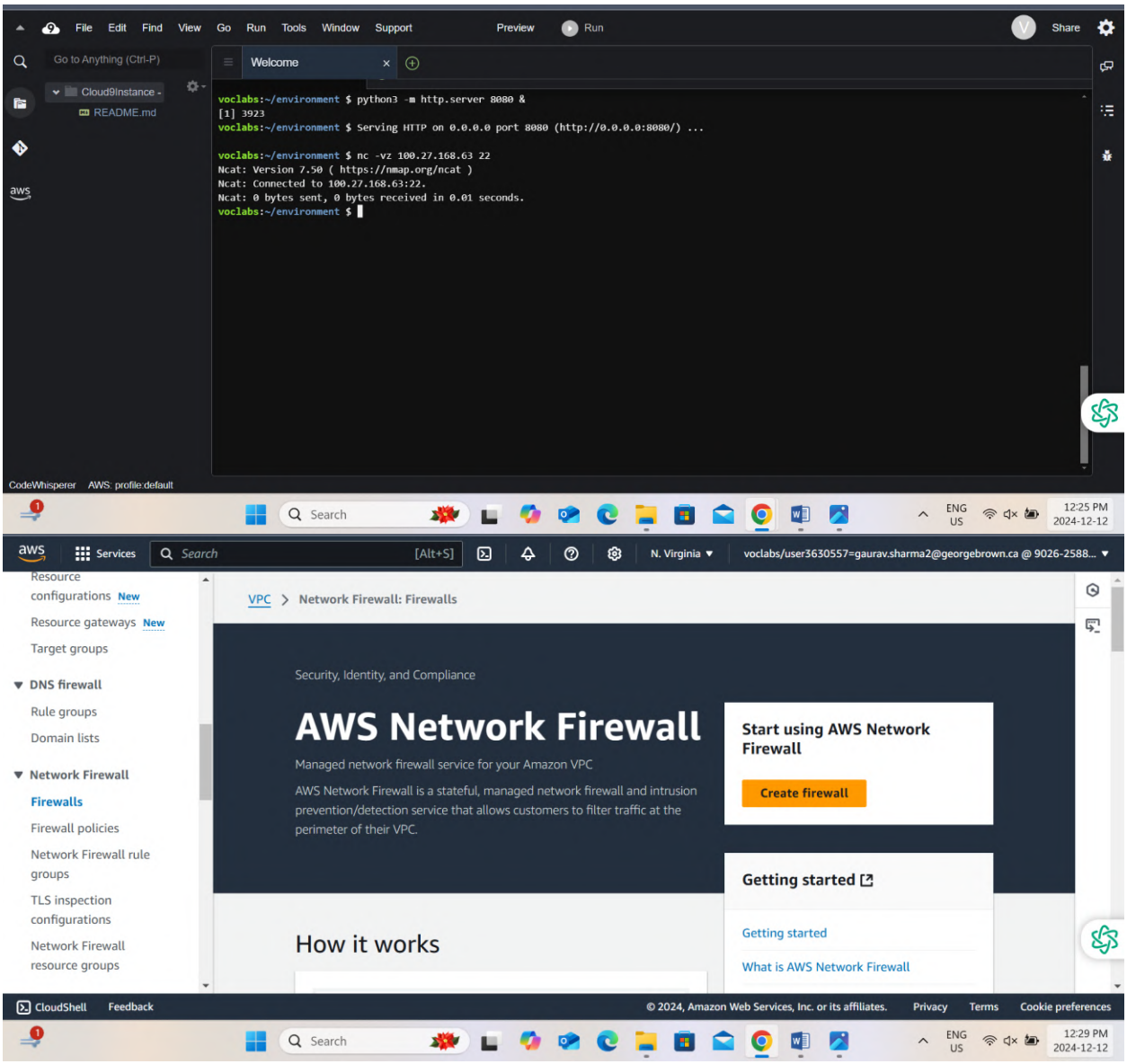
AWS-Cloud-Security-Project



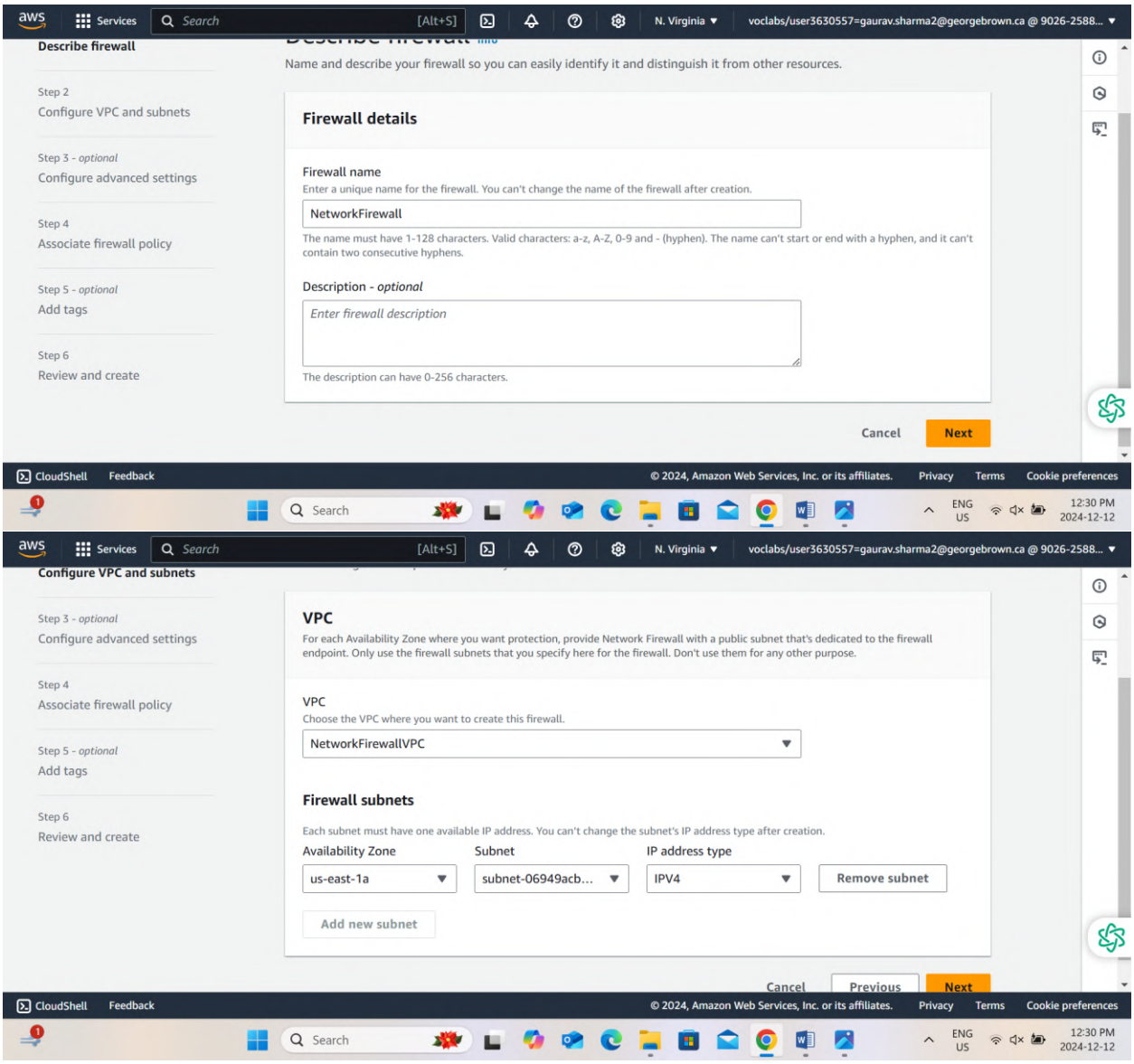
Hello world from WebServer2!



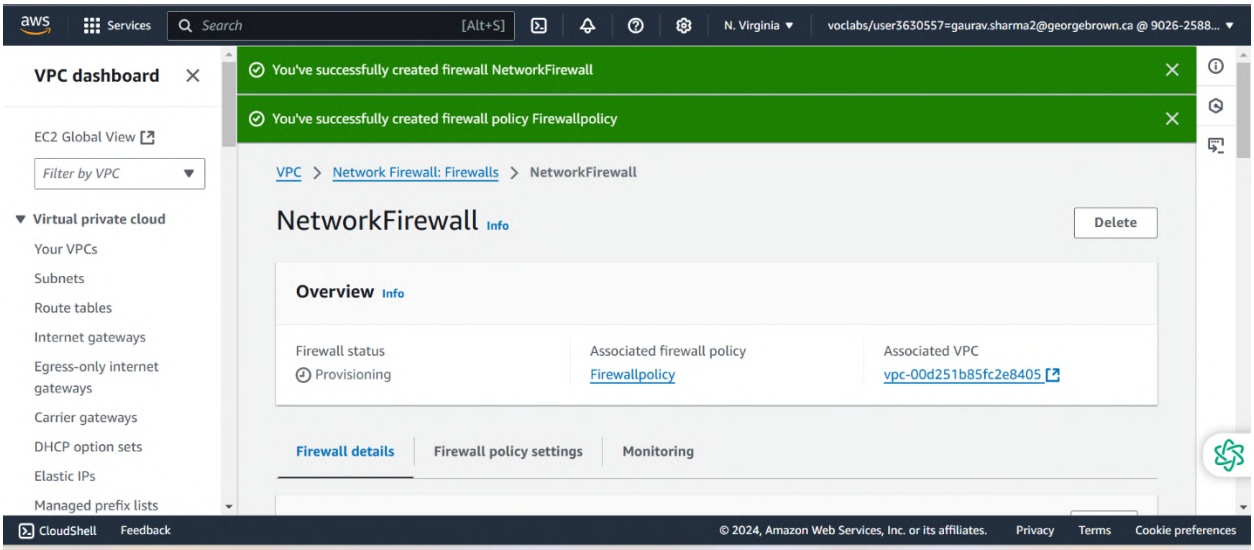
AWS-Cloud-Security-Project

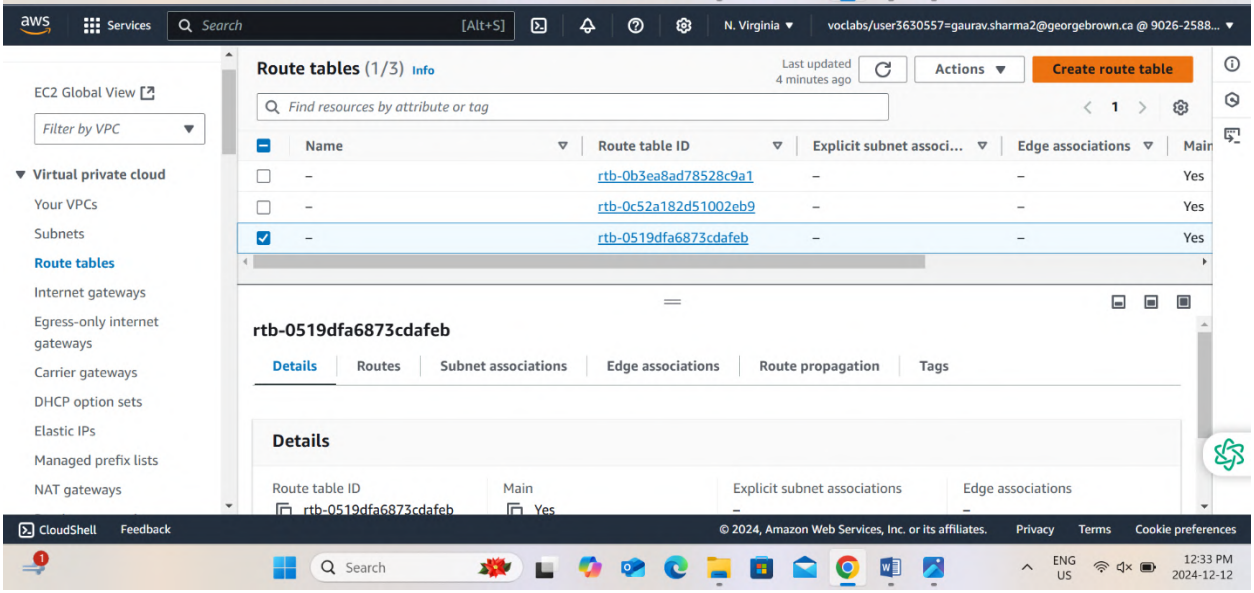


AWS-Cloud-Security-Project

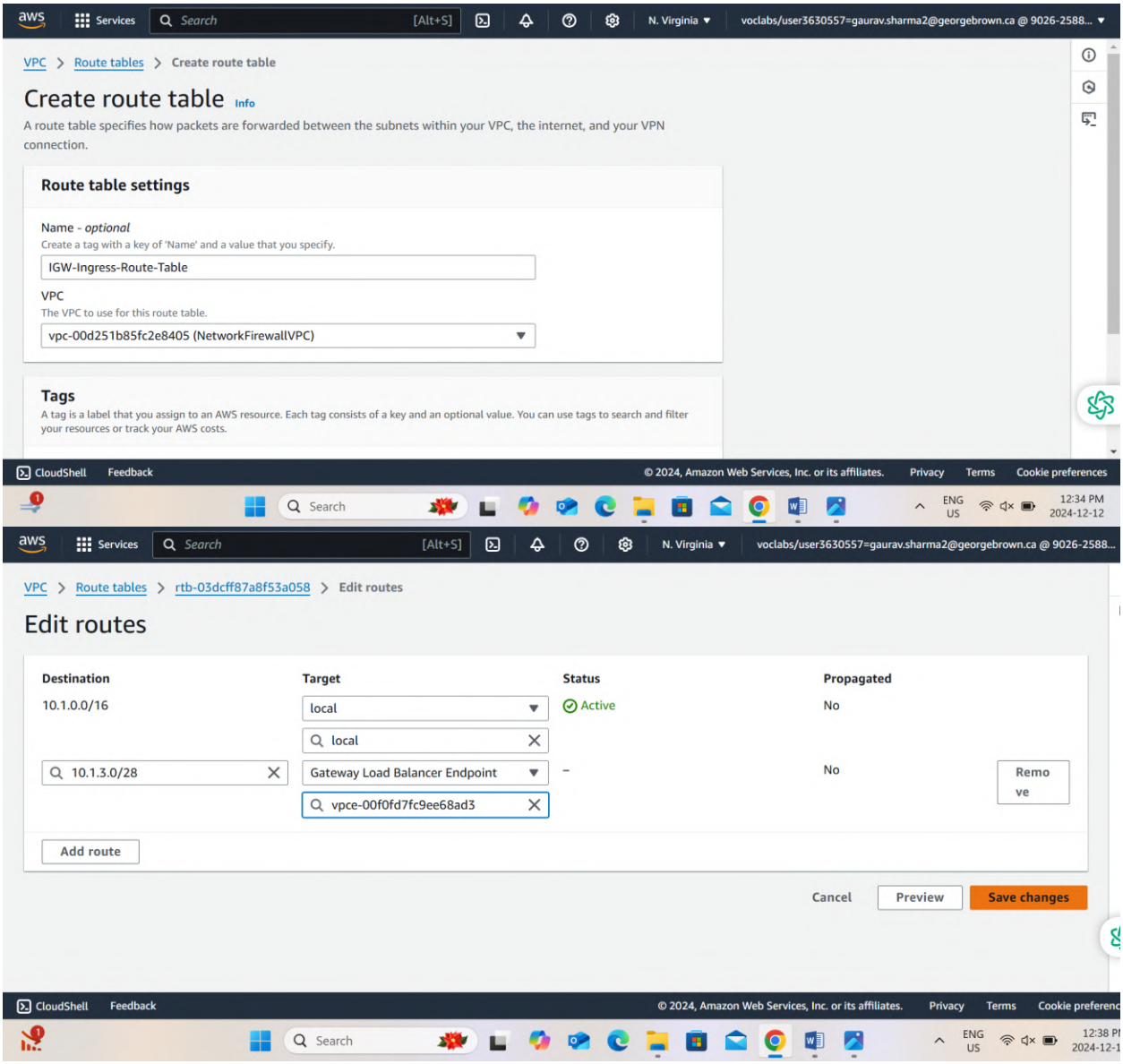


AWS-Cloud-Security-Project

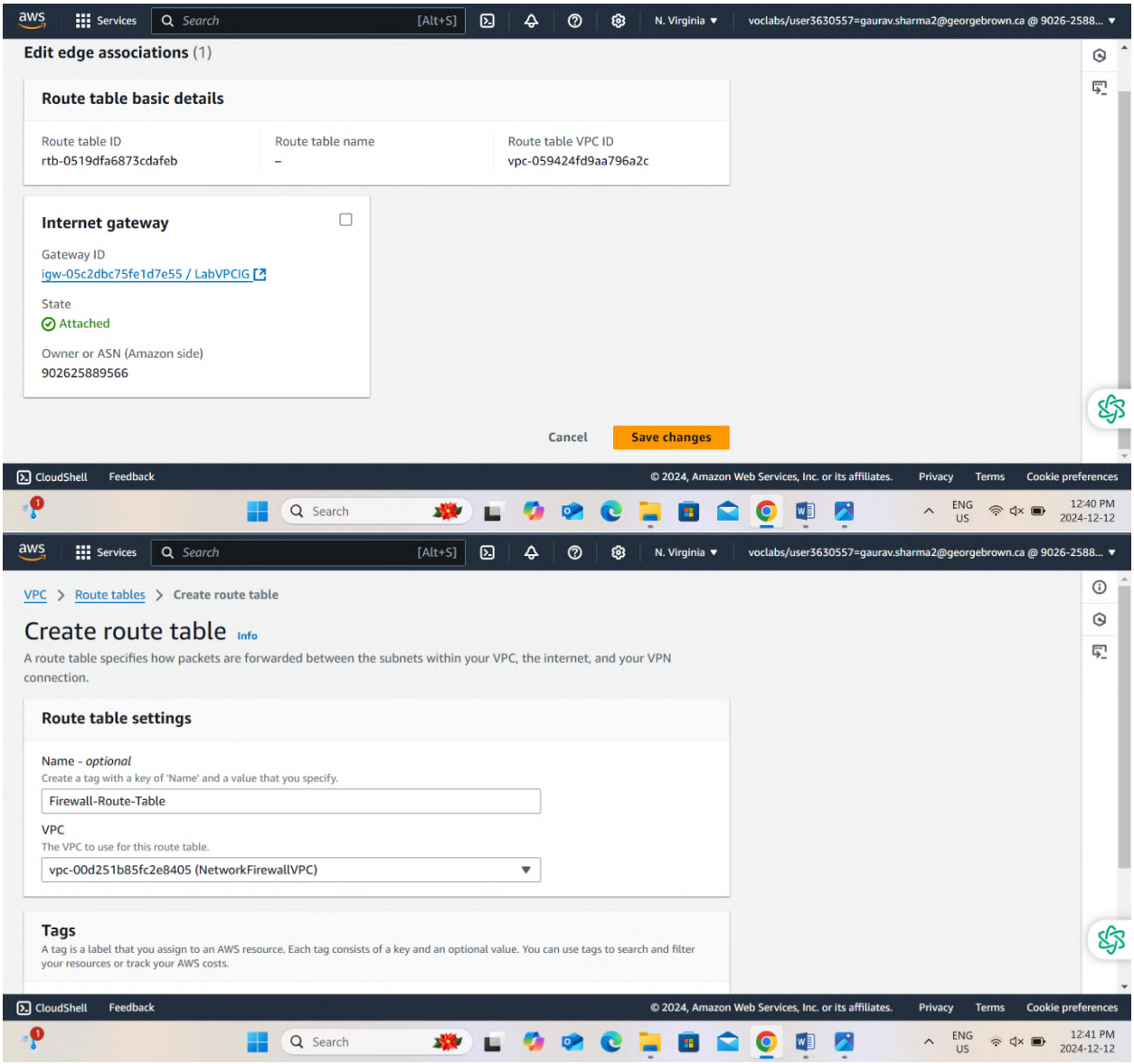




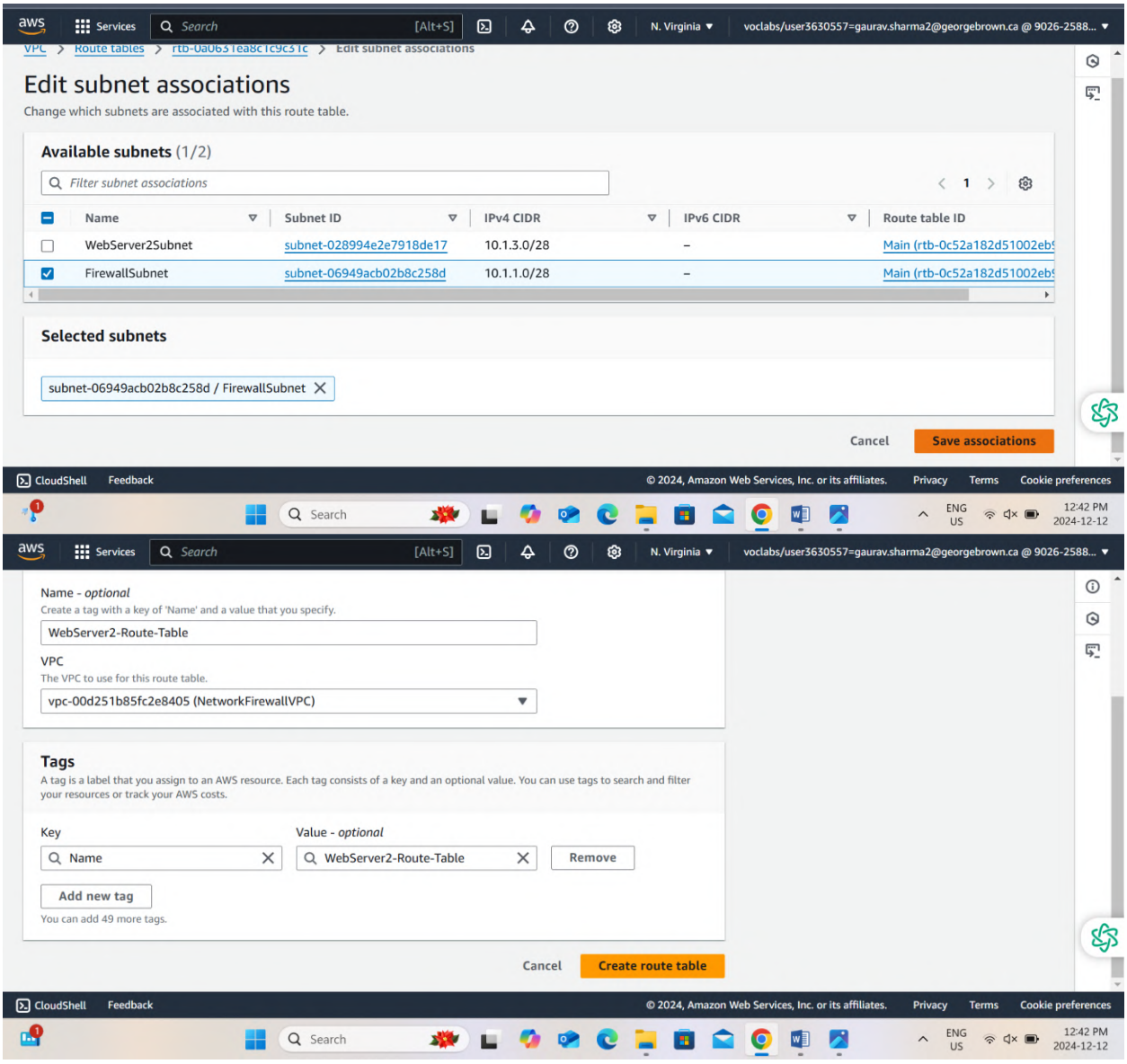
AWS-Cloud-Security-Project



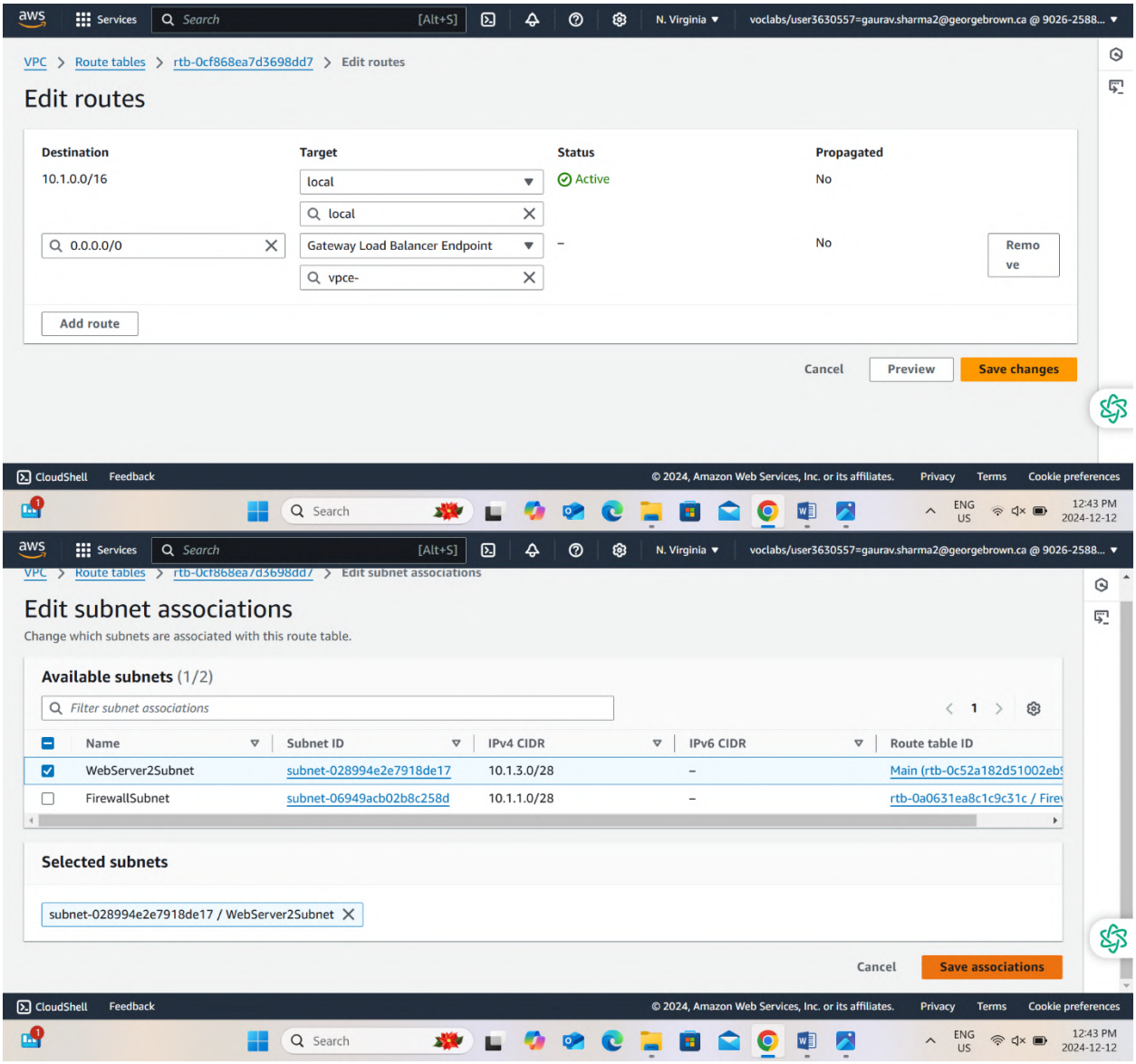
AWS-Cloud-Security-Project



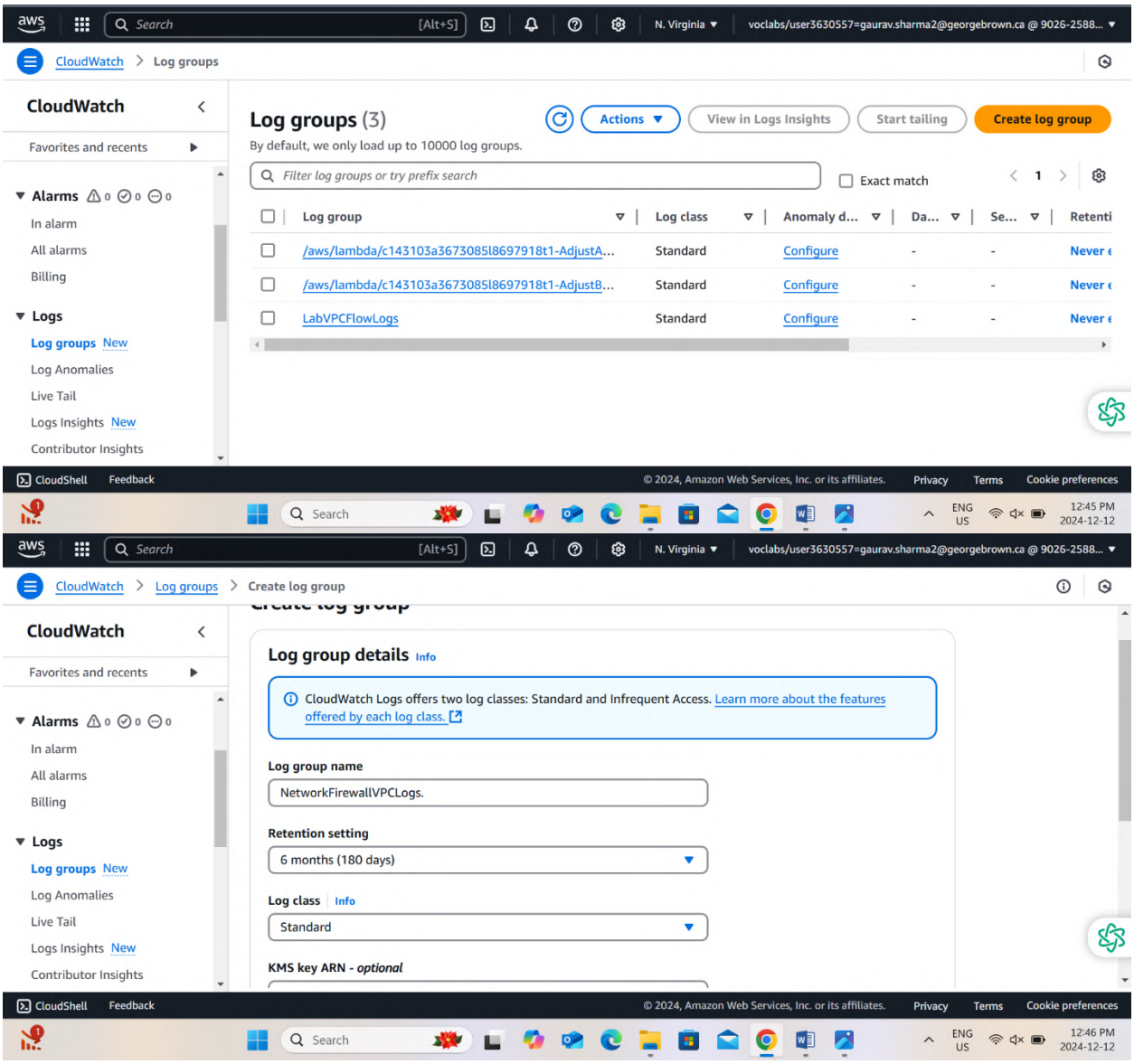
AWS-Cloud-Security-Project



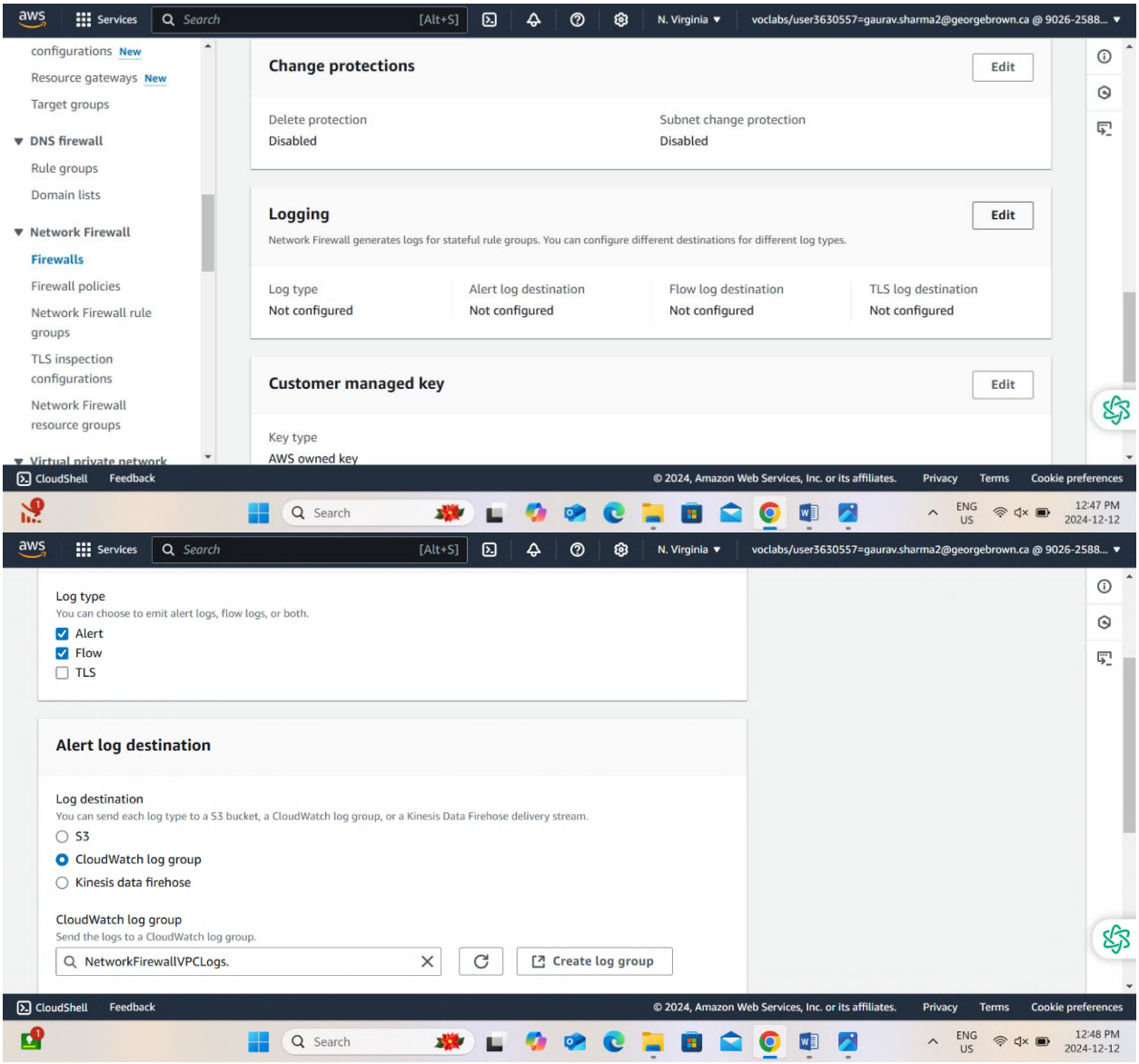
AWS-Cloud-Security-Project



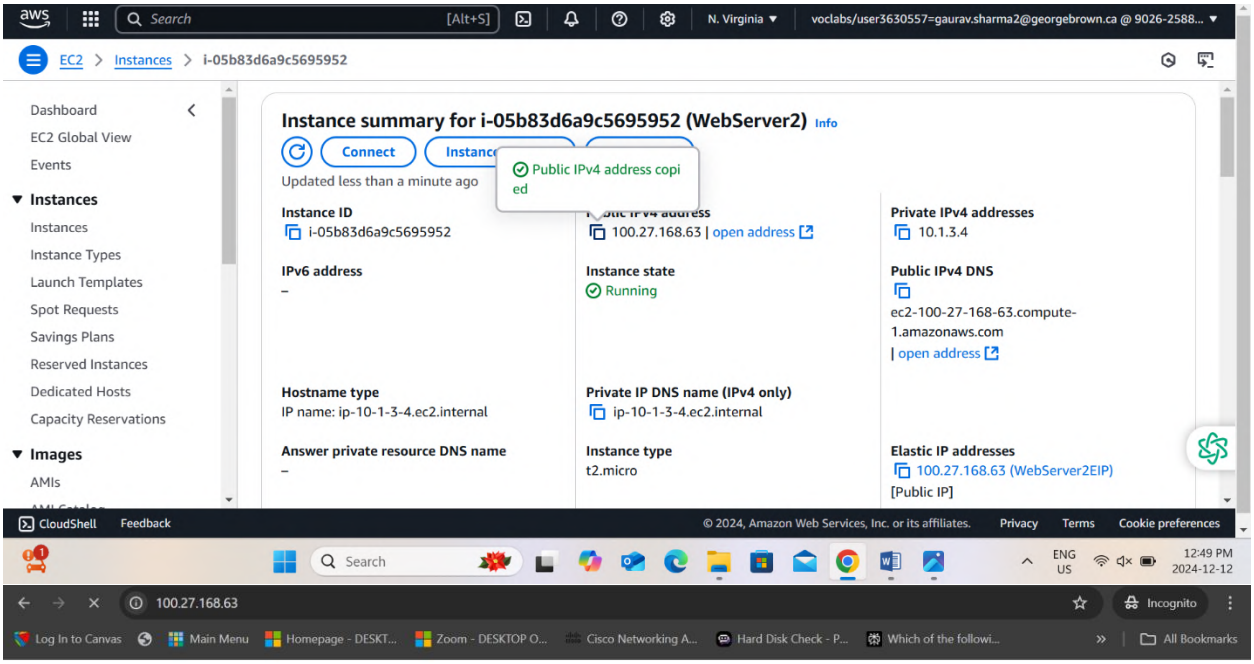
AWS-Cloud-Security-Project

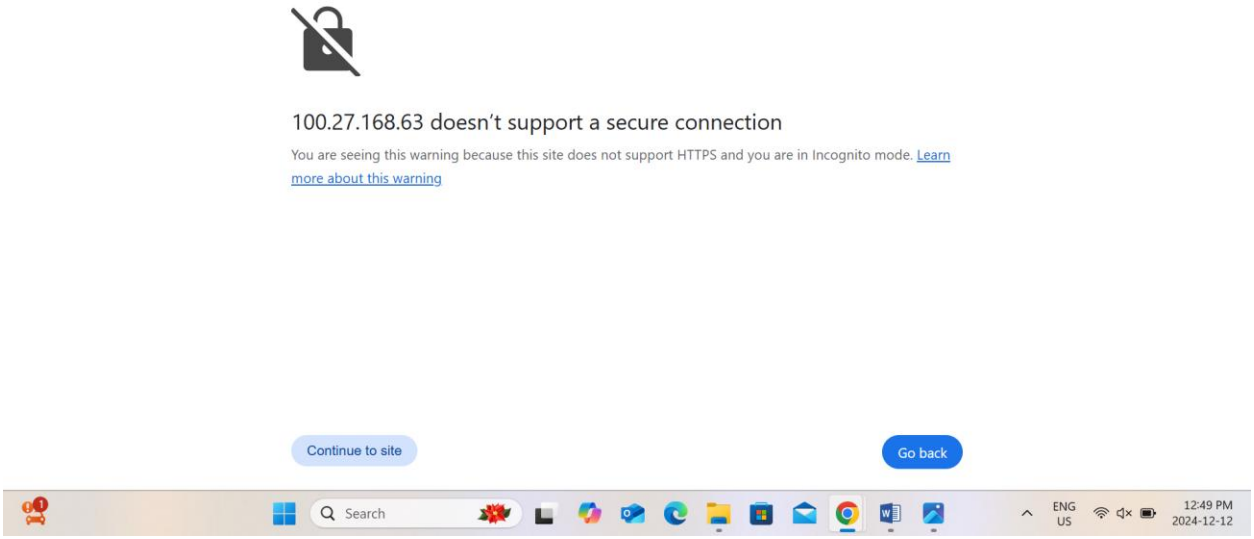


AWS-Cloud-Security-Project

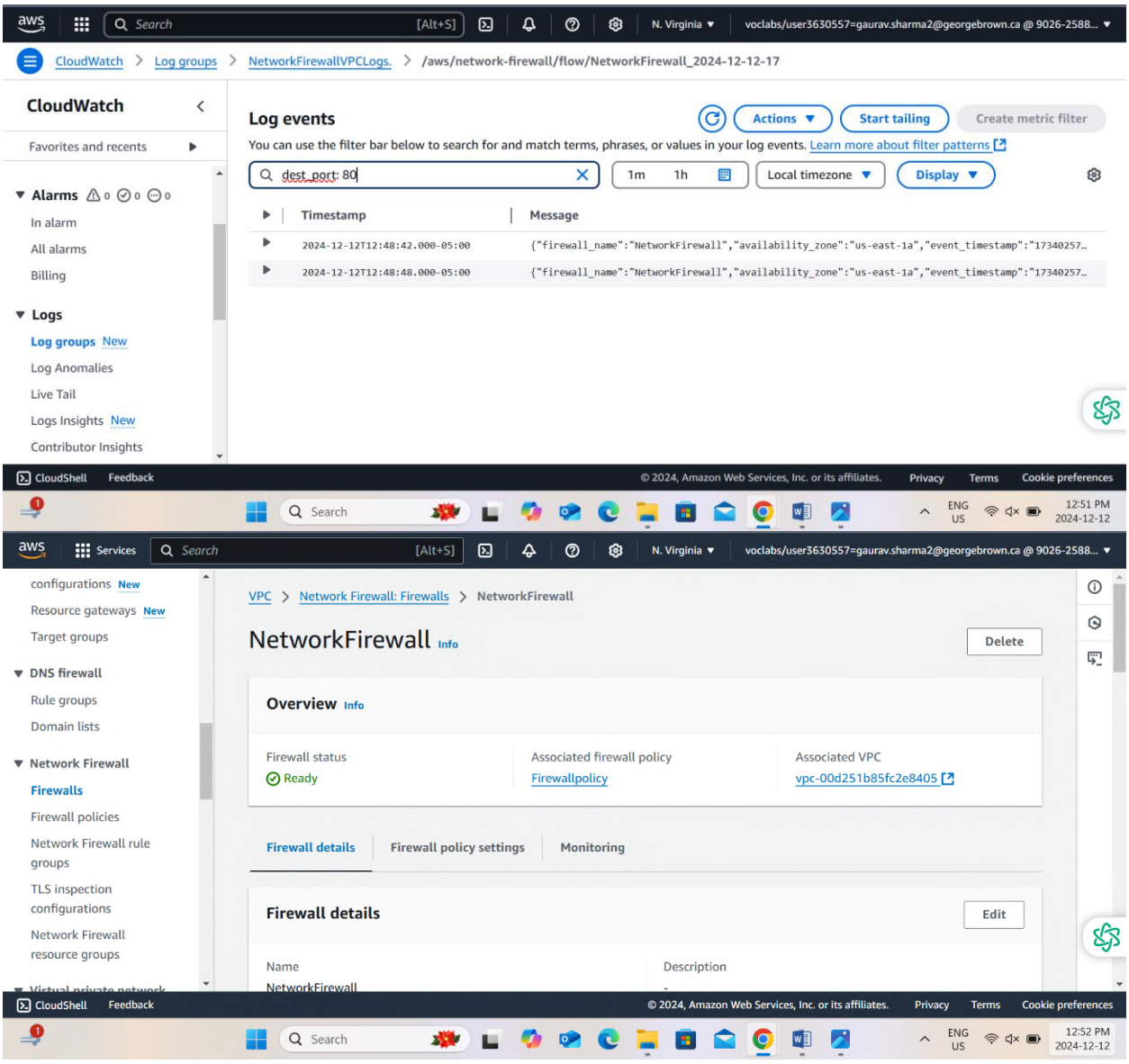


AWS-Cloud-Security-Project

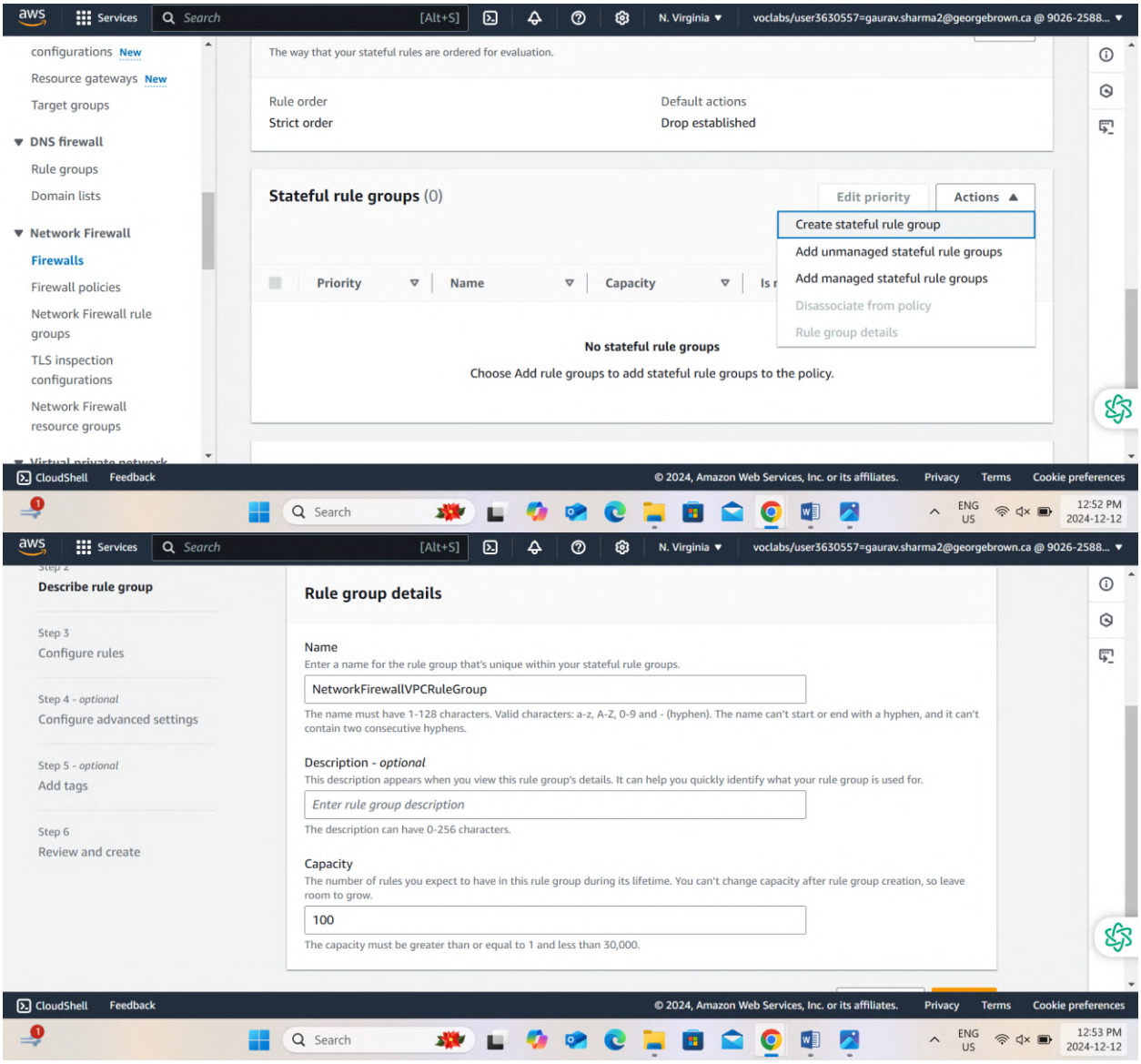




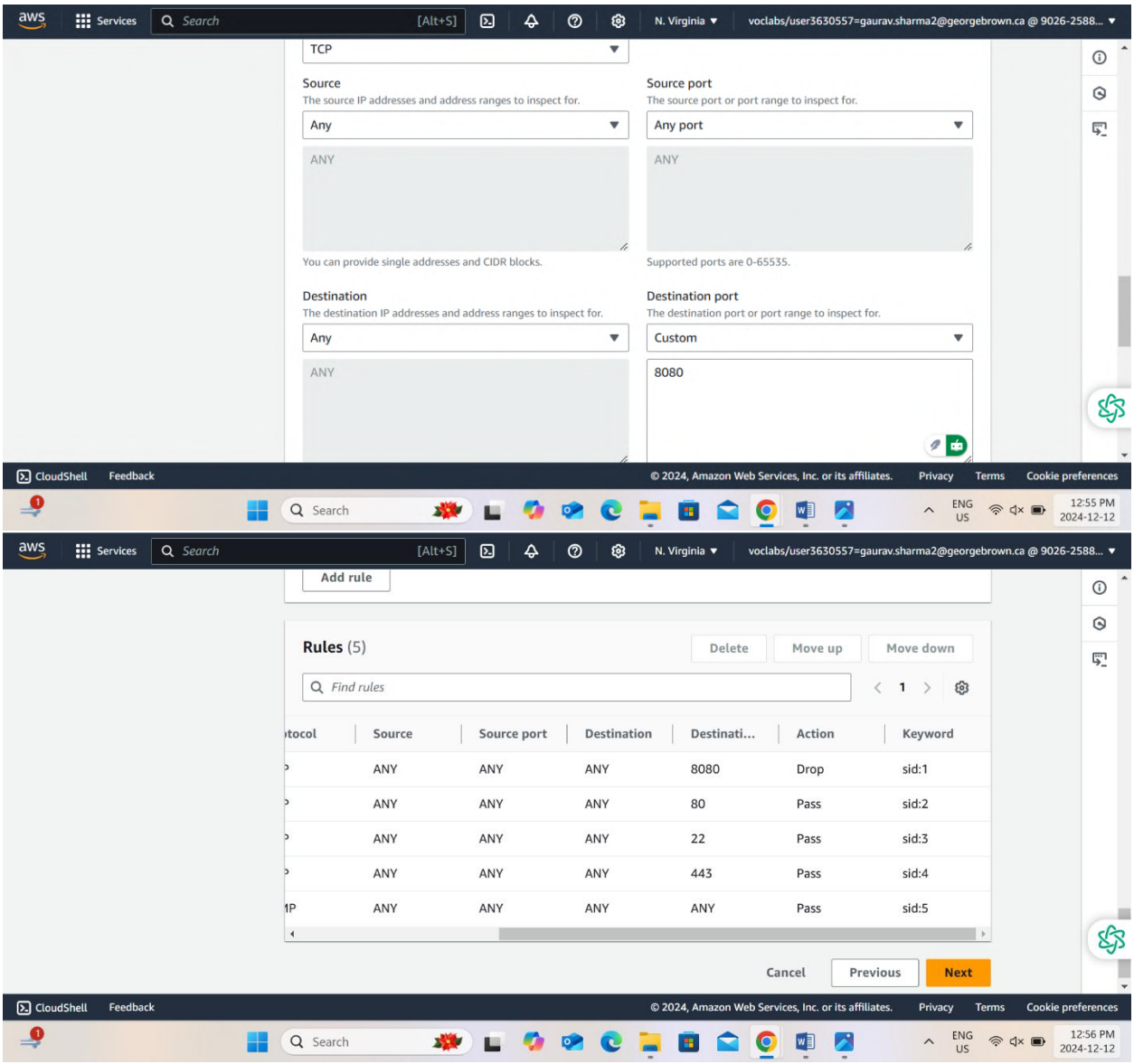
AWS-Cloud-Security-Project



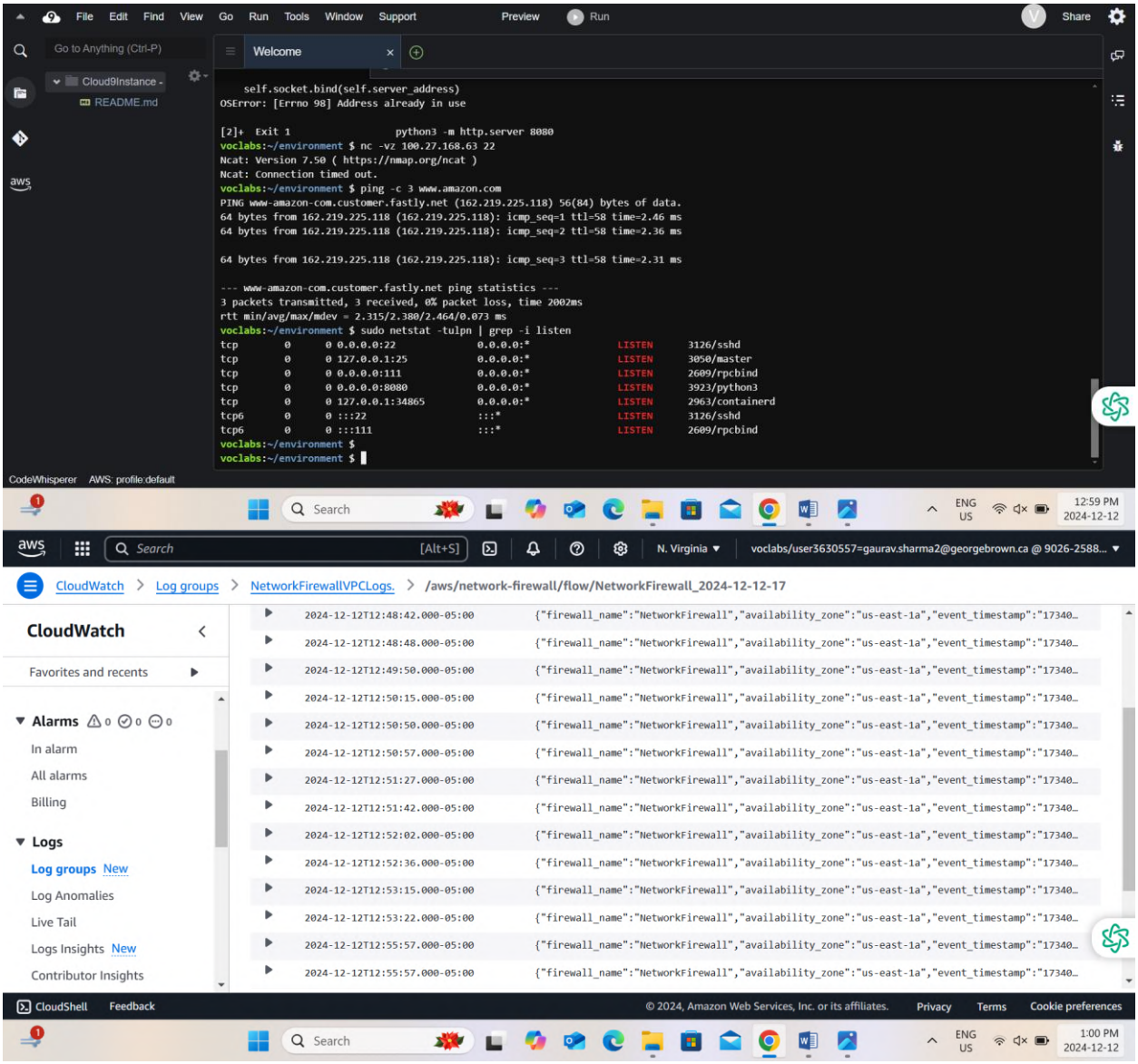
AWS-Cloud-Security-Project



AWS-Cloud-Security-Project



AWS-Cloud-Security-Project



Phase 3: Securing AWS resources by using AWS KMS

Task 3.1: Create a customer managed key and configure key rotation

AWS-Cloud-Security-Project

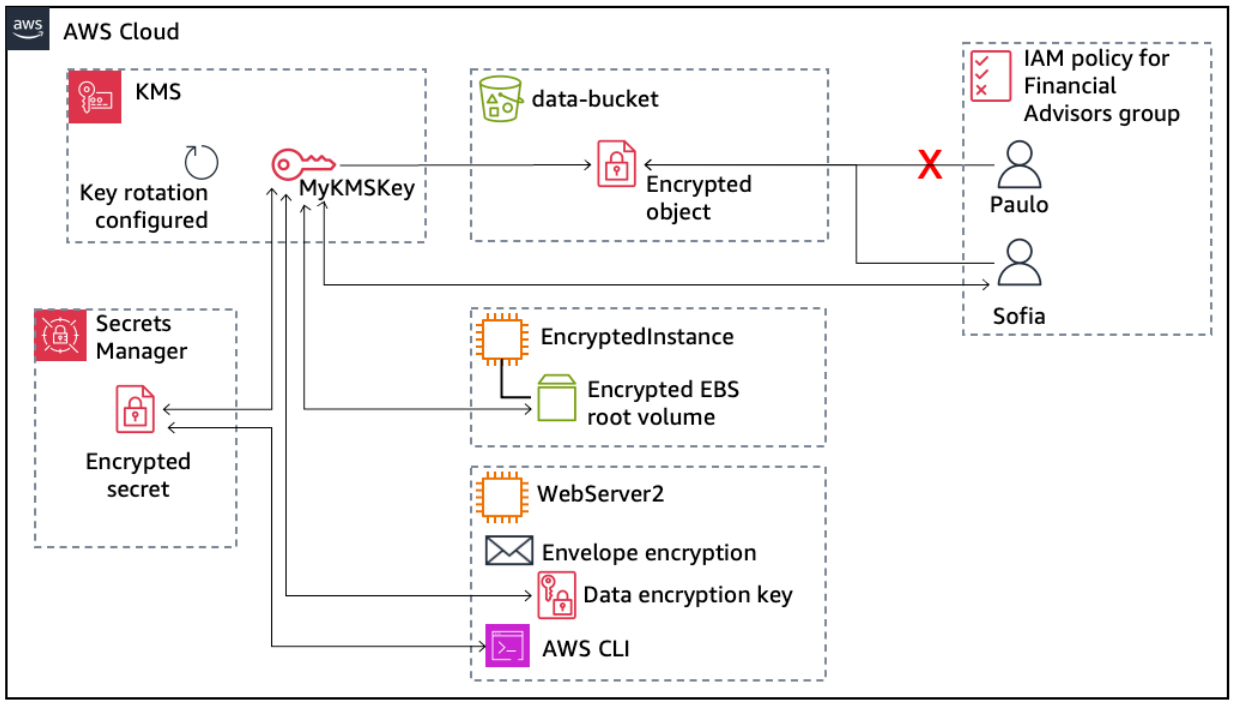
Task 3.2: Update the AWS KMS key policy and analyze an IAM policy

Task 3.3: Use AWS KMS to encrypt data in Amazon S3

Task 3.4: Use AWS KMS to encrypt the root volume of an EC2 instance

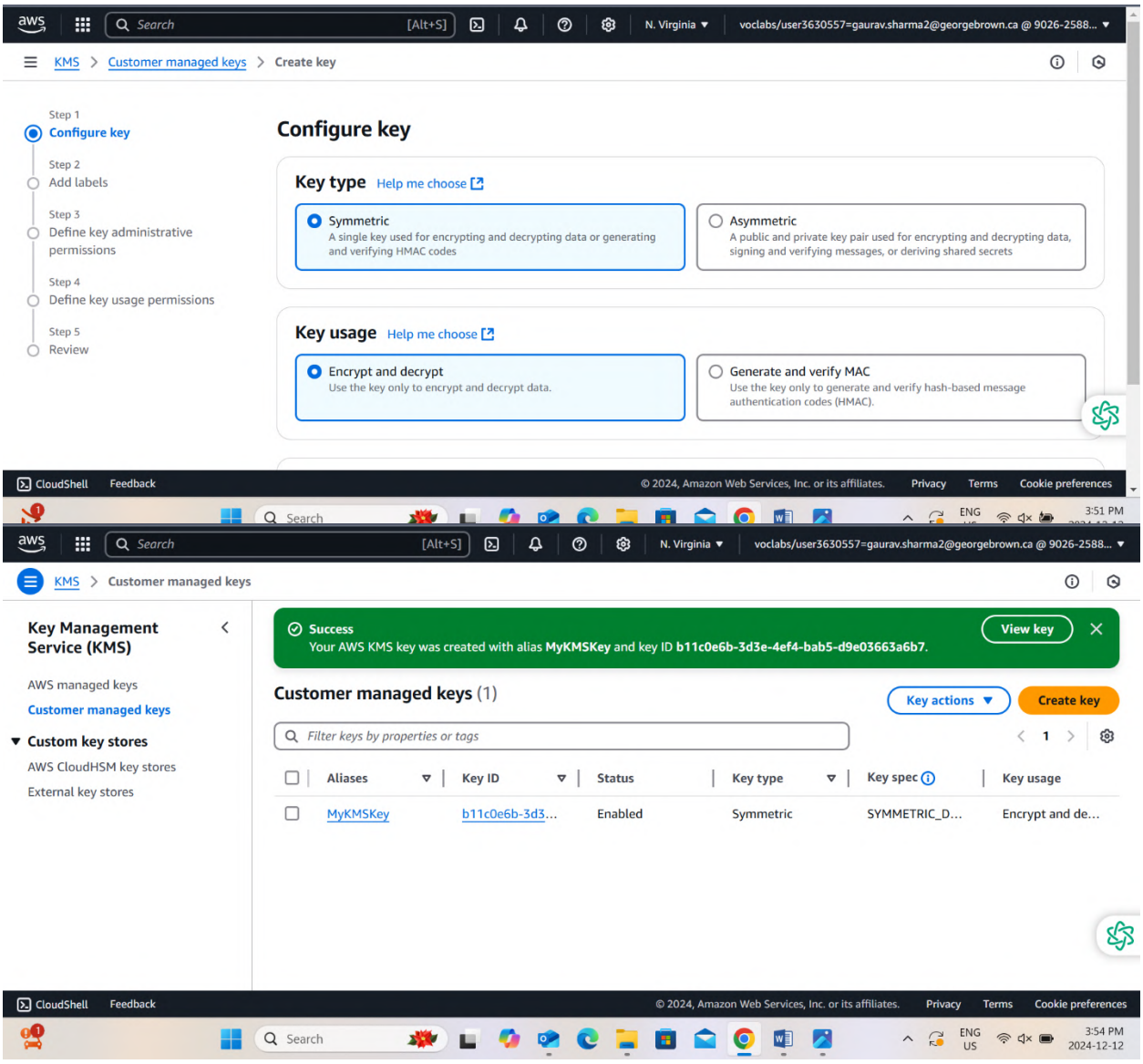
Task 3.5: Use AWS KMS envelope encryption to encrypt data in place

Task 3.6: Use AWS KMS to encrypt a Secrets Manager secret

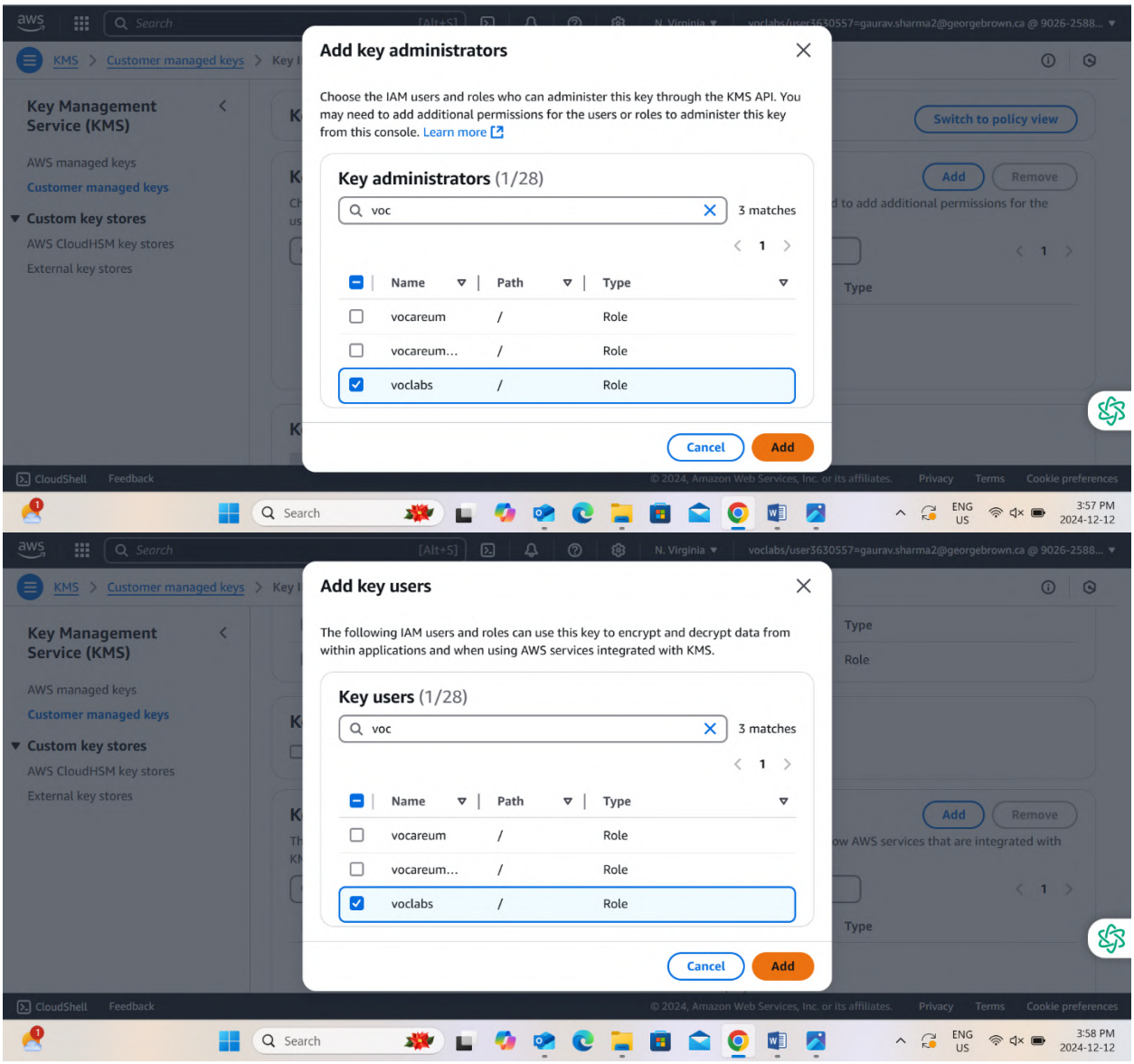


AWS-Cloud-Security-Project

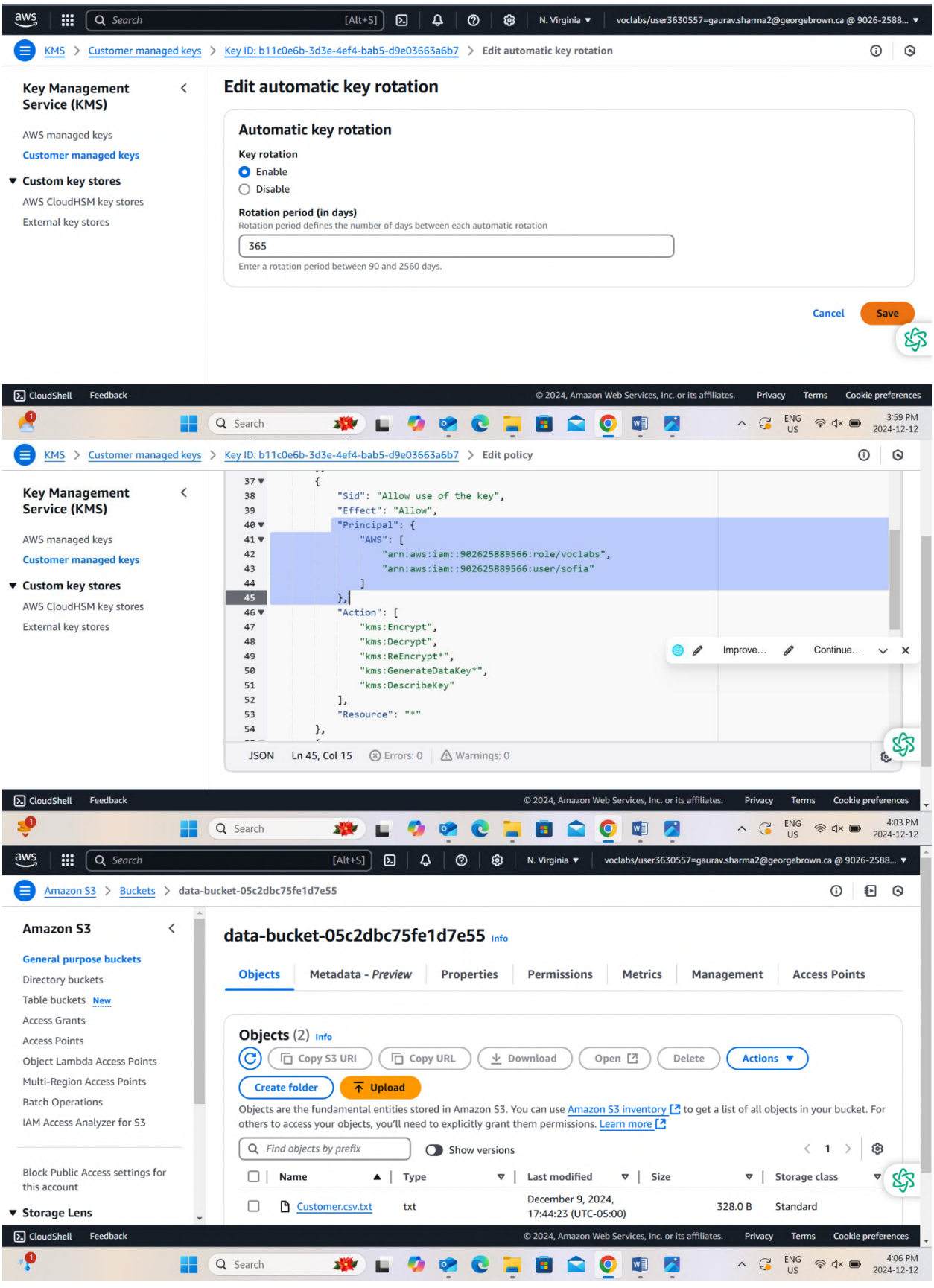
AWS-Cloud-Security-Project



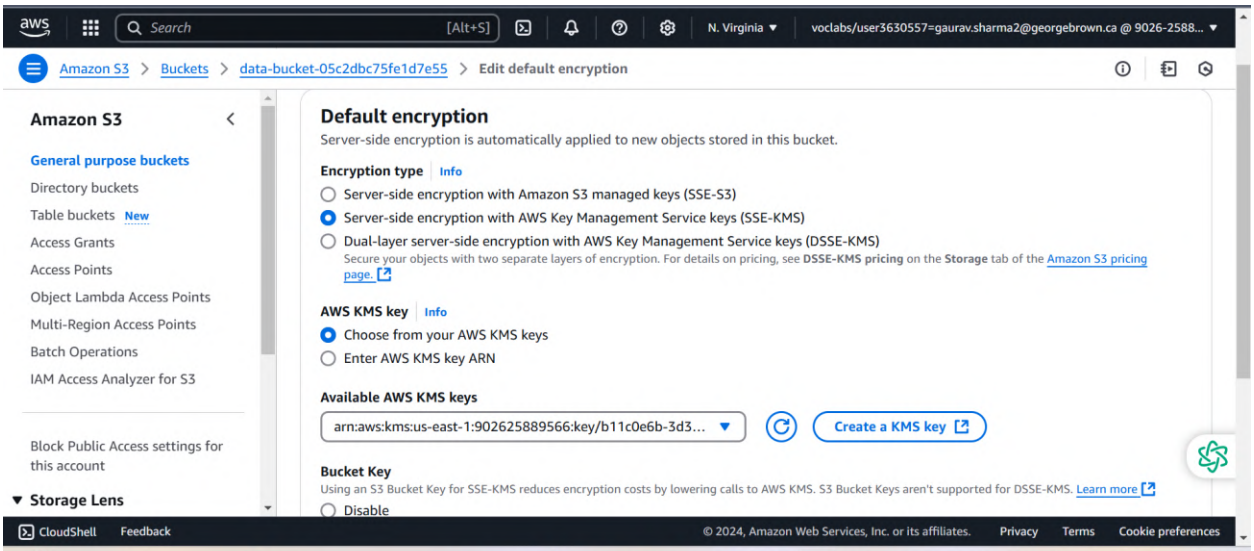
AWS-Cloud-Security-Project

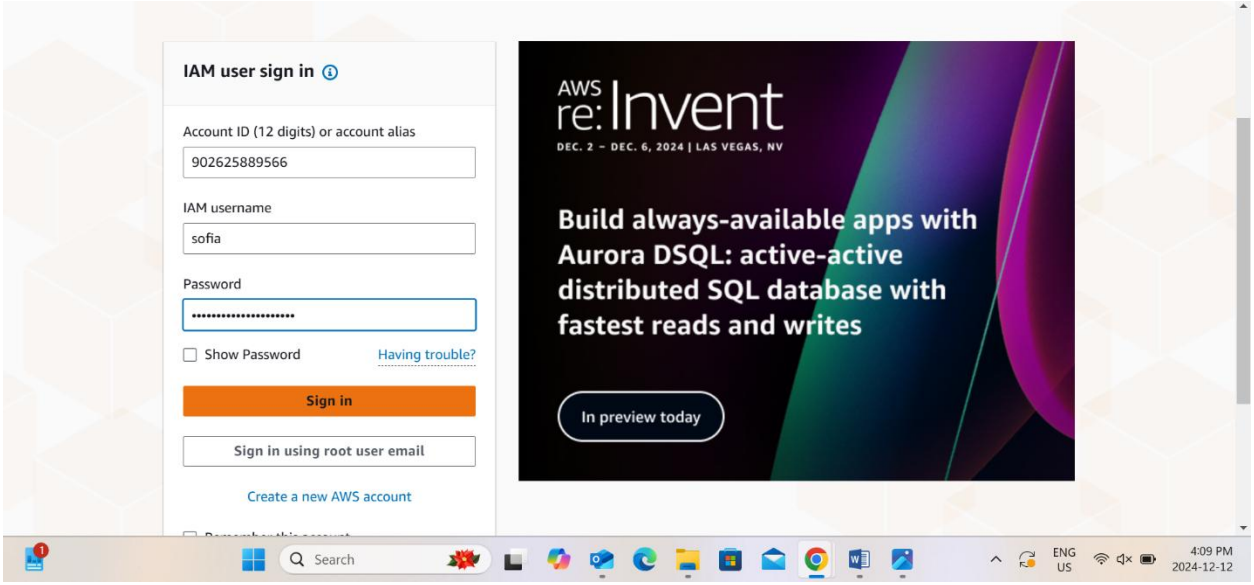


AWS-Cloud-Security-Project

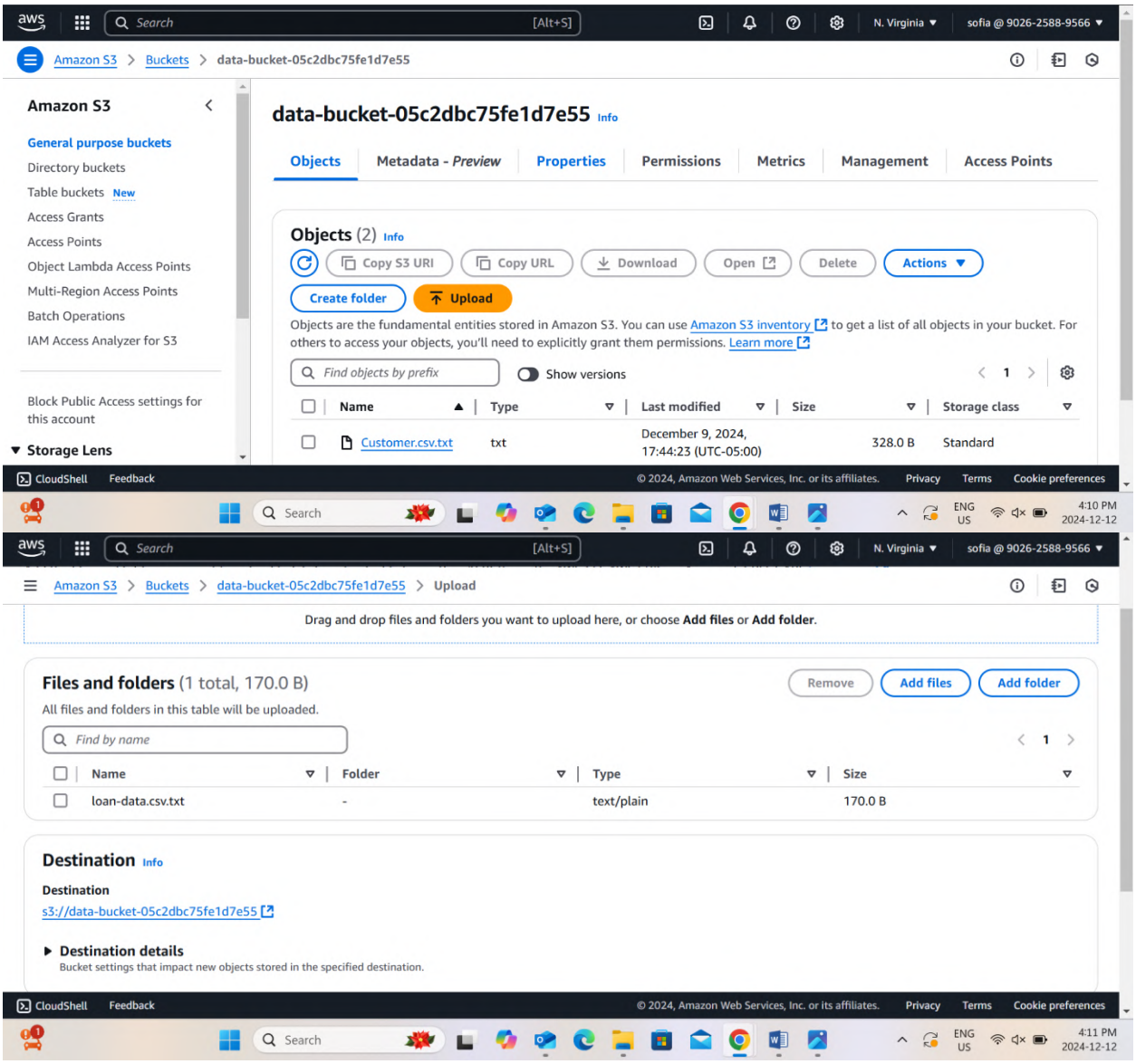


AWS-Cloud-Security-Project

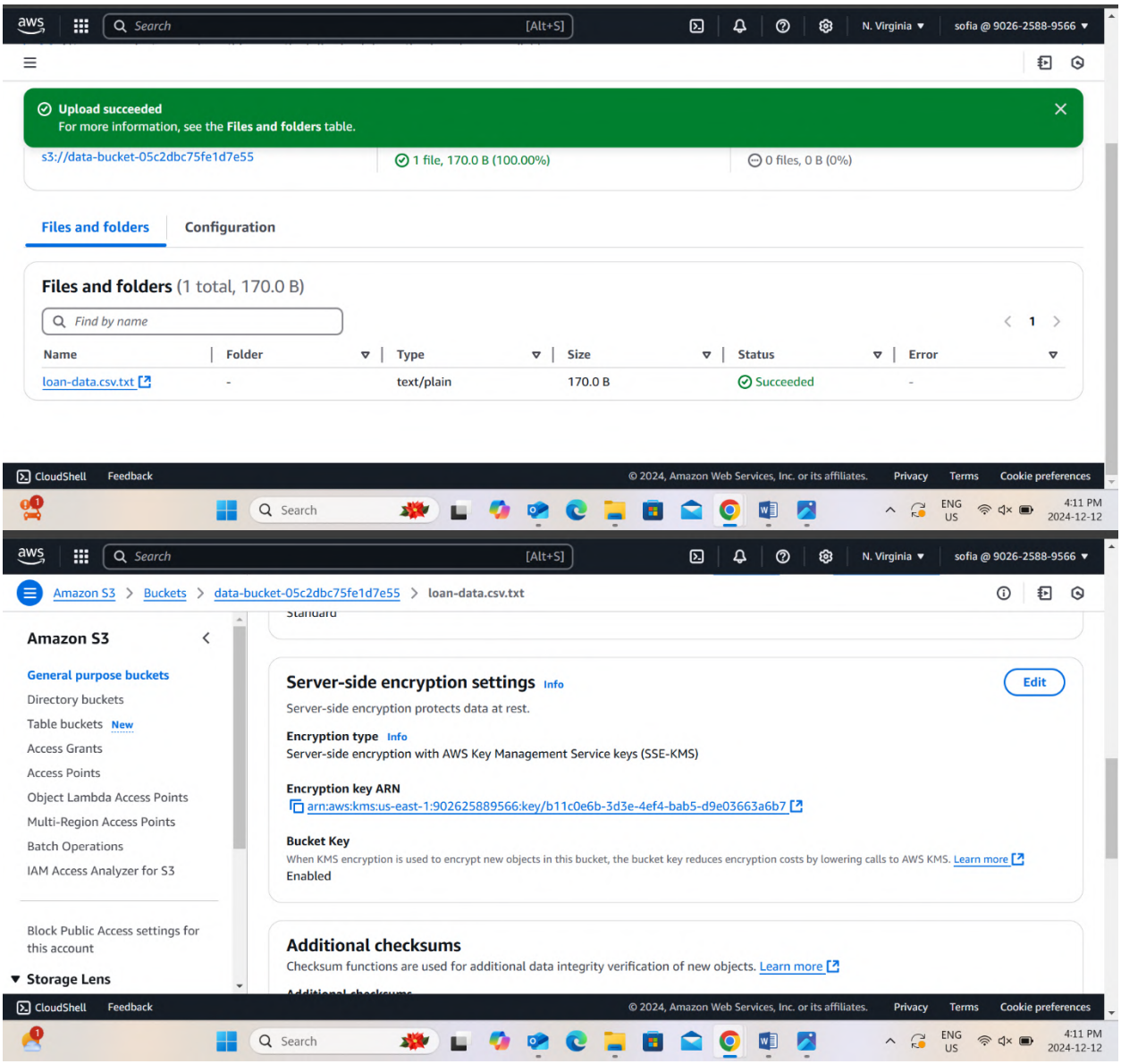




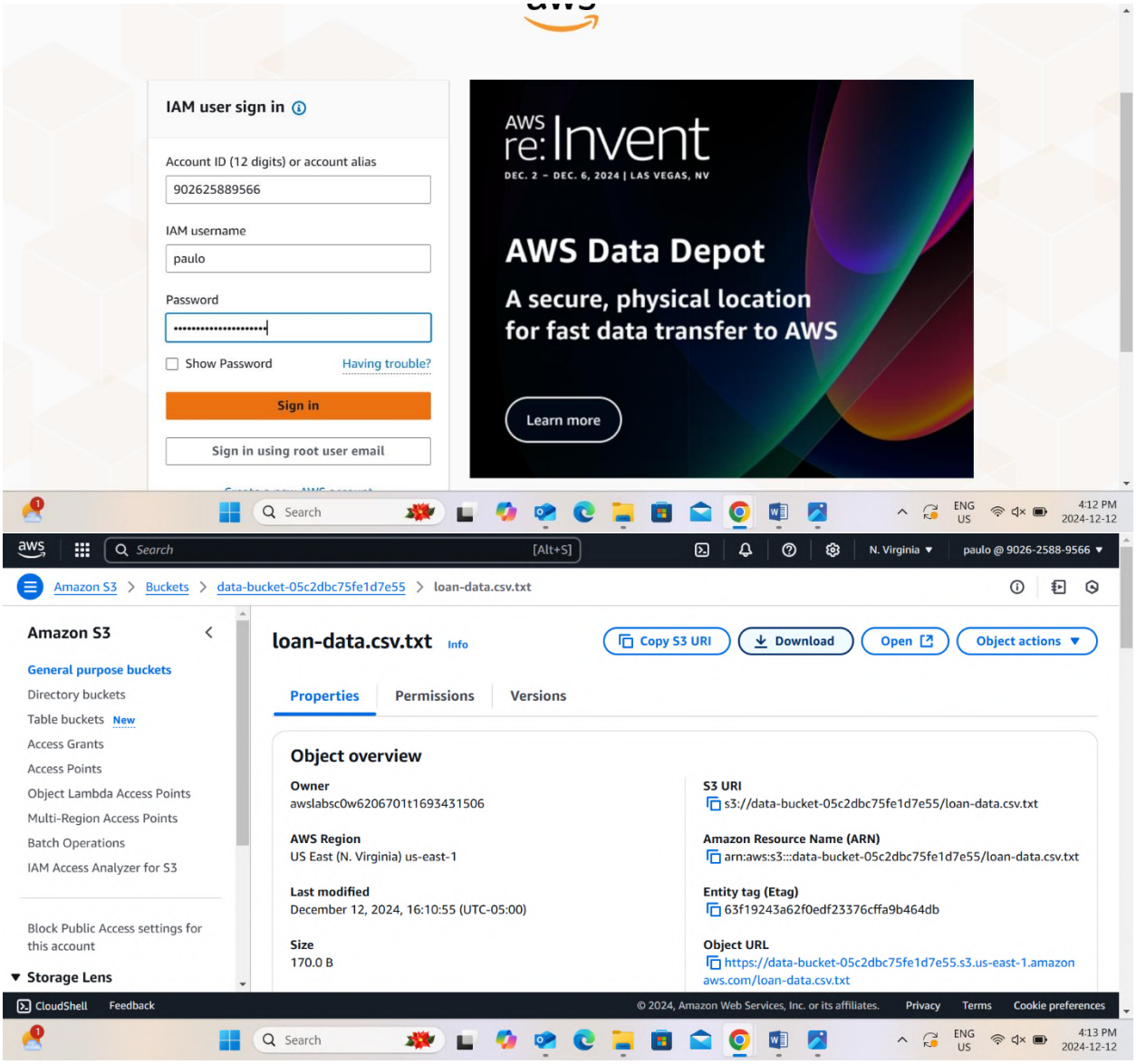
AWS-Cloud-Security-Project



AWS-Cloud-Security-Project



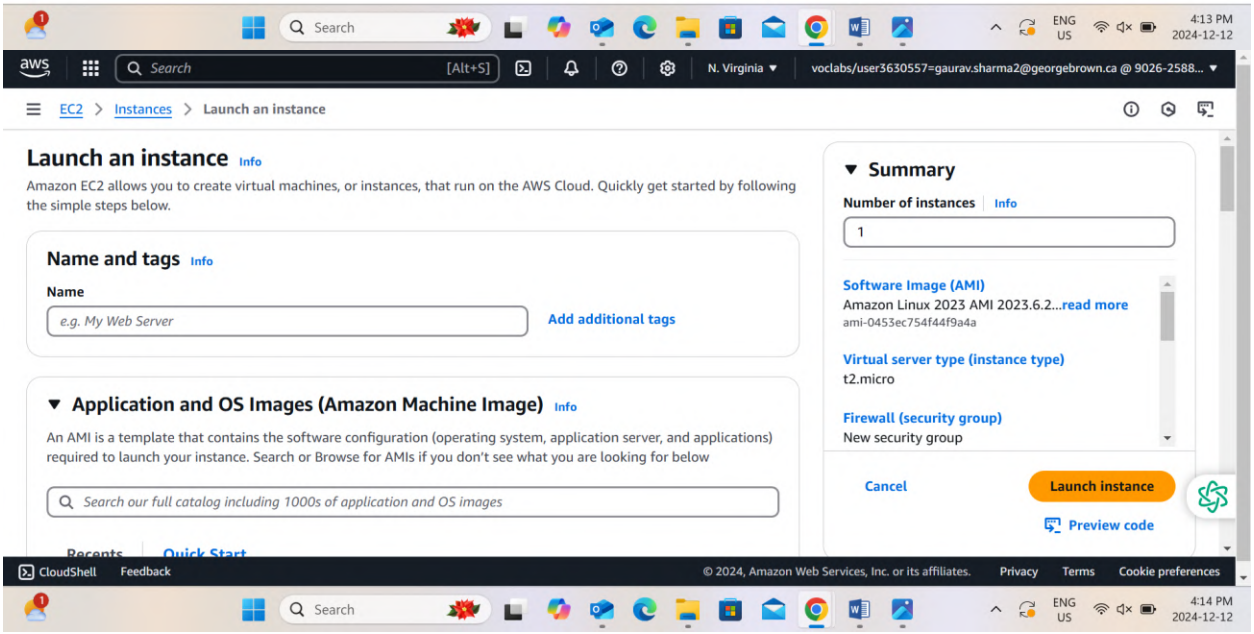
AWS-Cloud-Security-Project



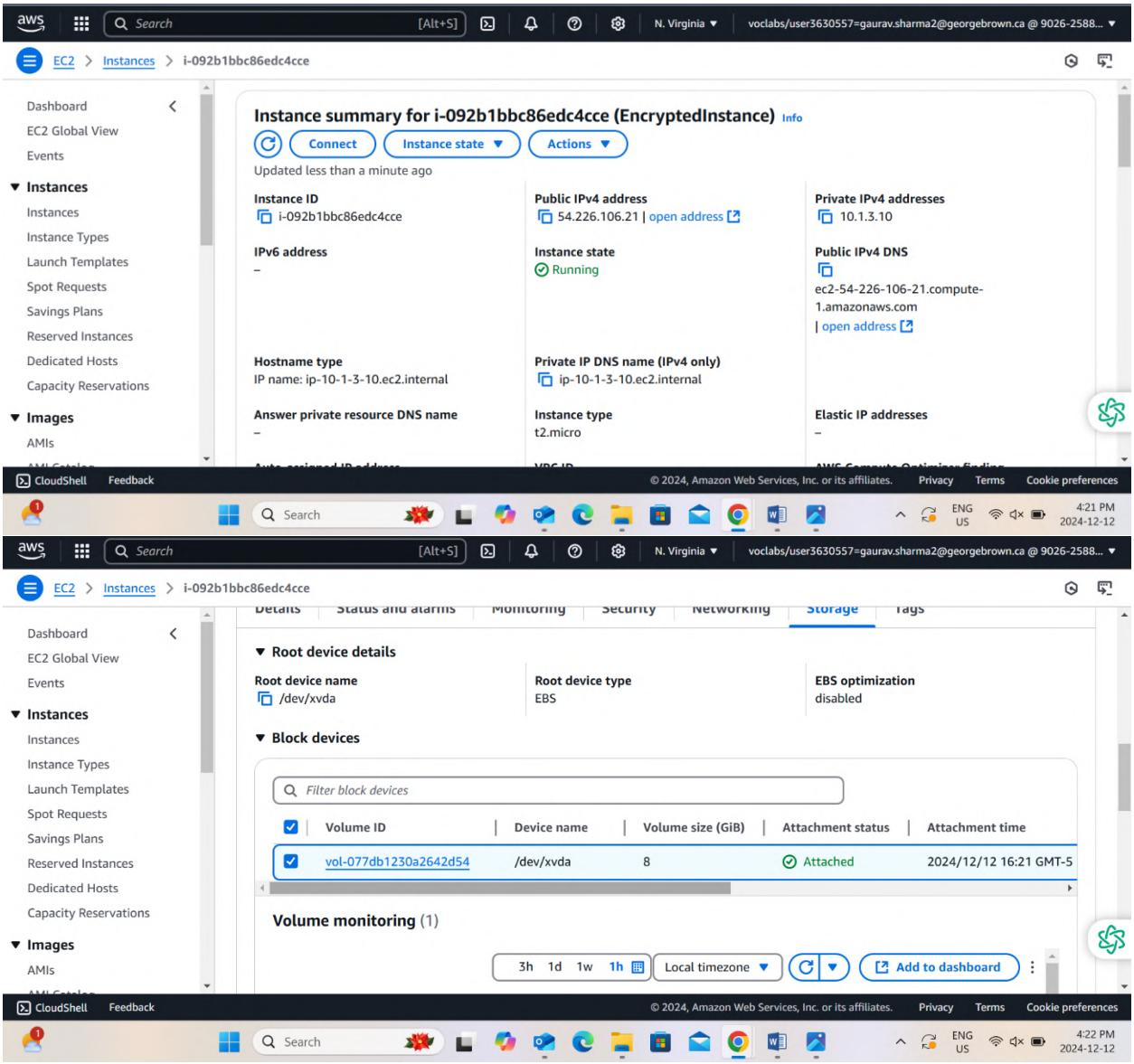
AWS-Cloud-Security-Project

This XML file does not appear to have any style information associated with it. The document tree is shown below.

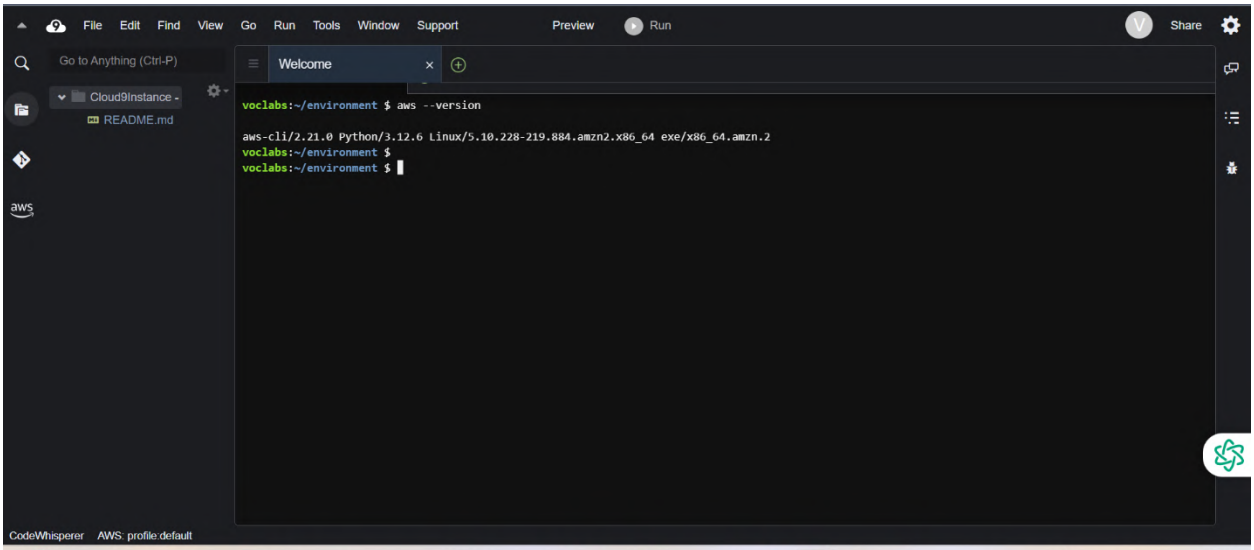

```
<Error>
  <Code>AccessDenied</Code>
  <Message>User: arn:aws:iam::902625889566:user/paulo is not authorized to perform: kms:Decrypt on resource: arn:aws:kms:us-east-1:902625889566:key/b11c0e6b-3d3e-4ef4-bab5-d9e03663a6b7 because no identity-based policy allows the kms:Decrypt action</Message>
  <RequestId>EJ76VQWEE1RH5XW2</RequestId>
  <HostId>yC10I7ObIDlzpBX89kH9HZuVtZgNjAbu3gImL7yJIkE+MFRi55z9MOnUs6IU8NiEZ7yg8fo4YFQ=</HostId>
</Error>
```

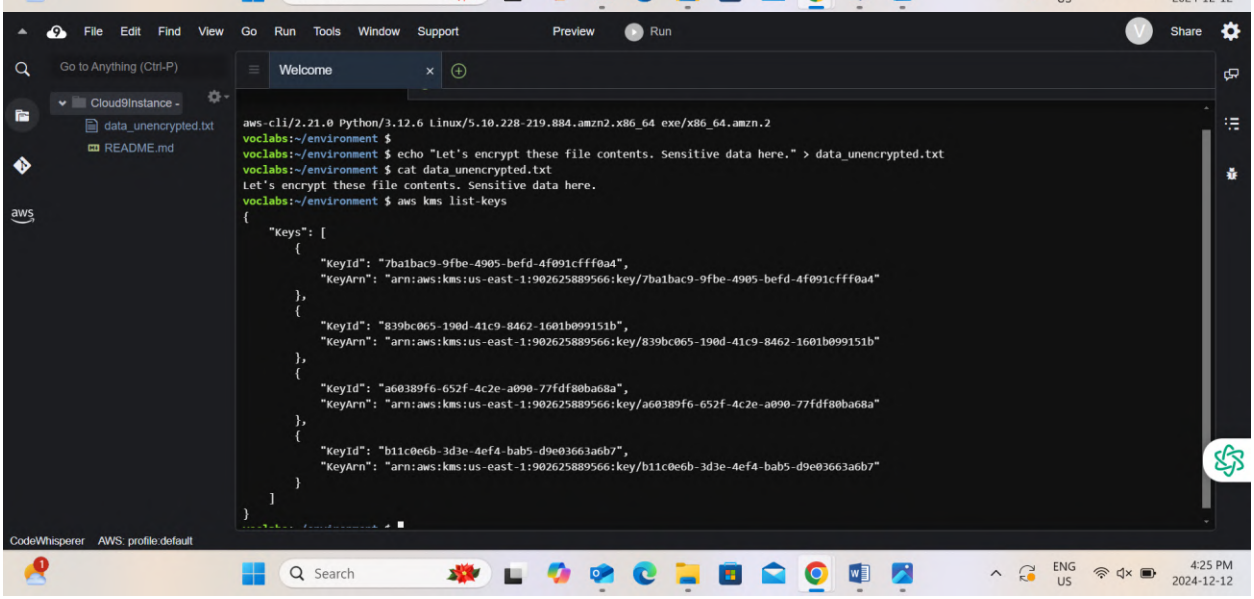



AWS-Cloud-Security-Project

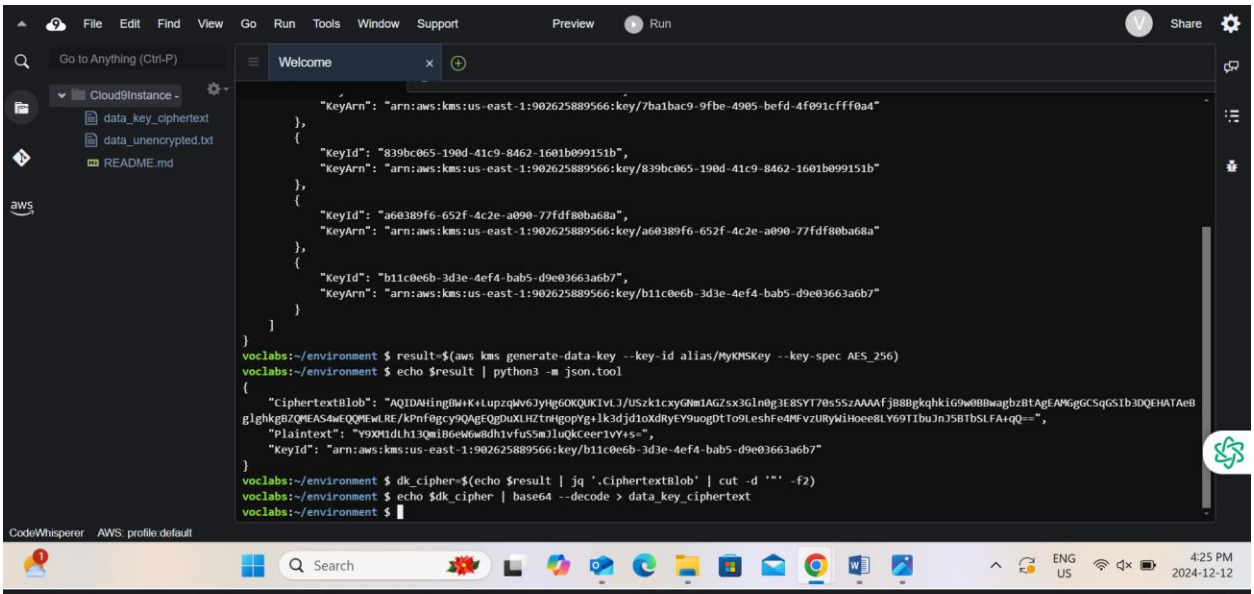


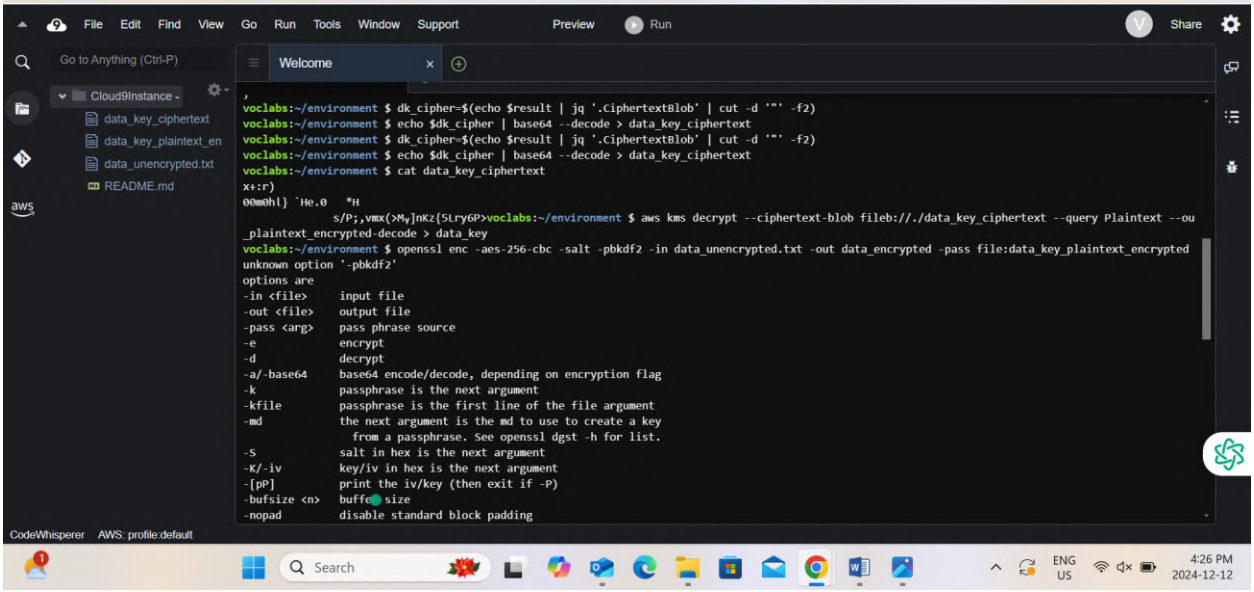
AWS-Cloud-Security-Project



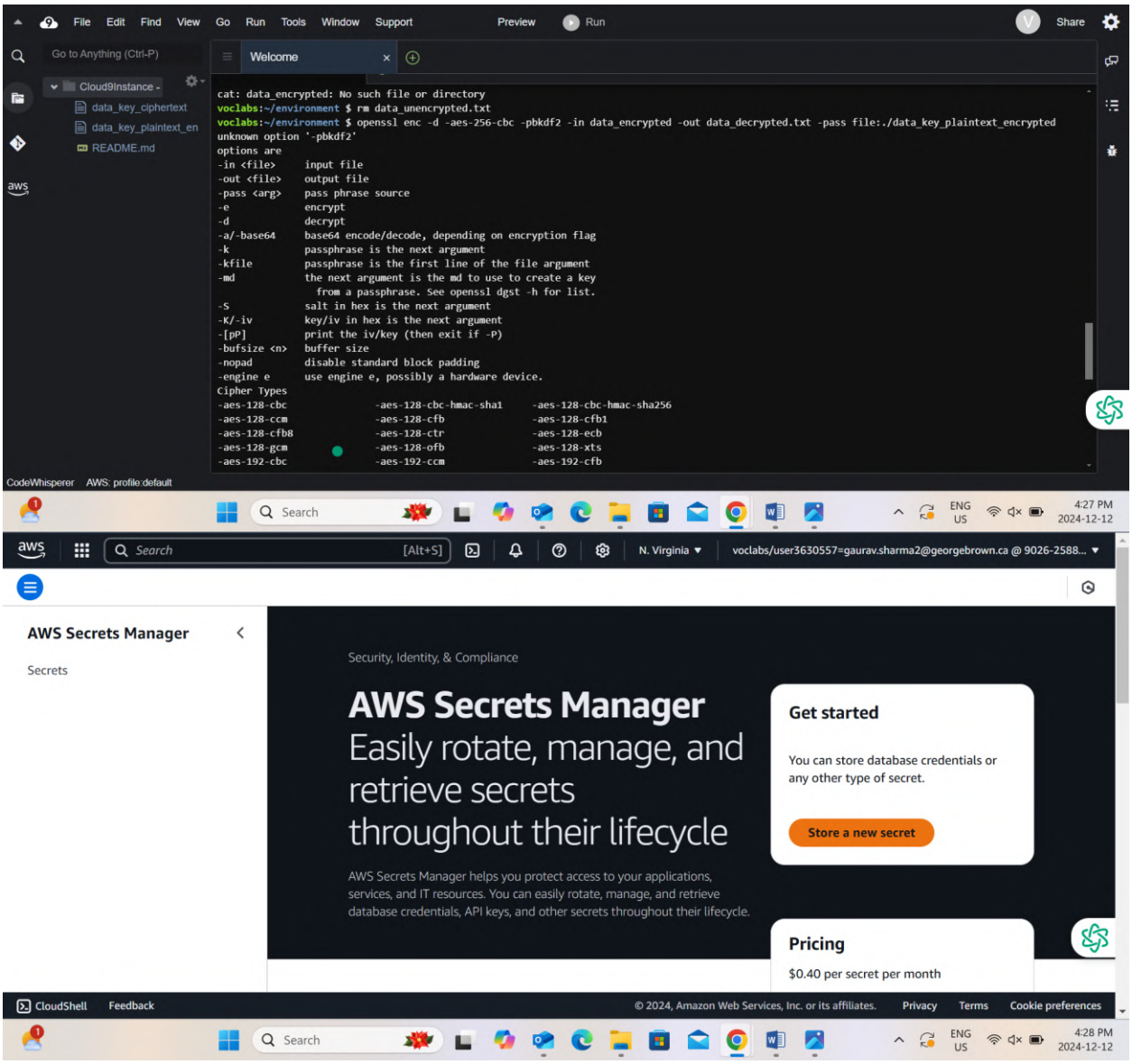


AWS-Cloud-Security-Project

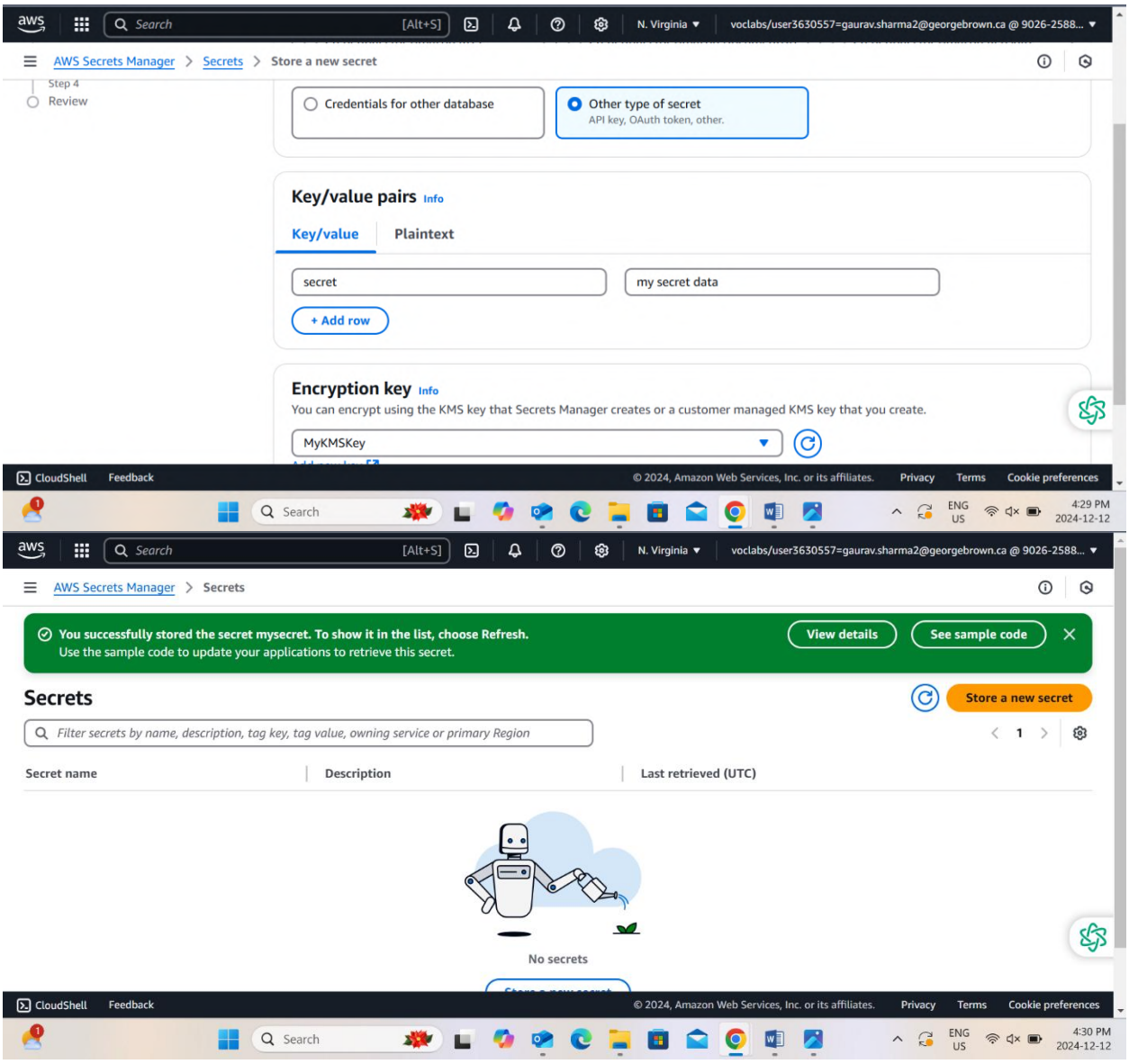


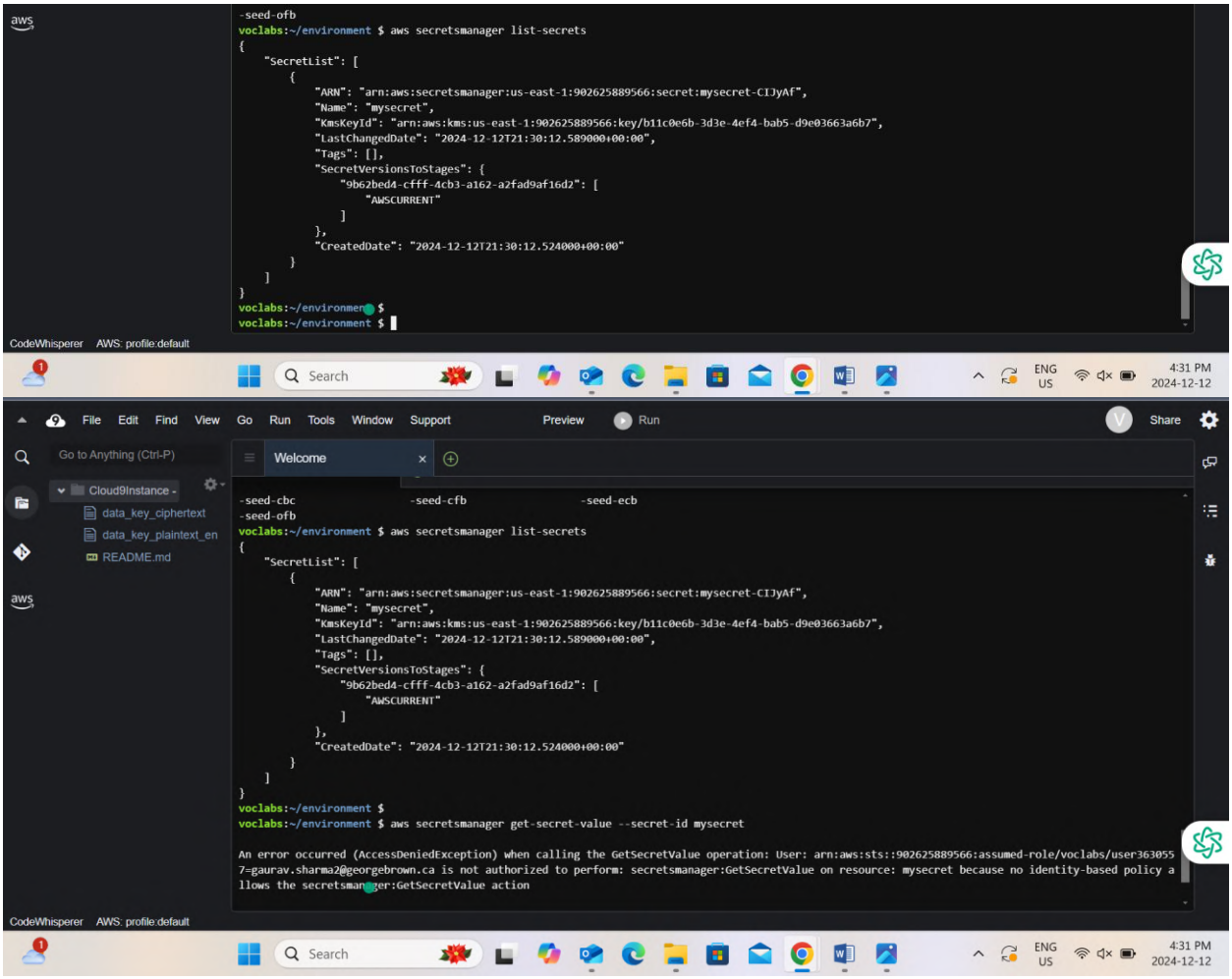


AWS-Cloud-Security-Project



AWS-Cloud-Security-Project





Question: In this lab, does your use of AWS KMS result in additional cost in the account? If so, what usage would you be charged for?

Yes, using AWS KMS incurs additional costs in your account.

Charges for AWS KMS Usage:

Key Usage: Each request to AWS KMS to encrypt, decrypt, or generate a data key incurs a cost.

Customer-Managed Keys:

Creation and storage of customer-managed keys are free. However, you pay $1 per month for each key if it is actively used.

Key Rotation: If enabled, automatic key rotation is included at no additional cost.

Secrets Manager: Storing secrets in Secrets Manager incurs charges starting at $0.40 per secret per month.

Usage Scenarios Resulting in Costs:

Encrypting and decrypting secrets with AWS KMS.

Retrieving secrets using the Secrets Manager API.

Generating data keys for encryption operations.

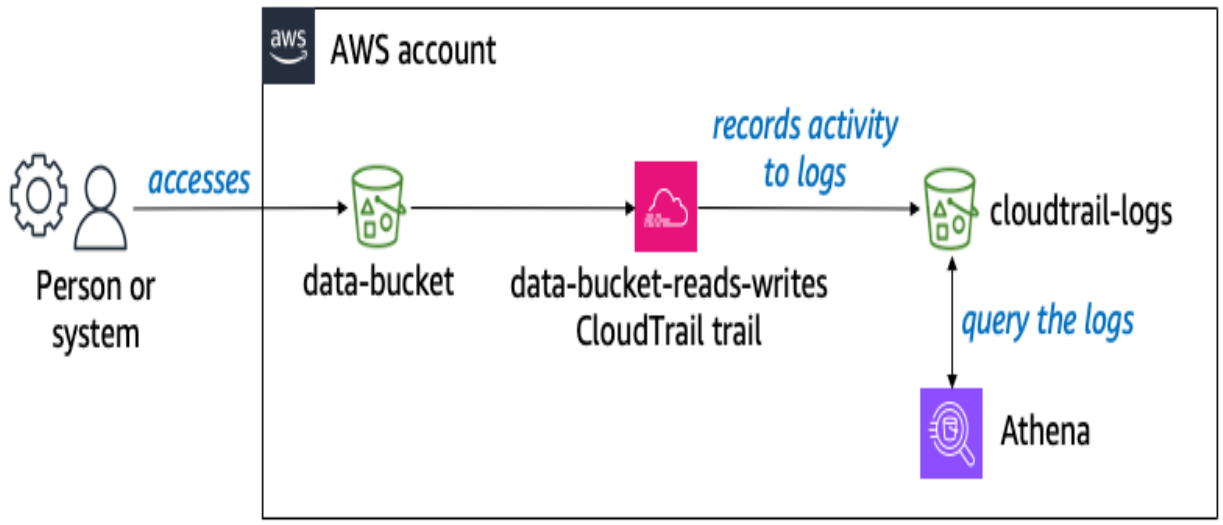
Phase 4: Monitoring and logging

Task 4.1: Use CloudTrail to record Amazon S3 API calls

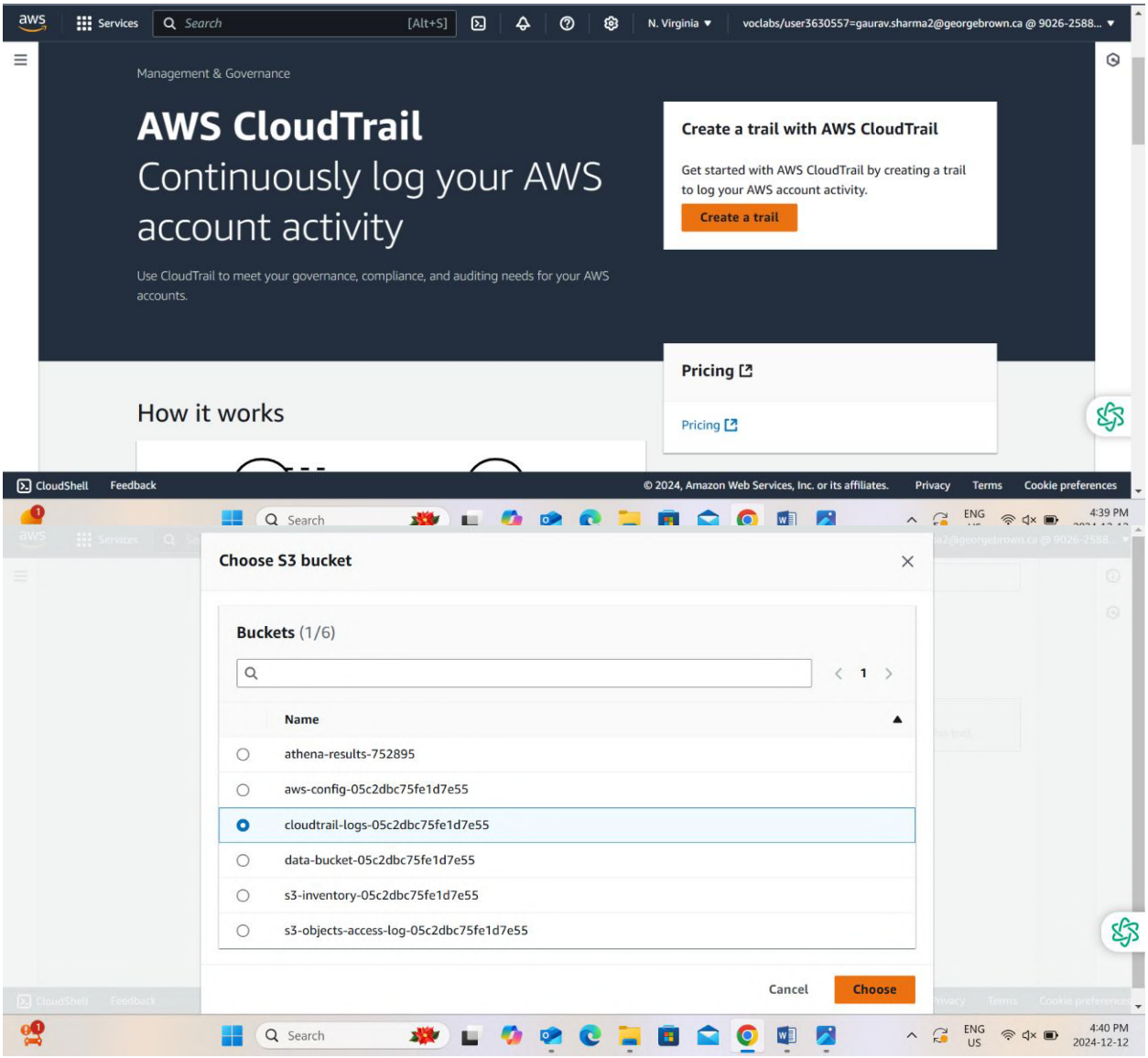
Task 4.2: Use CloudWatch Logs to monitor secure logs

Task 4.3: Create a CloudWatch alarm to send notifications for security incidents

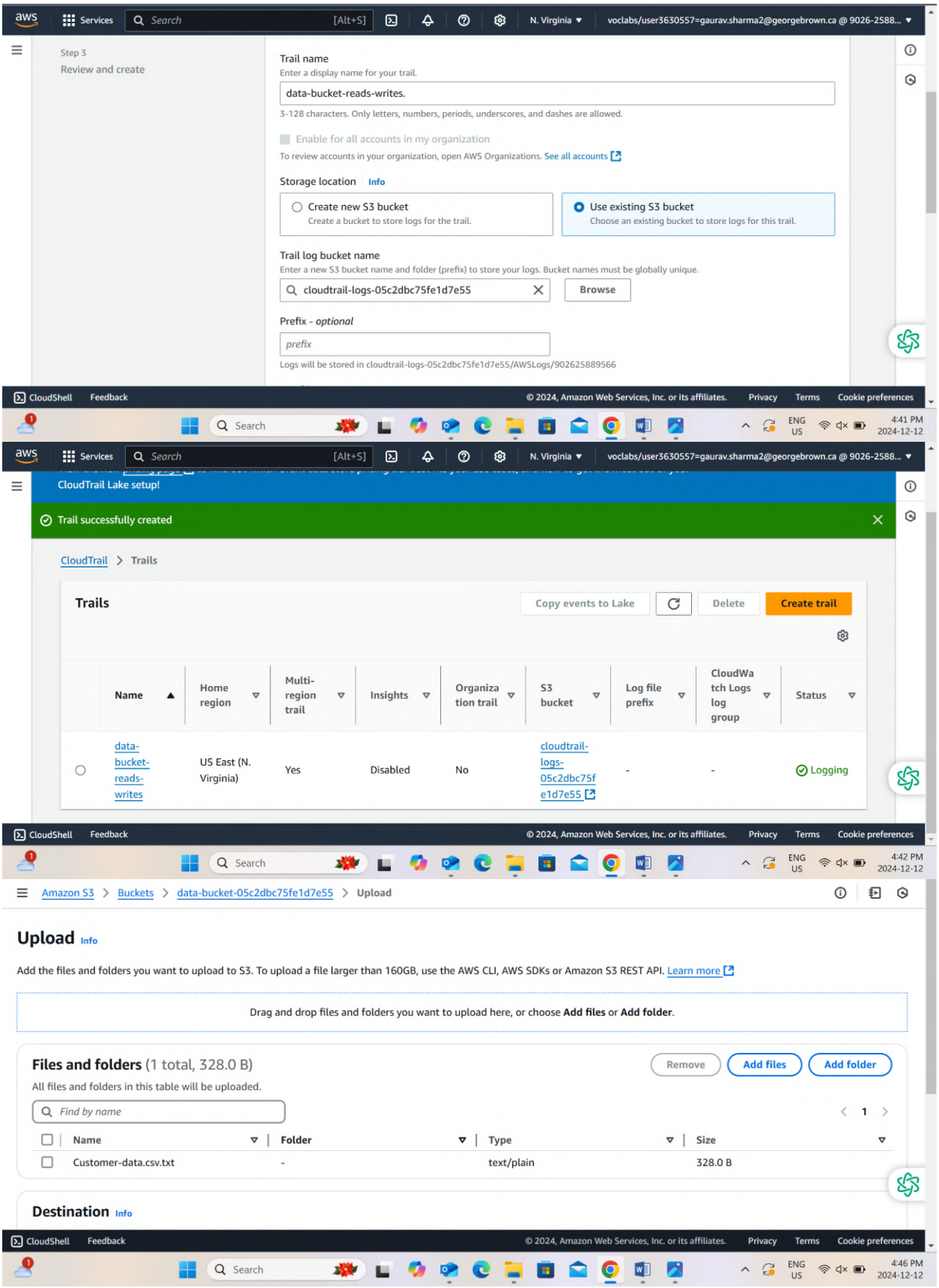
Task 4.4: Configure AWS Config to assess security settings and remediate the configuration of AWS resources



AWS-Cloud-Security-Project

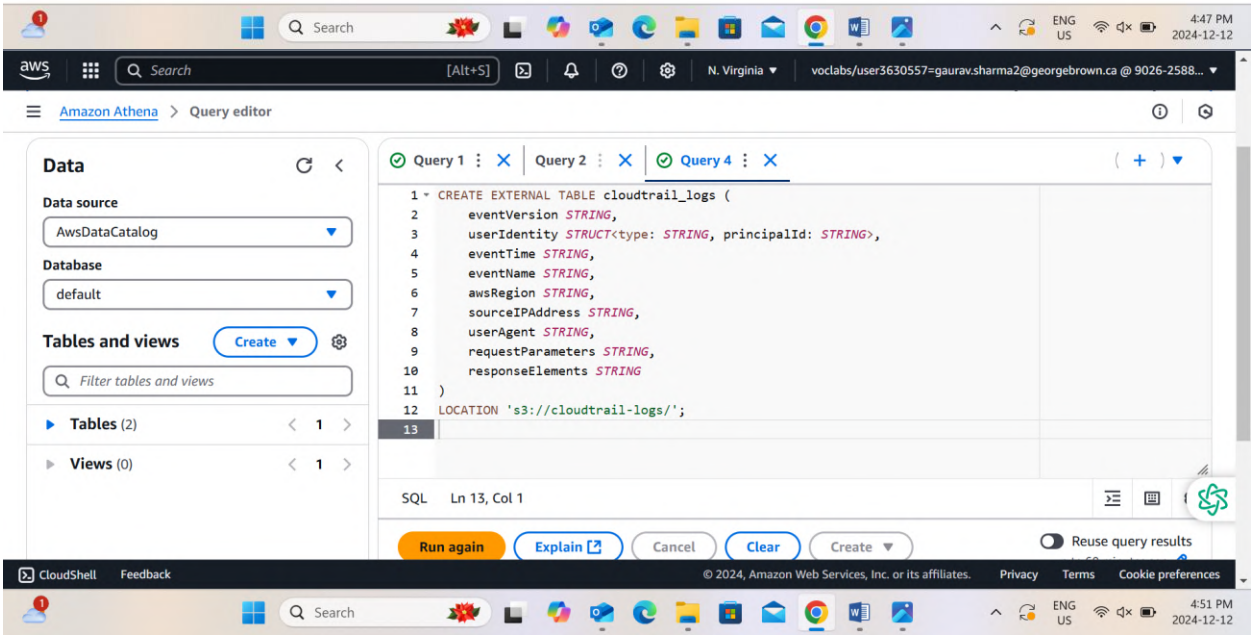


AWS-Cloud-Security-Project

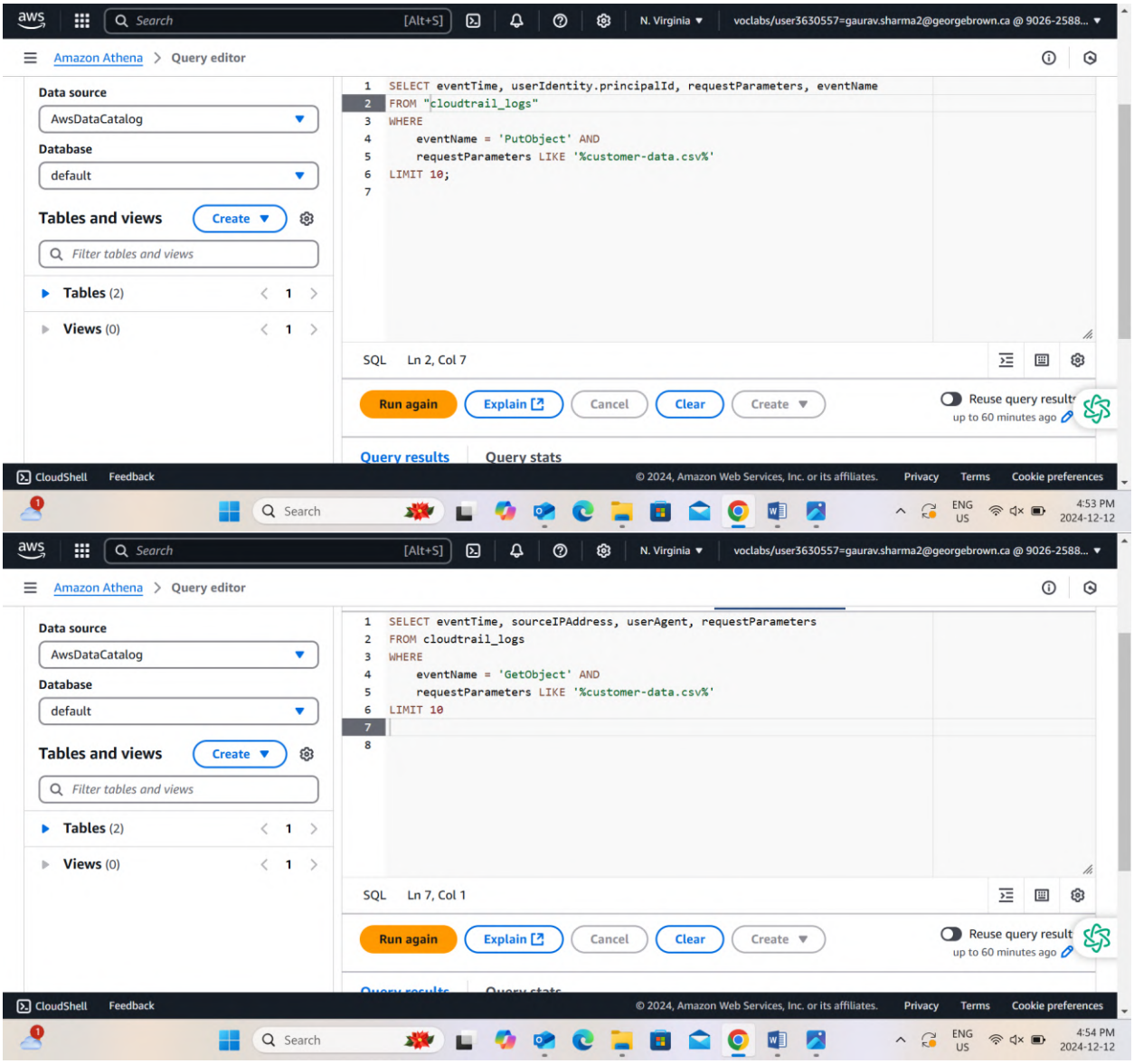


AWS-Cloud-Security-Project

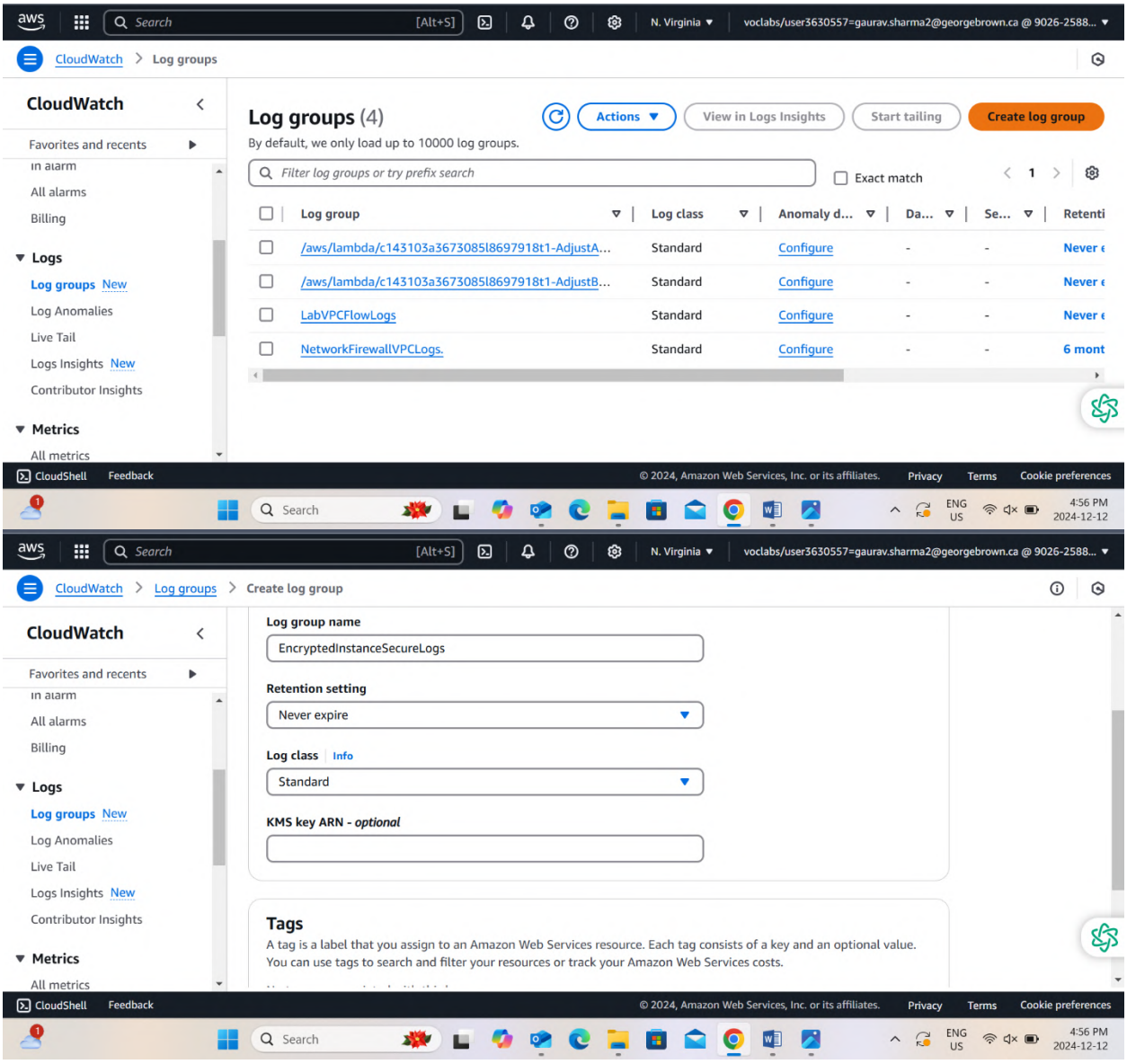
```
CustomerID,First Name,Last Name,Join Date,Street Address,City,State,Phone
1,Alejandro,Rosalez,12/12/2013,123 Main St.,Any Town,MD,301-555-0158
2,Jane,Doe,10/5/2014,456 State St.,Anywhere,WA,360-555-0163
3,John,Stiles,9/20/2016,1980 8th St.,Nowhere,NY,914-555-0122
4,Li,Juan,6/29/2011,1323 22nd Ave.,Anytown,NY,914-555-0149
```



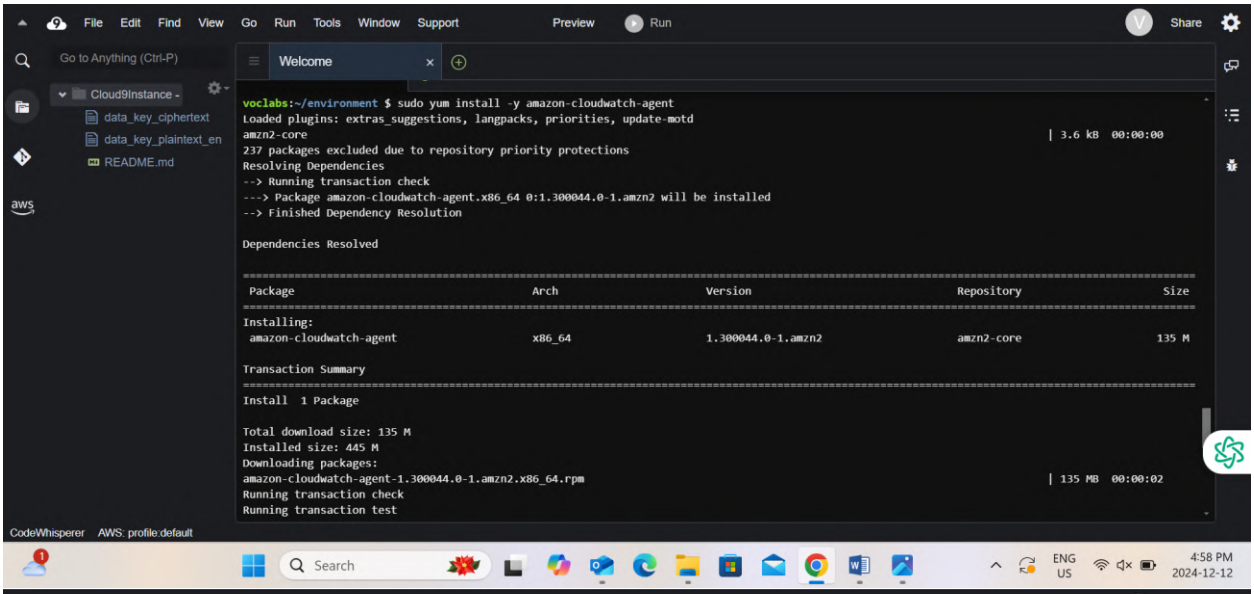
AWS-Cloud-Security-Project

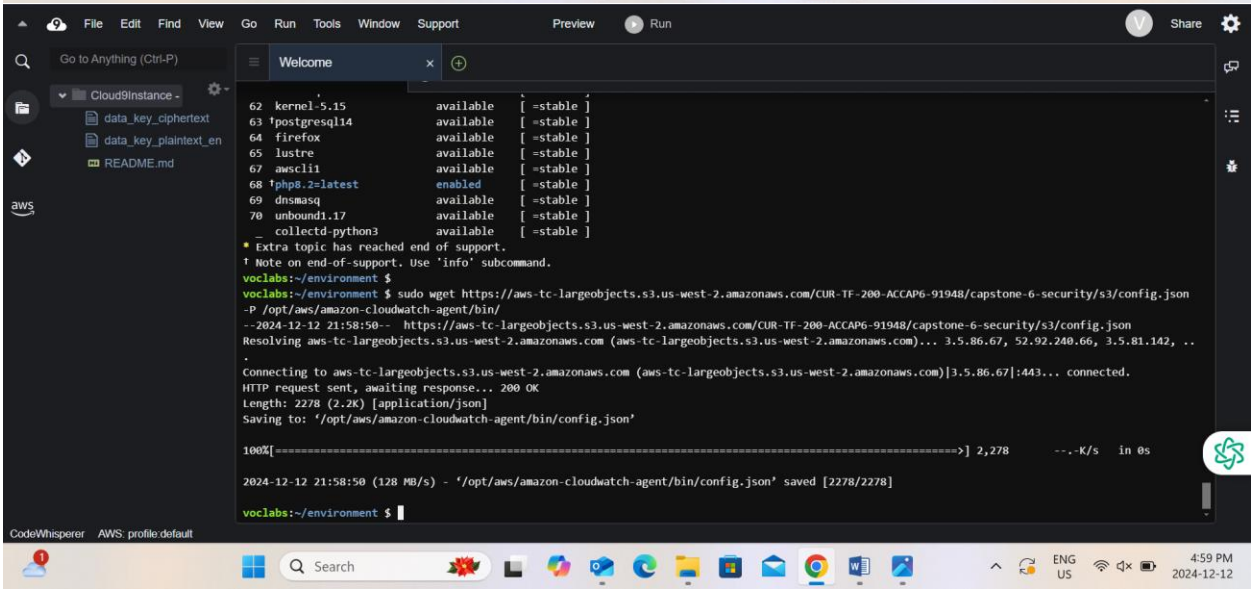


AWS-Cloud-Security-Project

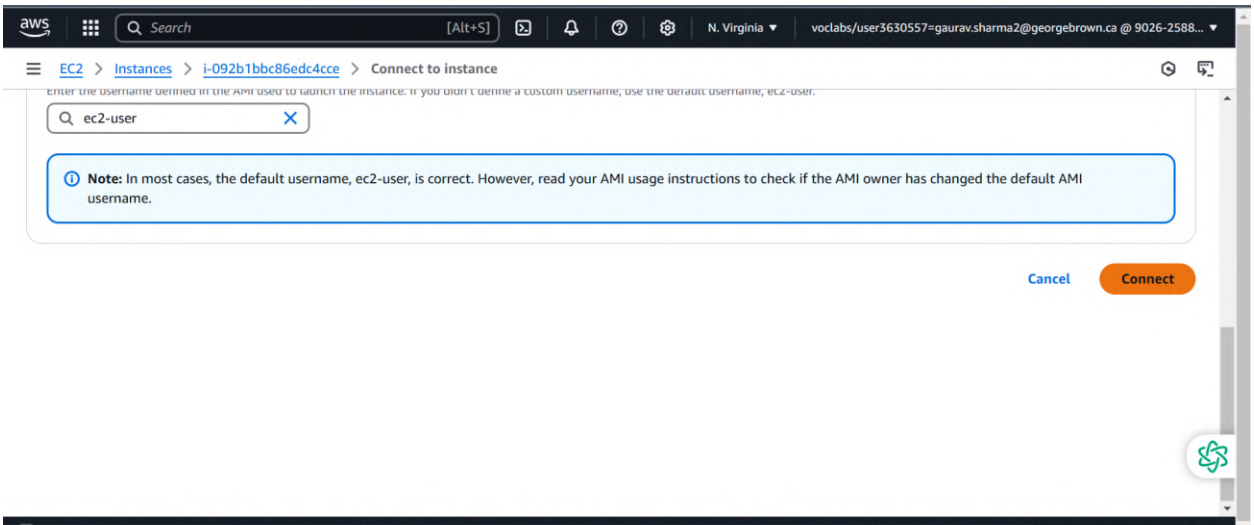


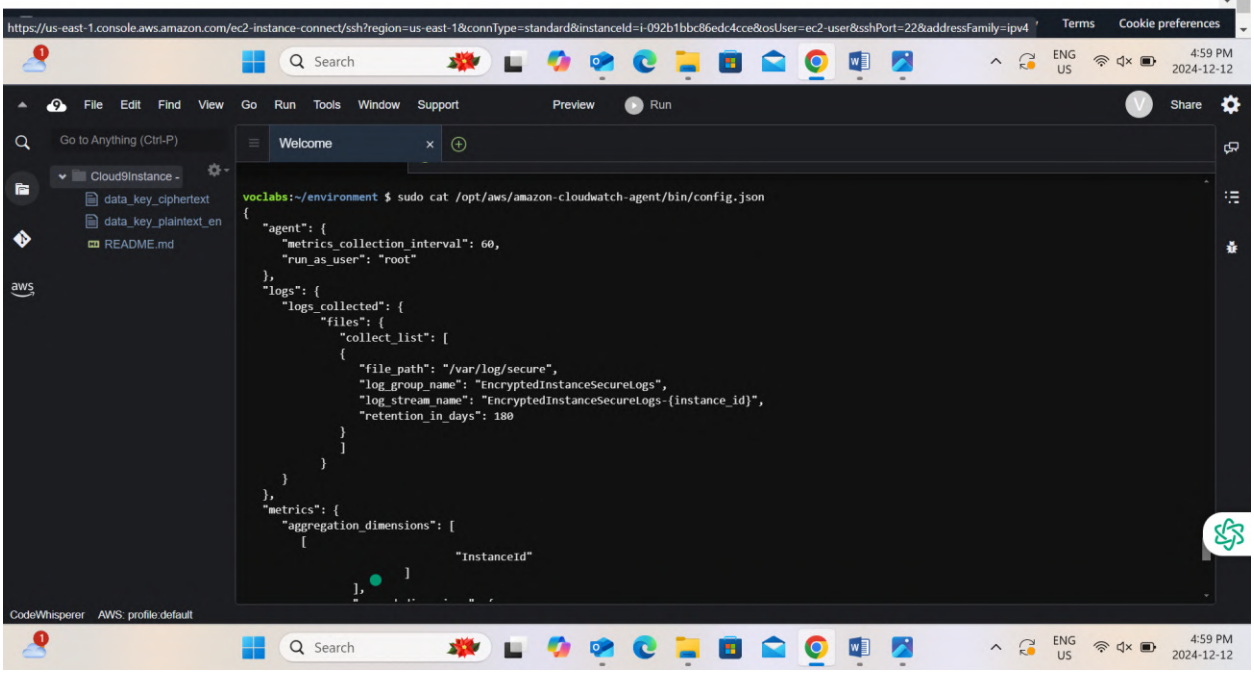
AWS-Cloud-Security-Project



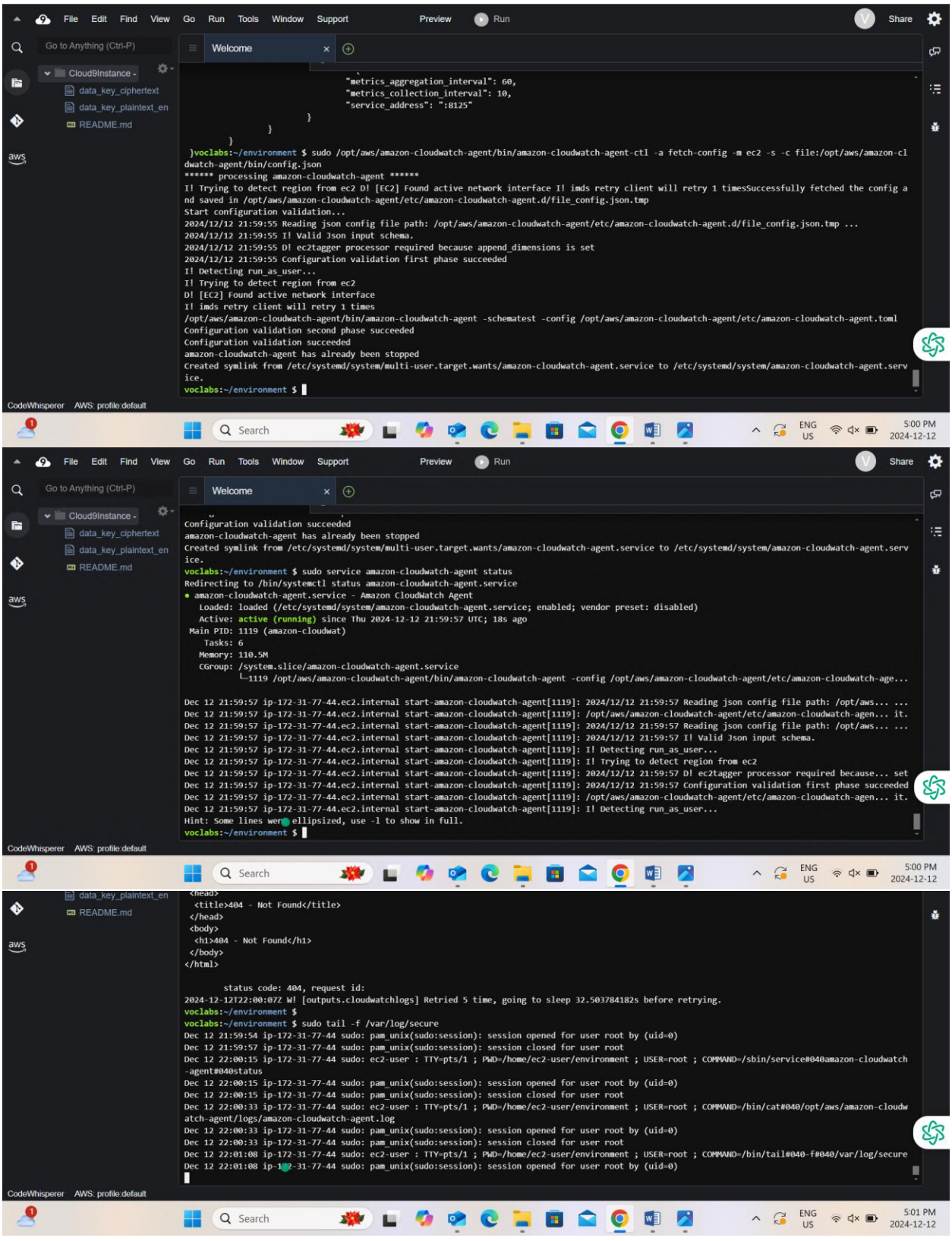


AWS-Cloud-Security-Project

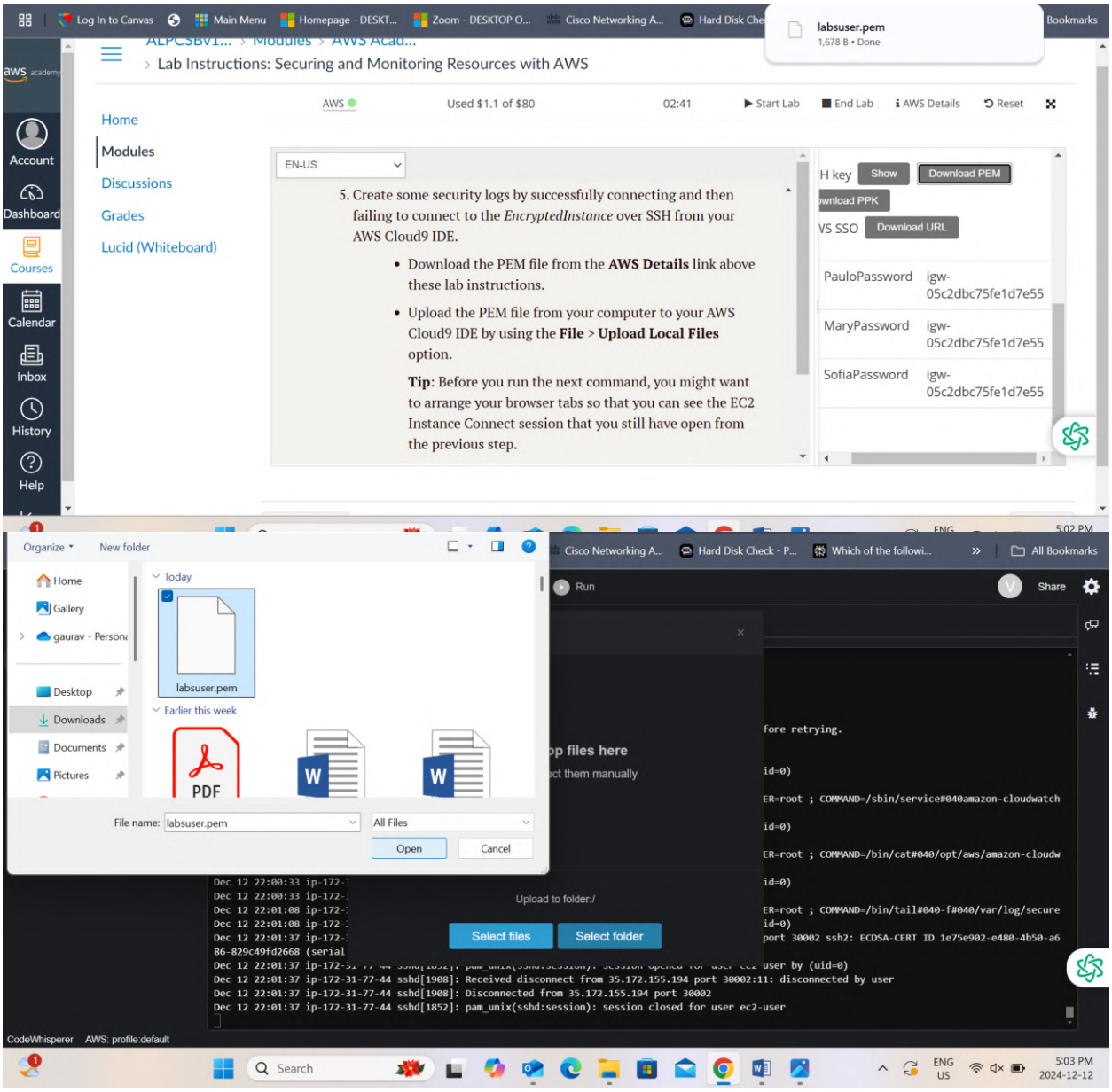




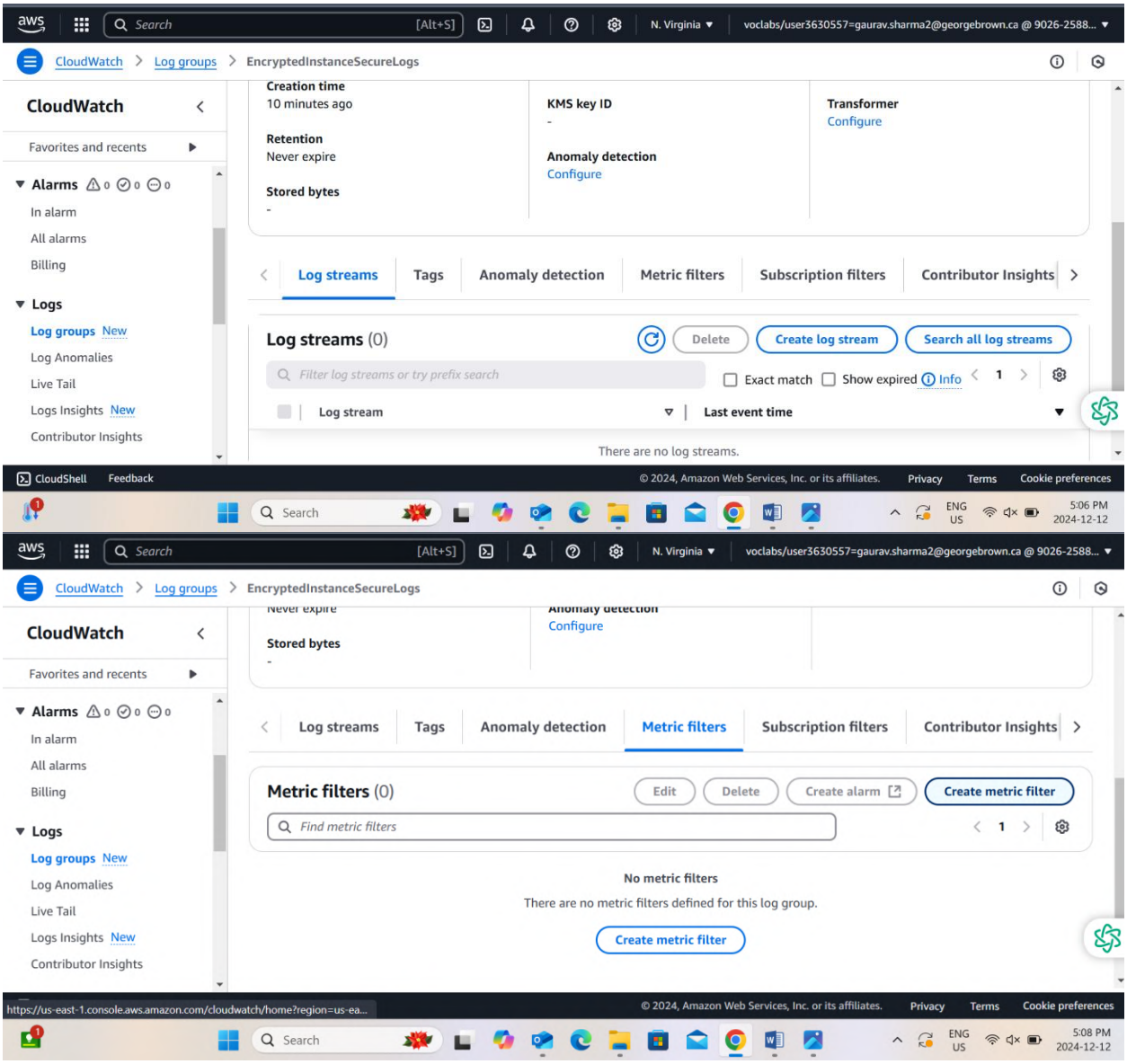
AWS-Cloud-Security-Project



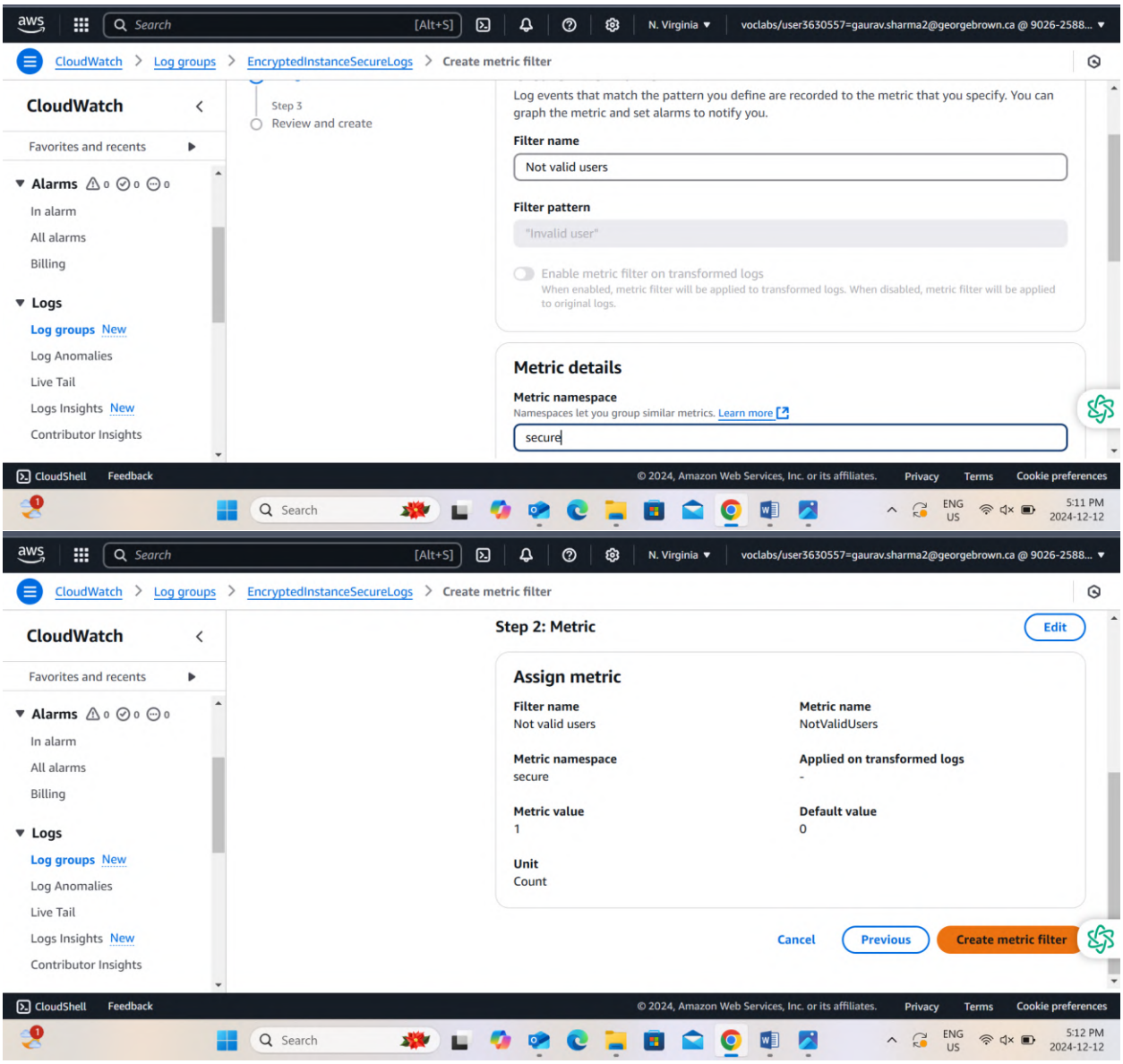
AWS-Cloud-Security-Project



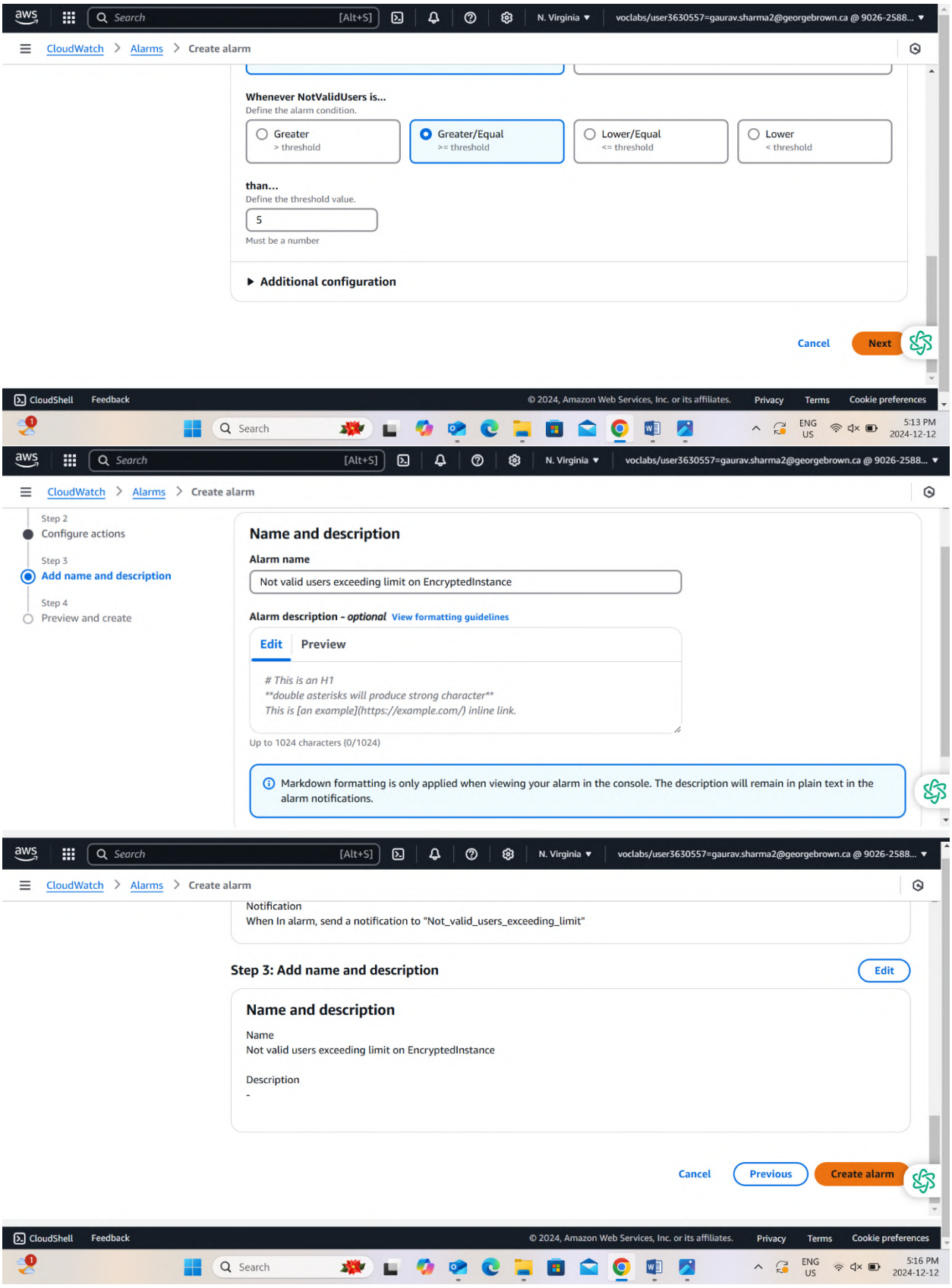
AWS-Cloud-Security-Project



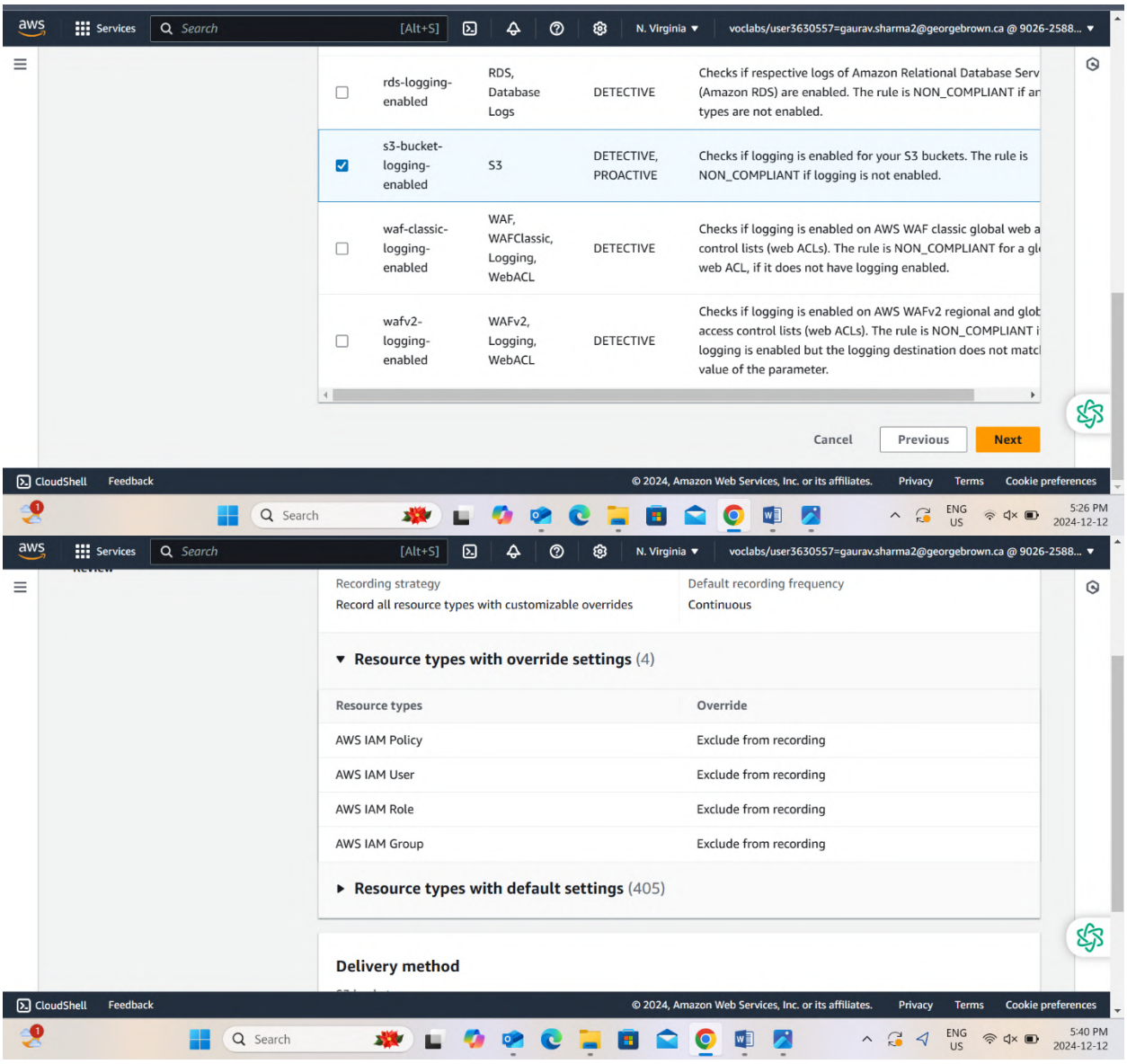
AWS-Cloud-Security-Project



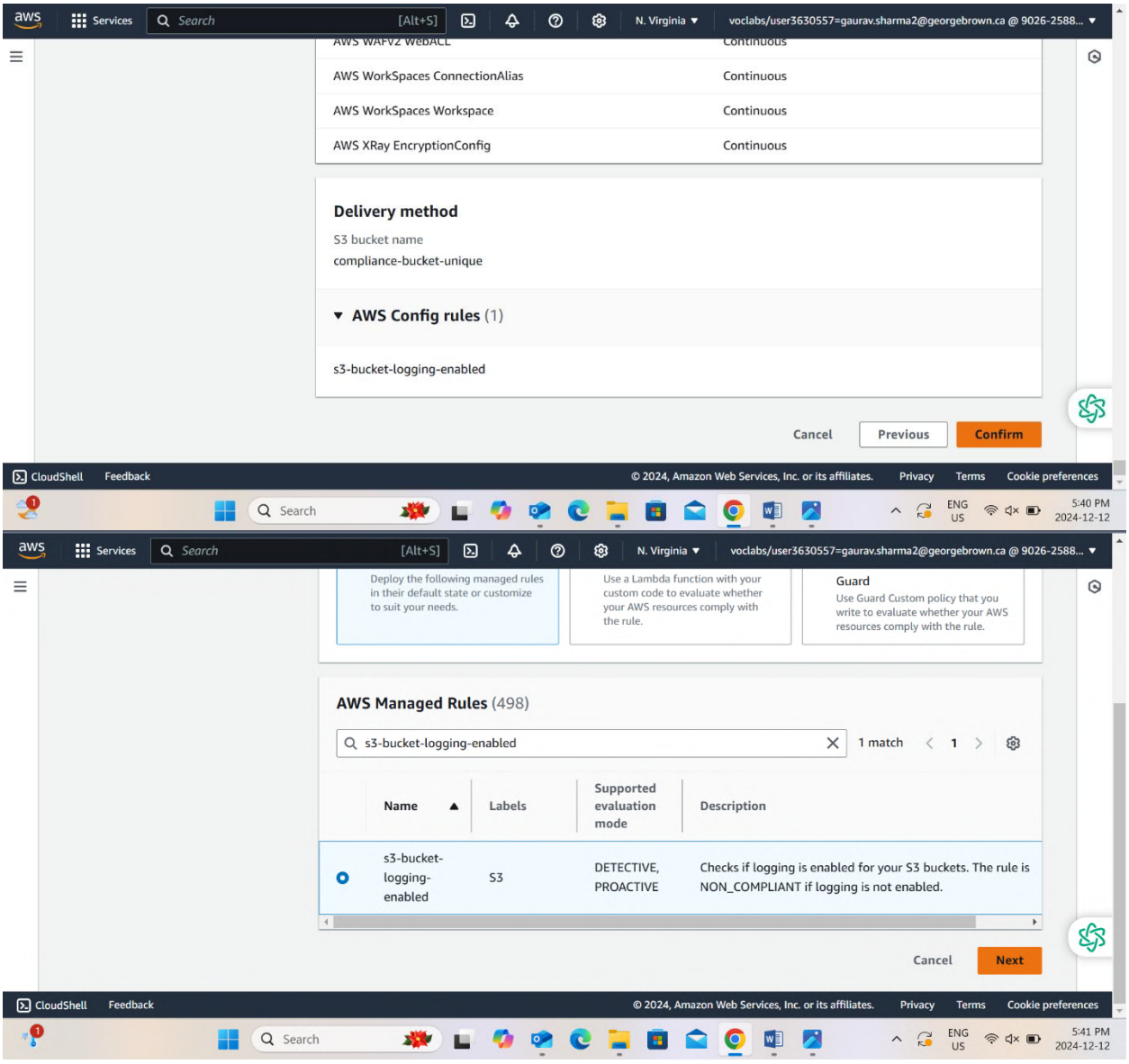
AWS-Cloud-Security-Project



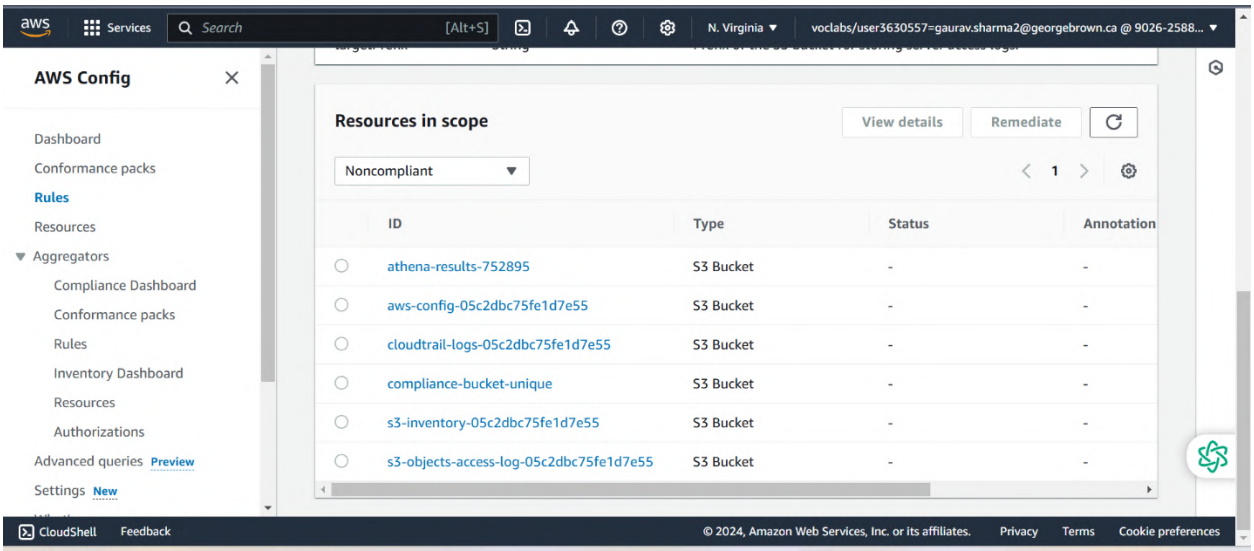
AWS-Cloud-Security-Project

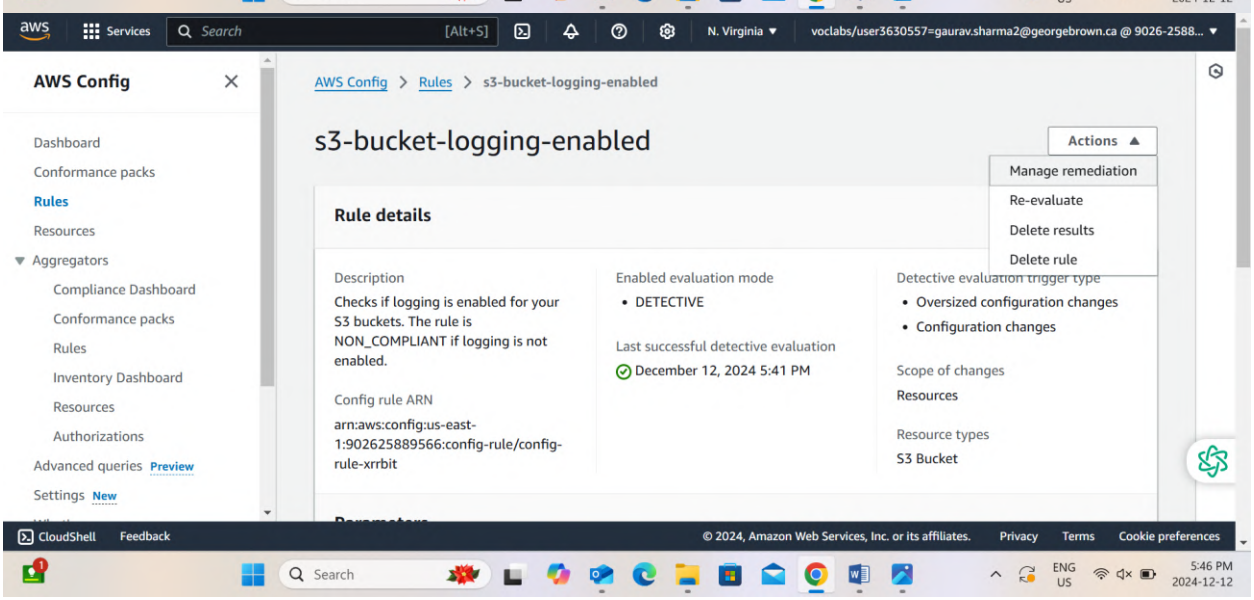


AWS-Cloud-Security-Project

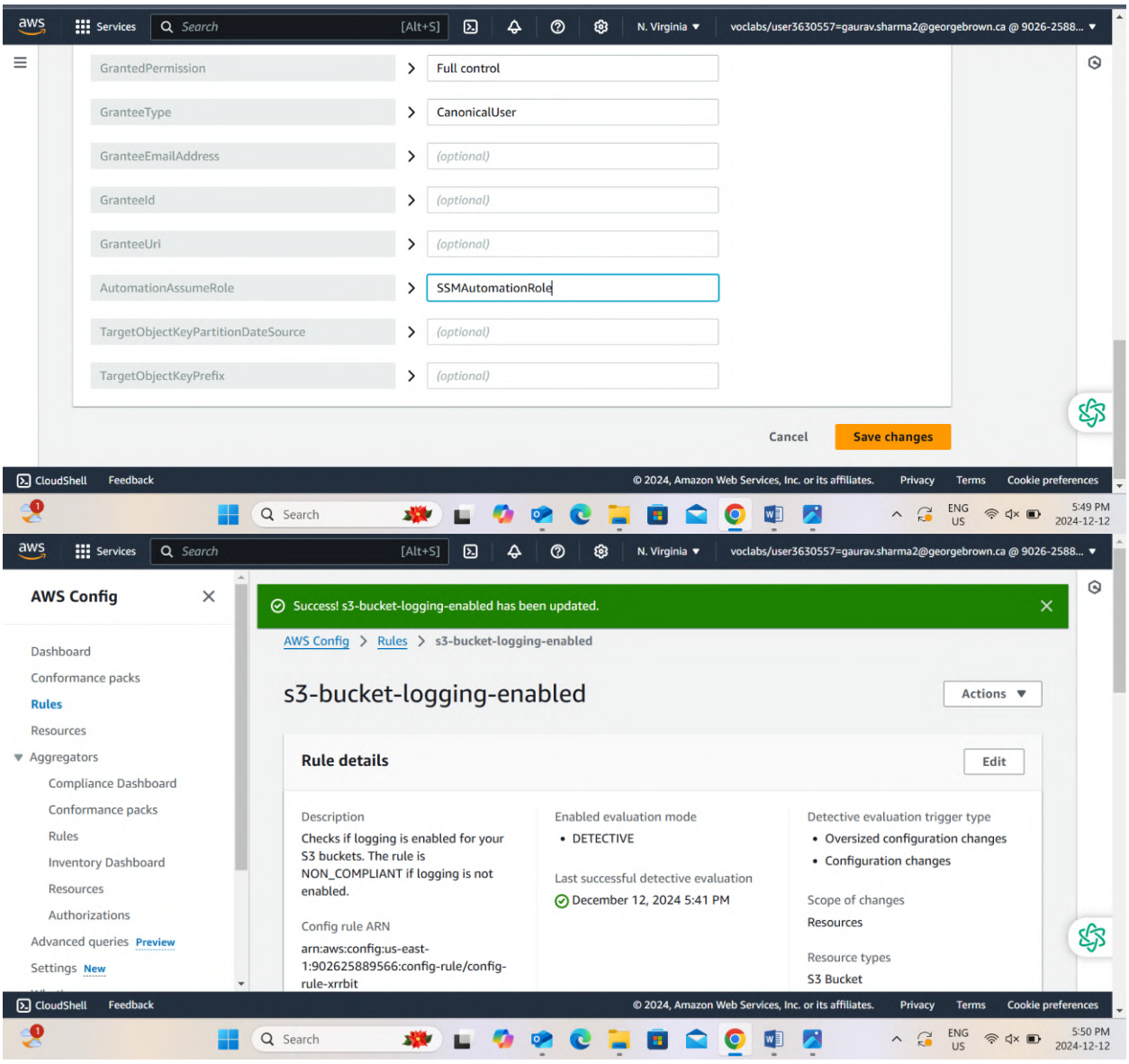


AWS-Cloud-Security-Project





AWS-Cloud-Security-Project



- **Question: In this lab, does your use of CloudTrail, CloudWatch, and AWS Config security features result in additional cost in the account? If so, how much do you estimate that it will cost?**

  Cost Structure:

  - **Management events (read/write) within a single region are free for the first copy.**
  - **Additional copies and data events (e.g., S3 or Lambda function invocations) are charged.**

- **Estimated Cost:**
  - **If you enable only management events and have a moderate amount of activity, the cost might be $0.**
  - **If you log data events, the cost is $0.10 per 100,000 events.**

2. CloudWatch

- **Cost Structure:**
  - **Log ingestion: $0.50 per GB of log data ingested.**
  - **Log storage: $0.03 per GB per month.**
  - **Custom metrics: $0.30 per metric per month.**
  - **Alarms: $0.10 per alarm per month.**
  - **Estimated Cost:**
    - **For the metric filter and alarm in this lab, the cost might be ~$0.40 (one custom metric and one alarm for a month).**
    - **Additional log ingestion costs depend on the volume of logs generated, which could add ~$1–$5 if logs are moderate in size.**

3. AWS Config

- **Cost Structure:**
  - **$0.003 per configuration item recorded.**
  - **Managed rules are charged at $2 per rule per region per month.**
  - **Remediation actions are not directly charged but could incur costs if they invoke other services.**
  - **Estimated Cost:**
    - **For recording resources and one managed rule (e.g., s3-bucket-logging-enabled), the monthly cost might be ~$2–$3, depending on the number of resources recorded.**

Total Estimated Cost

- **If the lab is run over a short period (e.g., a few hours), the costs would be minimal, perhaps under $1–$5.**
- **If these configurations remain active for a full month, the estimated cost would be ~$5–$10, depending on the volume of logs, resources recorded by AWS Config, and usage of managed rules.**