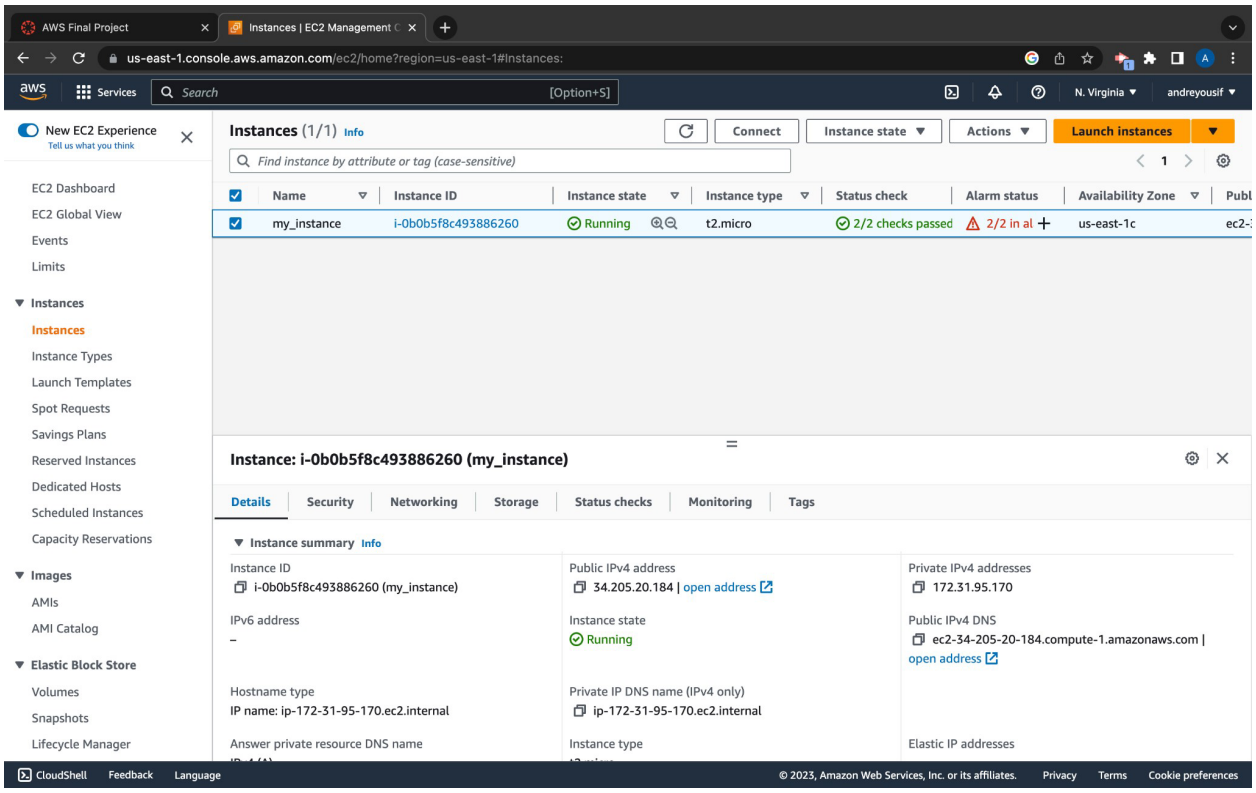
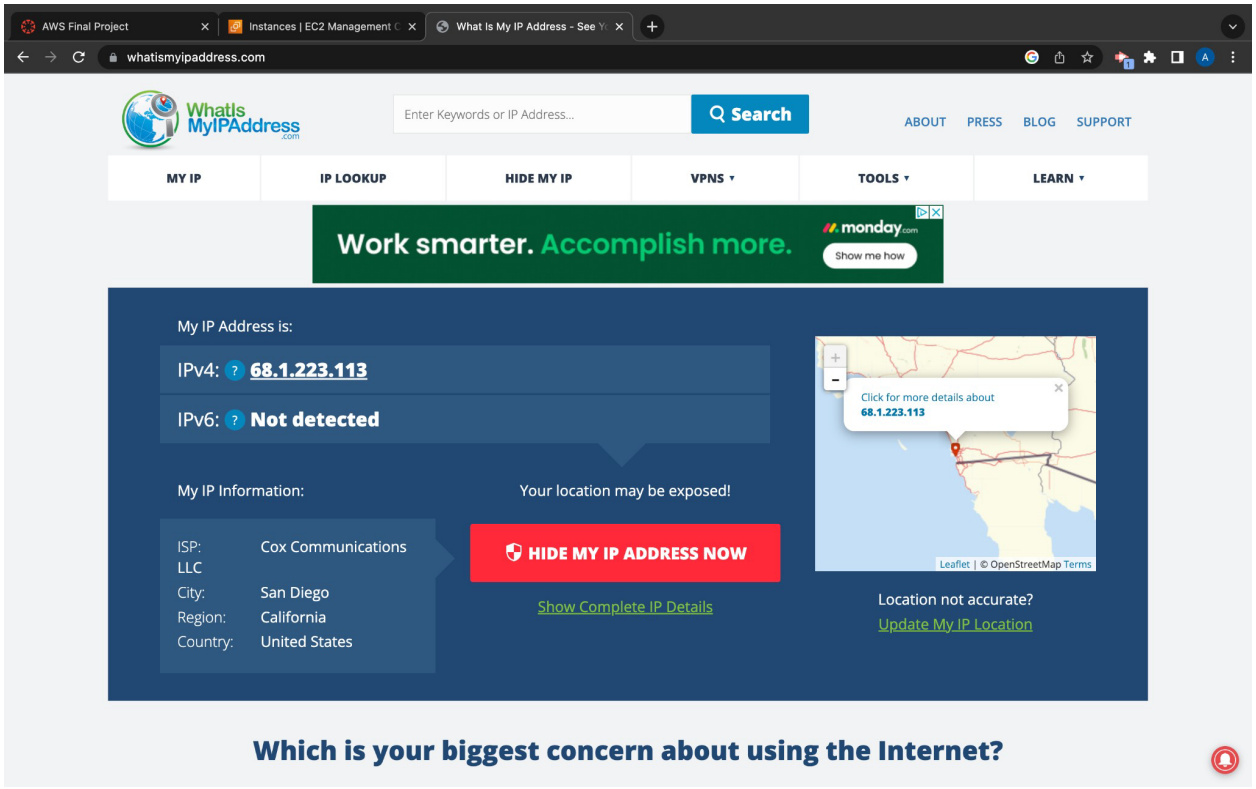
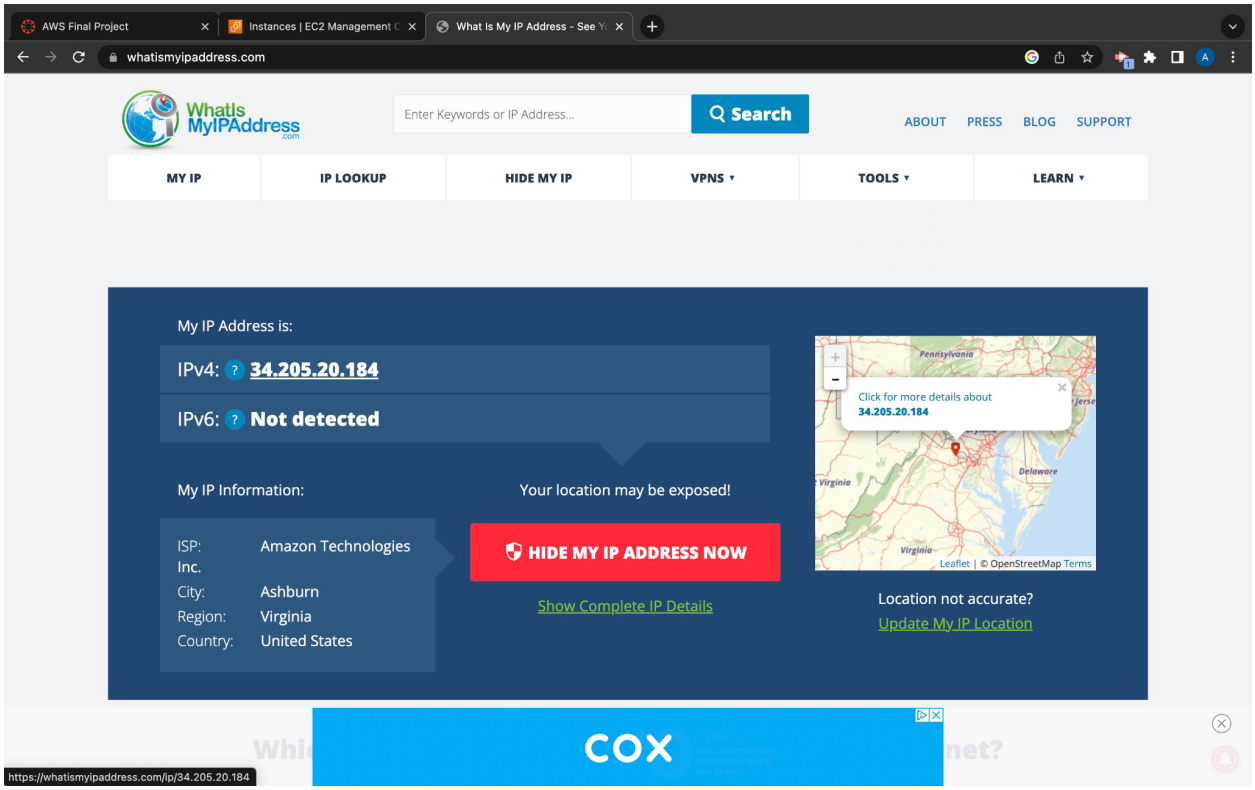
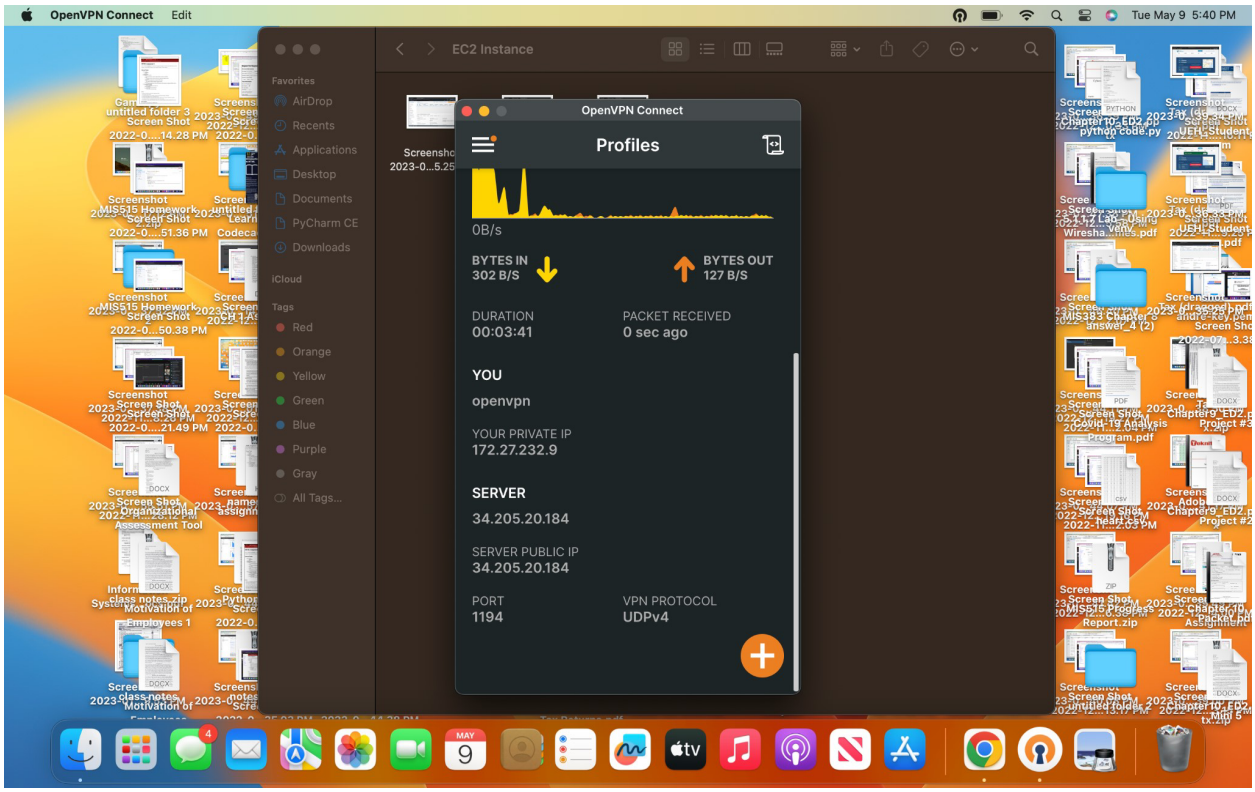
Launching an EC2 instance for OpenVPN - IP before and after connecting to VPN

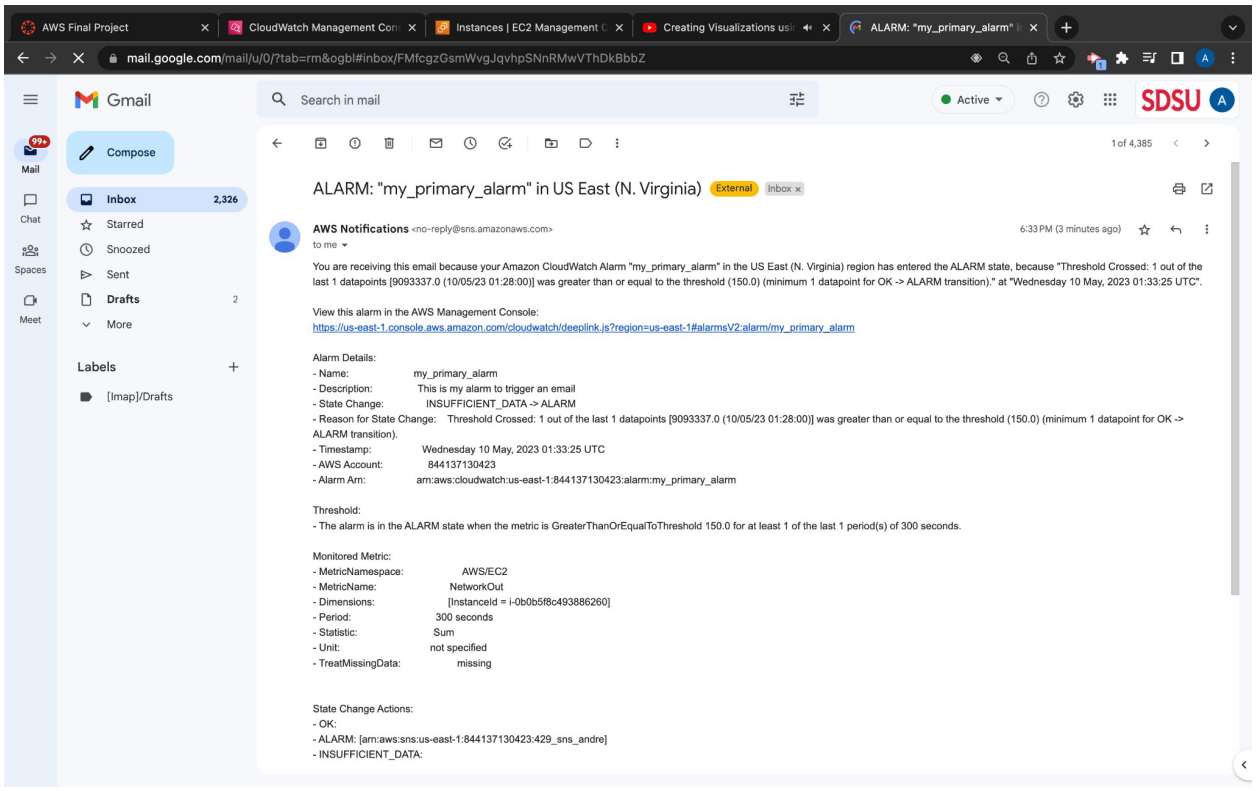


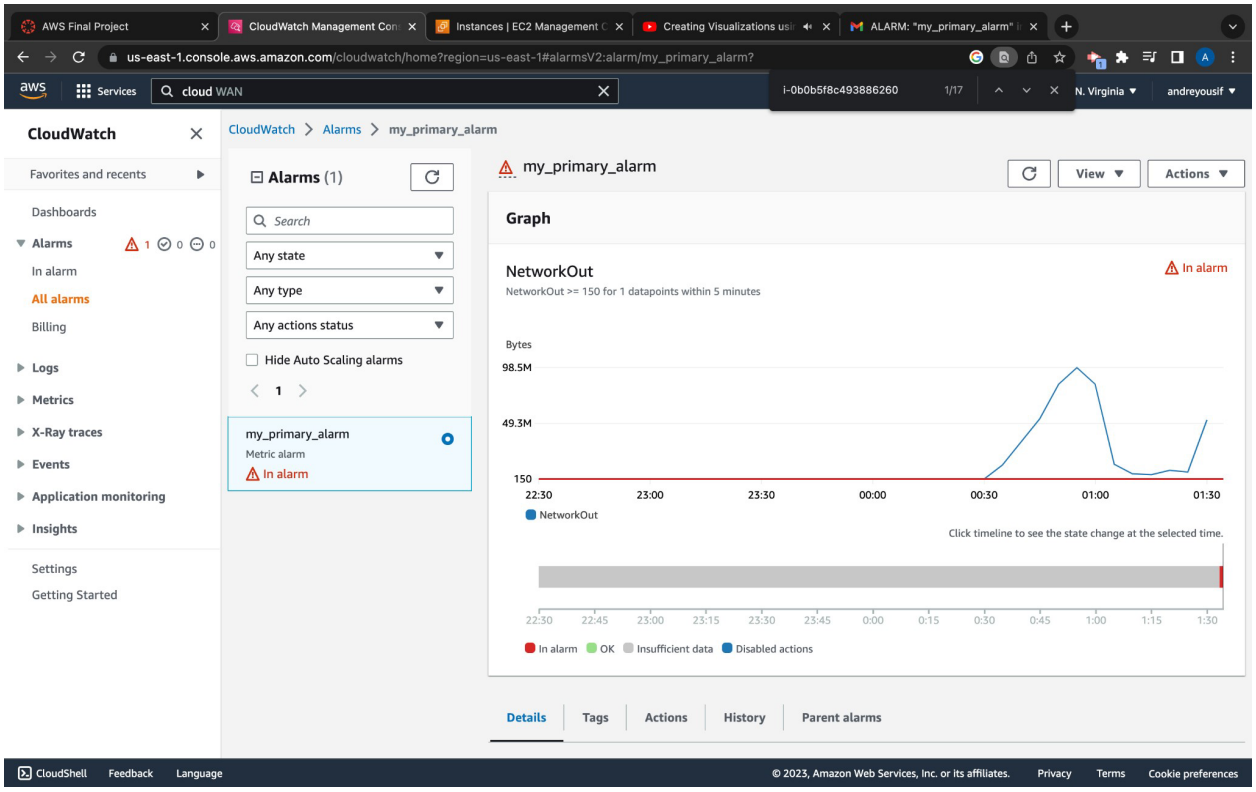


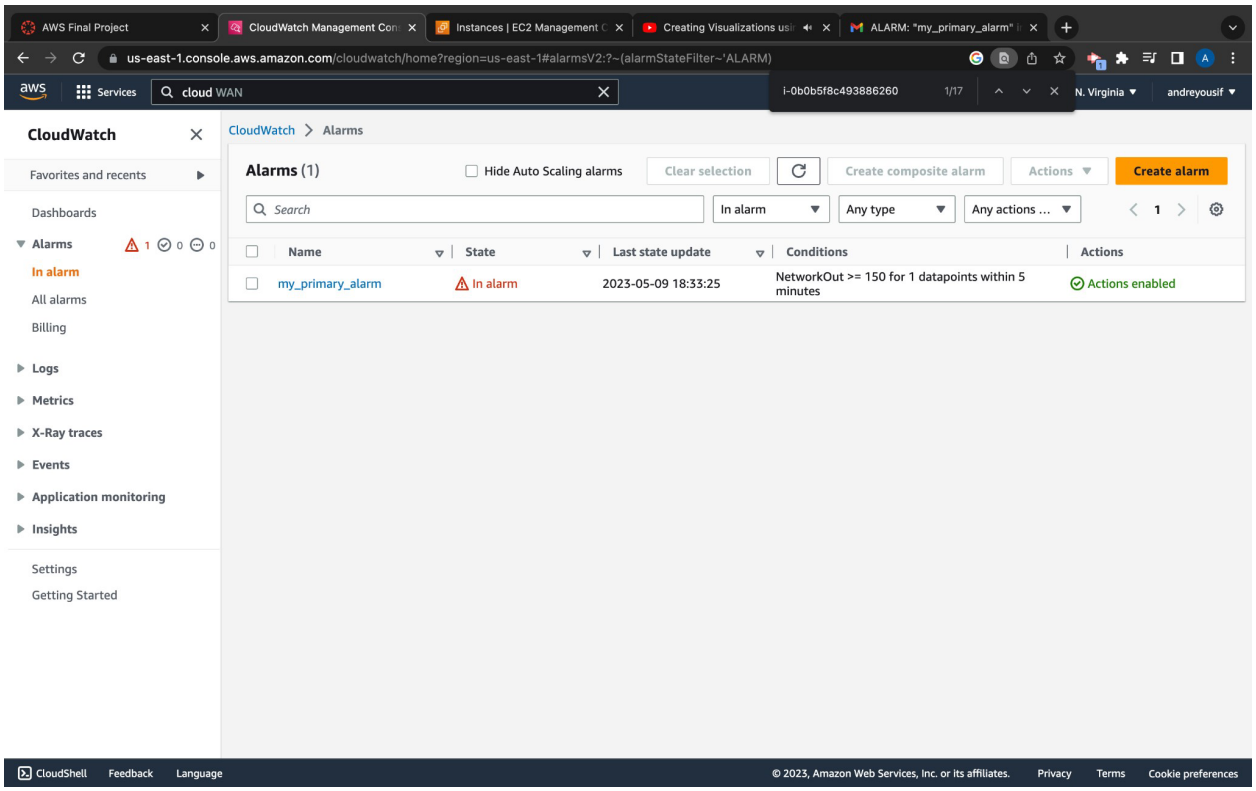

AWS Final Project
Instances | EC2 Management
What Is My IP Address - See Y
whatismyipaddress.com
WhatIsMyIPAddress.com
Enter Keywords or IP Address...
Search
ABOUT
PRESS
BLOG
SUPPORT
MY IP
IP LOOKUP
HIDE MY IP
VPNS
TOOLS
LEARN
My IP Address is:
IPv4: 34.205.20.184
IPv6: Not detected
My IP Information:
ISP: Amazon Technologies Inc.
City: Ashburn
Region: Virginia
Country: United States
Your location may be exposed!
HIDE MY IP ADDRESS NOW
Show Complete IP Details
Click for more details about 34.205.20.184
Leaflet | © OpenStreetMap Terms
Location not accurate?
Update My IP Location
COX
https://whatismyipaddress.com/ip/34.205.20.184


OpenVPN Connect
Edit
Tue May 9 5:40 PM
EC2 Instance
Favorites
AirDrop
Recents
Applications
Desktop
Documents
PyCharm CE
Downloads
iCloud
Tags
Red
Orange
Yellow
Green
Blue
Purple
Gray
All Tags...
OpenVPN Connect
Profiles
0B/s
BYTES IN
302 B/S
BYTES OUT
127 B/S
DURATION
00:03:41
PACKET RECEIVED
0 sec ago
YOU
openvpn
YOUR PRIVATE IP
172.27.232.9
SERVER
34.205.20.184
SERVER PUBLIC IP
34.205.20.184
PORT
1194
VPN PROTOCOL
UDPv4

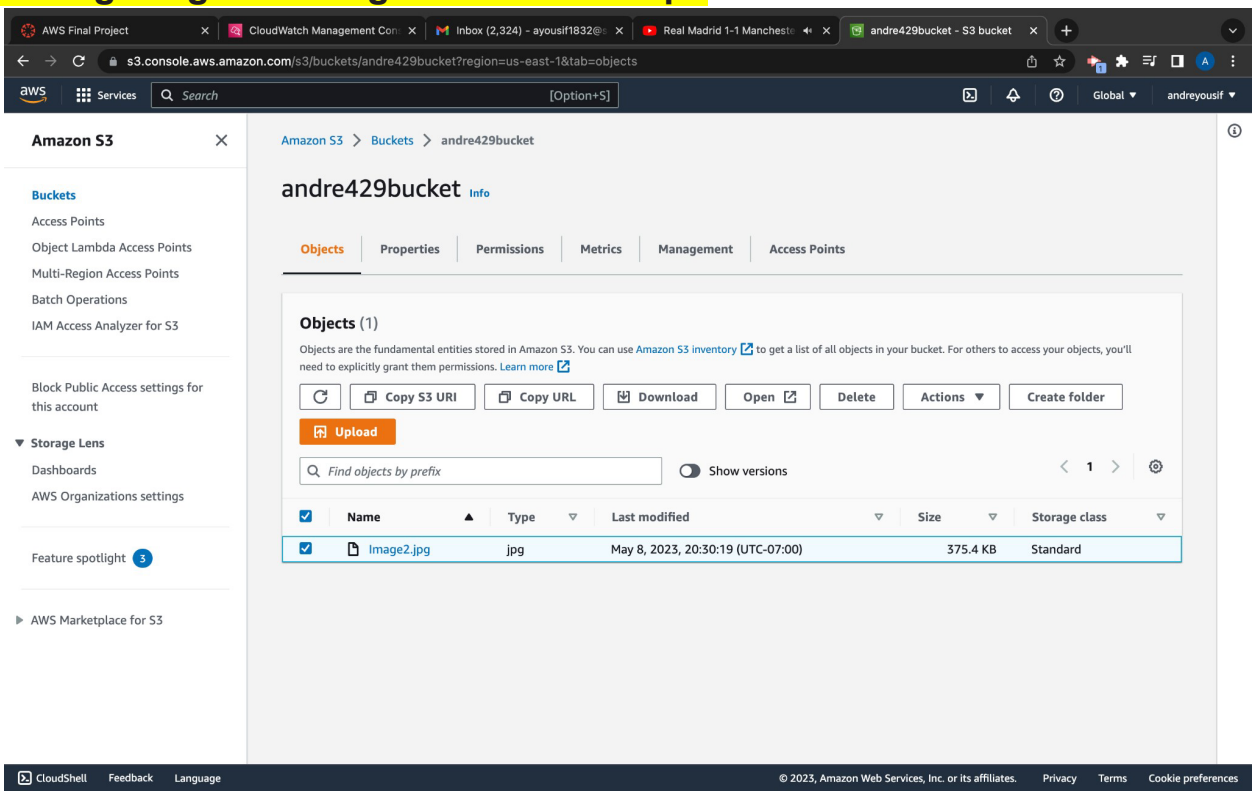
Setting up monitoring for traffic on the instance - CloudWatch Alarms and Simple Notification Service (SNS).

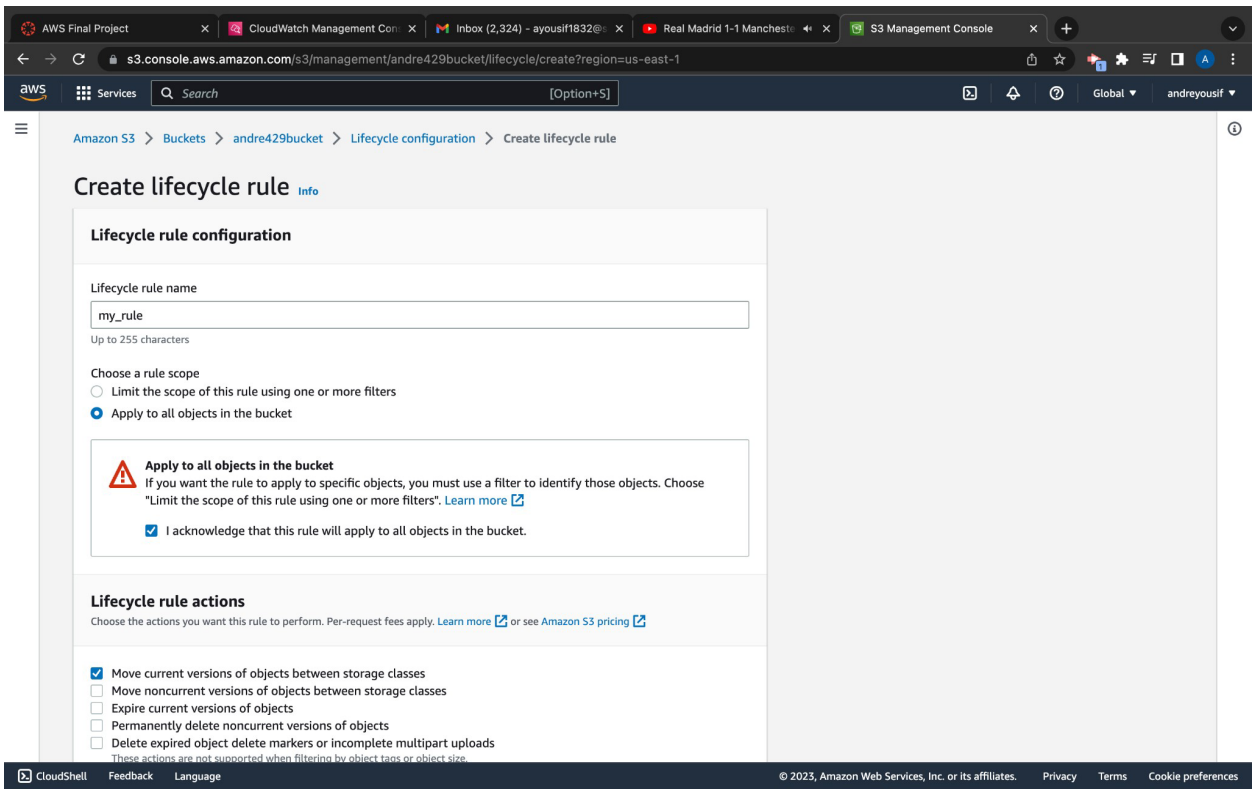

AWS Final Project
CloudWatch Management Con
Instances | EC2 Management
Creating Visualizations usi
ALARM: "my_primary_alarm"
mail.google.com/mail/u/0/?tab=rm&ogbl#inbox/FMfcgzGsmWvgJqvhpSNnRMwVThDkBbbZ
Gmail
Search in mail
Active
SDSU
Compose
Inbox 2,326
Starred
Snoozed
Sent
Drafts 2
More
Labels
[Imap]/Drafts
1 of 4,385
ALARM: "my_primary_alarm" in US East (N. Virginia)
External
Inbox
AWS Notifications <no-reply@sns.amazonaws.com>
6:33 PM (3 minutes ago)
to me
You are receiving this email because your Amazon CloudWatch Alarm "my_primary_alarm" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [9093337.0 (10/05/23 01:28:00)] was greater than or equal to the threshold (150.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Wednesday 10 May, 2023 01:33:25 UTC".
View this alarm in the AWS Management Console:
https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/my_primary_alarm
Alarm Details:
- Name: my_primary_alarm
- Description: This is my alarm to trigger an email
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [9093337.0 (10/05/23 01:28:00)] was greater than or equal to the threshold (150.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Wednesday 10 May, 2023 01:33:25 UTC
- AWS Account: 844137130423
- Alarm Arn: arn:aws:cloudwatch:us-east-1:844137130423:alarm:my_primary_alarm
Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 150.0 for at least 1 of the last 1 period(s) of 300 seconds.
Monitored Metric:
- MetricNamespace: AWS/EC2
- MetricName: NetworkOut
- Dimensions: [InstanceId = i-0b0b5f8c493886260]
- Period: 300 seconds
- Statistic: Sum
- Unit: not specified
- TreatMissingData: missing
State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-east-1:844137130423:429_sns_andre]
- INSUFFICIENT_DATA:

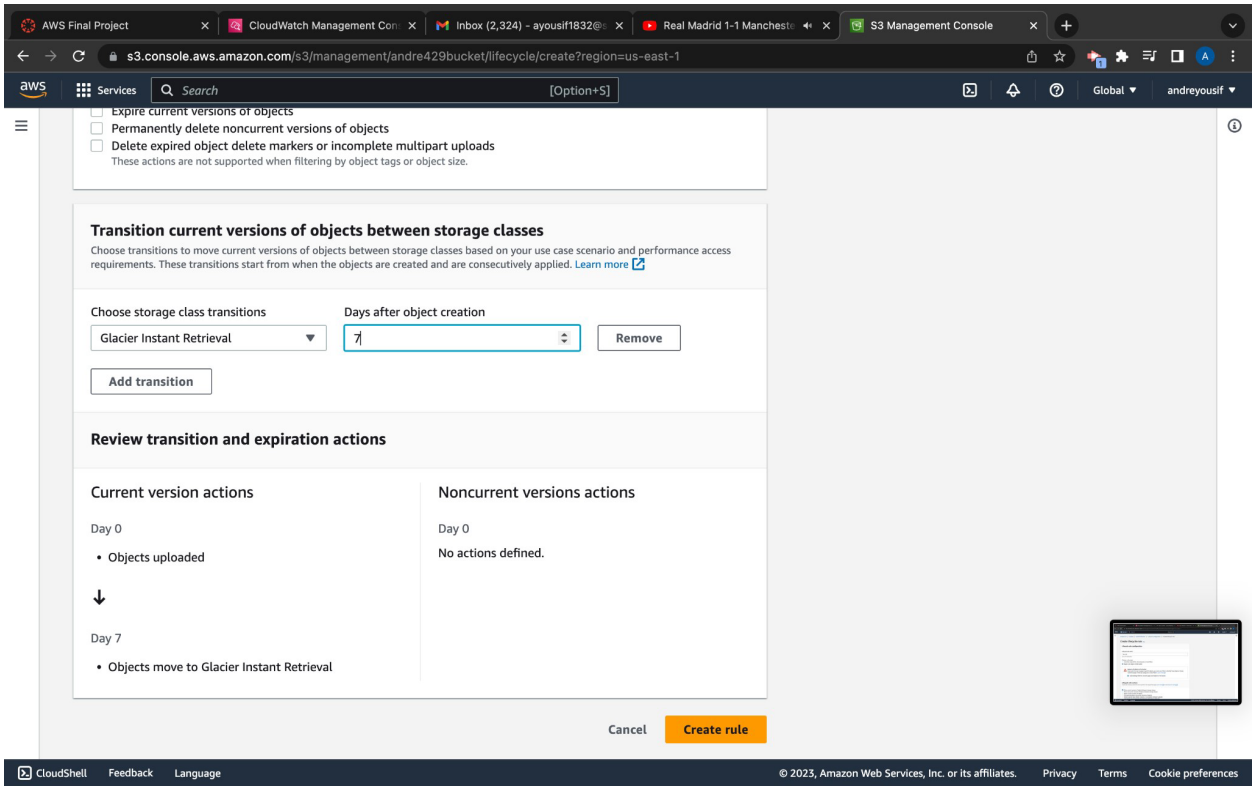

AWS Final Project
CloudWatch Management Con
Instances | EC2 Management
Creating Visualizations usi
ALARM: "my_primary_alarm"
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:alarm/my_primary_alarm?
aws
Services
cloud WAN
i-0b0b5f8c493886260
1/17
N. Virginia
andreyousif
CloudWatch
Favorites and recents
Dashboards
Alarms 1 0 0
In alarm
All alarms
Billing
Logs
Metrics
X-Ray traces
Events
Application monitoring
Insights
Settings
Getting Started
CloudWatch > Alarms > my_primary_alarm
Alarms (1)
Search
Any state
Any type
Any actions status
Hide Auto Scaling alarms
1
my_primary_alarm
Metric alarm
In alarm
my_primary_alarm
View
Actions
Graph
NetworkOut
NetworkOut >= 150 for 1 datapoints within 5 minutes
In alarm
Bytes
98.5M
49.3M
150
22:30
23:00
23:30
00:00
00:30
01:00
01:30
NetworkOut
Click timeline to see the state change at the selected time.
22:30
22:45
23:00
23:15
23:30
23:45
0:00
0:15
0:30
0:45
1:00
1:15
1:30
In alarm
OK
Insufficient data
Disabled actions
Details
Tags
Actions
History
Parent alarms
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

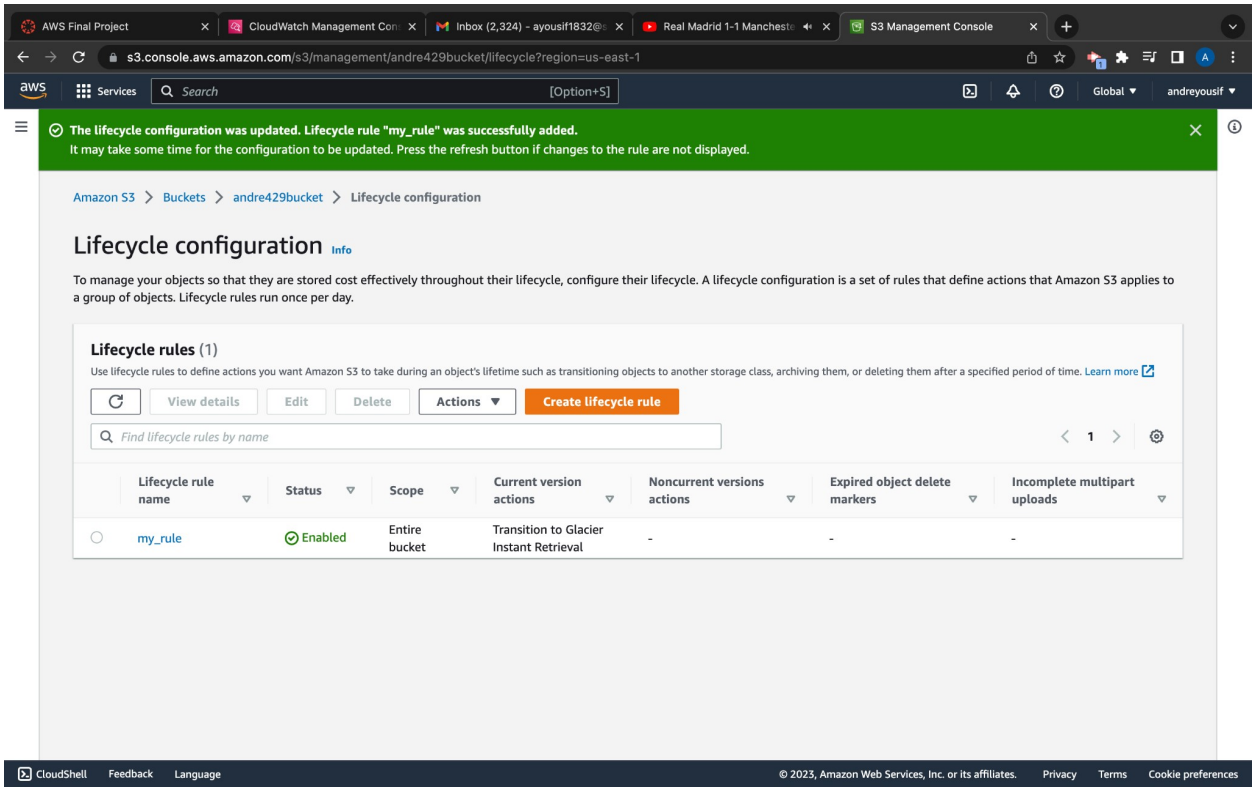

AWS Final Project
CloudWatch Management Con
Instances | EC2 Management
Creating Visualizations usi
ALARM: "my_primary_alarm"
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:?~(alarmStateFilter~'ALARM)
aws
Services
cloud WAN
i-0b0b5f8c493886260
1/17
N. Virginia
andreyousif
CloudWatch
Favorites and recents
Dashboards
Alarms
In alarm
All alarms
Billing
Logs
Metrics
X-Ray traces
Events
Application monitoring
Insights
Settings
Getting Started
CloudWatch > Alarms
Alarms (1)
Hide Auto Scaling alarms
Clear selection
Create composite alarm
Actions
Create alarm
Search
In alarm
Any type
Any actions ...
Name
State
Last state update
Conditions
Actions
my_primary_alarm
In alarm
2023-05-09 18:33:25
NetworkOut >= 150 for 1 datapoints within 5 minutes
Actions enabled
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Configuring S3 storage to hold backups

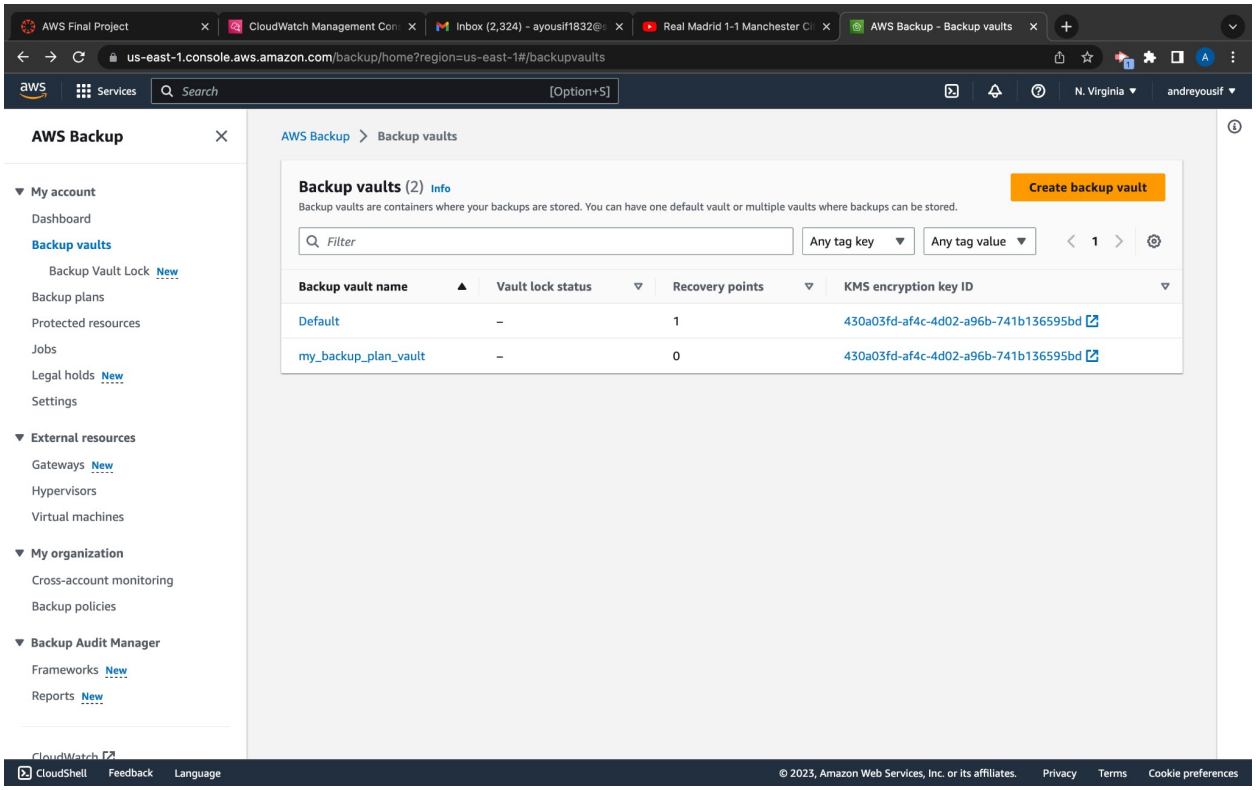


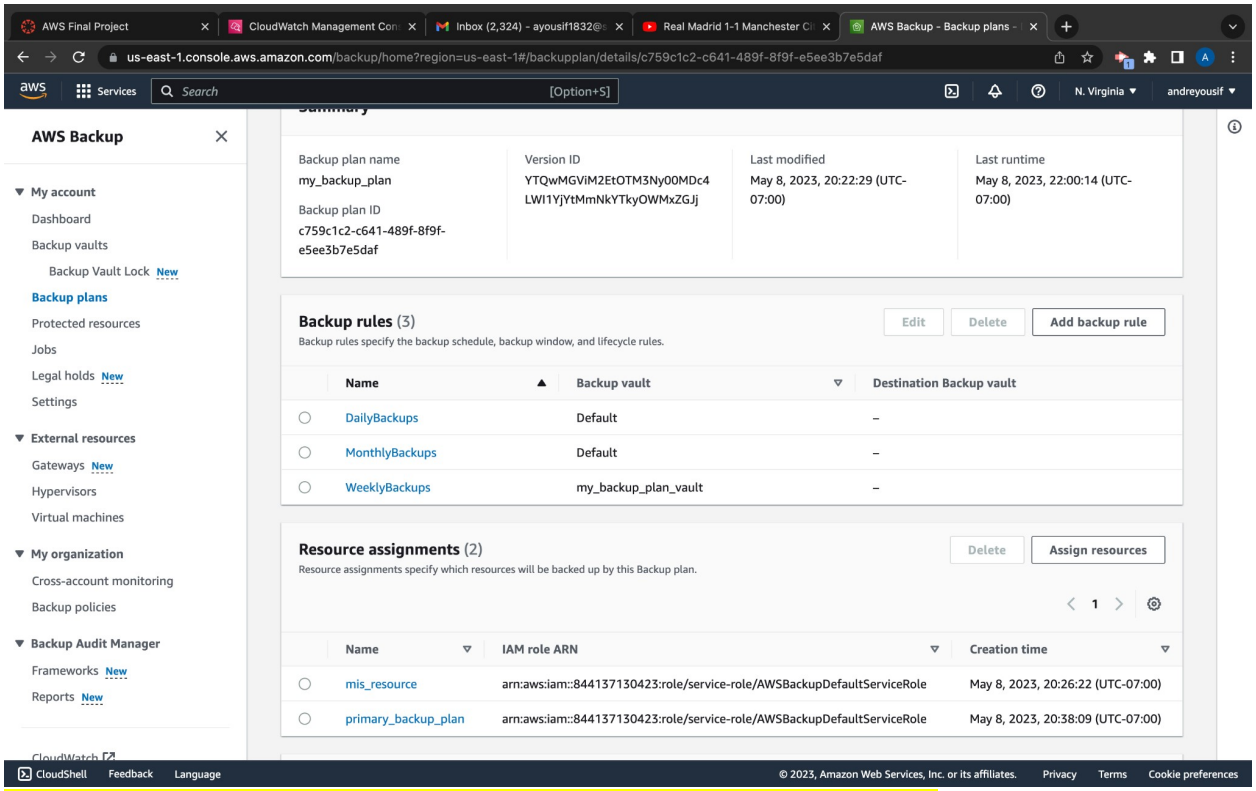




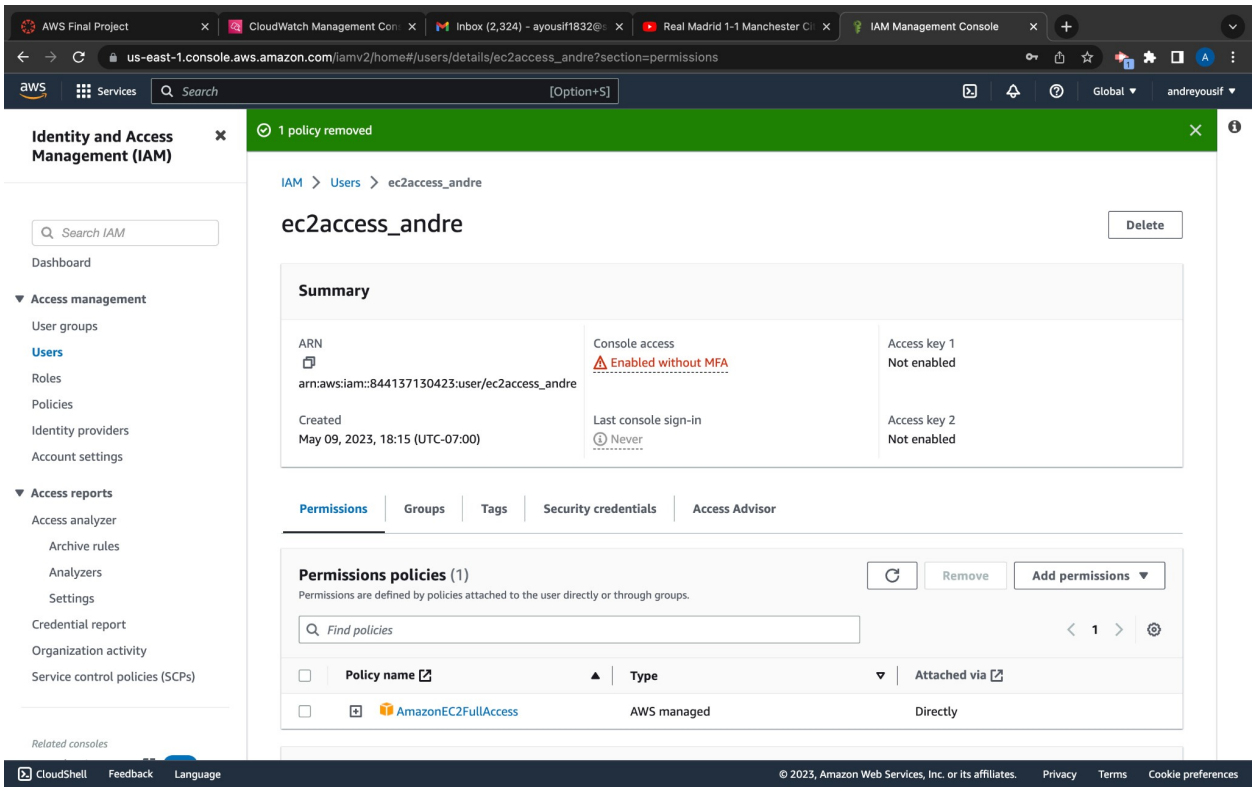


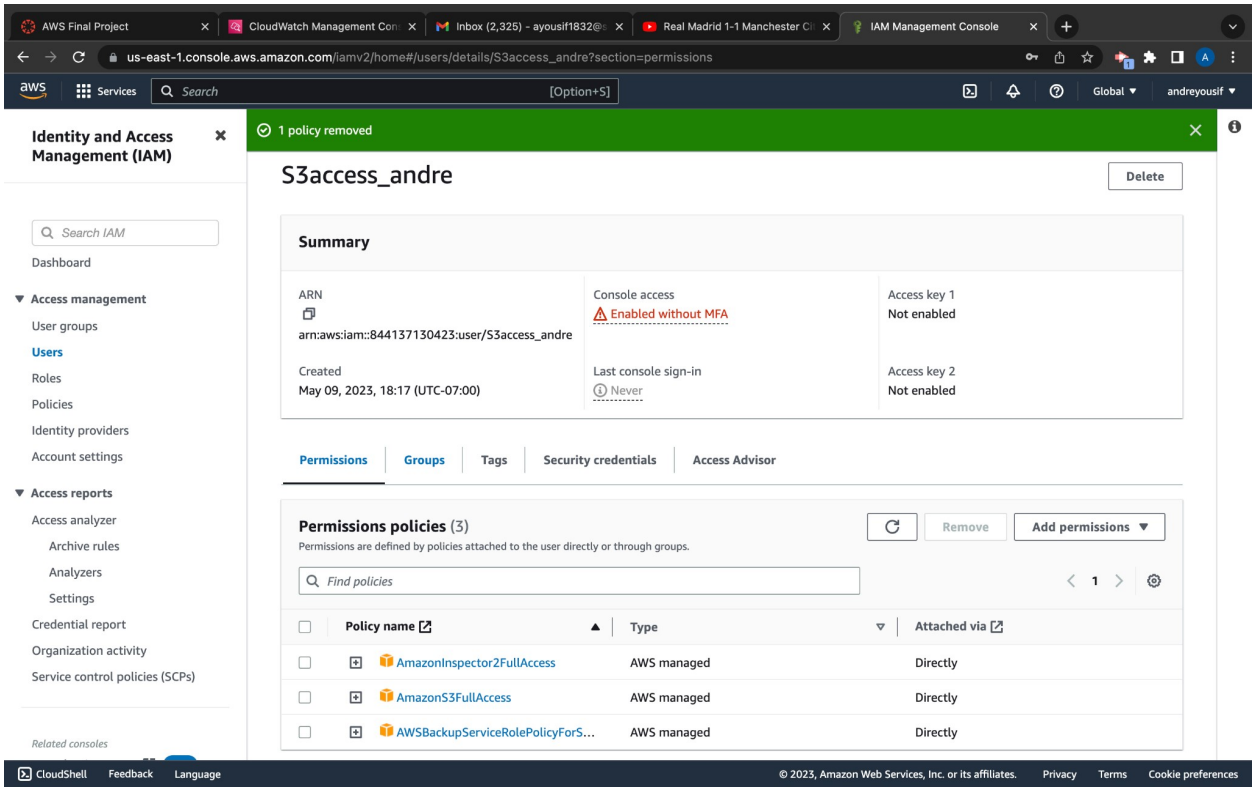
Configuring a backup tool to auto backup the instance- AWS Backup Service

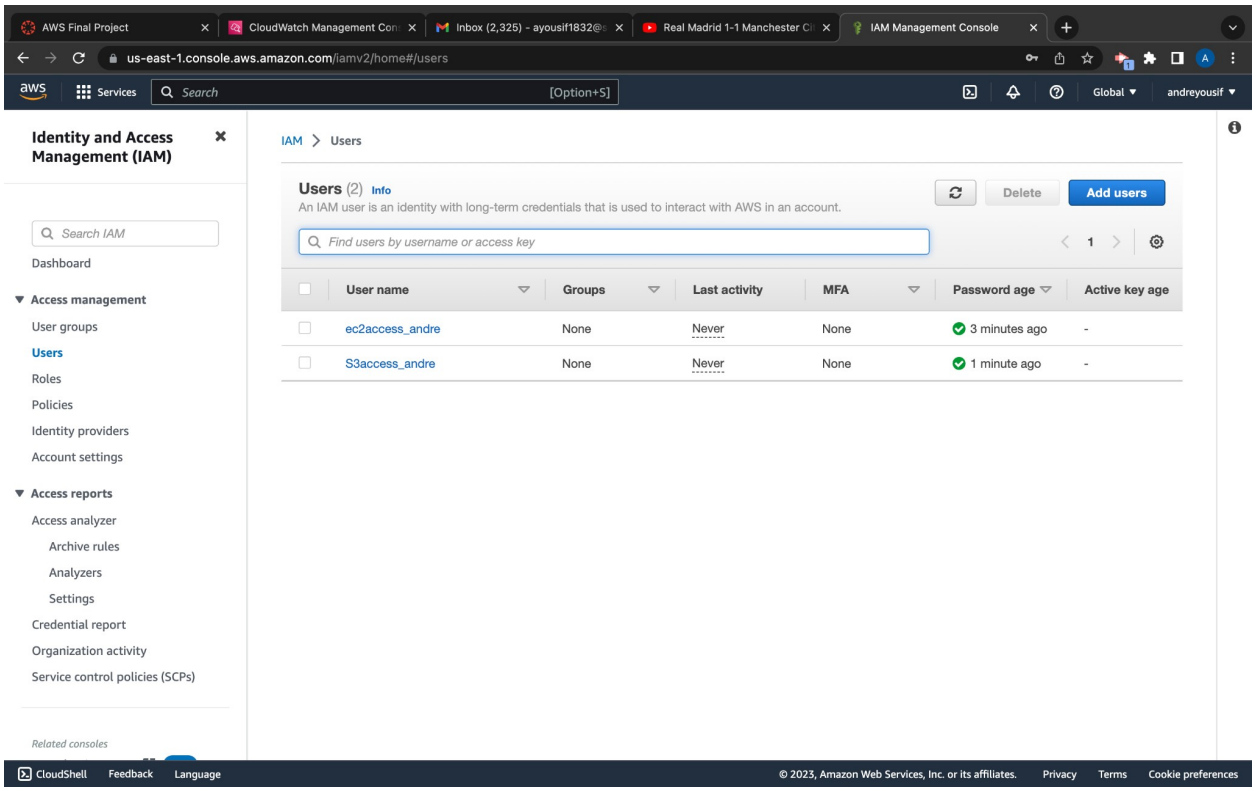




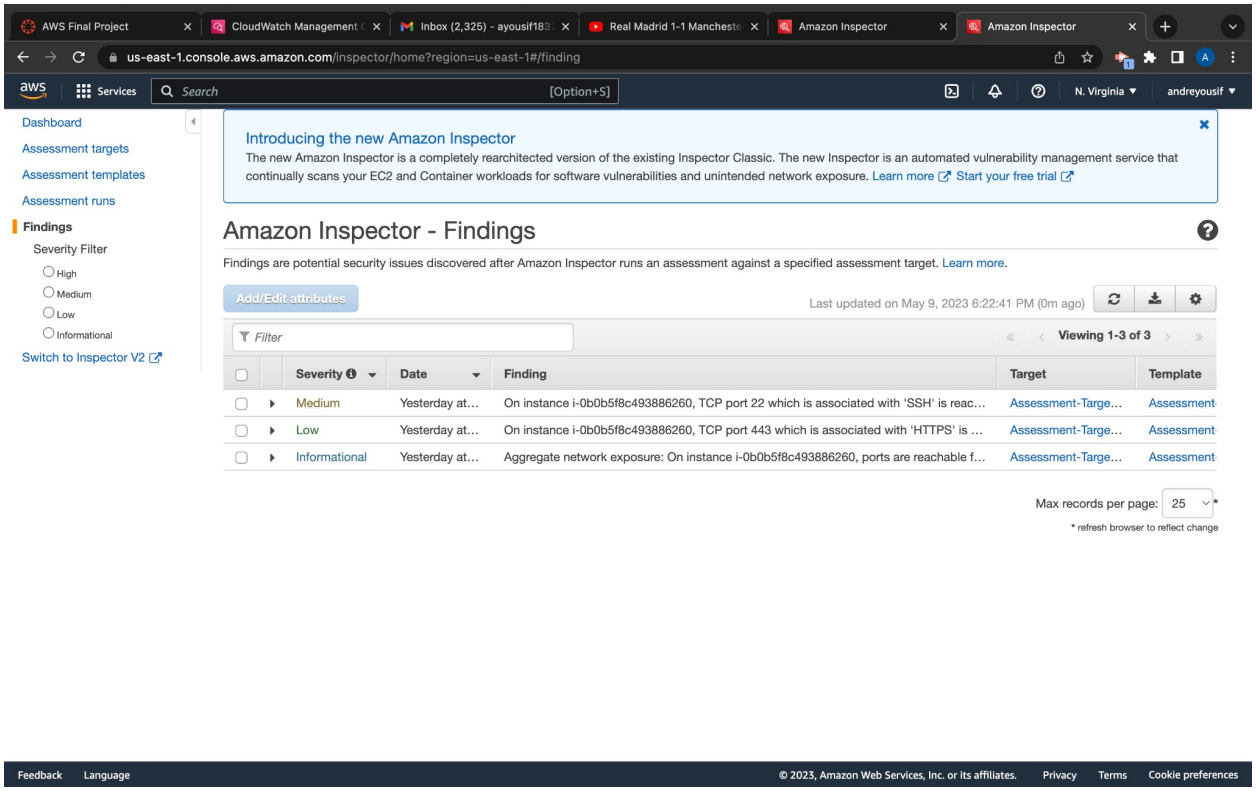
Creating IAM users with the permissions/policies


AWS Final Project
CloudWatch Management Con
Inbox (2,324) - ayousif1832@
Real Madrid 1-1 Manchester Ci
IAM Management Console
us-east-1.console.aws.amazon.com/iamv2/home#/users/details/ec2access_andre?section=permissions
Services
Search
[Option+S]
Global
andreyousif
Identity and Access Management (IAM)
1 policy removed
IAM > Users > ec2access_andre
ec2access_andre
Delete
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Related consoles
Summary
ARN
arn:aws:iam::844137130423:user/ec2access_andre
Console access
Enabled without MFA
Access key 1
Not enabled
Created
May 09, 2023, 18:15 (UTC-07:00)
Last console sign-in
Never
Access key 2
Not enabled
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (1)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Find policies
1
Policy name
Type
Attached via
AmazonEC2FullAccess
AWS managed
Directly
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


AWS Final Project
CloudWatch Management Con
Inbox (2,325) - ayousif1832@
Real Madrid 1-1 Manchester Ci
IAM Management Console
us-east-1.console.aws.amazon.com/iamv2/home#/users/details/S3access_andre?section=permissions
Services
Search
[Option+S]
Global
andreyousif
Identity and Access Management (IAM)
1 policy removed
S3access_andre
Delete
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Related consoles
Summary
ARN
arn:aws:iam::844137130423:user/S3access_andre
Console access
Enabled without MFA
Access key 1
Not enabled
Created
May 09, 2023, 18:17 (UTC-07:00)
Last console sign-in
Never
Access key 2
Not enabled
Permissions
Groups
Tags
Security credentials
Access Advisor
Permissions policies (3)
Permissions are defined by policies attached to the user directly or through groups.
Remove
Add permissions
Find policies
1
Policy name
Type
Attached via
AmazonInspector2FullAccess
AWS managed
Directly
AmazonS3FullAccess
AWS managed
Directly
AWSBackupServiceRolePolicyForS...
AWS managed
Directly
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Configuring a vulnerability scanner - Inspector - REPORT



Creating and Deploying an EC2 Instance with OpenVPN

As part of this project, I have implemented an AWS-based cloud system that utilizes EC2 instances with OpenVPN Server, CloudWatch, backup services, IAM, and Inspector. Throughout the process, I have taken into consideration the principles of cloud and information security, recognizing their importance and the benefits they bring to the system and its users.

I began by launching an EC2 instance for OpenVPN Server and configuring it by SSH into the instance. I then set up monitoring for traffic on the instance by enabling detailed monitoring and configuring CloudWatch Alarms to monitor network traffic on the instance. I configured S3 storage to hold backups, and set up a vulnerability scanner by creating an assessment template and launching an assessment run.

One of the key components of my system is the use of EC2 instances with OpenVPN Server. This allows for secure remote access to the system while also ensuring that all data transmissions are encrypted. To further enhance the security of my system, I have implemented Identity and Access Management (IAM) to control access to AWS resources, limiting access to only authorized users and groups.

As part of my AWS-based cloud system, I have also created an S3 bucket and implemented lifecycle rules to move backups to Glacier. First, I created an S3 bucket to store my backups and other data. I ensured that the bucket was configured with appropriate permissions and access controls to limit access to authorized users and groups only. I also enabled versioning

to ensure that previous versions of files could be recovered if necessary. Next, I implemented lifecycle rules to manage the lifecycle of my backups.

To ensure the reliability and availability of my system, I have implemented backup services, including AWS Backup, to protect against data loss and to ensure that my data is always recoverable in the event of a disaster. Additionally, I have implemented CloudWatch to monitor my application's network traffic.

Furthermore, I have implemented Inspector to perform regular security assessments and vulnerability scans, ensuring that my system is secure and up-to-date with the latest security patches and updates. Throughout the design and implementation of my system, I have prioritized information security by adhering to key principles such as confidentiality, integrity, and
availability.

In conclusion, the implementation of an AWS-based cloud system utilizing EC2 instances with OpenVPNServer, CloudWatch, backup services, IAM, and Inspector has proven to be an effective solution for any organization. By adhering to the principles of cloud and information security, I have created a secure and reliable system that meets the needs of users while also protecting their data and privacy.

Securing the System

When it comes to further securing a system, there are several measures that can be taken beyond the basic security controls already in place. Regularly updating and patching the system is an important topic in system hardening. Regularly applying security updates and patches to the system is very important because it can help to address known vulnerabilities and prevent attackers from exploiting them. Also, disabling services and protocols that are not needed can reduce the attack surface of the system and minimize the risk of a successful attack.

In addition, network security measures such as firewalls, intrusion detection and prevention systems, and virtual private networks can help to protect the system from network-based attacks. Also, using secure protocols such as HTTPS, SSH, and TLS can help to protect data in transit and prevent attacks. Encrypting sensitive data at rest can also provide an additional layer of protection.

Furthermore, implementing access controls such as user accounts and permissions, can help to limit access to sensitive information and prevent unauthorized access. Monitoring system logs can help to detect suspicious activity and potential security breaches. Log files should be stored securely and regularly reviewed for any unusual activity.

Finally, conducting regular security audits can help to identify any vulnerabilities or weaknesses in the system and provide recommendations for improving security. Also, implementing Multi-Factor Authentication (MFA) adds an extra layer of security to the authentication process, making it more difficult for attackers to gain unauthorized access.

3 Months Support Plan

I provided a three month support plan to continue running this VPN Server in AWS and described how I would support it while keeping security in mind. The plan includes regular patching and updating of the system, and monitoring logs for malicious or unauthorized access. I also identified the roles and responsibilities of the System Administrator and Security Analyst in carrying out these tasks. By following this plan, I can ensure the system's availability and protect it from security threats.

I would recommend applying security patches and updates as soon as they become available. Depending on the severity of the vulnerability, I would either update the system immediately or schedule a maintenance window. I would check for updates weekly and apply them during a maintenance window.

Monitoring logs for any suspicious activity, such as unauthorized access attempts or unusual traffic patterns. Reviewing logs weekly to identify any security incidents and take necessary actions to mitigate them. Implementing Multi-Factor Authentication (MFA) for all users to restrict access to the VPN and setting up ACL.

As of roles and responsibilities, the following roles would be responsible for the above tasks. A System Administrator would be responsible for applying patches and updates, maintaining the system, and configuring security features. A Security Analyst would be responsible for monitoring logs, analyzing security incidents, and providing recommendations for improving the system's security.

In conclusion, these three months support plan outlines the approach to supporting the VPN system in AWS while keeping security in mind. By implementing regular patching, monitoring logs, and improving security features, it can ensure the system's availability and protect it from security threats.

Incident Response Plan

In the event of a security breach or compromise of my EC2 instance and VPN, my incident response plan will involve the following steps. The first step would be to isolate the affected system from the network to prevent further damage and to preserve evidence for forensic analysis. Once the system has been contained, I will conduct an analysis of the incident to determine the scope and nature of the attack, the information that may have been compromised, and the potential impact on my application. I will take immediate steps to mitigate the damage caused by the attack, such as changing access codes and passwords, scanning for malware, and implementing additional security controls. Depending on the severity of the attack, I may need to rebuild the affected application from scratch. If backups are available, I will restore the application from the most recent backup that has been verified as clean. I will also conduct a thorough review of my backup procedures to ensure that they are secure and up-to-date. I will investigate the source of the attack to determine whether it was the result of an external threat or an internal security breach. I will use all available resources to identify the attacker, including network logs, system logs, and any other relevant data.

In conclusion, my incident response plan is designed to help me quickly and effectively respond to security incidents and minimize the impact on my application. I will continually review and update my plan to ensure that it remains effective against new and evolving threats.