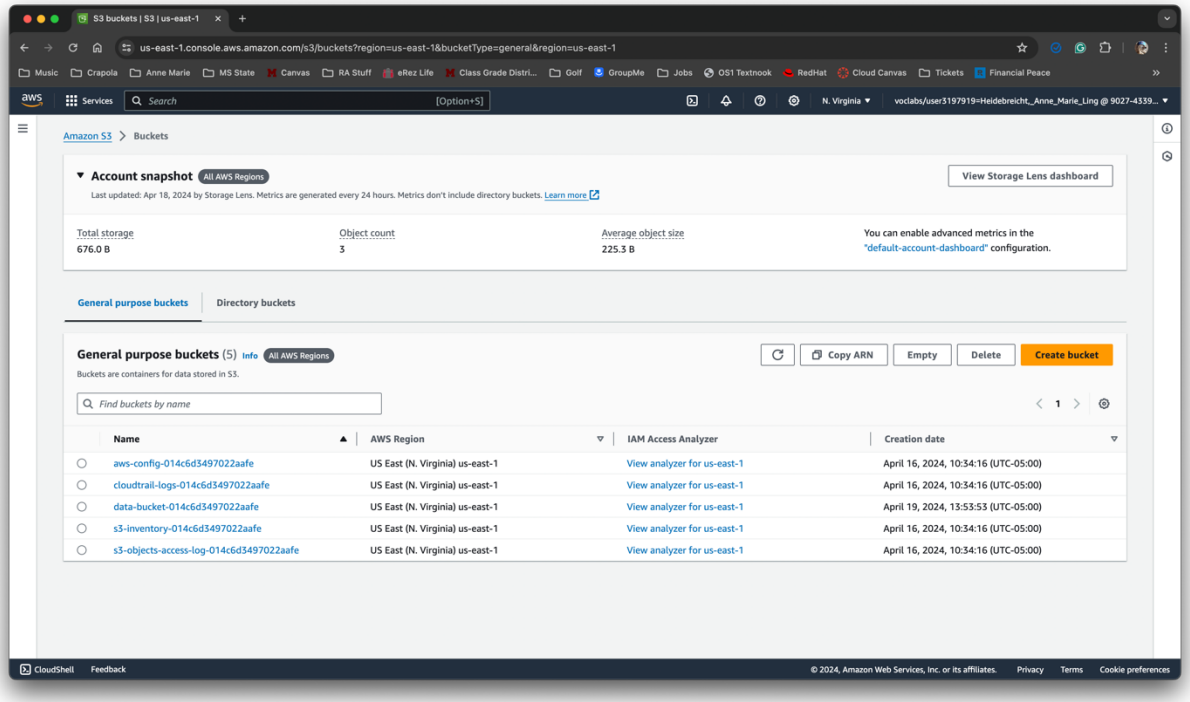
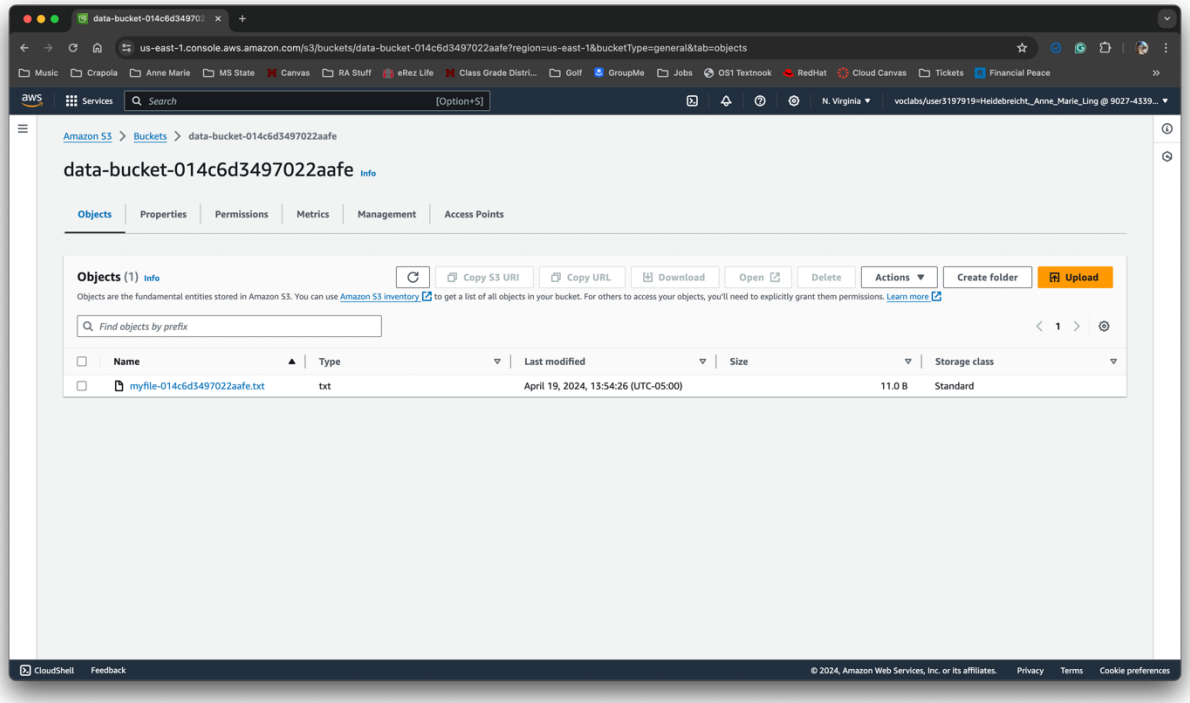
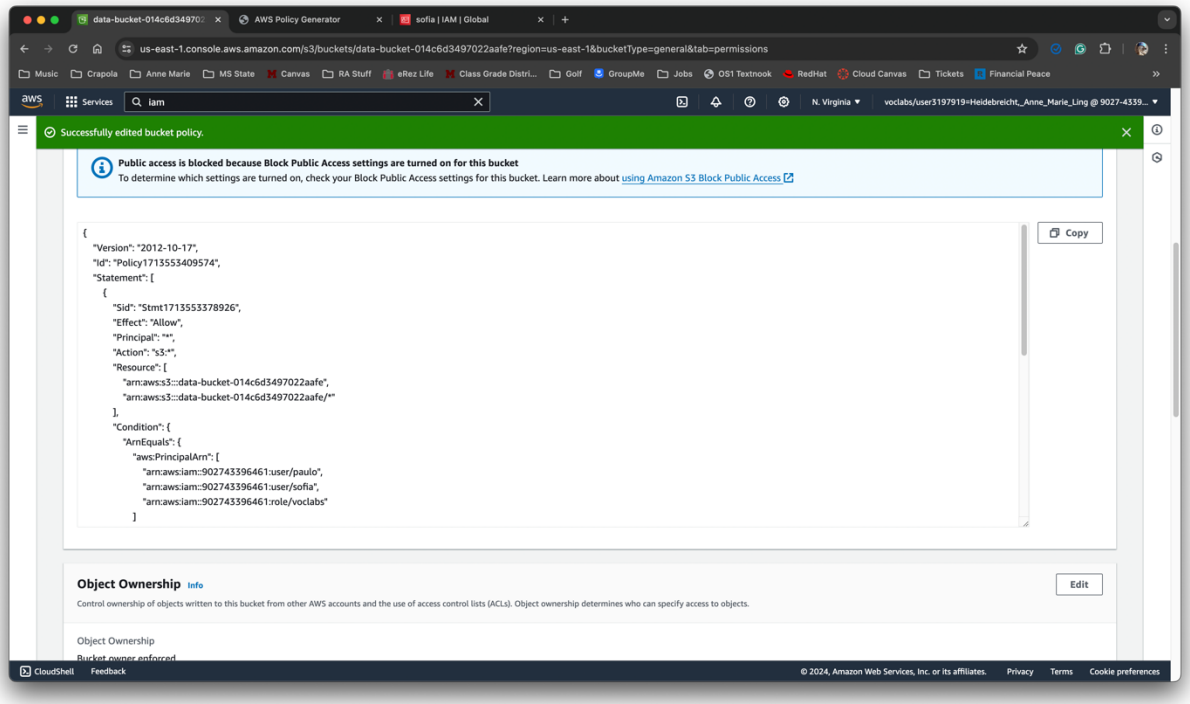
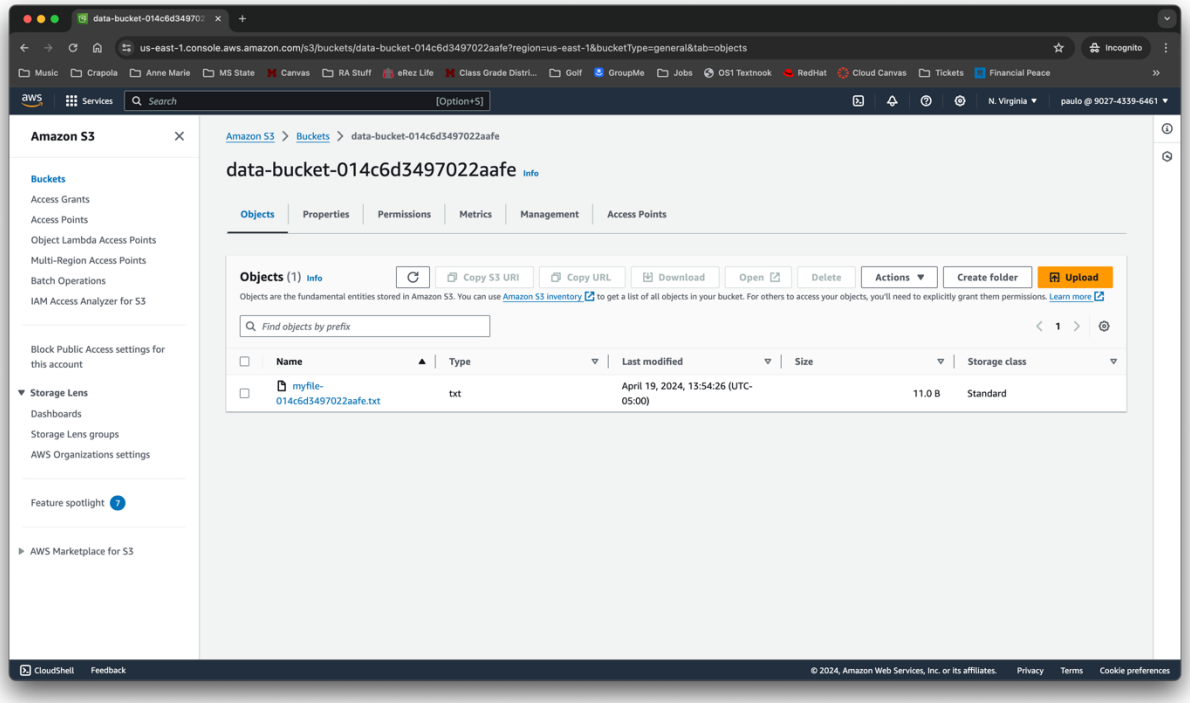
Phase 1 – Securing data in Amazon S3

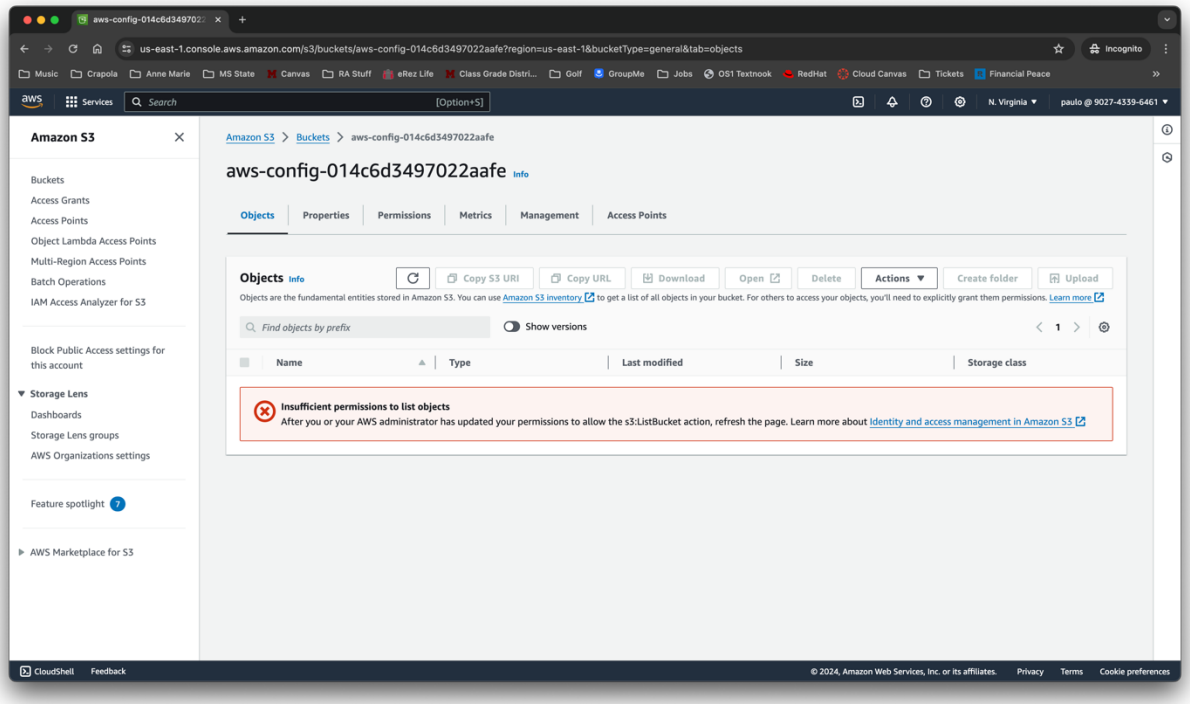
Task 1.1: Create a bucket, apply a bucket policy, and test access

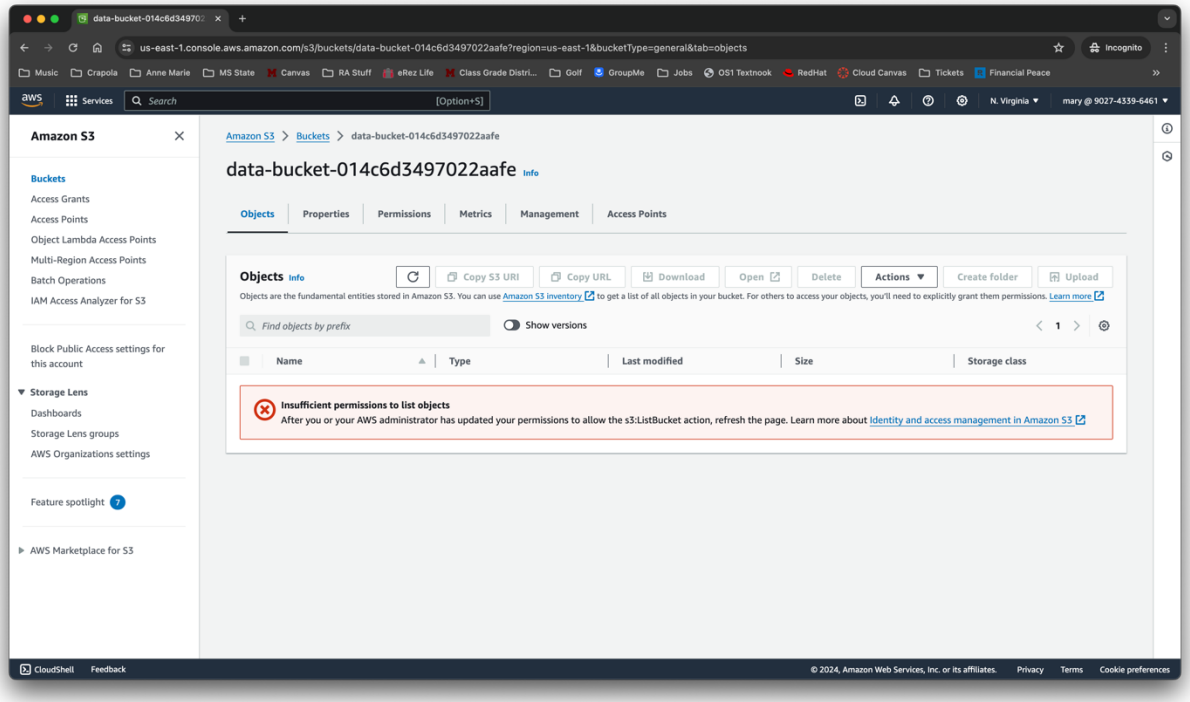




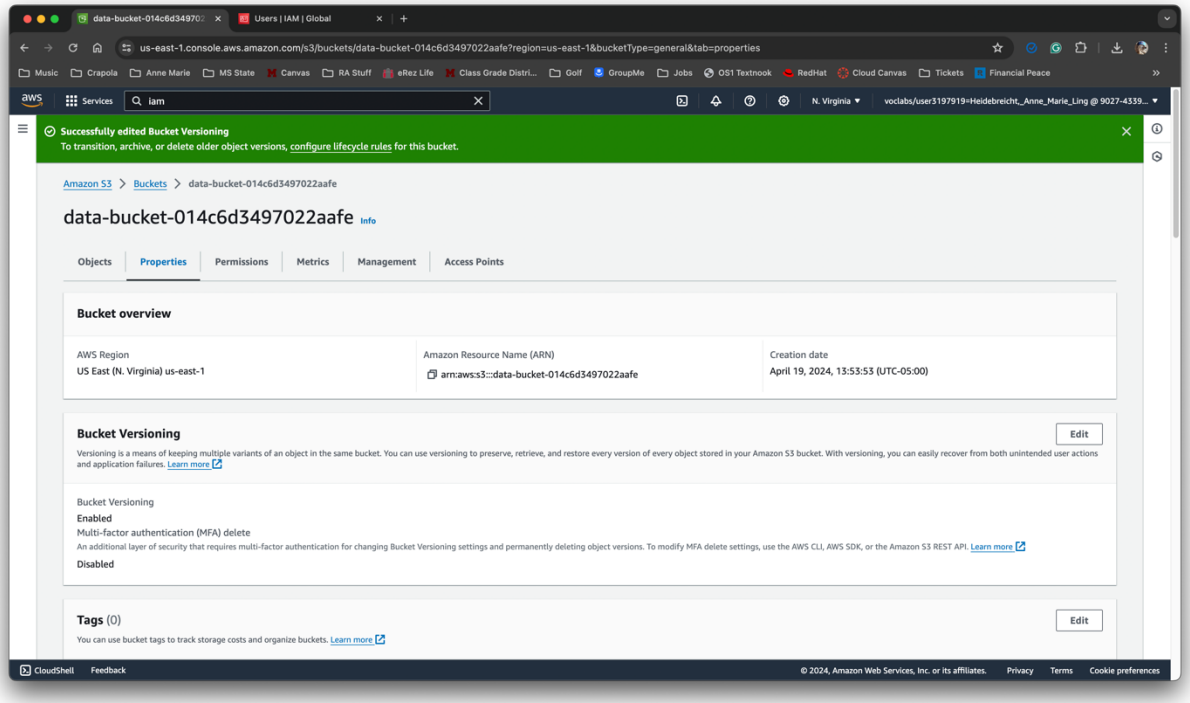

data-bucket-014c6d349702
AWS Policy Generator
sofia | IAM | Global
us-east-1.console.aws.amazon.com/s3/buckets/data-bucket-014c6d3497022aafe?region=us-east-1&bucketType=general&tab=permissions
Music
Crapola
Anne Marie
MS State
Canvas
RA Stuff
eRez Life
Class Grade Distri...
Golf
GroupMe
Jobs
OS1 Textnook
RedHat
Cloud Canvas
Tickets
Financial Peace
aws
Services
iam
N. Virginia
voclabs/user3197919=Heidebreicht,_Anne_Marie_Ling @ 9027-4339...
Successfully edited bucket policy.
Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket. Learn more about using Amazon S3 Block Public Access
Copy
{
"Version": "2012-10-17",
"Id": "Policy1713553409574",
"Statement": [
{
"Sid": "Stmt1713553378926",
"Effect": "Allow",
"Principal": "*",
"Action": "s3:*",
"Resource": [
"arn:aws:s3:::data-bucket-014c6d3497022aafe",
"arn:aws:s3:::data-bucket-014c6d3497022aafe/*"
],
"Condition": {
"ArnEquals": {
"aws:PrincipalArn": [
"arn:aws:iam::902743396461:user/paulo",
"arn:aws:iam::902743396461:user/sofia",
"arn:aws:iam::902743396461:role/voclabs"
]
Object Ownership
Info
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
Edit
Object Ownership
Bucket owner enforced
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

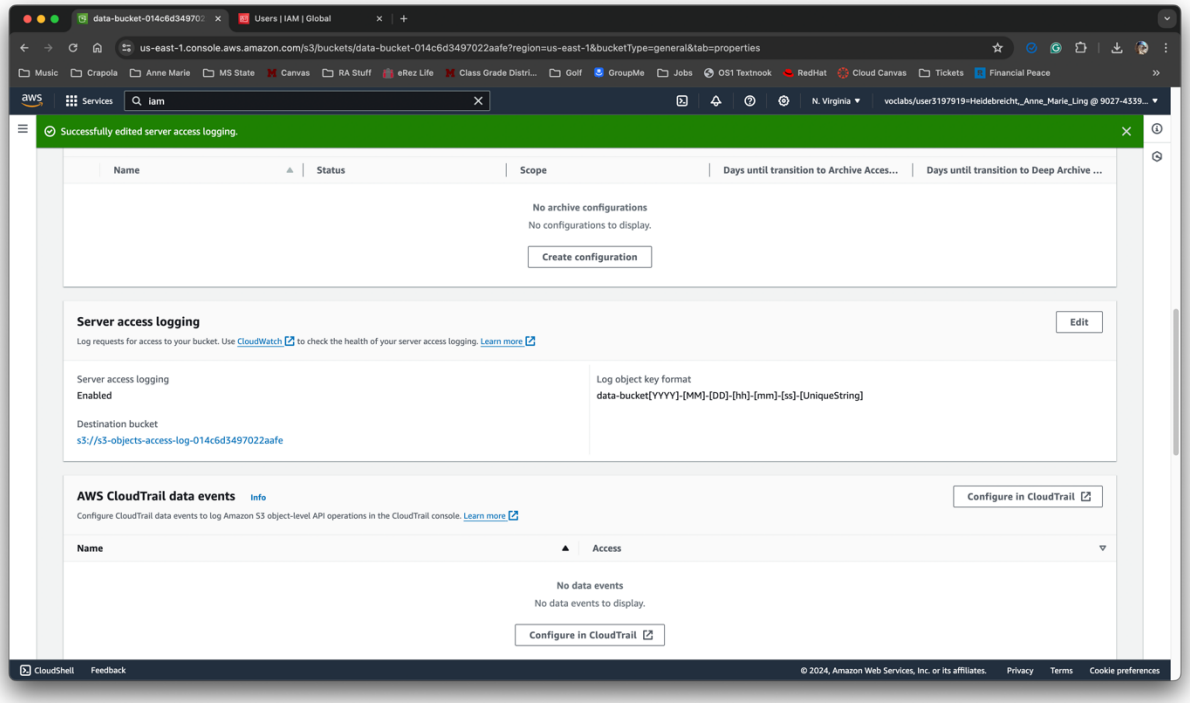

data-bucket-014c6d349702
us-east-1.console.aws.amazon.com/s3/buckets/data-bucket-014c6d3497022aafe?region=us-east-1&bucketType=general&tab=objects
Incognito
Music
Crapola
Anne Marie
MS State
Canvas
RA Stuff
eRez Life
Class Grade Distri...
Golf
GroupMe
Jobs
OS1 Textnook
RedHat
Cloud Canvas
Tickets
Financial Peace
aws
Services
Search
[Option+S]
N. Virginia
paulo @ 9027-4339-6461
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
7
AWS Marketplace for S3
Amazon S3 > Buckets > data-bucket-014c6d3497022aafe
data-bucket-014c6d3497022aafe
Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Objects (1)
Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Find objects by prefix
1
Name
Type
Last modified
Size
Storage class
myfile-014c6d3497022aafe.txt
txt
April 19, 2024, 13:54:26 (UTC-05:00)
11.0 B
Standard
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

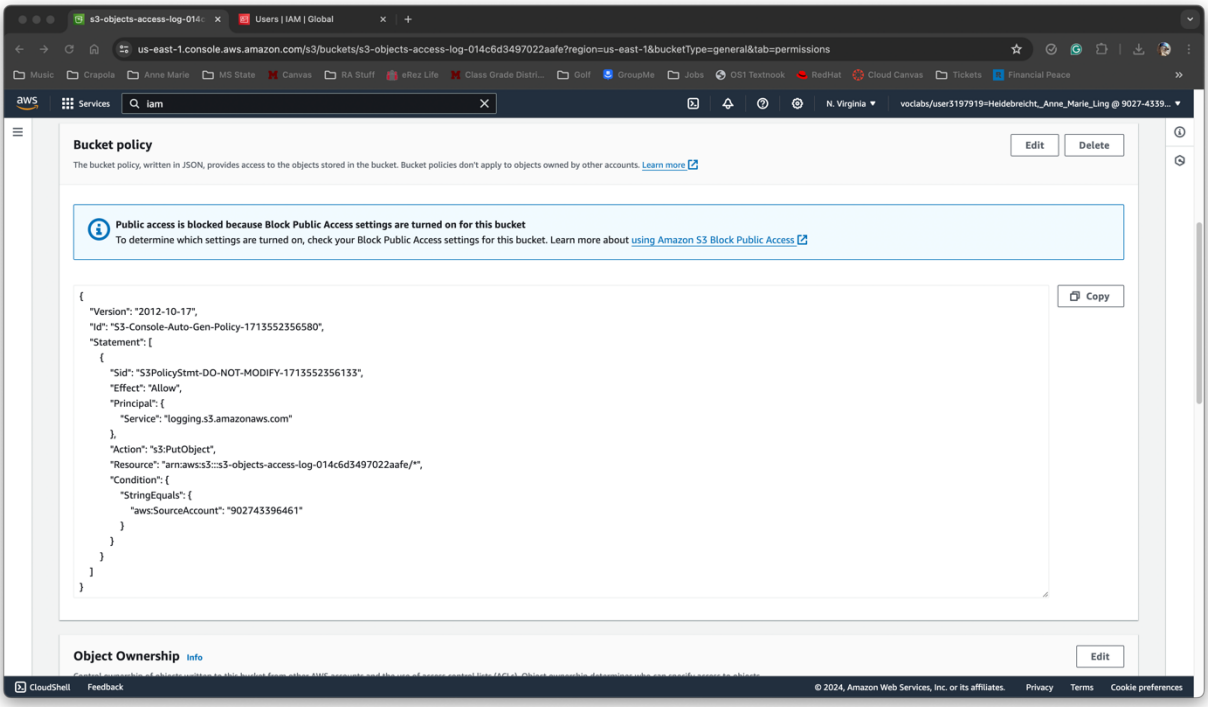




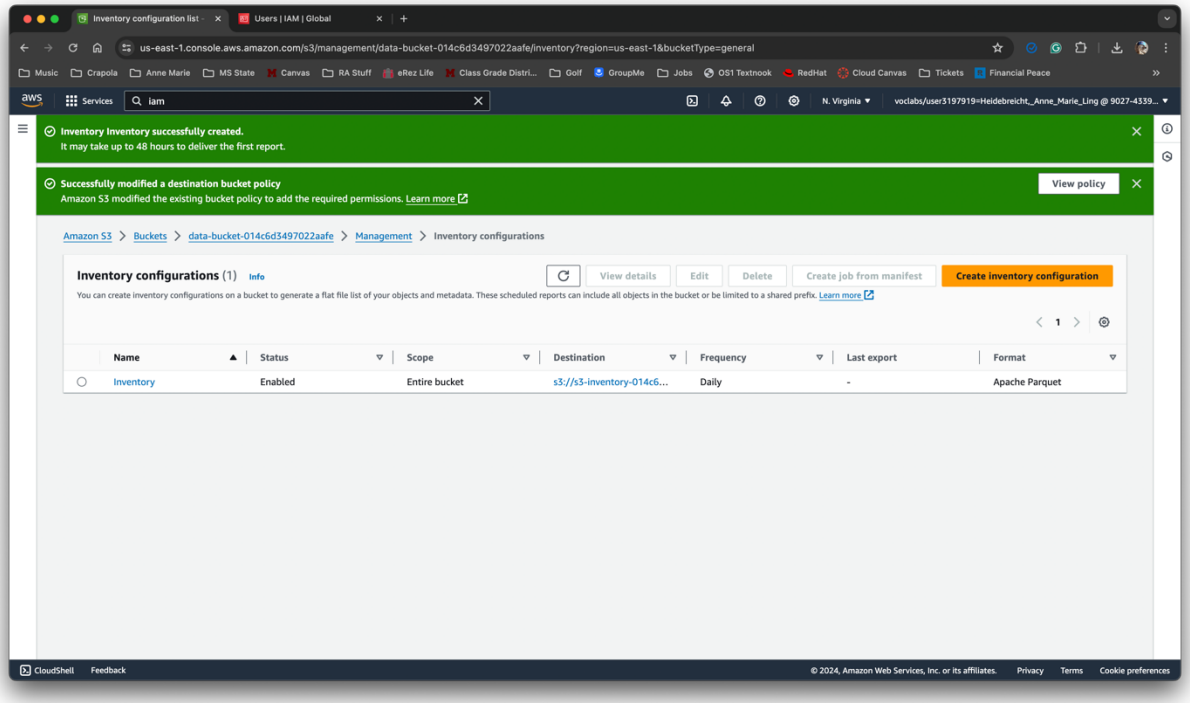
Task 1.2: Enable versioning and object-level logging on a bucket


data-bucket-014c6d349702
Users | IAM | Global
us-east-1.console.aws.amazon.com/s3/buckets/data-bucket-014c6d3497022aafe?region=us-east-1&bucketType=general&tab=properties
Music
Crapola
Anne Marie
MS State
Canvas
RA Stuff
eRez Life
Class Grade Distri...
Golf
GroupMe
Jobs
OS1 Textnook
RedHat
Cloud Canvas
Tickets
Financial Peace
aws
Services
iam
N. Virginia
voclabs/user3197919=Heidebreicht,_Anne_Marie_Ling @ 9027-4339...
Successfully edited Bucket Versioning
To transition, archive, or delete older object versions, configure lifecycle rules for this bucket.
Amazon S3
Buckets
data-bucket-014c6d3497022aafe
data-bucket-014c6d3497022aafe
Info
Objects
Properties
Permissions
Metrics
Management
Access Points
Bucket overview
AWS Region
US East (N. Virginia) us-east-1
Amazon Resource Name (ARN)
arn:aws:s3:::data-bucket-014c6d3497022aafe
Creation date
April 19, 2024, 13:53:53 (UTC-05:00)
Bucket Versioning
Edit
Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more
Bucket Versioning
Enabled
Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled
Tags (0)
Edit
You can use bucket tags to track storage costs and organize buckets. Learn more
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

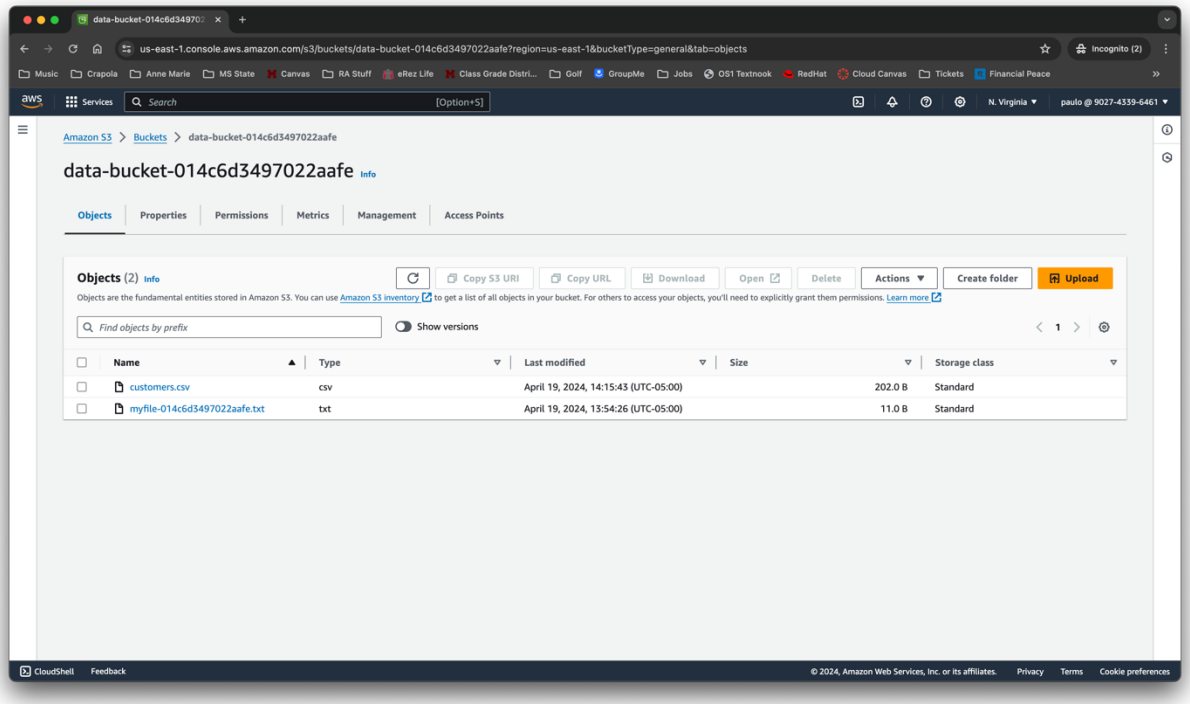

data-bucket-014c6d349702
Users | IAM | Global
us-east-1.console.aws.amazon.com/s3/buckets/data-bucket-014c6d3497022aafe?region=us-east-1&bucketType=general&tab=properties
Music
Crapola
Anne Marie
MS State
Canvas
RA Stuff
eRez Life
Class Grade Distri...
Golf
GroupMe
Jobs
OS1 Textnook
RedHat
Cloud Canvas
Tickets
Financial Peace
aws
Services
iam
N. Virginia
voclabs/user3197919=Heidebreicht,_Anne_Marie_Ling @ 9027-4339...
Successfully edited server access logging.
Name
Status
Scope
Days until transition to Archive Acces...
Days until transition to Deep Archive ...
No archive configurations
No configurations to display.
Create configuration
Server access logging
Edit
Log requests for access to your bucket. Use CloudWatch to check the health of your server access logging. Learn more
Server access logging
Enabled
Log object key format
data-bucket[YYYY]-[MM]-[DD]-[hh]-[mm]-[ss]-[UniqueString]
Destination bucket
s3://s3-objects-access-log-014c6d3497022aafe
AWS CloudTrail data events
Info
Configure in CloudTrail
Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. Learn more
Name
Access
No data events
No data events to display.
Configure in CloudTrail
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

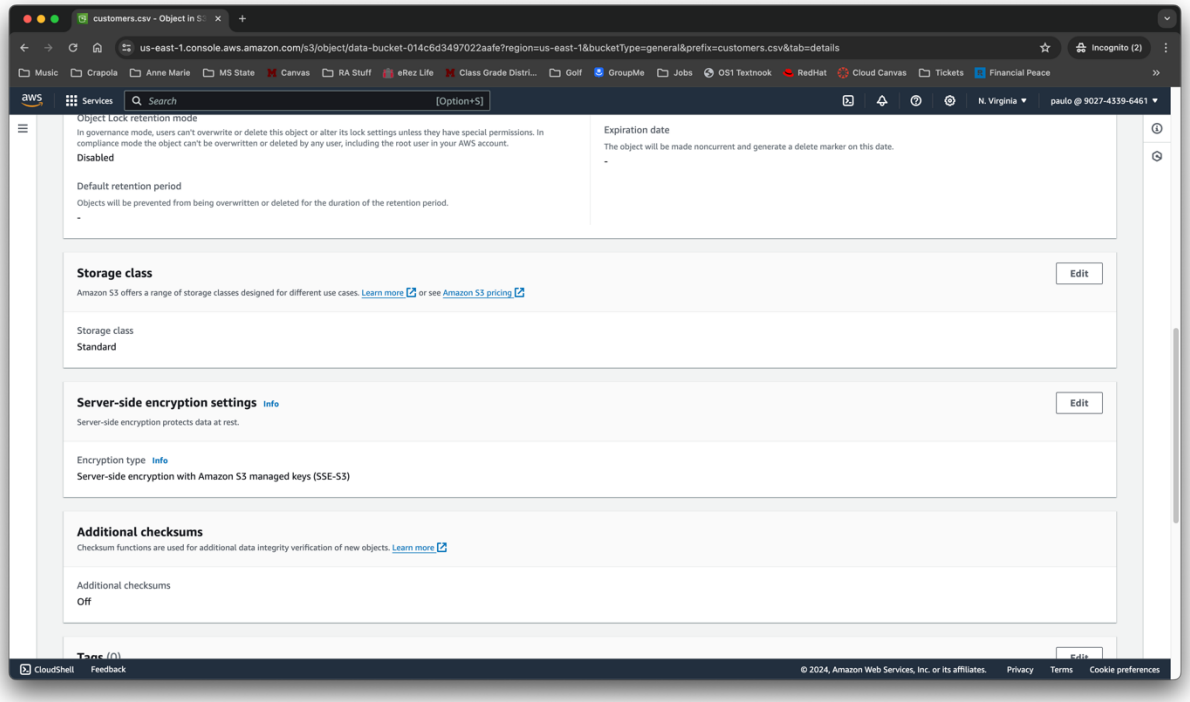


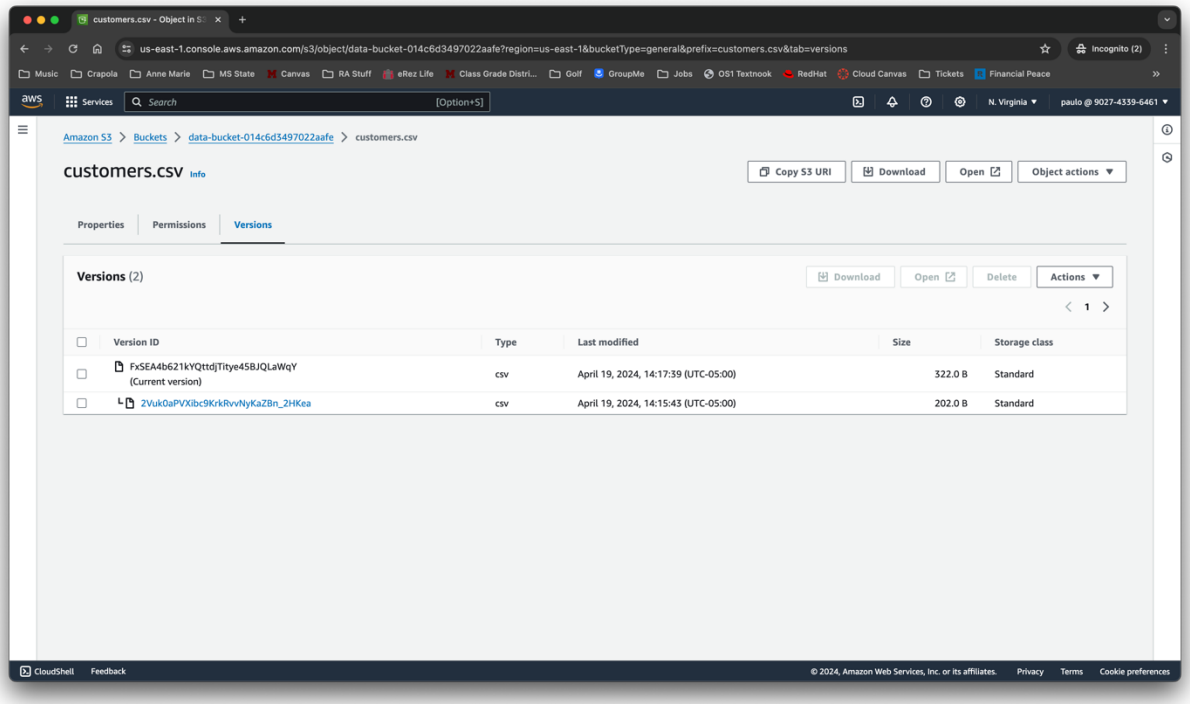
Task 1.3: Implement the S3 Inventory feature on a bucket

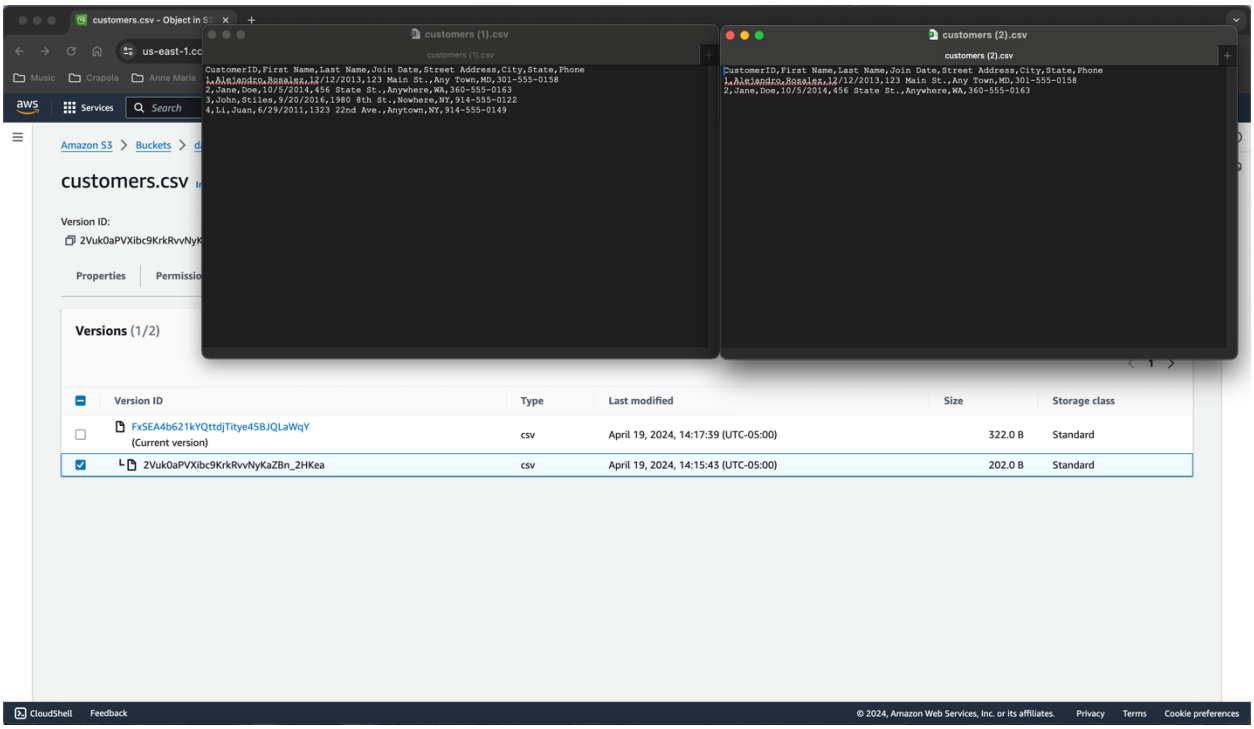


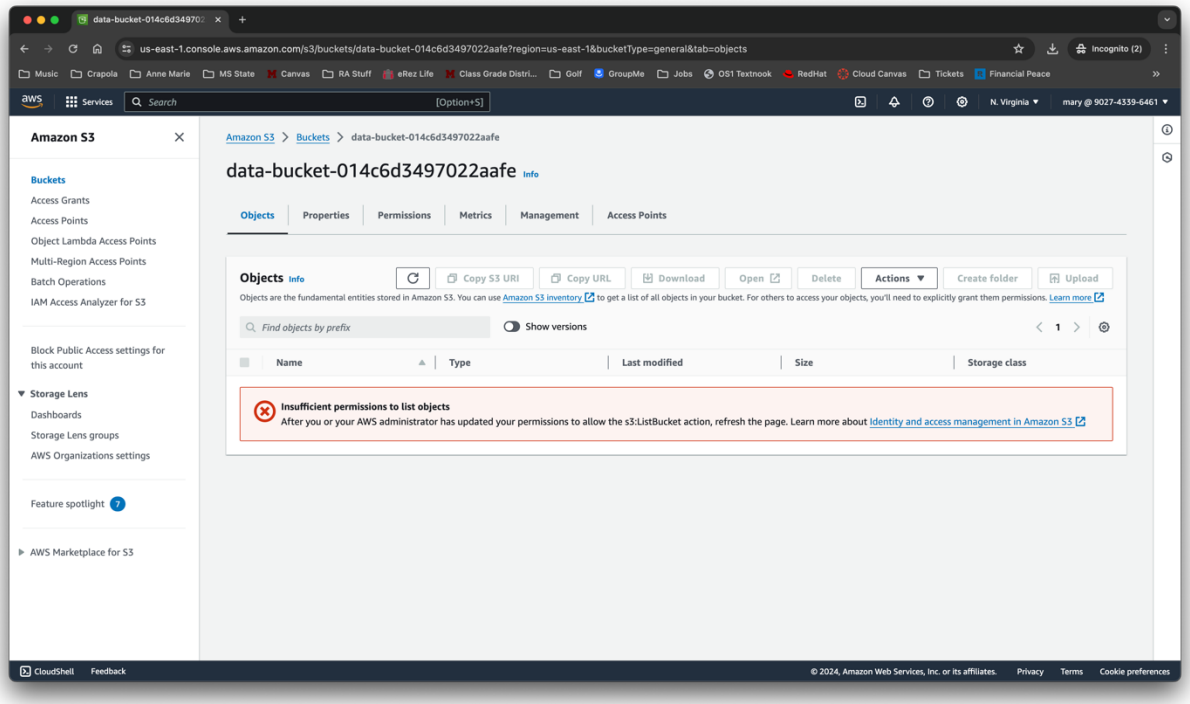
Task 1.4: Confirm that versioning works as intended


data-bucket-014c6d3497022aafe
us-east-1.console.aws.amazon.com/s3/buckets/data-bucket-014c6d3497022aafe?region=us-east-1&bucketType=general&tab=objects
Incognito (2)
Music Crapola Anne Marie MS State Canvas RA Stuff eRez Life Class Grade Distri... Golf GroupMe Jobs OS1 Textnook RedHat Cloud Canvas Tickets Financial Peace
aws Services Search [Option+S] N. Virginia paulo @ 9027-4339-6461
Amazon S3 > Buckets > data-bucket-014c6d3497022aafe
data-bucket-014c6d3497022aafe Info
Objects Properties Permissions Metrics Management Access Points
Objects (2) Info
Copy S3 URI Copy URL Download Open Delete Actions Create folder Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Find objects by prefix
Show versions
1
Name Type Last modified Size Storage class
customers.csv csv April 19, 2024, 14:15:43 (UTC-05:00) 202.0 B Standard
myfile-014c6d3497022aafe.txt txt April 19, 2024, 13:54:26 (UTC-05:00) 11.0 B Standard
CloudShell Feedback
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

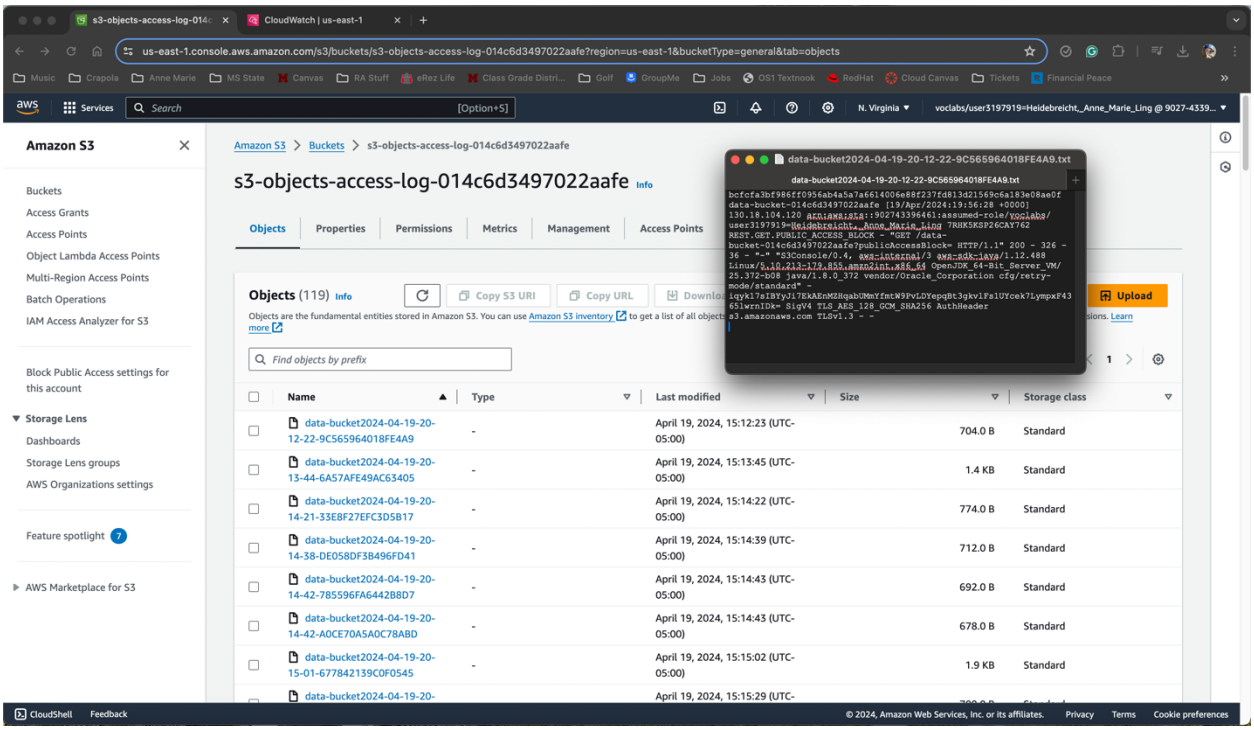

customers.csv - Object in S3
us-east-1.console.aws.amazon.com/s3/object/data-bucket-014c6d3497022aafe?region=us-east-1&bucketType=general&prefix=customers.csv&tab=details
Incognito (2)
Music Crapola Anne Marie MS State Canvas RA Stuff eRez Life Class Grade Distri... Golf GroupMe Jobs OS1 Textnook RedHat Cloud Canvas Tickets Financial Peace
aws Services Search [Option+S] N. Virginia paulo @ 9027-4339-6461
Object Lock retention mode
In governance mode, users can't overwrite or delete this object or alter its lock settings unless they have special permissions. In compliance mode the object can't be overwritten or deleted by any user, including the root user in your AWS account.
Disabled
Default retention period
Objects will be prevented from being overwritten or deleted for the duration of the retention period.
-
Expiration date
The object will be made noncurrent and generate a delete marker on this date.
-
Storage class
Edit
Amazon S3 offers a range of storage classes designed for different use cases. Learn more or see Amazon S3 pricing
Storage class
Standard
Server-side encryption settings Info
Edit
Server-side encryption protects data at rest.
Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)
Additional checksums
Checksum functions are used for additional data integrity verification of new objects. Learn more
Additional checksums
Off
CloudShell Feedback
© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

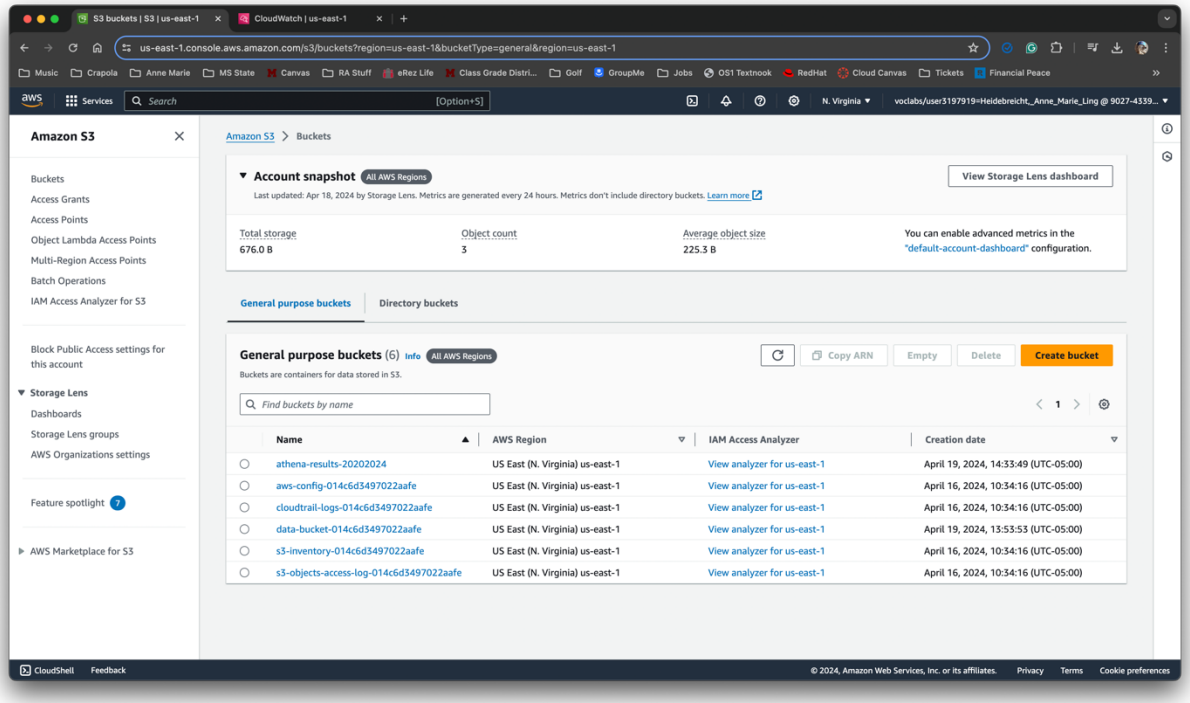

customers.csv - Object in S3
us-east-1.console.aws.amazon.com/s3/object/data-bucket-014c6d3497022aafe?region=us-east-1&bucketType=general&prefix=customers.csv&tab=versions
Amazon S3 > Buckets > data-bucket-014c6d3497022aafe > customers.csv
customers.csv Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Versions (2)
Download
Open
Delete
Actions
Version ID
Type
Last modified
Size
Storage class
FxSEA4b621kYQttdjTitye45BJQLaWqY
(Current version)
csv
April 19, 2024, 14:17:39 (UTC-05:00)
322.0 B
Standard
2Vuk0aPVXibc9KrkRvvNyKaZBn_2HKea
csv
April 19, 2024, 14:15:43 (UTC-05:00)
202.0 B
Standard
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

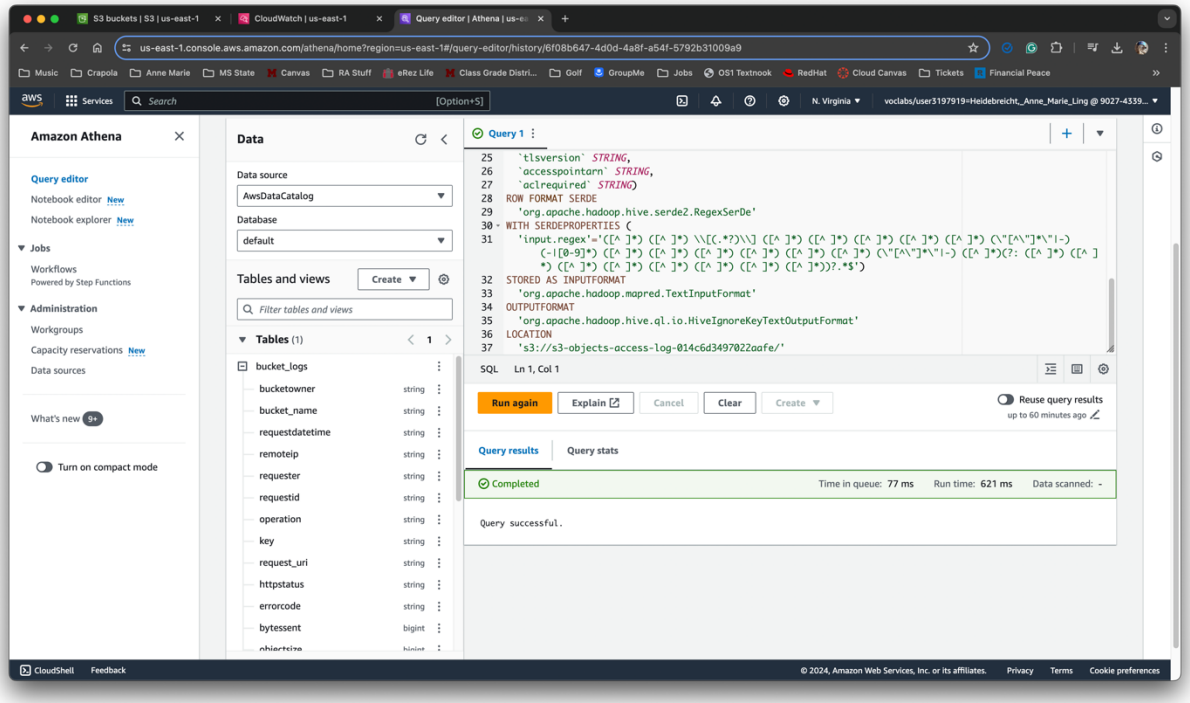

customers (1).csv
CustomerID,First Name,Last Name,Join Date,Street Address,City,State,Phone
1,Alejandro,Rosalez,12/12/2013,123 Main St.,Any Town,MO,301-555-0158
2,Jane,Doe,10/5/2014,456 State St.,Anywhere,WA,360-555-0163
3,John,Stiles,9/20/2016,1980 8th St.,Nowhere,NY,914-555-0122
4,Li,Juan,6/29/2011,1323 22nd Ave.,Anytown,NY,914-555-0149
customers (2).csv
CustomerID,First Name,Last Name,Join Date,Street Address,City,State,Phone
1,Alejandro,Rosalez,12/12/2013,123 Main St.,Any Town,MO,301-555-0158
2,Jane,Doe,10/5/2014,456 State St.,Anywhere,WA,360-555-0163
customers.csv
Version ID:
Versions (1/2)
Version ID
Type
Last modified
Size
Storage class
FxSEA4b621kYQttdjTitye45BJQLaWqY
(Current version)
csv
April 19, 2024, 14:17:39 (UTC-05:00)
322.0 B
Standard
2Vuk0aPVXibc9KrkRvvNyKaZBn_2HKea
csv
April 19, 2024, 14:15:43 (UTC-05:00)
202.0 B
Standard
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

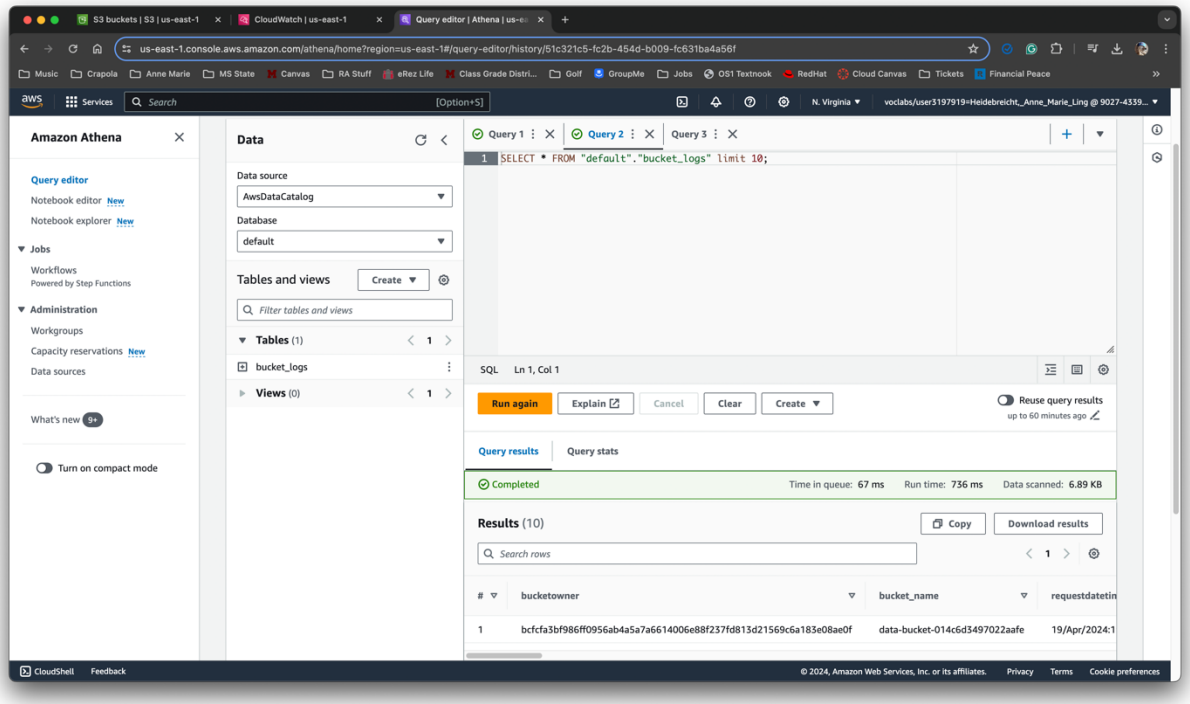


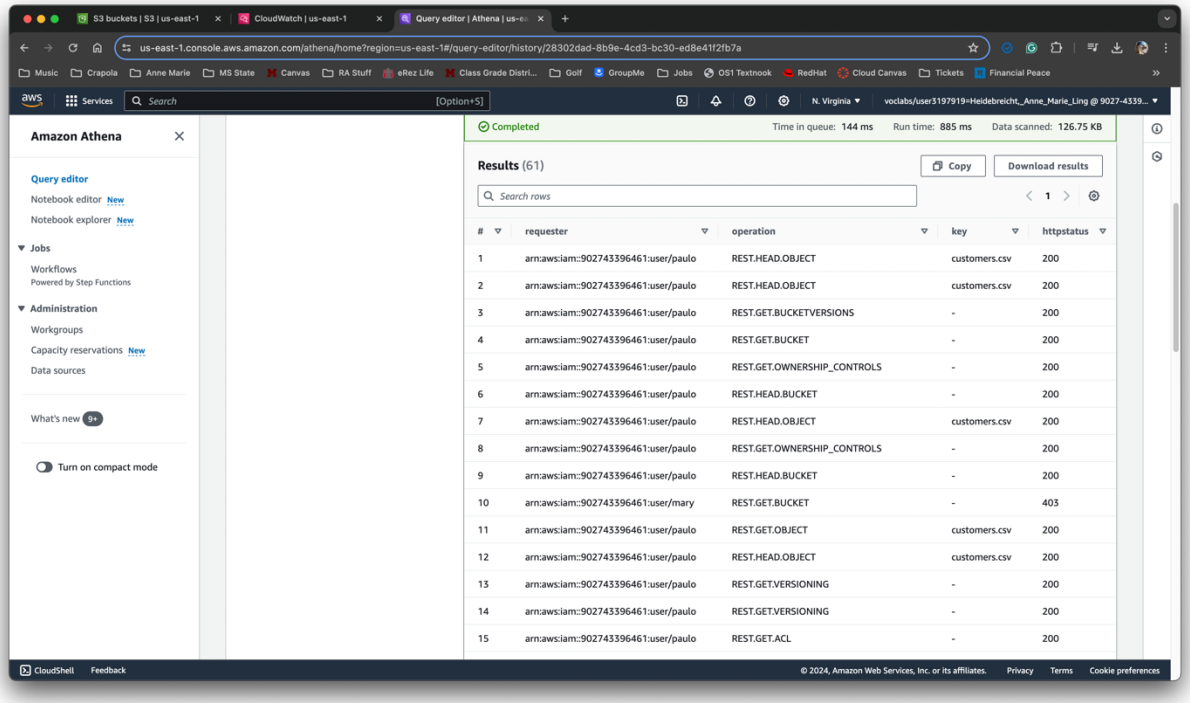
Task 1.5: Confirm object-level logging and query the access logs by using Athena



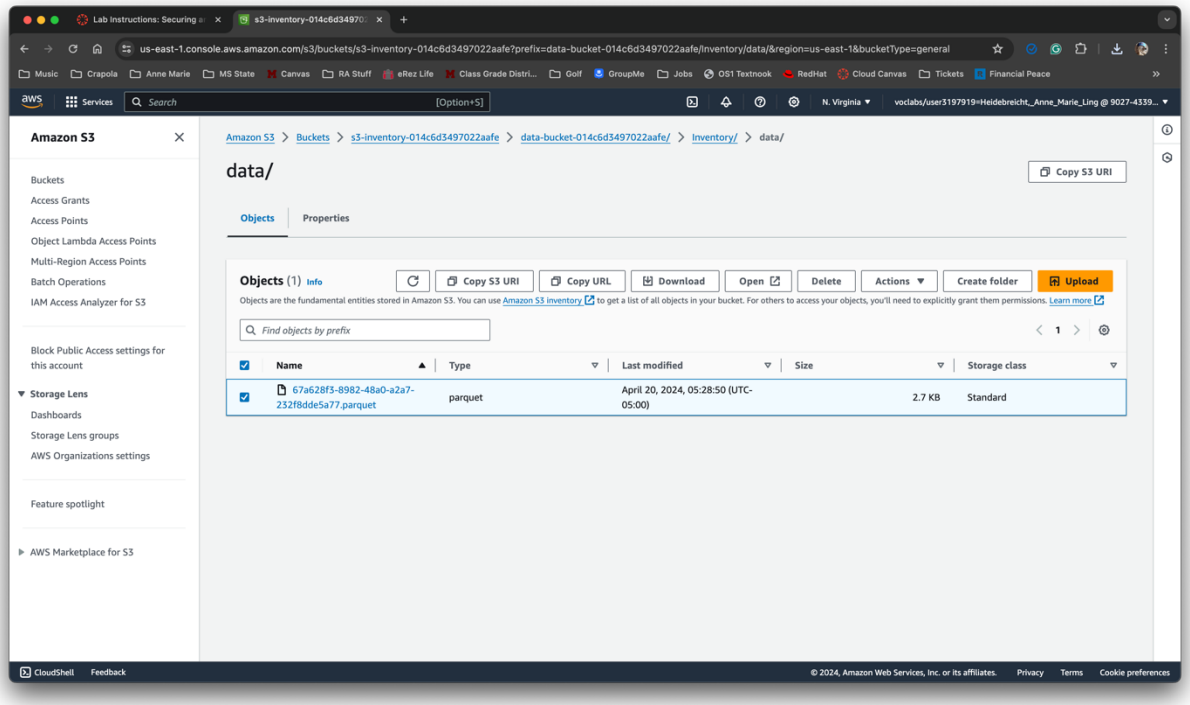

S3 buckets | S3 | us-east-1
CloudWatch | us-east-1
us-east-1.console.aws.amazon.com/s3/buckets?region=us-east-1&bucketType=general&region=us-east-1
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets
Account snapshot
All AWS Regions
View Storage Lens dashboard
Total storage
676.0 B
Object count
3
Average object size
225.3 B
You can enable advanced metrics in the "default-account-dashboard" configuration.
General purpose buckets
Directory buckets
General purpose buckets (6) Info
All AWS Regions
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
athena-results-20202024
US East (N. Virginia) us-east-1
View analyzer for us-east-1
April 19, 2024, 14:33:49 (UTC-05:00)
aws-config-014c6d3497022aafe
US East (N. Virginia) us-east-1
View analyzer for us-east-1
April 16, 2024, 10:34:16 (UTC-05:00)
cloudtrail-logs-014c6d3497022aafe
US East (N. Virginia) us-east-1
View analyzer for us-east-1
April 16, 2024, 10:34:16 (UTC-05:00)
data-bucket-014c6d3497022aafe
US East (N. Virginia) us-east-1
View analyzer for us-east-1
April 19, 2024, 13:53:53 (UTC-05:00)
s3-inventory-014c6d3497022aafe
US East (N. Virginia) us-east-1
View analyzer for us-east-1
April 16, 2024, 10:34:16 (UTC-05:00)
s3-objects-access-log-014c6d3497022aafe
US East (N. Virginia) us-east-1
View analyzer for us-east-1
April 16, 2024, 10:34:16 (UTC-05:00)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

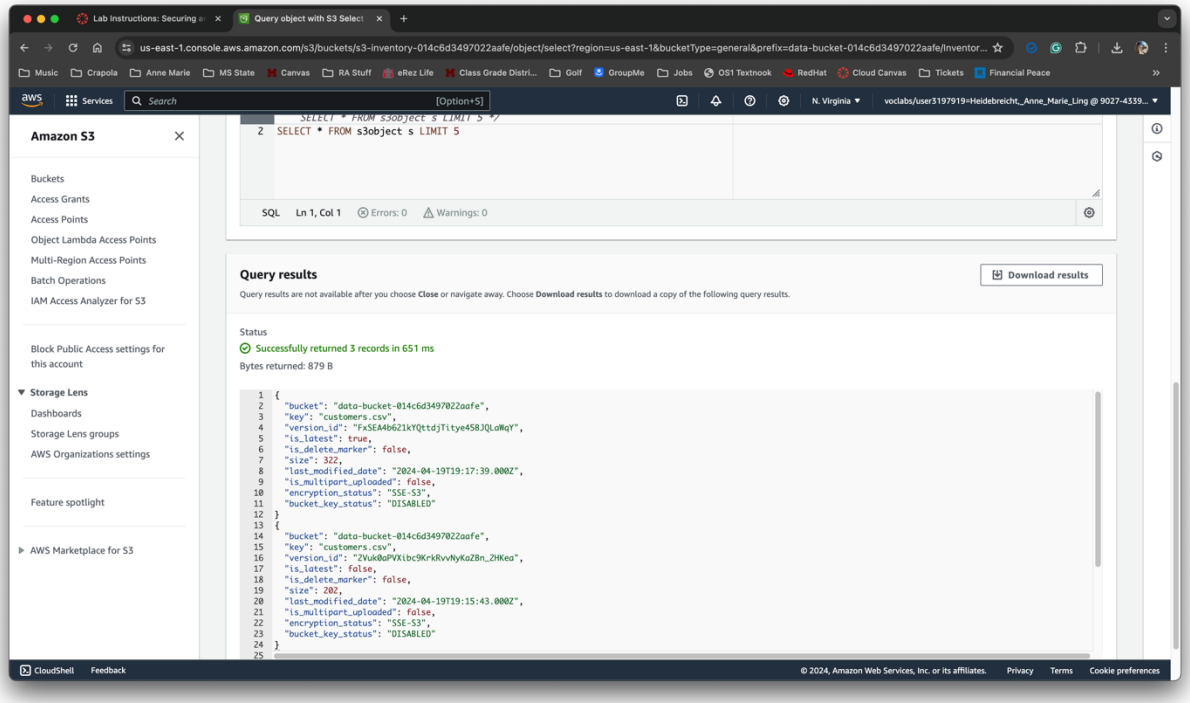

Query editor | Athena | us-east-1
us-east-1.console.aws.amazon.com/athena/home?region=us-east-1#/query-editor/history/6f08b647-4d0d-4a8f-a54f-5792b31009a9
Amazon Athena
Query editor
Notebook editor New
Notebook explorer New
Jobs
Workflows
Powered by Step Functions
Administration
Workgroups
Capacity reservations New
Data sources
What's new 9+
Turn on compact mode
Data
Data source
AwsDataCatalog
Database
default
Tables and views
Create
Filter tables and views
Tables (1)
bucket_logs
bucketowner string
bucket_name string
requestdatetime string
remoteip string
requester string
requestid string
operation string
key string
request_uri string
httpstatus string
errorcode string
bytessent bigint
Query 1
`tlsversion` STRING,
`accesspointarn` STRING,
`aclrequired` STRING)
ROW FORMAT SERDE
'org.apache.hadoop.hive.serde2.RegexSerDe'
WITH SERDEPROPERTIES (
'input.regex'='([^]*) ([^]*) \\[(.*?)\\] ([^]*) ([^]*) ([^]*) ([^]*) ([^]*) (\"[^\"]*\"|-)
(-|[0-9]*) ([^]*) ([^]*) ([^]*) ([^]*) ([^]*) ([^]*) (\"[^\"]*\"|-) ([^]*)(?: ([^]*) ([^]
) ([^]) ([^]*) ([^]*) ([^]*) ([^]*))?.*$')
STORED AS INPUTFORMAT
'org.apache.hadoop.mapred.TextInputFormat'
OUTPUTFORMAT
'org.apache.hadoop.hive.ql.io.HiveIgnoreKeyTextOutputFormat'
LOCATION
's3://s3-objects-access-log-014c6d3497022aafe/'
SQL Ln 1, Col 1
Run again
Explain
Cancel
Clear
Create
Reuse query results
up to 60 minutes ago
Query results
Query stats
Completed
Time in queue: 77 ms
Run time: 621 ms
Data scanned: -
Query successful.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

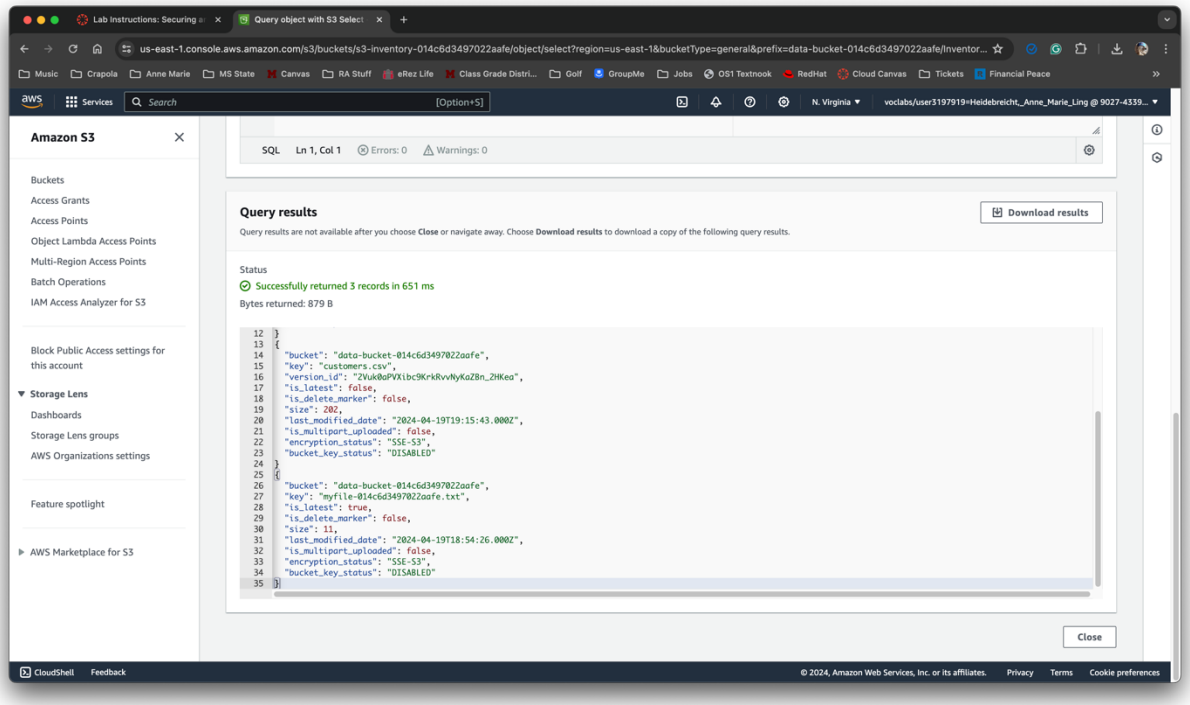




Task 1.6: Review the S3 Inventory report using S3 Select

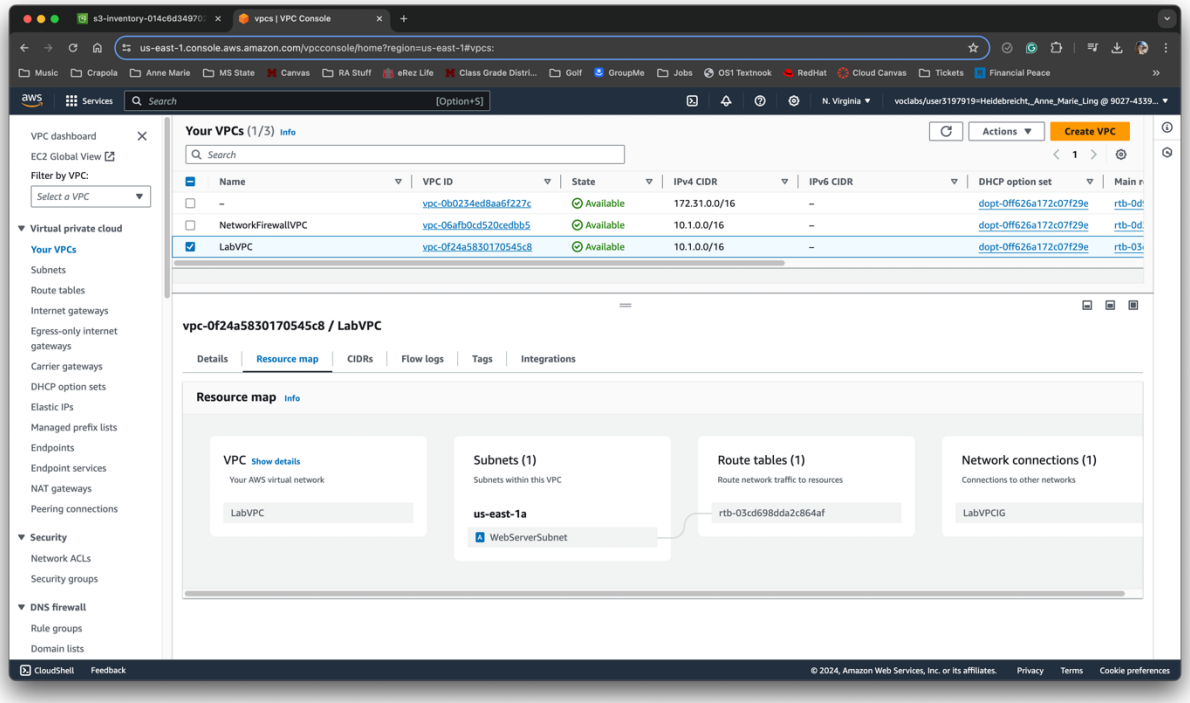

Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Amazon S3 > Buckets > s3-inventory-014c6d3497022aafe > data-bucket-014c6d3497022aafe/ > Inventory/ > data/
data/
Copy S3 URI
Objects
Properties
Objects (1) Info
Copy S3 URI
Copy URL
Download
Open
Delete
Actions
Create folder
Upload
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more
Find objects by prefix
Name
Type
Last modified
Size
Storage class
67a628f3-8982-48a0-a2a7-232f8dde5a77.parquet
parquet
April 20, 2024, 05:28:50 (UTC-05:00)
2.7 KB
Standard
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

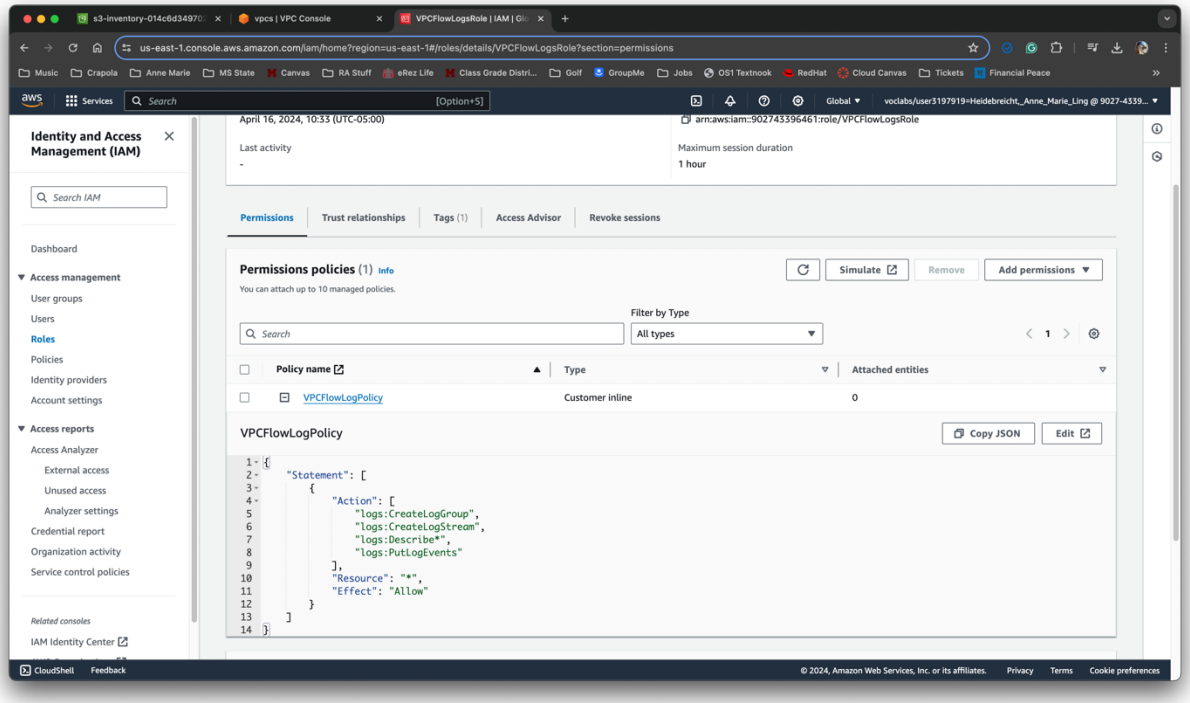

SELECT * FROM s3object s LIMIT 5
SQL
Ln 1, Col 1
Errors: 0
Warnings: 0
Query results
Download results
Query results are not available after you choose Close or navigate away. Choose Download results to download a copy of the following query results.
Status
Successfully returned 3 records in 651 ms
Bytes returned: 879 B
{
"bucket": "data-bucket-014c6d3497022aafe",
"key": "customers.csv",
"version_id": "FxSEA4b621kYQttdjTitye458JQLaWqY",
"is_latest": true,
"is_delete_marker": false,
"size": 322,
"last_modified_date": "2024-04-19T19:17:39.000Z",
"is_multipart_uploaded": false,
"encryption_status": "SSE-S3",
"bucket_key_status": "DISABLED"
}
{
"bucket": "data-bucket-014c6d3497022aafe",
"key": "customers.csv",
"version_id": "ZVuk0dPVXibc9KrkRvvNyKaZBn_ZHKea",
"is_latest": false,
"is_delete_marker": false,
"size": 202,
"last_modified_date": "2024-04-19T19:15:43.000Z",
"is_multipart_uploaded": false,
"encryption_status": "SSE-S3",
"bucket_key_status": "DISABLED"
}

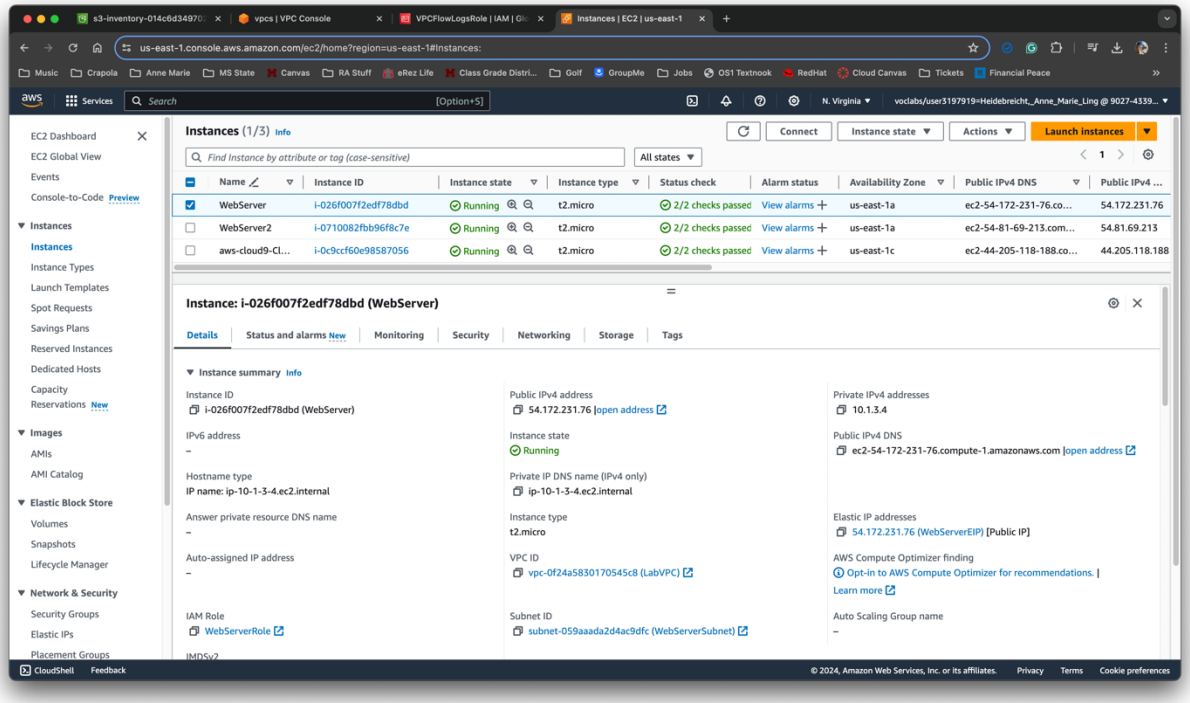


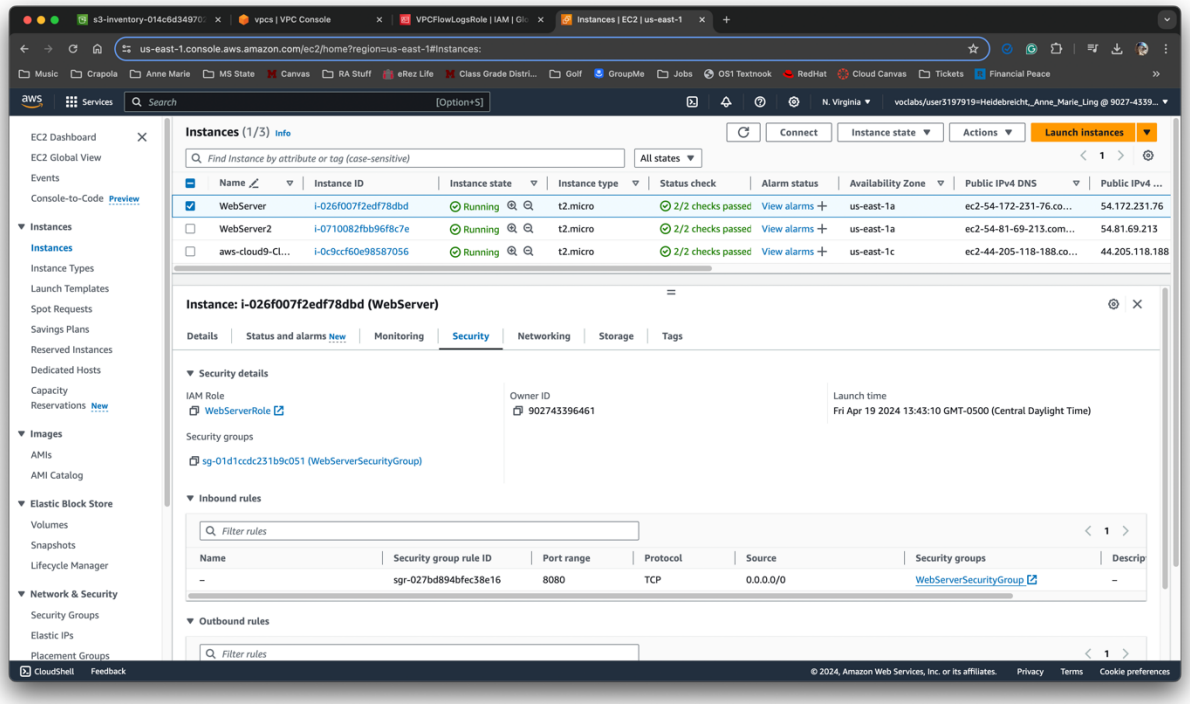
Phase 2 – Securing VPCs

Task 2.1: Review LabVPC and its associated resources

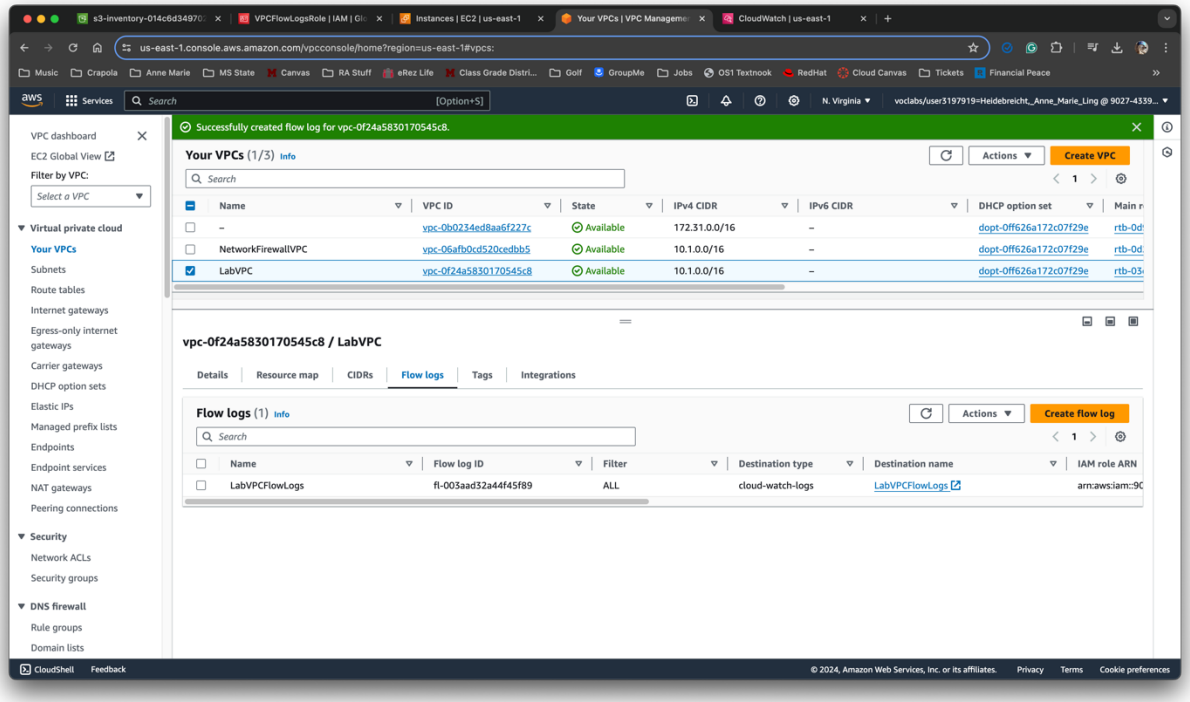



VPCFlowLogsRole | IAM | Global
us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/details/VPCFlowLogsRole?section=permissions
Identity and Access Management (IAM)
April 16, 2024, 10:33 (UTC-05:00)
arn:aws:iam::902743396461:role/VPCFlowLogsRole
Last activity
-
Maximum session duration
1 hour
Permissions
Trust relationships
Tags (1)
Access Advisor
Revoke sessions
Permissions policies (1) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter by Type
All types
Policy name
Type
Attached entities
VPCFlowLogPolicy
Customer inline
0
VPCFlowLogPolicy
Copy JSON
Edit
{
"Statement": [
{
"Action": [
"logs:CreateLogGroup",
"logs:CreateLogStream",
"logs:Describe*",
"logs:PutLogEvents"
],
"Resource": "*",
"Effect": "Allow"
}
]
}

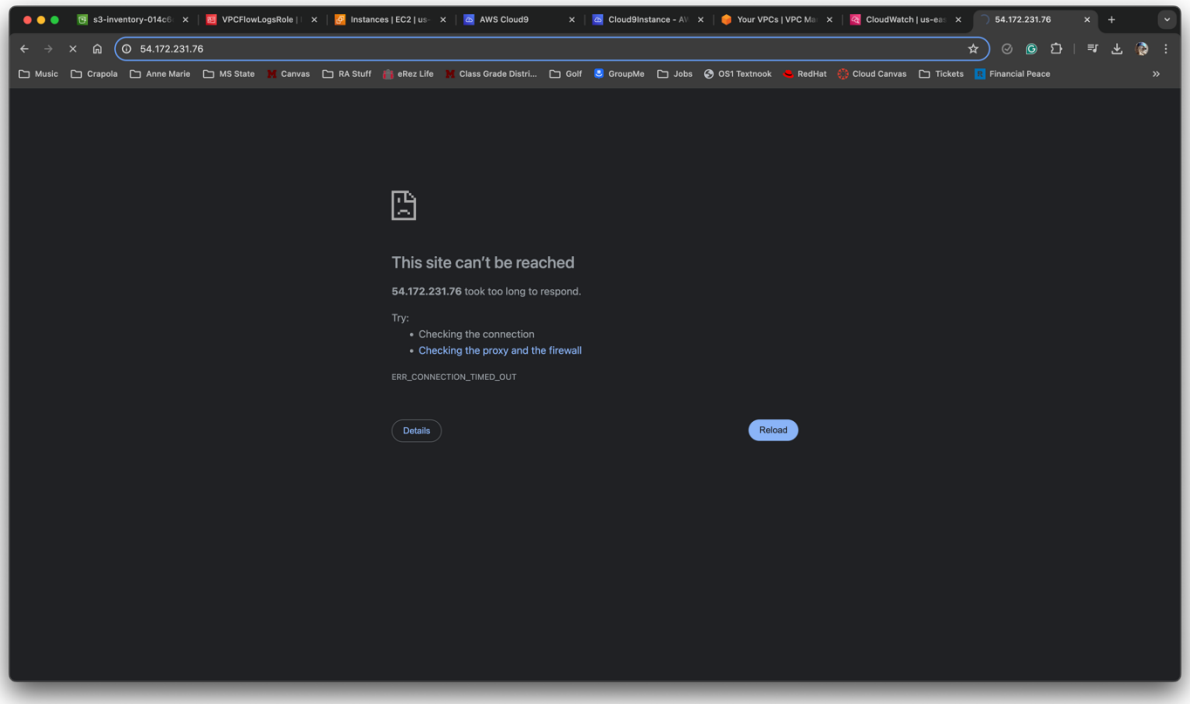

Instances | EC2 | us-east-1
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:
Instances (1/3) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
WebServer
i-026f007f2edf78dbd
Running
t2.micro
2/2 checks passed
View alarms
us-east-1a
ec2-54-172-231-76.co...
54.172.231.76
WebServer2
i-0710082fbb96f8c7e
Running
t2.micro
2/2 checks passed
View alarms
us-east-1a
ec2-54-81-69-213.com...
54.81.69.213
aws-cloud9-Cl...
i-0c9ccf60e98587056
Running
t2.micro
2/2 checks passed
View alarms
us-east-1c
ec2-44-205-118-188.co...
44.205.118.188
Instance: i-026f007f2edf78dbd (WebServer)
Details
Status and alarms New
Monitoring
Security
Networking
Storage
Tags
Instance summary Info
Instance ID
i-026f007f2edf78dbd (WebServer)
Public IPv4 address
54.172.231.76 |open address
Private IPv4 addresses
10.1.3.4
IPv6 address
-
Instance state
Running
Public IPv4 DNS
ec2-54-172-231-76.compute-1.amazonaws.com |open address
Hostname type
IP name: ip-10-1-3-4.ec2.internal
Private IP DNS name (IPv4 only)
ip-10-1-3-4.ec2.internal
Answer private resource DNS name
-
Instance type
t2.micro
Elastic IP addresses
54.172.231.76 (WebServerEIP) [Public IP]
Auto-assigned IP address
-
VPC ID
vpc-0f24a5830170545c8 (LabVPC)
AWS Compute Optimizer finding
Opt-in to AWS Compute Optimizer for recommendations. |
Learn more
IAM Role
WebServerRole
Subnet ID
subnet-059aaada2d4ac9dfc (WebServerSubnet)
Auto Scaling Group name
-
IMDSv2



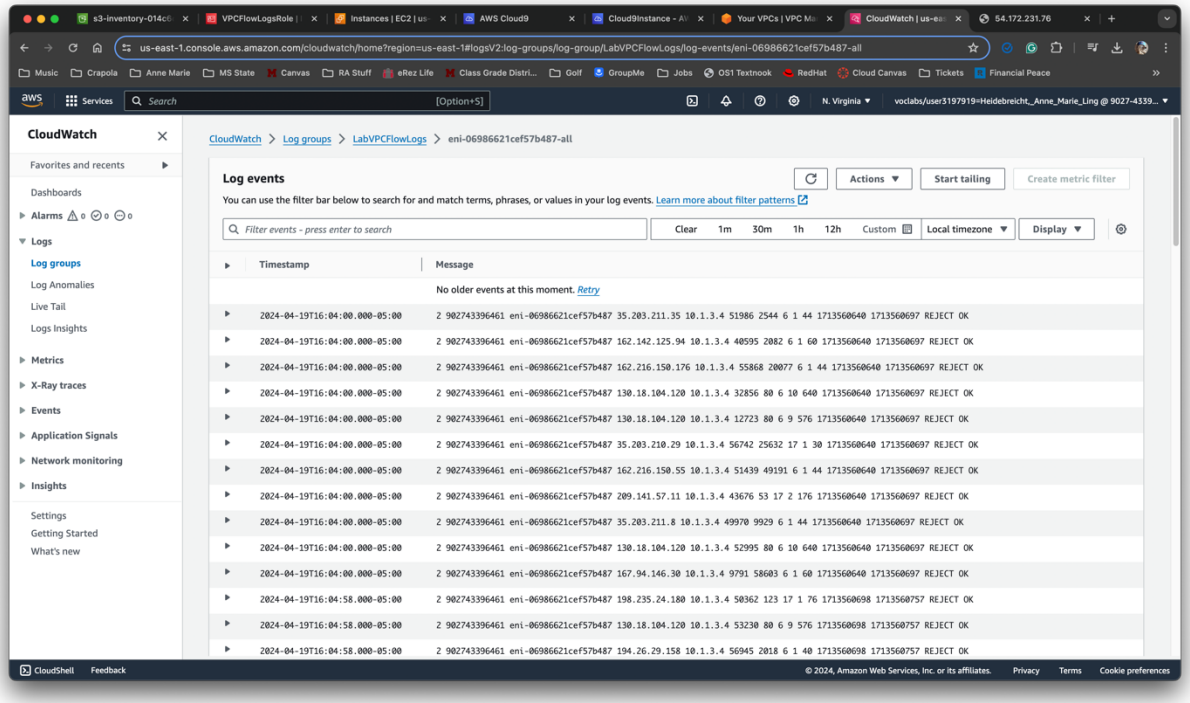
Task 2.2: Create a VPC flow log

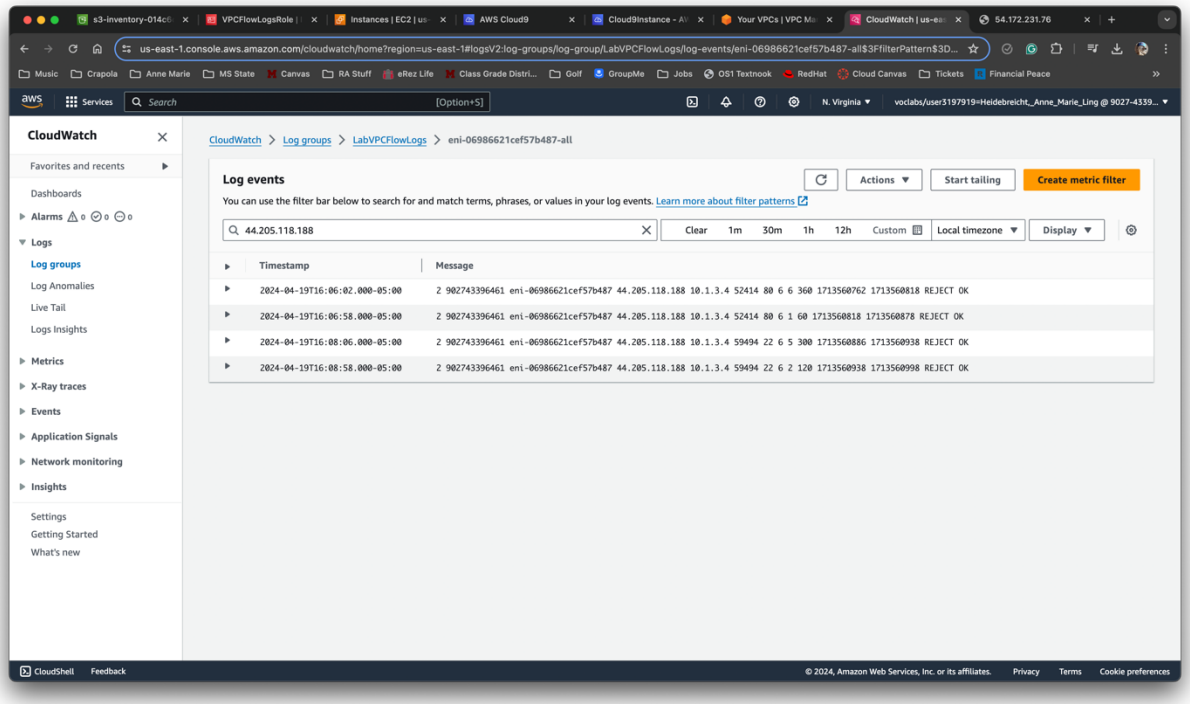


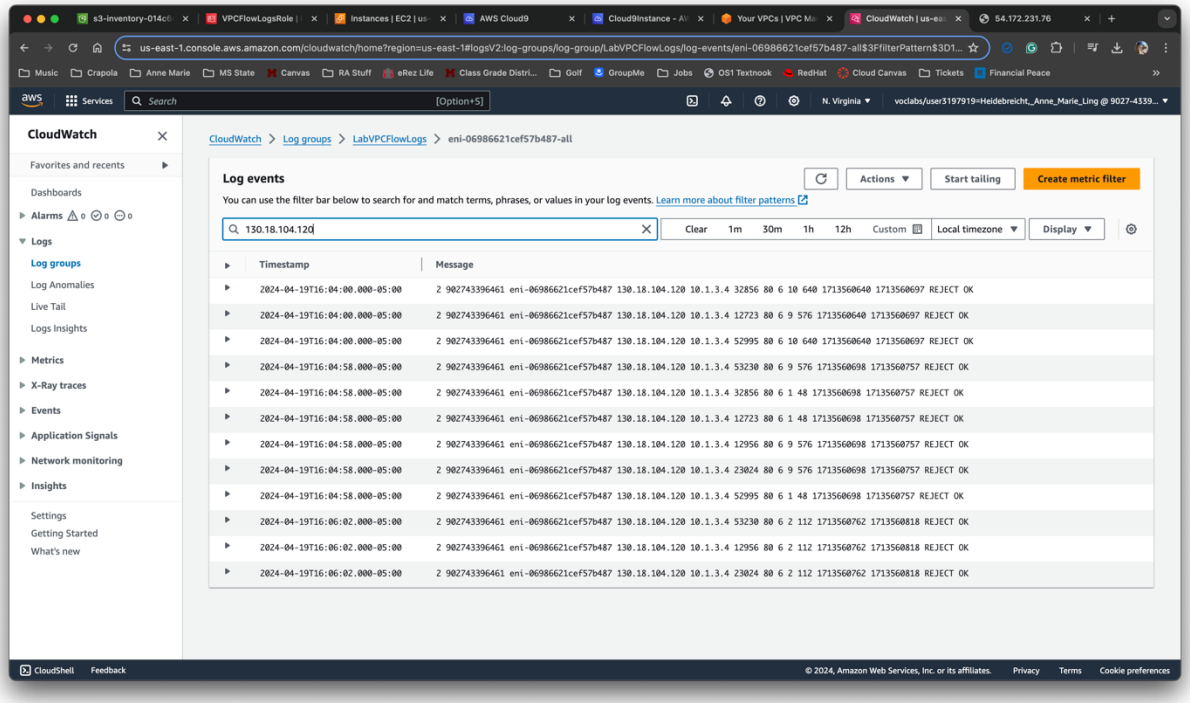
Task 2.3: Access the WebServer instance from the internet and review VPC flow logs in CloudWatch



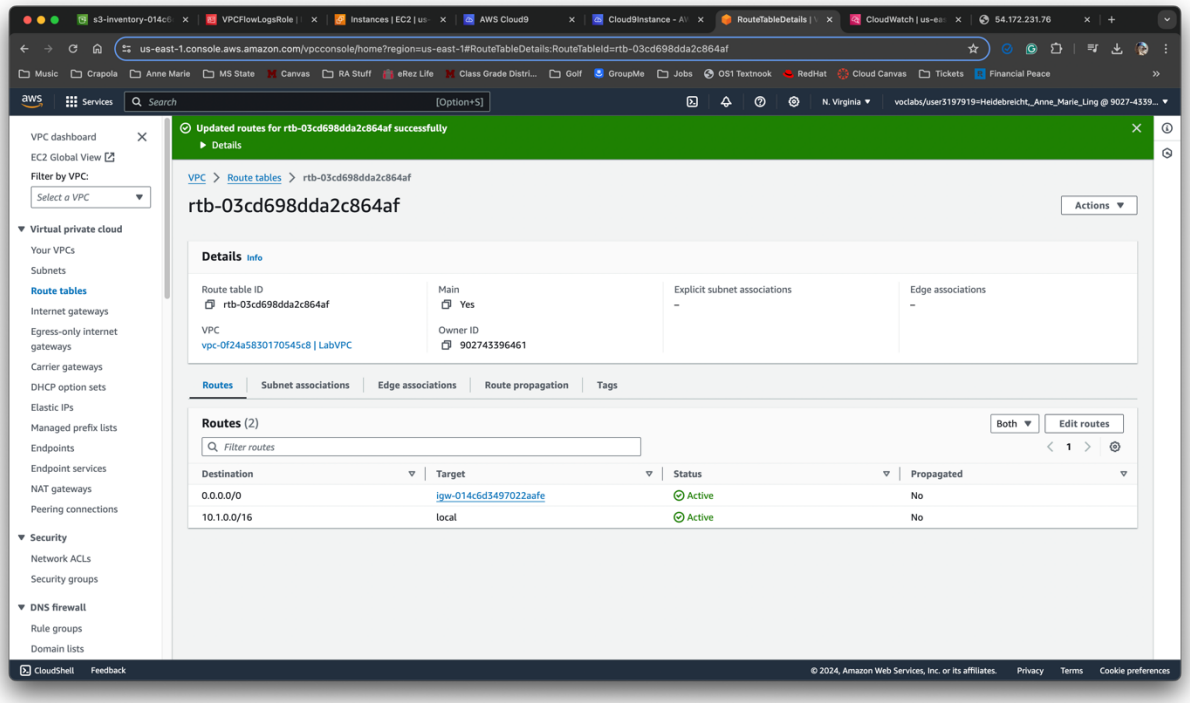

```
voclabs:~/environment $ nc -vz 54.172.231.76 80
nc: connect to 54.172.231.76 port 80 (tcp) failed: Connection timed out
voclabs:~/environment $ nc -vz 54.172.231.76 22
nc: connect to 54.172.231.76 port 22 (tcp) failed: Connection timed out
voclabs:~/environment $
```



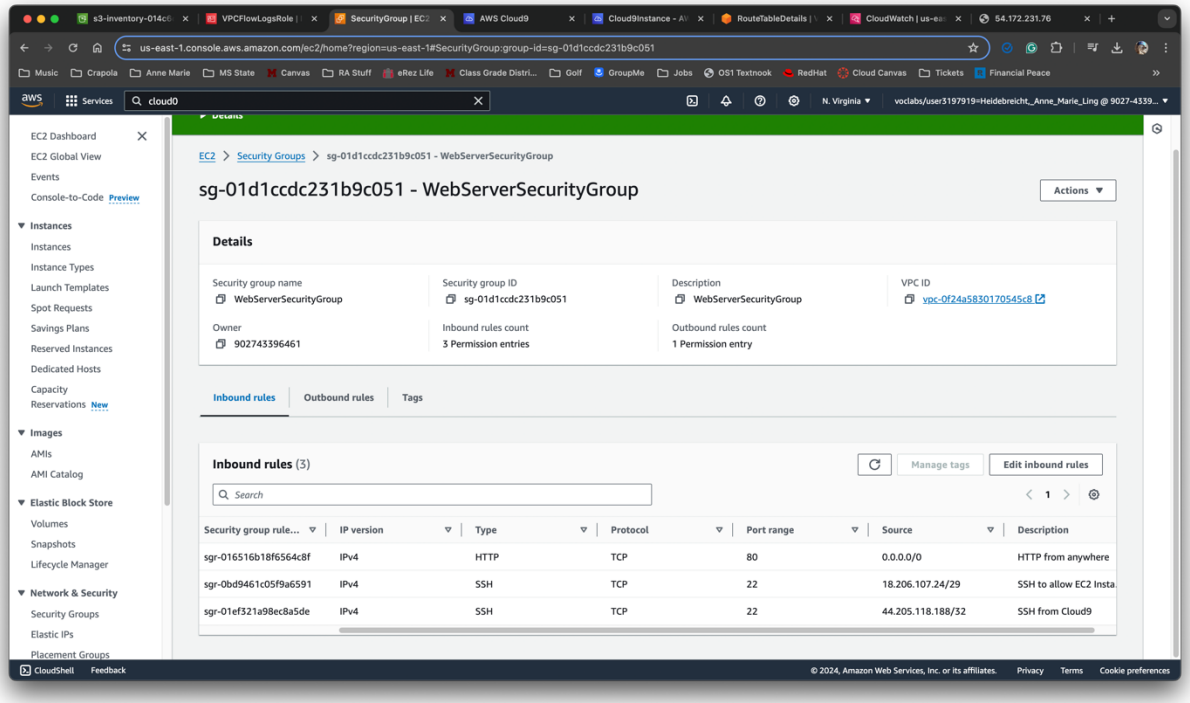

CloudWatch
Favorites and recents
Dashboards
Alarms
Logs
Log groups
Log Anomalies
Live Tail
Logs Insights
Metrics
X-Ray traces
Events
Application Signals
Network monitoring
Insights
Settings
Getting Started
What's new
CloudWatch > Log groups > LabVPCFlowLogs > eni-06986621cef57b487-all
Log events
Actions
Start tailing
Create metric filter
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns
44.205.118.188
Clear
1m
30m
1h
12h
Custom
Local timezone
Display
Timestamp
Message
2024-04-19T16:06:02.000-05:00 2 902743396461 eni-06986621cef57b487 44.205.118.188 10.1.3.4 52414 80 6 6 360 1713560762 1713560818 REJECT OK
2024-04-19T16:06:58.000-05:00 2 902743396461 eni-06986621cef57b487 44.205.118.188 10.1.3.4 52414 80 6 1 60 1713560818 1713560878 REJECT OK
2024-04-19T16:08:06.000-05:00 2 902743396461 eni-06986621cef57b487 44.205.118.188 10.1.3.4 59494 22 6 5 300 1713560886 1713560938 REJECT OK
2024-04-19T16:08:58.000-05:00 2 902743396461 eni-06986621cef57b487 44.205.118.188 10.1.3.4 59494 22 6 2 120 1713560938 1713560998 REJECT OK
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


CloudWatch
Favorites and recents
Dashboards
Alarms
Logs
Log groups
Log Anomalies
Live Tail
Logs Insights
Metrics
X-Ray traces
Events
Application Signals
Network monitoring
Insights
Settings
Getting Started
What's new
CloudWatch > Log groups > LabVPCFlowLogs > eni-06986621cef57b487-all
Log events
Actions
Start tailing
Create metric filter
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns
130.18.104.120
Clear
1m
30m
1h
12h
Custom
Local timezone
Display
Timestamp
Message
2024-04-19T16:04:00.000-05:00 2 902743396461 eni-06986621cef57b487 130.18.104.120 10.1.3.4 32856 80 6 10 640 1713560640 1713560697 REJECT OK
2024-04-19T16:04:00.000-05:00 2 902743396461 eni-06986621cef57b487 130.18.104.120 10.1.3.4 12723 80 6 9 576 1713560640 1713560697 REJECT OK
2024-04-19T16:04:00.000-05:00 2 902743396461 eni-06986621cef57b487 130.18.104.120 10.1.3.4 52995 80 6 10 640 1713560640 1713560697 REJECT OK
2024-04-19T16:04:58.000-05:00 2 902743396461 eni-06986621cef57b487 130.18.104.120 10.1.3.4 53230 80 6 9 576 1713560698 1713560757 REJECT OK
2024-04-19T16:04:58.000-05:00 2 902743396461 eni-06986621cef57b487 130.18.104.120 10.1.3.4 32856 80 6 1 48 1713560698 1713560757 REJECT OK
2024-04-19T16:04:58.000-05:00 2 902743396461 eni-06986621cef57b487 130.18.104.120 10.1.3.4 12723 80 6 1 48 1713560698 1713560757 REJECT OK
2024-04-19T16:04:58.000-05:00 2 902743396461 eni-06986621cef57b487 130.18.104.120 10.1.3.4 12956 80 6 9 576 1713560698 1713560757 REJECT OK
2024-04-19T16:04:58.000-05:00 2 902743396461 eni-06986621cef57b487 130.18.104.120 10.1.3.4 23024 80 6 9 576 1713560698 1713560757 REJECT OK
2024-04-19T16:04:58.000-05:00 2 902743396461 eni-06986621cef57b487 130.18.104.120 10.1.3.4 52995 80 6 1 48 1713560698 1713560757 REJECT OK
2024-04-19T16:06:02.000-05:00 2 902743396461 eni-06986621cef57b487 130.18.104.120 10.1.3.4 53230 80 6 2 112 1713560762 1713560818 REJECT OK
2024-04-19T16:06:02.000-05:00 2 902743396461 eni-06986621cef57b487 130.18.104.120 10.1.3.4 12956 80 6 2 112 1713560762 1713560818 REJECT OK
2024-04-19T16:06:02.000-05:00 2 902743396461 eni-06986621cef57b487 130.18.104.120 10.1.3.4 23024 80 6 2 112 1713560762 1713560818 REJECT OK
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

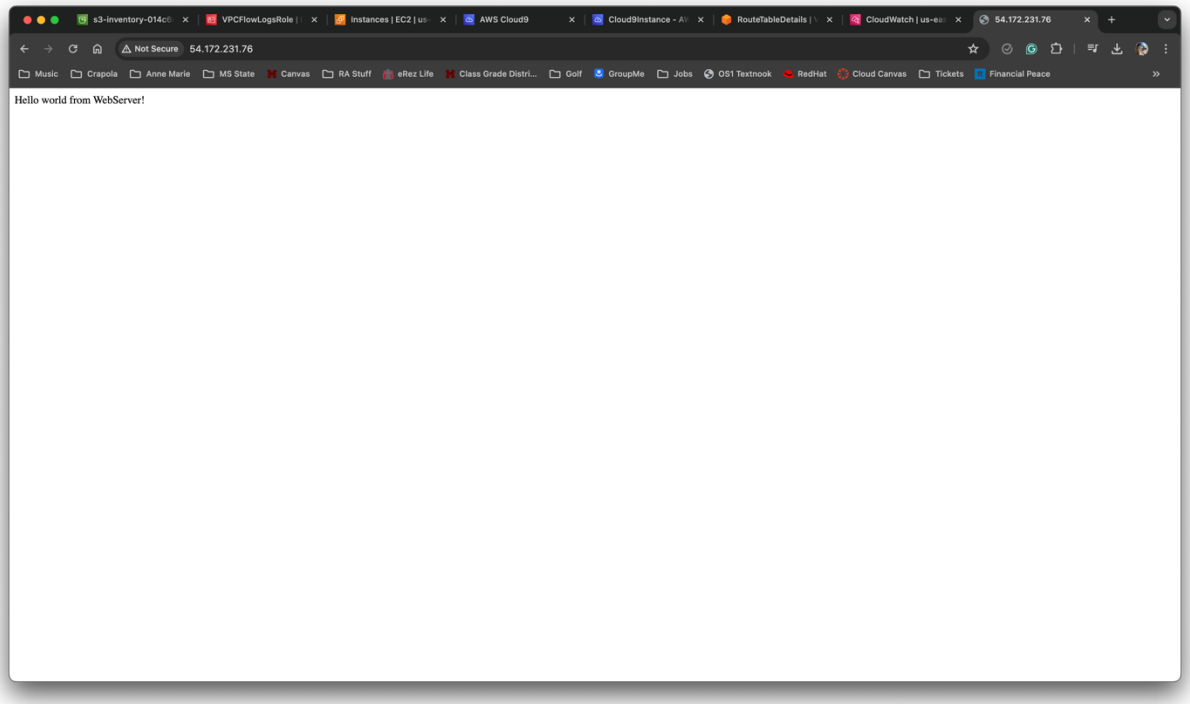
Task 2.4: Configure the route table and security group settings

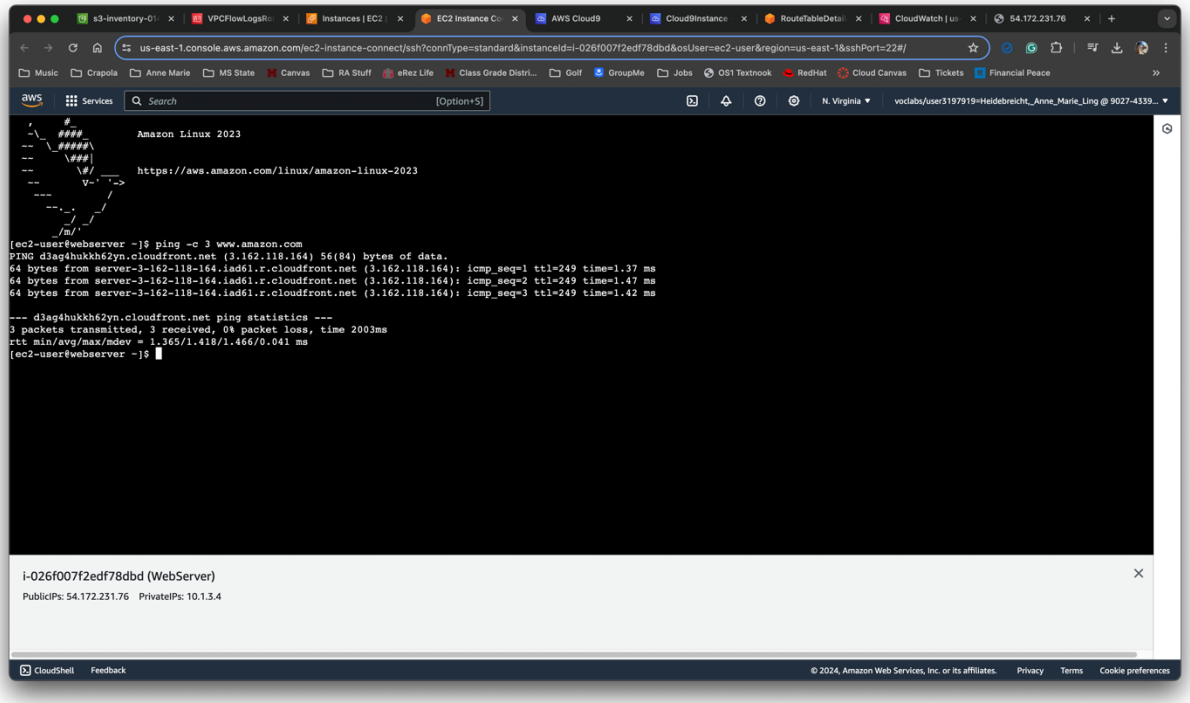



```
voclabs:~/environment $ nc -vz 54.172.231.76 80
nc: connect to 54.172.231.76 port 80 (tcp) failed: Connection timed out
```

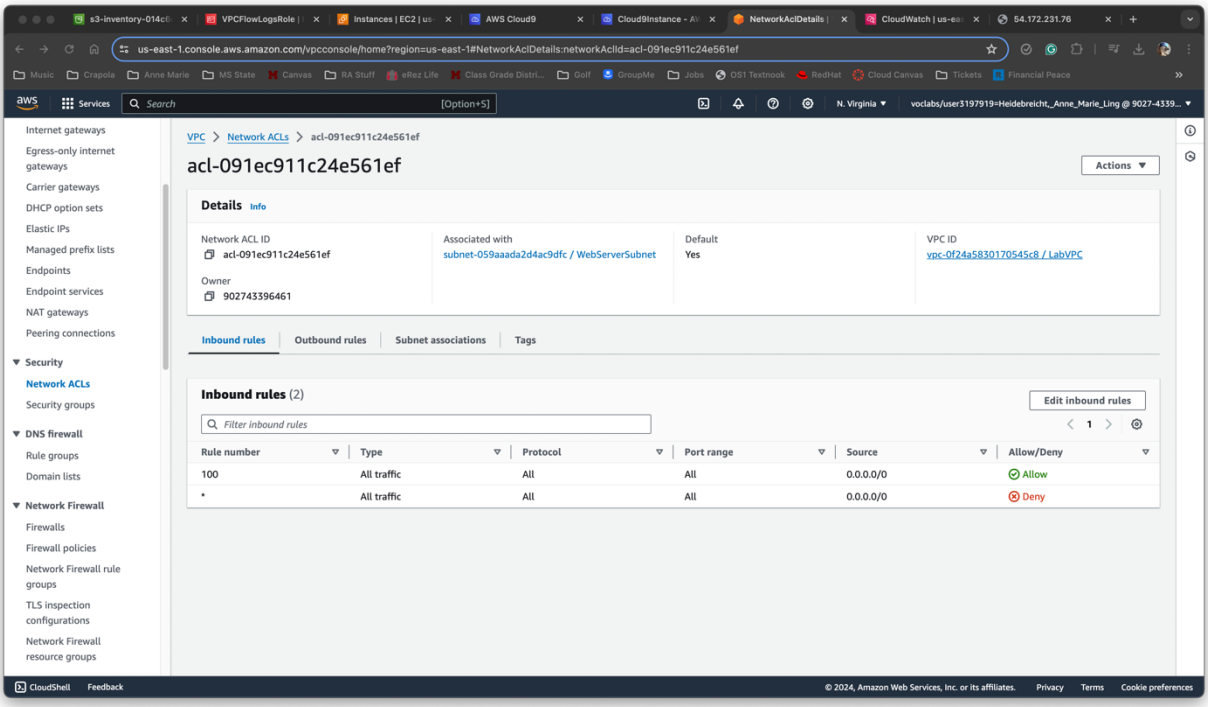



```
voclabs:~/environment $ nc -vz 54.172.231.76 22
Connection to 54.172.231.76 22 port [tcp/ssh] succeeded!
```

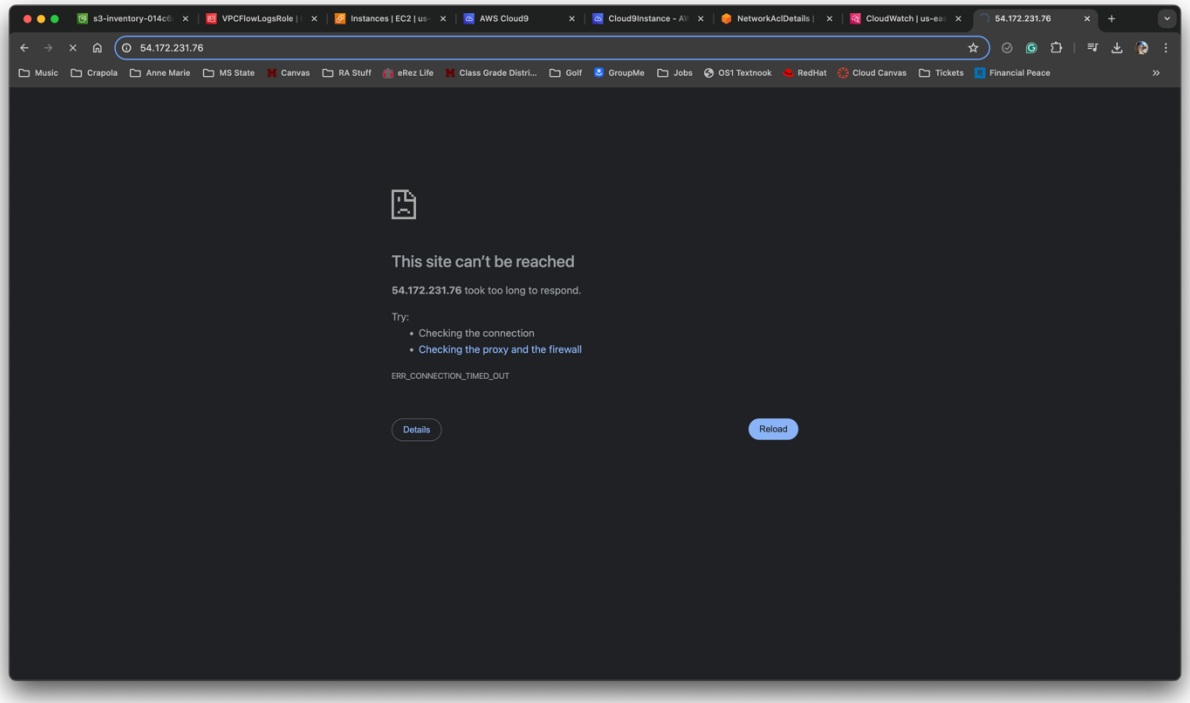




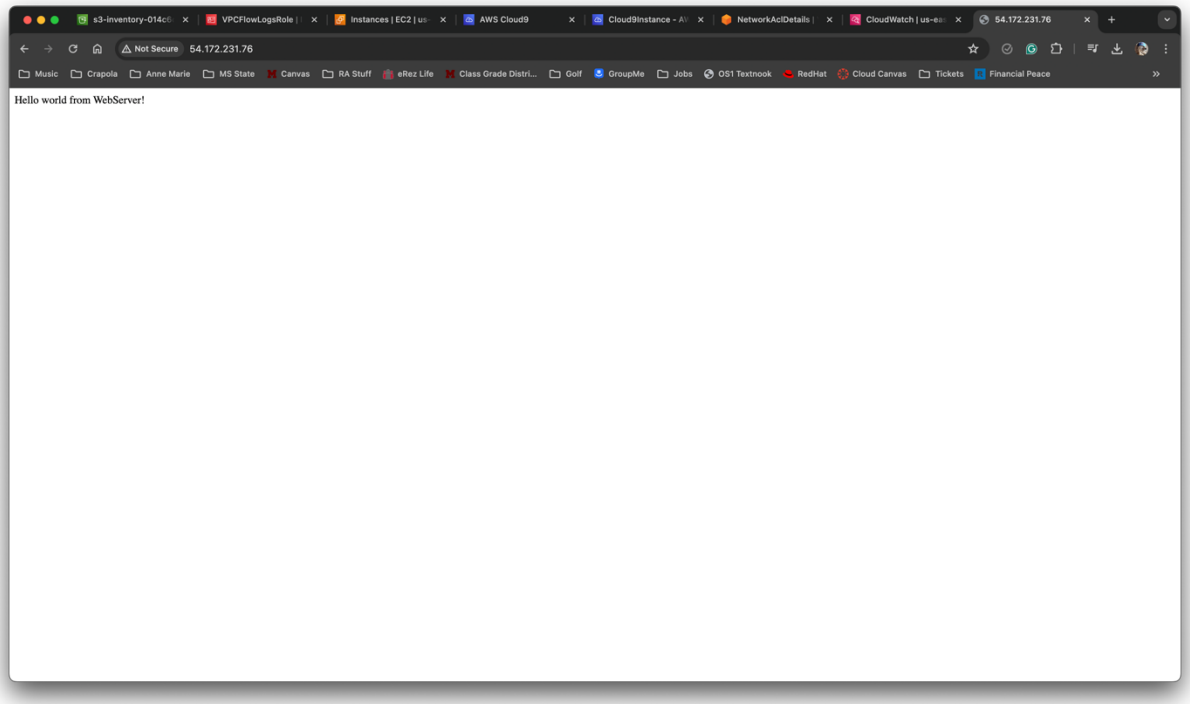
Task 2.5: Secure the WebServerSubnet with a network ACL



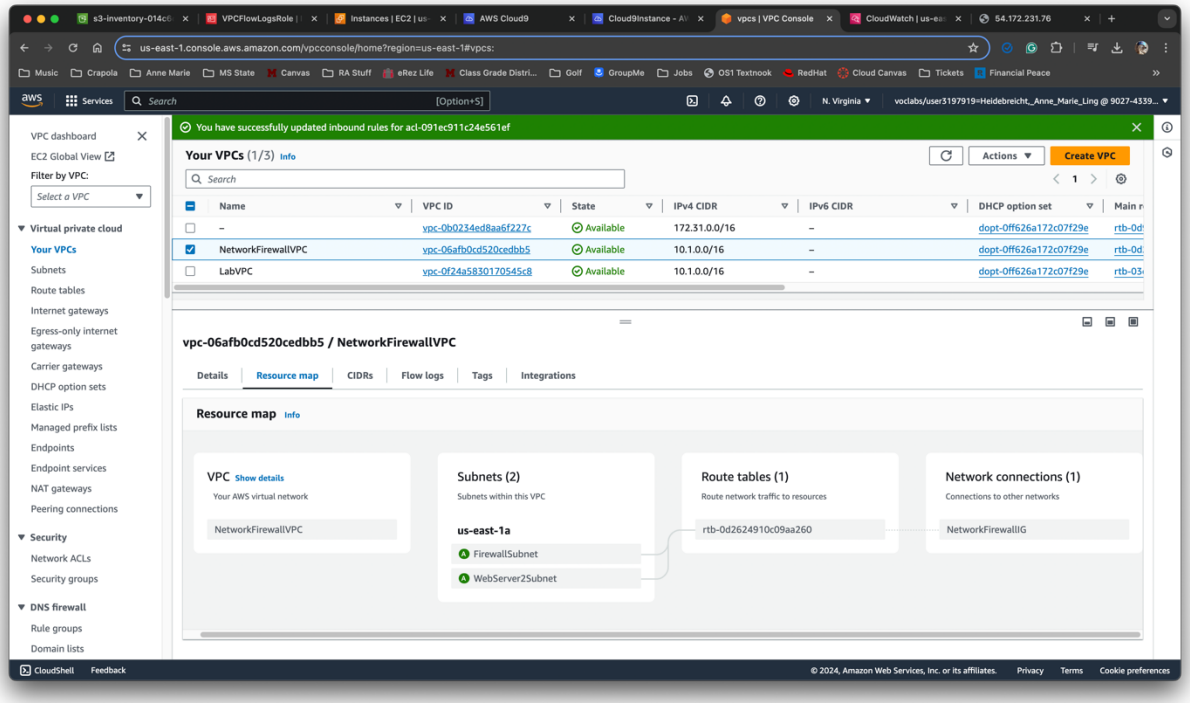

```
voclabs:~/environment $ nc -vz 54.172.231.76 22
nc: connect to 54.172.231.76 port 22 (tcp) failed: Connection timed out
```

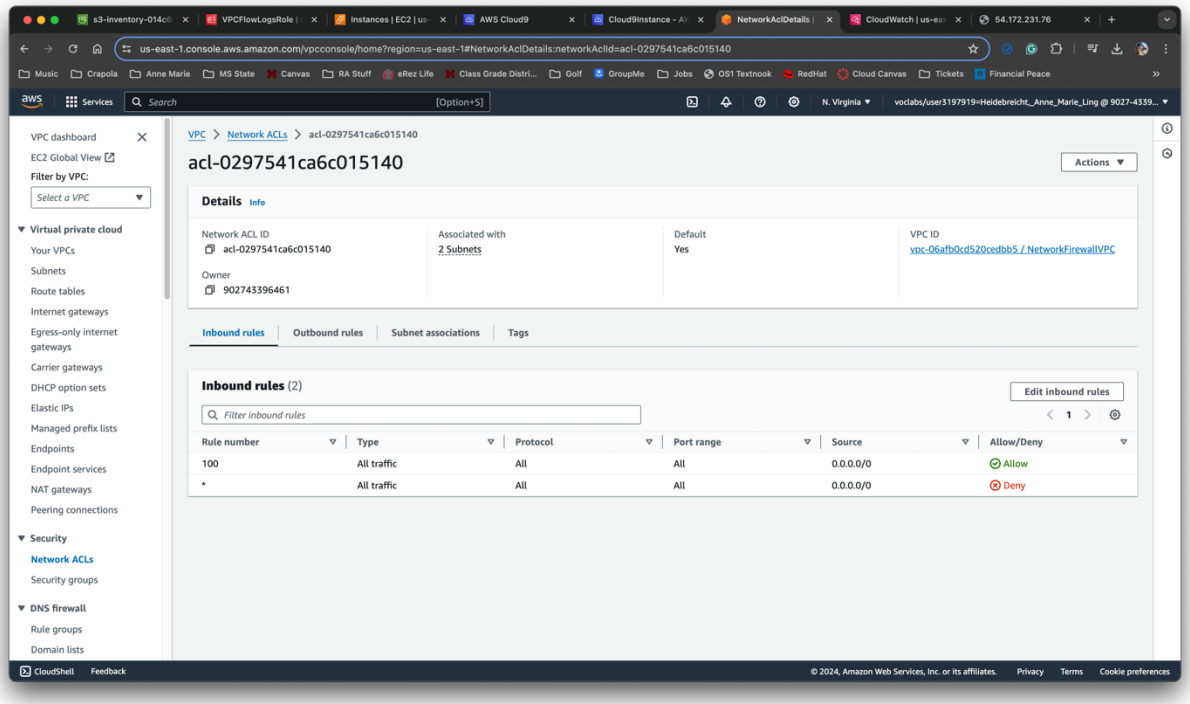


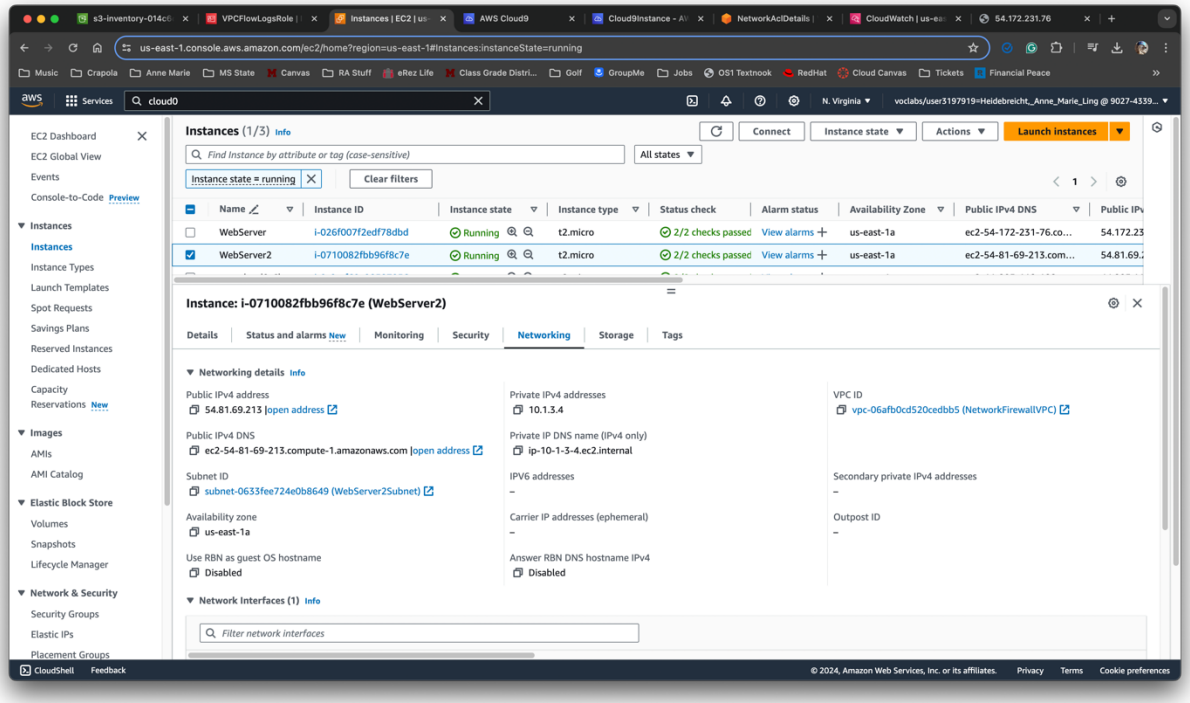

```
voclabs:~/environment $ nc -vz 54.172.231.76 22
Connection to 54.172.231.76 22 port [tcp/ssh] succeeded!
```

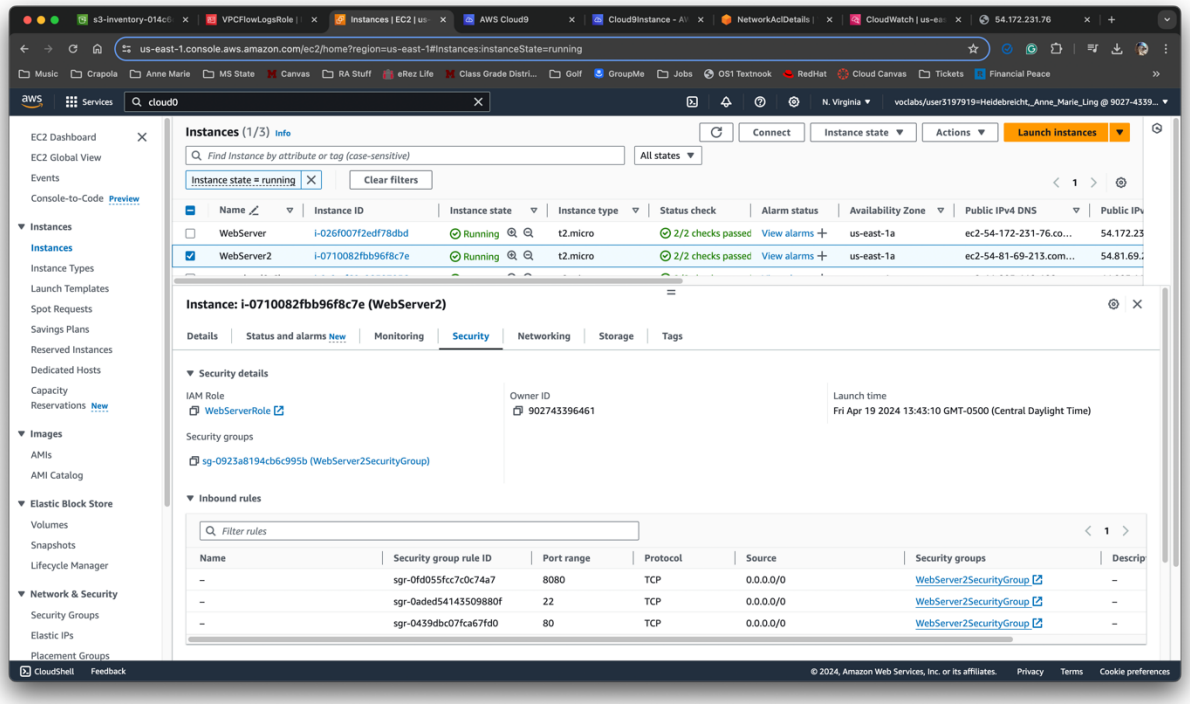


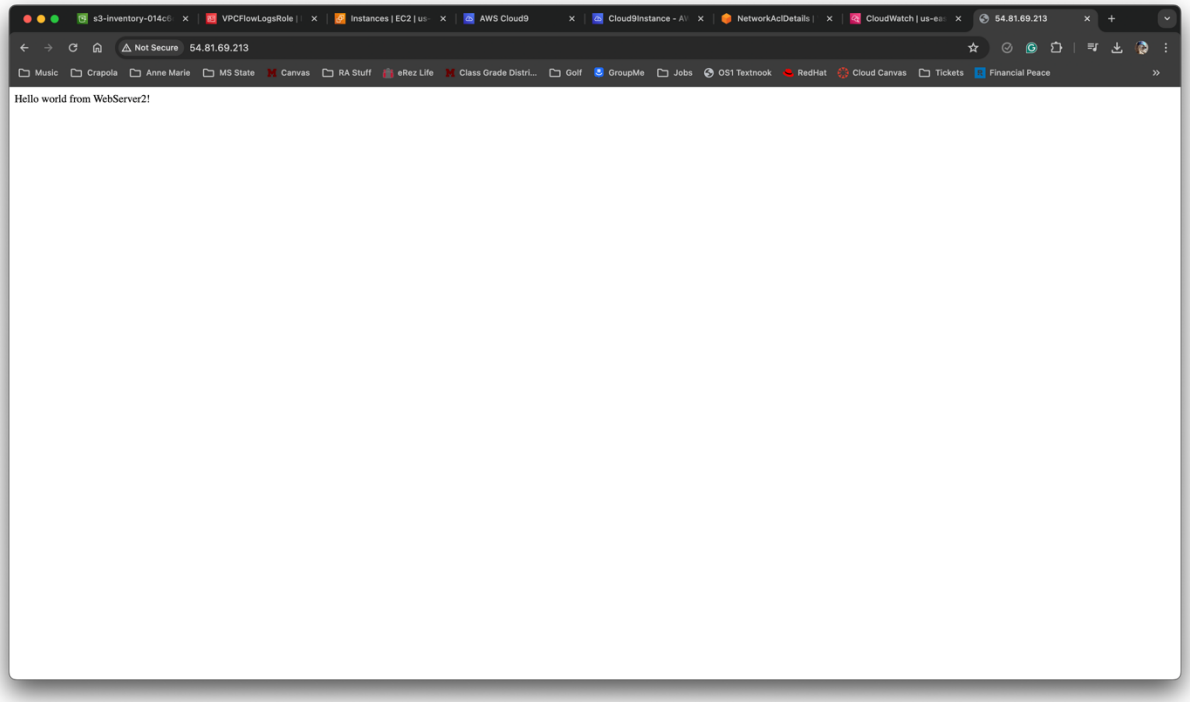
Task 2.6: Review NetworkFirewallVPC and its associated resources



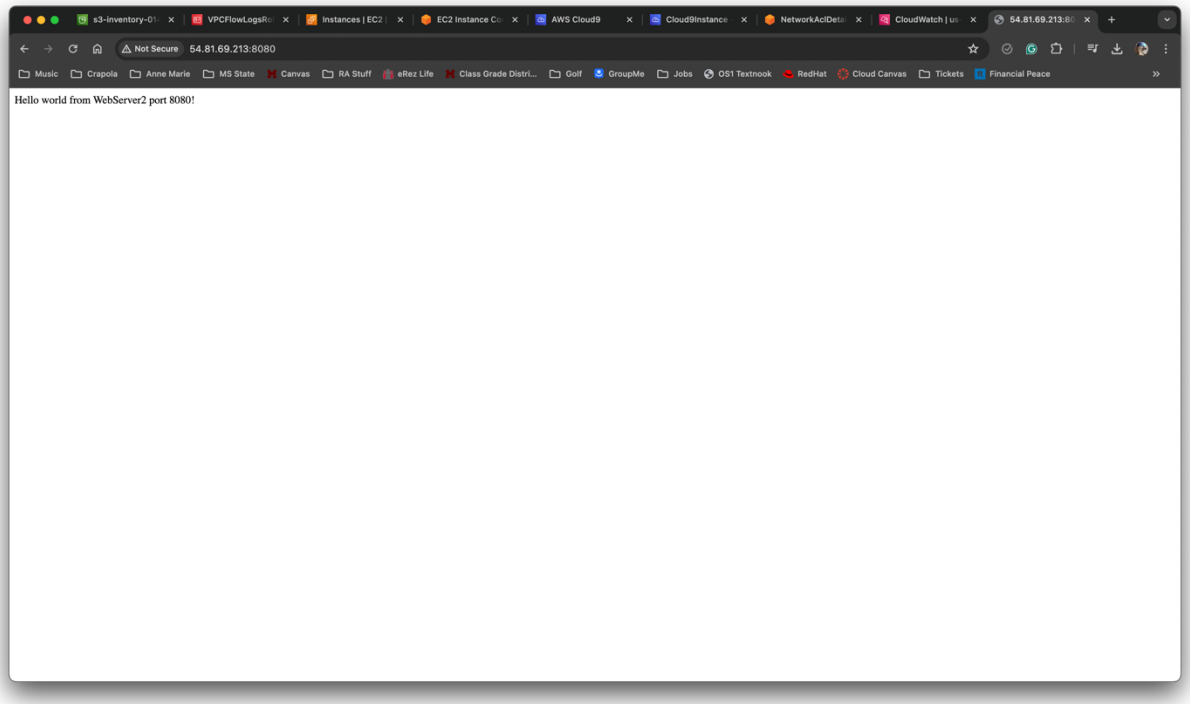

us-east-1.console.aws.amazon.com/vpcconsole/home?region=us-east-1#NetworkAclDetails:networkAclId=acl-0297541ca6c015140
VPC > Network ACLs > acl-0297541ca6c015140
acl-0297541ca6c015140
Actions
Details Info
Network ACL ID
acl-0297541ca6c015140
Associated with
2 Subnets
Default
Yes
VPC ID
vpc-06afb0cd520cedbb5 / NetworkFirewallVPC
Owner
902743396461
Inbound rules
Outbound rules
Subnet associations
Tags
Inbound rules (2)
Edit inbound rules
Filter inbound rules
Rule number
Type
Protocol
Port range
Source
Allow/Deny
100
All traffic
All
All
0.0.0.0/0
Allow
*
All traffic
All
All
0.0.0.0/0
Deny


us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:instanceState=running
Instances (1/3) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
Instance state = running
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
WebServer
i-026f007f2edf78dbd
Running
t2.micro
2/2 checks passed
View alarms
us-east-1a
ec2-54-172-231-76.co...
WebServer2
i-0710082fbb96f8c7e
Running
t2.micro
2/2 checks passed
View alarms
us-east-1a
ec2-54-81-69-213.com...
Instance: i-0710082fbb96f8c7e (WebServer2)
Details
Status and alarms New
Monitoring
Security
Networking
Storage
Tags
Networking details Info
Public IPv4 address
54.81.69.213 |open address
Private IPv4 addresses
10.1.3.4
VPC ID
vpc-06afb0cd520cedbb5 (NetworkFirewallVPC)
Public IPv4 DNS
ec2-54-81-69-213.compute-1.amazonaws.com |open address
Private IP DNS name (IPv4 only)
ip-10-1-3-4.ec2.internal
Subnet ID
subnet-0633fee724e0b8649 (WebServer2Subnet)
IPV6 addresses
Secondary private IPv4 addresses
Availability zone
us-east-1a
Carrier IP addresses (ephemeral)
Outpost ID
Use RBN as guest OS hostname
Disabled
Answer RBN DNS hostname IPv4
Disabled
Network Interfaces (1) Info
Filter network interfaces

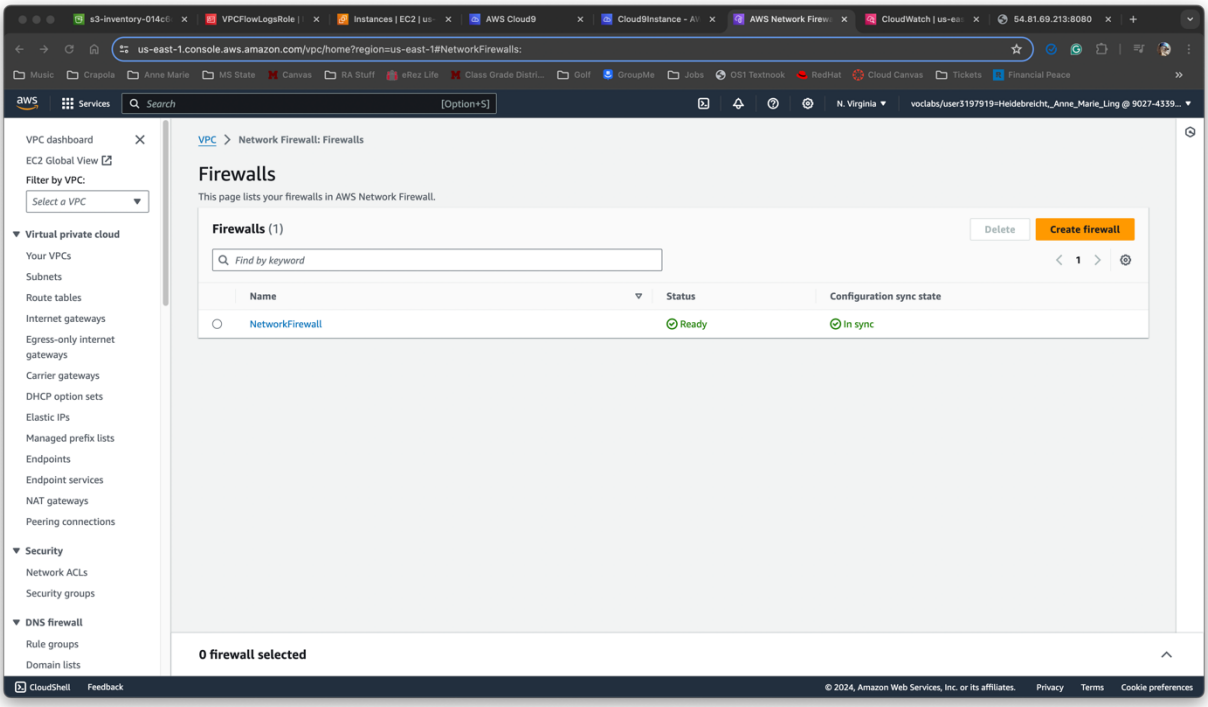




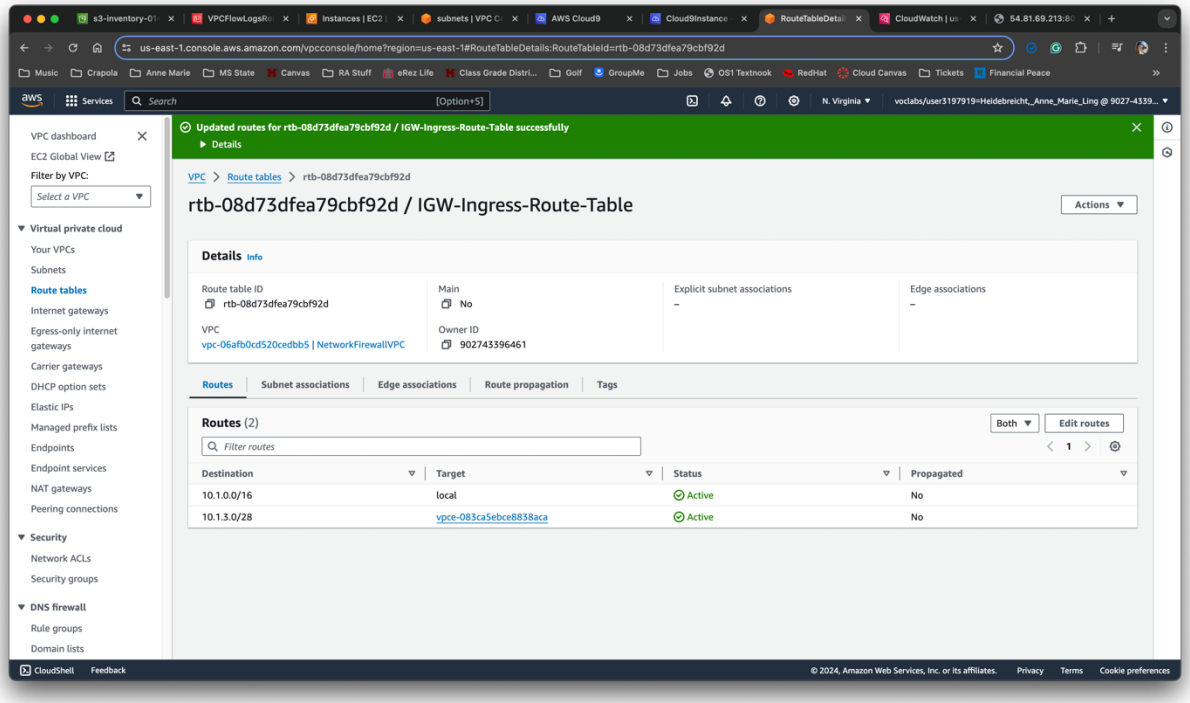

```
voclabs:~/environment $ nc -vz 54.81.69.213 22
Connection to 54.81.69.213 22 port [tcp/ssh] succeeded!
```

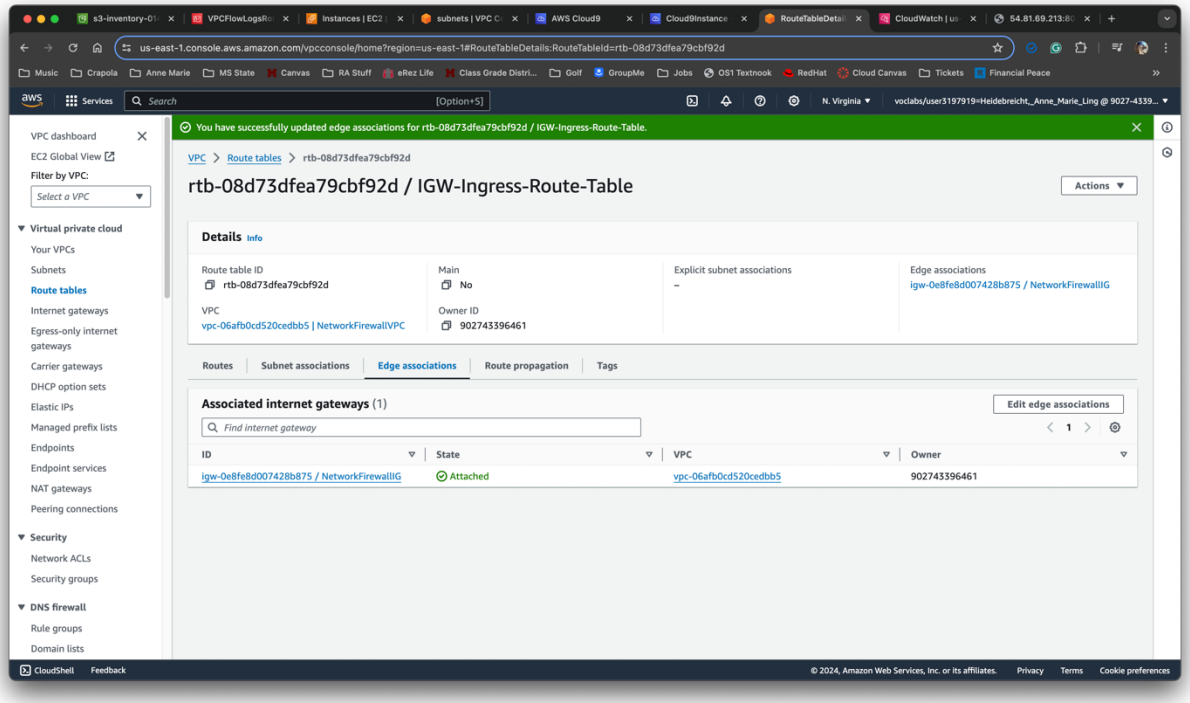


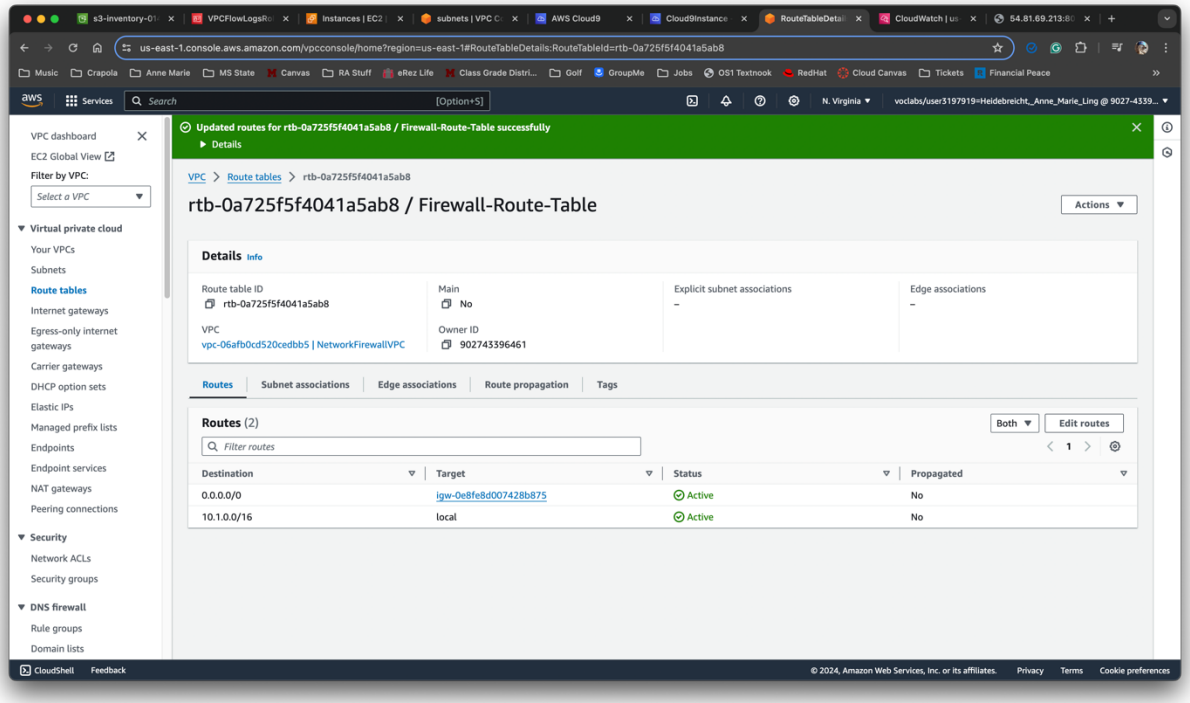
Task 2.7: Create a network firewall

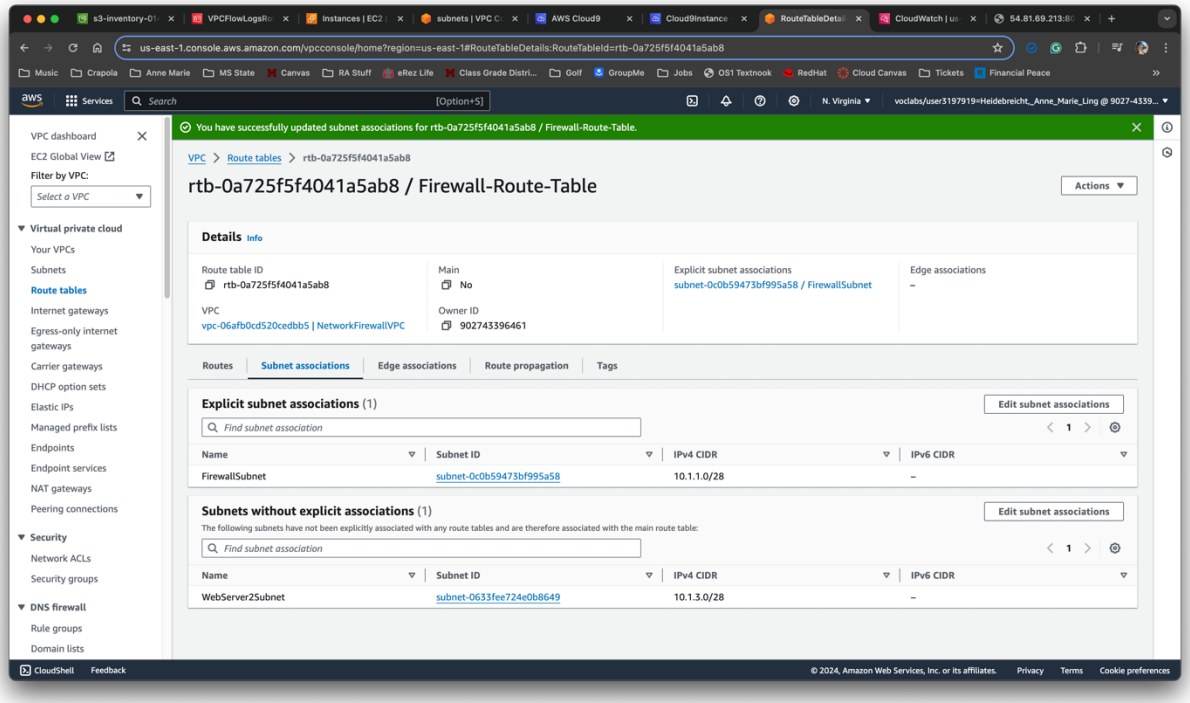


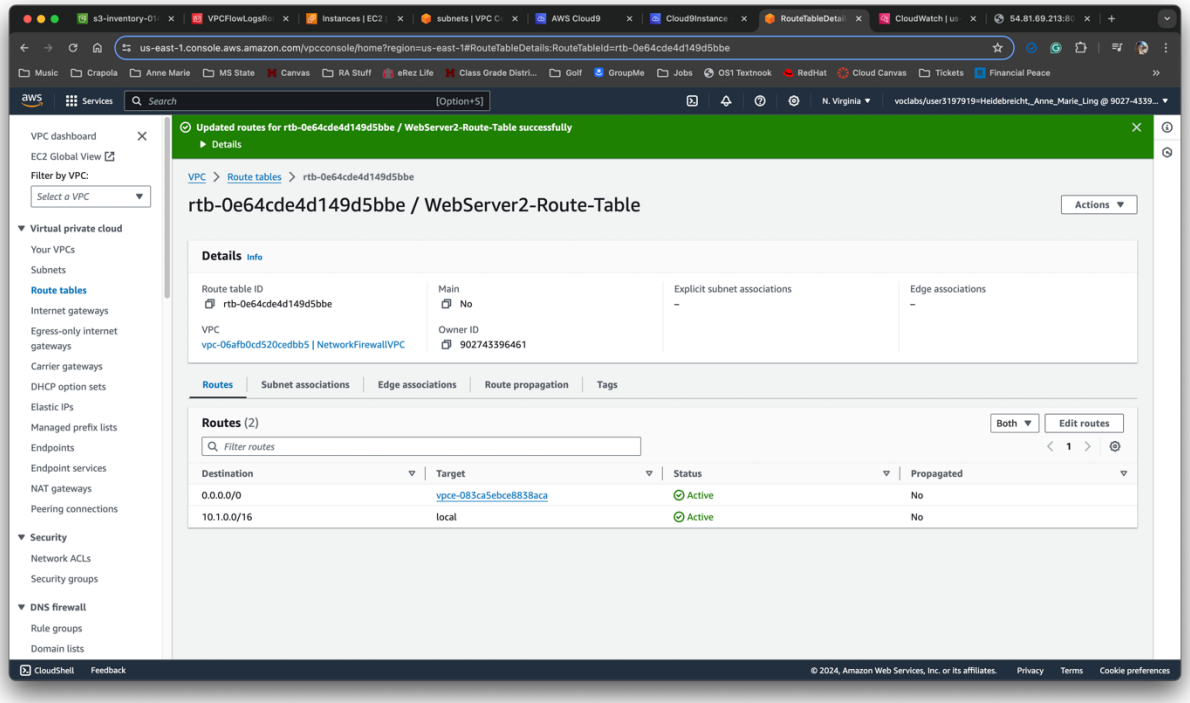
Task 2.8: Create route tables

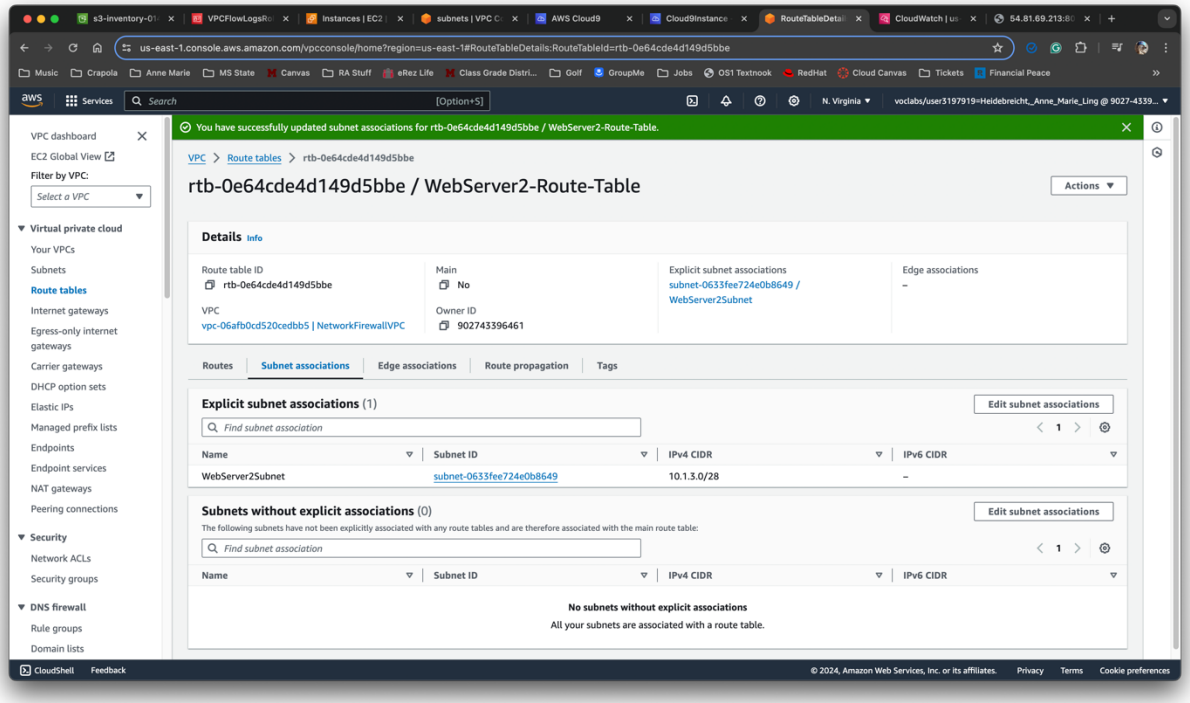

Updated routes for rtb-08d73dfea79cbf92d / IGW-Ingress-Route-Table successfully
Details
VPC > Route tables > rtb-08d73dfea79cbf92d
rtb-08d73dfea79cbf92d / IGW-Ingress-Route-Table
Actions
Details Info
Route table ID
rtb-08d73dfea79cbf92d
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-06afb0cd520cedbb5 | NetworkFirewallVPC
Owner ID
902743396461
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
10.1.0.0/16
local
Active
No
10.1.3.0/28
vpce-083ca5ebce8838aca
Active
No

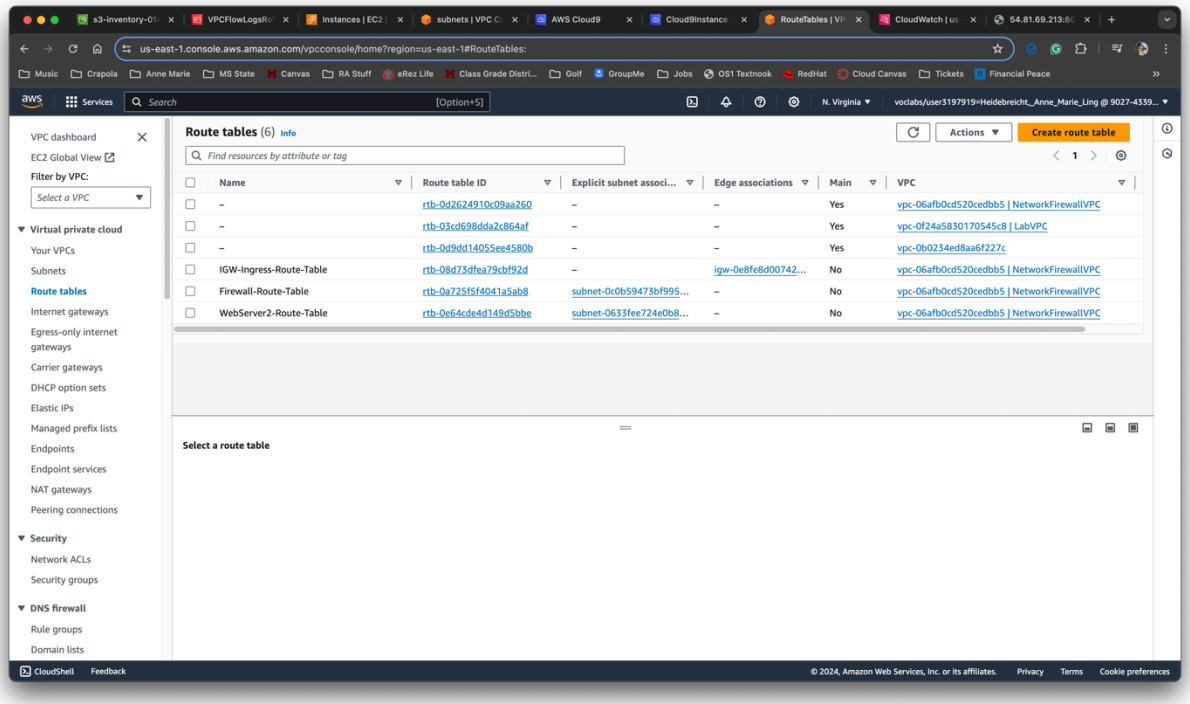

You have successfully updated edge associations for rtb-08d73dfea79cbf92d / IGW-Ingress-Route-Table.
VPC > Route tables > rtb-08d73dfea79cbf92d
rtb-08d73dfea79cbf92d / IGW-Ingress-Route-Table
Actions
Details Info
Route table ID
rtb-08d73dfea79cbf92d
Main
No
Explicit subnet associations
–
Edge associations
igw-0e8fe8d007428b875 / NetworkFirewallIG
VPC
vpc-06afb0cd520cedbb5 | NetworkFirewallVPC
Owner ID
902743396461
Routes
Subnet associations
Edge associations
Route propagation
Tags
Associated internet gateways (1)
Edit edge associations
Find internet gateway
ID
State
VPC
Owner
igw-0e8fe8d007428b875 / NetworkFirewallIG
Attached
vpc-06afb0cd520cedbb5
902743396461


Updated routes for rtb-0a725f5f4041a5ab8 / Firewall-Route-Table successfully
Details
VPC > Route tables > rtb-0a725f5f4041a5ab8
rtb-0a725f5f4041a5ab8 / Firewall-Route-Table
Actions
Details Info
Route table ID
rtb-0a725f5f4041a5ab8
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-06afb0cd520cedbb5 | NetworkFirewallVPC
Owner ID
902743396461
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
0.0.0.0/0
igw-0e8fe8d007428b875
Active
No
10.1.0.0/16
local
Active
No

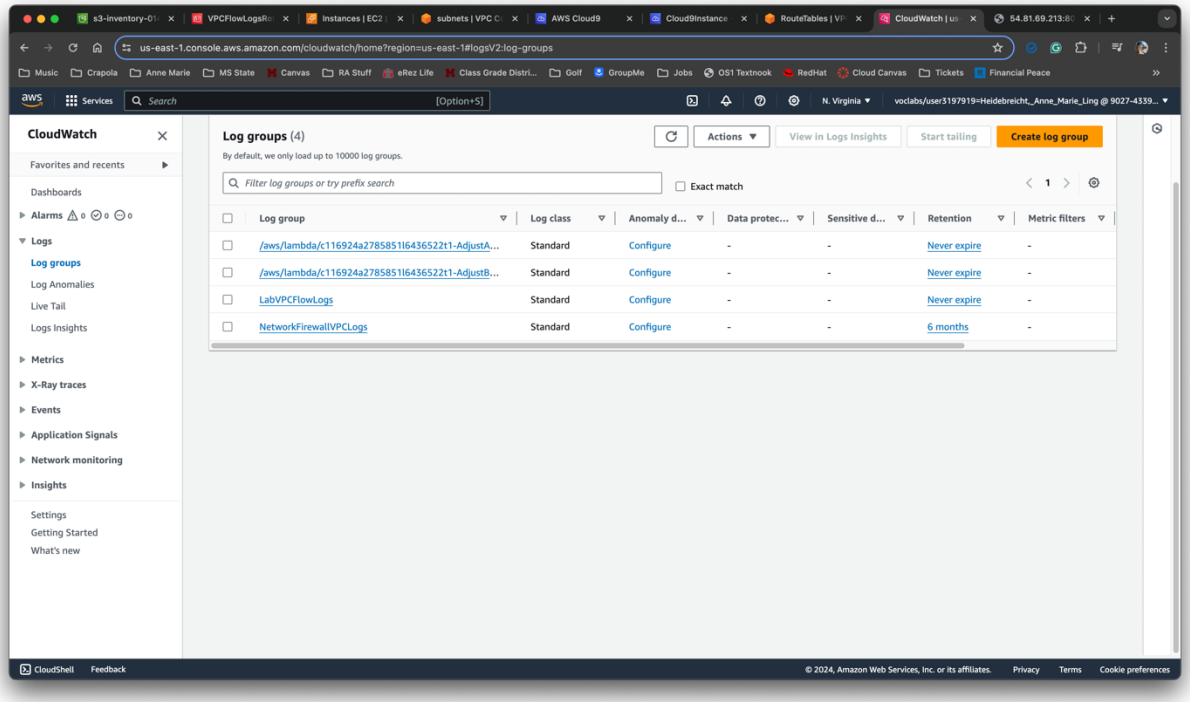

You have successfully updated subnet associations for rtb-0a725f5f4041a5ab8 / Firewall-Route-Table.
VPC > Route tables > rtb-0a725f5f4041a5ab8
rtb-0a725f5f4041a5ab8 / Firewall-Route-Table
Actions
Details Info
Route table ID
rtb-0a725f5f4041a5ab8
Main
No
Explicit subnet associations
subnet-0c0b59473bf995a58 / FirewallSubnet
Edge associations
–
VPC
vpc-06afb0cd520cedbb5 | NetworkFirewallVPC
Owner ID
902743396461
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (1)
Edit subnet associations
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
FirewallSubnet
subnet-0c0b59473bf995a58
10.1.1.0/28
–
Subnets without explicit associations (1)
Edit subnet associations
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
WebServer2Subnet
subnet-0633fee724e0b8649
10.1.3.0/28
–

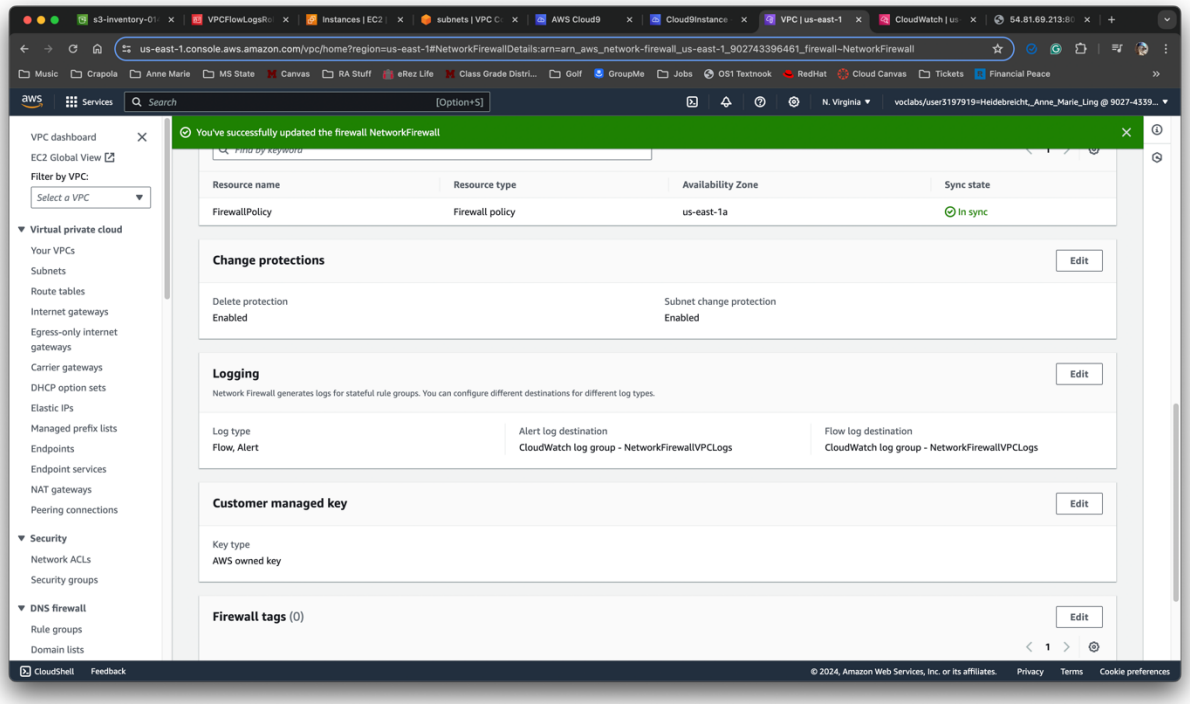

Updated routes for rtb-0e64cde4d149d5bbe / WebServer2-Route-Table successfully
Details
VPC > Route tables > rtb-0e64cde4d149d5bbe
rtb-0e64cde4d149d5bbe / WebServer2-Route-Table
Actions
Details Info
Route table ID
rtb-0e64cde4d149d5bbe
Main
No
Explicit subnet associations
–
Edge associations
–
VPC
vpc-06afb0cd520cedbb5 | NetworkFirewallVPC
Owner ID
902743396461
Routes
Subnet associations
Edge associations
Route propagation
Tags
Routes (2)
Both
Edit routes
Filter routes
Destination
Target
Status
Propagated
0.0.0.0/0
vpce-083ca5ebce8838aca
Active
No
10.1.0.0/16
local
Active
No

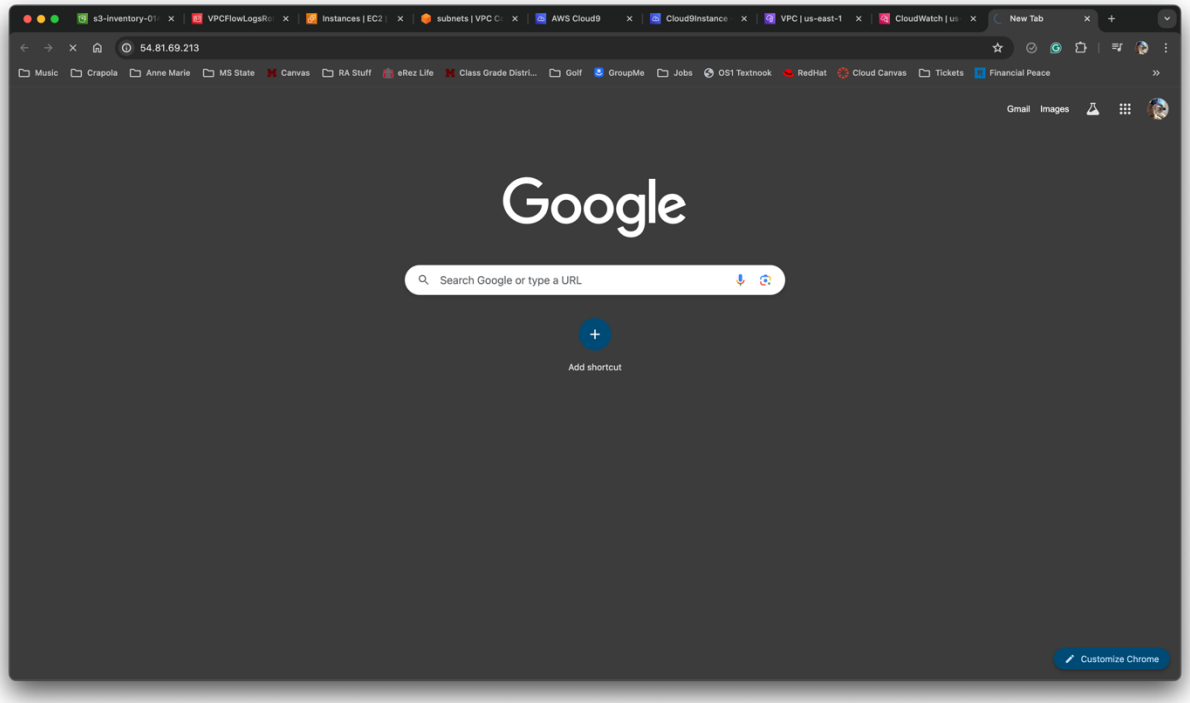

You have successfully updated subnet associations for rtb-0e64cde4d149d5bbe / WebServer2-Route-Table.
VPC > Route tables > rtb-0e64cde4d149d5bbe
rtb-0e64cde4d149d5bbe / WebServer2-Route-Table
Actions
Details Info
Route table ID
rtb-0e64cde4d149d5bbe
Main
No
Explicit subnet associations
subnet-0633fee724e0b8649 / WebServer2Subnet
Edge associations
–
VPC
vpc-06afb0cd520cedbb5 | NetworkFirewallVPC
Owner ID
902743396461
Routes
Subnet associations
Edge associations
Route propagation
Tags
Explicit subnet associations (1)
Edit subnet associations
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
WebServer2Subnet
subnet-0633fee724e0b8649
10.1.3.0/28
–
Subnets without explicit associations (0)
Edit subnet associations
The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:
Find subnet association
Name
Subnet ID
IPv4 CIDR
IPv6 CIDR
No subnets without explicit associations
All your subnets are associated with a route table.

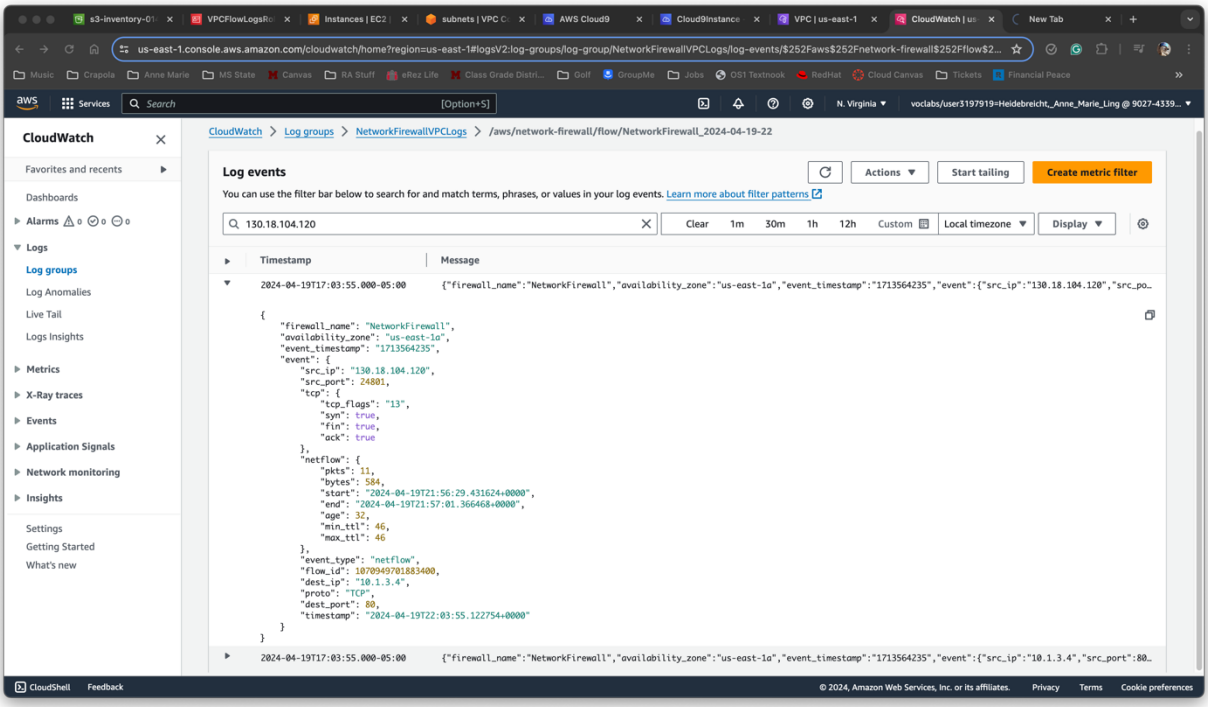


Task 2.9: Configure logging for the network firewall

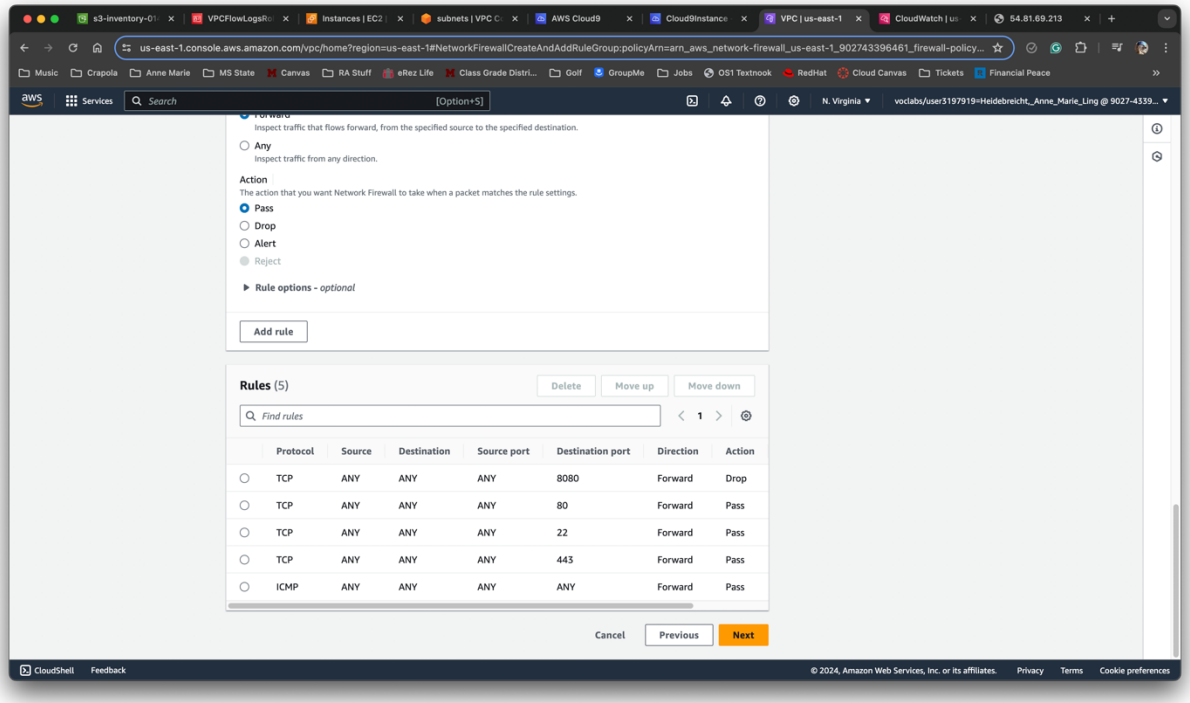


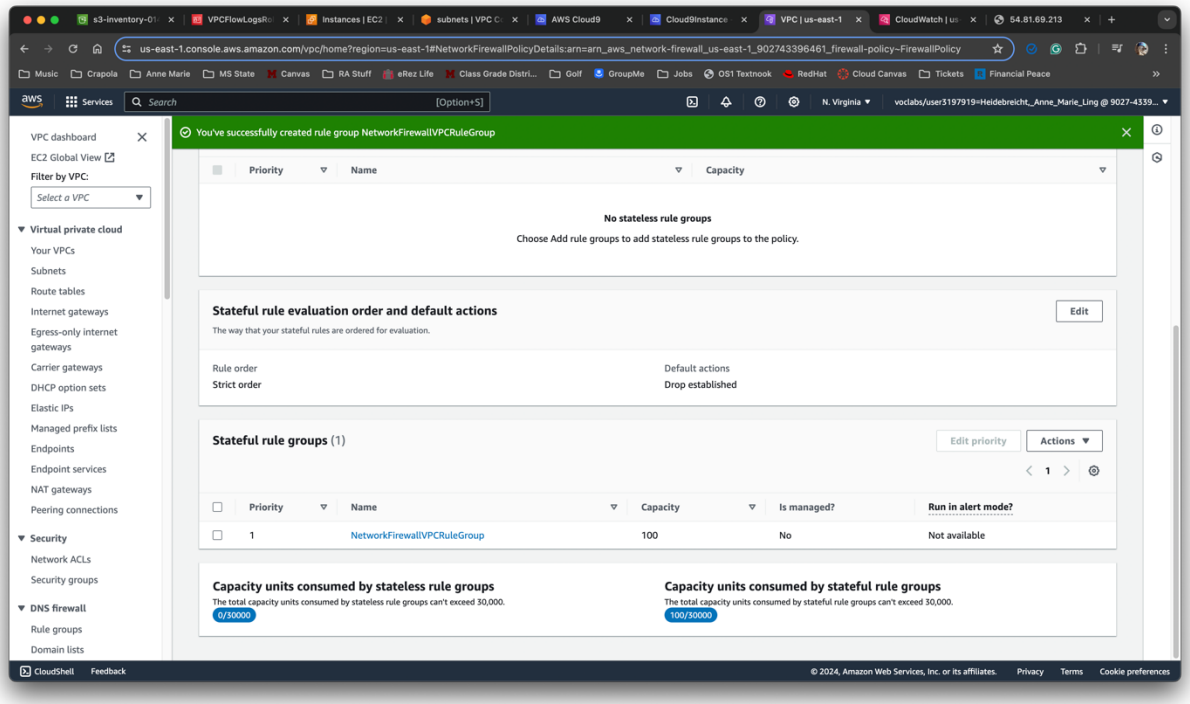

us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#NetworkFirewallDetails:arn=arn_aws_network-firewall_us-east-1_902743396461_firewall~NetworkFirewall
You've successfully updated the firewall NetworkFirewall
VPC dashboard
EC2 Global View
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Resource name
Resource type
Availability Zone
Sync state
FirewallPolicy
Firewall policy
us-east-1a
In sync
Change protections
Edit
Delete protection
Enabled
Subnet change protection
Enabled
Logging
Network Firewall generates logs for stateful rule groups. You can configure different destinations for different log types.
Log type
Flow, Alert
Alert log destination
CloudWatch log group - NetworkFirewallVPCLogs
Flow log destination
CloudWatch log group - NetworkFirewallVPCLogs
Customer managed key
Key type
AWS owned key
Firewall tags (0)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

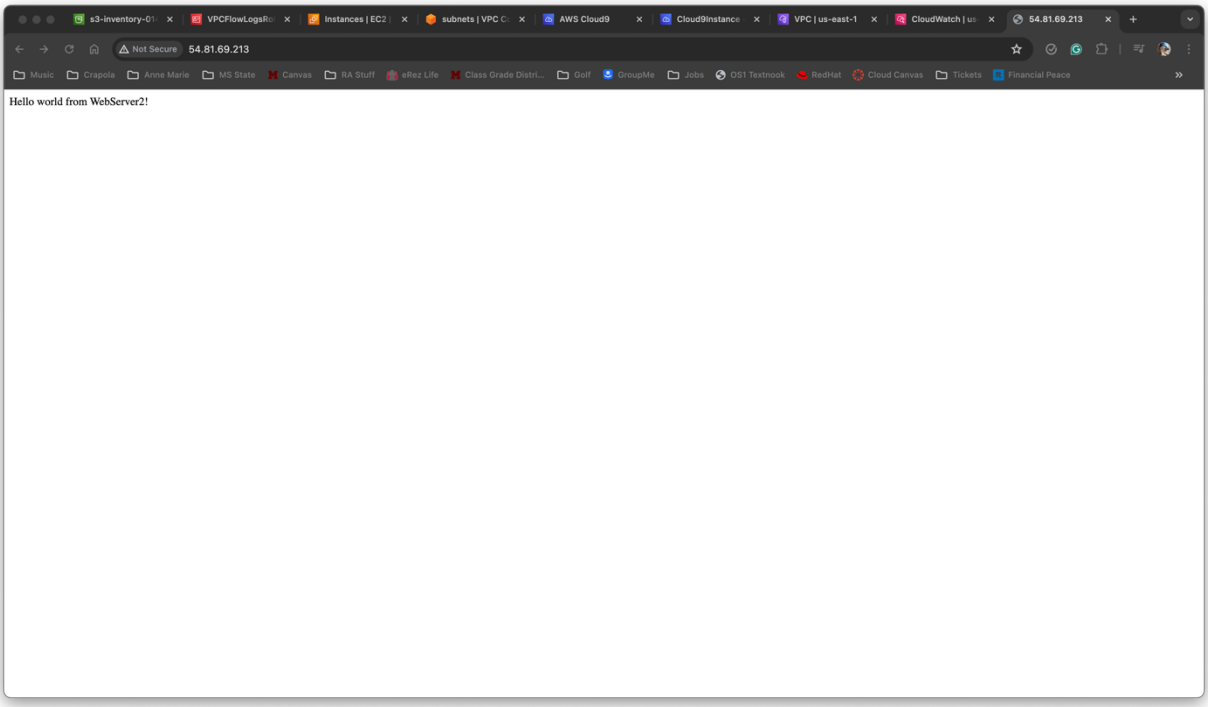

54.81.69.213
Gmail
Images
Google
Search Google or type a URL
Add shortcut
Customize Chrome



Task 2.10: Configure the firewall policy and test access

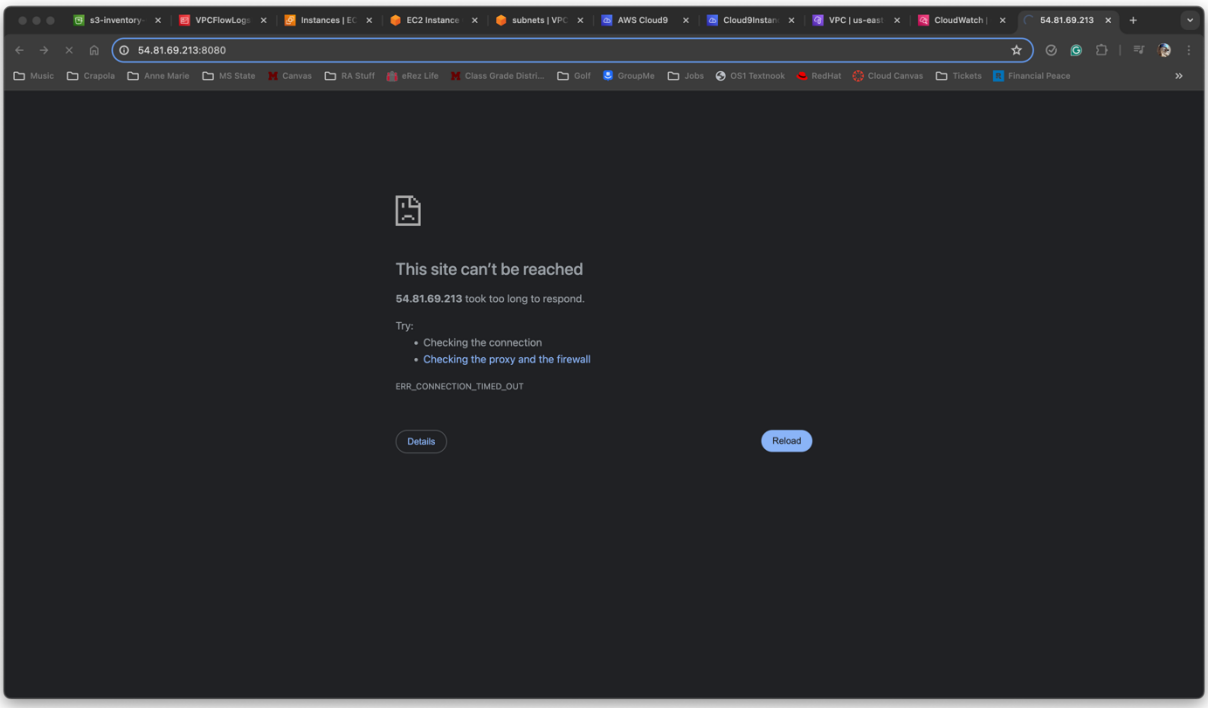


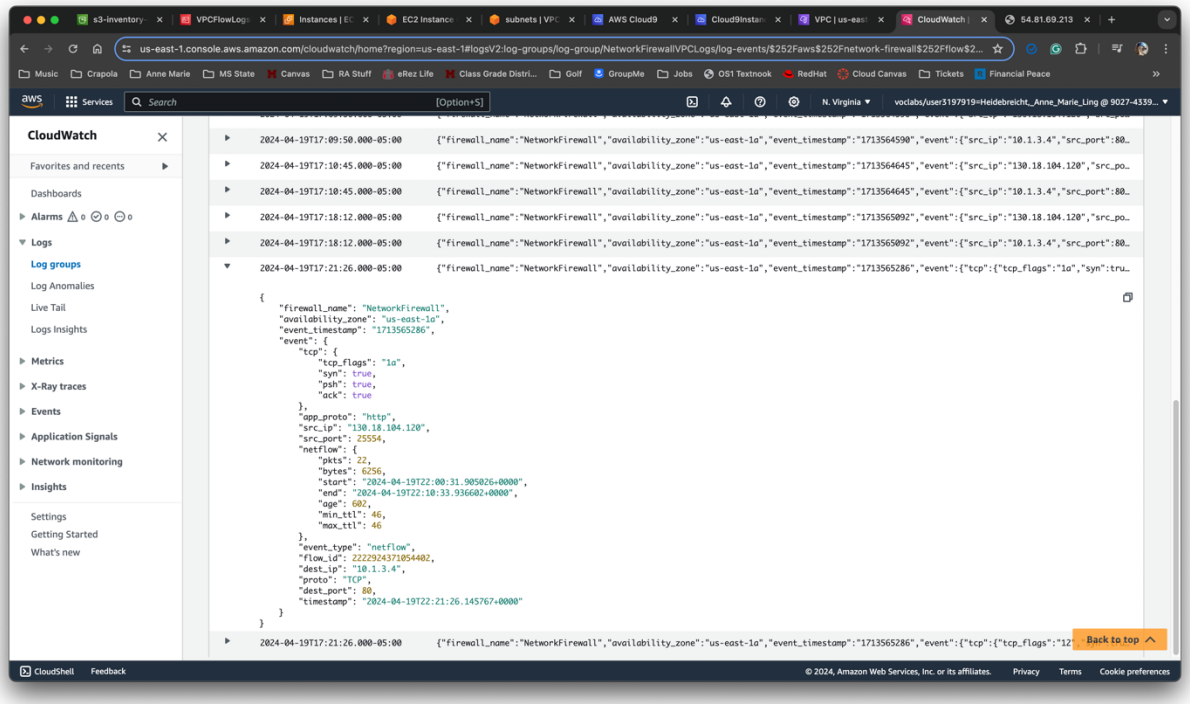





```
voclabs:~/environment $ nc -vz 54.81.69.213 22
Connection to 54.81.69.213 22 port [tcp/ssh] succeeded!
```

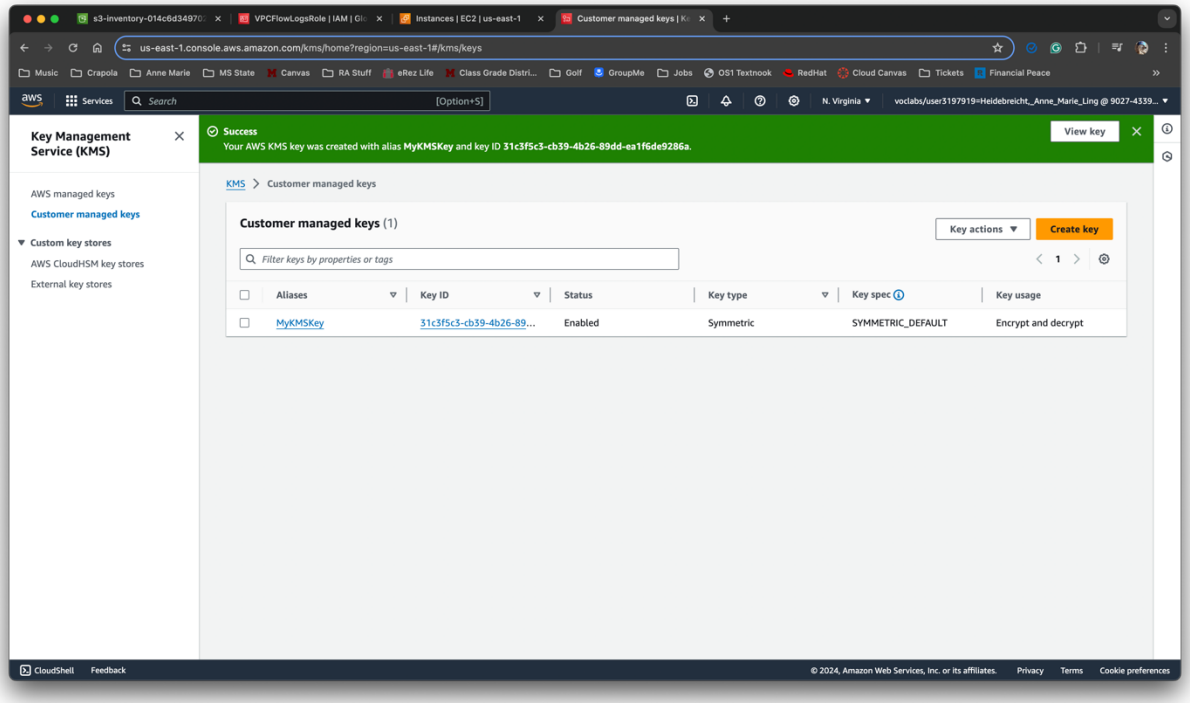
```
Last login: Fri Apr 19 21:35:43 2024 from 18.206.107.28
[ec2-user@webserver2 ~]$ ping -c 3 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (3.162.118.164) 56(84) bytes of data.
64 bytes from server-3-162-118-164.iad61.r.cloudfront.net (3.162.118.164): icmp_seq=1 ttl=247 time=3.42 ms
64 bytes from server-3-162-118-164.iad61.r.cloudfront.net (3.162.118.164): icmp_seq=2 ttl=247 time=1.85 ms
64 bytes from server-3-162-118-164.iad61.r.cloudfront.net (3.162.118.164): icmp_seq=3 ttl=247 time=1.95 ms

--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.846/2.403/3.416/0.717 ms
[ec2-user@webserver2 ~]$ sudo netstat -tulpn | grep -i listen
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2291/sshd: /usr/sbi
tcp6       0      0 :::80                   :::*                    LISTEN      1954/httpd
tcp6       0      0 :::22                   :::*                    LISTEN      2291/sshd: /usr/sbi
[ec2-user@webserver2 ~]$ python3 -m http.server 8080 &
[1] 12146
[ec2-user@webserver2 ~]$ Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...

[ec2-user@webserver2 ~]$ sudo netstat -tulpn | grep -i listen
tcp        0      0 0.0.0.0:8080            0.0.0.0:*               LISTEN      12146/python3
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      2291/sshd: /usr/sbi
tcp6       0      0 :::80                   :::*                    LISTEN      1954/httpd
tcp6       0      0 :::22                   :::*                    LISTEN      2291/sshd: /usr/sbi
[ec2-user@webserver2 ~]$
```

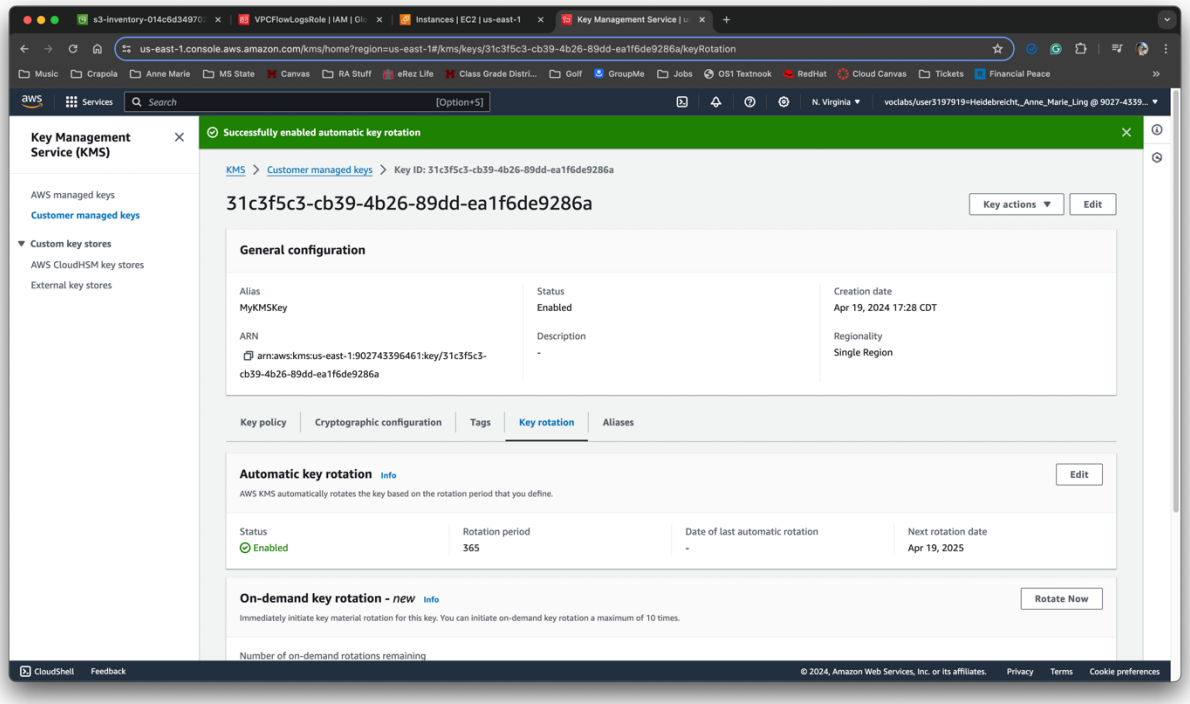




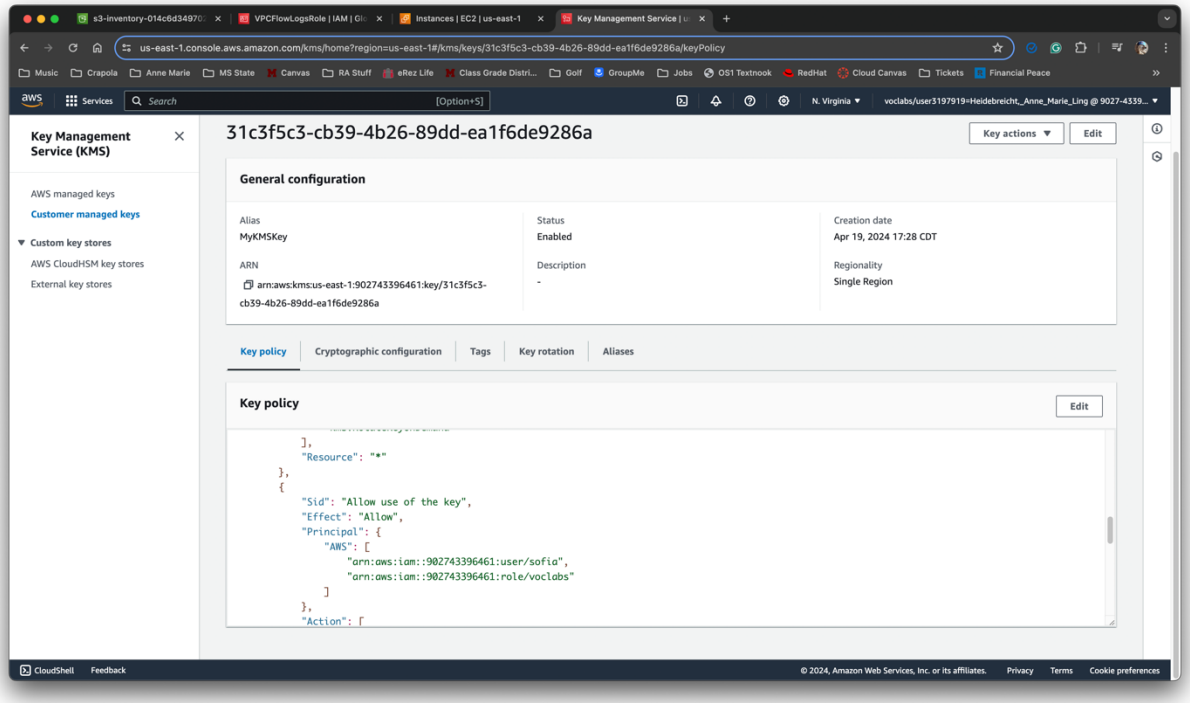
Phase 3 – Securing AWS resources

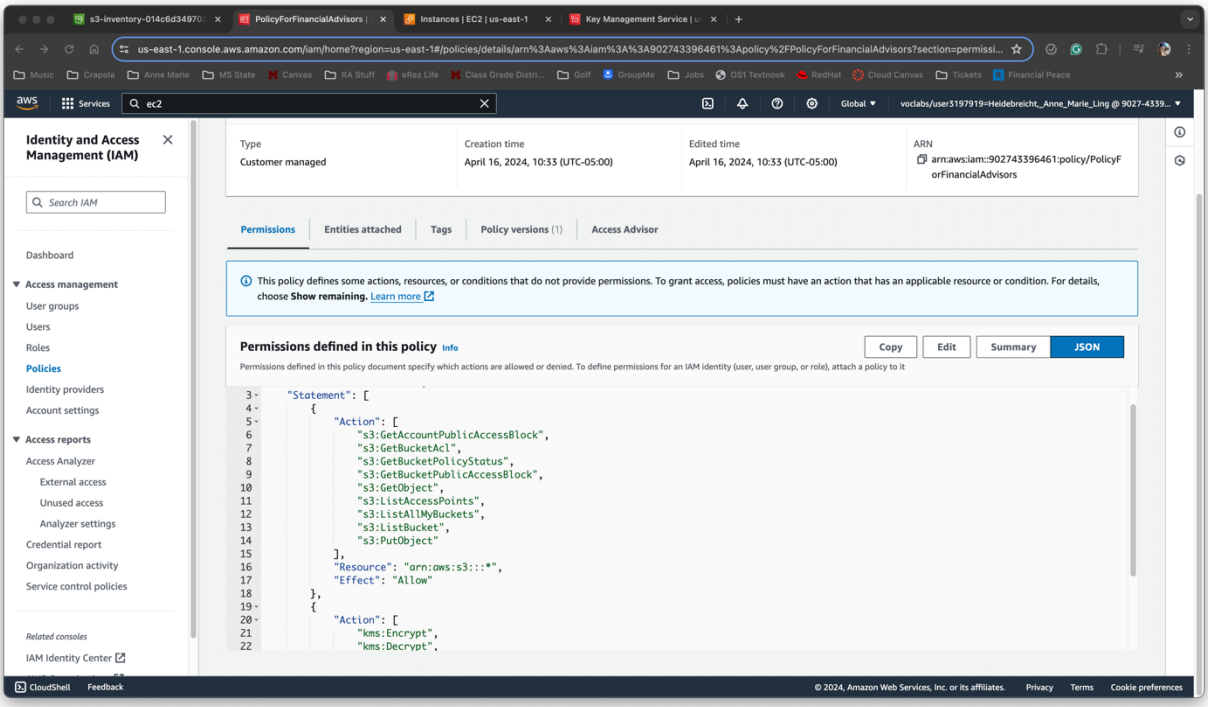
Task 3.1: Create a customer-managed key and configure key rotation



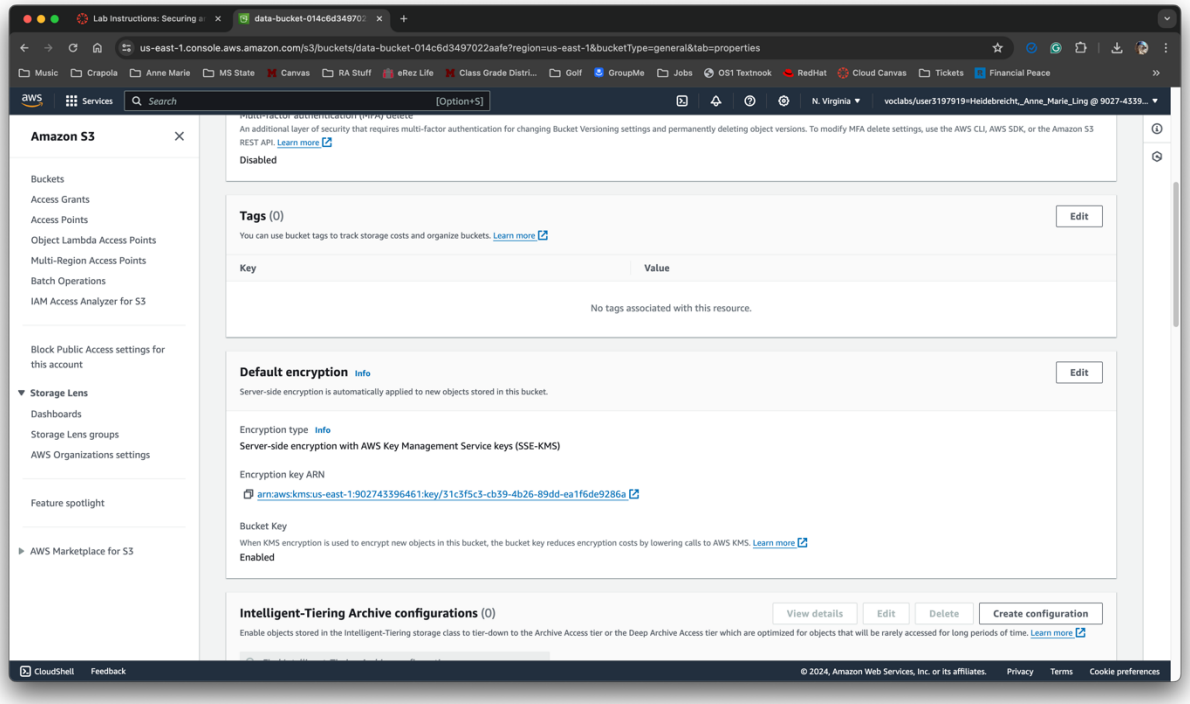


Task 3.2: Update the AWS KMS key policy and analyze an IAM policy





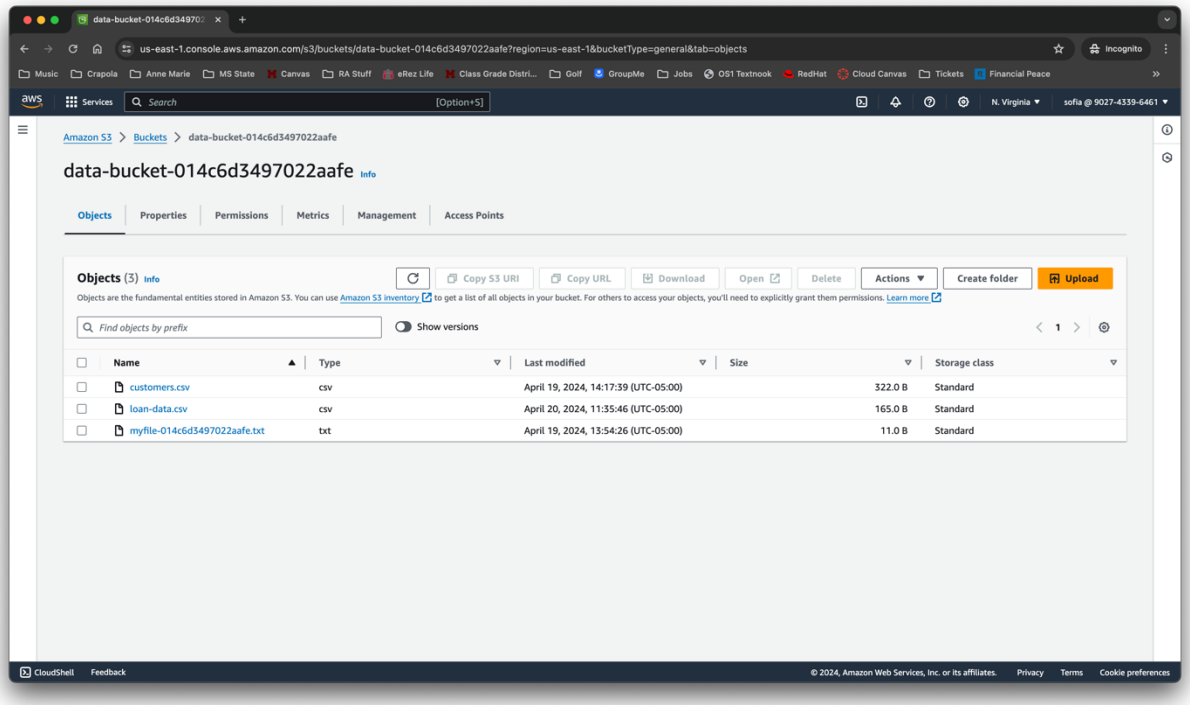
Task 3.3: Use AWS KMS to encrypt data in Amazon S3

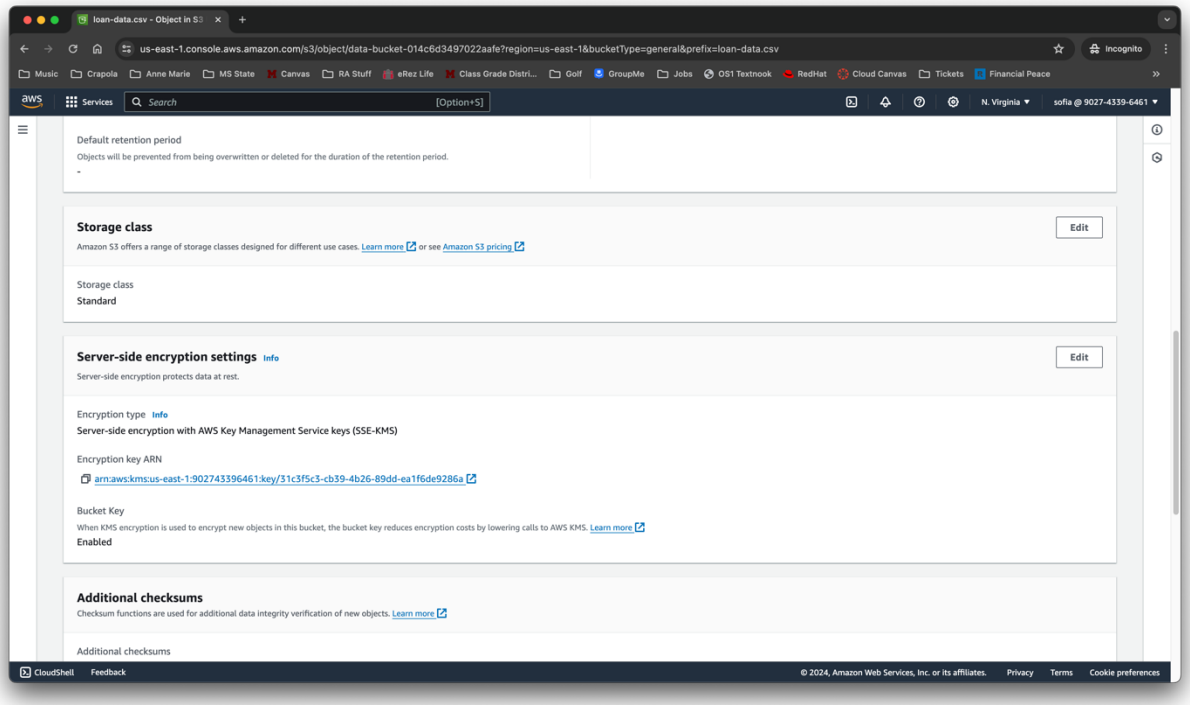


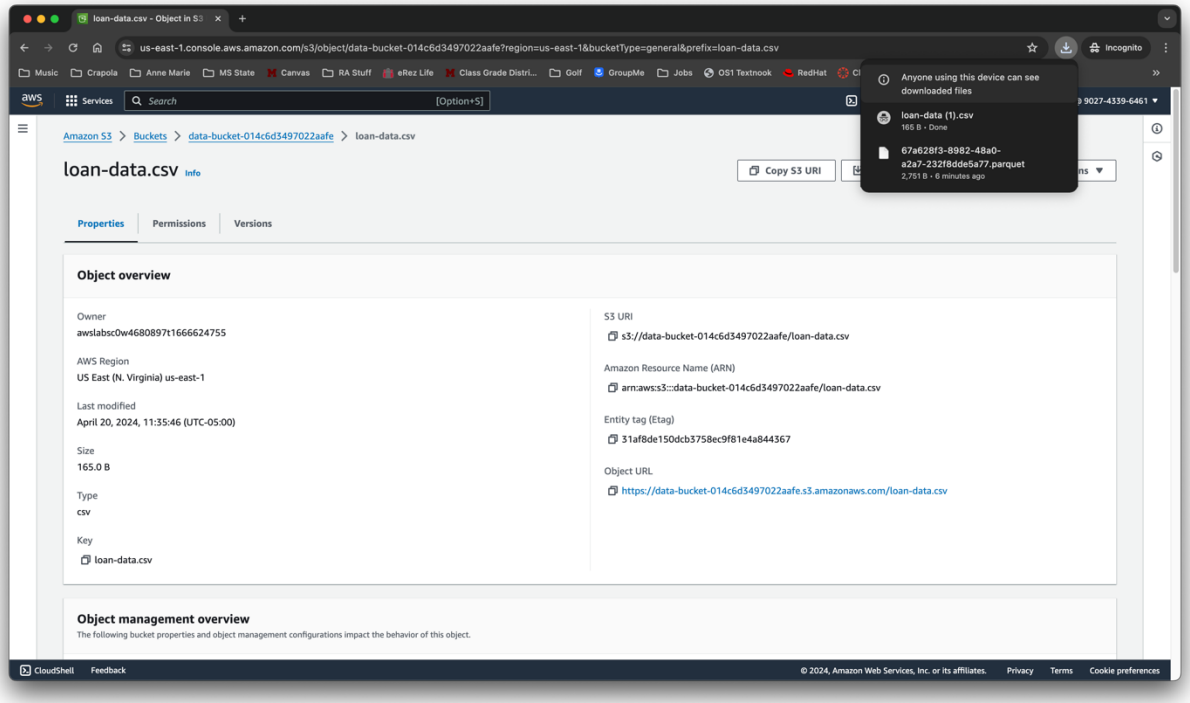
loan-data.csv

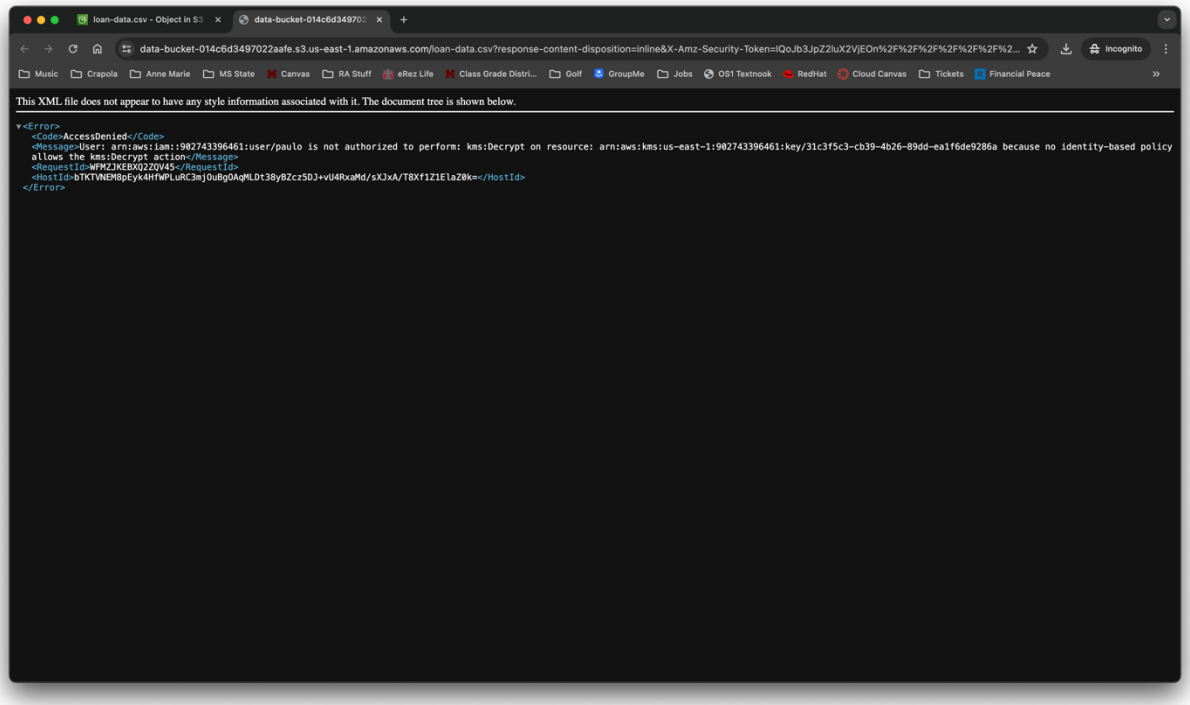
loan-data.csv

```
date,description,amount,principal,interest
2023-01-14,payment,1000.00,845.52,154.48
2022-12-22,payment,1021.52,742.80,278.72
2022-11-15,payment,1000.00,855.27,144.73
```

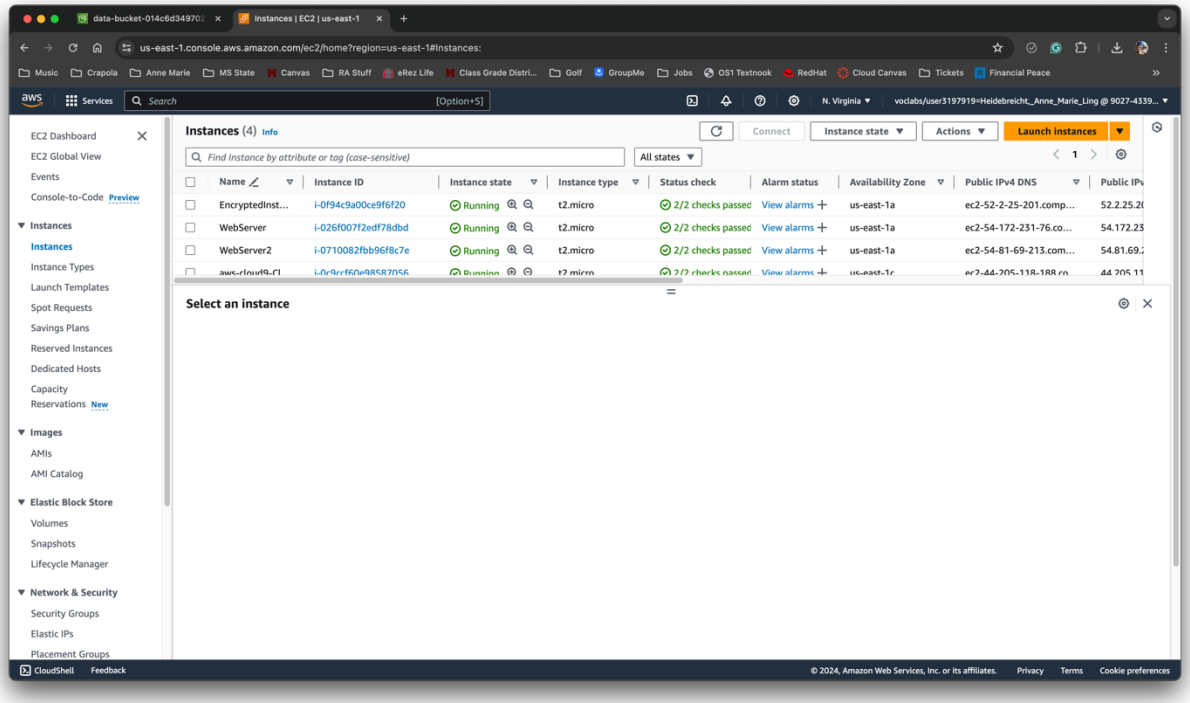


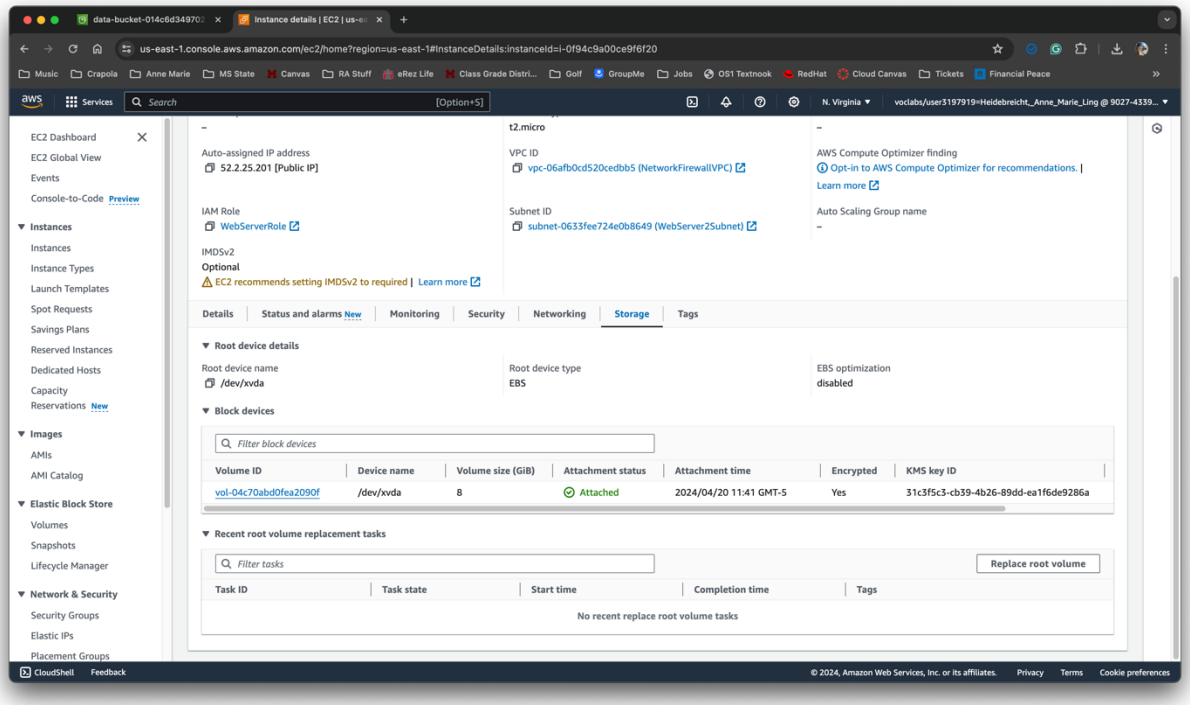

loan-data.csv - Object in S3
us-east-1.console.aws.amazon.com/s3/object/data-bucket-014c6d3497022aafe?region=us-east-1&bucketType=general&prefix=loan-data.csv
Default retention period
Objects will be prevented from being overwritten or deleted for the duration of the retention period.
-
Storage class
Amazon S3 offers a range of storage classes designed for different use cases. Learn more or see Amazon S3 pricing
Edit
Storage class
Standard
Server-side encryption settings Info
Server-side encryption protects data at rest.
Edit
Encryption type Info
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Encryption key ARN
arn:aws:kms:us-east-1:902743396461:key/31c3f5c3-cb39-4b26-89dd-ea1f6de9286a
Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. Learn more
Enabled
Additional checksums
Checksum functions are used for additional data integrity verification of new objects. Learn more
Additional checksums
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


loan-data.csv - Object in S3
us-east-1.console.aws.amazon.com/s3/object/data-bucket-014c6d3497022aafe?region=us-east-1&bucketType=general&prefix=loan-data.csv
Anyone using this device can see downloaded files
loan-data (1).csv
165 B • Done
67a628f3-8982-48a0-a2a7-232f8dde5a77.parquet
2,751 B • 6 minutes ago
Amazon S3 > Buckets > data-bucket-014c6d3497022aafe > loan-data.csv
loan-data.csv Info
Copy S3 URI
Properties
Permissions
Versions
Object overview
Owner
awslabsc0w4680897t1666624755
AWS Region
US East (N. Virginia) us-east-1
Last modified
April 20, 2024, 11:35:46 (UTC-05:00)
Size
165.0 B
Type
csv
Key
loan-data.csv
S3 URI
s3://data-bucket-014c6d3497022aafe/loan-data.csv
Amazon Resource Name (ARN)
arn:aws:s3:::data-bucket-014c6d3497022aafe/loan-data.csv
Entity tag (Etag)
31af8de150dcb3758ec9f81e4a844367
Object URL
https://data-bucket-014c6d3497022aafe.s3.amazonaws.com/loan-data.csv
Object management overview
The following bucket properties and object management configurations impact the behavior of this object.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

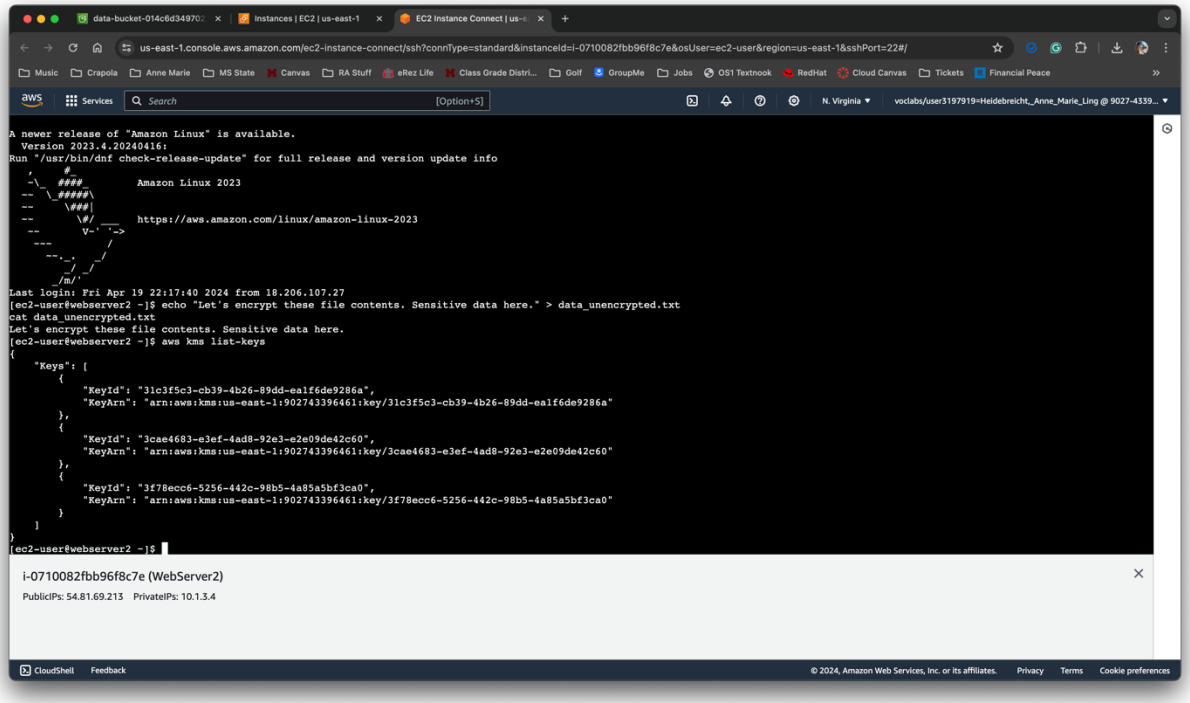


Task 3.4: Use AWS KMS to encrypt the root volume of an EC2





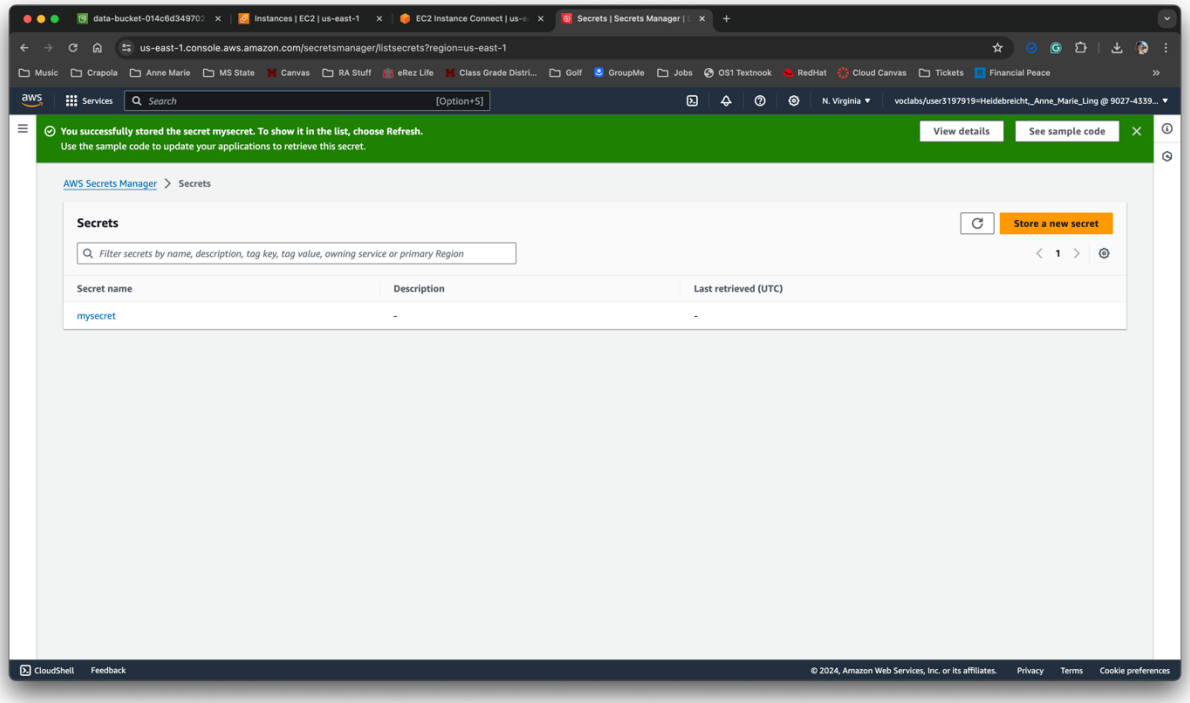
Task 3.5: Use AWS KMS envelope encryption to encrypt data in place

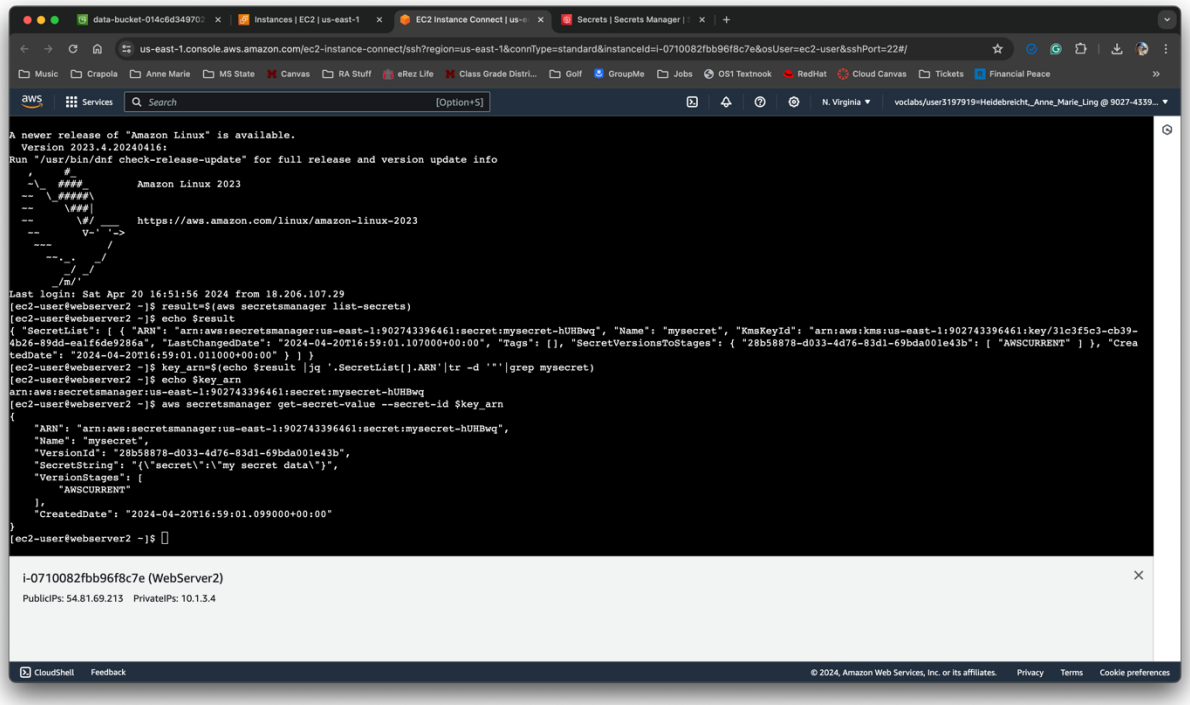



```
[ec2-user@webserver2 ~]$ result=$(aws kms generate-data-key --key-id alias/MyKMSKey --key-spec AES_256)
echo $result | python3 -m json.tool
{
    "CiphertextBlob": "AQIDAHgaZueItWbvFalwiEK3bmxkmpolnTAZ5WzqXOCMkIKlngGJbrXZFI3xnZgHs0YR9uFoAAAAfjB8BgkqhkiG9w0BBwagbzBtAgEAMGgGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMfsNZiEPz3XpwHAchAgEQgDs/dkUa9Aq2VYQIP7xnnAEUU7UQUF/i9m84ZlPNlXQmvCvsUhUijdgJ0oTDqEqfszw2Sw/yRjxv+sOlg==",
    "Plaintext": "ItQdzo3nPFRA/mWQo4JymdRkSTrti4fGZcYbKpxyvQ4=",
    "KeyId": "arn:aws:kms:us-east-1:902743396461:key/31c3f5c3-cb39-4b26-89dd-ea1f6de9286a"
}
```

```
[ec2-user@webserver2 ~]$ dk_cipher=$(echo $result| jq '.CiphertextBlob' | cut -d '"' -f2)
[ec2-user@webserver2 ~]$ echo $dk_cipher
AQIDAHgaZueItWbvFalwiEK3bmxkmpolnTAZ5WzqXOCMkIKlngGJbrXZFI3xnZgHs0YR9uFoAAAAfjB8BgkqhkiG9w0BBwagbzBtAgEAMGgGCSqGSIb3DQEHATAeBglghkgBZQMEAS4wEQQMfsNZiEPz3XpwHAchAgEQgDs/dkUa9Aq2VYQIP7xnn
AEUU7UQUF/i9m842lPNlXQmvCvsUhUijdgJOBoTDqBqfszw2Sw/yRjxv+sOlg==
[ec2-user@webserver2 ~]$ echo $dk_cipher | base64 --decode > data_key_ciphertext
[ec2-user@webserver2 ~]$ echo $dk_cipher | base64 --decode > data_key_ciphertext
[ec2-user@webserver2 ~]$ cat data_key_ciphertext
0o0m0h0p`0He.0@@i0@l0\@@@@@@n@@@@r@@h~0|     *0H@@
          -0y0c@@zpl@;?vz@
0U7@g@S@P_@@o8fSt&@+@R"@@aws kms decrypt --ciphertext-blob fileb://./data_key_ciphertext --query Plaintext --output textey_ciphertext --query Plaintext --output text
ItQdzo3nPFRA/mWQo4JymdRkSTrti4fGZcYbKpxyvQ4=
[ec2-user@webserver2 ~]$ aws kms decrypt --ciphertext-blob fileb://./data_key_ciphertext --query Plaintext --output text | base64 --decode > data_key_plaintext_encrypted
[ec2-user@webserver2 ~]$
[ec2-user@webserver2 ~]$ openssl enc -aes-256-cbc -salt -pbkdf2 -in data_unencrypted.txt -out data_encrypted -pass file:data_key_plaintext_encrypted
[ec2-user@webserver2 ~]$ cat data_encrypted
Salted__@C@@@@,P@#u@@@?u@@6@@@@@@@o@@_@(Y@6@@@+@@_e
                                                  ق@fDă@@@@@@@[ec2-user@webserver2 ~]$ rm data_unencrypted.txt
[ec2-user@webserver2 ~]$
[ec2-user@webserver2 ~]$ openssl enc -d -aes-256-cbc -pbkdf2 -in data_encrypted -out data_decrypted.txt -pass file:./data_key_plaintext_encrypted
[ec2-user@webserver2 ~]$ cat data_decrypted.txt
Let's encrypt these file contents. Sensitive data here.
[ec2-user@webserver2 ~]$
```

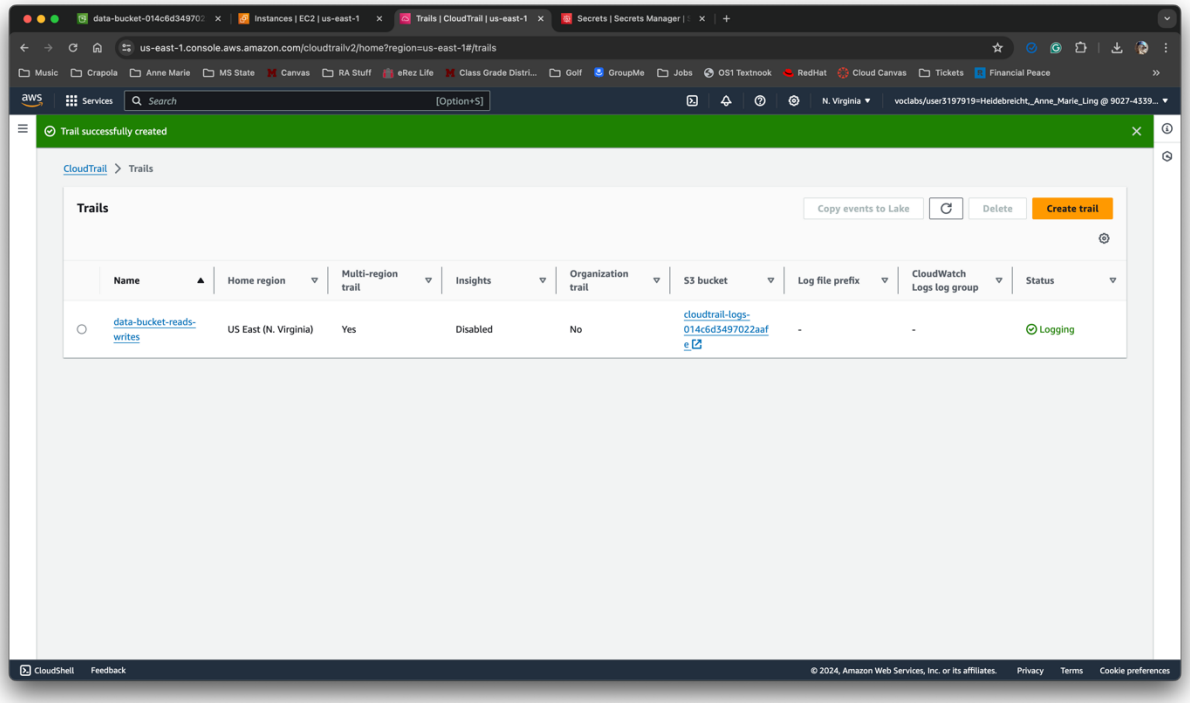
Task 3.6: Use AWS KMS to encrypt a Secrets Manager secret





Phase 4 – Monitoring and logging

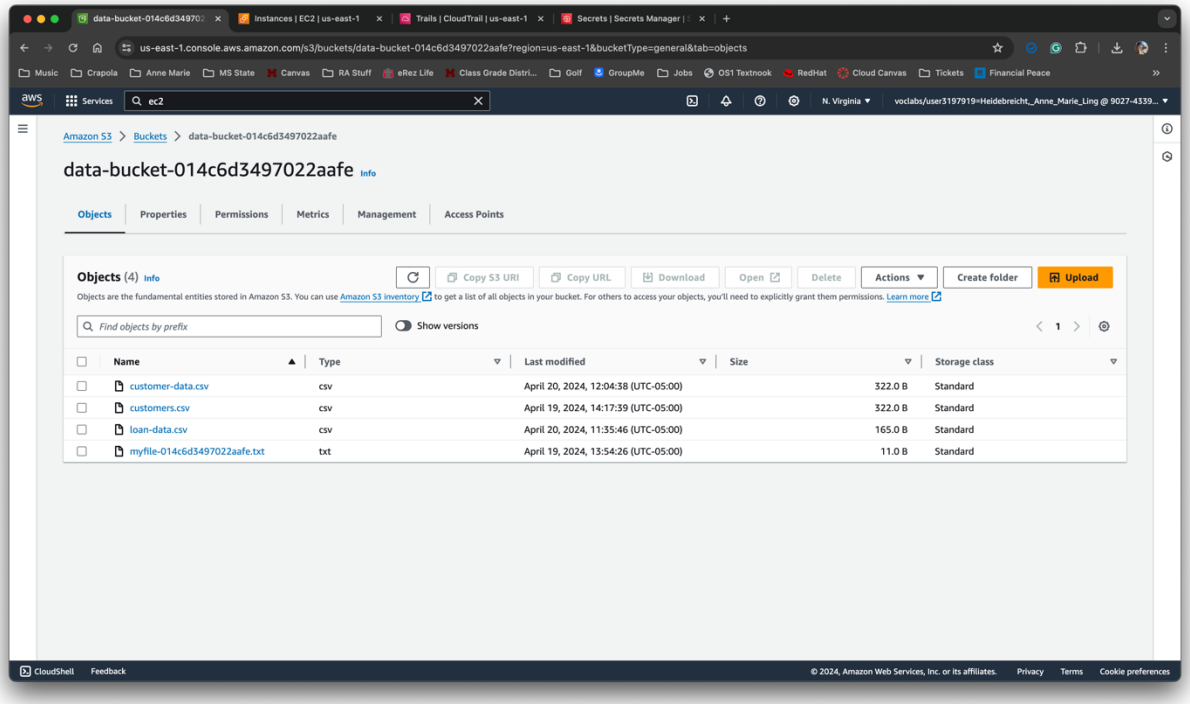
Task 4.1: Use CloudTrail to record Amazon S3 API calls

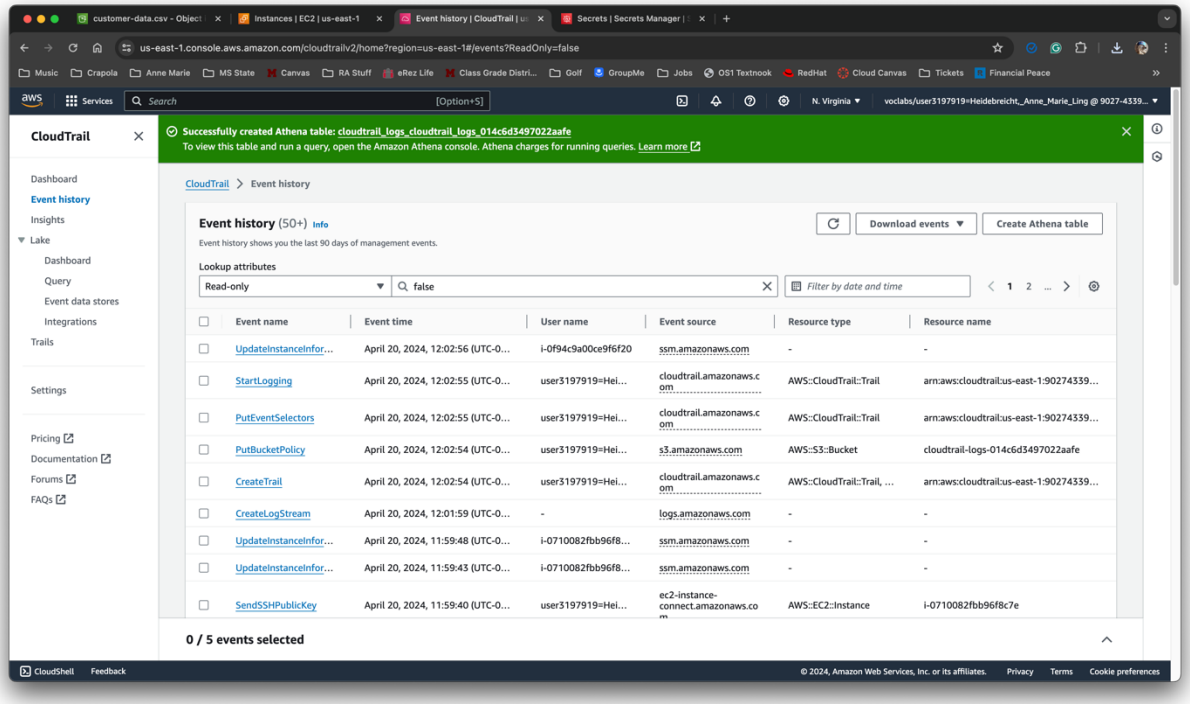


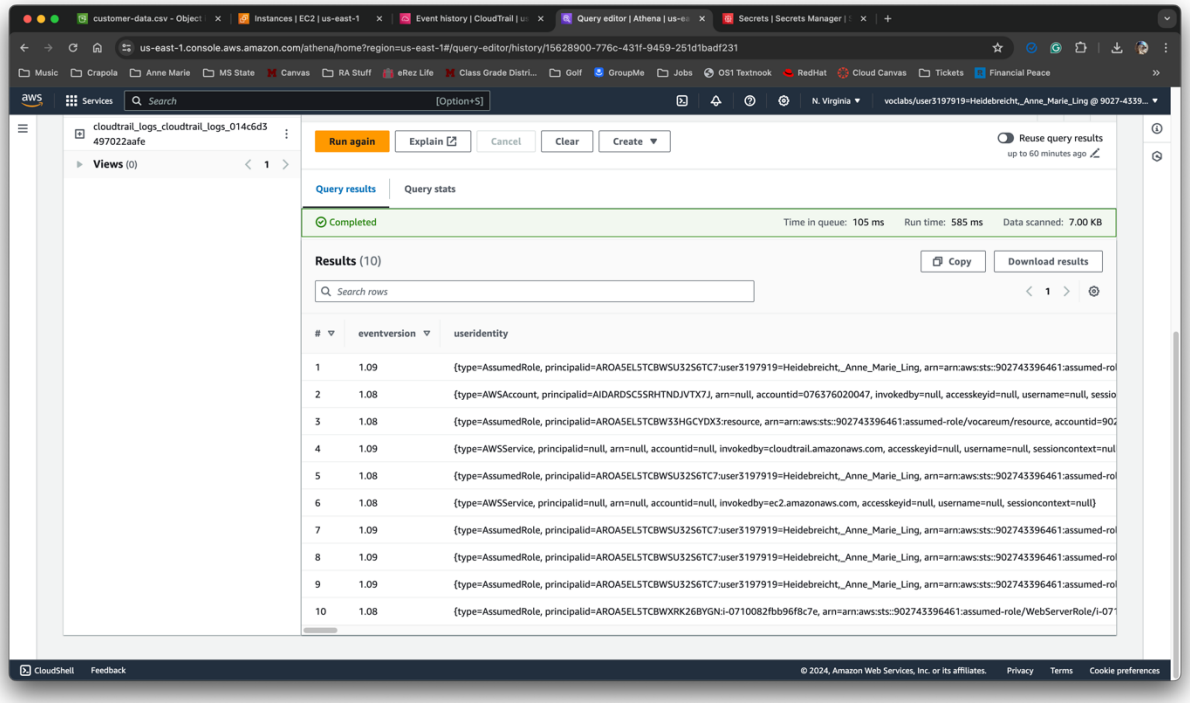
customer-data.csv

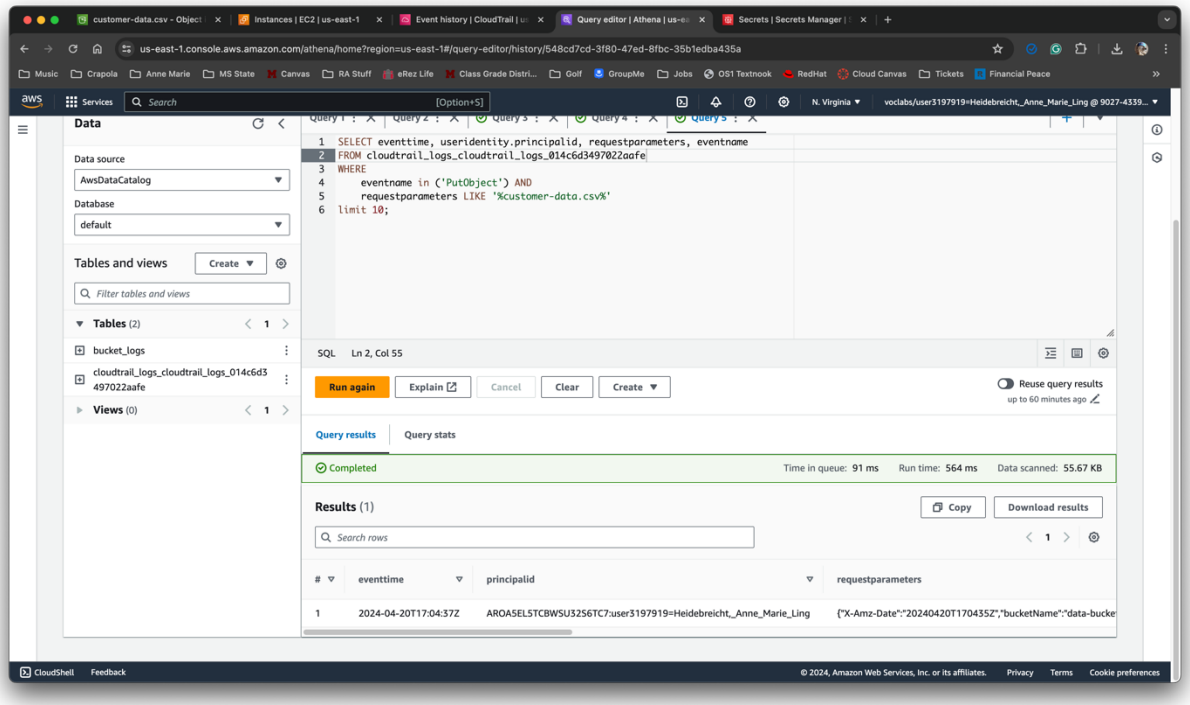
customer-data.csv

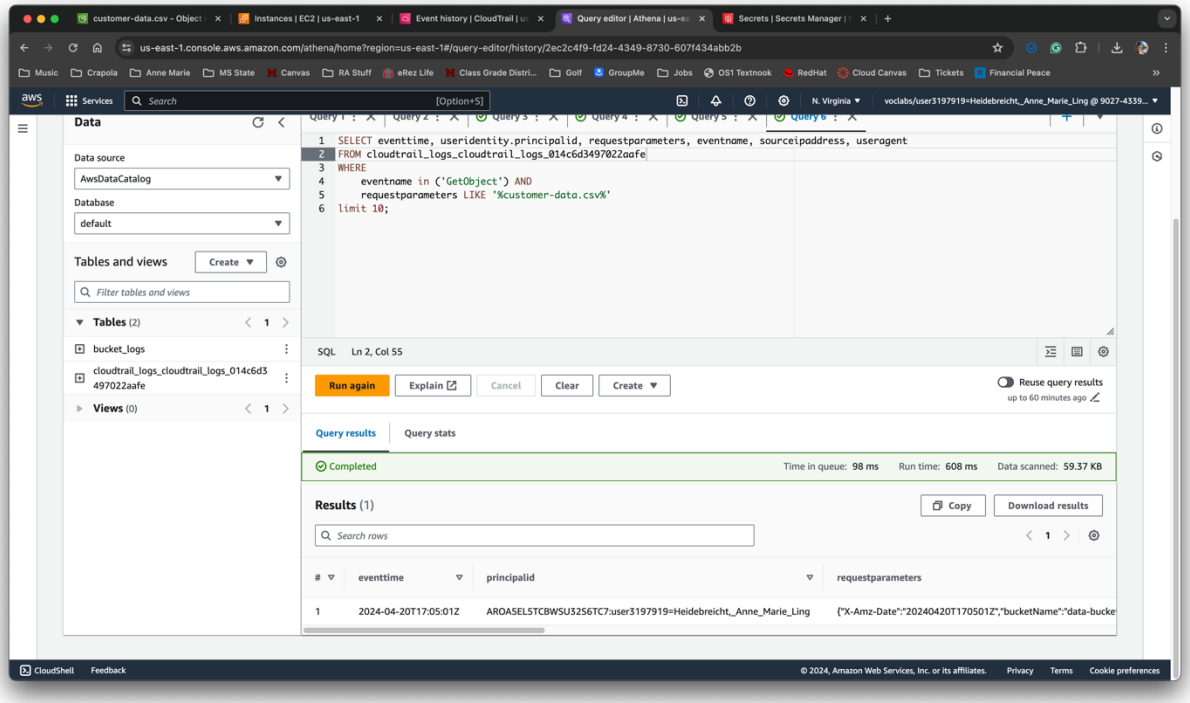
```
CustomerID,First Name,Last Name,Join Date,Street Address,City,State,Phone
1,Alejandro,Rosalez,12/12/2013,123 Main St.,Any Town,MD,301-555-0158
2,Jane,Doe,10/5/2014,456 State St.,Anywhere,WA,360-555-0163
3,John,Stiles,9/20/2016,1980 8th St.,Nowhere,NY,914-555-0122
4,Li,Juan,6/29/2011,1323 22nd Ave.,Anytown,NY,914-555-0149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



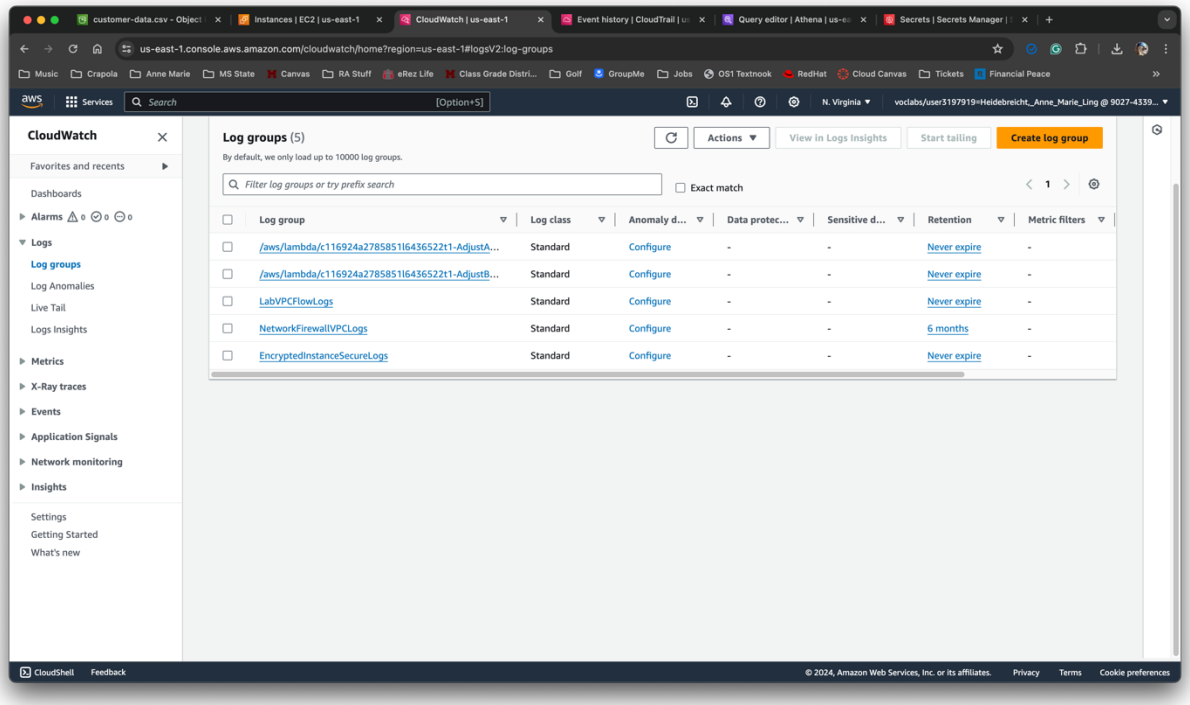

customer-data.csv - Object
Instances | EC2 | us-east-1
Event history | CloudTrail
Secrets | Secrets Manager
us-east-1.console.aws.amazon.com/cloudtrail/v2/home?region=us-east-1#/events?ReadOnly=false
Services
Search
[Option+S]
N. Virginia
voclabs/user3197919=Heidebreicht,_Anne_Marie_Ling @ 9027-4339...
CloudTrail
Dashboard
Event history
Insights
Lake
Dashboard
Query
Event data stores
Integrations
Trails
Settings
Pricing
Documentation
Forums
FAQs
Successfully created Athena table: cloudtrail_logs_cloudtrail_logs_014c6d3497022aafe
To view this table and run a query, open the Amazon Athena console. Athena charges for running queries. Learn more
CloudTrail > Event history
Event history (50+) Info
Event history shows you the last 90 days of management events.
Download events
Create Athena table
Lookup attributes
Read-only
false
Filter by date and time
Event name
Event time
User name
Event source
Resource type
Resource name
UpdateInstanceInfor...
April 20, 2024, 12:02:56 (UTC-0...
i-0f94c9a00ce9f6f20
ssm.amazonaws.com
StartLogging
April 20, 2024, 12:02:55 (UTC-0...
user3197919=Hei...
cloudtrail.amazonaws.com
AWS::CloudTrail::Trail
arn:aws:cloudtrail:us-east-1:90274339...
PutEventSelectors
April 20, 2024, 12:02:55 (UTC-0...
user3197919=Hei...
cloudtrail.amazonaws.com
AWS::CloudTrail::Trail
arn:aws:cloudtrail:us-east-1:90274339...
PutBucketPolicy
April 20, 2024, 12:02:54 (UTC-0...
user3197919=Hei...
s3.amazonaws.com
AWS::S3::Bucket
cloudtrail-logs-014c6d3497022aafe
CreateTrail
April 20, 2024, 12:02:54 (UTC-0...
user3197919=Hei...
cloudtrail.amazonaws.com
AWS::CloudTrail::Trail, ...
arn:aws:cloudtrail:us-east-1:90274339...
CreateLogStream
April 20, 2024, 12:01:59 (UTC-0...
-
logs.amazonaws.com
UpdateInstanceInfor...
April 20, 2024, 11:59:48 (UTC-0...
i-0710082fbb96f8...
ssm.amazonaws.com
UpdateInstanceInfor...
April 20, 2024, 11:59:43 (UTC-0...
i-0710082fbb96f8...
ssm.amazonaws.com
SendSSHPublicKey
April 20, 2024, 11:59:40 (UTC-0...
user3197919=Hei...
ec2-instance-connect.amazonaws.com
AWS::EC2::Instance
i-0710082fbb96f8c7e
0 / 5 events selected
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

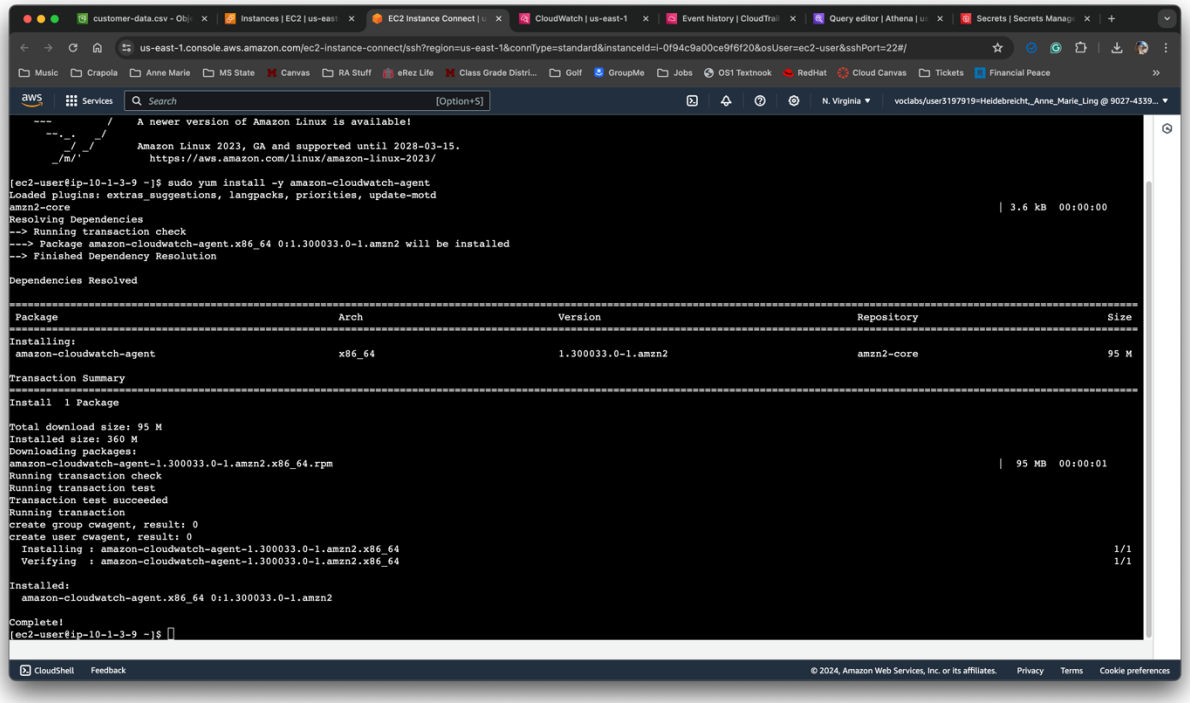

customer-data.csv - Object
Instances | EC2 | us-east-1
Event history | CloudTrail
Query editor | Athena
Secrets | Secrets Manager
us-east-1.console.aws.amazon.com/athena/home?region=us-east-1#/query-editor/history/15628900-776c-431f-9459-251d1badf231
Services
Search
[Option+S]
N. Virginia
voclabs/user3197919=Heidebreicht,_Anne_Marie_Ling @ 9027-4339...
cloudtrail_logs_cloudtrail_logs_014c6d3497022aafe
Views (0)
Run again
Explain
Cancel
Clear
Create
Reuse query results
up to 60 minutes ago
Query results
Query stats
Completed
Time in queue: 105 ms
Run time: 585 ms
Data scanned: 7.00 KB
Results (10)
Copy
Download results
Search rows
eventversion useridentity
1 1.09 {type=AssumedRole, principalid=AROA5EL5TCBWSU32S6TC7:user3197919=Heidebreicht,_Anne_Marie_Ling, arn=arn:aws:sts::902743396461:assumed-rol
2 1.08 {type=AWSAccount, principalid=AIDARDSC5SRHTNDJVTX7J, arn=null, accountid=076376020047, invokedby=null, accesskeyid=null, username=null, sessio
3 1.08 {type=AssumedRole, principalid=AROA5EL5TCBW33HGCYDX3:resource, arn=arn:aws:sts::902743396461:assumed-role/vocareum/resource, accountid=902
4 1.09 {type=AWSService, principalid=null, arn=null, accountid=null, invokedby=cloudtrail.amazonaws.com, accesskeyid=null, username=null, sessioncontext=nul
5 1.08 {type=AssumedRole, principalid=AROA5EL5TCBWSU32S6TC7:user3197919=Heidebreicht,_Anne_Marie_Ling, arn=arn:aws:sts::902743396461:assumed-rol
6 1.08 {type=AWSService, principalid=null, arn=null, accountid=null, invokedby=ec2.amazonaws.com, accesskeyid=null, username=null, sessioncontext=null}
7 1.09 {type=AssumedRole, principalid=AROA5EL5TCBWSU32S6TC7:user3197919=Heidebreicht,_Anne_Marie_Ling, arn=arn:aws:sts::902743396461:assumed-rol
8 1.09 {type=AssumedRole, principalid=AROA5EL5TCBWSU32S6TC7:user3197919=Heidebreicht,_Anne_Marie_Ling, arn=arn:aws:sts::902743396461:assumed-rol
9 1.09 {type=AssumedRole, principalid=AROA5EL5TCBWSU32S6TC7:user3197919=Heidebreicht,_Anne_Marie_Ling, arn=arn:aws:sts::902743396461:assumed-rol
10 1.08 {type=AssumedRole, principalid=AROA5EL5TCBWXRK26BYGN:i-0710082fbb96f8c7e, arn=arn:aws:sts::902743396461:assumed-role/WebServerRole/i-07
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

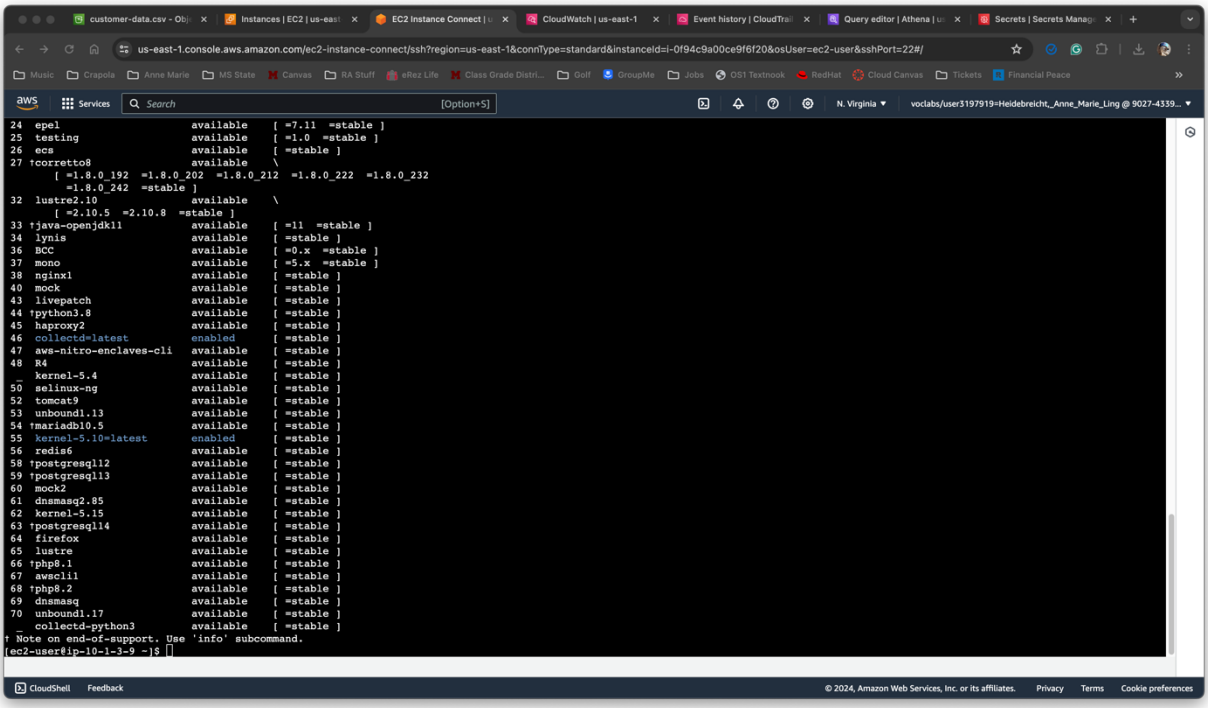


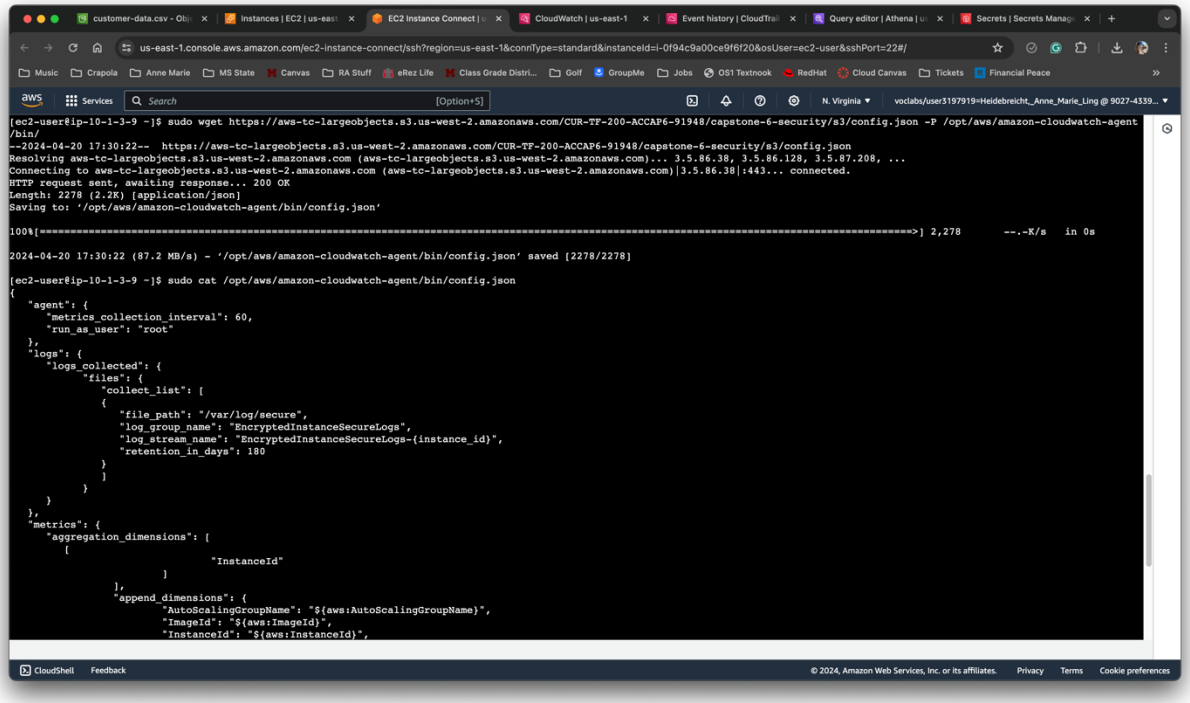


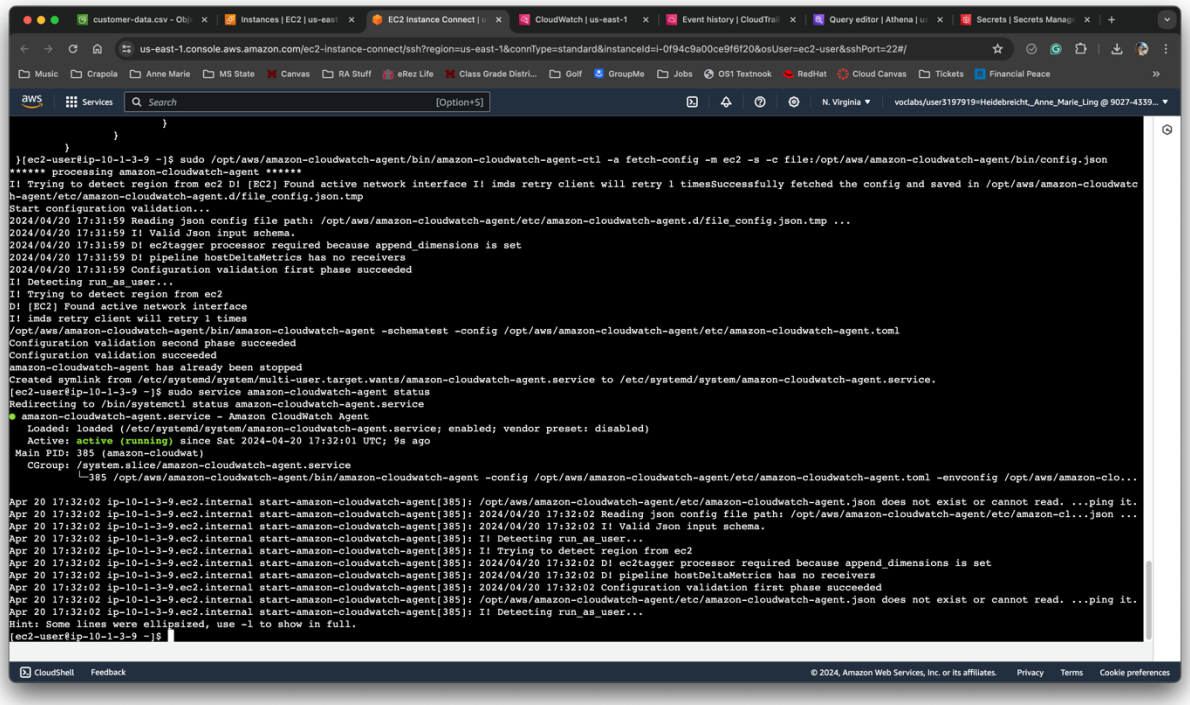
Task 4.2: Use CloudWatch Logs to monitor secure logs

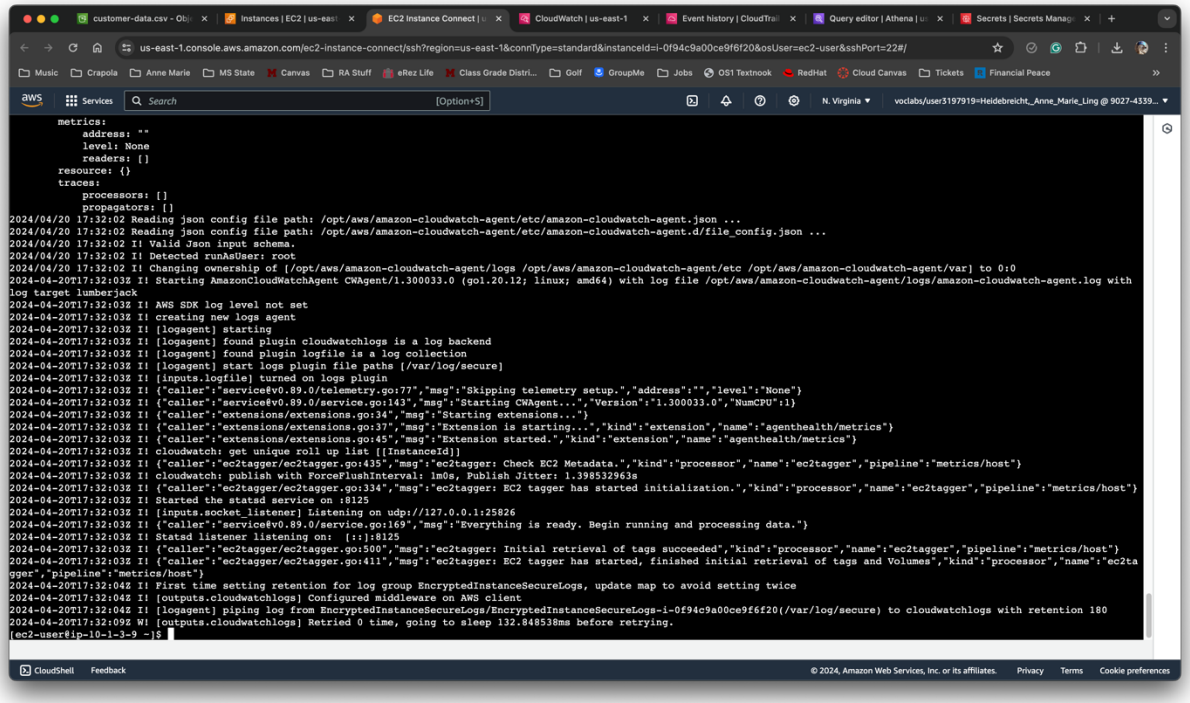

customer-data.csv - Object
Instances | EC2 | us-east-1
CloudWatch | us-east-1
Event history | CloudTrail | us
Query editor | Athena | us-ea
Secrets | Secrets Manager |
us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#logsV2:log-groups
Music
Crapola
Anne Marie
MS State
Canvas
RA Stuff
eRez Life
Class Grade Distri...
Golf
GroupMe
Jobs
OS1 Textnook
RedHat
Cloud Canvas
Tickets
Financial Peace
aws
Services
Search
[Option+S]
N. Virginia
voclabs/user3197919=Heidebreicht,_Anne_Marie_Ling @ 9027-4339...
CloudWatch
Favorites and recents
Dashboards
Alarms
Logs
Log groups
Log Anomalies
Live Tail
Logs Insights
Metrics
X-Ray traces
Events
Application Signals
Network monitoring
Insights
Settings
Getting Started
What's new
Log groups (5)
By default, we only load up to 10000 log groups.
Actions
View in Logs Insights
Start tailing
Create log group
Filter log groups or try prefix search
Exact match
Log group
Log class
Anomaly d...
Data protec...
Sensitive d...
Retention
Metric filters
/aws/lambda/c116924a2785851l6436522t1-AdjustA...
/aws/lambda/c116924a2785851l6436522t1-AdjustB...
LabVPCFlowLogs
NetworkFirewallVPCLogs
EncryptedInstanceSecureLogs
Standard
Configure
Never expire
6 months
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

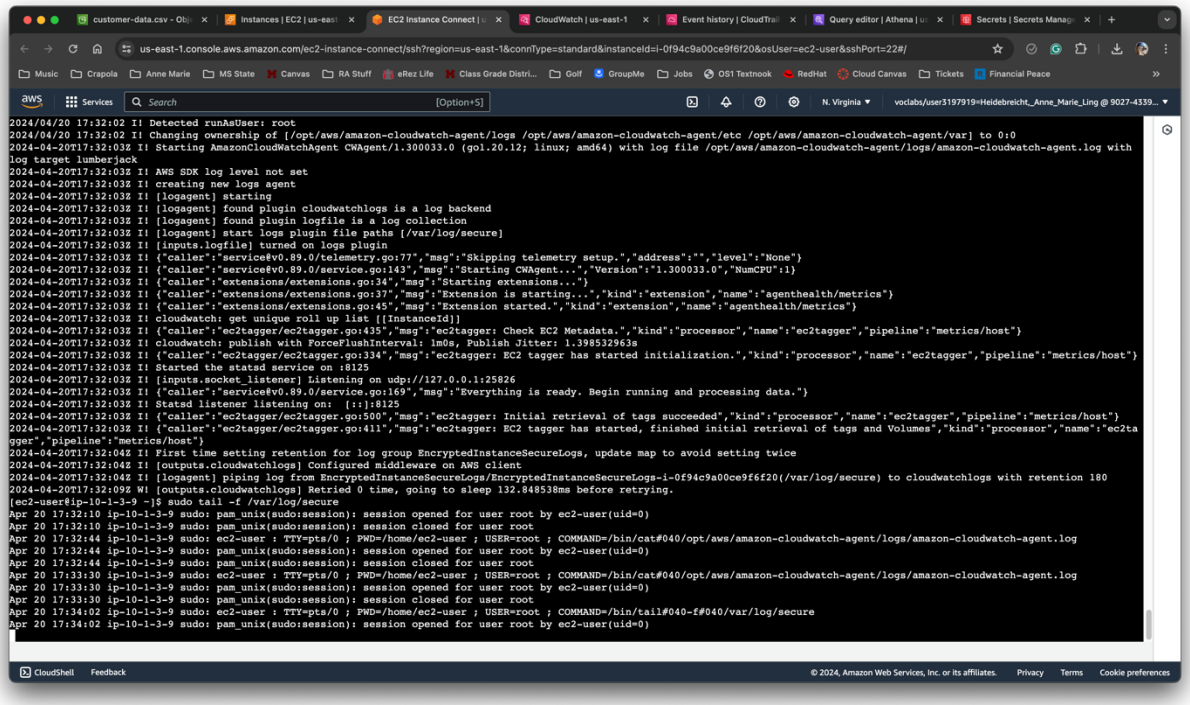

customer-data.csv - Obj
Instances | EC2 | us-east
EC2 Instance Connect |
CloudWatch | us-east-1
Event history | CloudTrail
Query editor | Athena |
Secrets | Secrets Manag
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-0f94c9a00ce9f6f20&osUser=ec2-user&sshPort=22#/
Music
Crapola
Anne Marie
MS State
Canvas
RA Stuff
eRez Life
Class Grade Distri...
Golf
GroupMe
Jobs
OS1 Textnook
RedHat
Cloud Canvas
Tickets
Financial Peace
aws
Services
Search
[Option+S]
N. Virginia
voclabs/user3197919=Heidebreicht,_Anne_Marie_Ling @ 9027-4339...
A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/
[ec2-user@ip-10-1-3-9 ~]$ sudo yum install -y amazon-cloudwatch-agent
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core | 3.6 kB 00:00:00
Resolving Dependencies
--> Running transaction check
---> Package amazon-cloudwatch-agent.x86_64 0:1.300033.0-1.amzn2 will be installed
--> Finished Dependency Resolution
Dependencies Resolved
Package Arch Version Repository Size
Installing:
amazon-cloudwatch-agent x86_64 1.300033.0-1.amzn2 amzn2-core 95 M
Transaction Summary
Install 1 Package
Total download size: 95 M
Installed size: 360 M
Downloading packages:
amazon-cloudwatch-agent-1.300033.0-1.amzn2.x86_64.rpm | 95 MB 00:00:01
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
create group cwagent, result: 0
create user cwagent, result: 0
Installing : amazon-cloudwatch-agent-1.300033.0-1.amzn2.x86_64 1/1
Verifying : amazon-cloudwatch-agent-1.300033.0-1.amzn2.x86_64 1/1
Installed:
amazon-cloudwatch-agent.x86_64 0:1.300033.0-1.amzn2
Complete!
[ec2-user@ip-10-1-3-9 ~]$
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

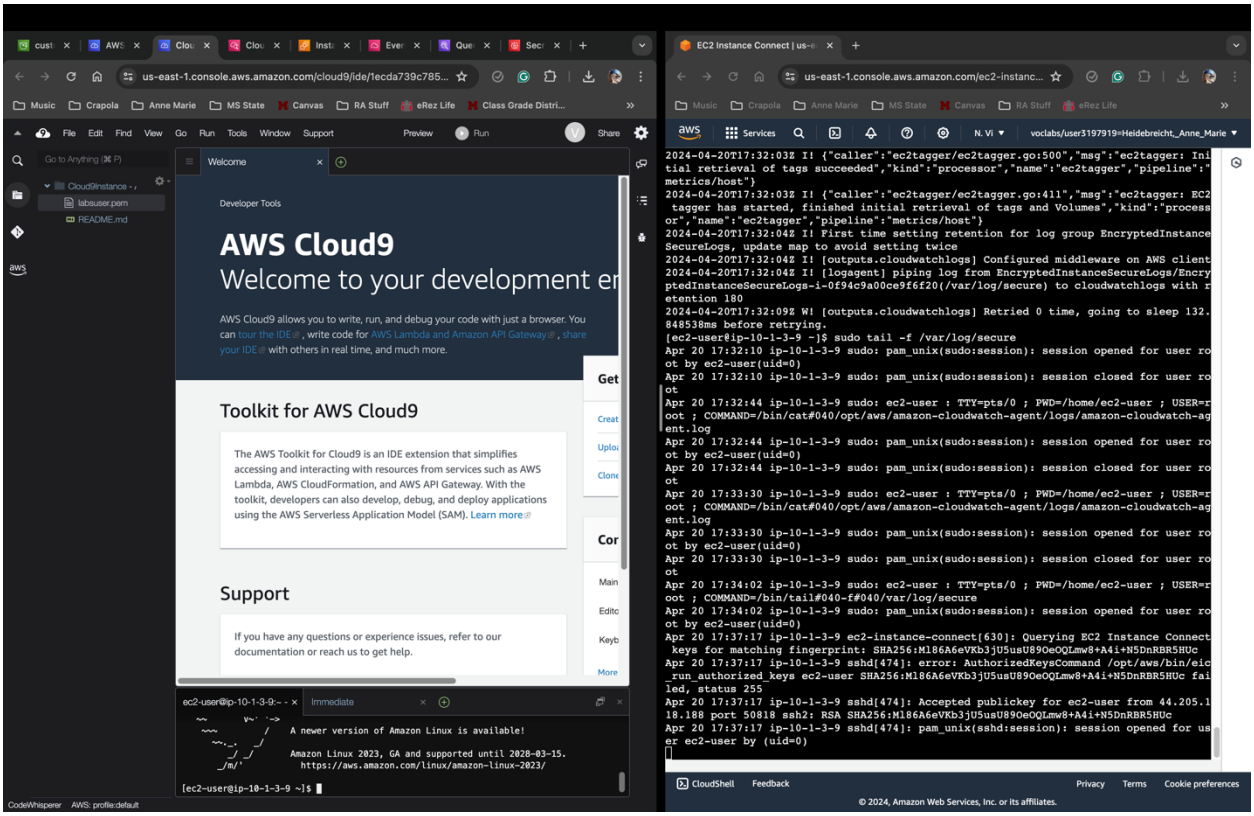

customer-data.csv - Obj
Instances | EC2 | us-east
EC2 Instance Connect | u
CloudWatch | us-east-1
Event history | CloudTrail
Query editor | Athena | u
Secrets | Secrets Manag
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-0f94c9a00ce9f6f20&osUser=ec2-user&sshPort=22#/
Music
Crapola
Anne Marie
MS State
Canvas
RA Stuff
eRez Life
Class Grade Distri...
Golf
GroupMe
Jobs
OS1 Textnook
RedHat
Cloud Canvas
Tickets
Financial Peace
aws
Services
Search
[Option+S]
N. Virginia
voclabs/user3197919=Heidebreicht,_Anne_Marie_Ling @ 9027-4339...
24 epel available [=7.11 =stable]
25 testing available [=1.0 =stable]
26 ecs available [=stable]
27 †corretto8 available \
[=1.8.0_192 =1.8.0_202 =1.8.0_212 =1.8.0_222 =1.8.0_232
=1.8.0_242 =stable]
32 lustre2.10 available \
[=2.10.5 =2.10.8 =stable]
33 †java-openjdk11 available [=11 =stable]
34 lynis available [=stable]
36 BCC available [=0.x =stable]
37 mono available [=5.x =stable]
38 nginx1 available [=stable]
40 mock available [=stable]
43 livepatch available [=stable]
44 †python3.8 available [=stable]
45 haproxy2 available [=stable]
46 collectd=latest enabled [=stable]
47 aws-nitro-enclaves-cli available [=stable]
48 R4 available [=stable]
_ kernel-5.4 available [=stable]
50 selinux-ng available [=stable]
52 tomcat9 available [=stable]
53 unbound1.13 available [=stable]
54 †mariadb10.5 available [=stable]
55 kernel-5.10=latest enabled [=stable]
56 redis6 available [=stable]
58 †postgresql12 available [=stable]
59 †postgresql13 available [=stable]
60 mock2 available [=stable]
61 dnsmasq2.85 available [=stable]
62 kernel-5.15 available [=stable]
63 †postgresql14 available [=stable]
64 firefox available [=stable]
65 lustre available [=stable]
66 †php8.1 available [=stable]
67 awscli1 available [=stable]
68 †php8.2 available [=stable]
69 dnsmasq available [=stable]
70 unbound1.17 available [=stable]
_ collectd-python3 available [=stable]
† Note on end-of-support. Use 'info' subcommand.
[ec2-user@ip-10-1-3-9 ~]$
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


customer-data.csv - Obj
Instances | EC2 | us-east
EC2 Instance Connect | u
CloudWatch | us-east-1
Event history | CloudTrail
Query editor | Athena | u
Secrets | Secrets Manag
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-0f94c9a00ce9f6f20&osUser=ec2-user&sshPort=22#/
Music
Crapola
Anne Marie
MS State
Canvas
RA Stuff
eRez Life
Class Grade Distri...
Golf
GroupMe
Jobs
OS1 Textnook
RedHat
Cloud Canvas
Tickets
Financial Peace
aws
Services
Search
[Option+S]
N. Virginia
voclabs/user3197919=Heidebreicht,_Anne_Marie_Ling @ 9027-4339...
[ec2-user@ip-10-1-3-9 ~]$ sudo wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACCAP6-91948/capstone-6-security/s3/config.json -P /opt/aws/amazon-cloudwatch-agent/bin/
--2024-04-20 17:30:22-- https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACCAP6-91948/capstone-6-security/s3/config.json
Resolving aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)... 3.5.86.38, 3.5.86.128, 3.5.87.208, ...
Connecting to aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)|3.5.86.38|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2278 (2.2K) [application/json]
Saving to: '/opt/aws/amazon-cloudwatch-agent/bin/config.json'
100%[=========>] 2,278 --.-K/s in 0s
2024-04-20 17:30:22 (87.2 MB/s) - '/opt/aws/amazon-cloudwatch-agent/bin/config.json' saved [2278/2278]
[ec2-user@ip-10-1-3-9 ~]$ sudo cat /opt/aws/amazon-cloudwatch-agent/bin/config.json
{
"agent": {
"metrics_collection_interval": 60,
"run_as_user": "root"
},
"logs": {
"logs_collected": {
"files": {
"collect_list": [
{
"file_path": "/var/log/secure",
"log_group_name": "EncryptedInstanceSecureLogs",
"log_stream_name": "EncryptedInstanceSecureLogs-{instance_id}",
"retention_in_days": 180
}
]
}
}
},
"metrics": {
"aggregation_dimensions": [
[
"InstanceId"
]
],
"append_dimensions": {
"AutoScalingGroupName": "${aws:AutoScalingGroupName}",
"ImageId": "${aws:ImageId}",
"InstanceId": "${aws:InstanceId}",
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


customer-data.csv - Obj
Instances | EC2 | us-east
EC2 Instance Connect | u
CloudWatch | us-east-1
Event history | CloudTrail
Query editor | Athena | u
Secrets | Secrets Manag
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-0f94c9a00ce9f6f20&osUser=ec2-user&sshPort=22#/
Music
Crapola
Anne Marie
MS State
Canvas
RA Stuff
eRez Life
Class Grade Distri...
Golf
GroupMe
Jobs
OS1 Textnook
RedHat
Cloud Canvas
Tickets
Financial Peace
aws
Services
Search
[Option+S]
N. Virginia
voclabs/user3197919=Heidebreicht,_Anne_Marie_Ling @ 9027-4339...
}
}
}
}{ec2-user@ip-10-1-3-9 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl -a fetch-config -m ec2 -s -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json
****** processing amazon-cloudwatch-agent ******
I! Trying to detect region from ec2 D! [EC2] Found active network interface I! imds retry client will retry 1 timesSuccessfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Start configuration validation...
2024/04/20 17:31:59 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2024/04/20 17:31:59 I! Valid Json input schema.
2024/04/20 17:31:59 D! ec2tagger processor required because append_dimensions is set
2024/04/20 17:31:59 D! pipeline hostDeltaMetrics has no receivers
2024/04/20 17:31:59 Configuration validation first phase succeeded
I! Detecting run_as_user...
I! Trying to detect region from ec2
D! [EC2] Found active network interface
I! imds retry client will retry 1 times
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
Configuration validation second phase succeeded
Configuration validation succeeded
amazon-cloudwatch-agent has already been stopped
Created symlink from /etc/systemd/system/multi-user.target.wants/amazon-cloudwatch-agent.service to /etc/systemd/system/amazon-cloudwatch-agent.service.
[ec2-user@ip-10-1-3-9 ~]$ sudo service amazon-cloudwatch-agent status
Redirecting to /bin/systemctl status amazon-cloudwatch-agent.service
● amazon-cloudwatch-agent.service - Amazon CloudWatch Agent
Loaded: loaded (/etc/systemd/system/amazon-cloudwatch-agent.service; enabled; vendor preset: disabled)
Active: active (running) since Sat 2024-04-20 17:32:01 UTC; 9s ago
Main PID: 385 (amazon-cloudwat)
CGroup: /system.slice/amazon-cloudwatch-agent.service
└─385 /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml -envconfig /opt/aws/amazon-clo...
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json does not exist or cannot read. ...ping it.
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: 2024/04/20 17:32:02 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cl...json ...
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: 2024/04/20 17:32:02 I! Valid Json input schema.
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: I! Detecting run_as_user...
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: I! Trying to detect region from ec2
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: 2024/04/20 17:32:02 D! ec2tagger processor required because append_dimensions is set
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: 2024/04/20 17:32:02 D! pipeline hostDeltaMetrics has no receivers
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: 2024/04/20 17:32:02 Configuration validation first phase succeeded
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json does not exist or cannot read. ...ping it.
Apr 20 17:32:02 ip-10-1-3-9.ec2.internal start-amazon-cloudwatch-agent[385]: I! Detecting run_as_user...
Hint: Some lines were ellipsized, use -l to show in full.
[ec2-user@ip-10-1-3-9 ~]$
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


customer-data.csv - Obj
Instances | EC2 | us-east
EC2 Instance Connect | u
CloudWatch | us-east-1
Event history | CloudTrail
Query editor | Athena | u
Secrets | Secrets Manag
us-east-1.console.aws.amazon.com/ec2-instance-connect/ssh?region=us-east-1&connType=standard&instanceId=i-0f94c9a00ce9f6f20&osUser=ec2-user&sshPort=22#/
Music
Crapola
Anne Marie
MS State
Canvas
RA Stuff
eRez Life
Class Grade Distri...
Golf
GroupMe
Jobs
OS1 Textnook
RedHat
Cloud Canvas
Tickets
Financial Peace
aws
Services
Search
[Option+S]
N. Virginia
voclabs/user3197919=Heidebreicht,_Anne_Marie_Ling @ 9027-4339...
metrics:
address: ""
level: None
readers: []
resource: {}
traces:
processors: []
propagators: []
2024/04/20 17:32:02 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json ...
2024/04/20 17:32:02 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json ...
2024/04/20 17:32:02 I! Valid Json input schema.
2024/04/20 17:32:02 I! Detected runAsUser: root
2024/04/20 17:32:02 I! Changing ownership of [/opt/aws/amazon-cloudwatch-agent/logs /opt/aws/amazon-cloudwatch-agent/etc /opt/aws/amazon-cloudwatch-agent/var] to 0:0
2024-04-20T17:32:03Z I! Starting AmazonCloudWatchAgent CWAgent/1.300033.0 (go1.20.12; linux; amd64) with log file /opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log with log target lumberjack
2024-04-20T17:32:03Z I! AWS SDK log level not set
2024-04-20T17:32:03Z I! creating new logs agent
2024-04-20T17:32:03Z I! [logagent] starting
2024-04-20T17:32:03Z I! [logagent] found plugin cloudwatchlogs is a log backend
2024-04-20T17:32:03Z I! [logagent] found plugin logfile is a log collection
2024-04-20T17:32:03Z I! [logagent] start logs plugin file paths [/var/log/secure]
2024-04-20T17:32:03Z I! [inputs.logfile] turned on logs plugin
2024-04-20T17:32:03Z I! {"caller":"service@v0.89.0/telemetry.go:77","msg":"Skipping telemetry setup.","address":"","level":"None"}
2024-04-20T17:32:03Z I! {"caller":"service@v0.89.0/service.go:143","msg":"Starting CWAgent...","Version":"1.300033.0","NumCPU":1}
2024-04-20T17:32:03Z I! {"caller":"extensions/extensions.go:34","msg":"Starting extensions..."}
2024-04-20T17:32:03Z I! {"caller":"extensions/extensions.go:37","msg":"Extension is starting...","kind":"extension","name":"agenthealth/metrics"}
2024-04-20T17:32:03Z I! {"caller":"extensions/extensions.go:45","msg":"Extension started.","kind":"extension","name":"agenthealth/metrics"}
2024-04-20T17:32:03Z I! cloudwatch: get unique roll up list [[InstanceId]]
2024-04-20T17:32:03Z I! {"caller":"ec2tagger/ec2tagger.go:435","msg":"ec2tagger: Check EC2 Metadata.","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
2024-04-20T17:32:03Z I! cloudwatch: publish with ForceFlushInterval: 1m0s, Publish Jitter: 1.398532963s
2024-04-20T17:32:03Z I! {"caller":"ec2tagger/ec2tagger.go:334","msg":"ec2tagger: EC2 tagger has started initialization.","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
2024-04-20T17:32:03Z I! Started the statsd service on :8125
2024-04-20T17:32:03Z I! [inputs.socket_listener] Listening on udp://127.0.0.1:25826
2024-04-20T17:32:03Z I! {"caller":"service@v0.89.0/service.go:169","msg":"Everything is ready. Begin running and processing data."}
2024-04-20T17:32:03Z I! Statsd listener listening on: [::]:8125
2024-04-20T17:32:03Z I! {"caller":"ec2tagger/ec2tagger.go:500","msg":"ec2tagger: Initial retrieval of tags succeeded","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
2024-04-20T17:32:03Z I! {"caller":"ec2tagger/ec2tagger.go:411","msg":"ec2tagger: EC2 tagger has started, finished initial retrieval of tags and Volumes","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
2024-04-20T17:32:04Z I! First time setting retention for log group EncryptedInstanceSecureLogs, update map to avoid setting twice
2024-04-20T17:32:04Z I! [outputs.cloudwatchlogs] Configured middleware on AWS client
2024-04-20T17:32:04Z I! [logagent] piping log from EncryptedInstanceSecureLogs/EncryptedInstanceSecureLogs-i-0f94c9a00ce9f6f20(/var/log/secure) to cloudwatchlogs with retention 180
2024-04-20T17:32:09Z W! [outputs.cloudwatchlogs] Retried 0 time, going to sleep 132.848538ms before retrying.
[ec2-user@ip-10-1-3-9 ~]$
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

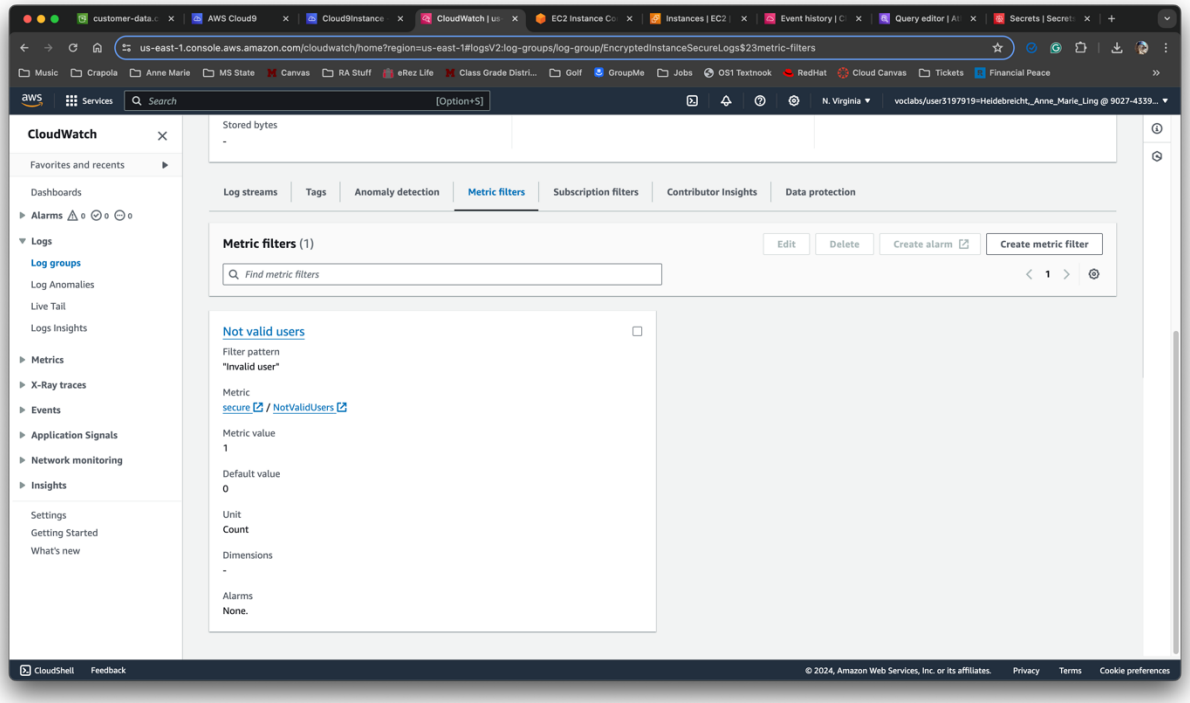

2024/04/20 17:32:02 I! Detected runAsUser: root
2024/04/20 17:32:02 I! Changing ownership of [/opt/aws/amazon-cloudwatch-agent/logs /opt/aws/amazon-cloudwatch-agent/etc /opt/aws/amazon-cloudwatch-agent/var] to 0:0
2024-04-20T17:32:03Z I! Starting AmazonCloudWatchAgent CWAgent/1.300033.0 (go1.20.12; linux; amd64) with log file /opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log with log target lumberjack
2024-04-20T17:32:03Z I! AWS SDK log level not set
2024-04-20T17:32:03Z I! creating new logs agent
2024-04-20T17:32:03Z I! [logagent] starting
2024-04-20T17:32:03Z I! [logagent] found plugin cloudwatchlogs is a log backend
2024-04-20T17:32:03Z I! [logagent] found plugin logfile is a log collection
2024-04-20T17:32:03Z I! [logagent] start logs plugin file paths [/var/log/secure]
2024-04-20T17:32:03Z I! [inputs.logfile] turned on logs plugin
2024-04-20T17:32:03Z I! {"caller":"service@v0.89.0/telemetry.go:77","msg":"Skipping telemetry setup.","address":"","level":"None"}
2024-04-20T17:32:03Z I! {"caller":"service@v0.89.0/service.go:143","msg":"Starting CWAgent...","Version":"1.300033.0","NumCPU":1}
2024-04-20T17:32:03Z I! {"caller":"extensions/extensions.go:34","msg":"Starting extensions..."}
2024-04-20T17:32:03Z I! {"caller":"extensions/extensions.go:37","msg":"Extension is starting...","kind":"extension","name":"agenthealth/metrics"}
2024-04-20T17:32:03Z I! {"caller":"extensions/extensions.go:45","msg":"Extension started.","kind":"extension","name":"agenthealth/metrics"}
2024-04-20T17:32:03Z I! cloudwatch: get unique roll up list [[InstanceId]]
2024-04-20T17:32:03Z I! {"caller":"ec2tagger/ec2tagger.go:435","msg":"ec2tagger: Check EC2 Metadata.","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
2024-04-20T17:32:03Z I! cloudwatch: publish with ForceFlushInterval: 1m0s, Publish Jitter: 1.398532963s
2024-04-20T17:32:03Z I! {"caller":"ec2tagger/ec2tagger.go:334","msg":"ec2tagger: EC2 tagger has started initialization.","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
2024-04-20T17:32:03Z I! Started the statsd service on :8125
2024-04-20T17:32:03Z I! [inputs.socket_listener] Listening on udp://127.0.0.1:25826
2024-04-20T17:32:03Z I! {"caller":"service@v0.89.0/service.go:169","msg":"Everything is ready. Begin running and processing data."}
2024-04-20T17:32:03Z I! Statsd listener listening on: [::]:8125
2024-04-20T17:32:03Z I! {"caller":"ec2tagger/ec2tagger.go:500","msg":"ec2tagger: Initial retrieval of tags succeeded","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
2024-04-20T17:32:03Z I! {"caller":"ec2tagger/ec2tagger.go:411","msg":"ec2tagger: EC2 tagger has started, finished initial retrieval of tags and Volumes","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
2024-04-20T17:32:04Z I! First time setting retention for log group EncryptedInstanceSecureLogs, update map to avoid setting twice
2024-04-20T17:32:04Z I! [outputs.cloudwatchlogs] Configured middleware on AWS client
2024-04-20T17:32:04Z I! [logagent] piping log from EncryptedInstanceSecureLogs/EncryptedInstanceSecureLogs-i-0f94c9a00ce9f6f20(/var/log/secure) to cloudwatchlogs with retention 180
2024-04-20T17:32:09Z W! [outputs.cloudwatchlogs] Retried 0 time, going to sleep 132.848538ms before retrying.
[ec2-user@ip-10-1-3-9 ~]$ sudo tail -f /var/log/secure
Apr 20 17:32:10 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Apr 20 17:32:10 ip-10-1-3-9 sudo: pam_unix(sudo:session): session closed for user root
Apr 20 17:32:44 ip-10-1-3-9 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/cat#040/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
Apr 20 17:32:44 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Apr 20 17:32:44 ip-10-1-3-9 sudo: pam_unix(sudo:session): session closed for user root
Apr 20 17:33:30 ip-10-1-3-9 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/cat#040/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
Apr 20 17:33:30 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Apr 20 17:33:30 ip-10-1-3-9 sudo: pam_unix(sudo:session): session closed for user root
Apr 20 17:34:02 ip-10-1-3-9 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/tail#040-f#040/var/log/secure
Apr 20 17:34:02 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

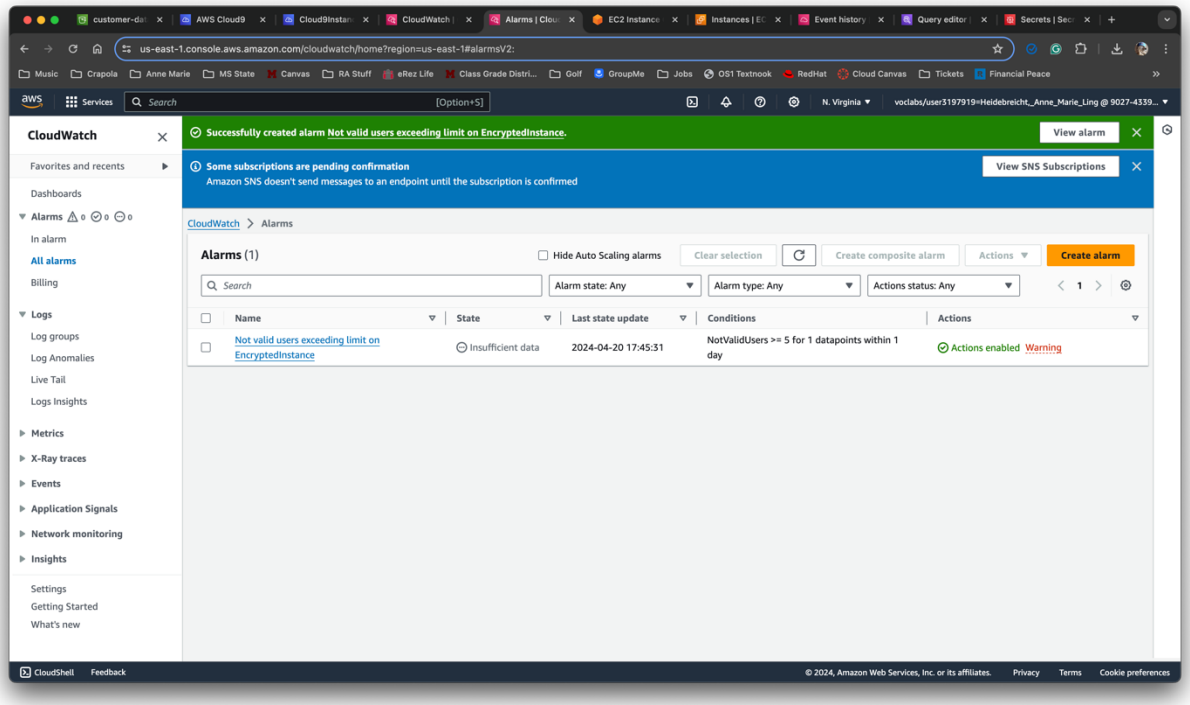

AWS Cloud9
Welcome to your development
Toolkit for AWS Cloud9
Support
A newer version of Amazon Linux is available!
Amazon Linux 2023, GA and supported until 2028-03-15.
https://aws.amazon.com/linux/amazon-linux-2023/
[ec2-user@ip-10-1-3-9 ~]$
2024-04-20T17:32:03Z I! {"caller":"ec2tagger/ec2tagger.go:500","msg":"ec2tagger: Initial retrieval of tags succeeded","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
2024-04-20T17:32:03Z I! {"caller":"ec2tagger/ec2tagger.go:411","msg":"ec2tagger: EC2 tagger has started, finished initial retrieval of tags and Volumes","kind":"processor","name":"ec2tagger","pipeline":"metrics/host"}
2024-04-20T17:32:04Z I! First time setting retention for log group EncryptedInstanceSecureLogs, update map to avoid setting twice
2024-04-20T17:32:04Z I! [outputs.cloudwatchlogs] Configured middleware on AWS client
2024-04-20T17:32:04Z I! [logagent] piping log from EncryptedInstanceSecureLogs/EncryptedInstanceSecureLogs-i-0f94c9a00ce9f6f20(/var/log/secure) to cloudwatchlogs with retention 180
2024-04-20T17:32:09Z W! [outputs.cloudwatchlogs] Retried 0 time, going to sleep 132.848538ms before retrying.
[ec2-user@ip-10-1-3-9 ~]$ sudo tail -f /var/log/secure
Apr 20 17:32:10 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Apr 20 17:32:10 ip-10-1-3-9 sudo: pam_unix(sudo:session): session closed for user root
Apr 20 17:32:44 ip-10-1-3-9 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/cat#040/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
Apr 20 17:32:44 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Apr 20 17:32:44 ip-10-1-3-9 sudo: pam_unix(sudo:session): session closed for user root
Apr 20 17:33:30 ip-10-1-3-9 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/cat#040/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log
Apr 20 17:33:30 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Apr 20 17:33:30 ip-10-1-3-9 sudo: pam_unix(sudo:session): session closed for user root
Apr 20 17:34:02 ip-10-1-3-9 sudo: ec2-user : TTY=pts/0 ; PWD=/home/ec2-user ; USER=root ; COMMAND=/bin/tail#040-f#040/var/log/secure
Apr 20 17:34:02 ip-10-1-3-9 sudo: pam_unix(sudo:session): session opened for user root by ec2-user(uid=0)
Apr 20 17:37:17 ip-10-1-3-9 ec2-instance-connect[630]: Querying EC2 Instance Connect keys for matching fingerprint: SHA256:Ml86A6eVKb3jU5usU89OeOQLmw8+A4i+N5DnRBR5HUc
Apr 20 17:37:17 ip-10-1-3-9 sshd[474]: error: AuthorizedKeysCommand /opt/aws/bin/eic_run_authorized_keys ec2-user SHA256:Ml86A6eVKb3jU5usU89OeOQLmw8+A4i+N5DnRBR5HUc failed, status 255
Apr 20 17:37:17 ip-10-1-3-9 sshd[474]: Accepted publickey for ec2-user from 44.205.18.188 port 50818 ssh2: RSA SHA256:Ml86A6eVKb3jU5usU89OeOQLmw8+A4i+N5DnRBR5HUc
Apr 20 17:37:17 ip-10-1-3-9 sshd[474]: pam_unix(sshd:session): session opened for user ec2-user by (uid=0)
CloudShell
Feedback
Privacy
Terms
Cookie preferences
© 2024, Amazon Web Services, Inc. or its affiliates.

```
[ec2-user@ip-10-1-3-9 ~]$ exit
logout
Connection to 52.2.25.201 closed.
voclabs:~/environment $ ssh -i labsuser.pem ubuntu@52.2.25.201
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $
```

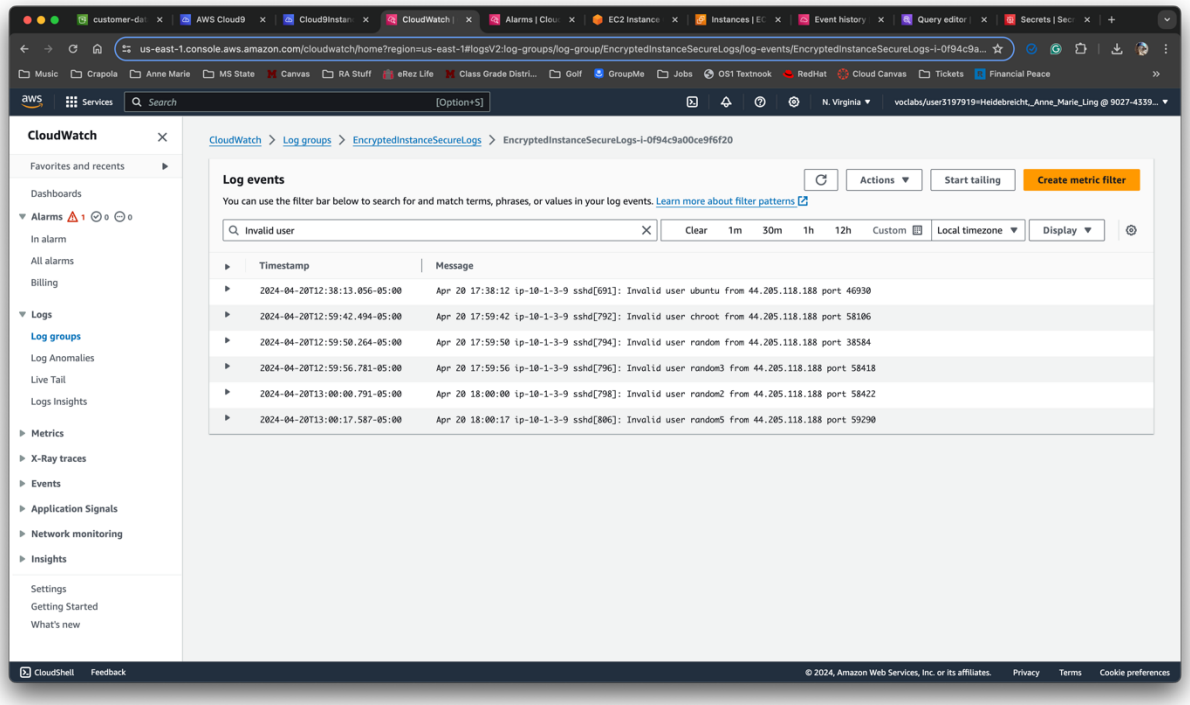
2024-04-20T12:37:48.994-05:00	Apr 20 17:37:17 ip-10-1-3-9 sshd[474]: Accepted publickey for ec2-user from 44.205.118.188 port 50818 ssh2: RSA SHA256:Ml86A6eVKb3jU5usU89Oe0…
	Apr 20 17:37:17 ip-10-1-3-9 sshd[474]: Accepted publickey for ec2-user from 44.205.118.188 port 50818 ssh2: RSA SHA256:Ml86A6eVKb3jU5usU89Oe0QLmw8+A4i+N5DnRBR5HUc
2024-04-20T12:37:48.994-05:00	Apr 20 17:37:17 ip-10-1-3-9 sshd[474]: pam_unix(sshd:session): session opened for user ec2-user by (uid=0)
2024-04-20T12:37:48.994-05:00	Apr 20 17:37:48 ip-10-1-3-9 sshd[665]: Received disconnect from 44.205.118.188 port 50818:11: disconnected by user
2024-04-20T12:37:48.994-05:00	Apr 20 17:37:48 ip-10-1-3-9 sshd[665]: Disconnected from 44.205.118.188 port 50818
2024-04-20T12:37:53.111-05:00	Apr 20 17:37:48 ip-10-1-3-9 sshd[474]: pam_unix(sshd:session): session closed for user ec2-user
2024-04-20T12:38:13.056-05:00	Apr 20 17:38:12 ip-10-1-3-9 sshd[691]: Invalid user ubuntu from 44.205.118.188 port 46930
	Apr 20 17:38:12 ip-10-1-3-9 sshd[691]: Invalid user ubuntu from 44.205.118.188 port 46930

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

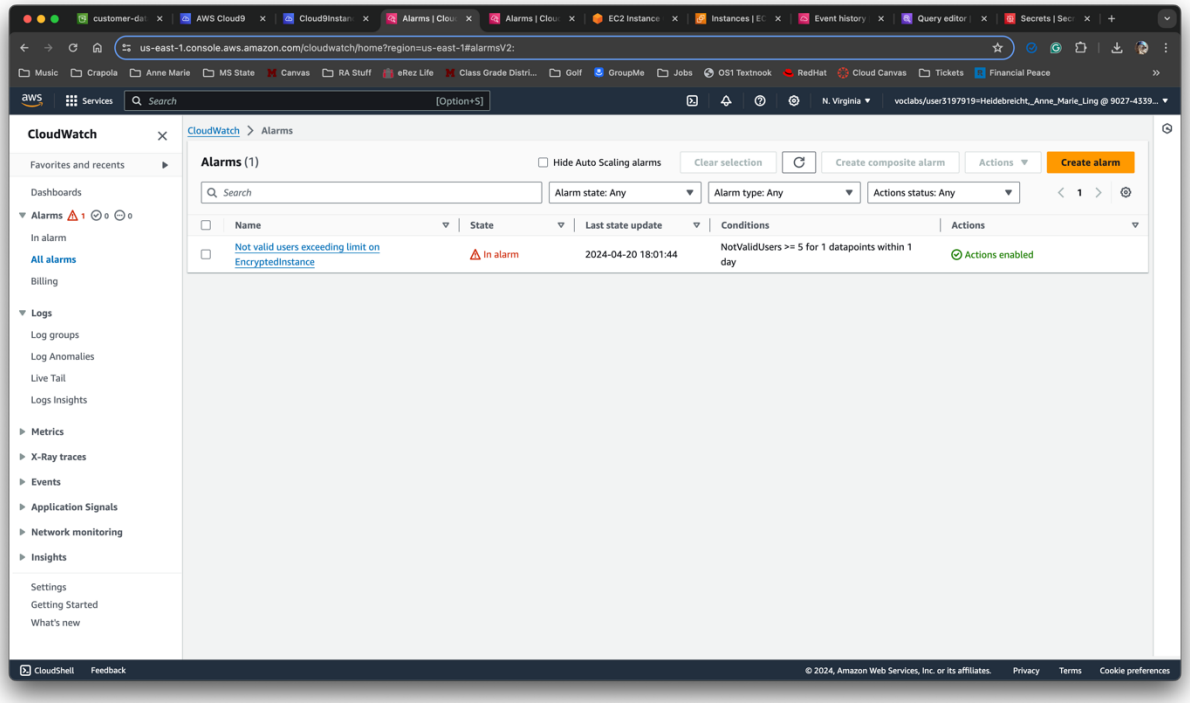


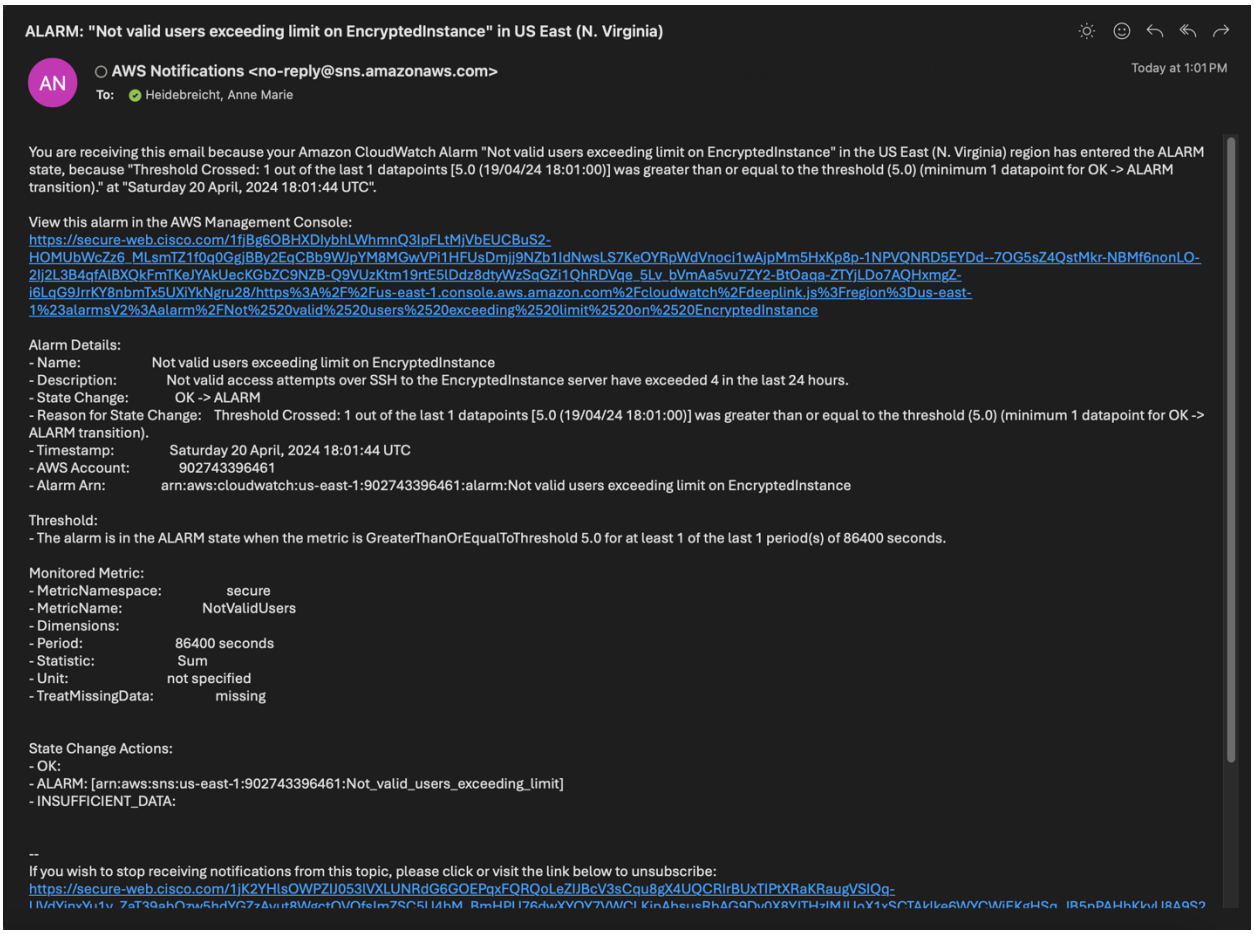



```
voclabs:~/environment $ ssh -i labsuser.pem chroot@52.2.25.201
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh -i labsuser.pem random@52.2.25.201
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh -i labsuser.pem random3@52.2.25.201
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh -i labsuser.pem random2@52.2.25.201
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $ ssh -i labsuser.pem random5@52.2.25.201
Permission denied (publickey,gssapi-keyex,gssapi-with-mic).
voclabs:~/environment $
```

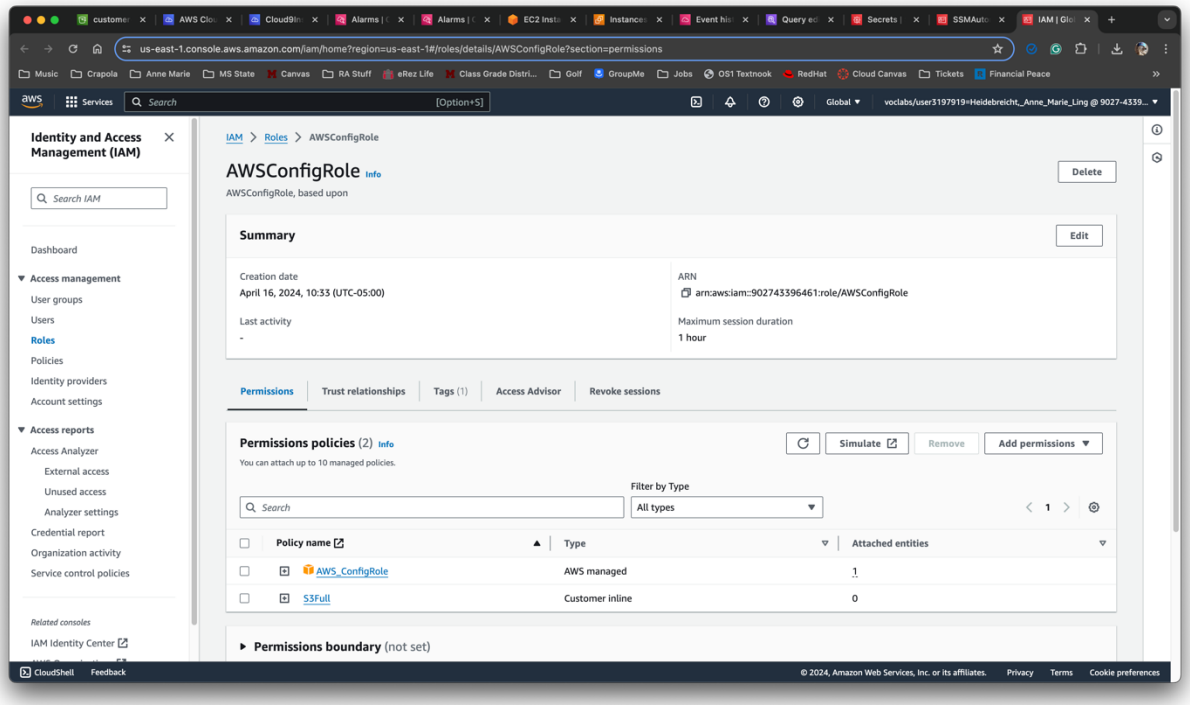

CloudWatch
Log events
Actions
Start tailing
Create metric filter
You can use the filter bar below to search for and match terms, phrases, or values in your log events. Learn more about filter patterns
Invalid user
Timestamp
Message
2024-04-20T12:38:13.056-05:00 Apr 20 17:38:12 ip-10-1-3-9 sshd[691]: Invalid user ubuntu from 44.205.118.188 port 46930
2024-04-20T12:59:42.494-05:00 Apr 20 17:59:42 ip-10-1-3-9 sshd[792]: Invalid user chroot from 44.205.118.188 port 58106
2024-04-20T12:59:50.264-05:00 Apr 20 17:59:50 ip-10-1-3-9 sshd[794]: Invalid user random from 44.205.118.188 port 38584
2024-04-20T12:59:56.781-05:00 Apr 20 17:59:56 ip-10-1-3-9 sshd[796]: Invalid user random3 from 44.205.118.188 port 58418
2024-04-20T13:00:00.791-05:00 Apr 20 18:00:00 ip-10-1-3-9 sshd[798]: Invalid user random2 from 44.205.118.188 port 58422
2024-04-20T13:00:17.587-05:00 Apr 20 18:00:17 ip-10-1-3-9 sshd[806]: Invalid user random5 from 44.205.118.188 port 59290

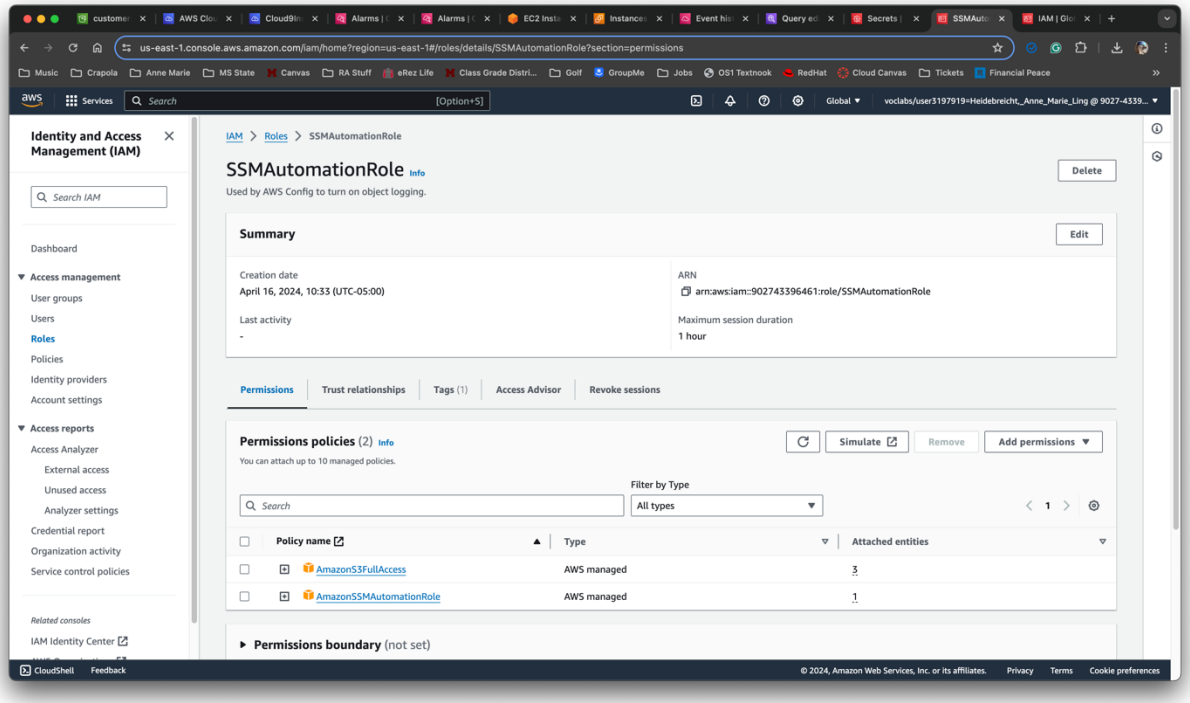
,

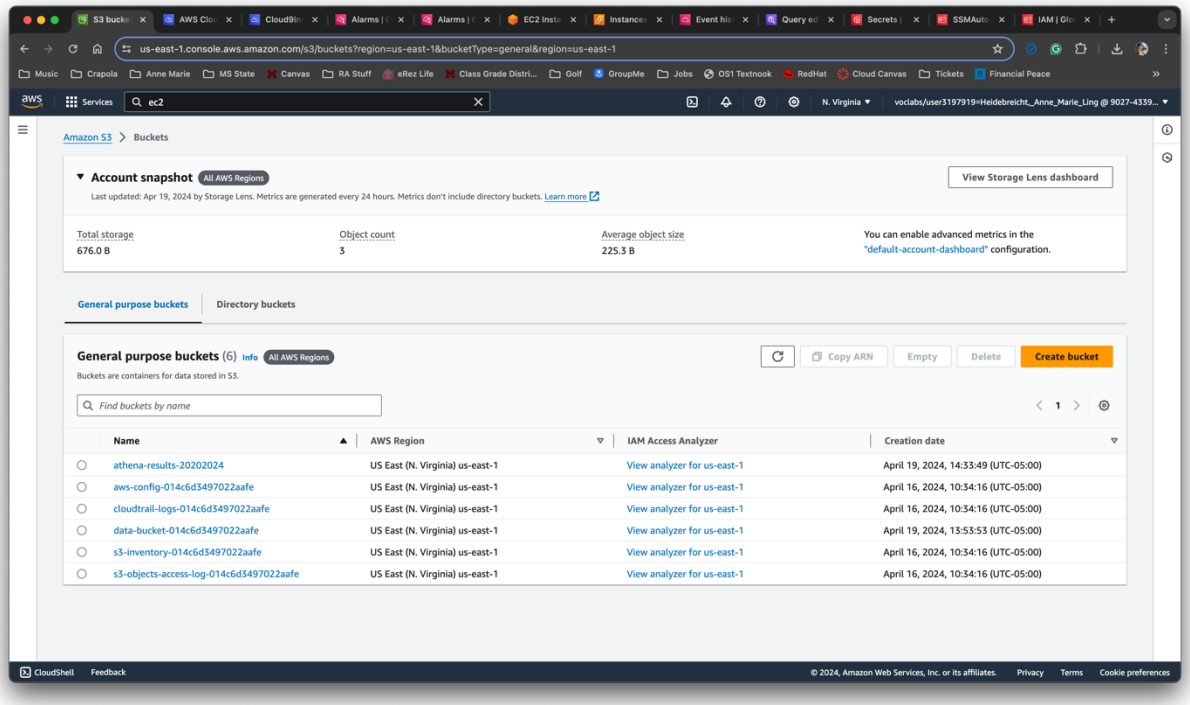

CloudWatch
Alarms (1)
Create alarm
Not valid users exceeding limit on EncryptedInstance
In alarm
2024-04-20 18:01:44
NotValidUsers >= 5 for 1 datapoints within 1 day
Actions enabled

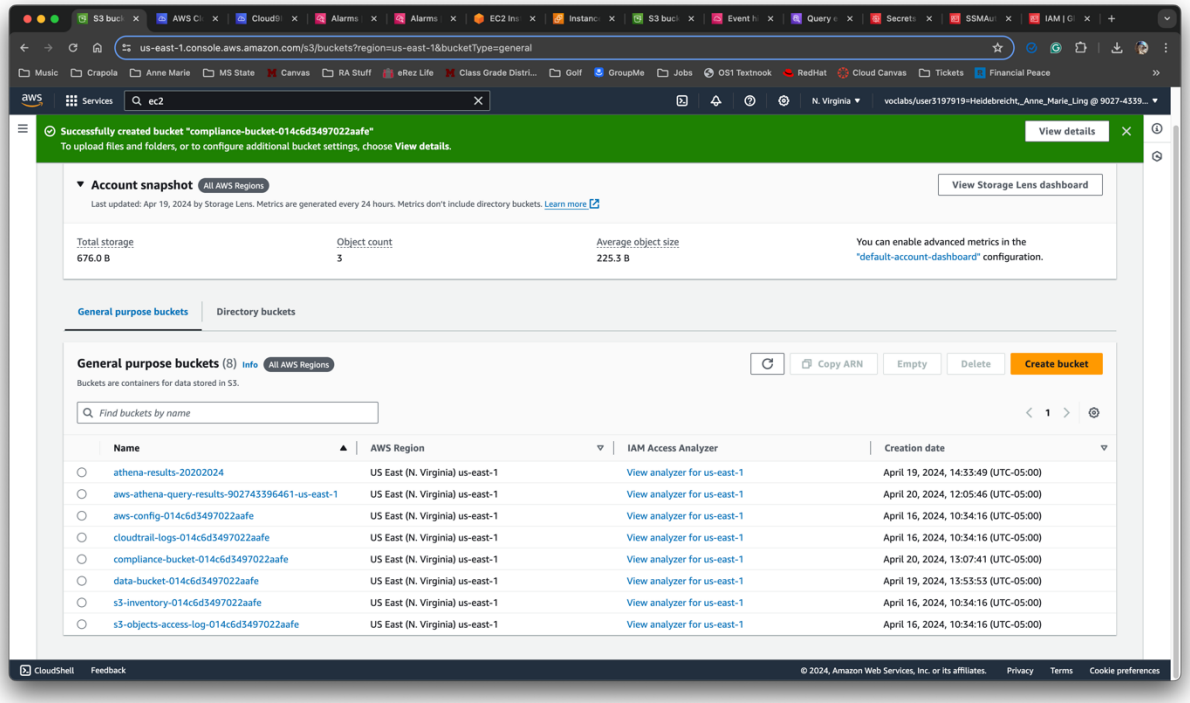


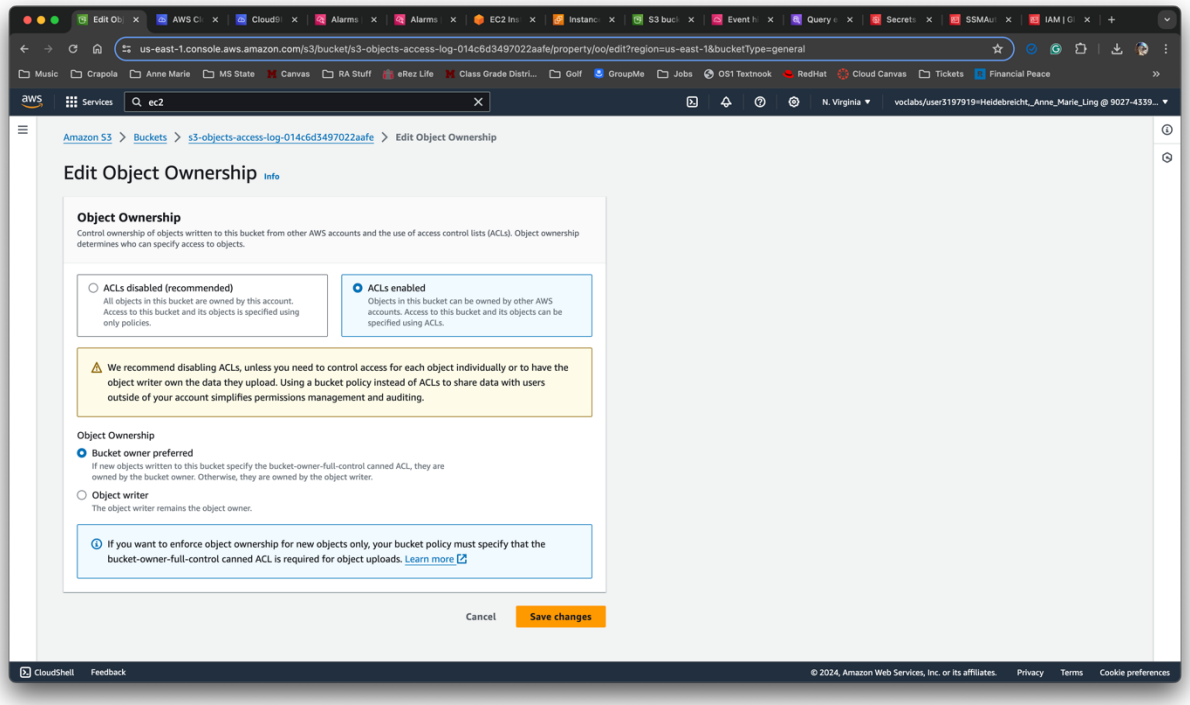
Task 4.4: Configure AWS Config to assess security settings and remediate the configuration of AWS resources

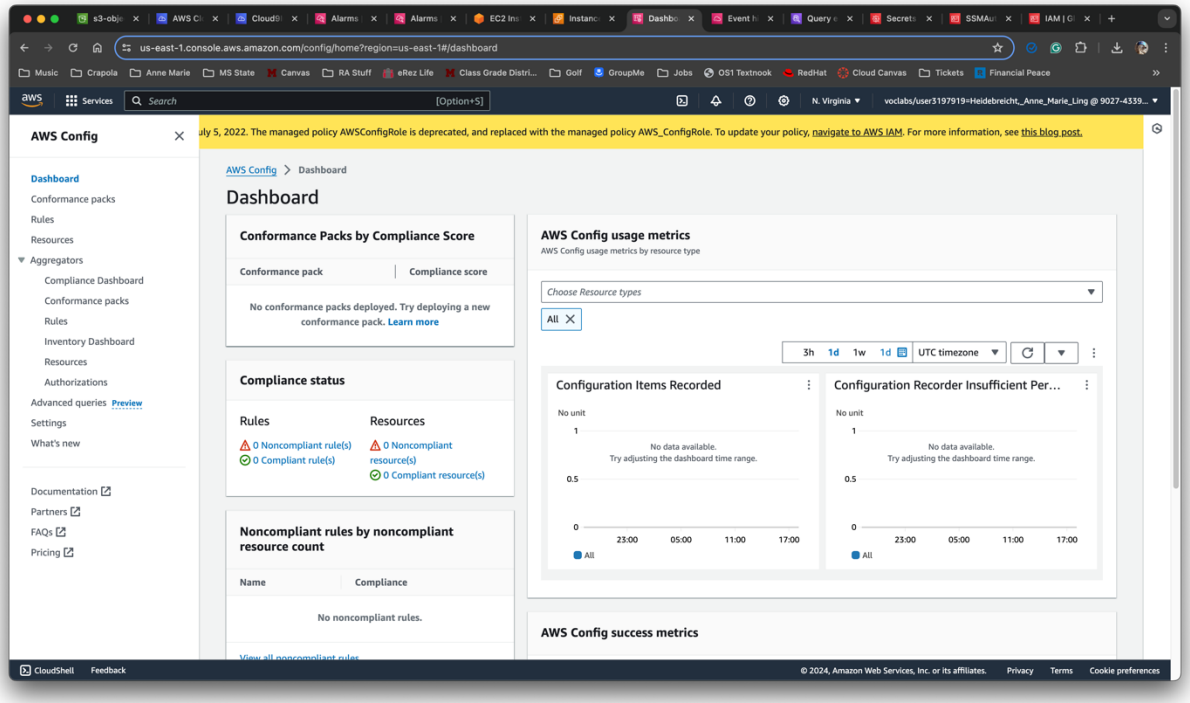

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/details/AWSConfigRole?section=permissions
Identity and Access Management (IAM)
IAM > Roles > AWSConfigRole
AWSConfigRole Info
AWSConfigRole, based upon
Delete
Summary
Edit
Creation date
April 16, 2024, 10:33 (UTC-05:00)
ARN
arn:aws:iam::902743396461:role/AWSConfigRole
Last activity
-
Maximum session duration
1 hour
Permissions
Trust relationships
Tags (1)
Access Advisor
Revoke sessions
Permissions policies (2) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter by Type
All types
Policy name
Type
Attached entities
AWS_ConfigRole
AWS managed
1
S3Full
Customer inline
0
Permissions boundary (not set)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

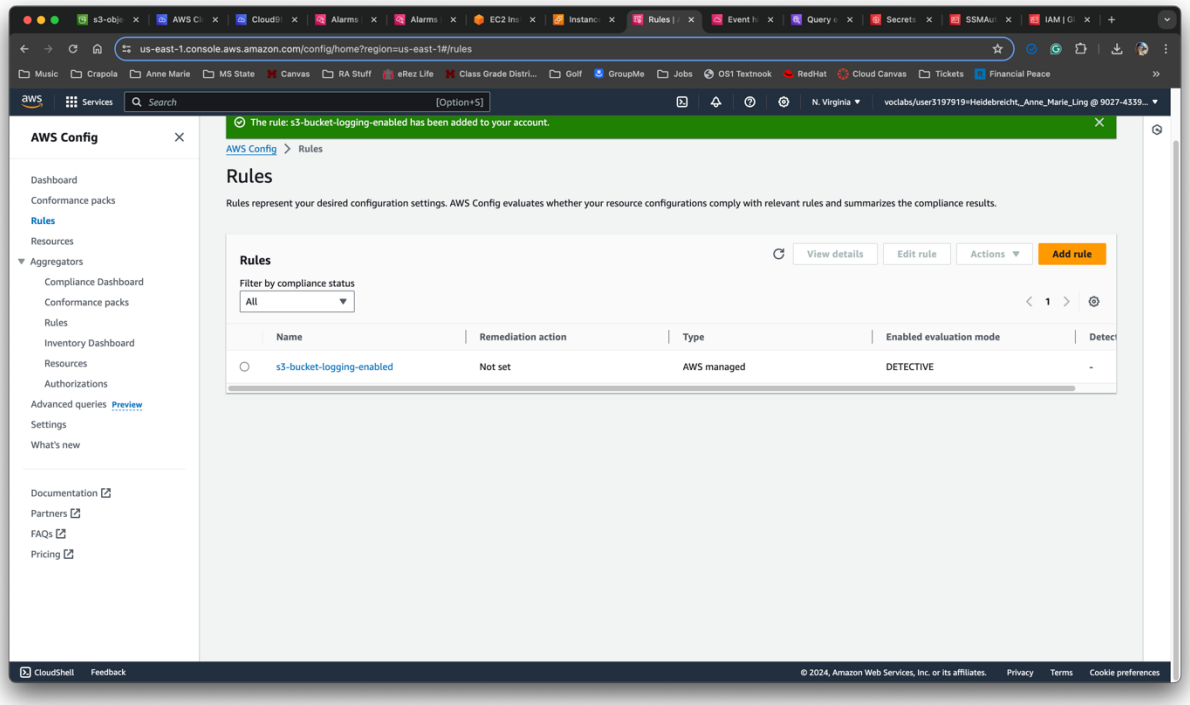

us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/details/SSMAutomationRole?section=permissions
Identity and Access Management (IAM)
IAM > Roles > SSMAutomationRole
SSMAutomationRole Info
Used by AWS Config to turn on object logging.
Delete
Summary
Edit
Creation date
April 16, 2024, 10:33 (UTC-05:00)
ARN
arn:aws:iam::902743396461:role/SSMAutomationRole
Last activity
-
Maximum session duration
1 hour
Permissions
Trust relationships
Tags (1)
Access Advisor
Revoke sessions
Permissions policies (2) Info
You can attach up to 10 managed policies.
Simulate
Remove
Add permissions
Filter by Type
All types
Policy name
Type
Attached entities
AmazonS3FullAccess
AWS managed
3
AmazonSSMAutomationRole
AWS managed
1
Permissions boundary (not set)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/s3/buckets?region=us-east-1&bucketType=general&region=us-east-1
ec2
Amazon S3 > Buckets
Account snapshot All AWS Regions
Last updated: Apr 19, 2024 by Storage Lens. Metrics are generated every 24 hours. Metrics don't include directory buckets. Learn more
View Storage Lens dashboard
Total storage 676.0 B
Object count 3
Average object size 225.3 B
You can enable advanced metrics in the "default-account-dashboard" configuration.
General purpose buckets
Directory buckets
General purpose buckets (6) Info All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
athena-results-20202024 US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 19, 2024, 14:33:49 (UTC-05:00)
aws-config-014c6d3497022aafe US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 16, 2024, 10:34:16 (UTC-05:00)
cloudtrail-logs-014c6d3497022aafe US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 16, 2024, 10:34:16 (UTC-05:00)
data-bucket-014c6d3497022aafe US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 19, 2024, 13:53:53 (UTC-05:00)
s3-inventory-014c6d3497022aafe US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 16, 2024, 10:34:16 (UTC-05:00)
s3-objects-access-log-014c6d3497022aafe US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 16, 2024, 10:34:16 (UTC-05:00)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

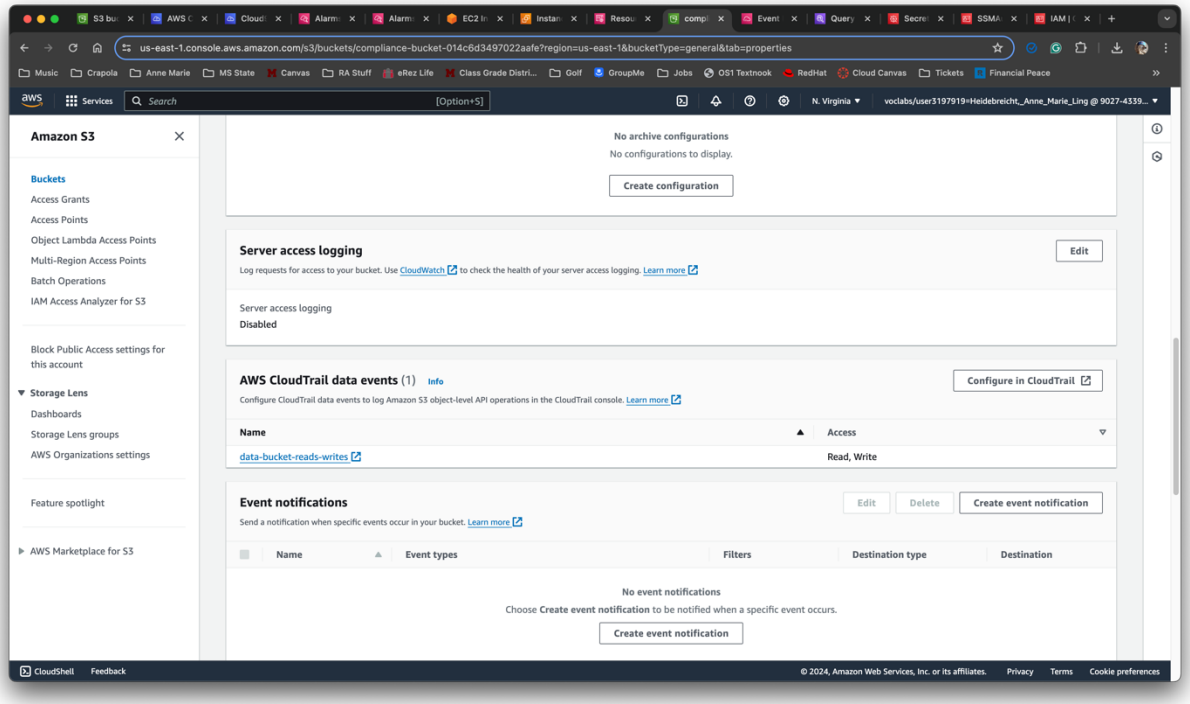

us-east-1.console.aws.amazon.com/s3/buckets?region=us-east-1&bucketType=general
ec2
Successfully created bucket "compliance-bucket-014c6d3497022aafe"
To upload files and folders, or to configure additional bucket settings, choose View details.
View details
Account snapshot All AWS Regions
Last updated: Apr 19, 2024 by Storage Lens. Metrics are generated every 24 hours. Metrics don't include directory buckets. Learn more
View Storage Lens dashboard
Total storage 676.0 B
Object count 3
Average object size 225.3 B
You can enable advanced metrics in the "default-account-dashboard" configuration.
General purpose buckets
Directory buckets
General purpose buckets (8) Info All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
Name
AWS Region
IAM Access Analyzer
Creation date
athena-results-20202024 US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 19, 2024, 14:33:49 (UTC-05:00)
aws-athena-query-results-902743396461-us-east-1 US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 20, 2024, 12:05:46 (UTC-05:00)
aws-config-014c6d3497022aafe US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 16, 2024, 10:34:16 (UTC-05:00)
cloudtrail-logs-014c6d3497022aafe US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 16, 2024, 10:34:16 (UTC-05:00)
compliance-bucket-014c6d3497022aafe US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 20, 2024, 13:07:41 (UTC-05:00)
data-bucket-014c6d3497022aafe US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 19, 2024, 13:53:53 (UTC-05:00)
s3-inventory-014c6d3497022aafe US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 16, 2024, 10:34:16 (UTC-05:00)
s3-objects-access-log-014c6d3497022aafe US East (N. Virginia) us-east-1 View analyzer for us-east-1 April 16, 2024, 10:34:16 (UTC-05:00)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

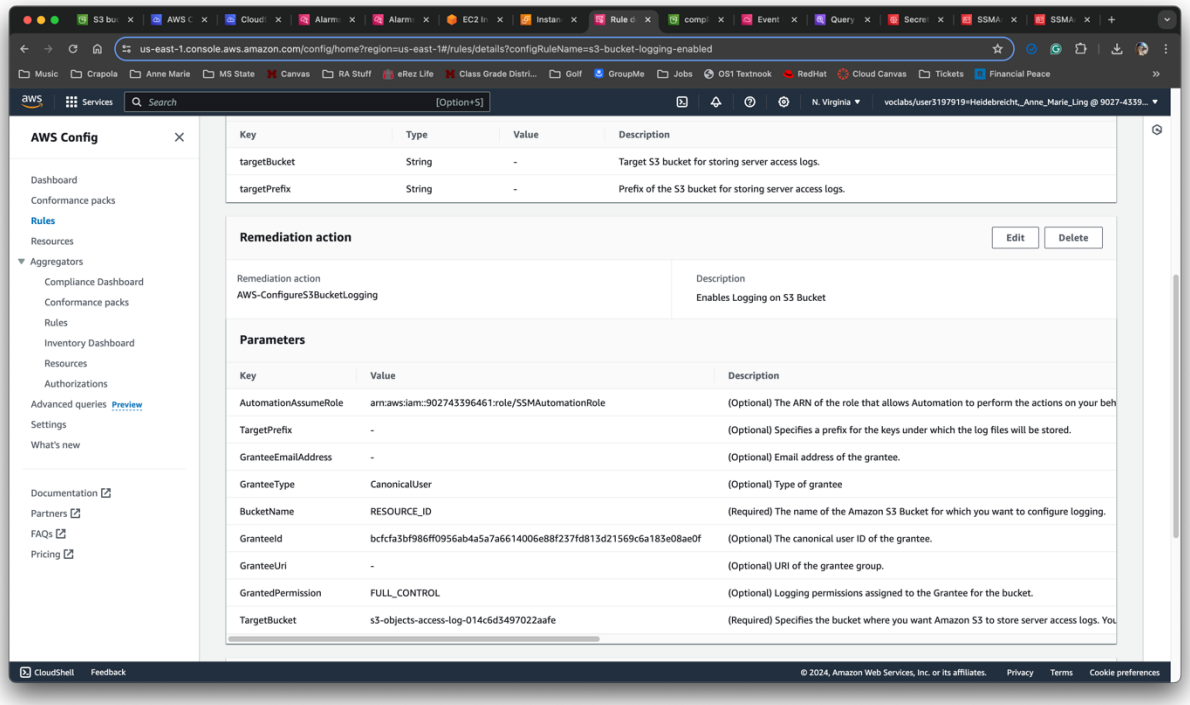

us-east-1.console.aws.amazon.com/s3/bucket/s3-objects-access-log-014c6d3497022aafe/property/oo/edit?region=us-east-1&bucketType=general
Amazon S3 > Buckets > s3-objects-access-log-014c6d3497022aafe > Edit Object Ownership
Edit Object Ownership Info
Object Ownership
Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.
ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.
ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.
We recommend disabling ACLs, unless you need to control access for each object individually or to have the object writer own the data they upload. Using a bucket policy instead of ACLs to share data with users outside of your account simplifies permissions management and auditing.
Object Ownership
Bucket owner preferred
If new objects written to this bucket specify the bucket-owner-full-control canned ACL, they are owned by the bucket owner. Otherwise, they are owned by the object writer.
Object writer
The object writer remains the object owner.
If you want to enforce object ownership for new objects only, your bucket policy must specify that the bucket-owner-full-control canned ACL is required for object uploads. Learn more
Cancel
Save changes
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

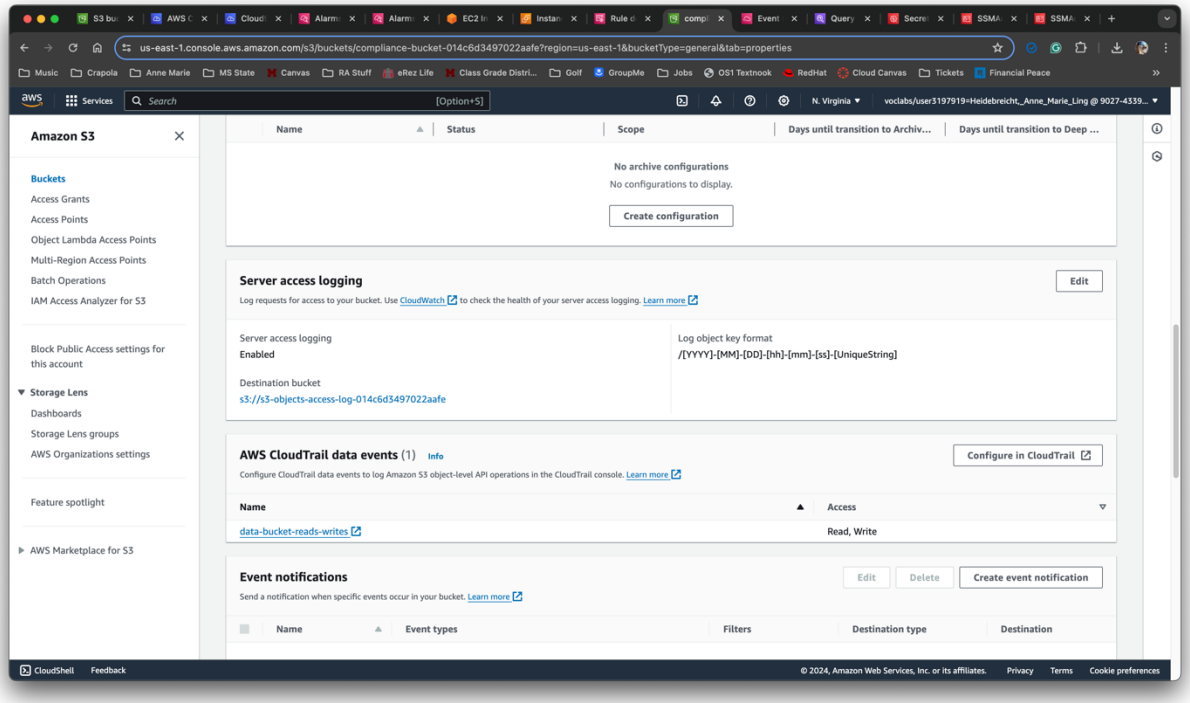

us-east-1.console.aws.amazon.com/config/home?region=us-east-1#/dashboard
AWS Config
Dashboard
Conformance packs
Rules
Resources
Aggregators
Compliance Dashboard
Conformance packs
Rules
Inventory Dashboard
Resources
Authorizations
Advanced queries Preview
Settings
What's new
Documentation
Partners
FAQs
Pricing
uly 5, 2022. The managed policy AWSConfigRole is deprecated, and replaced with the managed policy AWS_ConfigRole. To update your policy, navigate to AWS IAM. For more information, see this blog post.
AWS Config > Dashboard
Dashboard
Conformance Packs by Compliance Score
Conformance pack
Compliance score
No conformance packs deployed. Try deploying a new conformance pack. Learn more
Compliance status
Rules
0 Noncompliant rule(s)
0 Compliant rule(s)
Resources
0 Noncompliant resource(s)
0 Compliant resource(s)
Noncompliant rules by noncompliant resource count
Name
Compliance
No noncompliant rules.
AWS Config usage metrics
AWS Config usage metrics by resource type
Choose Resource types
All
3h
1d
1w
1d
UTC timezone
Configuration Items Recorded
Configuration Recorder Insufficient Per...
No unit
No data available.
Try adjusting the dashboard time range.
1
0.5
0
23:00
05:00
11:00
17:00
All
AWS Config success metrics
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



○	cloudtrail-logs-014c6d349702...	S3 Bucket	-	-	⚠ Noncompliant







Reflection

This project was very difficult and time-consuming. However, I did get some hands-on experience with AWS Security tools. It helped me learn about what the different tools did and

how they worked with other tools to create a secure application. Without the guided exercise, this project would have taken me two to three times longer to complete. I wish that we had an entire semester to complete a project like this or Project 1: Web Application Builder. Both of them were complicated and time-consuming. I think assigning one project at the beginning of the semester and having it due around midterms and then assigning the next project until the last day of finals would be a good way to divide the work so it's not so overwhelming. The project definitely was interesting, and under less stressful circumstances, I feel like I would have learned a lot more about AWS Cloud Computing.