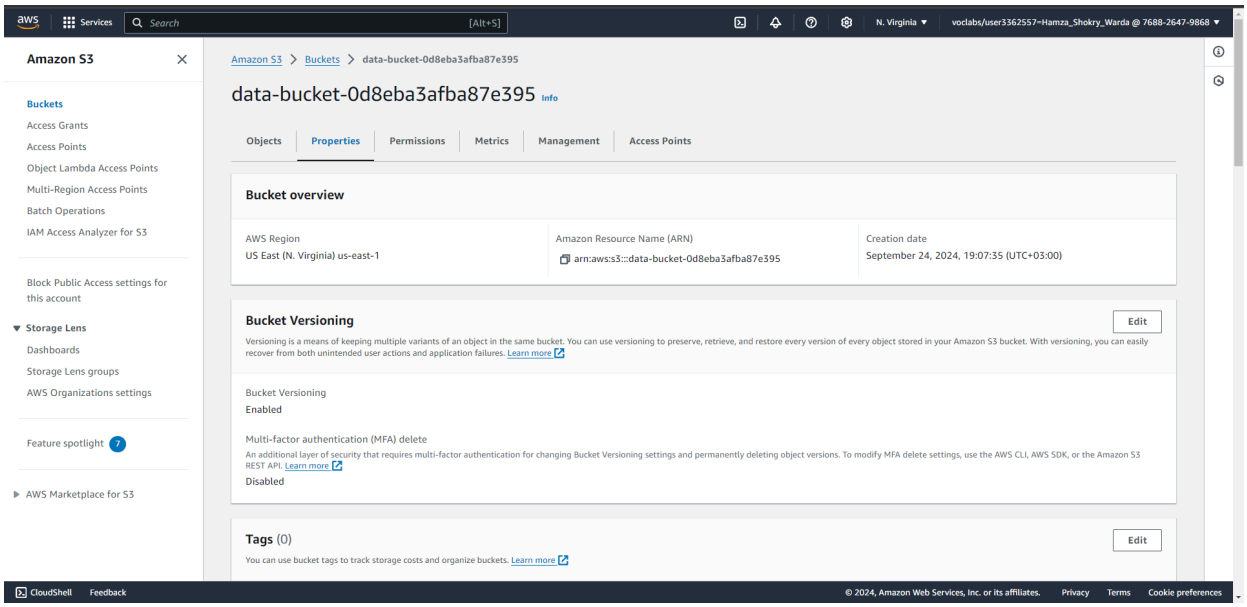
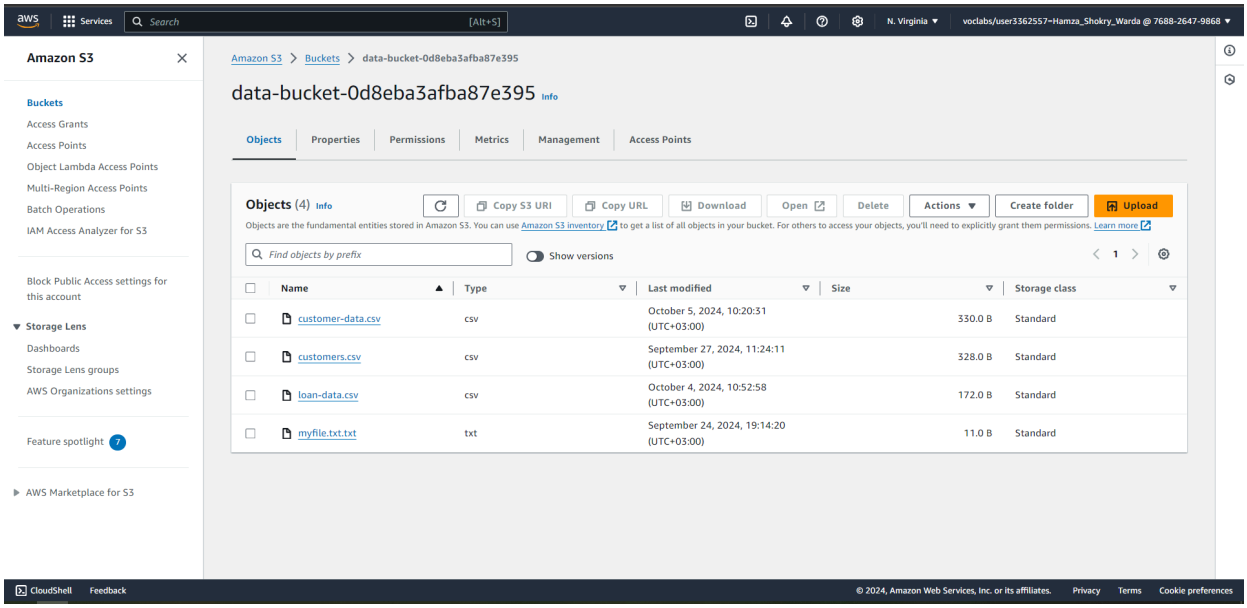
Digital Egypt Pioneers Initiative - DEPI
New Horizon Alex.
AWS Academy - AWS Cloud Architect
Project report
By: Hamza Shokry Warda

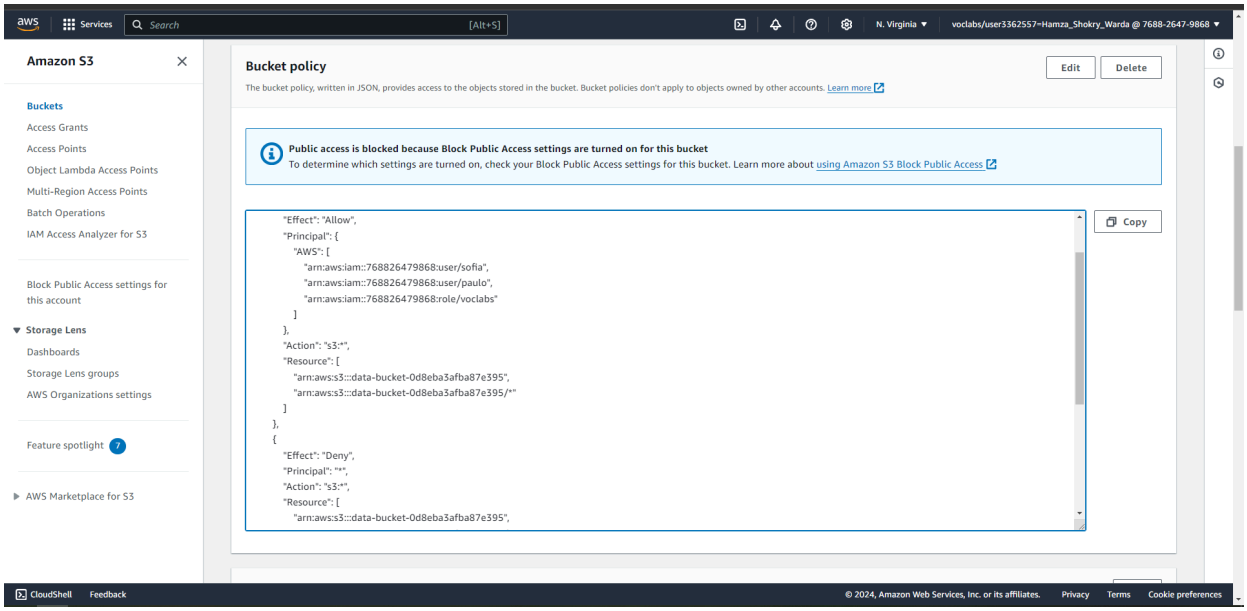
Securing and Monitoring Resources with AWS

Phase 1: Securing data in Amazon S3

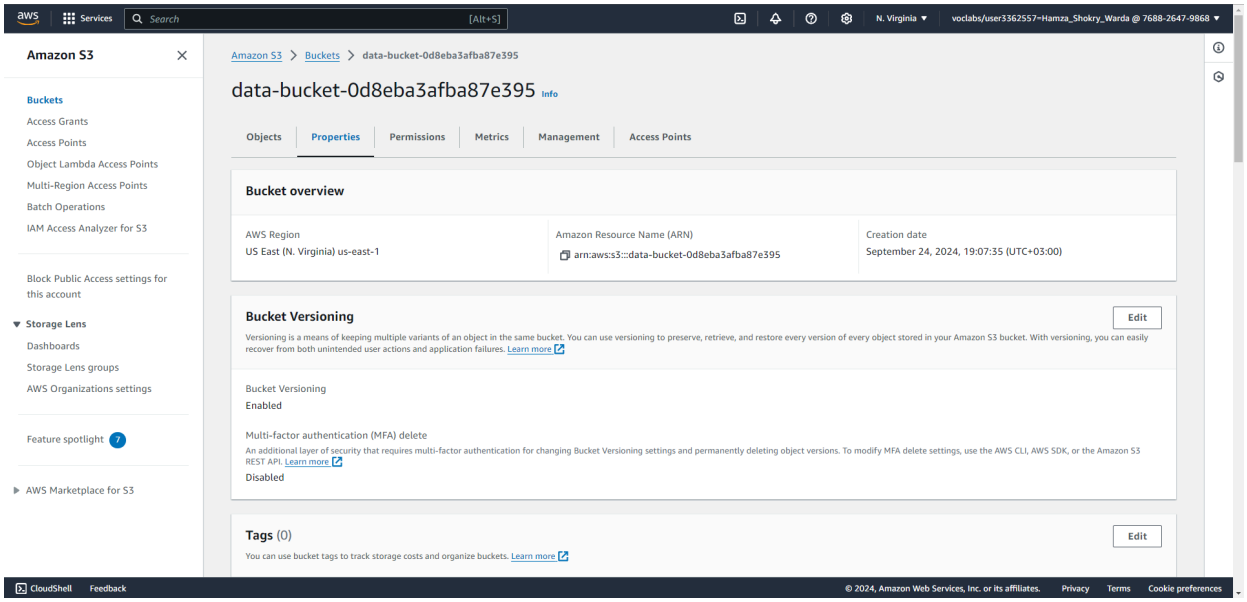
Task 1.1: Create a bucket, apply a bucket policy, and test access

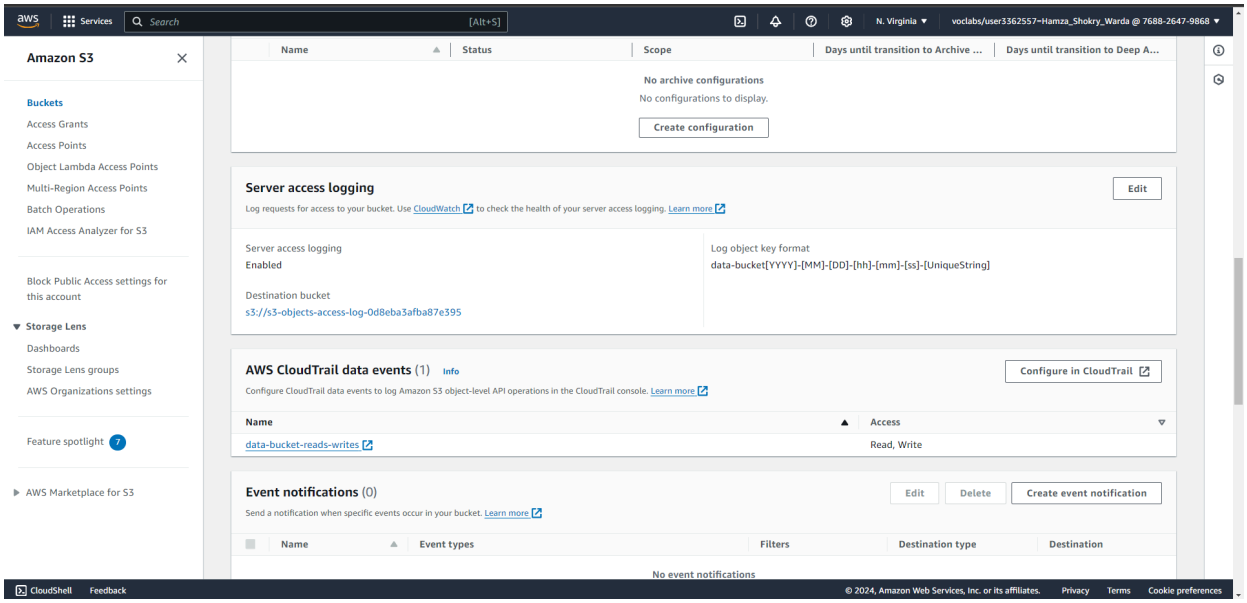


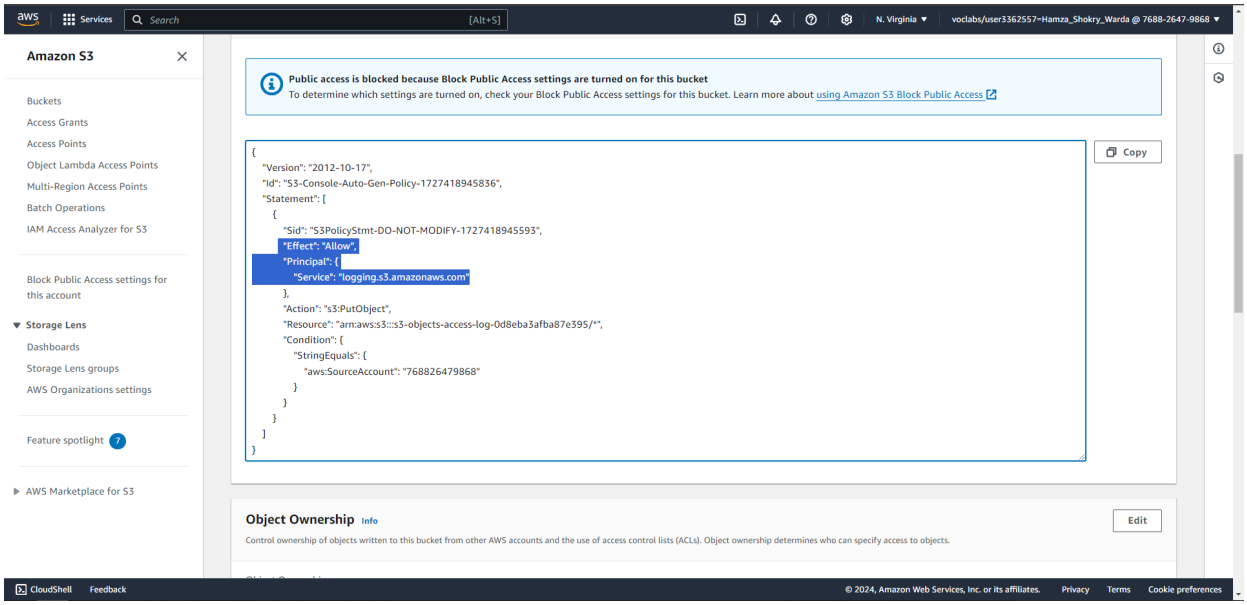




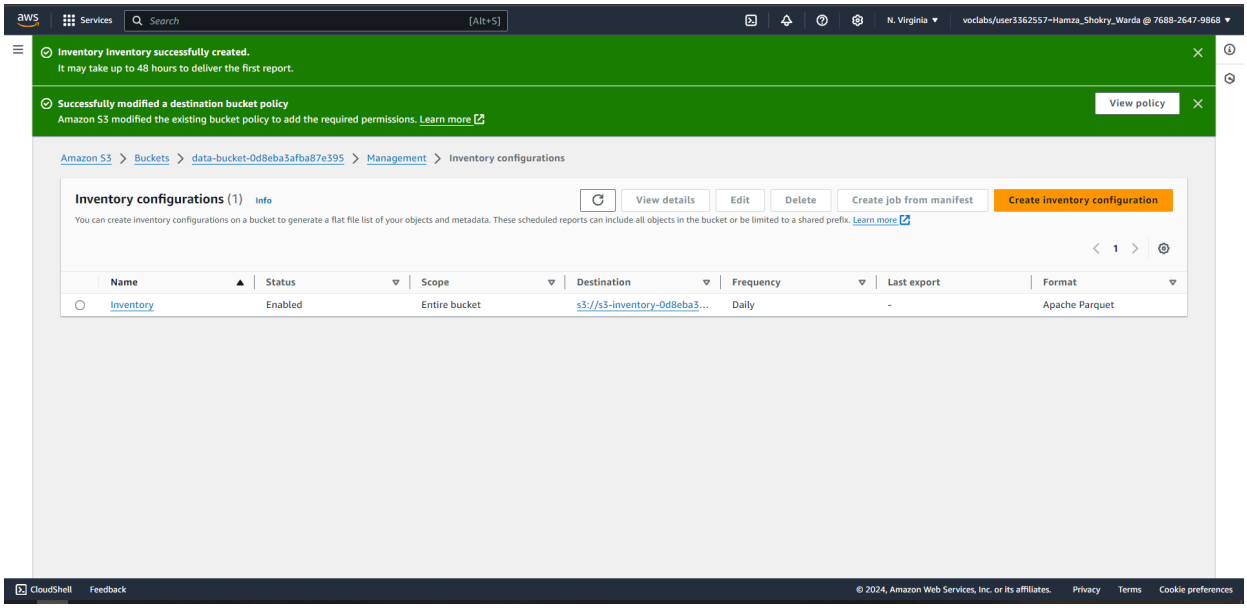
Task 1.2: Enable versioning and object-level logging on a bucket


Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
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 > data-bucket-0d8eba3afba87e395
data-bucket-0d8eba3afba87e395 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-0d8eba3afba87e395
Creation date
September 24, 2024, 19:07:35 (UTC+03:00)
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

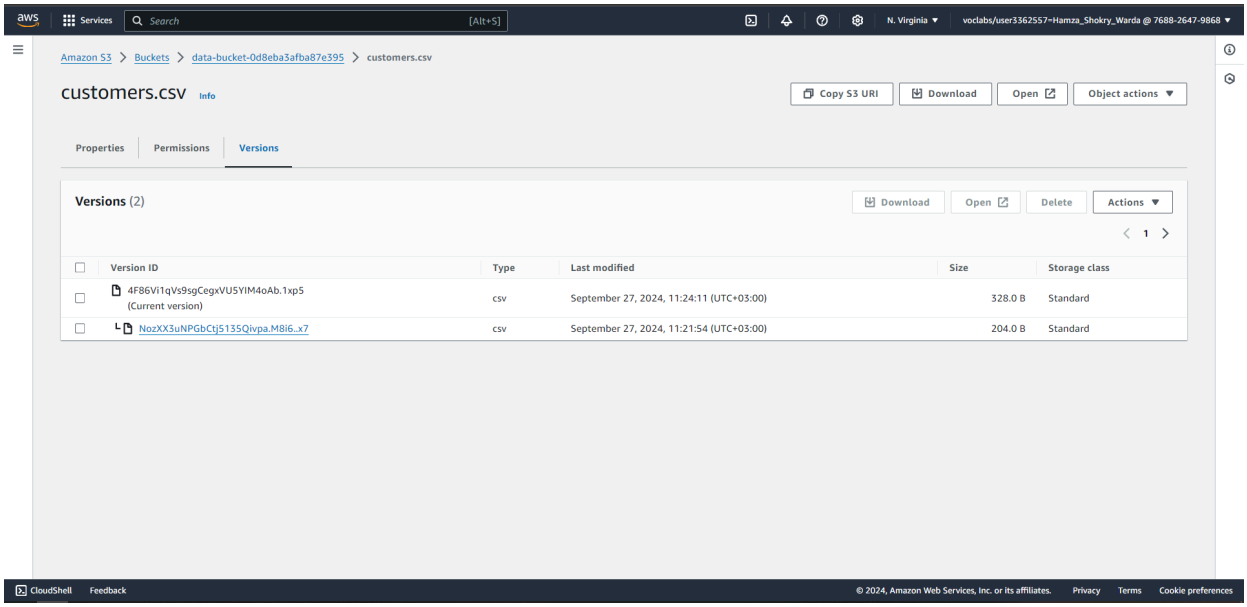

Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Name
Status
Scope
Days until transition to Archive ...
Days until transition to Deep A...
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-0d8eba3afba87e395
AWS CloudTrail data events (1) Info
Configure in CloudTrail
Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. Learn more
Name
Access
data-bucket-reads-writes
Read, Write
Event notifications (0)
Edit
Delete
Create event notification
Send a notification when specific events occur in your bucket. Learn more
Name
Event types
Filters
Destination type
Destination
No event notifications
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



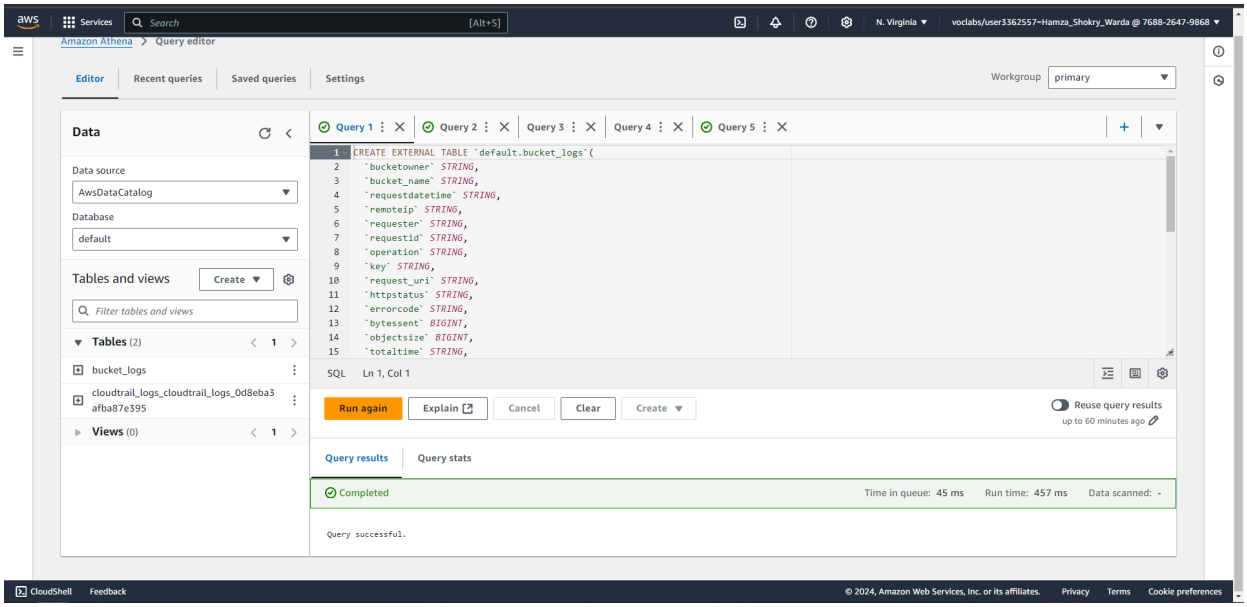
Task 1.3: Implement the S3 Inventory feature on a bucket

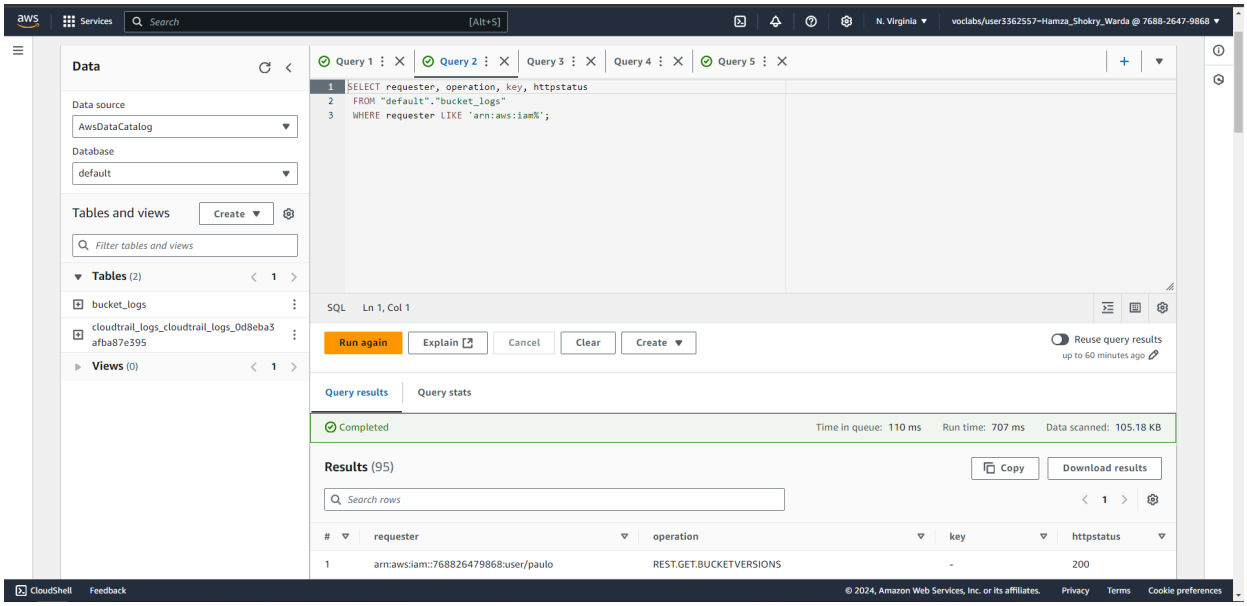


Task 1.4: Confirm that versioning works as intended

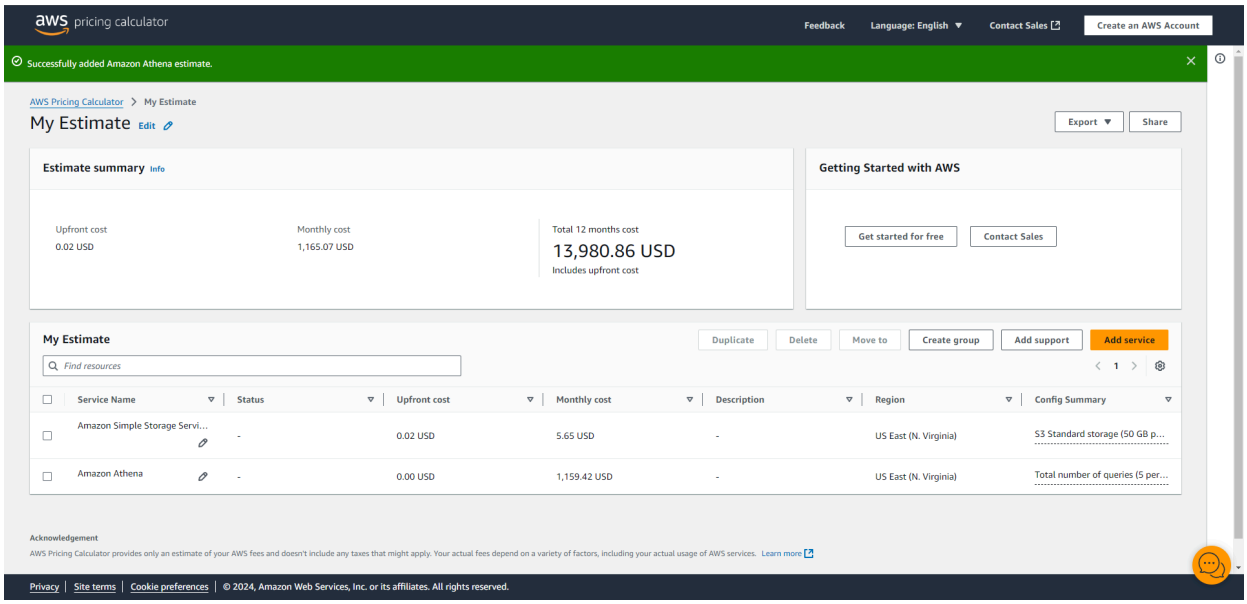


Task 1.5: Confirm object-level logging and query the access logs by using Athena



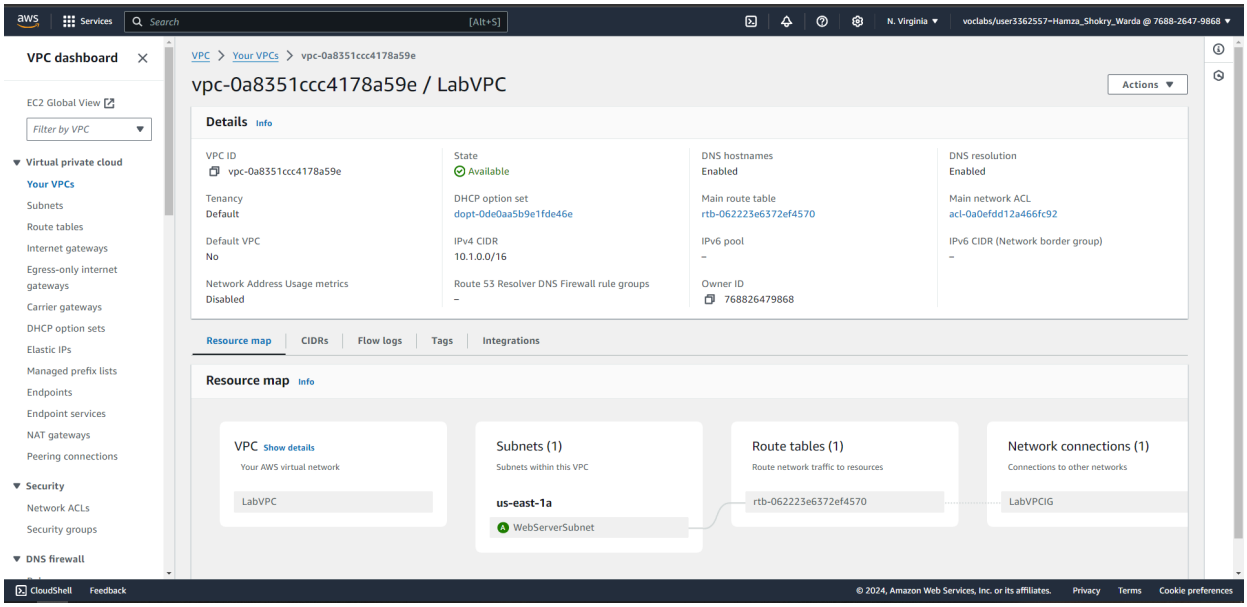


Cost assessment to secure Amazon S3

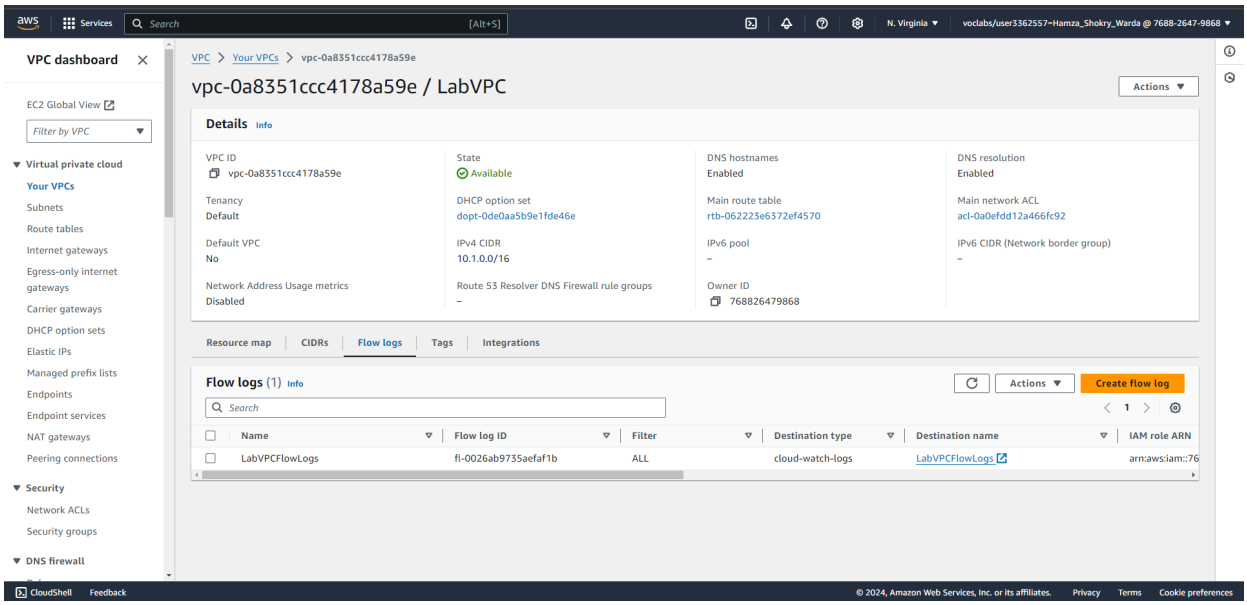


Phase 2: Securing VPCs

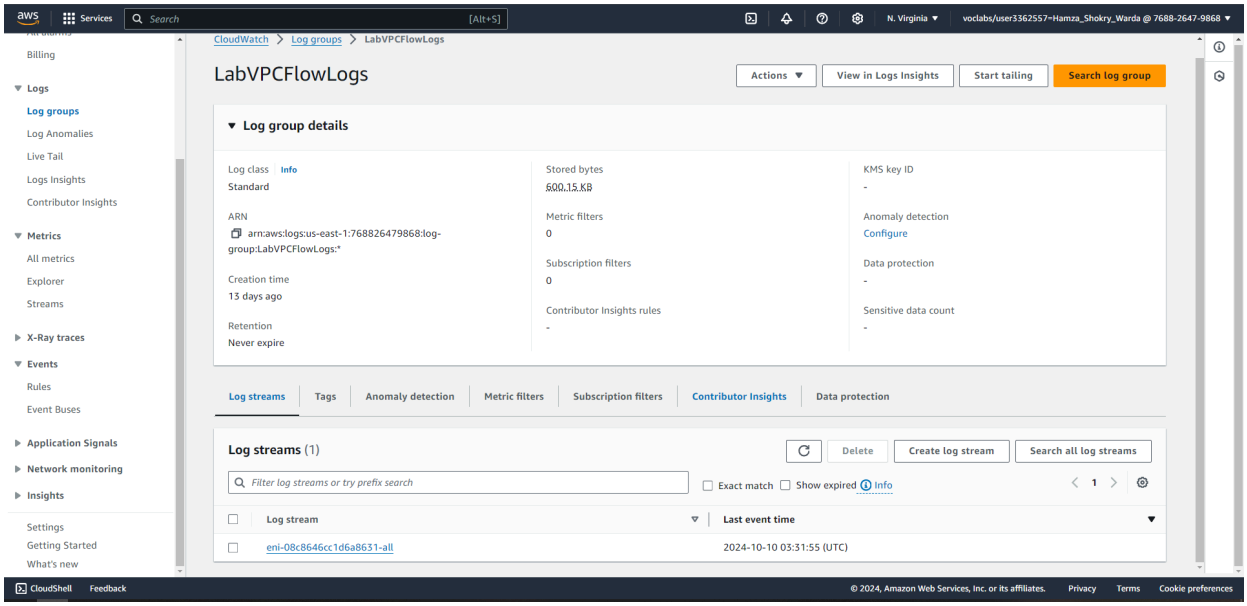
Task 2.1: Review LabVPC and its associated resources

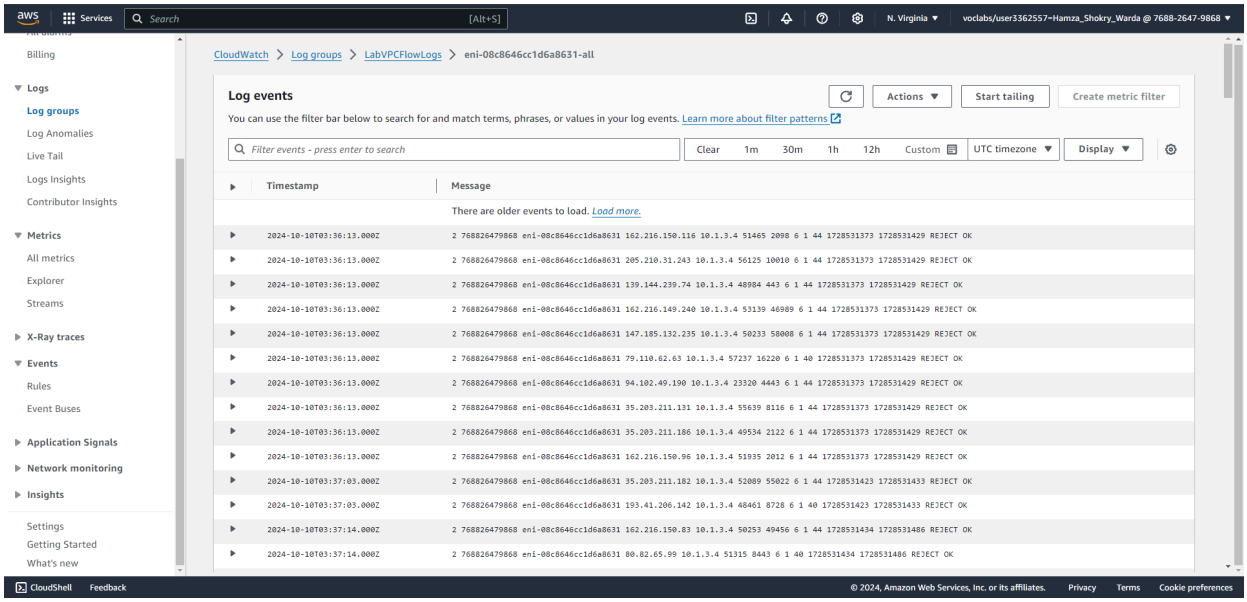


Task 2.2: Create a VPC flow log

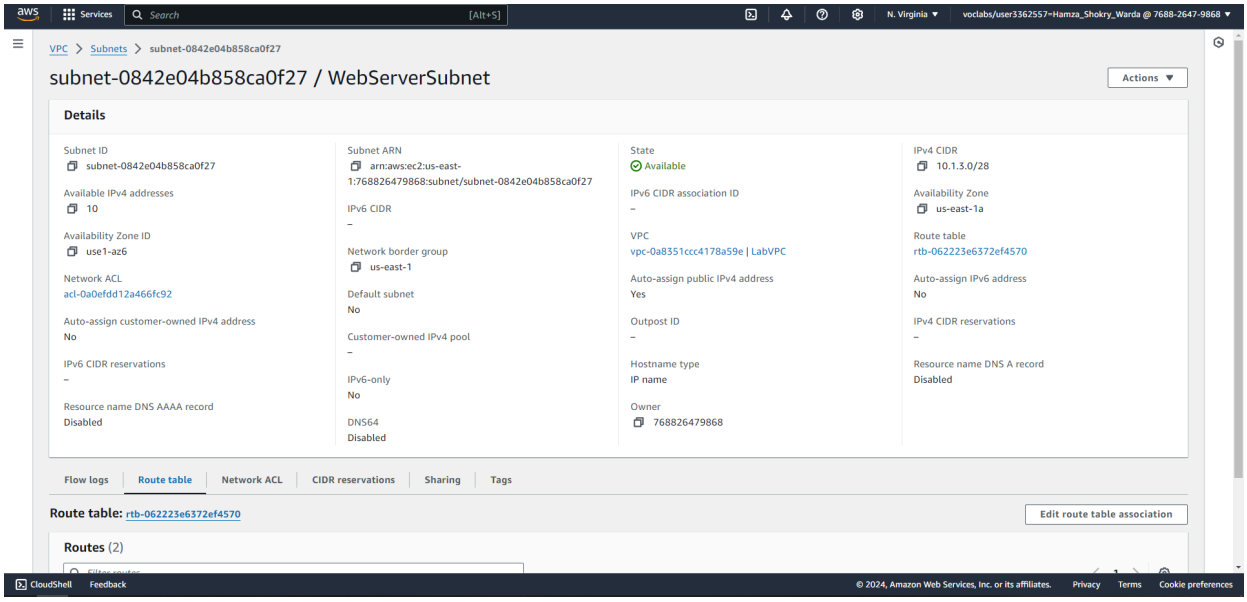


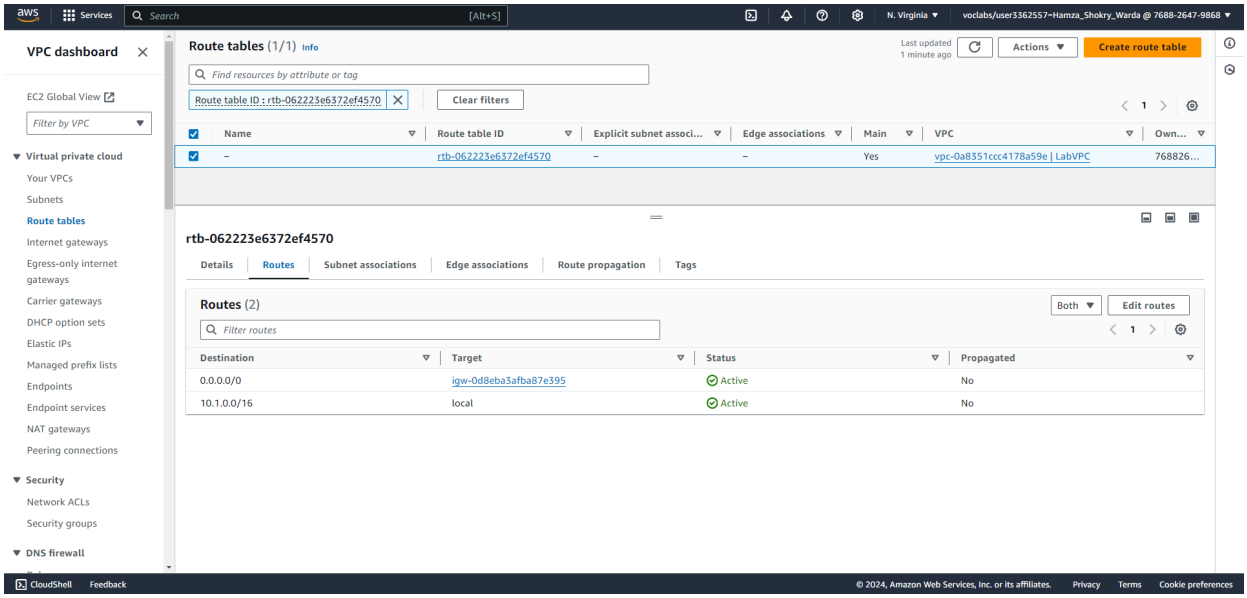
Task 2.3: Access the WebServer instance from the internet and review VPC flow logs in CloudWatch

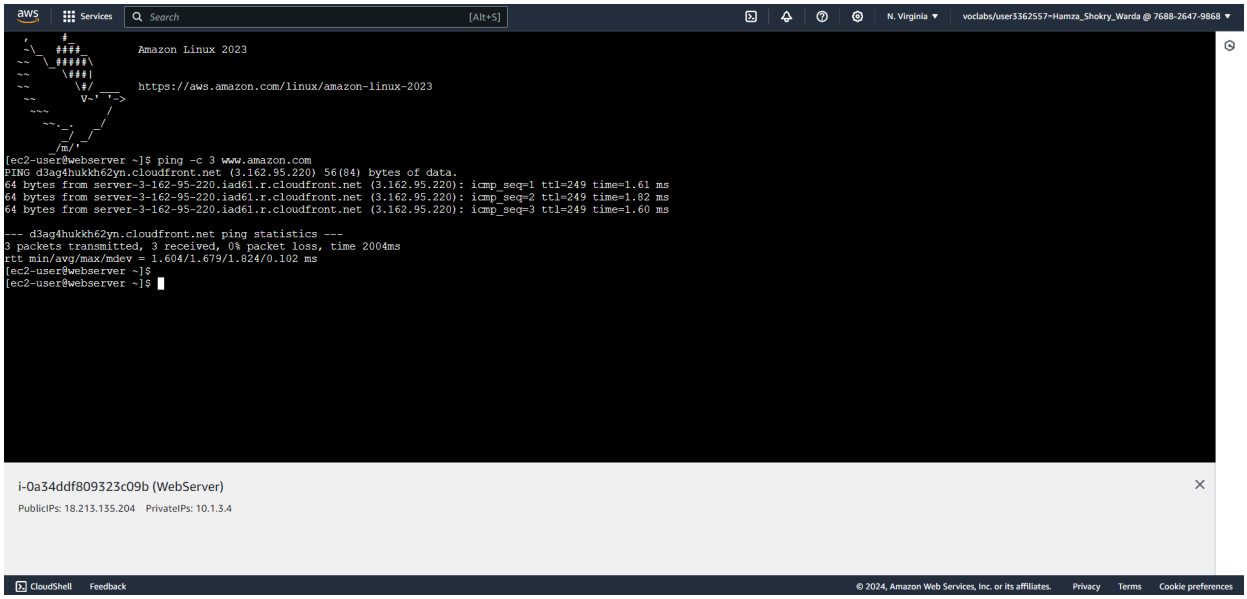




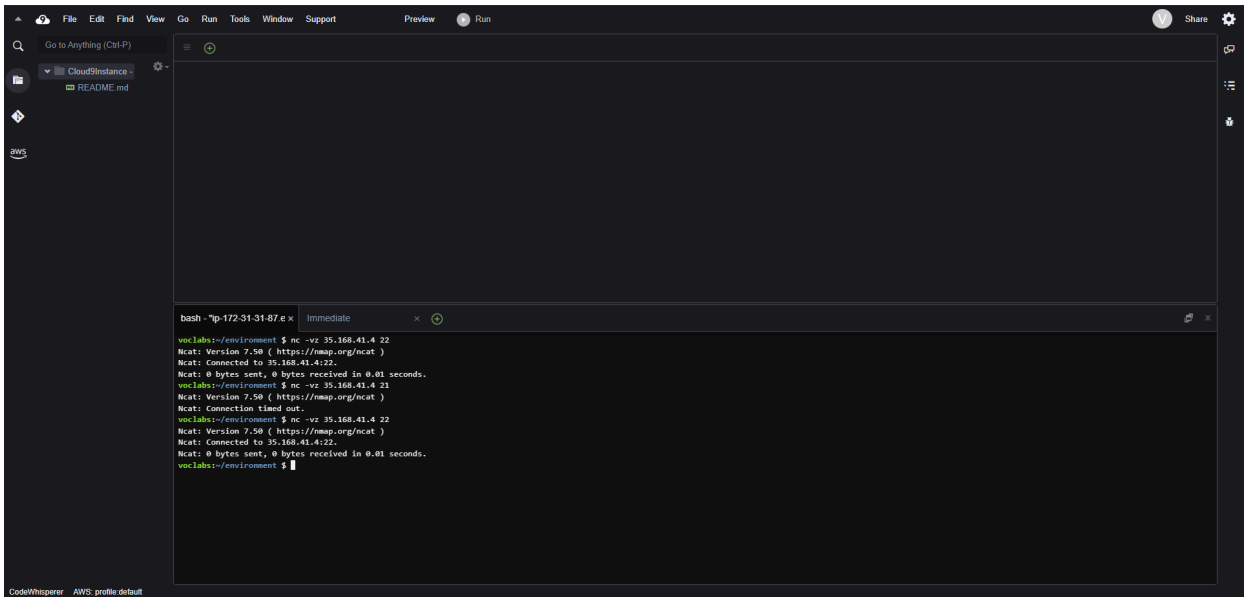
Task 2.4: Configure route table and security group settings

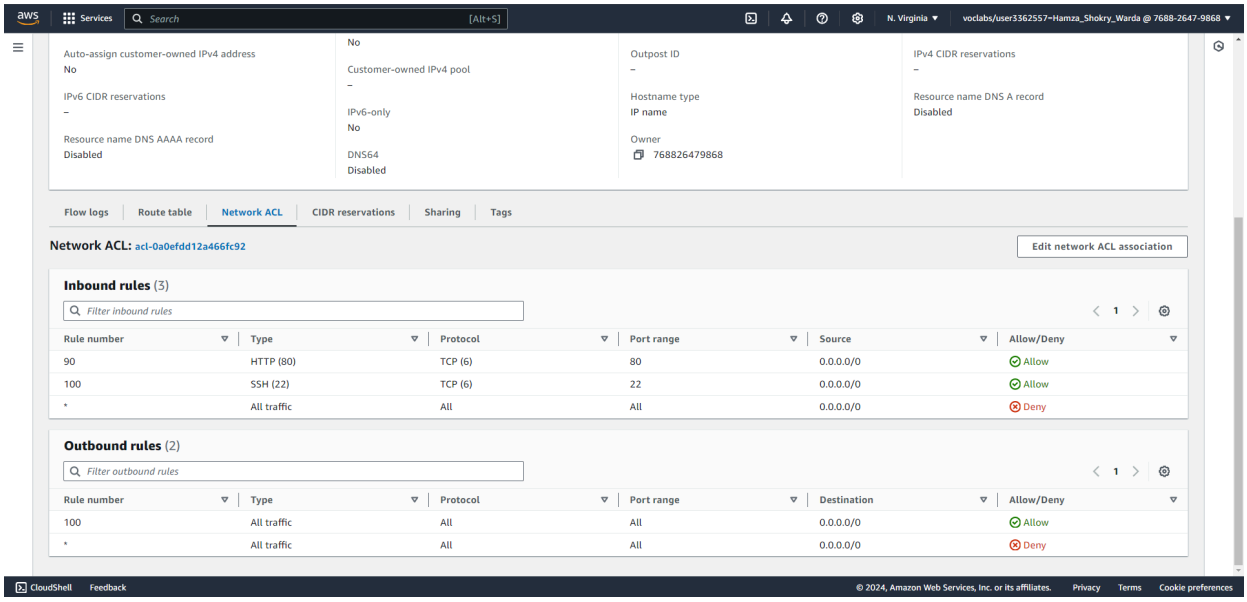

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
VPC > Subnets > subnet-0842e04b858ca0f27
subnet-0842e04b858ca0f27 / WebServerSubnet
Actions
Details
Subnet ID
subnet-0842e04b858ca0f27
Available IPv4 addresses
10
Availability Zone ID
use1-az6
Network ACL
acl-0a0efdd12a466fc92
Auto-assign customer-owned IPv4 address
No
IPv6 CIDR reservations
–
Resource name DNS AAAA record
Disabled
Subnet ARN
arn:aws:ec2:us-east-1:768826479868:subnet/subnet-0842e04b858ca0f27
IPv6 CIDR
–
Network border group
us-east-1
Default subnet
No
Customer-owned IPv4 pool
–
IPv6-only
No
DNS64
Disabled
State
Available
IPv6 CIDR association ID
–
VPC
vpc-0a8351ccc4178a59e | LabVPC
Auto-assign public IPv4 address
Yes
Outpost ID
–
Hostname type
IP name
Owner
768826479868
IPv4 CIDR
10.1.3.0/28
Availability Zone
us-east-1a
Route table
rtb-062223e6372ef4570
Auto-assign IPv6 address
No
IPv4 CIDR reservations
–
Resource name DNS A record
Disabled
Flow logs
Route table
Network ACL
CIDR reservations
Sharing
Tags
Route table: rtb-062223e6372ef4570
Edit route table association
Routes (2)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
VPC dashboard
EC2 Global View
Filter by 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
Route tables (1/1) Info
Last updated 1 minute ago
Actions
Create route table
Find resources by attribute or tag
Route table ID : rtb-062223e6372ef4570
Clear filters
Name
Route table ID
Explicit subnet associ...
Edge associations
Main
VPC
Own...
rtb-062223e6372ef4570
vpc-0a8351ccc4178a59e | LabVPC
768826...
rtb-062223e6372ef4570
Details
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-0d8eba3afba87e395
Active
No
10.1.0.0/16
local
Active
No
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

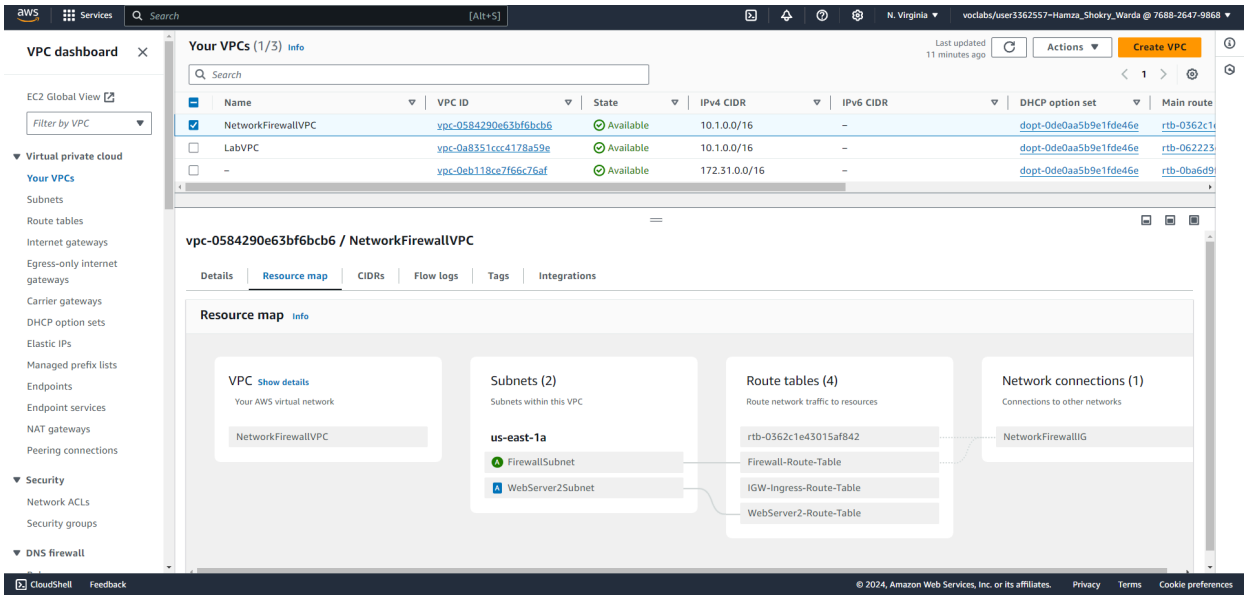


Task 2.5: Secure the WebServerSubnet with a network ACL

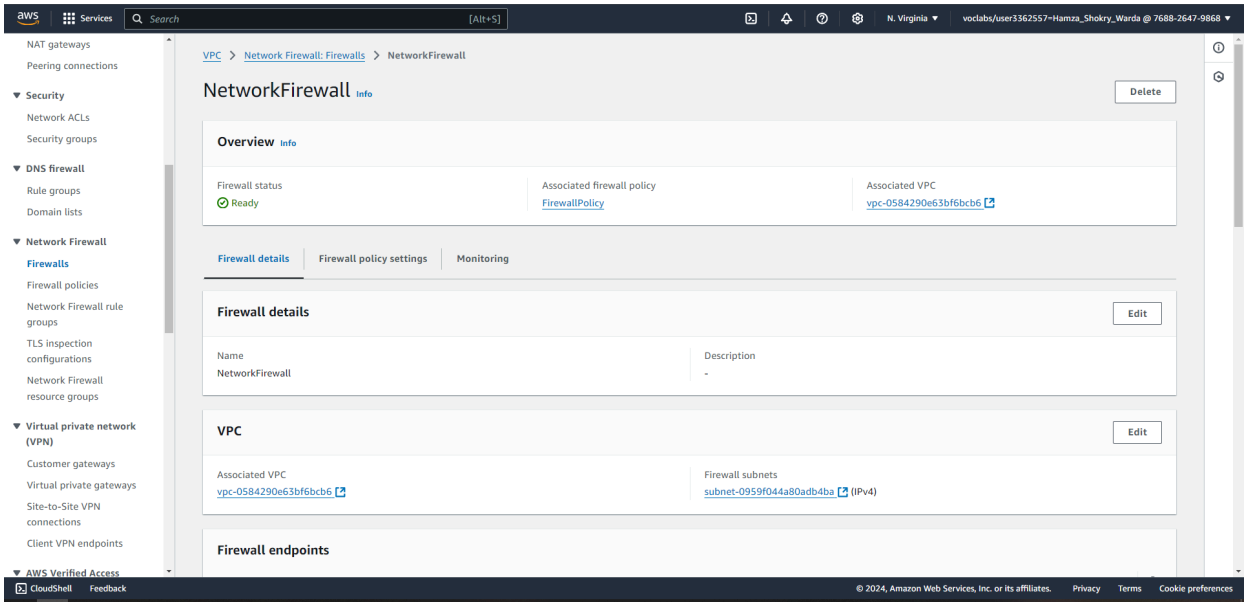




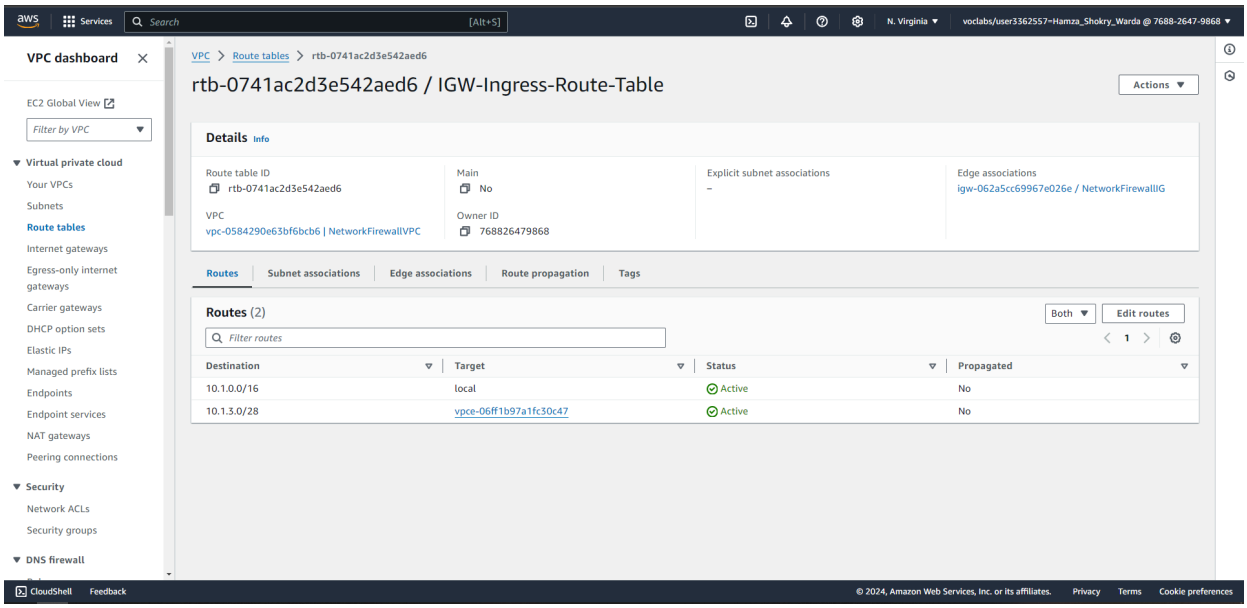
Task 2.6: Review NetworkFirewallVPC and its associated resources

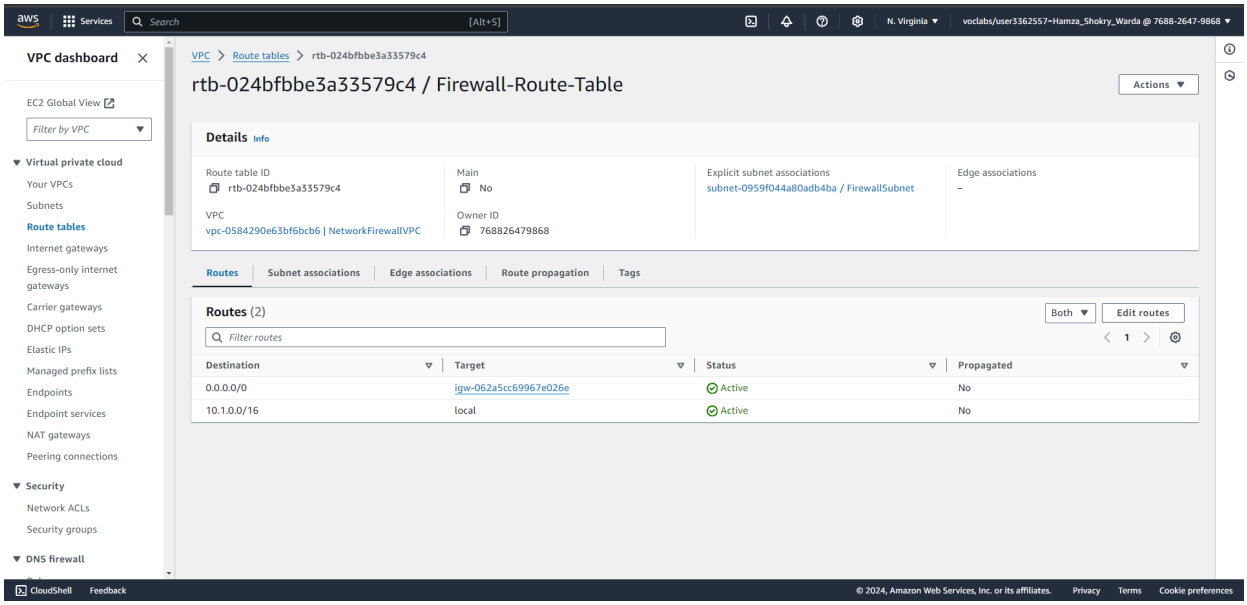


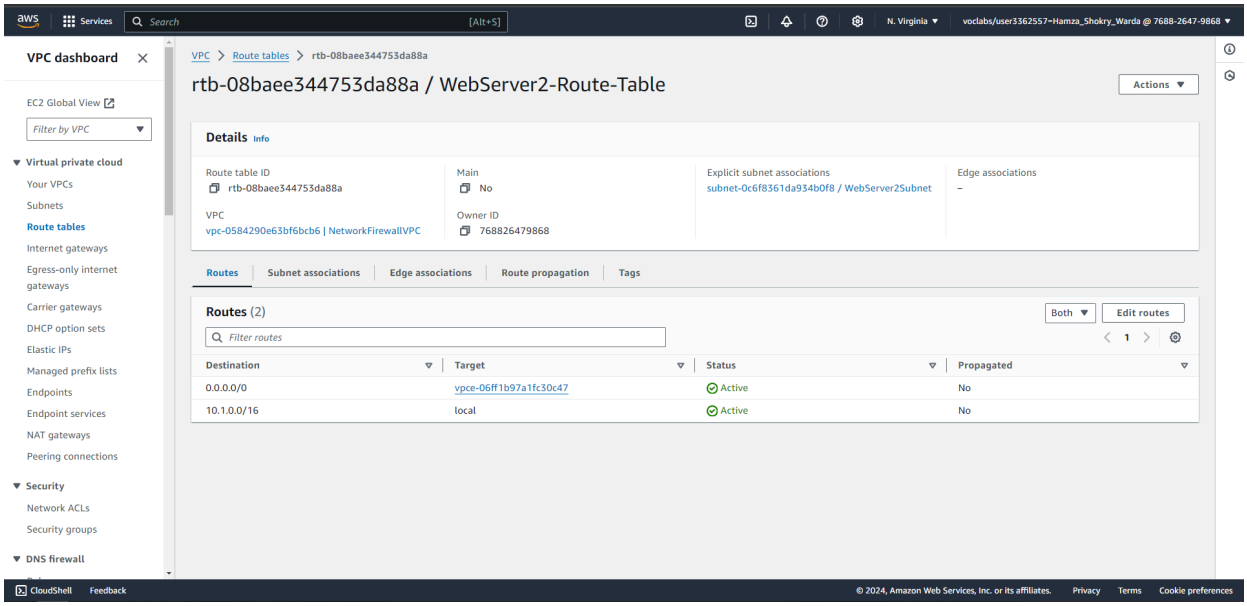
Task 2.7: Create a network firewall



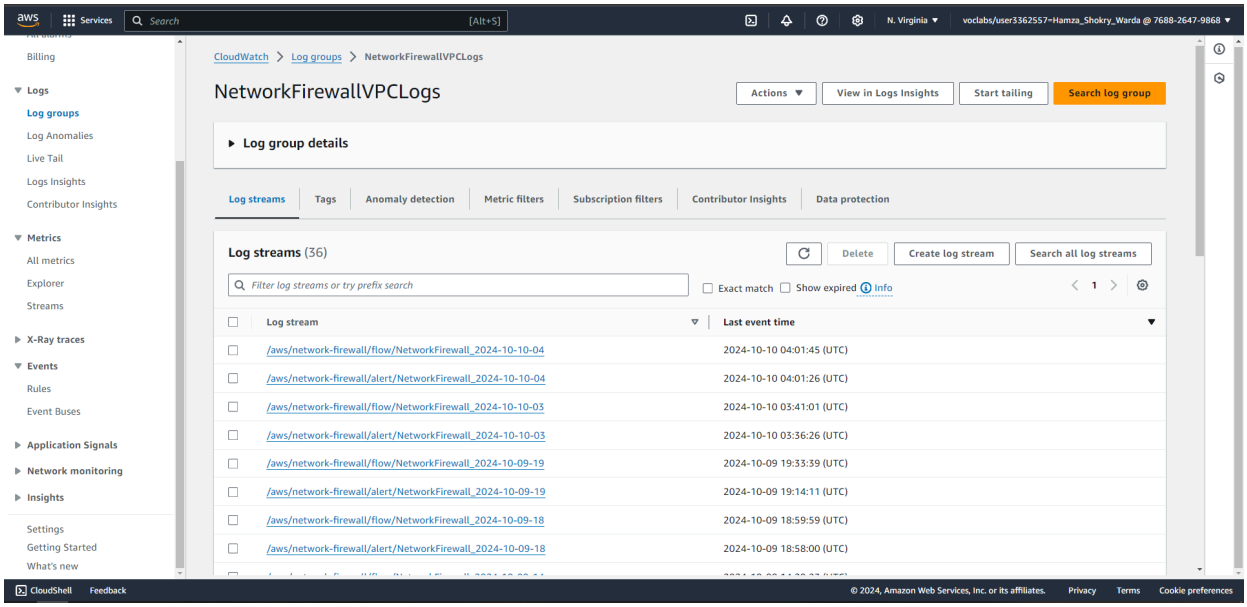
Task 2.8: Create route tables

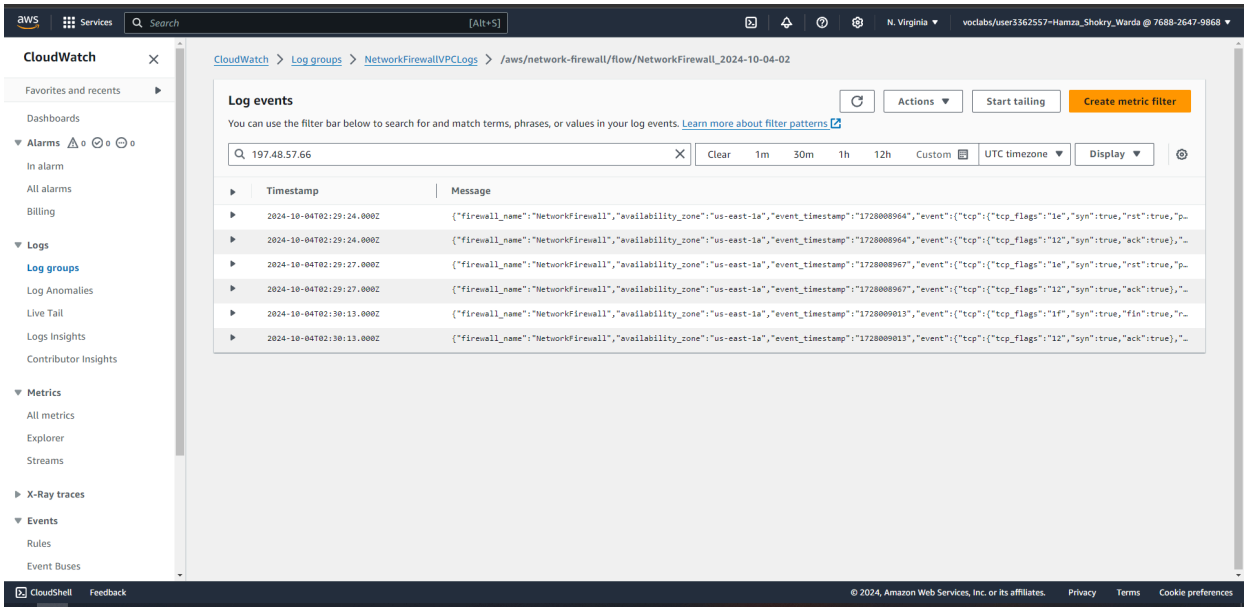




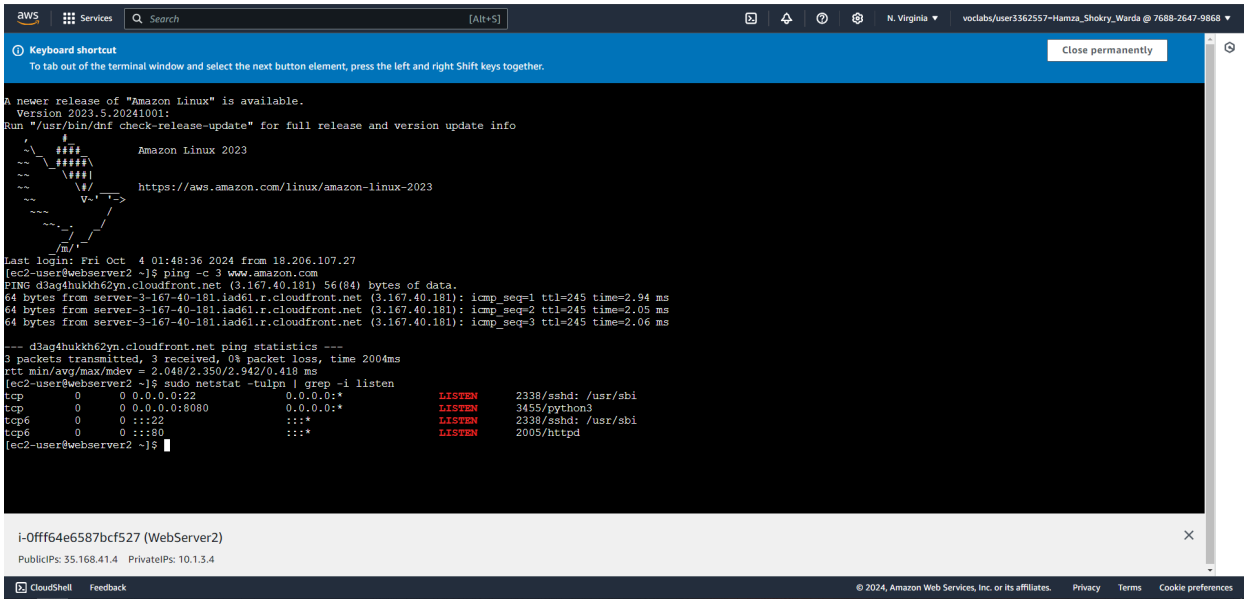


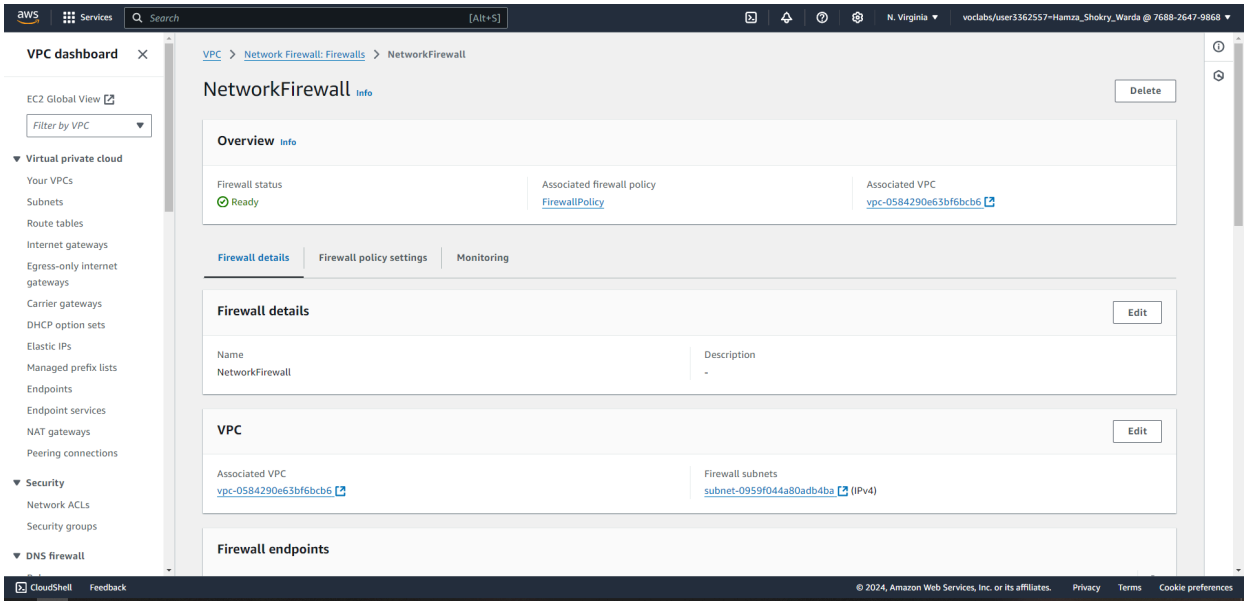
Task 2.9: Configure logging for the network firewall

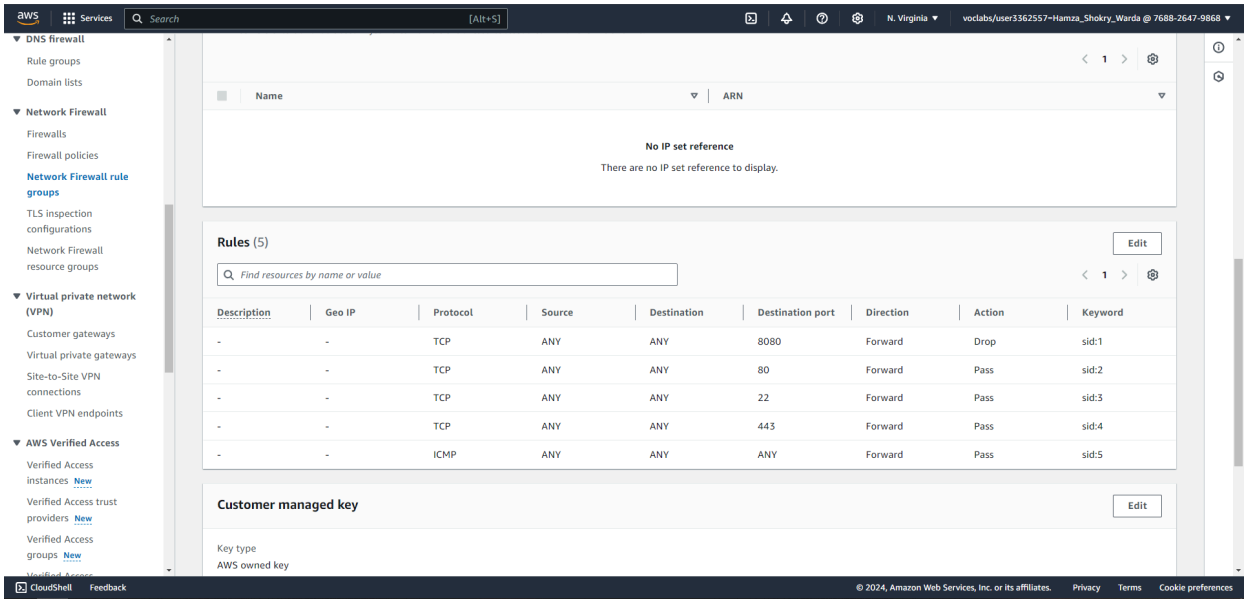


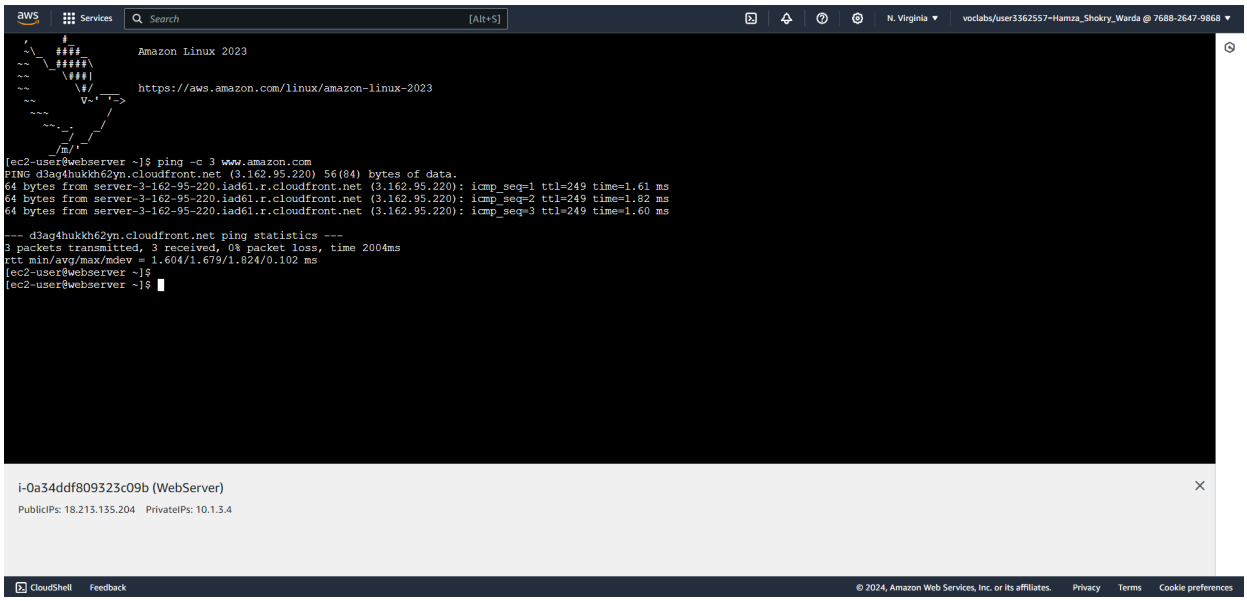


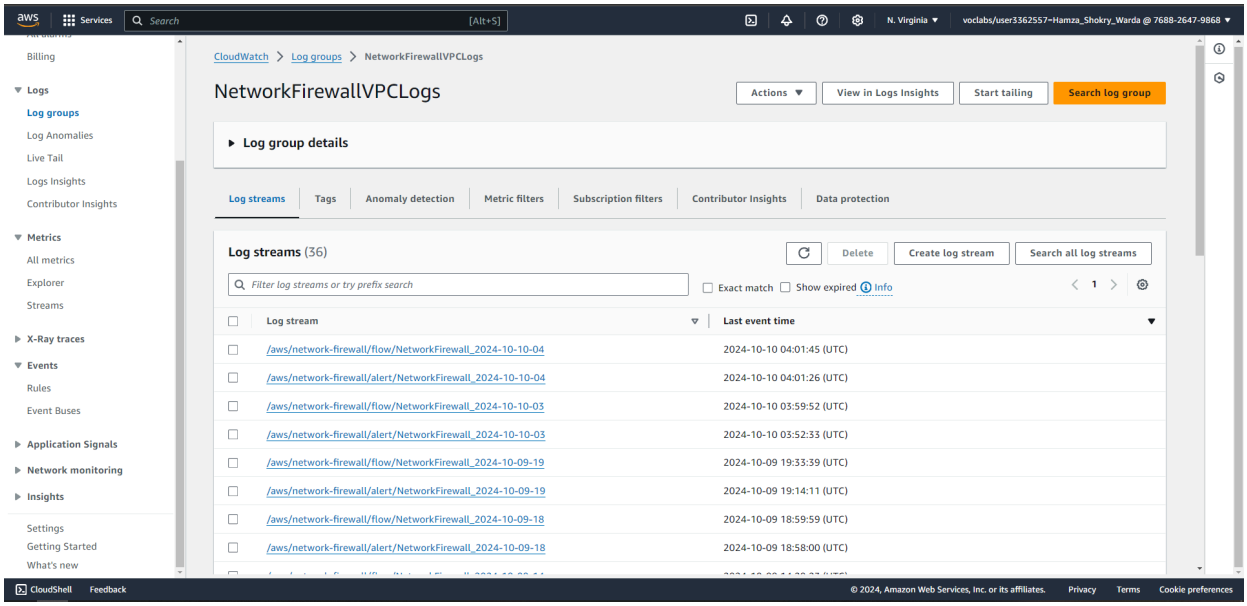
Task 2.10: Configure the firewall policy and test access


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
Keyboard shortcut
To tab out of the terminal window and select the next button element, press the left and right Shift keys together.
Close permanently
A newer release of "Amazon Linux" is available.
Version 2023.5.20241001:
Run "/usr/bin/dnf check-release-update" for full release and version update info
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
Last login: Fri Oct 4 01:48:36 2024 from 18.206.107.27
[ec2-user@webserver2 ~]$ ping -c 3 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (3.167.40.181) 56(84) bytes of data.
64 bytes from server-3-167-40-181.iad61.r.cloudfront.net (3.167.40.181): icmp_seq=1 ttl=245 time=2.94 ms
64 bytes from server-3-167-40-181.iad61.r.cloudfront.net (3.167.40.181): icmp_seq=2 ttl=245 time=2.05 ms
64 bytes from server-3-167-40-181.iad61.r.cloudfront.net (3.167.40.181): icmp_seq=3 ttl=245 time=2.06 ms
--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 2.048/2.350/2.942/0.418 ms
[ec2-user@webserver2 ~]$ sudo netstat -tulpn | grep -i listen
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 2338/sshd: /usr/sbi
tcp 0 0 0.0.0.0:8080 0.0.0.0:* LISTEN 3455/python3
tcp6 0 0 :::22 :::* LISTEN 2338/sshd: /usr/sbi
tcp6 0 0 :::80 :::* LISTEN 2005/httpd
[ec2-user@webserver2 ~]$
i-0fff64e6587bcf527 (WebServer2)
PublicIPs: 35.168.41.4 PrivateIPs: 10.1.3.4
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

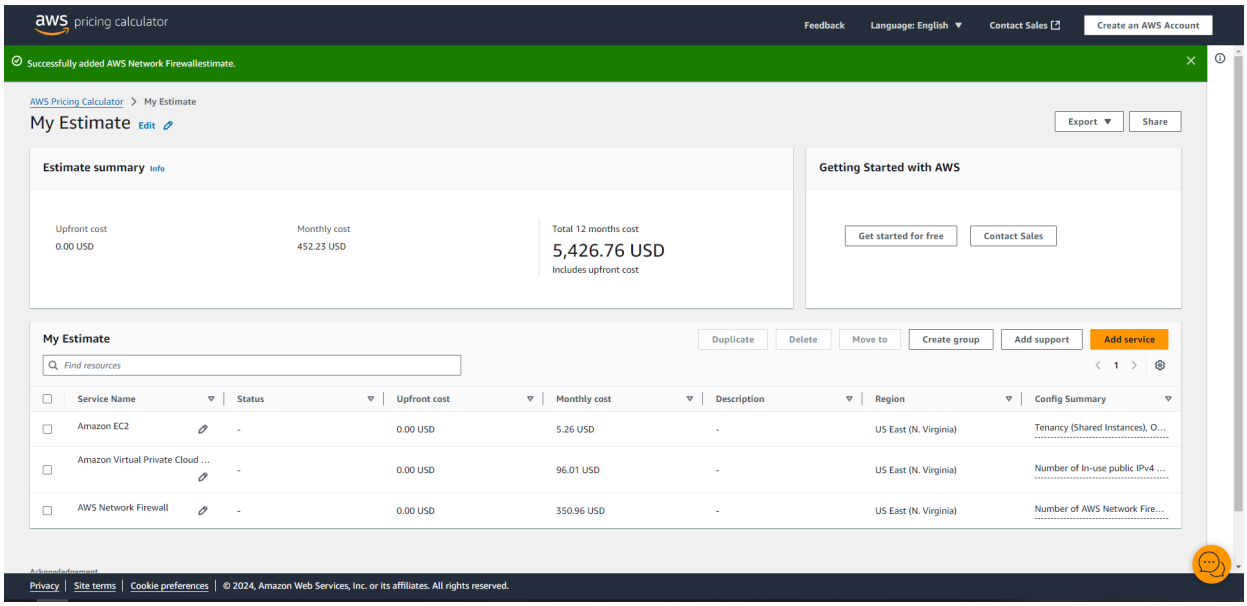

aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
VPC > Network Firewall: Firewalls > NetworkFirewall
NetworkFirewall Info
Delete
Overview Info
Firewall status
Ready
Associated firewall policy
FirewallPolicy
Associated VPC
vpc-0584290e63bf6bcb6
Firewall details
Firewall policy settings
Monitoring
Firewall details
Edit
Name
NetworkFirewall
Description
-
VPC
Edit
Associated VPC
vpc-0584290e63bf6bcb6
Firewall subnets
subnet-0959f044a80adb4ba (IPv4)
Firewall endpoints
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
Firewall policies
Network Firewall rule groups
TLS inspection configurations
Network Firewall resource groups
Virtual private network (VPN)
Customer gateways
Virtual private gateways
Site-to-Site VPN connections
Client VPN endpoints
AWS Verified Access
Verified Access instances New
Verified Access trust providers New
Verified Access groups New
Name
ARN
No IP set reference
There are no IP set reference to display.
Rules (5)
Edit
Find resources by name or value
Description
Geo IP
Protocol
Source
Destination
Destination port
Direction
Action
Keyword
- - TCP ANY ANY 8080 Forward Drop sid:1
- - TCP ANY ANY 80 Forward Pass sid:2
- - TCP ANY ANY 22 Forward Pass sid:3
- - TCP ANY ANY 443 Forward Pass sid:4
- - ICMP ANY ANY ANY Forward Pass sid:5
Customer managed key
Edit
Key type
AWS owned key
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
Amazon Linux 2023
https://aws.amazon.com/linux/amazon-linux-2023
[ec2-user@webserver ~]$ ping -c 3 www.amazon.com
PING d3ag4hukkh62yn.cloudfront.net (3.162.95.220) 56(84) bytes of data.
64 bytes from server-3-162-95-220.iad61.r.cloudfront.net (3.162.95.220): icmp_seq=1 ttl=249 time=1.61 ms
64 bytes from server-3-162-95-220.iad61.r.cloudfront.net (3.162.95.220): icmp_seq=2 ttl=249 time=1.82 ms
64 bytes from server-3-162-95-220.iad61.r.cloudfront.net (3.162.95.220): icmp_seq=3 ttl=249 time=1.60 ms
--- d3ag4hukkh62yn.cloudfront.net ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.604/1.679/1.824/0.102 ms
[ec2-user@webserver ~]$
[ec2-user@webserver ~]$
i-0a34ddf809323c09b (WebServer)
PublicIPs: 18.213.135.204 PrivateIPs: 10.1.3.4
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

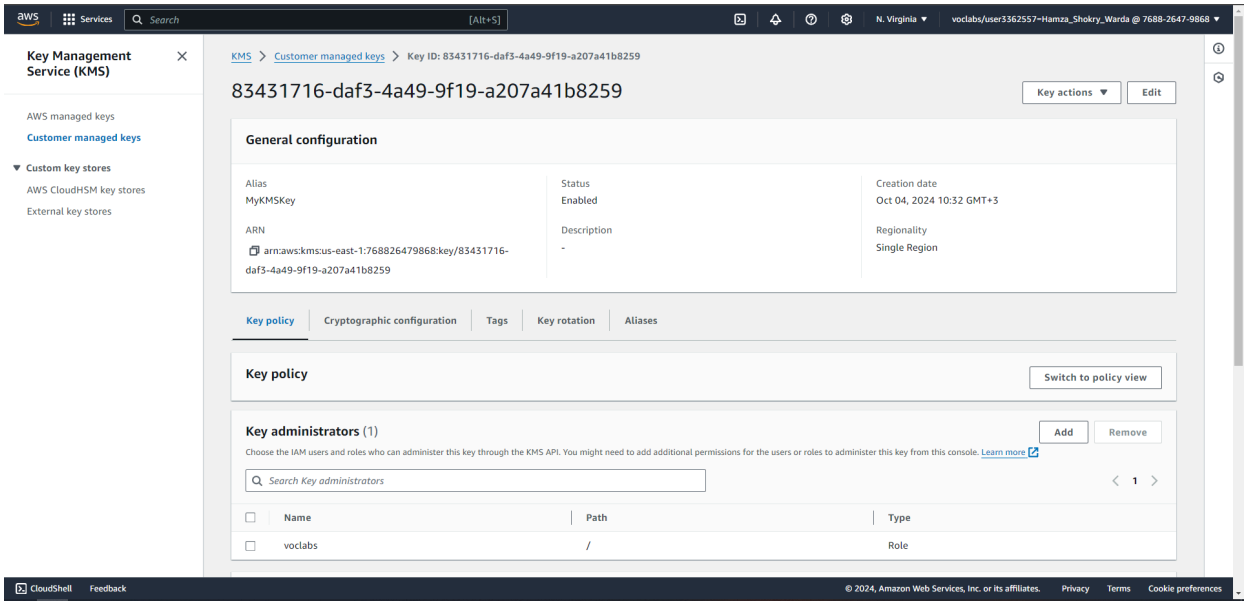


Cost estimate to secure a VPC with a network firewall

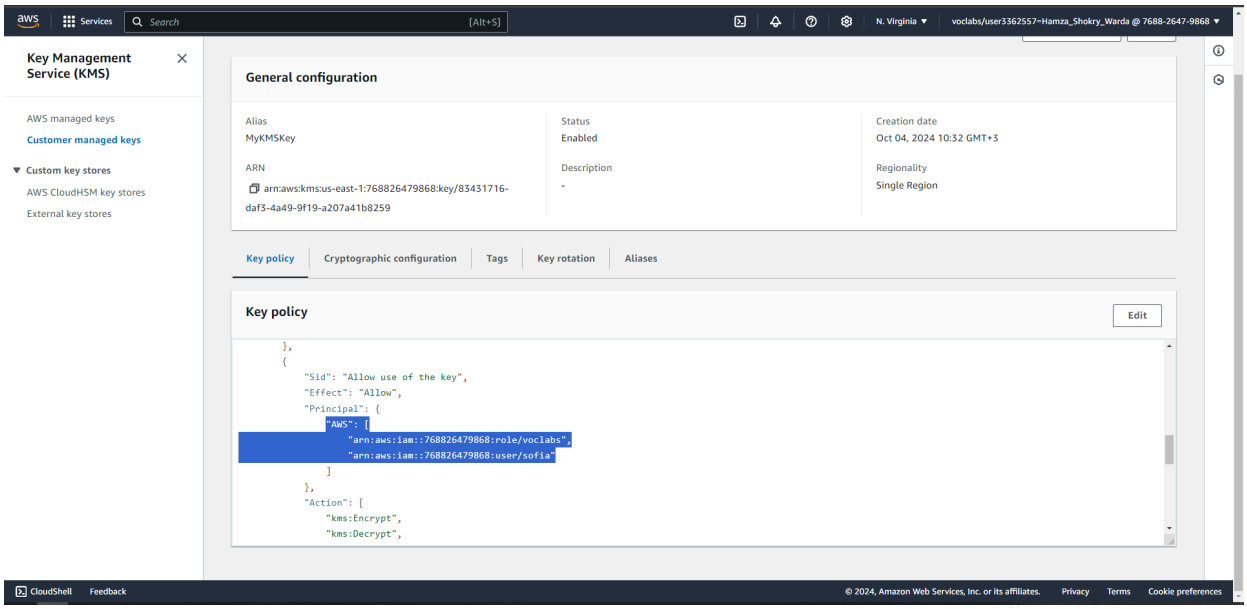


Phase 3: Securing AWS resources by using AWS KMS

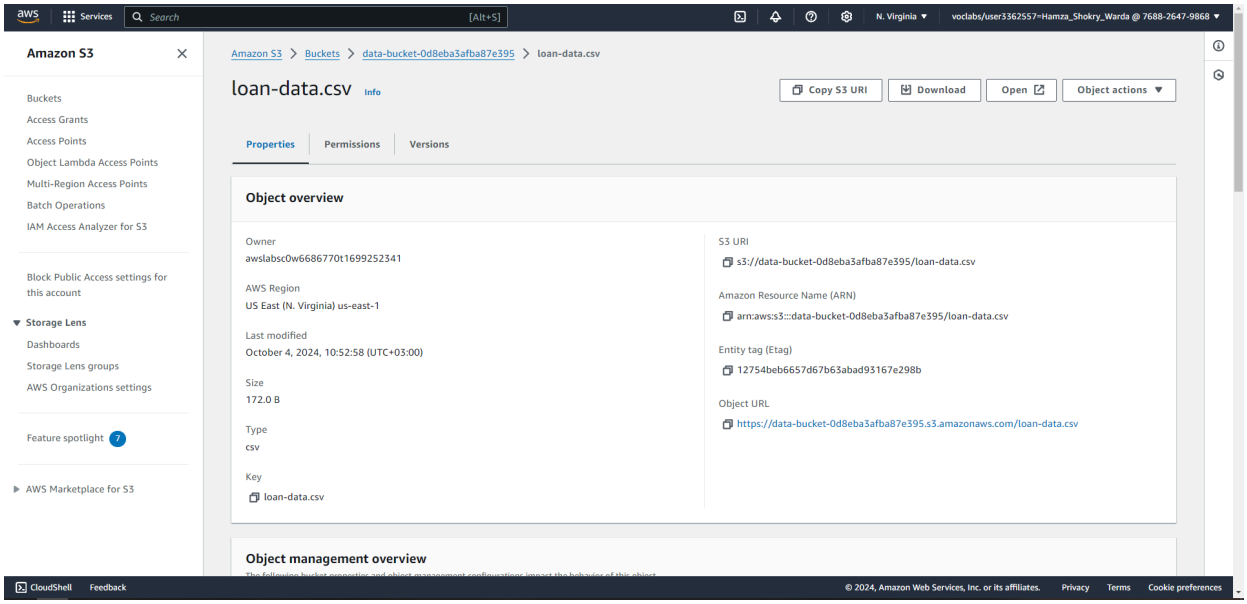
Task 3.1: Create a customer managed key and configure key rotation

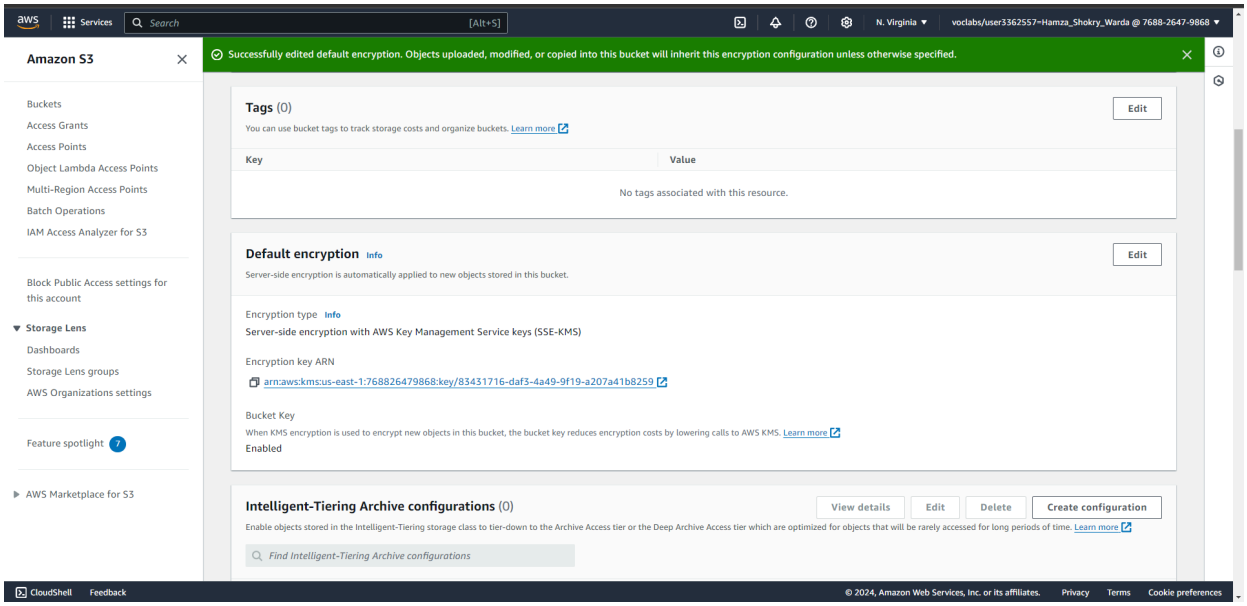


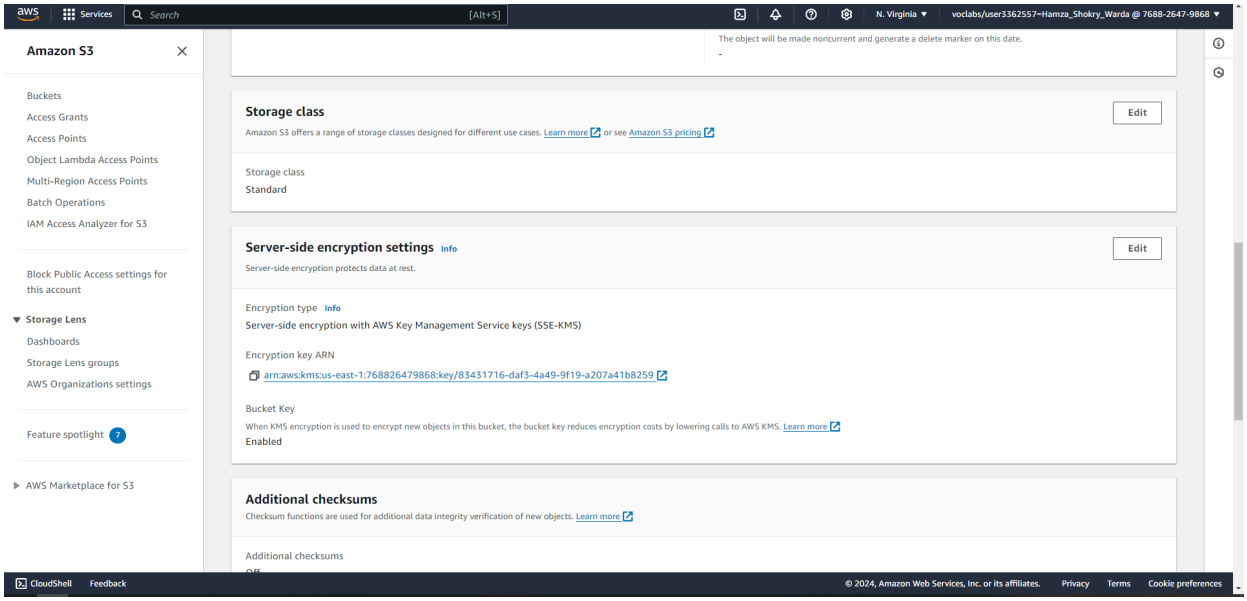
Task 3.2: Update the AWS KMS key policy and analyze an IAM policy



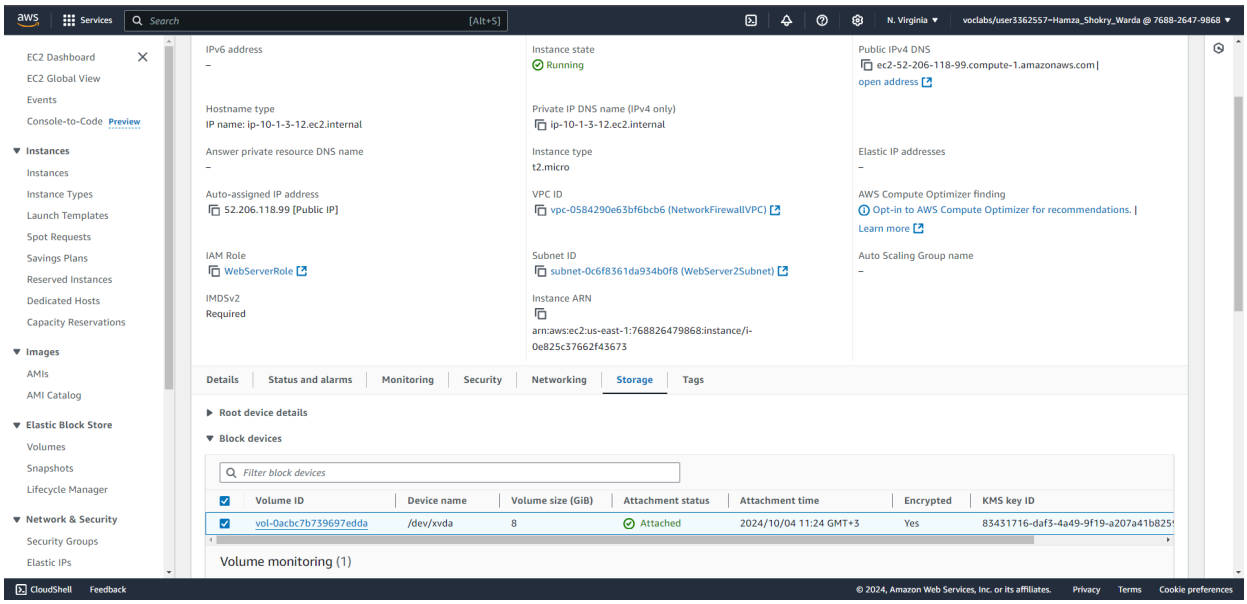
Task 3.3: Use AWS KMS to encrypt data in Amazon S3


Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
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 > data-bucket-0d8eba3afba87e395 > loan-data.csv
loan-data.csv Info
Copy S3 URI
Download
Open
Object actions
Properties
Permissions
Versions
Object overview
Owner
awslabsc0w6686770t1699252341
AWS Region
US East (N. Virginia) us-east-1
Last modified
October 4, 2024, 10:52:58 (UTC+03:00)
Size
172.0 B
Type
csv
Key
loan-data.csv
S3 URI
s3://data-bucket-0d8eba3afba87e395/loan-data.csv
Amazon Resource Name (ARN)
arn:aws:s3:::data-bucket-0d8eba3afba87e395/loan-data.csv
Entity tag (Etag)
12754beb6657d67b63abad93167e298b
Object URL
https://data-bucket-0d8eba3afba87e395.s3.amazonaws.com/loan-data.csv
Object management overview
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

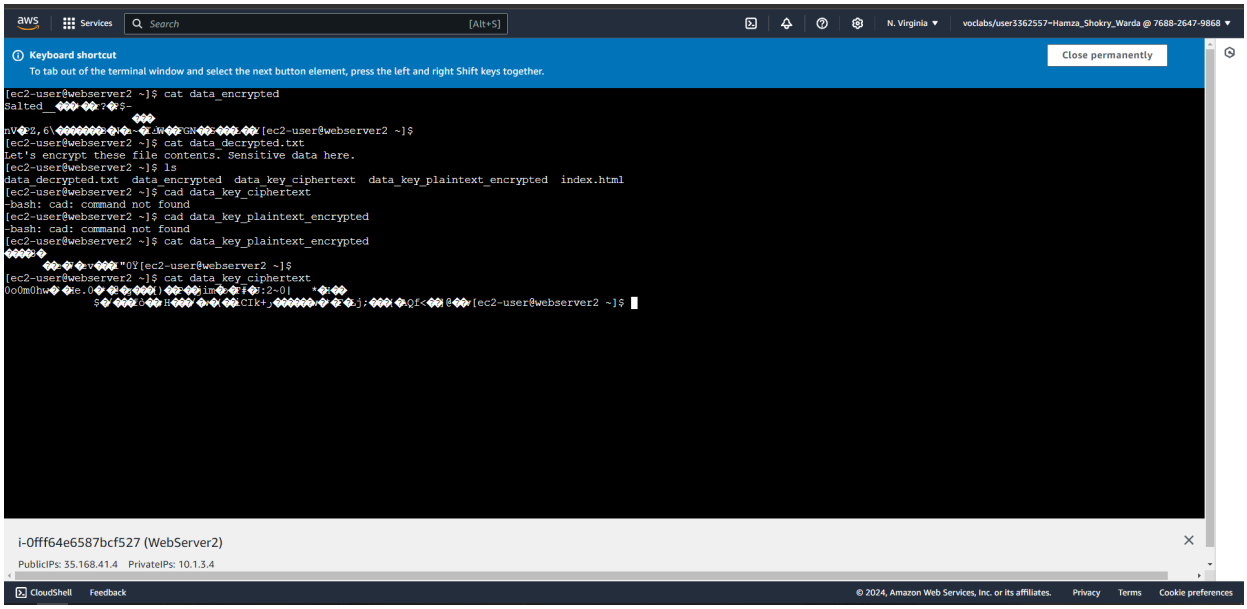

Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
Amazon S3
Successfully edited default encryption. Objects uploaded, modified, or copied into this bucket will inherit this encryption configuration unless otherwise specified.
Buckets
Access Grants
Access Points
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
Tags (0)
Edit
You can use bucket tags to track storage costs and organize buckets. Learn more
Key
Value
No tags associated with this resource.
Default encryption Info
Edit
Server-side encryption is automatically applied to new objects stored in this bucket.
Encryption type Info
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Encryption key ARN
arn:aws:kms:us-east-1:768826479868:key/83431716-daf3-4a49-9f19-a207a41b8259
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
Intelligent-Tiering Archive configurations (0)
View details
Edit
Delete
Create configuration
Enable objects stored in the Intelligent-Tiering storage class to tier-down to the Archive Access tier or the Deep Archive Access tier which are optimized for objects that will be rarely accessed for long periods of time. Learn more
Find Intelligent-Tiering Archive configurations
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



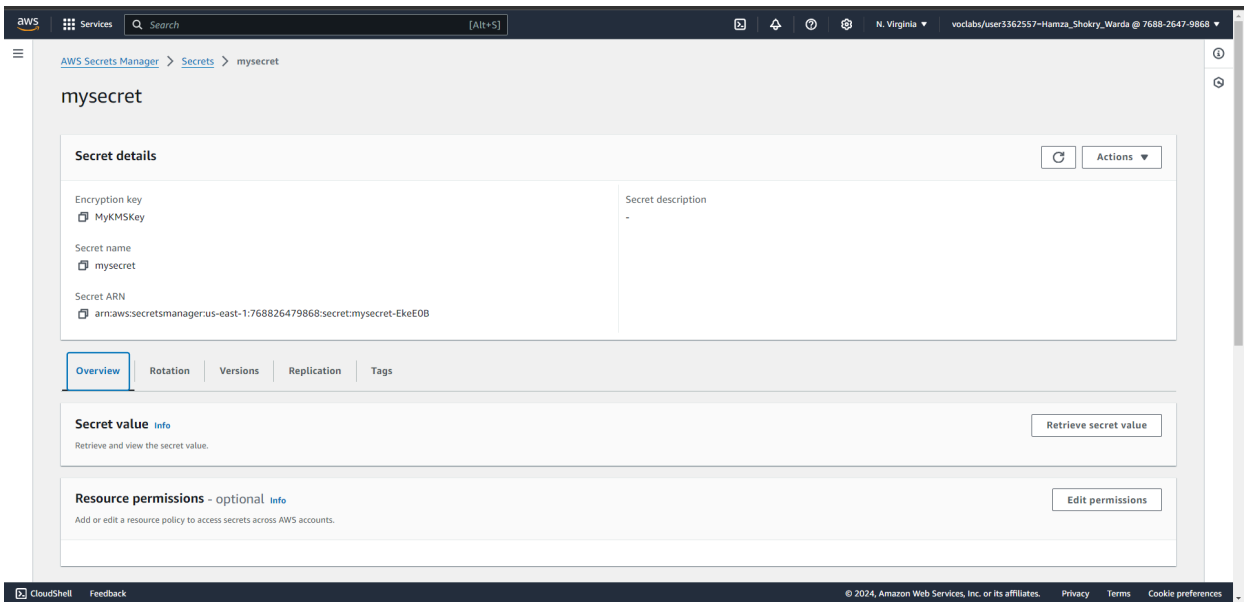
Task 3.4: Use AWS KMS to encrypt the root volume of an EC2 instance

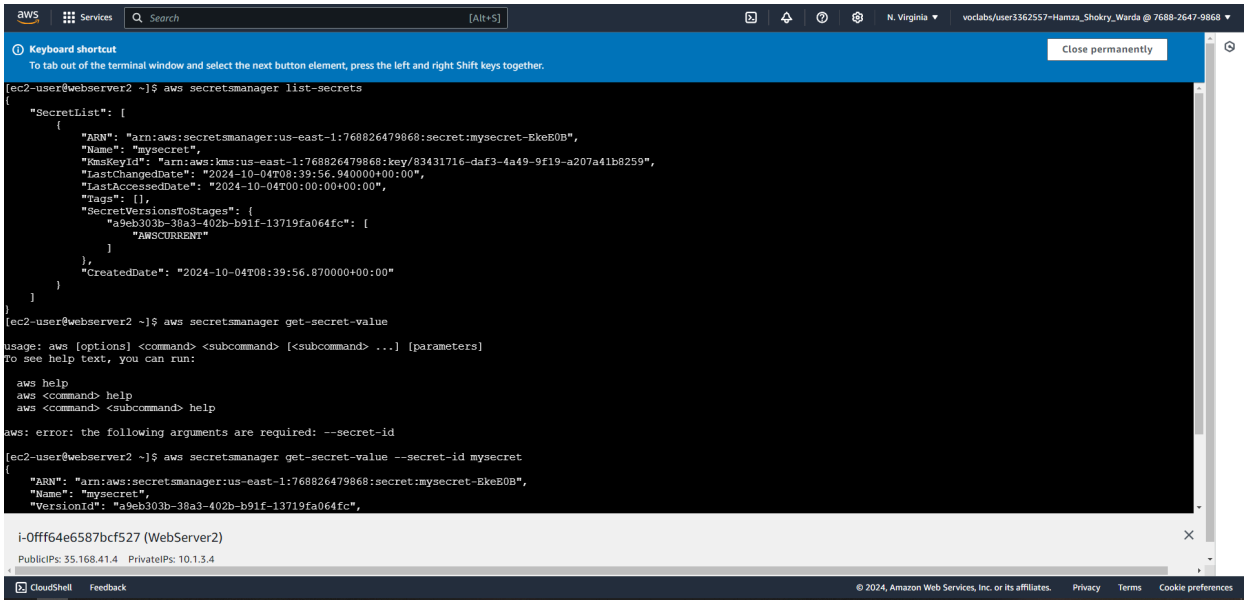


Task 3.5: Use AWS KMS envelope encryption to encrypt data in place

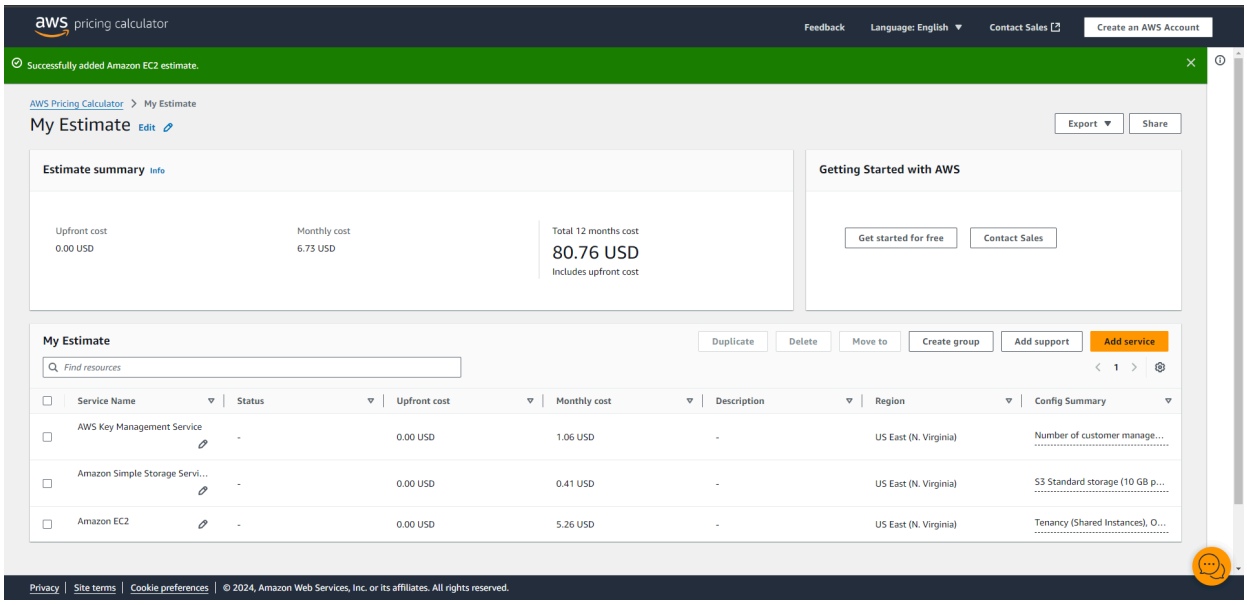


Task 3.6: Use AWS KMS to encrypt a Secrets Manager secret



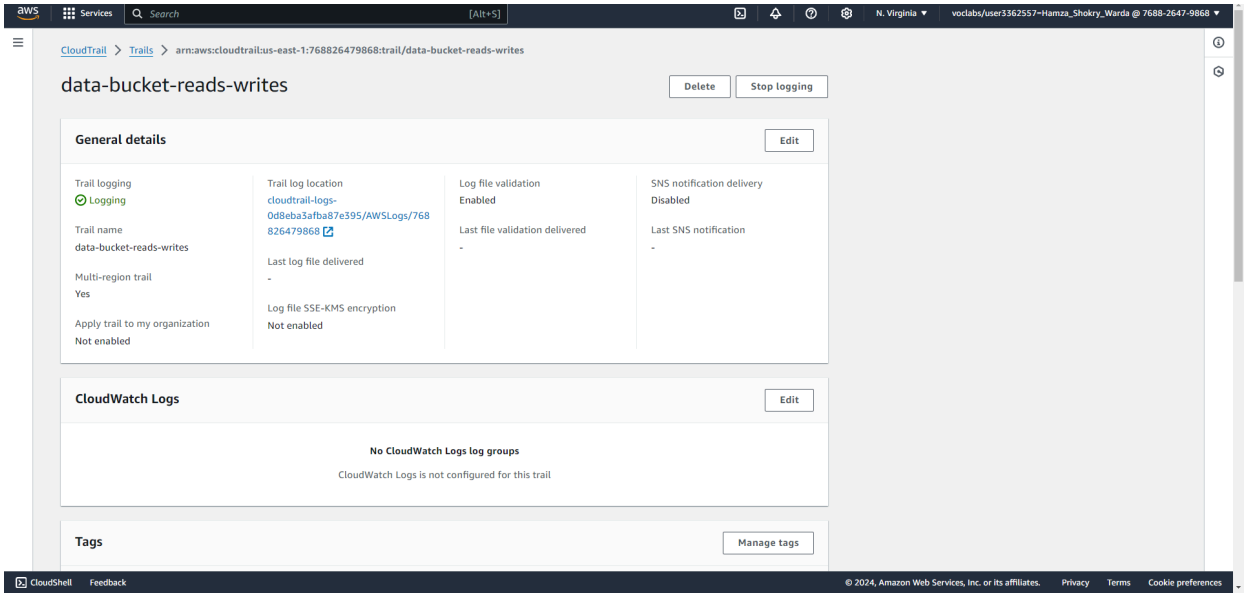


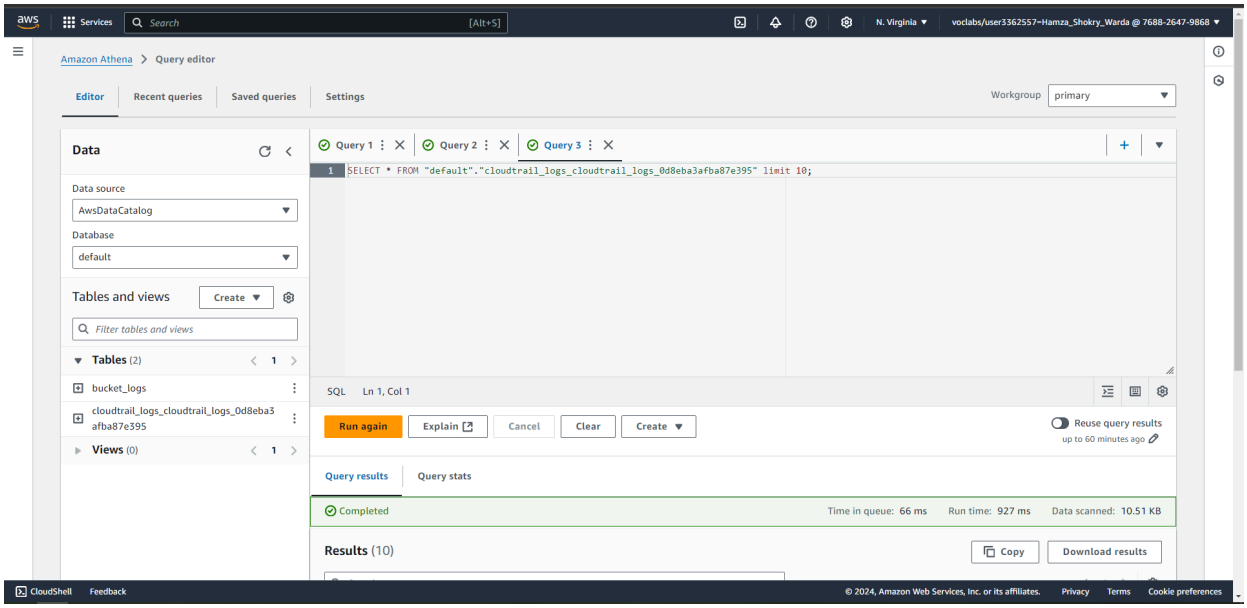
Cost assessment for using AWS KMS

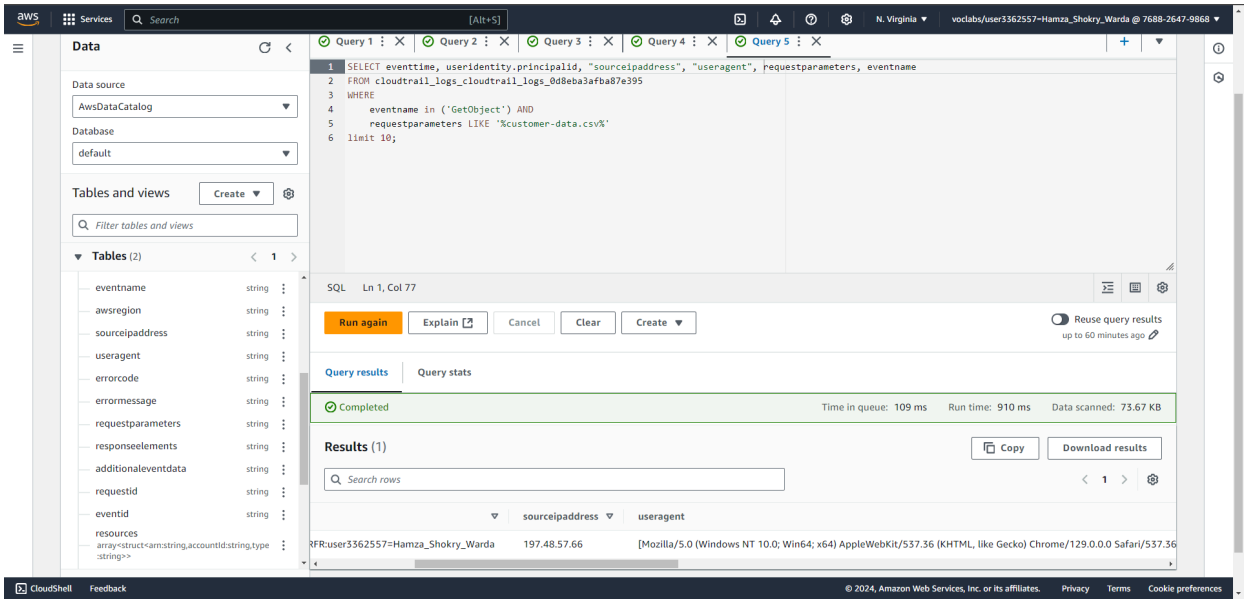


Phase 4: Monitoring and logging

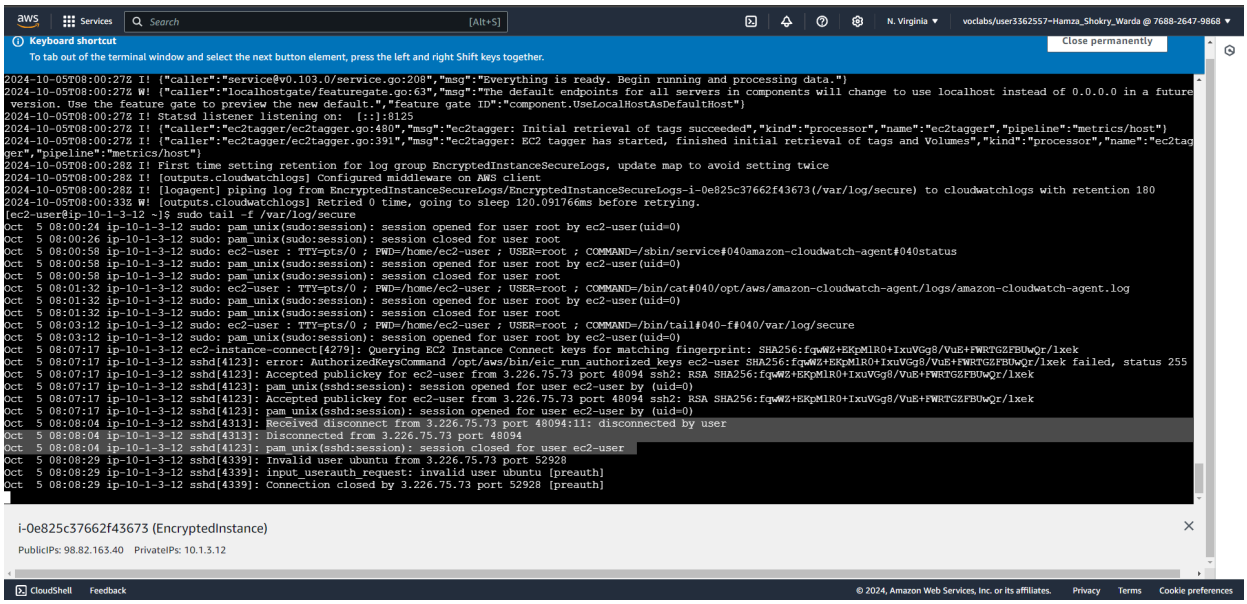
Task 4.1: Use CloudTrail to record Amazon S3 API calls

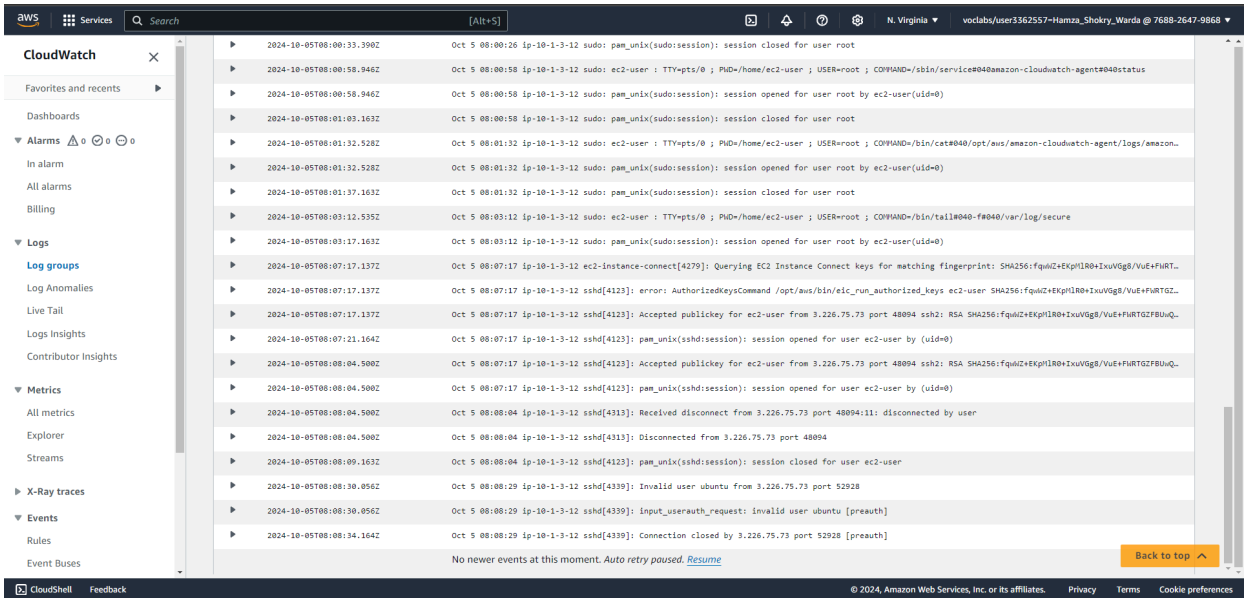

Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
CloudTrail > Trails > arn:aws:cloudtrail:us-east-1:768826479868:trail/data-bucket-reads-writes
data-bucket-reads-writes
Delete
Stop logging
General details
Edit
Trail logging
Logging
Trail name
data-bucket-reads-writes
Multi-region trail
Yes
Apply trail to my organization
Not enabled
Trail log location
cloudtrail-logs-0d8eba3afba87e395/AWSLogs/768826479868
Last log file delivered
-
Log file SSE-KMS encryption
Not enabled
Log file validation
Enabled
Last file validation delivered
-
SNS notification delivery
Disabled
Last SNS notification
-
CloudWatch Logs
Edit
No CloudWatch Logs log groups
CloudWatch Logs is not configured for this trail
Tags
Manage tags
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
Amazon Athena > Query editor
Editor
Recent queries
Saved queries
Settings
Workgroup
primary
Data
Data source
AwsDataCatalog
Database
default
Tables and views
Create
Filter tables and views
Tables (2)
bucket_logs
cloudtrail_logs_cloudtrail_logs_0d8eba3afba87e395
Views (0)
Query 1
Query 2
Query 3
SELECT * FROM "default"."cloudtrail_logs_cloudtrail_logs_0d8eba3afba87e395" limit 10;
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: 66 ms
Run time: 927 ms
Data scanned: 10.51 KB
Results (10)
Copy
Download results
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

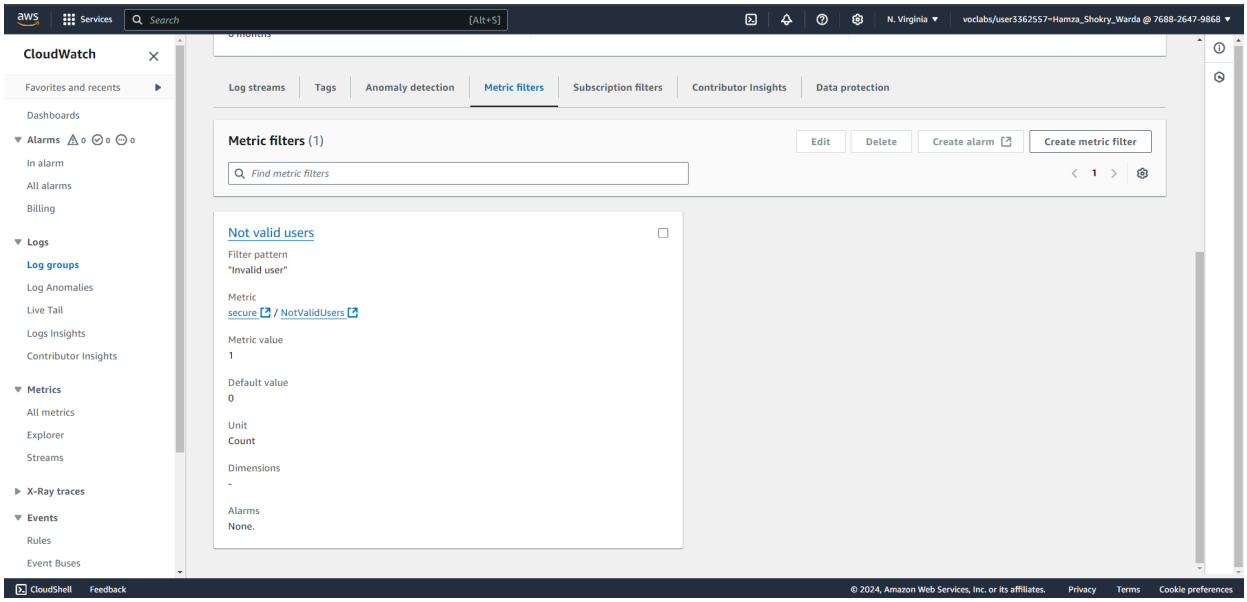


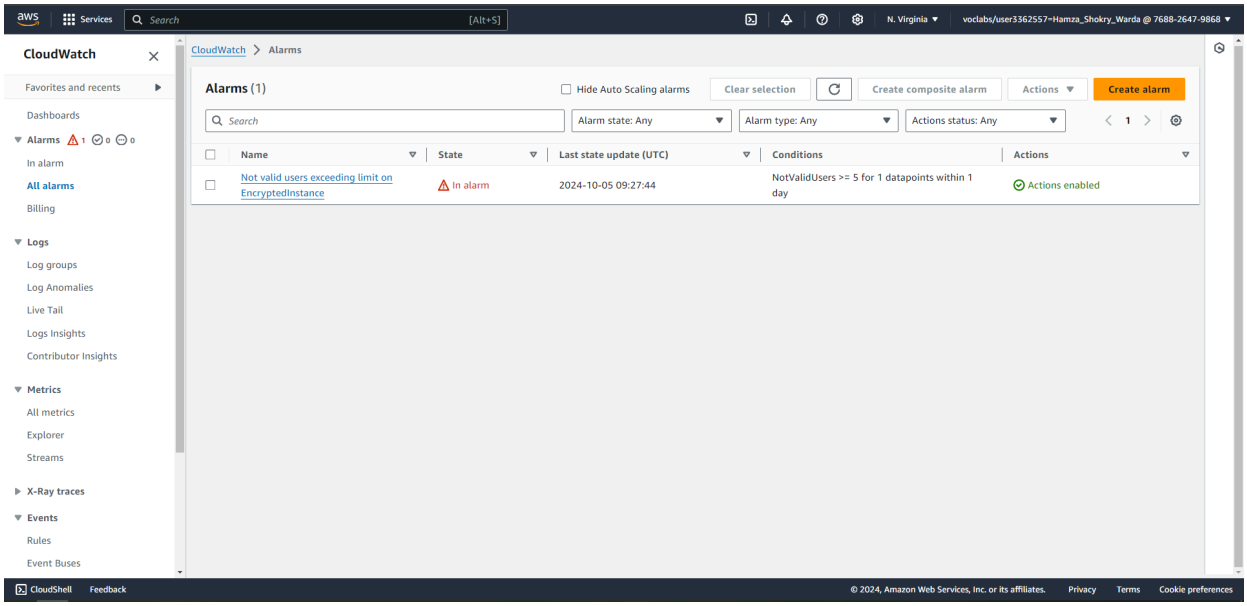
Task 4.2: Use CloudWatch Logs to monitor secure logs



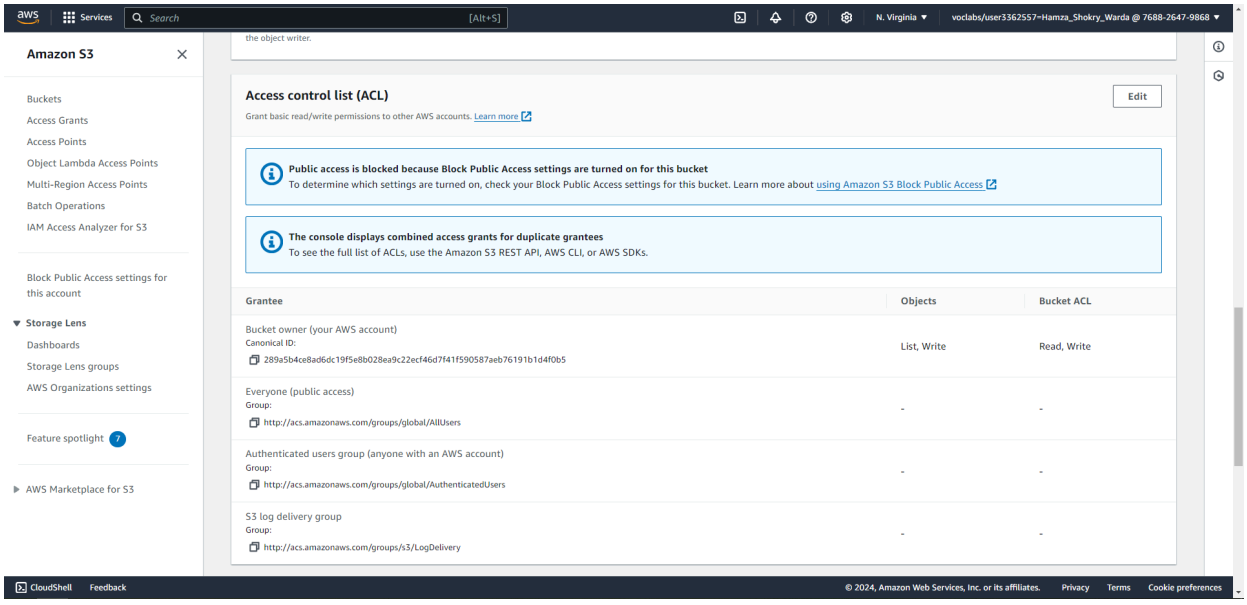


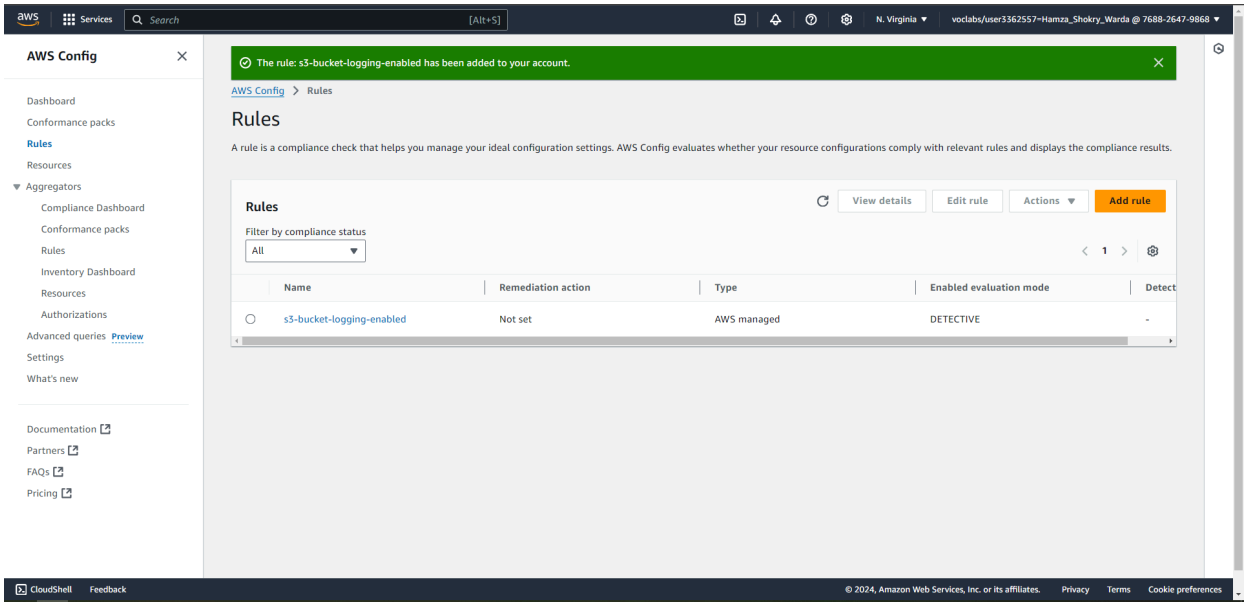
Task 4.3: Create a CloudWatch alarm to send notifications for security incidents

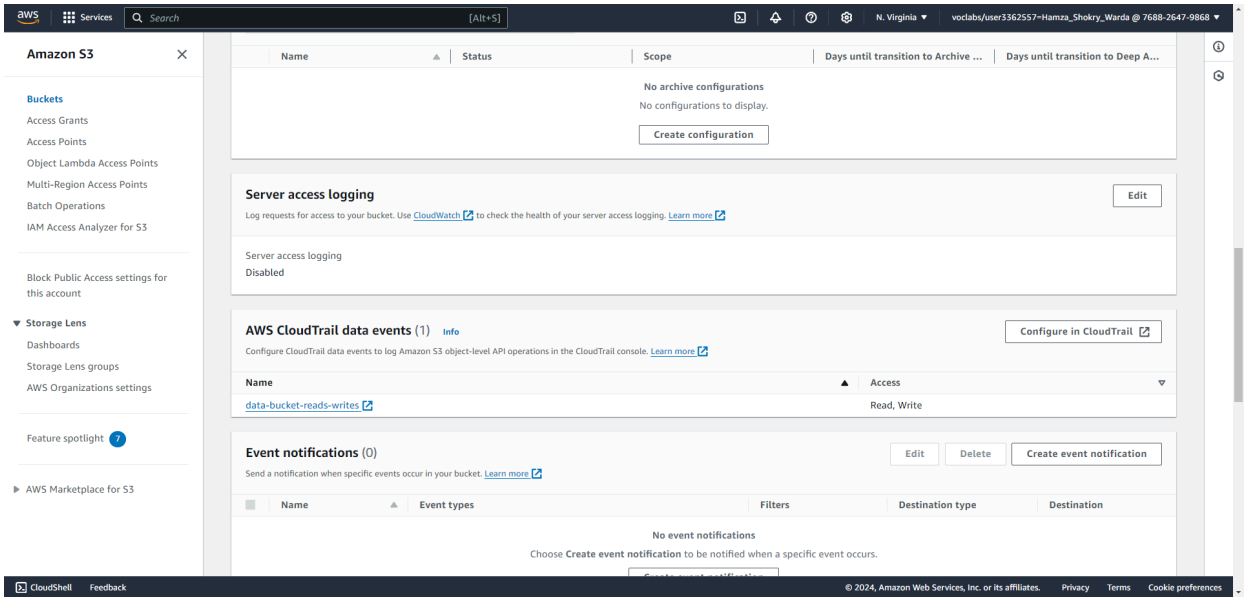


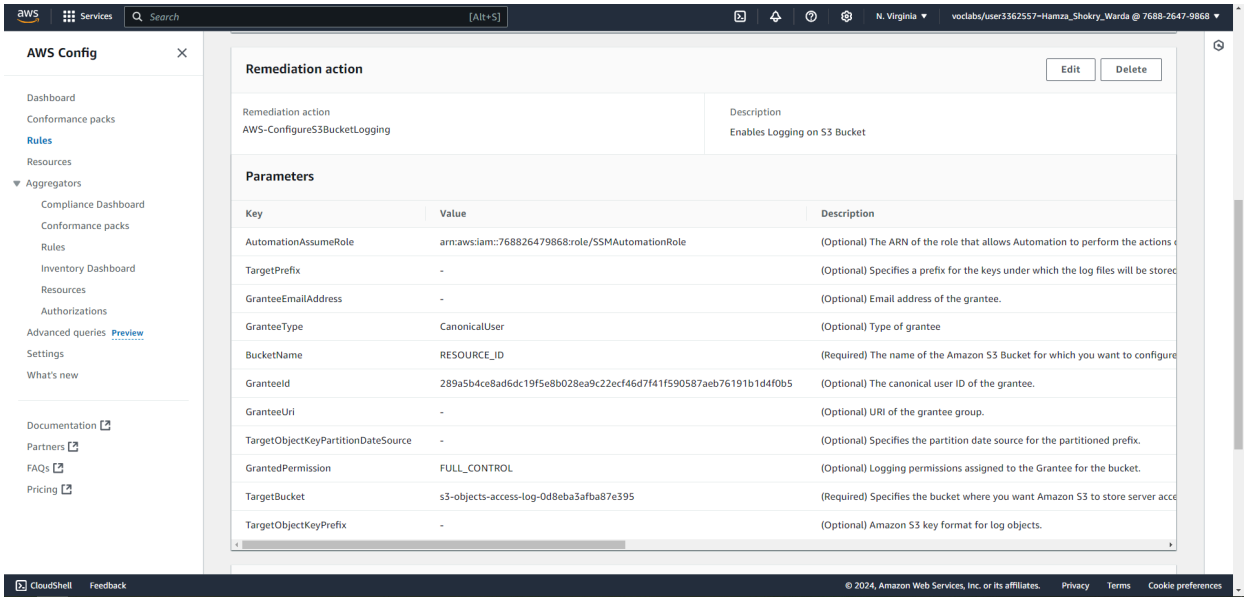


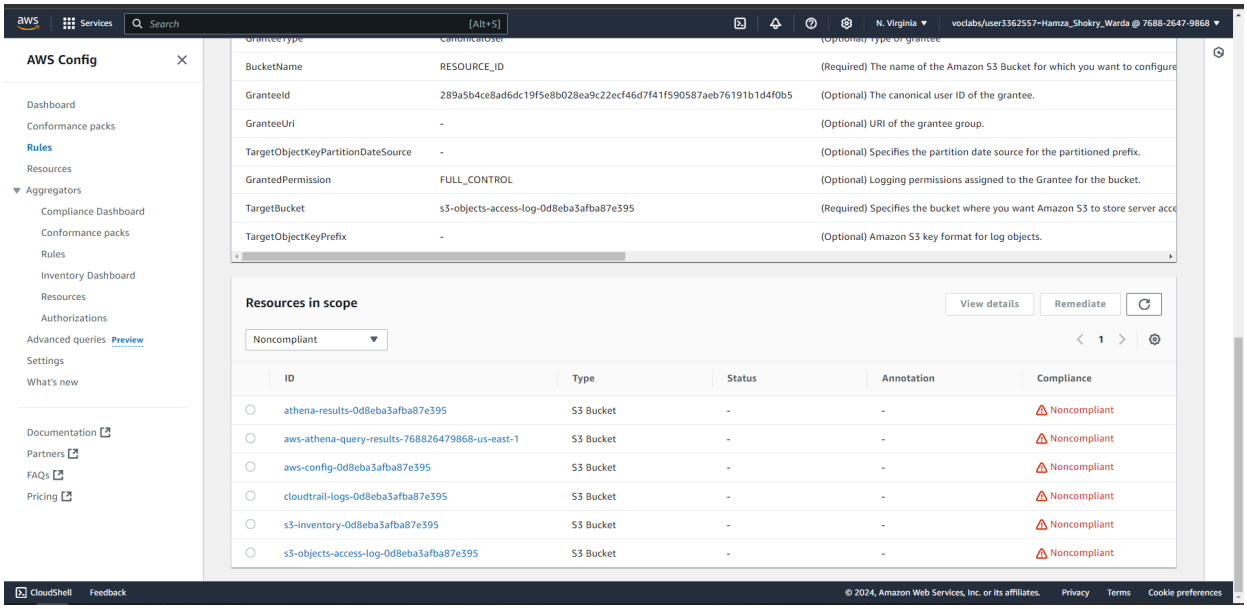
Task 4.4: Configure AWS Config to assess security settings and remediate the configuration of AWS resources

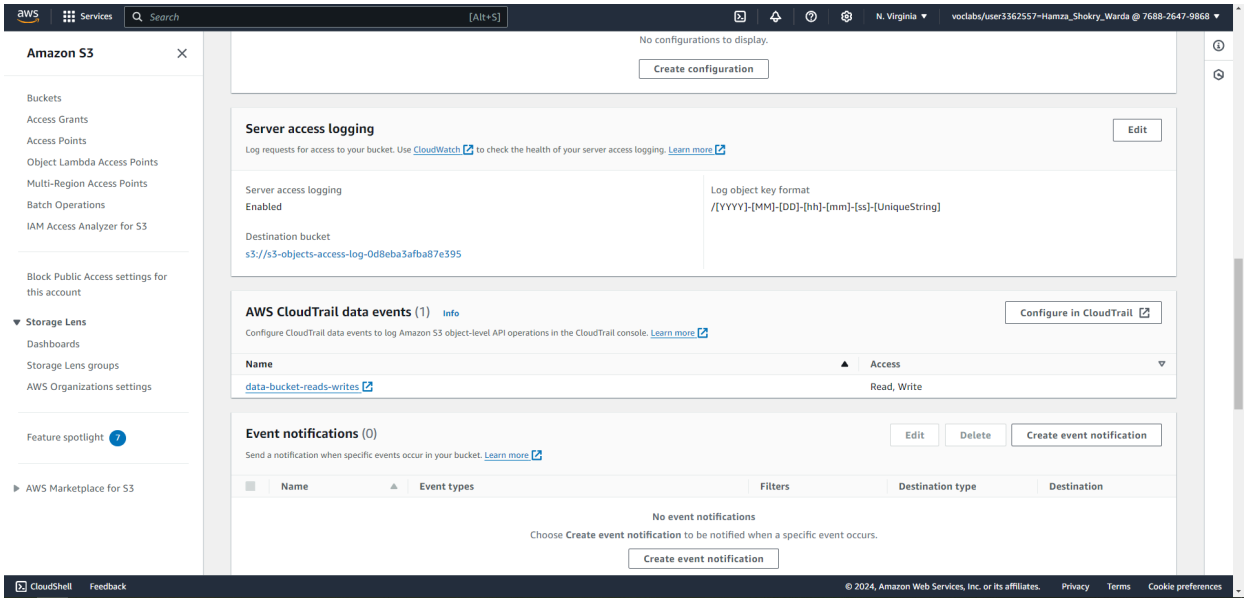



Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
AWS Config
Dashboard
Conformance packs
Rules
Resources
Aggregators
Compliance Dashboard
Conformance packs
Rules
Inventory Dashboard
Resources
Authorizations
Advanced queries Preview
Settings
What's new
Documentation
Partners
FAQs
Pricing
The rule: s3-bucket-logging-enabled has been added to your account.
AWS Config > Rules
Rules
A rule is a compliance check that helps you manage your ideal configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and displays the compliance results.
Rules
View details
Edit rule
Actions
Add rule
Filter by compliance status
All
1
Name
Remediation action
Type
Enabled evaluation mode
Detect
s3-bucket-logging-enabled
Not set
AWS managed
DETECTIVE
-
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
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
Name
Status
Scope
Days until transition to Archive ...
Days until transition to Deep A...
No archive configurations
No configurations to display.
Create configuration
Server access logging
Log requests for access to your bucket. Use CloudWatch to check the health of your server access logging. Learn more
Edit
Server access logging
Disabled
AWS CloudTrail data events (1) Info
Configure CloudTrail data events to log Amazon S3 object-level API operations in the CloudTrail console. Learn more
Configure in CloudTrail
Name
Access
data-bucket-reads-writes
Read, Write
Event notifications (0)
Send a notification when specific events occur in your bucket. Learn more
Edit
Delete
Create event notification
Name
Event types
Filters
Destination type
Destination
No event notifications
Choose Create event notification to be notified when a specific event occurs.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
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
Remediation action
Edit
Delete
Remediation action
AWS-ConfigureS3BucketLogging
Description
Enables Logging on S3 Bucket
Parameters
Key
Value
Description
AutomationAssumeRole
arn:aws:iam::768826479868:role/SSMAutomationRole
(Optional) The ARN of the role that allows Automation to perform the actions
TargetPrefix
-
(Optional) Specifies a prefix for the keys under which the log files will be stored
GranteeEmailAddress
-
(Optional) Email address of the grantee.
GranteeType
CanonicalUser
(Optional) Type of grantee
BucketName
RESOURCE_ID
(Required) The name of the Amazon S3 Bucket for which you want to configure
GranteeId
289a5b4ce8ad6dc19f5e8b028ea9c22ecf46d7f41f590587aeb76191b1d4f0b5
(Optional) The canonical user ID of the grantee.
GranteeUri
-
(Optional) URI of the grantee group.
TargetObjectKeyPartitionDateSource
-
(Optional) Specifies the partition date source for the partitioned prefix.
GrantedPermission
FULL_CONTROL
(Optional) Logging permissions assigned to the Grantee for the bucket.
TargetBucket
s3-objects-access-log-0d8eba3afba87e395
(Required) Specifies the bucket where you want Amazon S3 to store server acce
TargetObjectKeyPrefix
-
(Optional) Amazon S3 key format for log objects.
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


aws
Services
Search
[Alt+S]
N. Virginia
voclabs/user3362557=Hamza_Shokry_Warda @ 7688-2647-9868
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
BucketName
RESOURCE_ID
(Required) The name of the Amazon S3 Bucket for which you want to configure
GranteeId
289a5b4ce8ad6dc19f5e8b028ea9c22ecf46d7f41f590587aeb76191b1d4f0b5
(Optional) The canonical user ID of the grantee.
GranteeUri
-
(Optional) URI of the grantee group.
TargetObjectKeyPartitionDateSource
-
(Optional) Specifies the partition date source for the partitioned prefix.
GrantedPermission
FULL_CONTROL
(Optional) Logging permissions assigned to the Grantee for the bucket.
TargetBucket
s3-objects-access-log-0d8eba3afba87e395
(Required) Specifies the bucket where you want Amazon S3 to store server acce
TargetObjectKeyPrefix
-
(Optional) Amazon S3 key format for log objects.
Resources in scope
View details
Remediate
Noncompliant
1
ID
Type
Status
Annotation
Compliance
athena-results-0d8eba3afba87e395
S3 Bucket
-
-
Noncompliant
aws-athena-query-results-768826479868-us-east-1
S3 Bucket
-
-
Noncompliant
aws-config-0d8eba3afba87e395
S3 Bucket
-
-
Noncompliant
cloudtrail-logs-0d8eba3afba87e395
S3 Bucket
-
-
Noncompliant
s3-inventory-0d8eba3afba87e395
S3 Bucket
-
-
Noncompliant
s3-objects-access-log-0d8eba3afba87e395
S3 Bucket
-
-
Noncompliant
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



Cost assessment for monitoring and logging