2023

Summer Training Project Report [Cloud Computing with AWS]

ATTACK-PROOF WEBSITE WITH AUTOMATED BACKUP OF OS AND LOGS

ASHISH PANDEY

Project Report: Attack-Proof Website with Automated Backup of OS and Logs

1. **Introduction**

   The purpose of this report is to provide an overview of the "Attack-Proof Website with Automated Backup of OS and Logs" project implemented on the Amazon Web Services (AWS) platform. The project aims to create a secure website infrastructure that minimizes the risk of attacks while ensuring the availability and integrity of data.

2. **Project Overview**

   The project involves the following key components and configurations:
   - **EC2 Instance:** A Linux-based EC2 instance hosts the PHP-based website.
   - **RDS Database:** The website's database, powered by MySQL, is hosted on an RDS instance.
   - **S3 Bucket:** An S3 bucket is used to synchronize logs and webpages from the HTTPS server at regular intervals of 5 minutes.
   - **Autoscaling:** The infrastructure is designed to automatically scale the number of EC2 instances based on demand, with a minimum of 1 instance and a maximum of 3 instances. A load balancer is implemented to distribute traffic across the instances efficiently.
   - **Bucket Lifecycle:** A bucket lifecycle policy is established to remove or move previous versions of logs after 2 days, optimizing storage and managing data retention.
   - **SNS Notifications:** The Simple Notification Service (SNS) is configured to send email notifications whenever the number of instances increases or decreases.
   - **OS Disk Snapshots:** Regular snapshots of the EC2 instance's OS disk are taken every 12 hours, retaining the last 2 snapshots.

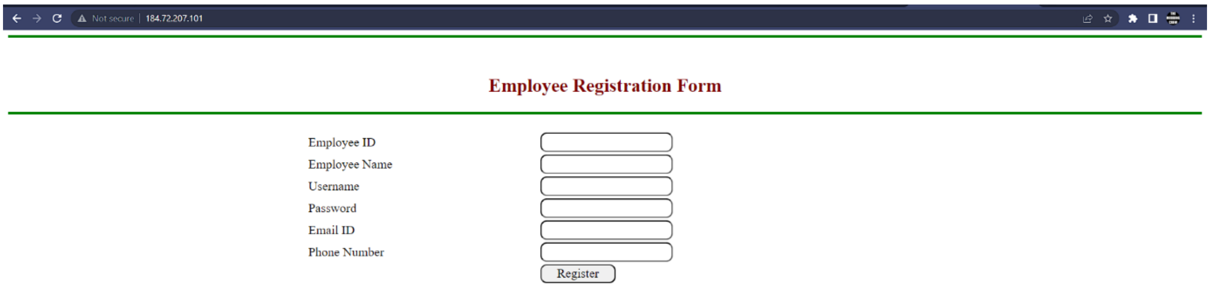
3. **Security Measures**

   The project incorporates various security measures to ensure an attack-proof website:

   - **Isolated Environment:** By separating the website and database components, potential attacks are contained withing specific areas, reducing the impact of any successful breaches.
   - **Automated Backup:** The frequent synchronization of logs and webpages to the S3 bucket ensures that critical data is regularly backed up and can be recovered in case of attacks or system failures.
   - **Autoscaling and Load Balancer:** The use of autoscaling and a load balancer helps mitigate overloading during peak traffic, improving performance and preventing potential attacks due to resource exhaustion.
   - **Bucket Lifecycle Management:** The bucket lifecycle policy ensures that older logs are either deleted or moved to Glacier after 2 days, optimizing storage costs and maintaining a manageable log history.
   - **SNS Notifications:** Administrators receive email notifications whenever instances increase or decrease, keeping them informed about the infrastructure's capacity changes and facilitating timely actions.
   - **OS Disk Snapshots:** Regular snapshots of the OS disk provide a restore point in the event of attacks or system failures, enabling the restoration of the instance to a known secure state.

4. Screenshots

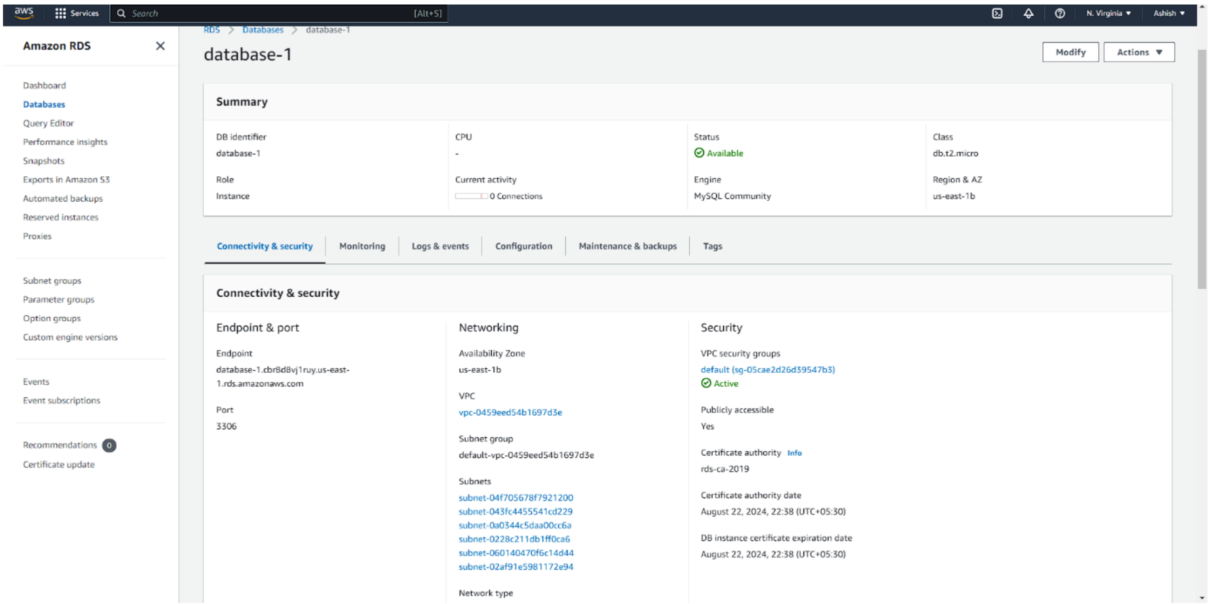
Figure 1: Website



Employee Registration Form

Employee ID
Employee Name
Username
Password
Email ID
Phone Number

Figure 2: RDS Database Configuration



database-1

Summary

DB identifier
database-1

CPU
-

Status
Available

Class
db.t2.micro

Role
Instance

Current activity
0 Connections

Engine
MySQL Community

Region & AZ
us-east-1b

Connectivity & security

Endpoint & port

Endpoint
database-1.cbr8d8vj1ruy.us-east-1.rds.amazonaws.com

Port
3306

Networking

Availability Zone
us-east-1b

VPC
vpc-0459eed54b1697d3e

Subnet group
default-vpc-0459eed54b1697d3e

Subnets
subnet-04f705678f7921200
subnet-043fc4455541cd229
subnet-0a0344c5daa00cc6a
subnet-0228c211db1ff0ca6
subnet-060140470f6c14d44
subnet-02af91e5981172e94

Network type

Security

VPC security groups
default (sg-05cae2d26d39547b3)
Active

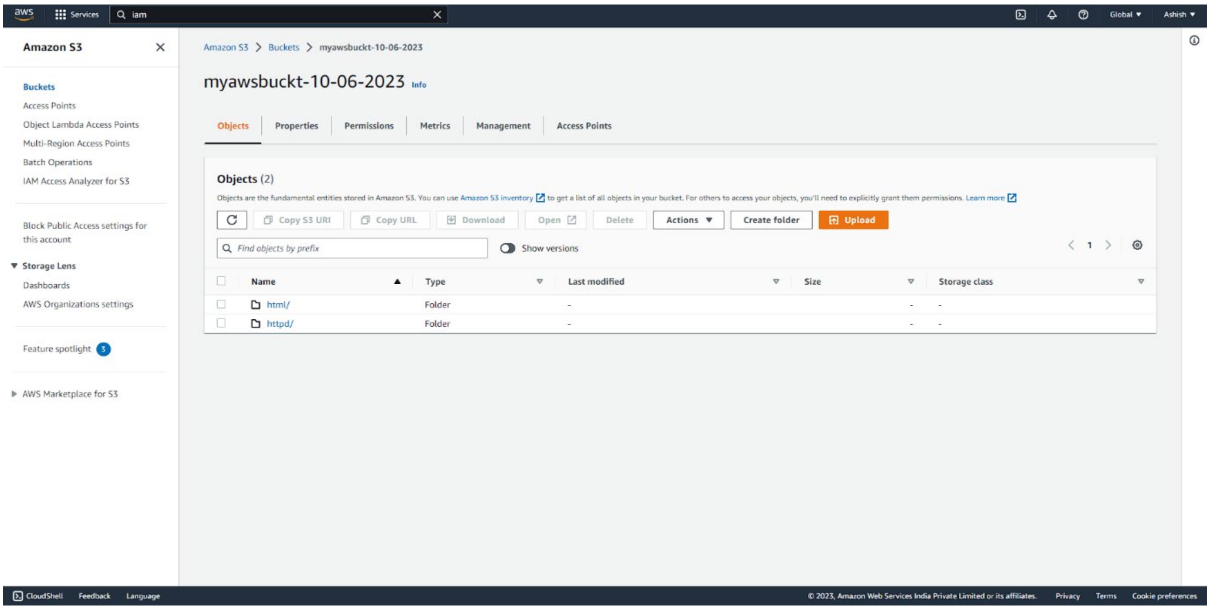
Publicly accessible
Yes

Certificate authority Info
rds-ca-2019

Certificate authority date
August 22, 2024, 22:38 (UTC+05:30)

DB instance certificate expiration date
August 22, 2024, 22:38 (UTC+05:30)

Figure 3: S3 Bucket Configuration

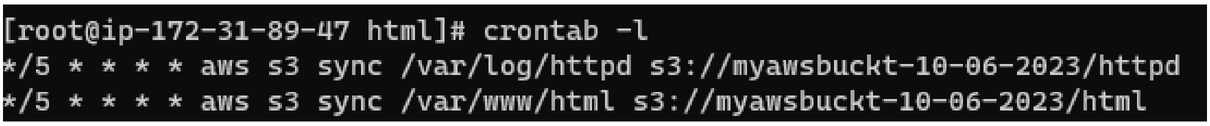


myawsbuckt-10-06-2023

Objects (2)

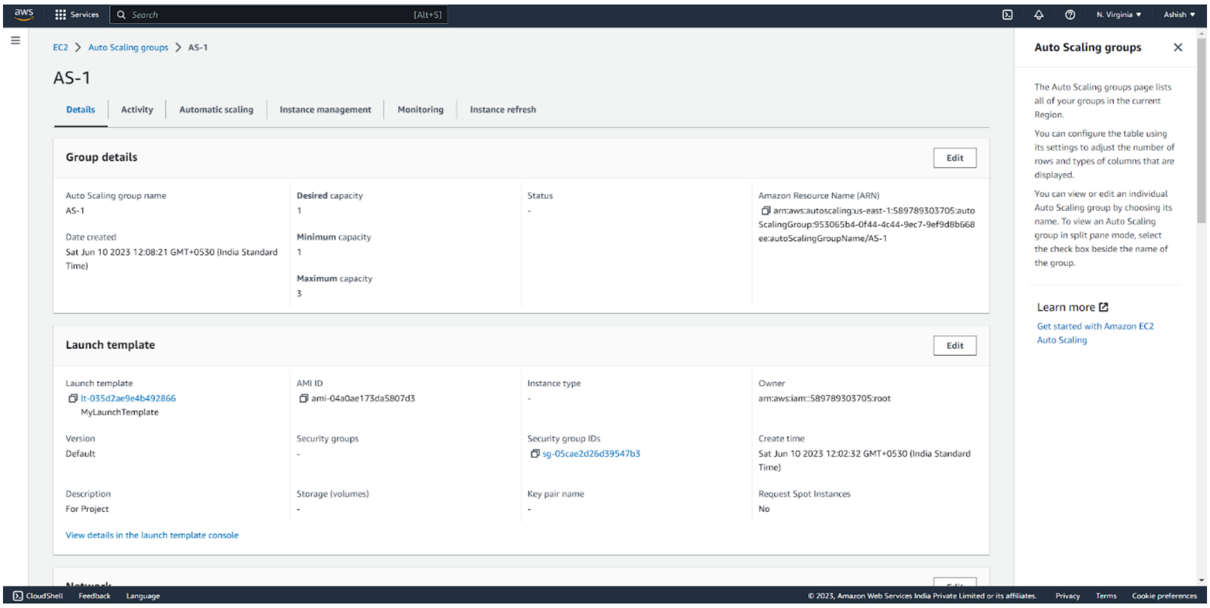
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

□	Name ▲	Type	Last modified	Size	Storage class
□	html/	Folder	-	-	-
□	httpd/	Folder	-	-	-



```
[root@ip-172-31-89-47 html]# crontab -l
*/5 * * * * aws s3 sync /var/log/httpd s3://myawsbuckt-10-06-2023/httpd
*/5 * * * * aws s3 sync /var/www/html s3://myawsbuckt-10-06-2023/html
```

Figure 4: Autoscaling Configuration



AS-1

Group details

Auto Scaling group name
AS-1

Date created
Sat Jun 10 2023 12:08:21 GMT+0530 (India Standard Time)

Desired capacity
1

Minimum capacity
1

Maximum capacity
3

Status
-

Amazon Resource Name (ARN)
arn:aws:autoscaling:us-east-1:589789303705:autoScalingGroup:953065b4-0f44-4c44-9ec7-9ef9d8b668ee:autoScalingGroupName/AS-1

Launch template

Launch template
lt-035d2ae9e4b492866
MyLaunchTemplate

AMI ID
ami-04a0ae173da5807d3

Instance type
-

Owner
arn:aws:iam::589789303705:root

Version
Default

Security groups
-

Security group IDs
sg-05cae2d26d39547b3

Create time
Sat Jun 10 2023 12:02:32 GMT+0530 (India Standard Time)

Description
For Project

Storage (volumes)
-

Key pair name
-

Request Spot Instances
No

Auto Scaling groups

The Auto Scaling groups page lists all of your groups in the current Region.

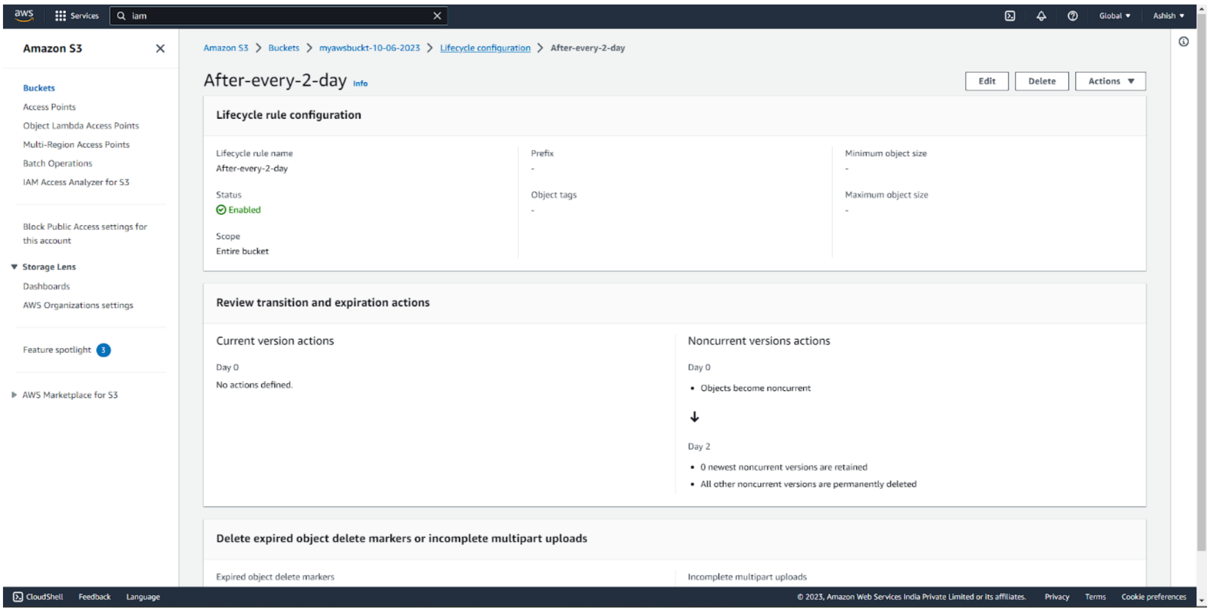
You can configure the table using its settings to adjust the number of rows and types of columns that are displayed.

You can view or edit an individual Auto Scaling group by choosing its name. To view an Auto Scaling group in split pane mode, select the check box beside the name of the group.

Learn more

Get started with Amazon EC2 Auto Scaling

Figure 5: Bucket Lifecycle Policy Configuration


aws
Services
iam
Global
Ashish
Amazon S3
Buckets
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
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > Buckets > myawsbuckt-10-06-2023 > Lifecycle configuration > After-every-2-day
Info
Edit
Delete
Actions
CloudShell
Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences

After-every-2-day

Lifecycle rule configuration

Lifecycle rule name
After-every-2-day

Status
Enabled

Scope
Entire bucket

Prefix
-

Object tags
-

Minimum object size
-

Maximum object size
-

Review transition and expiration actions

Current version actions

Day 0
No actions defined.

Noncurrent versions actions

Day 0
- Objects become noncurrent

↓

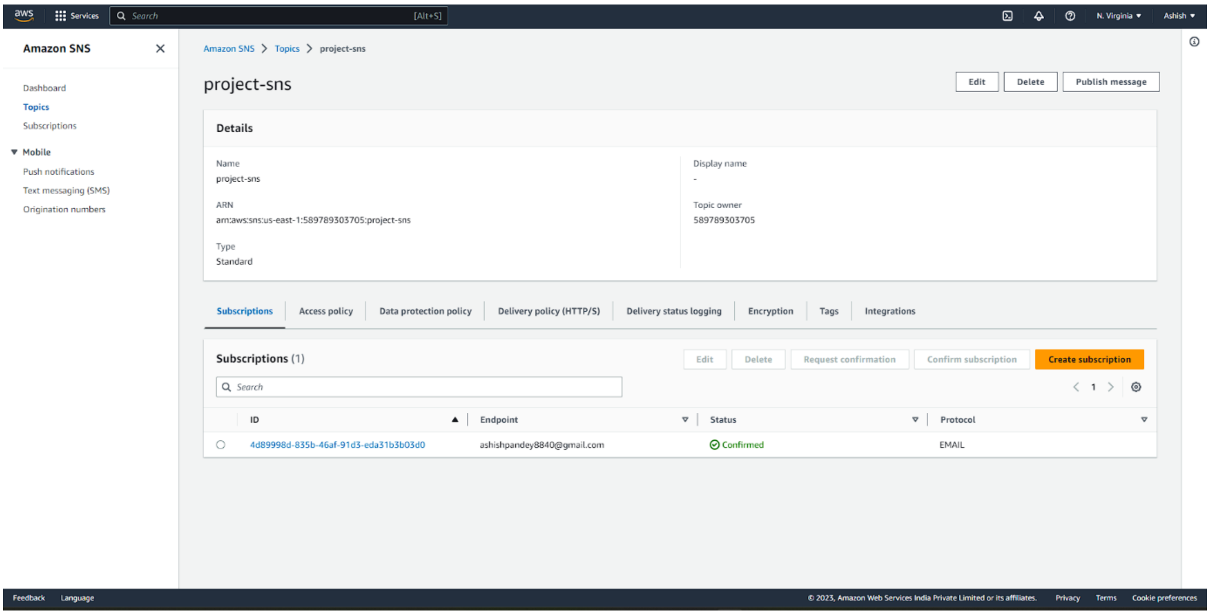
Day 2
- 0 newest noncurrent versions are retained
- All other noncurrent versions are permanently deleted

Delete expired object delete markers or incomplete multipart uploads

Expired object delete markers

Incomplete multipart uploads

Figure 6: SNS Notification Configuration



project-sns

Details

Name
project-sns

ARN
arn:aws:sns:us-east-1:589789303705:project-sns

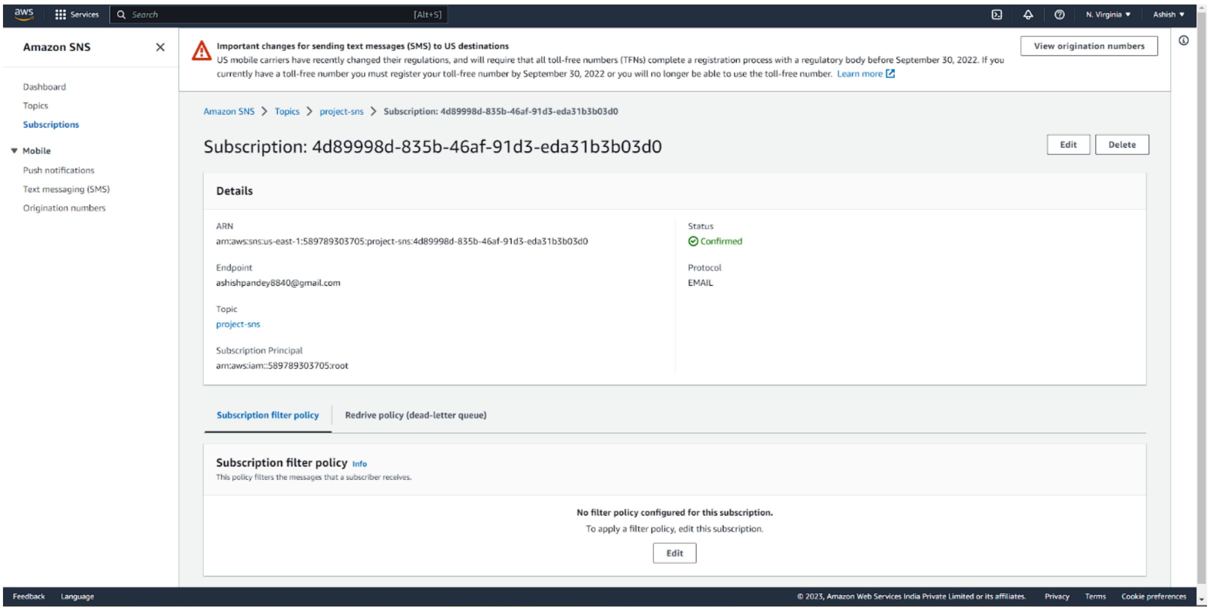
Type
Standard

Display name
-

Topic owner
589789303705

Subscriptions (1)

	ID	Endpoint	Status	Protocol
○	4d89998d-835b-46af-91d3-eda31b3b03d0	ashishpandey8840@gmail.com	Confirmed	EMAIL



Important changes for sending text messages (SMS) to US destinations
US mobile carriers have recently changed their regulations, and will require that all toll-free numbers (TFNs) complete a registration process with a regulatory body before September 30, 2022. If you currently have a toll-free number you must register your toll-free number by September 30, 2022 or you will no longer be able to use the toll-free number. Learn more

Amazon SNS > Topics > project-sns > Subscription: 4d89998d-835b-46af-91d3-eda31b3b03d0

Subscription: 4d89998d-835b-46af-91d3-eda31b3b03d0

Details

ARN
arn:aws:sns:us-east-1:589789303705:project-sns:4d89998d-835b-46af-91d3-eda31b3b03d0

Status
Confirmed

Endpoint
ashishpandey8840@gmail.com

Protocol
EMAIL

Topic
project-sns

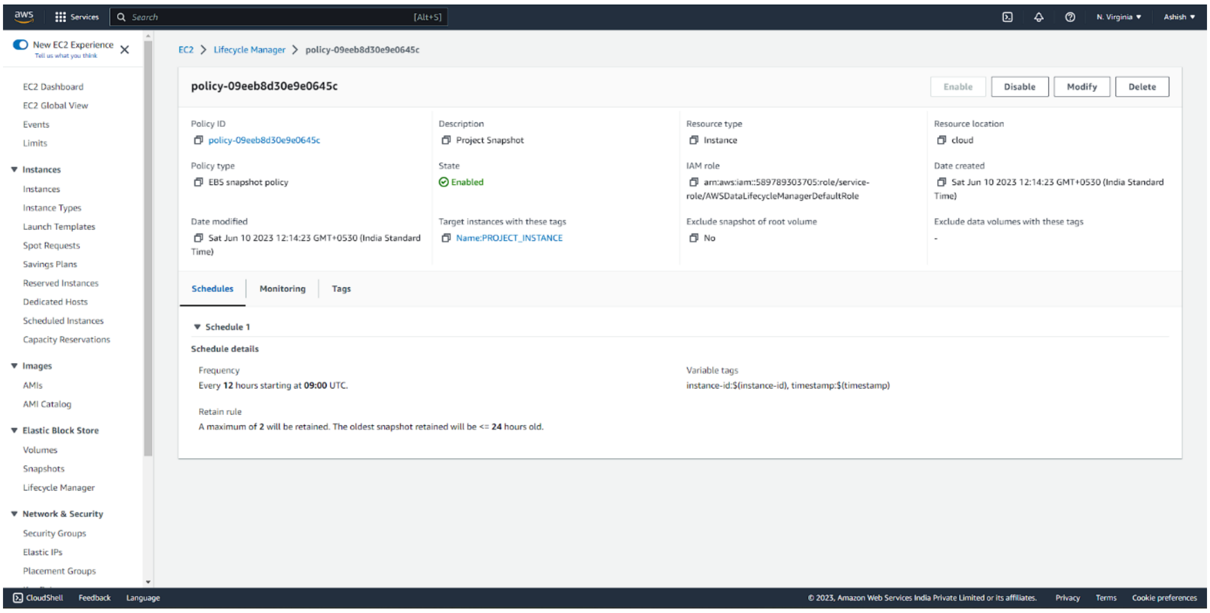
Subscription Principal
arn:aws:iam::589789303705:root

Subscription filter policy | Redrive policy (dead-letter queue)

Subscription filter policy Info
This policy filters the messages that a subscriber receives.

No filter policy configured for this subscription.
To apply a filter policy, edit this subscription.
Edit

Figure 7: OS Disk Snapshot Configuration



EC2 > Lifecycle Manager > policy-09eeb8d30e9e0645c

policy-09eeb8d30e9e0645c

Policy ID
policy-09eeb8d30e9e0645c

Description
Project Snapshot

Resource type
Instance

Resource location
cloud

Policy type
EBS snapshot policy

State
Enabled

IAM role
arn:aws:iam::589789303705:role/service-role/AWSDataLifecycleManagerDefaultRole

Date created
Sat Jun 10 2023 12:14:23 GMT+0530 (India Standard Time)

Date modified
Sat Jun 10 2023 12:14:23 GMT+0530 (India Standard Time)

Target instances with these tags
Name:PROJECT_INSTANCE

Exclude snapshot of root volume
No

Exclude data volumes with these tags
-

Schedules | Monitoring | Tags

Schedule 1

Schedule details

Frequency
Every **12** hours starting at **09:00** UTC.

Variable tags
instance-id:$(instance-id), timestamp:$(timestamp)

Retain rule
A maximum of **2** will be retained. The oldest snapshot retained will be <= **24** hours old.

5. Conclusion

The “Attack-Proof Website with Automated Backup of OS and Logs” project successfully implements several security measure and configurations to enhance the website’s security and resilience. By isolating components, automating backups, implementing autoscaling, managing log retention, and taking regular OS disk snapshots, the project reduces the risk of attacks, improves system availability, and ensures data integrity.

The project's isolated environment provides containment, limiting the impact of potential breaches. Automated backups through the synchronization of logs and webpages to the S3 bucket guarantee the ability to recover critical data in the event of attacks or system failures.

Autoscaling, coupled with the load balancer, ensures optimal performance during peak traffic, preventing potential attacks due to resource exhaustion.

The bucket lifecycle policy efficiently manages log retention, optimizing storage costs and maintaining a manageable log history. SNS notifications keep administrators informed about instances increasing or decreasing, enabling timely actions and efficient capacity management. Furthermore, the regular snapshots of the OS disk provide a reliable restore point, enabling the restoration of the instance to a known secure state in case of attacks or system failures.

While the implemented security measures greatly enhance the website's protection against attacks, it is important to note that achieving absolute "attack-proof" status is challenging. Ongoing security practices such as regular updates, strong access controls, and comprehensive testing should be employed to maintain a robust security posture.

Overall, the "Attack-Proof Website with Automated Backup of OS and Logs" project successfully combines various security features and configurations to create a resilient and secure website infrastructure. By incorporating these measures, the project ensures that the website remains available, protected, and resilient against potential attacks.