# COBRA KAI

**BARATH BHASKARAN**

**119257395**

## 1.0 Introduction

This document provides technical details on how we can migrate the existing on-premise application to the cloud.

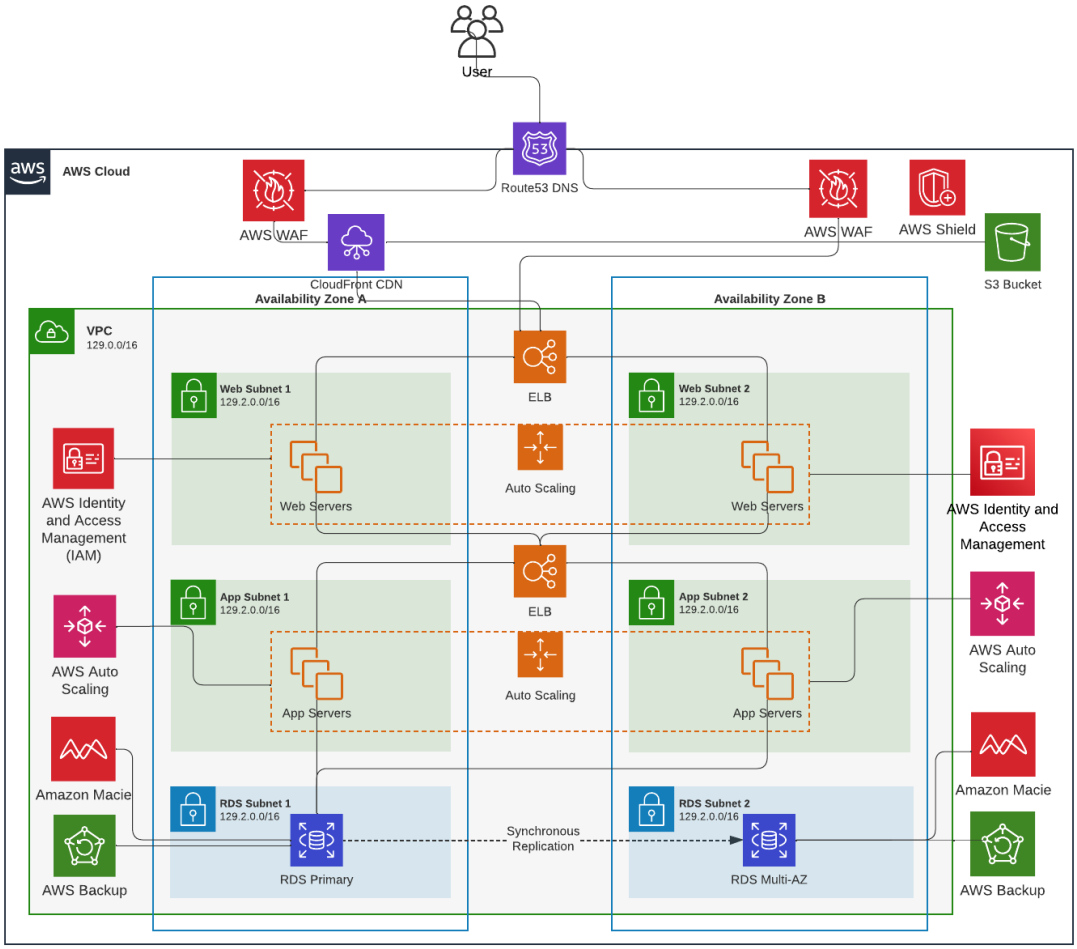
## 2.0 Issues in Current Architecture

- No patching strategy
- No backup strategy
- Vulnerable to DDOS attack
- No scaling when demand arises
- Slow streaming
- Non-PCI compliance

## 3.0 Advantages of Migrating to Cloud

- On-demand scalability
- Highly resilient
- Reduce infrastructure cost
- High availability
- No interruption of service
- Convenient access
- Increased availability and performance
- Continuous application monitoring
- Realtime DDoS protection
- Regulated user access

# 4.0 Proposed Architecture



## 5.0 Amazon VPC (Virtual Private Cloud)

Amazon Virtual Private Cloud is an AWS service that helps us to create AWS resources into a virtual network that we can define. This network is similar to a network that we operate in a data center but it comes with the advantage of using scalable infrastructure of AWS. Some of the features of VPC are

### 5.0.1 Subnets

A subnet is a set of IP addresses in the VPC. A subnet must be present in a single Availability Zone.

1.IP addressing

2.Routing

3.Gateways and endpoints

4.Peering connections

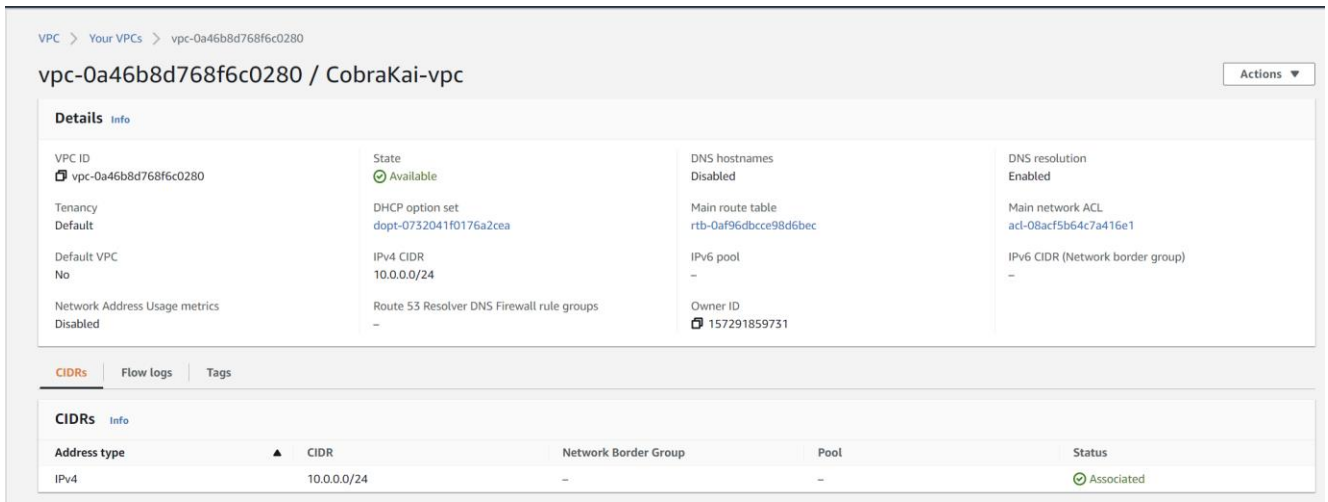
5.Traffic Mirroring

6.Transit gateways

7.VPC Flow Logs

8.VPN connections

The computing and network resources required for CobraKai application can be deployed in a VPC so that even if a availability zone fails the other availability zone will make the application available at all times.



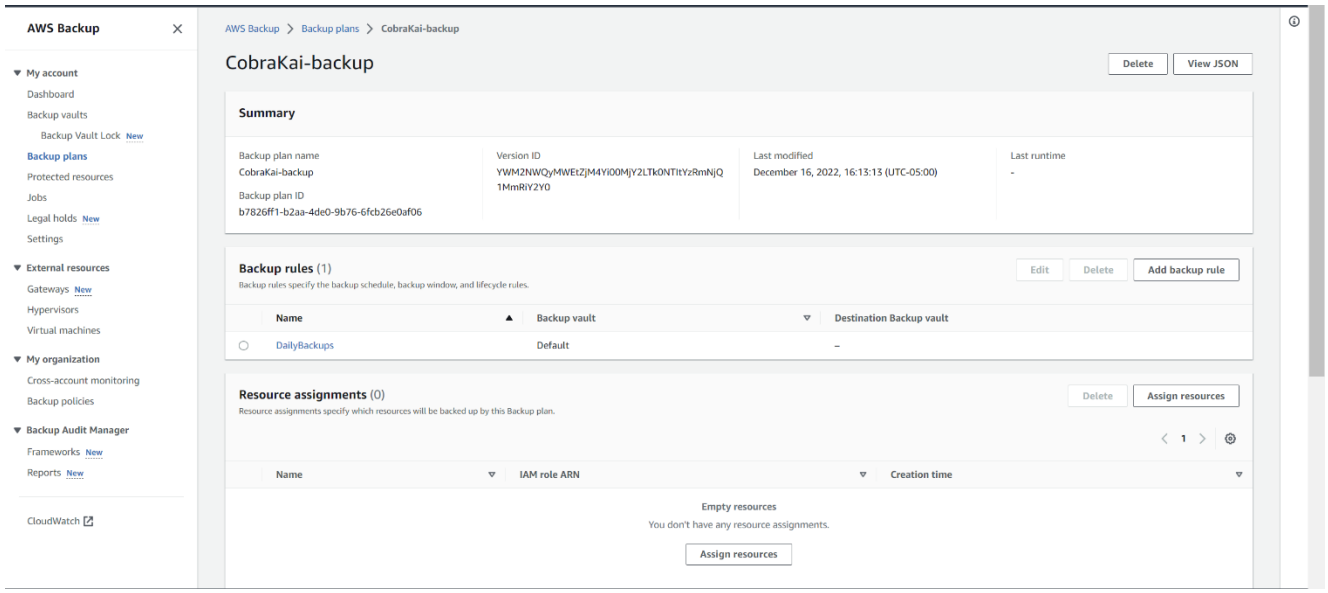
## 5.1 Backup and recovery

AWS Backup is a backup service that is fully managed and it automatically  stores data across a number of AWS services. It allows us to automate the backup tasks and removes the need of manual processes. By AWS Backup we can create backup policies and monitor all the AWS resources.

The content for the Cobra Kai application, which is stored on a conventional hard drive, can be moved to the cloud with the help of the AWS Backup service and easily recovered in the event of a disaster or hardware failure.

Creating a backup plan and configuring rules to backup data on a daily basis.

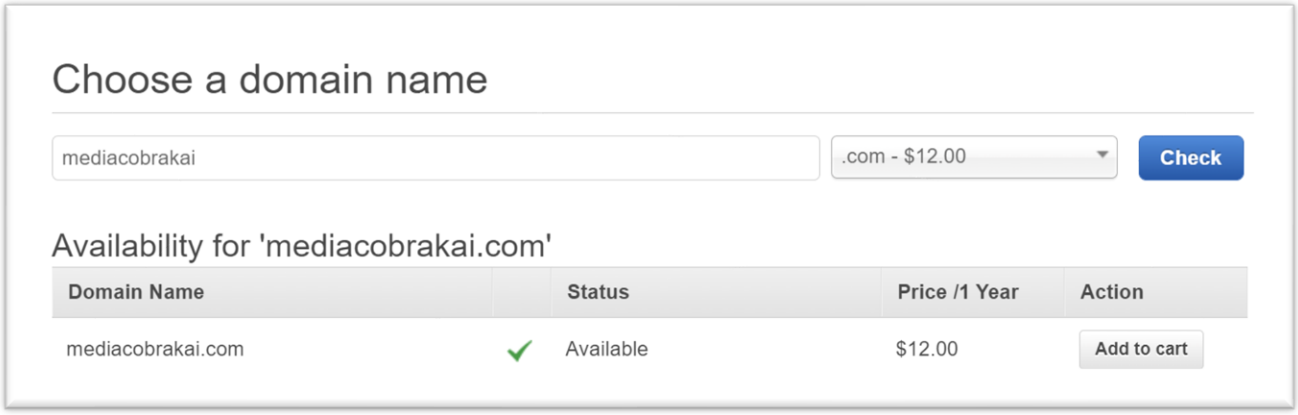
### 5.1.1 Creation of Backup plan




## 5.2 AWS Route 53

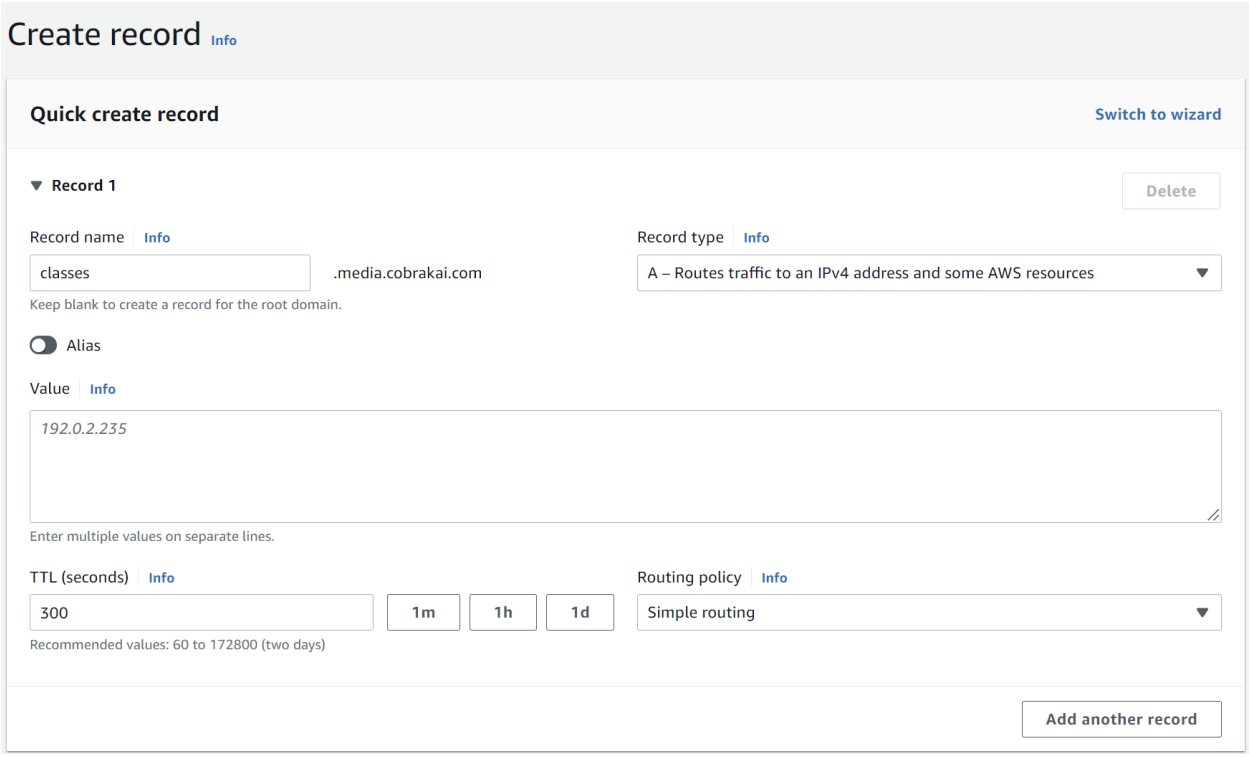
Route 53 is a DNS(Domain Name System) service available in AWS. It has three main functions

1. Domain Registration – This allows us to create and register a name(name of the website) for the application.




2. Routing user traffic to our domain.

When user enters the URL for CobraKai (media.CobraKai.com) in the browser it helps connects the browser to the CobraKai application.




3.Checks resource health

It automatically sends requests to a resource to check its availability. It also sends notifications when a resource becomes unavailable.

Creating a hosted zone for CobraKai application

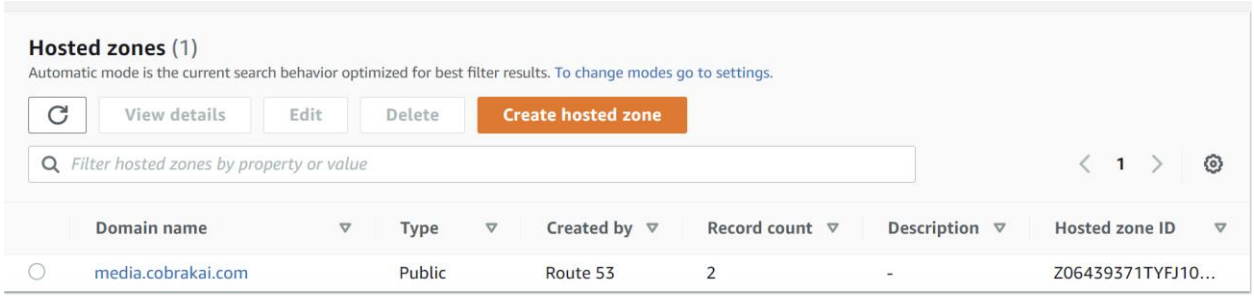
It contains routing details about how we need to route traffic to a domain and all the other subdomains within the domain. There are two types of hosted zones they are

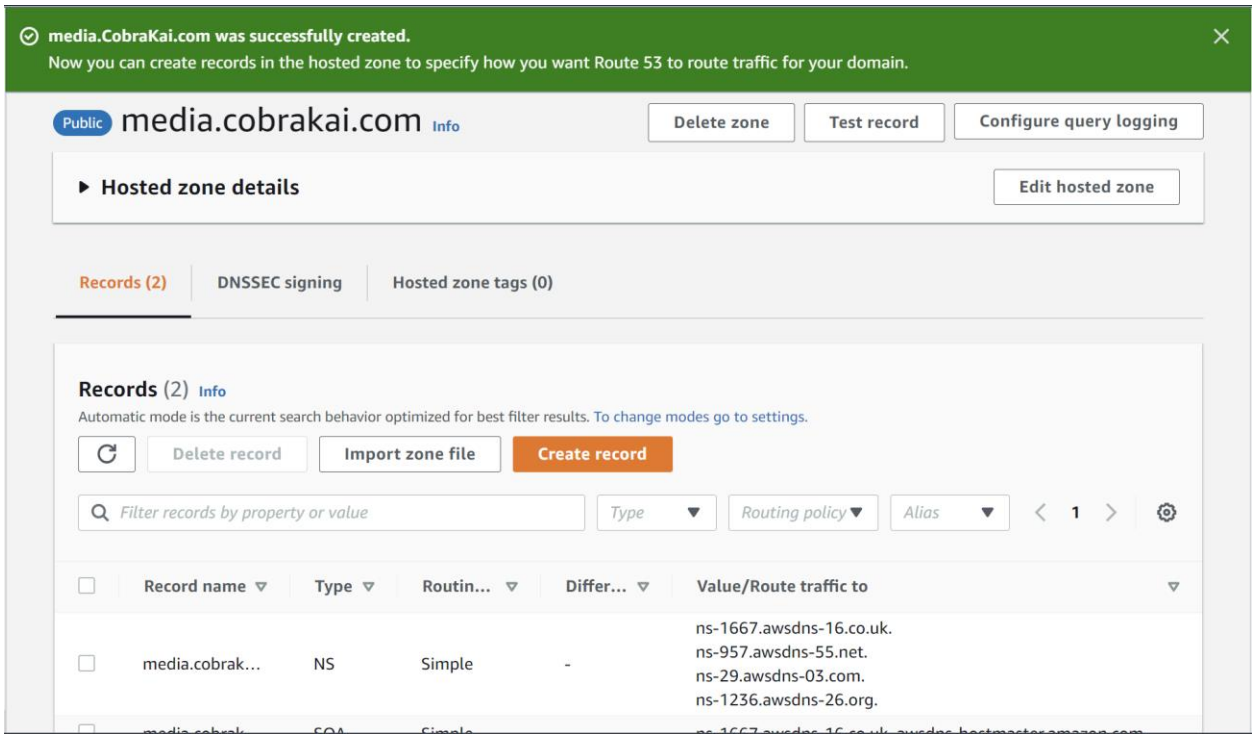
1. Public hosted zone :

It contains details that show how we should route user traffic on the internet.

2. Private hosted zone:

It contains information that indicate how we need to route user traffic in a VPC.

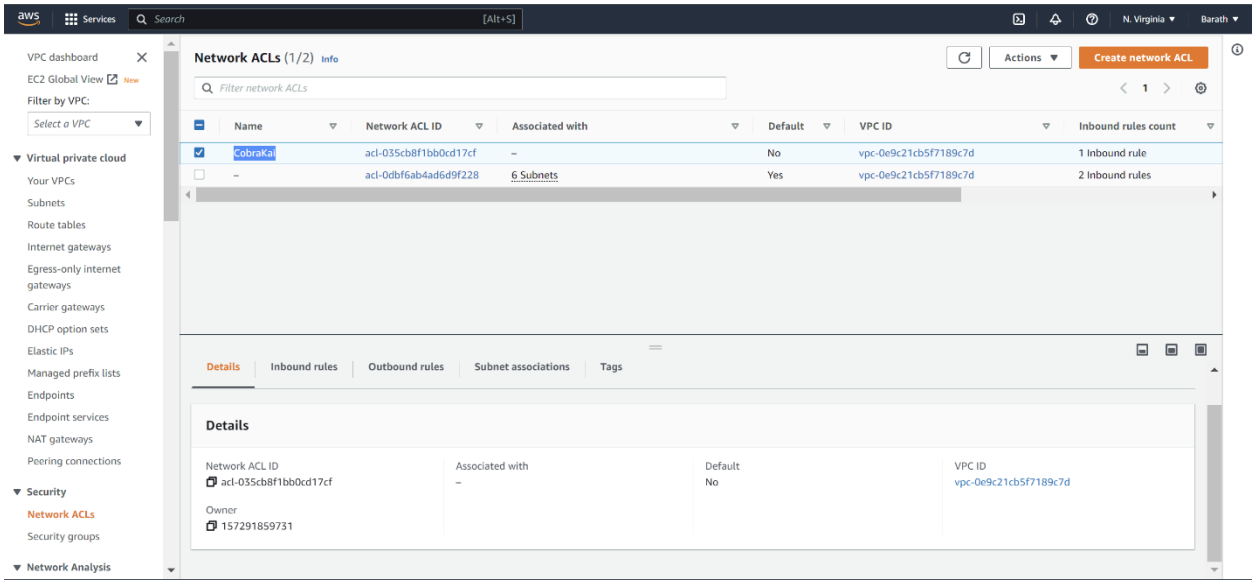


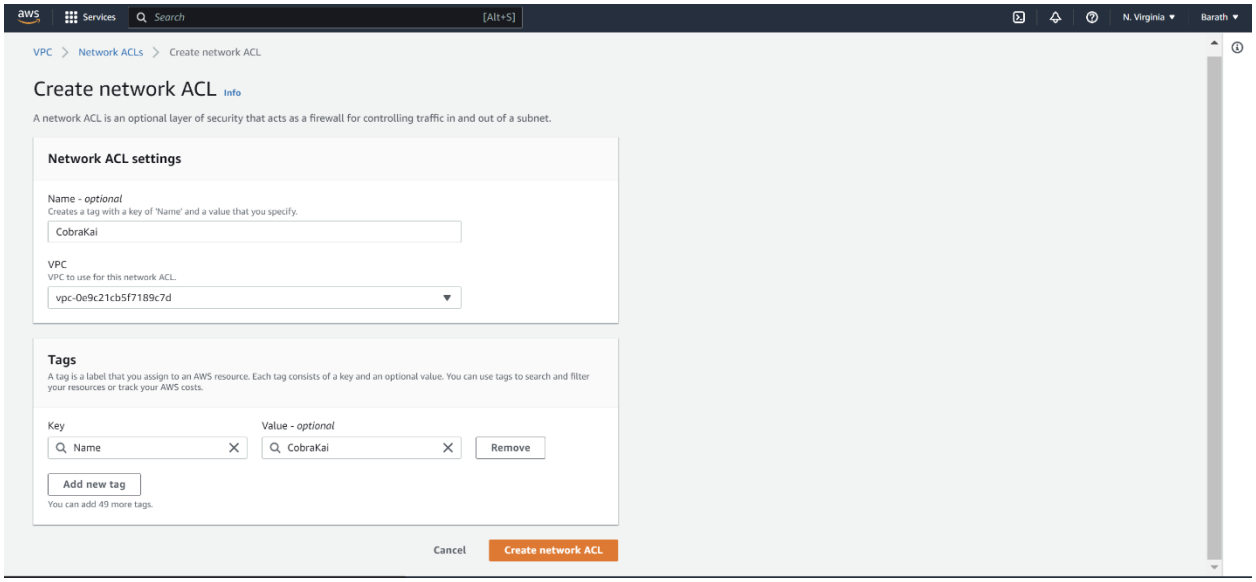




## 5.3 Network Access Control List (NACL)

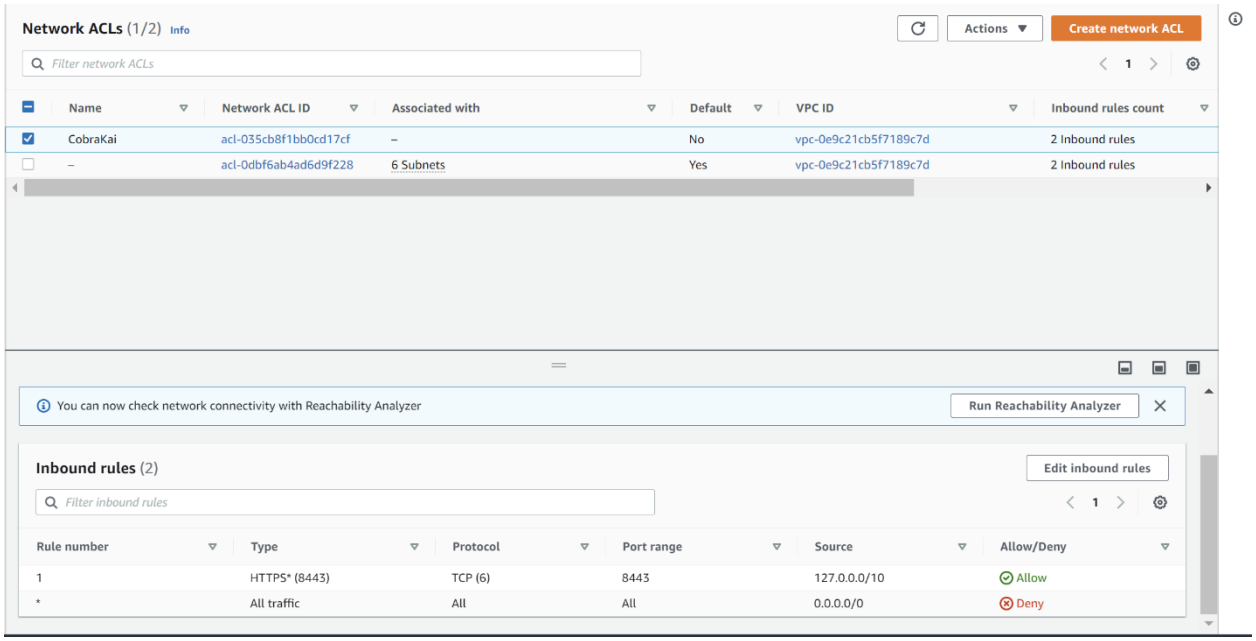
An access control list acts like a firewall at the network level for regulating traffic between subnets. We can configure network ACL's with rules that specify the requests that are allowed and the requests that are not allowed. Network Access Control List's are limited to 200 per. An Access Control List added to a network inside the VPC has a default deny.

Creating a NACL for the Cobra Kai application will reduce the overhead to network administrators since NACL is applied at the subnet level which means that any resource residing within the subnet will have the NACL applied.

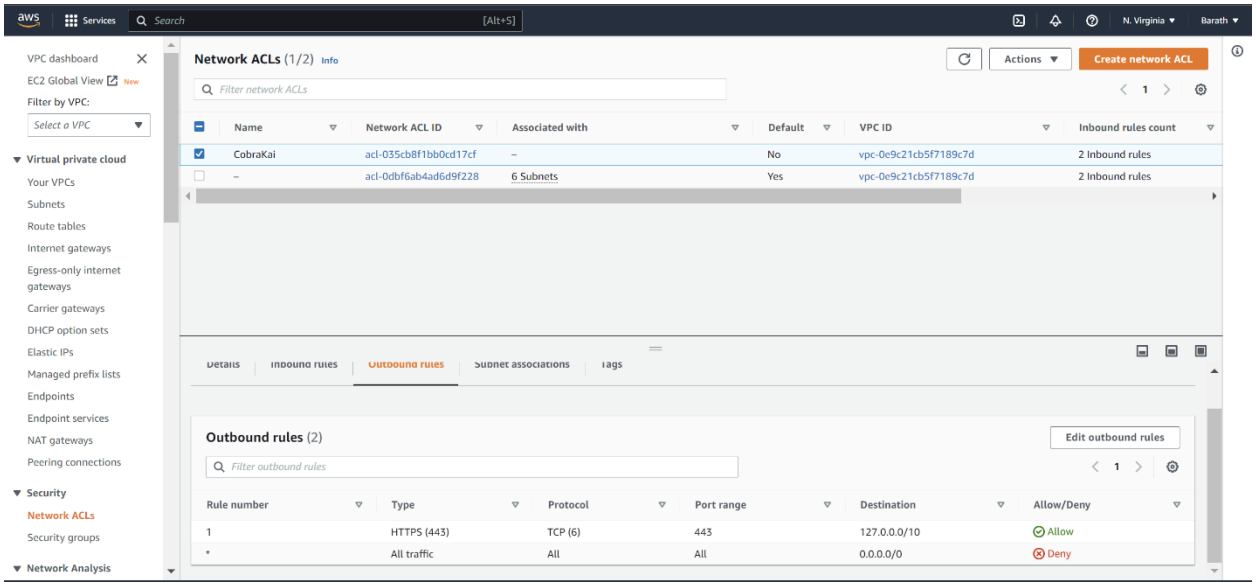

aws
Services
Search
[Alt+S]
N. Virginia
Barath
VPC dashboard
EC2 Global View
New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
Network Analysis
Network ACLs (1/2) Info
Actions
Create network ACL
Filter network ACLs
Name
Network ACL ID
Associated with
Default
VPC ID
Inbound rules count
CobraKai
acl-035cb8f1bb0cd17cf
–
No
vpc-0e9c21cb5f7189c7d
1 Inbound rule
–
acl-0dbf6ab4ad6d9f228
6 Subnets
Yes
vpc-0e9c21cb5f7189c7d
2 Inbound rules
Details
Inbound rules
Outbound rules
Subnet associations
Tags
Details
Network ACL ID
acl-035cb8f1bb0cd17cf
Associated with
–
Default
No
VPC ID
vpc-0e9c21cb5f7189c7d
Owner
157291859731


aws
Services
Search
[Alt+S]
N. Virginia
Barath
VPC > Network ACLs > Create network ACL
Create network ACL Info
A network ACL is an optional layer of security that acts as a firewall for controlling traffic in and out of a subnet.
Network ACL settings
Name - optional
Creates a tag with a key of 'Name' and a value that you specify.
CobraKai
VPC
VPC to use for this network ACL.
vpc-0e9c21cb5f7189c7d
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
CobraKai
Remove
Add new tag
You can add 49 more tags.
Cancel
Create network ACL

## Network ACL with inbound rules



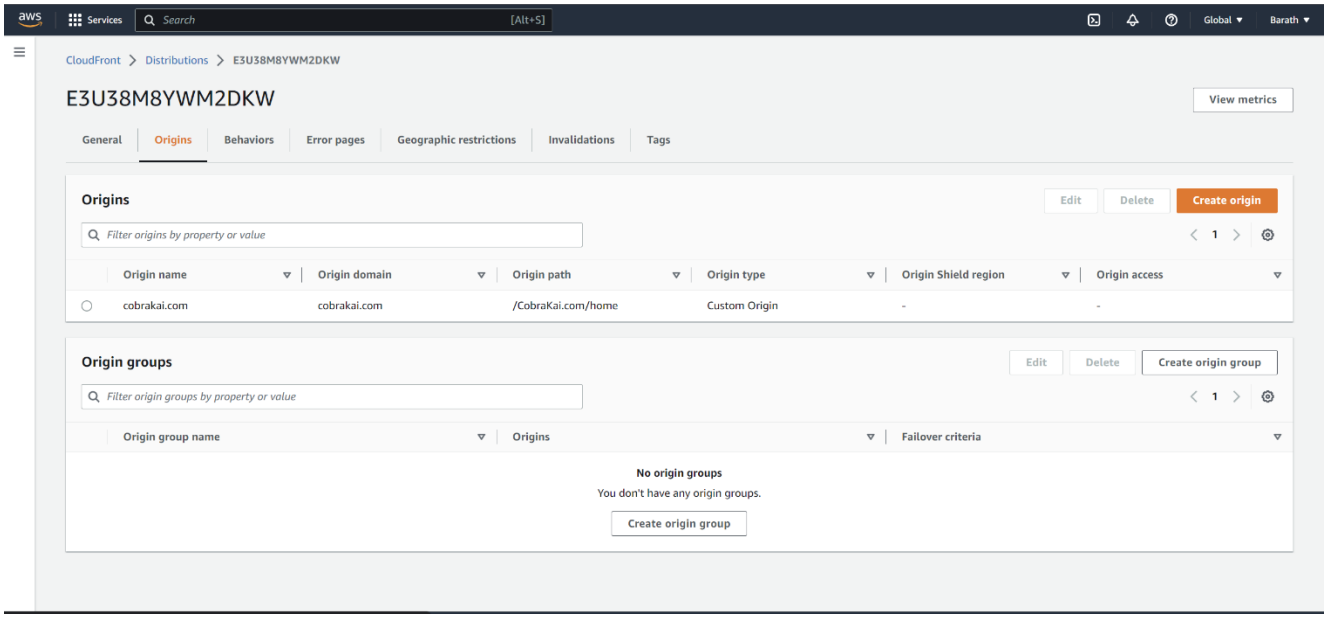

## Network ACL with outbound rules



## 5.4 AWS CloudFront

**CloudFront** is a content delivery network (CDN) that helps us to cache the content at "edge locations" all over the world. Users  can access content more quickly and DDoS(Distributed Denial of Service) attacks are protected by this. Applications, data, videos, APIs, and CloudFront are all options. Hackers are kept at bay without affecting application availability or performance thanks to a large amount of network bandwidth and security tools.

The Cobra Kai application's content can be cached at **edge locations** so that it can be served to users quickly without having to request the actual server for information. This significantly reduces latency and contributes to improved application performance.




## 5.5 IAM (Identity and Access Management)

It is a service that allows us to control access to AWS resources. The benefits of using IAM are as follows.

1. Granular permissions.
2. Secure access to AWS resources
3. Multi-factor Authentication
4. Identity Federation

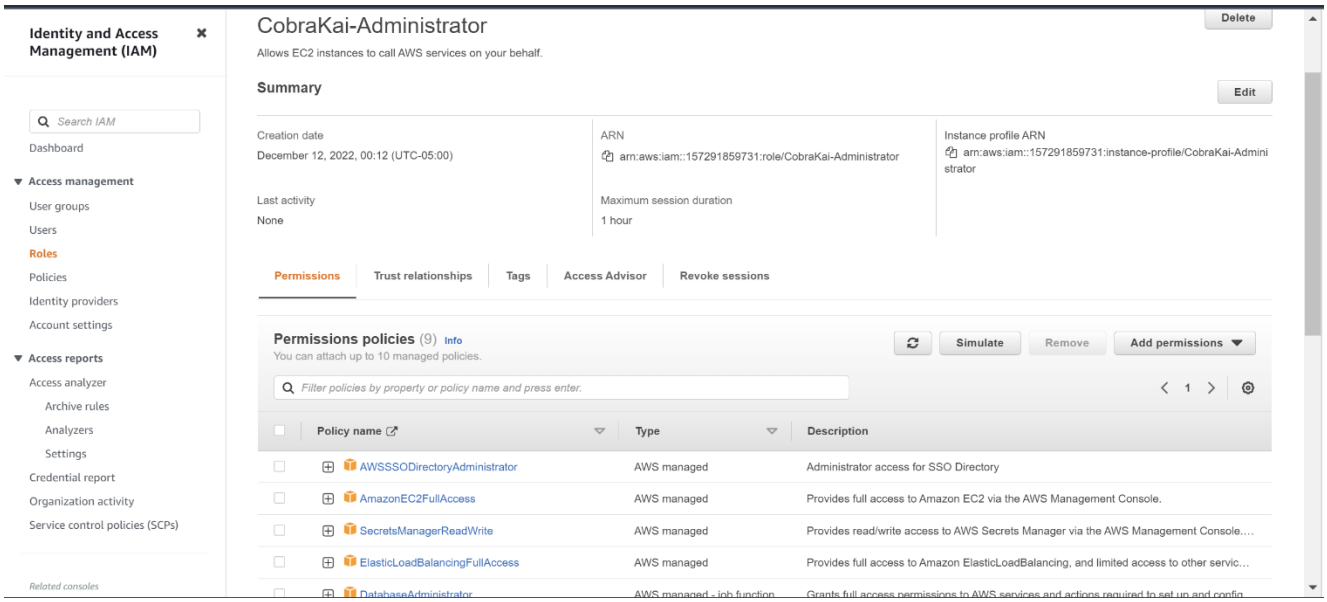
5. PCI DSS Compliance

6.Integration with other AWS services

### 5.5.1 Roles

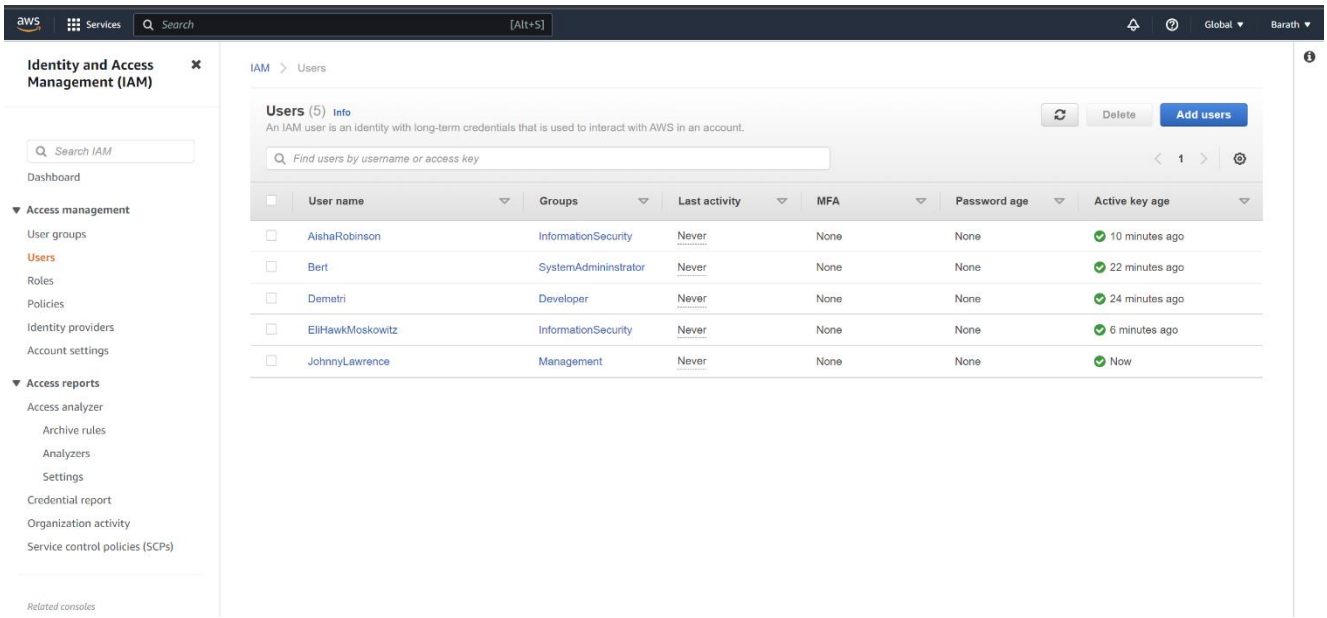
A role is an identity that we can configure in our AWS account to have specific permissions. A role is an AWS identity that contains permission policies that determine the privileges of the users who assume that specific role. An IAM role can be used to grant to users and services. We can implement Role-Based-Access-Control in CobraKai application to make sure that only authorized users can access the resources.

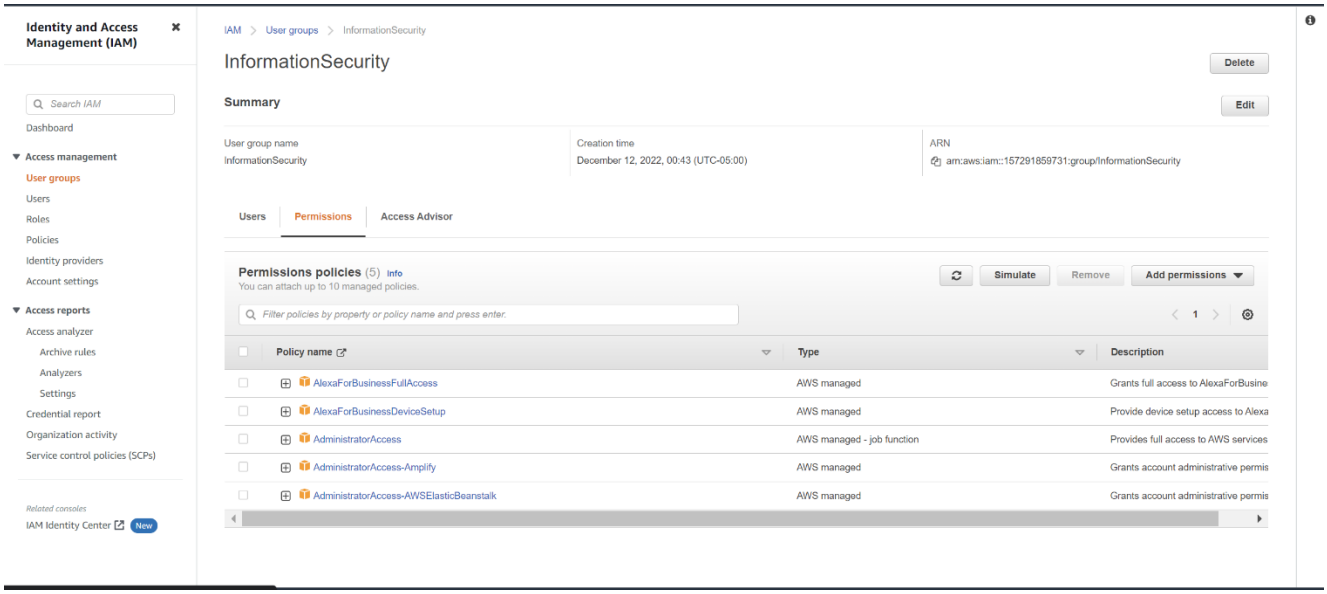
### Creation of role for CobraKai-Administrator



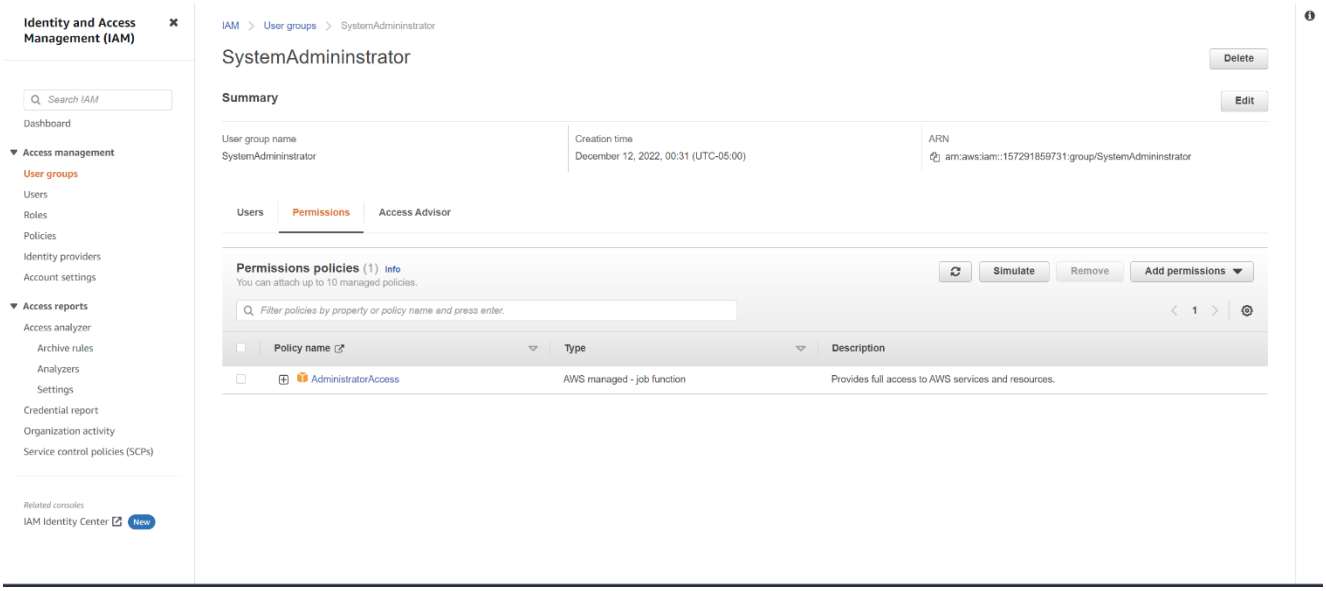
### 5.5.2 IAM Users and Groups

They are identities with permanent credentials. A group is a collection of users which allows us give permissions for several users who are part of the same IAM group.

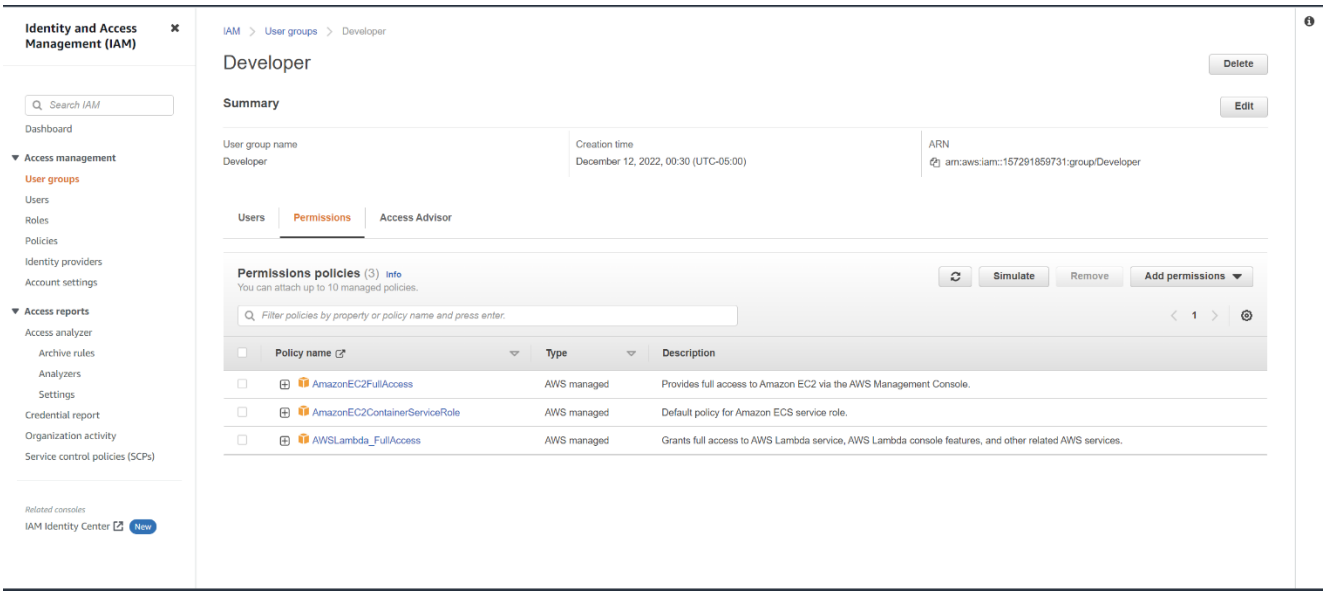


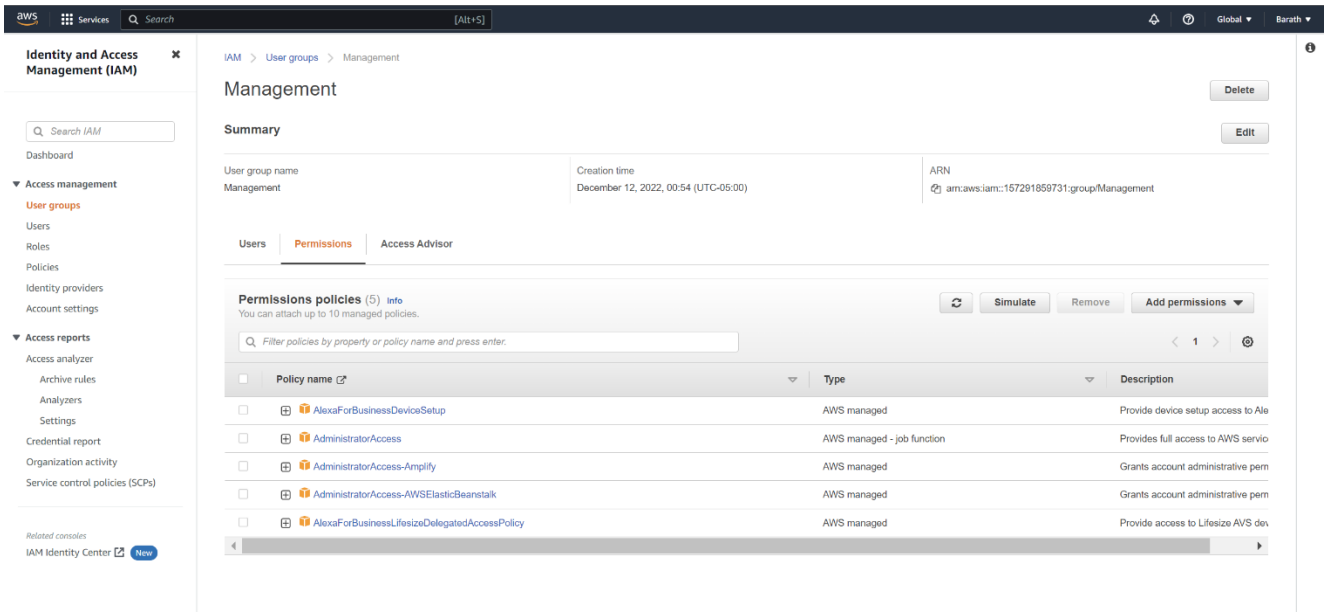
## Creation of user group named System Administrator




## Creation of user group named Developer



**Creation of user group named Management**




## 5.6 Security Groups

A Security group acts like a virtual firewall at the instance level for control inbound and outbound traffic. We can define rules to regulate the incoming the incoming and outgoing traffic. A default security group is always attached whenever we create a new EC2 instance. Security groups form the first layer of defense since it provides security at the instance level. The rules defined in the security group are made up of four primary components. They are

1. Rule

It allows for the selection of protocols such as TCP, UDP,SSH,HTTPS etc.

2.Protocols

This defines the type of protocol that the users can use to access the resource such as SMTP,HTTPS etc.

3.Port Range

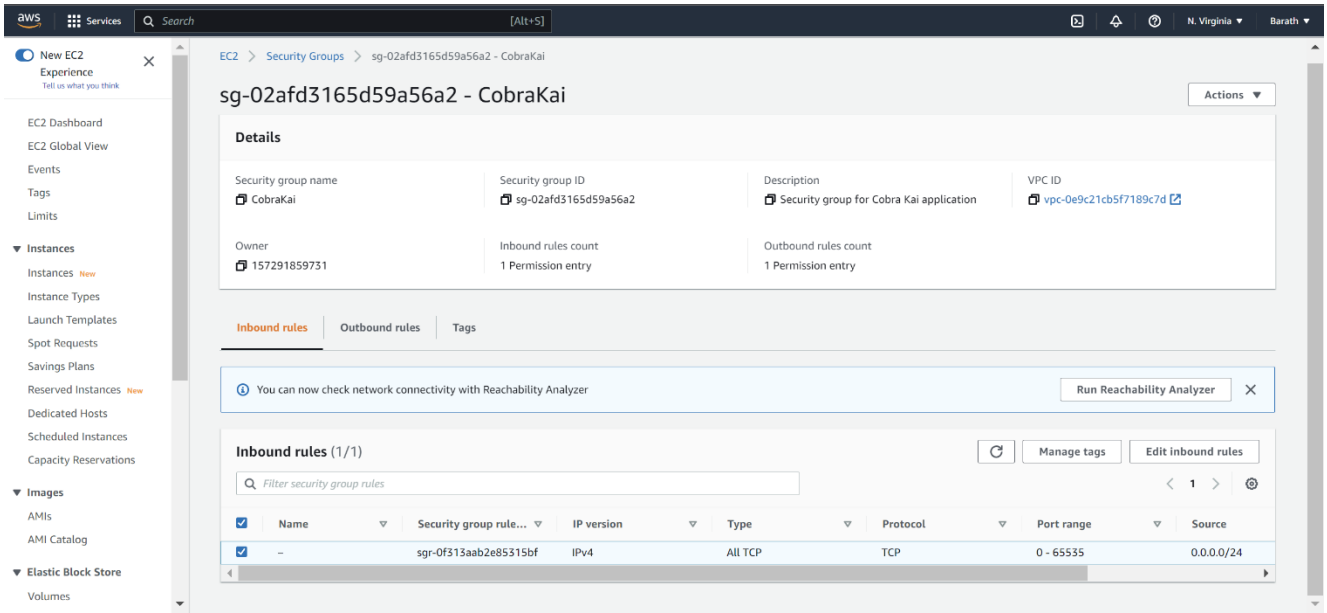
This can be used if we have to use a port number in the custom range.

4.Source

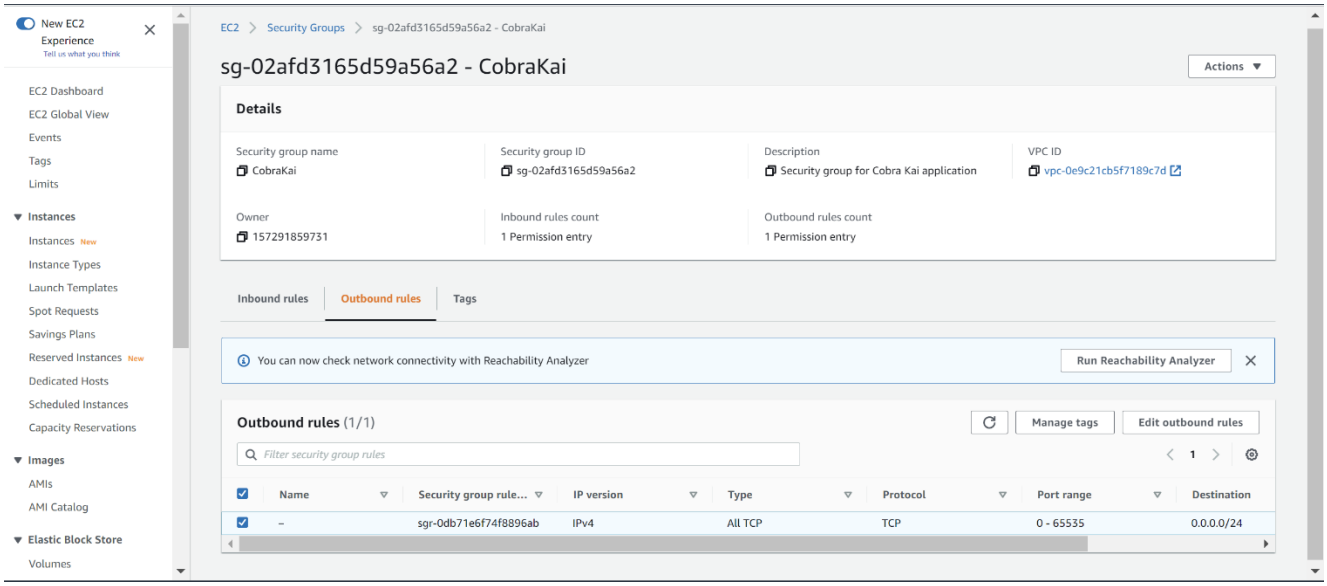
The IP address range of the machine from where the packet originated.

The EC2 instances maintained for the CobraKai application should be configured with a security group since security group rules are evaluated according to a **default deny everything unless allowed** policy. This means that if there is no ALLOW for a specific traffic then it will be blocked. Security groups helps us to implement security at the instance level ensuring that the instances are safeguarded from attacks.

### Creation of Security Group named CobraKai with Inbound rules




### Security Group configured with outbound rules



## 5.7 DDOS Protection

**AWS Shield** is a DDoS protection service that protects applications running on AWS. It has the following functions.

1. Detects and mitigates sophisticated network-level DDoS attacks. It minimizes application downtime and latency.

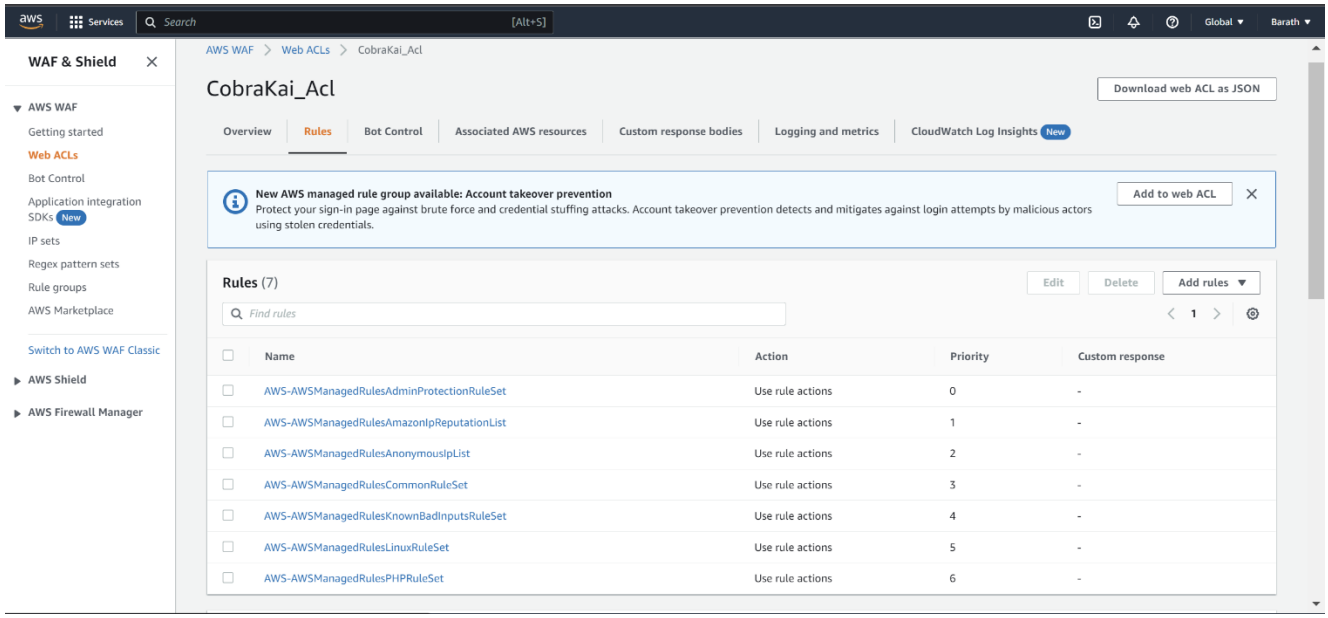
2. Provides application level security against DDoS by integrating with Shield Response Team (SRT) protocol or Web Application firewall.

Moving the Cobra Kai application to the cloud could prevent it from getting affected from a **DDOS attack**(Distributed Denial of service) since we can scale resources(EC2 instances) when there is a sudden increase in the number of requests and also investigate the attack source thus ensuring that the application is available to the users minimizing downtime

## 5.8 AWS WAF(Web-Application Firewall)

WAF is a firewall which helps us to protect web applications  by constantly filtering HTTP and HTTPS requests between the application and the internet. It helps in mitigating attacks such as cross-site-scripting, SQL injection and cross-site-request-forgery.

By implementing a WAF for the CobraKai application we can prevent the application from attacks such as cross-site-scripting(XSS), SQL injection and Cross-site-request-forgery.

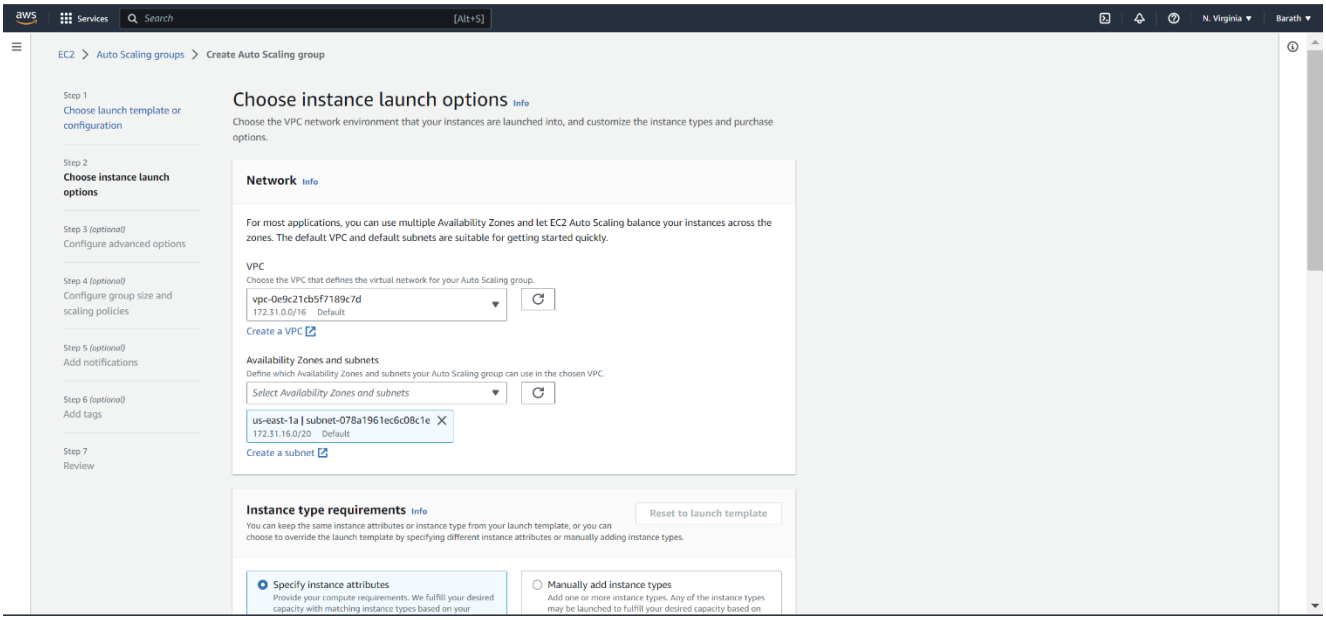


## 5.9 Scalability

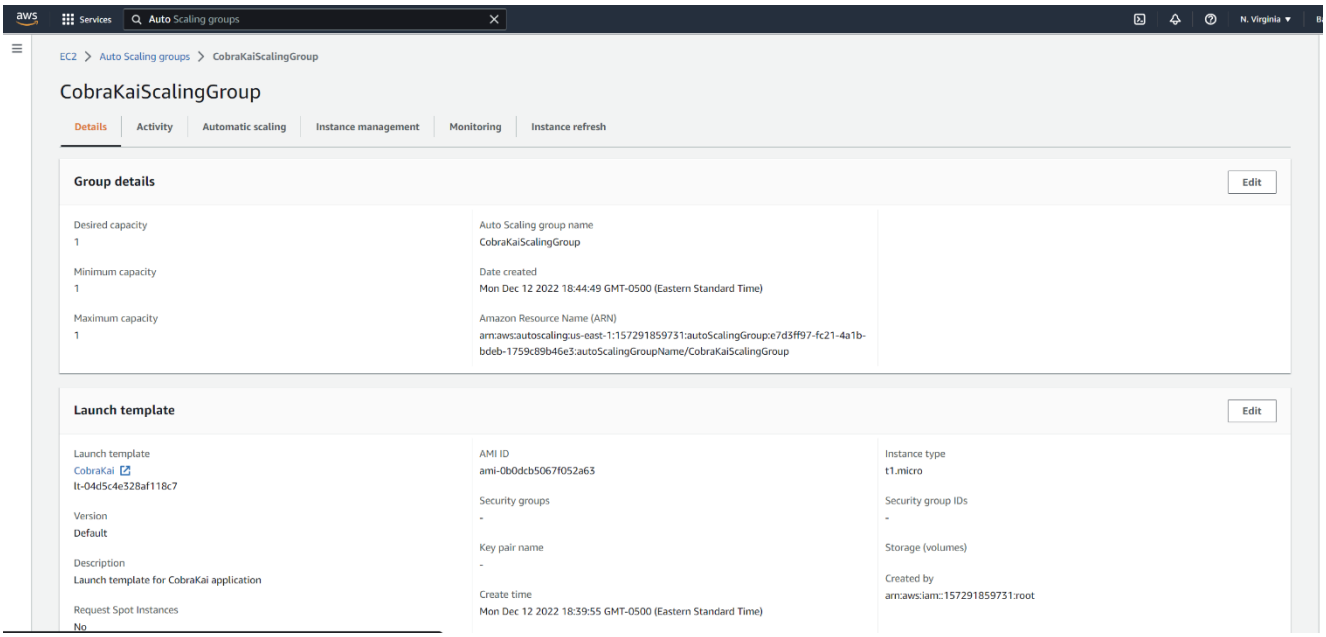
### 5.9.1 Amazon AutoScaling Group

The EC2 instances that will be used by the CobraKai application can be placed under an AutoScaling Group to spin up as many instances as required whenever there is a rise in demand. We can also implement group by deploying sufficient instances to meet the desired capacity so that  maintains a fixed number of instances even if an instance becomes unhealthy. If an instance is found unhealthy the auto scaling group then terminates the unhealthy instance and launches a new instance as replacement.

**Configuration of Auto Scaling Group**



**Creation of Auto Scaling Group**

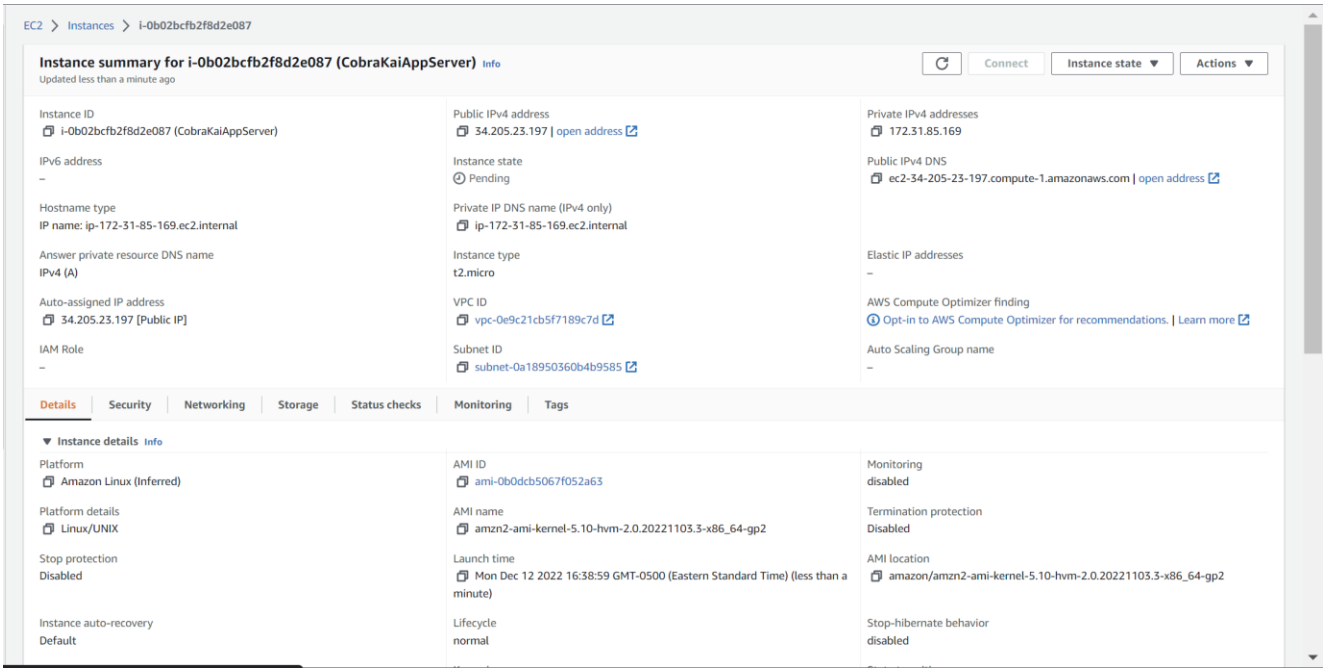



## 5.10 AWS Elastic Compute Cloud(EC2)

EC2 provides scalable computing in the cloud. It helps us to eliminate the need to invest in hardware up front which aids in faster application deployment. EC2 provides the following features.

- Virtual machines known as instances.
- Amazon Machine Images (Preconfigured templates) that packages the resources like Operating System, Kernel , Virtual Network Adapter etc.
- IPv4 address for scalable cloud computing know as Elastic IP addresses.
- Additional information can be stored in tags and assigned to EC2 instances.
- The users of EC2 can create virtual networks that are isolated from the rest of the cloud.

### EC2 instance for CobraKai application




## 5.11 Monitoring and Logging services

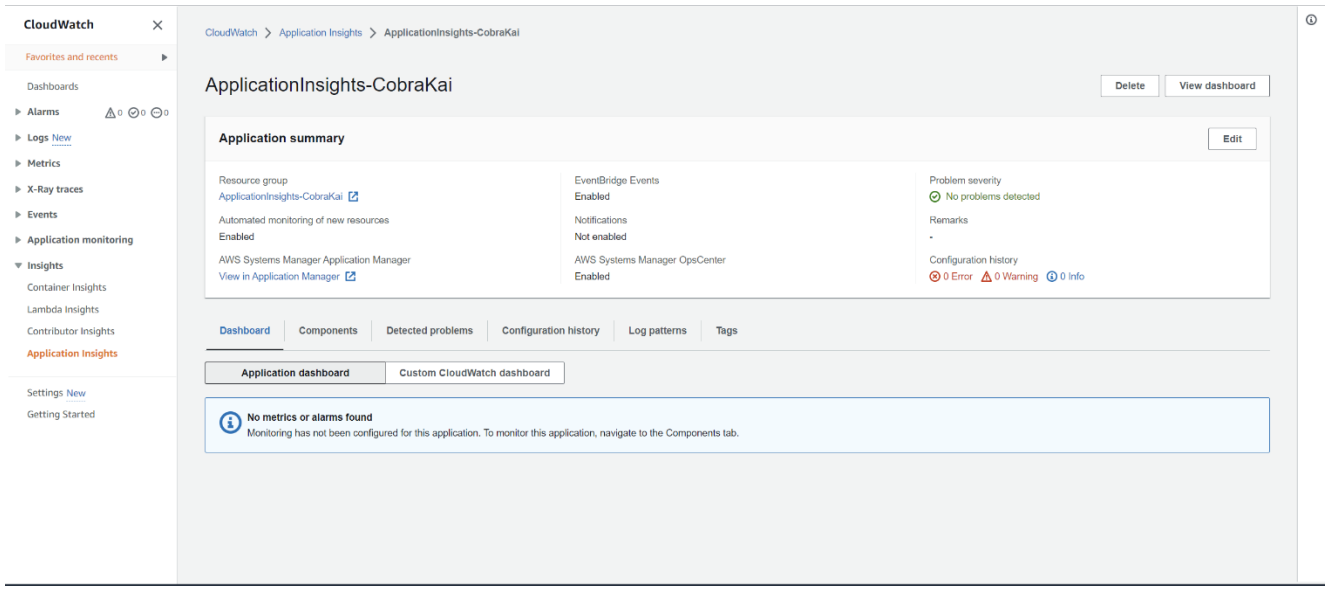
### AWS Inspector

It is a monitoring service that continuously looks for vulnerabilities in our environment. It can discover and scans EC2 instances for known vulnerabilities.

### AWS CloudWatch

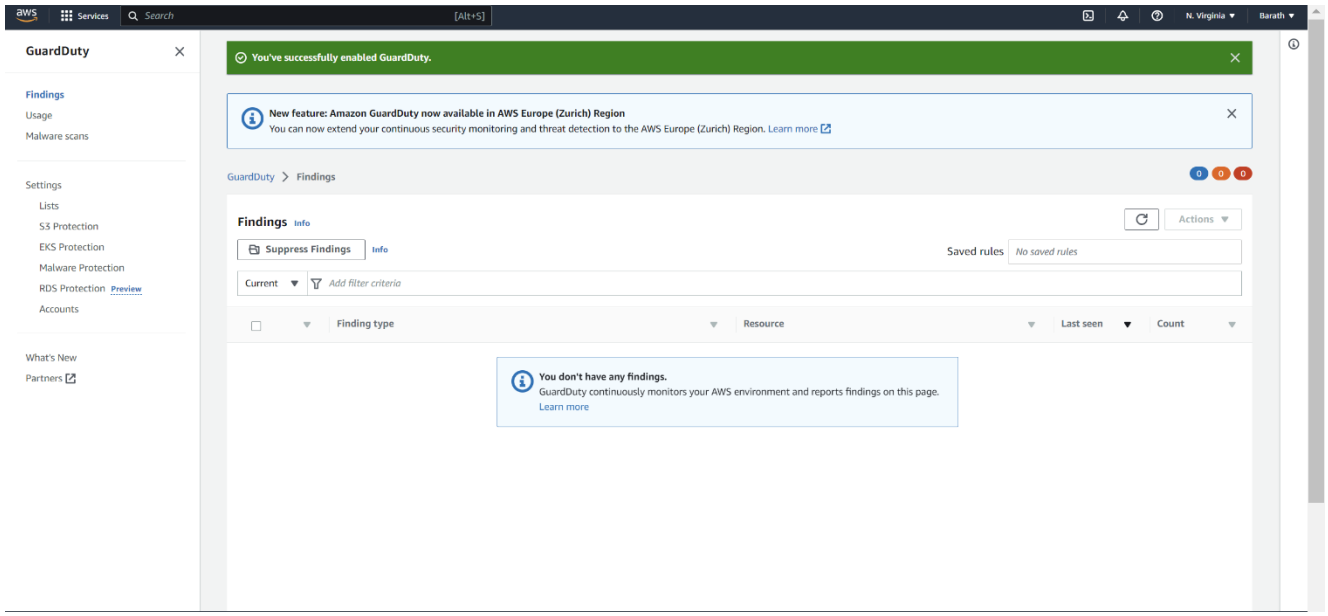
It is a real time monitoring service that checks resources and applications that run on the cloud in real time. It can collect and keep track of metrics that are user defined  for resources.

## CloudWatch ApplicationInsights




## AWS GuardDuty

Amazon GuardDuty is a security monitoring service that analyzes and processes data sources, such as AWS CloudTrail data events for Amazon S3 logs, Amazon VPC flow logs and RDS login activity. GuardDuty informs the status of AWS environment by producing security findings that can be viewed in the GuardDuty console or Amazon CloudWatch events.




## 5.11 Protecting data

Amazon Macie is a fully managed service that uses machine learning and pattern matching to discover, monitor, and protect sensitive data by creating data discovery jobs.

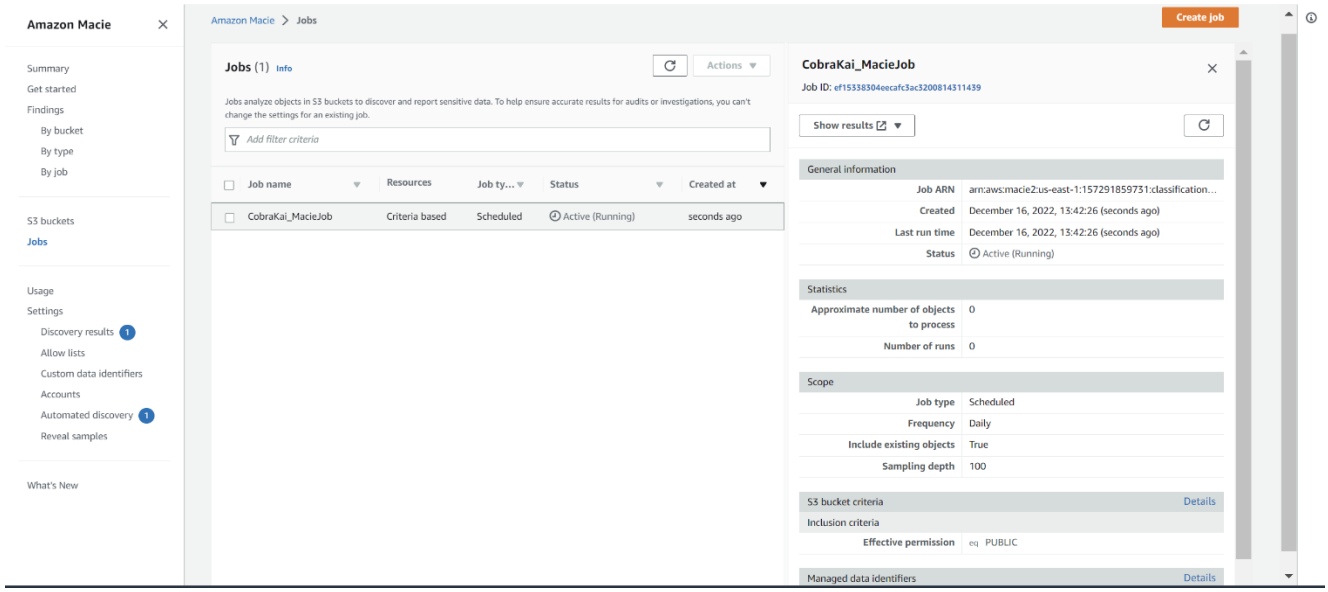
1. Macie automates reporting and discovery of important data by creating jobs.

2. Gain visibility of your stored data.

3. Receive alerts about unencrypted buckets, publicly accessible buckets.

4. Develop and manage resources programmatically – can be accessed using the Amazon Macie API.

By using Macie, we can detect possible issues with respect to security or privacy and rectify them. The findings can be analyzed in Macie or can be processed using services, applications and systems.




## 5.12 PCI DSS Compliance

Payments Card Industry Data Security Standard is a security standard administered by the PCI Security Standards Council. PCI DSS applies to entities that store, process or transmit cardholder information or sensitive authentication data.

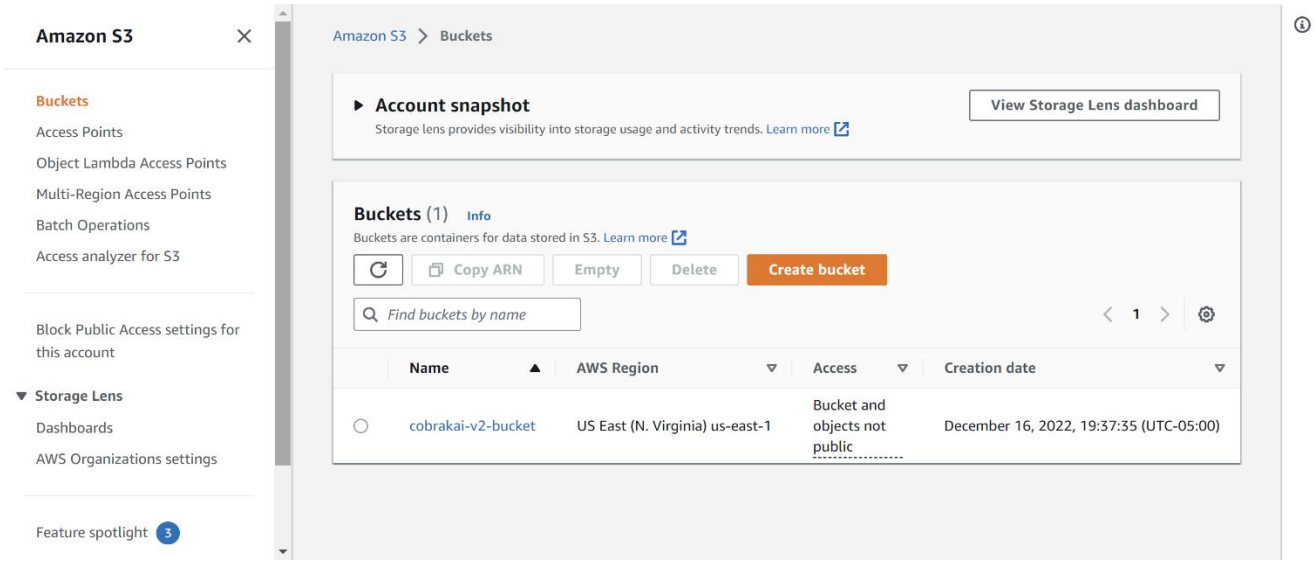
We can ensure that customer sensitive data can be handled appropriately by following these steps

1. Processing and protecting the credit card transactions by following secure transmission of data through the network and also following the principles of encryption at rest and encryption at transit.

2. Ensuing all systems are patched regularly to avoid vulnerabilities that persist in the older versions.

## 5.13 Amazon S3(Simple Storage Service)

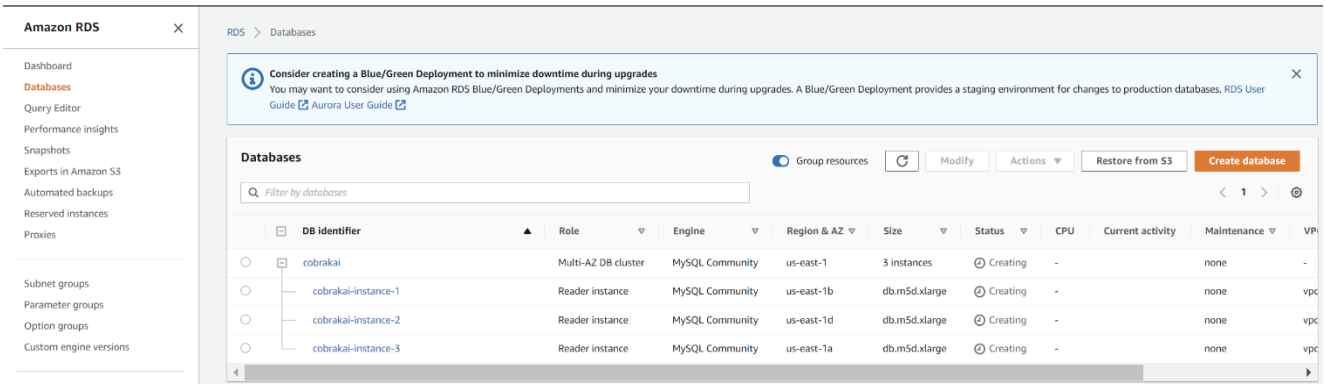
S3 is an object storage service that we can use to store the content required for CobraKai application. Storing media content in S3 buckets helps them to serve on-demand reliable streaming service.




## 5.14 Amazon Relational Database Service (RDS)

RDS is a  service that can be used to create, maintain and scale a relational database in the cloud. It provides secure and reliable database and takes care of administration tasks.

The tables required to run the CobraKai application can be created in the RDS database which will help Database administrators to manage the databases effectively.

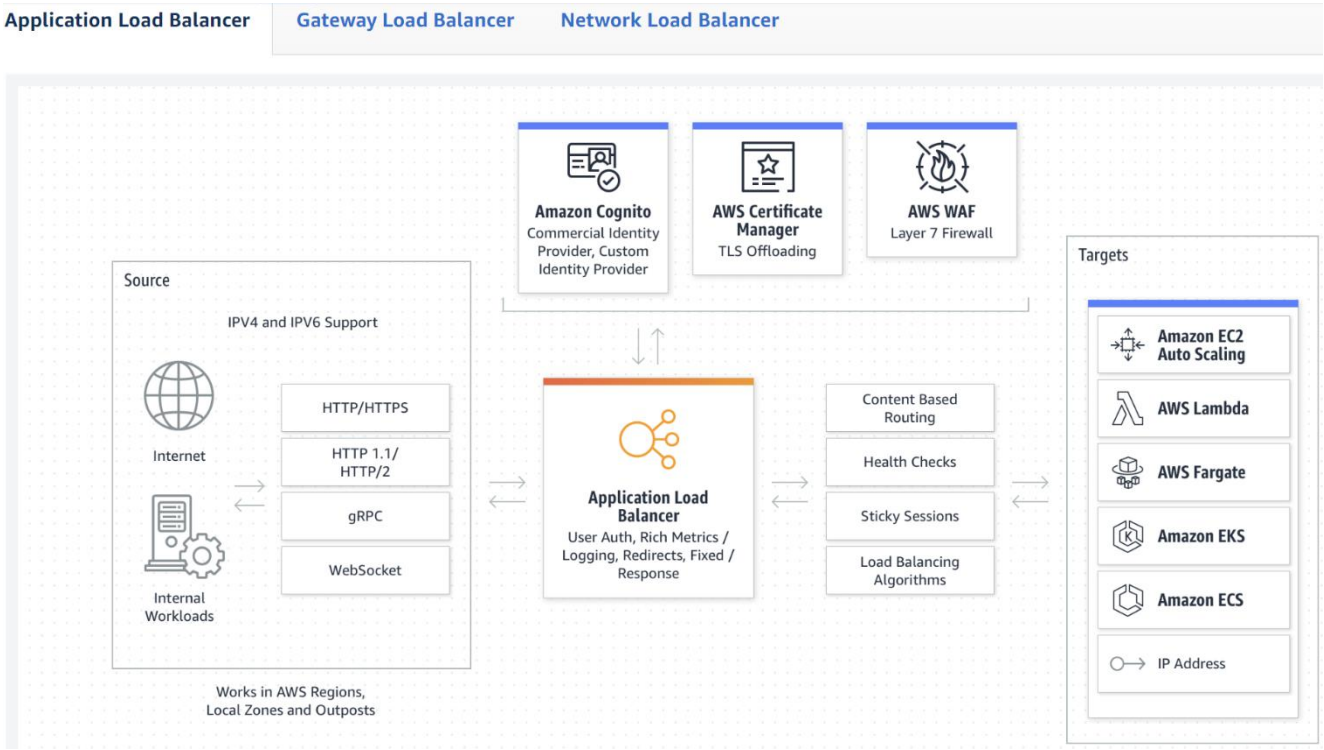



## 5.15 Amazon Elastic Load Balancer (ELB)

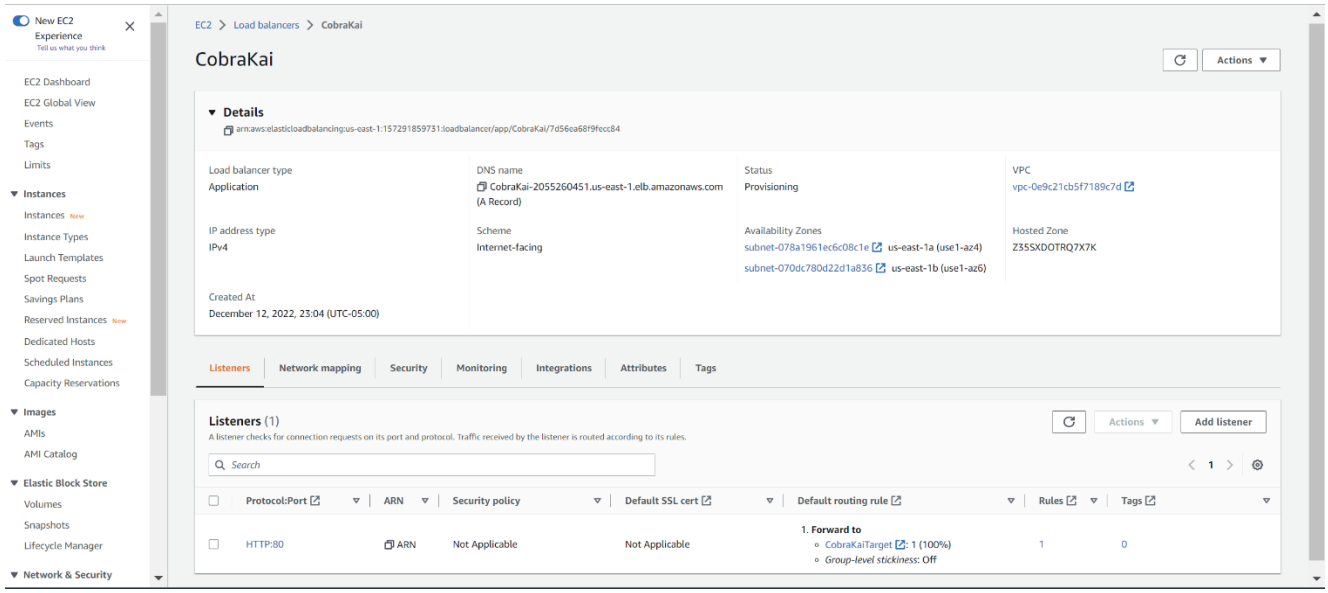
Load Balancer distributes traffic to several endpoints automatically into one or more Availability Zones.

Incoming requests to the CobraKai application can be handled by the LoadBalancer when there is sudden increase in traffic and the requests can be distributed to the resources that are available in the alternate Availability zone.

## Overview of Application Load Balancer




## Creation of Application Load Balancer




## 5.16 AWS CloudFormation

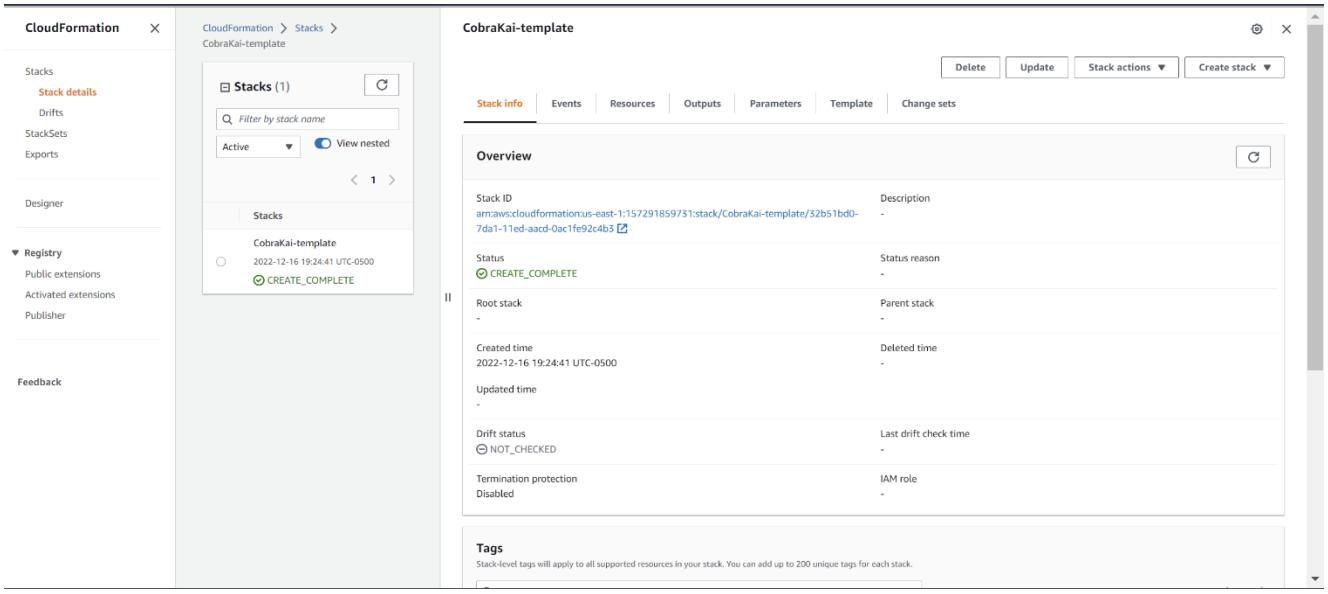
CloudFormation is a service that helps to deploy infrastructure using code so that we spend less time in the management of resources and more time on focusing on the application. We can create a template that specifies the required resources like EC2 instances, Amazon RDS instances and it will provision and configure the resources. The advantages of using CloudFormation templates are as follows:

1. Quickly replicate your infrastructure
2. Easily control and track changes to infrastructure

**Link to CloudFormation template file**

CloudFormationTemplate.pdf (Command Line)

## Creation of CloudFormation template




## 5.17 Patch Management

**AWS Patch Manager** provides an automatic patch management solution for security related patches as well other types of updates. It gives us the option of scanning our managed resources and report compliance. It also integrates with other services to provide a secure patching experience.

By moving the Cobra Kai application to the cloud, we can automate the process of patching by using the Patch Manager available in AWS. By automating patching we can mitigate the risk of running our application on unpatched systems thereby avoiding security vulnerabilities

**List of References**


https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/Welcome.html

https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/hosted-zones-working-with.html

https://docs.aws.amazon.com/managedservices/latest/userguide/restrict-nacl.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-security-groups.html

https://aviatrix.com/learn-center/cloud-security/aws-security-groups/

https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html

https://docs.aws.amazon.com/waf/latest/developerguide/fms-chapter.html

https://aws.amazon.com/iam/faqs/

https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-groups.html

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html

https://umd.instructure.com/courses/1334609/pages/week-seven-aws-overview

https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Welcome.html

https://aws.amazon.com/elasticloadbalancing/

https://kevwells.com/it-knowledge-base/aws-nacls-network-access-control-lists/

https://docs.aws.amazon.com/guardduty/latest/ug/what-is-guardduty.html

https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html

https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html

https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/distribution-web-awswaf.html

https://docs.aws.amazon.com/macie/latest/user/macie-suspend-disable.html

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/Welcome.html

https://aws.amazon.com/compliance/pci-dss-level-1-faqs/

https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/