

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.

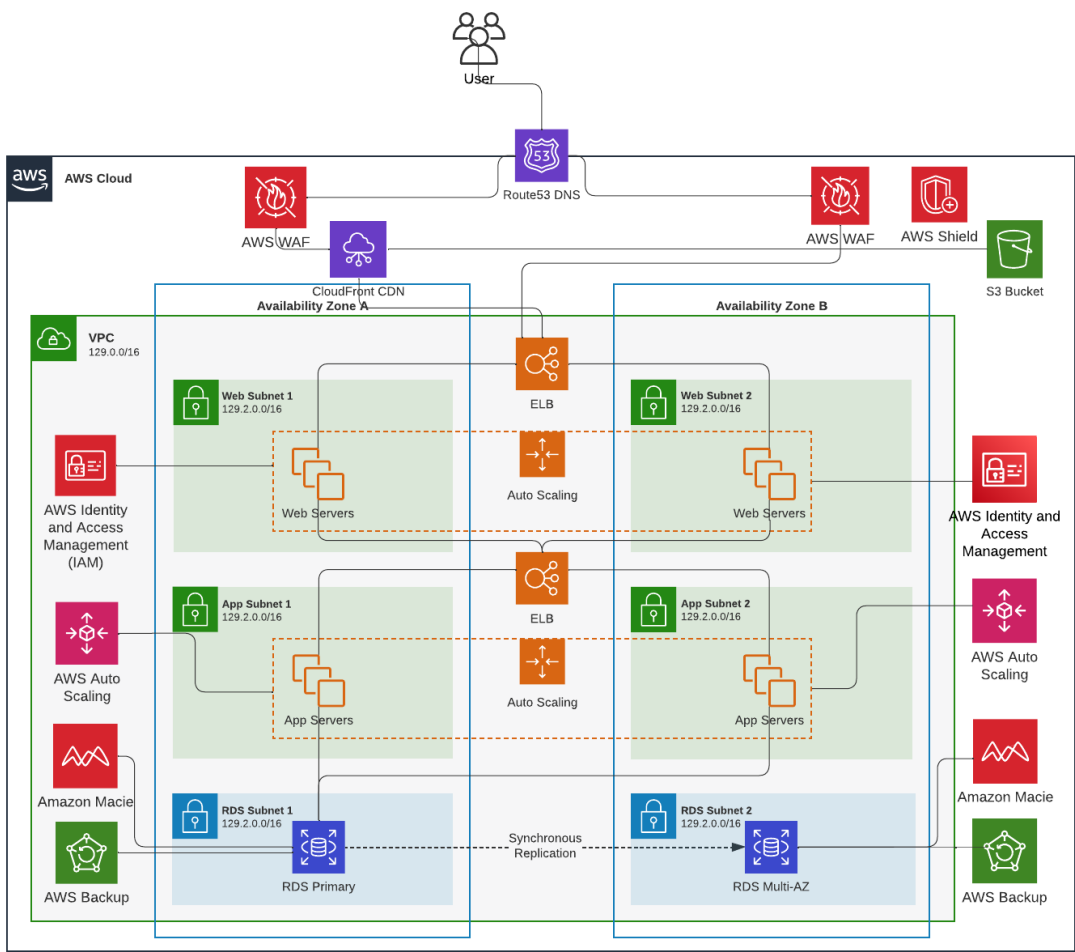
2.0 Issues in Current Architecture

- 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.

VPC > Your VPCs > vpc-0a46b8d768f6c0280

vpc-0a46b8d768f6c0280 / CobraKai-vpc

Actions

DetailsInfo

VPC ID

vpc-0a46b8d768f6c0280

Tenancy

Default

Default VPC

No

Network Address Usage metrics

Disabled

State

Available

DHCP option set

dopt-0732041f0176a2cea

IPv4 CIDR

10.0.0.0/24

Route 53 Resolver DNS Firewall rule groups

-

DNS hostnames

Disabled

Main route table

rtb-0af96dbcce98d6bec

IPv6 pool

-

Owner ID

157291859731

DNS resolution

Enabled

Main network ACL

acl-08acf5b64c7a416e1

IPv6 CIDR (Network border group)

-

CIDRsFlow logsTags

CIDRsInfo

Address type	CIDR	Network Border Group	Pool	Status
IPv4	10.0.0.0/24	-	-	Associated

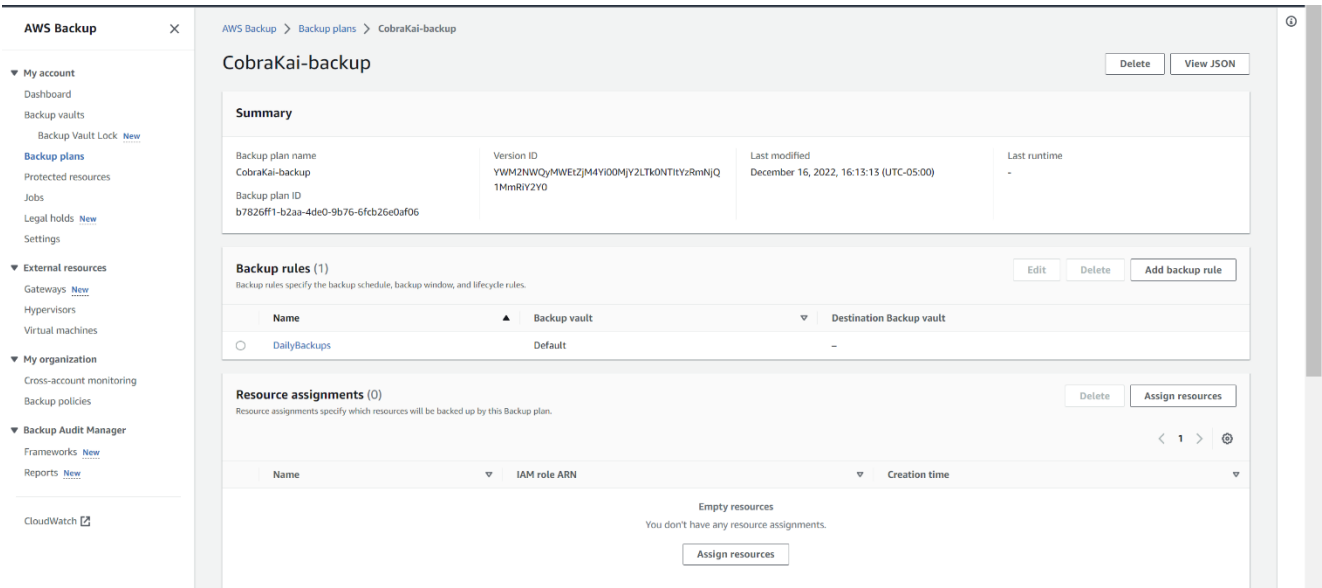
5.1 Backup and recovery

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.

Choose a domain name

.com - \$12.00

Check

Availability for 'mediacobrakai.com'

Domain Name	Status	Price /1 Year	Action
mediacobrakai.com	Available	\$12.00	Add to cart

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.

Create record [Info](#)

Quick create record

Switch to wizard

▼ Record 1

Delete

Record name [Info](#)

Record type [Info](#)

A – Routes traffic to an IPv4 address and some AWS resources

Keep blank to create a record for the root domain.

☒ Alias

Value [Info](#)

192.0.2.235

Enter multiple values on separate lines.

TTL (seconds) [Info](#)

Routing policy [Info](#)

1m
1h
1d

Simple routing

Recommended values: 60 to 172800 (two days)

Add another record

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.

The screenshot displays the AWS Route 53 console interface. At the top, under 'Hosted zones (1)', there's a search bar and buttons for 'View details', 'Edit', 'Delete', and 'Create hosted zone'. Below this is a table with columns: Domain name, Type, Created by, Record count, Description, and Hosted zone ID. A single entry is shown for 'media.cobrakai.com' with Type 'Public', Created by 'Route 53', Record count '2', and Hosted zone ID 'Z06439371TYFJ10...'. A green banner below the table states 'media.CobraKai.com was successfully created.' and provides instructions on creating records. The 'Hosted zone details' section shows the domain 'media.cobrakai.com' as 'Public' with buttons for 'Delete zone', 'Test record', and 'Configure query logging'. The 'Records (2)' section is active, showing a table with columns: Record name, Type, Routing policy, Differ..., and Value/Route traffic to. Two records are listed: one for 'media.cobrakai.com' with Type 'NS' and Routing policy 'Simple', and another for 'media.cobrakai.com' with Type 'CAA' and Routing policy 'Simple'. The 'Value/Route traffic to' column for the NS record lists four nameservers: ns-1667.awsdns-16.co.uk, ns-957.awsdns-55.net, ns-29.awsdns-03.com, and ns-1236.awsdns-26.org.

Record name	Type	Routing policy	Differ...	Value/Route traffic to
media.cobrakai.com	NS	Simple	-	ns-1667.awsdns-16.co.uk. ns-957.awsdns-55.net. ns-29.awsdns-03.com. ns-1236.awsdns-26.org.
media.cobrakai.com	CAA	Simple	-	ns-1667.awsdns-16.co.uk, awsdns-hostmaster.amazon.com.

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

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)

Filter network ACLs

< 1 >

Actions

Create network ACL

	Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
<input checked="" type="checkbox"/>	CobraKai	acl-035cb8f1bb0cd17cf	-	No	vpc-0e9c21cb5f7189c7d	1 Inbound rule
<input type="checkbox"/>	-	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

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

Q Name

Value - optional

Q CobraKai

Remove

Add new tag

You can add 49 more tags.

Cancel

Create network ACL

Network ACL with inbound rules

Network ACLs (1/2) Info

Filter network ACLs

< 1 >

	Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
<input checked="" type="checkbox"/>	CobraKai	acl-035cb8f1bb0cd17cf	-	No	vpc-0e9c21cb5f7189c7d	2 Inbound rules
<input type="checkbox"/>	-	acl-0dbf6ab4ad6d9f228	6 Subnets	Yes	vpc-0e9c21cb5f7189c7d	2 Inbound rules

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Inbound rules (2)

Filter inbound rules

< 1 >

Rule number	Type	Protocol	Port range	Source	Allow/Deny
1	HTTPS* (8443)	TCP (6)	8443	127.0.0.0/10	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Network ACL with outbound rules

aws Services Search [Alt+S]

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

Network Analysis

Network ACLs (1/2) Info

Filter network ACLs

< 1 >

	Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
<input checked="" type="checkbox"/>	CobraKai	acl-035cb8f1bb0cd17cf	-	No	vpc-0e9c21cb5f7189c7d	2 Inbound rules
<input type="checkbox"/>	-	acl-0dbf6ab4ad6d9f228	6 Subnets	Yes	vpc-0e9c21cb5f7189c7d	2 Inbound rules

Details

Inbound rules

Outbound rules

Subnet associations

Tags

Outbound rules (2)

Filter outbound rules

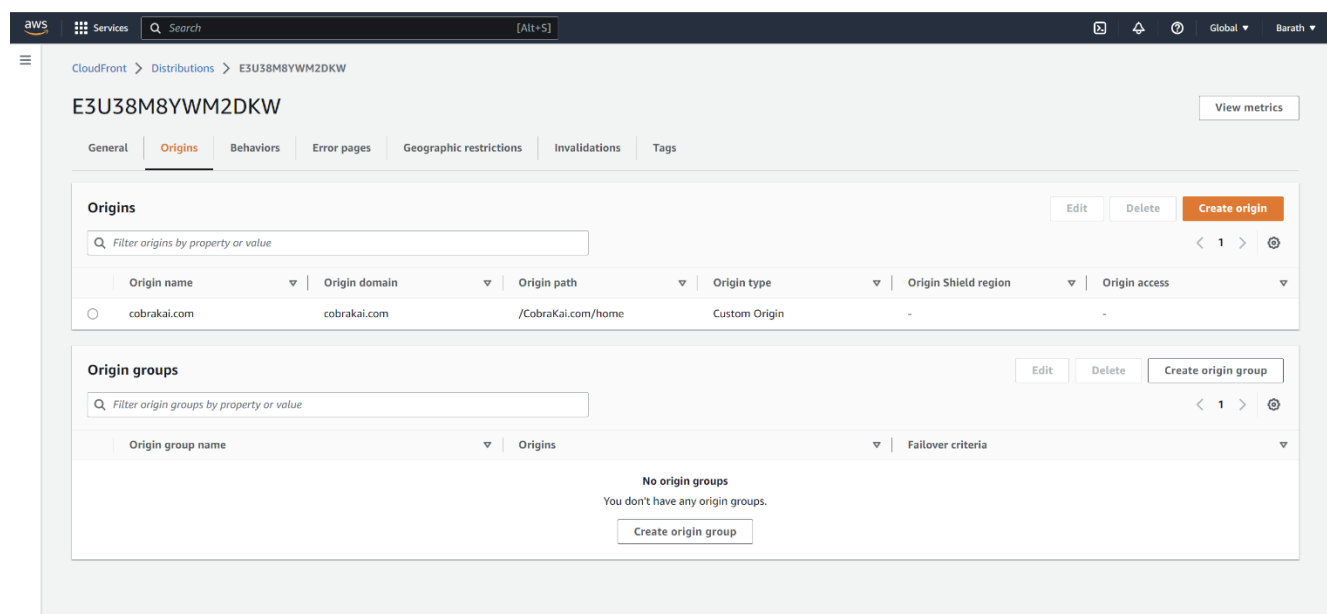
< 1 >

Rule number	Type	Protocol	Port range	Destination	Allow/Deny
1	HTTPS (443)	TCP (6)	443	127.0.0.0/10	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

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

The screenshot displays the AWS IAM console interface for the 'CobraKai-Administrator' role. The left sidebar shows the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and Related consoles. The main content area is titled 'CobraKai-Administrator' and includes a description: 'Allows EC2 instances to call AWS services on your behalf.' Below this is a 'Summary' section with details such as Creation date (December 12, 2022, 00:12 UTC-05:00), ARN (arn:aws:iam::157291859731:role/CobraKai-Administrator), Instance profile ARN (arn:aws:iam::157291859731:instance-profile/CobraKai-Administrator), Last activity (None), and Maximum session duration (1 hour). The 'Permissions' tab is active, showing a list of 9 attached policies. The policies are:

Policy name	Type	Description
AWSSSODirectoryAdministrator	AWS managed	Administrator access for SSO Directory
AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS Management Console.
SecretsManagerReadWrite	AWS managed	Provides read/write access to AWS Secrets Manager via the AWS Management Console....
ElasticLoadBalancingFullAccess	AWS managed	Provides full access to Amazon ElasticLoadBalancing, and limited access to other servic...
DatabaseAdministrator	AWS managed - job function	Grants full access permissions to AWS services and actions required to set up and config...

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.

The screenshot displays the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services', a search bar, and a user profile 'Barath'. The left sidebar shows the 'Identity and Access Management (IAM)' menu with options like Dashboard, Access management, Access reports, and Related consoles. The main content area is divided into two sections.

Top Section: IAM > Users

This section shows a list of IAM users. The header indicates 'Users (5)' and provides a brief description: 'An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.' Below this is a search bar and a table of users.

<input type="checkbox"/>	User name	Groups	Last activity	MFA	Password age	Active key age
<input type="checkbox"/>	AishaRobinson	InformationSecurity	Never	None	None	10 minutes ago
<input type="checkbox"/>	Bert	SystemAdministrator	Never	None	None	22 minutes ago
<input type="checkbox"/>	Demetri	Developer	Never	None	None	24 minutes ago
<input type="checkbox"/>	EliHawkMoskowitz	InformationSecurity	Never	None	None	6 minutes ago
<input type="checkbox"/>	JohnnyLawrence	Management	Never	None	None	Now

Bottom Section: IAM > User groups > InformationSecurity

This section shows the details for the 'InformationSecurity' user group. It includes a 'Summary' tab with the following information:

- User group name: InformationSecurity
- Creation time: December 12, 2022, 00:43 (UTC-05:00)
- ARN: `arn:aws:iam:157291859731:group:InformationSecurity`

Below the summary is a 'Permissions' tab showing a list of permissions policies. The header indicates 'Permissions policies (5)' and provides a brief description: 'You can attach up to 10 managed policies.' Below this is a search bar and a table of policies.

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	AlexaForBusinessFullAccess	AWS managed	Grants full access to AlexaForBusine
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	AWS managed	Provide device setup access to Alexa
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	Provides full access to AWS services
<input type="checkbox"/>	AdministratorAccess-Amplify	AWS managed	Grants account administrative permis
<input type="checkbox"/>	AdministratorAccess-AWSElasticBeanstalk	AWS managed	Grants account administrative permis

Creation of user group named System Administrator

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analyzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Related consoles

IAM Identity Center

SystemAdministrator

Delete

Edit

Summary

User group name

Creation time

ARN

SystemAdministrator

December 12, 2022, 00:31 (UTC-05:00)

arn:aws:iam::157291859731:group/SystemAdministrator

Users

Permissions

Access Advisor

Permissions policies (1) info

You can attach up to 10 managed policies.

Filter policies by property or policy name and press enter.

< 1 >

	Policy name	Type	Description
<input type="checkbox"/>	AdministratorAccess	AWS managed - job function	Provides full access to AWS services and resources.

Creation of user group named Developer

Identity and Access Management (IAM)

Dashboard

Access management

User groups

Users

Roles

Policies

Identity providers

Account settings

Access reports

Access analyzer

Archive rules

Analzers

Settings

Credential report

Organization activity

Service control policies (SCPs)

Related consoles

IAM Identity Center

New

Developer

Delete

Edit

Summary

User group name

Developer

Creation time

December 12, 2022, 00:30 (UTC-05:00)

ARN

arn:aws:iam::157291859731:group/Developer

Users

Permissions

Access Advisor

Permissions policies (3)

Info

You can attach up to 10 managed policies.

↺

Simulate

Remove

Add permissions

Filter policies by property or policy name and press enter.

<

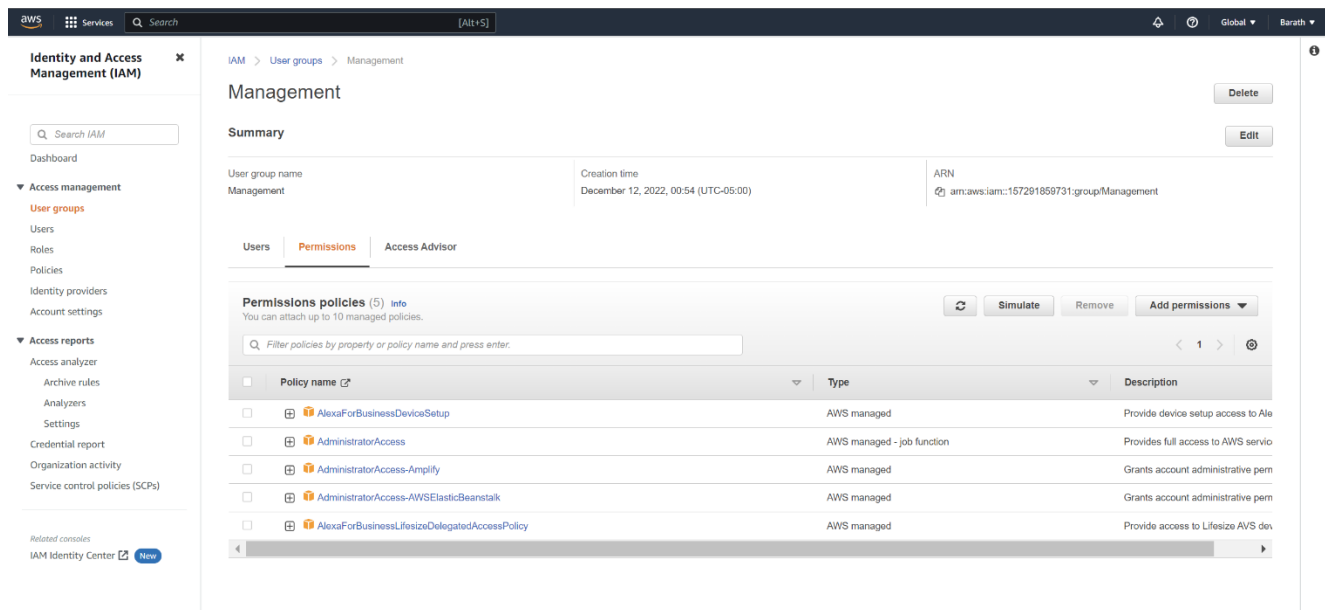
1

>

⌕

<input type="checkbox"/>	Policy name	Type	Description
<input type="checkbox"/>	AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via the AWS Management Console.
<input type="checkbox"/>	AmazonEC2ContainerServiceRole	AWS managed	Default policy for Amazon ECS service role.
<input type="checkbox"/>	AWSLambda_FullAccess	AWS managed	Grants full access to AWS Lambda service, AWS Lambda console features, and other related AWS services.

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 help 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

The screenshot shows the AWS Management Console interface for the security group **sg-02afd3165d59a56a2 - CobraKai**. The left sidebar contains navigation links for EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances, Images, and Elastic Block Store. The main content area displays the details of the security group, including its name, ID, description, VPC ID, owner, and rule counts. The **Inbound rules** tab is selected, showing a single rule with the following details:

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
-	sgr-0f313aab2e85315bf	IPv4	All TCP	TCP	0 - 65535	0.0.0.0/24

Security Group configured with outbound rules

The screenshot shows the AWS Management Console interface for the security group **sg-02afd3165d59a56a2 - CobraKai**. The left sidebar contains navigation links for EC2 Dashboard, EC2 Global View, Events, Tags, Limits, Instances, Images, and Elastic Block Store. The main content area displays the details of the security group, including its name, ID, description, VPC ID, owner, and rule counts. The **Outbound rules** tab is selected, showing a single rule with the following details:

Name	Security group rule...	IP version	Type	Protocol	Port range	Destination
-	sgr-0db71e6f74f8896ab	IPv4	All TCP	TCP	0 - 65535	0.0.0.0/24

5.7 DDoS Protection

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

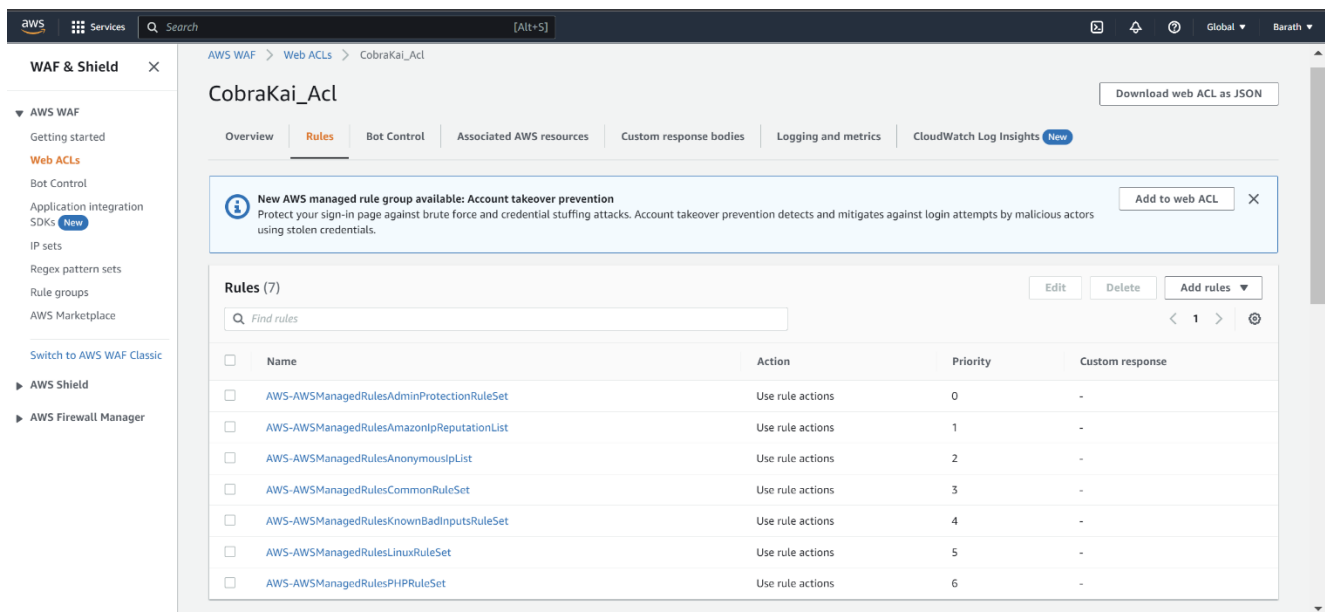
1. Detects and mitigates sophisticated network-level DDoS attacks. It minimizes application downtime and latency.
2. Provides application level security against DDoS by integrating with Shield Response Team (SRT) protocol or Web Application firewall.

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.



The screenshot shows the AWS WAF console interface for a Web ACL named 'CobraKai_Acl'. The left sidebar contains navigation options for WAF & Shield, including AWS WAF, Bot Control, and AWS Firewall Manager. The main content area shows the 'Rules' tab for the selected Web ACL. A notification banner at the top states: 'New AWS managed rule group available: Account takeover prevention'. Below this, a table lists 7 rules, all of which are AWS managed rule groups. The table has columns for Name, Action, Priority, and Custom response.

Name	Action	Priority	Custom response
AWS-AWSManagedRulesAdminProtectionRuleSet	Use rule actions	0	-
AWS-AWSManagedRulesAmazonIpReputationList	Use rule actions	1	-
AWS-AWSManagedRulesAnonymousIpList	Use rule actions	2	-
AWS-AWSManagedRulesCommonRuleSet	Use rule actions	3	-
AWS-AWSManagedRulesKnownBadInputsRuleSet	Use rule actions	4	-
AWS-AWSManagedRulesLinuxRuleSet	Use rule actions	5	-
AWS-AWSManagedRulesPHPRuleSet	Use rule actions	6	-

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

aws

Services

Search

[Alt+S]

N. Virginia

Barath

EC2 > Auto Scaling groups > Create Auto Scaling group

Step 1
Choose launch template or configuration

Step 2
Choose instance launch options

Step 3 (optional)
Configure advanced options

Step 4 (optional)
Configure group size and scaling policies

Step 5 (optional)
Add notifications

Step 6 (optional)
Add tags

Step 7
Review

Choose instance launch options

Choose the VPC network environment that your instances are launched into, and customize the instance types and purchase options.

Network

For most applications, you can use multiple Availability Zones and let EC2 Auto Scaling balance your instances across the zones. The default VPC and default subnets are suitable for getting started quickly.

VPC

Choose the VPC that defines the virtual network for your Auto Scaling group.

vpc-0e9c21cb5f7189c7d

172.31.0.0/16

Default

Create a VPC

Availability Zones and subnets

Define which Availability Zones and subnets your Auto Scaling group can use in the chosen VPC.

Select Availability Zones and subnets

us-east-1a | subnet-078a1961ec6c08c1e

172.31.16.0/20

Default

Create a subnet

Instance type requirements

You can keep the same instance attributes or instance type from your launch template, or you can choose to override the launch template by specifying different instance attributes or manually adding instance types.

Specify instance attributes

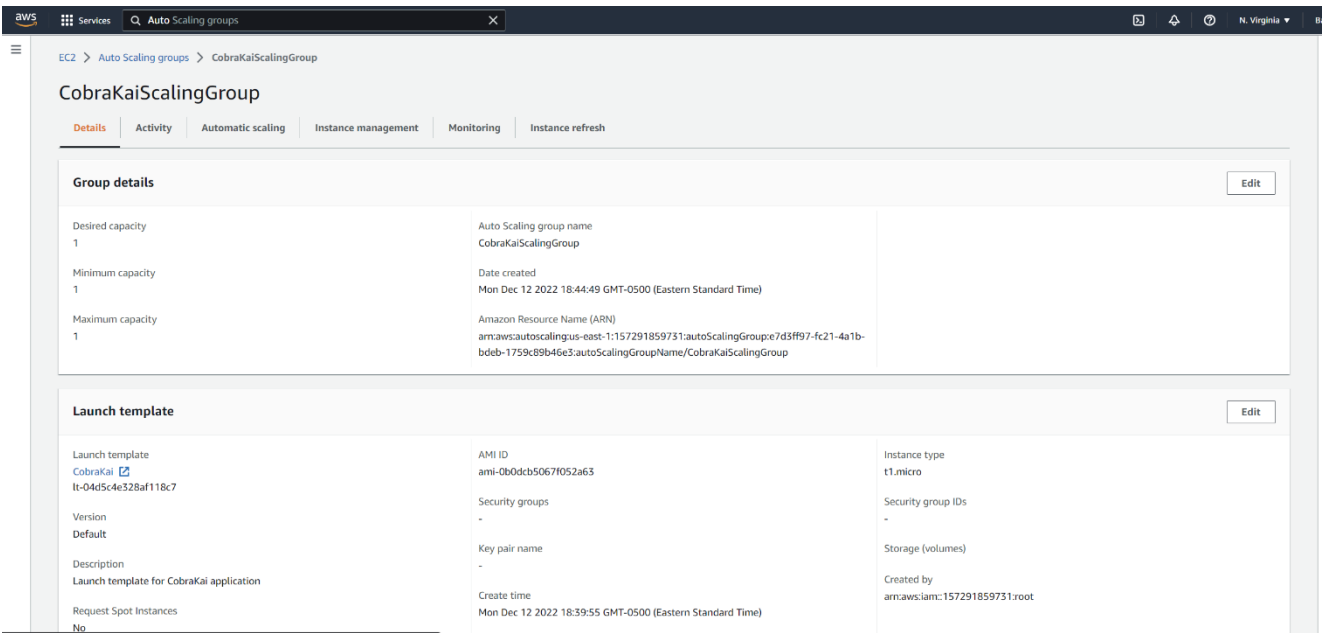
Provide your compute requirements. We fulfill your desired capacity with matching instance types based on your

Manually add instance types

Add one or more instance types. Any of the instance types may be launched to fulfill your desired capacity based on

Reset to launch template

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

EC2 > Instances > i-0b02bcfb2f8d2e087

Instance summary for i-0b02bcfb2f8d2e087 (CobraKaiAppServer) Info

Updated less than a minute ago

Instance ID

i-0b02bcfb2f8d2e087 (CobraKaiAppServer)

Public IPv4 address

34.205.23.197 | open address

Private IPv4 addresses

172.31.85.169

IPv6 address

-

Instance state

Pending

Public IPv4 DNS

ec2-34-205-23-197.compute-1.amazonaws.com | open address

Hostname type

IP name: ip-172-31-85-169.ec2.internal

Private IP DNS name (IPv4 only)

ip-172-31-85-169.ec2.internal

Answer private resource DNS name

IPv4 (A)

Instance type

t2.micro

Elastic IP addresses

-

Auto-assigned IP address

34.205.23.197 [Public IP]

VPC ID

vpc-0e9c21cb5f7189c7d

AWS Compute Optimizer finding

Opt-in to AWS Compute Optimizer for recommendations. | Learn more

IAM Role

-

Subnet ID

subnet-0a18950360b4b9585

Auto Scaling Group name

-

Details

Security

Networking

Storage

Status checks

Monitoring

Tags

▼ Instance details Info

Platform

Amazon Linux (Inferred)

AMI ID

ami-0b0dcb5067f052a63

Monitoring

disabled

Platform details

Linux/UNIX

AMI name

amzn2-ami-kernel-5.10-hvm-2.0.20221103.3-x86_64-gp2

Termination protection

Disabled

Stop protection

Disabled

Launch time

Mon Dec 12 2022 16:38:59 GMT-0500 (Eastern Standard Time) (less than a minute)

AMI location

amazon/amzn2-ami-kernel-5.10-hvm-2.0.20221103.3-x86_64-gp2

Instance auto-recovery

Default

Lifecycle

normal

Stop-hibernate behavior

disabled

5.11 Monitoring and Logging services

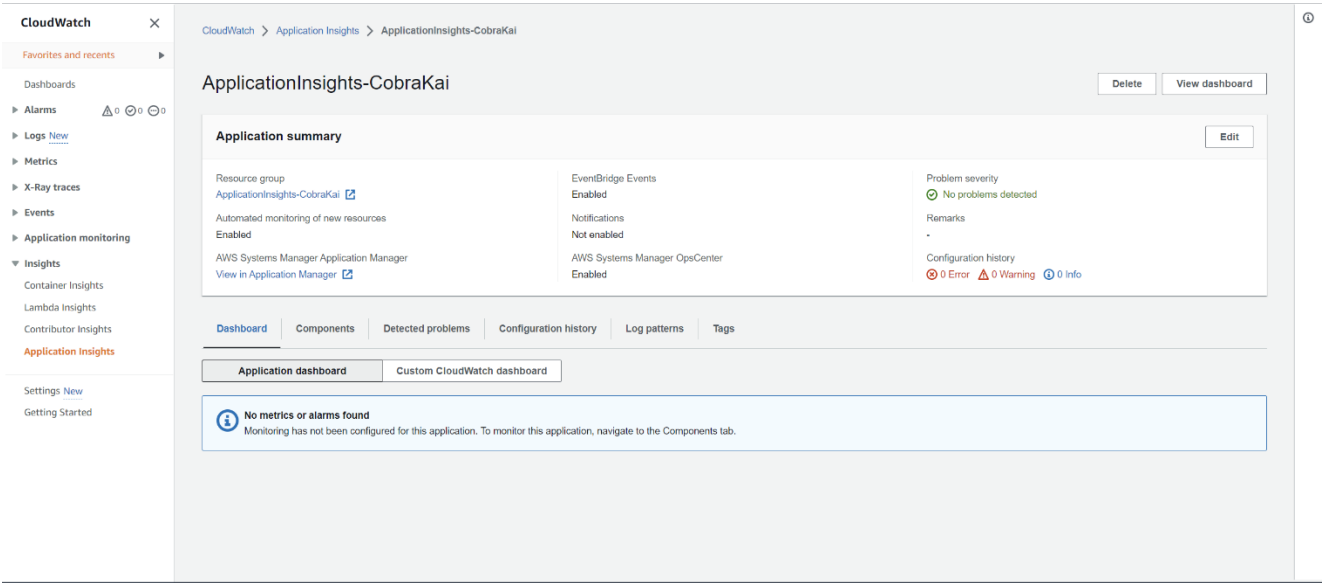
AWS Inspector

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

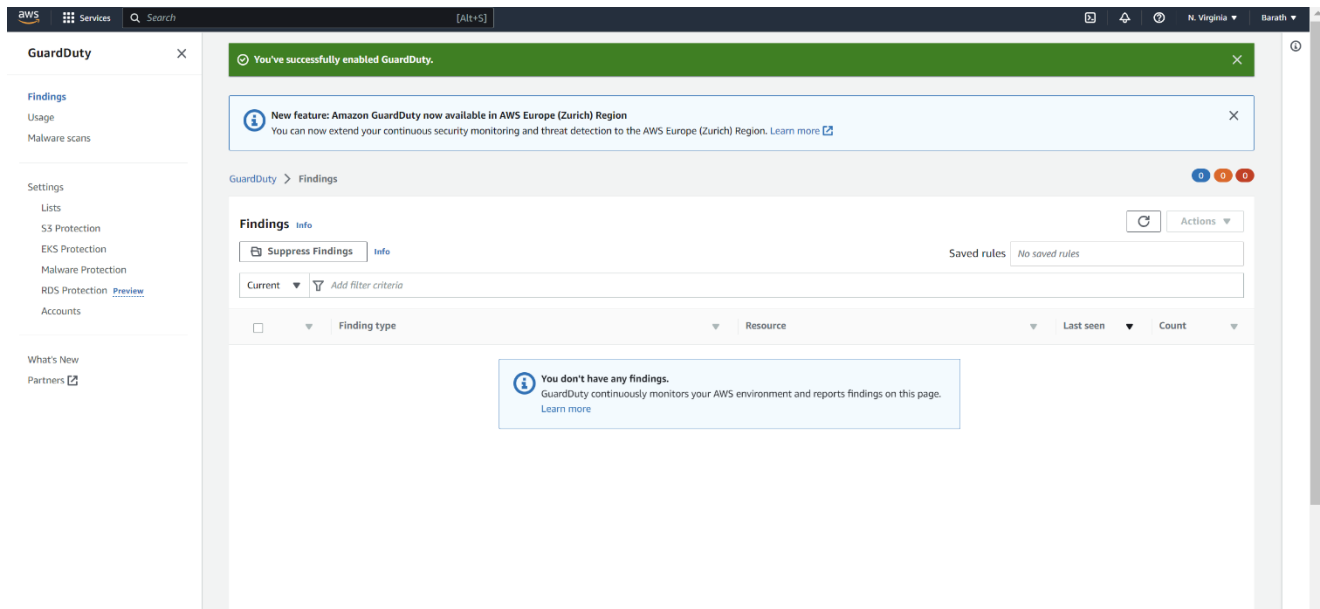
It is a real time monitoring service that checks resources and applications that run on the cloud in real time. It can collect and keep track of metrics that are user defined for resources.

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.

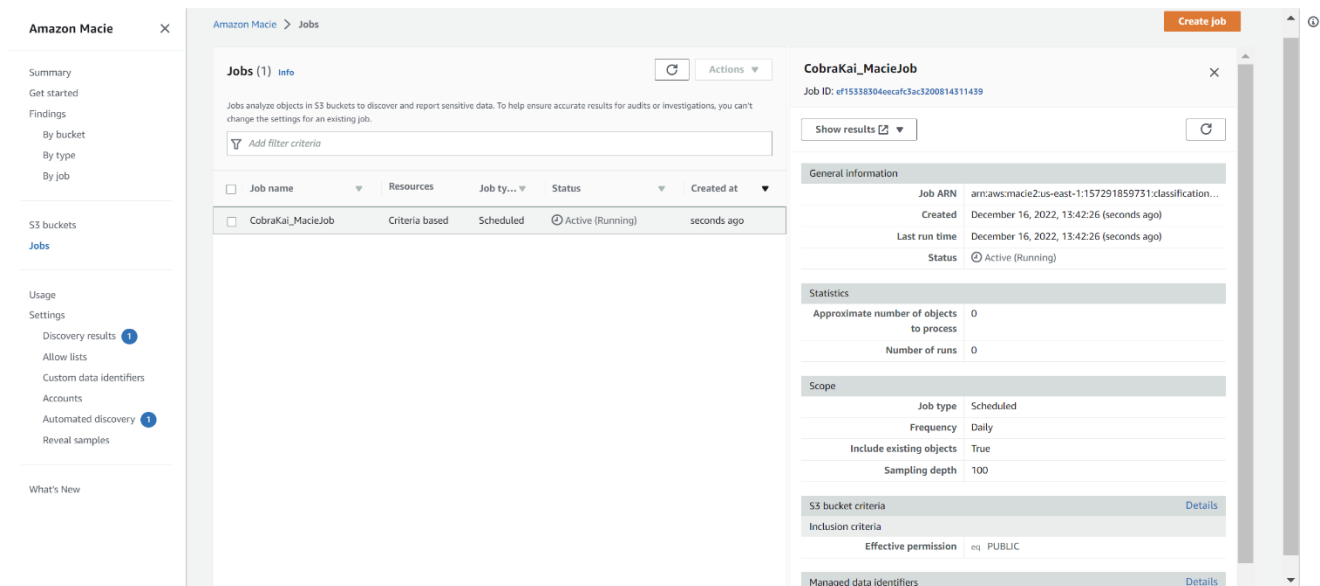


5.11 Protecting data

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

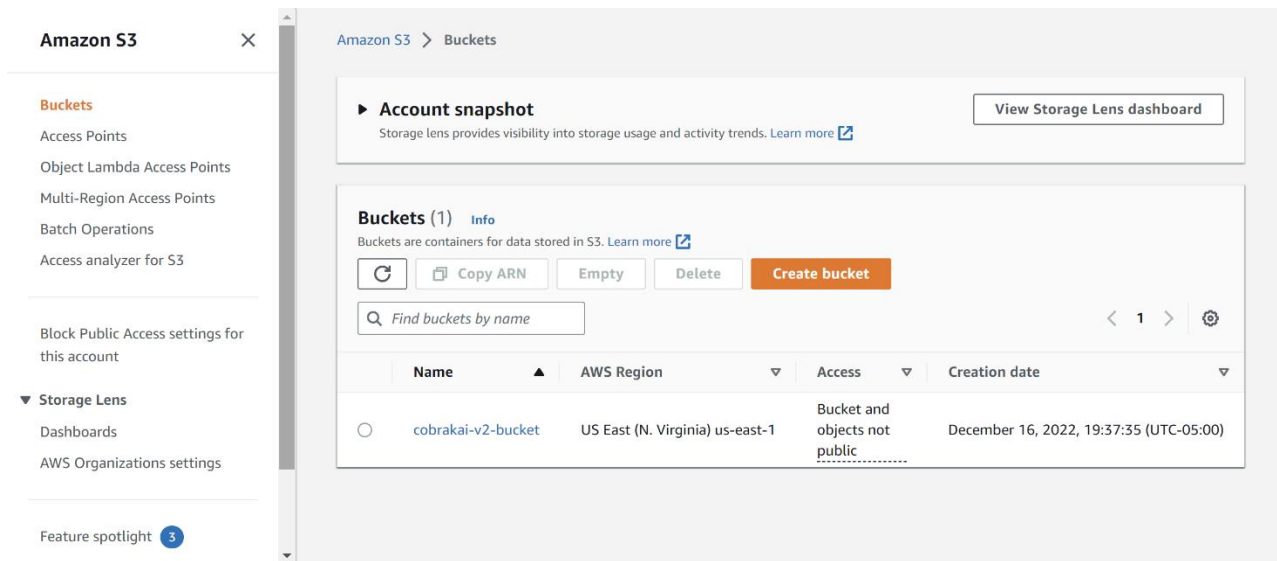
Payments Card Industry Data Security Standard is a security standard administered by the PCI Security Standards Council. PCI DSS applies to entities that store, process or transmit cardholder information or sensitive authentication data.

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)

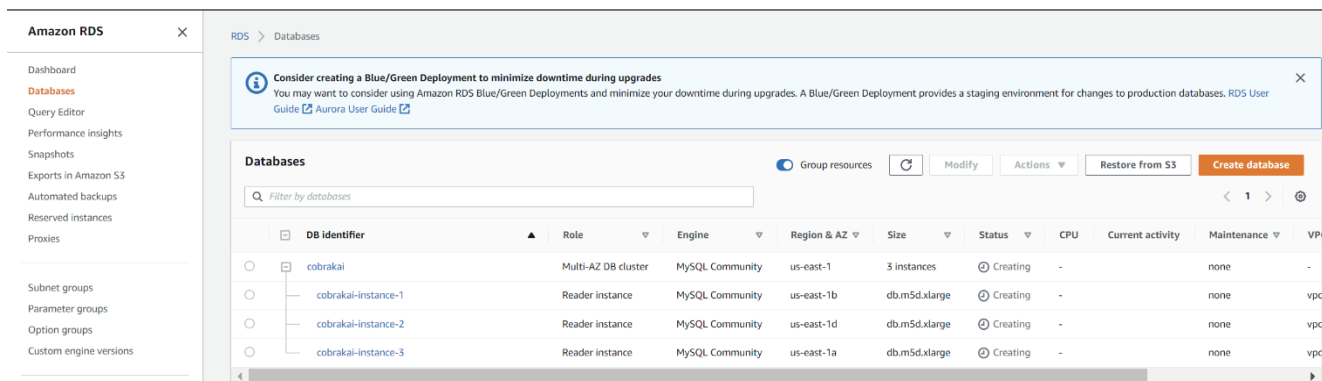
S3 is an object storage service that we can use to store the content required for CobraKai application. Storing media content in S3 buckets helps them to serve on-demand reliable streaming service.



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.

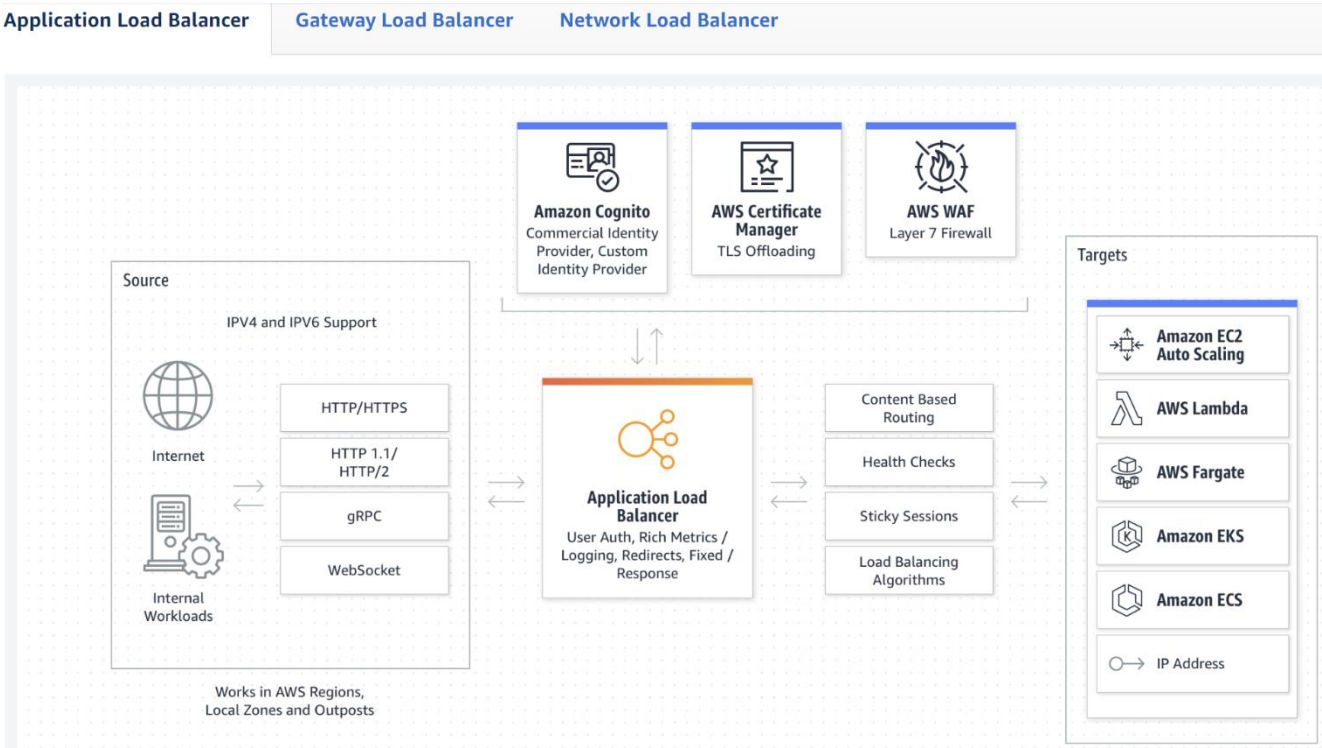


5.15 Amazon Elastic Load Balancer (ELB)

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

New EC2 Experience

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

EC2 > Load balancers > CobraKai

CobraKai

Details

Load balancer type

Application

IP address type

IPv4

Created At

December 12, 2022, 23:04 (UTC-05:00)

DNS name

CobraKai-2055260451.us-east-1.elb.amazonaws.com (A Record)

Scheme

Internet-facing

Status

Provisioning

Availability Zones

subnet-078a1961ec6c08c1e us-east-1a (use1-az4)

subnet-070dc780d22d1a836 us-east-1b (use1-az5)

VPC

vpc-0e9c21cb5f7189c7d

Hosted Zone

Z355XDOTRQ7X7K

Listeners

Network mapping

Security

Monitoring

Integrations

Attributes

Tags

Listeners (1)

A listener checks for connection requests on its port and protocol. Traffic received by the listener is routed according to its rules.

Search

Protocol:Port

ARN

Security policy

Default SSL cert

Default routing rule

Rules

Tags

HTTP:80

ARN

Not Applicable

Not Applicable

1. Forward to

CobraKaiTarget: 1 (100%)

Group-level stickiness: Off

1

0

5.16 AWS CloudFormation

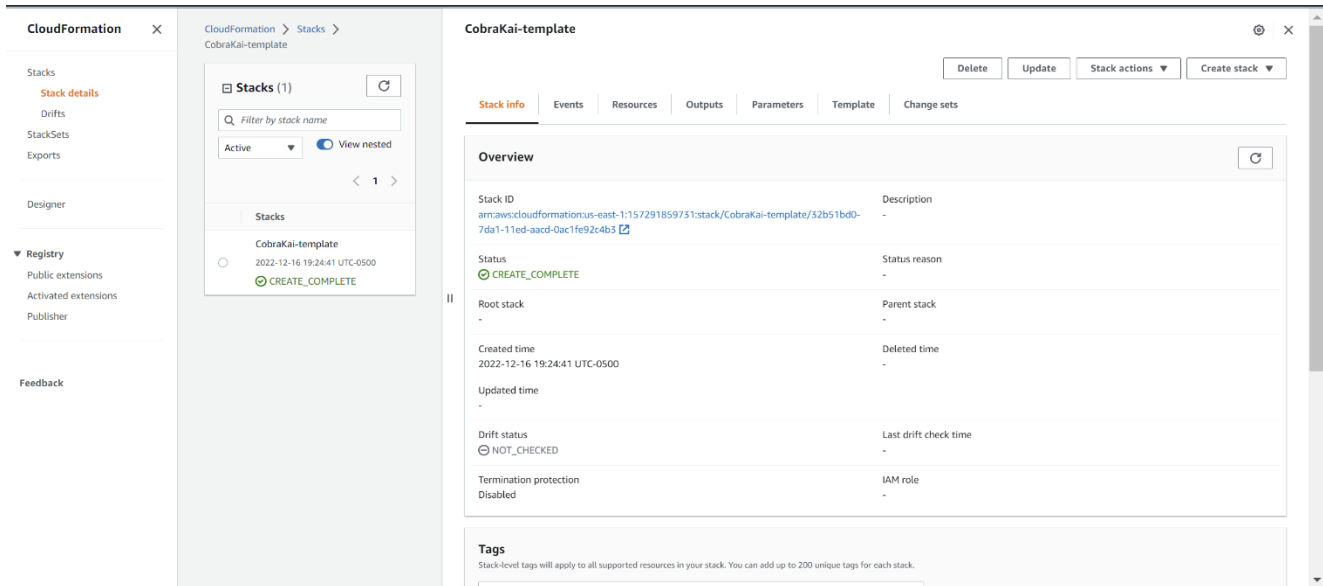
CloudFormation is a service that helps to deploy infrastructure using code so that we spend less time in the management of resources and more time on focusing on the application. We can create a template that specifies the required resources like EC2 instances, Amazon RDS instances and it will provision 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-aws-waf.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/>