Cloud Security

Migrating Cobra Kai Web Application to AWS cloud platform

Contents

1 Introduction

1.1 Migration of Cobra Kai to AWS cloud platform

Moving from on-premise to the AWS cloud is not a one-go process, but involves various configurations and measures to be made in order to make the migration secure. Since there are already many possible threats from Daniel LaRusso and his associates every step must be configured and monitored cautiously. This technical document demonstrates all the measures and steps to be followed for the safe deployment of Cobra Kai onto the cloud platform. The following architecture is implemented step by step through the document. AWS offers many more services which can be added once the current implementation is completed.

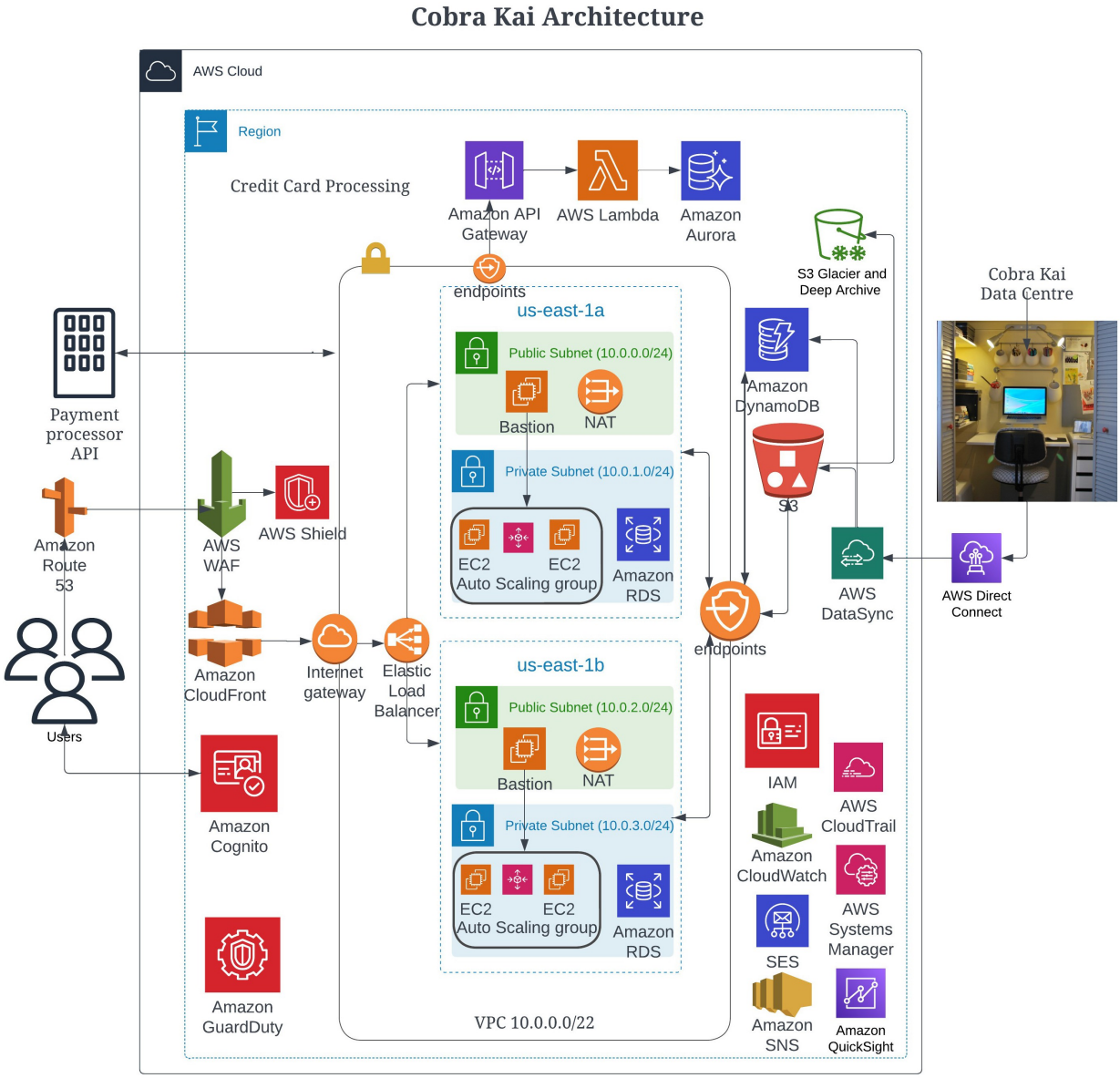


Figure 1: Architecture

2 CloudTrail

2.1 Enable secure logging using the AWS CloudTrail:

The CloudTrail is a service provided by AWS which allows you to activate operational and risk auditing, governance, and compliance of the AWS account. Any action performed on the AWS cloud by any role or user is registered in the events of CloudTrail. The events of AWS CloudTrail consist of every action performed on the AWS CLI (Command Line Interface), AWS SDKs, APIs, and the AWS Management Console.

1. Create an S3 bucket which is used by the CloudTrail to store the logs. As shown below screenshot shows an S3 bucket is created with the name enpm665cloudtrail (Fig.2).

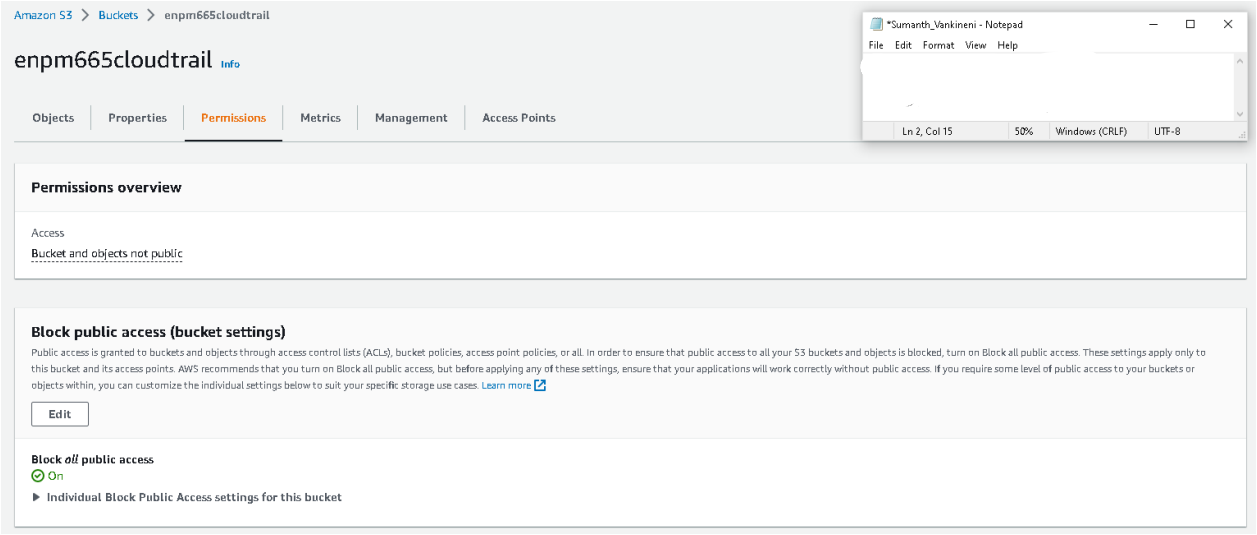


Figure 2: S3 Bucket

2. Select the trail attributes for the Cloud Trail selecting the bucket previously created. Encryption is also enabled for further protection (Fig.3).

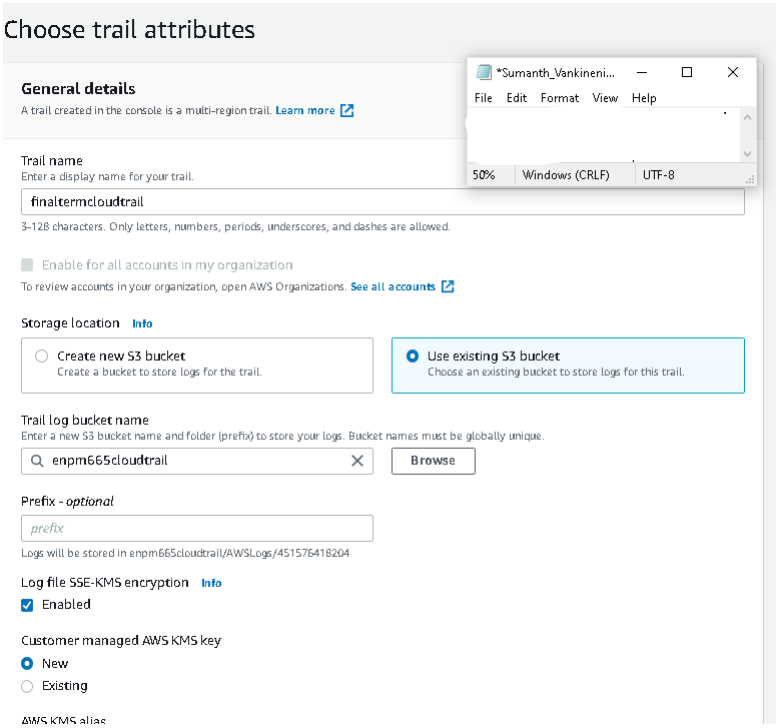


Figure 3: Trail attributes

3. Select all read and write operations to be logged (Fig.4).

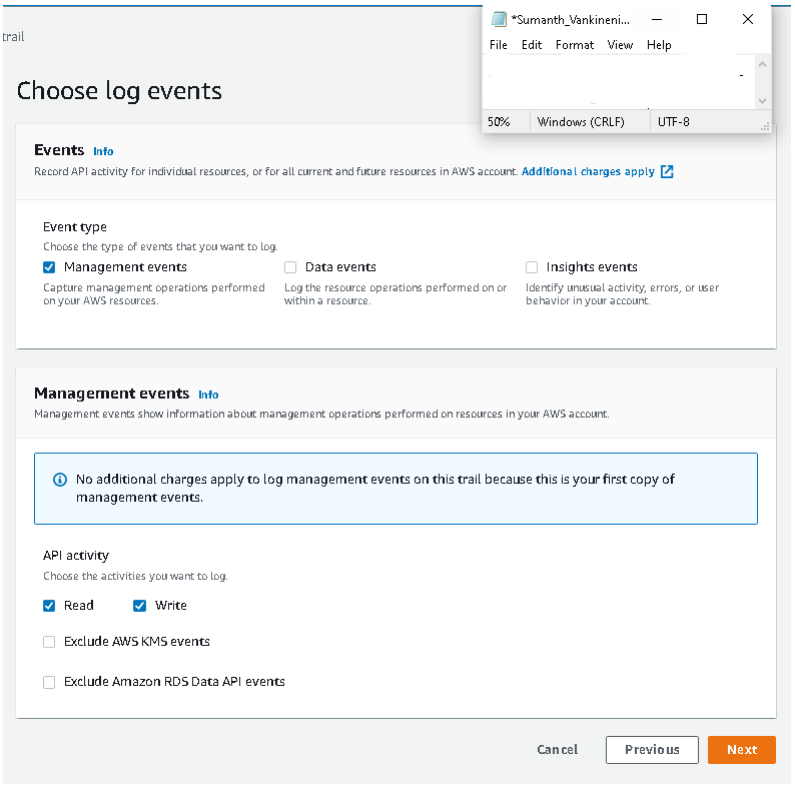


Figure 4: Log events

4. The CloudTrail is enabled and the trail logging has begun. Further SNS notifications can be enabled to get an alert to the selected emails immediately after the incident (Fig.5).

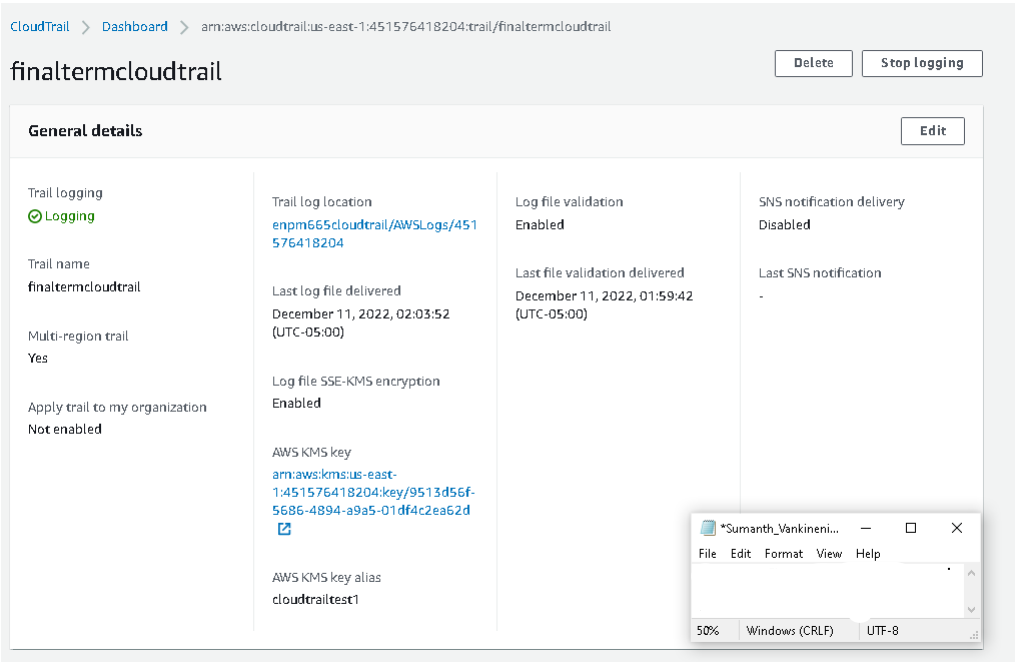


Figure 5: Dashboard

5. The (Fig.6) shows the current Bucket Policy configured for logging.

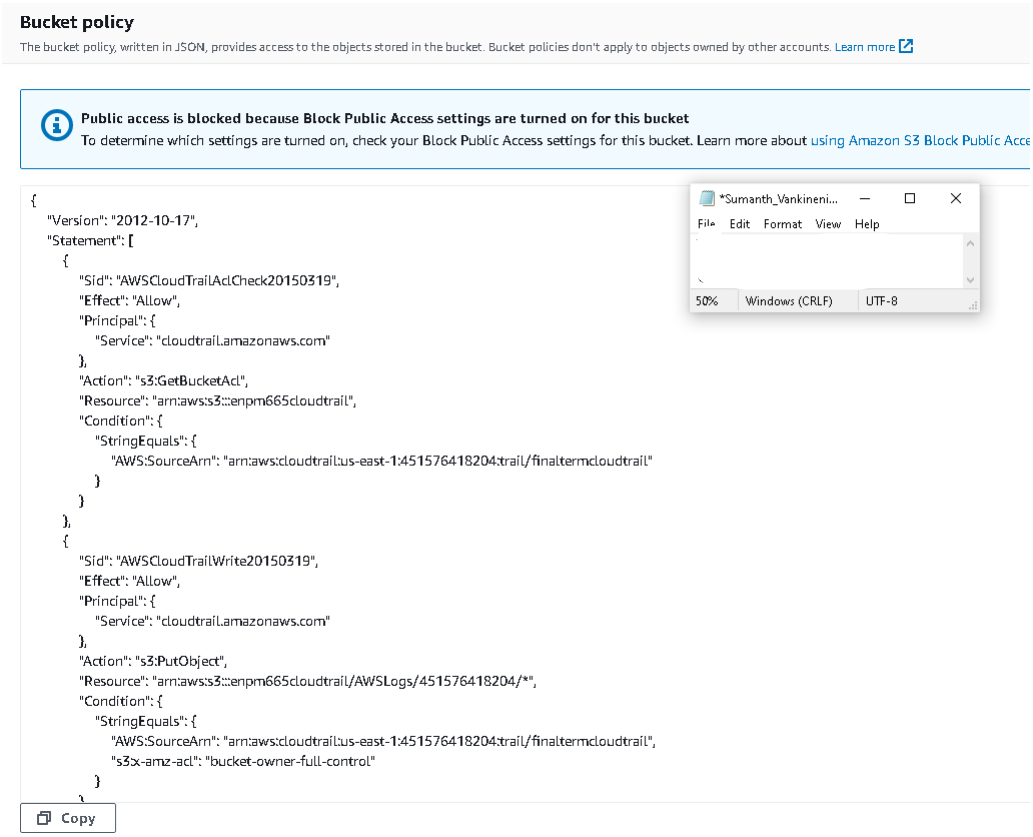


Figure 6: Bucket Policy

The following are the CloudTrail logs captured after the complete migration of Cobra Kai to the AWS cloud. It is clearly evident that every single log is stored and can be inspected(Fig.7).

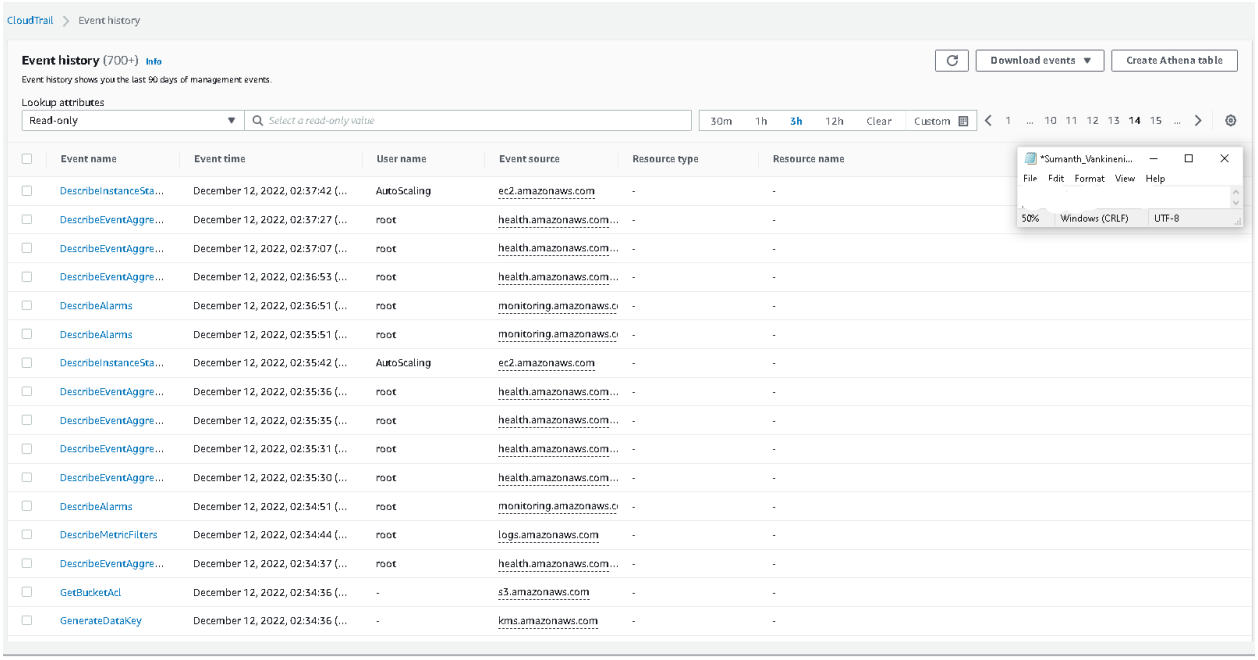


Figure 7: CloudTrail logs

3 Virtual private cloud (VPC)

The AWS VPC gives Cobra Kai the ability to launch a network virtually with the provided configurations. The VPC provides many features such as subnets, gateways, endpoints, VPN connections, and a lot more. For the current Demonstration purpose a VPC is created with the mentioned subnets as shown in (Fig.8).

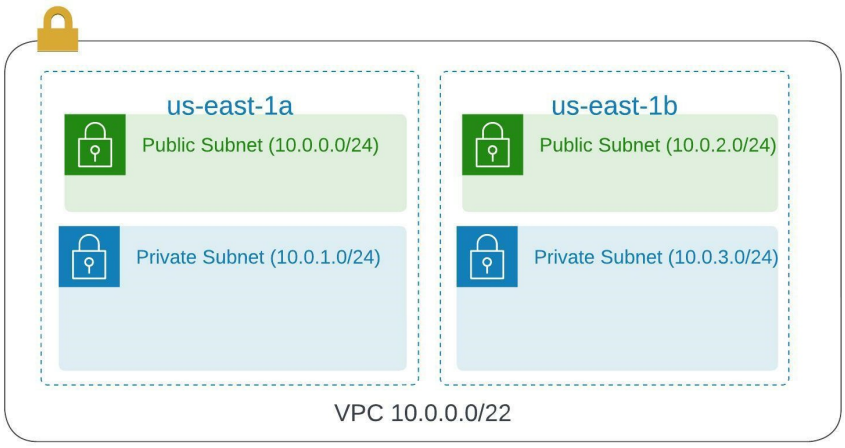


Figure 8: VPC subnets

1. Give a name for the VPC and give the IPv4 CDIR block as 10.0.0.0/24 and select 2 availability zones and 2 public and private subnets(Fig.9).

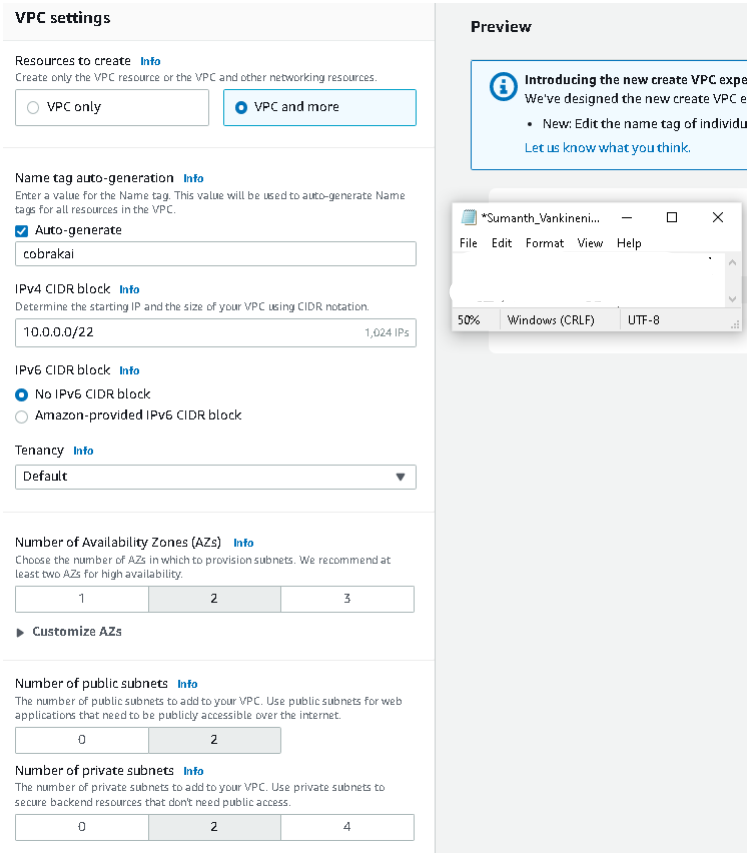


Figure 9: VPC settings

2. The following tables will be generated containing the subnet addresses, Subnets, Route tables, and network connections(Fig.10).

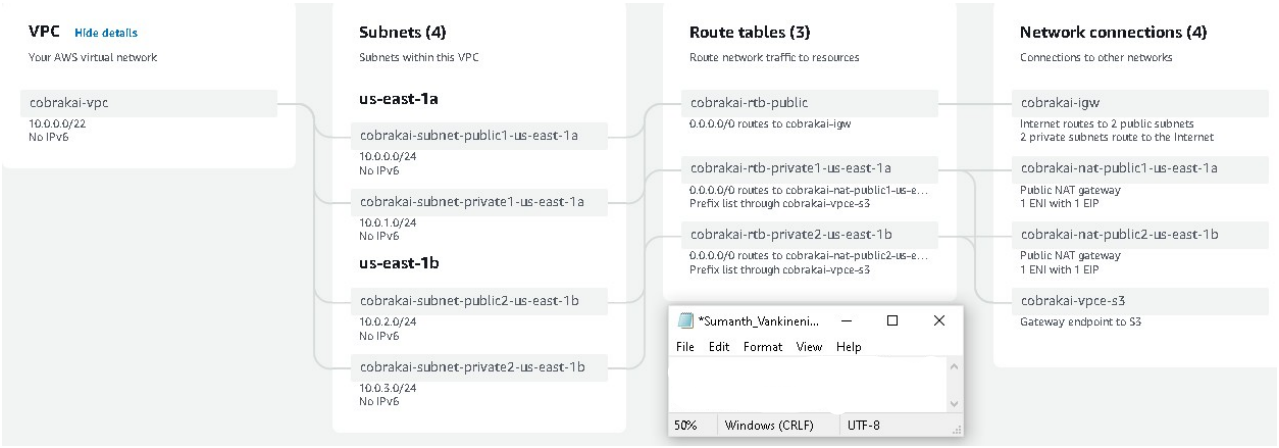


Figure 10: Tables

3. After successfully creating the VPC the following availability zones can be viewed with their private and public subnets(Fig.11).

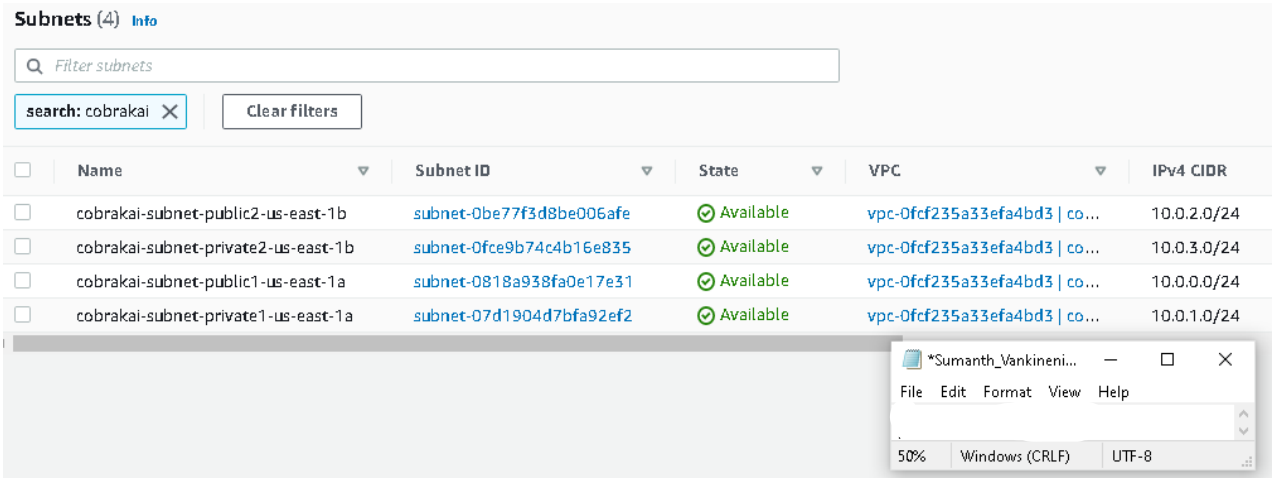


Figure 11: Subnets

4 Securely moving the Data to the AWS cloud

4.1 AWS DataSync

The DataSync is a very secure service provided by AWS which achieves the automation of transferring files between the on-premise and the AWS Cloud. DataSync offers end-end security using techniques such as encryption and integrity validation. The service connects to the storage of the AWS with the security features such as CloudTrail, CloudWatch, and Identity and Access management(Fig.12).

Since Cobra Kai contains a lot of Karate training videos where the storage can be in Terabytes, the transmission of the data will consume a lot of time. DataSync resolves this issue by using certain network protocols and a multithreaded architecture to speed up the data transfer process. The DataSync offers one of the lowest rates with a flat gigabyte pricing compared to any of the commercial transfer tools.

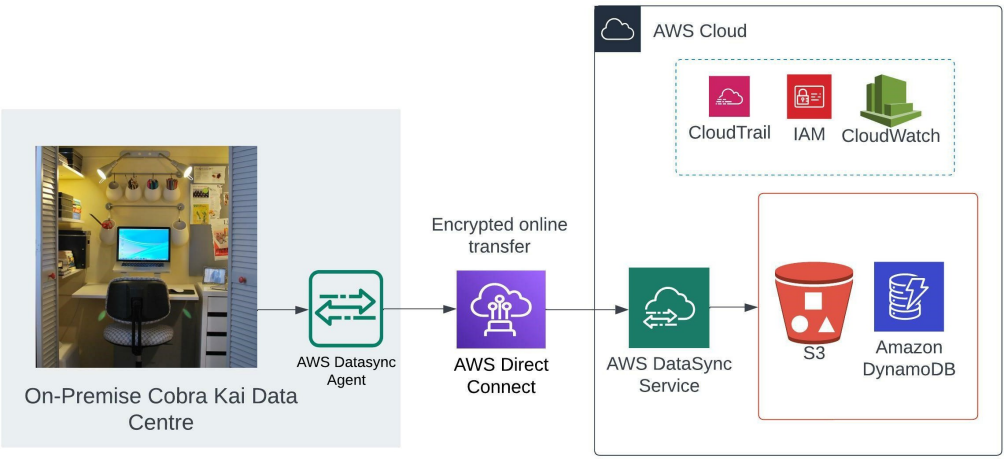


Figure 12: Data Transfer

4.2 AWS Direct Connect

The AWS Direct Connect offers great speeds ranging from 50 Mbps to 100 Gbps thus acting as an intermediate for the AWS DataSync to have faster transmission rates. On top of that, it also provides encryption techniques such as MACsec and IPsec adding extra protection along with maintaining high speeds.

4.3 Running the Cobra Kai server

For the demonstration purpose, we've used the EC2 instance directly in the public subnets but during the finaManagement tation, A bastion host will be used to connect to the EC2 instances in the private subnet. A bastion host can be compared to a special-purpose computer that has been set up to fend against attacks. The machine just houses one application that it hosts. It is also referred to as a "Jump Box" and has access to the public network. Being the only host with access to the public network makes it a strong server that offers high levels of network security.

System administrators can use this device to connect to other service instances, which takes place in the infrastructure back-end. This usage location makes sure the system is secure with the aid of numerous authentication measures.SSH or RDP are used as access methods to these hosts. It enables utilizing SSH or RDP to log in to other instances (thereby acting like a "jump server") that are present within the private network/subnet when communication (remotely) is established with the bastion host.

Bastion host acts as a bridge between the private instances of the service and the internet once the connection has been correctly setup with the aid of security groups and network ACLs (NACL), defending the instances from attacks from the outside.

1. The following screenshot shows the running of the Cobra Kai web application on the EC2 instance inside the VPC(Fig.13).

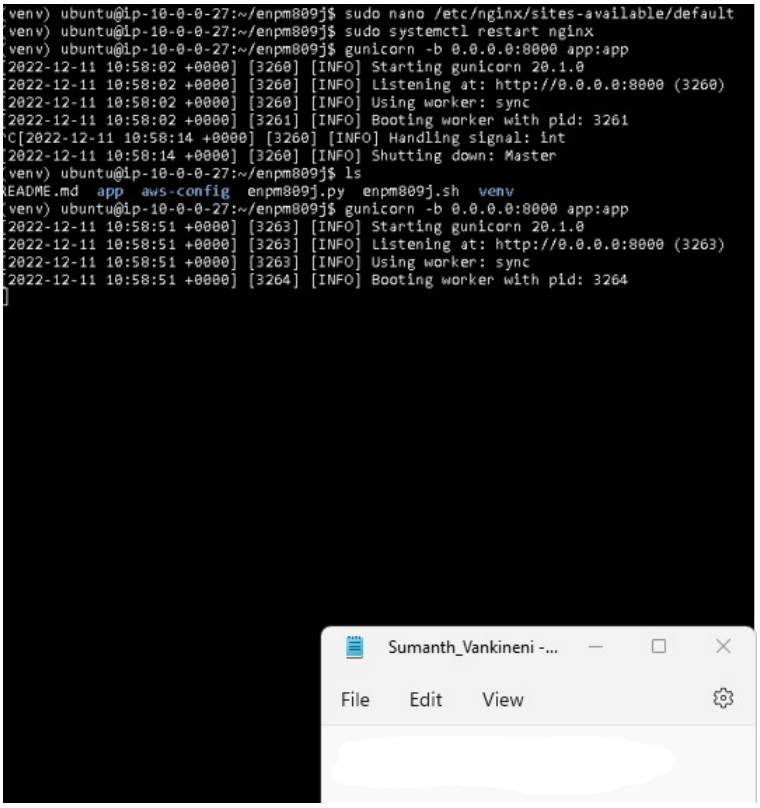


Figure 13: EC2 instance

2. By navigating to the DNS address of the EC2 instance we can connect to the web application through the internet(Fig.14).

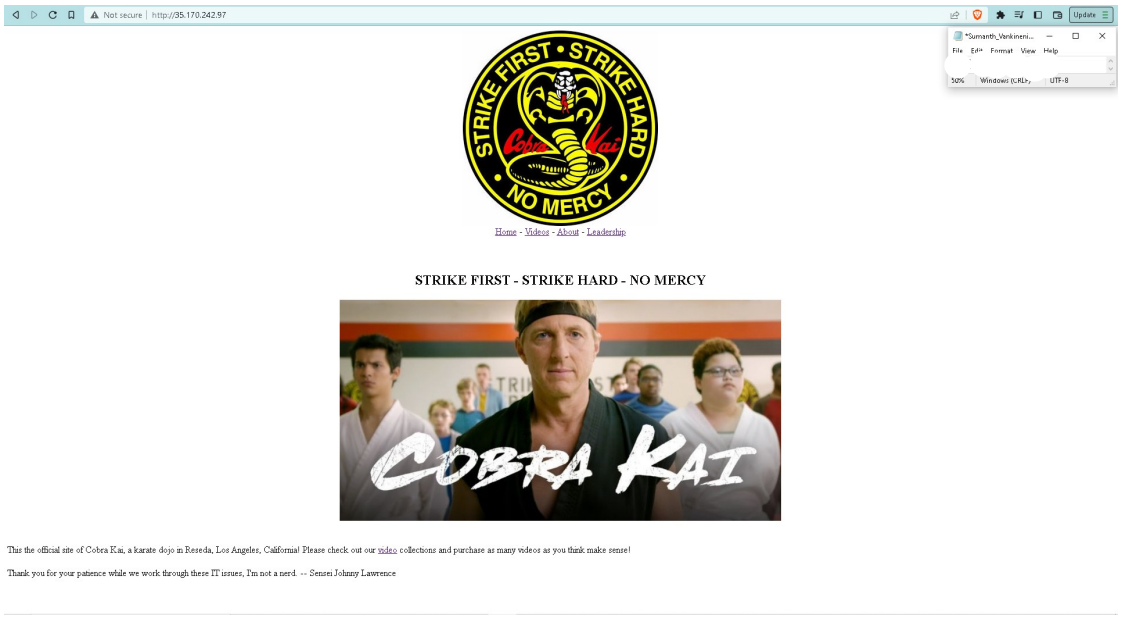


Figure 14: Cobra Kai web server

3. The content of the web application is stored in the S3 buckets which can be viewed by inspecting the page(Fig.15).
4. The content of the S3 bucket can be viewed as shown in the (Fig.16).

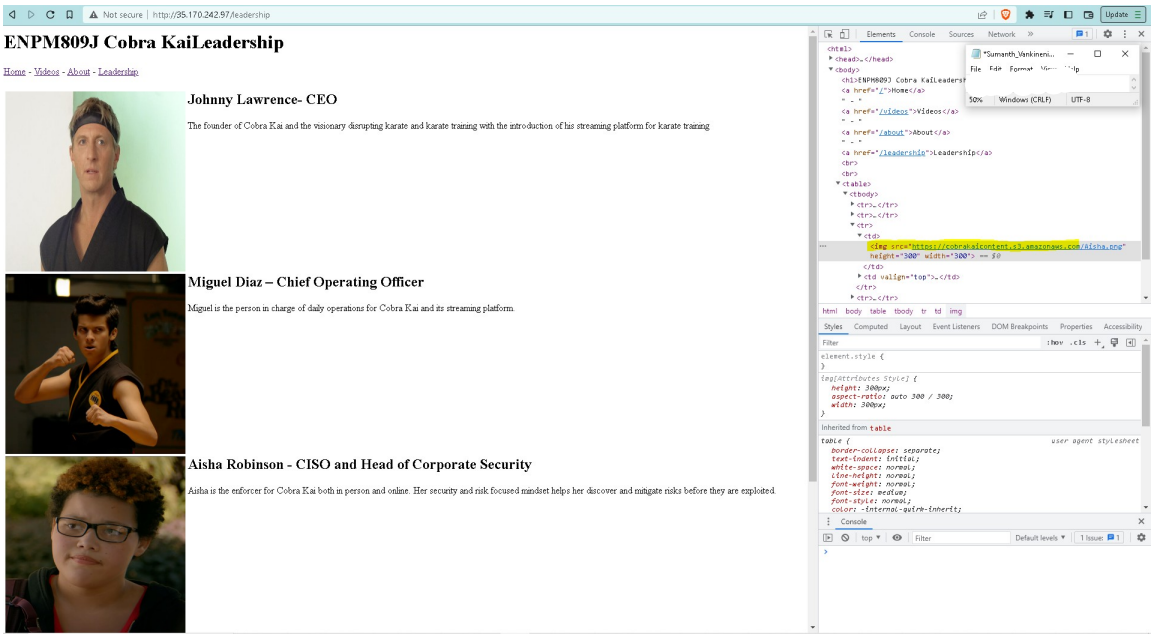


Figure 15: Inspecting the page

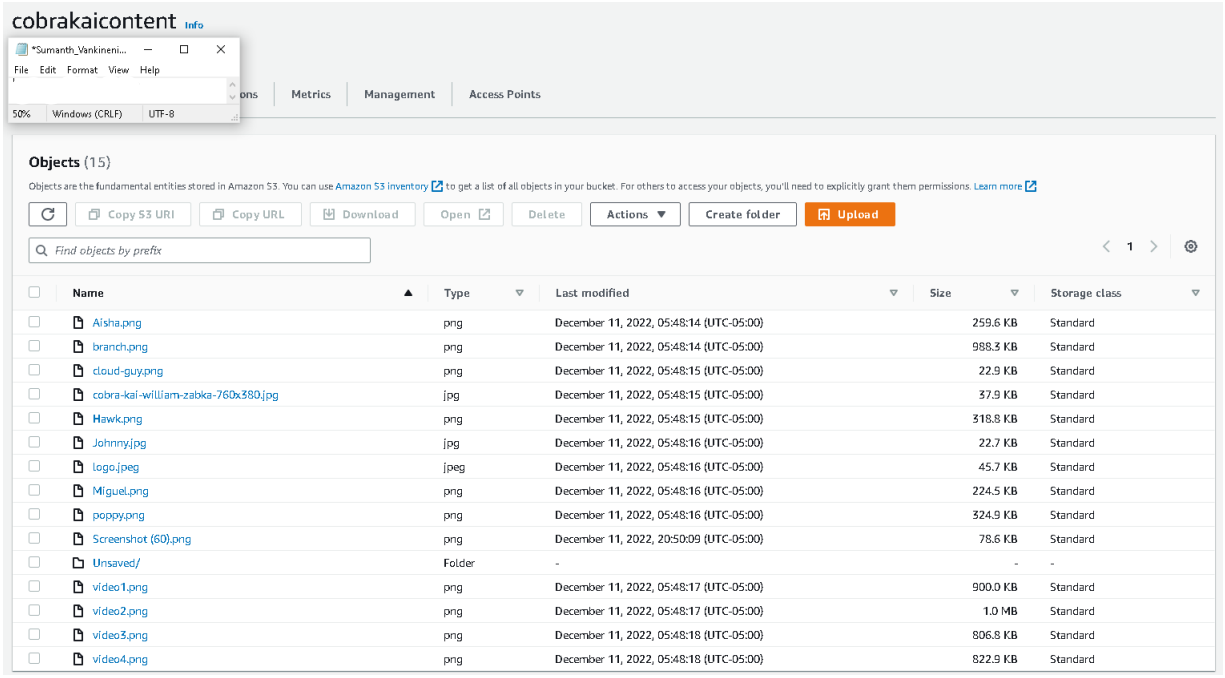


Figure 16: S3 bucket contents

5 Load Balancer and Auto Scaling

5.1 Load Balancer

The AWS Load Balancer helps in the automation of distributing the incoming traffic among various EC2 instances among one or more Availability zones. The Load Balancer can be used to monitor the health and status of the EC2 usage status based on which it redirects incoming traffic to the healthy running instance. The AWS Elastic Load Balancer can automatically scale the Load Balancer depending on the load of the incoming traffic to the Cobra Kai server(Fig.17).

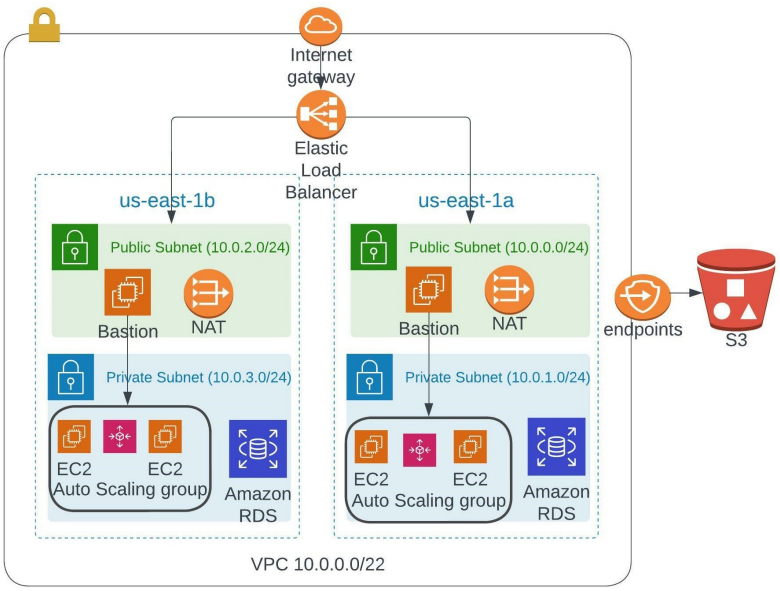


Figure 17: ELB

1. Configure the Load Balancer with both the region public subnets where the bastion host is to be hosted(Fig.18).

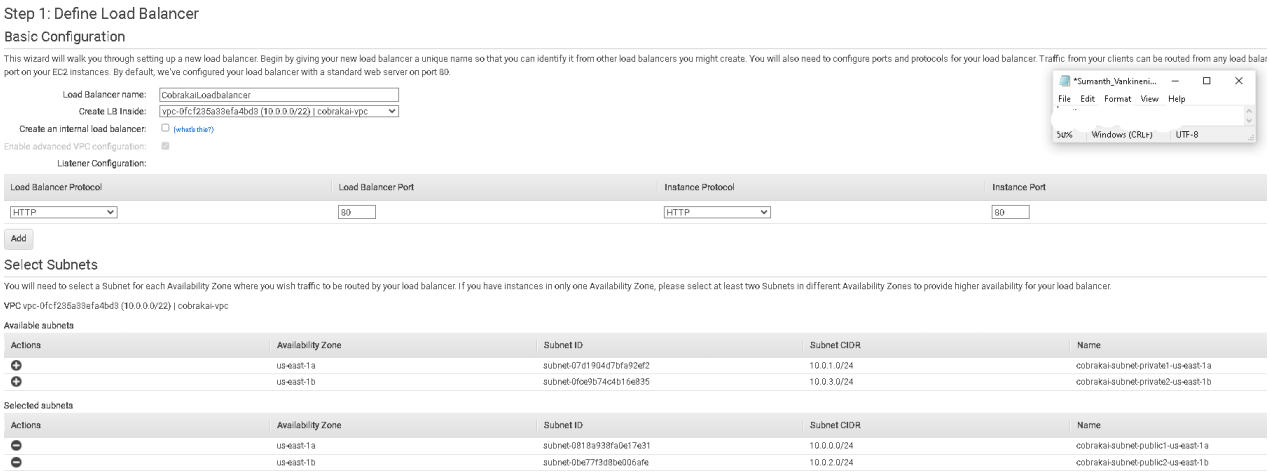


Figure 18: Caption

2. Attach the Web server Security groups to the Load Balancer(Fig.19).
3. In the target groups we can see that both instances are in a healthy state and running(Fig.20).

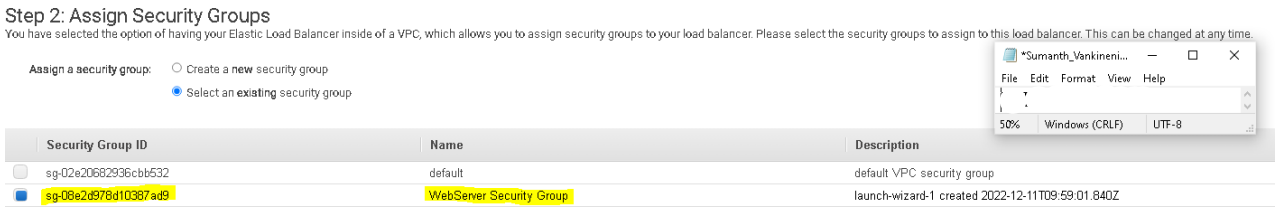


Figure 19: Caption

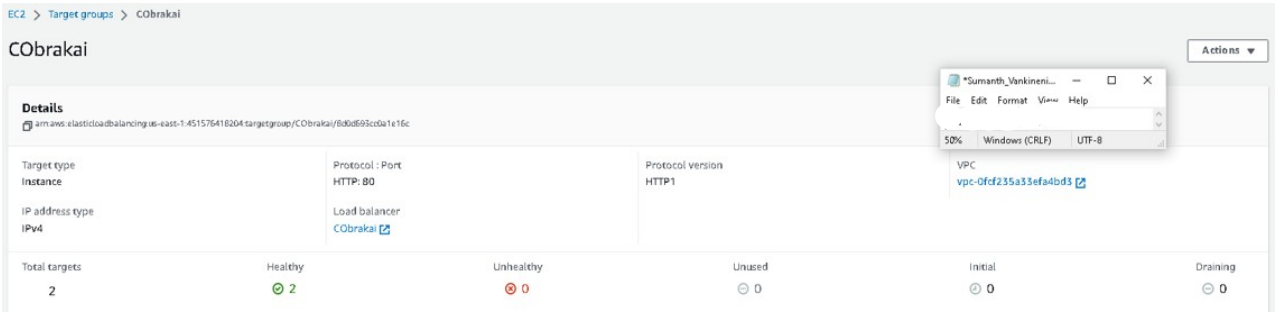


Figure 20: Caption

5.2 Auto Scaling

As the Cobra Kai application is monitored by AWS Auto Scaling, capacity is automatically adjusted to provide constant, predictable performance at the lowest feasible cost. Setting up application scaling for numerous resources across numerous services is simple with AWS Auto Scaling and takes only a few minutes.

Even during peak loads when workloads are irregular, unpredictable, or constantly changing, you can maintain optimal performance for the Cobra Kai web application and availability using AWS Auto Scaling. AWS Auto Scaling continuously checks your apps to make sure they are performing at the levels you want. In order to maintain a high level of service when demand spikes, AWS Auto Scaling automatically raises the capacity of limited resources.

1. Select the Amazon Machine image to be used for the autoscaling and the instance type(Fig.21).

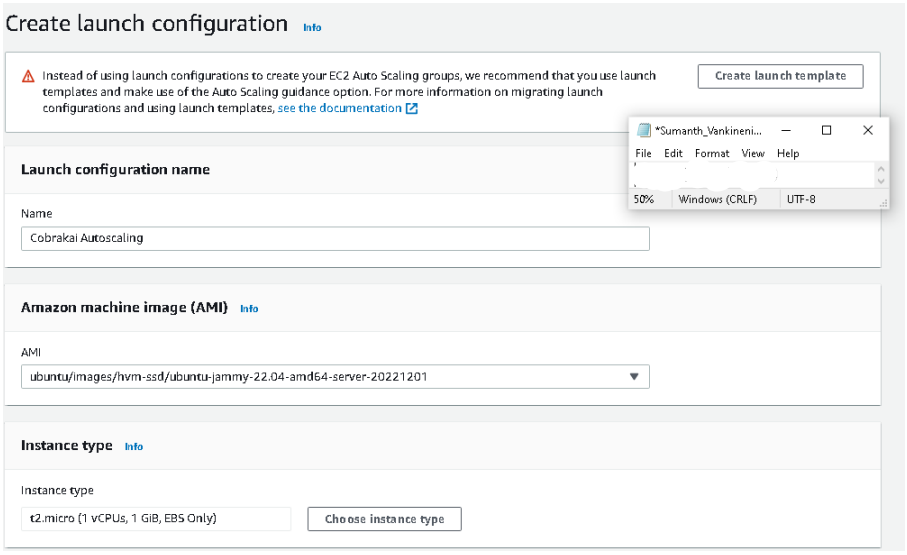


Figure 21: Launch configuration

2. Select the Web server Security group and chose a key pair login(Fig.22).

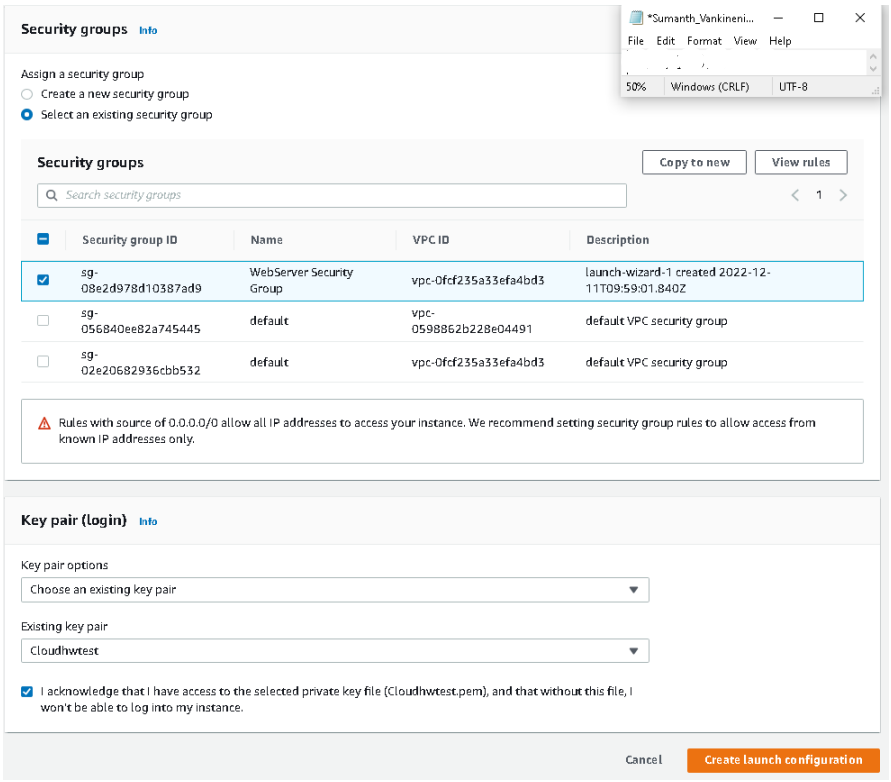


Figure 22: Security groups

3. Select the availability zone us-east-1a and us-east-2a and the cobra kai VPC(Fig.23).

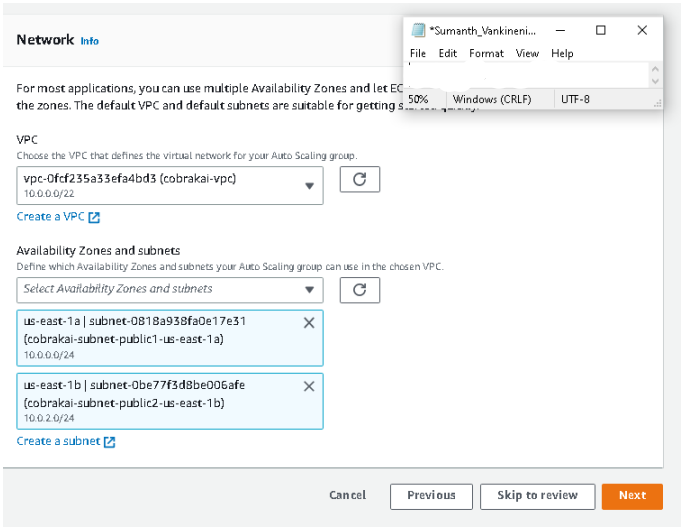
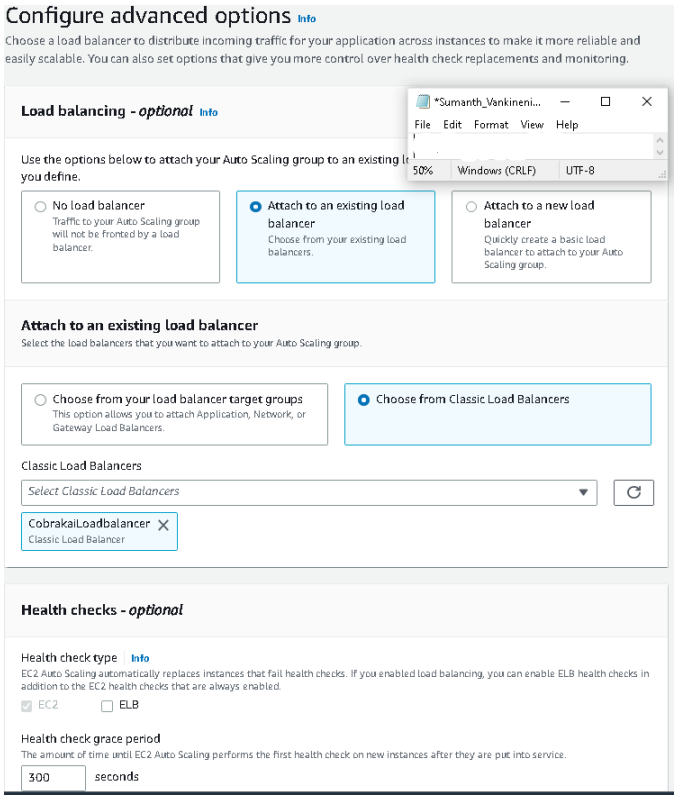
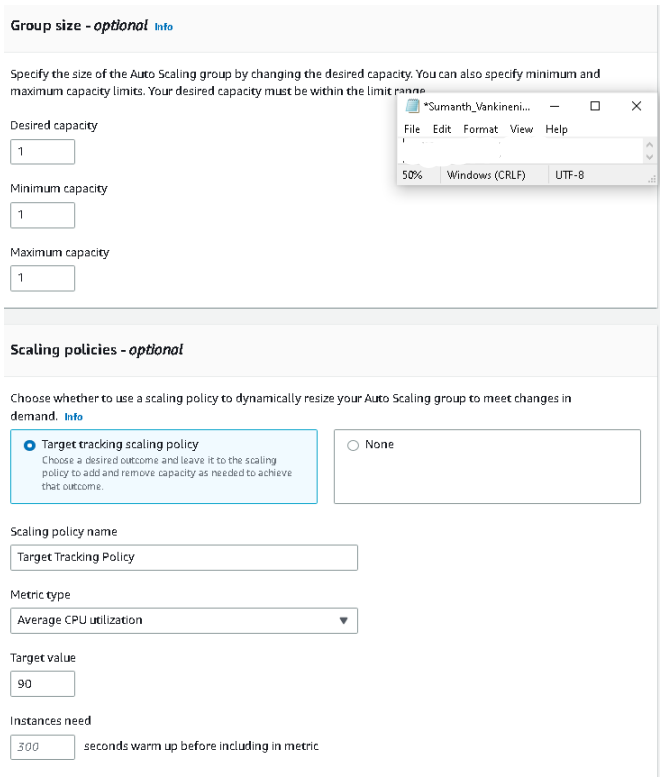


Figure 23: Network

4. The Autoscaling should be attached to the existing Load Balancer and the required health checks parameters can be specified(Fig.24a).
5. Select the desired capacity to increase depending on the state of the EC2 instance for example on reaching the CPU utilization of 90(Fig.24b).
6. SNS notifications can be enabled with the following events(Fig.25).
7. For the SNS notifications to be received the subscription should be confirmed(Fig.26).



(a) Advanced options



(b) Group size

Figure 24: Step 4 and 5

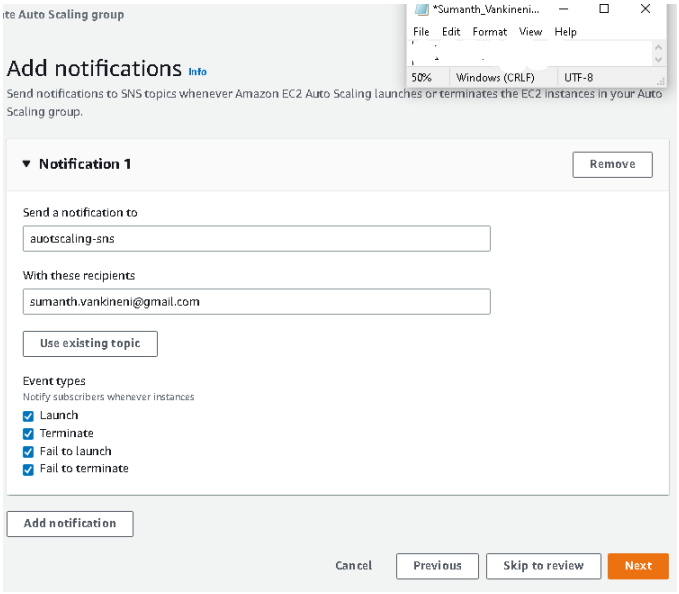


Figure 25: Notifications

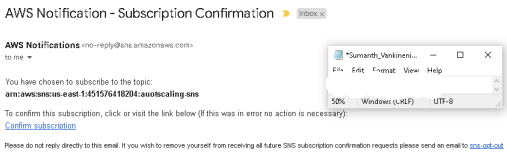


Figure 26: SNS

6 AWS CloudFront

Enabling the online service CloudFront provided by AWS makes it faster for users to access the Cobra Kai web application. Edge locations are a global network of data centers that CloudFront uses to deliver your content. In order to serve content with optimal performance to the users of Cobra Kai, every user's request for the content provided with CloudFront is routed to the edge location that has the lowest latency (time delay) so that the users do not face any problems with long durations for viewing the content.

A lambda function can be created to retrieve the cache from the S3 bucket using the AWS CloudFront. Suppose the viewer enters the Cobra Kai URL to request the website. If the requested object is already in the cache, CloudFront returns it to the viewer quickly. If the object is not already cached by CloudFront, it is requested from the origin (an S3 bucket), upon which the lambda function is invoked and the retrieved object is stored in the cache.

6.1 Configuring CloudFront

Create a CloudFront distribution by selecting the load balancers domain name. For demonstration purposes, HTTP protocol is used but when implemented HTTPS protocol has to be used for higher security. Give a name for this distribution and then create it(Fig.27).

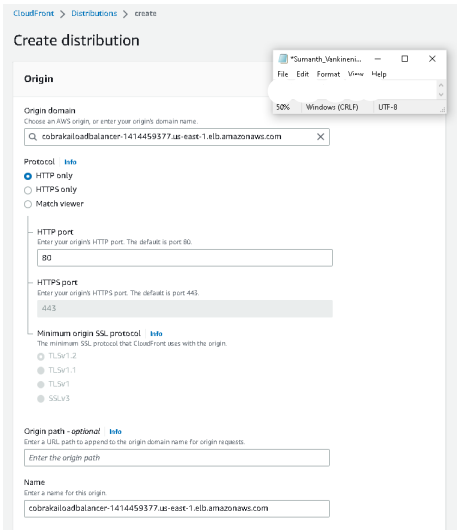


Figure 27: Distribution creation

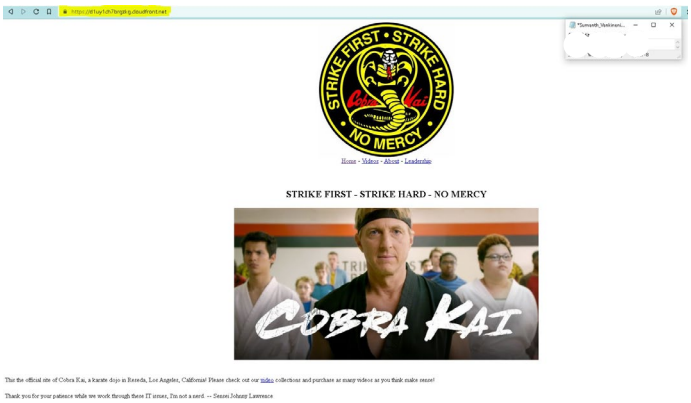


Figure 28: Cobra Kai web server

The highlighted section of the screenshot above shows the DNS provided by the CloudFront by AWS which can be used to connect to the Cobra Kai Web application. Route 53 is another layer that can be added on top of CloudFront where a custom domain address can be configured which can be used to deliver traffic among multiple regions(Fig.28).

7 Identity and Access Management

For Cobra Kai developers and administrators, a variety of permissions can be set via the IAM. On AWS, access is typically refused and is only permitted when permissions specifically state ”Allow.” We can create users, groups, rules, and roles using the IAM. Permissions, such as who has access to which resources and what actions they can take on them, can be set using the policies.

1. Enter the name of the user and enable the password reset option which will be prompted when the user logs in for the first time(Fig.29).

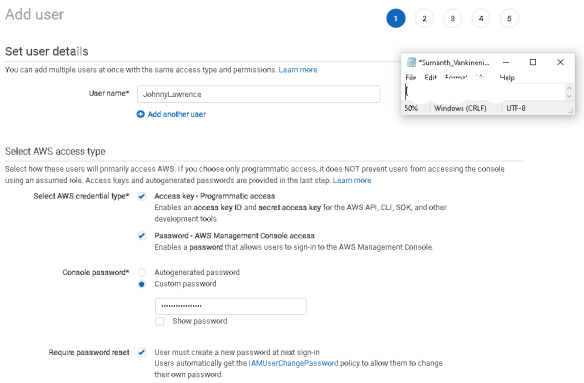


Figure 29: User details

The identities in the service are IAM users. When you establish an IAM user, nothing in your account is accessible to them unless you grant them access. An identity-based policy, which is a policy linked to a person or a group to which the user belongs, is how you grant permissions to a user. The example shown in the following figure illustrates a JSON policy that enables users to read any resources in the AWS region. This policy is attached to Johnny Lawrence so that he can view any content or resources he wishes on the AWS cloud platform.

2. Attach the policy(Fig.31b).

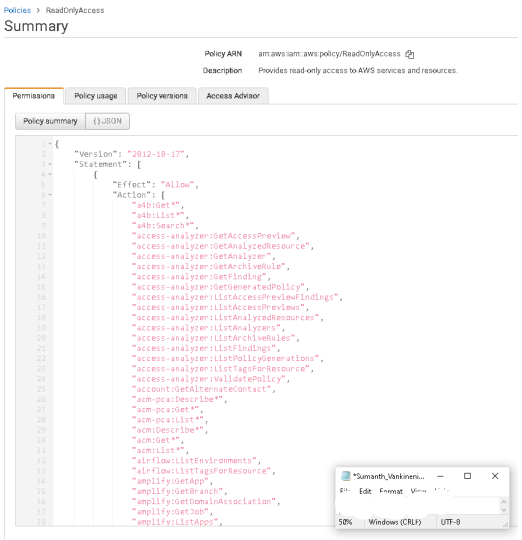
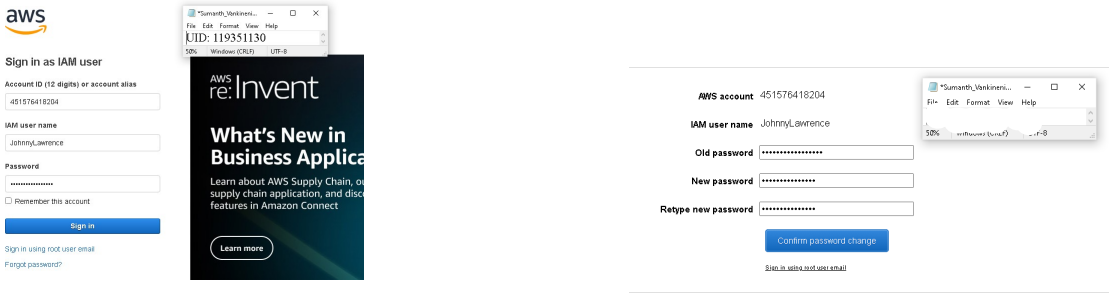


Figure 30: Policy

After attaching the policy to the IAM user, the user can log in using the default credentials created either by using the AWS management console or using AWS API, CLI, SDK, and other developer tools.

3. Log in using the credentials of Johnny Lawrence. A new password has to be created for higher security purposes as we specified while creating the user(Fig.31b).

4. The dashboard for Johnny Lawrence after the successful login is shown below. MFA should be configured by all the users for a higher level of security for the AWS account(Fig.32).



(a) Log-in page (b) Password change

Figure 31: Step 3 and 4

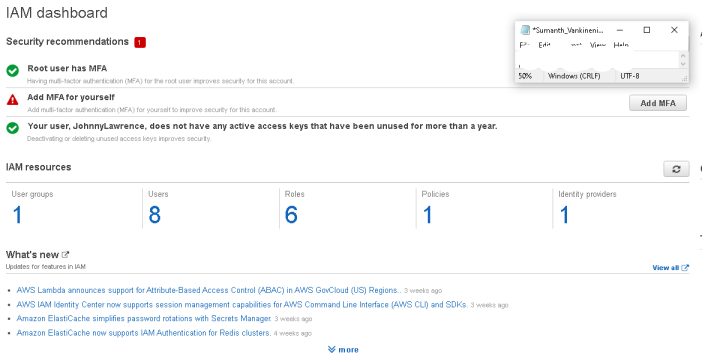


Figure 32: IAM dashboard

5. Let us test what all actions can be performed with the user Johnny Lawrence(Fig.34).

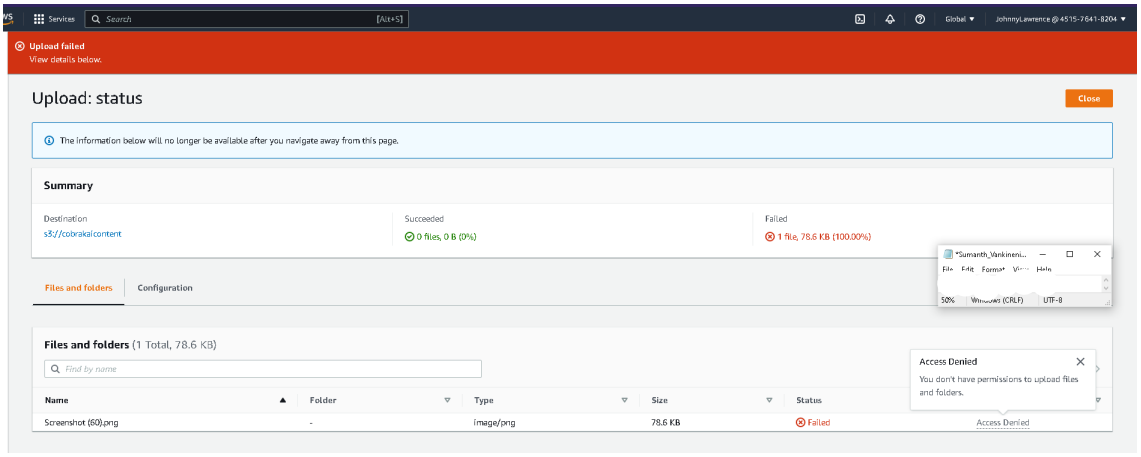


Figure 33: Failed upload

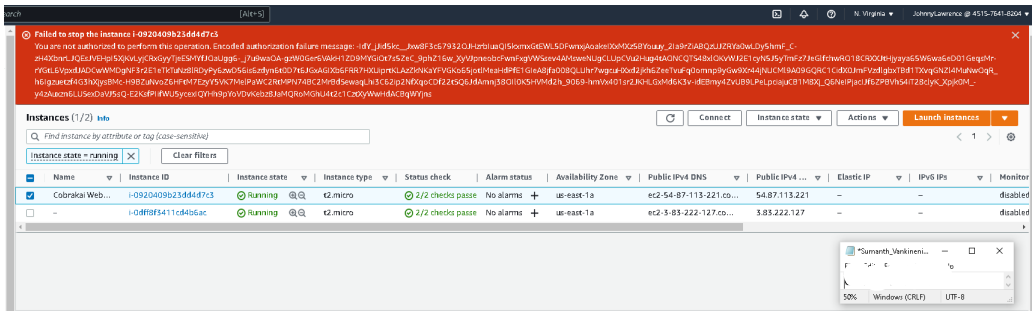


Figure 34: Policy error

All the contents of the S3 buckets can be viewed by Johnny Lawrence but he does not have any write permissions so as shown in the above screenshot the upload of a new image has failed due to the user permissions on AWS.

Similarly, Johnny does not have permission to stop the EC2 instance as shown in the above screenshot.

6. Let us show you the demonstration of a different policy for the user Demetri on IAM. Similar steps can be followed to create an IAM user for Demetri as done previously for Johnny Lawrence but with a different policy. The PowerUserAccess is given to Demetri as he is a developer and needs access to configure and manage the resources on the AWS cloud platform for the Cobra Kai web application(Fig.**??**).

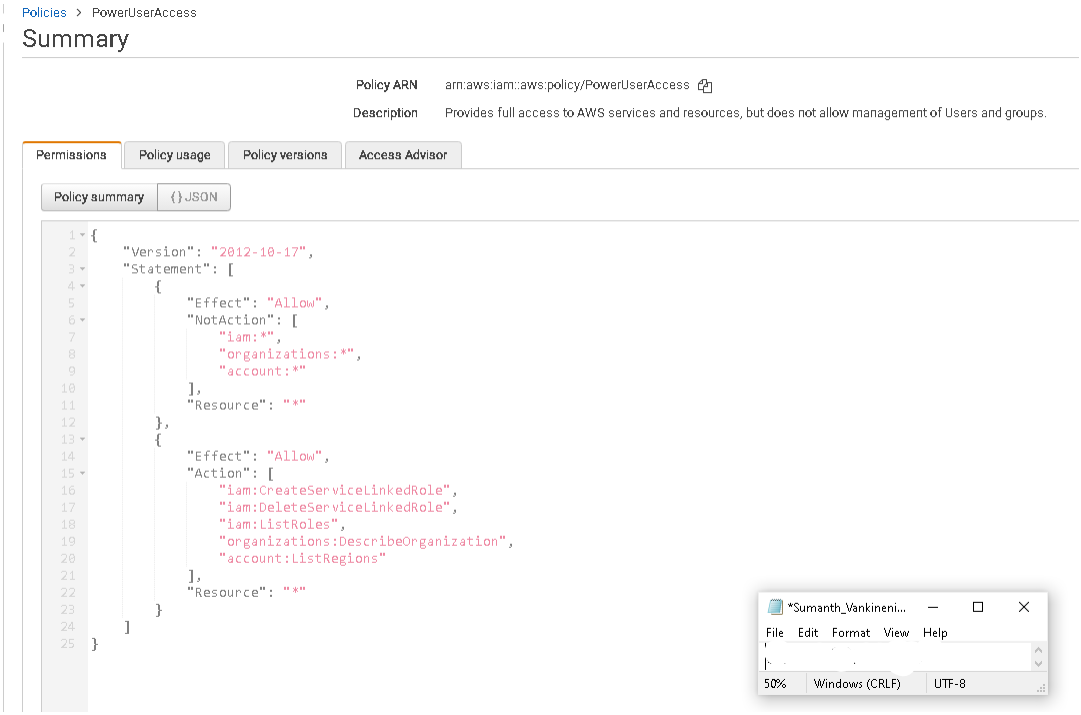


Figure 35: PowerUserAccess

7. Demetri user can log in with his credentials and he has permission to update the S3 buckets. The following screenshot shows that the upload is successful(Fig.36).

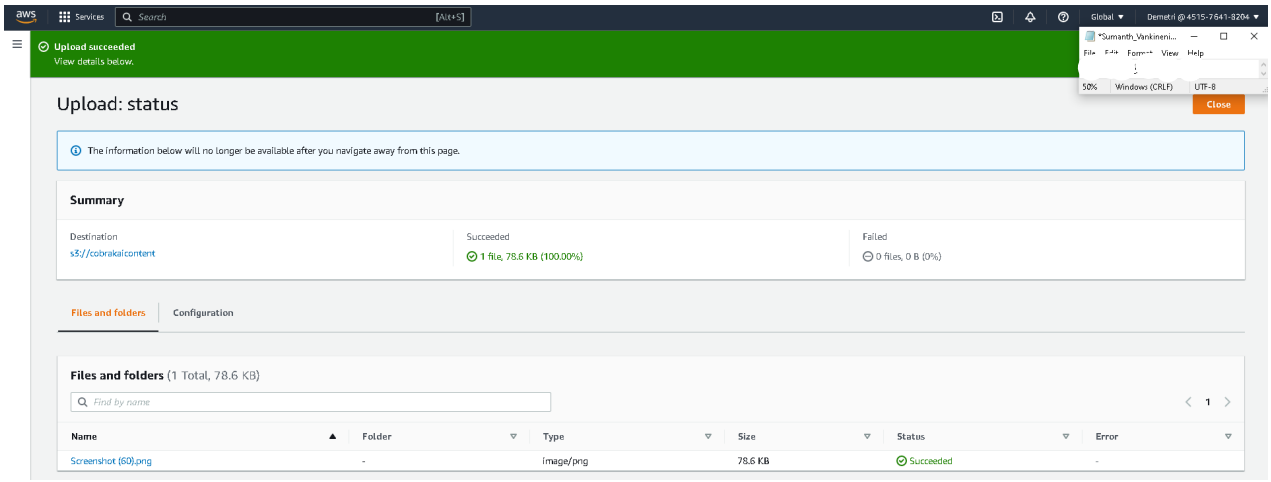


Figure 36: Successfull upload

8. Demetri cannot access the IAM dashboard since in his policy he is denied access to the IAM console(Fig.37).

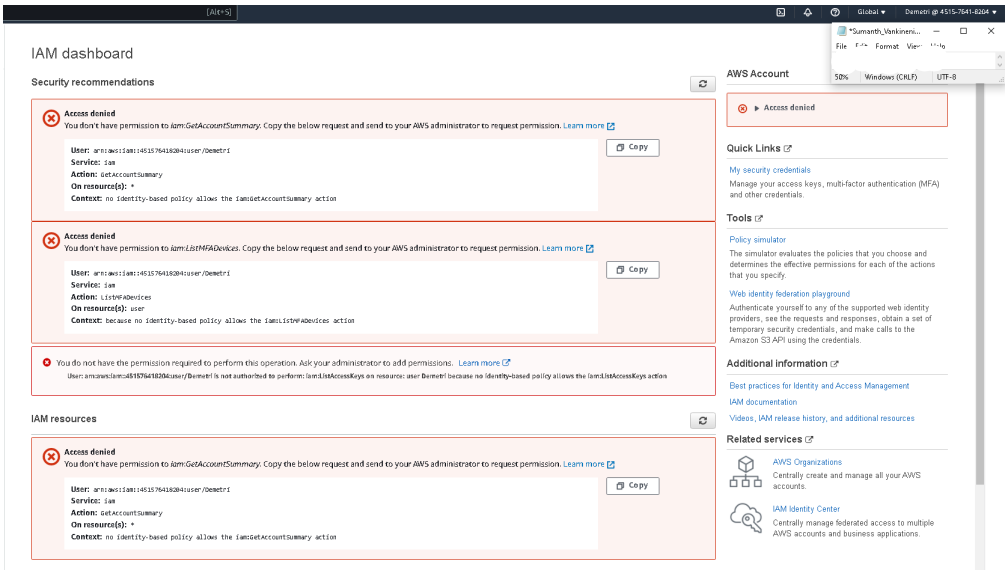


Figure 37: Denied Access

The following policies have been attached to the mentioned users on IAM are shown in the following screenshots(Fig.38)(Fig.39).

USER	POLICY NAME	PERMISSIONS
Johnny Lawrence	ReadOnlyAccess	Read only access to every resource on the AWS account
Miguel Diaz	Data Scientist	AWS Quicksight and AWS EC2 instances
Aisha Robinson	SecurityAUudit	AWS WAF, Route 53, Cloudwatch, SNS, AWS Shield
Eli Moskowitz	Adminstrator Access	All permission on all the resoruces in the AWS account
Demetri	PowerUserAccess	All resources except AWS IAM
Bert	System Adminstrator	Cloudwatch, EC2, AWS IAM, S3, VPC, AWS lambda

Figure 38: IAM users and policies

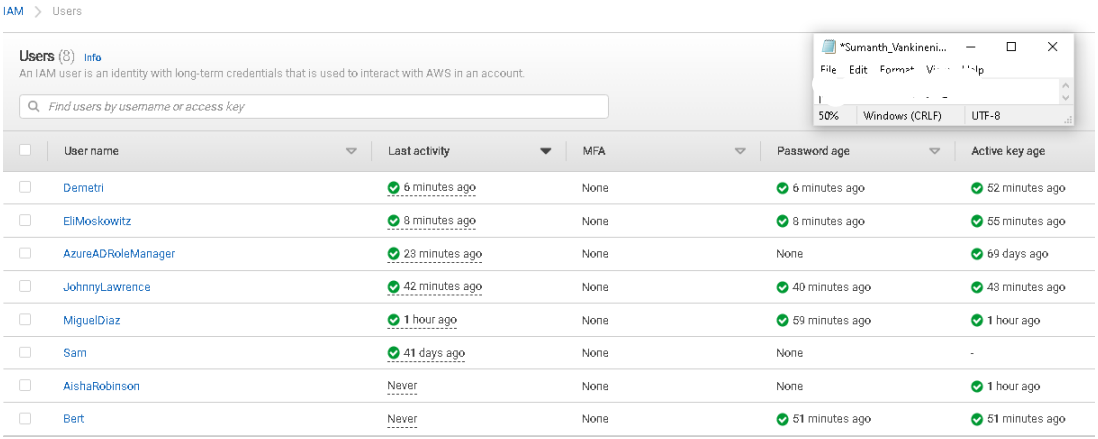


Figure 39: IAM users dashboard

8 Patching Strategy (Using Lambda functions and CloudWatch)

AWS lambda functions paired with the CloudWatch provided by AWS can be used for various functions. Here we have shown how the Cobra Kai server can be shut down at a particular time every week automatically for server maintenance and updates.

1. Create a custom Policy to start and stop the EC2 Instance(Fig.40).

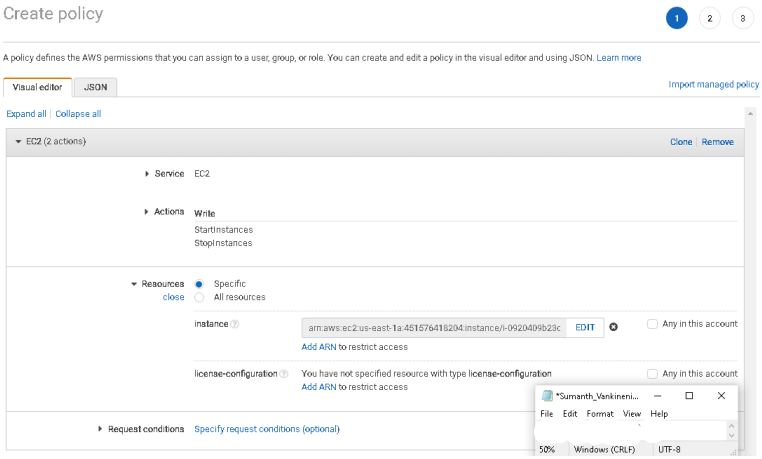


Figure 40: Policy creation

2. Mention the resources, in our case, it's the EC2 instances. Next, specify the ARN and the specific region you want to shut down as shown in the following screenshot(Fig.41).

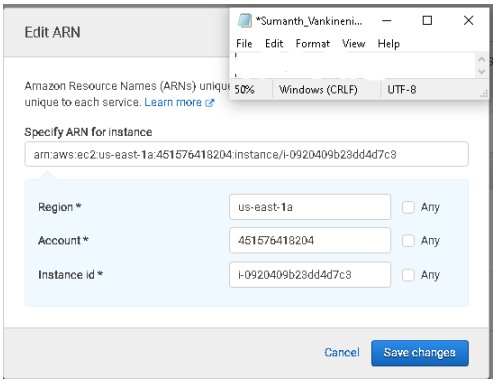


Figure 41: Resources

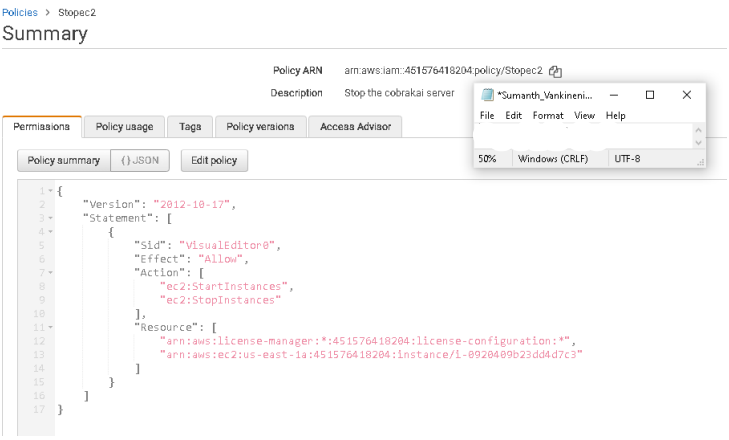
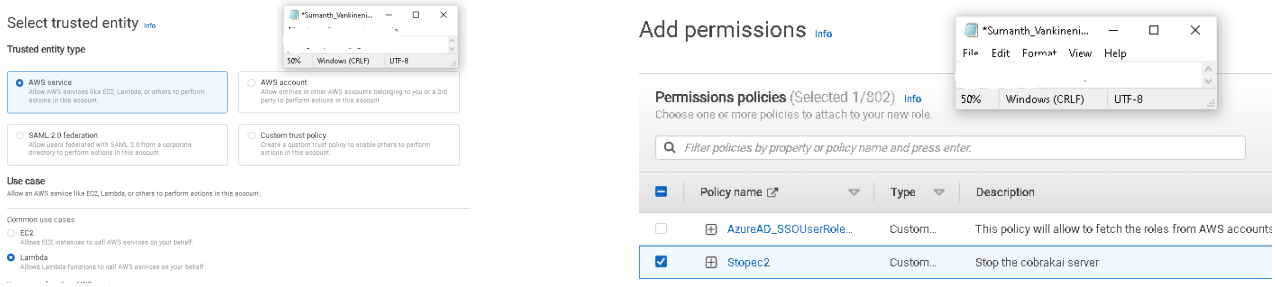


Figure 42: Policy

The above policy describes the action for stopping and starting an EC2 instance(Fig.42).



(a) Entity (b) permissions

Figure 43: Step 3

3. Create a Role using the policy created to Stop the EC2 instance and select the policy created previously to stop the Cobra Kai server(Fig.43a)(Fig.43b).

4. Create a Lambda function using the role created and a small python script to stop the instance(Fig.44)(Fig.45).

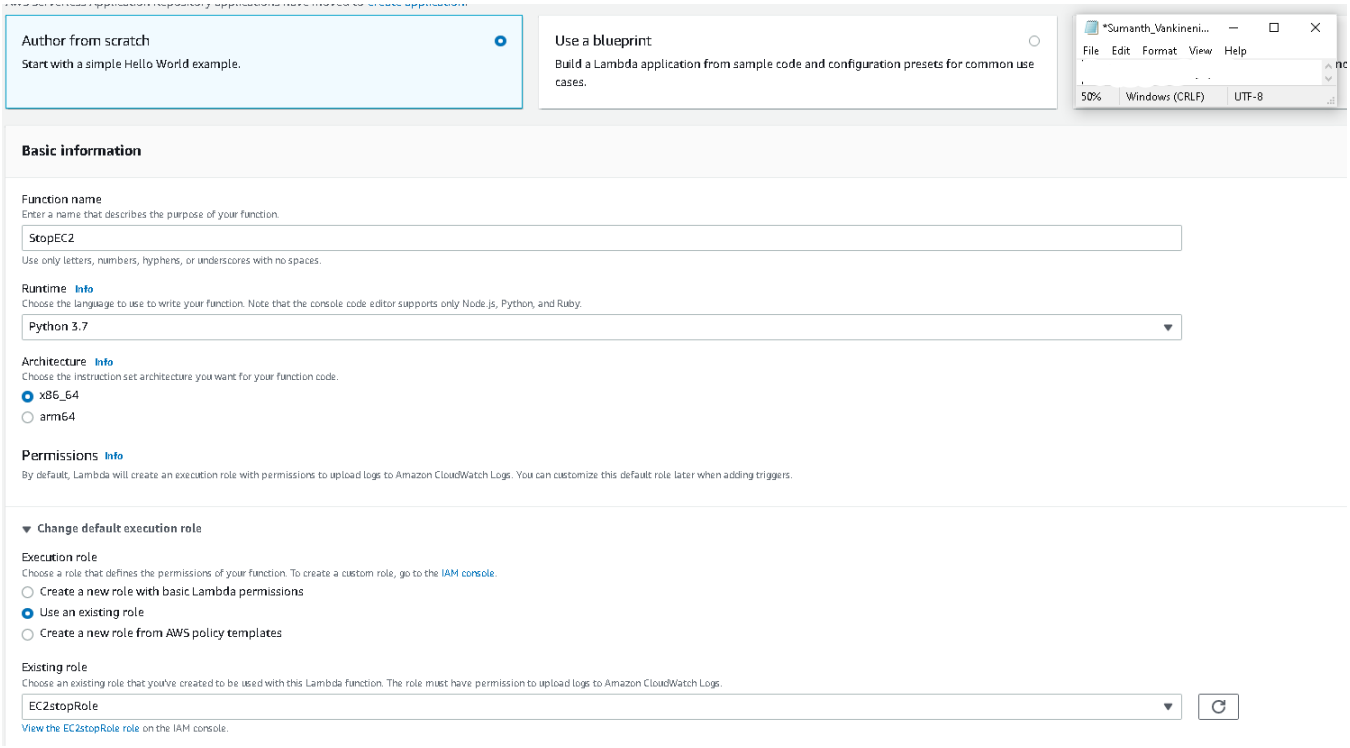


Figure 44: Configuring lambda function

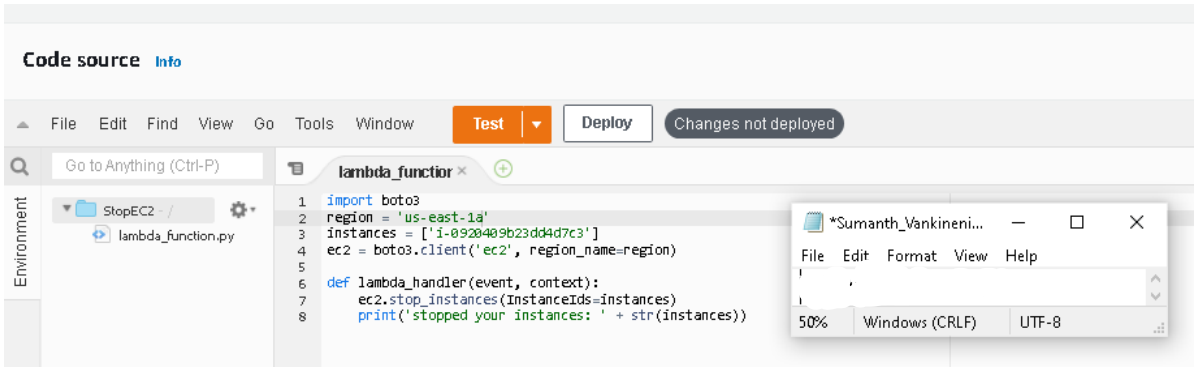


Figure 45: lambda function

5. Create a rule on the CloudWatch to stop the EC2 instance with the given schedules(Fig.46).

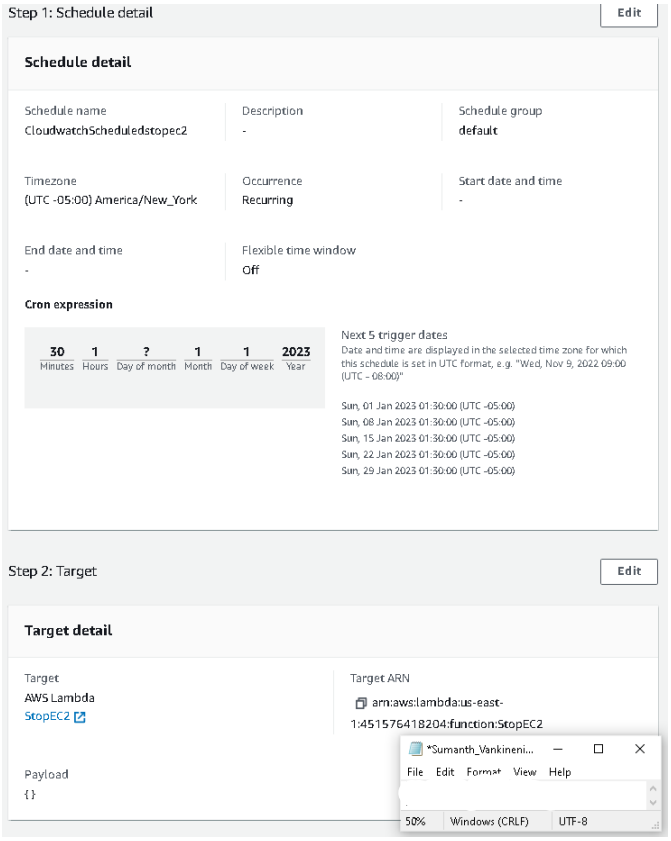


Figure 46: CloudWatch schedule

A recurring schedule is created starting from January 1st of 2023 on the first day of every week at 01:30. With the help of this automated process, the Maintenance and updates for the cobra kai server can be performed without any hassle.

Successful creation of the Schedule to stop the Cobra Kai server in one region(Fig.47).

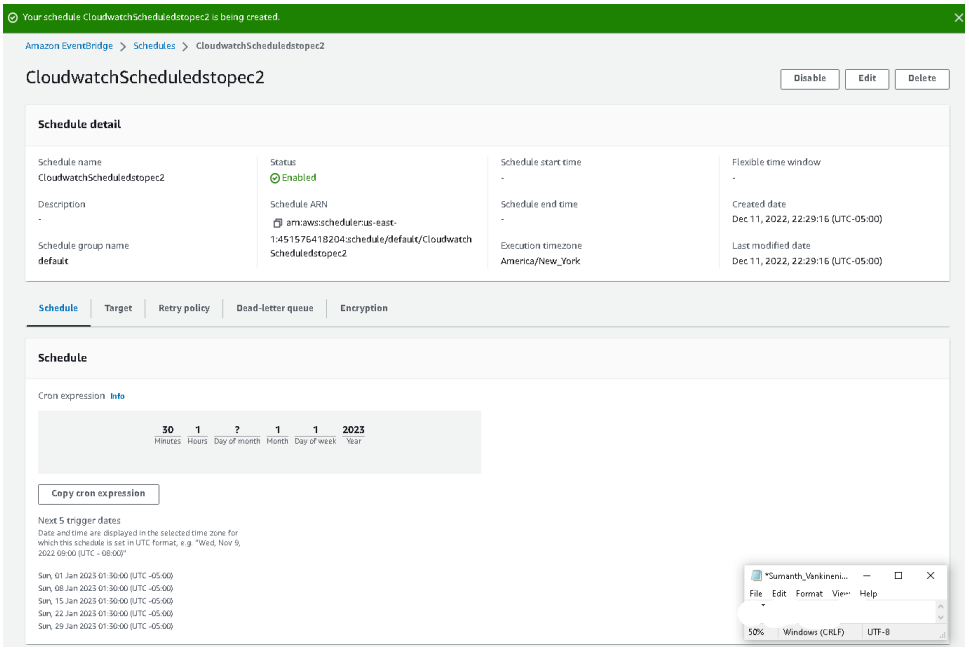


Figure 47: CloudWatch

9 AWS WAF

With the help of the service AWS WAF, Cobra Kai's Security Auditor Aisha Robinson can monitor the HTTP and HTTPS requests that are sent to the resources of your secure online applications. Using the AWS WAF many rules can be configured such as allowing only certain requests or running captcha challenges for the suspected request lists created etc.

9.1 AWS WAF Setup:

Give a name to the WAF and select the resource CloudFront distribution. Rules or groups must be added which define a set of actions that help in the protection of the web application. Since Cobra Kai has a high level of threat from its competitor security measures have to be taken very carefully in order to protect Cobra Kai's data and sensitive information(Fig.48).

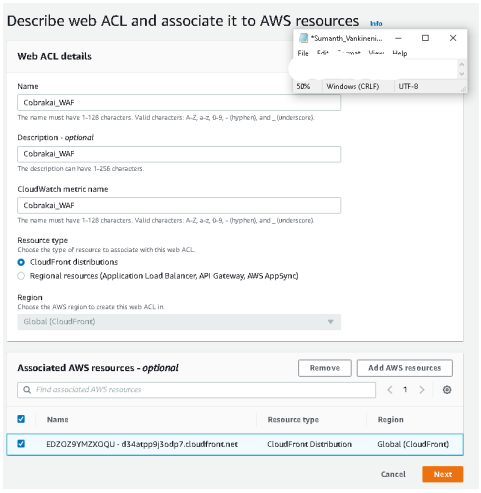


Figure 48: ACL details

- **AdminProtectionRuleSet:** It contains special rules which block any access to the exposed admin pages.
- **AmazonIPRuleSet:** Amazon threat intelligence is used in order to block incoming traffic from sources such as bots and other threats
- **AnonymousIPList:** Incoming traffics which prevents hides the viewer's identity such as VPN and proxies which are blocked by the WAF.
- **KnownBadInputs:**All the requests which contain known bad inputs which are used to exploit and discover the vulnerabilities of the web application are blocked. Using this the process of vulnerability discovery by hackers can be eliminated.

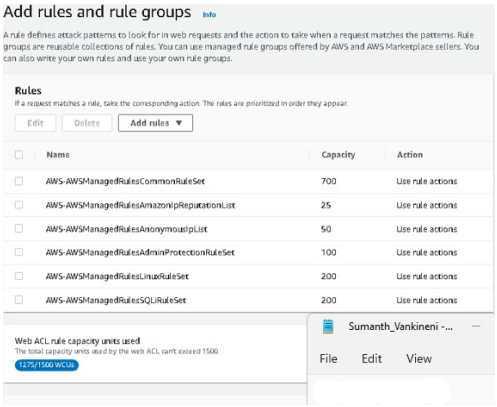


Figure 49: Caption

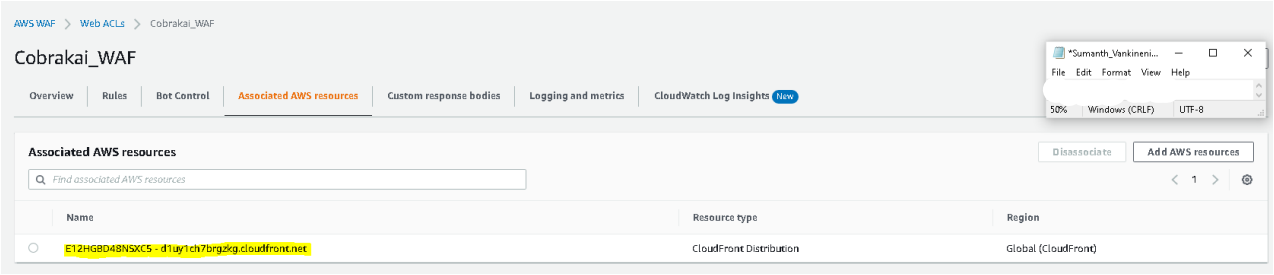


Figure 50: WAF

Navigating to the Cobra Kai web server after setting up the WEB ACLs the webpage is successfully loaded without any errors. Since our IP address is not a threat, we are allowed to access the server and view its contents(Fig.50)(Fig.51).

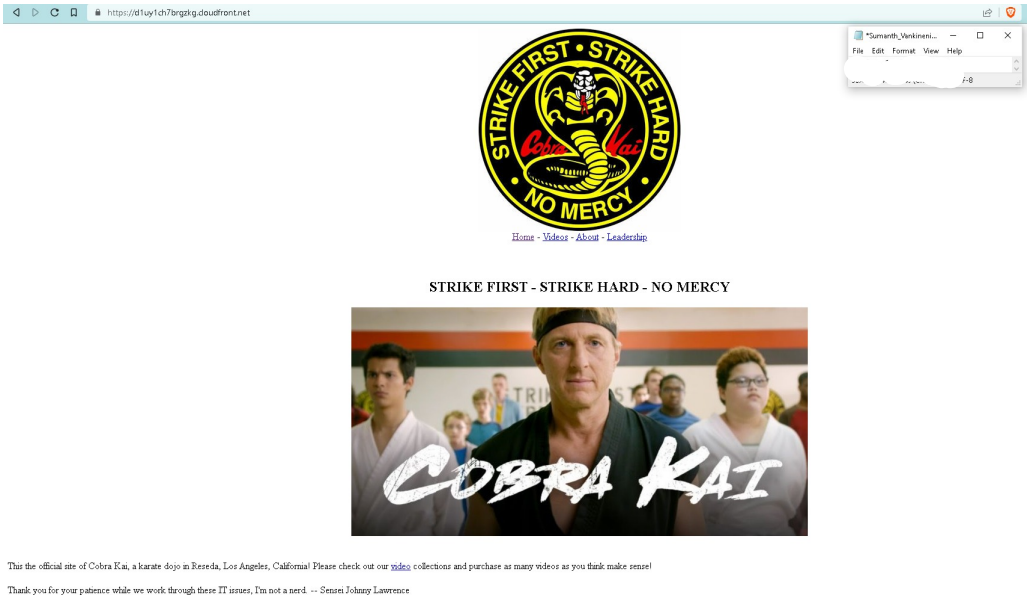


Figure 51: Cobra Kai web server

Additionally, custom rules can be created of choice specify rules and bounds which have to be implemented by the WAF. In the following screenshots, we've demonstrated how the WAF works by blocking our own IP address(Fig.52).

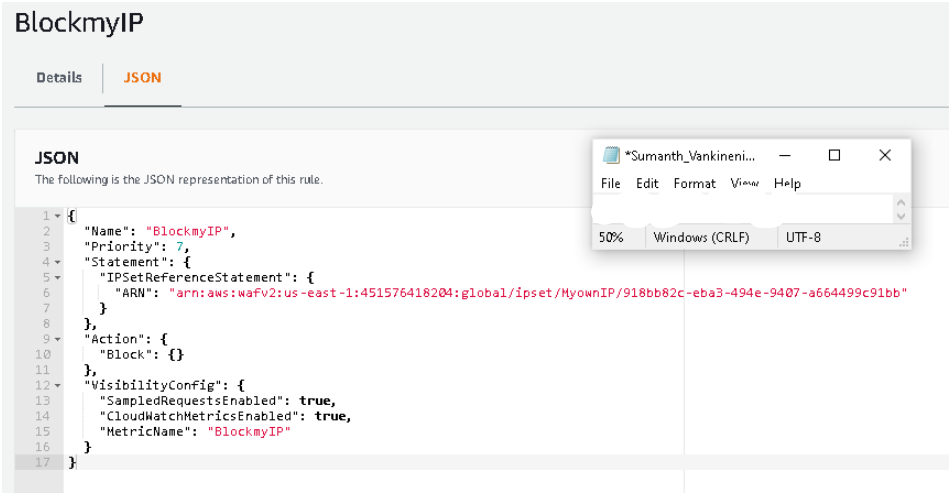


Figure 52: IP block

A custom error page can be configured depending on the rule created. We have set the 403 error to be displayed for the blocked IP users when trying to access the Cobra Kai web server(Fig.53).

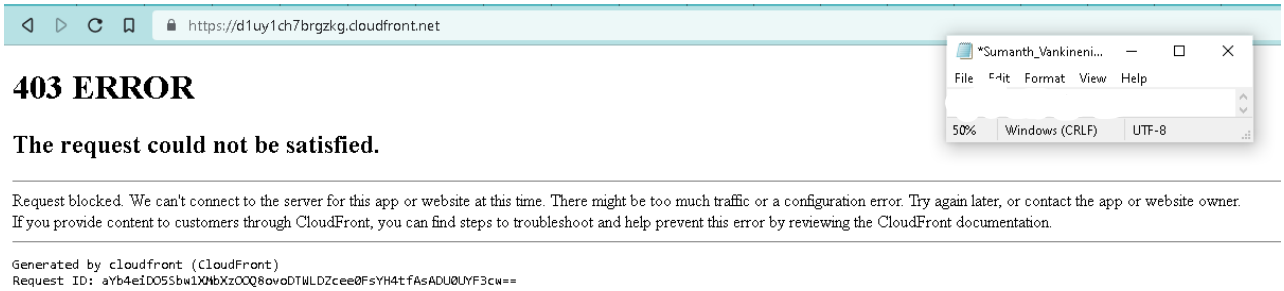


Figure 53: 403 Error

Our recommendation to Cobra Kai is to enable the AWS shield advanced for a higher level of security to protect against threats such as Daniel LaRusso attempting DDoS attacks. Shield Advanced offers further detection and mitigation against big and complex DDoS attacks, near real-time visibility into attacks, and interaction with AWS WAF, a web application firewall, in addition to the network and transport layer protections that come with Standard. AWS Shield Advanced additionally protects Cobra Kai's EC2 instances, Elastic Load Balancer, CloudFront, and Route 53 from DDoS-related surges and gives Cobra Kai's security team 24/7 access to the AWS Shield Response Team (SRT).

10 VPC Firewall

With Amazon Virtual Private Cloud, you may construct a stateful, managed, network firewall and intrusion detection and prevention service for your virtual private cloud (VPC) (Amazon VPC). You can use Network Firewall to filter traffic at the VPC's outer border. This includes NAT gateways, VPNs, AWS Direct Connect, and traffic going to and coming from internet gateways. Suricata, an open-source IPS, is used by the network firewall to perform a stateful inspection(Fig.54).

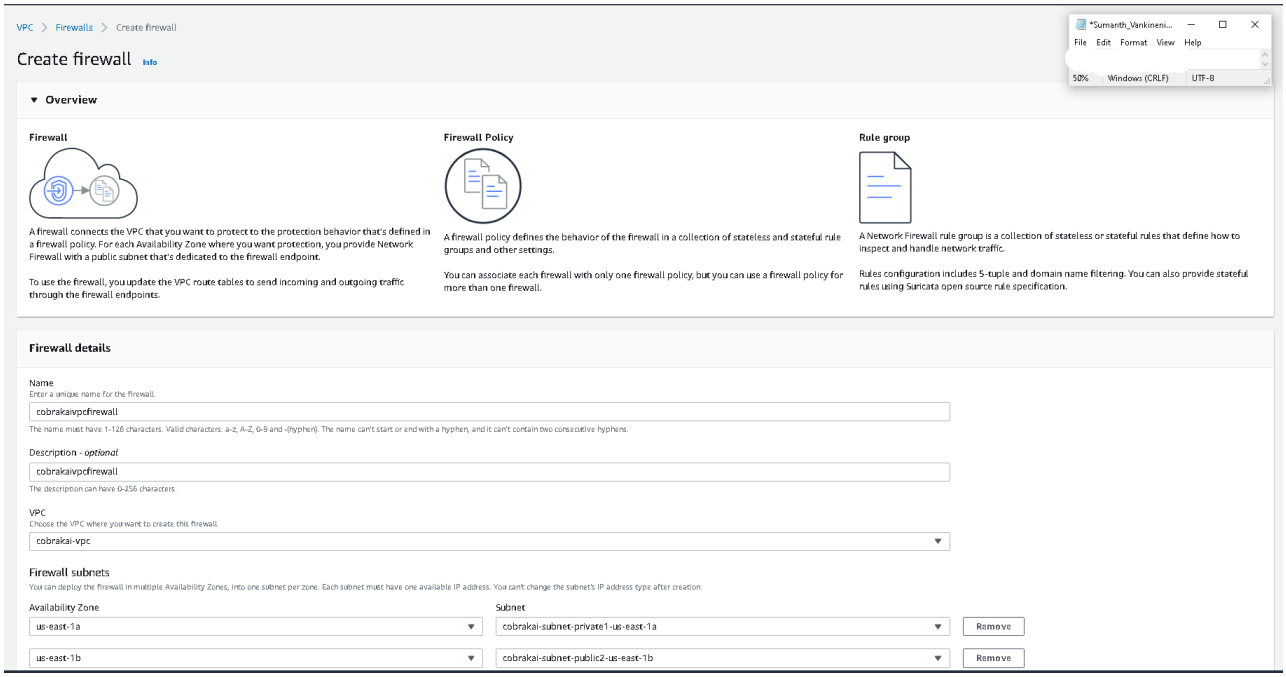


Figure 54: VPC firewall

VPC firewall should be enabled by selecting both the availability zones and the subnets.

11 AWS Cognito

Amazon Cognito offers user management, authentication, and authorization which can be utilized for the users of the Cobra Kai. Either directly with a username and password or through a third party like Facebook, Amazon, Google, or Apple, Cobra Kai users can sign in.
User pools and identity pools are Amazon Cognito's two fundamental building blocks. User pools are user directories that give your app's users sign-up and sign-in alternatives. You can provide your users access to additional AWS services by using identity pools. User pools and identity pools may be used alone or jointly.

11.1 Enabling AWS Cognito

The users should be allowed to have alternatives to sign in to the web server such as a verified phone number and verified email address. Case insensitivity can be enabled for the username only. A lot of attribute options are available to choose from while creating the pool(Fig.**??**).

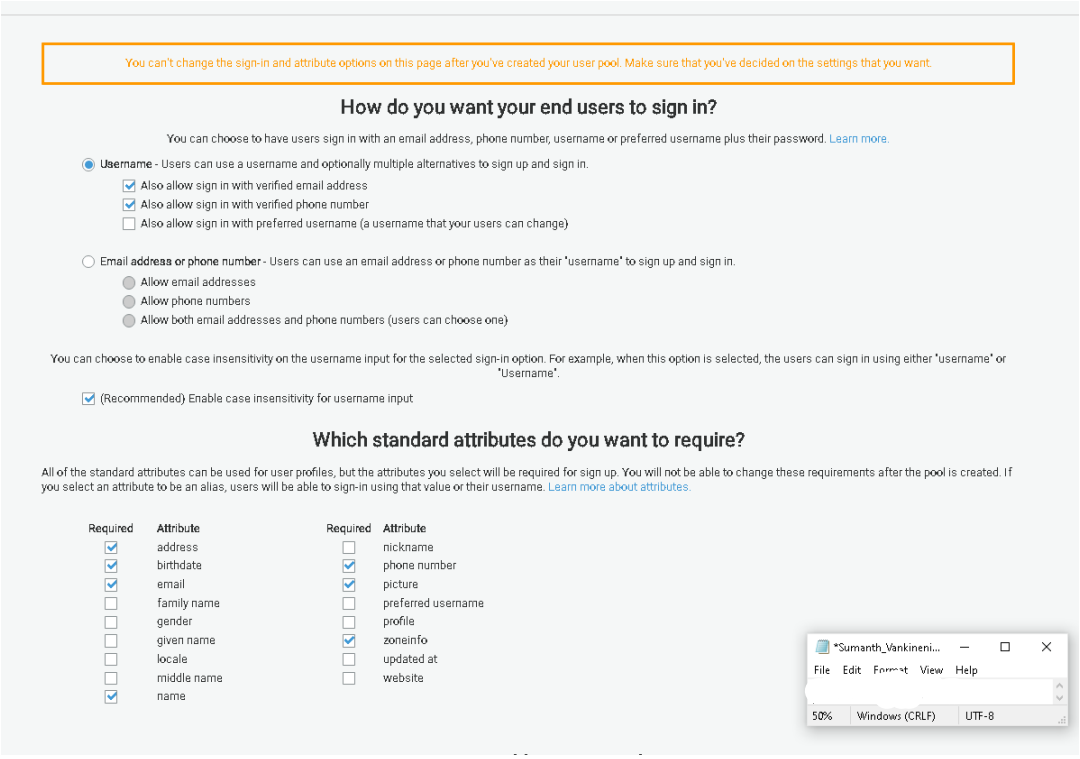


Figure 55: Attributes

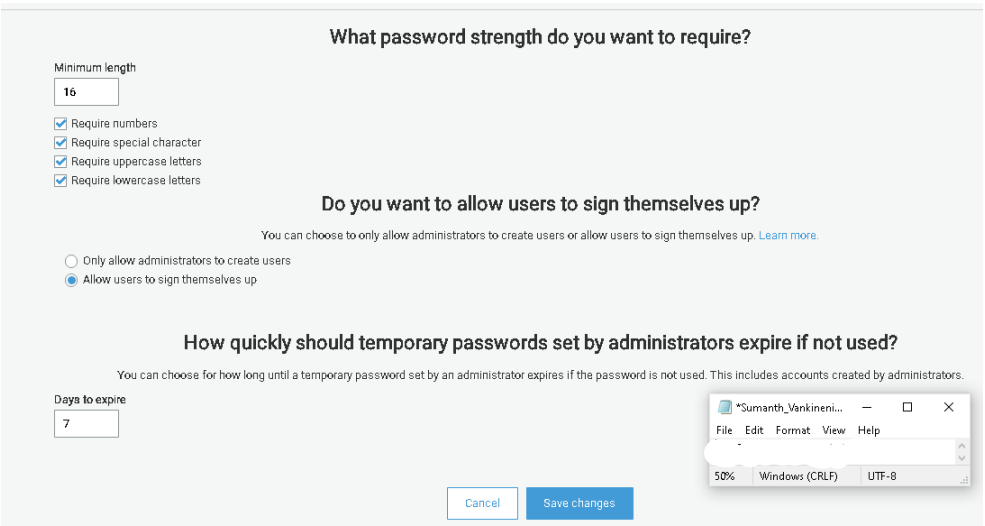


Figure 56: Password strength

The password strength is set to a minimum of 16 for high-security purposes including numbers, special characters, and uppercase and lowercase letters. The new users of Cobra Kai should be able to create an account by themselves without the administrators' interference. The password can be set to expire depending on the value given for the number of days(Fig.56).

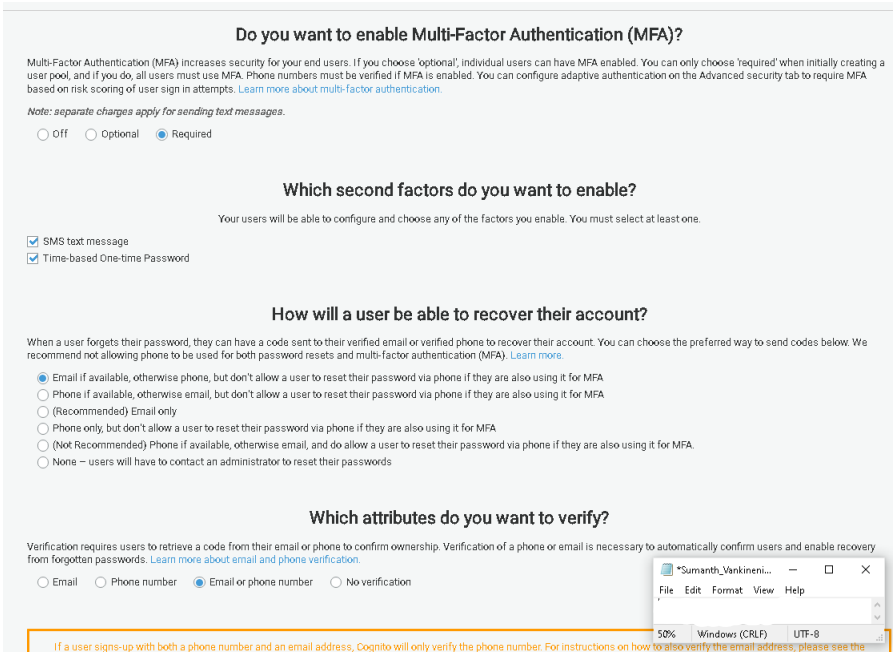


Figure 57: MFA

Multi-Factor authentication is to be enabled mandatorily for all users. Either a text message or a time-based One-time password can be enabled. The users should be allowed to recover their account only via email if the user is using their phone for the MFA(Fig.57).
Workflow triggers can be customized using AWS Cognito using advanced lambda functions.

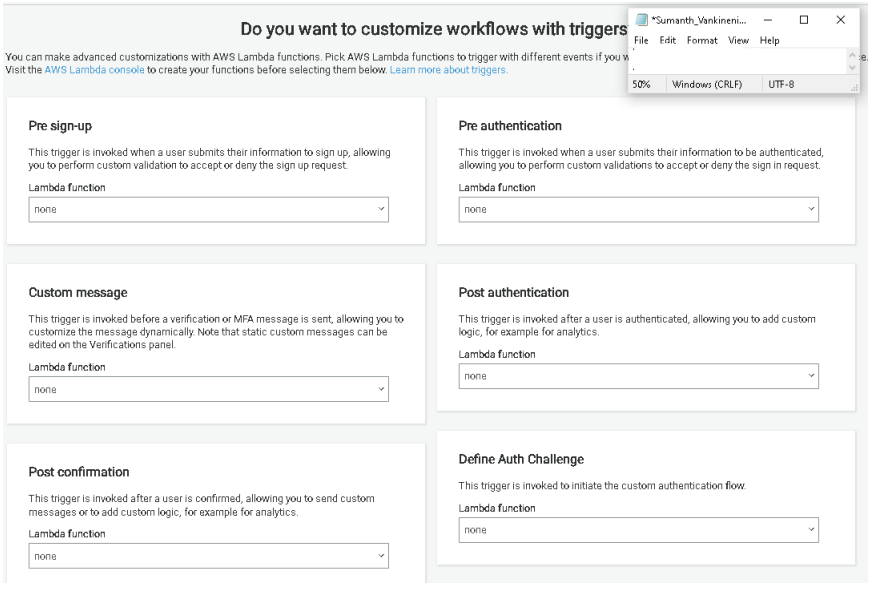


Figure 58: Workflows

Lambda functions can be created for workflows such as Pre signup which is invoked when a user creates an account and the verification has to be performed by the management team. A custom message can be dynamically sent when users are invoked for the MFA. A lot more custom-made workflows can be configured with the help of Aws Cognito(Fig.58).

12 Credit card processing for the Cobra Kai users

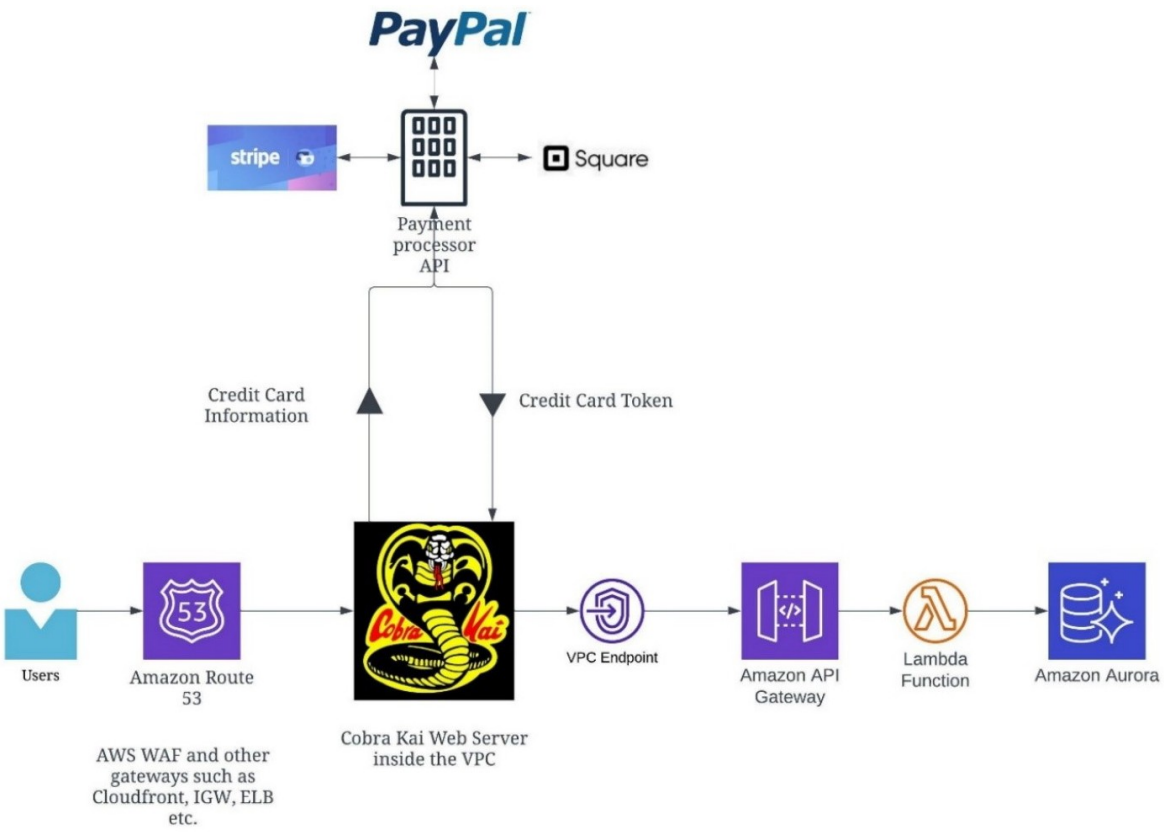


Figure 59: Credit card processing

The users connect to the Cobra Kai web application through Route53 with the security features enabled such as WAF and then further through CloudFront and the ELB. The AWS Cognito is used for user authentication. The payment request is created by the web application to an external payment processor such as PayPal, Stripe, or Square with the credit card information of the user. The payment processor API replies with the credit card token to the Cobra Kai(Fig.59).

The Cobra Kai application forwards this credit card token to the Amazon API gateway through the VPC endpoints. A custom Lambda function is to be created upon which the token is transmitted to the Amazon Aurora where it's stored along with the users' details.

13 AWS GuardDuty

Amazon GuardDuty is a threat detection service used to safeguard Cobra Kai's AWS accounts, Amazon Elastic Compute Cloud (EC2) workloads, container apps, Amazon Aurora databases, and data saved in Amazon Simple Storage Service. To help safeguard workloads and data on AWS, GuardDuty integrates machine learning, anomaly detection, network monitoring, and malicious file identification, employing both AWS-developed and prominent third-party sources. Tens of billions of events can be analyzed by GuardDuty from a variety of AWS data sources, including DNS query logs, Amazon Virtual Private Cloud (VPC) flow logs, and AWS CloudTrail event logs. GuardDuty can easily be enabled with the click of a button(Fig.60).

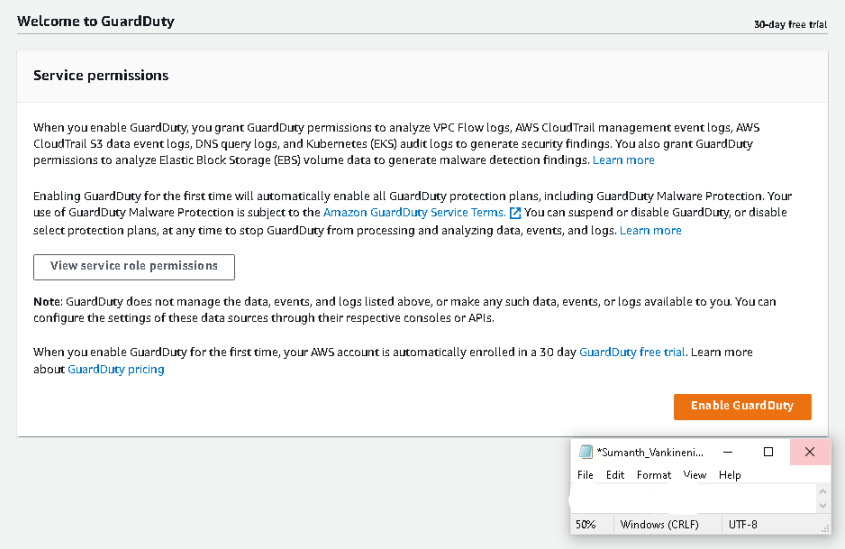


Figure 60: Enabling GuardDuty

Sample findings have been created to demonstrate how the AWS GuardDuty would display any finding ina real scenario(Fig.61).

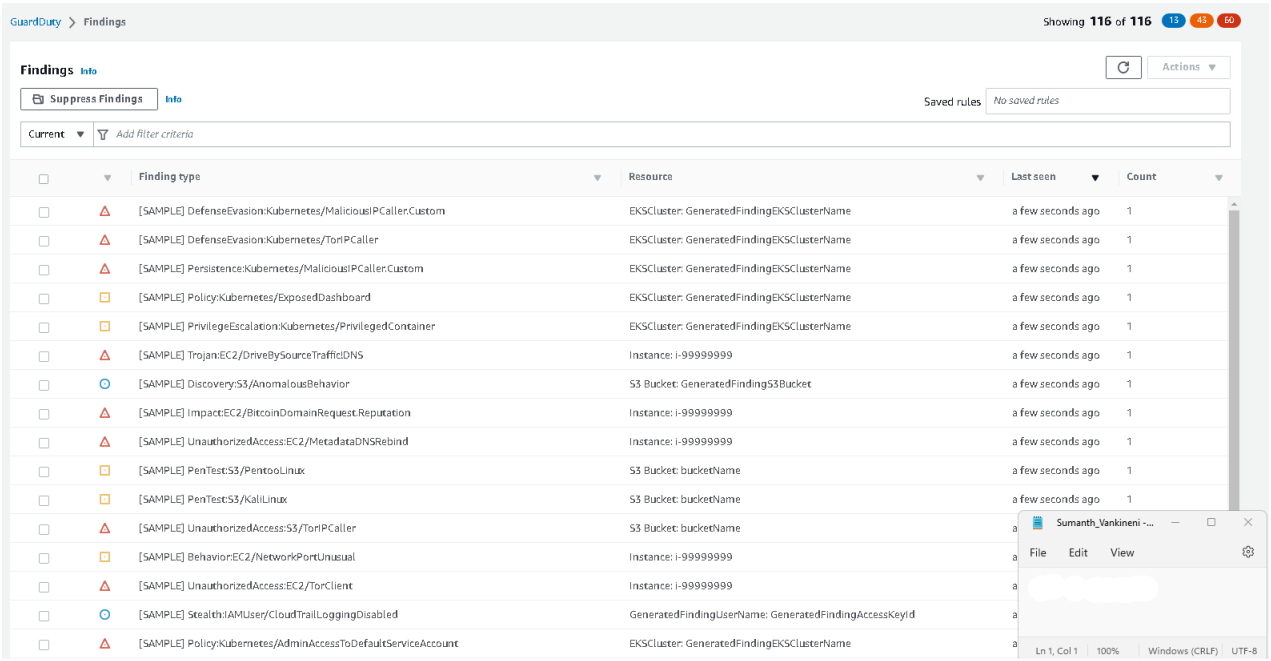


Figure 61: Sample findings

14 References

1. https://aws.amazon.com/datasync/
2. https://docs.aws.amazon.com/datasync/latest/userguide/what-is-datasync.html
3. https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html
4. https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/what-is-load-balancing.html
5. https://aws.amazon.com/autoscaling/
6. https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/Introduction.html
7. https://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/getting-started-secure-static-website-cloudformation-template.html
8. https://docs.aws.amazon.com/waf/latest/developerguide/what-is-aws-waf.html
9. https://aws.amazon.com/shield/features/
10. https://docs.aws.amazon.com/cognito/latest/developerguide/what-is-amazon-cognito.html
11. https://aws.amazon.com/guardduty/features/