



Cobra Kai – Cloud Migration Strategies

NOTE

Upon thoroughly assessing the background of **Cobra Kai**, this personalized report-cum-playbook is documented, which governs the structure of the organization and suggests how the process flow of the current services offered by the company can be improvised and be efficiently delivered to its customers hasslefree.

Existing Challenges at Cobra Kai



1. Security Point-of-View

- a. Application is directly exposed to the internet and there is no security around the application.
- b. The architecture framework of the system is very primitive and vulnerable to cyber attacks.
- c. There is no system administration. At the moment, all permissions and privileges of the entire application are available to all employees. Basically, everyone has root/admin access to do anything.
- d. Patch Management and Updating of operating system and underlying software - Not regulated.
- e. No data backup and recovery in case of compromise, data loss or system failure.

2. No PCI Compliance (Payment Card Industry)

- a. No standards, existing laws or policies that cater the PCI Compliance
- b. Cardholder information is stored but in a highly insecure way. Unsafe for both merchant and customers.
- c. Non-compliance to PCI could miss out on a large amount of sales by losing the privilege to accept online credit card payments.

3. Performance Inefficiency

- a. Data processing for small number of people , Multi-national audience 
Scaling of existing of business is a necessity.
- b. High Traffic of HTTP requests by users resulting in an increased load on the 3 app-servers.
- c. Underperforming hardware resulting in laggy user experience.
- d. Lack of a CDN (Content Distribution Network)

Plausible Solution

Cloud to the rescue!

a. But what is Cloud?

In really simple words, Cloud is someone else's high performing computer that you lease from them.

b. Why Cloud?

The key benefit of cloud computing is that more people and businesses today have access to a lot more computing power than ever before, and access to this computing power is *from any place in the world* that has Internet connectivity.

c. How migrating to Cloud can help Cobra Kai?

- Pay as you go - No long term contracts or capital expenses on infrastructure.
- Elasticity - If 3 web servers are not sufficient for your business, you can take 10.
- Self-provisioning of resources - Get a server with the click of a button.
- Massive scalability - Have global customers? Set up servers across the world, increase speed of access
- Resiliency - Migration to Cloud protects web-based applications against DDoS (Distributed Denial of Service) attacks, where a cyberattack affects the system's bandwidth and makes the computer unavailable to the user.
- Better than on-prem infrastructure, as you can cut down costs of
 - Licensing
 - Servers
 - Storage
 - Network Infrastructure

d. Why migrate to AWS?

One of the top AWS advantages is its pricing model. AWS platform works on the pay-as-you-go pricing model. The flexible pricing structure drastically improves the organizational bottom line, keeping cloud computing affordable. You don't have to pay heavy subscription fees for resources that you won't even use.

Migration Steps & Strategies

Step 1 : Analysis and Planning

There are 6 common migration strategies typically used by businesses big and small. They are,

1. Re-hosting or “Lift and Shift”
2. Re-platform
3. Re-factor/Re-architect
4. Revise
5. Rebuild
6. Replace

After evaluating the problems and assessing the business-case of **Cobra Kai**, the best recommended migration strategy would be to “Re-platform”, based on the following analysis,

- This methodology allows businesses to maximize their own resources and focus on its priorities by shifting the administrative burden to the cloud service provider at a **reasonable cost** premium.
- The integration of key technologies present in the cloud environment like a database-as-a-service such as the Amazon Relational Database Service (RDS), which offloads **patching and administration** to the cloud service provider, could prove essential as currently these are NOT being take care of, in the on-prem operations.
- The **downtime** involved in data transfer from on-premises to the cloud is comparatively low. Therefore, streaming and video hosting for the customers can resume at the earliest using this strategy.

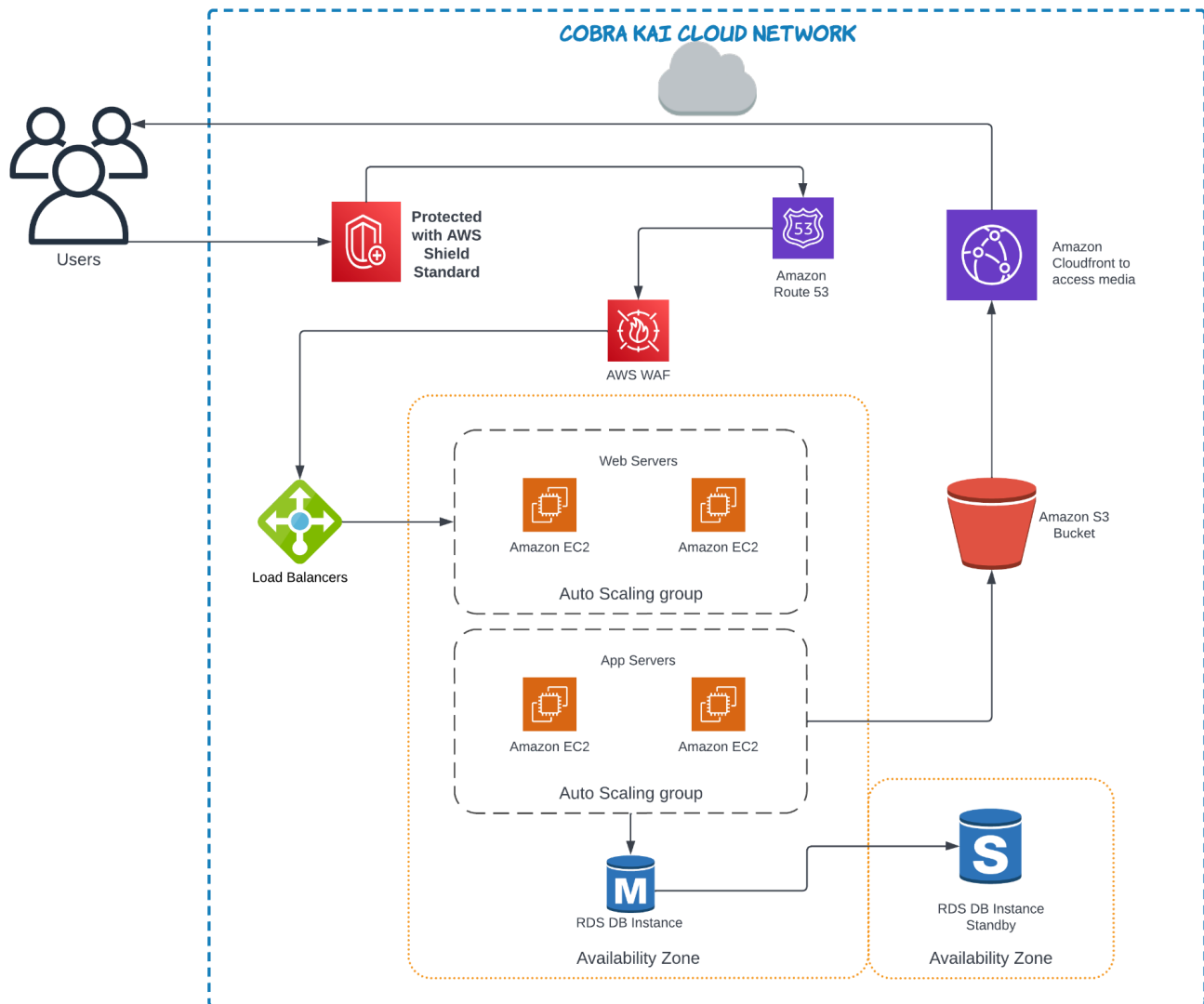
Step 2 : Areas to Focus

There are a few essential domains to plan and take care of, before performing the migration of the entire on-prem architecture. They are,

1. Rearchitcting the Existing Architecture
2. Estimating current infrastructure costs
3. Identity and Access Management (IAM)
4. Resiliency and DDoS Protection
5. Performance Optimization (Scalability and Load Balancing)
6. Data Storage and Backup
7. PCI Compliance and Data Protection
8. Coding Practices

Step 3 : Migration Work-flow

1. Refurbished Architecture diagram



2. Current Estimated infrastructure costs

Direct Costs	Indirect Costs
Physical Servers	Non-compliance Penalties
Operating System License	Unplanned Downtime
Softwares License	Poor equipment reliability
Maintenance Contracts	
Warranties	
Database Storage	
Electricity	
Labor Costs	

As a result, organizations that deploy software on-premise must bear the continuous expenditures of server hardware, power usage, and space. Enterprises who utilize a cloud computing model just pay for the resources they use, with no maintenance or upkeep charges, and the price changes up or down based on how much is consumed.

3. Identity and Access Management (IAM)

- Currently, there is no system administration and management, and any employee can run any type of commands across the system. Basically, everyone has access to everything, which is highly insecure. Thus, having a system administrator manage the root/admin account and create users and groups for employees accessing resources, can evaluate permissions and only give access to what is required.
- IAM adds an extra layer of security over the network. Having multiple authentication factors can prevent breaches in the network, like usage of MFA apart from passwords.
- Users and Groups management will not only be useful in managing the lifecycle of employees, but limiting the end-user access to resources will only shorten the blast radius in case of an identity theft or data breach within the organization.
- Mainly, AWS does not charge for IAM, so strengthening the security of services at **Cobra Kai** with no extra costs is another driving factor to consider.

4. Resiliency and DDoS Protection

- Resiliency for a business is mainly about continuity without any disruptions. Planning for known threats like DDoS isn't enough, there must be a plan for unknown threats as well. Testing the workflow during power outages, hardware failures, ransomware and flooding, is essential.
- Observing the mal-intent of the adversaries of **Cobra Kai**, trying to disrupt its services, placing a DDoS protection service like AWS Shield will safeguard the application when it runs on AWS.
- Using AWS shield will automatically dump bad traffic, minimize application downtime, and finally reduce latency. Due to this, issues like slow streaming, downloads and order processing could be overcome.
- Apart from this, attackers on the application can sometimes try to exploit the employees, to gain access to the internal network. For this, a managed service like AWS WAF can be used to allow or block requests based on a set of rules in a web access control list.
- Additionally, Amazon EC2 enables you to scale up or down to handle changes in requirements or spikes in popularity, reducing your need to forecast traffic.

5. Performance Optimization (Scalability and Load Balancing)

- In order to meet the rising demand for the training offered by **Cobra Kai**, it is important to ensure a seamless and non-disruptive live streaming service. The AWS Auto Scaling service monitors applications and automatically adjusts capacity to maintain steady, predictable performance at the lowest possible cost.
- To ensure High Availability of the application, the addition of a load balancer would help by distributing incoming traffic across multiple EC2 instances in different Availability zones. This way, the entire traffic wouldn't need to be handled by one web-server instance. An Elastic Load Balancer is designed to handle traffic as it grows and can load balance millions of requests/sec.
- Apart from these, for enhancing performance a Content Delivery Network like Amazon CloudFront start streams quickly, plays them with consistency, and delivers high-quality video.

6. Data Storage and Backup

- Currently, all the video training data at **Cobra Kai** is being stored in a hard-disk which is highly risky because it is prone to physical failure and thus data loss. Also, in case of a ransomware attack, the video files and customer data on a local drive might be unencrypted and can be easily compromised.
- Therefore, to solve this issue Amazon Simple Storage Service (Amazon S3), which is an object storage service that offers industry-leading scalability, data availability, security, and performance, can be used.
- Amazon S3 along with a managed service like Amazon RDS, creates and saves automated backups of the DB instance securely in Amazon S3 bucket. RDS also handles patching and administration.
- More importantly, Amazon RDS helps organizations handle relational database management tasks such as migration, backup, recovery and patching, which will be useful during the shift from on-prem to cloud.

7. Data Protection and PCI Compliance

- Since **Cobra Kai's** platform is processing the usage of Credit cards, there are a set of security standards that are designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment. But all the Cardholder data that is currently stored is unencrypted in the database. If in case the system ever gets compromised, all the customer data will be exposed to the internet.
- Therefore, the usage of Amazon RDS could help as stored data is encrypted in DB instances, which use the industry standard AES-256 encryption algorithm to encrypt it, on the same server that hosts the Amazon RDS DB instances.
- PCI compliance requires adherence to the six control objectives, or goals, outlined in the PCI DSS. They are, building and maintaining secure network and systems, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, monitoring and testing networks regularly, and lastly constructing an information security policy.

8. Coding Practices

- It is important to note that the current web application is very insecure and directly exposed to the internet which is highly vulnerable to attacks. The fact that cloud service providers have a relatively high security wouldn't be very relevant if the service being hosted on the cloud is very vulnerable.
- One mistake can lead to the loss of sensitive data so instead of taking chances, automation can be used to eliminate the possibility of human error. Security automation can help developers speed up the development process and should be made a regular practice.
- Code scanning tools can help developers detect vulnerabilities that the chosen programming language can cause. These tools analyze code and raise flags on the possible issues to fix. Using automated tools can help developers at **Cobra Kai** test and develop code efficiently and re-build the platform better.
- Building and testing a developed code isn't enough, old code needs to be reviewed from time to time. Code review not only helps developers learn a code base well, it also helps them learn new technologies that could be essential for incorporating in the existing code.

References

1. On Premise vs. Cloud: Key Differences, Benefits and Risks -
<https://www.cleo.com/blog/knowledge-base-on-premise-vs-cloud>
2. Amazon IAM Documentation -
https://docs.amazonaws.cn/en_us/IAM/latest/UserGuide/introduction.html
3. Amazon Cloudfront Documentation -
<https://aws.amazon.com/cloudfront/>
4. Amazon Elastic Load Balancing Documentation -
<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html>
5. Amazon S3 Documentation -
<https://docs.aws.amazon.com/AmazonS3/latest/userguide/Welcome.html>
6. Amazon EC2 Auto Scaling Documentation -
<https://docs.aws.amazon.com/autoscaling/ec2/userguide/auto-scaling-groups.html>
7. Amazon RDS Documentation -
<https://aws.amazon.com/rds/faqs/>
8. Amazon AWS Shield Documentation -
<https://aws.amazon.com/shield/>
9. What is PCI Compliance? - Digital Guardian -
<https://digitalguardian.com/blog/what-pci-compliance>
10. Secure Coding Best Practices and Its Checklist -
<https://www.xenonstack.com/blog/secure-code-best-practices>



Cobra Kai

Technical Documentation for Cloud Migration

Created by **Aaryash** Raj Sinha
UID 119222119

Table of Contents

Table of Contents	2
Migration Steps & Strategies	3
1. Planning the Migration	3
2. Roadmap for Migration	3
Infrastructure Planning	4
1. Refurbished Architecture diagram	4
2. Security and Networking	4
a. IAM	4
b. VPC	7
c. NACL	8
d. Security Groups	9
Data Management	10
1. S3 Buckets	10
2. EC2 Instances	12
3. EBS Volumes	13
4. Data Encryption	13
Performance Optimization	14
1. Resiliency	14
a. Elastic Load Balancing	14
b. Auto Scaling	16
c. Cloudfront	17
2. DDoS Protection	18
d. CloudWatch	18
e. Route53	19
f. Shield	20
g. WAF	21
Coding Practices & PCI Compliance	22
System Adminsistration	24
References	25

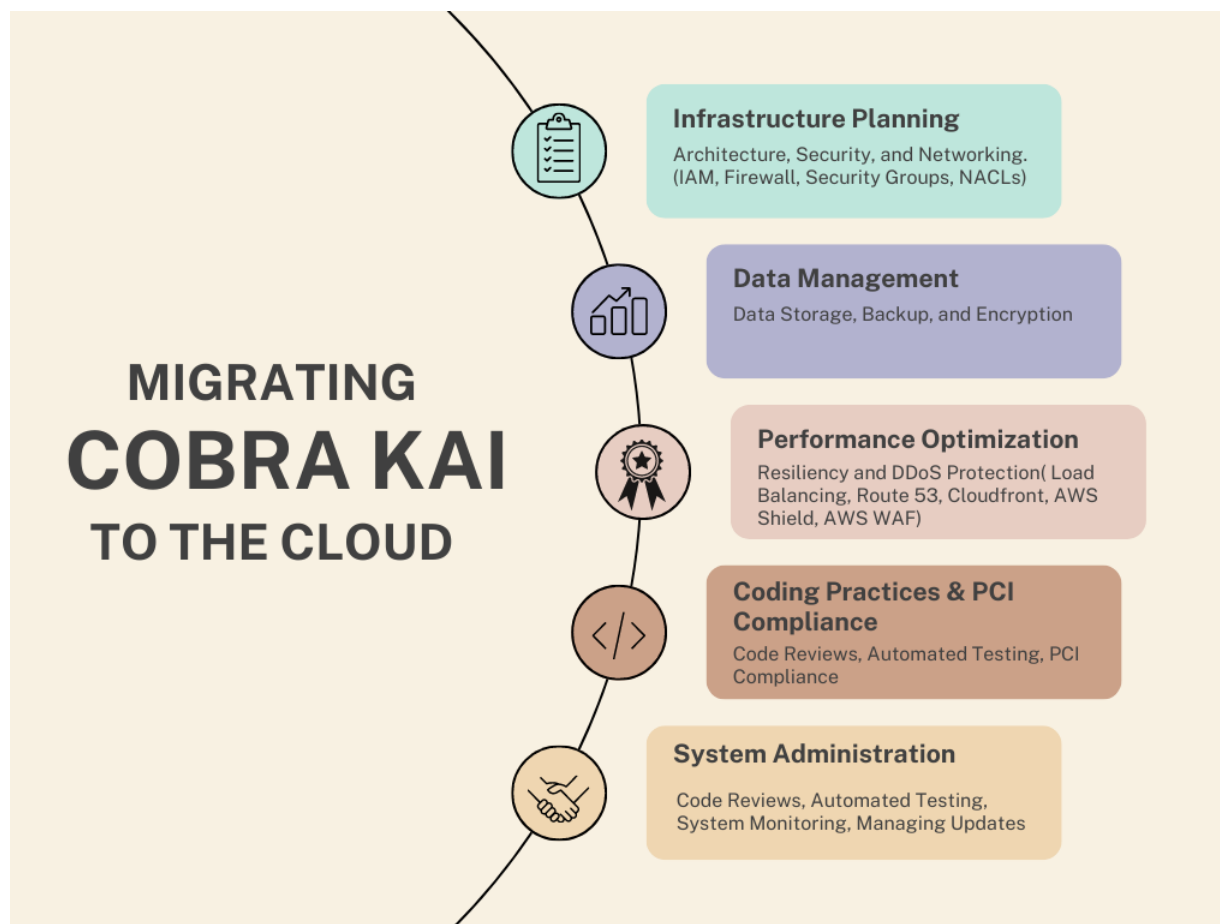
Migration Strategies

This document outlines the technical plan for migrating the **Cobra Kai** application to the cloud. The plan includes considerations for resiliency, identity and access management (IAM), data protection, compliance, secure system administration, and coding practices. Moreover, as **Cobra Kai** Web Application does not currently provide video-on-demand services or credit card processing, additional considerations has been taken into account in order to adequately handle large files and the processing of credit cards (PCI).

1. Planning the Migration

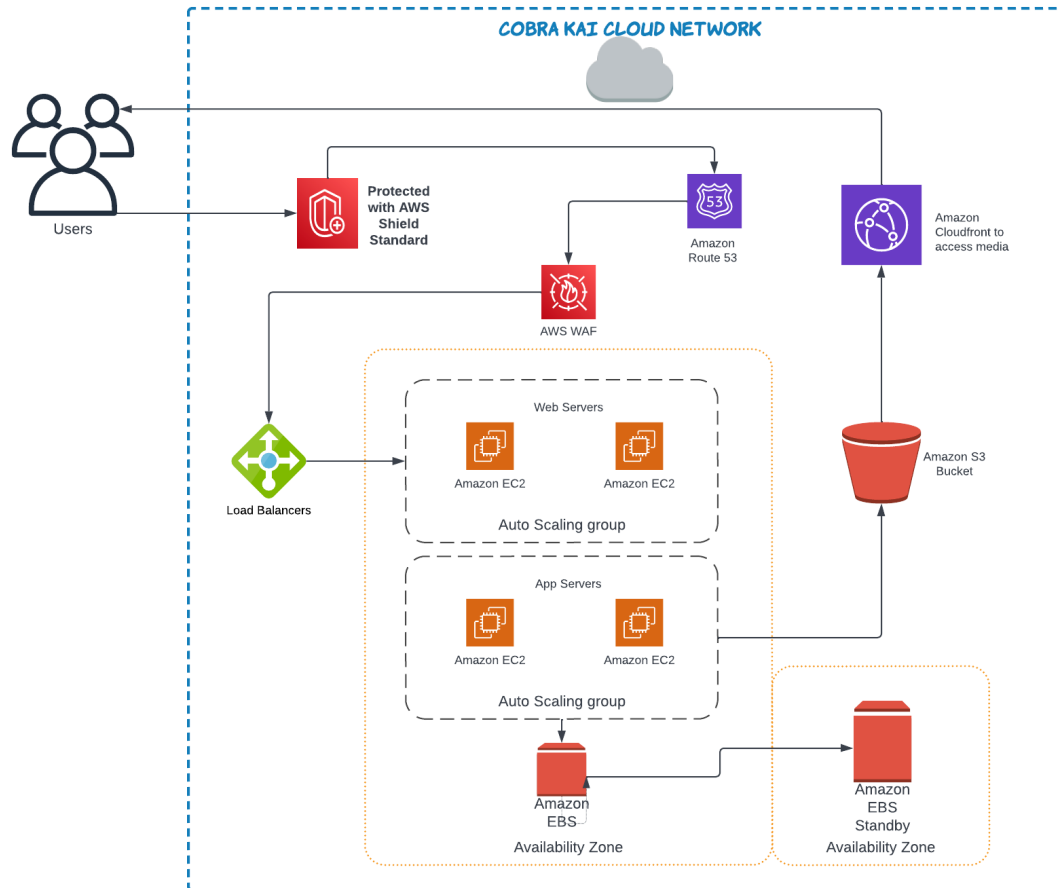
Replatform Cloud Migration Strategy would be suitable for a business like **Cobra Kai**, as it allows the team to migrate the existing application and workload to the cloud without having to rewrite the code. Replatforming can be secure when done correctly however, it is important to ensure that the security practices are being followed during the process.

2. Road Map for Migration



Infrastructure Planning

1. Refurbished Architecture diagram



2. Security and Networking

Cobra Kai's cloud migration should include measures to ensure security and networking. Therefore, **Cobra Kai** should implement an **Identity and Access Management (IAM)** system to ensure that only authorized users are able to access the system. This system should include measures such as multi-factor authentication, role-based access control, and regular audits to ensure that user access is appropriate.

Furthermore, security measures should also include the use of **Virtual Private Clouds (VPCs)** to isolate the cloud resources. A step-by-step description for setting up a **VPC** for **Cobra Kai** has been elucidated below.

Additionally, since **Cobra Kai** offers on-demand video streaming service, both **Network Access Control Lists** and **Security Groups** could be used to ensure a secure cloud environment. **NACLs** could be used to control ingress and egress traffic, while security groups could be used to control access to resources.

A) Identity and Access Management

For **IAM**, Considering the individual roles of **Cobra Kai's** Team, the following user-roles should be created:

- **Johnny Lawrence** – Owner role, with access to all resources

IAM Roles - AmazonIAMFullAccess, AmazonEC2FullAccess, AmazonRDSFullAccess, AmazonS3FullAccess, AmazonCloudWatchFullAccess, AmazonCloudFrontFullAccess, AWSWAFConsoleFullAccess, AmazonInspectorFullAccess

- **Miguel Diaz** – Read-only access to all resources

IAM Roles - AmazonIAMReadOnlyAccess, AmazonEC2ReadOnlyAccess, AmazonS3ReadOnlyAccess

- **Aisha Robinson** – Security Administrator role, with access to all security-related resources

IAM Roles - AmazonIAMFullAccess, AmazonGuardDutyFullAccess, AmazonInspectorFullAccess, AmazonCloudWatchFullAccess, AWSWAFConsoleFullAccess

- **Eli Moskowitz** – Read-only access to all resources

IAM Roles - AmazonIAMReadOnlyAccess, AmazonEC2ReadOnlyAccess, AmazonS3ReadOnlyAccess

- **Demetri** – Web Developer role, with access to web development and deployment resources

IAM Roles - AmazonS3FullAccess, AmazonEC2FullAccess, AmazonCloudFrontFullAccess, AmazonCloudWatchFullAccess

- **Bert** – System Administrator role, with access to system administration and server management resources

IAM Roles - AmazonEC2FullAccess, AmazonVPCFullAccess, AmazonRoute53FullAccess, AmazonS3FullAccess, AWSWAFConsoleFullAccess

More information about what each of these roles is explained below.

AmazonIAMFullAccess: This role provides full access to all features of Amazon Identity and Access Management (IAM). It allows users to manage user permissions, create and manage IAM policies, and manage multi-factor authentication settings.

AmazonEC2FullAccess: This role grants full access to all features of Amazon Elastic Compute

Cloud (EC2). This includes the ability to create, modify, and delete instances, manage security groups, and control access to Amazon Machine Images (AMIs).

AmazonRDSFullAccess: This role provides full access to all features of Amazon Relational Database Service (RDS). This includes the ability to create, modify, and delete databases, manage database security, and manage database parameters.

AmazonS3FullAccess: This role grants full access to all features of Amazon Simple Storage Service (S3). This includes the ability to create, modify, and delete buckets, manage security policies, and manage access to Amazon S3 objects.

How to assign IAM Roles to Cobra Kai's Team?

1. Log into the AWS console.
 2. Navigate to the IAM service.
 3. Select Users in the left-hand navigation panel.
 4. Select the user for which you want to assign the role.
 5. Click the Permissions tab.
 6. Click the Add permissions button.
 7. Select the type of trusted entity.
 8. Select the roles for the respective users as described above.
 9. Click the Add permissions button.
 10. Click the Update permissions button.
-

B) Virtual Private Cloud

Moving ahead, the **Virtual Private Cloud (VPC)** for **Cobra Kai** would provide a secure and isolated environment for the organization to run the video-streaming application and store data. This environment is separate from the public internet, making it virtually impossible for unauthorized access. Additionally, a VPC can be used to control the traffic between different parts of the cloud, allowing for better control and security of the data. It also allows for segmentation of the network, so that different teams can have access to different parts of the cloud and keep their data secure. Finally, a VPC could provide **Cobra Kai** with the ability to customize their network to meet their specific needs, such as setting up firewalls, routing tables, and more.

For setting up a **Virtual Private Cloud** for the **Cobra Kai**, the following steps need to be implemented. Also, considering that **Cobra Kai's** corporate IP range is **129.2.0.0/16**.

1. To create a VPC, log into the AWS Console and select the VPC service in the “Networking & Content Delivery” section. Then, click the “Your VPCs” link and select “Create VPC”.
 2. Create a VPC in AWS and specify the Corporate IP range (129.2.0.0/16).
 3. Configure the subnets for the VPC.
 4. Create and configure an Internet Gateway.
 5. Set up security groups to control access to the VPC.
 6. Configure a NAT Gateway for outbound internet access.
 7. Set up an Elastic IP address for the NAT Gateway.
 8. Create and configure a Route Table to route traffic in the VPC.
 9. Configure a Network Access Control List (ACL) to control the traffic in the VPC.
-

Now the final step for setting up the Security and Networking environment is to configure **NACL** or/and **Security Groups**. As mentioned previously, because of the services offered by **Cobra Kai**, there have been adversaries with the intent to conduct detrimental activities. Therefore, it could only prove beneficial to configure and maintain additional security within the environment.

C) Network Access Control Lists

NACL helps with controlling access to resources within a network by allowing or denying traffic from specific IP addresses or ranges of IP addresses. NACLs can be used to restrict access to certain ports, secure SSH connections, and filter malicious traffic.

To setup a new access control list, please follow the steps below.

1. To create a NACL, log into the AWS Console and select the VPC service in the “Networking & Content Delivery” section. Then, click the “Network ACLs” link and select “Create Network ACL”.
 2. Upon creating a Network Access Control List, specify the Cobra Kai’s Corporate IP range **(129.2.0.0/16)**.
 3. Define the rules to control the traffic in the VPC that allow specific type of network traffic (e.g., HTTP, HTTPS, SSH, etc.)
 - a. Define rules to allow specific traffic to flow in and out of the VPC.
 - b. Define rules to deny specific traffic from entering the VPC.
 - c. Define rules to allow specific services to be accessed from the VPC.
 - d. Define rules to specify the source and destination of the traffic.
 4. Assign the ACL to the subnets.
 5. Configure the ACL to allow the desired traffic to flow in and out of the VPC. A set of which allows outbound internet access from within the VPC. This ensures that the traffic originating from within the VPC is able to reach the internet, which is a requirement in case of on-demand-video streaming.
-

D) Security Groups

Security groups are important for **Cobra Kai** because they provide an additional layer of security within their network. Security groups allow administrators to control the flow of traffic between resources within the network, such as between two applications or between two servers. This helps to ensure that only authorized resources are able to communicate with each other and that malicious traffic is blocked. Additionally, security groups help to improve performance by allowing administrators to limit traffic to only the necessary ports. Some of the ports that need to be kept open for the video streaming platform are,

- HTTPS (port 443): This port is used to access secure web-based services.
- RTMP (port 1935): This port is used to stream video and audio content.
- RTSP (port 554): This port is used to control the streaming of video and audio content.
- FTP (port 21): This port is used for file transfers. SSH (port 22): This port is used for secure remote access.

To configure a new Security Group, please follow the steps below.

1. To create a security group, log into the AWS Console and select the EC2 service in the “Compute” section. Then, click the “Security Groups” link and select “Create Security Group”.
 2. Define the rules for each security group to control the inbound and outbound traffic.
 3. Specify the source and destination of the traffic.
 4. Allow traffic from the public internet to the application servers.
 5. Allow traffic from the application servers to Cobra Kai’s video streaming platform.
 6. Allow traffic from Cobra Kai’s streaming platform to the application servers.
 7. Allow traffic from the application servers to the database servers.
 8. Allow traffic from the database servers to the application servers.
 9. Deny all other traffic.
-

Data Management

Data storage for the **Cobra Kai** application in the cloud can be managed using a variety of different methods. First, data should be encrypted at rest and in transit in order to protect the data from unauthorized access. Secondly, secure data access should be implemented using identity and access management (IAM) policies and roles. Thirdly, disaster recovery and backup & restore processes should be implemented in order to ensure the data is kept safe in the event of a failure. Finally, cloud formation templates and security group/NACL/firewall rule configurations should be used to configure the systems in a secure manner.

The process flow for migrating the existing **Cobra Kai** data from on-premise onto the Cloud using AWS would look like this,

- Creating an **Amazon S3 bucket** to store the data and utilizing it to transfer the data between the on-premises environment and the cloud.
- Configuring **Amazon EC2 instances** to host the application components and utilizing it to transfer the application components to the cloud.
- Creating an **Amazon EBS volume** to store any persistent data associated with the application and utilizing it to store and manage the persistent data associated with the application.

1. Amazon S3 Buckets

Setting up an **S3** bucket for **Cobra Kai** is beneficial for a few reasons. First, it provides a secure and reliable storage solution for the data. Second, it allows for scalability, meaning that it is easy to add or remove storage space as needed. Finally, it allows for automated backups so that the data is always safe and secure. S3 buckets make it easy to store and manage data, and are essential for any business that needs to store large amounts of data.

To configure a new S3 bucket, please follow the steps below.

1. On the Services menu, select S3.
2. Click the Create Bucket button.
3. Enter a name for the bucket, choose a region, and check the Enable versioning box.
4. Click the Create button.
5. On the Properties tab, click the Edit button.
6. Check the box next to Public access and then click Save.
7. On the Permissions tab, select Bucket Policy.
8. Since the streaming/recorded video data has to be publicly accessible to the users, it is required to allow read-access to this S3 bucket so that anyone who wants to make use of the contents can access it. we need to allow reCopy and paste the following policy into the Bucket Policy Editor:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowPublicRead",
      "Effect": "Allow",
      "Principal": "*",
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::your-bucket-name/*"
    }
  ]
}
```

9. Replace bucket-name with the desired name of the bucket.
 10. Click the Save button.
 11. On the Overview tab, click the Upload button.
 12. Select the recorded video files to upload and click the Start Upload button.
 13. Once the files have finished uploading, click the Manage Access Permissions button.
 14. Check the boxes next to Public and Authenticated, and then click the Save button.
 15. You have now successfully configured and setup S3 for Cobra Kai.
-

2. Amazon EC2 Instances

The benefits of hosting **Cobra Kai's** streaming application on an **EC2 instance** include scalability, cost savings, and flexibility. The scalability of EC2 allows the organization to quickly and easily scale up or down depending on their needs. This can help save on costs since the instance can quickly scale up when needed, and scale down when not in use. EC2 also offers flexibility since it can host a variety of services, including web applications and databases. Finally, EC2 is cost-effective, as it allows organizations to pay for only the resources they use, and can help them save money by avoiding the costs associated with purchasing and maintaining physical hardware.

To configure a new EC2 Instance, please follow the steps below.

1. Set up an Amazon EC2 instance with the appropriate instance type, storage, and networking configurations.
 2. Upload the application files and any necessary dependencies to the EC2 instance.
 3. Install the necessary software packages, such as a web server, database, or other components necessary for running the application.
 4. Configure the application, including setting up the database, setting environment variables, and so on.
 5. Test the application to make sure it is running correctly.
 6. Set up the security group to restrict access to the instance from the outside world.
 7. Configure a public IP address or domain name to make the application accessible from the outside world.
 8. Set up monitoring and logging to ensure the application is running smoothly.
 9. Upload the existing data of Cobra kai to the EC2 instance.
 10. Test and verify the data to make sure it is working correctly.
-

3. Amazon EBS Volume

Creating an Amazon **EBS volume** to store any persistent data associated with the application for **Cobra Kai** is important for a few reasons. First, it ensures that the data is stored securely and reliably in the cloud. Second, it supports scalability of the application as the data can be easily expanded or reduced as needed. Finally, it can improve the performance of the application as the data is stored on a highly-available and durable storage platform that is built to handle large amounts of data.

To configure EBS after configuring EC2 and S3 buckets, the following steps need to be performed,

1. Set up the EBS volumes: Create the EBS volumes and attach them to the EC2 instance. You can use the AWS Management Console to create the EBS volumes and specify their size and type.
2. Configure the EBS volumes: Once the EBS volumes have been created, configure them to meet the needs of your application. This includes setting up RAID configurations, assigning mount points, and configuring partitioning.
3. Configure the file system: You will need to create the file systems that will be used to store your application's data. This includes creating the directory structure and setting the appropriate permissions.
4. Create the EBS snapshots: You can use the AWS Management Console to create EBS snapshots of your EBS volumes. This will allow you to back up your data and restore it in the event of a disaster.
5. Configure the EBS volumes for Cobra Kai: Finally, configure the EBS volumes for Cobra Kai. This will involve configuring the security settings and setting up the necessary automation and monitoring.

4. Data Encryption

Cobra Kai can use encryption capabilities for Amazon EBS volumes, Amazon S3 buckets, and data stored at rest within an Amazon EC2 instance. Encryption protects data from unauthorized access and complies with security and compliance standards. Amazon EC2 also offers support for encryption of data in transit using the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols.

Performance Optimization

1. Resiliency

The performance of **Cobra Kai** can be enhanced when the entire business is shifted to the cloud by leveraging cloud-native technologies such as Amazon Elastic Compute Cloud (EC2) for computation of daily tasks, Amazon Elastic Load Balancing (ELB) for load balancing, and Amazon Auto Scaling for scalability.

Amazon Elastic Load Balancing (ELB) can be used to manage traffic for **Cobra Kai's** by distributing incoming traffic across multiple virtual machines (VMs) and ensuring that the application is able to handle the increased load of customers.

In a worst case scenario very high load, **Amazon Auto Scaling** can also be used to automatically scale the number of VMs up and down based on the amount of traffic to ensure that the application is always able to handle the load. This solution provides a highly scalable and available architecture that can easily handle increased traffic.

Additionally, **Amazon CloudFront** can be used to deliver content closer to the user and reduce latency. Finally, **Amazon CloudWatch** can be used to monitor the performance of the application and provide detailed insights into the workloads, allowing for optimizations to be made.

A) Elastic Load Balancing

AWS **Elastic Load Balancing (ELB)** is an essential part of Cobra Kai's application. By using ELB, **Cobra Kai** can distribute incoming application traffic across multiple targets such as Amazon EC2 instances, containers, IP addresses, and Lambda functions. This helps to improve the availability and scalability of applications, as well as providing fault tolerance. It also provides enhanced security by allowing **Cobra Kai** to protect their applications from malicious traffic, as well as providing an additional layer of protection against DDoS attacks. Additionally, ELB allows **Cobra Kai** to monitor the health of its targets and make routing decisions based on that information. This helps to ensure that their applications remain available and performant even during periods of high demand or traffic spikes.

Before beginning the setup, make sure to complete the steps to prepare the VPC and EC2 instances. Now, to setup Cloudfront within the **Cobra Kai's** cloud environment, follow the steps below.

1. Log in to AWS Console and go to the EC2 instance on which the Load Balancer is to be configured.
2. Select "Create Load Balancer" and Select a load balancer type.
3. Give a load balancer a name, specify the region, select the port(s) to be used and add any

other optional settings. Select the EC2 instance (or instances) to add to the load balancer.
Assign security groups to the load balancer.

4. Assign security groups to load balancer in a VPC
 5. Configure health checks for your EC2 instances
 6. Register EC2 instances with load balancer
 7. Select the “Listeners” tab to view the status of load balancer.
 8. Select the “Instances” tab to view the list of EC2 instances that are associated with load balancer.
 9. Create and verify load balancer
-

B) Auto Scaling

AWS **Auto Scaling** can help **Cobra Kai** by automatically scaling their cloud infrastructure to meet the demands of their customers. It can scale up or down the number of EC2 instances depending on the workload, ensuring that your application always has the right amount of resources for optimal performance. Additionally, Auto Scaling can also detect and scale out when there are spikes in customer demand, allowing **Cobra Kai** to handle increased traffic without any manual intervention.

To configure the Auto Scaling Group, follow the steps below.

1. Go to the Amazon Web Services Management Console and select the “EC2” service.
2. Select the “Auto Scaling” option from the left sidebar.
3. Click the “Create Auto Scaling Group” button.
4. Provide a Group Name, then select the region in which the instance is located.
5. Select the “Instance Type” of the instance you want to use for your auto scaling group.
6. Select the “Launch Configuration” for the instance you want to use for your auto scaling group.
7. Select the “Maximum Group Size” and “Minimum Group Size” for your auto scaling group.
8. Configure the “Scaling Policies” for your auto scaling group.
9. Configure the “Notification” settings for your auto scaling group.
10. Click the “Create Auto Scaling Group” button.
11. Select the “Instances” tab from the left sidebar.
12. Select the “Create Instance” button.
13. Select the “Auto Scaling Group” option from the “Instance Type” drop-down menu.
14. Select the auto scaling group you created from the list of available options.
15. Select the “VPC” that the instance is located in.
16. Select the “Subnet” for the instance.
17. Select the “Security Group” for the instance.
18. Select the “AMI” for the instance.
19. Configure the instance “User Data” if necessary.
20. Select the “Key Pair” for the instance if necessary.
21. Click the “Create Instance” button. The auto scaling group is now configured and ready to use on Cobra Kai’s Network.

C) Cloudfront

CloudFront is a content delivery network (CDN) that helps to distribute web content to end-users with low latency and high transfer speeds. CloudFront will help **Cobra Kai** with their on-demand video streaming service by providing fast, reliable delivery of video content to users. With CloudFront, content is cached and served from edge locations in the network, which helps to reduce the load on the web server, making it easier for the web application to handle more traffic and hence, reducing latency and improving streaming performance for the users.

Additionally, CloudFront can be used to scale the streaming service by providing the ability to quickly provision additional capacity in response to spikes in demand.

To setup Cloudfront within the Cobra Kai's cloud environment , please follow the steps below.

1. Select File-based delivery method for Cobra Kai's application.
 2. Configure the CloudFront distribution settings.
 3. Create an origin for the distribution and configure the origin settings.
 4. Add your web application's domain name to the CloudFront distribution.
 5. Configure the caching and expiration settings.
 6. Configure the security settings.
 7. Test the CloudFront distribution.
 8. Monitor the performance and availability of the CloudFront distribution.
-

2. DDoS Protection

As mentioned previously, based on services offered by **Cobra Kai**, there have been adversaries with the intent to conduct detrimental activities. Therefore, setting up **DDoS protection** is important for **Cobra Kai** because it helps to protect the cloud environment from malicious and distributed denial of service attacks. DDoS attacks can cause downtime and disruption to the applications and services hosted in the cloud environment.

For protection against DDoS attacks, **Cobra Kai** can make use of various services provided by AWS. First, it is required to set up **Amazon CloudFront**, as it caches static content such as images, videos, and other static files, reducing the amount of traffic to the origin server. Additionally, usage of **Amazon Route 53** which is a DNS service can allow to route traffic to **Cobra Kai's** origin server as well as to CloudFront. They can also use **Amazon Shield** to protect their application layer from DDoS attacks. Finally, they can use **AWS WAF** to filter out malicious traffic from their origin server. By adopting these services, **Cobra Kai** can better protect their cloud infrastructure from DDoS attacks.

A) CloudWatch

CloudWatch is an important tool for **Cobra Kai** because it enables monitoring the performance of the video streaming service. It not only helps in detecting and diagnosing issues with services but also track the performance of applications over time. It also helps to set up alarms and notifications to alert when certain thresholds have been exceeded. This helps in ensuring that **Cobra Kai's** services are running at their optimal level and makes sure that any issues are handled quickly.

To use Cloudfront within the Cobra Kai's cloud environment , please follow the steps below.

1. Sign in to the Amazon Web Services (AWS) Console and select CloudWatch from the Services menu.
2. Select the "Create Alarm" button in the top right corner of the page.
3. Select the service or application for which you would like to create an alarm.
4. Select a metric to monitor and set the thresholds for when the alarm should be triggered.
5. Select the action that should be taken when the alarm is triggered.
6. Enter a name for the alarm and click "Create Alarm".
7. Select the "Enable Alarm" button to enable the alarm.
8. Repeat steps 3-7 for any additional services or applications you would like to monitor with CloudWatch.

B) Route53

Route53 is an essential tool for **Cobra Kai** because it enables the management of domain name registrations. With Route53, **Cobra Kai** can easily register and manage their own domain names and set up DNS records to point to its web servers. Additionally, Route53 can help **Cobra Kai** quickly and easily manage their DNS records and make sure their web presence is secure and reliable. With Route53, **Cobra Kai** can quickly and easily configure the DNS records to ensure that the web traffic is routed to the correct servers and applications, as well as help to keep track of the domain registrations.

To use Route53 using **Cobra Kai's** existing Domain Name, follow the steps below,

1. Sign in to the Amazon Web Services (AWS) Console.
 2. Select the Route53 service from the list of services.
 3. Create a Hosted Zone by clicking the “Create Hosted Zone” button.
 4. Enter the desired domain name to register, and then click the “Create” button.
 5. Create the necessary DNS records for the domain. This can include A records, CNAME records, MX records, TXT records.
 6. Once the records are created, click the “Save Record Set” button to save your changes.
 7. Once saved, you will be given a list of nameservers. These are the DNS servers that are required to set up with the domain registrar in order for the domain to be routed to the correct server.
 8. Copy the nameservers and submit them to your domain registrar.
 9. Wait for the domain to be propagated, which could take up to 24 hours (max).
 10. Once the domain is propagated, DNS records can be tested to make sure they are configured correctly.
-

C) AWS Shield

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on AWS. It provides always-on detection and automatic inline mitigations that minimize application downtime and latency. An online web-service like **Cobra Kai**, can use AWS Shield to stay protected from malicious DDoS attacks that could disrupt the service and cause user frustration. Additionally, AWS Shield can monitor for suspicious activity and alert the **Cobra Kai** Security team so that they can take proactive steps to mitigate any potential threats.

To configure AWS Shield, the following steps need to be performed,

1. Sign in to the AWS Console.
 2. Go to the Security & Identity section of the AWS Services menu and select AWS Shield.
 3. Select the Activate AWS Shield Standard option to begin the setup process.
 4. Select the Cobra Kai AWS account from the list of accounts available.
 5. Select the appropriate AWS Region for the Cobra Kai application.
 6. Select the Enable advanced protection option if required.
 7. Review the activation summary and select Activate AWS Shield Standard if everything looks correct.
 8. Once the activation process is complete, select the Cobra Kai AWS account from the AWS Shield dashboard to view the protection details.
 9. Review the protection details and adjust the settings as necessary.
 10. Select Save to complete the configuration process.
-

D) AWS WAF

AWS WAF (**Web Application Firewall**) is an important security tool for **Cobra Kai**, as it helps protect the application from malicious actors trying to access the applications or steal data. It provides protection from common web exploits such as SQL injection, cross-site scripting, and malicious bots. It also helps protect against application layer DDoS (Distributed Denial of Service) attacks. With AWS WAF, **Cobra Kai** can also control access to the applications and set rules to allow or block traffic based on certain criteria such as IP addresses, geographic locations, and web requests. By implementing AWS WAF, **Cobra Kai** can reduce their risk of attack and improve its overall security posture.

To configure AWS WAF, mainly these steps are needed to be performed,

1. Create an AWS WAF instance and configure the rules for the application.
2. Define Rules: Define the rules to be applied to the application. This can include IP address, URL, and HTTP request methods.
3. Configure Firewall Rules: Configure the rules to allow or deny requests based on the criteria defined in the previous step.
4. Test Rules: Test the rules to ensure they are configured correctly.
5. Monitor Logs: Monitor the logs to detect any suspicious activity or potential threats.
6. Review and Update Rules: Review the rules and make any necessary changes to ensure the application is secure.

Coding Practices & PCI Compliance

Coding practices are essential for the cloud platform for **Cobra Kai** as they help ensure that the applications running on the cloud platform are secure, reliable, and cost-efficient. Utilizing best practices for cloud security, such as implementing AWS IAM for user access control, monitoring the resources with AWS Config, and leveraging CloudTrail for auditing and logging, can help protect the platform from malicious actors. Additionally, utilizing automated infrastructure provisioning with AWS Auto Scaling can help ensure that the platform is always running efficiently and cost-effectively. Implementing these best practices can help **Cobra Kai** ensure that the cloud platform is secure, reliable, and cost-effective.

A general set of **administrative practices** that must be followed are as follows,

1. All data related to **Cobra Kai** should be stored in a secure, encrypted cloud storage solution. This prevents any unauthorized access to the data.
2. Access to the data should be restricted to authorized personnel only and should require authentication using a secure username and password. Access should be monitored and logged to ensure that only authorized personnel are accessing the data.
3. All data should be backed up regularly to ensure that in the event of an emergency or data loss, the data can be recovered quickly.
4. All data should be encrypted when being transmitted over networks to prevent unauthorized access.
5. All data should be protected by appropriate firewalls and intrusion detection systems.
6. All data should be regularly scanned for malicious threats and malware.

The **coding practices** that must be followed by twithin **Cobra Kai** are are as follows,

1. Utilizing AWS CloudFormation for Infrastructure as Code (IaC).
2. Using the AWS Identity and Access Management (IAM) for user access control.
3. Leveraging AWS CloudTrail for auditing and logging user activity.
4. Automating infrastructure provisioning with AWS Auto Scaling.
5. Utilizing AWS Security Groups to control access to your applications.
6. Implementing AWS Config to monitor your resources.
7. Utilizing the AWS Trusted Advisor to identify potential cost savings.
8. Setting up CloudWatch alarms to monitor your resources.
9. Regularly backing up data with Amazon S3 and Amazon EBS.
10. Utilizing Amazon SNS for push notifications.

To implement automated testing for the Cobra Kai application, in order to look for any potential threats or a regular check for all running services, follow the steps below

1. Set up an automated pipeline for continuous testing in the cloud environment by using **AWS CodePipeline**. This will allow Cobra Kai's development team to create a workflow that will automatically detect changes in the source code, build, and test the application.
 2. Use **AWS CodeBuild** to set up an automated testing infrastructure. This allows to quickly and easily create build and test jobs that can be triggered by code changes.
-

PCI Compliance

Since **Cobra Kai's** platform is processing the usage of Credit cards, there are a set of security standards that are designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

PCI compliance requires adherence to the six control objectives, or goals, outlined in the PCI DSS. They are, building and maintaining secure network and systems, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, monitoring and testing networks regularly, and lastly constructing an information security policy.

To implement PCI compliance, the website must implement technical and organizational measures to ensure the security of cardholder data. These measures include:

1. Installing and maintaining a firewall configuration to protect cardholder data.
2. Encrypting transmission of cardholder data across open, public networks.
3. Using and regularly updating anti-virus software or programs.
4. Developing and maintaining secure systems and applications.
5. Restricting access to cardholder data by business need-to-know.
6. Assigning a unique ID to each person with computer access.
7. Restricting physical access to cardholder data.
8. Tracking and monitoring all access to network resources and cardholder data.
9. Regularly testing security systems and processes.
10. Maintaining a policy that addresses information security.

In addition, the website must also meet certain PCI Data Security Standards (DSS) requirements. These requirements include regular vulnerability scans, maintaining an information security policy, and implementing strict access control measures. The website must also conduct regular audits and reviews to ensure that the security measures are in place and working as intended.

By following these measures, the website can ensure that it meets all of the necessary PCI compliance requirements.

System Administration

System administration in cloud for **Cobra Kai** is essential for ensuring that the company's cloud infrastructure and resources are running efficiently and securely. System administrators are responsible for maintaining and monitoring the cloud environment, which includes setting up and managing accounts, configuring security and access privileges, setting up and managing storage, and managing the network and server performance. By doing so, system administrators ensure that cloud users have secure access to their data, applications, and environment. They also ensure that the cloud environment is optimized for cost and performance. **System administrators** play a key role in safeguarding the security of **Cobra Kai's** cloud environment, and in helping their customers get the most out of their cloud experience.

Moreover, system administration in cloud for **Cobra Kai** also helps to ensure that the cloud-based services and applications are running as expected and that the customers' data remains safe and secure. System administrators can also be called upon to help in troubleshooting and resolving any technical issues that may arise. Finally, system administrators are responsible for the overall health of the cloud environment and can help Cobra Kai scale and optimize their cloud environment as the company grows.

Some principles that the System Administrators must follow are as follows,

1. **Ensure Proper Authentication and Authorization:** Establishing user authentication and authorization processes to protect and manage access to sensitive data and resources.
2. **Monitoring System Performance:** Closely monitoring the performance and availability of cloud systems as well as the utilization of resources such as storage, memory and CPU.
3. **Using Automation for Deployments:** Automating the deployment of applications and services to ensure more consistent, reliable results.
4. **Maintaining Backups:** Storing backups of data, applications and configurations in case there is a need to restore or quickly provision systems.
5. **Monitoring System Logs:** Monitor system logs for any suspicious activity and take appropriate action if needed.
6. **Updating Software:** Keeping cloud systems up-to-date with the latest security patches, software updates and hotfixes.
7. **Educating Users:** Educating users on security best practices and the appropriate use of cloud systems.

References

1. Amazon IAM Documentation -

https://docs.amazonaws.cn/en_us/IAM/latest/UserGuide/introduction.html

2. Amazon Cloudfront Documentation -

<https://aws.amazon.com/cloudfront/>

3. Amazon Route 53 Documentation

<https://docs.aws.amazon.com/route53/index.html>

4. Amazon Elastic Load Balancing Documentation -

<https://docs.aws.amazon.com/elasticloadbalancing/latest/application/introduction.html>

5. Amazon S3 Documentation -

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

6. Amazon EC2 Auto Scaling Documentation -

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

7. Amazon EBS Documentation -

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AmazonEBS.html>

8. Amazon AWS Shield Documentation -

<https://aws.amazon.com/shield/>

9. What is PCI Compliance? - Digital Guardian -

<https://digitalguardian.com/blog/what-pci-compliance>

10. Secure Coding Best Practices and Its Checklist -

<https://www.xenonstack.com/blog/secure-code-best-practices>