My Resume Hosted On a Static Website Using Amazon S3

—

By Akosa Mora

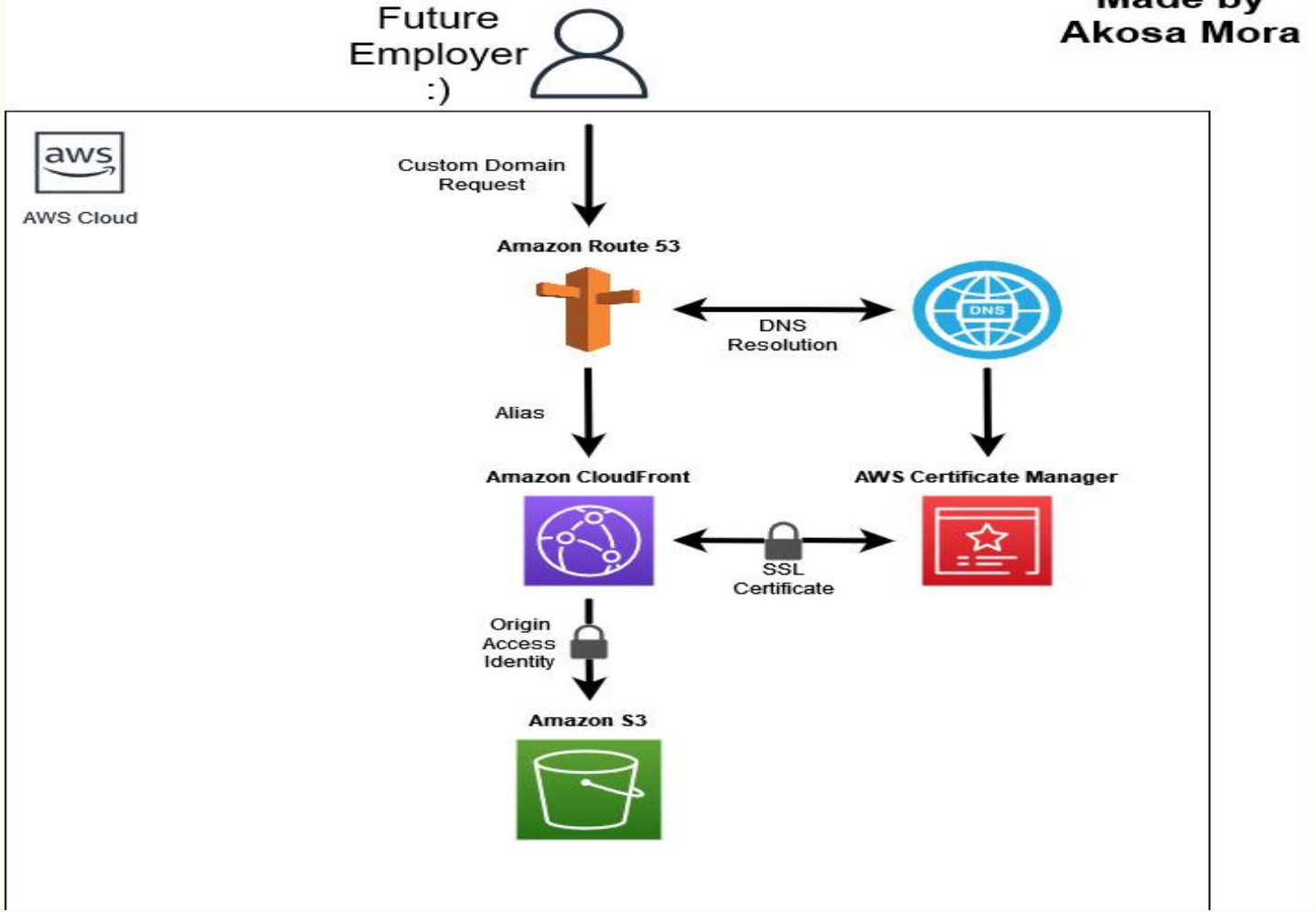
Hello, my name is Akosa Mora and I am a Results-driven Senior DevSecOps Engineer with a strong background in application security, extensive expertise in Kubernetes security, and comprehensive knowledge of Cloud/DevOps practices. Seeking a challenging role to lead security initiatives, implement secure architectures, and ensure the protection of critical applications and infrastructure.

All AWS services included in this project:

- S3 (simple storage service)
- Route53
- CloudFront
- Certificate Manager

The Architecture

Made by
Akosa Mora



Explanation

I have leveraged the power of Amazon S3 to host my resume website, which is a highly scalable and secure object storage service. I have used Route 53, AWS's Domain Name System (DNS) service, to point my domain to my S3 bucket, ensuring that my website is easily accessible to anyone who visits.

To improve the performance and availability of my website, I have distributed it using CloudFront, which is a content delivery network (CDN) that delivers your website's content to users with low latency and high transfer speeds.

Explanation Continued ..

Finally, to ensure that my website is secure, I have used Amazon Certificate Manager (ACM) to secure my website with an SSL/TLS certificate. This allows for secure communication between my website and its users and also gives me peace of mind knowing that my resume is protected.

Overall, by using these AWS services, I have been able to create a fast, secure, and highly available website for hosting my resume. I hope that this approach is helpful for those looking to host their own static website. Thank you for your time.

References & Resume Website

IAM JSON policy elements reference - AWS Identity and Access Management

AWS Certificate Manager

What is Amazon CloudFront? - Amazon CloudFront

Akosa Mora
Senior DevSecOps Engineer

GitHub: https://github.com/cloudsecakosa
Website: https://cloudsecakosa.github.io/
LinkedIn:https://www.linkedin.com/in/akosalovescloud

Summary

Results-driven Senior DevSecOps Engineer with a strong background in application security, extensive expertise in Kubernetes security, and comprehensive knowledge of Cloud/DevOps practices. Seeking a challenging role to lead security initiatives, implement secure architectures, and ensure the protection of critical applications and infrastructure.

Experience

FEB 2020 - PRESENT

Vizient, Inc - *Senior DevSecOps Engineer*

- Led the design and implementation of DevSecOps practices to embed security into the software development lifecycle, focusing on application security and Kubernetes security.
- Conducted comprehensive application security assessments, including secure code reviews, vulnerability scanning, and penetration testing.
- Developed and enforced secure coding practices and standards, ensuring compliance with industry security frameworks and regulations.
- Collaborated with cross-functional teams to implement secure CI/CD pipelines and automate security testing using tools such as SAST, DAST, and IAST
- Mentored and provided technical guidance to junior team members, fostering their growth and knowledge in DevSecOps and Kubernetes security.

MAR 2018 - FEB 2020

Vizient, Inc - *Cloud Security Engineer*

- Conducted security assessments and vulnerability scanning using tools like SonarQube, Nessus, and OpenVAS.
- Orchestrated and managed Kubernetes clusters, including deployment, scaling, monitoring, and troubleshooting of containerized applications.
- Reduced deployment time by 50% by deploying Docker containers for the different stages of software application development, testing, and production
- Implemented network security measures, including firewall rules and security group configurations, to protect cloud infrastructure.
- Implemented CI/CD pipelines for containerized applications, integrating with source control, build systems, and container registries.
- Monitored and analyzed logs and security events using tools like Splunk and ELK Stack, identifying and mitigating security risks.