



Centralized logging and analysis of multi-regional AWS WAF logs for near real-time Threat Detection using Amazon Elasticsearch Service, Kinesis and Kibana

**About Hostbooks**

**About Challenge**

HostBooks provides a comprehensive cloud-based platform for all the major accounting solutions like GST, E-Way Bill, TDS, Point of Sale(POS), Payroll, and Accounting. With the perfect blend of Accounting and Cutting-edge Technology, it aims at minimizing the compliance time with seamless user experience. Be it filing GST/TDS returns, E-way Bill generation or managing your business finances, it boosts up productivity and cuts down the operational costs by keeping everything intact.

HostBooks has an online portal, used by accountants and commerce professionals. They use the portal to use services like GST filing and E-way bill payments.

Though they had an on-premise firewall in place but the customer was facing multiple challenges in analyzing the logs generated by the firewalls deployed at multiple locations. AWS cloud service WAF can consolidate firewall data from multiple regions at one place.

The biggest challenge here is the collection of WAF firewall logs from client website for analysis and then combining these insights to be displayed together in a single dashboard as a one-stop solution.

The next challenge is performing log analysis which is critical for understanding the effectiveness of any solution offered, it is valuable for day-to-day troubleshooting and also for long-term understanding of how the application is performing.

Also, while troubleshooting logs from multiple regions, how to perform root cause analysis for exceptional cases like IP repudiation, BOT Requests, 403 error, Firewall blocking is a difficult task.



**AWS Services used**



Amazon Simple  
Storage Service (S3)

Amazon Kinesis

Data Firehose

AWS WAF

Kibana

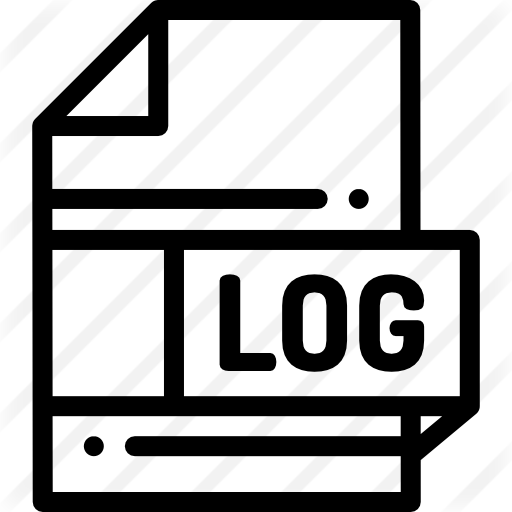
Amazon Elasticsearch  
Service

**Proposed Solution**

MIND discussed the problem with the customer and after analyzing the business problem, it was determined that Amazon Kinesis Data Firehose would fit the business problem. Solution flow proposed consisted of the following steps.

* With the access to [full AWS WAF logs](https://aws.amazon.com/about-aws/whats-new/2018/08/aws-waf-launches-new-comprehensive-logging-functionality/), we currently have the ability to analyze all the logs generated by [AWS WAF](https://aws.amazon.com/waf/) while it’s protects the web applications. In addition, Amazon Kinesis Data Firehose is used to forward these logs to [Amazon Simple Storage Service](https://aws.amazon.com/s3/) (Amazon S3) for the purpose of archival, and to Amazon Elasticsearch Service for further analysis which is then represented in Kibana as dashboard.
* This allows us to find out in near-real time that which AWS WAF rules are getting triggered, the reason why are they being triggered, and by which request.
* Long-term analysis is also done by creating a historical view of previous logs.
* The Centralized Logging solution offering enables organizations to collect, analyze, and display Amazon WAF logs in a single dashboard.
* These collected logs provide troubleshooting and root-cause analysis for any kind of exception for say Blacklist IP, IP repudiation, BOT Requests, 403 error, Firewall blocking, IP repudiation limit cross etc.
* The offering contains a suite of infrastructure services that deploy a centralized logging solution.
* It uses Amazon Elasticsearch Service (Amazon ES) and Kibana, an analytics and visualization platform that is integrated with Amazon ES, which together results in a unified view of all the log events.
* Amazon Kinesis Data Firehose streams the data coming from WAF to Amazon Elasticsearch Service and concurrently stores the data to S3.
* Then these errors are visualized in Kibana which will use streamed data to perform real-time root cause analysis for exceptions in a customizable, user-friendly dashboard.





**Solution Outcome**





Full access to WAF logs in 1 unified location.

Increased reliability of infrastructure at lower cost & significant improvement in performance to cost ratio

More secure business operations with timely threat detection

**Architecture Diagram**

Diagram

Description automatically generated

**How AWS services helped in building the Solution.**

**Amazon Kinesis Data Firehose**

Amazon Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling near real-time analytics with existing business intelligence tools.

**Amazon WAF**

AWS WAF is a web application firewall that lets you monitor the HTTP(S) requests that are forwarded to an Amazon CloudFront distribution, Amazon API Gateway REST API, Application Load Balancer, or AWS AppSync GraphQL API.

**AWS ElasticSearch**

Amazon Elasticsearch Service (Amazon ES) is a managed service that makes it easy to deploy, operate, and scale Elasticsearch clusters in the AWS Cloud. Elasticsearch is a popular open-source search and analytics engine for use cases such as log analytics, real-time application monitoring, and clickstream analysis.

**Amazon S3** **to store meta-data**

It is an object storage service that offers industry-leading scalability, data availability, security, and performance. In this solution it.

**Kibana**

Kibana is a popular open source visualization tool designed to work with Elasticsearch. Amazon ES provides an installation of Kibana with every Amazon ES domain.

**About the Partner**

**MothersonSumi INfotech &Designs Ltd.**

MothersonSumi INfotech & Designs Limited (MIND), a SEI CMMI Level 5 IT services company and the IT back bone of Motherson group. MIND is a trusted technology partner to over 200 clients globally. Our value proposition is in our strength in specific Industry segments and years of experience in the areas of intelligent warehousing, Supply chain enablement, software application development, smart ERP customization, infra managed services, cloud, IoT & Analytics. MIND is serving customers in 41+ countries with a strong team of 1500+ professionals.