

# ADEWALE ALAKE

Richardson, TX 75082

[alaskaalake@gmail.com](mailto:alaskaalake@gmail.com) | 573-578-3818

---

## Professional Summary

Splunk Engineer with over 6 years background experience in Information Technology. Expertise in installation, configuration, integration, trouble-shooting and maintenance of Splunk environments as part of providing technical support to the Security Engineering team. Highly skilled in developing and implementing solutions to increase the value of internal operations and strengthen data security capabilities. Passionate about machine data and operational intelligence to achieve SLAs. Adept at performing tasks on the Linux OS platform, working on the server side/backend of Splunk and also creating knowledge objects on the frontend for monitoring overall performance.

## Key Competencies

Splunk Maintenance & Integration  
Dashboard Design & Implementation  
Data Structure & Process Development

SPL Query Development  
Performance Monitoring  
Solution Development

Splunk Administration  
Data Mining and Analytics  
Security Engineering

## Technical Skills

**Technology Tools:** Splunk, Vagrant, VMware

**Operating Systems:** UNIX/Linux, Redhat/CentOS, Ubuntu, Windows Server (2008,2016), MacOS

**Languages/UI:** SPL, Bash Scripting, XML, T-SQL, DAX, MDX

**File Sharing:** WINSCP, SCP, SFTP

**Network Protocols:** TCP/IP, UDP, HTTP, SSL, HTTPS, DNS, DHCP, ICMP

**Databases:** Microsoft SQL Server, MySQL, MS Access

## Certifications and Licenses

- Splunk Enterprise Certified Architect
- Splunk Enterprise Security Certified Admin
- CompTIA Security+ Certification
- Splunk IT Service Intelligence Certified Admin
- Querying Data with Transact-SQL
- Analyzing and Visualizing Data with Power BI
- AWS Certified Cloud Practitioner

## Professional Experience

**Optm Inc**

*Splunk Engineer*

**Roseville, CA**

March 2022 - Present

- Deployed new Splunk systems and monitor Splunk internal logs from the monitoring Console (MC) to identify and troubleshoot existing or potential issues
- Created, maintained, supported, customized System components & Splunk applications
- Created and maintained Splunk reports, dashboards, forms, visualizations using Splunk SPL driven queries
- Installed and configured Splunk components following Splunk recommended best practices
- Configured index retention in indexes.conf
- Installed and configured Splunk Indexer Cluster and Deployment Server
- Configure Rsyslog server to write logs from network appliances to disk
- Configured heavy forwarder to monitor logs from Rsyslog server
- Configurations with deployment server, search heads, indexers, serverclass.conf, server.conf, apps.conf, props.conf, transform.conf, forwarder management configurations
- Optimized searches for better performance, search time and index time extractions using regex in props.conf and transform.conf
- Installed Technical Add-ons; "Splunk Add-on for Linux and Unix" and "Splunk Add-on for Windows" to parse logs on the Heavy Forwarder

**UnitedHealth Group***Splunk Engineer***San Antonio, TX**

December 2020 – March 2022

- Installed Universal forwarders on endpoints and pointed them to the Deployment Server
- Deployed inputs.conf and output.conf to endpoints via the Deployment Server
- Used regex to create field extractions, and SED function to anonymize data
- Set-up a test environment to test data prior to pushing to production
- Created Serverclass on the Deployment server, added clients and associated with deployed apps
- On-boarded data from different sources: Active Directory logs, Firewall Logs, routers, switches, Nagios
- Set-up test environment with Indexer Cluster of 3 peers, 2 heavy forwarders and 3 Cluster members
- Resolved data on-boarding issues with indexers and Universal Forwarders by conducting root cause analysis, also documented lessons learned
- Installed and managed Splunk apps and Technical Add-ons from Splunkbase
- Monitored Installation and configuration of Splunk apps to onboard data sources into Splunk

**CTX Solutions Group***Splunk Administrator***Brownsville, TX**

October 2019 – December 2020

- Created complex Dashboards, statistical reports, alerts and worked on other knowledge objects
- Managed user accounts and access control policies
- Installed Splunk Universal Forwarder across applications to collect the data.
- Extracted complex Fields from different types of Log files using Regex
- Managed Scheduling and Automating Database tasks including Jobs, Alerts, Notification and Emails
- Developed interactive dashboards using HTML to monitor production phases
- Installed Splunk components, Splunk TA's like "Splunk Add-on for Unix and Linux", "Splunk Add-on for Windows Infrastructure" to ingest and parse customer logs to be CIM compliant
- Created scheduled reports to monitor login defaulters and failed logins across the organization
- Monitored applications and server infrastructure for optimization, performance and utilization metrics

**Impac Exploration Services.***Linux System Administrator***Fort Stockton, TX**

July 2017 - October 2019

- Involved in installing OS, software, monitor performance, applying patches and troubleshooting alerts
- Performed troubleshooting on Linux servers and also contributing to application migration efforts
- Built and configured various services like DNS, DHCP, NFS, Apache Web Server, SSH, HTTP, RPM package management
- Created and managed user and group accounts, network access configuration, passwords, permissions and storage quotas
- Performed troubleshooting with network tools like ping, netstat, traceroute, nslookup, etc.
- Set up cron jobs to perform system backup and automated administration tasks using scripting
- Monitoring and maintaining system configuration and log files with password recovery and performance tuning, perform fault isolation and root-cause analysis of recurring issues

**Education**

Missouri University of Science and Technology, Rolla MO

May 2017

**M.S. Petroleum Engineering**

Obafemi Awolowo University, Ile-Ife Nigeria

March 2012

**B.S. Civil Engineering****References**

Available upon request