# **VASAVI Nagamalla**

# **vasavi.splunk@gmail.com**

# **Phone: +1(813) 906-5869**

# **CAREER OBJECTIVE**

Nearly 8+ years of impressive success as an IT and Splunk Security Professional in enabling leading organizations to achieve strategic objectives and growth plans by establishing & championing a robust environment; 4+ years of experience as a Splunk Developer and Admin. Currently spearheading as Lead Splunk Developer.

# **PROFESSIONAL SUMMARY**

* Highly skilled in Splunk to build, configure and maintain different environments and in-depth knowledge of log analysis generated by various operating systems.
* Installed and monitored Splunk Forwarders on Windows, UNIX and LINUX servers.
* Used XML, Advanced XML and Search Processing Language (SPL) for creating Dashboards, views, alerts, reports, and saved searches.
* Upgraded and Optimized Splunk setup with new discharges.
* Used various Splunk Apps such as Splnuk on Splunk, Universal Field Extractor, Splunk App for UNIX/Linux, Splunk DBI Connect.
* Created Splunk app for Enterprise Security to identity and address emerging security threats using continuous monitoring, alerting and analytics.
* Supported Splunk Cloud with 3 Indexers, 120 forwarders and Generated 300 Gb of data per day.
* Experience with Linux and Windows specialists for Splunk organization with a strong comprehension of the Splunk framework.
* Installed Splunk on nix & Splunk SOS and maintained Splunk instance for monitoring the health of the clusters
* Configuration of SPLUNK data inputs by understanding various parsing parameters like Index, source, source typing, queue sizes, index locations, read/write timeout values, line breaks, event breaks, time formats etc. during index-time.
* Skilled in deploying, configuring and administering Splunk clusters.
* Created Shell Scripts to install Splunk Forwarders on all servers and configure with common configuration files such as Bootstrap scripts, Outputs.conf and Inputs.conf files.
* Worked with source code organization instruments like CVS, SVN and Git. Presentation to outline organization gadgets like puppet.
* Extensively used various extract keyword, search commands like stats, chart, time chart, transaction, strptime, strftime, eval, where, xyseries, table etc.
* Familiar in System Administration with Windows 2003-2008 Servers, Red Hat Linux Enterprise Servers, Solaris and IBM AIX servers.
* Developed customized Shell scripts in order to install, manage, configure multiple instances of SPLUNK forwarders, indexers, search heads, deployment servers.
* Handled the Site Minder Web Agent foundation and summarized the Web Agent on Web Server cases.
* Troubleshooting and handling post production issues, on-site support, worked closely with engineering to coordinate and provide all the required information and interacting with the client.
* Strong qualitative analysis skills to lend insight into highly ambiguous and sensitive business problems. In-depth understanding of processes and technology integration challenges.

# **TECHNICAL SKILLS**

* **Splunk:** Splunk 5.x and Splunk 6.x, Splunk Enterprise, Splunk on Splunk, Splunk DB Connect, Splunk IT Service Intelligence, Splunk Web Framework, Splunk Machine Learning Tool kit, Splunk Hunk.
* **Operating Systems:** Windows, Unix/Linux.
* **Data Analysis:** Requirement Analysis, Business Analysis, detail design.
* **Web technologies:** HTML, CSS, JavaScript, XML, Advanced XML.
* **Concepts:** SIEM, SDLC, Object Oriented Analysis and Design.
* **Programming Languages:** C, Python, UNIX shell scripts.
* **Database:** Oracle, MySQL, SQL queries, SQL Procedures.

# **PROFESSIONALEXPERIENCE**

**Client: BMW, South Carolina January 2016 to till date**

**Role: Splunk Developer/ Admin**

**Responsibilities:**

* Experience with Splunk searching and reporting modules, knowledge objects, Administration, Add-on’s, Dashboards, Clusters and forwarder management.
* Experience in Splunk GUI development creating Splunk apps, searches, Data models, dashboards, and Reports using the Splunk query language.
* Responsible to filter the unwanted data in heavy forwarder level thereby reducing the license cost.
* Optimized Splunk for peak performance by splitting Splunk indexing and search activities across different machines.
* Extracted complex Fields from different types of Log files using Regular Expressions.
* Migrated Splunk config file to multiple remote servers.
* Extensive knowledge in writing the scripts to automate the tasks in Linux environment.
* Able to create fields through Splunk Web and vis Splunk configurations.
* Expertise to analyze and correlate events through Spunk grouping commands such as transaction, join and append.
* Performed into the Splunk Admin responsibilities such as capturing, analyzing and monitoring front end and middle ware applications.
* Creating Vulnerability Assessment dashboard using Rapid7, Joval that aggregates data across multiple services to identify critical threats and proactively mitigate risks.
* Parsing, indexing, searching, concepts hot, warm, cold, frozen buckets.
* Onboard new log sources with log analysis and parsing to enable SIEM correlation. Analyzed large datasets to identify metrics, drivers, performance gaps and opportunities for improvement.
* Responsible for security monitoring, analysis and troubleshooting of events generated by network security devices (IPS, IDS, Firewall), OSs, Application Servers, from different data sources (DB, log file, SNMP, Syslog) on ArcSight ESM.
* Implemented summary indexing for daily and monthly business reports with job scheduling.
* Generated Shell Scripts to install Splunk Forwarders on all servers and configure with common Configuration Files such as Bootstrap scripts, Outputs.conf and Inputs.conf files.
* Prepared, arranged and tested Splunk search strings and operational strings.
* Experience on use and understand to complex RegEx (regular expressions).
* Implemented Google map identifiers in Splunk dashboards using geo lookup commands.
* Involved prediction in application events using Splunk Algorithms.
* Deployed Splunk instances in the Linux environment.
* Good knowledge in building Splunk Apps for custom application requirement.
* Created Dashboards to monitor CPU Performance Peak, Memory Leakage.
* Monitor and track Splunk performance problems, administrations and open tickets with Splunk if there is need.
* Responsible for Scheduling and Automating Database tasks - Jobs, Alerts, Emails, Notification.
* Maintained and managed the application errors during production.
* Write automation scripts for APIs, Unit and functional test cases using Selenium WebDriver.
* Write automation scripts for REST API's using TestNG and Java.
* Worked on DB Connect configuration for MySQL and MSSQL.
* Splunk DB Connect 2.0 in search head cluster environments of Oracle, MySQL
* Created Splunk Dashboards to capture the Authentication breaches across application.
* Enables log debugging in Splunk using btool, Splunk on Splunk storm.
* Scheduled Reports to find the login defaulters across organization/application.
* Helped deploy Red Hat Enterprise Linux servers on VM Ware.
* Worked on Virtual Machine creation, templates, clones and snapshots.

**Environment: SPLUNK 6.3.1, Linux, UNIX, Oracle 11g, MS SQL Server 2012, SQL, Joval, Rapid 7, Bluecoat, IBM QRadar, IBM Guardium,VMF, Tripwire, Resilient, Service Now (ITAM)**

**Client: AT&T, El Segundo, California December 2013 to November2015**

**Role: Splunk Admin/ Developer**

**Responsibilities:**

* Implemented Splunk installation and administration of Linux servers using Red Hat Enterprise Linux and Oracle Enterprise Linux.
* Created Splunk knowledge bundles, Forms/Views/Dashboards.
* Buildup of Forwarders and perform Software installation upgrades and upgrading Splunk as and when required using automation tools.
* Performed Splunk Indexers/Search Heads up gradation, installation and configuration of Splunk Apps.
* Involved as a Splunk Admin in capturing, analyzing and monitoring front end and middle ware applications.
* Created Shell Scripts to install Splunk Forwarder on all servers and configure with common configuration files such as Bootstrap scripts, Outputs.conf and Inputs.conf Files.
* Configuring and base lining Hardware for Splunk on Linux Hosts. Conducting operational testing with Splunk Users.
* Created Bash Scripts for Automation of Splunk day to day tasks.
* Created complex Rex and Multikv commands to extracts the field from the log files.
* Involved in admin activities and worked on inputs.conf, index.conf, props.conf and transform.conf to set up time zone and time stamp extractions, complex event transformations and whether any event breaking.
* Monitored license usage, indexing metrics, Index Performance, Forwarder performance, death testing.
* Experience in handling network resources and protocols such as TCP/IP, Ethernet, DNS
* Configured Node manager to remotely administer Managed servers.
* Provide support with ensuring appropriate audit logs are captured and stored via the DLA Enterprise implementation of the ArcSight logger system.
* Creation and implementation of shell scripts to take care of Splunk file backup, monitoring alert log and log rotation.
* Installation and configuration of own Apps to monitor system performance including Splunk internal logs.
* Supporting migration from Splunk On Premise data center to Amazon AWS
* Launching, Configuring, Supporting large scale instances on AWS
* Handled configuration of advanced dashboard creation and optimization.
* User/Group Administration – Splunk authentication with LDAP for user accounts/groups creation and bindings of LDAP groups to Splunk.
* Dealt with Splunk Utilities (bucket rolling, user index creation and management, sourcetype, forwarder log monitoring input and output configuration).
* Installed Splunk Common Information Model add-on is packaged with Splunk Enterprise Security, Splunk IT Service Intelligence, and the Splunk App for PCI Compliance.
* Created an Active-Passive SPLUNK framework for fulfilling BCP requirements.
* Interaction with various application workgroups for requirements gathering, so as to design and plan the software and hardware infrastructure.
* Coordinated with various app support teams, training new hires, support team members.

**Environment: Splunk 6.x, Splunk Enterprise and splunk modules, WebLogic server 8.x/9.x/10.x/11g, Tomcat 6.0, IBM HTTP Server, Microsoft IIS 7.0, Apache 2.x, Solaris10, Windows 2008, Oracle 11g/10g, web services, LDAP, Oracle Access Manager, HTML, XML, SSL.**

**Client: Surya Technologies Inc., Cary, NC August 2011 to November 2013**

**Role: Splunk Consultant**

**Responsibilities:**

* Must have strong Splunk UI experience and able to debug expensive search queries.
* Understands Splunk configuration and able to debug Splunk related issues.
* Setup splunk Forwarders for new application environments and also for existing applications.
* Involved in standardizing Splunk forwarder deployment, configuration and maintenance across UNIX and Windows platforms.
* Good experience with scripting languages like perl, python and bash.
* Design solutions and concepts for data aggregation and visualization.
* Work with a small team to enhance the existing Infrastructure.
* Debug complex Splunk configuration issues.
* Server monitoring using tools likes Splunk, Solarwinds-Orion, HP BSM and HP Open View.
* Automating in Splunk using Perl with Service-Now for event triggering.
* Maintain or bring in industry standards in network and storage solutions.
* Build Splunk apps from ground up for Splunk to interact with 3rd party software/hardware.
* Communicate with peers and supervisors routinely, document work, meetings, and decisions.
* Define process for centralized application log file ingestion into Splunk
* Identify the amount of work needed to ingest, interrogate and map log files correctly
* Identify critical data elements that must be present to ensure log files can be used for monitoring & Define desired format for log files to be used
* Define a mapping & exception process for those log files that cannot be generated in the desired format
* Perform log interrogation to determine elements
* Perform mapping/parsing in Splunk for various log feeds
* Define process to keep inventory updated as new feeds come in
* Experience in working with Splunk authentication and permissions and having significant experience in supporting large scale Splunk deployments
* Interacted with the data warehousing team regarding extracting the data and suggest the standard data format such that Splunk will identify most of the fields.

**Environment: SPLUNK 6.1.3, Linux, UNIX, MS SQL Server, Splunk Enterprise Security.**

**Client: Silex Infotech, India May 2009 to August 2011**

**Role: SQL Developer**

**Responsibilities:**

* Responsible for the study and analysis of the systems design and implementation.
* Developed reports using SQL Server Reporting services and utilizing complex SQL queries and stored procedures.
* Involved in tuning the existing T-SQL code for performance improvement.
* Followed the best practices in writing T-SQL for universal readability and reusability of code.
* Participated in all the phases of Software Development Life Cycle (SDLC) like, Requirements Review, Test Documentation, Application testing, detect tracking.
* Created various database objects including tables, stored procedures and functions.
* Analyzed code to find causes of errors and revise programs as needed.
* Well versed with all types of manual testing like functional testing, smoke testing, positive & negative testing, regression testing, integration testing, GUI testing & browser compatibility testing.
* Fixed data issues and bags by changing code or business rules. Troubleshoot import function/daily feed file failure.
* Good understanding of application build cycles and following the required test strategy to meet the testing requirement.
* Reviewed and analyzed Business Requirements, Project Plans, Prototype, Flow Diagrams, Use Cases, System Design documents and created Detailed Test Cases.
* Created stored procedures to hold the business logic.
* Created views as per client requests.

**Environment: MS SQL Server 2000, T-SQL, Quality center, MS-Office, Internet Explorer, UNIX, Windows XP/Vista.**

# **EDUCATION QUALIFICATION AND CERTIFICATION**

* Bachelor of Technology, JNTU Hyderabad, India.
* Master of Science Degree, Texas A&M University-Kingsville, Texas.
* Splunk certified Power User.
* Splunk Certified Admin.