Ravi S. Dandamudi

Sr. Splunk Certified Developer & Admin

(732) 734 – 0440

GREEN CARD Work Status

**Summary of Qualifications:**

* IT Professional with 8+ years of strong & referable experience analysis, design, development, and, integration of large client- server and web-based applications.
* Highly skilled on Splunk 5.x,6.x, Splunk Enterprise Security 6.x, Splunk DB Connect 1.x, 2.x on distributed and Clustered Splunk environments on Linux and Windows operating systems.
* Extensive experience in Installation, Configuration, and Migration, Trouble-Shooting and Maintenance of Splunk, Apache Web Server on different UNIX flavors like Linux.
* Expert in Splunk development creating Apps, Dashboards, Data Models, etc.
* Experience in installing and using Splunk apps for UNIX and Linux (Splunk nix).
* Experience on Splunk Enterprise Deployments and enabled continuous integration on as part of configuration management.
* Experience in Splunk GUI development creating Splunk apps, searches, Data models, dashboards, and Reports using the Splunk query language (SPL).
* Excellent logical, analytical & debugging skills with good interpersonal skills, highly motivated, fast learner, good team player and very proactive in problem solving and providing best solutions.

**Technical competencies:**

Log Monitoring / Management Tools Splunk Enterprise 4.x/5.x/6.x, Nagios, Puppet, Chef

Operating Systems Windows 10.x/8.x/7.x, Unix/Linux, Red Hat 6.x/ ubuntu13.x or later, AIX, Solaris

Programming / Scripting Languages C++, Java, C#, HTML, XML, CSS, JavaScript, JQuery, Bootstrap, Shell Script, Perl, Batch

Databases SQL Server, Web Logic, DB2 Connect

Servers Apache Tomcat

Cloud Technologies Amazon Web Services (AWS)

**Professional Experience:**

***Client: General Motors -Detroit, MI*** *July 2016 – Present*

***Role: Splunk Administrator/ Developer***

**Roles & Responsibilities:**

* Installation and configuration of Splunk product at different environments.
* Upgraded Splunk Enterprise from v 6.2 to v 6.5.2 in clustered environments and non-clustered environments.
* Monitoring & analyzing the real-time events for the security devices like Firewall, IDS, Anti-Virus etc., using SIEM tools.
* Weekly/Monthly incident analysis report.
* Analyzing the events and providing solutions for the incidents.
* Involved in setting up alerts for a different type of errors.
* Data Enrichment using the lookups and data Interpretation using the Fields and Fields Extraction and performing the data Normalization using the Tags.
* Worked as part of Cyber Security Incident Response team to check on malware virus and threat emails.
* Developed Splunk Search Processing Language (SPL) queries, created Reports, Alerts and Dashboards and customized them.
* Implemented Dynamic drilldowns that provide greater flexibility to the end user.
* Publishing data into Splunk through configurations such as inputs.conf, severclass.conf, server.conf, apps.conf and outputs.conf configurations.
* Developed robust, efficient queries that will feed custom Alert, Dashboards and Reports.
* Worked on Parsing, Indexing, Searching concepts Hot, Warm, Cold, Frozen bucketing.
* Assisted in various projects related to Bay Dynamics and CASB and ingested Splunk into their environment.
* Planned, implemented, and managed Splunk for log management and analytics
* Monitor security violations, flag potential violations and logging security incidents in Service Now.
* Implemented AWS solutions using EC2, S3, Dynamo DB, EBS, Elastic Load Balancer, and Auto scaling Groups.
* Configured AWS Config Rules to evaluate AWS resources for compliance.
* Migrated applications from Legacy data to the AWS cloud.
* Administered Linux servers for several functions including managing Apache/Tomcat server, mail server, and MySQL databases in both development and production.
* Validate the existing rules and provide recommendation on fine tuning the rules.
* Analyzed AWS configuration logs, AWS Cloud watch flow logs.
* Provide deployment strategies with the understanding of affordable risk based on customer acceptance.
* Developed Splunk Dashboards, searches and reporting to support various internal clients in Security, IT Operations and Application Development.
* Played part in Proof-of-Concepts (POC) on Splunk implementation.
* Mentored and guided other team members on Understanding the use case of Splunk.
* Introduced Sumo Logic, a cloud-based application (SaaS).
* Developed Proof of Concepts (POC) for various applications for log analysis. Started migrating (re-building) few applications to Sumo Logic from Splunk.

***Client: Loomis Sayles - Boston, MA*** *August’15 – June’16*

***Role: Splunk Administrator/ Developer***

**Roles & Responsibilities:**

* Troubleshoot technical issues to establish the root cause of problems and form a solution or workaround across a range of environments.
* Reproduce issues and if necessary file bug reports, escalate cases to Vendor, and provide necessary documentation.
* Developed a POC on usage of Puppet Configuration Management tool.
* Splunk server configurations (web, indexing retention, authentication, etc.)
* Splunk data onboarding operations (inputs, SQL, index-time configurations)
* Splunk data parsing operations (search-time field extractions, event types, tags).
* Worked on Python general scripting
* Monitoring and response for security events in Security Operations Center (SOC) team.
* Mentor members of the technical staff to support and assist in Splunk-related activities.
* Create and maintain documentation related to Architecture and Operational processes for Splunk.
* Involved in Installation, Administration and Configuration of Splunk Enterprise and integration with local legacy systems.
* Splunk DB Connect 2.0 in search head cluster environments of Oracle.
* Developed scripts to consume Salesforce Event Monitoring API, providing stakeholders with insights into user behavior and usage trends.
* Customized Splunk dashboards, visualizations, configurations, reports and search capabilities using customized Splunk queries.
* Worked on Splunk, Shell scripting to automate and monitor the environment routine tasks.
* Managed indexes and cluster indexes, Splunk web framework, data model and pivot tables.
* Performed troubleshooting and/or configuration changes to resolve Splunk integration issues.
* Played a key role in identifying and driving process changes within the team.

***Client: IBM India - Bangalore, India*** *October’12 – June’15*

***Role: Splunk Developer***

**Roles & Responsibilities:**

* Responsible for the end-to-end event monitoring infrastructure of business-aligned applications.
* Installation, Configuration, Migration, Trouble-Shooting and Maintenance of Splunk, WebLogic Server 7.0/8.1/9.x/10.x, Apache Web Server on different UNIX, Linux.
* Prepared, arranged and tested Splunk Search Strings and Operational Strings.
* Created and configured management reports and dashboards.
* Monitored Database Connection Health by using Splunk DB connect health dashboards.
* Monitoring Splunk dashboards, Splunk Alerts and configure scheduled alerts based on the internal customer requirement.
* Created EVAL Functions where necessary to create new field during search run time.
* 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.
* Generated Search Commands to retrieve multiline log events in the form Single transaction giving Start Line and End Line as inputs.
* Guarantee high accessibility & execution through flat scaling and burden adjusted segments.
* Deliver inputs for identifying best fit architectural solutions - deployment for Splunk project.
* Setting up dashboards for senior management and production support- required to use Splunk.
* Architected various components within Splunk (indexer, forwarder, search head, deployment server), Heavy and Universal Forwarder, Parsing, Indexing, Searching concepts, Hot, Warm, Cold, Frozen bucketing, License model.
* Maintained and managed assigned systems, Splunk related issues and administrators.
* Used Splunk Enterprise REST API that uses HTTP requests to configure and manage Splunk instance, create and run searches.

***Client: IBM India - Bangalore, India*** *May’10 – September’12*

***Role: Java / J2EE Developer***

**Roles & Responsibilities:**

* Involved in gathering and analyzing system requirements.
* Used Multi-threading and Exceptional Handling in the development of applications.
* Developed the application using Spring Web MVC architecture.
* Worked extensively on Spring IOC/ Dependency Injection.
* Configured the crosscutting concerns like logging, security using Spring AOP.
* Developed Data Access Layer using Hibernate ORM framework.
* Coded numerous DAO's using Hibernate Dao Support. Used Criteria, HQL and SQL as the query.
* Extensive involvement in database schema design, development and coding.
* Tuned SQL Queries, created complex stored procedures, packages, functions, triggers, jobs.
* Coded the logic for performing the integrity checks for numerous source files in the Controller layer.
* Involved in the understanding and designing of the complex back-end framework.
* Used JSTL expression language for validation.
* Used XML for data exchange and schemas (XSDs) for XML validation. Used XSLT for transformation of XML.
* Involved in all phases of SDLC including requirements Collection, Design and Analysis of the customer specifications from business analyst.
* Designed and developed user interface screens using HTML, DHTML and JSP.
* Developed and maintained the data layer using the EJB's.
* Created and maintained the configuration of the Application Framework.
* Used Eclipse as Java IDE tool for creating Action classes and XML files.
* Involved in maintenance of the application.
* Used Bugzilla as a Bug Reporting Tool.

**Certification & Education:**

* **Bachelor’s Degree in Information Technology**

Amity University, Noida, India

**References:** Provided upon request…