Splunk Admin/ Developer Splunk Admin/Developer Splunk Admin/ Developer - American Express Phoenix, AZ Over 9 Years of IT experience in field as Splunk Engineer, Linux/UNIX, Java, PLSQL and SQL DBA, Monitoring, Data Analytics performance, tuning, Troubleshooting and Maintenance of Data Base. In depth and extensive knowledge in Splunk 5.x and 6.x product, Distributed Splunk architecture and components including search heads, indexers, forwarders, etc. and various components. Passionate about Machine data and operational Intelligence. 5 + years of experience as Splunk Admin/ Developer, performed activities including requirement analysis, design and implementations of various client-server-based applications. Created Splunk Dashboards for different sorts of business clients in association. Expertise in writing SQL Queries, Dynamic-queries, sub-queries and complex joins for generating Complex Stored Procedures, Triggers and User-defined Functions. Experience with Splunk technical implementation, planning, customization, integration with big data and statistical and analytical modeling. Expertise in Actuate Reporting, development, deployment, management and performance tuning of accurate reports. Setting up Splunk and using it in Cloud Hosted environments like Amazon AWS. Experienced in Preparing, arranging and testing Splunk search strings and operational strings. Headed Proof-of-Concepts (POC) on Splunk implementation, mentored and guided other team members on Understanding the use case of Splunk. Expert in Analyzing the Security Related Logs from various sources using SIEM system which creates alerts whenever it detects Anomalous Transactions and blocks malicious activities. Worked on Splunk ES (SIEM) that enable organizations to detect, respond and prevent these threats by providing valuable context and visual insights to help you make faster and smarter security decisions. In depth Knowledge with search head clustering and Index clustering. Implemented workflow actions to drive troubleshooting across multiple event types in Splunk. Stay current with the latest features/capabilities of the AWS platform. Expertise in creating accurate reports, Dashboards, Visualizations and Pivot tables for the business users. Interacted with using configuration files, modular inputs, and data models. Expert in using rex, Sed, erex and IFX to extract the fields from the log files. Installed Splunk DB Connect 2.0 in Single and distributed server environments and Parsing, Indexing, Searching

concepts Hot, Warm, Cold, Frozen bucketing. Worked with Restful API and shell scripting. Standardize Splunk forwarder deployment, configuration and maintenance in Linux and windows platforms. Created rolled based AD access for Splunk. Installing the Splunk Light Weight Forwarders, Forwarders, Indexers, Search Heads after configuring the files like output.conf, input. conf etc. Managing of Splunk licenses based on the requirement. Extensive experience and actively involved in Requirements gathering, Analysis, Reviews, Coding and Code Reviews, Unit and Integration Testing. Install different Splunk Applications, for example, Cisco for Splunk, Windows for Splunk and VMware for Splunk. Expertise in designing and developing applications using Java, J2EE Technologies like Servlets, JSP, EJB, JDBC, XML, JMS, AJAX, WebServices using SOAP and RESTful Services. Experience in implementing J2EE compliant applications using various Designpatterns, Struts, Spring, MVCframework, Hibernate and Messaging Middleware using JMS. Worked in Multi Clustered HadoopEcho-System environment. Familiar with components of Hadoop Ecosystem. Experience using XML, XSD and XSLT and knowledge of Log4j for error logging. Developed end to end monitoring script for the content publishing system. Team player with excellent communication, presentation and interpersonal skills. Worked on Agile methodology, SOA for many of the applications. Authorized to work in the US for any employer Work Experience Splunk Admin/ Developer American Express - Phoenix, AZ October 2016 to Present Responsibilities: Expertise with Splunk 6.3.04 Involved in various phases of Software Development Life Cycle (SDLC) including Analysis, Design, Testing, Implementation and Maintenance. Created Splunk Search Processing Language (SPL) queries, Reports, Alerts and Dashboards Installed and configured heavy, universal, and intermediate forwarders. Created data models and used report acceleration for faster searches. Splunk configuration that involves different web application and batch, create Saved search and summary search, summary indexes. Actively involved in trouble shooting issues. Worked on AppDynamics as a monitoring tool. ITSI integration with the information from these files across the ITSI app as part of ITSI workflows. Set up of Splunk dashboards for continuous monitoring for production support. Played a major role in understanding the logs, server data and brought insight of the data for the users. Designing and

maintaining production-quality Splunk dashboards using Xml. Able to make handle assumed names crosswise over application occasions and store data in Splunk storage Database (MongoDB). Analyzed various types of charts Alert settings Knowledge of app creation, user and role access permissions Analyzed EVAL Functions where necessary to create new field during search run time. Splunk configuration that involves Saved search, summary search and summary indexes. Integrated Splunk with Service now to create automatic incidents based on the alert. Helped in maintaining Splunk Instance and Monitoring health of the Cluster. Extracted various fields using field extractor, field extractions (rex) and calculated fields to optimize the search performance and reduce the load on the search ahead. Use techniques to optimize searches for better performance, Search time vs. Index timefield extraction and understanding of configuration files, precedence and working. Continuous monitoring of the alerts received through mails to check if all the application servers and web servers are up. Configured various summary indexes by created saved searches to collect the aggregated data to run create dashboards on top of summary index. Assisted various other power users in optimizing the searches. Very good understanding of software development lifecycle (SDLC) process, Followed Agile scrum and story maps for dev tracking. Environment: Splunk 6.3.04, Splunk Apps, Linux, XML, Splunk Tools, Search Processing Language (SPL), Testing, AppDynamics, Perl. Splunk Engineer First Data - Atlanta, GA October 2015 to September 2016 Responsibilities: Worked in Splunk 6.3.04 (Currently involved in cluster upgrade to 6.3.15). Create Splunk Search Processing Language (SPL) queries, Reports, Alerts and Dashboards Installed and configured heavy, universal, and intermediate forwarders. Created data models and used report acceleration for faster searches. Installed and deployed forwarders with the help of puppet team. Created and Managed Splunk DB connect Identities, Database Connections, Database Inputs, Outputs, lookups, access controls. Implementation of medium scale Splunk ES architectures Designing and maintaining production-quality Splunk dashboards. Deployed applications on multiple WebLogic Servers and maintained Load balancing, High availability and Fail over functionality. Worked on Proactive Monitoring alerts using tools like ELK & SysDig monitoring components. Experience with search

ahead clustering and Index clustering. Helped in maintaining Splunk Instance and Monitoring health of the Cluster. On boarded data from various sources such as Oracle, Informatica, Salesforce, Autosys and Cognos. Extracted various fields using field extractor, field extractions (rex) and calculated fields to optimize the search performance and reduce the load on the search ahead. Configured various summary indexes by created saved searches to collect the aggregated data to run create dashboards on top of summary index. Wrote complex alert logics for smart proactive alerting for the various other teams. Lead the team in communicating with Application subject matter expertise to understand the pain point of the logs. Provided solutions for understanding microservices architecture including Couchbase/NoSQL DB for upgrading technical skills for Development & Operations support. Lead the team in actively implementing smart Splunk solutions. Developing custom web application solutions for internal ticket metrics reporting, onboard new log sources with log analysis and parsing to enable SIEM correlation. In depth experience with props. conf, transforms. conf, inputs. Conf. Followed Agile scrum methodology. Environment: Splunk 6.3.04, AppDynamics, Micro Services, NewRelic, Linux, Bash, Perl, Sed, rex, erex, Splunk Knowledge Objects, Python. Splunk Admin/ Developer Cuna Mutual group - Madison, WI July 2014 to September 2015 Responsibilities: Expertise with Splunk 6.2.3, Involved in the Splunk Upgrade from 6.1 to 6.2 Created EVAL Functions where necessary to create new field during search run time. Coordinating with the business analysts and developers and discussed issues in interpreting the requirements. Installed Forwarders for MDT and involved in data grooming to check that data is arriving clean in Splunk. Setup Splunk Forwarders for new application tiers introduced into environment and existing application. Involved in data migration for the VCloud setup. Active monitoring of Jobs through alert tools and responding with certain action to logs analyses the logs and escalate to high level teams on critical issues. Integrated Splunk with Active directory and LDAP authentication. Extensive experience on setting up the Splunk to monitor the customer volume and track the customer activity. Managed the 19 indexers clusters. Configured Nagios and integrated Splunk with Incident management tool. Used Splunk Deployment server. Have involved as a Splunk Admin in capturing, analyzing and monitoring front

end and middle ware applications. Involved in trouble shooting issues. Installed Splunk on nix and Splunk SOS for monitoring the health of the clusters. Created set of user roles to in LDAP and single sign on implementation. Followed Agile scrum and story maps for development. Environment: Splunk 6.2.3, Datameer, Linux, Bash, Perl, Hbase, Hive, Pig, Sed, rex, erex, Splunk Knowledge Objects, Python. Splunk Engineer State Farm - Bloomington, IL November 2012 to June 2014 Responsibilities: Involved in various phases of Software Development Life Cycle (SDLC) including Analysis, Design, Testing, Implementation and Maintenance. Getting data and Managing Splunk apps Splunk and Python Script is used to show how these logs can be analyzed for certain Events / Patterns and deduce information which can in turn be used to Self-learn and Self-Heal when these events re-occur on a regular basis. Used Splunk for Application Log, Security Log and Performance monitoring. Experience in Operational Intelligence using Splunk. Troubleshoot Splunk indexers, search heads and forwarder problems. Analyzed FACETS for Group Information, Enrolling Subscribers, adding members, Related Entities, Class/Plan definition and Premium Rate Tables. Configured Splunk multisite indexer cluster for data replication. Worked on log parsing, complex Splunk searches, including external table lookups. Created Splunk Search Processing Language (SPL) queries, Reports, Alerts and Dashboards Create rolled based AD access for Splunk. Onboard new log sources with log analysis and parsing to enable SIEM correlation. Active monitoring of Jobs through alert tools and responding with certain action w.r.t to logs, analyses the logs and escalate to high level teams on critical issues. Developed Splunk infrastructure and related solutions as per automation tool sets. Provide regular support guidance to Splunkproject teams on complex solution and issue resolution with the objective of ensuring best fit and high quality for Application teams. Knowledge of security threats and vulnerabilities and how to detect and mitigate them, experience in building security monitoring and incident management solutions using Splunk. Environment: Splunk 6.2.3, Datameer, Linux, Perl, Informatica, ServiceNow, Splunk Knowledge Objects, Python. Java Developer Lavu Soft - Hyderabad, Telangana November 2011 to October 2012 Responsibilities: Developed using new features of Java 1.5 like Annotations, Generics, enhanced for loop and Enums. Developed various

generic JavaScript functions used for validations. Developed screens using JSP, JavaScript, HTML, CSS, JQuery, AJAX and JSON. and Angular JS. Developed Web Services clients to consume those Web Services as well other enterprise wide Web Services. Created DDL and DML SQL scripts for creation of database objects. Created logical and physical data models putting to practice, concepts of normalization and RDBMS. Created and injected Spring services, Spring controllers and DAOs to achieve dependency injection and to wire objects of business classes. Used Core Java Design Patterns like Singleton, Factory, MVC, Intercepting Filter, Front Controller, Business Delegate, Service Locator, Session Facade and DAO. Designed and implemented Struts (MVC Paradigm) components such as Action Mapping, Action class, Dispatch action class, Action Form bean, and a form set for validation and used JavaBeans to return dynamic information. Used Spring Inheritance to develop beans from already developed parent beans. Defined Multi Action, Abstract Wizard Form and Simple Form Controllers using Spring MVC framework providing very clean division between controllers, flexibility with the use of interfaces and providing thinweb layer over business layer. Used JSF framework in developing user interfaces using JSF UI Components. Worked in all the modules of the application which involved front-end presentation logic developed using Tiles,JSP, JSTL and java script, XML Business objects developed using POJOs and data access layer using Hibernate. Involved in configuring Hibernate mapping files and POJO objects. Involved in writing Thread Safe blocks for multithread access to make valid transactions. Exposed the Web Services to the client applications by sharing the WSDL's. Database development required creation of new tables, PL/SQL stored procedures, functions, views, indexes and constraints, triggers and required SQL tuning to reduce the response time in the application. Used Junit unit testing, Selenium for UI testing and Fitnesse for Integration testing. Environment: Spring, Hibernate, PL/SQL, HTML, CSS, JSP, JavaScript, POJO, DAO, MVC, JST, XML, JSF, Java 1.5, JavaBeans, Singleton, Intercepting Filter. Java Developer Quinnox - Mumbai, Maharashtra March 2009 to October 2011 Responsibilities: Developed Use Cases, Class diagrams and Sequence and Activity diagrams using Rational Rose. Coded Servlet classes in java web server environment. Used JDBC to connect to Oracle8i database. Created web pages using

JSP. Developed the presentation layer and GUI framework that are written using HTML, CSS and Client-Side validations were done using JavaScript. Used java features such as Generics, Collections API. Wrote SQL/PL-SQLQueries, Stored Procedures and Functions in Oracle. Used SVN for version control. Developed test cases using JUnit and tested the application. Responsible for the performance PL/ SQL procedures and SQL queries Used SVN for the concurrent development in the team and for code repository. Deployed applications on Linux client machines Involved in regression testing, evaluating the response times, and resolving the connection pooling issues. Environment: Java 1.6, JDBC, Servlets, SQL, Oracle9i, HTML, JSP, XML, UML, HTML, CSS JavaScript, WebSphere, UNIX, Subversion. Education Bachelor's Skills Apache, Linux, Shell scripts, Unix, Hdfs, Big data analytics, Data analytics, Datameer, Db2, Etl, Informatica, Splunk, Design patterns, Html, Javascript, Python, Xml, Jdbc, Sql server, Mysql Certifications/Licenses Driver's License Additional Information TECHNICAL SKILLS: Splunk/ Java: Splunk 6, Splunk Cloud, Splunk Enterprise, Splunk modules, Splunk DB Connect, Splunk IT Service Intelligence, Splunk Web Framework Splunk, Splunk Hunk, Splunk on Splunk HDFS, Java, J2EE, Eclipse, Windows NT 4.0, UNIX, My Eclipse IDE, JSP/Servlets, Design patterns, Struts, Spring, MVC framework, Hibernate, JDBC, XSD, SAX, JAXP, Oracle8, UNIX. Big data Analytics: Datameer 2.0.5, Splunk, Tableau, AppDynamics ETL Tools: Informatica, Talend Programming Languages: Python, Linux, shell scripts Databases: Oracle 11g/10g/9i, MySQL, DB2, MS-SQL Server Web Servers: Web Logic, Web Sphere, Apache Tomcat Web Technologies: JQuery, Java Script, HTML, XML, JavaScript, AJAX, SOAP, WSDL Network Protocols: TCP/IP, UDP, HTTP, DNS, DHCP

Name: Virginia Bruce

Email: zkennedy@example.net

Phone: (643)646-8202x1232