** **

**Abhishek Sharma**

**Sr. Splunk Engineer**

+918335866647

Abhishek.msharma@outlook.com

**SUMMARY:**

* Experience working on **Splunk** 5.x, 6.x on **distributed** and **Clustered** Splunk Environments on Linux and Windows operating systems.
* Expertise in configuring and administering complete splunk Infrastructure - **Search Head**s, **Indexers**, **Heavy Forwarders**, **Deployment Server**, **Cluster Master**, **Deployer**, **License Master** and **Universal Forwarder** on Linux and Windows operating systems.
* Configured Clusters for load balancing and fail over solutions.
* Hands on experience on administrative tools like **Splunk** AdministrationConsole and Command line interface.
* Proficient in setup Splunk forwarder agents across various OS platforms to gather the data.
* Used **Splunk Enterprise Security**, which helped to quickly detect and respond to internal and external attacks thus minimizing the risks.
* Experience with Splunk Searching and Reporting modules, **Knowledge Objects**, Add-On’s, Dashboards, Clustering and Forwarder Management, deployment model.
* Installed and configured **Splunk** **DB Connect** in Single and distributed server environments.
* Created and Managed Splunk DB connect Identities, Database Connections, Database Inputs, Outputs, **lookups**, access controls.
* Monitored Database Connection Health by using Splunk DB connect health dashboards.
* Experience on **Splunk** search construction with ability to create well-structured search queries that minimize performance impact.
* Expertise with the usage of various search commands like stats, chart, timechart, transaction, strptime, strftime, eval, where, xyseries, table etc.
* Experience on **Splunk** data flow, components, features and product capability.
* Expertise in creatingKPI’s, Services and Glass Tables in **Splunk IT Service Intelligence.**
* Developing **Splunk Queries** and dashboards targeted at understanding application performance and capacity analysis.
* Experienced in providing quick fixes as **production** **support** analyst.
* Developed reports, dashboards, alerting, creating roles, user provisioning and clustering using **Splunk**.
* Drive complex deployments of **Splunk** **dashboards** and reports while working side by side with technical teams to solve their integration issues.
* Hands on development experience in customizing **Splunk** dashboards, visualizations, configurations, reports and search capabilities using customized **Splunk** queries.
* Worked on log parsing, complex Splunk searches, including external table lookups.
* Experienced working with Agile Methodology.
* Maintain various level of documentation. Co-ordinate with change management.
* Excellent interpersonal and communication skills to work cooperatively with persons at all levels in the organization.

**Education Details:**

**Certifications:**  
**Splunk Certified User**

**Splunk Certified Power User.**

**Splunk Certified Administrator**

**Splunk Certified Developer**

**Splunk ITSI Certified Admin**

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| **Monitoring Tools** | SPLUNK (5.0 – 6.6.3) , Premium APP’s – ITSI , Enterprise Securtiy. |
| **Development Tools** | MSBI SUITE (SSAS,SSIS and SSRS) |
| **Networking & Protocols** | TCP/IP, Telnet, HTTP, HTTPS, FTP, SNMP, LDAP, DNS, DHCP, firewalls, proxies DNS, malware detection |
| **ETL Tools** | SQL Server Integration Service (SSIS) |
| **Reporting Tools** | SQL Server Reporting Services (2000/2005/2008 R2/2012), MS Access, MS Excel, Crystal Reports 10, |
| **Database** | MS SQL Server 2014/2008 R2/2005/2000, MS Access. |
| **Web Technologies** | HTML, CSS, XML |
| **Other Tools** | MS Office Suite (Microsoft Word, Power Point, MS Visio), OLAP & OLTP,TFS. |
| **Operating Systems** | Windows 2003/2008 Server, Windows XP, Windows Vista.Linux |

**Employer Details**

|  |  |
| --- | --- |
| 2014- 2017 | Ericsson Global India Pvt Ltd |
| 2017 - 2019 | Reliance Jio |
| 2019 - Till Date | HCL technology |

**Professional Experience**

**Deutsche Bank Jan’ 2020 – Till Date**

**Sr. Splunk Engineer**

* **I**nstalled, Configured, Maintained, Tuned and Supported Splunk Enterprise Server 6.0 and Splunk Universal Forwarder 6.0.
* Administered a complex cluster based environment involving search heads in a cluster while the indexers are in standalone mode.
* Configured Splunk forwarder to send unnecessary log events to "Null Queue" using props and transforms configurations.
* Created and configured management reports and dashboards in Splunk for application log monitoring.
* 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.
* Responsible for developing Splunk queries and dashboards targeted at understanding application performance and capacity analysis.
* Extensive experience on setting up the Splunk to monitor the customer volume and track the customer activity.
* Have involved as a Splunk Admin in capturing, analyzing and monitoring front end and middle ware applications.
* Created Splunk app for Enterprise Security to identify and address emerging security threats using continuous monitoring, alerting and analytics.
* Created and configured management reports and dashboards in Splunk for application log monitoring.
* Responsible for administering, maintaining, and configuring a 24 x 7 highly available, Splunk apps for production portal environment.
* Work closely with Application Teams to create new Splunk dashboards for Operation teams using advance XML and CSS.
* 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.
* Extensively used Splunk Search Processing Language (SPL) queries, Reports, Alerts and Dashboards.
* Installation and implementation of the Splunk App for Enterprise Security and documented best practices for the installation and performed knowledge transfer on the process.
* Using DB connect for real-time data integration between SplunkEnterprise and databases.
* Analyzing in forwarder level to mask the customer sensitive data able to manage distributed search across set of indexers.
* Responsible to filter the unwanted data in heavy forwarder level thereby reducing the license cost.
* Worked with administrators to ensure Splunk is actively, accurately running, and monitoring on the current infrastructure implementation.
* Worked on properly creating/maintaining/updating necessary documentation for Splunk Apps, dashboards, upgrades and tracked issues.
* Provided On-call support for various production applications.
* Administered various shell and Python scripts for monitoring and automation.

**JP Morgan Chase, USA. Jan’ 2018 – Nov 2019**

**Sr. Splunk Developer**

* Administering Unix and windows servers
* Installed Splunk Enterprise, Splunk forwarder, Splunk Indexer, Apps in multiple servers on splunk Infrastructure.
* Involved in standardizing Splunk forwarder deployment, configuration and maintenance across UNIX and Windows platforms.
* Monitoring the server and collaborate with the teams to resolve the issues.
* Created **Splunk** Search Processing Language (SPL) queries, Reports, Alerts and Dashboards.
* Experience on Application migration between the different servers such as DEV, STAGE and PROD both on- prem and Cloud environments.
* Extracting the fields using regular expression.
* Gathering and documenting the requirements from the clients and reviewing them accordingly in the Splunk Usage perspective.
* Configured JDBC **connections** and data sources for Oracle 11g.
* Designed, developed and implemented multi-tiered **Splunk** log collection solutions.
* Monitored error logs, fixed problems and **tuned** **parameters** in **Tomcat** environment.
* Strong knowledge / understanding of **Splunk** Index Clustering and Search Head pooling.
* Experience in creating, testing and deploying operational search strings.
* Installed, configured, integrated, tuned and administered Tomcat 7.0 in various environments viz. Dev, Test, Pre-Prod and Prod.
* Experience in creating visualizations of reports, dashboards for customer interfacing, alerting, roles/user provisioning and clustering with **Splunk**.
* Experience with **Splunk** forwarders and intermediate forwarders as well as index and search head clusters.
* Involved in Splunk administration roles including version upgrades, permissions, and audit compliance.
* Help application teams in on-boarding Splunk and creating dashboards/alerts/reports etc.
* Expertise in creatingKPI’s, Services and Glass Tables in **Splunk IT Service Intelligence.**
* Worked on new indexers and search head in Cluster environment on Linux platform with **Splunk 6.x** version.
* Troubleshoot production issues and fixed Java Heap size errors.
* Involved in configuration management, software deployment, change management, performance monitoring, and application maintenance.
* Troubleshoot **Splunk** server and forwarder issues.

**Blue Cross Blue Shield of Anthem, USA. Feb’ 2017 – Dec 2017**

**Sr. Splunk Admin**

* Supported on call 24x7 schedule for Production Support.Worked on Splunk architecture and various components (indexer, forwarder, search head, deployment server, deployment model) Heavy & Universal forwarder, and License model.
* Good Understanding of configuration files, precedence and daily work exposure to Props.conf, transforms.conf, inputs.conf, outputs.conf and Setting up a forwarder information based on requirement.
* Maintained Splunk Environment with multiple indexers; managed and configured settings with deployment model.
* Improved search performance by configuring to search heads for all Indexes in production.
* Analyzed security based events, risks and reporting instances.
* Developed Splunk queries and dashboards targeted at understanding application performance and capacity analysis.
* Worked for getting data in managing Splunk apps.
* Assisted internal users of Splunk in designing and maintaining production-quality dashboards.
* Installation and implementation of several kind of visualizations to Splunk dashboards.
* Continuous monitored of the alerts received through emails to check if all the application servers and web servers are up.
* Knowledge on Parnsing, Indexing, Searching concepts Hot, Warm, Cold, Frozen bucketing.
* Conducted surveillance on various phishing emails and created alerts from future spam.
* 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 us

**Kaiser Permanente, Pleasanton, CA July ’15 - Oct ‘16**

**Sr. Splunk Engineer**

**Key Responsibilities:**

* Created several different dashboards for multiple different teams and clusters in splunk infastructure.
* Install Splunk forwarder on various platforms like windows, Linux, Unix.
* Install Splunk indexers and Search heads for various Splunk environments.
* Troubleshoot Splunk components like forwarders, indexers and search heads and performance issues.
* Created Splunk Search Processing Language (SPL) queries, Reports, Alerts and Dashboards.
* Importing the data in Splunk through inputs.conf, props.conf and transforms.conf.
* Create multiple Splunk role based LDAP authentication.
* Designed core scripts to automate Splunk maintenance and alerting tasks
* Maintenance of splunk Environment with multiple Indexers.
* Created many of the proof-of-concept dashboards for IT operations, and service owners which are used to monitor application and server health.
* Deploy, configure and maintain Splunk forwarder in different platforms.
* Creating Reports, Pivots, alerts, advance Splunk search and Visualization in Splunk enterprise.
* Provide power, admin access for the users and restrict their permission on files.
* Installed and upgraded Splunk software in distributed and clustered environments for numerous

corporations and public entities.

* Well versed in both remote and on-site user Splunk Support.
* Configured and deployed applications in various work environments like Development, System Test and Production.
* Research and Troubleshooting of emerging application issues, from WebLogic configuration to code issues, Change control processes.
* Maintain, grow and improve the TVX Splunk environment.
* Integrated Service Now with Splunk to generate the Incidents from Splunk.
* Developed ANT build scripts, UNIX shell scripts and auto deployment process.
* Problem determination using local error logs and by running user traces and service traces.
* Documenting design procedures and test plans.

**Burger King, Miami, FL** **Jan’14-July ‘15**

**Splunk Engineer**

**Key Responsibilities:**

* As primary for Splunk support, supported Splunk circulated environment comprising of search heads, indexers and forwarders across different OS including Aix, Solaris and Windows.
* Configured Indexer replication to achieve Data availability, Data fidelity and Disaster tolerance.
* Improved search performance by configuring 2 search heads for all Indexes in production.
* Parsing, Indexing, SearchingconceptsHot, Warm, Cold, Frozen bucketing.
* Involved in standardizing Splunk forwarder deployment, configuration and maintenance across UNIX and Windows platforms.
* Worked on setting up Splunk to capture and analyze data from various layers Load Balancers, Webservers and application servers.
* Install different Splunk Applications, for example, Cisco for Splunk, Windows for Splunk and VMware for Splunk.
* Created and configured management reports and dashboards in Splunk for Application Log Monitoring and Change control processes.
* Responsible for administering, maintaining and configuring a 24 x 7 highly available, Splunk apps for production portal environment.
* Efficiently handled Work Load Management for load balancing and failover, improving performance, reliability and scalability.
* Gathering different wellsprings of syslog and XML information from different gadgets, applications, and information bases.
* Various types of Charts Alert Settings Knowledge of app creation, user and role access permissions. Creating and managing app, Create user, role, Permissions to knowledge objects.
* Work towards accomplishing a speedier ROI and keeping up partners persuaded of the worth and undiscovered open doors in Splunk.
* Worked on large datasets to identify metrics, drivers, performance gaps and opportunities for improvement.
* Supporter and execute arrangements considering a full information lifecycle (Search & Investigate, Add Knowledge, Monitor & Alert, Report & Analyze).
* Basic understanding of Network Firewalls, Load-balancers, LDAP and complex network design.

**Blue Cross Blue Shield of Louisiana, USA. Nov’ 2013 – Dec’ 2014**

**Sr. SQL Server Developer**

**Responsibilities:**

* Designed a complex SSIS package for data transfer from three different firm sources to SQL Server 2008.
* Implemented data views and control tools for guarantee data transformation using SSIS.
* Extensively worked on SCD transformation in SSIS package.
* Used SSIS and T-SQL stored procedures to transfer data from OLTP databases to staging area and finally transfer into data warehouse.
* Used various SSIS tasks such as Conditional Split, Derived Column, lookup which were used for Data Scrubbing, data validation checks during Staging, before loading the data into the Data warehouse.
* Developed and deployed data transfers packages to the appropriate destinations using SSIS.
* Experience in creating Jobs, Alerts, SQL Mail Agent, and schedule SSIS Packages.
* Created SQL server configurations for SSIS packages.
* Successfully deployed SSIS packages with defined security.
* Involved to write complex T-SQL queries and Stored Procedures for generating reports.
* Responsible for creating reports based on the requirements using SSRS 2008.
* Identified the database tables for defining queries to generate reports for analysis of data using SQL Server Reporting Services in Report Builder.
* Defined the report layout and identified Datasets for the report generation.
* Created different type of reports including Cross-tab, Conditional, Drill-down, Sub reports also parameterized reports.
* Generated reports on wealth information, account information, research reports using adhoc reporting to be used by the clients and advisors.
* Created numbers of complex formula in sub report.
* Designed and created Report templates, bar graphs and pie charts based on the financial data.
* Scheduled the monthly/weekly/daily reports to run automatically.
* Developed, implemented and maintained various database objects such as Stored Procedures, Triggers, Functions, Indexes and Views.
* Performance tuning of SQL queries and stored procedures using SQL Profiler and Index Tuning Wizard.
* Performed development support, document reviews, test plan, integration of the system.
* Pivot table are used to provide structured to Reports in proper manner like months etc.

**Client: AOL America Online, USA. Oct’ 2012 – Oct’ 2013**

**Senior SQL/SSIS Developer (Offsite from Hyderabad)**

**Responsibilities:**

* Worked as onsite coordinator for the VUE Compensation Management System.
* Responsible for gathering requirements from clients and sharing the requirements with the off-shore team.
* Worked closely with developers, end users and Administrators in designing and creating databases and other objects.
* Actively involved in designing databases for the system.
* Optimized database queries and stored procedures.
* Reduced considerable amount of execution time on compensation procedure.
* Designed SSIS packages to extract data into VUE from various carriers.
* Designed and developed SSIS packages to load policy and premium data from source systems.
* Actively participated to resolve the production tickets.
* Maintained databases, performed VUE software installations and upgrades, monitored Database Performance.
* Used Visual Source Safe for file maintenance.
* Documentation of the new assignments, technical specifications and requirement documents.
* Performed unit testing, integration testing and system testing.

**Vista Health plan, Sunrise, FL Aug ’ 2011 – Sep’ 2012**

**Software Engineer**

**Responsibilities:**

* Job responsibilities include involvement in SDLC, requirement gathering and understanding, documentation, application development and providing support for technology and functionality related bugs reported by client.
* Worked closely with developers, end users and Administrators in designing and creating databases and other objects.
* Created stored procedures, user defined functions for calculating commissions and payments in PL/SQL.
* Created batch processes and procedures for data export received in flat files.
* Created SQL load batch process for loading flat files to destination system.
* Coordinated with the team members to develop the application on time and in line with the quality requirements.
* Maintained databases, performed VUE software installations and upgrades, monitored Database Performance.
* Used Visual Source Safe for file maintenance.
* Documentation of the new assignments, technical specifications and requirement documents.
* Designed and developed applications including UI layer, business layer, data layer, and common layer in VB Programming language.
* Worked with Implementation team and closely moved with end users to implement/support production issues.