**Poonam K**

**Sr. Splunk Engineer**

[povnamk@gmail.com](mailto:povnamk@gmail.com) **8104601312**

**SUMMARY:**

* Experience working on **Splunk** 5.x, 6.x,7x,8x 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.

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| **Monitoring Tools** | SPLUNK (5.0 – 6.6.3,7.0.7,3.8.0) , Premium APP’s – ITSI , Enterprise Securtiy. |
| **Development Tools** | MSBI SUITE (SSAS,SSIS and SSRS) |
| **Operating Systems** | Windows 2003/2008 Server, Windows XP, Windows Vista.Linux |

**Employer Details**

|  |  |
| --- | --- |
| 2012-2017 | Ionic Pvt Ltd |
| 2017 - 2019 | Klouddata Labs |

**Professional Experience**

**JIo Telecom Jan’ 2017– 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.

**Ionic Pvt Ltd, 2012 – June 2017**

**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.
* 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.