**Sahithi Chowdary**

**Snr Splunk Engineer**

[**sahithii54@gmail.com**](mailto:sahithii54@gmail.com)

**972-521-9996**



|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **SUMMARY:**   * Over **6** years of experience in Information Technology field with strong experience as **Splunk Developer, Administrator, Application Performance Monitoring and Business Intelligence** * Worked on large datasets to generate insights by using Splunk.  Experienced developing **Splunk queries, alerts** and **dashboards** for application performance and capacity analysis. * Strong experience on **Application Performance Monitoring and Security Information Event Management (SIEM)** * Worked with **Splunk 5.x and 6.x product, and distributed Splunk architecture**. Experienced in Operational Intelligence using Splunk. * Participated in various phases of Software Development Life Cycle (**SDLC**) including Analysis, Design, Testing, Implementation and Maintenance. * Excellent communication, analytical and interpersonal skills and ability to learn new concepts and supported 24/7 on call in production and development environment.   **TECHNICAL SKILLS:**   |  |  | | --- | --- | | Tools | Splunk 6.4/6.3, Splunk ES 4.0, Splunk ITSI 2.4, Nagios, AppDynamics, Dynatrace NewRelic, JIRA, and Confluence. | | SQL Server Tools | Enterprise Manager, SQL Profiler, Query Analyzer, SQL Server Management Studio, SSRS and SSAS. | | Database | MS SQL Server 2008R2, Oracle Database 11g, Microsoft Office 2007/2003. | | Programming Languages | C, C++, JavaScript, HTML, XML, Java, Ruby, Python and Shell Scripting. | | Operating System | Windows XP/NT/2000/2003/2008, Red Hat Linux, HPUX and Solaris | | Architecture | Relational DBMS, Client-Server Architecture, OLAP, OLTP. |   **PROFESSIONAL EXPERIENCE:**  **Senior Splunk Administrator/Developer March 2016 - Till Now**  **Xerox Corporation, Portland, OR**  **Responsibilities:**   * Created Dashboards and Reports to show Login count of each application, to show which app resources being accessed more, Number of failed logins, statistics on High hitting applications. * Developed a custom application in Splunk. * Generated Shell Scripts to install **Splunk Forwarders** on all servers and configure with common Configuration Files such as Bootstrap scripts, Outputs’ and Inputs’ files * Developed a POC on usage of Puppet Configuration Management tool. * Assigning User and role authentication including **LDAP authentication** and scripted authentication * Worked on **Splunk ITSI** to correlate relevant metrics/events into ‘Swim lanes’ to speed up investigations and diagnosis. * Worked on Puppet and chef for Automation of Configuration Management. * Setting up trusted proxies for Single Sign-on of the authentication. * Upgraded Splunk older version to Splunk enterprise 6.4. * Actively used Atlassian Products**- JIRA and Confluence** for Project Management. * Installed different Splunk Applications, for example, Cisco for Splunk, Windows for Splunk and VMware for Splunk. * Efficiently handled Work **Load Management** for load balancing and failover, improving performance, reliability and scalability. * Assisted internal users of **Splunk in designing** and maintaining production-quality dashboard. * Implemented Splunk Enterprise security in the environment for Security Operations. * Created Regular Expressions for **Field Extractions** and Field Transformations in Splunk. * Troubleshooting and resolve the **Splunk Performance**, Log Monitoring Issues; Roles, Mapping, Dashboard creation etc. * Worked on **Nagios i**ntegration with Splunk for Operations team to monitor the system metrics. * And, integrated JIRA with Splunk for ALM team to alert and submit a ticket for various issues in the application development phase.   **Environment:** Splunk Enterprise 6.4, Splunk ITSI 2.4, Splunk ES 4.0, RHEL 6, Windows Server’ 2008 R2 Enterprise and Citrix Receiver 4.5.  **Sr. Splunk Developer Dec 2015 – Mar 2016**  **Inovalon, Bowie, MD**  **Roles & Responsibilities:**   * Design, support and maintain the **Splunk infrastructure** on Windows, Linux and UNIX environments. * Installation **of Splunk Enterprise, Splunk forwarded, Splunk Indexer**, Apps in multiple servers (Windows and Linux) with automation. * Install and maintain the **Splunk adds-on** including the **DB** Connect 1, Active Directory LDAP for work with directory and SQL database. * Configure the adds-on app **SSO Integration** for user authentication and Single Sign-on in Splunk Web. * Configure and Install Splunk Enterprise, Agent, and Apache Server for user and role authentication and SSO. * Manage **Splunk configuration** files like inputs, props, transforms, and lookups. * Upgrading the **Splunk Enterprise to 6.2.**3 and security patching. * Deploy, configure and maintain **Splunk** **forwarder** in different platforms. * Creating Reports, **Pivots**, **alerts**, advance Splunk search and **Visualization** in Splunk enterprise. * Monitor and troubleshoot the applications using tools like **ITCAM**, **Dynatrace**, **Splunk**, **Wily**.   **Environment:** Windows Server 2012/2008/2003R2, Linux and Unix Servers, Splunk, SQL Server 2008, SAN, WLAN, Service Now, Tivoli.  **Splunk Power User/Developer Sept 2014- Dec 2015**  **Home Depot, Atlanta, GA**  **Roles & Responsibilities**:   * Install, configure and administer **Splunk** **Enterprise Server 6.0.4** and **Splunk Forwarder 4.x.x/5.x.x/6.x.x** on Red hat Linux and Windows severs. * Setup Splunk Forwarders for new application tiers introduced into environment and existing applications. * Work closely with Application Teams to create new **Splunk dashboards** for Operation teams. * Troubleshooting and resolve the Splunk – performance, log monitoring issues; role mapping, dashboard creation etc. * Created Splunk app for Enterprise Security to identify and address emerging security threats using continuous monitoring, alerting and analytics. * Created **Regular Expressions** for Field Extractions and Field Transformations in Splunk. * Anonymize the **PII** (Personally Identifiable Information) data in Splunk. Masked sensitive information such SSN numbers, addresses when showing results in Splunk. * Configure Splunk for all the mission critical applications and using Splunk effectively for Application troubleshooting and monitoring post go lives * Supported **8+ Splunk search Heads, 50 + Indexers, 3200 + forwarders**. * Created **Dashboards and Reports** to show Login count of each application, to show which app resources being accessed more, Number of failed logins, statistics on High hitting applications. * 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 * Configured Splunk forwarder to send unnecessary log events to “Null Queue” using props and transforms configurations to reduce license costs. * Developing a custom application in Splunk * Fetching the data from databases using "**DB Connect Application**" * Extensively involved in troubleshooting the issues and document the problem resolutions for future references and Attended Change management meetings for approval for the applications which are supposed to go live and provided the MOM of CM meetings to the team. * Experienced in attending the bridge calls for production issues and non-prod issues and involved application teams or database teams or networking teams to resolve the issues and involved in Root cause analysis for the issues encountered. Also provided 24/7 on call support for all the production applications. * Involved in developing complex scripts to **automate batch jobs**. * Developed a POC on usage of Puppet Configuration Management tool.   **Environment:** Splunk Enterprise Server 4.x.x/5.x.x/6.x.x, Universal Splunk Forwarder 4.x.x/5.x.x/6.x.x, RedHat Linux, IBM HTTP Web Server 6.1/7/8, Oracle, HACMP 5.4, HTML, Java Script, XML, Wily Introscope 9.x, IIS 7, Windows 2003, Windows 2008 R2, Python (Jython), Regular Expressions.  **DevOps Engineer Apr 2012 – Sept 2014**  **ELIC INC, Hyderabad, India**  **Role & Responsibilities:**   * Responsible for Developing a user-friendly DevOps environment - **Build, Test & Deploy on cloud**. * Installing, configuring and administering Jenkins **Continuous Integration (CI)** tool on Linux machines along with adding/updating plugins such as **GIT, Maven, SonarQube** etc. * Performing **CI**/CD using **JENKINS**, for faster code deploying using **GIT**. * Developing the web-page for user to build/test/deploy with limited entry to build the image. * Participated in configuring and monitoring distributed and multiple platform servers using Puppet. Experience in writing Puppet manifests to automate configuration of a broad range of services. * Analyze and resolve conflicts related to merging of source code for GIT. * Involved in configuring **Nagios** monitoring tool for monitoring the server/app status, disk space issues, and log parsing. * Perform S3 bucket creation, configured the storage on S3 bucket policies and the IAM role-based policies * Developed **Shell** and **Yaml** Scripts for automation purpose. * Planed, deployed, monitored, and maintained Amazon **AWS cloud infrastructure** consisting of multiple EC2 nodes and VMWare Vm's as required in the environment. * Automating developer, tester and DevOps engineer role in setting up environment to reduce cost and resource utilization via virtual environment. * Deployment and management through AWS cloud formation on EC2 instances and maintaining Amazon S3 storage. * Part of the team Installing and using **chef server** Enterprise on premise/workstation/bootstrapped the nodes using knife and automated by testing chef recipes, cookbooks with test-kitchen/chef spec. * Implementing a Continuous Delivery framework using Jenkins & Maven in Linux environment. * Performed routine maintenance checks across Linux servers for running jobs/processes. * Completed a RHEL install on a utility/demo server for use as a testing environment.   **Environment:** Jenkins, Puppet, Chef, Ansible, GitHub, Python, CentOS, RedHat, Ubuntu, Docker, Sonar-Qube  **Certifications:**   * Splunk User * AWS SysOps Admin |  |