**Sathish Kumar Reddy Gaddam**

[**sathish.splunk1@gmail.com**](mailto:sathish.splunk1@gmail.com)

**(903)-326-9996**

**PROFESSIONAL SUMMARY**

* **Over 5 years** of experience in configuring, **implementing and supporting Splunk Server Infrastructure** across Windows, UNIX and Linux. Experience with a variety of **operating systems protocols and tools**, depending on the type of platform or application to be administered.
* Experienced in installing, configuring and administer **Splunk Enterprise Server** and **SplunkUniversal Forwarder** in large distributed environment comprising Windows, Redhat, Solaris, AIX with exposure to various Splunk Apps to monitor Splunk deployments.
* Architecture 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.
* Experience in analyzing big data and reporting it to the leadership and technology teams to improve the processes.
* Expert in analyzing data, correlating trends, building reports and report writing.
* **Upgrade and Optimize Splunk** setup with new discharges, setup Splunk Forwarders for new application tiers introduced into environment.
* Setup **Splunk Forwarders** for new application levels brought into environment.
* Expertise in Actuate Reporting, development, deployment, management and performance tuning of Actuate reports.
* Developed **RESTful** web application layer that brokered search requests to the back-end via

**JSON** and **XML**

* Support design and configuration of CI/CD using **Jenkins** at the enterprise level.
* Experience in using Chef and **Jenkins** to automate deployments across multiple servers
* Implemented and created LDAP authentication to the **ITSI** environment.
* Created services and added to the top-level services and created **glass tables** views to make the application teams to understand the architectural view of environment
* Worked on large datasets to generate insights by using **Splunk**.
* **Develop custom app configurations** (deployment-apps) within SPLUNK to parse, index multiple types of log format across all application environments.
* Extensive experience in deploying, configuring and administering **Splunk clusters**.
* Have Knowledge in various search commands like stats, chart, time chart, transaction, strptime, strftime,eval, where, xyseries, table etc.and difference between event stats and stats.
* DevelopedSplunk infrastructure and related solutions as per automation toolsets.
* Experience in **Operational Intelligence** using Splunk.
* Scripting and development skills (Perl, Python, Java) with strong knowledge of **regular expressions**.
* Used techniques to optimize searches for better performance, Search time vs Index time field extraction. And understanding of configuration files, precedence and working.
* Experience in **Shell scripting** and extensively used **Regular expressions** in search string and data anonymization.
* Maintenance of Splunk Environment with **multiple Indexers**.
* 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.
* Highly motivated and adaptive with an ability to grasp things quickly and possesses excellent interpersonal, leadership, technical and communication skills.
* Excellent communication, analytical and interpersonal skills and ability to learn new concepts and supported 24/7 on call in production and development environment.

**PROFESSIONAL QUALIFICATION**

* Masters in Computer & Information Sciences, Southern Arkansas University, Magnolia, 2015
* Bachelors in Electronics & Communication Engineering, Jawaharlal Nehru Technological University Hyderabad, 2012

**TECHNICAL SKILLS**

|  |  |
| --- | --- |
| **Log Analysis Tool** | Splunk Enterprise Server 4.x.x/5.x.x/6.x.x, Splunk Universal Forwarder 4.xx/5.xx/6.xx |
| **Operating Systems** | RHL Linux, Unix, Windows, VMWare, Ubuntu |
| **Scripting** | Python, Shell, HTML 5, CSS3, JQuery, Javascript |
| **Databases**  **Networking** | MySQL, MS SQL Server, IBM DB2, Teradata  TCP/IP Protocols, Socket Programming, DNS. |
|  |  |

**PROFESSIONAL EXPERIENCE**

**American Express, Phoenix AZ Apr ‘16 - till date**

**Splunk Administrator and Developer**

American Express is a financial services company based in New York which offers charge cards and other forms of credit to individuals and companies. Implemented Splunk to monitor compliance issues proactively caused due to the technology defects that impact the customer transactional data. Monitoring and capacity planning of the organizational infrastructure enabling a smooth business and enabling scope for more proactive measures than reactive. The solution also provides better insights from the data; thus, enhancing the application owners to gain operational visibility to troubleshoot issues seamlessly. The ingested data include transactional data, Database logs, Teradata logs, various security logs and much more. The ingestion is done using universal forwarders and using syslogs for better optimization.

**Responsibilities:**

* Ingesting **structured data** into Splunk receiving from different application teams.
* Installing and configuring Splunk Enterprise Server 6.0.4 and Splunk Forwarder 4.x.x/5.x.x/6.x.x on Redhat Linux and Windows severs.
* Developing **python scripts** for continuous flow of data and alerting the team when any data related issues occur.
* Setting up of splunk**dashboards** for continuous monitoring for production support.
* Creating **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, AMEX card numbers when showing results in Splunk.
* Implemented **kvstore** to reduce the load and improve the performance of searches.
* Setting up Splunk multisite clusters and support existing infrastructure by adding new data sources/forwarders.
* Involved in **migration** of entire project from their old infrastructure to new infrastructure without loss of any data.
* Creating Splunk apps for **Enterprise Security** to identify and address emerging security threats using continuous monitoring, alerting and analytics.
* Developing of graphical visualizations, Splunk searches, custom platform related features and system integration.
* Developed dashboards to monitor the user behavior for the Information Risk Management.
* Installing and configuring Splunk forwarder in Solaris platform.
* Created dashboards using Solaris 11 app in Splunkbase for exploring Solaris features not visible in the default App for \*nix
* Optimized **Splunk** for peak performance by splitting **Splunk indexing** and search activities across different machines.
* Written and developed scripts for automating tasks using **Jenkins** and UNIX shell scripting.
* Created a set of base searches in **ITSI** and tested in different scenarios.
* Added aggregate and per entity thresholds based on applications inputs.
* Added URL monitor to the glass table.
* Created Search Commands to retrieve multiline log events in the form Single transaction giving Start Line and End Line as inputs.
* Guarantee high accessibility & execution trough flat scaling and burden adjusted segments.
* Prepared, arranged and tested **Splunk search strings** and operational strings. Created and configured management reports and dashboards.
* Created **EVAL** Functions where necessary to create new field during search run time.
* Provide inputs for identifying best fit architectural solutions - deployment for Splunk project.
* **Splunk Engineer/Dashboard Developer** responsible for the end-to-end event monitoring infrastructure of business-aligned applications.
* Experience in setting up dashboards for senior management and production support- required to use **SPLUNK**.
* Maintained and managed assigned systems, **Splunk** related issues and administrators.

**Environment:**Splunk Enterprise Server 6.3.x, Universal Splunk Forwarder 6.3.x, Shell, Python Scripting, Splunk DB connect

**Nationwide Insurance, Columbus, OH Jun ‘15 – Mar ‘16**

**Splunk Administrator and Developer**

Nationwide, a Fortune 100 company is one of the largest insurance and financial services companies in the world, focusing on domestic property and casualty insurance, life insurance and retirement savings, asset management, and strategic investments.

**Responsibilities:**

* Provide regular support guidance to **Splunk** project teams on complex solution and issue resolution.
* Troubleshooting issues and setting up Infra related **proactive alerts**.
* Gathering and **analyze requirements** and implementation planning and coordinating the same with the team.
* Train various application on Splunk SPL which enables users to develop their own work flow dashboards.
* Develop **dashboards** for investigation into the incidents that happen in the organization.
* Correlating the failures and provide better insights into the data enabling the work flow.
* Build instant reports upon ad-hoc requests.
* Integrated Splunk with **LDAP** to enable users to use same as their organizational credentials for Splunk.
* Manage and configure index settings and Create event type definitions
* Created various **roles** so that the users have access to their data only and limiting user functionality for security
* As in production environment, I was involved in resolving various complex production issues by analyzing data from various monitoring tools from Sys logs and application logs. This involves working with various teams’ real time on a conference call.
* Written many Python and Shell Scripts, created many automation and applied into operations successfully.
* Created Dashboards, report, scheduled searches and alerts.
* Integrated **ServiceNow** with Splunk to generate the Incidents from Splunk.
* Worked on DB Connect configuration for Oracle, MySQL and MSSQL.
* Extracted complex Fields from different types of Log files using **Regular Expressions**.
* Created many of the **proof-of-concept dashboards** for IT operations, and service owners which are used to monitor application and server health.
* Knowledge about **Splunkarchitecture** and **various components** (indexer, forwarder, search head, deployment server), Heavy and Universal forwarder, License model.
* Involved in standardizing **Splunk forwarder deployment**, configuration and maintenance across UNIX and Windows platforms.
* **Parsing**, Indexing, searching concepts Hot, Warm, Cold, Frozen bucketing.
* Field Extraction, Using Ifx, **Rex Command** and **Regex** in configuration files.
* 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.
* Use techniques to optimize searches for better performance, Search time vs Index time field extraction. And understanding of configuration files, precedence and working.
* Create dashboard from search, scheduled searches online search vs scheduled search in a dashboard.

**Environment:**Splunk Enterprise Server 5.1.2, Splunk Forwarder 5.1, 5.4, Linux, UNIX, Splunk Knowledge Objects.

**Domino’s - Ann Arbor, MI Jan ‘14 – May ’15**

**Splunk Administrator and Developer**

Domino's Pizza, Inc. is a pizza retail chain. The Company operates pizza stores at 11,900 locations in over 80 markets. The Company operates in three business segments: domestic stores, international franchise and supply chain. The Company’s Domestic Stores segment consists primarily of its franchise operations, through which the Company operates network of 4,722 franchised stores located in the United States. Implemented Splunk to analyze the patterns of the customers and all the data generated from various web and server logs to analyze the behavioral pattern of the customers.

**Responsibilities:**

* Prepared, arranged and tested **Splunk** search strings and operational strings.
* Prepared, arranged and tested**Splunk** search strings and operational strings.
* Using **SPL** created Visualizations to get the value out of data
* On call for support bi weekly and resolved issues based on the priority.
* Responsible to check the **Splunk logs** for web server to avoid server time down during production.
* Troubleshooting **log feeds**, extraction and feed times.
* Assisted internal users of **Splunk** in designing and maintaining production-quality dashboard.
* Used Data meter to analyze the transaction data for the client.
* Involved in installing and using Splunk app for **Linux** and **Unix**.
* Created alerts on the requests from managers for certain tasks
* Experience in using **Splunk** with Data power to provide debugging and monitoring capabilities.
* Set up Splunk to capture and analyze data from various layers **Load Balancers**, Web servers and application servers.
* Set up alerts when the response time or traffic falls above or below expected limit.
* Installation and Maintenance of **Splunk** Universal Forwarders, Solving Forwarder Issues, **Deployment Server** Classes and Apps through Deployment Server.
* Props file management for event breaking and time stamp matching.
* **Implemented Forwarders** (Universal and Heavy) with Load Balancing, **Splunk** Forwarder Management
* Managed the **Splunk** Enterprise Deployment
* Had installed Splunk on remote graphic work station and by using forwarders monitored and reported data by using Splunk on another work station.
* Installation and Maintenance of Splunk Universal Forwarders, **Solving Forwarder Issues**, Deployment Server Classes and Apps through Deployment Server.

**Environment:**Splunk Enterprise, Universal Splunk forwarder, Regular expressions, Windows, UNIX, UNIX shell scripting, XML, Splunk DB connect

**Saggezza, Bangalore, India**                            **Dec ’11 – Dec ’13**

**SQL Server Developer**

Saggezza is a global solutions provider. Working in partnership with you at every step, we’ll understand your business and where you want to be, then build the technology solutions that will get you there, faster.

**Responsibilities:**

* Involved in installation and configuration of **SQL server 2000** on servers.
* Defined various facts and dimensions in the data mart including Fact Less Facts and designed the **Data Mart defining Entities**, **Attributes** and relationships between them.
* **Implemented triggers** and stored procedures and enforced business rules via checks and constraints.
* Fine-tuned Stored Procedures, using **Execution Plan** in T-SQL for better performance.
* Troubleshoot and minimize production down issues.
* Extensively used XML documents to pass multiple parameters for stored procedures to read and write database table.
* Involved in optimize stored procedures and queries for faster retrieval and **Serverefficiency**.
* Designed new job process, new database maintenance plans, **DTS programs** and did Performance tuning of the existing processes.
* Created, Scheduled maintenances and backup procedures to the database as a disaster recovery method.
* Monitored failed and long running **MS SQL Server** jobs.
* Monitored, tuned, and analyzed database performance and allocate server resources to achieve optimum database performance.

**Environment**: SQL Server 2000, T-SQL, DTS, MS Visual Studio 2005, Windows 2000 Server, .Net Programming.