Gautam Gajra

Senior Splunk Engineer | Passionate about Infra Stability, Cloud Automation & Observability | Opsview | Nagios | Splunk
Email: ggajra22@gmail.com | Phone: 7021038516 | LinkedIn: www.linkedin.com/in/gautam-gajra/

Professional Summary

Accomplished and results-driven Senior Splunk Engineer with over 3 years of experience in designing, automating, and maintaining resilient cloud and on-premises infrastructure with hands-on experience across Splunk Enterprise 8.x/9.x, IT Service Intelligence (ITSI), and DB Connect. Administered and upgraded 6+ complex clustered environments (Search Head Clusters and Indexer Clusters) including Deployer, Cluster Master, and Forwarders. Deep expertise building data models, correlation searches, NEAP policies, dashboards (Classic + Dashboard Studio), alerting, and advanced SPL with regex-driven field extractions and lookups. Proven background integrating Splunk with enterprise systems and clouds (AWS, Azure, SCOM, SNMP, Zabbix, Opsview) and optimizing platforms for capacity, reliability, and performance. Trusted partner to operations and engineering teams for RCA, monitoring, and reporting.

Core Competencies

- **Splunk Enterprise**: Splunk Administration, Data Onboarding & Integration, Splunk Query Language (SPL) , Dashboards & Reporting, Alerting & Monitoring, Forwarder Management, Indexing & Data Parsing, User & Role Management, Data Hygiene & Filtering,
- **Splunk ITSI**: Services, KPIs,, Correlation Searches, Knowledge Objects- Data & Onboarding: Heavy Forwarders (Linux/Windows), HEC, TA/Add-ons, SNMP, SCOM, Zabbix, Opsview, AWS, Azure
- **Visualization & Reporting**: Classic + Dashboard Studio, drilldowns, tokens, alerting, availability and performance reporting
- **Scale & Reliability**: Upgrades, capacity planning, index/lifecycle management, performance tuning, monitoring, optimization
- **Integrations**: Splunk DB Connect (real-time DB integrations), SCOM Add-on, AWS/Azure cloud data, custom solutions
- **Operations & RCA**: Production incident analysis, post-production performance troubleshooting, observability for infra/apps
- **Scripting & Automation:** Shell, Perl, Python (Basic), PowerShell, RegEx, Java (Basic), REST APIs

Professional Experience

Capgemini Technology Service Ltd – (July 2022 – Present)
Business Unit – Cognitive & Robotics

- **Implement and manage Splunk ITSI**: define services, KPIs, correlation searches build and maintain knowledge objects to support operations workflows.
- Design and maintain Data Models to accelerate searches and reporting; standardize naming, tags, and data hygiene to improve query performance and consistency.
- Onboard data from diverse sources (logs, HTTP Event Collector, add-ons/TAs) and enterprise tools (SNMP, SCOM) with robust sourcetypes, timestamps, line-breaking, and index retention policies.
- Integrate Splunk with cloud platforms (AWS, Azure) using add-ons and custom ingestion frameworks; implement role-based access and index strategies for multi-tenant use.
- Build modern dashboards (Classic + Dashboard Studio) with drilldowns, tokens, and visualizations; deliver standardized availability and performance reports for stakeholders.
- Develop advanced SPL with regex-based field extractions and transforms; implement efficient lookups (CSV/KV) to enrich events and reduce search-time cost.

- Establish alerting and monitoring for infrastructure, applications, and KPIs; fine-tune thresholds and routing to reduce noise and improve MTTA/MTTR.
- Onboard data from diverse sources (logs, HTTP Event Collector, add-ons/TAs) and enterprise tools (SNMP, SCOM) with robust sourcetypes, timestamps, line-breaking, and index retention policies.

Recent Integrations & Projects

- SCOM Integration: Deployed and tuned Splunk Add-on for Microsoft SCOM; normalized alerts/events for triage dashboards and ITSI correlation.
- SNMP Ingestion: Implemented SNMP-based collection for network and infra telemetry; standardized MIB mappings and source type conventions.
- Cloud Ingestion (AWS, Azure): Built custom ingestion patterns for cloud logs/metrics; established index, role, and lifecycle policies aligned to cloud accounts/subscriptions.
- Zabbix & Opsview: Integrated monitoring outputs to Splunk for unified observability and reporting; mapped severities to ITSI notable events for consolidated NOC workflows..

Education & Certifications

- **Bachelor of Engineering in Computer Engineering** – Shivajirao Jondhale College of Engineering (June 2019 - 2022)
  Published IEEE project paper on Blockchain-Based Electronic Voting System
- **Diploma in Information Technology** – Vidyalankar Polytechnic
- **Certifications**:
  - **AWS Certified Cloud Practitioner**
  - **Power BI Practioner Certification** – Capgemini OCEAN
  - **Agile Software Development** – Coursera
  - **MongoDB SI Associate Certification**
  - Splunk Power User Certification
  - **In Progress:** Actively pursuing, Azure, and GCP certifications to deepen multi-cloud expertise.