Gautam Gajra

Senior System Analyst | Spearheaded the automation of routine infrastructure tasks using Opsview and Nagios, saving the team 60 hours per week and enabling a 20% faster response time to critical alerts| Opsview | Nagios | Splunk ITSI | Splunk Admin

Email: ggajra22@gmail.com | Phone: 7021038516 | LinkedIn: www.linkedin.com/in/gautam-gajra/

Splunk Engineer with 3 years designing and scaling multi-region, multi-tenant Splunk Enterprise 8.x/9.x platforms. Operated NA/EU/UK estates with 4+ Search Heads per region (12+ SH total), supporting 80+ global clients. Specializes in Universal Forwarders (UF), Heavy Forwarders (HF), Indexers (IDX), Search Heads (SH) and Search Head Clusters (SHC), props/transforms, Splunk IT Service Intelligence (ITSI) with Notable Event Aggregation Policies (NEAP), accelerated data models, and dashboard/search performance. Integrates SCOM, SNMP, Zabbix, Opsview, and AWS/Azure to deliver stable upgrades, reliable onboarding, and actionable monitoring.

Professional Experience

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

- Operated multi-region Splunk Enterprise (NA, EU, UK) with 12+ Search Heads and clustered Indexers; maintained predictable search performance and clean package governance across regions
- Supported 80+ global clients; standardized per-customer ingestion using 3-node UF clusters (about 240 UFs total) and Heavy Forwarders where required across Linux/Windows fleets
- Led 3 region-wide upgrades (8.x → 9.x) across Search Heads, Indexers, Deployer, Cluster Manager, and forwarders; authored runbooks and pre/post validations to reduce change risk
- Built ITSI services/KPIs and 10+ correlation searches (NEAP); reduced duplicate incidents by about 25% and improved NOC/SRE signal quality
- Engineered 12+ accelerated data models enabling tstats-based analytics; stabilized key dashboard loads to under 5 seconds (typically 3–5 seconds) via SPL and data model tuning
- Delivered 40+ dashboards (20+ Dashboard Studio, 20+ Classic) with drilldowns/tokens; standardized availability/performance reporting across multiple services
- Automated forwarder onboarding and app lifecycle with Deployment Server classes and versioning; reduced configuration drift by 30–40% and improved rollout consistency
- Implemented regex-based extractions/transforms and optimized CSV/KV lookups to expand enrichment while lowering search-time overhead
- Integrated telemetry from SCOM, SNMP, Zabbix, and Opsview; unified alert routing into ITSI correlation workflows for streamlined triage
- Enabled AWS/Azure ingestion via add-ons and custom collectors; standardized indexes, RBAC, and retention tiers per account/subscription (30/90/365 days)
- Onboarded 6+ RDBMS inputs using Splunk DB Connect; scheduled queries, secured connections, and validated end-to-end data completeness
- Tuned platform health/capacity (knowledge bundle replication, search affinity, scheduler concurrency) as tenant data volumes scaled
- Documented deployer bundle patterns, app namespaces, and upgrade runbooks; accelerated peer onboarding and handovers

Outcomes

- Maintained a 3-region (NA/EU/UK), 80+ client footprint with consistent onboarding patterns and governance.
- Established repeatable upgrade/runbook practices across regions to minimize risk during 8.x → 9.x transitions.
- Improved dashboard predictability and report turnaround through data model acceleration and SPL tuning.

Education

- **Bachelor of Engineering in Computer Engineering** – Shivajirao Jondhale College of Engineering (June 2019 – 2022)

Certifications

- AWS Cloud Practioner , Power-BI, Splunk Power User Certification

Technical Skills

- **Monitoring & Observability**: Opsview, Splunk (ITSI), Nagios
- **Cloud & Virtualization**: Amazon Web Services (AWS), VMware (vSphere/ESXi), Linux (RHEL), Windows Server
- **Scripting & Automation:** Shell, Perl, Python (Basic), PowerShell, RegEx, Java (Basic)
- **Infrastructure as Code (IaC)**: Terraform (Basic)
- **Networking:** SNMP, TCP/IP, DNS, Firewalls, Routers, Switches (BGP/OSPF Monitoring)
- **Databases:** Oracle, MySQL,
- **ITSM & Collaboration:** ServiceNow, IPaaS