GAUTAM GAJRA

Senior Observability Engineer — Cloud Automation & Infrastructure Stability
ggajra22@gmail.com | 7021038516 | linkedin.com/in/gautamgajra

PROFESSIONAL SUMMARY

Results-driven Senior Observability Engineer with 3+ years designing, automating, and maintaining resilient cloud and on-premises infrastructure. Expert in Splunk Enterprise 8. x/9.x, ITSI, DB Connect with proven track record administering 6+ clustered environments (SHC, Indexer Clusters). Deep expertise in SPL, data modeling, correlation searches, regex-driven field extractions, and integrations with AWS, Azure, Opsview, SNMP, Datadog. Trusted partner for RCA, monitoring, capacity planning, and performance optimization.

CORE COMPETENCIES

Splunk & Observability: Enterprise Administration, ITSI (Services, KPIs, Correlation Searches), SPL, Dashboard Studio, Alerting, Data Models, Knowledge Objects, Index Lifecycle, Capacity Planning, Performance Tuning, Opsview, Nagios, Datadog, New Relic, Prometheus, Grafana, AppDynamics, Dynatrace, QRadar, SolarWinds, Zabbix
Data Integration: Heavy/Universal Forwarders, HEC, TA/Add-ons, SNMP, SCOM, DB Connect, AWS/Azure Cloud Data, REST APIs
Cloud & Infrastructure: AWS (Certified Cloud Practitioner), Azure, Multi-cloud Architectures, Infrastructure Monitoring, SIEM, SOC Analysis
Scripting & Automation: Shell, Python, Perl, PowerShell, RegEx, Java, REST APIs
Operations: RCA, Incident Response, Post-Production Analysis, MTTA/MTTR Optimization, Data Hygiene, User/Role Management

PROFESSIONAL EXPERIENCE

Capgemini Technology Services Ltd *July 2022 – Present*
Senior Observability Engineer – Cognitive & Robotics Business Unit

- Architected and administered 6+ Splunk clustered environments (SHC, Indexer Clusters, Deployer, Cluster Master, Forwarders) serving enterprise-scale observability for global clients
- Implemented Splunk ITSI services, KPIs, correlation searches, and knowledge objects; reduced MTTR by 30% through automated alerting workflows and enriched event correlation
- Designed and maintained data models, accelerated searches, and standardized naming conventions; improved query performance by 40% through optimized SPL and field extractions
- Onboarded multi-source data (logs, HEC, SNMP, SCOM, AWS, Azure) with custom sourcetypes, timestamp extraction, line-breaking, and index retention policies aligned to compliance requirements
- Built advanced dashboards and reports in Dashboard Studio and Classic; delivered availability/performance reports to C-level stakeholders and operational teams
- Developed regex-based field extractions, transforms, and CSV lookups to enrich events and reduce search-time overhead; established data hygiene policies reducing index bloat by 25%
- Integrated Splunk with Microsoft SCOM (normalized alerts for ITSI correlation), SNMP (network/infra telemetry with MIB mappings), Opsview (unified NOC workflows), and cloud platforms (AWS/Azure add-ons)
- Led capacity planning, platform upgrades (8.x to 9.x), performance tuning, and licensing optimization; maintained 99.9% platform uptime through proactive monitoring
- Partnered with engineering/operations teams for real-time incident analysis, post-production RCA, and root-cause mitigation; documented runbooks and best practices for knowledge transfer
- Authored and published IEEE paper on *Blockchain-Based Electronic Voting System* demonstrating research capabilities and technical writing proficiency

KEY PROJECTS & INTEGRATIONS

SCOM Integration: Deployed Splunk Add-on for Microsoft SCOM; normalized alerts/events for ITSI correlation reducing alert noise by 35%
SNMP Ingestion: Implemented SNMP-based collection for network/infra telemetry; standardized MIB mappings improving device visibility
Multi-Cloud Ingestion (AWS, Azure): Architected data ingestion pipelines for cloud logs/metrics; established index, role, lifecycle policies aligned to cloud accounts/subscriptions
Opsview Integration: Integrated monitoring outputs to Splunk for unified observability; mapped severities to ITSI notable events consolidating NOC workflows

EDUCATION

Bachelor of Engineering in Computer Engineering *June 2019 – 2022*
Shivajirao Jondhale College of Engineering — Published IEEE project paper on Blockchain-Based Electronic Voting System
Diploma in Information Technology
Vidyalankar Polytechnic

CERTIFICATIONS

AWS Certified Cloud Practitioner | Splunk Power User | MongoDB SI Associate | Power BI Practitioner (Capgemini OCEAN) | Agile Software Development (Coursera) | *In Progress: Azure & GCP Certifications*

TECHNICAL SKILLS

Monitoring & Observability: Splunk Enterprise, Splunk ITSI, Opsview, Nagios, Datadog, New Relic, Prometheus, Grafana, AppDynamics, Dynatrace, QRadar, SolarWinds, Zabbix
SIEM & Security: SOC Analysis, Correlation Searches, Alerting, Incident Response, Compliance Reporting
Splunk Architecture: Search Head Clusters, Indexer Clusters, Deployer, Cluster Master, Deployment Server, License Master, Universal/Heavy Forwarders, HEC
Data & Integration: DB Connect, SNMP, SCOM, Data Models, Knowledge Objects, Lookups, Field Extractions, Sourcetypes
Cloud Platforms: AWS, Azure, Multi-cloud Architectures
Scripting: Shell, Python, Perl, PowerShell, RegEx, Java, REST APIs
Databases: MongoDB, SQL
Methodologies: Agile, DevOps, CI/CD, Infrastructure as Code