SOWMYA V

Contact: +91 8220729978 **E-mail:** sowmyasowmi30@gmail.com

Splunk Admin

*Seeking challenging assignments in the domain of **Splunk administration** acrossthe IT industry*

ROLE

- **Splunk Admin and Developer PROFILE**

- Qualified B. E Computer Science & Engineering from SNS College of Technology Coimbatore currently working with Cognizant Technology Solutions India Pvt. Ltd. as Senior Infra Developer.
- **Splunk Admin and Power User Certified.**
- **6 years 1 month working experience with Splunk Enterprise & Splunk Cloud**
- **Design, Deploy, and Support enterprise Splunk logging application.**
- Proficient with Splunk architecture and various components (indexer, forwarder, search head, deployment server), Heavy and Universal forwarder.
- Expert with various search commands like stats, chart, timechart, lookup, strptime, strftime, eval, where, join, table, etc.
- **Knowledge of Splunk Infrastructure i.e. deployment, inputs, apps, indexes, monitoring.**
- Experience in creating lookups, field extractor, Tags and event types, Alerts and Scheduled reports, Macros with Splunk
- Experience in creating different visualizations using Bar, Line and Pie chart, Bubble chart, Heat maps etc.
- **Parsing, Indexing, Searching concepts Hot, Warm, Cold, Frozen bucketing.**
- **Hand-on experience in creation of dashboard and visualization with Splunk.**
- **Worked on Agile way of working**
- Hands on experience in Gitlab CI/CD pipeline, Repository, Branches

Technical Skills:

Operating System	Windows 7/10, Linux
Server	Windows Server 2003,2008R2,2012, Linux RHEL, Ubuntu
Splunk Enterprise	7.x, 8.x, 9.x
Tools	Putty, Service Now, WinSCP, Gitlab, Ansible, AWS, JIRA

Certifications:

Certification Name	**Version**	**License ID**
Splunk Certified User	9.x	Cert-275146
Splunk Certified Power User	9.x	Cert-274925
Splunk Enterprise practical	9.x	
Splunk Certified Admin	9.x	Cert-276561

PROFESSIONAL EXPERIENCE

Cognizant Technology Solutions India Pvt Ltd

Senior Infra Developer

July 2022 – Present

Client: Loblaw

Duration: 2 year 1 month

Customer	Loblaw
Skills	Splunk Administrator
Role	Splunk Admin & Developer
Tools	Splunk Enterprise 8.x, 9.x
Description	Client. Splunk Servers are hosted on GCP, Azure & On-prem . Search heads on SPLUNK Cloud(SAAS), On-prem Heavy forwarder Splunk servers are running on 9.x version. Universal forwarders running on 9.x 8.x. Syslog are onboarded from various components.
Contribution	• Maintaining the splunk cloud environment. • Worked on REST endpoints data ingestion using Splunk Cisco TA & App for DNA Center • Incident handling for environment health checks • Service request handling incase of access request, dashboard creation, alert creation, index creation. • Upgrading splunk agent & splunk servers version to latest(n-1) • Onboarding application logs for various teams. • Worked on REST endpoints data ingestion using Splunk Cisco Catalyst UCS • Documenting the procedure followed during integration • Vulnerability remediation on splunk servers • Scripting for Splunk UF installation as part of windows golden image & auto deployment of post installation packages • Following the Change management procedure to implement activity on production • Troublshooting the log ingestion from various tools • Field extraction for unorganized data format. • Applying syslog configuraions on servers to onboard syslog into splunk cloud • WEB Certificate Renewal • Splunk with SD-WAN Integartion • Worked on redirecting logs based on Region oriented Deployment servers.

Senior Infra Developer

October 2021 – June 2022

Projects Accomplished:

Client: Kohls

Duration: 9 months

Customer	Kohls
Skills	Splunk Administrator
Role	Splunk Admin & Developer
Tools	Splunk Enterprise 8.x, 9.x
Description	Client has various Data Center. Each Data Center has Splunk environment with Indexers, Search Head, License master. Few Data Centers are hosted on GCP which is clustered. Splunk enterprise servers are running on 8.x version. Universal forwarders running on 9.x 8.x
Contribution	• Worked on REST endpoints data ingestion using SNOW TA. • Onboarding AWS logs & setup monitoring for it. • Creating complex dashboards & onboarding complex logs like mbeans JMX • Worked on setting up Clustered Environment & maintaining it. • Monitoring splunk infrastructure health & functioning on daily basis. • Installing & configuring Heavy forwarders. • Worked on design catalog item in service now for splunk related requests. • Extensively worked on onboarding ServiceNow data & vmware data. • Created various Dashboards, Operations Head Dashboards, and Prediction Dashboards. • Worked on Splunk DBConnect App from initial setup to creation of Complex queries SPL. • Worked with Splunk Machine Learning Toolkit and various prediction visualizations associated with it. • Supported in Upgrading splunk clustered Environment. • Installing & configuring Search heads , indexers & clustering. • Receiving promptly, handling, gathering requirements through remedy tickets and resolving it on time. • Data collection from various systems/servers, Forwarder Management, creating and managing Splunk apps. • Creating, maintain, support, repair, customizing System & Splunk applications, search queries and dashboards. • Working closely with Infrastructure, Application, Development and Business or project teams on Splunk. • Communicating and collaborating with customers, Splunk users.

HCL Technologies Pvt Ltd

Senior Analyst June 2018

– October 2021 Projects

Accomplished:

Client: NXP Semiconductors

Duration: 3 years 4 months

Customer	NXP Semiconductors
Skills	Splunk Administrator
Role	Splunk Admin and Developer
Tools	Splunk Enterprise 7.x, 8.x
Description	Customer already have Multi-site clustered Splunk Environment available. We have upgraded different Splunk Components from 7.3.2 to 8.0.3 Version. Upgradation of Splunk apps. Installation and setting up data from Splunk Universal forwarders, Indexers, Search Head, deployment server. Creation of reports and Alerts which are helpful in Infrastructure Monitoring.
Contribution	✞ Gathering environment information and check the compatibility of different components and maintain documentation. ✞ Analyse the risk in upgradation and provide proper communication to stakeholders. ✞ User change management process to upgrade the production Clustered environment. ✞ Upgrade apps and add-ons as per Splunk version compatibility Installation of new forwarders ✞ Monitoring the Splunk instances health and errors. Experience on Macros, Lookups, Views and Apps. ✞ Working experience on Creating Alerts, Saved Searches. ✞ Working with end-user monitoring teams and providing the dashboards for monitoring ✞ Hosted splunk application on AWS Kubernetes service & container services using terraform & AWS CLI. ✞ Creating custom Dashboards, Alerts and Reports. ✞ Experience in basic troubleshooting and debugging problems. ✞ Knowledge on configuration files (inputs.conf, outputs.conf, props.conf, transforms.conf, serverclass.conf, indexes.conf) ✞ Created EVAL Functions where necessary to create new field during search run time. ✞ Field Extraction, using rex command. ✞ Worked with administrators to ensure Splunk is actively and accurately running and monitoring on the current infrastructure implementation. Create interface between Splunk and Service now through Service now add on. ✞ Creating dashboards and reports through the data pulled from Service now. Worked on various apps and add-on like Splunk addon for ServiceNow, Splunk Add on for AWS, Splunk App for Infrastructure, Splunk add-on for JMX, Splunk add-on for metrics ✞ Worked on premium app such as Splunk ITSI ✞ Worked on setting up Splunk AWS firewall Security groups ✞ Basic knowledge on Ansible playbook ✞ Have worked on GITLAB Repositories and CI/CD pipeline, good knowledge of commits, merges and push-pull requests. Direct client

	exposure and handling client calls.

AWS ECS/EKS

- Created & pushed docker image to AWS ECR
- Hosted Splunk application in AWS ECS using task definition, service.
- Created EFS, Mount points & targets using json files in AWS ECS • Featured AWS EKS & host splunk application using terraform deploy.
- Knowledge about pricing & scaling of AWS ECS/EKS.
- Enabling of SSH in AWS instances
- Connected Splunk SH on AWS with indexers

SERVICENOW DEVELOPMENT

- Experience in creating servicenow catalogs for splunk requests
- Flow design creation in Servicenow
- Supported in automating the splunk access, index creation etc.. in Servicenow flow design
- Designing for servicenow flow & catalog of splunk requests

MISCELLANEOUS

- Experience with working on Windows and *NIX systems (vi, cat, chmod, etc.) and with tools like, putty,WinSCP, Windows RDP, etc.
- Have worked on GIT Repositories (for version control), good knowledge of commits, merges and push-pull requests.
- Good knowledge with working on AWS systems
- Worked on Ansible Automation also.

EDUCATIONAL CREDENTIALS

B. E (Computer Science & Engineering), 2018

SNS College of Technology, Coimbatore; 93.2%

12 th Standard, 2014

P.S.G.R Krishnammal Hr Sec School, Coimbatore; 87.3%

10 th Standard, 2012

P.S.G.R Krishnammal Hr Sec School, Coimbatore; 94.2%

Date of Birth: 30 May 1997

Languages known: English, Tamil

Permanent Address: LIG- I 3928/1543, Ganapathy Maa Nagar, Ganapathy, Coimbatore641006, Tamil Nadu, India