SHRUTI ANEKAR

Senior DevOps Engineer **Mumbai, India | +91-9664198706 | shruti.anekar@gmail.com | @shrutianekar**

PROFESSIONAL SUMMARY

- Hands-on DevOps Engineer with 4+ years of experience in DevOps, Cloud Computing, CI/CD, Automation, Cloud Server Administration, Architecture, Designing, Deployment, Configuration, Migration, Testing, Troubleshooting & Security.
- Looking for a challenging career where there is scope for Demonstration, thrive for Imagination & Passion is valued
- Terraform Expert. Proficient in Shell Scripting, Go, and Python, Lambda Functions for Automation.
- Developed and Designed APIs using Spring Boot framework, REST APIs, and Frontend with React.js.
- Developed Kubernetes Custom Resources (CRs) and Custom Resource Definitions (CRDs), implementing webhook functionality using Golang.
- Extensive hands-on experience with cloud infrastructure, spanning AWS, Azure, and Google Cloud, demonstrating a deep understanding of cloud best practices.

Education: Bachelor of Engineering in Information Technology, Ramrao Adik Institute of Technology, Mumbai University

SKILLS

Languages	: Go, Python, Bash
DevOps Tools	: Docker, Prow, Jenkins, Github Actions, Artifactory, X-ray, SonarQube, GitLab CI
Frameworks	: Helm, Kubernetes, Controllers & CRDs, Bazel, Ginkgo, Terratest, Gotest, Spring Boot, React, Ruby on Rails. For QA Automation - Robot & BDD
Cloud	: AWS, GCP, Azure,OpenShift
Infrastructure as Code	: Terraform, Ansible, CloudFormation, Chef
Version Control	: Git, Svn, GitLab, Code Commit
Observability Tools	: Prometheus, Grafana, Loki, Promtail, EFK,ELK, DataDog, Splunk, CloudWatch, StackDriver

PROJECT EXPERIENCE

Coupa Software: It is a leading provider of cloud-based spend management solutions. Their platform helps organizations effectively manage their procurement, expenses, invoices, and supplier relationships. With a focus on driving cost savings, improving compliance, and enhancing visibility into spending, Coupa Software empowers businesses to streamline their financial operations and make smarter purchasing decisions.Their solutions are trusted by companies of all sizes across various industries to optimize their spend and drive bottom-line results.

Role: Senior DevOps Engineer (Contractor)

Responsibilities:

- Spearheaded the migration of services from EC2 to CCP (Coupa Container Platform), ensuring seamless transition and minimal disruption to operations.
- Conducted upgrades of services on ECS (Elastic Container Service), enhancing system reliability and performance.
- Contributed significantly in the migration from monolithic to microservices architecture, facilitating greater scalability and agility in application development and deployment processes.
- Championed the migration to containers, resulting in significant performance improvements and cost optimization measures.
- Implemented robust monitoring solutions using ELK dashboards, Grafana, and New Relic, ensuring comprehensive observability across the infrastructure.
- Proficiently troubleshooted Kubernetes containers to identify and resolve root causes of issues, thereby enhancing system stability and performance.

- Provided continuous monitoring and observability support for over 1000 customers migrated onto CCP, ensuring optimal performance and reliability of services.

Key Achievements:

- Successfully migrated over 1000 customers onto CCP, achieving seamless transition and minimal disruption to services.
- Implemented monitoring and troubleshooting strategies that resulted in improved system stability and performance, contributing to enhanced customer satisfaction and retention.
- **Tech Stack: Kubernetes, Docker, Rundeck, Shell scripting, Linux, AWS, ELK, Grafana, Ruby on Rails**

Trilio for Kubernetes: It is a cloud native, application-centric data protection platform that was designed to support the scale, performance, and mobility requirements of Kubernetes container environments across any public or hybrid cloud environment. It offers backup and recovery of the entire application, including data, metadata and any other Kubernetes objects associated with the application so it is protected and able to be restored from any point in time.
Role: DevOps Engineer

Responsibilities:

- Implemented Prow CI/CD for automated builds and multiple CI jobs, covering tasks like linting, vulnerability scanning, test case execution, and Docker image scanning.
- Developed a Trilio-Prometheus Metrics exporter in GoLang to create custom app-related metrics and expose them on the /metrics endpoint for scraping by the Prometheus Stack, and crafted Grafana dashboards based on these custom metrics.
- Created “triliotest”, a GoLang-based e2e tool to automate Kubernetes platform setup as a pre-requisite across various deployment solutions, such as Kops, GKE, EKS, AKS, Rancher, D2iQ Konvoy, k3s, OpenShift, micro k8s and to perform complete e2e automated testing.
- Built “'trivybot”,' a Slack bot in python for periodic vulnerability scanning of images and filesystems using Trivy.
- Researched and created proof of concepts around multiple logging and monitoring tools to enhance observability for TrilioVault including Grafana Loki Promtail (PLG) stack, EFK, ELK, Sumologic, Graylog, Datadog, Stackdriver, Splunk, CloudWatch.
- Implemented automation for air-gapped installations of Trilio on Kubernetes environments, significantly improving deployment efficiency and ensuring seamless operation in environments with restricted or no internet access.
- Contributed to OLM operator's Backup & Restore functionality, involving API updates, webhooks, validation code for restoration, and end-to-end test case development in Go.
- Proficient in Git for source code management, with expertise in branch strategies to support parallel development, code stability, and release management.

- **Tech Stack: Go, Helm, Kubernetes, Docker, Prow, Shell scripting, Linux, GKE, OCP, Trivy**

Protegrity Database Gateway (PDG): It is a data security company that focuses on tokenization and data encryption. PDG is a product that is built on top of Starburst Data Enterprise, it is a Gateway that protects, unprotects data present in Postgres, MySQL, MS SQL, and other DBs using Trino as an underlying layer.
Role: Software Engineer

Responsibilities:

- Designed and Developed a highly scalable service built on top of Starburst data enterprise on Azure (Azure Synapse, Storage Accounts, AKS) which is used to protect and unprotect any type of data, using data elements (tokenization, encryption, alphanumeric Data Elements, etc created in a Policy).
- Utilized the Starburst Helm Kubernetes deployment and made enhancements by updating helm charts, deployment templates to meet specific requirements. Introduced an init container approach to perform initial tasks and streamline the deployment process.
- Automated end-to-end CI/CD pipelines, encompassing the building of JAR files, creation of Docker images, and packaging of Helm charts. Additionally, automated QA pipelines using the BDD framework in conjunction with Cucumber and Terraform for Infrastructure as Code.
- Integrated a Go utility into the code base for secure file encryption, decryption, file retrieval from AWS S3, GCP storage, and Azure Storage blobs, and data uploads to shared memory.
- Built Trino JAR files and Jpeplite JAR files, packaging them within Docker images. Incorporated the Go Utility to download policies from various cloud storage solutions into containers. Updated Kubernetes Worker and Co-Ordinator

Pod Deployments for unified usage.

- **Tech Stack: Java, Maven, Gradle, Azure EKS, Azure Synapse, Trino DB.**

Enterprise Security Administrator (ESA): Enterprise Security Administrator is an integration product of different types of components that helps in the protection and unprotected of Data.
Role: Associate Software Engineer

Responsibilities:

- Automated Continuous Integration/Continuous Deployment (CI/CD) pipeline for ESA and enhanced code quality through the integration of SonarQube for code scanning and coverage analysis
- Collaborated within a team to develop a Robot Framework for product testing. Automated testing processes were orchestrated to execute in a containerized Docker environment as part of the QA pipeline.
- Devised a streamlined process using QEMU and KVM to transform ISO images into VHDs, subsequently creating AWS AMIs, GCP Images, and Azure Disks. Orchestrated the entire image creation workflow on Jenkins, resulting in a remarkable 50% efficiency gain and a 90% reduction in execution time.
- Automated the comprehensive Resiliency and Performance testing of ESA on AWS, conducting a rigorous 7-day test cycle with failover scenarios. This automation led to significant time savings, replacing days of manual effort.

- **Tech Stack: Shell Scripting, Robot, Python, QEMU, Jenkins**

Immutable Protector Containers: Protegrity Protector's Kubernetes Deployment to improve scalability and performance of protected, unprotect operations on Data. Works on Immutable Policy once Fetched from ESAs, it's not required unless there is an update**.**
Role: Associate Software Engineer

Responsibilities:

- Implemented and automated end-to-end CI/CD pipelines for IMP-Containers for packaging Docker Images, Helm Charts, Sample Applications and Protectors. Additionally, established a robust QA pipeline for product testing across AWS, GCP, Azure and Openshift.
- Led the integration of JFrog's X-RAY scanning for Docker Images, enhancing security by identifying vulnerabilities, and established Splunk integration for effective logging and real-time monitoring.
- Single-handedly deployed Notary as a platform harnessing the power of TUF (The Update Framework), for robust Docker Image signing and ensuring the highest levels of security with Docker Content Trust.
- Automated Kubernetes (k8s) environment provisioning across EKS, AKS, and GKE using a combination of Terraform, Ansible, and CloudFormation, resulting in a remarkable 60% improvement in access management and testing efficiency.

- **Tech Stack: AWS EKS, GCP GKE, Azure AKS, Openshift, Jenkins, Terraform, Ansible.**

Vulnerability Management System: Designed and developed VMS for identifying, evaluating, treating, and reporting on security vulnerabilities in products. Comparing the components with various open-source data like NVD, checking the CVEs, and Reporting vulnerable components by creating JIRA tickets.
Role: Associate Software Engineer
Responsibilities:

- Designed and developed a highly scalable AWS based service utilizing SQS, RDS, and ECS. This service's core function is to identify product vulnerabilities by comparing their components against various sources such as NVD and relevant metadata.
- Designed and implemented an API for Subscription Management with SMTP integration. This API enables scheduled notifications and offers users the capability to subscribe or unsubscribe for each product. Additionally, integrated the system with JIRA, creating an API to generate JIRA tickets for identified vulnerabilities.
- Orchestrated the integration of Vulnerability Management System (VMS) with JFrog Artifactory's X-ray scanning functionality. This integration enabled comprehensive scans of products for security and license violations, among other factors.
- Containerized the project and deployed it on Amazon Elastic Container Service (ECS), with an Application Load Balancer (ALB) serving as the front-end and a PostgreSQL RDS serving as the project's database.
- Furthermore, implemented automation for CI/CD and QA pipelines using Jenkins.

- **Tech Stack: Java, Spring Boot Framework, React, AWS RDS, AWS ALB, AWS ECS, AWS SQS, SSM**

Miscellaneous Activities, Protegrity:

- Created proofs of concept for innovative new solutions like RASA ChatBots.
- Configured, installed and tuned Softwares like Jenkins, GitLab, SonarQube and Notary for entire RnD organizations usability.
- Worked on POCs of integration with Lacework Solutions and BlackDuck.
- Researched and identified new technologies and tools helping to grow an agile development environment .

ACHIEVEMENTS

- **Awards & Recognition:**
  - Spot Award & Bright Beginner in Protegrity - 2019
  - Rockstar Rookie at Velotio Technologies - 2022
- **Certifications:**
  - AWS Certified Solutions Architect Associate
  - Certified Kubernetes Administrator (CKA)
- **Additional Activities:**
  - Speaker in Velotio Elevate Session on "k3s: The Crazy things we do to make k8s simple."
  - Written Technical Blogs for different websites - How to get started with logging in kubernetes
  - Speaker in Tech talk and Tech Shorts for Velotio on - Secret Management
  - Speaker and Host for a week long DevOps Session at Dr. D.Y.Patil's RAIT on Kubernetes, Terraform and Ansible.
  - Written Blog on Topics like - "Considering Managed Kubernetes? 20 questions to ask" and "Your secret's safe with me"