Ranjith Katanguri

Lead Cloud & DevOps Engineer

Contact: +1 571-663-6609 Email: ranjithrrk16@gmail.com

LinkedIn: https://www.linkedin.com/in/ranjith-katanguri-s1987/

Professional Summary:

- Total 14+ years of IT experience specializing in **Cloud (Azure, AWS), DevOps, Terraform, Kubernetes**, and **Linux** across banking, healthcare, and retail domains
- Hands-on experience in deploying and managing AWS services **EC2, Route 53, IAM, EBS, EFS, S3, VPC, EKS, RDS, CloudFront,** and **Lambda**.
- Built and maintained **CI/CD pipelines** using **Jenkins, GitHub Actions, GitLab CI/CD,** AWS CodePipeline and Argo CD, reducing deployment times by 40%.
- Experienced in Azure services including **Azure Repos, Pipelines, Boards, Artifacts, AKS**, **Virtual Machines, App Services, Bicep, and Azure Storage (Blob and File).**
- Experienced in monitoring and observability tools such as **Grafana, Prometheus, Splunk, CloudWatch, Cavisson, OpenSearch,** and **Kibana.**
- Worked on deployment, configuration, monitoring, and maintenance of **OpenShift** Container Platform using **Helm** charts.
- Experienced in managing microservices using Kubernetes to orchestrate Docker containers and in setting up Kubernetes clusters on **AWS EKS**
- Knowledge advanced Kubernetes operations, including multi-cluster management and service mesh (**Istio**) implementation for scalable, cloud-native applications
- Experienced in Kubernetes upgrades, scaling, and optimization for high performance cluster management.
- Experience on **GIT**, **Jenkins, Maven, Ansible, Terraform, Docker and Kubernetes.**
- Experience with Infrastructure as Code (**IaC**) to automate provisioning, configuration, and management of AWS, Azure cloud environments using tools like **Terraform** and **ARM** templates.
- Developed **Python** scripts for automation, integration, and system health monitoring, improving deployment accuracy and reducing manual effort by 40%
- Improved incident response time by 60% through effective observability practices and runbooks.
- Reduced cloud spend by 25% through proactive monitoring and reserved resource utilization.
- Provided operational and production support on regular release cycles by following scrum calls.

IT Certifications:

- Certified Kubernetes Administrator (**CKA**) - LF-0l3qjctcss (The Linux Foundation)
- AWS Certified Solution Architect Associate - (**AWS-CSAA**) - GVYRD0B1P1RQ15CM

- RedHat Certified Engineer - (**RHCE**)
- RedHat Certified System Administrator - (**RHCSA**)

Technical Skills:

Cloud Platforms	**AWS, Azure Cloud**
DevOps CI/CD Tools	**Azure DevOps, Jenkins, GITHub Actions, GitLab CI/CD, ArgoCD, Harness, Helm**
Infrastructure as Code	**Terraform, Ansible, ARM Templates, Bicep, CloudFormation**
Containerization	**Docker, Kubernetes (AKS/EKS), Helm, OpenShift**
Web Servers	**Tomcat, Apache, Nginx**
Security & Compliance	**IAM, RBAC, Azure Key Vault, Secrets Manager, AWS Inspector, WAF, AWS VPC Security Tools, Zero Trust, KMS, Conjur, AWS KMS, OWASP, Sonarqube, Snyk**
Workflow Tools	**Rally, Jira, Mural, Bitbucket, Azure board**
Observability Tools	**Cloud Watch, Prometheus, Grafana, Splunk, Azure Monitor, ELK Stack, New Relic, Datadog, OpenTelemetry**
Programming & Scripting	**Bash, Python, PowerShell, YAML, Go, groovy**

PROFESSIONAL EXPERIENCE:

Role: Kubernetes & Cloud DevSecOps Lead **Duration: Sept 2025 to Present**

Client: ANZ (Australia and New Zealand Banking Group) **Location: New York (Remote)**

Project Description: Perform cloud application migration Openshift to AWS EKS

Responsibilities:

- Designed and managed multi-cloud infrastructure (AWS, Azure) ensuring high availability, scalability, and cost efficiency.
- Implemented secure secrets management via Azure Key Vault and GitHub Actions secrets.
- Applied Azure best practices for security, governance, monitoring, and cost optimization
- Built observability using Azure Monitor, Log Analytics, and pipeline monitoring tools.
- Maintained Kubernetes clusters (EKS/AKS) with automated scaling, networking policies, and resource optimization.
- Built and maintained CI/CD pipelines using Jenkins, GitLab CI/CD, Argo CD, and Helm, GitHub Actions, to streamline application delivery across multiple environments.
- Migrated applications from OpenShift to EKS, updating workloads and CI/CD pipelines.
- Deployed apps using Helm, GitOps, and Operators for automated, consistent deployments.
- Implemented RBAC, network policies, and monitoring with Prometheus, Grafana, and CloudWatch.
- Designed and automated serverless application deployments using AWS SAM, enabling consistent infrastructure provisioning via CloudFormation.

- Automated Azure infrastructure provisioning with Terraform (AKS, Key Vault, VNets, Storage).
- Implemented enterprise grade security with RBAC, Key Vault, image scanning, and policy-as-code integrations.
- Integrated secret management solutions Vault into CI/CD pipelines for secure credential handling.
- Implemented observability solutions using Prometheus, Grafana, ELK/EFK, enabling proactive monitoring and root cause analysis
- Collaborated with developers and SRE teams to provide self-service platform tooling, reducing operational overhead.
- Developed Infrastructure as Code (IaC) using Terraform, CloudFormation, and Azure Bicep to automate platform provisioning.
- Perform applications migration by following a re-platform strategy for OCP apps migrated to AWS EKS.
- Integrated AWS Secrets Manager for secure MongoDB credential storage and rotation
- Integrated static code analysis (SonarQube) and vulnerability scanning (Trivy) in CI/CD pipelines for DevSecOps compliance.
- Configured and managed CloudWatch metrics, logs, and alarms for EC2, EKS, and Lambda workloads, RDS resources and Monitor applications health check, provide backup and DB connectivity.
- Collaborate with cross-functional teams including customer stakeholders, developers, QA, and cloud Architects ensure high availability, performance, and security across environments for seamless project delivery in an Agile environment.
- Implemented AWS Secrets Manager to securely store and manage sensitive credentials, database passwords, and API keys across microservices, integrating with IAM and AWS SSO for centralized identity and access management under a Zero Trust model.
- Manage resource allocation and utilization analysis, leading to the optimization of container resource limits and requests.
- Automated provisioning of AWS resources (VPC, EC2, RDS, ALB, S3) using CloudFormation.
- Experience using the Azure Managed Identities to Integrate Azure Services.
- Built and secured CI/CD pipelines using GitHub Actions, GitLab CI, Jenkins, and Azure DevOps, automating security scanning, policy enforcement, secrets management, and environment hardening.
- Conducted IaC security reviews with Terraform, CloudFormation, ARM and enforced cloud security best practices across AWS, Azure, and GCP and deployed cloud-native tools like GuardDuty, Azure Defender
- Secured containerized environments by building hardened images, enforcing Kubernetes RBAC, network policies, pod security, and monitoring cluster vulnerabilities with Trivy
- Implemented security throughout the SDLC by performing threat modeling, secure code reviews, and risk assessments; leveraged SAST, DAST, and SCA tools to detect and remediate OWASP.
- Perform migrating service repos from Azure to Github for code scan activities.

- Created and maintained Helm charts for packaging and deploying microservices with parameterized configurations.
- CVE fixes via ADO aquascan, appscan, nexusiq, sonarqube, gitleaks.
- Managed Git, Branching and Merging, resolved conflicts, push changes etc
- Perform repo migration with specified team access and involved azure pipeline deployments.
- Managing Azure DevOps build and release pipeline, setting up new repos managing the permissions for various GIT branches.
- Implemented Azure AD and MFA for secure authentication, enhancing identity protection
- Developed self-healing systems by implementing automated rollback, restarts and auto-scaling policies for Kubernetes clusters.
- Used Kubernetes to manage containerized applications using its nodes, config maps, selector, services and Deployed application containers as pods.
- Integrated GitLab CI/CD pipelines with Kubernetes and Helm/Argo CD to automate application promotion across environments (Dev to QA then Prod).
- Automate deployment pipeline using CI/CD tools and change the active node in Jenkins pipeline and Kubernetes operations.
- Provide branch protection in GitHub and updated various files and submitted pull requests for team leads.
- Designed and maintained OpenShift-based multi-tenant environments, leveraging Operators for automated deployments, monitoring, updates of mission-critical workloads.
- Worked on gradle builds, GitHub Administration tasks and user separation tickets.
- Collaborated with development teams to embed SRE best practices into applications life cycle, improving Service uptime and reliability.
- Implemented and managed Azure ExpressRoute to establish secure, high-performance private connectivity between on-premises and Azure environments
- Performed cloud security assessments with AWS Config, Trusted Advisor, and Checkov, and set up CloudWatch and Azure Monitor alerts for proactive monitoring
- Integrated Terraform into Azure DevOps pipelines to automate plan/apply stages, enforce policies, and manage infrastructure updates via pull requests.”
- Designed and provisioned EKS clusters via Terraform with custom VPCs, subnets, and node groups for scalable, secure workloads.
- Collaborated with security teams to implement Azure Policy as Code via Terraform, ensuring compliance for tagging, encryption, and access management while managing existing Azure resources without downtime or drift.
- Designed and deployed containerized microservices on AKS and ACI with optimized Docker images.
- Hands-on experience supporting mission-critical Kubernetes and Red Hat OpenShift (OCP v4) platforms in high-availability, low-latency, and regulated environments.
- Deep expertise in Azure DevOps (ADO) including Git repos, branching strategies, pull requests, work item governance, CI/CD controls.
- Developed and maintained OpenShift and Kubernetes manifests (BuildConfigs, DeploymentConfigs, CRDs) and custom Helm charts aligned with firm-wide standards.

- Led centralized logging and observability using Elastic Stack (Elasticsearch, Logstash, Kibana), including performance tuning, capacity planning, and retention policies to meet audit requirements.
- Embedded DevSecOps controls by integrating SonarQube into ADO pipelines and PR flows, enforcing code quality, licensing, and security policies.
- Implemented observability solutions using Prometheus, Grafana, ELK/EFK, OpenTelemetry, enabling proactive monitoring and root cause analysis
- Integrated Snyk for automated scanning of open-source dependencies, container images, and IaC templates within CI/CD pipelines.
- Deployed Aqua Security to secure container images and Kubernetes runtimes, enforcing image scanning, runtime protection, and admission control policies.
- Implemented Prisma Cloud for continuous cloud security posture management (CSPM), workload protection, and vulnerability monitoring across AWS, Azure, and Kubernetes environments.
- Integrated Snyk into CI/CD pipelines to scan Docker images, Helm charts, Go modules, and Terraform code, enabling early vulnerability detection and remediation.
- Built and maintained Go (Golang) based automation and controllers to improve reliability, observability, and operational efficiency of large-scale AWS EKS platforms.
- Configured Kubernetes RBAC and NetworkPolicies to enforce secure, multi-tenant access control.
- Configured Linkerd service mesh for mTLS encryption and traffic observability.

Environment: OpenShift (OCP), AWS EKS,IAM,Code fresh (CI), GitHub Actions (CD), Jfrog artifactory, Azure, Jenkins, docker, Kubernetes, Python, Helm, GitLab CI/CD, Argo CD, Terraform, CloudFormation, Bicep, Prometheus, Grafana, ELK, OpenTelemetry, Conjur/Vault

Role: Cloud & DevOps Lead **Duration: Mar 2020 to Sept 2025**
Client: Standard Chartered Bank
Project Description: Multi country segregation activities performed with cloud and devops implementation for banking transactions.

- Delivered end-to-end DevOps automation across the SDLC, collaborating with architecture, development, QA, networking, CDN, and vendor teams to ensure scalable and reliable deployments.
- Deployed and managed containerized workloads using Docker, Kubernetes, custom Helm charts, and ArgoCD, including chart customization and environment-specific configurations.
- Implemented Terraform IaC for AWS environments managing modules, state, Vault integration, and provisioning services such as ALB/NLB, ECS, EC2, ElastiCache, Auto Scaling, and PrivateLink.
- Enhanced AWS infrastructure by managing cloud resources, applying advanced Linux administration, optimizing DNS/CDN routing, and supporting multi-region, multi-tenant architectures.
- Automated cloud infrastructure using Terraform, ARM, and Bicep across Azure App Services, AKS, Storage, Networking, and Key Vault.

- Developed automation using PowerShell, Bash, Python, and YAML to streamline operations and reduce manual work.
- Enhanced monitoring and security using Azure Monitor, App Insights, Grafana, RBAC, and secrets management.
- Implemented CI/CD pipelines with Jenkins, GitLab, and AWS CodePipeline for microservices and monolithic applications.
- Orchestrated containerized workloads using Docker and Kubernetes, improving deployment speed and reliability.
- Integrated CloudWatch, Prometheus/Grafana, and ELK for centralized logging, monitoring, alerting, and enhanced observability of performance metrics.
- Integrated Conjur/Vault for secret management across all environments.
- Participated in cloud migration projects from on-premises OpenShift to AWS EKS, reducing infrastructure costs and improving scalability.
- Implemented Canary, Blue/Green, and Rolling deployments using Harness for microservices running on Kubernetes/EKS.
- Perform Helm deployments in multi country segregation environments by updating configs and overrides.
- Provide Azure ADO pipeline for requested services in multiple environments and update endpoints for specified services by using proxy setup.
- Deploy services in multiple clusters in specified environments like Dev, QA, OPT, Production
- Created custom CloudWatch dashboards to visualize system metrics, latency, and application performance in real time.
- Update TLS certificate, update solace cert in EKS and SSL cert for kong interface connectivity.
- update secret in AWS secret manager, create service account as part of setting up the new environment.
- Whitelisting GIT secrets, creating replicas and implementing pod autoscaling nodes in AWS, Monitoring health check of production services.
- Perform Image helm tagging, Update docker image and manual helm deployment from artifactory
- Namespace defined, certification generation for vault in new environment setup.
- Creating playbooks and working on log4j service remediation for penetration testing
- Update on Bitbucket repository config changes in Kafka, Mongo DB, Axon servers, cname for different environments and respond to Liquibase DB requests.
- Perform Helm file generation, helm rollback deployments, migrating services to ADO.
- Experience on deployments, services, volumes, service networking and troubleshooting.
- Experience on scheduling pod, node affinity, replica sets, deployments, namespaces, services, resource limits, multiple pod scheduler.
- Provide Microsoft ADO access to users to run azure build pipeline, Manage SCM access to users and create repositories in ADO.
- Automated container image build and push to Amazon ECR, followed by deployment to EKS using Helm.
- Check UI issues, manually patch tx-web-frontend services, update static secrets in vault.

- Scale the environments when resources are down in the AWS environment, configure Kubernetes auto scaling using HPA (horizontal pods autoscaling).
- Kubernetes secrets installed via tp-common helm chart and maintain Confluence for all activities to follow instructions.
- Managed IAM roles/policies, ensuring secure access control and Setup Kubernetes ingress and ingress controller, optimizing application routing and resource allocation.
- enable endpoints for newly onboarded services Traefik ingress setup, port allocation.
- Automated application builds and deployments to Kubernetes using Helm, resolved Azure DevOps build issues, and managed deployments and troubleshooting on AKS for smooth, reliable rollouts.
- Deployed service-to-service authentication using mutual TLS (mTLS) and certificate-based trust within EKS clusters.
- Deploy traefik load balancer through helm chart in kube-system namespace.
- Manage Kubernetes environments across multi-cloud platforms (Azure, AWS) with a focus on high availability.
- Analyze performance metrics to enhance Kubernetes cluster efficiency and reliability.
- Configure YAML files of the pods with necessary resources and environment variables to up and running pods.
- Integrated GitOps practices using ArgoCD and FluxCD to manage Kubernetes deployments declaratively.
- Enforced SSL/TLS encryption, MFA & SAML/OIDC-based SSO for secure cloud access.
- Integrated code review & merge approval processes in GitLab/GitHub for quality control.
- Automated service mesh deployments using Istio for secure service-to-service communication.
- Implemented Amazon Inspector for vulnerability management across EC2, ECR, and Lambda environments.
- Integrated Azure Key Vault with AKS to implement secure secrets management, allowing stateful sets to securely access and mount sensitive data, certificates, encryption keys
- Automated provisioning of Azure resources including VNets, NSGs, Load Balancers, AKS clusters, Storage Accounts, and App Services using Terraform.
- Automated Axon server lifecycle management including AMI refreshes, license updates, event backups to S3, and monitoring using Terraform to ensure reliable and up-to-date deployments.
- Automated cloud infrastructure provisioning using Terraform and CloudFormation, ensuring consistent, repeatable, and scalable deployments.
- Integrated Python-based validation scripts with Terraform to automatically verify post-deployment configurations and maintain compliance.
- Managed Terraform states, variables, and plan/apply workflows to enable reliable, controlled, and auditable infrastructure updates
- Created multi-branch pipelines for microservices applications enabling parallel deployment and testing.
- SCDF task deployment for task registration request and restart SCDF service
- Developed reusable IaC templates with Terraform, CloudFormation, and AWS CDK to standardize provisioning of AWS resources including EC2, S3, RDS, Lambda, and VPC.

- Automated multi-cloud infrastructure provisioning and updates using Terraform, CloudFormation, Azure Bicep, AWS CDK, and Python scripts, ensuring consistent, repeatable deployments.
- Created custom monitoring agents using Python (boto3/azure-sdk) to collect metrics and push them to Azure Monitor and Log Analytics
- Followup issues with Jira ADO tickets, scrum calls, retrospective, sprint review meetings.

Environment : EKS, EC2, S3, IAM, RDS, CloudFront, Route 53, Lambda, Docker, Kubernetes,, blue green deployment, Maven, Helm, Kibana, AWS, Azure, Terraform, Jenkins, GitLab CI/CD, Argo CD, Vault, Prometheus, Grafana, ELK, Python, Bash, Git, SonarQube, Nexus.

Role: Site Reliability Engineer (SRE) **Duration: Feb 2017 to Feb 2020**
Client:Macys Technologies
Project Description: managing ecommerce of macys, kohls services, load balancing with observability tools.
Responsibilities:

- Implemented end-to-end observability using Datadog APM, metrics, logs, and dashboards across cloud-native applications, reducing incident detection time by 30%.
- Integrated Datadog with Slack and PagerDuty to streamline alerting and escalation workflows, enhancing operational reliability and team coordination.
- Managed SLIs, SLOs, and SLAs to ensure system reliability, leveraging metrics and dashboards to monitor performance against targets and proactively mitigate downtime.
- Integrated Dynatrace alerts with Slack, PagerDuty, and ServiceNow for automated incident workflows.
- Designed and executed chaos engineering experiments to proactively validate system resilience, increasing uptime and fault tolerance
- Created custom dashboards, alerts, and service level monitoring to track application performance and system health.
- Managed and administered high-performance Redis cache clusters to support high-traffic applications, reducing database load and improving response times.
- Set up comprehensive monitoring and alerting for Redis metrics (e.g., memory usage, hit rate, connected clients) using tools like Prometheus and Grafana
- Automated deployment and management of Kafka components (brokers, topics, Zookeeper, Schema Registry) in containerized environments using Docker and Kubernetes.
- Set up robust monitoring for Kafka clusters using tools such as Prometheus, Grafana, or splunk creating dashboards to track key metrics and set up alerts for anomalies.
- Implemented and integrated secure secrets management using Vault, AWS Secrets Manager, and Conjur to ensure safe handling and storage of credentials.
- Implemented centralized logging with ELK(Elasticsearch, Logstash, Kibana) and configured Prometheus and Grafana dashboards for infrastructure and application performance monitoring
- Extract logs from pods and upload to a server, Force sync bitbucket repos permissions and default reviewers.

- Automated blue-green and canary deployments using Jenkins and Kubernetes, ensuring zero-downtime releases.
- Implemented auto-scaling mechanisms using Horizontal Pod Autoscaler (HPA) and Cluster Autoscaler for optimized resource utilization.
- Orchestrated and optimized containerized workloads with Docker and Kubernetes, leveraging rolling updates for seamless application upgrades.
- Strong collaboration across cross-functional teams (Dev, QA, Security, Operations).
- Reduced operational things by automating repetitive tasks and standardizing runbooks, alerts, and incident response procedures.
- Collaborated in Agile/Scrum environments, participating in sprint planning, stand-ups, and retrospectives
- Improved observability with monitoring dashboards, alert tuning, and anomaly detection; collaborated with global teams for seamless incident response.
- Installed, configured, and administered highly available Elasticsearch clusters, managing nodes, shards, and index lifecycle policies.
- Monitored cluster health, performance, and availability using Kibana, Grafana, and Prometheus, proactively identifying and resolving bottlenecks.
- Implemented Elasticsearch security controls including authentication, role based access control (RBAC), TLS encryption, and audit logging.
- Diagnosed and resolved issues related to cluster stability, node communication, indexing performance, and data ingestion pipelines.
- Implemented centralized observability and monitoring with Prometheus, Grafana, ELK/EFK, CloudWatch, and X-Ray, creating dashboards and metrics to ensure system performance and reliability.
- Led on call rotations, handled high severity incidents (P1/P2), conducted post-incident reviews and implemented long term corrective actions
- Built robust alerting systems using alert manager, pagerduty and custom scripts to proactively address Performance degradation.
- Reduced mean time to detect (MTTD) and mean time to resolve (MTTR) incidents by 40% through real-time monitoring and automated alerts.
- Strong collaboration across cross-functional teams (Dev, QA, Security, Operations).
- Collaborated in Agile/Scrum environments, participating in sprint planning, stand-ups, and retrospectives

Environment: Jenkins, Grafana, Prometheous, Mysql, Bitbucket, Ansible, Jenkins, GitLab CI/CD, Docker, Kubernetes, Helm, ELK, Linux, Git, Agile/Scrum.

Role: Senior Cloud Engineer **Duration: Jan 2016 to Feb 2017**
Client: Hewlett Packard Enterprise **Location: Cyberjaya, Malaysia.**
Project Description: Cloud implementation for Alstom, Ericson, Nokia Projects and provide operational support

- Designed and deployed highly available, fault-tolerant applications on AWS (EC2, S3, RDS, Route53, Load Balancers, VPC) and managed resources including EC2, RDS, VPCs, subnets, NAT/Internet gateways, and auto-scaling groups

- Configured Security group for EC2 instances, created backup using AMI for critical instances, worked on S3 to create buckets to store objects.
- Established strong identity-based access control (IAM + SSO) with MFA enforcement for both users and service accounts
- Assisted in setting up basic IAM roles and S3 bucket permissions for secure Redshift access.
- Designed and maintained high-performance, scalable and reliable systems in AWS environments, ensuring Optimal uptime and performance using Open Telemetry metrics.
- Configured High Availability and backup strategy with EBS, S3 for microservices.
- Designed and managed multi-cloud environments across AWS and Azure with Terraform workspaces, modules, and remote state for scalable, reliable infrastructure delivery.
- Applied cost optimization strategies by right-sizing EC2 instances and leveraging Reserved Instances and Savings Plans
- Helped team with snapshot scheduling and cluster backup activities in Redshift.
- Managed VPN, NAT Gateway, and firewall configurations for hybrid connectivity setups.
- Enforced tagging policies and created budgets with alerts for cost governance.
- Enforced security and compliance standards across all cloud resources.
- Configured monitoring and alerting systems to reduce incident response times by 50%.
- Managed Identity and Access Management (IAM) with granular roles, policies, and least-privilege principles across multi-account environments.
- Participated in cloud migration projects from on-premises to AWS and Azure, improving scalability, reliability, and cost efficiency.
- Implemented S3 storage strategies, including cross-region replication, bucket creation, lifecycle policies, versioning, and cost optimization using Standard, Infrequent Access, and Reduced Redundancy storage classes.
- Conducted VPC peering, secure network configurations, and security group implementations to ensure compliance and protect cloud environments.
- Managed cloud resources and ongoing maintenance, including VM data migration, NAT instance launches, and overall security and compliance enforcement.
- Designed and implemented monitoring dashboards and alerting solutions with AWS CloudWatch and Dynatrace, enhancing system and application performance visibility and reducing incident response times by 50%.

Environment: VPC, S3, GIT, EC2, Route53, RDS, Docker, Jenkins, GitLab CI/CD, CloudFormation, Prometheus, Grafana, ELK, Vault, Python, Bash, PowerShell, Git

Role: AWS Cloud Engineer **Duration: May 2014 to May 2015**
Client: Agilent Technologies
Project Description: Perform server migrations on-premise to cloud and manage resources.
Responsibilities:

- Designed and deployed highly available, secure, and scalable cloud infrastructures using AWS services (EC2, S3, RDS, VPC, IAM, Lambda, EKS) and implemented network segmentation with VPCs, subnets, route tables, and security groups to enforce compliance.
- managed IAM roles, policies, and permissions to enforce least privilege across accounts.

- Configured load balancers (ALB/NLB) and DNS (Route53) for application traffic management.
- Designed and deployed multi-cloud solutions ensuring high availability, scalability, and cost optimization.
- Implemented and integrated secure secrets management using Vault, AWS Secrets Manager to ensure safe handling and storage of credentials.
- Enforced security policies and compliance standards across all cloud environments.
- Monitored and optimized cloud resource usage through AWS Cost Explorer and Azure Cost Management, improving operational efficiency and reducing costs.Contributed to AWS cloud migration projects, enhancing scalability, reliability, and cost efficiency of enterprise workloads.
- Designed and managed highly available, fault-tolerant, and cost-optimized AWS infrastructures leveraging EC2, S3, ELB, EBS, Auto Scaling, and IAM.
- Configured EC2 instances with auto-scaling architectures, security groups, and Apache Tomcat for dynamic and secure application hosting.
- Created and managed S3 buckets, implemented CloudWatch monitors, alarms, and log configurations to ensure real-time observability and incident response.
- Built data analytics pipelines using AWS Glue, Redshift, and S3, improving data integration, transformation, and reporting efficiency.
- Developed and maintained Ansible playbooks to configure servers, deploy applications, and manage software across multiple environments consistently.
- Implemented IAM best practices with RBAC, SSO, MFA, and privileged access management, enforcing cloud security and compliance using IAM policies and KMS encryption across AWS
- Built and maintained CI/CD pipelines using Jenkins to automate regression and smoke test executions, improving release quality and reducing manual effort.
- Managed Git versioning and branch tagging across environments to ensure consistent and controlled code releases.

Environment: AWS, EC2, S3, RDS, Lambda, VPC, IAM, KMS, CloudFormation, ELB, AWS CDK, Jenkins, GitLab CI/CD, AWS CodePipeline, ECS, CloudWatch, ELK/EFK, Python, Bash.

Role: Linux System Administrator (SME) **Duration: Feb 2011 to Apr 2014**
Client: L&T Technology Services
Project Description: Perform linux server migration to VM, experienced on storage, networking, handled datacenter issues.
Responsibilities:

- Installed, configured, and managed Linux OS (RHEL, CentOS, Ubuntu, RHEL6) on physical servers (Dell PowerEdge, HP-UX DL380, Supermicro) and virtual environments (VMware ESXi 5.5), including VM deployment, snapshots, and troubleshooting.
- Executed P2V and V2V migrations using Double-Take Availability Tool, supporting lift-and-shift migration initiatives.
- Perform pre and post migration activities like networking and volumes mounts.
- Managed and maintained Cisco switches, routers, VLANs, and trunking across multiple datacenters for high availability.

- Configured and managed file systems, NetApp LUNs, CIFS/NFS shares, DNS, Apache Tomcat, Samba, FTP, and NFS services
- Performed server hardening, kernel upgrades, OS patching, security configurations, backup/recovery, and SLA-aligned maintenance within downtime windows to ensure service reliability.
- Administered user accounts, permissions, and access controls, wrote shell scripts for scheduled backups and automated tasks.
- Monitored system performance, troubleshoot boot and network issues, coordinated with vendors for hardware replacements, and maintained comprehensive server inventories and project documentation
- Perform Disk management and filesystem management, configuring multipath.
- Attend client meetings, provide support within the downtime window.
- Documented recurring issues, perform firmware upgrade and monitored systems, escalating incidents via ServiceNow, Jira to ensure timely resolution and troubleshoot network and hardware failure issues of AMD, Nvidia GPU servers.
- Advanced Linux automation and scripting using Bash and Python to support operational resilience, incident response, and platform stability.

Environment: Datacenter, Networking, Linux, Windows, Apache tomcat, Linux, NetApp storage, VMware ESXi, Netbox, BMC and shell scripting,

Educational Qualification:

B. Tech from Sindhura College of Engineering (Affiliated to JNTU, HYDERABAD) 2010.