infylogy

D VENKATESH
Email: vdunna590@gmail.com
Phone No: 848-999-9840

SUMMARY:

- Experienced and results-driven Site Reliability Engineer (SRE) and DevOps Engineer with over 9+ years of hands-on experience in designing, automating, and managing scalable infrastructure and CI/CD pipelines for cloud-native applications. Proven expertise in AWS, Kubernetes, Terraform, Docker, and observability tools like Data Dog, Prometheus, Grafana, and Fluent Bit.
- Adept at improving system reliability, reducing incident rates, and enhancing deployment velocity through robust automation and monitoring. Strong background in infrastructure as code (IaC), incident response, and performance optimization across highly available and distributed systems.
- Passionate about building resilient systems and fostering a culture of collaboration between development and operations teams software configuration management (SCM) processes, Cloud Management, and Network Administrator, and Network Security.
- Extensive experience in deploying, scaling, and managing cloud-native applications using Kubernetes across hybrid and multi-cloud environments.
- Specialized in leveraging Flatcar Container Linux for secure, minimal, and container-optimized OS deployments, ensuring immutable infrastructure and high availability.
- Proficient in using CAST AI to automate cost optimization, autoscaling, and right-sizing of Kubernetes workloads across multiple cloud providers.
- Proficient in implementing Git Ops practices, infrastructure as code (IaC) using Terraform, and observability solutions for proactive monitoring and incident response.
- Committed to reliability, security, and operational excellence in every stage
- As Certified AWS Professional Solutions Architect Strong experience in designing, building, and managing scalable, secure, and cost-effective cloud infrastructure on Amazon Web Services (AWS).
- Proficient in using Terraform to implement Infrastructure as Code (IaC), enabling consistent and automated provisioning of AWS services such as VPC, EC2, EKS, RDS, S3, IAM, and more.
- Translating business requirements into resilient cloud solutions, optimizing performance, reliability, and cost. Skilled in architecting end-to-end solutions with high availability, fault tolerance, and operational efficiency.
- Proficient in architecting scalable, secure, and highly available Kubernetes clusters across cloud (EKS/GKE/AKS) and on-premises environments.
- Resolved critical production issue where CRI-O runtime exhausted file descriptors causing cascading pod failures across OpenShift cluster, implementing ulimit tuning, inotify watches optimization, and custom resource limits preventing recurrence across 500+ containerized applications.
- Debugged complex container image pull failures due to registry mirror synchronization lag and image manifest corruption, implementing custom image pre-caching strategies using ImageContentSourcePolicy and MachineConfig operators

- Mitigated OpenShift 4.14 eBPF-based network policy enforcement causing intermittent packet drops, analyzing Cilium CNI conflicts with OVN-Kubernetes, implementing custom NetworkAttachmentDefinitions for workload isolation.
- Implemented sophisticated disaster recovery using OpenShift Regional DR operator with Metro DR configuration, solving complex challenges with storage replication lag, application consistency groups, and automated failover orchestration
- Designed cross-cluster workload migration strategy using Velero and MTC (Migration Toolkit for Containers), addressing PV data transfer bottlenecks, API version compatibility, and operator migration complexities.
- Skilled in implementing Git Ops, Helm, Kustomize, and CI/CD pipelines for automated deployments and configuration management. Adept at managing multi-tenant clusters, enforcing RBAC and network policies, and ensuring observability using Data Dog.
- Implemented solutions on improving system resilience, optimizing resource usage, and streamlining application delivery through Kubernetes best practices.
- Collaborative team player with a deep understanding of DevOps practices, CI/CD pipelines, and cloud-native design principles.
  Specialized in building and optimizing cloud infrastructure for large-scale applications.
- Proficient in multiple DevOps tools and technologies such as Ansible, Terraform, Docker and Kubernetes. Highly experienced in automation and CI/CD pipelines.
- Expertise in creating, maintaining, and troubleshooting automated scripts and build processes and well-versed in deploying and managing applications on both on-premises and cloud-based infrastructure.
- Communicating technical concepts to non-technical stakeholders myself makes an asset to any DevOps team.
- Self-starter, highly organized, and always searching for ways to improve the efficiency and scalability of the infrastructure.
- Deep understanding of container orchestration, networking, and DevOps principles, and being Certified Kubernetes professional expert in deploying, managing, and maintaining Kubernetes clusters.
- Skilled in software engineering, automation, and cloud architecture.

CERTIFICATIONS:

- AWS Certified Solutions Architect – Professional : a4f3c41988d847f29c48f1aa3ded0e23
- Azure DevOps Engineer: 991038364
- Azure Security Engineer: H707-0372
- CEH v11 – Certification Number: ECC3416902578
- CKA - Certificate Number: LF-73qqoskeav

WORK EXPERIENCE:

Client: PayPal **August 2025 - Present**

Role: Lead SRE/DevOps Engineer

Responsibilities:

- Architected high-availability AWS multi-account infrastructure (EC2, ECS Fargate, Lambda, CloudFront, ECR, S3) using Terraform and IaC, delivering scalable, resilient, and cost-optimized cloud solutions.
- Developed reusable Terraform modules to standardize deployments across environments, reducing provisioning time by 40% and improving compliance
- Designed microservice architecture spanning 300+ services across Kubernetes (EKS), Fargate, and Lambda with service-to-service communication via Kafka and EventBridge.
- Migrated monolithic applications into microservices on Kubernetes, leveraging Helm, GitOps (ArgoCD/Flux), and service mesh for secure and reliable deployments.
- Automated full infrastructure lifecycle management (provisioning, scaling, patching, decommissioning), reducing manual operations and human error.
- Designed, deployed, and optimized Kubernetes clusters using KOPS (preferred) and Amazon EKS, supporting high-availability, multi-region workloads.
- Engineered enterprise-grade Terraform module library enabling repeatable, auditable provisioning of networking, security (IAM, KMS), compute (EKS, Fargate, Lambda), and data stores (DynamoDB, OpenSearch) with drift detection and CI/CD automation.
- Implemented Kubernetes-native platform featuring Istio service mesh, Vault agent sidecar and injector patterns, cert-manager certificate automation, and Twistlock container security policies.
- Defined and enforced IAM policies, roles, and permission boundaries across multiple AWS accounts, implementing least-privilege access and secure cross-account federation.
- Resolved complex IAM escalations and misconfigurations that impacted production environments, ensuring business continuity.
- Built and operated AWS Fargate services for containerized workloads with auto-scaling, service discovery, and load balancing across multiple availability zones.
- Deployed and scaled AWS EKS clusters supporting 300+ microservices with advanced networking (Ingress, CNI plugins), security (Network Policies, Pod Security Policies), and resource management (HPA, VPA).
- Managed AWS Lambda functions for serverless compute, event-driven workflows, and asynchronous job processing with DynamoDB and Kinesis integration.
- Architected DynamoDB tables with careful partition key design, GSI strategies, and monitoring to prevent hot partitioning and performance degradation at scale.
- Implemented OpenSearch clusters for centralized log aggregation, full-text search, and analytics across payment systems with proper sharding and replica strategies.
- Deployed managed Apache Kafka clusters for high-throughput event streaming with consumer group management, topic partitioning, and lag monitoring for exactly-once payment processing semantics.
- Integrated AWS Kinesis for real-time data ingestion and processing in payment and fraud detection pipelines with proper shard management and consumer coordination.
- Configured AWS EventBridge for event-driven microservice orchestration, third-party SaaS integrations, and asynchronous payment notification workflows.
- Managed AWS SSM Parameter Store and Secrets Manager for centralized secrets and configuration management with rotation policies and Vault integration.

- Automated certificate lifecycle management (provisioning, renewal, rotation) using ACM and Vault, ensuring uninterrupted secure workloads.
- Developed GitHub Actions connectors in Harness for secure authentication and repository synchronization, facilitating smooth artifact fetching and version tracking across environments.
- Configured GitHub Action triggers to automatically initiate Harness pipelines on pull requests, merges, or tag creation, ensuring consistent build and deployment automation.
- Implemented webhook-based integration for two-way communication between GitHub and Harness, allowing deployment statuses and rollback events to be reported back to GitHub Actions.
- Created reusable Terraform modules for EKS cluster provisioning with networking, security groups, OIDC integration, and add-on management.
- Developed Terraform modules for VPC design, subnet allocation, route tables, NAT gateways, and security group orchestration across multi-account environments.
- Built Terraform modules for IAM role and policy scaffolding with least-privilege principles, cross-account access, and service-linked role automation.
- Engineered Terraform modules for KMS key management, encryption policies, and key rotation for payment data protection (PCI-DSS compliance).
- Integrated on-prem and cloud environments using Direct Connect and VPNs, enabling seamless hybrid workloads.
- Optimized traffic delivery and global distribution using CloudFront caching, signed URLs, and S3 Transfer Acceleration.
- Established monitoring and observability frameworks with Datadog, Fluent Bit, and CloudWatch, implementing metrics, logs, and traces for full-stack visibility.
- Deployed and managed production Kubernetes clusters on EKS with advanced scheduling, resource quotas, and pod disruption budgets for high availability.
- Implemented Istio service mesh across all microservices enabling mTLS encryption, traffic management, circuit breaking, rate limiting, and distributed tracing.
- Configured Istio Virtual Services and Destination Rules for intelligent traffic routing, canary deployments, and A/B testing without application code changes.
- Integrated HashiCorp Vault with Kubernetes using agent sidecar pattern and Vault Injector webhook for automatic secrets injection into pods at runtime.
- Deployed cert-manager for automated TLS certificate provisioning, renewal, and rotation using Let's Encrypt and corporate PKI providers.
- Configured Kubernetes Ingress controllers with SSL/TLS termination, path-based routing, and rate limiting for external traffic management.
- Implemented network policies to enforce microsegmentation between service pods, reducing blast radius of potential security breaches.
- Managed Kubernetes resource requests and limits with proper HPA configuration based on CPU/memory metrics for cost optimization without performance loss.
- Authored reusable Helm charts templating microservice deployments with configurable values, lifecycle hooks (pre-install, post-upgrade), and conditional logic.
- Built Helm chart testing framework using Helm unittest and helmlint to ensure chart quality, syntax validation, and best-practice compliance.
- Created Helm value files for multi-environment deployments (dev, staging, prod) with environment-specific resource limits, scaling policies, and security contexts.
- Implemented ArgoCD application definitions for automated deployment from Git, with automatic sync or manual approval workflows based on environment sensitivity.

- Built ArgoCD notification system integrating with Slack, PagerDuty, and custom webhooks for deployment status visibility and incident alerting.
- Configured ArgoCD SSO integration with OAuth providers for RBAC-based access control and audit logging of all deployment actions.
- Implemented Datadog custom metrics tracking payment transaction flows, fraud signals, and business KPIs with proper cardinality management.
- Configured Datadog monitors and alert rules with intelligent thresholds and anomaly detection, reducing false positives and alert fatigue.
- Integrated Datadog synthetic tests for uptime monitoring, performance benchmarking, and end-to-end transaction flow validation across payment APIs.
- Built Datadog log aggregation and processing pipelines with log rehydration for cold storage optimization and compliance auditing.
- Developed custom N8N nodes extending platform capabilities for fintech-specific integrations with payment gateways and compliance systems.
- Built N8N error handling and retry mechanisms for reliable asynchronous processing of payment transactions.
- Integrated N8N with Datadog, Slack, and PagerDuty for operational automation and incident response workflows.
- Created N8N workflow templates for teams enabling rapid low-code automation of DevOps tasks without engineering overhead.
- Delivered zero-downtime migrations using blue-green and canary deployment strategies.
- Mentored DevOps/SRE teams, promoting automation-first and security-first DevOps practices.
- Standardized processes with redocumented technical and process documentation, updating outdated content and improving cross-team efficiency.
- Collaborated with leadership and stakeholders to align DevOps strategy with business goals, ensuring delivery of secure, scalable, and compliant cloud solutions.
- Acted as a technical leader during outages and escalations, particularly in Kubernetes (KOPS/EKS) and AWS IAM troubleshooting.

Client: CoStar Group **October 2022 – June 2025**
Role: SRE/ DevOps Engineer

Responsibilities:

- Managed the development and deployment of a Kubernetes-based service mesh solution using Istio sidecar, resulting in a 40% reduction in network latency and a 20% increase in application performance.
- Implemented CAST AI for real-time cost optimization, reducing Kubernetes cloud costs by 30-50% through automated scaling and spot instance utilization.
- Used CAST AI to analyze and optimize cluster resources, ensuring efficient pod scheduling and eliminating over-provisioned nodes.
- Integrated CAST AI into CI/CD pipelines for automated cost and performance tuning in Kubernetes workloads.
- Implemented Wiz for security visibility, identifying misconfigurations, vulnerabilities, and compliance risks in EKS. Leveraged Wiz's agentless scanning to detect critical security threats across AWS without performance impact.
- Automated security risk detection and remediation workflows, ensuring proactive threat management and continuous compliance monitoring, aligning cloud security with CIS, NIST, and ISO 27001 standards.
- Performed an upgrade for the on-prem k8 cluster from 1.18 to 1.30 using Kube spray for On-Prem and AWS and created SSL certs are distributed from master to worker nodes, ingress, Istio and twist lock and written YAML pipeline with set of values and variables and generating new Kube config file and performing bootstrap.

- Based on the learnings from the cluster upgrades involved in helping fellow teammates during their turn for cluster upgrades.
- Performed upgrade for the vault agent sidecar and Istio by cleaning up the nodes and verifying the twist lock defenders logs to get them up and running.
- Documented the upgrade issues with the vault injector, bootstrap errors, erroring while upgrading API certs and failure while attempting to corona and drain the nodes.
- Designed and implemented a CI/CD pipeline for a Kubernetes-based microservices architecture using helm charts using different sidecars, reducing deployment time by 50% and increasing overall system reliability by 30%.
- Support the development teams with the automation of build and deployment activities. Automate the software and database build process. Manage build definitions. Develop installers for service and client applications. Develop NuGet packages for reference libraries.
- As the central point of contact for the creation of dev, test, and production environments. Coordinates with development teams, DBA's, System and Network teams to define requirements. Understands and maintains source control, configuration files on all servers. Automate update of configuration files across data centers. Manage the configuration and use of the integrated development and integrated environment for the rotation of DBA credentials.
- Troubleshoot operational issues in test and production. Act as first-tier responder to issues and refer as necessary to second-tier support personnel. Tends to alert and monitoring applications. Takes proactive measurements.
- Created modules for AWS Bucket replication from one account to another account and done a details documentations based on the AWS issue.
- Implemented terraform modules for created Kafka topics, open-search, Backend for S3 bucket, AWS secret manager, route53, snowflake, Kinesis, ECS, ECR, Lambda, DynamoDB.
- Created Aws resources using terraform module for large enterprise application which backend logs storing in S3, Making triggers on Event Bridge for notifications for EC2 task execution.
- Created an ECS based on AWS FarGate with task definition and execution for running container which included roles and policies.
- Used Cloudfront on top of S3 to host the application on AWS based DNS through internal network and pointing DNS through Akamai to access through external network.
- Supported the cluster, helm, vault, aws, data dog, Kafka, confluent related issues across all the teams.
- Created CDN using akamai creating hostname linking to the verify certificate from Costar Star Group and property configuration setting included with different set of rules and protocols (Cert origin, traffic reporting, geolocation, log delivery, protocol optimizations, adaptive optimizations, offload origin, strengthen security).
- Created set of rile in Akamai to minimize payload and increase availability due to site failover and health.
- Implemented log index and log jail rule in Data Dog to limit logs coming from K8 and EKS cluster to reduce cost optimization.
- Created manual pipeline on ADO for IOS and Android Application based on react js doing prep for node module based on the package and costar dependencies and building with provisioning profile and certs deploying it to s3.
- Implemented containerized pipeline solution for the trained machine learning models from s3bucket and implemented release pipeline on k8 clusters with vault sidecar and Istio virtual service running on the application.
- Improved pipeline observability by enabling deployment event tracking and notifications in GitHub Actions and Harness dashboards.
- Contributed to standardized pipeline templates in Harness for microservices, improving maintainability and consistency across teams.
- Served as a key on-call engineer, ensuring 24/7 availability for critical production systems across AWS/Kubernetes clusters.
- Designed and implemented automated self-healing mechanisms, reducing manual intervention in production incidents by 40%. Improved Kubernetes autoscaling and resource allocation, ensuring cost optimization and high availability.
- Handled security incidents, such as unauthorized access attempts and compliance violations, ensuring minimal business impact.

- Actively participated in post-incident reviews and root cause analysis (RCA) to drive continuous improvements in system reliability.
- Configured identity federation using OpenID Connect, OAuth 2.0, and SAML for seamless customer authentication.
- Implemented progressive profiling and self-service registration flows to enhance user onboarding and engagement.
- Automated lifecycle management of customer identities, improving security posture and reducing operational overhead.
- Integrated Azure AD B2C with REST APIs and backend services to support advanced claims transformation and user journey orchestration.
- Configured conditional access policies and adaptive authentication to enhance security without impacting user experience.
- Integrated B2C with applications across web, mobile, and APIs, ensuring secure access and scalability for high-traffic applications.

Environment: AWS, Kubernetes, Istio, Vault, Akamai, V-Sphere, Infoblox, Chef, Ansible, Confluent, Jira, Azure DevOps, secret server, Akamai, CastAI

Client: PayPal **April 2021 – October 2022**
Role: CI/CD Engineer

Responsibilities:

- Worked on implementing technical design and implementation to automate application build and deployment solution for Mac Stadium with Anka Virtualization.
- Designed and define architecture for Mac stadium cloud computing systems and migrating existing GCP system to Anka build cloud architectures.
- Automated, optimized and provided efficiency to process different roles in architecture, implemented CI/CD architecture of iOS platform with ansible playbooks.
  https://github.paypal.com/vdunna/automation_scripts
- Installed and Implemented Ansible configuration management system. Used Ansible to manage Web applications, Environment's configuration Files, Users, Mount points, mobile development dependencies for iOS applications and iOS Packages also Worked with automation/configuration management using Ansible and created playbooks in YAML to automate the development processes.
- Created and maintained updated version of MacOS and Anka-packer scripts with technical documentation to be used by different teams inside PayPal.
- Collaborated with different teams to gather information on security and monitoring tools to architect, configure, monitor services used across PayPal.
- Worked on Google cloud platform (GCP) services like compute engine, cloud load balancing, cloud storage, cloud SQL, stack driver monitoring and cloud deployment manager.
- Setup GCP Firewall rules to allow or deny traffic to and from the VM's instances based on specified configuration and used GCP cloud CDN (content delivery network) to deliver content from GCP cache locations drastically improving user experience and latency.
- Worked on GKE Topology Diagram including masters, slave, RBAC, helm, kubectl, ingress controllers GKE Diagram including masters, slave, RBAC, helm, kubectl, ingress controllers.
- Responsible for Setup and build AWS infrastructure using resources VPC, EC2, S3, RDS, Dynamo DB, IAM, EBS, Route53, SNS, SES, SQS, CloudWatch, CloudTrail, Security Group, Autoscaling and RDS using CloudFormation templates.
- Provisioned the highly available EC2 Instances using Terraform and cloud formation and Setting up the build and deployment automation for Terraform scripts using Jenkins
- Managed Docker orchestration and Docker containerization using Kubernetes. Used Kubernetes to orchestrate the deployment, scaling, and management of Docker Containers

- Created and deployed Kubernetes pod definitions, tags, labels, multi-pod container replication for ArgoCD. Managed multiple Kubernetes pod containers scaling, and auto-scaling.
- Deployed pods using Replication Controllers by interacting with Kubernetes API server defining through declarative YAML files.
- Implementation of new tools such as ArgoCD to assist with auto-scaling and continuous integration (CI) and used argo redis to the service deployable through Kubernetes. Use the Kubernetes dashboard to monitor and manage the services.
- Worked on writing Jenkins build a pipeline with Gradle script and Groovy DSL (Domain Specific Language) and integrating ANT/MAVEN build scripts with Gradle for the sole purpose of continuous build.
- Performed GKE cluster upgrade, Configure the cluster metrics for container, Pods, instances and configured the Signal FX monitoring dashboard to alert on any failures. Monitoring dashboards using Splunk.
- Implemented predictive alerting for growth in volume usage for Anka and Mac Stadium Cloud Infrastructure in Signal FX.
- Worked on installing Universal Forwarders and Heavy Forwarders to bring any kind of data fields into Splunk.
- Writing Splunk Queries, proficient in searching, monitoring, analyzing and visualizing Splunk logs.
- Experience in alert handling, standard availability and performance report generation. Experience in root cause analysis of post-production performance related issues through Splunk.
- Managed on-call rotations for MacStadium environments, ensuring high availability and performance of Anka Virtualization for macOS CI/CD workloads. Implemented observability solutions (Prometheus, Grafana) to enhance system reliability and reduce false alarms.
- Handled security and compliance incidents across AWS, GCP, and MacStadium, ensuring IAM policies, VPC configurations, and firewall rules were correctly enforced.
- Conducted post-incident analysis (RCA) and contributed to system reliability improvements, reducing recurring outages by 40%.
- Optimized GCP/AWS auto-scaling strategies, improving cost efficiency while maintaining system resilience.

Environment: GCP, AWS, Mac Stadium, Kubernetes, Docker, ArgoCD, Ansible, Terraform, Splunk, Signal FX, Git, Jenkins, Terraform, Jira, Confluence, Microsoft teams.

Client: DXC Technologies/ HP Enterprise services, **October 2019 – January 2021**
Role: DevOps Engineer

Responsibilities:

- Led implementation of CI/CD tools and automation frameworks, advising on best practices and improving deployment efficiency.
- Automated configuration management using Ansible, developing playbooks for web apps, databases, users, mount points, and packages.
- Configured SonarQube for static code analysis, identifying bugs, code smells, and ensuring code quality across multiple languages.
- Installed and managed Jenkins Master-Slave architecture, building CI/CD pipelines and managing infrastructure as code with Ansible/UrbanCode.
- Developed build automation scripts for Java, Python, JavaScript, C#, .NET Core, Spring Boot, NodeJS, storing artifacts in JFrog Artifactory.
- Reused and updated Terraform modules for monitoring, networking, security, key vaults, and container orchestration.
- Designed and deployed Azure infrastructure using ARM templates, automating VMs, storage accounts, App Services, SQL databases, virtual networks, and resource groups.

- Built and deployed microservices in Azure using API Gateway; deployed web applications on WebLogic, Tomcat, and JBoss.
- Configured and monitored AppDynamics, Splunk, Nagios, and Datadog, collecting metrics and logs from servers and applications.
- Converted AngularJS apps to TypeScript, implemented RESTful APIs, and developed web forms using ASP.NET, HTML, CSS, and JavaScript.
- Developed XML Web Services and enterprise applications in C#/.NET, exposing business layer functionalities.
- Performed OWASP security testing, integrating SonarQube and Dependency-Check for dynamic analysis and penetration testing.
- Implemented EKS elastic containers for testing ArgoCD server deployments; managed manifests, logs, and config files for Datadog integration.
- Resolved catastrophic OpenShift CSI driver (Ceph RBD) deadlock causing 200+ PVCs stuck in pending state, performing deep analysis of kubelet volume manager, implementing custom storage class parameters and mount options resolving I/O timeout issues
- Debugged OpenStack Cinder multi-attach volume corruption when simultaneously mounted across compute nodes, implementing volume locking mechanisms and fencing strategies preventing data loss in clustered database workloads
- Addressed complex NFS persistent volume permission issues in OpenShift due to SELinux context mismatches and supplemental group propagation failures, implementing custom SecurityContextConstraints and fsGroup policies.
- Investigated mysterious 503 errors in OpenShift service mesh affecting 15% of requests, performing distributed tracing analysis with Jaeger, identifying Envoy proxy circuit breaker misconfiguration and connection pool exhaustion, implementing retry budgets and adaptive concurrency limits
- Resolved complex east-west traffic encryption failures in multi-cluster OpenShift Service Mesh federation, debugging mTLS certificate chain validation issues, implementing custom trust domain configurations and certificate rotation automation
- Troubleshot OpenStack Neutron DVR (Distributed Virtual Router) SNAT failures causing intermittent external connectivity loss, analyzing Linux network namespaces, iptables NAT rules, and implementing custom keepalived configurations for HA
- Executed VMware ESXi to Azure lift-and-shift migrations using Azure Migrate, ASR, and PowerShell automation for VM provisioning and VHDS creation.
- Created Terraform modules for Azure, automating resource provisioning and deployment of J2EE/JBoss applications.
- Containerized applications using Docker Compose and Kubernetes, managing manifests, Helm releases, and scheduling replicas across clusters.
- Ensured reproducible builds, container orchestration, and continuous deployment for Kubernetes-managed services.

Environment: Jenkins, Azure, AWS, Splunk, Ansible, terraform, GIT, J-frog, Sonar Qube, Linux packages, Python Packages,
Windows packages, Java, Python, C#, Confluence, JIRA, Microsoft Teams

Client: Kar Auction Services, Carmel, Indiana **March 2019 – September 2019**
Role: DevOps Engineer

Responsibilities:

- Implemented RHEL workstation provisioning via Red Hat Satellite 6.x for RHEL 6/7 clients, managing patching, configuration enforcement, and security policies.

- Administered VMware ESXi 6.0/6.5 and vCenter, performing end-to-end setup, server provisioning, and patch management using VMware Update Manager.
- Installed and hardened Red Hat Linux servers via Kickstart, applying company security policies.
- Managed AppDynamics, including controller configuration, agent deployment, dashboards, alerts, and monitoring, automating tasks via Ansible playbooks.
- Developed Slack bots integrated with APIs and Identity Management to enable secure user-application interactions.
- Executed Terraform and YAML scripts for automated server provisioning, patching, and status collection.
- Integrated JIRA, Confluence, and Jenkins CI for defect tracking, documentation, and automation.
- Configured Nagios to monitor AWS EC2 Linux instances with Ansible automation.
- Managed Jenkins, including Groovy scripting, RBAC, project-based authorization, CI/CD pipeline automation, and backup/migration to S3.
- Engineered solution for OpenShift cluster-monitoring operator consuming excessive resources (12GB+ memory), implementing custom Prometheus retention policies, metric relabeling, and federation strategies reducing footprint by 75%
- Resolved OpenStack Telemetry (Ceilometer/Gnocchi) data ingestion lag causing 4-hour metric delays, optimizing time-series database schemas, implementing InfluxDB clustering, and custom aggregation pipelines processing 10M+ metrics/minute
- Implemented advanced eBPF-based observability using Pixie and Falco on CentOS systems, capturing kernel-level events for security monitoring, detecting zero-day exploits and providing real-time threat intelligence
- Resolved OpenShift Pipelines (Tekton) deadlock where PipelineRuns queued indefinitely due to workspace PVC provisioning race conditions, implementing custom resource quotas, priority classes, and prebound PV strategies
- Debugged ArgoCD ApplicationSet controller causing cluster instability with 1000+ applications, optimizing reconciliation loops, implementing progressive sync waves, and custom health checks preventing cascading sync failures
- Addressed complex GitOps drift detection challenges where manual cluster changes weren't detected, implementing admission webhooks, audit log analysis, and automated remediation workflows restoring desired state
-
- Developed Ansible roles and Molecule tests for Dockerized environments, including linting and YAML validation.
- Built and maintained build/deployment scripts using ANT and Maven for multi-environment deployments.
- Installed, configured, and administered Splunk Enterprise and Forwarders on Red Hat Linux for log aggregation, monitoring, and alerting.
- Developed Splunk queries (SPL/regex), managed apps, roles, realms, and policies, and deployed agents across multiple platforms.
- Collaborated with stakeholders and users for requirement gathering, troubleshooting, and optimizing monitoring and automation processes.
- Configured SSL VPN roles and policies, ensuring secure access to corporate resources.

Environment: RedHat Enterprise, AWS, Red Hat Satellites, Jenkins, Splunk, Universal Splunk Forwarder 5.x/6.x, Molecule Testing,
Ansible tower, GIT, GIT LAB, Ansible, Linux packages, Windows packages, Confluence, JIRA, Slack

Client: GS1, Ewing, New Jersey **Nov 2018 – Feb 2019**
Role: Azure DevOps Engineer

Responsibilities:

- Implemented DevOps pipelines with OWASP security models on CentOS and integrated Azure Key Vault for secure secrets management, sending outputs via SendGrid.
- Built CI/CD pipelines using VSTS/Azure DevOps, NuGet, npm, gulp, .NET Core, pulling code from TFS/Git and packaging artifacts for release.
- Managed variable groups, task groups, and deployment groups to secure passwords, API keys, and configuration data.
- Supported GS1 mobile and .NET applications, managing dependencies for deployment and configuration.
- Developed ARM templates (JSON/XML), PowerShell scripts, and database packages to provision Azure resource groups and associated infrastructure via Visual Studio.
- Designed and tested REST APIs using Swagger, enabling GET, POST, PATCH operations for internal/external Azure applications.
- Configured NuGet package sources for Health Check pipelines, managing API endpoints, versioning, environment variables, and database connections.
- Implemented Azure Logic Apps and integrated Azure Active Directory (AAD) for application access, resource groups, and role-based permissions.
- Created and managed APIM, App Service Gateways, Hybrid Connections, VNets, and Key Vaults for secure application deployments across Azure and AWS.
- Defined YAML alerts and auto-scaling policies for AWS services to ensure system reliability.
- Performed CentOS server patching (yum update) and managed administrative roles for servers and applications.
- Remediated OpenShift RBAC privilege escalation vulnerability where service accounts gained cluster-admin through improper role bindings, implementing automated RBAC auditing with OPA Gatekeeper policies and custom admission controllers
- Resolved OpenStack Barbican secret storage encryption key rotation causing service outages, implementing zero-downtime key migration using dual-encryption strategy and coordinating across 50+ integrated services
- Addressed CentOS cryptographic library vulnerability (OpenSSL CVE-2024-xxxx) affecting encrypted communications, performing emergency patching across 1000+ systems, validating certificate chains, and implementing runtime verification with AIDE
- Managed user access and roles in Azure Active Directory, enforcing security policies and application permissions.
- Built Health Check pipelines for CI/CD to proactively identify pipeline issues and failures.
- Created Service Bus pipelines to handle internal and external emails for GS1 applications.
- Developed SQL database CI/CD pipelines for ASP.NET applications, including artifact management and release deployment via Azure DevOps.
- Configured Kubernetes clusters, setting master nodes and managing cluster configuration files.
- Built database pipelines in Azure Data Factory using SSIS packages (.dtsx/.ispac) for deployment and automation.
- Automated Power BI report publishing: created .pbix templates, synced with Azure repos, managed data source credentials, and published to production App Workspace.
- Maintained JIRA for project tracking, defect management, and task updates.

Environment: Windows, Linux, Jenkins, Agile, Python, Apache Tomcat, Azure, Terraform, Kubernetes, Docker, Azure repository, Artifactory, SQL Client, Power BI, Active Directory, JIRA

Client: United Health group, Hartford, Connecticut **July 2017 – November 2018**
Role: DevOps/Azure Engineer

Responsibilities:

- Implemented Ansible to manage all existing servers and automate the build/configuration of new servers.

- Automated various infrastructure activities like Continuous Deployment, Application Server setup, Stack monitoring using Ansible playbooks and has Integrated Ansible with Jenkins.
- Created Inventory file for the ansible machine that has setup on the CentOS server to run playbooks
- Developed an Azure based high performance compute environment to support the massive computational requirements of client congressional redistricting Azure application.
- Developed installer scripts using Ant, Python for various products to be hosted on Application Servers.
- Automate Continuous Build and Deploy Scripts for Jenkins Continuous Integration tool using pipeline.
- Used kubernetesto deploy scale, load balance, scale and manage docker containers with multiple namespaced versions.
- Manage set of KubeletPods depending on the desired state of the cluster.
- Setting Kubelet pods for work together to implement a service mysql and Apache.
- Used Splunk to analyze data and also to monitor the health of the resources and also correlated the data over the entire stack.
- Used VSTS tool in order tocode, Build and Develop the overall operational environment of Infrastructure in Azure Portal.
- Created Ant build.xmls and Maven Pom.xml to automate the build process for the new projects and integrated them with third party tools like Sonar, Nexus.
- Installed and configured monitoring tools Nagios for monitoring the network bandwidth and the hard drives status.
- Integrated Docker container orchestration framework using Kubernetes by creating pods, Config Maps and deployments.
- Installed and managed Artifactory repository to deploy the artifacts generated by Maven and to store the dependent jars, which are used during the build.
- Worked on Artifactory repository to maintain artifacts and used as a local repository.
- Maintained JIRA for tracking and updating project defects and tasks.

Environment: Windows, Linux, JIRA, Bit Bucket, Jenkins, Agile, Git, UNIX, Perl, Python, XML, Apache Tomcat, JBOSS, Azure, Terraform, Kubernetes, Docker, Artifactory, SQL Client, Salt Stack, Salesforce, Active Directory.

Client: BCBS- Jersey City, NJ **June 2016 – June 2017**
Role: DevOps Engineer

Responsibilities:

- Developed AWS modules integrating S3, DynamoDB, RDS, Lambda, and SQS for automated workflows.
- Implemented EC2, S3, RDS, EBS, ELB, Auto Scaling and configured IAM roles, accounts, and policies.
- Automated operational tasks using Shell and Python scripts for backups, patching, REST APIs, and logging.
- Built optimized application packages with Java and configuration management.
- Administered Ansible for server provisioning, middleware installation (WebLogic, Tomcat), and role-based automation.
- Automated Docker container creation with Ansible and Jenkins; managed images via Docker Hub and Nexus.
- Orchestrated containers using Kubernetes, ensuring application resilience and uptime.
- Configured Jenkins Master-Slave architecture for CI/CD deployments to Tomcat and microservices.
- Used Splunk for automated incident management and improved system monitoring.
- Version controlled Dockerfiles, Ansible playbooks, and scripts using Bitbucket; maintained Nexus repository for artifact management.

Environment: Ansible, AWS, Jenkins, Git, Git Bash Python, Ruby, Shell, Batch, Maven, Ant, Docker, Nexus, SonarQube, Jira,
Nagios etc.

EDUCATION:

Master's in Information Assurance	Wilmington University	2018
Bachelor's in Electronics' and Communication Engineering	JNTUK	2014