**VISHNU VARDHAN P**

A blue hexagon with white text

Description automatically generatedA circular logo with a cloud in the center

Description automatically generatedA blue and white logo

Description automatically generated**Senior DevOps Engineer**

***Phone:*** ***682-777-5993***

***Mail:*** [**vishnupachva81@gmail.com**](mailto:vishnupachva81@gmail.com.m)

**PROFESSIONAL SUMMARY:**

* **12 years as a Cloud/DevOps Engineer** with deep expertise in **AWS, Azure, and GCP**, specializing in **CI/CD, Infrastructure as Code (IaC), automation, and Linux Systems Administration**.
* **Automated infrastructure deployment and management** using **Terraform and CloudFormation** in AWS, **Azure Resource Manager (ARM) Templates**, and **GCP Deployment Manager**—achieving consistency, faster provisioning, and eliminating configuration drift across environments.
* **Developed and managed CI/CD pipelines** with **Jenkins, GitLab, and Azure DevOps**, integrating **GCP Cloud Build** to automate build, test, and deployment processes, supporting continuous delivery with minimal manual intervention.
* **Skilled in security and identity management** with **AWS IAM, Azure Active Directory, and GCP IAM**—implementing **role-based access control (RBAC)**, multifactor authentication (MFA), and least privilege principles for enhanced security.
* **Managed Kubernetes clusters across AWS (EKS), Azure (AKS), and GCP (GKE)** for **container orchestration**, implementing **blue-green deployments, canary releases**, and **progressive delivery** strategies for high availability and zero-downtime releases.
* **Designed and deployed secure API management solutions** with **AWS API Gateway, Azure API Management, and GCP API Gateway**, ensuring seamless and secure communication between microservices and external clients.
* **Configured hybrid cloud networks** using **AWS VPC, Azure Virtual Network, and GCP VPC** and integrated **AWS Direct Connect, Azure ExpressRoute, and GCP Interconnect** for secure connectivity to on-premises environments.
* **Implemented SRE best practices** with **monitoring, alerting, and incident response systems** using **AWS CloudWatch, Prometheus, Grafana, and GCP Stackdriver**, creating detailed dashboards for real-time visibility into application health, performance, and error tracking.
* **Deployed advanced logging and monitoring solutions** with **ELK Stack, CloudTrail, and Azure Activity Logs**, capturing comprehensive event data and **setting up alerts for proactive incident management**.
* **Automated repetitive infrastructure tasks** with **Ansible, Puppet, and GCP Cloud Functions**, improving efficiency and maintaining a consistent, high-quality configuration across environments.
* **Enabled data encryption** with **AWS KMS, Azure Key Vault, and GCP Cloud KMS**, enforcing security compliance with industry standards for **data encryption at rest and in transit**.
* **Built hybrid cloud cost optimization solutions** using **AWS Cost Explorer, Azure Budgets, and GCP Cost Management**, achieving significant cost reductions and financial transparency.
* **Implemented disaster recovery and business continuity** solutions with **AWS Backup, Azure Site Recovery, and GCP Backup** to protect critical data and minimize recovery time in case of failure.
* **Created containerized applications and services** with **Docker and Kubernetes**, optimizing deployments with **Docker Swarm and Kubernetes orchestration** for scalability, reliability, and performance across multi-cloud environments.
* **Designed and managed microservices in Golang and Python**, creating high-performing, scalable applications integrated with **GCP, AWS, and Azure** cloud platforms for resilient and responsive architectures.
* **Configured and optimized load balancing solutions** using **AWS ELB, Azure Application Gateway, and GCP Load Balancer**, ensuring efficient traffic distribution and fault tolerance.
* **Enhanced security and compliance** through centralized **logging, auditing, and monitoring**, using **CloudTrail, ELK Stack, Azure Monitor, and GCP Logging** to maintain regulatory standards and enforce cloud security policies.
* **Integrated multi-cloud observability tools** like **Datadog, New Relic, Grafana**, and **GCP Monitoring** for **detailed insights and troubleshooting** across environments, ensuring optimal performance and reliability.
* **Optimized software deployment processes with Backstage.io**, streamlining workflows across AWS, Azure, and GCP, and enabling efficient, repeatable DevOps practices.

**TECHNICAL SKILLS:**

|  |  |
| --- | --- |
| Cloud Technologies: | AWS, Microsoft Azure, GCP |
| AWS Services & Tools: | EC2, Lambda, IAM, S3, Elastic Load Balancer (ELB), CloudFormation, Route 53, VPC, AWS CLI |
| Azure Services & Tools: | Virtual Machines, App Services, Blob Storage, Azure CLI, Azure Active Directory, Azure DevOps, Azure SQL Database |
| GCP (Google Cloud Platform) Services & Tools: | Compute Engine, Cloud Storage, Cloud SQL, Google Kubernetes Engine (GKE), BigQuery, Cloud Functions, Cloud IAM |
| Operating Systems: | Linux, Ubuntu, Windows, Red Hat Enterprise Linux (RHEL) |
| Scripting: | Bash, Python, Groovy, PowerShell, JavaScript |
| CI/CD Tools: | Jenkins, GitHub Actions, GitLab, CircleCI |
| Automation Tools: | Ansible, Terraform, AWS CloudFormation, Pulumi |
| Web/App Servers: | Apache Tomcat, Nginx |
| Containerization: | Docker, Kubernetes, ECS, EKS, OpenShift |
| Virtualization: | VMware, OpenStack |
| Infrastructure as Code: | Terraform, CloudFormation, Ansible |
| Monitoring Tools: | Splunk, CloudWatch, Datadog, Prometheus, Grafana |
| Networking: | DHCP, DNS, LAN, TCP/IP, HTTP/HTTPS |
| Databases: | MySQL, PostgreSQL, MongoDB, DynamoDB, Couchbase |
| SDLC Methodologies: | Agile, Scrum, Kanban |
| Project Management: | JIRA, Confluence, Azure DevOps Board |
| Source Control: | Git, BitBucket |
| Artifact Management: | JFrog Artifactory, Azure Artifacts |
| Build Automation Code Quality &Testing: | Selenium, Maven, Gradle, SonarQube, JaCoCo |
| IAM and Security Best Practices: | Access Controls, Encryption, AWS IAM policies, Multi-factor Authentication (MFA), Role-Based Access Control (RBAC), Security Compliance |

**CERTIFICATIONS:**

* **AZ-400: Designing and Implementing Microsoft DevOps Solutions**
* **Google Cloud Certified Professional Cloud Architect**
* **AWS Certified Solutions Architect**
* **AZ-104: Microsoft Azure Administrator**

**EDUCATION:**

Bachelors in Electronics and Communication Engineering from GITAM University, India.

**PROFESSIONAL EXPERIENCE:**

**Client: Macquarie / Houston, Texas Sep/2021 to till date.**

**Role: Sr. DevOps Engineer**

**Responsibilities:**

* Implemented and maintained CI/CD pipelines using **Jenkins**, **Ansible**, and **Terraform** for streamlined, automated deployment across environments, ensuring seamless code promotion from development to production.
* Architected and managed **AWS Kubernetes** clusters for containerized applications, enhancing scalability and reliability of critical services.
* Automated infrastructure provisioning using **Terraform** for **AWS** resources (EC2, VPC, RDS, S3), ensuring consistency and repeatability.
* Implemented robust **monitoring** and **logging solutions** with **Prometheus**, **Grafana**, and **ELK Stack**, proactively identifying and resolving system issues to improve application performance.
* Automated configuration management with **Ansible**, streamlining the setup and management of cloud environments by efficiently managing instances, networks, and security groups.
* Standardized microservices deployment through **Docker** containers, simplifying deployment from development to production stages.
* Optimized performance and reduced operational overhead for serverless applications using **AWS Lambda**, **S3**, and **CloudFront**.
* Led on-premise to **cloud migration initiatives** (AWS, GCP), including **Dockerizing** legacy applications and managing deployments with **Kubernetes** for improved scalability and cost-effectiveness.
* Configured **Redis Cache** on AWS, enhancing application responsiveness and reducing latency.
* Developed automated **backup** and **disaster recovery plans** with AWS RDS and S3 to support business continuity.
* Automated builds and deployments in **Kubernetes** with **Jenkins X**, ensuring reliable, fast delivery pipelines.
* Centralized **logging** and **monitoring for Kubernetes** using **Fluentd** and **Prometheus**, providing real-time insights into performance and system health.
* Leveraged **cloud-native monitoring tools** to enhance visibility into application performance and quickly respond to issues.
* Implemented **automated testing** in the **CI/CD pipeline** to ensure quality and performance benchmarks are met before deployment.
* Engaged with the **Kubernetes community** to stay updated on best practices and emerging trends, enhancing team capabilities.
* Developed workflows for **automated scaling** of applications in **GKE** based on performance metrics and demand.
* Promoted a culture of collaboration and knowledge sharing within the team, facilitating a smooth transition to **GKE** and **DevOps practices**.
* Automated **server provisioning** and configuration through **Ansible** playbooks to ensure consistency across development, staging, and production.
* Simplified **Kubernetes deployments** with **Helm charts** for easy packaging and distribution of applications.
* Enabled **AWS CloudWatch** for real-time monitoring and alerting, setting up custom metrics and alarms to track application health.
* Demonstrated **expertise** in deploying, managing, and optimizing **containerized applications** using **GKE**, ensuring **high availability** and **scalability**.
* Deep understanding of **Kubernetes architecture**, including **Pods**, **Deployments**, **Services**, and **Persistent Volumes**, facilitating seamless **application orchestration**.
* Leveraged **Google Cloud Platform (GCP)** services to enhance **GKE** capabilities, optimizing **cloud resources** for improved application performance and cost-effectiveness.
* Managed **incident response** processes using tools like **ServiceNow**, ensuring timely resolution of **production issues** and maintaining **service reliability**.
* Provided 24/7 **production support** for critical applications running on **GKE**, implementing **monitoring** and **alerting strategies** to proactively address system anomalies.
* Developed and maintained **Ansible playbooks** for automated **configuration management**, improving **deployment speed** and consistency across environments.
* Implemented best practices for **containerization**, including **image optimization** and **security hardening**, to enhance application performance and security.
* Configured and managed **Kubernetes networking**, including **Ingress controllers** and **service meshes**, to enable seamless communication between microservices.
* Designed and implemented **CI/CD pipelines** for **GKE** using tools like **Jenkins** and **GitLab CI**, streamlining the deployment process and reducing time to market.
* Monitored and optimized **resource utilization** on **GKE**, ensuring efficient use of **CPU** and **memory resources** to improve application responsiveness.

**Environment:** GIT, AWS (Lambda, S3, EC2, RDS, CloudFront, CloudWatch, VPC), **Jenkins**, **Ansible**, **Terraform**, **Kubernetes**, **Docker**, **Helm**, **Redis Cache**, **Fluentd**, **Prometheus**, **Grafana**, **ELK Stack**, **Couchbase**, **NGINX**, **GCP**, **Azure**, Security Groups.

**Client: GE Healthcare/ Waukesha, Wisconsin (Remote) April/2019 to Aug/2021**

**Role: Sr Azure Cloud DevOps Engineer**

**Responsibilities:**

* Implemented **Azure Virtual Appliances** for security, covering **firewall** and **intrusion detection**, ensuring robust protection of cloud-based infrastructure against unauthorized access and malicious activities.
* Established **Azure Virtual Appliances** for enhanced security in **healthcare systems**, ensuring the protection of patient data and compliance with healthcare industry regulations such as **HIPAA**.
* Established **TFS VNext Build agents** and seamlessly integrated **TeamCity** and **Octopus** build tools with TFS, enabling smooth build processes and collaboration between teams working on healthcare software solutions.
* Developed **automation scripts** (Bash, Ruby, Python, PowerShell) and applied **ANT/Maven** for Java code releases, automating critical release tasks for medical applications, improving efficiency and reliability in deploying healthcare solutions.
* Managed **Azure AD** identities, security groups, roles, and **App registrations**, including **SAML SSO**, ensuring secure access control for healthcare professionals accessing cloud-based healthcare systems and services.
* Applied **database indexing** and **query optimization** best practices, significantly improving the performance of healthcare applications, reducing response times, and ensuring efficient access to critical patient information.
* Developed and maintained **CI/CD pipelines** for **microservices architectures** in healthcare solutions, ensuring seamless integration, deployment, and management of services that support healthcare applications across multiple environments.
* Automated infrastructure provisioning using **Infrastructure as Code (IaC)** tools, creating consistent, reproducible environments for healthcare software systems, reducing configuration errors, and ensuring high availability.
* Configured continuous **monitoring** and **alerting** for healthcare production systems, ensuring proactive identification of issues to maintain uptime for critical healthcare services, improving patient outcomes through reliable access to data.
* Led the migration of legacy healthcare applications to modern **cloud-based architectures**, significantly enhancing performance, scalability, and security, and ensuring compliance with healthcare standards.
* Provided technical leadership to cross-functional teams in **DevOps best practices** within healthcare environments, fostering collaboration to improve software delivery for healthcare applications and services.
* Implemented **encryption** and **access control** measures to safeguard sensitive healthcare information, ensuring data confidentiality, integrity, and compliance with healthcare industry security regulations.
* Collaborated with healthcare stakeholders to define and prioritize technical requirements, aligning the development of healthcare solutions with the needs of medical professionals and regulatory requirements.
* Utilized **Helm** to manage **Kubernetes deployments**, simplifying the management of complex healthcare applications running in Kubernetes environments, ensuring scalability and efficient resource utilization.
* Utilized **JIRA** for managing **bug tracking**, sprint planning, and storyboarding in the development of healthcare applications, ensuring clear visibility and traceability of project progress.
* Designed **data models** and **schemas** on **SQL Azure** and deployed healthcare mobile applications on Azure cloud, leveraging Azure services for secure and scalable data storage and application deployment.
* Trained teams on using **JIRA** effectively for managing healthcare projects, contributing to improved collaboration and tracking of healthcare solution development and deployment.
* Integrated automated **testing procedures** into the **CI/CD pipelines** on **TeamCity**, improving the quality assurance process for healthcare code releases and minimizing risks in production environments critical to healthcare operations.
* Expanded the use of **Kubernetes** for container orchestration in healthcare applications, enhancing scalability and resource management, optimizing the performance of containerized workloads supporting healthcare services.
* Implemented cost optimization strategies within **Microsoft Azure**, **AWS**, and **GCP** cloud environments for healthcare systems, ensuring efficient resource allocation while managing cloud costs to fit healthcare budgets.
* Configured and managed resources using **Google Cloud Console**, **Cloud Shell**, and **Cloud SDK**, supporting healthcare applications and ensuring the efficient management of cloud resources.
* Utilized **GCP tools** like **Compute Engine**, **Cloud Storage**, and **Cloud SQL** for healthcare infrastructure provisioning and data storage, ensuring scalable, secure, and reliable environments for critical healthcare data.
* Implemented **container orchestration** using **Google Kubernetes Engine (GKE)** for managing Docker containers running healthcare services, ensuring scalability and resilience in cloud-based healthcare applications.
* Set up **monitoring** and **logging** for GCP resources using **Stackdriver** to maintain visibility into healthcare systems and ensure the reliability of cloud-based healthcare applications.
* Leveraged **Google Cloud Deployment Manager** for **IaC** and automation in healthcare systems, automating infrastructure provisioning and configuration to ensure reproducibility and compliance with healthcare standards.

**Environment:** Azure, GCP, AWS, **Jenkins**, **JIRA**, **TeamCity**, **Octopus**, **Docker**, **Kubernetes**, **Helm**, Bash, Ruby, Python, PowerShell, **Maven**, **CI/CD**, **IaC** tools, **Stackdriver**.

**Client: JLL Technologies (Remote) June/2017 to Mar/2019**

**Role: AWS DevOps Engineer**

**Responsibilities:**

* Implemented **AWS cloud services** including **EC2, S3, RDS, ELB, EBS, VPC, Route53, Auto Scaling groups, CloudWatch, CloudFront**, and **IAM**, facilitating server migration from physical to cloud environments.
* Developed comprehensive **architectural diagrams** for applications pre-transition, ensuring adherence to principles of **flexibility, cost-effectiveness, reliability, scalability, high performance**, and **security**.
* Managed **IAM accounts** and policies on AWS and demonstrated familiarity with **GCP security measures** such as **Identity and Access Management (IAM)**, **Cloud Identity**, **Cloud Armor**, and **Security Command Centre**.
* Developed **RESTful APIs** with a focus on **security** and **scalability** for efficient data exchange between systems.
* Engaged in **troubleshooting** and **performance tuning** of applications, resolving critical issues, optimizing performance, and improving application reliability.
* Designed scalable, robust **system architectures** in collaboration with software architects to meet business requirements.
* Integrated **third-party APIs** and services into applications to enhance functionality and expand software capabilities.
* Implemented **logging** and **monitoring solutions** using the **ELK Stack** for visibility into application performance and system health.
* Advocated and implemented **DevOps best practices**, driving **automation** and improving deployment processes.
* Created and managed **Ansible templates** for application and environment management, and developed **Docker containers** for application lifecycle management.
* Utilized **Terraform** extensively for **infrastructure provisioning** and management, ensuring consistency and scalability.
* Managed **mainframe integration** and data exchange within cloud infrastructure, ensuring compatibility between mainframe systems and cloud solutions.
* Participated in **disaster recovery planning** and execution using **AWS Backup**, **Azure Site Recovery**, and GCP tools like **Google Cloud Backup**.
* Established **backup** and **disaster recovery** strategies for **GKE** workloads, ensuring data integrity and availability in case of failures.
* Enforced **security best practices** in **GKE** environments, including **role-based access control (RBAC)** and **network policies**, to safeguard applications.
* Conducted **performance tuning** of **Kubernetes clusters** to enhance application responsiveness and reliability under varying workloads.
* Worked closely with **development teams** to facilitate the adoption of containerization and **GKE**, promoting a **DevOps culture** and best practices.
* Implemented centralized **monitoring** and **logging solutions** using tools like **Prometheus** and **Grafana** to gain insights into system health and performance.
* Conducted **incident response drills** to test and refine incident management processes, ensuring the team's preparedness for real-world scenarios.
* Created and maintained **documentation** for **GKE processes**, configurations, and incident management protocols, ensuring knowledge sharing across teams.
* Analyzed **incident trends** to identify root causes and implement preventive measures, reducing incident recurrence and improving system reliability.
* Engaged in **continuous improvement** initiatives to enhance **GKE operational efficiency** and reduce manual intervention in workflows.
* Integrated **security scanning tools** into the **CI/CD pipeline** to ensure compliance with security standards and identify vulnerabilities in container images.
* Assisted in the **migration** of legacy applications to **GKE**, optimizing performance and scalability while minimizing downtime.
* Participated in **architecture design reviews** to ensure best practices for **GKE deployments** and adherence to organizational standards.
* Utilized **Helm** for managing **Kubernetes applications**, simplifying deployment and version management of microservices on **GKE**.
* Conducted **training sessions** for team members on **GKE best practices** and incident management tools to enhance team capabilities.
* Collaborated with stakeholders to define **service level objectives (SLOs)** and **service level indicators (SLIs)** for **GKE applications**, ensuring alignment with business goals.

**Environment:** AWS (EC2, S3, RDS, ELB, VPC, IAM), GCP (Compute Engine, GKE, Cloud SQL), Jenkins, Ansible, Docker, Kubernetes, ELK Stack, Terraform, Git/SVN, Maven, JIRA, Grafana, Nagios, CloudFormation, DevOps CI/CD.

**Client: Paycom, Oklahoma, OK Oct /2013 to May/2017**

**Role: DevOps Engineer**

**Responsibilities:**

* Established the **AWS Virtual Private Cloud (VPC)** network, ensuring secure communication between installed instances, and configured **Security Groups** and **Elastic IPs** to enforce access controls and facilitate seamless connectivity.
* Established the **Google Cloud Virtual Private Cloud (VPC)** network, ensuring secure communication between instances, and configured **Firewall Rules** and **Cloud VPN** to enforce access controls and facilitate seamless connectivity.
* Demonstrated proficiency in various **GCP services**, including **Compute Engine**, **Cloud Storage**, **Cloud SQL**, **Pub/Sub**, **Cloud Functions**, and **Google Kubernetes Engine (GKE)**.
* Leveraged **Docker** technology for portable application deployment, ensuring consistent execution across environments in GCP and AWS.
* Monitored **Cloud SQL** and **GCP Load Balancer** configurations to ensure optimal performance, availability, and scalability of cloud infrastructure.
* Administered **Jenkins** for continuous integration, orchestrating automated application packaging and deployment processes.
* Utilized Docker and Kubernetes technologies to manage **microservices architecture**, developing **CI/CD** pipelines for containerized applications.
* Created Docker images with **Dockerfiles**, leveraging snapshots and volumes for efficient management of application dependencies.
* Utilized **Terraform** for **infrastructure as code (IaC)** to provision and manage **GKE clusters** and associated resources efficiently.
* Monitored **Kubernetes cluster health** and performance metrics, proactively identifying and addressing potential issues before they impact users.
* Worked with **cloud networking teams** to ensure proper configuration of **VPCs** and **subnets** for **GKE deployments**, optimizing network performance and security.
* Managed **GKE cluster upgrades** and maintenance, ensuring minimal disruption to services and compliance with industry standards.
* Implemented **application performance monitoring (APM)** solutions to track and analyze application performance metrics within **GKE**.
* Developed custom monitoring solutions to meet specific application needs, enhancing visibility into application behavior and resource utilization.
* Engaged in **post-incident reviews** to analyze failures and identify opportunities for improvement in processes and technology.
* Collaborated with **security teams** to conduct regular audits and assessments of **GKE environments**, ensuring compliance with security policies.
* Contributed to the development of internal tools for **monitoring** and managing **GKE environments**, enhancing operational efficiency.
* Assisted in the development and execution of **disaster recovery drills** for **GKE workloads**, validating the effectiveness of backup strategies.
* Collaborated closely with stakeholders to ensure alignment of DevOps initiatives with business objectives.
* Committed to quality and excellence, adhering to industry best practices and organizational policies.
* Fostered a positive and collaborative work culture, promoting open communication and teamwork.

**Environments:** GCP (Compute Engine, Cloud SQL, GKE), AWS (EC2, S3), Jenkins, Docker, Kubernetes, Terraform, Ansible, Python, Grafana, Splunk.

**Client: Atos-Syntel / India May/2012 to Sep /2013**

**Role: DevOps Engineer / Build and Release Engineer**

**Responsibilities:**

* Managed **bare metal infrastructure**, ensuring optimal performance and reliability for enterprise-level deployments.
* Automated provisioning and maintenance of **bare metal servers**, streamlining resource allocation and reducing manual effort.
* Developed custom **scripting solutions** for automating Linux system configurations, enhancing system efficiency.
* Implemented automated workflows for **Linux systems** using **bash, Python,** and **PowerShell** to minimize downtime and streamline operations.
* Configured and managed **Chef** to automate system configurations and enforce infrastructure consistency.
* Created and optimized **Chef cookbooks** for scalable deployment across Linux environments.
* Designed and maintained **Elasticsearch clusters**, ensuring high availability and efficient search capabilities.
* Tuned **Elasticsearch indices** to optimize query performance and data ingestion rates for real-time analytics.
* Deployed and managed **MaaS (Metal as a Service)** to streamline provisioning of bare metal resources in dynamic environments.
* Integrated **NetBox** for IP address management and data center infrastructure tracking, ensuring accurate inventory and documentation.
* Automated **Linux patch management** and system updates, reducing vulnerabilities and ensuring compliance.
* Built and deployed **monitoring scripts** for Linux systems to proactively identify and resolve performance issues.
* Designed robust **backup and recovery strategies** for bare metal systems to ensure data integrity and availability.
* Collaborated with cross-functional teams to optimize bare metal infrastructure for diverse application needs.
* Configured advanced **network settings** for bare metal environments, enhancing connectivity and security.
* Implemented **infrastructure as code (IaC)** practices using **Chef** for consistent and repeatable deployments.
* Conducted performance tuning for **Linux servers**, optimizing hardware utilization and improving processing speeds.
* Used **Elasticsearch APIs** to develop custom dashboards and reporting tools for operational insights.
* Managed server inventory and capacity planning using **NetBox**, improving infrastructure scalability.
* Conducted troubleshooting and root cause analysis for bare metal hardware and Linux system issues, ensuring rapid resolution and system reliability.

**Environment:** Git, Jenkins, Ansible, Docker, ELK Stack, SonarQube, AWS, Azure, Java, Ruby, Gradle, Apache Tomcat, Nginx, Linux (Ubuntu, RHEL), Windows, MySQL, PostgreSQL, MongoDB, TCP/IP.