RAJA ALETI
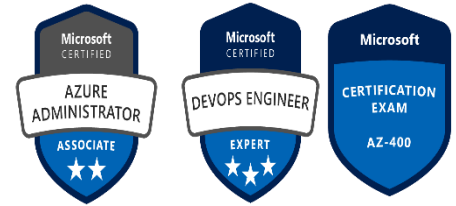
☎ (972) 325-8344

✉ rajaa2080@outlook.com

PROFESSIONAL SUMMARY

Cloud Infrastructure and DevOps Engineer with hands-on experience designing, automating, and operating scalable infrastructure across **both Azure and AWS cloud platforms**, including S3, Glue, and EMR. Specialized in Infrastructure as Code (IaC) using **Terraform, ARM templates, and CloudFormation**, ensuring consistent deployments across multi-cloud environments.

- Proficient in **Administrating Azure IaaS/PaaS Services** like **Compute Azure Virtual Machines, Web, and Worker roles, VNET, Network Services, Azure DevOps, SQL Databases, Storages, Azure Active Directory, Monitoring, Auto scaling, PowerShell Automation, Azure Search, DNS, VPN**.
- Implement automation tools such as **Azure PowerShell, Terraform, and ARM templates** to streamline network management, seamlessly integrating with various Azure services to enhance overall operational efficiency.
- Strong experience in container orchestration with **Kubernetes** on **Azure AKS** and **AWS EKS**, leveraging **Helm**, **GitOps (Argo CD)**, and CI/CD pipelines.
- Leveraged **Argo CD & Spacelift** for **automated deployments of AKS, API services, and network resources**, integrating **Terraform execution policies and compliance enforcement**.
- Ability in deploying Microservices, their application improvement and upgradation using Azure administrations like Azure DevOps, **Kubernetes Service (AKS),** Container Services, **MySQL DB**, Grafana, Azure pipelines, RBAC, and Checking Groups.
- Managed **Azure Kubernetes Service (AKS) & AWS Elastic Kubernetes Service (EKS)** clusters, optimized **networking, scaling policies**, and **automated deployments** using **Helm, ArgoCD, and Kubernetes Operators**. Implemented **Kubernetes RBAC, Pod Security Policies (PSP), and Istio-based service mesh**.
- Experience in writing Infrastructure as a code (IaaC) in **Terraform, Azure resource management, and AWS Cloud formation. Created reusable Terraform modules in both Azure and AWS cloud environments.**
- Deployed Kubernetes clusters on **AWS**, creating services using **YAML** (pods, deployments, auto-scaling, health checks, namespaces) and integrated with **EMR**, **Glue**, and **S3** for analytics and storage.
- Configured AWS messaging and database services including **SNS**, **SQS**, **SES**, **Pinpoint**, **Aurora**, **RDS**, **DynamoDB**, and **Redshift** to support event-driven and scalable application architecture.
- Designed and automated **Azure networking** solutions using **Traffic Manager**, **Application Gateway**, **DNS**, **Network Watcher**, **ExpressRoute**, and **NSGs**, ensuring secure, resilient connectivity across hybrid cloud environments.
- Automated cloud infrastructure using **PowerShell**, **Python**, **Terraform**, and **CloudFormation,** including converting AWS workloads to **serverless architecture** with **Lambda** and fine-tuning Azure load distribution for fault tolerance.
- Deploy **Azure Network Watcher** for proactive **monitoring and diagnostics**, ensuring consistent best performance across the network.
- Ability in using **Docker Hub, Docker Engine, Docker images, Docker Weave, Docker Compose, Docker Swarm, and Docker Registry** and used containerization to make applications platform when moved into different environments.
- Ability in configuring the monitoring and alerting tools according to the requirement like **Prometheus and Grafana** setting up alerts and deploying multiple dashboards for individual applications in **Kubernetes**.
- Governance and compliance experience with **Azure Policy, EPAC, Secure Score, and AWS equivalents (e.g., AWS Config, Trusted Advisor) for audit readiness (CIS, NIST, ISO**).
- Applied **SRE principles** such as **SLIs/SLOs**, **incident response**, **RCA**, and **chaos testing** to enhance system reliability, while managing operations and escalations using tools like **JIRA** and **ServiceNow**.
- Skilled in implementing end-to-end **observability solutions** using tools like **Prometheus**, **Grafana**, **Azure Monitor**, **AWS CloudWatch**, **Splunk**, **ELK**, and **Nagios**, with experience resolving system bottlenecks through **recording rules**, aggregation strategies, and log-based analysis.
- Well versed with **Software development life cycle (SDLC)**, **Software Test life cycle (STLC)**, and Bug life cycle and worked with testing methodologies like Waterfall and Agile (SCRUM).

Technical Skills:

Cloud Services	Azure, AWS
Infrastructure Management Tools	Terraform, ARM Templates, Cloud Formation

Configuration Management Tools	Ansible, Chef
CI/CD Tools	Jenkins, Azure DevOps, GitHub Actions, Spacelift
Build Tools	Maven, Gradle, Ant
Container Orchestration Tools	Docker, Kubernetes, Docker Swarm
Version-Control Tools	GIT, GitHub, Azure Repo, Bit Bucket
Monitoring Tools	ELK, Cloud watch, Splunk, Grafana, Data dog
Scripting	Python, Shell, PowerShell, Json, YAML
Identity & Access Management (IAM)	Azure AD, Entra ID, PIM, Conditional Access, RBAC policy automation.
Networking	TCP/IP, DHCP, DNS, SNMP, SMTP, Ethernet, NFS
Bug Tracking Tools	Bugzilla, JIRA, ServiceNow
Operating Systems	Ubuntu, CentOS, Red hat, Linux, Windows.
Governance & Compliance	Azure Policy, EPAC (Enterprise Policy as Code), Secure Score optimization, audit readiness for CIS, NIST, ISO
Languages	Java, SQL, HTML, JavaScript, XML

EXPERIENCE:

Client: Starbucks, WA ||**TEKsystems**	. May 2024– Present
Sr. Cloud DevOps Engineer	

Key Responsibilities:

- Designed and deployed **multi-cloud infrastructure** with a **70% Azure** and **30% AWS** footprint using **Terraform modules** and **Sentinel/EPAC** policy enforcement.
- **Designed cost optimization** using **Azure Cost Management** and **Azure Advisor**, identifying underutilized resources, implementing cost-saving recommendations, and automating deprovisioning of unused resources to reduce cloud expenditure.
- Automated **RBAC** and **IAM** policy enforcement across **Azure** and **AWS** using **API-driven** methods, implementing **PoLP** role assignments; managed identity lifecycle with **Azure AD**, **Entra ID**, **PIM**, and **MFA**, while enforcing compliance with **CIS benchmarks** and documenting audit workflows to support regulatory readiness and third-party assessments.
- **Reviewed and validated customer requests** for non-production and production environments through **Verde**, ensuring compliance with required configurations (including **VMware workloads migrated to Azure** and **Azure Stack HCI**) and organizational standards.
- **Developed and validated EPAC (Enterprise Policy as Code)** policies, enforcing governance, security compliance, and automation-driven infrastructure standardization across cloud environments.
- Developed and implemented **network APIs** for both **Azure VNETs** and **AWS VPCs**, automating **peering**, **route tables**, and **security group** configurations.
- **Created reusable Terraform modules** with **Go tests** and **Terraform tests**, targeting sandbox, non-prod, and production environments, ensuring robust infrastructure-as-code deployments, modularization, and reusability.
- **Automated Code Owner assignments** across multiple **GitHub organizations** using **Python scripts** and **GitHub APIs**, dynamically updating **CODEOWNERS** files to ensure proper repository ownership, streamlined code reviews, and CI/CD compliance.
- **Managed Kubernetes clusters across Azure AKS and AWS EKS**, deploying services using Helm and Argo CD, and enabling GitOps across cloud boundaries.
- Implemented **GitOps workflows** and unified **CI/CD pipelines** across **Azure** and **AWS** using **Argo CD**, **Spacelift**, and **GitHub Actions**, enabling version-controlled infrastructure updates and seamless integration with **SonarQube** and **Artifactory** for secure, automated deployments.

- **Automated operations with PowerShell and Python across Azure and AWS**, including subscription/account management, resource cleanup, and infrastructure provisioning.
- **Integrated REST APIs** and used **Postman** for cloud resource validation, API security testing, and automation-driven monitoring to ensure policy compliance.
- **Managed hybrid cloud infrastructure across Azure (AKS, Landing Zones) and AWS (EKS, VPCs)**, ensuring compliance, scalability, and operational continuity.
- Implemented centralized logging by deploying agents and configuring **Azure Monitor**, **Diagnostic Settings**, **Log Analytics**, and **AWS CloudWatch**, with unified log ingestion into **Splunk** and **Dynatrace** via **Event Hub** integrations.
- Architected **scalable cloud infrastructure** for **GenBI analytics**, ensuring **high availability** and **low-latency** processing; enabled **hybrid deployments** with **VPC/VNet integration** to support **data federation** across analytics platforms.
- **Led incident response and troubleshooting** for Azure cloud environments, diagnosing network, computing, and storage issues, and collaborating with support teams for fast resolution.
- **Worked in an ITSM environment** using **ServiceNow** to manage change requests, incidents, and problems in accordance with **ITIL-aligned processes**.

Client: Fisher Investments, CA ||**TEKsystems**	.
Sr. Cloud Infrastructure Engineer	May 2022 – April 2024

Key Responsibilities:

- Led cloud infrastructure projects with **70% focus on Azure** and **30% on AWS**, designing scalable solutions using **Terraform** modules for virtual networks, scale sets, and application gateways.
- Designed backup and disaster recovery strategies using **Azure Site Recovery** and **Azure Backup**; incorporated **AWS S3** snapshots and lifecycle policies for secondary workloads.
- Applied **Azure Security Center** recommends improving Secure Score and hardening workloads across all environments.
- Designed and Architecture for multiple subscriptions in **Azure** and involved with the Network team in setting connection from online to multiple **VNETs** (with peering and custom routing) using **Azure** through **VNet Peering**.
- Engineered cohesive workflows by integrating **SonarQube** and **JFrog Artifactory** into GitHub repositories, ensuring consistent code quality analysis, secure artifact management, and collaborative development practices.
- Implemented **CI/CD pipelines** using **GitHub Actions** with **Azure** as the primary deployment target, and integrated **SonarQube** and **Artifactory** for cross-cloud artifact management.
- Developed reusable **Terraform modules** with integrated **Go** and **Terraform tests** for multi-environment deployments; enforced governance using **EPAC**, **Azure Policy**, and **Sentinel**.
- Automated **Azure VM provisioning**, subscription management, and agent setup using **PowerShell**, and validated **AWS infrastructure** with **Python scripts**; also developed custom scripts for complex Windows configurations.
- Managed **Azure DevOps pipelines** for build, test, and deployment workflows, integrating testing strategies to improve code quality and early issue detection; used **Azure Container Registry** to store and manage private Docker images.
- Implemented versioning and state-locking mechanisms to ensure the reliability and integrity of the **Cloud infrastructure** deployment process.
- Deployed **Dynatrace** for real-time application insights, **Splunk** for log analysis, and **Grafana** for dynamic dashboards.
- Supported secure deployment strategies (blue/green, canary) with built-in monitoring and rollback using **Azure DevOps** and **Application Gateway WAF policies**.
- Configured **Azure Monitor** and **Log Analytics** to capture telemetry and logs from **VMs**, **databases**, and **apps**, enabling proactive, log-based monitoring and troubleshooting within a **DevSecOps** strategy.
- Designed and implemented **data lake architecture** using **AWS S3**, **EMR**, and **Glue** for scalable ETL and analytics; collaborated with DevSecOps to enforce security via **Azure Policy**, **EPAC**, and **AWS Config**, and aligned **SLIs/SLOs** with business goals using **Prometheus**, **Grafana**, and **Azure Monitor**.
- Participated in **incident response** and **postmortem analysis**, identifying root causes and writing **RCAs**, while driving improvements through **self-healing automation** triggered by alerts/log anomalies and conducting **chaos testing** to enhance infrastructure **resilience**.

Verizon, Cary, NC, USA	**Duration:**
Azure Cloud Infrastructure Engineer	**Dec 2020 – May 2022**

Key Responsibilities:

- Designed and provisioned **Azure resources** such as **Computing**, **Networking**, and **Application Gateway** while maintaining dev, test, staging, and production environments using **ARM templates**.
- Created **Azure Infrastructure** using **ARM templates** and **Azure Pipelines** to build, test, release, and manage **Azure Container Registry** to store private Docker images deployed to **Grafana** for collecting metrics and logs.
- Configured **Azure App Services**, **Azure App Service Environment**, **Azure Function App**, **Azure Application Insights**, **Azure Application Gateway**, and **Azure DNS**, using **ARM templates** and **Azure DevOps YAML pipelines**.
- Created **CI/CD pipelines** for **.NET**, **Node.js**, and **Python** apps in **Azure DevOps** by integrating with **GitHub**, **VSTS**, and **Artifacts**.
- Orchestrated effective release management strategies within **Azure DevOps**, including deployment and rollback procedures, resulting in smooth and reliable software releases.
- Integrated testing strategies into **Azure DevOps pipelines**, enhancing code quality and enabling early issue identification.
- Created dashboards in **Azure DevOps** for CI/CD pipelines, work items, and bugs, identified and logged defects, and interacted with developers to prioritize issues.
- Configured **Azure Role-Based Access Control (RBAC)** to enforce granular access management, segregate duties, and ensure least privilege principle for all users.
- Worked on **Site-to-Site & Point-to-Site VPNs**, **Virtual Networks**, **NSGs**, **Load Balancers**, and **Storage Accounts**, configuring RBAC and **Azure Monitor** to enhance security posture.
- Automated creation of **NSGs** with **PowerShell**, managing inbound/outbound rules and subnet/NIC associations; configured **Azure Key Vault** for secure storage of secrets and certificates. Also designed **Automation Accounts** with Runbooks and migrated on-prem **Active Directory** to **Azure AD** using **AD Connect**.
- Worked on **Azure Site Recovery (ASR)** to migrate on-prem physical servers and VMware to Azure and implement disaster recovery strategies.
- Created and managed **Azure Kubernetes Service (AKS)** clusters with deployment areas for dev, QA, and production, and configured **App Insights**, **Prometheus**, and **Grafana** dashboards for observability.
- Managed Kubernetes charts using **Helm**, created reproducible builds, and maintained Helm package versions for deployments.
- Implemented containerized applications on **AKS**, deploying apps through Kubernetes clusters with ingress API Gateway, **MySQL**, **Cosmos DB**, and configured **Nginx** reverse proxy for traffic routing.
- Developed **Ansible playbooks**, inventories, and custom roles in **YAML**, utilizing **Ansible Vault** for secrets management and **Ansible Tower** for access control; implemented orchestration to automate multi-server deployments and application rollouts across client environments.
- Created and configured **Azure Functions** with **HTTP triggers**, integrated with **App Insights** for monitoring, and performed load testing via **Azure DevOps** to validate performance under real-world conditions.
- Provisioned **Azure infrastructure** using **Terraform** and **ARM templates**, ensuring consistent, version-controlled deployments across dev, test, and prod environments; visualized execution plans using **Terraform Graph**.
- Implemented **DevSecOps** practices with **Azure Log Analytics**, security auditing, and continuous monitoring to enhance compliance, detect anomalies, and proactively prevent vulnerabilities.

| Mastercard, St. Louis, USA | Duration: |
| AWS Cloud Engineer | Nov 2018 – Nov 2020 |

:

Key Responsibilities:
- Used **S3 buckets** to store data across regions for backup, restore, and disaster recovery purposes.
- Written custom scripts using the **shell** to automate the Backup and DR process for applications running in the **EKS clusters**.
- Automated deployment of a **WordPress** environment on **AWS** using **Terraform** and **Ansible**, provisioning custom **VPC**, **EC2**, **RDS**, **S3**, **ELB**, **ASG**, **Route53**, and secure networking components.
- Provisioned **EKS clusters** using **Terraform**, developed reusable **IAM modules**, and integrated roles with **Kubernetes service accounts**; managed workloads using **EBS**, **EFS**, **RDS Aurora**, and services like **S3**, **EFS**, **EKS**, and **ECS** to support both shared and unshared storage needs in Kubernetes.
- Deployed and managed **Kubernetes clusters** on cloud platforms, using **YAML manifests** to configure **pods**, **deployments**, **auto-scaling**, and **load balancers**; managed Helm charts for both custom and third-party applications.

- Automated Helm-based deployments to **EKS** using **Jenkins pipelines**, enabling continuous delivery of containerized workloads across clusters.
- Experience in managing software artifacts required for development using repository managers like **Nexus** and **JFrog Artifactory** and writing **Jenkins Pipeline** scripts for Continuous Integration (CI) and built workflows also used Jenkins for uploading Artifacts into Nexus Repository.
- Designed end-to-end CI/CD workflows with **AWS CodePipeline**, automating source code integration, testing, and deployment for rapid and reliable application releases.
- Implemented and maintained CI environments using **Jenkins**, performing deployments, Packaging, build optimization, production rollouts, staging, defect tracking (**JIRA**) and root cause analysis.
- Used **Datadog** to create dashboards for different applications and **AWS accounts** to get real-time metrics for services like Kubernetes workloads by deploying Datadog agents in the **EKS cluster**.

Trammel Crow Company (TCC), Raleigh, NC, USA	Duration:
Aws DevOps Engineer	**Oct 2017 – Oct 2018**

Key Responsibilities:
- Used **S3 buckets** to store data across regions for backup, restore, and disaster recovery purposes. Monitored and fine-tune Java applications for optimal execution on **AWS**.
- Written custom scripts using the **shell** to automate the Backup and DR process for applications running in the **EKS clusters**.
- Created a **WordPress environment** on **AWS** using **Terraform** and **Ansible**, which consists of custom **VPC**, **S3**, **RDS**, **EC2**, Public and Private subnets, Security Groups, Auto Scaling Groups, ELB, and Route53.
- Implemented IAM configurations in disaster recovery plans within **CloudFormation templates** and ensured that access management remains consistent across different environments.
- Used **Terraform** in **AWS Virtual Private Cloud** to automatically set up and modify settings by interfacing with the control layer.
- Used **Terraform** for Infrastructure as code to deploy **EKS clusters** and spin up an agent to access the cluster. Created many **AWS services** using Terraform to automate the process for higher environments.
- Developed many **Terraform modules** to create **IAM roles** and policies for different third-party applications and used **Kubernetes service accounts** to use the roles.
- Worked on different **AWS services** like **S3**, Route53, EFS, EKS, and ECS to manage and maintain the workloads in the **EKS cluster**. Used different storage services like **EBS volumes**, **EFS** and **RDS Aurora** in a Kubernetes application as shared and un-shared storage classes.
- I wrote many **Ansible playbooks** which are the entry point for Ansible provisioning, where the automation is defined through tasks using **YAML format**. Run Ansible Scripts to provision Dev servers.
- Implemented and maintained CI environments using **Jenkins**, performing deployments, Packaging, building optimization, production rollouts, staging, defect tracking (**JIRA**), and root cause analysis.
- Used **Nexus** as a Binary, Artifact hub to store application-related artifacts, and **Helm charts** and download them through **Jenkins** deployment jobs.
  Integrated **Prometheus** with **Kubernetes** for service discovery and application monitoring, and configured **Datadog agents** in the **EKS** cluster to collect and visualize metrics through custom **dashboards** across multiple **AWS accounts**.

Education:

College	Course	GPA	Year Of Attendance
University of Central Missouri	**Master's in computer science**	3.90	**2021 Jan - 2022 May**