

SHAIK BASHA



AWS Solutions Architect | DevOps | Platform | Cloud Engineer (AWS | Azure)

Phone: +1 331-271-7419

Email: shaik.8020@outlook.com

LinkedIn: [shaikbasha](#)

PROFESSIONAL SUMMARY

A highly accomplished and multi-certified **Senior Cloud Architect & DevOps Lead** with 9+ years of experience specializing in the design, security, and optimization of large-scale, multi-cloud (AWS and Azure) platforms for global enterprise clients, including **Citi Bank, JCB, and IBM**. Proven expertise in migrating legacy systems, architecting high-availability solutions (99.99% uptime), and driving **FinOps** practices to achieve significant cost efficiencies.

KEY ACHIEVEMENTS

- **Enterprise Governance:** Designed and implemented a global AWS multi-account architecture leveraging AWS Organizations, Control Tower, and SCPs to enforce unified governance and security across 50+ business units.
- **FinOps & Cost Reduction:** Operationalized FinOps practices using AWS Budgets, Cost Anomaly Detection, and Savings Plans, successfully achieving a 25% reduction in total cloud spend without sacrificing scalability.
- **Zero-Downtime Migration:** Led the zero-downtime migration of over 500 virtual servers and transformed legacy apps into serverless microservices (Lambda/API Gateway), which cut infrastructure overhead by 40%.
- **Reliability & DR Engineering:** Engineered high-availability and disaster recovery architectures using Aurora Global Database, DynamoDB Global Tables, and AWS Backup/CloudEndure, enabling sub-15-minute RTOs for critical workloads.
- **Hybrid Networking:** Architected robust hybrid cloud networks using AWS Direct Connect and Azure ExpressRoute with Transit Gateway, ensuring 99.99% reliability and centralized routing.
- **Azure Governance:** Designed and managed multi-subscription Azure environments using Management Groups, Azure Blueprints, and Policy Definitions to enforce security and compliance across business units.
- **CI/CD & Containerization:** Designed and managed production-grade EKS and AKS (Kubernetes) clusters, implementing advanced blue/green deployment strategies through ArgoCD (GitOps) and continuous integration pipelines.
- **Infrastructure-as-Code (IaC):** Developed and maintained advanced IaC frameworks using Terraform, CloudFormation StackSets, and Bicep to automate consistent, compliant deployments and virtually eliminate manual configuration drift.
- **Security & Compliance:** Implemented a multi-layered audit and security system using AWS Config Conformance Packs, Security Hub, and GuardDuty for continuous monitoring and automated remediation.
- **Access Management:** Integrated AWS IAM Identity Center (SSO) with Active Directory/Okta to provide federated access for thousands of users while enforcing strict RBAC and Permission Boundaries.
- **Observability:** Established end-to-end observability using Prometheus/Grafana, Azure Monitor, and OpenSearch Service, providing SRE teams with complete visibility for predictive issue detection.
- **System Administration:** Provided 24x7 production support and core systems administration for 1500+ virtual servers (Linux/Windows) on VMware vSphere and cloud platforms, resolving complex root-level bottlenecks.
- **Automation & ITIL:** Automated patching and configuration management using Ansible and Systems Manager, participated in Major Incident (MI) bridge calls, and implemented Confluence runbooks to streamline operations.

CERTIFICATIONS:

- AWS Solutions Architect -Associate
- Microsoft Certified Azure Administrator
- Certified Kubernetes Administrator

EDUCATION DETAILS:

M.A., Information Technology Management – **Webster University, St. Louis, USA** (2023 – 2025)

B.Sc., Computer Science – **Vyshnavi Degree & PG College, India** (2013)

TECHNICAL SKILLS:

- **Cloud Platforms:** Amazon Web Services (AWS), Microsoft Azure

- **AWS Core Services:** EC2, S3, VPC, IAM, RDS, EBS, ELB, Auto Scaling, Route 53, CloudFormation, Lambda, ECS, EKS (Kubernetes), Fargate, CloudWatch, CloudTrail, SNS, SQS, WAF, Shield, CodeBuild, CodeDeploy, CodePipeline, DMS, Secrets Manager, GuardDuty, Config, Systems Manager (SSM), Inspector, CloudFront, Control Tower, AWS X-Ray, Transit Gateway, Global Accelerator, API Gateway, Elastic Beanstalk, Organizations, Trusted Advisor, Certificate Manager (ACM), AWS Backup, Storage Gateway, Direct Connect, Glue, Athena, QuickSight.
- **Azure Core Services:** Virtual Machines, App Services, Key Vault, Azure AD, Function App, Blob Storage, Azure Container Registry (ACR), Azure Kubernetes Service (AKS), Service Bus, Azure DevOps, Azure Monitor, Application Insights, Azure SQL, Cosmos DB.
- **Serverless & Containers:** Kubernetes (EKS, AKS), Fargate, ECS, Lambda, API Gateway, Docker, Helm
- **Infrastructure as Code (IaC):** Terraform, CloudFormation, Bicep, YAML, JSON
- **CI/CD & DevOps:** Jenkins, Azure DevOps Pipelines, CodePipeline, CodeBuild, CodeDeploy, Argo CD, Git, GitLab, GitHub
- **Configuration & SCM:** Ansible, Systems Manager (SSM), Chef, Puppet, GitLab, Bitbucket
- **Monitoring & Observability:** Prometheus, Grafana, CloudWatch, Azure Monitor, Datadog, X-Ray, Application Insights, Splunk
- **Migration & Virtualization:** AWS Migration Hub, DMS, SMS, DataSync, VMware vSphere, CloudEndure
- **Security & Compliance:** GuardDuty, Security Hub, Inspector, Network Security Groups (NSGs), **RBAC**, **PIM**, HashiCorp Vault
- **Scripting & Languages:** Python, Bash/Shell Script, PowerShell
- **Documentation & Process:** Confluence, JIRA, ServiceNow
- **Operating Systems:** Linux (RHEL, CentOS, Ubuntu), Windows Server

WORK EXPERIENCE:

Client: Citi Bank, Dallas,
Present

Aug 2024 –

Role: Senior Aws Cloud Engineer | Aws Infrastructure Engineer

Project Title: Multi-Cloud Security Enhancements and Infrastructure Hardening AWS–Azure

Project Description:

As the Senior AWS Cloud Engineer at Citi Bank, I am responsible for driving a large-scale cloud modernization initiative to bring consistency, security, and cost efficiency across more than 50 business units. I designed a unified AWS governance model using Control Tower and SCPs, introduced FinOps practices that reduced cloud costs by 25%, and managed the seamless migration of over 500 legacy servers with zero downtime. Using EKS, Fargate, and GitOps with Argo CD, I built automated, secure deployments and established a CloudFormation StackSets framework that delivered 99.99% reliability across the hybrid AWS–Azure environment.

- Architected and deployed AWS landing zones using AWS Control Tower and Organizations, enforcing governance and compliance through SCPs, resource tagging, and centralized cost control.
- Designed infrastructure following AWS Well-Architected Framework pillars to ensure security, performance, and cost efficiency across production and DR environments.
- Implemented IAM Identity Center (SSO) with Active Directory Federation and Amazon Cognito, enabling role-based access and secure authentication for distributed applications.
- Designed and implemented a hub-and-spoke network architecture using AWS Transit Gateway, enabling secure, scalable connectivity between multiple VPCs and on-prem environments while simplifying routing and network management.
- Established a centralized cost controller leveraging AWS Budgets, Cost Explorer, and Savings Plans, achieving a verified 25% annual cost reduction.
- Utilized Reserved Instances and Compute Savings Plans to optimize compute costs while maintaining 24/7 service reliability.
- Enhanced application performance and resilience using AWS Fargate, EKS (Kubernetes), and ECS, automating blue/green deployments with Helm and Argo CD.
- Automated infrastructure provisioning and environment builds using Terraform, CloudFormation StackSets, and parameterized templates for scalable, consistent deployments.
- Built an end-to-end observability stack using Prometheus, Grafana, CloudWatch, and X-Ray to monitor system health and real-time transaction performance.
- Architected secure and compliant network topologies using VPC, Transit Gateway, NAT Gateways, and PrivateLink, ensuring isolated communication between workloads.
- Integrated Security Hub, GuardDuty, AWS Config, and Amazon Inspector for continuous compliance monitoring and proactive vulnerability detection.
- Automated remediation using AWS Lambda, EventBridge, and Step Functions to resolve misconfigurations and enforce tagging and encryption standards dynamically.
- Managed and optimized multiple database services including RDS (PostgreSQL/MySQL), Aurora Global Database, DynamoDB, and Redshift, ensuring data integrity, replication, and high availability.

- Deployed serverless data workflows with AWS Glue, Kinesis, and Firehose to process real-time operational and financial data with sub-second latency.
- Designed hybrid connectivity using AWS Direct Connect and Site-to-Site VPN, linking AWS environments with on-prem systems securely and efficiently.
- Implemented encryption at rest and in transit using AWS KMS, with WAF and Shield Advanced providing perimeter protection against external threats.
- Designed and validated multi-region disaster recovery using Route 53 and Aurora Global Database, achieving RTO under 60 seconds.
- Conducted Fault Injection Simulator (FIS) testing to validate infrastructure resilience and recovery under simulated failure conditions.
- Supported FinOps initiatives by analyzing usage reports, implementing automated budget alerts, and reducing unutilized resource waste across environments.

Environment: AWS (EC2, VPC, S3, RDS, Aurora, EKS, Fargate, Lambda, CloudFormation, Control Tower, IAM, KMS, WAF, GuardDuty, Transit Gateway, Direct Connect, CloudWatch), Azure (VMs, vNets, ExpressRoute, Azure AD, Defender for Cloud), DevOps & IaC (Terraform, ArgoCD, Jenkins, CodePipeline), Monitoring (Prometheus, Grafana, OpenSearch), Security (SSO, SCPs, FinOps), Tools (JIRA, Confluence, ServiceNow).

Client: Wipro Ltd, India,
2023

December 2021 – August

Role: Senior Cloud Platform Engineer | Senior Cloud Administrator

Project Title: AWS–Azure Infrastructure Modernization for Enterprise Clients

Project Description:

As part of Wipro's multi-cloud transformation initiative, I designed and optimized AWS and Azure infrastructures for enterprise clients including JCB, IBM, and Southern Water. I modernized legacy systems, automated provisioning using Terraform, CloudFormation, and Bicep, and implemented secure hybrid connectivity with Direct Connect and ExpressRoute. I built high-availability and DR architectures ensuring 99.99% uptime, enhanced security with IAM and Azure AD, and improved observability through CloudWatch, Azure Monitor, and Datadog while optimizing cost and performance across workloads.

- Architected the enterprise-wide AWS governance model by implementing **AWS Organizations, Control Tower, and SCPs**, enforcing compliance and centralized billing across business units managing **1,500+ virtualized servers**.
- Engineered resilient hybrid networking using **AWS Direct Connect, Transit Gateway, and Route 53 Resolver Endpoints**, achieving 99.99% link reliability for secure cloud-to-on-prem communication.
- Deployed fault-tolerant web applications using EC2, Auto Scaling Groups, ALB/NLB, **CloudFront**, and Route 53 Failover, while optimizing access with **VPC Peering** and PrivateLink for cross-account service integration.
- Secured core data services by managing RDS (PostgreSQL/MySQL) multi-AZ DR and configuring S3 with **SSE-KMS encryption**, lifecycle rules, and Glacier archival.
- Managed advanced container infrastructure on **EKS clusters**, enforcing RBAC, PodSecurityPolicies, and **Istio Service Mesh** for secure microservice communication and canary deployments.
- Enforced access control using **AWS SSO integrated** with Active Directory for seamless **federation**, leveraging IAM permission boundaries and role delegation for least-privilege access.
- Integrated auditing via CloudTrail/AWS Config Rules, automating non-compliant resource remediation through **Lambda/EventBridge functions**.
- Designed and managed Azure environments using Management Groups, **Azure Blueprints**, and Policy Definitions to enforce security and resource governance across multiple subscriptions.
- Built resilient Azure hybrid connectivity using **ExpressRoute, VPN Gateway, and BGP routing**, utilizing **hub-and-spoke vNets** with VNet Peering and NSGs for secure traffic segmentation.
- Configured highly available compute platforms using Azure Virtual Machines/Scale Sets, and deployed **Application Gateway WAF** and Front Door for Layer 7 security and global traffic management.
- Deployed secure and scalable Azure Kubernetes Service (AKS) clusters, managing access via **RBAC**, Pod Security Policies, and Managed Identities.
- Managed critical data stores (Azure SQL Database, Cosmos DB) with **geo-replication**, utilizing **Azure Storage** Accounts with **Blob Lifecycle Management** and customer-managed encryption.
- Enforced access governance using Azure Role-Based Access Control (RBAC), Conditional Access Policies, and Privileged Identity Management (PIM).
- Implemented business continuity using **Azure Backup** and Site Recovery/Recovery Vaults for disaster recovery, ensuring compliance with **RTO/RPO** objectives.
- Drove multi-cloud provisioning consistency using Terraform alongside native tools (CloudFormation StackSets and Bicep/ARM templates).

- Managed comprehensive CI/CD workflows by integrating **Azure DevOps Pipelines**, GitHub Actions, and Jenkins for automated container builds, releases, and IaC validation.
- Optimized observability as an SRE, utilizing Datadog, Prometheus, Grafana, CloudWatch, and Azure Monitor/Application Insights to track **SLA/SLO metrics**, successfully reducing MTTR by 30%.
- Automated OS patching and configuration management using **Ansible Playbooks** and Systems Manager Run Commands, minimizing manual intervention across the hybrid fleet.
- Supported large-scale migration initiatives using **AWS DMS, DataSync, and Server Migration Service (SMS)**, ensuring zero-downtime cutovers.
- **Conducted Well-Architected Reviews** (AWS/Azure) and leveraged **Azure Cost Management** to optimize spending, delivering knowledge transfer to **mentor** junior engineers.

Environment: AWS (EC2, VPC, S3, RDS, Lambda, CloudFormation, Control Tower, EKS, ECS, Transit Gateway, Direct Connect, CloudWatch), Azure (VMs, vNets, ExpressRoute, Azure AD, AKS, Azure DevOps, Application Gateway, Azure Monitor), DevOps & IaC (Terraform, Bicep, ARM Templates, Jenkins, GitHub Actions, Ansible, Docker, Helm), Monitoring (Datadog, Prometheus, Grafana), Security (KMS, WAF, GuardDuty, Azure Defender, RBAC), Tools (JIRA, Confluence, ServiceNow).

Client: McAfee, India.

October 2018 –

December 2021

Role: DevOps Engineer | Production Support Engineer

Project Title: WEB Security Anti-Virus Research

Project Description:

The WEB Security Anti-Virus Research Project focused on maintaining and optimizing a large-scale production environment consisting of over 1500 virtual servers to support antivirus research, analysis, and deployment operations. The project involved managing VMware infrastructure, Linux and Windows servers, IIS web applications, and load balancers, while ensuring system security, stability, and high availability through proactive monitoring, automation, and incident resolution.

Responsibilities:

- Managed and maintained **VMware** infrastructure supporting 1500+ virtual servers, including creating, cloning, and taking snapshots for environment stability and recovery.
- Configured and monitored **VMware clusters**, virtual networks, and resource pools to ensure optimal performance and load distribution.
- Administered Linux and Windows servers, performing patching, **vulnerability remediation**, and performance optimization to maintain a secure and reliable infrastructure.
- Oversaw IIS web servers and **Loadbalancers**, ensuring effective traffic distribution, redundancy, and high availability across production environments.
- Monitored and validated backend servers for uptime, connectivity, and application stability across multiple regions.
- Managed the McAfee Antivirus infrastructure, including updating application builds, modifying configurations, and managing core services across production and staging servers.
- Collaborated with the development team to push new code updates as per **JIRA** and **Confluence** workflows, ensuring smooth releases and zero production failures.
- Performed post-deployment validations and proactive monitoring to ensure continuous application functionality and minimal downtime.
- Monitored Antivirus modules, handled backlogs, optimized file processing throughput, and ensured timely completion of scanning and security tasks.
- Participated in **Major Incident** (MI) bridge calls to troubleshoot and restore critical infrastructure services during outages.
- Implemented automation for **patching**, configuration, and deployment processes to improve operational efficiency and reduce manual errors.

Environment: VMware vSphere, vCenter, ESXi, Red Hat Enterprise Linux, CentOS, Windows Server 2008/2012, IIS, Apache, Load Balancers (F5/HAProxy), McAfee Antivirus Infrastructure, Shell Scripting (Bash), PowerShell, JIRA, Confluence, Nagios, Grafana, ELK Stack (Elasticsearch, Logstash, Kibana), WSUS, YUM/RPM, TCP/IP Networking, ServiceNow, Remedy.

Client: Sutherland, India.

October 2016 – September

2018

Role: Senior Systems Administrator | Operations Support Engineer

Project Title: Chimera Malware Automation

Project Description:

The Chimera Malware Automation Project focused on maintaining a secure and scalable infrastructure to support automated malware detection, processing, and analysis across production and staging environments. It involved managing Windows and Linux

servers, VMware virtualization, MongoDB replication, and proactive monitoring through Kibana to ensure high availability, performance, and SLA compliance.

Responsibilities:

- Administered Windows and Linux servers supporting the Chimera Malware Automation platform in production and staging.
- Managed Windows Server 2008/R2 and 2012, handling Active Directory, group policies, IIS, and performance tuning.
- Performed Linux admin tasks including YUM/RPM management, service control, networking, and security hardening.
- Managed LVM on Linux servers, resizing partitions and provisioning storage for critical apps.
- Troubleshoot CPU, memory, I/O, and filesystem issues to minimize downtime.
- Monitored logs, kernel messages, and app errors to resolve recurring issues.
- Created and maintained VMs in VMware, ensuring HA, resource optimization, and snapshot management.
- Supported Chimera malware apps and dashboards, resolving alerts on disk, throughput, and backlog.
- Performed daily system checks for integrity, availability, and performance of hardware and storage.
- Managed MongoDB replication, monitored lag, and handled failover for high availability.
- Maintained malware automation scripts to ensure accurate file processing within SLAs.
- Used Kibana dashboards for log monitoring and root cause analysis of recurring failures.
- Handled incident, problem, and change management with dev teams for deployments.
- Provided 24x7 production support and on-call coverage to meet SLAs.
- Performed patching, config management, and security updates to maintain compliance.

Environment: RedHat Enterprise Linux, CentOS, Ubuntu, Windows Server 2008/R2/2012, VMware vSphere, vCenter, ESXi, MongoDB (Replication & Failover), Kibana, ELK Stack, Nagios, Grafana, Shell Scripting (Bash), PowerShell, LVM, IIS, Apache, Git, JIRA, Confluence, WSUS, YUM/RPM, ServiceNow, Remedy.