DevOps/Cloud Engineer

Teja

Ontario, Canada

[Mgouni0328@gmail.com](mailto:Mgouni0328@gmail.com)

+1(647) 691-4661

**SUMMARY:**

* Overall, 6+ years of experience as Development Operations (DevOps)/Build and Release Engineer in automating, building, deploying, managing, and releasing of code from one environment to another environment.
* Led and managed the planning and execution of a successful migration project using tools such as AWS Migration Services, Azure Migrate, and Google Cloud Migrate.
* Experienced with configuration management tool like **Ansible**.
* Extensive Knowledge and hands-on experience implementing PaaS, IaaS, SaaS style delivery models inside the Enterprise (Data center) and in Public Clouds using like AWS, Google Cloud, and Kubernetes etc.
* Installed, configured, and maintained both Windows and Linux servers and workstations.
* Proficient with container systems like **Docker and container orchestration** like **EC2 Container** Service, Kubernetes, worked with Terraform.
* Very good understanding of Microservices architecture, adapting Industry best practices for Microservices while we break down existing apps into micro services.
* Strong advocate of Microservices over monolithic approach, architect applications to be independently scalable, versionable and deployable.
* Developing the solution by writing code, managing versions, conducting tests, and deploying it using Azure DevOps pipelines.
* Strong troubleshooting and debugging skills to resolve issues and ensure smooth operation of GCP environments.
* Analyze business requirements or user stories and design a software solution.
* Experience in creating and maintaining Helm charts to package and version applications, enabling reproducible deployments and simplifying application lifecycle management.
* Knowledgeable in utilizing **Azure Defender** for SQL to secure and protect Azure SQL databases.
* Proficient in utilizing HashiCorp Vault for secure secret management and data protection, including secret storage, encryption, and dynamic secrets generation.
* Working with developers to deploy applications ready for **production with runbooks**, **instructions, and processes**.
* Managed both Windows Active Directory and Linux LDAP user authentication and authorization.
* Experience implementing monorepos using Git submodules, Git subtrees, or tools like Lerna, facilitating code sharing, dependency management, and unified versioning across projects.
* Experience in Cloud Provisioning like Amazon Web Services (AWS), Azure administration.
* Experienced with **CI/CD** process with **Azure DevOps** build and release pipelines.
* Expertise in Azure Service Offering, like Azure cloud services, Azure storage, IIS, Azure Active Directory (AD), Azure Resource Manager (ARM), Azure Storage, Azure, Blob Storage, Azure VMs, SQL Database, Azure Functions, Azure Service Fabric, Azure Monitor, and Azure Service Bus.
* Experienced with **Azure Artifacts and JFROG Artifactory**.
* Provide engineering design across different workloads including **incident & problem** **management, change management, security, and compliance**.
* Expertise in building CI/CD on AWS environment using AWS Code Commit, Code Build, Code Deploy and Code Pipeline and skill in using **AWS CloudFormation**, API Gateway, and AWS Lambda in automation and securing the infrastructure on AWS.
* Skilled in monitoring and troubleshooting Hadoop clusters to ensure optimal performance, scalability, and reliability.
* Managing cloud infrastructure resources, such as **virtual machines**, **storage solutions**, and **networking resources**, using tools such as **AWS, Azure, or GCP**.
* Improve **security** and **performance** of infrastructure by working with other teams.
* Experience in changing over existing AWS infrastructure to Serverless architecture **AWS** **Lambda, AWS Kinesis** through the creation of a Serverless Architecture using **AWS Lambda, API gateway, Route 53, S3 buckets.**
* Experienced with automation tools like **Terraform, CloudFormation** and **ARM templates**.
* Experience in automated builds using TFS team build and cruisecontrol.net build for .net applications and salesforce.
* Efficient experience in using Nexus and Artifactory Repository managers for Maven builds.
* Hands on experience in installing and administrating CI tools like **Hudson/Jenkins, Sonar**, **Subversion/Accurev and Nexus/Artifactory**
* Experience in managing the Artifacts generated by MAVEN in the Nexus Repository.
* Deployed and maintained Chef role - based application servers, including **Apache, Resin, Nginx** and **Tomcat.**
* Proficiency in **Azure cloud services and technologies,** such as **Azure VMs, Azure Storage, Azure Networking, and Azure Security**
* Used to write an install script in Ruby using all the extra helper functions from Chef.
* Experience in working on source control tools like Tortoise SVN, CVS, IBM Clear case, Perforce, and GIT.

**TECHNICAL SKILLS:**

* Operating System: Ubuntu, UNIX, LINUX, Mac OS.
* Build Tools: Ant, Maven, MS Build
* Scripting Languages: PowerShell scripting, Perl scripting, Python.
* Version Control Tools: Git, GitHub
* SDLC: Agile, Scrum Methodologies, Waterfall
* Platforms: Linux and Windows family
* CI/CD tools: Bamboo, Jenkins, AzureDevOps
* Monitoring Tools: Icinga, Newrelic, Grafana, splunk, Sumologic
* Automation Tools: Terraform, CloudFormation, ARM Templates
* Configuration management Tools: Ansible, Chef
* Web/ Application Servers: Apache Tomcat, JBOSS, Web sphere, Web logic.
* SCM Tools: AzureDevOps, Team Foundation Server (TFS), Clear Case.

**EDUCATION:** Bachelor’s in technology, JNTUH.

**WORK EXPERIENCE:**

**Client: TD BANK, CANADA Aug 2022 to Till Date**

**Role: DevOps/Onboarding Consultant**

**Responsibilities:**

* Involved in Planning, Architecting, Implementing the Security and Disaster Recovery processes for the whole infrastructure.
* Designed and implemented a CI/CD pipeline using GitLab and Jenkins, enabling automated build, testing, and deployment of the application code, leading to faster release cycles and improved software quality.
* Used Azure artifacts for storing the build artifacts where versioning is solid and accurate, also used JFROG artifactory for storing Docker images.
* Deployed build artifacts automatically from JFROG using Terraform scripts to deploy to ECS clusters.
* Used Azure Defender to protect Azure resources and workloads against various threats and attacks.
* Experienced in Site Reliability for high-traffic applications, a solid understanding of Service level objectives (SLO), Service Level Indicators (SLI), and SLA, and sound knowledge of implementing them.
* Implementing and managing continuous integration and continuous delivery (CI/CD) pipelines to enable frequent and reliable software releases.
* Configuring and managing Azure Active Directory, including managing users and groups, configuring single sign-on, and setting up conditional access policies.
* Developing scripts and automation tools to streamline deployment and management of Azure resources.
* Participated in on-call rotations and incident response, utilizing SRE practices and frameworks such as ITIL, and ensuring post-incident reviews were conducted to identify and address root causes and prevent similar incidents from occurring in the future.
* Designed and maintained both Windows and Linux network infrastructures, including routers, switches, firewalls, and VPNs.
* Employed infrastructure-as-code principles with tools such as Terraform and Ansible to automate the provisioning and configuration of cloud resources on AWS, ensuring consistent and reproducible environments across development, testing, and production stages.
* Designed and configured Azure Virtual Networks (VNets), subnets, Azure network settings, DHCP address blocks, DNS settings, security policies and routing.
* Collaborated with development teams to ensure the scalability and reliability of applications, using tools such as LoadRunner and JMeter for performance testing, and working closely with product owners to prioritize feature development and incident response, in line with SRE principles.
* Configured DNS with Route53 to route users to internet-based applications by using Hosted Zones. Restrict the users to route to their application with Private Hosted Zones.
* All infrastructure components for different environments (Dev/Test/Prod) are provisioned via Terraform scripts, CloudFormation with no manual intervention in AWS.
* Deployed application secrets and sensitive configuration data like tokens, passwords, certificates, encryption keys etc., into AWS Secrets Manager.
* Implementing and managing Azure security solutions, including Azure Security Centre, Azure Firewall, and Azure Sentinel.
* Designing and implementing DevOps solutions using Java-based tools and technologies, such as Jenkins, Ansible, and Docker.
* Integrated JMeter Performance Testing into release pipeline so that every build after it is deployed into DEV, UAT, or PROD it will do a performance test automatically. Depends on the threshold that I setup it will check and break the release if the performance is below threshold value.
* Updated runbooks, tools, and documentation to help prepare on-call teams for future incidents.
* Setup security groups in VPC to manage the inbound and outbound traffic where all the rules get evaluated.
* Integrating Azure Active Directory for user authentication/authorization and organization profiles.
* Maintained compliance with security and regulatory standards using tools such as Vault, Keycloak, and AWS Security Hub to manage access control, authentication, and authorization.
* Automating build and deployment processes for Java applications using modern CI/CD tools, such as Jenkins, Bamboo, or GitLab CI/CD
* Implemented Azure DevOps Pipelines for CI/CD setup, deployed applications automatically by enabling the triggers to deploy.
* Migrate Database Services from on-premises to Azure Cloud Environments using DMA and SSMS, updating the connection strings, collaborate with development and QA teams to maintain high-quality deployment.
* Ensuring the security and compliance of Java applications and infrastructure, including managing access controls, implementing encryption, and adhering to industry best practices.
* Setup Network ACL’s on VPC which blocks the inbound and outbound explicitly.
* Setup VPC peering between 2 different VPC’s.
* Created ARM template to join VM to existing domains, Create a sandbox setup of Azure Firewall with Zones.
* Worked on System and application Monitoring setup with Icinga, Newrelic, Grafana etc.
* Worked on Azure Site Recovery, PowerShell Scripts and ARM templates.

**Environment:** **Azure CI/CD, Azure artifacts, AWS, S3, Cloud Watch, Kibana, API Gateway, ECS, Azure Devops, Key vault, AAD groups, Log analytics, Azure Monitor, ACS, Service principals, AWS, PowerShell, Python, Bash, Shell, Java, Kubernetes, Docker Compose, Docker Swarm, Ansible Tower, Splunk, Sensu, SQL. ARM Templates, Fargate, Terraform, AKS, Ansible, Docker, Git, Jenkins, CI/CD**.

**Client: CIBC, Toronto - Canada Aug 2021 to July 2022**

**Role: Cloud Consultant**

**Responsibilities:**

* Data Ingestion to one or more Azure Services – (Azure Data Lake, Azure Storage, Azure SQL, Azure DW).
* Worked closely with the operations team to manage the production environment, ensuring high availability, scalability, and security of the application.
* Designed and implemented a migration plan using tools such as Terraform, Ansible, and Chef to automate the infrastructure provisioning and configuration management.
* Documented the migration process using tools such as Confluence and Markdown to create a reference guide for future migrations, ensuring that the process was repeatable and scalable.
* Implemented an automated testing suite integrated into the pipeline, including unit tests, integration tests, and end-to-end tests, to ensure code changes did not impact the production environment negatively.
* Implemented containerization using Docker and orchestrated the deployment of microservices in a Kubernetes cluster, ensuring scalability, fault tolerance, and efficient resource utilization.
* Used Helm's templating capabilities and values files to customize deployments, allowing for flexible configuration management and environment-specific settings.
* Hands on Experience working with the Microsoft Azure Cloud Services and deploying the servers Through Azure, Resource Manager Templates or Azure Portal.
* Worked on Microsoft Azure (Public) Cloud to provide IaaS support to client. Create Virtual Machines through Power Shell Script and Azure Portal.
* Created **ARM template** to join VM to existing domains, Create a sandbox setup of Azure Firewall with Zones.
* Deploying VM's, Storage, Network and Affinity Group through PowerShell Script.
* Creating Storage Pool and Stripping of Disk for Azure Virtual Machines.Backup, Configure and Restore Azure Virtual Machine using Azure Backup.
* Implemented security controls and best practices across the infrastructure and application stack, including network security, IAM policies, and vulnerability scanning, resulting in compliance with industry standards and customer requirements.
* Develop PowerShell scripts from scratch, Azure CLI, and ARM templates to automate the provisioning and deployment process.
* Worked on ARM templates to automate the provisioning and deployment process.
* Responsibilities include virtual networks, image creation and maintenance, subscription management, storage management, Backup/DR, Network Security Groups, Role Based Access Controls, Azure Active Directory, Azure Automation, Monitoring and Logging.
* Created docker images and stored under ACR and deployed the build artifacts and docker images onto AKS as a container service with ARM template where infrastructure is provisioned automatically with ARM template.
* Recommend, coordinate, and perform the implementation of cloud solutions.
* Install, troubleshoot, and maintain all supported cloud infrastructure and services
* Implemented and maintained automated deployment and monitoring solutions for Hadoop using tools such as Ansible, Puppet, or Chef.
* Troubleshoot server hardware and software, networking.
* Drive to the Azure DevOps GitHub repository.
* Worked with Network Security Groups (NSGs).
* Worked with Google Cloud Networking to configure VPCs, firewall rules, VPNs, and private connectivity options.

**Environment:** **Azure CI/CD, Azure artifacts, Cloud Watch, Kibana, API Gateway, Java, Terraform, AKS, Ansible, Docker, Git, Jenkins, CI/CD, Azure Devops, Keyvault, AAD groups, Log analytics, Azure Monitor, Service principals, PowerShell, Python, Bash, Shell, Kubernetes, Docker Compose, Docker Swarm, Ansible Tower, Splunk, SQL,** **ARM Templates.**

**Bell, Canada.** Dec 2018 to July 2021

Azure DevOps Engineer

**Roles and Responsibilities:**

* Expertise in Architecting and Implementing Azure Service Offering, such as Azure cloud services, Azure Resource Manager (ARM), Azure storage, Azure Active Directory (AD), Azure Storage, Azure, Blob Storage, Azure VMs, SQL Database, Azure Functions, Azure Service Fabric, Azure Monitor, and Azure Service Bus.
* Designed and implemented a continuous delivery pipeline for a custom-built application, utilizing Azure DevOps tools and services.
* Collaborated with the development team to establish guidelines and best practices for code modularization and scalability, ensuring efficient and streamlined development processes.
* Worked closely with the infrastructure team to ensure the necessary Azure infrastructure was in place to support the application's deployment, including virtual machines, networking, and storage resources.
* Utilized Azure DevOps features such as Azure Repos for source control, Azure Pipelines for build automation, and Azure Test Plans for testing and quality assurance.
* Implemented infrastructure as code (IaC) using Azure Resource Manager (ARM) templates and PowerShell scripting, enabling consistent and repeatable infrastructure provisioning.
* Leveraged Azure Kubernetes Service (AKS) to containerize and orchestrate application deployments, ensuring scalability, high availability, and efficient resource utilization.
* Implemented monitoring and alerting solutions using Azure Monitor and Application Insights, providing real-time visibility into the application's performance and health.
* Implemented security best practices in Azure, including role-based access control (RBAC), Azure Key Vault for secrets management, and SSL/TLS encryption for data in transit.
* Conducted regular performance and scalability testing to identify bottlenecks and optimize the application's performance on Azure infrastructure.
* Collaborated with cross-functional teams and stakeholders to ensure smooth deployment and maintenance of the application, providing timely support and troubleshooting.
* Created AKS clusters with basic and advanced networking where Basic Networking Model Called Kubenet which is default configuration when creating an AKS cluster and k8s cluster is completely separate from Azure network and on-prem network Suitable if you are deploying in an Isolated Environment.
* Secured Windows and Linux servers in Azure using Azure Defender for Servers.
* Created AKS cluster with advanced networking where It makes Pods first class citizens in our network with Azure CNI, Every Pod will get an Ip address from the Virtual Network.
* Created external and internal ASE in azure which is a deployment of Azure App Service into a subnet in an Azure virtual network (VNet).
* Utilized windows PowerShell to create a master table of content page for the desktop support knowledge.
* Developing and maintaining monitoring and alerting systems for NodeJS applications, such as Prometheus, Grafana, or Nagios
* Implemented a CI/CD pipeline with Docker, Jenkins (TFS Plugin installed),**Team Foundation** Server (TFS), GitHub and Azure Container Service, whenever a brand new TFS/GitHub branch gets started, Jenkins, our Continuous Integration (CI) server, automatically attempts to create a replacement Docker container from it.
* Created multiple EBS volumes and attached to single EC2 instance.
* Excellent knowledge of Azure compute services, Azure Web apps, Data Factory & Blob Storage, Azure Networking, and Identity & Access Management, Azure AD, Multi-Factor Authentications. Expertise in Azure Development, worked on Azure web application, App services, Azure storage, Azure SQL Database, Virtual Machines, Fabric controller, Azure AD, Azure search, and Notification hub.
* Added Azure CDN to an Azure App Service web app and Accessed storage blobs using an Azure CDN custom domain over HTTPS.
* Assist in the Development Priority List process working with Product Management group to address issue identified as part of Problem Management
* Configured ELB to support routing and load balancing of HTTP, HTTPS, TCP and SSL traffic to EC2 instance.
* Configured Internet facing load balancers and Internal load balancers. Offloaded SSL certificates on ELB to improve the performance. Used ELB to health checks for EC2.
* Configured Sticky sessions on ELB where all the requests are served to single EC2 instance.
* Configured DNS with Route53 to route users to internet-based applications by using Hosted Zones. Restrict the users to route to their application with Private Hosted Zones.
* Integrated JMeter Performance Testing into release pipeline so that every build after it is deployed into DEV, UAT, or PROD it will do a performance test automatically. Depends on the threshold that I setup it will check and break the release if the performance is below threshold value.
* Updated runbooks, tools and documentation to help prepare on-call teams for future incidents.
* I also have worked on System and application Monitoring setup with Icinga, Newrelic, grafana etc.
* Integrated Ansible Tower to our environment, non-administrative users can safely request and manage virtual resources using the Playbooks we provide them all without needing access to sensitive credentials.

Environment: Azure CI/CD, Azure artifacts, Nodejs, AWS, S3, Cloud Watch, Kibana, API Gateway, ECS, Fargate, Terraform, AKS, Ansible, Docker, Git, Jenkins, CI/CD, Azure Devops, Keyvault, AAD groups, Log analytics, Azure Monitor, ACS, Service principals, AWS, PowerShell, Python, Bash, Shell, Kubernetes, Docker Compose, Docker Swarm, Ansible Tower, Splunk, Sensu, SQL, **Google Cloud Platform (GCP)**

**BFI Limited, India.** Sep/2016 to Nov/2018

**DevOps Engineer**

**Roles and Responsibilities:**

* Setup API gateway for services and included a load balancer and add an entry in F5 pointing to our API gateway since some of env’s are publicly accessible.
* Setup logs streaming into Kibana and setup indexes to search for application logs when there is an issue.
* Created multiple Python, Bash, Shell and Ruby Shell Scripts for various application level tasks.
* Implemented CI/CD builds and releases of our software and infrastructure and Monitoring and alerting of our production environment.
* Thorough understanding of IaaS, PaaS, SaaS, and public & private &hybrid Cloud.
* Worked on AWS EC2/VPC/S3/SQS/SNS based on automation **Terraform, Ansible, Python, Bash** Scripts.
* Wrote PowerShell scripts to automate application deployment and data collection.
* Enabled developers with good practices and Help with containerization efforts for production systems.
* Created docker images and stored under ACR and deployed the build artifacts and docker images onto AKS as a container service with ARM template where infrastructure is provisioned automatically with ARM template.
* Created AKS clusters with basic and advanced networking where Basic Networking Model Called Kubenet which is default configuration when creating an AKS cluster and k8s cluster is completely separate from Azure network and on-prem network Suitable if you are deploying in an Isolated Environment.
* Created AKS cluster with advanced networking where It makes Pods first class citizens in our network with Azure CNI, Every Pod will get an Ip address from the Virtual Network.
* Created external and internal ASE in azure which is a deployment of Azure App Service into a subnet in an Azure virtual network (VNet).
* Familiarity with GCP security features and compliance standards, ensuring data protection and regulatory compliance.
* Created Maven POMs to automate build process for the new projects and integrated them with third party tools like SonarQube, Nexus.
* Internal ASE is deployed into a private subnet within our private VNET will allow access to the app service internally.
* Moved app services from one service plan to other service plan without any service discerption to the app.
* Added Azure CDN to an Azure App Service web app and Accessed storage blobs using an Azure CDN custom domain over HTTPS.
* Developed Terraform scripts for AWS deployment and openstack deployments.
* **I**ntegrated our ILB App Service Environment with the Azure Application Gateway.
* Enable customers to elastically scale throughput and storage based on demand, globally with Azure Cosmos DB.
* Azure Cosmos DB’s highly modular and fully resource governed approach to solve a variety of coordination problems including, cross region replication and transparent partition management.
* Help track and maintain uptime for production systems and Help and document Root Cause Analysis (RCA).
* Used Ansible to Remediate faster-automatingactions like blacklisting attacking IP addresses or domains, whitelisting non-threatening traffic or isolating suspicious workloads for further investigation.
* Build effective monitoring, logging and auditing of production systems to ensure compliancy with mandated policies.
* Guide and support application teams with onboarding, troubleshoot and resolve implementation issues like Troubleshoot and identify performance, connectivity and other issues for the applications hosted in Azure platform.
* Writing custom gradle tasks, publishing pulgins to gradle plugins portal.
* Created an event source mapping in Lambdathat reads items from a stream or queue and invokes a function.
* Created AKS internal load balancers and external load balancers to communicate the traffic between the pods internally and externally.
* Migrated TFS CI/CD pipeline into AzureDevops pipeline and restored the artifacts into azureartifacts.
* Stored the state of the files and configuration stored under S3 buckets.
* Setup metrics logs through CloudWatch **a**nd trigger an alert email when a threshold is meet.

**Environments:** - Azure CI/CD, AWS, SaaS, Jenkins, TFS, Bitbucket, Kafka, Fargate, Newrelic, Appdynamics, Azure artifacts, AWS, S3, Cloud Watch, Kibana, API Gateway, ECS, Fargate, Terraform, AKS, Ansible, Docker, Git, Jenkins, CI/CD, Azure Devops, Keyvault, AAD groups, Log analytics, Azure Monitor, ACS, Service principals, AWS, PowerShell, Python, Bash, Shell, Kubernetes, Docker Compose, Docker Swarm, Ansible Tower, Splunk, Sensu, SQL..