**Vineeth kumar milatari**

**Sr. Cloud / DevOps Engineer**

**Professional Summary**

Sr. Cloud & DevOps professional with around 10 Years of experience in the IT industry comprising Cloud Management, dedicated to automation and optimization. Has experience with Cloud Solutions, build and release management, version control, continuous integration, continuous deployment, and Linux system administration, as well as DevOps automation development for Linux systems

* A seasoned Cloud professional with a deep understanding of cloud technologies, infrastructure, and best practices, dedicated to optimizing and enhancing business operations through innovative cloud solutions on the AWS and Azure cloud platforms.
* Skilled in implementing Infrastructure as Code (IAC) using tools like AWS CloudFormation and Terraform, enabling repeatable and automated deployments.
* Professional AWS security practices, including IAM roles, policies, and VPC configurations to ensure data privacy and compliance and in setting up CI/CD pipelines using AWS CodePipeline and CodeDeploy for seamless application delivery.
* Have extensive experience building, implementing, and maintaining sophisticated cloud applications using Azure services. I am a tremendous asset in facilitating successful Azure migrations and transformations because of my knowledge of cloud infrastructure, application architecture, DevOps techniques, security, and data analytics.
* Proficiency in integrating Azure services, such as Azure Active Directory, Azure SQL Database, Azure Storage, and Azure Functions, to create comprehensive cloud solutions.
* Highly skilled and experienced Application Security Engineer/Specialist with a proven track record in analyzing risks from open-source threats and implementing robust security practices.
* Expertise in software security, threat detection, and vulnerability remediation to optimize information technology Software and Platform Engineering processes.
* Experienced in writing and optimizing SQL queries and working with GraphQL queries for efficient data retrieval.
* Proficient in using Docker for containerization and Linux for server management and development environments.
* Strong understanding of development and QA practices, ensuring high-quality software delivery through best practices and methodologies.
* In-depth knowledge of software development principles, including best practices, concepts, technology, and methodologies.
* Implemented TDD to ensure robust and reliable code, focusing on writing tests before the actual development.
* Developed secure applications adhering to best practices for information security to protect sensitive data.
* Committed to continuous learning and staying updated on technical developments and industry practices.
* Maintains a positive attitude focused on finding solutions and developing new approaches, effectively managing distractions and challenges.
* Developed AWS Lambdas using Node.js, ensuring scalable and efficient serverless functions.
* Skilled in production issue triage, prevention, and release management support from a technical standpoint.
* Conducted research and development for AWS proof of concepts (POCs).
* Highly skilled in Node.js and TypeScript for building robust and efficient applications.
* Extensive experience in developing and managing AWS Lambda functions.
* Proficient in AWS CloudWatch scripting for monitoring and managing cloud resources.
* Highly skilled with AWS Cloud Development Kit (CDK) for infrastructure as code (IaC) development.
* Strong verbal and written communication skills, capable of effectively communicating with all levels of employees and management.
* Proven ability to work well in a collaborative setting, supporting team efforts, contributing to discussions, and fostering positive relationships.
* Top of Form

**Technical skills**

|  |  |
| --- | --- |
| Cloud Environments | Amazon Web Services (Lambda, CloudWatch, AWS CDK, DynamoDB, API Gateway, S3), Azure, Google Cloud platform |
| Configuration Management  Tools | Chef, Puppet, Ansible, Terraform, Saltstack, AWS cloud formation, Azure Resource Manager Templates. |
| Containerization Tools | Kubernetes, Docker, OpenShift, Docker compose, Podman, Nomad, Amazon ECS,  Google Kubernetes Engine, Azure Kubernetes service, Rancher, Portainer. |
| Version Control Tools | SVN, GIT, GIT-Hub, Bitbucket, Gitlab, Mercurial, Subversion. |
| CI-CD Tools | ANT, MAVEN, Gradle, AWS code build, circle CI, Travis CI, GitLab CI/CD, Jenkins, Team City, Bamboo, Azure DevOps, Make. |
| Web Servers | Apache Tomcat, Web Sphere, GraphQL, Nginx, Microsoft internet information service (IIS), Apache HTTP server. |
| Bug Tracking Tools | JIRA, Bugzilla, Remedy, Bugzilla, Trello, Gitlab issues, Redmine. |
| Monitoring Tools | Splunk, Dynatrace, New Relic, Zabbix, ELK, Datadog, Nagios, Grafana, Prometheus, Zabbix, App Dynamics, Graylog. |
| Databases | Aurora, DynamoDB, RDS, MySQL, MongoDB, SQL Server, MS SQL, Cassandra DB |
| Virtualization Tools | VMWare ESX/ESXi, Windows Hyper-V, Virtual box, Vagrant |
| Testing Tools | Selenium, JUnit, Cucumber, Jenkins, Selenium, JUnit, Cucumber, SonarQube, TestNG. |
| Scripting Languages | Ruby, Perl, Python, Node, TypeScript, JavaScript, Bash shell, PowerShell, Groovy, YAML, SQL, GraphQL. |
| Operating Servers | Ubuntu, Linux, Windows, CentOS, Debian, Mac OS. |
| DevOps Tools | Docker, AWS CDK, AWS CloudWatch, AWS Lambda |
| Development Practices | Test-Driven Development (TDD), Secure Application Development |

* Top of Form

**Professional Experience**

**CLIENT: LOWES SEP 2022 - PRESENT**

**Lowe's Charlotte Technology Hub**

**Sr AWS DevOps Engineer**

**Responsibilities:**

* Utilizing AWS for hosting and migrating an e-commerce platform Using AWS while modernizing the architecture for improved scalability, fault tolerance, and automation including web servers, databases, and content delivery, to ensure a seamless online shopping experience.
* Spearheaded the establishment of software security best practices, collaborating closely with software engineering teams to ensure adherence to secure coding principles and threat detection protocols.
* Conducted comprehensive analysis of open-source threats, including zero-day vulnerabilities, evaluating their potential impact on the organization's software products deployed on AWS.
* Developed and deployed serverless applications using AWS Lambda with Node.js and Typescript.
* Created and deployed serverless functions using Node.js, leveraging AWS Lambda to enhance application scalability and efficiency.
* Managed and resolved production issues, ensuring minimal downtime and maintaining application performance.
* Provided technical support during release management, ensuring smooth deployment processes and version control.
* Conducted research and development of proof of concepts (POCs) for AWS services, evaluating new technologies and methodologies.
* Utilized Node.js and TypeScript to build robust, scalable applications and services, ensuring high code quality and maintainability.
* Implemented AWS CloudWatch scripts for monitoring and logging, enabling proactive identification and resolution of issues.
* Employed AWS Cloud Development Kit (CDK) to define cloud infrastructure as code, streamlining deployment processes and improving infrastructure management.
* Integrated SQL queries and GraphQL for efficient data retrieval and manipulation, enhancing data accessibility and application performance.
* Leveraged Docker for containerizing applications, ensuring consistency across development, testing, and production environments.
* Managed and maintained Linux servers, optimizing performance and ensuring system reliability and security.
* Applied TDD principles to write tests before development, ensuring robust and error-free code.
* Developed applications with a focus on security best practices, protecting sensitive data and ensuring compliance with security standards.
* Worked closely with development and QA teams, following best practices to ensure high-quality software delivery.
* Effectively communicated with team members and stakeholders, fostering a collaborative environment and contributing to team success.
* Implemented container security measures using Docker, orchestrating secure deployments on AWS ECS and EKS.
* Developed custom scripts for automating security checks and monitoring of AWS resources, enhancing incident response capabilities.
* Stayed updated with the latest security threats and industry trends, disseminating knowledge through workshops and training sessions.
* Supported the integration of security controls into the CI/CD pipeline, ensuring seamless security testing and validation throughout the software development lifecycle.

**Environment**: AWS, AWS Lambda, AWS CDK, AWS CloudWatch, Prometheus, Blackbox exporter, Sonatype, OWASP, alert manager, GraphQL, Docker, Kubernetes, GitHub, Node.JS, TypeScript, Jenkins, TDD, Yaml.

**CLIENT: PILOT COMPANY JAN 2022 – AUG 2022**

**Knoxville, TN**

**DevOps Engineer**

**Responsibilities:**

* Migrating Services from On-premise to Azure Cloud Environments. Collaborate with development and QA teams to maintain high-quality deployment.
* Worked with Terraform Templates to automate the Azure Iaas virtual machines using Terraform modules and deployed virtual machine scale sets in the production environment.
* Used Ansible and Ansible Tower as Configuration management tool to automate repetitive tasks, quickly deploys critical applications, and proactively manages change.
* Integrated Datadog monitoring solutions to provide real-time insights into AWS data infrastructure, enabling proactive identification and resolution of performance bottlenecks.
* Developed an automated deployment tool for dev, UAT, and production environments using Ansible. Allows new services to be deployed and released simply by developers, including an Ansible playbook.
* Used Kubernetes to manage containerized applications using its nodes, Config Maps, selector, Services & deployed application containers as Pods.
* Making deployments of Microservices as containers using containerization tools like Docker and Docker Compose. Docker Swarm and Kubernetes for orchestration and Microsoft Azure to ensure continuous deployments into the different environments.
* Managed Kubernetes charts using Helm, Created reproducible builds of the Kubernetes applications, managed Kubernetes manifest files, and Managed releases of Helm packages.
* Created additional Docker Slave Nodes for Jenkins using custom Docker Images and Worked on all major components of Docker like Docker Daemon, Hub, Images, Registry, Swarm, etc.
* Built end-to-end CI/CD Pipelines in Jenkins to retrieve code, compile applications, perform tests and push build artifacts to Nexus and UDeploy to orchestrate changes across servers and components.
* Implemented branching & tagging strategy to maintain the source code in the GIT repository. Coordinated with developers to establish and apply appropriate branching, labelling/naming conventions using GIT source control.
* Responsible for Setup and integrated Prometheus with Grafana for Monitoring. Used Elasticsearch (ELK stack) for centralized logging and analytics in the continuous delivery pipeline to store logs and metrics in Azure storage using the storage function.
* Utilized Datadog Log Tracing to identify and resolve critical issues in real-time, ensuring optimal application reliability in an Azure environment.
* Collaborated with cross-functional teams to integrate Datadog monitoring solutions seamlessly into Azure-based workflows.
* Extract Transform and Load data from Sources Systems to Azure Data Storage services using a combination of AzureData Factory, T-SQL, Spark SQL, and U-SQL Azure Data Lake Analytics. Data Ingestion to one or more Azure Services-(Azure Data Lake, Azure Storage, Azure SQL, Azure DW) and processing the data in In Azure Databricks.
* Involved in setting up Azure Functions to execute a PowerShell script that regularly backs up data from one region to another. Provided data redundancy and backup files from an Azure Storage container to a different location.
* Setting up Nginx, HTTP web server as a reverse proxy to critical applications such as Jira, Jenkins, and Application Server.

**Environment:** Azure,Office 365, Terraform, Grafana, Maven, Jenkins, Ansible, Docker, Kubernetes, Git, PowerShell, Apache-Tomcat server, Jira, AEM, RHEL, ELK, PowerShell script, Python, Mac OS.

**CLIENT: FIDELITY INVESTMENTS JULY 2016– DEC 2021**

**Boston, MA**

**DevSecOps Engineer**

**Responsibilities:**

* Implemented robust security measures within AWS cloud infrastructure, ensuring compliance with OWASP, WASC, and CWE standards.
* Collaborated with software engineering teams to integrate security best practices throughout the development lifecycle, including threat detection, vulnerability assessment, and remediation.
* Conducted in-depth analysis of open-source threats and vulnerabilities, prioritizing high-risk components for mitigation based on severity and exploitability.
* Implemented continuous integration and continuous deployment (CI/CD) pipelines using Jenkins and Docker.
* Advised development teams on secure coding practices and strategies for mitigating application vulnerabilities in alignment with OWASP guidelines.
* Administered security tools such as Sonatype, Black Duck, and Snyk to perform software composition analysis and enforce secure coding standards.
* Conducted code reviews and analysis to identify and address potential security issues, ensuring adherence to OWASP, WASC, and CWE recommendations.
* Collaborated with enterprise and application architecture teams to review and enhance security architecture, incorporating best practices for threat mitigation and risk management.
* Utilized AWS Lambda for backend processing and AWS API Gateway for API management.
* Created CloudWatch alerts for instances and utilizing them in Auto-scaling launch configurations.
* Developed frontend interfaces using React and integrated them with backend GraphQL endpoints.
* Acted as a change agent and thought leader within the organization, providing direction to engineering and security teams on emerging threats and mitigation measures. Stayed abreast of emerging threats and vulnerabilities in the open-source community, communicated project-related security risks and remediation measures accurately and promptly to stakeholders and impacted teams.
* Integrated and adhered to defined development and delivery processes, ensuring compliance with change management, SLA, and productivity goals, while also serving as a thought leader and change agent within the organization.
* Demonstrated strong competencies in communication, with a developer background and experience in various types of application security testing, including software composition analysis, web application security, static security testing, cloud security, and container security.
* Worked on code review, and analysis, along with proficiency in source code review and collaboration with cross-functional teams to identify and mitigate application vulnerabilities.
* Utilized industry-standard tools such as Sonatype, Black Duck, Snyk, GitHub, SonarQube, AWS technologies, Docker containers, and infrastructure as code to enhance security posture and ensure robust software security practices.

**Environment**: AWS, AWS Lambda, GraphQL, Prometheus, Blackbox exporter, Sonatype, OWASP, alert manager, CI/CD, Docker, Kubernetes, GitHub, Jenkins, Yaml.

**CLIENT: MAROLIX MAY 2015 – JUNE 2016**

**Hyderabad, India**

**DevSecOps Engineer**

**Responsibilities:**

* Implemented and maintained an on-premises SAST tool Checkmarx, Fortify within the organization's infrastructure. Developed custom rules and configurations to tailor the tool to the specific software development environment.
* Integrated the SAST scans into the CI/CD pipeline to identify and remediate security vulnerabilities early in the development process.
* Setting up an on-premises SCA solution like Sonatype Nexus Lifecycle to identify and track open-source software components and their vulnerabilities.
* Integrated the SCA tool into the CI/CD pipeline to automatically scan and generate reports on third-party dependencies, enabling teams to address vulnerabilities promptly.
* Implemented and managed security controls in AWS environments to protect against various security threats.
* Developed and maintained secure Terraform infrastructure as code templates, automating security checks and compliance enforcement.
* Hardened and secured Kubernetes clusters, implementing network policies, RBAC, and security contexts.
* Ensured compliance with industry standards and regulations, actively participating in security audits and assessments.
* Orchestrated the integration of security tools and tests (SAST, DAST, SCA) into the CI/CD pipeline, using on-premises CI/CD tools such as Jenkins and Bamboo. Ensured that security checks were automated and provided feedback to developers in real-time.
* Leveraged scripting languages such as PowerShell, Python, Bash, or tools like Postman to automate security tasks, streamline processes, and enhance the efficiency of security operations.
* Integrated container security scanning into the CI/CD pipeline to prevent the deployment of insecure containers.
* Automated Datadog Dashboards and assisted internal users for Splunk in designing and maintaining production-quality dashboards.
* Worked with Nagios for Windows Active Directory & LDAP and Data consolidation for LDAP users. Monitored system performance using Nagios, maintained Nagios servers, and added new services & servers.

**Environment:** AWS, OpenStack, OpenShift, Git, Maven, Jenkins, Linux, Jira, Chef, Ansible, Docker, Splunk, Python, EC2, S3, EBS, ELB, Opswork, Nexus, Bash, Unix/Linux, Nagios, Datadog. Mac OS.

**CLIENT: RESOURCE SOLUTIONS MAY 2014– APRIL 2015**

**HYDERABAD, INDIA**

**Site Reliability Engineer**

**Responsibilities:**

* Administered Bamboo servers which included installing, upgrading, backup, adding users, creating plans, establishing the local/remote agent, adding capabilities, performance tuning, troubleshooting issues, and maintenance.
* Setting up continuous integration and formal builds using Bamboo with the Artifactory repository and Resolving update, merge, and password authentication issues in Bamboo and JIRA.
* Developed Puppet modules and manifests to automate critical cluster deployment, configuration, and lifecycle management. Wrote Puppet manifests for configuration management and deployed .Net and Java applications.
* Implemented continuous integration using Jenkins master and slave configuration. Configured security to Jenkins and added multiple nodes for continuous deployment.
* Developed Maven build scripts for maintaining test automation, makes & Java based library to read test data from XML & Properties files using Junit and loading it into Selenium.
* Initiated responsibility for administering the SVN servers, which included installing, upgrading, backup, adding users, creating repositories/branches, merging, writing hooks scripts, performance tuning, troubleshooting issues, and maintenance. Implemented a GIT mirror for the r SVN repository, which enables users to use both SVN and GIT.
* Configured and maintained the Shell/Perl deployment scripts for Web logic and UNIX server, analysed the Maven Build projects for conversion.
* Migrated other ticket management tools to Jira server version and Migrated h2/postgres/oracle DB to MySQL database for Jira/Confluence server.
* Deployed Java Enterprise applications to Apache Tomcat, Web Server, and JBoss Application server.
* In the production environment, implemented and configured Nagios for continuous monitoring of applications and enabled notifications via emails and text messages.
* Involved in Building and configuring Red Hat Linux Servers using Kick Start server as required for the project. Maintained maximum uptime and performance capacity for enterprise production, QA, and UAT/staging.

**Environment:** CVS, SVN, Bamboo, Tomcat, Red Hat Enterprise Linux, Centos, Maven, Shell/Perl Scripting, ANT, Splunk, Puppet, Ngnix.