 **Anjali Rao Gunuganti**

A picture containing text, clipart

Description automatically generatedA picture containing text, clipart

Description automatically generated

**Sr. Cloud Engineer**

[**gunugantianjali@gmail.com**](mailto:gunugantianjali@gmail.com)

**737-238-0442  
 LinkedIn: https://www.linkedin.com/in/anjaliraogunuganti**

**Professional Summary**

* Dedicated 10 + years of experience in which 6 years of working as a Cloud DevOps and Site Reliability Engineer along with experience in Redhat Linux, CentOs, Ubuntu, and Windows environments, Cloud computing such as Azure DevOps through Continuous Integration (CI) and Continuous Deployment (CD) tools like Jenkins, Azure DevOps, Chef and Ansible. 4 years of Java Development Experience.
* Configured Continuous Integration from source control, setting up build definition within Visual Studio Team Services (VSTS) and configure continuous delivery to automate the deployment of ASP.NET MVC applications to Azure web apps and managed Azure Active Directory, Office 365 and applied upgrades on a regular basis.
* Implemented Okta authentication and authorization solutions for web applications, enabling secure and seamless user authentication using OpenID Connect (OIDC) and OAuth 2.0 protocols.
* Deployed CWPP solutions to safeguard cloud workloads and containers against advanced threats and malware, implementing runtime protection and vulnerability management.
* Integrated CWPP capabilities into Kubernetes orchestration environments, ensuring end-to-end security across containerized applications and microservices.
* Conducted thorough evaluations of CWPP vendors and technologies, selecting and implementing solutions aligned with organizational security requirements and compliance mandates.
* Configured and managed ADO agents to automate build, test, and deployment processes efficiently.
* Maintained and administered ADO Repos for version control, ensuring code integrity and collaboration among team members.
* Integrated Azure Key Vault (AKV) for secure storage and management of sensitive credentials, certificates, and secrets used in CI/CD pipelines.
* Developed and maintained shell scripts (Bash, sh) for system administration tasks, including file management, process automation, and system monitoring.
* Automated routine tasks and cron jobs using shell scripting, improving operational efficiency and reducing manual intervention.
* Created deployment scripts in shell to facilitate the installation and configuration of software packages and dependencies across multiple environments.
* Orchestrated and managed RedHat OpenShift Container Platform infrastructure, including installation, configuration, and ongoing maintenance of clusters.
* Implemented and managed Operators, OpenShift Data Foundation, OpenShift Pipelines, and Image Registry to streamline application deployment and management workflows.
* Experience in using Docker including Docker Hub, Docker Engine, Docker images, Docker compose, Docker swarm, and Docker Registry and used containerization to make our applications platform to be consistent flexible when they are moved into different environments.
* Designed, implemented, and maintained automated deployment pipelines for Hadoop clusters using tools like Ansible, Puppet, or Chef.
* Implemented Palo Alto Panorama for centralized management, policy orchestration, and monitoring of firewall deployments across distributed environments.
* Utilized Azure DevOps (ADO) Repos for version control, collaborating with development teams to manage source code and related artifacts.
* Developed Python scripts and automation tools to streamline manual processes, resulting in a significant reduction in deployment time and operational costs.
* Implemented data processing and analysis scripts in Python, utilizing libraries such as pandas and NumPy to manipulate and visualize large datasets.
* Designed and maintained RESTful APIs using Python frameworks like Flask and Django, enabling seamless integration with web applications and services.
* Leveraged Python for web scraping and data extraction tasks, employing libraries like BeautifulSoup and Scrapy to gather information from websites and APIs.
* Implemented branching and merging strategies within ADO Repos to facilitate code collaboration and manage code changes effectively.
* Expert in writing scripts like Power Shell, JSON, Node.js, YAML, Groovy, Bash/Shell, Python for automating the build and release process.
* Experience in system administration working on multiplatform VMware, LINUX (Red hat, SUSE), UNIX (Oracle Solaris 9/10) and windows server.
* Implemented Infrastructure as Code (IaC) principles using tools like Terraform or Ansible to automate the provisioning and configuration of infrastructure components required for RedHat OpenShift.
* Exposure to all aspects of Software Development Life Cycle (SDLC) such as Analysis, Planning, Development, Testing, Implementation, Post-production analysis of the projects.
* Knowledge of the Microsoft .Net Framework (WinForms, Web Forms, WCF, WPF).
* Utilized Java 7/8 features like Lambda expressions and Stream API for Bulk data operations on Collections which would increase the performance of the Application.
* Proficient in Java 8 features, Lambda Expression, Functional Interfaces.
* Experience in developing client-side validations using React JS, and in developing Custom pipes, Shadow DOM.
* Managed large-scale Hadoop clusters, ensuring high availability, scalability, and optimal performance.
* RIA applications using Flex, HTML5, CSS, Ajax, Dojo and Node JS
* Have good experience on NoSQL database like Mongo.
* Proficient in MVC architecture using spring framework / JSP-Servlet and J2EE Design Patterns

**Technical Skills**

|  |  |
| --- | --- |
| Cloud Environments | Microsoft Azure, Amazon Web Services (AWS) |
| Version Control Tools | GIT, GITHUB, GITLAB, Bitbucket, SVN |
| CI/CD Tools | Jenkins, Azure DevOps, Bamboo |
| Build tools | Maven, SonarQube, ANT |
| Automation Tool | Ansible, Terraform, ARM templates |
| Deployment Tools | Azure DevOps Server, Octopus |
| Monitoring Tools | Nagios, Splunk, ELK, CloudWatch, Azure Monitor, Prometheus, New Relic, Grafana. |
| Container Tools | Docker, Docker Swarm, Kubernetes, Mesos, OpenShift, Aws ECS. |
| Bug Tracking Tools | JIRA, Bugzilla, Remedy, HP Quality Center, IBM Clear Quest, Mingle Repositories Artifactory, Nexus |
| Database | Data Lake, Date Bricks, Cosmos DB, My SQL, MS SQL, Oracle, Dynamo DB, Cassandra, Mongo DB 7 SQL Server |
| Scripting & Programming Languages | Shell Scripting, RUBY, C, Java, XML, PL/SQL, HTML, PERL, Power Shell, Python, .Net, Gradle, Groovy |
| Application/Web Servers | Web logic, Web sphere, Apache Tomcat, Nginx, Oracle application server |
| Operating Systems | UNIX, Linux, Windows, Solaris, CentOS, UBUNTU and RHEL. |

**Certifications:**

* Certified Kubernetes Administrator
* AWS Developer – Associate
* Azure Administrator Associate

**Professional Experience**

**Sr Azure Cloud Engineer**

**United Airlines, Houston, TX, USA May 2022 to Present**

**Responsibilities:**

* Successfully migrated applications from private/internal cloud to Azure, establishing migration processes and patterns for development teams.
* Leveraged Palo Alto Networks' cloud security offerings and Cisco's networking solutions to ensure secure and scalable cloud environments.
* Configured virtual networks, subnets, and security groups, integrating Palo Alto and Cisco technologies for robust network security and traffic management.
* Provisioned multiple Azure resources, including Compute, Network, and Application Gateway. Managed dev, test, staging, and production environments using Azure ARM templates.
* Implemented Continuous Integration (CI) using Azure DevOps (VSTS) to facilitate an agile development process. Automated and repeatable deployment pipelines using VSTS, enabling safe code deployment in Azure Kubernetes Services (AKS).
* Led successful migrations from on-premises infrastructure to AWS cloud, ensuring seamless transition while strictly adhering to AWS security best practices.
* Demonstrated proficiency in AWS technologies, leveraging services such as EC2, S3, RDS, and VPC to architect scalable and secure cloud solutions.
* Extensive experience in designing and implementing high-availability and fault-tolerant AWS architectures, optimizing performance and reliability for mission-critical applications.
* Familiarity with container orchestration platforms including Amazon ECS Fargate and Amazon EKS, orchestrating containerized workloads efficiently on AWS infrastructure.
* Collaborated with cross-functional teams to architect, deploy, and manage AWS solutions, providing expertise in cloud infrastructure design, implementation, and optimization.
* Implemented security controls and compliance measures in AWS environments, utilizing AWS Identity and Access Management (IAM), AWS Key Management Service (KMS), and AWS CloudTrail.
* Implementing CNAPP to fortify security measures tailored specifically for cloud-native applications, ensuring their resilience against evolving cyber threats.
* Utilizing CNAPP to enforce security policies and protocols seamlessly within cloud-native architectures, safeguarding sensitive data and critical workloads.
* Leveraging CNAPP's advanced threat detection capabilities to proactively identify and mitigate security vulnerabilities across cloud-native application ecosystems.
* Integrating CNAPP into DevOps workflows to automate security processes and streamline the deployment of secure cloud-native applications.
* Implemented CI/CD best practices using ADO pipelines to achieve faster release cycles and improve overall software quality.
* Orchestrated pipeline stages and tasks to integrate with version control systems and deployment targets within the ADO environment.
* Utilized ADO pipeline templates and parameterization to promote reusability and maintainability across multiple projects.
* Implemented error handling and logging mechanisms in shell scripts to capture and report errors, facilitating troubleshooting and debugging efforts.
* Configured and managed Linux/Unix servers using shell scripts to set up users, permissions, and file systems in compliance with security policies.
* Collaborating with cross-functional teams to optimize the configuration and deployment of CNAPP, maximizing its effectiveness in securing cloud-native environments
* Collaborated with cross-functional teams to develop machine learning models and algorithms in Python, utilizing libraries like scikit-learn and TensorFlow.
* Applied object-oriented programming (OOP) principles in Python to design modular and reusable code, enhancing maintainability and scalability of software systems.
* Leveraged Palo Alto Networks' cloud security offerings and Cisco's networking solutions to ensure secure and scalable cloud environments.
* Configured virtual networks, subnets, and security groups, integrating Palo Alto and Cisco technologies for robust network security and traffic management.
* Provisioned multiple Azure resources, including Compute, Network, and Application Gateway. Managed dev, test, staging, and production environments using Azure ARM templates.
* Integrated ACR with CI/CD pipelines to automate image builds, vulnerability scanning, and deployment processes.
* Integrated third-party tools and services into ADO pipelines for code analysis, artifact management, and notification purposes.
* Employing CSPM solutions to continuously assess and enhance the security posture of cloud infrastructures, ensuring compliance with industry regulations and best practices.
* Utilizing CSPM to detect and remediate misconfigurations and vulnerabilities in cloud environments, reducing the risk of data breaches and unauthorized access.
* Worked on Azure ExpressRoute to establish connection from Azure to On-premise datacenter. Working knowledge on Azure Fabric, Micro services, Lot & Docker containers in Azure.
* Worked on Integrating Azure DevOps Boards with Microsoft Teams and Pipelines for Notifying Sprint Boards and Teams
* Designed and deployed Cisco networking solutions, including routers, switches, and wireless access points, to build scalable and resilient network infrastructures.
* Implemented Cisco ASA firewalls and Cisco Firepower Next-Generation Firewalls (NGFWs) for network security and threat prevention.
* Deployed Palo Alto firewalls to secure network traffic and protect against cyber threats in on-premises and cloud environments.
* Integrated Hadoop deployments into CI/CD pipelines using Jenkins, GitLab CI/CD, or similar tools, enabling rapid and reliable software delivery.
* Automated testing, packaging, and deployment of Hadoop applications, reducing manual errors and deployment time.
* Implemented security measures within CI/CD pipelines, including code scanning, vulnerability assessments, and compliance checks using Azure Security Center.
* Fostered collaboration by setting up and managing communication channels within Azure DevOps, ensuring effective communication among cross-functional teams.
* Implemented Azure AD Privileged Identity Management (PIM) to manage, monitor, and audit privileged roles and access rights, reducing the risk of insider threats and unauthorized access to critical resources.
* Worked on AWS Cloud platform and its features which includes EC2, VPC, S3, AMI, SNS, RDS, Cloud Watch, Auto scaling, Cloud Front, IAM, S3 for Configuring and managing IaaS. Wrote CloudFormation scripts to deploy different AWS Infrastructure components related to the respective services, managed various resources and data elements defined in the scripts.
* Deployed Cisco Umbrella for cloud-delivered security, protecting users and devices from internet-based threats such as malware, phishing, and ransomware.
* Configured and maintained CI/CD pipelines using Jenkins and GitLab to automate the build, test, and deployment of containerized applications on RedHat OpenShift.
* Administered and Engineered Jenkins for managing weekly Build, Test and Deploy chain as a CI/CD process, GIT with Development/Test/Prod Branching Model for weekly releases.
* Automated deployment pipelines using CI/CD tools such as Jenkins enabling swift and reliable updates to applications within the EKS ecosystem.
* Maintained version-controlled configurations for Hadoop services to facilitate reproducibility and disaster recovery.
* Implemented Azure Multi-Factor Authentication (MFA) and Microsoft Authenticator App to add an extra layer of security to user sign-ins, mitigating the risk of credential theft and unauthorized access.
* Designed and enforced Conditional Access Policies using Azure Active Directory and/or Intune (Microsoft Endpoint Management) to control access to applications and resources based on user context, device compliance, and risk factors.
* Managed Intune RBAC and Intune Connector to configure and enforce device management policies, ensuring compliance with security standards and regulatory requirements.
* Implemented Azure AD Join and Hybrid Azure AD Join to seamlessly connect devices to Azure Active Directory, enabling single sign-on (SSO) and access to cloud-based resources.
* Configured Intune Policies and/or Azure subscriptions to manage and secure endpoints, applications, and data on mobile devices and PCs, improving data protection and compliance posture.
* Administration of CentOS/RHEL 5.x, 6.x, 7.x, installation, testing, tuning, upgrading and patching, troubleshooting both physical and virtual servers. Installed, configured and maintained Tomcat, Apache and WebSphere Applications on Red Hat Linux.
* Configured Prometheus within an Amazon EKS environment to collect and analyze metrics from Kubernetes clusters and applications, facilitating precise monitoring and ensuring optimal performance and uptime.
* Utilized Grafana on EKS for advanced data visualization, creating custom dashboards to monitor Kubernetes cluster health and application performance, enabling swift identification and resolution of issues

**Cloud DevOps Engineer**

**Goldman Sachs, California, USA Jan 2020 to April 2022**

**Responsibilities:**

* Conducted thorough security assessments and audits for AWS deployments, identifying and remediating vulnerabilities to maintain a robust security posture.
* Actively involved in optimizing AWS costs and resource utilization, implementing cost-effective solutions and monitoring AWS billing and usage reports.
* Provided technical guidance and mentorship to junior team members, fostering a culture of continuous learning and innovation within the AWS engineering team.
* Stayed abreast of AWS best practices, emerging technologies, and industry trends, continuously enhancing skills and knowledge to drive innovation and excellence in AWS cloud engineering.
* Automating security checks and policy enforcement with CSPM to maintain a proactive security posture across dynamic cloud infrastructures.
* Integrating CSPM into DevSecOps pipelines to embed security controls throughout the software development lifecycle, fostering a culture of security and compliance.
* Providing comprehensive visibility and reporting capabilities through CSPM dashboards, enabling stakeholders to monitor and audit cloud security posture effectively.
* Configured access control policies and permissions in ADO Repos to enforce security and compliance requirements.
* Integrated ADO Repos with development tools and IDEs to enable seamless code editing, versioning, and collaboration workflows.
* Conducted regular repository audits and cleanup activities to optimize storage usage and maintain repository hygiene within ADO.
* Led migration projects for Teams, applications, devices, file shares, Exchange on-premises, and Exchange Online to Azure Active Directory, ensuring seamless transition and minimal disruption to business operations.
* Applied object-oriented programming (OOP) principles in Python to design modular and reusable code, enhancing maintainability and scalability of software systems.
* Conducted code reviews and provided technical guidance to junior developers, ensuring adherence to Python coding standards and best practices.
* Configured Azure Privileged Identity Management (PIM) to manage and monitor privileged roles and access rights in Azure Active Directory, reducing the risk of unauthorized access and potential security breaches.
* Experience in Azure infrastructure management (Azure Web Roles, Worker Roles, SQL Azure, Azure Storage, Azure AD Licenses, Office365) using Packer and Terraform and managed Azure Infrastructure through SCOM.
* Experienced in utilizing Azure Stack (Compute, Web &Mobile, Blobs, ADF, Resource Groups, Azure Data Lake, HDInsight Clusters, Azure Data Factory, Azure SQL, Cloud Services, and ARM) and services for configuring and deploying Azure Automation Scripts for multiple applications.
* Deployed multiple microservices into Azure Kubernetes by Dockerizing them and using Jenkins and Azure DevOps.
* Migrated the Build forge projects to Azure DevOps with all the work items, source codes, build and release pipelines by using custom PowerShell tool.
* Created Azure Automation Assets, Graphical runbooks, PowerShell Scripts that will automate specific tasks.
* Integrated Azure Key Vault (AKV) with Azure DevOps (ADO) pipelines to securely store and manage sensitive credentials, certificates, and secrets.
* Configured ADO pipeline tasks to retrieve and inject secrets from AKV during runtime, ensuring secure access to protected resources.
* Implemented access policies and role-based access control (RBAC) in AKV to restrict and manage permissions for pipeline operations.
* Automated secret rotation processes within ADO pipelines, enhancing security posture and compliance with regulatory requirements.
* Involved in Server less services (Azure Functions) where I created and configured HTTP Triggers in the Azure Functions with Application insights for monitoring and performing the load testing on the Applications.
* Worked on Bastion Server as a secure gateway to access resources within a private network from a public network in Azure.
* Communicated effectively with stakeholders to gather requirements, provide status updates, and address issues related to Hadoop infrastructure and XLR deployments.
* Enhanced container management and security by integrating Azure Container Registry with our deployment processes, optimizing container image storage and retrieval, and incorporating automated vulnerability scanning to maintain high-security standards.
* Provisioned and managed Azure AKS clusters using Terraform templates by creating Terraform modules for each environment.
* Created azure DevOps pipeline from scratch to deploy application into AKS cluster.
* Implemented disaster recovery strategies for Azure AKS by creating clusters in multiple regions ensuring business continuity and minimizing downtime in case of failures.
* Worked with Helm Package manager in creating custom charts as per application requirement and deployed them in Kubernetes Cluster.
* Implementing CIEM solutions to centralize and manage permissions and access controls across multi-cloud and hybrid cloud environments, ensuring least privilege access.
* Leveraging CIEM to enforce granular access policies and identity governance, reducing the risk of insider threats and unauthorized access to sensitive resources.
* Extensively designed and implemented CI (Continuous Integration) system: configuring Azure DevOps Build and Release servers, creating required scripts (PowerShell & Python), and creating/configuring VMs (Windows/Linux). Setup and configured continuous delivery within Azure using a combination of Azure Resource Manager (ARM) templates and Visual Studio Team Services (Azure DevOps).
* Extensively used Azure PaaS solutions and hosted Isolated App service environment integrated with PaaS Azure SQL and Virtual network to host different type of applications like Web app, API App, Function App etc.
* Wrote bash shell scripts for automation, deployments, server configuration, system tasks, iptables configuration, Kernel updates, package installation, and system resource inventory, resulting in increased productivity.

**DevOps Engineer**

**CVS Health, Minneapolis Nov 2017 to Dec 2019**

**Responsibilities:**

* Experience in Software Integration, Configuration, building, automating, managing and releasing code from one environment to another environment and deploying to servers.
* Worked with Windows, Linux and AWS teams to resolve issues and plan for infrastructure changes.
* Provided documentation of solutions for VMWare, Windows, and Linux and AWS teams.
* Launching EC2 instances and involved in AWS RDS, S3, Load Balancing, IAM, VPC, Cloud Formation, Lambda, and Cloud Watch.
* Automating entitlement reviews and access certification processes with CIEM to streamline compliance efforts and maintain security hygiene.
* Integrating CIEM with identity and access management (IAM) solutions to orchestrate consistent access controls and authentication mechanisms across cloud environments.
* Collaborating with identity governance teams to align CIEM policies with organizational security policies and regulatory requirements, ensuring compliance and risk mitigation.
* Used AWS Route53, to route the traffic between different availability zones. Deployed and supported Mem-cache/AWS Elastic-Cache and then Configured Elastic Load Balancing (ELB) for routing traffic between zones.
* Working closely with Cassandra loading activity on history load and incremental loads from Teradata and Oracle Databases and resolving loading issues and tuning the loader for optimal performance.
* Written Templates for AWS infrastructure as a code using Terraform to build staging and production environments.
* Worked on Multiple AWS instances set the security groups, Elastic Load Balancer (ELB) and AMIs, Auto-scaling to design cost effective, fault tolerant and highly available systems.
* Implemented cloud services IAAS, PAAS, and SaaS, which include Open stack, Docker and Open Shift.
* Designed and worked with team to implement ELK (Elastic search, Log stash and Kibana) Stack on AWS.
* Migrated the production SQL server schema to the new AWS RDS Aurora instance.
* Wrote SQL queries and worked on administration for optimizing and increasing the performance of database.
* Installed and administered Docker and worked with Docker for convenient environment setup for development and testing.
* Developed Scripts for AWS Orchestration using EC2, EBS, S3, Cloud Formation and IAM.
* Develop/capture/document architectural best practices for building systems on AWS.
* Installed Docker Registry for local upload and download of Docker images and even from Docker hub.
* Worked on the Docker ecosystem with a bunch of open-source tool like Docker machine, Docker Compose, Docker Swarm.
* Expand Red Hat Open Shift Container Platform solution to multiple CPU architectures
* Worked on AWS Cloud Watch for monitoring the application infrastructure and used AWS email services for notifying & configured S3 versioning and lifecycle policies to and backup files and archive files in Glacier.
* Used the JIRA, Confluence for bug tracking, creating the dashboard for issues.
* Configured AWS IAM policies for user’s roles using JSON and adding project users to the AWS account with Multi-Factor authentication enabled and to protect data at transit used Transport Layer Security Protocol.
* Managing and optimize the Continuous Integration using Jenkins and troubleshoot the deployment build issues using the trigged logs.
* Carried automated Deployments and builds on various environments using continuous integration (CI) tool Jenkins.
* Used Git for source code version control and integrated with Jenkins for CI/CD pipeline, code quality tracking and user management with build tools Maven and Ant.
* Using deployed and configured Elastic search, Log stash and Kibana (ELK) for log analytics, full text search, application monitoring in integration with AWS Lambda and Cloud Watch.
* Created custom AWS CloudFormation templates in JSON tailored to our organization requirements to use them as blueprints for building & deploying EKS clusters which will set the proxy configured dynamically during the cluster creation.
* Involved in Architecting, building, and maintaining highly available secure multi-zone AWS cloud infrastructure utilizing Chef with AWS CloudFormation and Jenkins for continuous integration
* Deployed Puppet for configuration management to existing infrastructure.

**Java Developer**

**Invesco, Hyderabad, India Dec 2012 to Oct 2016**

**Responsibilities:**

* Involved in complete development of Agile Development Methodology/SCRUM, developed, and tested the application during various iterations.
* Responsible for creating Class diagrams, Sequence diagrams, Use Case diagrams, Object Model diagrams and deployment diagrams using Rational Rose for migration modules.
* Used Collection Framework and Multithreading for performing cache Operation.
* Developed, and debugged the servlets and EJB with WebSphere Application server.
* Developed the middle tier using EJBs, Java Servlets, session, entity beans and message driven beans.
* Designed and developed the UI using Struts view component, JSP, HTML, CSS and JavaScript, AJAX, JSON.
* Designed and developed web pages using HTML5, DHTML, XHTML, CSS3, Ajax, JSP and JQuery based on the W3C standards and Web 2.0.
* Achieved role control functionality mainly by retrieving JSON data from AJAX and combining the retrieved data with jQuery to manipulate nodes in the DOM tree.
* Utilized a combination of regular expression and jQuery Validation Plugin to conduct input check.
* Designed the data flow for the client-side screens and the object interaction layer for the server-side components using Rational Rose.
* Involved in Use Case Diagrams, Class Diagrams and Sequence diagrams using Rational Rose.
* Used XML/XSLT for transforming common XML format and SAML for Single Sign-On.
* Designed configuration XML Schema for the application.
* Developed Maven scripts and developed builds using Maven and continuous integration servers like Jenkins.
* Used JavaScript for client-side validation.
* Used XML Http Request Object to provide asynchronous communication as part of AJAX implementation.
* Prepared the test plans and executed test cases for unit, integration and system testing using different automation tools like Junit, Soap UI and Fiddler.
* Performance Testing experience using JMeter.