

# Jessica Claire

100 Montgomery St. 10th Floor • (555) 432-1000 • resumesample@example.com

## Summary

**Profile Summary** Over 9.5 years of IT Industry Experience with 5.3 years as DevOps Engineer Cloud Expertise: IaaS/PaaS service: Extensive experience in developing cloud solutions using IaaS (Infrastructure as a Service) and PaaS (Platform as a Service). VPC Network: Experience in configuring secure VPC through Private and Public networks in AWS and Azure.

## Skills

<b>Technical skills:</b>	<b>Platforms</b> Linux, Windows
<b>Cloud Platforms</b> AWS, CenturyLink, GCP, Azure	<b>Web/Application Servers</b> Apache2, Tomcat, Nginx
<b>DevOps services</b> Git, Jenkins, Maven, Ansible, Zabbix, ELK Stack, <b>Scripting Languages</b> Shell	
Docker, Jira	
<b>DBs</b> MongoDB, MySQL, Oracle	

## Experience

**Consultant**, 06/2021 to 01/2022

**Eplus Technology** – Irvine, CA

- TCS is Helping Clients Create the Future TCS combines tech expertise and business intelligence to catalyze change and deliver results.
- The primary responsibilities include:
- Integrated Amazon Cloud Watch with Amazon EC2 instances for monitoring the log files, store them and track metrics
- Integrated Cloud Front with S3 for data security
- Created AWS S3 buckets, performed folder management in each bucket, Managed cloud trail logs and objects within each bucket
- Created Highly Available Environments using Auto-Scaling, Load Balancers, and SQS
- Create Ansible Automation tools and builds and do an overall process improvement to any manual processes
- Developed and maintained the continuous integration and deployment systems using Jenkins, Maven
- Configured Elastic Load Balancers with EC2 Auto Scaling groups
- Experience in building Docker images using GitLab-ci build automation runner
- Automated deployment from GitLab-ci to Openshift
- Used Docker for running lower environments like DEV and UAT
- Created monitors, alarms and notifications for EC2 hosts using Cloud Watch
- Ability to design application on AWS taking advantage of Disaster recovery
- Configured AWS Identity Access Management (IAM) Group and users for improved login authentication
- As a part of Job I also had responsibility to maintain the networking form AWS cloud back to On-Primary connectivity and no direct internet access from AWS cloud VPC to the rest of the world (Internet)
- Worked with Custom AMI's, created AMI tags and modified AMI permissions
- Created Security Groups, configuring Inbound /Outbound rules, creating, and importing Key Pairs
- Leveraged Jfrog service as Build Artifact repository
- Technologies : Linux, GitLab, Maven, Ansible, AWS, Oracle, Openshift, Jira, Servicenow
- Environment: AWS (EC2, VPC, ELB, S3, CloudFront, Cloud Trail and Route 53), Linux (Ubuntu), Amazon Linux, Git version Control, VPC, Jira, AWS Auto Scaling, Maven.

**DevOps Engineer**, 08/2019 to 05/2021

**Koch Industries, Inc.** – Reno, NV

- Neutara is a US based technology company expertise in innovating cloud and e-commerce. It built several products and services in the areas of e-commerce, cloud, productivity, and enterprise collaboration
- The primary responsibilities include:
- Integrated CloudFront with S3 for data security
- Created AWS S3 buckets, performed folder management in each bucket, Managed cloud trail logs and objects within each bucket
- Created Highly Available Environments using Auto-Scaling, Load Balancers, and SQS
- Experience in AWS Cloud in various AWS Services such as Cluster, Route53 Domain configuration
- Create Ansible Automation tools and builds and do an overall process improvement to any manual processes
- Developed and maintained the continuous integration and deployment systems using Jenkins, Maven
- I have implemented CI pipelines on several consumer facing applications supporting Agile Projects and Ongoing Releases
- Configured Elastic Load Balancers with EC2 Auto Scaling groups
- Configured S3 to host Static Web content
- Experienced in S3 Versioning and lifecycle policies to and backup files and archive files in Glacier
- Configured AWS Identity Access Management (IAM) Group and users for improved login authentication
- As a part of Job I also had responsibility to maintain the networking form AWS cloud back to On-Primary connectivity and no direct internet access from AWS cloud VPC to the rest of the world (Internet)
- Worked with Custom AMI's, created AMI tags and modified AMI permissions
- Created Security Groups, configuring Inbound /Outbound rules, creating, and importing Key Pairs
- Leveraged AWS S3 service as Build Artifact repository and created release-based buckets to S3
- Technologies: Linux, Git, Maven, Ansible, Jenkins, AWS, CENTURYLINK(Cloud),
- Kibana, Zabbix, Docker, Jira
- Environment: AWS (EC2, VPC, ELB, S3, CloudFront, Cloud Trail and Route 53), Linux (Ubuntu), Amazon Linux, Git version Control, VPC, AWS EC2, S3, Route53, EBS, IAM, ELB, Jira, AWS Auto Scaling, Maven.

**DevOps Engineer**, 10/2015 to 04/2019

**Koch Industries, Inc.** – Troy, MI

- Paytm is also a leading payment solutions provider to e-commerce merchants using its RBI approved semi-closed wallet. One97 delivers mobile content and commerce services to millions of mobile consumers through India's most widely deployed telecom applications cloud platform
- The primary responsibilities include:
- Created AWS S3 buckets, performed folder management in each bucket, Managed cloud trail logs and objects within each bucket
- Created Highly Available Environments using Auto-Scaling, Load Balancers, and SQS
- Hands on Experience in AWS Cloud in various AWS Services such as Cluster, Route53 Domain configuration
- Defined branching, labeling, and merge strategies for all applications in Git
- Configured Elastic Load Balancers with EC2 Auto Scaling groups
- Configured S3 to host Static Web content
- Experienced in S3 Versioning and lifecycle policies to and backup files and archive files in Glacier
- Used Docker for running different testing applications
- Ability to design application on AWS taking advantage of Disaster recovery
- Versed Configuring Access for inbound and outbound traffic EBS volumes to set alarms for notifications or automated actions
- Configured AWS Identity Access Management (IAM) Group and users for improved login authentication
- As a part of Job, I also had responsibility to maintain the networking form AWS cloud back to On-Primary connectivity and no direct internet access from AWS cloud VPC to the rest of the world (Internet)
- Worked with Custom AMI's, created AMI tags and modified AMI permissions
- Created Security Groups, configuring Inbound /Outbound rules, creating, and importing Key Pairs
- Leveraged AWS S3 service as Build Artifact repository and created release-based buckets to S3
- Technologies: Linux, Git, Maven, Jenkins, AWS, Docker
- Environment: AWS (EC2, VPC, ELB, S3, Cloud Trail and Route 53), Linux (RHEL 6.1/6.6), Amazon Linux, Git version Control, VPC, AWS EC2, S3, Route53, EBS, IAM, ELB, Jira, AWS Auto Scaling, Maven.

**Linux Engineer**, 06/2012 to 09/2015

**Verizon** – Flushing, NY

- The primary responsibilities include:
- Creating Server with IP & Based on the Requirements Ports will be assigned
- Creations of pools
- Configuring Event for each port
- Based on the requirements, shall create OBD, SERVICE, PATCHING & FLASH
- Configuring Beachcomber for applications
- Domains configurations
- Maintaining the running of the applications
- Monitoring the applications
- Troubleshooting the application
- Security

## Education and Training

**Bachelor of Engineering:** Computer Science

**Jawaharlal Nehru Technological University (JNTU) - Hyderabad**

## Additional Information

- configuration: Configured auto scaling policies to scale up/down EC2 instances based on ELB health checks and created alarms to be used in auto scaling decision making policies. Infrastructure as a code: Experience in building environment on cloud with Terraform-tool for building and changing infrastructure safely and efficiently. S3 access management: Provisioned AWS S3 buckets for backup of the application and sync contents with remaining S3 backups, by creating entry for AWS S3 SYNC in Crontab. And restricted public access with CloudFront service. Provided 24 x7 on-call supports in debugging and fixing issues related to Cloud Environment using Amazon Web Services (AWS) and CenturyLink. DevOps Expertise: SCM: Extensive experience in deploying and administering GitHub & GitLab. Configuration management tool: Extensive experience in Ansible for deploy consistent infrastructure code across multiple environment. CICD: Integrated Jenkins with maven and docker, And automated application deployment on containers with pipeline. Containerization: Containerizing the application using Docker & deployment of Docker containers for development. Monitoring: Experience in installing and configuration Zabbix for server resource monitoring, And Kibana for Application logs monitoring. Having good Experience in configuring and working with FTP and NFS. Collaborate with application owners, IT operations and cloud providers to translate business and functional requirements into infrastructure solutions.