RANJAN KUMAR

DevOps Engineer

📞**:** +91-7020003950   📧**:** yadavranjan33@gmail.com   in**:** linkedin.com/in/ranjan-yadav-3b5aa419b

PROFESSIONAL SUMMARY

Experienced DevOps Engineer with demonstrated history of working in Multi-Cloud ecosystem and Development-Operations Environment. Aims to increase my knowledge and utilize skills in the growth of the organization.

TECHNICAL EXPERTISE

SCM: Bitbucket, GitHub, Gitlab, Azure Git

Cloud Computing: AWS, GCP and Azure

Orchestration: Kubernetes, and OpenShift

Virtualization Tools: Docker, Virtual Box, Vagrant

Automation Tools: Ansible, Terraform, CloudFormation

Programming Language: NodeJS, Django, Java

Enterprise Tools: Morpheus, CommVault, Terraform Enterprise, RedHat Satellite

Build Automation Tools: Jenkins, AWS CodePipeline, Gitlab CI, Azure DevOps

OS: CentOS, RHEL, Ubuntu, Windows, Mac

Scripting: Shell, Powershell, Python, YAML

Databases: PostgreSQL, MySQL

Web Servers: Nginx and Apache

Code Quality Test: SonarQube, Checkov

Linux: HTTP, ISCSI, FTP, NFS, DNS, SSH, LVM, LDAP, ACL, Cronjobs, Permissions

Other Tools: Jira, Nexus, Active Directory, Slack,ServiceNow, Apache Hadoop

PROFESSIONAL EXPERIENCE

Hashedin by Deloitte (13th Jan 2020 - Present) Bengaluru

Unisys: Multi-Cloud CMP

- Worked on Morpheus (100% Agnostic Hybrid Cloud Management Platform- CMP) to create Blueprints, Tasks, Workflows, Apps to work with AWS, Azure, GCP, and VMWare.
- Implemented Morpheus Single Sign-On (SSO) to Morpheus Application. SAML is integrated with Morpheus and an enterprise application is created in Azure to enable Azure AD SAML based SSO.
- Setup VPN Tunnel Connectivity between Azure VNet to AWS VPC and Azure VNet to GCP VPC for Inter VPC and VNet Communication between Private Subnets.
- Registered AWS, Azure, GCP and VMware Instances to Windows Active Directory Domain using Powershell and Shell Scripts such that Instances can be logged in via users from Windows Active Directory.
- Automated Cloud Enhancement Services and Extension Services like Joining Active Directory Domain, Cloud Native Backup, CommVault Backup, Cloud Native Monitoring, Vanda Monitoring, Cloud Native Patching, Satellite, and Winsus Patching.
  - Automated Patching Solution in Azure using Azure Automation account, azure log analytics with Morpheus Blueprint. So as the Instance gets provisioned, it gets registered to Azure Automation account and the patch gets installed at its Maintenance window.
  - Automated Monitoring Solution in Azure using Azure Monitor for Windows and Linux Instances. Created

Region Native Powershell Script and Shell Script to install monitoring Agent and Monitor Disk, CPU, Memory, and Health Status at Regular Intervals and create an alarm for the same.

- Automated Monitoring Solution in Vanda for Windows and Linux Instances. Powershell Script and Shell Script to install Monitor AWS, Azure, and VMWare Instances using Vanda.
- Automated Backup Solution in Azure using Azure Backup Service to configure backup policies and monitor backup activity for your Azure resources in one place

- DevSecOps CI/CD Story for CMP
    - Set up and configuration of Jenkins build machine (Slave node) for CMP. Integration with SCM, create a WHL file from the Python scripts, Include the WHL file and the scripts (terraform, ansible, python) in an installable package (.zip format). Save the Build Package with Build Number and Timestamp, and Upload the build artifacts (.zip file) to the Nexus repository
    - Analysis of IaaS Scripts using Checkov Static Code Analysis Tool to scan cloud infrastructure managed in Terraform and increase security and compliance best practices.
    - Did the Build Deployment that Runs Terraform Script to provision Azure Infrastructure, running Shell Script as part of Terraform script to install Morpheus Package in Provisioned Linux VM, and run the Python Enrichment Script to import CMP Configurations.
    - Clone the Sanity Test Code in Windows Node, Passing the Appliance URL in Jenkins from Linux Node to Windows Node and Run Powershell Commands to execute Python Automation Scripts for Sanity Testing in Windows Node.
    - Setup Email Approval Step in Jenkins to destroy Terraform Resources and Cleaning up of Workspace.
- DevSecOps K8s Story for CMP.
    - Worked on the Creation of AKS, EKS, and Kubernetes Cluster from CMP Morpheus. Deploy a Sample App in AKS Cluster and Create Helm Deployment.
    - Created Jenkins Server, Integrated to Bitbucket, Build Docker Image of the Code, Push Docker image to ACR, and Deploy containers using Morpheus Helm Charts. Monitor application status running in containers from Morpheus Console
- Created Ansible Playbooks for Installing Packages, Configuring the Servers with Kerberos Authentication for Windows and Linux (Ubuntu, RHEL, Centos, Amazon Linux) Servers. Incorporated Ansible Vault to Store Sensitive/Secret Data. Integrated Ansible with Morpheus.
- Created SSL Certificates and attached them to the Morpheus Nginx Servers to expose the Application on HTTPS.
- Created Shell Scripts and PowerShell Scripts for Scripts Cleanup, Logging Aggregation of every task in Shell Script/PowerShell Script, Exception Handling, Installing Immediate Patches in Instances (Windows and Linux) after Provisioning.
- Did Server Hardening for Unisys Environment - Creation of Bastion Hosts, Restricting Ports, Creating Load Balancers for Accessing traffic on 443, Azure Application Gateway, Azure WAF, Azure Security Center, Azure policies, Azure Log analytics, Azure monitor and alerts, Optimized their Monthly AWS/Azure Billing.
- Created Rules to trigger Azure function on a schedule to stop and start VM at regular intervals.
- Deploy the Landing Zone using terraform for production environment.
- Used terraform script as one click solution to provision cloud related resources like VM, VM Scale sets, Application Gateway, configuration of gateways, Azure Web Application Firewall and trigger python scripts for deploying the morpheus application on the instance and providing endpoints.
- **Technologies used** - Morpheus, Ansible, AWS, Azure, GCP, Shell Script, PowerShell Script, Jenkins, Kubernetes

Globallogic: JCI

- Deployed Openshift Cluster for the client Johnson Controls with proper security
- Implemented Aviatrix for VPN based logins as we had a cloud agnostic environment. Creating user profiles as per the access requirement like Dev/QA/Staging/Production. With help of the Aviatrix controller it was a piece of cake to manage the access for big clusters.
- Setup of Azure Application Gateway, WAF, ASG, NSG, traffic manager, ASC, Azure policies for the security purpose.
- Configured Highly Available nginx cluster on the Azure VM having different layers like TLS, Reverse Proxy, WAF providing protection from any type of attacks.
- Configured Consul/Vault for storing the secrets that was used inside the openshift cluster.
- Setup Azure Webapp and Azure functions for deploying microservices.
- Setup Azure Devops Pipeline to deploy the application in Azure SQL server or Azure Webapp or Azure functions.
- Created a self hosted agent on azure devops pipeline to run multiple pipelines parallely and make the process faster.
- Create production environment for deploying openshift cluster considering proper security, High availability, VPN, Load balancer, with terraform and ansible scripts.
- Written terraform scripts to provision the cluster of 12 nodes in azure
- Used terraform modules for cluster provisioning, stored the backend file in azure storage account
- Written jenkinsfile for provisioning the cluster using terraform
- Added proper security rules in the openshift cluster using terraform.
- Written ansible playbooks to install necessary packages, mount the volume for docker and install prerequisites for OpenShift cluster.
- Created Jenkins pipeline to containerise the application and deploy it in Openshift cluster.
- Configured JFROG for storing artifacts, storing docker images, running X-RAY Scans on images, blackduck and many more.
- Integrated sonarqube with Jenkins pipeline to check the code coverage and quality.
- Written helm charts to deploy the application to openshift cluster.

  Technologies Used: Azure, Openshift, Jenkins, Terraform, Azure Devops, Azure webapp, Azure functions, WAF, Application Gateway, nginx setup, Aviatrix, Docker, ASE, Helm, JFROG, Sonarqube, dynatrace, Jenkins.

BITS Pilani: EOn

- Automated Provisioning of VPC with Public and Private Subnets, EC2, ASG, LB, SG, Elastic Beanstalk Environment, Route53 Alias, S3 Buckets, CloudFront Distribution, RDS using Terraform. Maintained 3 different environments: Dev, QA, Prod for CodePipeline, RDS and Elastic Beanstalk with separate configurations.
- Created Multi-Stage CI/CD Pipeline for Frontend and Backend.
- Backend Pipeline takes source from GitHub, builds the Application Code & Pushes Docker Images to AWS ECR, does Unit/Functional Testing, and finally Deploys the tested application into Elastic Beanstalk.
- Frontend Pipeline takes source from GitHub, Builds the React Front End, Synchronizes the contents of a S3 bucket with Latest Changes, and Invalidates CloudFront Distribution.
- Integrated third-party Monitoring and Logging Tools. For Ex. Used Filebeat, ELK Stack for Docker Log Aggregation,

Indexing, Visualization, Used AWS CloudWatch and AWS Custom Metrics for Infrastructure Monitoring.

- Configured SES Server for sending out emails using the SMTP server. Setup SNS Notification using CloudWatch Event Rules which gets triggered on Pipeline Execution. Configured data management and secrets management in AWS SSM Parameter Store to store sensitive environment variables.

FUJITSU Fujitsu Consulting India (Oct 2016 – Jan 2020) Bengaluru

Blockchain As a Service: NodeJs & DevOps

- Created a PoC on Blockchain as a Service and got a customer based on that with one trigger platform setup which automatically provisions a sample Hyperledger Fabric network consisting of four organizations, each maintaining one peer node, and a kafka ordering service. Also, the script creates a channel, joins all peers to the channel, install chaincode on all peers and instantiate chaincode on channel. The pattern also helps to drive execution of transactions against the deployed chaincode.
- Worked on node SDK and cli for doing transactions on hyperledger fabric.
- Experience in deploying and configuration of Blockchain as a Service along with the components like EFK, GAP, Gluster FS, and Calico on azure cloud.
- Experience in writing chaincodes in Golang and calling them using Node SDK.
- Worked on security features like creation of HSM wallet instead of filesystem wallet for advanced level security.
- Build Automation scripts to deploy the above hyperledger fabric using Ansible Playbooks for azure cloud.
- Knowledge of Docker, Docker Enterprise edition, Kubernetes, App Containerization and deployment.
- Experience in creating CI/CD pipeline on kubernetes using DevOps tools like GitLab, Maven, SonarQube, Jenkins and Junit.
- Experience in managing servers, storage, clusters, SSH access, firewalls, networking, DNS configuration for Routing, in Azure and AWS.

ChatOps: DevOps

- Created a POC on ChatOps i.e. a branch of DevOps focusing on communication within the DevOps team using the chat server(slack), StackStorm and ansible and has performed various actions like infra deployment and checking status of the server from chat window etc.

Container Infra Design: DevOps

- Experience in deploying and configuration of OpenShift Origin and OpenShift Enterprise along with the components like EFK, GAP, Gluster FS, and Calico on K5 and azure cloud.
- Build Automation scripts to deploy the above OpenShift components using Ansible Playbooks for K5 and azure cloud.
- Knowledge of Docker, Docker Enterprise edition, SWARM, Kubernetes, App Containerization and deployment.
- Experience in creating CI/CD pipelines on OpenShift using DevOps tools like GitLab, Maven, SonarQube, Jenkins and Junit.
- Experience in managing servers, storage, clusters, SSH access, firewalls, networking, DNS configuration for

Routing, in Azure, K5 Cloud and AWS.

ACHIEVEMENT:

- Got ASTERIX award for contributing alone for deploying EFK and writing chaincodes with a very tight timeline.
- Got Spot award for Unisys Project to win the customer delight in very less time.

EDUCATION:

- Post Graduate Diploma in Advanced Computing (PG-DAC) from C-DAC, Pune.
- Bachelors of Technology in Electronics Engineering from DY Patil Institute of Engineering and Technology, Pune (Maharashtra).