My name is **name**, coming to my background, I have totally 5+ Years of IT Experience especially in On-premises & Cloud administration and DevOps Activity. In My previous experience I handled On-premises infrastructure Where my day to day activities are Provisioning and managing the Virtual Machines in VMware, and Active Directory and Office 365 administration and Datacentre Maintenance, Updating the patches on Monthly basis, Fixing the Security Vulnerabilities which is identified in VAPT (Vulnerability Assessment and Penetration Testing) and Performing the DR Activity on quarterly basis like (ISP Failover, Backup and Recovery, VMware Host failover like that.)

Parallelly, we maintained Client environment in AWS and Azure cloud as well. I have involved in designing and implementing the client infrastructure in AWS.

Where I had an exposure to work on varies AWS services like EC2, Load Balancer, Autoscaling, S3, EFS, IAM, VPC, cloud front, cloud watch, cloud trail and Route 53. my day-to-day activities are like Launching an Ec2 instances and mounting the EFS in it and creating snapshot and volume for the critical instances, creating the users and groups in IAM and assigning the permission and roles and Monitoring the Ec2 instances, ensuring that MFA was implemented for all the AWS Users if not I have to take care of it. and Creating a Elastic Bean Stack for the developer to test their applications. Implementing the Life cycle policies in S3 bucket. I have to Block the unused Ports in **subnet**(A subnet, or subnetwork, is a segmented piece of a larger network. More specifically, subnets are a logical partition of an IP network into multiple, smaller network segments. The Internet Protocol (IP) is the method for sending data from one computer to another over the internet) level NACL, and regularly need to fix the recommendations that are provided by **AWS Trusted advisors**(It inspects your and it provides best practice recommendations when opportunities exist to save money improves system availability and performance, there are specific set of checks in each pillar, the checks are based on best practices in each AWS service as well as learning from serving customers over time. For each check trusted advisors provided recommendations typically based on specific resources ). We are provisioning our entire infrastructure using terraform template.

I have hands on experience in DevOps tools like GitHub, Jenkins, Ansible, Docker and Kubernetes and terraform.

I had experience in deploying the microservice application inside AWS Kubernetes Cluster. For that I had created CI CD pipeline using a **Jenkins groovy file** which contains different stages like **Code Checkout**,

maven Build,

testing and

**Docker image** creation and pushing created image into a **docker hub registry** and we using **Yaml file** for deployment and service once we triggered the **yaml file application** will deployed in Kubernetes.

**SRE:**

Every month we do have monthly releases. We are following a **blue green deployment** in Prod environment. In Dev and QA, we are **following rollback**.

We will Help Operations and Support Teams, Fixing Support Escalation Issues, documenting all the issues and uploading in confluence page, we do Conduct Post-Incident Reviews.

We do follow Disaster Recovery Process for 6 months once.