

Job Description: Site Reliability Engineer Intern

Company: Blue Copper Technology

Location: Kolkata

Shift - Project Based

Role Overview

As a **Site Reliability Engineer Intern**, you will be responsible for ensuring the **availability, performance, and reliability** of our products/projects. You will work closely with development and infrastructure teams to build stable systems and proactively prevent issues.

Key Responsibilities

- Define and manage SLIs, SLOs, and error budgets
- Ensure high availability, performance, and scalability
- Monitor systems using metrics, logs, and traces; set up effective alerting
- Handle incidents, on-call duties, and postmortems
- Automate deployments, scaling, and recovery to reduce manual work
- Manage infrastructure using IaC (e.g., Terraform)
- Operate and scale containerized systems (e.g., Kubernetes)
- Plan capacity and optimize infrastructure costs
- Implement backup, disaster recovery, and resilience strategies
- Improve system reliability through testing (load, chaos, failover)
- Ensure production systems meet security and compliance standards
- Support reliability of ML/data systems (pipelines, inference, drift monitoring)
- Collaborate with CSE and FDE to improve production readiness and system design

Required Skills

- Understanding of **Linux/Unix & Windows systems**
- Experience with Docker/Kubernetes
- Knowledge of **cloud platforms** (AWS/Azure/GCP – any one)
- Familiarity with monitoring tools (e.g., CloudWatch, Site24X7, Azure Monitor, Zabbix etc.)
- Understanding of APIs, web applications, and system architecture
- Strong scripting and automation skills using Python/Bash
- Understanding of incident handling and troubleshooting
- Good problem-solving and analytical skills
- Hands-on experience with infrastructure-as-code tools (Terraform, CloudFormation, or Ansible)
- Understanding of relational and/or NoSQL databases (e.g., PostgreSQL, MySQL, MongoDB, SQL Server) — query debugging, replication, and performance basics.
- Awareness of security best practices — secret management (e.g., Vault, AWS Secrets Manager), least-privilege access, and basic compliance awareness (SOC2/ISO awareness a plus)
- Exposure to **DevOps practices**
- Knowledge of CI/CD tools (Jenkins, GitHub Actions, etc.)
- Understanding of microservices architecture