Position: HashiCorp Vault Contractor (DevOps Focus)

Location: Bangalore

Term: 6 Months (Extendible)

Notice Period: Immediate Joiner

Experience	Budget
5 - 6 years	1.5 - 1.8 LPM + GST
7-10 years	2 - 2.4 LPM + GST

Job Description: We are seeking an experienced HashiCorp Vault Contractor with a strong DevOps focus to join our team in Bangalore. The ideal candidate will have a proven track record in deploying, managing, and securing HashiCorp Vault in production environments. This role requires expertise in DevOps tools and technologies, Linux administration, security and compliance, scripting, and automation. The successful candidate will play a crucial role in ensuring the secure management of secrets and sensitive data across our infrastructure.

Key Responsibilities:

- **HashiCorp Vault Management:** Deploy, configure, and manage HashiCorp Vault in production environments. Handle Vault clusters, including backup, recovery, and performance tuning. Implement and manage Vault's authentication methods, secret engines, and access control mechanisms.
- **DevOps Integration:** Set up and integrate Vault with CI/CD tools such as GitHub Actions, Jenkins, GitLab CI, or Azure DevOps. Utilize Terraform for provisioning Vault infrastructure and integrate with other IaC tools like CloudFormation or Pulumi.
- **Configuration Management:** Use tools such as Ansible, Chef, or Puppet for managing Vault configurations and ensuring consistency across environments.
- **Containerization and Orchestration:** Secure secrets within containerized environments using Docker and Kubernetes. Ensure Vault is effectively integrated into container orchestration platforms.
- **Version Control and Automation:** Manage source code with Git, including experience with GitHub Actions for automating workflows. Develop and maintain automation scripts using Python, Bash, or PowerShell to streamline Vault operations.
- **Linux Administration:** Administer and troubleshoot Linux-based environments hosting Vault. Apply system monitoring, performance tuning, and security hardening best practices.

- **Security and Compliance:** Implement Vault in compliance-driven environments, adhering to standards such as SOC 2, GDPR, or HIPAA. Apply security best practices, including encryption, key management, and access control.
- **Monitoring and Logging:** Monitor Vault's performance and security metrics using tools like Splunk or New Relic. Experience with Prometheus and Grafana is a plus.
- **Networking:** Understand and configure networking concepts including firewalls, VPNs, and secure network configurations. Troubleshoot network settings related to Vault and its integrations.
- **Cloud Platforms:** Work with public cloud platforms (AWS, Azure, GCP) or private cloud platforms (VMware, OpenStack). Integrate Vault with cloud-based services and infrastructure.

Required Skills and Experience:

1. **HashiCorp Vault:**
    - Experience deploying and managing Vault in production environments.
    - Knowledge of Vault's authentication methods, secret engines, and access control mechanisms.
    - Experience with managing Vault clusters, including backup, recovery, and performance tuning.
2. **DevOps Tools and Technologies:**
    - CI/CD Pipelines: Expertise in integrating Vault with tools like GitHub Actions, Jenkins, GitLab CI, or Azure DevOps.
    - Infrastructure as Code: Proficiency with Terraform and experience with CloudFormation or Pulumi.
    - Configuration Management: Experience with Ansible, Chef, or Puppet.
    - Containerization and Orchestration: Knowledge of Docker and Kubernetes, including securing secrets in containerized environments.
    - Version Control: Proficiency with Git and experience with GitHub Actions.
3. **Linux Administration:**
    - Strong knowledge of Linux systems administration.
    - Experience with system monitoring, performance tuning, and security hardening.
    - Ability to manage and troubleshoot Linux-based environments hosting Vault.
4. **Security and Compliance:**
    - Understanding of security best practices including encryption, key management, and access control.
    - Experience implementing Vault in compliance-driven environments (e.g., SOC 2, GDPR, HIPAA).
5. **Scripting and Automation:**
    - Proficiency in Python, Bash, or PowerShell.
    - Ability to create and manage automation scripts for Vault operations.
6. **Monitoring and Logging:**
    - Experience with monitoring tools like Splunk or New Relic.
    - Familiarity with Prometheus and Grafana is a plus.
7. **Basic Networking Knowledge:**

    - Understanding of networking concepts including firewalls, VPNs, and secure network configurations.
    - Ability to configure and troubleshoot network settings related to Vault.
8. **Cloud Platforms:**
    - Experience with public (AWS, Azure, GCP) or private (VMware, OpenStack) cloud platforms.
    - Familiarity with integrating Vault with cloud-based services and infrastructure.

Preferred Qualifications:

- **Certifications:** HashiCorp Certified: Vault Associate or HashiCorp Certified: Vault Operations Professional.
- **Experience with Other HashiCorp Tools:** Knowledge of HashiCorp Consul or Nomad is a plus.
- **Kubernetes Experience:** Hands-on experience with Kubernetes for deploying and managing containerized applications.
- **Soft Skills:** Strong problem-solving skills, effective communication, and the ability to work collaboratively in a remote or hybrid environment.