Job Description: Windows Virtual Server Maintenance Engineer

Experience Required: 2 to 3 Years

Category: D

Role Overview

Responsible for maintaining, monitoring, and optimizing Windows-based virtual servers across enterprise environments. Ensures high availability, security compliance, and performance of production workloads hosted on Hyper-V, VMware, or cloud platforms (AWS/OCI/other).

Key Responsibilities

- **Server Maintenance & Monitoring**
  - Perform routine patching, updates, and hotfix deployments.
  - Monitor server health, performance, and resource utilization.
  - Troubleshoot OS, application, and network connectivity issues.
- **Configuration & Administration**
  - Manage Active Directory, DNS, DHCP, Group Policies.
  - Configure and maintain Windows Server roles (IIS, File Services, Print Services).
  - Handle virtualization platforms (Hyper-V/VMware) and cloud-hosted Windows servers.
- **Backup & Recovery**
  - Implement and monitor backup strategies (AWS Backup).
  - Test disaster recovery procedures and ensure RTO/RPO compliance.
- **Security & Compliance**
  - Apply security baselines (CIS, NIST).
  - Disable legacy protocols (e.g., TLS 1.0/1.1).
  - Manage endpoint protection, firewall rules, and vulnerability remediation.
- **Automation & Optimization**
  - Use PowerShell scripting for automation of routine tasks.

    - Optimize server performance and resource allocation.
- **Documentation & Reporting**
    - Maintain server inventory, configuration records, and change logs.
    - Prepare compliance and audit reports.

Required Skills & Qualifications

- Strong knowledge of **Windows Server (2016/2019/2022/2025)** administration.
- Experience with **virtualization technologies** (Hyper-V, VMware).
- Familiarity with **cloud hosting** (OCI, AWS).
- Proficiency in **PowerShell scripting** and automation.
- Knowledge of **networking fundamentals** (TCP/IP, VPN, firewalls).
- Experience with **backup/recovery tools** and disaster recovery planning.
- Understanding of **security hardening** and compliance frameworks.
- Excellent troubleshooting and problem-solving skills.

Preferred Experience

- Exposure to **SIEM tools** (Seceon, Imperva, Microsoft Sentinel).
- Knowledge of **DLP, IAM, and endpoint security solutions**.
- Experience in **multi-DC environments** with tunnels and managed firewalls.

Educational Background

- Bachelor’s degree in computer science, IT, or related field.
- Microsoft certifications (MCSA, MCSE, AZ-104, SC-300) preferred.