**SANVI PATEL**

Ahmedabad | +91 8849451927 | sanvip536@gmail.com

LinkedIn: https://www.linkedin.com/in/sanvi-p-3b85ba1b1/

**Objective**

To obtain a challenging role in DevOps or Cloud, where I can leverage my skills in cloud computing, infrastructure management, automation, and CI/CD processes. I aim to contribute to the company's growth while continuing to expand my knowledge and expertise in a dynamic and forward-thinking environment.

**Core Strengths**

- Strong communication and teamwork skills.

- Excellent time management and self-motivation.

- Ability to adapt quickly and learn new technologies.

- High work ethic and dedication to continuous learning.

**Education**

Bachelor of Science in Information Technology (Infrastructure Management Services) Ganpat University | 2021 – 2024  
CGPA: 9.85  
Relevant Coursework: Networking, Virtualization, Server Administration, SQL Databases, Shell Scripting, Python

**Professional Experience**

L1 Team Lead | 2 years of experience as L1 Support Engineer at NW9 Multifaceted

• Implemented custom VM images and automated VM scaling using Azure VM Scale Sets.

• Managed user access and identity roles using Azure Active Directory.

• Configured Kubernetes clusters and used kubectl to manage pods, services, and deployments.

• Configured Jenkins pipelines to pull projects from Git, build them using Docker, and deploy containers to test environments.

• Created and tested beginner-level CI/CD pipelines using Azure DevOps to automate code builds and deployments.

• Worked with Azure Portal and Intune Portal to manage device compliance, security.

• Set up Intune on Windows and macOS devices, ensuring seamless enrollment and policy application.

• Configured BitLocker encryption for device security and assisted users with BitLocker recovery keys.

• Set up and managed local admin accounts, ensuring proper access control while maintaining compliance.

• Provided post-setup support, troubleshooting Intune policy failures and resolving security compliance issues.

• Monitored and managed Intune policies, addressing failures, conflicts, and misconfigurations.

• Handled service requests and incident tickets, assisting users with various Intune-related issues.

• Ensured devices met corporate security standards, troubleshooting noncompliance cases and implementing corrective actions.

• Worked with Python scripts to set up an automation tool, reducing manual intervention and improving efficiency.

• Mentored and trained 12+ employees, enhancing their technical skills and productivity.

**Certifications**

- NSE-1 Network Security Associate – Fortinet | June 2022 – 2024

- Networking Essentials – Cisco | June 2022

- Networking Basics – Cisco | June 2022

- Introduction to Cybersecurity – Cisco | June 2022

- Cybersecurity Essentials – Cisco | July 2022

- NDG Linux Unhatched – Cisco | June 2022

- Hardware and Networking – The Digital Adda | December 2022

- Elastic Stack – Great Learning | February 2023

- Elastic Training Program: Kibana Fundamentals – Elastic | February 2023

- Palo Alto Networks – Palo Alto Networks | February 2023

-Microsoft Certified: Security, Compliance, and Identity Fundamentals (SC-900) |

May 2024

-Linux Tutorial - Great Learning | September 2024

-Python basics - IBM | December 2024

-AWS Cloud Assessment – Learn Tube | January 2025

-Microsoft Certified: Azure Fundamentals (AZ-900) | May 2025

**Technical Skills**

**Networking:**

• Expertise in networking, routing, and configuration of network devices such as routers and switches.

•Proficient in Cisco IOS and networking protocols (OSPF, RIP, EIGRP, VLANs).

• Strong knowledge of security protocols (SSH, IPSec) and security devices like firewalls, IDS/IPS.

**Server Administration:**

• Skilled in managing Linux (Red Hat, Ubuntu) and Windows Server environments.

• Experience in configuring and troubleshooting system services using systemctl, yum, PowerShell, and other management tools.

**Virtualization:**

• Hands-on experience with virtualization platforms such as VMware and VirtualBox.

• Proficient in VM creation, configuration, and resource management (CPU, memory, performance optimization).

**Cloud Computing:**

• Knowledge of Cloud Service Models (IaaS, PaaS, SaaS) and Cloud Deployment Models (Public, Private, Hybrid).

• Experience with cloud platforms (AWS, Azure), including EC2, S3, IAM, Autoscaling, Load Balancing, and High Availability.

• Familiar with serverless computing (AWS Lambda, Azure Functions) and cloud security best practices.

DevOps & Automation:

• CI/CD: Hands-on experience with Jenkins, GitHub/GitLab CI/CD pipelines.

• Infrastructure as Code (IaC): Proficient in Terraform and Ansible.

• Containerization: Skilled in Docker and Kubernetes (K8s) for container orchestration and deployment.

• Monitoring & Logging: Experience with Prometheus, Grafana, ELK Stack (Elasticsearch, Logstash, Kibana), AWS CloudWatch, and Azure Monitor.

• Version Control: Expertise in Git, GitHub, and GitLab for source code management and collaboration.

**Cybersecurity:**

• Basic knowledge of SIEM tools (ELK Stack, Splunk) and open-source security tools (Suricata IDS).

• Understanding of security threats such as malware, phishing, and social engineering.

• Experience in implementing network security policies, firewall rules, and intrusion detection mechanisms.

**Virtual Internship: Cybersecurity Management**

Completed Cybersecurity Virtual Experience Programs with Forage, focusing on security activities like phishing, malware, and social engineering

**Project**

Deploying Open Source Intrusion Detection System (IDS) with ELK Stack

Designed and implemented an IDS using ELK Stack for centralized logging and realtime analysis of network traffic.