

NIKHIL KUMAR POTLURI

Cloud and Systems Administrator

USA | Contact: | (817)405-9252 | Email: nikhil.a3613@gmail.com | [LinkedIn](#)

Professional Summary

Cloud and Systems Administrator with 4+ years of experience supporting enterprise hybrid environments across AWS, Azure, and on-prem infrastructure. Proven in managing Windows and Linux servers, automating access and configuration, maintaining system reliability, and supporting secure, regulated workloads in healthcare and financial services. Strong hands-on expertise in cloud operations, identity management, monitoring, and infrastructure automation, backed by AWS, Azure, and Linux certifications.

Education

Master of Science in Computer Science | Clark University, Worcester, MA, USA, Graduated May 2024

Core Skills

- Cloud Platforms & Infrastructure: AWS (EC2, S3, IAM, VPC, RDS), Microsoft Azure (VMs, Azure AD), Hybrid Cloud, VMware ESXi
- Operating Systems & Directory Services: Windows Server (2016/2019), Linux (RHEL, Ubuntu), Active Directory, DNS, DHCP
- Automation & Configuration Tools: PowerShell, Bash, Python, Ansible, YAML, JSON
- Monitoring & Logging Tools: AWS CloudWatch, Nagios, Prometheus, Grafana, ELK Stack
- Security & Access Technologies: IAM, MFA, RBAC, SSL/TLS, Firewall Rules, OS Hardening, Audit Logging
- IT Operations & Collaboration Tools: ServiceNow, JIRA, Confluence, Git, GitHub Actions, Agile/Scrum

Professional Experience

AbbVie, Mettawa, IL | December 2023 – Present

Cloud System Administrator

- Supported and stabilized a hybrid cloud environment spanning AWS and on-prem infrastructure, ensuring high availability and reliable operations for business-critical applications.
- Executed enterprise-wide server lifecycle management across Windows and Linux systems, including provisioning, configuration, patch cycles, and controlled upgrades in production environments.
- Streamlined identity and access operations by automating user access workflows across Active Directory and cloud IAM, improving turnaround time and reducing operational overhead.
- Strengthened platform reliability through proactive monitoring and alert management, identifying performance anomalies early and preventing service disruptions.
- Partnered with cybersecurity and compliance teams to enforce access controls, logging standards, and audit requirements aligned with regulated enterprise environments.
- Led incident response and escalation support for infrastructure, access, and recovery issues, providing L2/L3 troubleshooting and restoring services within SLA expectations.
- Developed and maintained operational runbooks and technical documentation, improving team onboarding efficiency and ensuring consistent incident resolution practices.

HSBC, Hyderabad, India | September 2020 – July 2022

System Administrator

- Deployed, configured, and supported Windows and Linux servers across development, testing, and production environments, maintaining system stability and availability.
- Executed OS patching, service updates, configuration changes, and scheduled maintenance within formal change management processes.
- Administered system backup and recovery operations, validating restores to support disaster recovery readiness and data integrity.
- Implemented automated server provisioning and configuration for development and test environments using Ansible to improve consistency and efficiency.
- Configured and managed user access, group policies, and system permissions in Active Directory and internal security frameworks.
- Monitored infrastructure and application performance using enterprise monitoring platforms, identifying issues and applying corrective actions.
- Supported migration of selected workloads to AWS by provisioning EC2, RDS, and S3 resources and validating post-migration system health.

Projects

1. AWS Cloud Platform Operations for Enterprise AI/Data & Clinical Systems (GAIA)

- Supported cloud platform operations for an AWS-backed enterprise AI/data and clinical authoring environment by maintaining reliable hybrid infrastructure across AWS and on-prem systems.
- Standardized server provisioning, patch cycles, and configuration baselines across Windows and Linux platforms to support secure and stable production workloads.

- Automated identity and access workflows across Active Directory and cloud IAM, enforcing least privilege access for teams handling sensitive R&D and clinical data.
- Strengthened platform reliability through proactive monitoring and alert management, identifying performance anomalies early and preventing service disruptions.
- Partnered with cybersecurity and compliance teams to support audit-ready operations, logging standards, and access controls aligned with regulated enterprise requirements.

2. Cloud-Based Identity Management Automation

- Deployed and supported Windows and Linux servers across development, testing, and production environments as part of HSBC's enterprise infrastructure modernization initiatives.
- Executed OS patching, configuration updates, and scheduled maintenance under formal change management to maintain stability and compliance in regulated banking systems.
- Administered backup and recovery operations, validating restores to ensure data integrity and disaster recovery readiness.
- Implemented automated server provisioning and configuration for dev/test environments using Ansible, improving consistency and reducing manual setup effort.
- Configured Active Directory user access, group policies, and system permissions in alignment with internal security and audit requirements.
- Monitored infrastructure and application performance using enterprise monitoring platforms, identifying issues and applying corrective actions to maintain service reliability.
- Supported migration of selected workloads to AWS by provisioning EC2, RDS, and S3 resources and validating system health post-migration.

Certifications

- AWS Certified Cloud Practitioner – Demonstrated foundational knowledge of AWS cloud concepts, core services, security, pricing models, and best practices for operating workloads in the AWS cloud.
- Microsoft Azure Fundamentals (AZ-900) – Validated understanding of Azure cloud concepts, core services, identity management, security principles, and cost management within Microsoft Azure environments.
- AWS Certified SysOps Administrator – Associate – Demonstrated hands-on knowledge of deploying, monitoring, managing, and operating AWS workloads, including automation, security controls, and system reliability.
- Linux Foundation Certified IT Associate (LFCA) – Validated foundational skills in Linux system administration, basic networking, security concepts, cloud computing fundamentals, and operational best practices.

Technical Proficiency

- Cloud & Hybrid Infrastructure — AWS (EC2, S3, RDS, VPC, IAM) and Microsoft Azure (VMs, Azure AD), supporting secure hybrid enterprise environments.
- Server & OS Administration — Windows Server 2016/2019 and Linux (RHEL, Ubuntu) for provisioning, patching, hardening, and production system support.
- Identity & Access Management — Active Directory, Azure AD, AWS IAM, RBAC, MFA, and group policy enforcement across regulated environments.
- Automation & Configuration — PowerShell, Bash, Python, and Ansible for automated server builds, configuration drift control, and access provisioning.
- Monitoring & Reliability Engineering — AWS CloudWatch, Nagios, Prometheus, Grafana, and ELK Stack for uptime, performance, and incident detection.
- Security & Compliance Operations — OS hardening, firewall rules, audit logging, least-privilege access, and vulnerability remediation aligned to enterprise standards.
- IT Operations & DevOps Tooling — ServiceNow, JIRA, Git, GitHub Actions, YAML, and JSON for change management, incident tracking, and infrastructure workflows.