MSP Tenured Senior Cloud Engineer

SUMMARY

Results-driven Network Engineer with 10+ years of experience in system administration, cloud technologies, and enterprise network security. Proven ability to lead and resolve complex infrastructure projects across hybrid and cloud environments (Azure, AWS). Skilled in automation, identity & access management, endpoint security, and scalable deployments using modern tools and technologies. Certified in CCNA, MCSA, Azure Fundamentals, and more.

WORK EXPERIENCE

Senior Cloud Engineer, MSP/ Cloud Solutions Provider **2021 - Present**

- Managed Microsoft Entra AD by administering user permissions and security groups, defining IAM roles for resource groups, and controlling access levels. In hybrid environments, utilized Active Directory to manage users and permissions, while leveraging AWS IAM roles and policies to govern user and group access to cloud resources.
- Troubleshot and maintained Azure Virtual Desktop and Azure Virtual Machines, deploying host pools and configuring remote applications via Microsoft Remote Desktop. Managed FSx storage for profile redirection, optimizing user experience and storage efficiency.
- Implemented SAML-based Single Sign-On (SSO) with Azure AD (Entra AD), enabling user provisioning and permission group assignments. Managed application secrets lifecycle, ensuring timely key rotations to maintain security compliance without service disruption.
- Administered device management through Microsoft Intune, creating configuration and compliance policies, deploying company portals, and automating application deployment. Utilized Intune Autopilot for seamless device enrollment during initial setup.
- Provisioned and scaled virtual machines per client requirements, monitoring performance and deploying applications on standalone or Remote Desktop Services (RDS) clusters to ensure high availability.
- Oversaw organizational DNS records and SSL certificates, including SPF, DKIM, and DMARC record management to ensure uninterrupted, secure email flow through third-party filters like Mimecast and Sophos or native Office 365. Conducted SSL certificate renewals and deployments with zero downtime.
- Automated administrative tasks and reporting using PowerShell across Office 365, Azure, SharePoint, Active Directory, and server environments. Employed macOS shell scripting to monitor running applications, deploy software, and enforce system lockdowns.
- Managed macOS devices using Addigy and JAMF, integrating Apple Business Manager for automatic MDM enrollment. Created custom .dmg packages via Addigy for streamlined application deployment during onboarding.
- Enforced endpoint security by deploying baseline policies and tailored security templates through Intune. Utilized Microsoft Defender for malware detection, remediation, and root cause analysis, reducing infection recurrence. Applied Group Policies in hybrid and non-cloud environments to consistently enforce organizational security standards.

Senior Systems Engineer, National MSP **2017-2021**

- Served as senior service desk escalation lead, resolving complex client issues and guiding engineers. Managed AWS clusters, deploying 50+ VMs and E3 instances integrated with on-prem domain controllers. Configured Route 53 DNS (CNAME, A records) for website redirection and load balancing, improving traffic management.
- Upgraded AWS machines and applied Group Policies to enhance security. Configured S3 storage with secure access controls for file sharing. Deployed Azure VMs with subnet configurations, enabling seamless hybrid cloud connectivity.
- Managed 500+ Windows, macOS, iOS, and Android devices via Microsoft Intune, enforcing compliance and deploying client-specific apps. Applied Azure AD Group Policies to secure hybrid and cloud environments.
- Deployed cloud applications with secure access controls at domain level. Provided 24/7 support for physical and virtual servers, maintaining high availability. Supported firewalls, IPS/IDS, and VPNs to protect network perimeter and managed web filtering to block unauthorized access.

Network Consultant, NYC-Based Boutique MSP **2016-2017**

- Configured and managed firewalls (SonicWALL, WatchGuard) for 10+ clients, creating rules for remote/VPN access, deep packet inspection, and ISP failover, ensuring high availability during failures. Configured and troubleshot switches, created VLANs and uplinks for subnet communication, and implemented failover setups to maintain network resilience.
- Deployed and maintained Windows Server 2012 environments, configuring DNS, DHCP scopes, and device reservations for

networks supporting 200+ devices. Managed Active Directory for multiple clients, creating OUs and implementing tailored Group Policies to enhance security and compliance.

- Automated routine network and system tasks using Python, PowerShell, CMD, HTML, PHP, and JavaScript, improving operational efficiency by 25%. Installed and configured Ubiquiti access points for multiple clients, creating segmented SSIDs including guest networks with appropriate access controls.

Network & Systems Administrator, Government-IT & Cybersecurity Solutions Provider **2015-2016**

- Maximized network performance by monitoring, troubleshooting, and resolving outages across LAN/WAN environments supporting 500+ users; collaborated with network architects to optimize infrastructure and scheduled critical upgrades.
- Administered Windows Server 2003, 2008, and 2012 for Employee Retirement Services, managing DNS, DHCP scopes, and server features to meet evolving client needs.
- Generated detailed network operational reports, prioritized tasks, and maintained comprehensive documentation to support network maintenance and continuity.

IT Support Analyst, IT Outsourcing & Automation Company **2013-2014**

- Provided Tier 1 and Tier 2 support in a 24/7 production environment, resolving issues for 300+ users across networks, servers, desktops, laptops, VOIP, printers, and scanners.
- Developed and enforced Group Policies to prevent data leaks and strengthen network security.
- Monitored daily backups, generated error reports, and ensured compliance with backup SLAs.
- Configured Cisco ASA firewalls for failover, remote access, VPN, and threat protection, achieving 99.9% network uptime.

ADDITIONAL INFORMATION

Cloud Platforms: Microsoft Azure, AWS, Google Cloud
Operating Systems: Windows Server 2008–2022, Windows 7–11, macOS (OS X to Big Sur), Linux (Ubuntu, Red Hat)
Cloud & Virtualization Platforms: Microsoft Azure (VMs, Virtual Desktop, Intune, AD, DNS), AWS (EC2, VPC, IAM, Route 53, Workspaces), Google Cloud, VMware vSphere, Hyper-V, Citrix, Oracle VirtualBox
Networking & Security: DNS, DHCP, SSL, SSO, VPN, SMTP, SMB, Routing, Unifi AP, Cisco Meraki, Fortinet, SonicWall, Palo Alto, Dell PowerEdge, DUO, OKTA, Group Policies, DFS Shares, Profile Redirection
Email & Collaboration Platforms: Microsoft Office 365, Exchange 2008/2013, GSuite, Mimecast, Edgewave, Intermedia, Rackspace, OneDrive, Dropbox, Microsoft RDP, Terminal Server
Device & Endpoint Management: Microsoft Intune, JAMF, Addigy, Apple Business Manager, Windows Autopilot, Bash
Backup & Restore Tools: Veeam, Dell Backup Exec, Symantec, Azure Backup, Hyper-V Restore Points, VMware Checkpoints
Monitoring, Automation & Scripting: PowerShell, LionGard, Kaseya, JIRA, IIS 8.5, Malwarebytes, Webroot, Symantec, IP Scanner
Technical Acumen: Understanding of technical ecosystems, including machine learning, to guide product strategy and development
Data Analysis: Strong analytical skills to drive decisions based on customer insights and market trends
Tools: SQL, Google Analytics, Tableau, Microsoft Excel (Advanced), Data Visualization, SharePoint, Google Workspace

EDUCATION

University of Maryland Baltimore County, M.S. in Information Systems **2014-2016**
Punjab Technical University, B.S. in Computer Science **2009-2012**

KEY ACHIEVEMENTS

- Reduced system downtime by 40% through proactive monitoring and PowerShell automation across hybrid environments.
- Deployed Azure Virtual Desktop for 500+ users with FSLogix profiles, ensuring secure, remote access and compliance.
- Streamlined endpoint onboarding by 60% using Intune Autopilot and JAMF across Windows, macOS, and iOS devices.
- Improved cloud security posture by designing and implementing IAM architecture for Azure and AWS.
- Blocked 95% of phishing threats by enforcing SPF, DKIM, and DMARC policies and integrating Mimecast filtering.

CERTIFICATIONS

- Cisco Certified Network Associate (CCNA)
- Microsoft Certified Solutions Associate (MCSA)
- Microsoft Certified Professional (MCP)
- Apple Certified MAC Integration
- CompTIA Linux+
- Microsoft Azure Fundamentals
- JAMF Certified Associate (100)