Chad Lester

Site Reliability Engineer – Agentic AI
Phoenix, US
chad.lester@outlook.com
+16025095365
linkiedin.com/in/chadalanlester
chadlester.com

SUMMARY

Professional Summary

I'm a seasoned Cloud Site Reliability Engineer with over eight years of experience in cloud infrastructure and systems reliability—and more than twenty years in IT. I specialize in automating and optimizing cloud environments to improve operational efficiency, particularly in AWS and Azure. My focus is on infrastructure resilience, DevOps practices, and incident response, with a strong emphasis on compliance in government-regulated cloud systems.

I've automated infrastructure using tools like Terraform, Ansible, and GitHub Actions to speed up deployments and reduce manual tasks. I'm committed to building scalable, automation-first solutions and have delivered self-healing architectures that reduce downtime and support high availability. I work closely with both engineering and security teams to align priorities and ensure reliable, secure systems. I'm always looking for ways to improve processes and foster a culture of operational excellence.

EXPERIENCE

Agentic AI SRE
FutureSecure.AI

- Site Reliability Engineer for a multi-tenant agentic AI platform, supporting customer-specific Kubernetes estates on Azure AKS and AWS EKS. Own end-to-end operational delivery: Helm-based application releases, Terraform infrastructure changes, runbooks, incident response, and documentation aligned with customer security and compliance expectations. Day-to-day work spans private-cluster access patterns, LLM workload tuning (e.g., Azure OpenAI rate limits and embeddings), data services (Postgres/Supabase, caching), ingress and load balancing, and cross-functional troubleshooting with developers and customer stakeholders.
- Kubernetes & GitOps: Plan and execute Helm upgrades and maintenance windows with scripted pre-checks, backups, and post-deploy verification; codify "temporary" cluster fixes into durable Helm values and repeatable procedures (DNS/TLS integration, configmaps/secrets alignment).
- Infrastructure as code: Build and operate AWS foundations with Terraform—EKS, networking, and tagging/compliance requirements—plus Helm overlays for platform components (e.g., ingress controllers, application charts).
- Incident management: Lead root-cause analysis for production-impacting issues (ingress/load balancers, Redis/Valkey, storage attachment, API throttling); document findings and follow-ups in runbooks and structured session summaries.
- Security & compliance: Implement customer policy constraints (e.g., internal-only load balancers, hardened bastion posture), support security audits with evidence and remediation tracking, and maintain compliance-oriented documentation.
- Observability & performance: Use cloud monitoring and cluster telemetry to validate hypotheses (e.g., Azure OpenAI client errors, queue/worker concurrency) and tune platform parameters without masking upstream capacity limits.
- Platform evolution: Support cluster lifecycle work (node pools, Kubernetes upgrades), database/platform extensions (e.g., pgvector on Postgres), and integration patterns for LLM gateways and application webhooks.

Cloud SRE
Broadcom | 06/2024 to 07/2025

- Automated infrastructure and service upgrades using Terraform, Ansible, and GitHub Actions, reducing manual workload by 40% and cutting deployment times from hours to minutes
- Led weekly Change Management Board sessions, aligning engineering, security, and compliance priorities—resulting in a 25% drop in unplanned downtime
- Deployed changes for multiple business units with Canary Deployments and Azure DevOps Pipelines, achieving zero-impact rollouts and faster release Cycles
- Built self-healing architectures with Prometheus and AWS Lambda auto-remediation via PagerDuty runbooks
- Maintained SCOPE cloud services using CI/CD pipelines (GitLab CI, Jenkins), sustaining 99.98% availability across production
- Monitored performance across distributed systems with ELK Stack, New Relic, and custom Runbooks, reducing MTTR by 32%
- Ensured compliance with FedRAMP, NIST, and PCI standards through hardening, policy enforcement, and quarterly audits—passed FedRAMP audit with zero findings
- Conducted high-severity postmortems using blameless RCA frameworks and Splunk log analysis, improving long-term reliability by 15%
- Delivered Tier 3 on-call support via Opsgenie and Slack incident channels, resolving 97% of urgent issues within SLA
- Managed patching, licensing, and compliance tasks using WSUS, Qualys, and Jira Service Management, keeping all assets fully secure and audit-ready
- Applied deep knowledge of FISMA, RMF, and NIST 800-53 to guide secure architecture and audit documentation

Cloud Systems Administrator
VMware | 04/2023 to 06/2024

- Automated cloud infrastructure deployment using Terraform, Ansible, and PowerShell, resulting in a 35% increase in deployment speed and significantly reduced manual configuration errors
- Maintained CI/CD pipelines with GitLab CI and Jenkins, allowing continuous integration and delivery across staging and production environments with zero rollback incidents for 6 months
- Developed custom scripts (Bash, PowerShell, Python) for automated backups, patching, and system monitoring, reducing overnight manual jobs by 70%
- Administered and monitored web servers including Apache, IIS, and Tomcat, ensuring 99.99% uptime and fast recovery from traffic spikes or errors
- Managed daily change control and root cause analysis processes using Jira, Confluence, and ServiceNow, improving issue resolution workflows and documentation quality
- Supported DoD and government audits, ensuring full compliance with FedRAMP, NIST, and DISA STIG benchmarks; prepared systems documentation that passed inspection without revisions

Senior Systems Administrator
Imagine Learning | 06/2021 to 03/2023

- Led the decommission and relocation of a major data center without service interruption by coordinating cross-team logistics, virtual machine migration to Azure, and post-move validation
- Managed MDM compliance across 2,000 devices by transitioning from SCCM to Microsoft Intune, improving visibility, patch coverage, and mobile access control
- Configured and enforced security policies using OKTA, Mimecast, and Microsoft Defender for Endpoint, reducing phishing incidents and access issues by 45% Monitored systems health and network traffic with SolarWinds and Splunk, proactively resolving bottlenecks and outages before they impacted users
- Authored and maintained internal documentation for disaster recovery, system access, and service onboarding—improving IT team onboarding and reducing internal tickets by 30%
- Trained junior admins and Help Desk staff through weekly learning sessions, creating custom labs and shadowing exercises that improved incident triage capabilities

Senior Systems Administrator
Forever Living International | 07/2017 to 06/2021

- Led the successful migration of on-rem infrastructure to Azure and Office 365, improving system availability, reducing licensing costs, and enabling secure remote work across the organization.
- Managed enterprise-wide infrastructure supporting HQ, remote work offices, manufacturing plants, and international sites—achieved 99.95% uptime across global systems
- Implemented and administered CyberArk Privileged Access Security (PAS), establishing PCI-compliant privileged identity workflows and reducing lateral movement risk
- Monitored and optimized performance of Windows (Server 2016/2019) and Linux (RHEL/CentOS) environments; tuned IIS, Apache, and Tomcat servers for better load distribution
- Created robust disaster recovery processes using Veeam, Windows Server Backup, and Azure Site Recovery, reducing RTO and RPO below 4 hours
- Led internal security audits and collaborated with vendors, using Qualys, Nessus, and GPO hardening to maintain security posture and ensure external compliance standards were met

Network Engineer II

Choice Hotels International | 03/2017 to 06/2017

- Maintained and troubleshot complex network systems, ensuring 99.9% uptime for enterprise applications across multiple hotel business systems.
- Engineered and optimized network configurations, resulting in a 30% increase in application delivery efficiency.
- Conducted device audits and managed firmware upgrades, safeguarding compliance and enhancing security protocols.

Network Engineer IV

Industrial Commission of Arizona | 06/2013 to 12/2016

- Managed daily operations of core networking systems, resolving over 150 complex service tickets with a 95% satisfaction rate.
- Supported installation and maintenance of LAN/WAN circuits, ensuring 99.9% uptime across all agency offices.
- Collaborated on IT infrastructure projects, meeting 100% of milestone deadlines while maintaining accurate documentation for audit readiness.

EDUCATION

Arizona State University

BA, History

- Earned over 120 hours towards a Bachelor of Arts in History from Arizona State University, focusing on critical analysis of historical events and trends.
- Developed strong research and writing skills through extensive coursework and projects.
- Engaged in collaborative discussions, enhancing my ability to communicate complex ideas clearly.

University of Phoenix

Information Technology

- Earned an MCSE certification from the University of Phoenix.
- Developed expertise in systems analysis, network security, and database management through hands-on projects.
- Completed coursework that enhanced my problem-solving skills and technical proficiency to support organizational goals.

CERTIFICATIONS

MCSE – Microsoft Certified Systems Engineer
Network+
A+

SKILLS

Cloud Infrastructure (AWS & Azure)
CI/CD Pipelines & Automation
Python and PowerShell scripting
Infrastructure as Code (IaC)
Monitoring, Observability, & Incident Response
Security & Compliance in Regulated Cloud Environments (FedRAMP, NIST, FISMA)
Linux and Windows administration
Containerization and Orchestration
Network Protocols and Principles
Problem Solving and Collaboration