BYRON FERGUSON

Infrastructure Engineer · Builder · Automation Architect

bferguson-dev@gmail.com · 615-359-3820 · linkedin.com/in/byronferguson · bferguson.dev

SUMMARY

Infrastructure engineer with 16+ years of experience who treats infrastructure as a product — something to architect, automate, and evolve. Deep operator background in high-volume, distributed systems (10,000+ VMs, 500+ ESXi hosts) transitioning into cloud-native and platform engineering. Open source contributor with shipped tooling for compliance automation, observability, and runbook execution. Builds tooling for infrastructure engineers: high-level languages operators already know, human-readable YAML configuration, modular architecture with a solid core and pluggable components, and documentation written for the person running the tool — not the person who built it. Applies AI and agentic workflows as a force multiplier to reduce manual operations, build self-documenting systems, and rapidly accelerates delivery — the kind of engineer who reduces the on-call queue by eliminating the conditions that create them.

EXPERIENCE

Self-Directed · *Independent Software Development & R&D* Dec 2024 – Present

- **Infrastructure as product:** Designed and shipped open-source tooling for compliance automation, runbook execution, and connectivity validation — treating every tool as a deployable artifact with CI/CD, docs, and testable interfaces
- **Operator-first design:** Standalone tools are built around operator ergonomics — YAML-driven configuration, modular architecture where components can be added or removed independently, and documentation written for infrastructure engineers already familiar with PowerShell or Bash who can read, copy, and extend any module without needing a software background
- **Parallel AI agent orchestration:** Operates Cline Kanban to run Claude Code and Codex as parallel workers in isolated git worktrees — managing task dependency chains, reviewing diffs, leaving line-level feedback for agent correction loops, and gated commits and PRs
- **AI governance & auditability:** Built structured frameworks using Claude, Codex, Gemini, and Ollama as engineering force multipliers; versioned prompt rules and session logging for full traceability of AI-assisted development
- **Terraform:** Used to define, provision, and manage homelab infrastructure as code — all lab environments version-controlled and reproducible from a single apply
- **CI/CD & DevOps discipline:** All projects shipped with GitHub Actions pipelines, atomic artifact writes, dry-run modes, and provenance headers — zero manual deploy steps
- **Platform breadth:** Proxmox homelab as a real cloud-native testbed: Cloudflare Tunnel, SSH key auth, GitLab CE, Kanban, Docker, LXC workloads, remote dev environment — built and operated end-to-end
- Pursuing AWS Certified Cloud Practitioner (CLF-C02) certification

Experian Health · *Systems Engineer / Infrastructure Engineer* Dec 2016 – Nov 2024

- **Scaled distributed infrastructure** to 10,000+ virtual machines across 500+ ESXi hosts and 400+ physical servers with near five nines availability — reliability engineering and automation at a scale where manual processes aren't an option
- **Multi-region data center operations:** Operated 3 geographically separated data centers across middle Tennessee, distributing compute load, backup duties, and DR failover across all three — active production, warm spare, and DR tiers running simultaneously
- **Distributed SQL & low-latency workloads:** Administered physically separated SQL Server nodes in an active/spare/DR configuration across geographically distinct locations — engineered for low latency and automatic failover
- **VMware + Nutanix HCI clustering:** Operated 16-node physical host clusters with automatic VM and container workload distribution and load balancing — distributed compute without manual intervention
- **Major data center migrations:** Core team member on 2 large-scale DC migrations involving tens of millions of dollars of equipment — ESXi hosts, storage arrays, tape backups, network gear, racks, and cabling — executed with zero unplanned downtime
- **Object storage & file protocols:** Administered Dell ECS (S3-compatible object storage) including bucket management; served multi-departmental file shares from remote data centers; executed file share data migrations; restored systems from both disk and tape
- **Data security:** Enforced encryption at rest and in transit across storage and network platforms for HIPAA and PCI-DSS requirements
- **Eliminated manual operations** via PowerShell and Ansible Automation Platform: automated patching cycles, configuration drift remediation, and compliance auditing across the entire fleet
- **Compliance automation:** Enforced HIPAA, PCI-DSS, NIST 800-53, and SOC 2 through automated internal audits, structured documentation, and runbook-driven remediation — compliance without developer friction
- **Disaster recovery engineering:** Designed and executed DR runbooks with regular test cycles; built business continuity posture from documentation through live failover validation
- **Monitoring & observability:** Administered Splunk for SIEM and log aggregation; SolarWinds for infrastructure and network monitoring; Dell OpenManage Enterprise for hardware-level alerting across 400+ physical nodes; VMware vCenter and Nutanix Prism for unified virtualization visibility; exposure to vRealize Operations (vROps) for performance monitoring
- **Storage at scale:** Managed Dell EMC Isilon, PowerFlex, Data Domain, ECS, and ExaGrid — multi-platform enterprise storage with documented runbooks and full auditability
- **On-call rotation:** 1 week per month across the full infrastructure stack — continuous on-call posture maintained since 2016
- **Hardened multi-platform environments:** Windows Server and RHEL/Linux system hardening; mentored junior engineers

City of Franklin · *Data Center Engineer / City Information Security Officer* Oct 2012 – Oct 2016

- **Data center migration & infrastructure build-out:** Led standup of Cisco UCS compute platform with Nexus switching as part of a full DC migration — racked, cabled, and commissioned the environment from the ground up
- **Exchange hybrid migration:** Administered Exchange Online and led migration from on-prem Exchange to a hybrid Exchange Online environment integrated with Azure Active Directory; administered Microsoft Exchange Online Protection
- **Security platform administration:** Stood up and administered Mandiant FireEye network threat prevention platform; administered Cisco IronPort web filter for organization-wide web security enforcement
- **VMware vSphere administration:** Administered vSphere environment as part of broader data center build-out and ongoing operations
- **Enterprise patching program:** Owned and operated the organization-wide patching program across workstations, servers, and network gear — full-environment coverage as part of the ISO function
- **Infrastructure monitoring:** Deployed and administered SolarWinds for network and infrastructure monitoring across the environment
- **On-call rotation:** 1 week on / 1 week off schedule as part of a continuous on-call posture — responsible for full-environment incident response covering infrastructure, security, and network
- **Rewrote Group Policy** infrastructure for consistent, auditable workstation and server security posture; deployed MBAM, Veeam, and Office 365 with security and compliance configurations
- **Administered DNS, ExaGrid, AD/DNS/DHCP, and file services**; managed workstation imaging; supported Cisco routing, switching, and VPN (NetMotion, AnyConnect)

OPEN SOURCE PROJECTS

YMC / YMC-L (You Must Comply) *Python · PowerShell · Go · WinRM · Docker*
Agentless compliance scanners for Windows and Linux, mapping checks to NIST 800-53, SOC 2, HIPAA, PCI DSS, and ISO 27001 with audit-ready structured output. Both platforms are active and currently being ported to Go as distributed container workloads.

The Collective *Go · Docker · Kubernetes · k3s · Python · actively in development*
Orchestration platform for distributed compliance scanning across enterprise environments. Scanner nodes (YMC/YMC-L) deploy as lightweight Go containers close to target endpoints eliminating single-point bandwidth saturation and avoiding network security policy triggers. Nodes report findings back to a centralized aggregation layer (the Queen). Designed for Kubernetes orchestration as a path to distributed deployment

FailWarden *Python · SSH · GitHub Actions*
YAML-driven runbook executor for infrastructure remediation over SSH. Compile-time validation, audit logging, dry-run mode, and a library of shipped runbooks — the kind of tool that turns an on-call incident into a documented, repeatable, one-command fix.

ReadyCheck *Python · CLI*
Connectivity validation CLI that compares observed network behavior against declared intent and emits structured review artifacts.

project-prompts *AI Governance · Prompt Engineering · CLI*
Structured library of versioned prompt engineering guidelines and session logging tooling for AI-assisted development — governance and auditability for agentic workflows at the project level.

TECHNICAL SKILLS

Infrastructure & Cloud: VMware vSphere/ESXi, Nutanix HCI, AWS (CLF-C02 in progress), Docker, Kubernetes/k3s, Linux/RHEL/Windows
Automation & IaC: Terraform, Ansible, Chef (familiar), PowerShell, Python, Go, Bash, GitHub Actions CI/CD
Observability & Monitoring: Splunk (SIEM), SolarWinds, Dell OpenManage Enterprise, VMware vCenter, Nutanix Prism, and vROps
Security & Compliance: NIST, HIPAA, PCI-DSS, SOC 2, ISO 27001, CIS Benchmarks, DISA STIG, encryption at rest/transit, system hardening
Storage & Data: Dell EMC Isilon, PowerFlex, Data Domain, ECS (S3-compatible), Veeam, disk/tape backup, data migration, file protocols
Networking: Cisco Nexus/IOS, Arista BCF SDN, DNS/DHCP at enterprise scale, Cloudflare Tunnel, Cisco IronPort, Mandiant FireEye
API & Integration: REST APIs, WinRM, SSH, S3-compatible object storage APIs, webhook-based integrations
AI & Tooling: LLMs, Prompt Engineering, Agentic AI (Claude, Codex, Gemini), Kanban agent orchestration, frameworks and auditability

CERTIFICATIONS & TRAINING

AWS Certified Cloud Practitioner (CLF-C02)	*In progress*
Red Hat Certified Specialist in Ansible Automation	*Training completed 2018*
Certified Ethical Hacker (CEH) & CHFI — EC-Council	*Formerly certified 2018*
CompTIA CASP+ · PowerShell for Systems Administration (New Horizons)	*Training completed 2015*

EDUCATION

M.S. Information Security and Assurance 2018
Western Governors University · Thesis: Disaster Recovery & Business Continuity grounded in NIST 800-53