

JEFFREY FONTENOT

Cloud & DevOps Engineering

New Orleans, LA (open to remote) | Active Secret Clearance

jeff.itodyssey.io | jeff@itodyssey.io | [linkedin.com/in/jeff-fontenot](https://www.linkedin.com/in/jeff-fontenot) | github.com/Jeff-Fontenot

PROFESSIONAL SUMMARY

Cloud-focused IT professional and infrastructure builder with a B.S. in Cloud Computing, an **Active Secret Security Clearance**, AWS Solutions Architect – Associate and CloudOps Engineer – Associate certifications. Builds and operates Linux, Docker, and k3s infrastructure with GitHub Actions CI/CD and live Prometheus/Grafana telemetry; developed a Terraform-provisioned AWS disaster recovery solution. Brings nearly two years of incident troubleshooting and hybrid Microsoft services support in a federal enterprise environment.

CORE QUALIFICATIONS

Cloud and Infrastructure as Code: AWS (EC2, S3, VPC, IAM), Terraform, hybrid cloud backup and recovery

Linux and Virtualization: Linux administration, Proxmox, virtual machines, LXC containers, self-hosted services

CI/CD and Container Platforms: GitHub Actions, Git, Docker, Docker Compose, Kubernetes (k3s)

Monitoring and Observability: Prometheus, Grafana, Grafana Alloy, Loki, infrastructure metrics and service health monitoring

Networking and Web Services: DNS, TCP/IP, HTTP/HTTPS, Pi-hole, Unbound, Tailscale, Traefik reverse proxy, TLS certificate automation

Scripting and Automation: Bash, cron, PowerShell project work, Python fundamentals

Enterprise Identity and Services: Active Directory, Microsoft 365, Exchange Online and hybrid messaging, Intune, BMC Remedy/Helix, CAC authentication, Windows 10/11 support

Federal IT Operations: Active Secret Security Clearance, Marine Corps Enterprise Network support, ITIL 4, incident escalation, authorization validation, technical documentation

SELECTED TECHNICAL PROJECTS

WakeTrail: DevOps Forensic Timeline (Pre-Release) | View [Portfolio](#) | View [GitHub](#)

Go | Bash | Linux | SQLite | Docker Compose | Kubernetes | Terraform | GitHub Actions

- **CLI Development:** Built an open-source Go application that reconstructs troubleshooting and deployment sessions from Bash commands, exit codes, execution durations, Git context, and observed infrastructure changes.
- **Infrastructure Correlation:** Implemented collectors for Docker/Compose, Kubernetes, systemd, Git, and Terraform/OpenTofu; correlated commands with resource transitions and grouped related observations into readable activities.
- **Privacy and Storage Hardening:** Added best-effort secret redaction, selective output capture, bounded temporary and persisted output, and restrictive local file permissions to reduce sensitive-data exposure.
- **Reporting Architecture:** Developed a shared timeline reconstruction pipeline for terminal reports and Markdown exports, providing concise activity summaries alongside verbose access to captured evidence.
- **Automated Validation:** Implemented GitHub Actions CI for formatting, static analysis, regression tests, and builds; added Bash lifecycle tests covering interrupted commands, capture cleanup, and output preservation.

Hybrid Cloud Disaster Recovery | View [Portfolio](#) | View [GitHub](#)

AWS | Terraform | Docker Compose | PostgreSQL | S3 | EC2

- **Hybrid Architecture:** Designed and implemented a hybrid disaster-recovery solution for a containerized Flask and PostgreSQL application hosted on an on-premises Ubuntu server.
- **Backup Automation:** Automated hourly PostgreSQL backups to Amazon S3 using Bash and cron, establishing an RPO of approximately one hour.
- **Infrastructure Provisioning:** Provisioned the AWS recovery environment with Terraform, including the VPC, networking, security group, IAM instance profile, EC2 instance, and initialization workflow.
- **Automated Recovery:** Developed restoration automation to retrieve the latest database backup from S3 and launch the application stack using Docker Compose.
- **Validation:** Conducted a simulated outage and restored application availability in 3 minutes 55 seconds; documented the architecture, operational steps, and test results.

Cloud-Native Homelab | View [Portfolio](#) | View [GitHub](#)

Proxmox | Linux | Docker Compose | Kubernetes (k3s) | GitHub Actions | Bash | Prometheus | Grafana

- **Infrastructure Architecture:** Designed and operated a Proxmox environment hosting Linux virtual machines, LXC containers, Docker Compose services, and a three-node Kubernetes cluster running Google's Online Boutique application.
- **CI/CD Automation:** Implemented GitHub Actions workflows for Compose validation and automated Dashy deployment over Tailscale and SSH, deploying validated commits with health verification and avoiding restarts for documentation-only changes.
- **Centralized Observability:** Integrated Prometheus, Grafana, and Loki for infrastructure metrics and centralized logging; developed PromQL recording rules for hypervisor utilization, container metrics, scrape health, and Kubernetes state.
- **Private Networking:** Configured authenticated remote administration through Tailscale, HTTPS service routing through Traefik, and DNS filtering and recursive resolution through Pi-hole and Unbound.
- **Live Portfolio Telemetry:** Built a Prometheus, Grafana Alloy, and Grafana Cloud pipeline that publishes selected sanitized infrastructure and Kubernetes metrics to a public portfolio while keeping management interfaces private.

PROFESSIONAL EXPERIENCE

Enterprise Service Desk Analyst | TEKsystems supporting Leidos | Marine Corps Enterprise Network | Jan 2025 – Present

Environment: Active Directory, Microsoft 365, Hybrid Exchange, BMC Helix, SmartCard Authentication, hybrid Microsoft services, secure federal enterprise support

- **Enterprise Troubleshooting:** Resolve authentication, DNS, CAC certificate, proxy, domain-trust, endpoint, and hybrid identity issues in a federal enterprise environment.
- **Diagnostic Automation:** Wrote a read-only PowerShell hybrid mailbox health verification for the current support toolbox. Previously piloted a separate menu-driven Active Directory lookup tool, which was discontinued after custom production scripts were restricted.
- **Incident Investigation and Escalation:** Investigate 20–30 support calls daily, document findings in BMC Helix, and escalate unresolved issues with troubleshooting evidence and clear handoff context.
- **Secure Access and Authorization:** Review account status, attributes, OU placement, and group membership in Active Directory; enable or restore existing accounts only after validating the required documentation and authorization.
- **Hybrid Microsoft Services:** Troubleshoot Exchange Online and hybrid messaging issues involving proxy and target addresses, licensing, GAL visibility, and Azure AD Connect synchronization.

Inventory Manager and Process Improvement Specialist | Smittys Supply | Oct 2011–Jan 2015

- **Process Improvement:** Led Six Sigma initiatives that improved inventory accuracy from 67% to 99.6%.
- **Data Analysis:** Created SQL, WMS, and ERP reports to identify inefficiencies and support operational decisions.
- **Root Cause Analysis:** Resolved a \$5 million inventory discrepancy through data validation and cross-functional investigation.

EDUCATION

- **Bachelor of Science, Cloud Computing:** Western Governors University, 2026
- **Associate of Arts, General Studies, 4.0 GPA:** Delgado Community College

CERTIFICATIONS AND CLEARANCE

- **Active Secret Security Clearance**
- AWS Certified: Solutions Architect – Associate
- AWS Certified: CloudOps Engineer - Associate
- CompTIA: Security+, Cloud+, Network+, A+, Project+
- Microsoft: Azure Fundamentals (AZ-900), 365 Fundamentals (MS-900)
- Other: ITIL 4 Foundation, PCEP: Python Certified Entry-Level Programmer, LPI Linux Essentials