

Marcus Holtz

marcusholtz.com Denver, CO

(720) 445-5887 contact@marcusholtz.com

Senior Systems Engineer — Linux infrastructure, cloud architecture, DevOps, networking, and security.

DevOps Engineer · Platform Engineer · Site Reliability Engineer · Systems Administrator

[GitHub](#) | [LinkedIn](#) | [Blog](#)

Professional Summary

Senior System Administrator, with 11+ years spanning infrastructure, web, and operations.

Resume Info

This resume has been created in a [dockerfile](#) built by a [makefile](#) and deployed using [Github Actions' CI/CD](#). The document is published everyday, with a timestamp at the last page denoting it's publishing date.

Download this document: <https://github.com/MarcusHoltz/resume-generator/>

Skills

Linux Systems Administration

Maintain reliable hybrid cloud environments using SSH tunneling, SSL/TLS, VPN, and SSO identity management across production and development tiers.

Monitor and log performance, bandwidth, memory, disk health, and application uptime using Glances, Netdata, Prometheus, Grafana, Loki, and Diskover.

Cross-platform administration across Debian, Ubuntu, CentOS, RHEL, and FreeBSD production systems.

Virtualization

Manage system virtualization with Docker, QEMU, KVM, Proxmox, and VMware ESXi; leverage virtio's 9p filesystem for improved I/O throughput.

Produce system templates for cloning, backup, and cross-platform restoration in vmdk, vdi, vhdx, qcow2, and raw formats.

Containers & Orchestration

Design, build, and deploy containers using Docker, Docker Compose, LXC, and containerd; maintain images on Docker Hub and GitHub/GitLab registries.

Work with distributed storage technologies (NFS, Ceph, S3) and cluster orchestration (Kubernetes, Docker Swarm).

Security, Hardening & DevSecOps

Deploy and tune Web Application Firewalls (WAF), IDS/IPS (SecurityOnion, Suricata, nzyme), and behavioral firewalls (CrowdSec) across cloud and on-prem environments.

Apply DevSecOps practices: WAF smoke testing against OWASP Top 10 vectors, secrets management in CI/CD pipelines, and cloud security hardening across containerized services.

Implement zero-trust network access, SSO with ForwardAuth, geo-IP filtering, and VPN obfuscation.

Networking (Virtual & Physical)

Design and document network infrastructure with VLAN segregation, virtualized edge routing (OPNsense, pfSense), and site-to-site WireGuard VPNs.

Operate technologies including OpenVSwitch, HAProxy, Traefik, and Nginx for load balancing and reverse proxying; Unbound, PowerDNS, DNSSEC, DNSCrypt, and DNS-over-TLS for DNS infrastructure.

Deploy virtual network infrastructure on VMware ESXi, Proxmox, Hyper-V, and Xen.

Disaster Recovery & Storage

Architect and maintain enterprise-grade Proxmox high-availability ZFS solutions with 15-minute incremental snapshots, Proxmox Backup Server 2, and off-site replication via Sanoid/Syncoid.

Manage ZFS pool design with tuned compression, deduplication, and snapshot scheduling across cluster migrations.

DevOps & Automation

Proficient in Infrastructure as Code (IaC) and configuration management: Ansible, Terraform, Helm, ArgoCD, Chef, Puppet, SaltStack, OpenStack.

Build and maintain CI/CD pipelines with GitHub Actions, GitLab CI, Jenkins, and self-hosted runners.

Use of core AWS, Azure, GCP, and Oracle Cloud services (ALB, ELB, EC2, RDS, S3).

Identity & Access Management (IAM)

Configure and maintain Active Directory, SCCM, Domain Controllers, FSMO roles, Group Policy, and AD replication.

Deploy and manage SSO and identity federation with Authentik and Keycloak using Kerberos, OAuth2, and OpenID Connect.

Administer OpenLDAP and RADIUS for on-premise and hybrid identity environments.

Web & Front-End Development

Design and build custom front-end interfaces and backend systems using TypeScript, JavaScript, and modern CMSs including WordPress and Drupal.

Integrate data from external APIs, election databases, employee directories, and interactive mapping services.

Enforce web standards, ADA/WCAG compliance, and SEO best practices across all client sites.

Data Analytics & Reporting

Produce weekly and monthly stakeholder reports using data-driven insights, A/B test results, and visualized metrics.

Execute SEO/SEM campaigns across web, email, and ad channels — consistently improving organic traffic and conversion.

Certifications

CompTIA Network+ — Vendor-neutral validation of core networking, troubleshooting, and infrastructure management competencies.

CompTIA Security+ — Industry and government-recognized certification covering threat analysis, incident response, digital forensics, and enterprise risk mitigation.

Pursuing: CISSP (Q4 2026) · CKA (Q2 2027) · RHCE (Q4 2027) · OSCP (Q2 2028)

Technical Projects

DevOps & Automation

Self-Hosted GitLab with CI Runners & TLS Full GitLab Omnibus deployment with registered CI runners and automated TLS certificate management via Traefik. Provides a completely private, git-controlled CI/CD platform with a demonstration project included out of the box. github.com/MarcusHoltz/docker-gitlab-runner

Auto-Updating Resume Pipeline CI/CD pipeline that rebuilds and publishes a polished resume every day via GitHub Actions. Containerized LaTeX/Pandoc rendering produces a versioned, timestamped PDF artifact on each run – the pipeline itself is the portfolio piece. github.com/MarcusHoltz/resume-generator

Docker Secrets & Vault Management Secure secrets injection pipeline using Docker Secrets integrated with GitLab CI. Eliminates plaintext credentials from pipelines and repositories – secrets never touch disk unencrypted. github.com/MarcusHoltz/setting-up-docker-secrets-in-gitlab

Traefik Docker Cron Scheduler Toggles Traefik-fronted services on and off based on a configurable cron schedule – automatically shutting down non-essential containers after hours without removing their configuration. github.com/MarcusHoltz/traefik-docker-cron

Proxmox 8→9 Upgrade Script Automated in-place upgrade path for Proxmox VE with preflight safety checks, cluster awareness, and Proxmox Backup Server 2 compatibility verification – no manual steps, no surprises. github.com/MarcusHoltz/proxmox-8to9-upgrade

Zammad Knowledge Base → Static Site Backup Self-contained Docker tool that exports a Zammad knowledge base entirely to a directory tree of Markdown files on a schedule, compresses the output, and transfers it off-site – zero manual intervention. github.com/MarcusHoltz/zammad-knowledge-base-export-to-static-site

Automated Job Search AI Assistant AI-powered agent that autonomously scrapes job listings, scores relevance against a target profile using an LLM, and delivers prioritized alerts – removing the noise from job hunting entirely. blog.holtzweb.com

Symlink Curator – MusicLink Browser-based tool for managing media collections spread across network shares. Browse shares from a web UI, select files and folders, and it places symlinks into a single output folder with no file duplication. Compatible with Navidrome, Plex, and Jellyfin; runs on UnRAID, TrueNAS, and OpenMediaVault via Docker. github.com/MarcusHoltz/musiclink

Animated Plymouth Boot Screen Creator Bash pipeline that converts MP4 videos to PNG sequences and packages them as installable custom Plymouth boot themes, automating frame extraction, theme config, and initramfs integration. github.com/MarcusHoltz/Animated-Boot-Screen-Creator-for-Linux

Security Infrastructure

Authentik SSO with Traefik ForwardAuth Full SSO layer using Authentik on a Docker MacVLAN bridge, enabling Traefik to delegate authentication via ForwardAuth middleware without network collisions. Supports OAuth token exchange across isolated container networks. github.com/MarcusHoltz/Authentik-Traefik-MacVLAN

Geofiltered IP Blocklist Aggregator Aggregates multiple public threat blocklists into a single optimized firewall-ready list with VLSM compression and country-level geolocation filtering. Runs twice daily via GitHub Actions; compatible with OPNsense, pfSense, iptables, and OpenWRT. github.com/MarcusHoltz/ipblocklist-geofiltered

VPN over Port 53 WireGuard VPN tunneled through port 53, with iodine DNS tunnel as fallback and CrowdSec as a behavioral DNS firewall. Bypasses carrier-level VPN blocking – nftables routes traffic, CrowdSec bans probers at the kernel level. github.com/MarcusHoltz/vpn-over-port-53

Unique Stateless Password Derivation Script Generates repeatable, unique passwords for every service from a single master secret – no password manager required. Deterministic hashing means you can always reproduce the same credential without storing it anywhere. github.com/MarcusHoltz/password-hash-script

Hidden VPN Disguised as a Website Docker setup deploying an HTTPS proxy disguised as a legitimate tech-company landing page. XRAY VLESS over WebSocket/TLS routes traffic through a convincing decoy site – six industry presets, browser-based terminal via ttyd, zero-SSH management. github.com/MarcusHoltz/hidden-vpn-tha

Piping Server — Ephemeral Secure Sharing Self-hosted one-time-use encrypted data channels over plain HTTP. Used for secure file transfers, encrypted chat, and remote command execution — no special client software needed. blog.holtzweb.com

Tor Hidden Service with Vanity .onion Address Automated Docker deployment for Tor hidden services with mkp224o vanity address generation and X25519 client authorization — no open ports required. github.com/MarcusHoltz/tor-hidden-service

Transparent Nginx WAF on OPNsense Transparent Web Application Firewall using Nginx on OPNsense with Caddy and Traefik failover — layer-7 inspection and active threat blocking for self-hosted services, with zero changes required at the application layer. blog.holtzweb.com

nzyme Wireless Security Monitoring Deploys nzyme — a Java-based WiFi threat detection system using libpcap packet capture — to identify and physically locate rogue access points and wireless attacks, backed by a PostgreSQL database and web dashboards. github.com/MarcusHoltz/nzyme-install-wizard

DNS Image Transfer Encodes images in Base64, splits them across Cloudflare DNS TXT records, and stores the retrieval script in DNS itself. Download and reconstruct the image anywhere with only dig — no server, no HTTP. github.com/MarcusHoltz/DNS-photo-download

WAF Smoke Test Script Lightweight shell script that tests WAF effectiveness by firing a battery of attack patterns — SQLi, XSS, path traversal, and more — to verify blocking rules are actually working against OWASP Top 10 vectors. github.com/MarcusHoltz/waf-smoke-test.sh

Docker Service Phone-Home Audit Network audit tool that captures every outbound connection made by a Docker service, geolocates each IP, and delivers a PASS/FAIL verdict for phone-home behavior. Tests services in sealed Docker-in-Docker environments with Wireshark-compatible PCAP output. github.com/MarcusHoltz/docker-service-audit

Network Engineering

After-Hours Network Lockdown Automated network curfew: OpenWRT kills the WiFi radio, OPNsense VLAN firewall rules lock down traffic, and Authentik policies block application logins — all on a schedule. Includes daily SSID rotation with the password hidden inside a math puzzle. blog.holtzweb.com

OPNsense Multi-Site HAProxy + Unbound Layer-7 traffic routing across multiple domains through a single OPNsense box — HAProxy for domain-based splitting, Unbound for split-DNS, DNSCrypt for encrypted upstream resolution, and WireGuard for secure remote access. blog.holtzweb.com

OPNsense WireGuard Site-to-Site VPN Full WireGuard VPN deployment on OPNsense for site-to-site tunnels and remote access — cryptographic key routing, firewall rules, DNSSEC-validating Unbound, and multi-site subnet routing. blog.holtzweb.com

HAProxy Proxy Protocol to Traefik Configures HAProxy on OPNsense to forward real client IPs through multiple proxy layers to Traefik using Proxy Protocol v2 — domain-based routing with full client metadata preserved end-to-end for accurate logging and rate limiting. blog.holtzweb.com

PowerDNS + Unbound DNS Infrastructure Authoritative (PowerDNS with web GUI) and recursive (Unbound with DNSSEC validation) DNS stack — fully self-hosted, no upstream provider dependency for internal zone resolution. blog.holtzweb.com

Monitoring & Observability

Grafana + Alloy + Loki Observability Stack Containerized full-stack observability: Grafana dashboards, Loki log aggregation, and Grafana Alloy as the OpenTelemetry-compatible collector — Docker Compose deployed with persistent storage and alerting rules. github.com/MarcusHoltz/grafana-loki-alloy-homelab-monitoring-stack

Docker MacVLAN Traefik Analytics Traefik deployed on a MacVLAN interface for direct physical network access, feeding un-NAT'd access logs through Promtail → Loki → Grafana for accurate per-client analytics without exposing the host network. github.com/MarcusHoltz/Traefik-MacVLAN

Homelab & Infrastructure

Proxmox Disaster Recovery System Enterprise-grade automated backup and disaster recovery for Proxmox clusters: ZFS snapshots managed by Sanoid, VM-level backups via cv4pve, and off-site incremental replication to Proxmox Backup Server 2 – fully hands-off with quarterly restore validation. github.com/MarcusHoltz/proxmox-autom

ZFS Storage & Snapshot Architecture Optimal ZFS datastore design for Proxmox – pool layout, compression, deduplication, snapshot scheduling, and cluster-friendly dataset naming conventions that survive live migrations without I/O storms. blog.holtzweb.com

Reticulum Mesh Network Demo Self-contained Docker demo for Reticulum – a cryptographic mesh networking stack where every address is the hash of a public key. Runs encrypted shells, file transfers, and LoRa mesh radio demonstrations from a browser-based terminal. github.com/MarcusHoltz/reticulum-demo

Immich Self-Hosted Photo Platform Complete Immich deployment on UnRAID with Docker – self-hosted Google Photos replacement with ML-powered photo analysis, duplicate detection, multi-user support, video compression, and NetBird VPN for remote access. github.com/MarcusHoltz/immich-setup

Cloudflare Email Routing & Aliasing Privacy-first infinite unique inbound email alias system using Cloudflare Email Routing – all addresses route to a single private mailbox with no third-party dependency and no PII exposed to senders. blog.holtzweb.com

Web Development

Astro Portfolio Site (*marcusholtz.com*) This portfolio, built on Astro with TypeScript and Tailwind CSS. Content driven by JSON files – multi-stage Docker CI with automatic one-command deploy to GitHub Pages, GitLab, Cloudflare, or a self-hosted VPS. github.com/MarcusHoltz/astro-portfolio-theme

Astro Marketing Theme Astro 6 + Tailwind CSS 4 marketing site template with persistent sidebar navigation, nested dropdowns, RSS blog importer, portfolio slider, Web3Forms contact integration, and a simulated chat widget. All content lives in JSON files. github.com/MarcusHoltz/astro-marketing-theme

Chrome/Firefox Extension – Zammad Time Tracker Browser extension for Chrome and Firefox that surfaces Zammad helpdesk ticket time tracking directly in the toolbar, eliminating context-switching when logging billable hours. github.com/MarcusHoltz/zammad-time-tracker-browser-extensions

WheelSpin – Self-Hosted Random Selector Self-hosted spinning wheel web application for randomly selecting outcomes, with fully configurable entry lists and Docker deployment. github.com/MarcusHoltz/wheelspin

Self-Hosted Interactive Map Web application for drawing and labeling geographic areas with persistent storage – used for network topology and infrastructure diagrams with no cloud dependency. github.com/MarcusHoltz/map-layer

Client Work (Holtzweb)

Clearwave (*Technology*) – Full frontend redesign and custom backend development for a technology sector client; clean architecture, fast load times, and conversion-focused layout.

Roberts Law (*Legal*) – Law firm site rebuilt for organic search performance with SEO-optimized information architecture; measurably increased organic traffic.

City of Carterville (*Municipalities*) – Full municipal government website with ADA-compliant, mobile-first resident services portal and content management system.

Carterville Parks & Recreation (*Municipalities*) – Parks department site with aquatics schedules, adult recreation program listings, and responsive layout.

Eclipse Tourism (*Tourism*) – Interactive JavaScript event map with filterable overlays, built for high traffic during a regional solar eclipse campaign.

Giant City Lodge (*Tourism*) – Lodge and restaurant website with full menu integration and responsive design for tourism visitors.

Warpath Industries (*Manufacturing*) – Company capabilities and product line showcase with animated homepage intro.

Level 7 Motorsports (*Manufacturing*) – Motorsports lifestyle brand with dynamic homepage, editorial content templates, and single-post layouts.

Images Framing (*Retail*) – Custom framing shop with services showcase and clean product-focused layout.

Chef Clash (*Non-Profit*) – Full fundraising platform for a live charitable cooking event – separate donor and recipient user flows, event management, and real-time updates; designed and deployed end-to-end.

Boys & Girls Club (*Non-Profit*) – Chapter website with membership signup, program pages, and community-focused design.

Cedar Court Imaging (*Healthcare*) – Medical imaging center site highlighting advanced scanning technology and patient services.

IESO Medical Cannabis (*Healthcare*) – Illinois medical cannabis provider site converted from PSD to HTML with compliant design for patient registration and education.

Milano Metal Recycling (*Manufacturing*) – Metal recycling company website covering accepted materials, pricing, and facility info for commercial and residential clients.

The Vape Shop (*Retail*) – Vape and e-juice storefront with animated product demos and dynamic inventory presentation.

SEO Performance Audit (*SEO*) – Comprehensive site crawl and audit dashboard identifying technical SEO deficiencies with a prioritized remediation roadmap.

Presentations

Web Confidentiality, Privacy & Security *BLUG – Boulder, CO (May 2024)* Presentation covering fingerprinting vectors, tracker evasion, DNS-over-HTTPS, compartmentalization strategies, and hardened browser profiles for everyday use. blog.holtzweb.com/posts/browsers-web-browser-privacy

Enterprise Security Across All Devices *Software Freedom School – Littleton, CO* Five-part deep dive into layered home network security: auditing Android traffic (TrackerControl, PCAPdroid, cert-pinning bypass), per-app outbound firewalls on every OS (OpenSnitch, Little Snitch, WFC), router-level visibility with ntopng and Suricata IDS/IPS, anonymous exit strategies (Tor, I2P, XRAY), and a hardened home network stack built on OpenWRT and OPNsense. holtzweb.com/talks/home_network_security

Automate Custom Deployments with Cloud-init *Software Freedom School – Littleton, CO (August 2023)* Practical guide to writing reusable Cloud-init templates for provisioning users, packages, SSH keys, and services from a single declarative config at first boot – enabling repeatable fleet deployments at scale. gitlab.com/marcusholtz/sfs

OpenWRT Network Infrastructure *Software Freedom School – Littleton, CO (April 2023)* Custom router firmware ecosystem overview covering 1,500+ supported devices, OpenWRT build systems, package management, and enterprise-grade features on consumer hardware. holtzweb.com/openwrt-presentation.html

Browser Privacy *BLUG – Boulder, CO (November 2022) | Software Freedom School (September 2022)* Audience-interactive session on understanding data collection by browsers and tools, with live opt-in/opt-out demonstrations. [Slides](#) | [Video](#)

Self-Hosted Social Networking Services (Mastodon) *Software Freedom School – Littleton, CO (December 2022)* Hands-on walkthrough of deploying Mastodon, configuring ActivityPub federation, and operating decentralized social infrastructure on private hardware. [Slides](#) | [Video](#)

Homelab: Introduction to Self-Hosting *Software Freedom School – Littleton, CO* Beginner-to-intermediate guide covering motivations (privacy, learning, custom solutions), a four-step framework for getting started, hardware choices from Raspberry Pi to rack servers, and real-world use cases: home automation, media streaming, file storage, and password management. holtzweb.com/talks/homelab

Industry Experience

IT Consulting & Systems Engineering

***Holtzweb / Holtzhost — Denver, CO2019 – Present*

Architect and maintain self-hosted, privacy-first hosting infrastructure for clients under holtzhost.com, running entirely on self-owned servers.

Establish cloud hosting environments, virtualization platforms, and operations tooling for client organizations across multiple industries.

Deliver SEO/SEM strategy and execution across web, email newsletters, and paid channels — achieving measurable increases in both web and in-person traffic (40%+ lift for select clients).

Operate a full-service IT helpdesk, network and server design practice, and WordPress/custom-build web development shop under holtzweb.com.

Leadership & Community

***Software Freedom School — Littleton, CO2022 – 2024*

Served as board member from March 2023 through 2024; contributed to organizational direction and technology strategy.

Maintained and triaged open tickets on the [SysOps board](#).

Delivered seven public talks on systems, networking, privacy, and security topics at monthly community meetings.

Participated in weekly Linux study group as both student and presenter.

Web Development

***Highline Ideas · 1187 · Mayer Networks — Carbondale, IL2013 – 2017*

Designed and built custom website layouts, user interfaces, and backend systems tailored to individual client requirements and deadlines.

Integrated external data sources including election data, employee directories, and interactive event mapping.

Worked directly with clients to translate business and marketing goals into technical specifications.

Executed SEO initiatives, web analytics analysis, and third-party A/B testing and optimization.

Enforced web standards and ADA/WCAG accessibility compliance across all delivered sites.

Diagnosed and repaired broken CMS installs, compromised sites, corrupted databases, and outdated plugin stacks.

Education

BS in Finance — Southern Illinois University Carbondale | 2011

Tools & Technologies

Operating Systems: Linux (Debian, Ubuntu, RHEL/CentOS, OpenSUSE, Alpine), FreeBSD, Windows Server

Infrastructure & Virtualization: Proxmox, QEMU/KVM, VMware ESXi/vSphere, Hyper-V, Xen, libvirt, Vagrant

Containers & Orchestration: Docker, Docker Compose, LXC, containerd, Kubernetes, Docker Swarm, Helm

Networking & Security: OPNsense, pfSense, OpenWRT, HAProxy, Traefik, Nginx, Caddy, WireGuard, OpenVPN, Suricata, CrowdSec, SecurityOnion, nzyme, Unbound, PowerDNS, BIND, DNSCrypt, DNSSEC

Identity & Access Management (IAM): Authentik, Keycloak, Active Directory, OpenLDAP, RADIUS, OAuth2,

OpenID Connect, Kerberos

Monitoring & Observability: Prometheus, Grafana, Loki, Alloy, ELK Stack, Netdata, Glances, Diskover, Promtail

Automation & IaC: Ansible, Terraform, Helm, ArgoCD, Chef, Puppet, SaltStack, OpenStack, GitHub Actions, GitLab CI, Jenkins, Cloud-init, n8n

Cloud Platforms: AWS (EC2, RDS, S3, ALB/ELB), Microsoft Azure, GCP, Oracle Cloud, DigitalOcean, Cloudflare

Languages & Scripting: Bash, Python, JavaScript, TypeScript, HTML, CSS

Databases: MySQL, PostgreSQL, MariaDB, Redis, MongoDB, SQLite

Web & Front-End: React, TypeScript, WordPress, Drupal, Joomla, DNN, Hugo, Astro, Apache, Nginx, Tailwind CSS, Bootstrap, Foundation

Version Control: Git, GitHub, GitLab

Storage: ZFS (OpenZFS), NFS, Ceph, S3-compatible object storage, Sanoid/Syncoid

Design: Adobe Creative Cloud (Photoshop, Illustrator, After Effects), LaTeX, Markdown

SEO & Analytics: Google Analytics, Matomo/Piwik, MOZ, SEMrush, Megalytic

This resume last built on: Sunday 24th May, 2026