Kevin C Davies

Senior Infrastructure Engineer | Linux Systems, Network Security & Incident Response

Cape Town, South Africa · Afrikaans, English
site_human@spac3.co.za · www.linkedin.com/in/kcdavies

Linux Systems Administration | Network & Firewall Security | Virtualization (Proxmox) | Automation (Python/Bash) | Monitoring (Zabbix) | High Availability (VRRP/BGP/OSPF) | Incident Response | AWS | DDoS Mitigation (L3/L4/L7)

EXECUTIVE SUMMARY

Infrastructure Engineer and Systems Administrator with 14+ years of IT Operations experience, including 7+ years at AWS owning network security, automation, and incident response for global enterprise infrastructure. Hands-on background spans Linux systems administration and hardening, virtualization (Proxmox, Docker), firewall and VPN configuration, storage and backup/recovery operations, high-availability networking (VRRP, BGP, OSPF), monitoring platform ownership (Zabbix), and Python/Bash automation that reduced manual operational effort across teams. Experienced in maintaining uptime, resilience, and high availability for regulated, customer-facing infrastructure within structured, ticket-driven change-management environments, with a track record of documentation, runbooks, mentoring, and cross-team knowledge transfer. Currently pursuing a BSc in IT (Security and Network Engineering).

KEY ACHIEVEMENTS

- Built Python automation for traffic-to-WAF rule conversion, used ~55 times per month — reducing mitigation time by 1+ hour per incident and saving an estimated 650+ hours annually.
- Owned uptime and resilience for enterprise banking and gaming infrastructure through high-volume DDoS events, in a regulated, customer-facing environment.
- Independently learned Linux and compiled Zabbix from source to replace an unreliable monitoring platform, later building a cross-team traffic-analysis platform adopted by multiple security teams.
- Recognized as AWS WAF Subject Matter Expert; delivered technical training on networking, Python, and security tooling to internal teams.

CORE SKILLS & SPECIALISATIONS

- Linux systems administration and hardening (Ubuntu, RHEL) across personal infrastructure, internal AWS environments, and production web-hosting environments
- Virtualization and infrastructure ownership (Proxmox, Docker, AWS EC2) — deployment, capacity planning, and lifecycle management

- Network and firewall security operations (TCP/IP, VPN, routing, switching, segmentation, MikroTik RouterOS, AWS Security Groups/NACLs)
- Storage, backup, and recovery operations (AWS volume snapshots, file/database backups, replication)
- High-availability networking and resilient routing (VRRP, BGP, OSPF)
- Monitoring platform ownership and operational visibility (Zabbix, custom traffic-analysis tooling)
- Security automation, scripting, and configuration management (Python, Bash, drift detection, CI/CD)
- Incident response leadership and uptime/resilience ownership under pressure
- Documentation, runbooks, and cross-team knowledge transfer
- DDoS mitigation and attack-surface reduction at scale (L3/L4/L7)

WORK EXPERIENCE

Amazon Web Services (AWS) Jan 2018 – May 2026

Security Engineer (DDoS Mitigation and Network Security) | Sep 2022 – May 2026

Owned network security operations, automation, and incident response for AWS global infrastructure — driving uptime, resilience, and continuous improvement of detection and mitigation tooling for enterprise customers.

- Owned firewall and network security configuration across a multi-account estate, building automated configuration-drift detection and remediation tooling to keep security configuration consistent across the firewall fleet.
- Led end-to-end incident response for high-volume network and application-layer attacks — triage, containment, and mitigation — maintaining uptime and resilience for enterprise banking and gaming infrastructure under sustained pressure.
- Built Python automation services with CI/CD pipelines, including a traffic-to-WAF rule conversion tool used ~55 times per month, reducing mitigation time by 1+ hour per incident and saving an estimated 650+ hours annually.
- Designed and operated an automated notification system (AWS SNS, Lambda, S3, DynamoDB) that alerted customers when firewall configuration changed for their resources, improving operational visibility and monitoring.
- Maintained and extended a cross-team traffic-analysis platform — largely as sole owner — used by multiple security teams for attack investigation, root-cause analysis, and threat-intelligence correlation.
- Built Python tooling for IP intelligence enrichment, PCAP scanning, and ticket-processing automation, reducing manual investigation time across the team.
- Investigated network and application-layer security incidents using packet analysis (Wireshark) and TLS fingerprinting (JA3/JA4), correlating indicators to harden infrastructure against attacker techniques.
- Delivered technical training and documentation on automation tooling, Python, and network security practices, improving team-wide operational consistency.

Technologies: DDoS Mitigation; AWS WAF (Web Application Firewall); AWS Shield Advanced; Network Security; Cloud Security; TLS Fingerprinting (JA3/JA4); Indicators of Compromise (IOCs); Python; Bash; Automation; Configuration Management (drift detection); CI/CD (AWS CloudFormation with custom internal tooling); Packet Analysis (Wireshark); Amazon VPC (Security Groups, NACLs, Routing, VPN); AWS Lambda; Amazon Athena; Amazon DynamoDB; Amazon API Gateway; Amazon SNS; Amazon S3; Linux (AWS Red Hat); Git; Elastic search

Cloud Support Engineer 2 (Networking) | Apr 2021 – Sep 2022

Provided advanced network infrastructure support, incident response, and escalation management for AWS enterprise customers, with a focus on networking fundamentals, security configuration, and operational reliability — using Linux (Red Hat) for internal testing and troubleshooting.

- Resolved complex networking and security issues for AWS customer environments — VPC, Route 53, security groups, and VPN configurations —

under time pressure, using Linux (Red Hat) systems for internal testing and troubleshooting.
- Led real-time incident troubleshooting on customer bridge calls, driving resolution from initial triage through incident closure.
- Partnered with internal engineering teams on escalated incidents, driving triage, resolution, and coordinated customer communications.
- Built Bash automation for DNS migration between Route 53 hosted zones and custom packet-capture troubleshooting scripts, reducing manual effort and time-to-diagnosis.
- Promoted to Cloud Support Engineer 2 in recognition of advanced networking/security troubleshooting performance and AWS WAF subject-matter expertise.

Technologies: Network Security; AWS WAF (Web Application Firewall); Amazon Route 53; Cloud Security; Amazon EC2; AWS Lambda; Amazon Athena; Amazon DynamoDB; Amazon API Gateway; Amazon VPC (Security Groups, NACLs, routing, VPN); Bash; Linux (AWS Red Hat); Packet Analysis (Wireshark); Git; BGP

Cloud Support Engineer (Networking) | Jan 2018 – Apr 2021

Diagnosed and resolved AWS customer network and security incidents — including application-layer attacks, WAF rule engineering, and core connectivity troubleshooting across DNS, VPC, and Direct Connect. Recognized as AWS WAF Subject Matter Expert and delivered technical training to internal teams.

- Diagnosed and resolved complex connectivity and security issues across AWS Direct Connect, VPC, Route 53, CloudFront, and EC2 — including security groups, NACLs, VPN, and routing — for enterprise customer environments.
- Designed custom AWS WAF rules, rate-limiting strategies, and L7 filtering controls to mitigate malicious traffic and DDoS attacks, reducing customer-facing risk.
- Led customer-facing incident calls to investigate active threats, scope impact from limited information, and coordinate containment in real time.
- Validated traffic flow and network/security architecture to ensure requests traversed intended controls before reaching backend resources.
- Recognized as AWS WAF Subject Matter Expert (December 2019); delivered technical training on AWS WAF, networking, and Python to internal teams and onboarded new hires on DNS (Route 53).

Technologies: DDoS Mitigation; AWS WAF (Web Application Firewall); Network Security; Amazon Route 53; Amazon CloudFront; Packet Analysis (Wireshark); Python; AWS Lambda; Amazon Athena; Amazon DynamoDB; AWS Direct Connect; Amazon EC2; Amazon VPC (Security Groups, NACLs, routing, VPN); Bash; PowerShell; Linux (AWS Red Hat); Git; BGP

The Copper RC

Sep 2020 – Feb 2022

Co-Founder

Co-founded a web development business focused on delivering WordPress websites, owning infrastructure, deployment architecture, and security end-to-end.

- Owned infrastructure architecture, deployment, and security end-to-end for a web-hosting business — administering Linux (Ubuntu) servers, Proxmox virtualization, and Docker-based environments for reproducible client delivery.
- Deployed production workloads on Amazon EC2 with Amazon CloudFront, restricting origin access to CloudFront-only traffic and leveraging edge caching to mitigate malicious request spikes.
- Managed backup and recovery for client infrastructure, including AWS EC2 volume snapshots and scheduled file/database backups.
- Engineered a static-site conversion process for non-authenticated WordPress sites and hosted outputs on Amazon S3, reducing hosting cost, operational overhead, and attack surface.
- Administered MySQL databases supporting client WordPress sites and internal tooling.

Technologies: WordPress; MySQL; Docker container; Amazon EC2; Cloud Security; Amazon CloudFront; Amazon S3; MySQL; Python; Virtualbox; Bash; Linux (Ubuntu); Git; OpenCRM; Proxmox; AWS volume snapshots; Backup and Recovery

OculusIP

Sep 2013 – Dec 2017

Network Operations Center (NOC) Administrator

Owned monitoring and operational reliability for customer and internal network infrastructure — implementing Zabbix monitoring at scale on self-administered Linux servers, automating operations with Python, and maintaining firewall security across distributed environments.

- Implemented and operated Zabbix monitoring at scale for customer and internal infrastructure, including distributed monitoring-proxy deployments across partner ISP networks.
- Administered routing and switching infrastructure (BGP, OSPF, VRRP) and firewall policy management (MikroTik RouterOS) across distributed network environments.
- Performed server backups of files and databases to support recovery and operational continuity.
- Developed Python scripts to automate NOC operational tasks and improve incident-response efficiency.
- Implemented firewall controls and automated IP block-listing to mitigate reflection attacks and abusive traffic patterns.
- Investigated SIP/VoIP compromise incidents using packet captures and call detail records, determining scope and recommending PBX hardening measures.
- Delivered internal training on networking fundamentals and MikroTik RouterOS configuration to improve operational readiness.

Technologies: Zabbix; MySQL; Python; Automation; Backup and Recovery; VoIP (SIP, RTP); 3CX PBX; Firewall Management; MikroTik RouterOS; Routing and Switching; Bash; Linux (Ubuntu); Packet Analysis (Wireshark); PortaOne PortaSwitch; Google Workspace; Ubiquity; Vtiger CRM; Zoho CRM; Freshdesk; BGP; OSPF; VRRP

Webcall

Feb 2012 – Aug 2013

Technical Support

Provided technical support for connectivity and network devices; independently learned Linux and built monitoring solutions (Zabbix) to replace an unreliable platform.

- Diagnosed and reported connectivity issues across ADSL, wireless, VPN, Diginet, and fiber services.
- Managed ISP account operations on a private RADIUS interface and maintained case workflows in Sage CRM.
- Administered Google Apps user accounts and support operations for business productivity services.
- Configured routers, IP phones, and VoIP gateways; supported PBX troubleshooting for vendors and customers.
- Independently learned Linux and compiled Zabbix from source to replace an unreliable monitoring platform.
- Built Linux and VirtualBox-based support environments to run monitoring services and technician proxy stations.

Technologies: VoIP (SIP, RTP); Zabbix; MySQL; MikroTik The Dude; Linux (Ubuntu); Routing and Switching; PortaOne PortaSwitch; Google Workspace; RADIUS; Virtualbox; PBX (Samsung MGI)

Sunglass Hut

Jan 2010 – Jan 2011

Junior Desktop Support Technician

Provided desktop support, hardware/software troubleshooting, and user administration for retail and head office staff.

- Delivered helpdesk and remote support for head office staff and a distributed retail store environment.
- Diagnosed communication and endpoint issues and coordinated escalations with third-party and international teams.
- Built and configured end-user devices and administered Microsoft Exchange and BlackBerry Enterprise Server services.
- Managed user access and support operations across hardware, software, and network-connected business systems.
- Provided telephonic hardware and software support for approximately 150 stores and onsite support for approximately 100 head office users.

Technologies: Microsoft Exchange Server; BlackBerry Enterprise Server (BES)

EDUCATION

Eduvos Jan 2024 – Dec 2027

Bachelor of Science (BSc) in Information Technology - Security and Network Engineering

CERTIFICATIONS

CompTIA A+ (IT Technician) (lapsed 2012); CompTIA Network+ (lapsed 2012); Microsoft Certified Professional (lapsed 2011); 3CX Phone System Advanced Certification v12.5 (issued 2014); 3CX Phone System Basic Certification v12.5 (issued 2014); MikroTik Certified Routing Engineer (MTCRE) (lapsed 2017); MikroTik Certified Network Associate (MTCNA) (lapsed 2017); PH526x: Using Python for Research (issued 2017)

SOFT SKILLS

Adaptability; Analytical Problem-Solving; Cross-Team Coordination; Escalation Management; Leadership Under Pressure; Mentoring & Knowledge Transfer; Stakeholder Communication