

# Jeff Kaleth

Indianapolis, Indiana, United States

[jkaleth@gmail.com](mailto:jkaleth@gmail.com)

317-294-3883

[linkedin.com/in/jeffkaleth](https://www.linkedin.com/in/jeffkaleth)

## Summary

INFRASTRUCTURE, CLOUD, SECURITY : AWS, Azure, Confluence, CrowdStrike, Redhat Enterprise Linux Windows Server, Proofpoint TAP/TRAP, Extrahop, Tenable.sc, Tenable.io, Zerofox, Devo.

AUDIO/VIDEO/CONTENT PRODUCTION : Visual Studio Code, GIT, Apple Logic Pro X, Ableton Live 11, Screenflow, Adobe Premier/Photoshop/After Effects, Keynote.

## Experience

### IT Engineer, Threat Intelligence

#### Ulta Beauty

Sep 2021 - Present (2 years 3 months)

- \* Vulnerability Management: Pen testing and analysis of server and web application vulnerabilities using Tenable.sc, Tenable.io, and Kali Purple.
- \* Threat Intelligence Gathering: Leverage Zerofox to collect, analyze, and disseminate threat intelligence from various sources, including open-source feeds and dark web forums.
- \* Digital Forensics: Leverage Kali Linux and other forensics tools to conduct data acquisition, preservation, and analysis on various digital media while adhering to strict chain of custody protocols.
- \* Incident Response: Participate in incident response activities, assisting in the identification, containment, and eradication of security incidents.
- \* Phishing Attack Mitigation: Utilizing Cortex XSOAR, Proofpoint TAP/TRAP to manage phishing threats.
- \* Security Tool Management: Operate Cortex XSOAR and Devo security tools to automate data collection, analysis, and remediations.
- \* Malware Analysis: Utilizing CrowdStrike Falcon to analyze and remediate malicious software and document findings, including indicators of compromise (IOCs).
- \* Risk Assessment: Conduct risk assessments on software, devices, and cloud services to evaluate the potential impact of threats and vulnerabilities on the organization's security posture.
- \* Cyber Threat Reporting: Prepare and deliver detailed threat intelligence reports, including actionable recommendations, to senior management and relevant stakeholders.
- \* Security Awareness Training: Collaborate with the security awareness team to develop training materials and programs to educate employees about current cyber threats and best practices.
- \* Intrusion Detection: Monitor network with Extrahop, Akamai, and CrowdStrike for suspicious activities, create custom detection rules, and investigate security incidents.
- \* Documentation: Development of end user documentation for threat management processes and procedures utilizing markdown and Confluence cloud.

### Multimedia Content Creator

#### Freelance

Jun 2005 - Present (18 years 6 months)

#### AUDIO

- \* Engineering audio with Apple Logic Pro X.

- \*Mix engineering
- \*Audio mastering
- \*Music distribution on Spotify

## PHOTOGRAPHY

- \* Landscape and abandoned photography
- \* Experience with DSLR, iPhone, and drone photography
- \* Utilizing Adobe Creative Suite for design

## VIDEO

- \*Created technical presentations covering Linux automation and cloud technologies
- \*Develop technical documentation for lessons processes and procedures.
- \*Built Linux lab environment running KVM virtualization for demonstrations.
- \*Utilized Keynote to create animated slides for video presentations.
- \*Edited raw video content in Screenflow and Adobe Premier.
- \*Leveraged Visual Studio Code to create markdown for technical documents.
- \*Used Atlassian's Confluence for lesson documentation.
- \*Utilized GIT for document and code repository
- \*Created and tested technical procedures to present during video lessons.
- \*Drone video of landscapes and real estate

## Media Links:

Meditation style Youtube channel

<https://www.youtube.com/@zentheater3091>

Technical IT content channel

<https://www.youtube.com/@techadventuresonline2156>

## **Associate Engineer, Infrastructure**

### Ulta Beauty

May 2016 - Sep 2021 (5 years 5 months)

- \*Obtained AWS Certified Solutions Architect - Associate SAA-C02 certification
- \*Created and presented training content to shift left support tasks to the operations team.
- \*Developed a technical knowledge base for process and procedure documents.
- \*Peer reviewed technical documents created by the infrastructure team.
- \*Management of Microsoft Azure Redhat Enterprise Linux 7.9 compute resources.
- \*Obtained Microsoft Azure AZ-900 certification
- \*Administration and support of Red Hat Enterprise Linux (RHEL) 6x, 7x, and 8x servers.
- \*Administration and support of Microsoft Windows 2008, 2012 and 2016 servers.
- \*Administration and Management of Solarwinds monitoring environment.
- \*Analysis of Active Directory security with AD Audit Plus
- \*Utilization of Extrahop for network traffic analysis.
- \*Resolution of Linux server security vulnerabilities using Tenable reports
- \*Management of code, inventories, and documentation with Git and Confluence.
- \*Infrastructure support of Red Hat 7.9 servers hosting Docker containers.
- \*Responsible for automation initiatives utilizing Red Hat Ansible and Tower.
- \*Engineered Linux patching process and automated patching using Ansible Tower.
- \*Management of content views and repositories with Redhat Satellite.
- \*Management of scripts including Powershell, Bash, and Ansible playbooks.

- \*Leading the development of procedural content for the Disaster Recovery initiative.
- \*Responsible for onboarding and mentoring contractors and engineers.
- \*Manhattan WMS Warehouse Management System support.
- \*Leveraging Solarwinds to monitor production environments.
- \*Manhattan warehouse WMOS SDN installation and technical configuration.
- \*Windows server patch management using IBM BigFix.
- \*Participation in 24X7 on call rotation schedule.
- \*Management of virtual machines with VmWare VSphere 6.5

## **IT Engineer/Ulta Beauty- Contractor**

### **Decision Focus IT Infrastructure and Cyber Security**

Oct 2015 - 2016 (1 year)

Responsible for RHEL Linux 6.x/7.x, Windows Server 2003, 2008, 2012, and VmWare infrastructure management and technical documentation in support of the IT Middleware Team at Ulta Beauty Inc.

- \*Administration of Red Hat Enterprise Linux (RHEL) 6x and 7x application servers.
- \*Configuration & management of CUPS printing services on Linux RHEL
- \*Linux SNMP service installation & configuration.
- \*Manhattan WMS Warehouse Management System support.
- \*Technical documentation of repeatable processes.
- \*Application configuration on Microsoft Windows Server 2012.
- \*Solarwinds installation, configuration and administration.
- \*Creation of network and application diagrams.
- \*Confluence configuration, design, and maintenance.

## **IT & Business Consultant**

### **System Engineer**

Mar 2008 - Sep 2015 (7 years 7 months)

Technologies utilized:

Linux, MySQL, PHP, Apache, Citrix, Exchange, Cisco, PHP, Wordpress, Windows Server, Adobe Echosign, Wireless IP Cameras, Stripe/Square Merchant Payment Gateways, Quickbooks, Apple OSX, Wordpress, CSS, HTML, CentOS, Photoshop, SEO optimization, MBO Online Scheduling.

Responsibilities/Accomplishments:

- \*Red Hat Linux operating system management- file systems, permissions, applications.
- \*Create Linux CRON jobs for logs file, backup job launching, and application restarts.
- \*Contract development, analysis, and proofreading.
- Creation of employee manuals, guides, and repeatable process documentation
- \*Development of marketing materials and copy for web and print.
- \*Apache web server configuration and administration running on CentOS
- \*Setup and configuration of secure https sites for client websites.
- \*Installation and configuration on VMware ESX Installations.
- Maintenance and backup of My SQL databases with PHP admin.
- Administration of hosted accounts running on a CentOS server running Apache.
- Microsoft Exchange Server 2003/2008 administration and support.
- Windows Server 2003/2008 administration and support.
- \*Development and management of business websites running on Wordpress.
- \*Creation of employment agreements for contractors and employees.
- \*Developed repeatable process documentation for system procedures.

- Preparation of legal documents including rental, sub-contractor, and non compete agreements.
- Management of payroll for employees utilizing Google Forms and Intuit Quickbooks.
- Responsible for Indiana state, Indiana unemployment, and federal tax accounts.

## **Infrastructure Engineer**

### **Blackboard**

Jan 2009 - Jan 2010 (1 year 1 month)

- \*Managed Red Hat Linux virtual machines.
- Developed and maintained PCI compliance documentation.
- \*Developed documentation and templates for server and site builds.
- \*Created process manuals for configuring NetApp and server test labs.
- \*Administration of SQL Server 2005/2008 clusters.
- Developed documentation and templates for server and site builds.
- Management of 150 Windows 2003.2008 servers in a hosting environment.
- Developed and Maintained PCI Compliance Documentation.
- Windows Server 2003 and 2008 cluster installation and configuration.
- Setup Windows Server 2008 and SQL 2008 Dev environment.
- Management of SQL 2005 maintenance agent jobs.
- Citrix XenApp 5.0 administration
- Deployed and managed Citrix Xendesktop/Edgesight for test users.
- Administration of VMWare ESX 3.0 environment.

## **Amplifier Engineer**

### **HotBottle Amplification**

Feb 2005 - May 2009 (4 years 4 months)

- \*Point-to-point guitar amplifier manufacturing
- \*Logo/Website development and maintenance
- \*Customer service, new business development
- \*Shipping and packaging of amplifiers



## **System Engineer- Contractor**

### **Smart Group**

Aug 2006 - Nov 2008 (2 years 4 months)

- Managed 150+ Windows 2003 Enterprise Servers
- Developed/implemented backup retention policy that saved the city \$30,000 per year.
- Windows Server 2003/2008 installation and configuration.
- Enterprise backup system management on Scalar I2000 tape library.
- Windows Active Directory/Exchange 2003 email administration.
- Created scanning system for tracking enterprise backup tapes
- Assisted with Novell 6.5 to Microsoft Windows 2003 migration
- Assisted with Groupwise to Exchange conversion for 7000 users.
- Responsible for Exchange 2003 cluster/mailbox backup/recovery.
- Created repeatable process documentation for multiple admin tasks.
- Responsible for server and desktop patching through Altiris
- Lead project to test Windows Server 2008 with Dell
- Lead proof of concept project for Citrix Xenserver/XenApp and Xendesktop



## **Network Administrator/Contractor**

Delta Faucet Company

May 2006 - Aug 2006 (4 months)

- Administration of Novell 6.0 servers and Windows NT,2000,2003 Servers including Exchange 2003, IIS 5.0, DHCP, DNS, file and print servers.
- Management of DHCP address scopes and DNS
- Responsible for enterprise backup and restores with backup library running Commvault Galaxy software.
- Responsible for resolving trouble-tickets with Heat helpdesk software.
- Responsible for LDAP, Active Directory, and NDS object management.

## **System Administrator/Contractor**

Barnes and Thornburg

Mar 2005 - Apr 2006 (1 year 2 months)

- Administration of Unix-based, Windows NT,2000 and 2003 servers, Novell servers, Groupwise and Exchange email servers, and all network attached devices.
- Responsible for enterprise backup policies, full and incremental backup, and restores of company information.
- Management of server security patches, OS updates, and drive defragmentation of 30 application, web and file servers.
- Network security administration with ISS, Symantec Antivirus, Anti-spam defense.
- Managed NAS devices for document imaging system

## **Network Administrator**

TNSMI-TES

Mar 2003 - Nov 2004 (1 year 9 months)

- Performed and monitored network backups and restores with Computer Associates Brightstor Arcserve and Veritas Backup Exec on Windows 2003 and Novell servers.
- Project Manager for desktop migration from Groupwise 5.5 to Exchange Server 2003 and Windows 2003 Active Directory.
- Managed Windows Active Directory user accounts and Novell NDS accounts.
- Responsible for all system security including service packs, patch deployment, system updates, virus, and spam defense.

## **Education**



**Indiana University Northwest**

B.S., Business, Information Technology



**Musicians Institute**

RIT Certificate, Recording/Audio Production and Engineering

Studied Recording Engineering

**Linux Academy**

AWS Essentials Course

2019 - 2019

Learned and gained hands on experience with essential AWS services including IAM, EC2, S3, VPC, Cloudwatch RDS, AWS Auto Scaling, and Route 53.



## **Linux Academy**

Docker Quick Start Course

2019 - Present

## **A Cloud Guru**

AWS Certified Solution Architect Course

2020 - 2021

## **Licenses & Certifications**



**Microsoft Certified: Azure Fundamentals** - Microsoft



**AWS Certified Solutions Architect** - Amazon Web Services (AWS)

Issued Jun 2021 - Expires Jun 2024

## **Skills**

Tenable.sc • Tenable.io • Cortex XSOAR • Zerofox • Dark Web Monitoring • Ansible • Red Hat Enterprise Linux (RHEL) • Kali Linux • Kali Purple • Crowdstrike Falcon