CASE STUDY: The Autonomous Hybrid-Cloud Datacenter

Project Scope: 6-Layer Zero-Trust Infrastructure & Automated SecOps

Architect: David Culp, Principal Solutions Architect

Core Objective: To eliminate manual "human-element" errors through Infrastructure as Code (IaC) and self-healing architecture.

---

1. EXECUTIVE SUMMARY

I engineered a production-grade, private-cloud ecosystem designed for maximum autonomy. This architecture integrates **on-premise High-Availability (HA)** clusters with **Cloud-Native security gateways** and **automated vulnerability scanning**. The result is a "Self-Healing" datacenter that manages its own identity, security patching, and disaster recovery failover.

---

2. THE ARCHITECTURAL STACK (The 6-Layer Model)

The environment is structured into six interlocking layers to ensure no single point of failure:

- **Layer 1-2 (Resilient Networking):** Managed via **OPNsense** with strict VLAN segmentation.
- **Layer 3 (Identity & Access):** Centralized **FreeIPA (LDAP/Kerberos)** and **FreeRADIUS** for 802.1X, gated by an **Apache Guacamole** clientless gateway with MFA.
- **Layer 4 (Observability):** A full **ELK Stack (Elasticsearch, Logstash, Kibana)** providing a "Single Pane of Glass" for GeoIP threat maps and patch status.
- **Layer 5-6 (Automation): Ansible** orchestration for drift management and automated Sunday 3 AM maintenance windows.

---

3. CORE TECHNICAL PILLARS

A. High-Availability (HA) Compute Logic

To ensure zero downtime for critical services, I deployed a 3-node **Proxmox HA Cluster**.

- **The "Plug-Pull" Test:** I implemented **ZFS Replication** with 1-minute sync intervals.
- **Result:** Verified sub-120-second automated failover. If a physical node loses power, the cluster detects the loss (Fencing/Quorum) and automatically reboots mission-critical VMs on healthy nodes.

B. Remote Security Operations (The OpenVAS "Drop Box")

I developed a "Headless" vulnerability management solution for remote site auditing.

- **The Hardware:** Repurposed ultra-small form factor nodes (Acer CX13) running **Dockerized Greenbone (OpenVAS)**.
- **The Logic:** A "Call Home" **WireGuard** tunnel that bypasses client-side NAT/Firewalls, allowing for remote internal security audits without on-site configuration.

C. Secure Email Gateway (SEG) on GCP

To bridge local infrastructure with the cloud, I architected a **Proxmox Mail Gateway** on Google Cloud Platform.

- **Innovation:** Bypassed GCP's Port 25 restrictions by leveraging Google's SMTP Relay (Port 587/TLS).
- **Impact:** Created a secure, authenticated mail pipeline that provides granular, self-hosted security inspection for Google Workspace Enterprise.

---

4. ACHIEVEMENTS & PROOF OF CONCEPT

- **Zero-Trust Identity:** Every service in the datacenter—from SSH to Wi-Fi—requires **LDAP/MFA** authentication.
- **Autonomous Maintenance:** Achieved 100% automated patching across the fleet via **Ansible**, reducing manual admin overhead by an estimated **80%**.
- **Hardened Compliance:** Created a **HIPAA Hardening Script** that validates BitLocker, SMBv1 status, and Audit logging, providing an instant "Pass/Fail" report for auditors.

---

5. TECHNICAL DOCUMENTATION INDEX

- **Deployment Guide:** [Link to The Autonomous Datacenter Guide]
- **HA Logic & POC:** [Link to Proxmox HA Lab Demo]
- **Vulnerability Scanning:** [Link to OpenVAS Drop Box Guide]

- **Cloud Mail Security:** [Link to Google-Native SEG on GCP]