Yosef Naabid Gutiérrez

Windows and Linux Infrastructure Administrator

yosefnaabid@gmail.com | yosefnaabid.com | github.com/yosefnaabid | www.linkedin.com/in/yosefnaabid | +34 602 47 31 24

(Almería, Spain)

SUMMARY

Systems and infrastructure administrator, **sole person technically responsible for a 24/7 production environment** and previously for the systems of a **network of clinics and university postgraduate programs with 90 sites**. Specialized in Windows and Linux environments, virtualization, network security and identity, and infrastructure automation with monitoring and backups. Seeking to join a stable, long-term project.

TECHNICAL SKILLS

Systems and virtualization: Windows Server, Linux (Debian, RHEL), VMware ESXi/vCenter, Proxmox VE, Hyper-V, Active Directory (LDAP, GPO), Entra ID, Microsoft 365, Intune, Exchange
Networking and security: firewalls (Sophos XGS, OPNsense, nftables), Sophos Endpoint, MikroTik RouterOS, VPN (WireGuard, Sophos VPN), SELinux, CrowdSec, Nginx, Cloudflare, Let's Encrypt (HTTPS/TLS), VLAN, DHCP, DNS
Automation and operations: Bash, PowerShell, Python (pytest), Ansible, Terraform, Docker, Kubernetes, Git, GitHub Actions, CI/CD, systemd, Zabbix, Prometheus, Alertmanager, Grafana, ServiceNow ITSM, Veeam Backup, PostgreSQL, RAID/NAS

EXPERIENCE

Systems and Infrastructure Administrator **November 2025 – Present**
Meridia Softworks *Remote*

- Consolidated **20+ services onto a single server**, each isolated in its own container with CPU and memory limits and automatic restart, so one runaway service cannot drag down the rest
- Removed administrative access from the public internet entirely; the only remaining way in is an **encrypted tunnel terminated on the router itself**, and access attempts are blocked automatically
- Hold a **10-minute maximum recovery time for the production database**, verified every month by a full restore into an isolated environment against a documented procedure
- Cut **failure detection to under 60 seconds across 20+ services** and removed manual intervention from recovery by designing alerting with automatic service restart and escalation
- Codified the entire infrastructure so the environment **rebuilds from scratch in 15 minutes**, leaving no step that depends on undocumented knowledge or on a single machine
- Moved production to a dedicated server **with no interruption visible to clients**, rebuilding the new host from that codified definition and cutting over in one window

Systems and Network Administrator **August 2024 – October 2025**
PgO UCAM Group (Catholic University of Murcia) and Clínicas DEA *Almería, Spain*

- **Migrated 20 physical servers to 25 virtual machines** spread between the data center cluster and high-availability hosts at branch sites, so a failed host no longer stopped the service
- Segmented **150+ devices into 6 isolated zones**, joined across sites by encrypted tunnels, with endpoint protection on every workstation, placing two barriers between an infected computer and the clinical records
- Prepared the clinical-record backups for the **GDPR audit** with a documented procedure, restores verified on 30+ servers and immutable copies that ransomware cannot delete
- Built the monitoring for **10 clinics and 300 users**, taking outage detection from a user's call to an alert and a ticket in under 10 minutes, then resolved those incidents as L2–L3 with the IT team
- Reduced Microsoft 365 licensing spend by **more than €5,000 a year**, measuring what each seat actually used and downgrading or reclaiming plans left unused or orphaned for years

PROJECTS

High-availability Kubernetes cluster verified with four disaster drills | *Three-node cluster stood up from code and governed from Git, where killing a node does not cut service and total loss of the cluster rebuilds itself, data included, in under 10 minutes*

Network segmentation with firewall rules generated as code | *Six-VLAN network whose firewall rules are built from a single file, with automated tests that fail any change leaving an isolated segment exposed*

Windows Server 2025 domain hardened with the CIS Benchmark | *Full domain stood up and administered from the command line instead of the GUI, hardened to the controls audits demand rather than the shipped defaults*

Zabbix monitoring defined as code | *Complete Zabbix server that comes up with a single command, with hosts, triggers and alerts defined in files and applied through the API instead of the web interface*

Proxmox backup and restore verified against a deliberate disaster | *Hypervisor and its VMs managed end to end with Ansible, scheduled backups with retention, and a script that destroys a VM and verifies the restore returns its IP, data and service*

EDUCATION

Higher Technician in Network Systems Administration *(ASIR)* *IES Aguadulce, Almería*
Technician in Microcomputer Systems and Networks *(SMR)* *IES Puebla de Vícar, Almería*

CERTIFICATIONS AND LANGUAGES

Certifications: CCNA 200-301, Azure AZ-104, ITIL Foundation, Google Cybersecurity, CompTIA Security+ (expected 2026)
Languages: Spanish (native), English (B2, Cambridge certificate)