MOAMEN KHALED FAROUK ALI

System Administrator | IT Infrastructure, Networking & Security

Dammam, Saudi Arabia • +966 57 098 7230 • momen.farouk98@gmail.com

PROFESSIONAL SUMMARY

System Administrator with end-to-end ownership of enterprise IT for a multi-company holding group operating across ~20 sites in Saudi Arabia's Eastern Province. Hands-on across networking (HP/H3C Comware, Sophos XGS, Peplink SD-WAN), virtualization and storage (VMware ESXi, HP Nimble/MSA), Microsoft 365 and Entra ID, and security operations (SentinelOne EDR, Wazuh, NIST-aligned incident response). Pairs daily operations with solution architecture — tiered backup design, PAM and SIEM evaluations, remote access at scale — and compliance implementation, including Saudi Aramco's Cybersecurity Compliance Certificate (CCC / SACS-002).

CORE SKILLS

- **Networking:** HP/H3C Comware & HP ProCurve switching, IRF stacking, STP/loop protection, VLANs, PoE, IPsec VPN, Peplink SD-WAN, Tailscale
- **Voice & PBX:** Yeastar P-Series IP-PBX (P570) administration, SIP trunking, Yealink IP endpoints
- **Security:** Sophos XGS firewalls, SentinelOne EDR, Wazuh SIEM, PAM (Fudo / WALLIX evaluation), MFA & Conditional Access, FIDO2/passkeys, Saudi Aramco CCC (SACS-002) compliance, NIST-aligned incident reporting
- **Microsoft Cloud:** Microsoft 365, Exchange Online, Entra ID, Microsoft Graph (PowerShell and app-only API)
- **Virtualization & Storage:** VMware ESXi, HP Nimble, HP MSA, Synology (Active Backup for Business / M365), tiered backup architecture
- **Systems:** Windows Server & Active Directory, Linux (Ubuntu, RHEL family, SLES, Debian), macOS
- **Monitoring & Automation:** Zabbix, Bash, PowerShell, Python
- **ERP Systems:** General working knowledge of Odoo administration; SAP Basis exposure on Solaris/SPARC

PROFESSIONAL EXPERIENCE

System Administrator — Al Osais International Holding, Eastern Province, Saudi Arabia *Mar 2023 – Present*

Core member of the IT department for a multi-company group (contracting, transport, industrial) spanning ~20 sites.

- Administer a mixed enterprise estate end to end: Sophos XGS firewalls, HP/H3C Comware and ProCurve switching, VMware ESXi, Windows Server/Active Directory, Microsoft 365/Entra ID, SentinelOne EDR, Zabbix, Peplink SD-WAN, and HP Nimble/MSA storage.
- Designed a self-hosted RustDesk Server Pro remote-access platform for 400 managed devices — a DMZ-resident VM on ESXi behind Sophos XGS and Peplink SDX multi-WAN, with no cloud dependency; deployment in progress.
- Resolved high-impact network incidents, including an IRF split-brain on the server-farm switch stack causing core ARP flapping, and a multi-switch STP loop/broadcast storm; hardened the access layer with spanning tree and loop protection.
- Designed a tiered backup architecture: HP Nimble as hot VM tier, MSA as capacity/archive tier, and Synology RS1221RP+ as backup primary with Active Backup for Business and for Microsoft 365.
- Led security tooling evaluations — PAM (Fudo Enterprise vs WALLIX Bastion) with a POC plan covering switch SSH, firewall HTTPS session recording, and Windows RDP just-in-time access — and authored an on-premises Wazuh SIEM deployment plan.
- Implemented Saudi Aramco's Cybersecurity Compliance Certificate (CCC / SACS-002) requirements across the group's IT environment.
- Administer Microsoft Active Directory across the group — domain services, user and group lifecycle, OU structure, and Group Policy, including GPO-based software deployment at fleet scale.
- Administer the Microsoft 365 tenant: audited and consolidated MFA/Conditional Access policy, remediated FIDO2 passkey re-registration failures via Graph PowerShell, deployed tenant-wide GAL contact sync for iOS devices, and resolved sender-reputation/blocklist mail-flow incidents.
- Administer the corporate IP telephony platform — a Yeastar P570 PBX deployment with SIP trunking.
- Managed an EDR false-positive incident end to end, authoring a NIST-aligned incident report and executive summary.
- Executing a legacy SAP production-system rescue on Sun SPARC M3000/M5000 hardware through golden-image cloning and staged verification.

- Designed multi-site and edge infrastructure: network architecture for a 20-site CCTV rollout (structured /16 addressing, Tailscale subnet routers vs IPsec analysis) and a relocatable solar-powered CCTV pole (48V DC, 800Wp PV, LiFePO4) with a complete engineering document set.
- Automated monitoring rollout with a ~1,200-line universal Zabbix agent installer (RHEL/Alma/Rocky, SLES, Debian/Ubuntu; 20 add-ons; four CLI modes) plus a GPO-based Wazuh agent deployment for AD environments.
- Driving digitization of HR approval workflows with DGA-licensed electronic-signature providers; handle vendor management and procurement across networking, storage, and security.

CERTIFICATIONS

- Sophos Firewall — Certified Administrator

EDUCATION

- Bachelor of Computer Science (Networking specialization) — Asia Pacific University (APU), Malaysia, 2022

LANGUAGES

- Arabic — Native • English — Excellent