Open questions / unknowns

- Firewall hosts (internal-fw / external-fw) management access (SSH closed / filtered). Confirm intended admin access method.
- Wazuh-siem services appear similar to observer in Nmap output; confirm intended app layout / reverse proxy behavior.
- Some MACs not discoverable via ARP due to segmentation; relied on authoritative network diagram for interface MACs (expected).

Items to confirm with MegaQuagga IT

- Confirm whether `cloudshare` hosts are intentional routers/edge services across multiple subnets.
- Confirm whether endpoints sharing hostnames/IP aliases in CMDB matches desired naming convention.

Security findings / insecure implementations

- Multiple endpoints expose SMB/RPC/NetBIOS (135/139/445) — restrict via host firewall if not needed.
- RDP exposed on endpoints/servers (3389) — enforce NLA + allow-list + MFA/jump host.
- SSH exposed on servers (22) — allow-list management subnets, disable password auth if possible.
- Web apps exposed (iTop/Nagios/Grafana/Prometheus/Wazuh) — confirm TLS and restrict admin access.