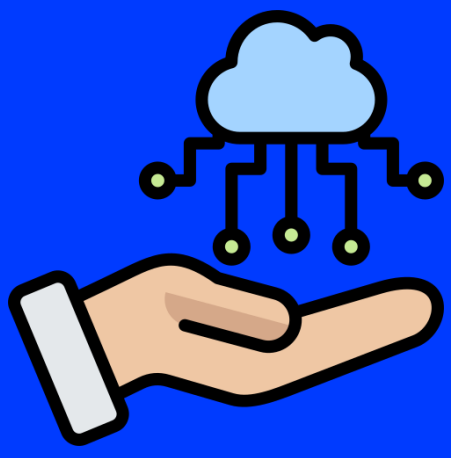
{EPITECH}

CIA_

< DEPLOYMENT AND SECURING OF A HYBRID INFRASTRUCTURE WITH PROXMOX />



CIA

As a member of the team *Cloud Infrastructure Architects*, a client asks you to **design, deploy, and secure a hybrid infrastructure** composed of two Proxmox sites (on-prem and remote) and a core set of services (VPN, firewall, IPAM, observability), with a **scalable approach** in order to add more sites over time.

Goals

Your main objectives are:

- ✓ Deploy a hybrid infrastructure: **Proxmox Site 1** + **Proxmox Site 2**;
- ✓ Set up a **secure site-to-site interconnection** via a **VPN**;
- ✓ Add **firewalls** on both sides, with an **emergency cut-off capability**;
- ✓ Set up a **bastion host** for external access to the remote site;
- ✓ Automate **IP management** via an IPAM (NetBox) and keep the IPAM **up to date**;
- ✓ Centralize logs and implement observability (Elastic / Elasticsearch);
- ✓ Publish a **website accessible only from the internal network**;
- ✓ Establish an architectural baseline that allows **integration of additional sites** later on.

Survival tips:

- ✓ Think **traffic separation** (admin / users / services) and **least privilege**.
- ✓ Prepare an **emergency cut-off** (kill switch) strategy that does not prevent recovery.
- ✓ Document **how to rebuild** (automation + procedures), not just **what was done**.

You are expected to deliver:

- ✓ A functional infrastructure that meets the client's needs (connectivity, security, access, monitoring);
- ✓ A project-oriented approach (planning, tickets, risk/blocker tracking);
- ✓ As many resources as possible deployed **as IaC** (Infrastructure as Code);
- ✓ Clear, usable, and reproducible documentation, including runbooks and diagram(s).

Core Stack Technologies

- ✓ Private Cloud:
  Proxmox VE is a **bare-metal** virtualization solution (ISO-based installation) used here to host the VMs for each site.
- ✓ VPN:
  OpenVPN enables the creation of an **encrypted VPN** between sites (site-to-site) to secure interconnection and remote access.
- ✓ IPAM:
  NetBox acts as the network **source of truth** (IPAM/DCIM), with an API, to document and automate the management of IP addresses, prefixes, and devices.
- ✓ Observability:
  Elasticsearch is used to **centralize**, **search**, and **analyze** logs (and potentially metrics) for monitoring and investigation purposes.
- ✓ Firewall:
  pfSense (FreeBSD-based) is used as a **router/firewall** to filter traffic and reduce exposure.

Expectations and constraints

The client expects:

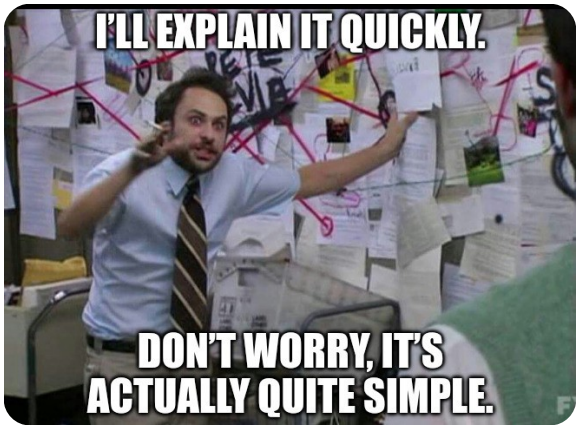
- ✓ 1 on-prem site + 1 remote site;
- ✓ Site-to-site VPN interconnection;
- ✓ Firewalls on both sides to limit exposure;
- ✓ Emergency disconnection capability;
- ✓ Automatically updated IPAM;
- ✓ External access to the remote site via a bastion host;
- ✓ Monitoring of the overall infrastructure;
- ✓ DNS forwarding between the two sites;
- ✓ A scalable architecture designed to support the future integration of additional sites.

The following technical constraints are non-negotiable:

- ✓ 3 VMs maximum per Proxmox Site.
- ✓ The stacks used must be actively supported, maintained and updated by the community.

Your infrastructure diagram must at minimum show:

- ✓ The two sites (S1 / S2) and their networks (LAN / DMZ / Admin if segmented);
- ✓ The VPN (termination points, routed subnets, encryption);
- ✓ Control points (firewalls, key rules);
- ✓ The bastion host (allowed flows, authentication, logging);
- ✓ NetBox + Elasticsearch (where they run, who can access them, which flows);
- ✓ DNS forwarding (who forwards to whom, zones, resolution).



Deliverables

Follow-up 1 — Scoping

- ✓ Initial technology exploration.
- ✓ Reporting of technical blockers encountered.
- ✓ Setup of *GitOps* repositories (give the appropriate permissions to your instructors/mentors).
- ✓ Gantt chart of project phases.
- ✓ Task breakdown into tickets (backlog).
- ✓ List of tickets to be completed for the next follow-up.
- ✓ Infrastructure diagram to be validated.

Follow-up 2 — First Building Blocks

- ✓ First infrastructure components in place.
- ✓ Updated Gantt / ticketing.
- ✓ Reporting of technical blockers encountered.
- ✓ List of tickets to be completed for the next follow-up.

Follow-up 3 — Beta

- ✓ Infrastructure + application stack in beta version.
- ✓ Updated Gantt / ticketing.
- ✓ List of final technology choices.
- ✓ Reporting of technical blockers encountered.

Keynote — Final Delivery

- ✓ Detailed technical document (with screenshots).
- ✓ Source-controlled code: network configurations + logs.
- ✓ Secure credential store (e.g. vault / password manager / encryption).
- ✓ Final infrastructure diagram.
- ✓ Disaster recovery documentation (DRP / runbook).

We will evaluate:

- ✓ the functionality and robustness of the infrastructure.
- ✓ your code quality and readability.
- ✓ the security and effectiveness of firewall configurations.
- ✓ the relevance of analyses performed via Elasticsearch.
- ✓ the justification of your technical choices.

Bonus

- ✓ CI/CD integration (IaC linting, tests, deployments).
- ✓ ”Golden paths”: reusable templates (VMs, rules, IPAM, logs).
- ✓ Advanced monitoring (dashboards, alerting, log parsing).
- ✓ Multi-site readiness: addressing conventions + onboarding of a third site.

v1