SIRIUS FG LAB · CLOUD ENGINEERING

Azure Lab — Project Overview

DISPOSABLE · PRIVATE-BY-DEFAULT · DESTROY-TO-ZERO

The `lab.nagini.io` cloud version — re-platforming the tested Docker estate onto isolated Azure IaaS.

Timeline — 50 hours over ~3 months (~3.8 h/week)

PHASE	FOCUS	HOURS
P0	Foundation — CLI, RG, guardrails	10
P1	Network + Bastion → Isolation Gate	10
P2	Estate VM, Docker, validate attacks	14
P3	Deployment stack, lifecycle → Cost Gate	6
P4	Optional — go native, demo button, steps 5–7	10
Core (P0–P3)		**40**

INDEPENDENT LINE ITEM

+12 h optional **Department Tier** (HR/IT/Finance) — runs independent of the core timeline.

EFFORT DISTRIBUTION



TWO GATES

Isolation Gate (no public IPs but Bastion) and **Cost Gate** (teardown verified to $0) are hard stops between phases.

Materials & services

Compute

One x64 D-series VM (`Standard_D2s_v4`) hosting the whole Docker estate; Windows D-series for the department tier.

Network

VNet 10.30.0.0/16, `snet-lab` /24, deny-by-default NSG — mirrors the local lab exactly.

Entry point

Azure Bastion (managed) — the single audited ingress. WireGuard / AVD are open alternatives.

IaC & lifecycle

Bicep + deployment stacks; one-command `deleteAll` teardown, no state file.

Governance

Dedicated subscription/RG; optional Defender for Servers; budget alerts.

Identity & secrets

Two-tier: human vault (Bitwarden/1Password) + Azure Key Vault for automation.

Observability

Launcher mission console + raw `az` log; portal resource-group view.

Estate payload

dc01/dc02/ca01/sql01/vault01/gateway — the validated vulnerable AD estate.

Accounts & access — before Phase 0

1. An Azure subscription with rights to create resources (dedicated strongly preferred).
2. Azure CLI (`az`) installed — on Kali, via `pipx`.
3. Bicep CLI (`az bicep install`).
4. The `bastion` and `ssh` CLI extensions.
5. An SSH keypair for the estate VM (`--generate-ssh-keys` will make one).
6. For the department tier: a public HTTPS host for the two provisioning scripts.

GUARDRAIL

No lab VM ever gets a public IP. Bastion is the single exception, and it's audited. A vulnerable DC on a public IP is a gift to scanners.

BLAST RADIUS

A dedicated subscription or resource group makes both the security boundary and the cost boundary unambiguous — and teardown absolute.

Skills developed

Cloud & IaC

Azure CLI, Bicep modules, deployment stacks, cloud-init, resource lifecycle. `applied`

Networking

VNet/subnet design, NSG rules, Bastion, private-only access, tunneling. `applied`

Identity & security

AD/Kerberos, ADCS, Kerberoast/AS-REP, ESC1 — plus AD **trusts & child domains**, cross-domain ACLs & **Universal groups**. `mastered`

Ops & cost

Disposable-estate cost modelling, "destroy don't stop," two-tier secrets, GUI automation. `learned`

Named tooling across phases: `az`, Bicep, Bastion, Docker Compose, Impacket, certipy, BloodHound, HashiCorp Vault, PowerShell AD DS.

Setup flow — operator · IaC · Azure



THE UP/DOWN LOOP

The launcher automates both directions: Build runs the seven phases; Tear Down deletes the stack and, on any failure, falls back to a resource-group delete that always returns to $0.

Department Tier — topology (optional, 7 VMs)

dc01 · SIRIUSFG.LOCAL
FOREST ROOT

dc-hr · HR-Share	dc-it · IT-Share	dc-fin · Finance-Share
HR.SIRIUSFG.LOCAL · .20	IT.SIRIUSFG.LOCAL · .30	FIN.SIRIUSFG.LOCAL · .50
cl-hr-01 · .22	cl-it-01 · .32	cl-fin-01 .52 · cl-fin-02 .53

CROSS-DOMAIN GRANT

`IT-Support` (IT domain, **Universal** scope) → Full Control on HR-Share and Finance-Share. Two-way transitive trust with the forest root is automatic. Each child DC also hosts its share — 7 VMs, not 10.

Cost posture & the rule

$0 when torn down

RUNNING COST	~$/HR
Bastion Standard (dominant)	0.29
Estate VM (D2s_v4, Linux)	0.10
Public IP	0.005
Core estate	**~0.40**
+ Department tier (7 Windows VMs)	~1.4

DESTROY, DON'T STOP

A deallocated VM still bills for its disks; a destroyed resource group bills nothing. "Stop" is not a cost control — teardown is.

DONE = $0

Teardown is complete only when `az group exists` prints `false` (cost dashboard lags ~24h).

Open decisions: entry point (Bastion vs WireGuard vs AVD) · AD fidelity (sim vs native) · region. Deferred: Azure Key Vault integration for the department admin password.