SIRIUS FG LAB · CLOUD ENGINEERING

Department Expansion Build Guide

HR · IT · FINANCE CHILD DOMAINS
COST-EFFICIENT 7-VM TIER

siriusfg.local forest · Azure IaaS
Companion to the Nagini Suite live demo
Authorized training use only · v1 · 2026-10-01

Department Expansion — cost-efficient build

This guide adds three department child domains — **HR, IT, and Finance** — to the existing `SIRIUSFG.LOCAL` forest as a seven-VM expansion of the Azure lab. Each department gets its own domain controller (which also hosts that department's file share) plus one or more domain-joined client workstations. It builds on the core estate and tears down with it.

WHAT YOU'LL STAND UP

3 child-domain DCs + 4 domain-joined clients = 7 VMs, each reachable only inside the VNet via Bastion, all in `rg-siriusfg-lab` so a single deployment-stack (or resource-group) teardown removes the lot.

1 · The estate at a glance

VM	IP	DOMAIN	ROLE
`dc-hr`	10.30.1.20	hr.siriusfg.local	Child DC + `\\dc-hr\HR-Share`
`dc-it`	10.30.1.30	it.siriusfg.local	Child DC + `\\dc-it\IT-Share`
`dc-fin`	10.30.1.50	fin.siriusfg.local	Child DC + `\\dc-fin\Finance-Share`
`cl-hr-01`	10.30.1.22	hr	Domain-joined Win11 client
`cl-it-01`	10.30.1.32	it	Domain-joined Win11 client
`cl-fin-01`	10.30.1.52	fin	Domain-joined Win11 client
`cl-fin-02`	10.30.1.53	fin	Domain-joined Win11 client

2 · Cost decisions baked in

- **File servers collapsed onto the DCs** — the share lives on the DC VM itself. Saves three whole VMs versus a dedicated file-server per department.
- **Plain domain-joined Windows clients, not AVD** — reproduces every attack path (Kerberos, mapped drives, lateral movement) with no AVD host-pool cost and no per-user licensing. Saves the entire AVD management layer.
- **Burstable intent, D-series in practice** — the design targets idle-cheap burstable sizes; the shipped Bicep uses `Standard_D2s_v4` because the B-series was NotAvailableForSubscription in eastus at build time.
- **Everything in `rg-siriusfg-lab`** — it joins the existing deployment stack, so it tears down to `$0` with the rest of the estate.

COST REALITY

These are seven **Windows** VMs (each carrying a Windows license on top of compute), roughly `~$1.4/hr` all-in on top of the core estate. Treat this tier as a look-and-destroy: build it, explore, tear it down within an hour or two. OS disks keep billing even when a VM is deallocated — **only destroy stops the meter.**

3 · Prerequisites

1. The base Azure lab already deployed — VNet `vnet-siriusfg-lab`, subnet `snet-lab`, forest root `dc01` at 10.30.1.10.
2. The two PowerShell scripts hosted at a URL the VMs can reach over HTTPS (a public raw GitHub path or an Azure Storage blob). They must be named exactly `Promote-ChildDomain.ps1` and `Join-Client.ps1`.
3. The forest-root **Administrator** password — creating a child domain requires Enterprise Admin rights of the forest root.

WHY THE SCRIPTS MUST BE HOSTED PUBLICLY

Each VM runs an Azure custom script extension at first boot that **fetches the two `.ps1` files by URL and runs them**. Azure cannot read files on your workstation, so the scripts have to be reachable anonymously over HTTPS before the VMs boot. They take every password as a runtime parameter — nothing secret is hardcoded — so they are safe to host publicly.

4 · Deploy

```
az deployment group create \
  --resource-group rg-siriusfg-lab \
  --template-file bicep/main-departments.bicep \
  --parameters \
      adminPassword='<local-admin+DSRM+join password>' \
      rootAdminPassword='<SIRIUSFG.LOCAL Administrator password>' \
      scriptBaseUri='https://<your-host>/path-to-scripts'
```

The single template provisions all seven VMs. **IT deploys first** (enforced with Bicep `dependsOn`) because its `IT-Support` group is referenced in the HR and Finance share ACLs — the group has to exist before those ACEs can resolve.

What each VM does on boot (two passes)

KEY CONCEPT — THE REBOOT TWO-STEP

Promoting a server to a domain controller, and joining a client to a domain, each **reboot the VM**. So both scripts are written to run **twice**: pass 1 does the privileged change and

reboots; pass 2 detects "already done" and finishes the follow-up work (share creation / drive mapping). Allow ~15–25 min for the whole estate to settle.

- **DCs** — install AD DS → promote to a child domain (single-label name, e.g. `hr`, under `SIRIUSFG.LOCAL`) → reboot → second pass creates the SMB share + NTFS ACLs, including the cross-domain `IT-Support` grant on HR/Finance.
- **Clients** — join their child domain → reboot → second pass registers a logon task that maps `Z:` to the department share.

5 · The file-share access model

Access is by **AD security group**, never by individual user:

SHARE	READ/WRITE	FULL CONTROL	NOTES
HR-Share	`HR-Users` (hr)	`IT-Support` (it)	Cross-domain support grant
IT-Share	`IT-Users` (it)	Administrators	`Tools\` subfolder forest-wide read-only
Finance-Share	`Finance-Users` (fin)	`IT-Support` (it)	Most sensitive data domain

KEY CONCEPT — UNIVERSAL GROUP SCOPE

`IT-Support` is created as a **Universal** group in the IT domain. Universal scope is what lets it be referenced in ACLs in the HR and Finance domains across the forest trust — a domain-local or global group could not span domains this way. The IT `Tools\` folder is granted to `Authenticated Users`, which spans the whole forest via the trusts, as read-only.

6 · Verify the trusts

Trust verification runs inside the domain (from `dc01`, over Bastion), not from the Azure control plane — so it's a manual check. From `dc01`:

```
Get-ADForest | Select-Object -ExpandProperty Domains
Get-ADTrust -Filter * | Format-Table Name,Direction,TrustType
```

CHECKPOINT

Expect `hr`, `it`, `fin` listed as domains; each trust Direction = **BiDirectional**. Two-way transitive trust with the forest root is automatic for child domains — no manual trust config needed.

7 · Teardown

If `main-departments.bicep` is wired into your top-level `main.bicep` as a module, the existing **Tear Down** removes the whole department tier with everything else via the deployment stack. Even

if it isn't, the launcher's teardown falls back to a resource-group delete, which clears all seven VMs and their disks regardless:

```
az group delete --name rg-siriusfg-lab --yes
az group exists --name rg-siriusfg-lab   # expect: false
```

8 · Security / lab honesty

- No public IPs on any of these VMs — reachable only inside the VNet via Bastion, same as the rest of the lab.
- The whole tier uses **one shared password** for local admin, DSRM, and domain join. That is a deliberate lab simplification and is itself a planted weakness — never do this in anything real.
- This build is **clean/realistic** as written. The vuln hooks (cross-domain escalation, Kerberoast across trusts, over-permissioned `IT-Support`, delegation abuse) are latent, left as exercises.

9 · File manifest

```
dept-expansion/
  bicep/
    main-departments.bicep   # orchestrator (deploy this)
    department-dc.bicep       # one child DC + share
    client-vm.bicep           # one domain-joined client
  scripts/
    Promote-ChildDomain.ps1   # AD DS install + child promo + share/ACLs
    Join-Client.ps1           # domain join + Z: drive map
  README.md
```

Source of truth: github.com/nagini-x/siriusfg-lab → `azure-launcher/dept-expansion/`. Deploy order and the IT-first dependency are enforced inside `main-departments.bicep`.