slaptain

A Kubernetes operator for multi-site, multi-master OpenLDAP

Dominik Epple · LDAPCon

slaptain.chuck-chuck-chuck.net · Apache-2.0

For starters: Two questions

Hands up:

1. Who runs OpenLDAP *somewhere* — production, lab, dev box, teaching system?

2. Keep it up if your favourite way of running OpenLDAP is on Kubernetes.

The gap between the first hand and the second is this talk.

Agenda

1. Motivation: The case for Kubernetes
2. What it wants to do, and where it stands
3. One site, then three
4. Backup, restore
5. Why an operator
6. How this got written

About me

Dominik Epple

DAY JOB

Principal Architect at Open-Xchange

Kubernetes-first, all in: our own components, and the entire stack (yes, this includes OpenLDAP)

Author of the OX App Suite Operation Guides[1]

1 — documentation.open-xchange.com/appsuite/operation-guides/

About me

Dominik Epple

SPARE TIME

New hobby: Creating missing Kubernetes operators.

slaptain is one of them.[1]

Today I am here as this one.

1 — github.com/chuck-chuck-chuck-net/littlered for Redis is the other one

Behind the name

`slapd`

n. stand-alone LDAP daemon

"It listens for LDAP connections on any number of ports (default 389), responding to the LDAP operations it receives over these connections."

— `slapd(8)`

A Kubernetes operator's job is to steer, automate and manage the lifecycle of a workload.

Making it the captain of `slapd` is a perfect conceptual fit.

`slaptain = slapd + captain`

And `chuck-chuck-chuck.net`? That is the little red hen, who said it a lot — github.com/chuck-chuck-chuck-net/littlered#behind-the-name

Motivation

Why you want this. Even if you do not know it yet.

It works.

A container is process isolation — same kernel, same syscalls

Persistence is the part Kubernetes already solved

> Postgres, Cassandra, Kafka run this way. This is not new ground.

It works **very well.**

Compute, storage, network, secrets — declared, and kept that way

Upgrading is a new image tag. Rolling back is the old one.

The same files run in a lab, in a cloud, or for one test run

Profit!

"Do you run on Kubernetes?" is now a procurement question

The directory stops being the exception with its own tooling

> The last workload on VMs does not cost you a VM.
> It costs you everything it takes to keep running VMs.

And my personal motivation?

Learn agentic coding. That was the actual starting point.

On something real. A gap that was blocking my day job.

In spare time, on purpose. So it belongs to everyone rather than to one vendor.

And to give something back. I have been taking from open source for decades.

> Which is why replication, migration and multi-site were in scope from day one.
> The success criterion was never a nice demo. It was my reality at work.

Requirements

Goals. What we set out to achieve.

`slaptain` requirements

THE PLATFORM

Make OpenLDAP meet the expectations people have of a cloud-native, Kubernetes-first application — which, by itself, it does not.

Declarative end to end. Fully gitops-able.

THE DIRECTORY

Production-grade OpenLDAP out of the box.

N-way multi-master delta-syncrepl, plus read-only consumers.

Multi-site and multi-cluster, with whichever cross-site transport that needs.

THE LIFECYCLE

Migration of existing deployments — syncrepl, delta-syncrepl, hot and cold.

Backup, restore, disaster recovery.

THE QUALITY BAR

First-class security by default — where it does not cost functionality.

Tooling worth having: deployment, observability, debugging, bug reports.

Requirements, and where we stand

- ☑ Declarative end-to-end, gitops all the way
- ☑ N-way multi-master delta-syncrepl, plus consumers
- ☑ Multi-site, cluster per site, cross-site transports
- ☑ Migration of existing deployments, hot and cold
- ☐ Production-grade OpenLDAP out of the box
- ☑ Backup, restore, disaster recovery — to S3
- ☑ Databases, schemas, ACLs as custom resources
- ☑ Security defaults that do not cost functionality
- ☑ Tooling: `slctl`, conditions, e2e across three sites

That last one is not mine to tick.

What it does not have

WHAT I DO TRUST

The legwork. The container image, the operator code, the data model of the CRDs, and an e2e suite that stands up three sites and tears them down again.

Putting things on Kubernetes has been my day job for years — our own components, and the whole stack around them. This is the half I am confident about.

WHAT IS MISSING

- OpenLDAP subject-matter review — `cn=config`, ACLs, replication design
- production exposure — it has run in a lab, and nowhere else
- a release — the tag is easy; freezing the CRD API is not
- more hands and brains — sparring, a second point of view, continuity beyond one person

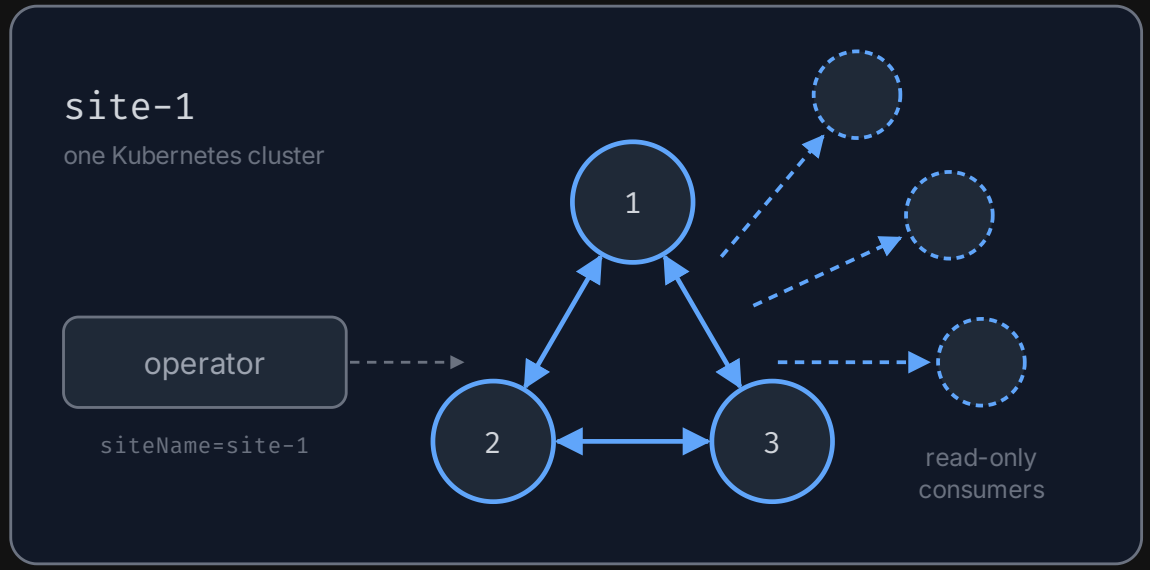
That gap is not code. It is review, confirmation and hands — which is what this room has.

First, one site

What it is, what you write, and how you check it worked.

One site

Three slapd pods, all read-write, all equal. One operator, and nothing else in the picture.



Every pod replicates from every other — N-way multi-master, no primary. Their `olcServerID`s are **1, 2, 3**: derived from the pod's ordinal, never configured by hand.

The dashed ones are **consumers**: they pull from the mesh and take reads. Nothing replicates from them, and they have no `olcServerID` at all.

Installing the operator

```
% helm install -n slaptain-system slaptain \
> oci://ghcr.io/chuck-chuck-chuck-net/charts/slaptain
```

Seven new kinds

The API server can now store, validate and serve `SlapdMesh`, `SlapdCluster`, `SlapdDatabase` and `SlapdSchema` — plus three more for backup and restore.

Until now it knew generic terms for compute, storage, network. Now it has words for a *directory* too.

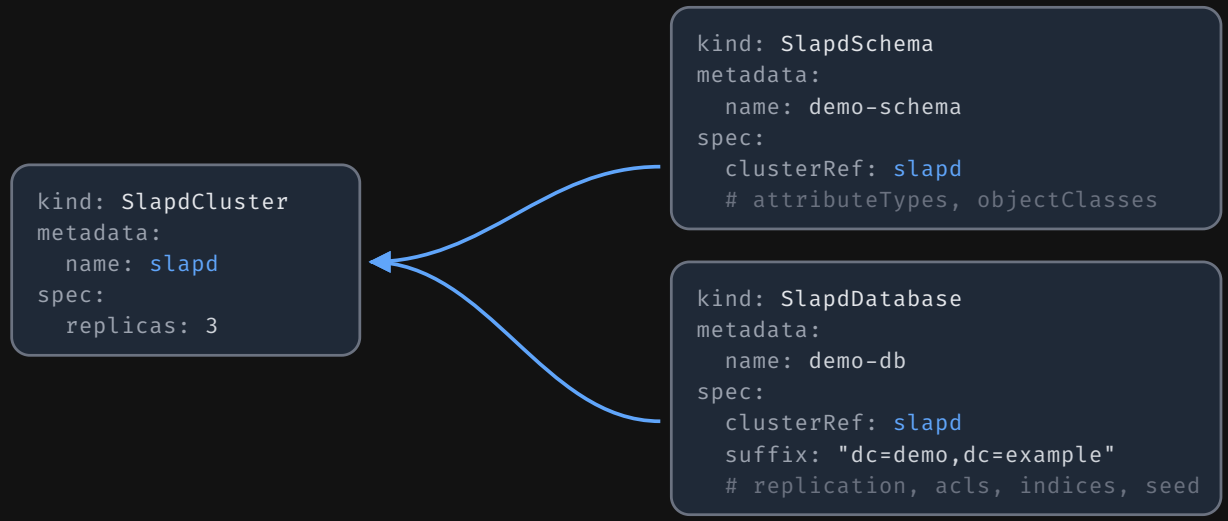
One pod

The controller. It watches those kinds and does nothing whatsoever until one of them appears.

Everything for the rest of this talk is its reaction to an object somebody applied.

`kubectl apply` gives you a noun and a verb. Everything between that and a running, correctly configured, replicating directory is knowledge — and it lives in that pod.

`slaptain` Custom Resources



The cluster carries the running things

pods, volumes, services, TLS, how many replicas and how many consumers. Nothing about what is *in* the directory.

The database and the schema carry the directory

a suffix, its ACLs, its indices, its replication — and schema separately, because schema outlives any one database.

One cluster can hold several databases. That is why they are separate objects and not fields on one.

How boring can a cluster be?

Replicas, TLS, replication on — and defaults for the rest. Nothing here carries meaning: the suffix, the ACLs, the indices, the schema all live in the other objects.

```yaml
# slapdcluster.yaml
apiVersion: ldap.chuck-chuck-chuck.net/v1alpha1
kind: SlapdCluster
metadata:
  name: slapd
  namespace: slaptain
spec:
  ldap:
    tls:
      enabled: true
      secretName: slapd-tls
  replicas: 3
  readReplicas: 1
  replication:
    enabled: true
```

```
% kubectl apply -f slapdcluster.yaml
```

What that produces

Two StatefulSets — `slapd` 3/3 and `slapd-readonly` 1/1.

Volumes per pod — read-write: `config`, `data`, `accesslog`. Read-only: `config`, `data`.

Four Services — `slapd` and `slapd-readonly` for clients, a headless pair for the pods themselves.

The Services answer on `389` and `636`. The pods listen unprivileged on `1024` and `1025` — clients never find out.

And now the considerably less boring part

```
# kubectl apply -f slapdschema.yaml
kind: SlapdSchema
metadata:
  name: demo-schema
spec:
  clusterRef: slapd
  priority: 100
  attributeTypes:
    - >-
      ( 1.3.6.1.4.1.99999.1.1.3
        NAME 'demoQuota'
        EQUALITY integerMatch
        SYNTAX 1.3.6.1.4.1.1466.115.121.1.27
        SINGLE-VALUE )
  objectClasses:
    - >-
      ( 1.3.6.1.4.1.99999.1.2.1
        NAME 'demoUser'
        SUP inetOrgPerson STRUCTURAL
        MAY ( demoContextId $ demoQuota ) )
```

```
# kubectl apply -f slapddatabase.yaml
kind: SlapdDatabase
metadata:
  name: demo-db
spec:
  clusterRef: slapd
  suffix: "dc=demo,dc=example"
  acls:
    - >-
      to attrs=userPassword
      by self write
      by anonymous auth
      by * none                  # …and two more
  indices:
    - "objectClass eq"           # …and four more
  replication:
    ridBase: 100
    deltaSync: true
  seed:
    entries:                     # …and four more
      - |
        dn: dc=demo,dc=example
        objectClass: organization
  cleanupPolicy: Retain
```

What differs between the pods

```
slctl ldapsearch --as config --pod slapd-N -- -b cn=config '(|(olcServerID=*)(olcSyncrepl=*))'
```

slapd-0

```
dn: cn=config
olcServerID: 1

dn: olcDatabase={2}mdb,cn=config
olcSyncrepl: {0}rid=102
  provider=ldaps://slapd-1…
olcSyncrepl: {1}rid=103
  provider=ldaps://slapd-2…
```

slapd-1

```
dn: cn=config
olcServerID: 2

dn: olcDatabase={2}mdb,cn=config
olcSyncrepl: {0}rid=101
  provider=ldaps://slapd-0…
olcSyncrepl: {1}rid=103
  provider=ldaps://slapd-2…
```

slapd-2

```
dn: cn=config
olcServerID: 3

dn: olcDatabase={2}mdb,cn=config
olcSyncrepl: {0}rid=101
  provider=ldaps://slapd-0…
olcSyncrepl: {1}rid=102
  provider=ldaps://slapd-1…
```

Same image, same chart, same CRs.
Two facts differ per pod — and the operator derived both.

Everything else in every stanza is identical: `searchbase`, `syncdata=accesslog`, `logbase`, `logfilter`, TLS, `retry`. `rid` = `ridBase` + peer ordinal + 1, so a stanza names the peer it points at — and no pod carries one for itself.

Is it actually replicating?

`ldapsearch -b dc=demo,dc=example -s base contextCSN` — anonymous, on every pod.

Before — all four pods

```
contextCSN: 2026…173503.489521Z#000000#001#000000
```

After — all four pods

```
contextCSN: 2026…173503.489521Z#000000#001#000000
contextCSN: 2026…180925.496164Z#000000#003#000000
```

In between, one write — `uid=alice,ou=People,dc=demo,dc=example`, added on *one* pod and read back from another.

`contextCSN` is a vector: one value per server that has ever written.

`#001#` is the founder's seed. `#003#` is slapd-2 taking Alice — the same `sid` as its `olcServerID`. Four pods, one vector, including the read-only replica.

Then, the mesh

The same three questions, at three sites.

First things first: a site identity

Going multi-cluster, every site — or rather, every site's *operator* — has to be told which site it is on.

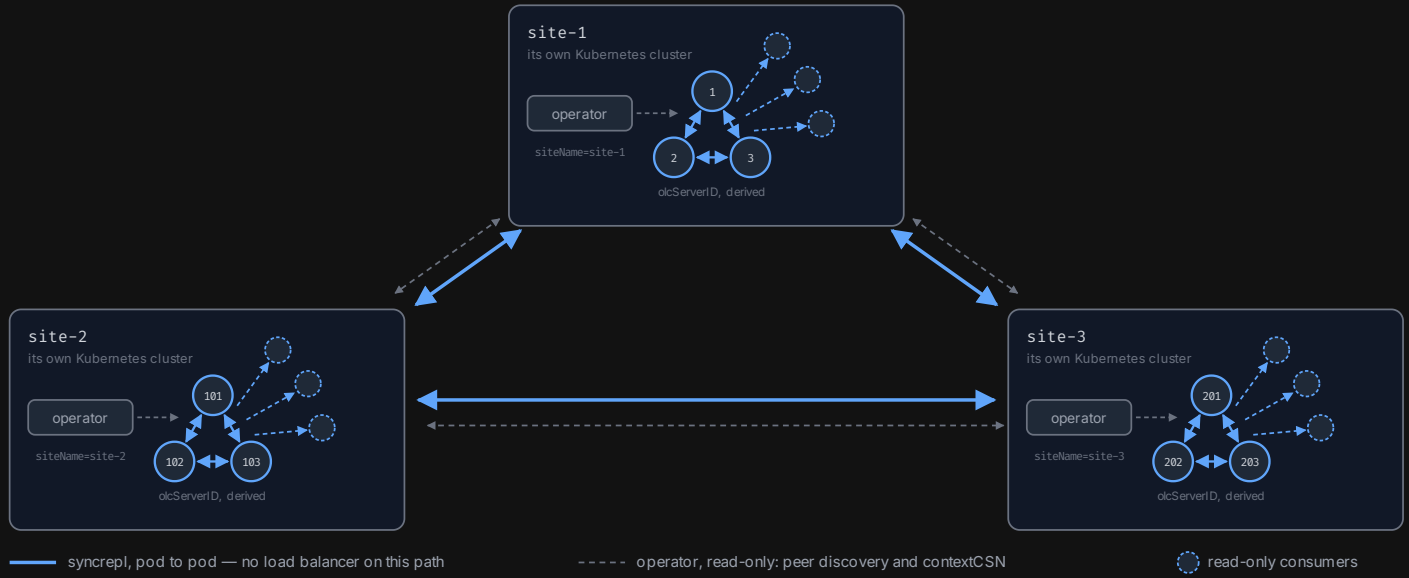
```
% helm install -n slaptain-system slaptain \
> oci://ghcr.io/chuck-chuck-chuck-net/charts/slaptain \
> --set siteName=site-2
```

Exactly what it needs that for comes later in this section. For now it is enough to picture the alternative: an operator asked to orchestrate a mesh, with no idea which of the sites in that mesh is the one it is standing in.

One flag, at install time, outside every custom resource. Everything else the site needs, it derives.

Three sites, all of them peers

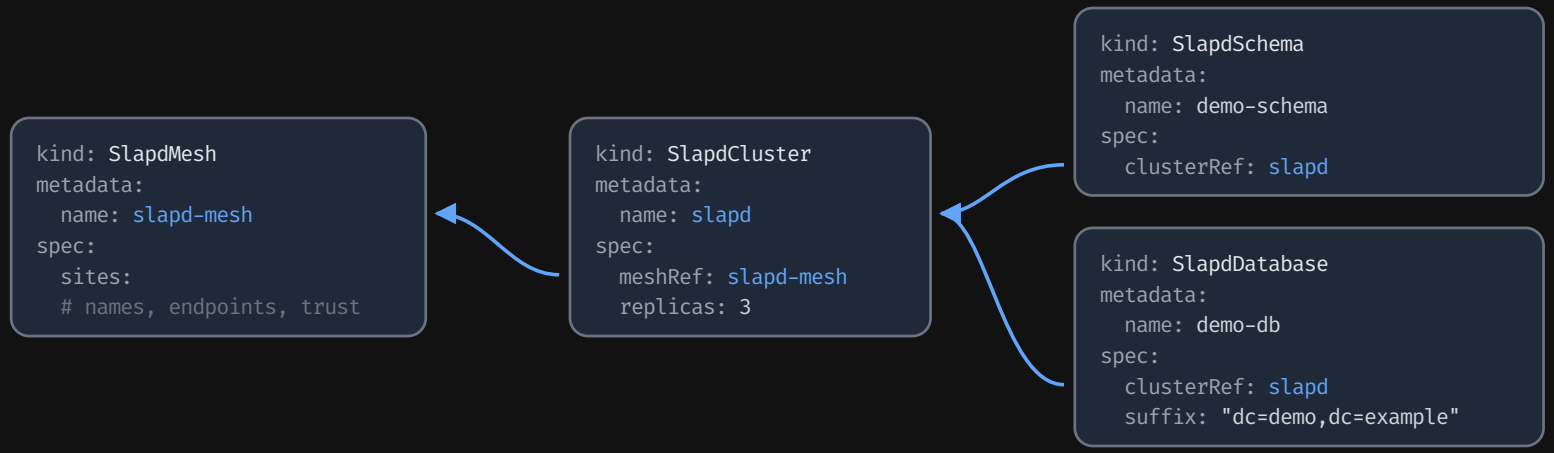
No hub, no meta-cluster, no shared control plane. Three Kubernetes clusters, each with its own operator, each of which keeps working while the other two are unreachable.



An operator only ever **reads** across sites — peer discovery from the remote API server, `contextCSN` from the remote pods. It writes configuration to its own pods and nowhere else.

No primary, no leader election. Every pod shown is an equal read-write peer, and `olcServerID` is derived from `siteName` — never configured.

A fourth kind: `SlapdMesh`



What the mesh carries

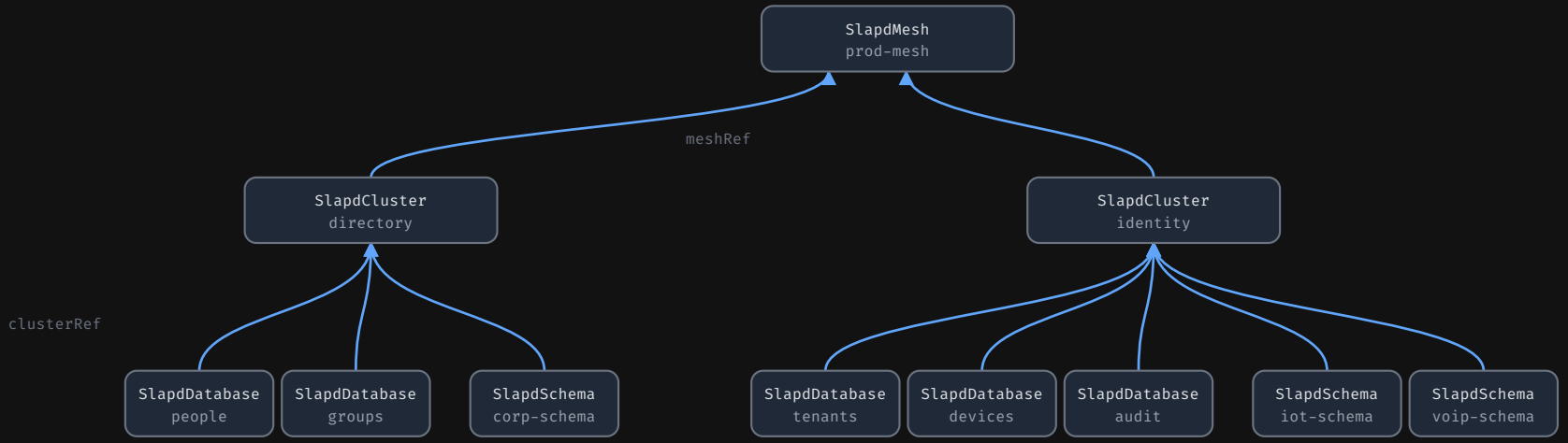
The sites, and the fabric between them: names, endpoints, network mode, trust. Nothing else.

Why the mesh is its own object

The site and topology facts that every cluster would otherwise repeat, written once and shared. On its own it reconciles nothing — it waits, inert, until a cluster references it.

It composes

One mesh. Two LDAP clusters that share its sites. Eight more objects.



The mesh is written once. Both clusters point at it, and neither one owns it.

No fact is written twice. Each one has a single authoritative home and everything else points at it — nothing to keep in sync, nothing that can drift.

All about topology

```yaml
apiVersion: ldap.chuck-chuck-chuck.net/v1alpha1
kind: SlapdMesh
metadata:
  name: slapd-mesh
  namespace: slaptain
spec:
  network:
    mode: pod-routed
    useForInCluster: false
  sites:
  - endpoint: https://10.2.1.10:6443
    name: site-1
    serverIDIndex: 0
  - endpoint: https://10.2.2.10:6443
    name: site-2
    serverIDIndex: 1
  - endpoint: https://10.2.3.10:6443
    name: site-3
    serverIDIndex: 2
```

Each site's slapd pods count from `serverIDIndex × 100 + 1` upwards:

`site-1: 1, 2, …`
`site-2: 101, 102, …`

Stable `olcServerID`s — the `sid` in every CSN — need stable `serverIDIndex` fields.

So they are explicit, not positional. Reordering or removing a `sites:` entry must never renumber a neighbour.

A `meshRef` makes it multi-site

Back to the `SlapdCluster` from the single-site section. It does not change — it gains one field.

One line added

```yaml
# slapdcluster.yaml — unchanged from earlier
kind: SlapdCluster
metadata:
  name: slapd
spec:
  meshRef: slapd-mesh      # ← that is all
  ldap:
    tls: { enabled: true, secretName: slapd-tls }
  replicas: 3
  readReplicas: 1
  replication:
    enabled: true
```

what it replaces — still available

```yaml
  replication:
    enabled: true
    serverIDBase: 200
    externalPeers:
      - name: site-1
        discovery:
          kubeconfigSecret:
            name: site-1-kubeconfig
      - name: site-2
        discovery: …
```

And the database's `rid`s follow from the same reference: a 100-wide band each — lower half for in-cluster providers, upper half for cross-site ones. Which is why the pods you saw earlier carry `rid=102` and `rid=103`.

`SlapdMesh` is autoconfiguration: one reference turns a single-site cluster into one site of a multi-site, N-way multi-master, delta-syncrepl directory.

The two objects, together

Both are applied at every site, byte-identical. Between them they define the whole mesh — and the operator derives the rest from `siteName`.

The mesh — who exists

```yaml
kind: SlapdMesh
spec:
  network:
    mode: pod-routed
  sites:
  - name: site-1
    endpoint: https://10.2.1.10:6443
    serverIDIndex: 0
  - name: site-2
    endpoint: https://10.2.2.10:6443
    serverIDIndex: 1
  - name: site-3
    endpoint: https://10.2.3.10:6443
    serverIDIndex: 2
```

The cluster — one line added

```yaml
kind: SlapdCluster
spec:
  meshRef: slapd-mesh
  replicas: 3
  readReplicas: 1
  replication:
    enabled: true
```

Neither object names *which* site it is on. That comes from the operator's own `--set siteName`, and it is the only per-site input anywhere.

find myself

`siteName` → my entry in `sites:` → my `serverIDIndex`

my identity

`index × 100 + ordinal + 1` → each pod's `olcServerID`

my peers

the same list minus me → the cross-site syncrepl stanzas

What every site applies

The same four objects, byte-identical at every site. None of them names a site.

SlapdMesh

The sites, the fabric between them, the trust. **The *only* object that knows a mesh exists at all.**

SlapdCluster

The single-site object, **plus one line.** Every tunable and sizing choice it carried, it keeps — and that one line is the *entire* replication topology.

SlapdSchema

Mesh-agnostic — byte-for-byte the object from the single-site section. It has no idea any of this is happening.

SlapdDatabase

Also mesh-agnostic, and also unchanged — suffix, ACLs, indices, seed, and its `ridBase`, still declared by hand.

> One site-specific input, and it is not in any of them: `siteName`, in the *operator's* own config. From it the operator filters itself out of the mesh's site list, takes its serverID decade, and builds its peer set.

No custom resource knows which site it is on.

A Helm chart ships them together, but that is packaging. The mechanism is the objects — and `ridBase` is a reminder that not everything is derived: it is declared, identical everywhere, and unique per database within a site.

The whole mesh, checked

One binary. Your laptop. No agent on the server, nothing installed next to slapd.

```
% slctl inspect -n slaptain slapd --short
```

```
[OK ] mesh-resolution            2 external peer(s) derived from SlapdMesh "slapd-mesh"
[OK ] csn-convergence            2 database(s): all 4 pods report identical contextCSN for each
[OK ] suffix-uuid-agreement      2 database suffix(es): all pods agree on the base entry's entryUUID
[OK ] accesslog-consistency      8 database/pod pair(s): logbase = olcAccessLogDB = log olcSuffix
[OK ] syncrepl-stanza-count      2 replicated database(s): RW 4 stanzas each, RO 3 each
[OK ] syncrepl-skip-self         no RW pod replicates from itself on any database
[OK ] rid-uniqueness             all RIDs unique within each pod, across its databases
[OK ] external-syncrepl          every replicated database on every RW pod has stanzas for all 2 external peers
[OK ] cross-site-csn             all external peers report Synced
… and nine more
```

18 passed, 0 warnings, 0 failed.

Three sites, two databases, four pods per site. In the replicated database the `contextCSN` carries three serverIDs, and they are hex — `#001#`, `#065#`, `#0c9#` — which is 1, 101 and 201: the `serverIDIndex × 100` decades, visible on the wire.

The same command, without `-short`

```
Pod: slapd-0 [Running, ready]
contextCSN (dc=example,dc=org):
  20260928164846.510135Z#000000#001#000000
  20260928164847.165922Z#000000#065#000000
  20260928164848.824633Z#000000#0c9#000000
syncRepl (dc=example,dc=org, in-cluster):
  {0}rid=102 provider=ldaps://slapd-1.slapd-headless…:1025 refreshAndPersist
  {1}rid=103 provider=ldaps://slapd-2.slapd-headless…:1025 refreshAndPersist
syncRepl (dc=example,dc=org, cross-site):
  [site-2] {2}rid=151 provider=ldaps://10.233.64.25:1025
  [site-3] {3}rid=152 provider=ldaps://10.233.128.101:1025
syncRepl (dc=second,dc=example,dc=net, in-cluster):
  {0}rid=202 … {1}rid=203
syncRepl (dc=second,dc=example,dc=net, cross-site):
  [site-2] {2}rid=251 … [site-3] {3}rid=252
… then slapd-1, slapd-2, slapd-readonly-0 — and the 18 checks across all of them
```

Two databases, two RID bands, and the operator kept them apart: `102–103` / `151–152` against `202–203` / `251–252`. Read out of a running server, not out of the spec that produced it.

Backup and restore

A directory is only as good as the copy you can put back.

How a backup is taken

Two steps, and the separation is deliberate.

SPOOL, THEN UPLOAD

1. `slapcat -b <suffix> | gzip` into a scratch directory on the node's disk
2. upload that file to S3

Why not stream straight to the bucket? Because a `slapcat` that dies half way would still leave a complete-looking object behind. Spooling first means a failed dump fails the backup, and no object is ever created.

The price is disk and a little time. The artifact is a plain `slapcat` LDIF — `gzip -dc` and read it.

HOW IT READS THE DATA AT ALL

We ask Kubernetes for volumes with access mode `ReadWriteOnce` — and that means one **node**, not one pod. Two pods on the same node can hold the same volume at once: the node mounts the filesystem once and bind-mounts it into each container.

So the backup is its own pod, pinned to the node `slapd-0` is on, reading the same `/data` while slapd keeps serving. `slapcat` on `back-mdb` is safe online — this is not an outage.

A finished pod still counts as a user of the volume — `kubernetes.io/pvc-protection` does not check the phase — so the operator deletes its own Jobs. Otherwise the first backup quietly prevents the cluster from ever replacing a pod.

One backup, asked for and answered

```yaml
kind: SlapdBackup
metadata:
  name: example-db-backup
spec:
  databaseRef: example-db
  storage:
    bucket: my-ldap-backups
    prefix: prod
    region: eu-central-1
    endpoint: https://s3.example:7443
    credentialsSecretName: my-s3-creds
```

The object key is legible from the bucket alone:
`<prefix>/<cluster>/<database>/<timestamp>.ldif.gz`

```yaml
status:
  phase: Completed
  sourcePod: slapd-0
  sourceContextCSN:
    - …Z#000000#001#000000
    - …Z#000000#002#000000
    - …Z#000000#003#000000
  conditions:
    - type: SourceConverged
      status: "True"
    - type: SourceSuffixHealthy
      status: "True"
```

A backup is **one pod's copy of one database at one instant** — and the CSN vector says which instant, in replication's own units.

Those conditions are not a gate. A backup always takes a backup and records its circumstances.

Backups, on a schedule

A cron expression, a retention policy, a bucket.

```yaml
kind: SlapdScheduledBackup
metadata:
  name: nightly
spec:
  databaseRef: directory
  schedule: "0 3 * * *"
  compression: gzip
  retention:
    maxCount: 14
    maxAge: 720h
  storage:
    bucket: slapd-prod
    endpoint: https://s3.example:7443
```

```yaml
status:
  lastScheduleTime: 2026-09-29T03:00:00Z
  nextScheduleTime: 2026-09-30T03:00:00Z
  lastBackupRef:    nightly-1790650800
```

Each tick creates an owned `SlapdBackup`. The schedule does no work itself — it is a factory and a broom.

Retention deletes the **S3 object** too, not just the record. Only *Completed* backups are pruned: failed ones are kept on purpose, so the morning after is diagnosable.

You declare the policy. Keeping it is somebody else's problem.

The easy restore is a new cluster

Nothing exists yet. So the backup is simply where the database comes from.

```
kind: SlapdDatabase
spec:
  suffix: dc=example,dc=org
  bootstrapFrom:
    backupRef: nightly-1790650800
```

It takes the place of `spec.seed` — the two are mutually exclusive, and it is one-shot. Or point `bootstrapFrom.s3` straight at an artifact: a `slapcat` dump from a directory that never heard of this operator.

WHY THIS ONE IS EASY

- nothing to scale down and nothing to stop — there are no pods yet
- nothing to wipe: the database is **created from** the artifact, it never had an earlier state
- it is ordinary **desired state** — declare the database, get the data
- and it is the right tool for a **new site**: seed locally, then let syncrepl carry only the delta

Put it on a database that already holds data and it declines — it is never an in-place overwrite. Which is exactly why there is a second way to do this.

Why `SlapdRestore` exists

You could do this by hand: delete the database, declare it again with `bootstrapFrom`. Nothing stops you — and that is worth saying, because the automation is not doing anything you could not.

BUT THE MANUAL VERSION DESTROYS FIRST

Is the artifact the right suffix? Did the gzip survive? Does the replication password in it still match the cluster's?

By hand you find all of that out *after* the data is gone — and every step is one you can skip at four in the morning.

SO THE OPERATOR DOES IT IN THIS ORDER

1 — preflight, cluster still serving. Fetch it, gunzip it, check the first DN *is* the target suffix, verify the replication password against the artifact's own metadata. Fail here and nothing has been touched.

2 — only then scale to zero, and per pod wipe *that database's* directory immediately before loading it. The other databases on the cluster are not touched.

Destroy last.

Nothing is wiped until the artifact has proved it can be put back. And if a pod fails to load anyway, the peers still hold the old data — come back up on them, and fail loudly.

Why an image and an operator

What we ship, and why a chart would not have been enough.

The `slapd` container image

We use our own purpose-built container image.

Because we can control and trust it. Meet our requirements, and global best practices.

base	`gcr.io/distroless/base-debian13`
built from	`debian:trixie-slim` builder — Debian's own OpenLDAP packaging[1]
runs as	uid/gid 1024 · ports 1024 / 1025 · no capabilities
root fs	read-only
volumes	`config` · `data` · `accesslog`
bootstrap	init container, same package set — no entrypoint script

1 — Currently: 2.7.1 built by us with Debian's own packaging scripts. Revert to Debian upstream once it ships 2.7. Reason: ITS#9580 — a rebuilt replica corrupts its accesslog; the fix is only in 2.7.

A Helm chart would get us far

With that image, we could write a Helm chart.

With thorough topology arithmetics in the bootstrap — *"I am pod 2 of 4, so this is my* `serverID`*, and these are my* `syncrepl` *stanzas."*

That bootstraps a working cluster, and it carries us a long way.

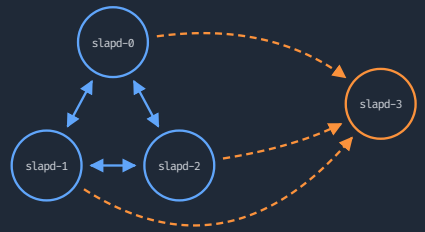
So what does an operator do beyond that?

Adding a fourth pod

Same image, same StatefulSet, same three pods to start with. One thing differs: whether something is still running when you ask for the fourth.

A — the Helm chart

```
% kubectl scale sts slapd --replicas=4
```

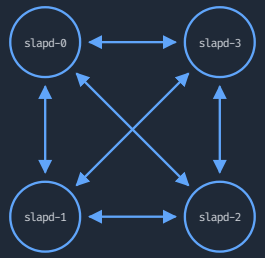


No template change, so nothing restarts — and nothing tells slapd-0..2 that slapd-3 exists.

It receives everything and sends nothing. Writes that land there are lost, and every pod reports Ready.

B — the operator

```
% kubectl edit slapdcluster slapd  # replicas: 4
```



The controller rewrites the syncrepl stanzas on every existing pod, over `ldaps://`.

Four pods, twelve stanzas, no restart — and no odd one out.

You could *almost* do it with a chart

> `helm upgrade --set replicas=4` *does* converge — at the price of a rolling restart of every pod, and other side effects.

SCALING IS THE SMALL CASE

- **multi-step operations over live data** — backup, restore, migration, replacing a pod without losing its volume
- **anything cross-cluster** — the local config is a function of another cluster's live pods
- **the repairs nobody has named yet**

WHICH THE OPERATOR HAS

- it is **running** — there is a now, not only an install time
- it sees the **whole cluster**
- it knows what `slapd` is
- it can **remember**, in the resource's status
- it can **act**, over `ldaps://`

the chart is the preprocessor
It runs once, before anything starts — and whatever it computes, it may only emit Kubernetes objects.

the operator is the daemon
It is still there at runtime, and it can do anything a program can do. Including speaking LDAP.

Limited expressive power at install time — or full power, for the whole runtime.

How this got built

A project this size, in spare time, is only realistic because AI agents did substantial implementation work. So: how that actually works here, where the industry stands — and what I think it costs.

How we work here

Four things, in this order. The first two are mine, and neither is delegated.

1 · EXPERTISE, FIRST

- Kubernetes, operators, distributed state: ground I can stand on.
- `slapd` is not. So: back to school — upstream docs, prior art, configurations that have been in production for years, this conference, and people who know it better than I do.

The agent is not a substitute for that. It is a multiplier on it — including on the gaps.

2 · THE DESIGN IS MINE

- requirements, and the in-scope / out-of-scope argument
- the architecture, and every decision that constrains it
- ADR-driven: the decision, the alternatives, the *why*
- principles, test discipline, history awareness — written into `CLAUDE.md`, and the agents are held to it

None of this is delegated.

Where the agents come in

Three and four. Only the last one is the agents doing the work.

3 · SPARRING

- root-cause analysis on complete evidence (`slctl debug-dump`) — genuinely brilliant at it
- carrying a working thing across: a deployment script is excellent input for an operator
- it has read everything, and proposes components I had never heard of

I never take an RCA I cannot explain myself, and never hand over the decision. Ask for a re-word, more context, a definition — it does not judge, and it explains it again.

4 · THEN THEY BUILD

- solution design and execution plan, worked out together, before a line is written
- an orchestrator briefs implementation agents and reviews what comes back
- red-first, e2e, no regressions
- real labs: three sites, real `slapd` , real replication — no mocks, no facades

A green test against a mock is the most expensive green there is.

Chances, and risks

Personal, and I am not going to talk the second half away.

COGNITIVE DEBT

I think a feature through, completely. I brief it. It goes through implementation, the tests, the plumbing, the small ugly fixes, review, main, release — and I was in almost none of that. Then I context-switch to the next big thing.

Months later I read my own documentation to find out how my own system works.

The mitigation happens to be good practice anyway: document while you still know. There is no other way back in.

BECOMING AN EXPERT

This section started with *be an expert in something*. Two things are true at once:

harder — expertise came from doing, and the doing is shrinking.

easier — "teach me Kubernetes, start at zero" is a genuinely excellent way to learn. I am convinced of that one.

But it no longer happens along the way. It costs explicit attention and explicit energy. Nothing comes for free.

WORKING ALONE

A team of agents is always available, never busy, and never needs the conversation. The tempting conclusion is that you need fewer people around you.

Human-to-human exchange is what quietly gets squeezed out to make the room.

It used to happen by itself. It does not any more — so it has to be culture, and it has to be deliberate.

Great benefits and great risks

Both — and I am not trading the second away to make the first sound better.

This is not going away. Either we learn to use it well and carry what it costs, or that gets settled by the people who do not care.

You only shape the rules if you are in the game.

Where this stands

The same list as before the walkthrough. You have now watched most of it run.

- ☑ Declarative end-to-end, gitops all the way
- ☑ N-way multi-master delta-syncrepl, plus consumers
- ☑ Multi-site, cluster per site, cross-site transports
- ☑ Migration of existing deployments, hot and cold
- ☑ Backup, restore, disaster recovery — to S3
- ☑ Databases, schemas, ACLs as custom resources
- ☑ Security defaults that do not cost functionality
- ☑ Tooling: `slctl`, conditions, e2e across three sites
- ☐ Production-grade OpenLDAP out of the box

One lab, one transport tested. One person, spare time, no release. What I cannot get by working harder is the half I do not have — twenty years of running directories in production.

A vision to sustainability

OWNED BY ITSELF

Apache-2.0, developed in the open, with governance that routes through neither me nor an employer. It should outlive my interest, my job, and my being wrong about things.

CO-MAINTAINERS

People with commit rights who know `slapd` better than I do — expertise and bandwidth both. Every design decision in this talk deserves someone able to say "no, and here is why".

GIVE IT A TRY

If your next project pushes you onto Kubernetes, put slaptain on the list — especially if the alternative is writing your own chart. Been there. This is further along.

> Use it, break it, tell me what broke. That is how this grows past the lab and past one person.

So — what is it that we have here?

A toy?

An academic proof of concept?

Or something with a future?

Concretely: attention, users, review, contributors — and above all OpenLDAP expertise.

slaptain.chuck-chuck-chuck.net · Apache-2.0

Back-pocket

Not part of the talk. Here if you ask.

Migration

Getting an existing directory in — with a maintenance window, or without one.

Getting an existing directory in

Nobody starts empty. Two ways in, and the choice is made by what you can afford, not by what is elegant.

COLD — a maintenance window

Freeze the writers, `slapcat` each database on the source, `slapadd` it into slaptain — that is `bootstrapFrom.s3` from earlier — and cut the clients over.

Simple and robust, and it costs a window. It asks *nothing* of the source: no config change, no reachability, no cooperation.

HOT — no window at all

slaptain joins the source's syncrepl mesh as a peer, takes client traffic gradually, and the source's nodes drain and retire.

It needs a source you are allowed to reconfigure — a `syncprov` overlay, a bind user, ACLs that let it read everything. A source whose replication config is frozen leaves only cold.

Choose by **downtime tolerance**, **directory size**, and **whether the source can be touched**. Cold is the floor and the fallback — and it stays available in the middle of a hot migration, which is what makes the hot path safe to attempt.

Hot migration, one stage at a time

Each stage is a stable configuration you can sit in. The operator never advances on its own — every transition is a deliberate edit.

	slaptain	the source	reversible?
0	not present	authoritative, serving everyone	—
1	consumer-only, read-only, pulling	unchanged	**totally**
2	peer, bidirectional	reciprocal stanzas added	yes, with source-side undo
3	peer, taking client traffic	losing client traffic	per client
4	peer, authoritative	draining node by node	until the last node drains
5	authoritative, alone	retired	forward only

1 → 2 is a field edit. Patching `replication.mode` promotes consumer-only to peer **in place** — no pod restart, and `entryUUID`s unchanged, which is how you know nothing re-synced.

Confidence, stated plainly. Stages 1 and 2 are covered by an e2e that stands up a deliberately legacy provider. Stages 3 to 5 are a written runbook, not a tested path.

Bootstrap, step by step

What happens between `kubectl apply` and a replicating directory.

Bootstrap, part 1 — what a pod can do alone

The `SlapdCluster` from the previous slide — 3 + 1, TLS on, replication on — lands. Then:

The operator creates — the Secret it reaches the pods with, the Services, and the StatefulSets.[1]

Kubernetes creates the pods — and their PVCs, from the StatefulSets.[2]

The init container runs — makes the LMDB directories,[3] and renders the `slapd.conf` it converts into `cn=config`.[4]

slapd starts — `-F /config/slapd.d`, ports 1024/1025.

Nothing on this slide needs another pod.

1 — `<name>-config-password` is the `cn=config` admin credential the operator binds with. Services: `slapd-headless` and `slapd`, plus the same pair for `-readonly`. Those two and the StatefulSets wait until the TLS Secret is present and usable; until then `TLSReady=False`, and the operator comes back.

2 — pod creation is ordered by the StatefulSet controller (`OrderedReady`): pod-0 is Ready before pod-1 is created. PVCs come from `volumeClaimTemplates` — config, data and accesslog per RW pod, config and data per read-only pod.

3 — `mkdir -p`, on every start. In a fresh `SlapdCluster` only the node-local auth DB exists; workload DBs are added later, via `SlapdDatabase` CRs.

4 — once per volume lifetime: `slaptest -f … -F /config/slapd.d`. Modules · core schemas · `serverID` = ordinal + 1 · TLS paths · the config database — and *no* data database, *no* custom schema, *no* ACLs, *no* syncrepl.

Bootstrap, part 2 — what a pod can’t do alone

The operator dials every pod — one connection each, over headless DNS. Not the Service.[1]

The cluster controller writes — server-global tunables, and the node-local auth database.[2]

The loop converges — and stays there.[3]

That is an *empty* cluster: four pods, a config database, no directory. More happens the moment a `SlapdSchema` or a `SlapdDatabase` exists.

1 — bound as `cn=admin,cn=config`, not through the ClusterIP Service: `cn=config` is node-local, so every pod is visited and written on its own.
2 — node-local, on every pod including the read-only fleet; it holds the per-database syncrepl bind identities.
3 — every pass re-reads and re-compares: drift, hand edits and operator upgrades heal unnoticed. Compare first, write only on divergence.

Bootstrap, part 3 — Adding content

Same loop as before — dial every pod, compare, write only on divergence. Now there is something to write.

The schema controller writes — for each `SlapdSchema`, on every pod: the attribute types and the object classes.[1]

The database controller writes — for each `SlapdDatabase`, on every pod: create the database → ACLs → indices → `syncprov` + `accesslog` overlays → the journal DB → modules → serverIDs → the bind identity → **then** the syncrepl stanzas.

And on pod-0 only, once: the seed.[2]

The order *is* the safety.[3]

1 — schema is global to the slapd process, so it is written per pod, not per database — hence `clusterRef`. Additive-only (ADR-006): you add, you never silently drop.

2 — recorded in the status, never repeated; replication carries it to the peers, and there is no second write path.

3 — a provider that lacks the bind identity rejects every bind with `err=49`, and the link stays dead until the entry appears — while slapd is up and serving. So the stanzas are written last, and withheld until every RW pod carries the identity.

Internals

The derivations, and where the configuration actually lives.

What the operator derives, so nobody maintains it

serverIDBase

`serverIDIndex × 100`, then `base + ordinal + 1` per pod — so `site 2, pod 3 → olcServerID 203`, which reads straight out of a CSN at three in the morning.

externalPeers

Every site the cluster spans, except this one — N×(N−1), a full mesh. Never peer with yourself; a pod must not be its own provider.

Network mode

From `mesh.network` — two clusters on one fabric cannot sensibly disagree about whether pod CIDRs are routed. Peer addresses are then *discovered* from each remote API server, never listed.

Trust wiring

Each site's `caSecretName`, mounted at every other site — N×(N−1) again. The consumer verifies the provider; peer *authentication* is the bind, not the certificate.

Applied in memory, never written back to the spec — writing it back would make each site's object differ from its neighbours' and destroy the property the whole design rests on.

Set any of them by hand *alongside* `meshRef` and the cluster refuses: `MeshResolved=False`, nothing reconciled. Deliberate — an ambiguous `serverIDBase` is how a serverID collision gets in quietly, and slapd validates nothing there.

Where the syncrepl stanza actually lives

Nowhere on disk that you would edit. It is an attribute of a running slapd, written by the operator over `ldaps://`, per pod:

```
dn: cn=config
olcServerID: 203

dn: olcDatabase={2}mdb,cn=config
olcSyncrepl: {0}rid=101 provider=ldaps://…:1025
  type=refreshAndPersist
  searchbase="dc=demo,dc=example"
  bindmethod=simple
  binddn="cn=repl-demo-db,cn=slaptain-auth"
  credentials=…
  logbase="cn=accesslog-demo-db"
  logfilter="(&(objectClass=auditWriteObject)
             (reqResult=0))"
  syncdata=accesslog
  retry="10 +"
```

One stanza per peer

In-cluster peers and cross-site peers, each with its own `rid` out of a per-database range — so a stanza can be traced back to the peer that owns it.

delta-syncrepl, per database

`syncdata=accesslog` and a `logbase` that names *this* database's journal: `cn=accesslog-<db>`, its own LMDB directory under the accesslog volume.

The bind identity

Not `cn=replication,<suffix>` in your data tree. The next slide is about why that matters more than it looks.

The credential, and where it is allowed to live

A syncrepl consumer binds to its provider. That one secret must exist twice, in two forms — the protocol requires both: plaintext on the consumer to present, a hash on the provider to verify.

where it used to live

An entry in the replicated data tree. Which means: it propagates mesh-wide and converges on one winner, while the per-site Secrets do not propagate at all.

Measured: three sites, three generated Secrets, one converged entry — two sites holding credentials that matched nothing, replication dead for **nineteen days**, every health signal green.

Where it lives now

A node-local database, `cn=slaptain-auth`, that is never replicated — no syncprov, no syncrepl, no accesslog, by construction.

The Secret is the single source of truth; the LDAP copy is a projection the operator solely owns, converged on every reconcile like any other node-local state.

→ The problem was never "two stores". It was that one of the two stores was shared, replicated, multi-writer state — in the customer's tree, under customer-defined ACLs. Rotation stopped being a design problem and became an ordinary operation.

Access control on the thing that answers binds

The auth database exists to answer binds. Its ACLs say exactly that, and nothing more:

```
olcAccess: to attrs=userPassword by anonymous auth by * none
olcAccess: to *                  by * none
```

`auth`, not `read`

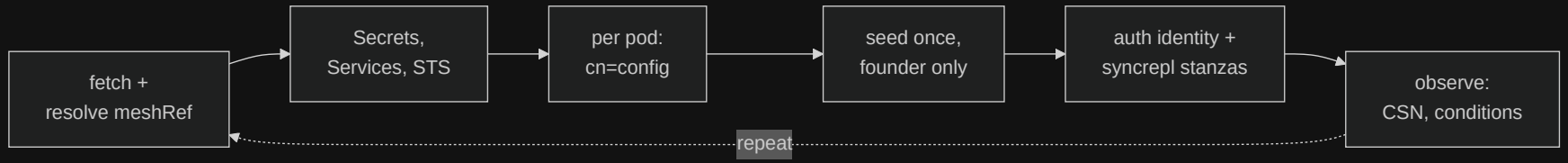
slapd needs the *auth* right to verify a simple bind. Granting only that means a successful bind never implies being able to read the hash back out.

the catch-all is not redundant

A database with no matching rule falls through to the frontend default — and that default is *read*. This database holds every replication credential on the pod.

One identity per database — `cn=repl—<db>,cn=slaptain-auth` — so one database's replication identity cannot read another database's journal. Your own ACLs, schemas and databases are custom resources, and they are yours.

The reconcile loop



A reconcile is not "apply the desired state". One step, repeated — and safe to interrupt at any point, because it will be.

An unresolvable mesh does not fall back and does not half-derive: that would empty the peer set, and the next pass would tear every cross-site stanza off every pod. Report and stall.

Unhealthy → tight retry. Healthy → a slow resync floor, so a rotated Secret is still picked up on a cluster where nothing else happens.

The lab underneath

Where three sites come from, when nobody is paying for three sites.

Where does a spare-time project get three sites?

Everything you just saw — the serverID decades, the peer sets, the cross-site syncrepl stanzas — is only worth anything if it was exercised on something that is genuinely three sites. A single `kind` cluster cannot tell you that.

Disjoint, routable pod networks

Cross-site syncrepl is pod-to-pod. Every site's pod CIDR must be reachable, as itself, from every other site.

an API reachable *from pods*

The operator discovers peers by dialling the other sites' Kubernetes APIs — from inside a pod, not from your laptop.

Sites that are actually separate

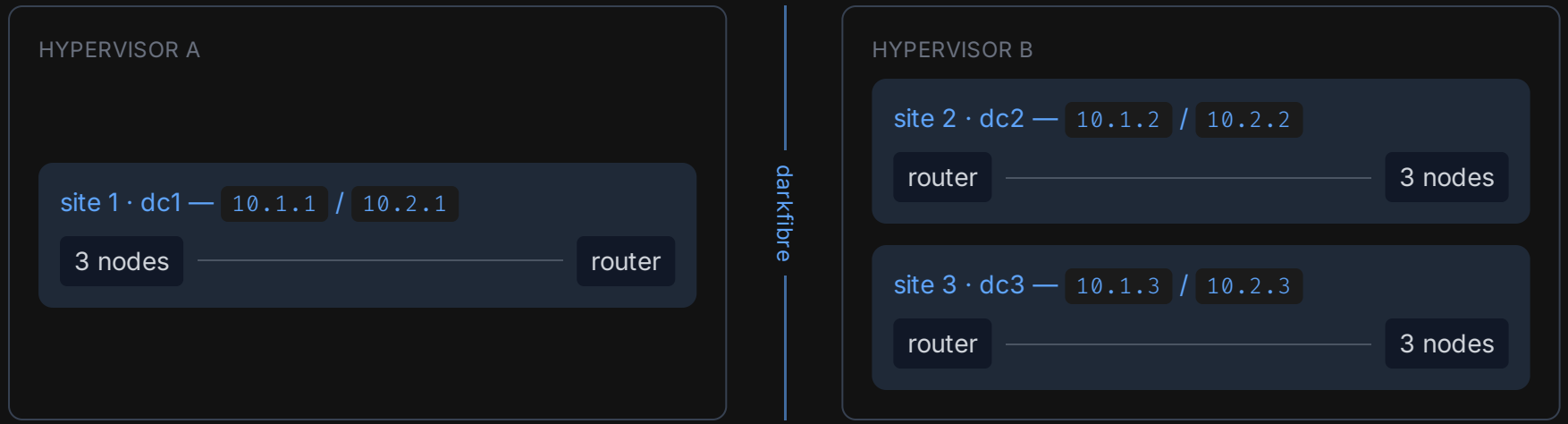
Distinct L3 segments with one path between them. On a flat network every topology bug reads as green.

No managed-cloud magic

Most places OpenLDAP actually runs have none. Whatever the lab leans on has to exist on plain VMs.

> From the basement. Two Linux boxes at home — 192 GB of memory between them and a handful of cores, bought privately. In the evenings one of them is a Steam box. That is the entire budget, and it is enough for three sites.

Two hypervisors, three sites, one darkfibre



libvirt networks in route mode, not NAT — so a VM keeps its real address everywhere, which is the whole point.

One bridged L2 across the two hosts plays the darkfibre. It is the only inter-site path, and a router VM per site is the only thing on it.

An nftables policy on each host drops bridge-to-bridge traffic and masquerades only towards the internet. Without it the sites are accidentally one network.

Eighteen VMs — three sites of five, plus a three-node control plane this project does not use — two physical machines, one `make apply`.

Dual-homed, by role

Every node has two NICs, and which one is which is a decision, not an accident.

internal — `10.1.N.0/24`

Site-local. Consumers, everything else on that site, and the only route to the internet. Does *not* cross sites.

replication — `10.2.N.0/24`

Routed between sites over the darkfibre. Carries cross-site pod traffic and the cross-cluster API. No internet.

The consequence lands directly in the operator's API:

the address in your kubeconfig is not the address a remote pod can dial.

```
sites:
- name: site-1
  endpoint: https://10.2.1.10:6443
  serverIDIndex: 0
```

That `endpoint` is the site's API on the *replication* network. Admin access uses the other one. Two addresses for the same apiserver, and only one of them is peer discovery.

A mesh field that looks like redundant configuration is usually a dual-homed network that has not been admitted to yet.

Every node is its own router

Cilium, native routing, no kube-proxy

Each node owns a pod `/24` out of the site's `/18`. No overlay, no encapsulation — a pod packet keeps the pod address on the wire the whole way.

The payoff

Nothing static about pod CIDRs anywhere. Add a node, drain a node, rebuild a cluster — its `/24` appears and disappears on its own, and no peer or router is hand-edited.

bird2 on every node

A system extension of the immutable OS. It advertises the node's own `/24` upstream and *installs* what it learns into the kernel FIB — which Cilium's own BGP will not do, being advertise-only.

the bill

An ASN tier per role *and* per site. Two co-sited clusters that share an AS number silently drop each other's routes — AS-path loop prevention working exactly as designed, on a topology that is not a loop.

Routers full-mesh over the darkfibre

Three sessions, re-originating each site's prefixes. Learned routes land in the kernel as `proto bird`.

This is what `network.mode: pod-routed` in the `SlapdMesh` is resting on: a pod IP in site 1 is an ordinary routable address in site 3.

The "semi" in semi-cluster-mesh

WHAT IT IS

- routed pod-to-pod, both directions, across sites
- a consumer outside the clusters reaches the site-local pods directly, SNAT'd to its own node address
- discovery by forwarding one DNS sub-zone to the site-local cluster
- **no proxy anywhere on the data path**

WHAT IT IS NOT

- not a service mesh, not a sidecar, not an overlay
- no cross-cluster `Service` abstraction, no global load balancing
- a consumer is pinned to its local site, on purpose — it can only route to the pods it is allowed to route to

We ran a real Cilium ClusterMesh, took it out — nothing queried it, and it sat at **3 of 9 nodes reachable** forever — then put it back when a workload turned up that genuinely needed cross-cluster `Service` semantics.

Why it can never be green: the health probe targets the node's `InternalIP`, picked by a hard-coded priority in the source, with no configuration hook. So the question was never "tune the mesh". It was which NIC carries the node address — and that one reshapes the whole lab.

slaptain is indifferent to all of it. Syncrepl is pod-to-pod; the operator needs routing, not a mesh.

What the lab proves — and what it does not

PROVEN

- three separate clusters, three L3-separated sites
- cross-site pod-to-pod with no overlay and no proxy
- each site’s API dialable from a remote site’s pods — the operator’s own discovery path
- rebuildable from VMs to clusters by automation, not by memory

HONEST

- the darkfibre is a bridge between two machines: no latency, no loss, no partition worth the name
- two machines wearing nine node hats: "three sites" here is a routing arrangement, not three buildings
- one lab, one transport — `pod-routed` is exercised, the alternative is written and untested
- it has taught me more about reboots than about replication

It is not a production proof. It is the smallest thing on which "three sites" stops being an assumption — and that turned out to be enough to find real bugs in the operator.

Things that break, and how they lie to you

nftables is runtime state. A hypervisor reboot silently removes the site isolation and the egress masquerade. Now a systemd unit — and something to *verify*, never assume.

`ip_forward` reverts to 0 on the router VMs, because modern `systemd-sysctl` does not read `/etc/sysctl.conf`. Tell: the box answers on its own addresses and drops every packet that was only passing through.

Asymmetric host routes. Small requests are instant, large uploads black-hole: `kubectl get nodes` fine, `helm` dead after 45 seconds with `http2: client connection lost`. MTU is a red herring; it was a missing route back.

Impatience. After a restart the pods come back with new addresses and a stretched control plane sits in CrashLoopBackOff for minutes after losing quorum. Verifying inside that window produces confident, false failures.

None of these are LDAP problems. They are the rent on a multi-site lab — and the reason a "does it replicate across sites?" question can take a day to answer honestly.

How this got built — in context

Where the industry stands. Kept back because it is other people's argument, not mine.

In context: what does the industry do?

DORA 2025: **90% of development professionals use AI at work.** So the interesting question is not whether — it is under what discipline.

LINUS TORVALDS

Open Source Summit NA, May 2026

"You need to understand not just your prompts, but you need to understand your end result, because that's the only way you can maintain it long term."

The most change-resistant codebase on the planet settled it institutionally — and attached exactly one condition.

ANDREJ KARPATHY

Sequoia Ascent, April 2026

"Vibe coding raises the floor. Agentic engineering raises the ceiling."

"You can outsource your thinking, but you can't outsource your understanding."

The man who coined *vibe coding*, calling it insufficient and naming the replacement a discipline.

THOUGHTWORKS RADAR

vol. 34, April 2026 — ring: Caution

"Codebase cognitive debt: the growing gap between a system's implementation and a team's shared understanding of how and why it works."

The risk I just described, with an industry name, a published definition and a *Caution* ring.

And the honest counterweight — METR, 2025/26: in a randomised trial, experienced developers on familiar codebases were **19% slower** with AI while believing they were 20% faster. Nobody on this slide is claiming the question is closed.