

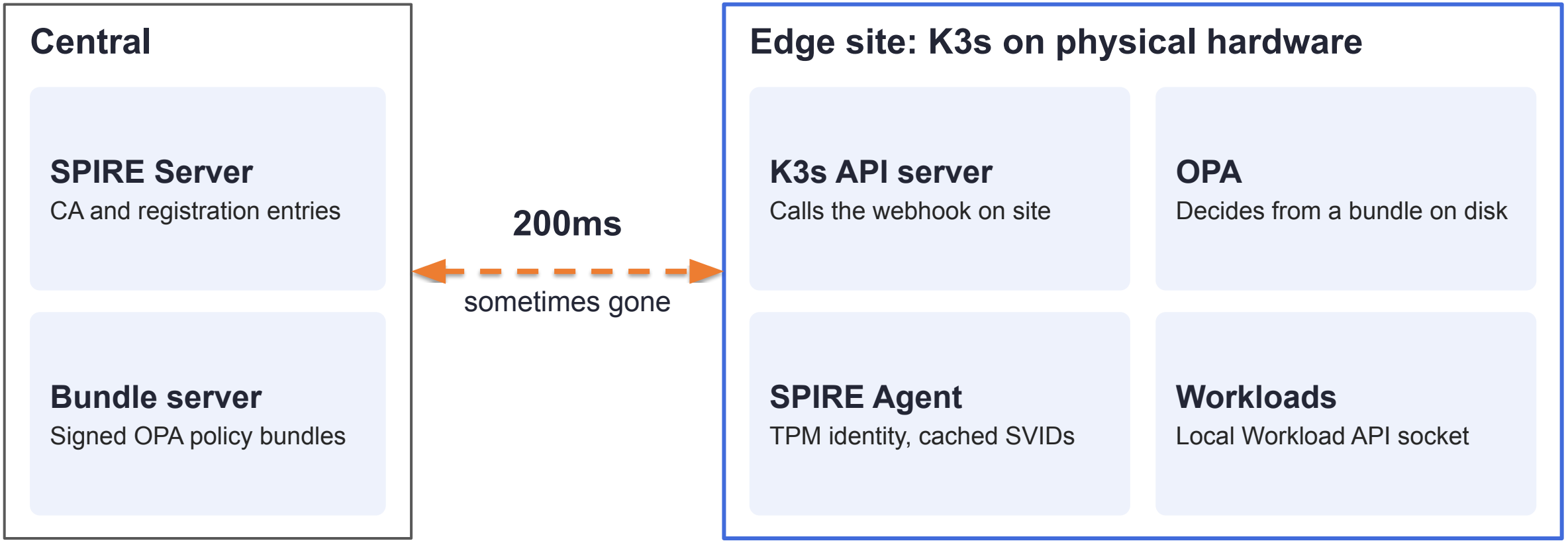
Kubernetes on EDGE DAY
NORTH AMERICA

Bootstrapping Edge Nodes When the SPIRE Server Is 200ms Away and Sometimes Gone

Manan Chawda
Software Engineer

One central trust root, many K3s sites

Kubernetes on EDGE DAY NORTH AMERICA



Cold attestation: 54ms becomes 2.7s. Local SVID fetch: still 13ms.

Latency only hurts issuance. An outage is the real problem.

Measured: SPIRE v1.15.5, K3s v1.33.5, OPA 1.10 in a lab rig.

Failure 1: WAN down, local mTLS down

Kubernetes on EDGE DAY NORTH AMERICA

WAN link to SPIRE Server



Agent and workload SVIDs (SPIRE defaults)



mTLS between two workloads on the same node



After reconnect: join_token

Never recovered. “Join token does not exist or has already been used.”

After reconnect: tpm_devid

Re-attested in 6s with no human, after its SVID expired offline.

Measured: SPIRE v1.15.5, K3s v1.33.5, OPA 1.10 in a lab rig. Multi-hour outages ran on an accelerated clock.

Bootstrap from the TPM, not a token

Kubernetes on EDGE DAY NORTH AMERICA

	Before: join_token	After: tpm_devid
Node identity	Secret, used once	DevID key held in the TPM
Copied off the box	An unused token works from anywhere	Key blob useless without that TPM
Can re-attest	false	true
Agent SVID expired	A person issues a new token	Back in 6s, no human

Cost: DevID certificates must be provisioned out of band, before the node ships.

Measured: SPIRE v1.15.5, K3s v1.33.5, OPA 1.10 in a lab rig. tpm_devid on swtpm 0.7.1, stock release, real time.

Rotate early, keep identity on disk



server.conf

```
server {
  ca_ttl                = "720h"
  default_x509_svid_ttl = "96h"
  agent_ttl             = "96h"
}
NodeAttestor "tpm_devid" { … }
```

96h SVIDs need a CA of at least 576h. SPIRE says so at startup.

agent.conf

```
agent {
  availability_target = "72h"
  data_dir            = "/var/lib/spire"
}
KeyManager "disk" { … }
```

Rotation fired with 72h left. Without the target: 50h left.

Measured: SPIRE v1.15.5, K3s v1.33.5, OPA 1.10 in a lab rig. Multi-hour outages ran on an accelerated clock.

Failure 2: longer TTLs hit the CA

Kubernetes on EDGE DAY NORTH AMERICA

`Default ca_ttl = 24h`



Asked for 96h, survived far less

First SVID: 23.9h. Late in the CA's life, a cut left only 4.3h. SPIRE only warns at startup.

Offline across the CA rollover

9h outage: 3 of 4 runs recovered. 13h: 0 of 4. The node can't verify the server, and rebootstrap_mode = auto didn't rescue it.

Rotation interval is a property of the whole chain, not one TTL.

Measured: SPIRE v1.15.5, K3s v1.33.5, OPA 1.10 in a lab rig. Multi-hour outages ran on an accelerated clock.

Size lifetimes backward from the outage

Kubernetes on EDGE DAY NORTH AMERICA

`longest outage`

48h

Measure it per site.

`availability_target`

72h

Outage plus margin. Minimum 24h.

`SVID TTL`

96h

Target plus at least 12h.

`ca_ttl`

720h

At least 6 × TTL, and ca_ttl / 3 above target.

48h outage: tested

Zero mTLS failures. No agent restarts.

90h outage: past the target

mTLS failed at 73h. Recovered in 12s, no human.

Ceiling: the 7-day SVID limit allows about 6.5 days offline.

Measured: SPIRE v1.15.5, K3s v1.33.5, OPA 1.10 in a lab rig. Multi-hour outages ran on an accelerated clock.

Run admission on the last good bundle


```
bundles:
  edge-policy:
    service: central
    resource: policy.tar.gz
    persist: true
    signing:
      keyid: edge
persistence_directory: /persist
```

Bundle server cut, then OPA restarted. Real K3s webhook, real pod creates.

After OPA restart, offline	Good pod	Bad pod
Persist on host volume	**Allowed**	**Denied**
emptyDir, failurePolicy Fail	Blocked	Blocked
emptyDir, failurePolicy Ignore	Allowed	**Allowed**
OPA not exempt from webhook	OPA never returned	

Only one row keeps enforcing policy. Test the other three.

Measured: SPIRE v1.15.5, K3s v1.33.5, OPA 1.10 in a lab rig.

Five things to take back to your fleet



Kubernetes on EDGE DAY
NORTH AMERICA

1. Bootstrap from hardware: tpm_devid re-attested in 6s, no human
2. Size lifetimes backward: outage, target, TTL, then ca_ttl
3. Keep ca_ttl / 3 above your target: past a CA rollover, 0 of 4 recovered
4. Keep decisions on site: persist OPA bundles to a real volume
5. Cut the WAN past your target, reboot a node, and watch what breaks

Measured: SPIRE v1.15.5, K3s v1.33.5, OPA 1.10 in a lab rig.

Let us connect!

Kubernetes on EDGE DAY
NORTH AMERICA



Manan Chawda

LINKEDIN

Scan to connect

linkedin.com/in/mananchawda