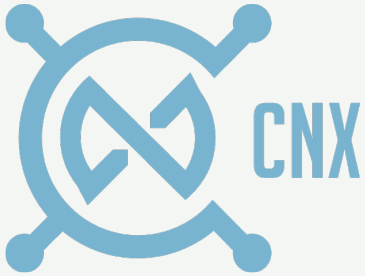
CNX / KHNOG 8 / 2026

IaC with AI, for AI

Keeping AI agents aligned through a yearlong infrastructure build



We started with DNS because every other Internet service stands on it.

DNS controls the first decision



Most queries look simple: a client supplies a name and receives an address.

`www.example.kh` $\longrightarrow$ `2001:db8::53`

- The answer determines where the client connects.
- It can determine whether domain validation and certificate issuance succeed.
- A wrong answer can redirect the client before the application receives a request.

DNS controls both the route and the identity the client expects.

Credible authoritative DNS

RFCs define protocol correctness. A credible service must also answer the control questions regulated industries ask.

THE ENGINEERING SYSTEM

- **Governance** provides review, approval, history, and recovery.
- **Validation** connects the accepted revision to the deployed zone.
- **Security** protects DNSSEC signing and key custody.
- **Delivery** controls propagation across the authoritative sites.
- **Operations** provide observable state and recovery evidence.

CONTROL EXPECTATIONS

- **NIST CSF 2.0** covers governance and cyber-risk outcomes.
- **NIST SP 800-53 Rev. 5** defines security and privacy controls.
- **NIST SP 800-57 Part 1 Rev. 5** guides cryptographic key management.
- **SOC 2 Trust Services Criteria** cover service controls and evidence.
- **ISO/IEC 27001:2022** defines information-security management.

Authoritative DNS architecture



Databases store data well. Configuration management is a change-control problem. Which system is built to manage changes?

CONFIGURATION AND SIGNING

- **Git** is the authoritative DNS configuration database. It records proposed, approved, and deployed revisions and provides the recovery history.
- Deployment automation validates the accepted revision before publication.
- An isolated **hidden master** signs through the HSM and never answers public queries.

SERVING AND ROUTING

- Our network is **IPv6-only**, with six NS servers across three sites.
- Each server announces its service virtual IP through **BIRD** into the internal BGP fabric.
- Internal and external anycast networks route queries to an available site.
- Logs, metrics, and DNS telemetry provide operational and customer evidence.

Platform scale

FLEET

51

compute and router nodes

FOOTPRINT

3

sites

DNS SERVICE

6

authoritative servers

TIME

2

local atomic clocks

KEY CUSTODY

3

HSMs

MONITORING

72 / 72

targets healthy

The software platform is built entirely on open-source components. Fourteen CNX-managed IX switches connect to it, but are outside this build.

The real build challenge



WHO BUILT IT

Principal architect
Architecture, implementation, testing, and integration.

Head of IT
Review of major decisions and continuity.

Claude and Codex
Implementation proposals, documentation, evidence analysis, and tests.

AI subscriptions: US$40 per month.

MY PRE-AI ESTIMATE

4–5
EXPERIENCED ENGINEERS

12–16
MONTHS

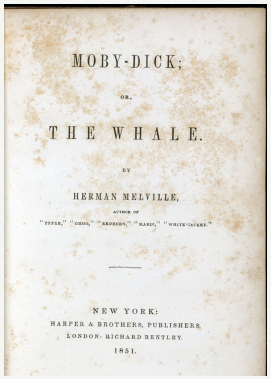
4–7
ENGINEER-YEARS

How do several AI agents and different models stay aligned over years without turning every server into a special case?

One decision at a time

2 APRIL 2026	DURING THE BUILD	2 NOVEMBER 2026
18	**185**	**428**
ACCEPTED DOCUMENTS	DOCUMENTATION COMMITS	ACCEPTED DOCUMENTS
17,648		**252,800**
WORDS		WORDS

The repository accumulated one accepted decision at a time. A service problem, a failure, or a missing boundary was documented beside the implementation that needed it.


MOBY-DICK;
OR,
THE WHALE.
BY
HERMAN MELVILLE,
NEW YORK:
HARPER & BROTHERS, PUBLISHERS,
LONDON: RICHARD BENTLEY.
1851.

We wrote a book.

1.19 × *Moby-Dick*
1851 title page,
Library of Congress

Contracts keep agents aligned



THE CONTRACT OUTLIVES THE MODEL

- models and agents will change
- repository contracts preserve accepted intent
- deterministic checks test every proposal
- a human authorizes deployment
- live evidence shows whether it worked

THE DOCUMENTS DEFINE

- ownership and allowed scope
- required behavior and forbidden actions
- security and least privilege
- failure behavior and activation rules
- evidence needed to accept the result

Our work shifted from writing code to writing contracts for AI. We now code in prose. AI translates accepted intent into proposed code. The agent may change tomorrow. The contract remains.

A DNS slave is a reusable stack



00 VM BIRTH
hypervisor/vm_deploy
netbox/set_staged

01 CLOUD-INIT HANDOFF
common/system/cloud_init_disable

02 PACKAGE FOUNDATION
common/packages/repos
common/packages/needrestart
common/packages/install
common/packages/os_update

03 HOST AND NETWORK
common/system/hosts
common/network/resolver
common/network/nft
common/system/sysctl

04 TRUST, IDENTITY, ACCESS
common/certs/ca_trust
common/certs/machine
common/certs/x509_signer_tss2
common/certs/x509_signer_pkcs11
common/system/users
common/system/user_env
common/system/motd
common/system/sshd

05 EVIDENCE, SECURITY, TIME
common/observability/logging
common/observability/node_exporter
common/observability/alloy
common/system/auditd
common/system/chrony

06 SERVICE NETWORK + IDENTITY
common/network/vips2
common/network/routing
common/network/bird3
common/network/nft (open)
common/certs/certbot
common/certs/service

07 DNS DATA AND WORKLOAD
dns/geodb_pull
dns/dnstap_sink
vm/server_dnsslave
dns/knot_collector

08 LIFECYCLE COMPLETION
netbox/set_active

Inventory changes the instance.
The stack stays the same.

~5 min
PLANNED TO ACTIVE

Reusable roles, composed policy



SEVEN POLICY DRIVERS

Software · Network · Identity · Trust · Service behavior · Operations · Lifecycle

FLEET BASELINE	PLATFORM	SERVICE	HOST
Common tools and authorities. Addressing, desired state, and shared evidence.	Repositories. Kernel, network, and runtime defaults. Image and staging.	Packages, identity, routes, and VIPs. Firewall, health, activation.	Site, interfaces, and machine identity. Instance values, labels, status.

Build the capability once, compose policy in layers, then ask which block owns the behavior and which layer owns the value.

systemd service sandboxing



A SERVICE UNIT CAN CONSTRAIN

- filesystem access
- Linux capabilities
- privilege escalation
- private namespaces
- devices and temporary files
- system-call families
- address families
- network access

`systemd-analyze security` scores

NGINX, INSTALLED OUT OF THE BOX

9.6 / 10

EXPOSURE SCORE

Ad hoc trials become a contract

SERVICE EXPOSURE CONTRACT

Tier	Service class	Target
A	CNX-written network code	**≤ 1.0**
B	Unprivileged third-party daemon	**≤ 2.0**
C	Network daemon with root master	**≤ 3.0**
D	Internal unit without listener	**≤ 4.0**

NGINX / TIER C

9.6
BEFORE

2.7
AFTER

This is now part of **Runtime 01: Scripts and Services**, the fleet-wide policy for custom scripts and systemd units. It sets the rules for safe reruns, journald evidence, secret delivery, and sandboxing. Every unit receives a mandatory confinement baseline, while capability and system-call restrictions are tested against its real execution paths and every exception is justified. Failures remain visible and bounded through explicit timeouts, nonzero exits, lifecycle markers, and crash-loop limits.

How agents receive the same rules



TASK ROUTING

01 Requested behavior

02 `AGENTS.md` routing and mandatory core

03 Applicable platform and service contracts

04 Relevant role README and DESIGN

05 Existing implementation, tests, and authoritative inputs

REPOSITORY BREADTH

65 platform + service policy documents

547 major policy sections

4 agent operating contracts

238 role-local README, DESIGN, TODO

Nobody reads the whole book before writing one role. AI agents do not either. The repository routes each task to the mandatory core and the small set of platform, service, and role contracts relevant to that change.

The observation platform



Every layer of the service feeds a small set of shared evidence systems.

LOGS

System journals and operational logs from across the fleet are collected into **Loki**.

METRICS

Prometheus collects network, service, host, and hardware measurements across the infrastructure, including SNMP-backed device readings.

DNS TELEMETRY

The **dnstap sink** collects query events from the authoritative servers and feeds **ClickHouse** for DNS analysis.

One observation platform holds the history of hosts, network devices, services, hardware, and DNS behavior.

Read-only MCP access

Controlled queries now span both live evidence and the systems that define what should exist.

LIVE EVIDENCE

- Loki logs and cross-host timelines
- Prometheus metrics and history
- ClickHouse DNS analytics
- SNMP device readings
- direct protocol checks

INTENT AND MODEL

- Ansible build repository
- switch configuration
- NetBox infrastructure model

This was the game changer: intended state can be compared with modeled state, fleet history, and protocol behavior.

AI investigation path



01 Customer symptom

02 NetBox: affected sites, nodes, interfaces, service addresses

03 Git and Ansible: intended infrastructure and zone state

04 Loki: approval, deployment, signing, transfer events

05 Prometheus: DNS, routing, interface, certificate, time, host health

06 ClickHouse: server, zone, response code, pattern

07 Direct DNS query: customer-visible behavior now

08 Finding with time range and remaining evidence gaps

One symptom can be tested against modeled state, intended state, history, and protocol behavior.

One reboot led to a fleet correction



WHAT THE PLATFORM SHOWED

- Fleet reboot for a kernel update.
- Knot started without reporting an error.
- The zone SOA check failed.
- The journal showed that the HSM key had not loaded through the PKCS #11 path.
- 2 HSMs were online. Neither recorded an access request.
- The boot sequence showed `network-online.target` before IPv6 DAD completed on `eth0`.

WHAT CHANGED

- The updated kernel exposed a race. Knot started moments before `eth0` completed IPv6 DAD.
- AI proposed `hsm-wait`. Knot now waits for three successful checks.
- Investigation continued into why `network-online.target` completed before DAD.
- An old template had masked wait-online after missing IPv6 caused timeouts.
- Fleet templates now set `RequiredForOnline=no` on addressless links.

The network’s morning report



MONITORING HISTORY

~600M

monitoring samples

LOG HISTORY

~600K

log records

TIME ALIGNMENT

10 µs*

p99 fleet clock offset

HOW THE REPORT IS BUILT

The agent starts with aggregate queries, then traces any odd signal through detailed evidence and correlates the finding on one timeline.

WHAT IT COVERS

Changes, updates, reloads, restarts, warnings, errors, absent logs, load, traffic, and DNS behavior.

* Referenced to our local atomic clocks. Yes we provide this as service

Samples from the report



5 November 2026 · Amber · no active outage · exchange traffic normal

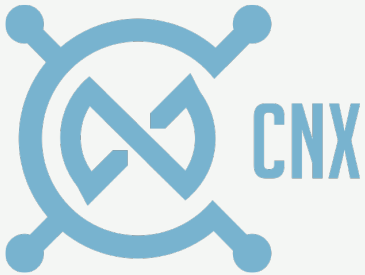
- **GCX-LF01 100GE1/0/1 lanes 1–3** are at -12.1 dBm against -13.6 dBm, which is 1.4 dB of margin and steady. `SwitchOpticRxLowMargin` is firing.
- **PTP (hypervisor):** worst offsets in the window were SCT 12,483 ns, KPH 1,758 ns, and BDC 380 ns. KPH is above 1,000 ns; its daily worst has ranged from 0.7 to 2.1 µs over the week. VM chrony is clean on all hosts and in line with p99 10 µs.
- **XXXX (ASxxxxx) on SCT-LF01 reached 88% egress**, with 155k output discards. This is a capacity finding.
- **2 100G core links into BSS flapped on Nov 4 between 13:56 and 15:07 ICT.** Operators were working on the optics at the time. KPH–BSS still has a low-margin receive lane, and BSS–GCX still logs input errors.
- **19:33:** a fleet-wide Ansible run installed `acl=2.3.2-2+b1`. Between 19:36 and 20:26, each router logged one `Jool error: The requested instance does not exist.` SIIT-DC traffic was still flowing afterwards: rp03 saw a `46::` client at 13:39 today.

CNX / KHNOG 8 / 2026

Contracts kept the platform coherent.

Shared capabilities kept servers consistent.

Live evidence showed whether the system behaved as designed.



We started with DNS because digital sovereignty needs dependable foundations.