

GOVERNED AI WORKFORCE • GOVERNANCE DEPARTMENT

The department that makes the other 366 agents trustworthy.

Governance is not a review step bolted onto the workforce — it is the control, enforcement, audit, and isolation plane that every governed call passes through, deny-by-default, before any work touches data.

● Asphodel + Tiresias-ZT • ACME Corporation

THE STAKES

325,154 identities can act. Governance decides which ones may.

ACME's real directory carries 120,120 humans and 205,034 non-human / service identities across 28 departments and 10 regions. An AI workforce inherits that surface. Without a governance plane in front of it, every agent is an ungoverned pathway to production data.

325,154 PRINCIPALS IN DIRECTORY	205,034 NHI / SERVICE IDENTITIES	28 DEPARTMENTS • 10 REGIONS	626 DISTINCT ROLES
---	--	---	--

SOURCE • Samba-AD directory (acme-directory), synced to tzt_principal via sync_ldap.py

367 agents. One deny-by-default gate. Zero exceptions.

The governed fleet is 7 showcase agents on a 14-edge topological hand-off DAG
plus 360 fleet agents mapped like-for-like to the real ACME org — every
department, by headcount. All 367 are tenants in the control-plane registry.

367 GOVERNED AGENTS	7 SHOWCASE • 14-EDGE DAG	360 FLEET AGENTS • ALL 28 DEPTS	1 ENFORCEMENT SITE • ACME-SITE
---	--	---	--

Five controls, one seam every call must cross.

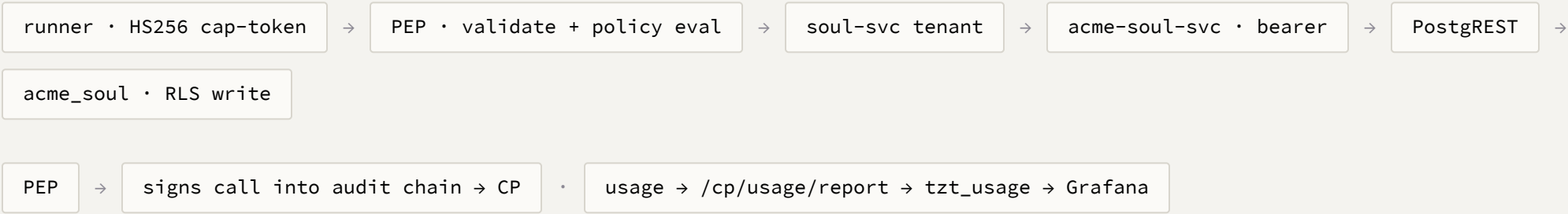
Governance is a department made of machinery. Each control is a postgres-backed, durable store — it survives restart, and it is the same seam for all 367 agents.

CP	Control Plane — policy authority Registry of 367 tenants, enrollment ledger, audit home, quarantine store. In-network only at tpiresias-cp:8343.	deny-by-default
PEP	Enforcement Plane — the gate Validates api-key + capability token, evaluates policy, forwards verbatim only on allow. Host :8343.	per-call
AUDIT	Signed audit chain — Ed25519 SoulKey Every call signed into the chain, shipped to CP, durable WAL at /data/audit-wal.	tamper-evident
RLS	Row-level isolation — forced at the database Each agent is a soul-svc tenant; FORCE RLS on Cloud SQL means even postgres is bound.	per-tenant
DRIFT	SoulWatch — behavioral quarantine Behavioral drift auto-quarantines the offending agent to the shared postgres store.	automatic

ONE JOB, END TO END

What a single governed request actually traverses.

No agent talks to data directly. The capability token is minted per-agent, the PEP is the only door, and the write lands RLS-isolated. The same path produces the audit record and the usage record as a side effect.



SOURCE · Governed request flow (one job), ARCHITECTURE-FACTS

LIVE PROOF

This is a running instance, not a diagram.

The stack is live on GCP — control, enforcement, runner, and observability planes on one VM, a real Samba-AD directory on another, and a dedicated data tier on Cloud Run + Cloud SQL. Every store is postgres-backed and reboot-durable.

8343 PEP • GOVERNED DATA PLANE	3001 ASPHODEL-UI • MANAGEMENT	1514 PROMTAIL SYSLOG • SIEM INGEST	636 LDAPS • REAL DIRECTORY
--	---	--	--

SOURCE • Port map • GCP project salucainfrastructure / us-central1 • ext 34.133.17.162

Authority lives in the CP. The PEP only ever says yes or no.

CONTROL PLANE — THE AUTHORITY

The CP holds the 367-tenant registry, the enrollment ledger, the audit home, and the quarantine store. Admins provision, list PEPs, and pull reports through `/cp/admin/*` behind X-Admin-Key. It is in-network only — never published.

ENFORCEMENT PLANE — THE GATE

The PEP enrolls to the CP, pulls the 367-agent tenant slice via ETag-cached `HttpRegistryProvider`, and evaluates every call. Policy is deny-by-default; on allow it forwards *verbatim* to that tenant's backend. Nothing else gets through.

Two credentials per call: the tenant api-key and an HS256 capability token the caller mints from its own 64-hex secret. Miss either, and the request never reaches data.

Even a compromised agent cannot read its neighbor.

Isolation is not enforced in application code — it is forced at the database.
Every agent is its own soul-svc tenant, and Cloud SQL runs FORCE RLS on the memory and key tables. The postgres superuser itself is subject to it.

TENANT	Each agent = one soul-svc tenant _soul_tenants + _soul_api_keys, key_hash = sha512(bearer).	367 tenants
FORCE	FORCE RLS on _memories and _soul_api_keys Cross-tenant reads require an explicit SET ROLE service_role.	database-enforced
STRIP	Caddy strips /rest/v1 before PostgREST App-layer JWT gate in front of the RLS-forced table.	multi-container

The audit chain is signed, durable, and reviewable.

Governance's product is evidence. Every governed call is signed into an Ed25519 audit chain with a SoulKey, written to a durable WAL, and shipped to the CP. Behavioral drift trips SoulWatch into automatic quarantine, and everything streams to SIEM.

SIGNED & DURABLE

Ed25519 SoulKey signatures make the chain tamper-evident. Durable WAL at `/data/audit-wal` survives restart. Review and verify through the PEP `/admin/*` analyst console (`pdp.tiresias.watch`).

DRIFT → QUARANTINE → SIEM

SoulWatch detects behavioral drift and auto-quarantines to the shared postgres store. Events flow RFC5424 syslog → Promtail:1514 → Loki, with trajectory / model-baseline / campaign / drift analytics.

The same seam that governs the fleet also proves the ROI.

Every governed call reports usage into tzt_usage, so the ROI board answers the self-host-vs-API question per model. Governance routing favors free / Ollama tiers — and the audit trail shows where the money actually goes.

MODEL	OBSERVED \$/CALL	RELATIVE COST
opus-4.8 (paid)	\$0.19	
sonnet-4.5 (paid)	\$0.03	
deepseek-v4-pro (Ollama)	\$0.002	
gpt-oss:120b (Ollama)	\$0.0015	
Llama-70B (HuggingFace)	\$0.0012	
gemma-4-31b:free	\$0	

CLOSE

Governance is the reason the other 366 can be trusted at all.

Deny-by-default enforcement, two credentials per call, a signed and durable audit chain, database-forced isolation, and automatic drift quarantine — one seam, 367 agents, every department. That is the function this department performs, live, today.

