

zapier.georgelambert.org · Markdown indexes

VERAE TIME × ZAPIER

05 network failures

<site/overview/05-network-failures.md>

5. Local network failures

“Local network” means the operator LAN, SSH to NS1, or a partitioned archive — not Zapier’s cloud.

Failure	What happens	What the customer sees
NATS node unreachable	Client reconnects to another cluster URL; JetStream consumers resume	Wait may return <code>pending</code> ; hook still fires later
All NATS down	Middleware cannot publish <code>jobs.watch</code> ; fleet marks workers unhealthy	503 / pending; no NATS leak to Zapier
One WORM / tree node partitioned	Bloom miss = no packet ; aggregator uses whoever answered	Lookup may miss attachments until the node returns; seal on chain still valid
SSH to a fleet host fails	Spawn fails; fleet places the next replica on another machine	Floor still met if capacity remains on <code>local</code> or another SSH host
Chain <code>api.veraetime.net</code> timeout	Poller retries; then <code>timestamp.timeout</code> event	Wait → pending or failed; async + hook still the recovery path
zappier-edge 402	QuotaExceeded with upgrade URL	Zap step error; no NATS involved
Tunnel to loopback NATS dropped	<code>NATS_URL=nats://127.0.0.1:14222</code> dies; restart <code>nats-tunnel.sh</code>	Workers on NS1 itself still see <code>127.0.0.1:4222</code>

Design choices that make partitions survivable

1. **Archive query is broadcast**, not a shared queue group — a dead node does not steal the message.
2. **Bloom miss is silence** — missing nodes do not send empty errors that look like “hash unknown”.
3. **Zero replies + known puts** is an outage, not a miss (simulator / fleet monitors flag this).
4. **NATS is not on the public NIC** — a WAN blip does not expose 4222.
5. **Idempotent seals** — retrying a Zap after a network error will not double-timestamp.

See fleet RTT (min / avg / p50 / p90) when planning extra tree nodes after a flaky path.