

# Guarded Two-Node Website Resilience System

Technical executive overview of an independent observer paired with a protected-host recovery agent. The system detects DNS, TLS, HTTP, TCP, service, and operating-system failures while explicitly preventing a single failed network path from authorizing disruptive recovery.

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Operating mode</b><br>Fail open by default: ambiguous evidence produces an alert, not a reboot.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   | <b>Decision boundary</b><br>Observer gathers evidence; only the protected host performs local recovery. | <b>Loop prevention</b><br>Escalating backoff, action budgets, cooldowns, persistent history, and lockout.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Protected Host: Guarded Local Recovery</b><br><br><b>Role:</b> make recovery decisions from direct local evidence on the Nginx server.<br><br><ul style="list-style-type: none"><li>- <b>Process layer:</b> systemd restarts Nginx after abnormal process exit.</li><li>- <b>Functional layer:</b> a timer performs a local HTTPS request using the correct hostname and TLS SNI; an external outage alone cannot trigger recovery.</li><li>- <b>Escalation:</b> confirmed failures trigger Nginx restart and retest before reboot is considered.</li><li>- <b>Backoff:</b> repeated failures wait progressively longer before another disruptive action.</li><li>- <b>Budgets:</b> restart and reboot counts are limited within rolling time windows.</li><li>- <b>Cooldown and lockout:</b> reboot cooldown prevents cycling; invalid configuration or exhausted budgets disables automation pending review.</li><li>- <b>Hardware watchdog:</b> systemd services the platform watchdog; a complete OS freeze causes an independent hardware reboot.</li></ul><br><b>Recovery sequence</b><br><br>Local HTTPS failure -> confirmation threshold -> Nginx restart -> local retest -> guarded reboot only after persistent local failure. Inconclusive or unsafe conditions -> alert and lockout. |                                                                                                         | <b>Observer: Independent Domain Watch</b><br><br><b>Role:</b> monitor multiple domains, servers, and TCP services from another Ubuntu host.<br><br><ul style="list-style-type: none"><li>- <b>DNS:</b> validates expected A/AAAA results; local split-DNS and public DNS should be modeled separately.</li><li>- <b>Web:</b> checks reachability, allowed status codes, redirects, response time, and optional page content.</li><li>- <b>TLS:</b> validates hostname and trust chain and warns before certificate expiration.</li><li>- <b>Infrastructure:</b> checks SSH, HTTP, HTTPS, and application ports to isolate host, proxy, and backend faults.</li><li>- <b>Alert control:</b> new failures alert immediately; unresolved incidents re-alert on escalating intervals; recovery notices close the incident.</li><li>- <b>State:</b> records first seen, last seen, alert count, next delay, and detailed failure evidence.</li><li>- <b>Authority:</b> no remote reboot permission by default. A failed observation is evidence, not proof of target failure.</li></ul><br><b>Fault interpretation</b><br><br>SSH and HTTPS fail -> host, power, or network path. SSH works but HTTPS fails -> proxy/TLS listener. Proxy works but backend port fails -> application. Local services work but public URL fails -> DNS, NAT, ISP, or external path. |
| <b>Observation pattern</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <b>Likely interpretation</b>                                                                            | <b>Automatic response</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Local agent healthy; observer cannot reach target                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Observer path, switch, routing, or monitor-node fault                                                   | Alert only; no target reboot                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Local HTTPS fails; Nginx restart succeeds                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Nginx functional/process fault                                                                          | Record recovery; reset counters                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Local HTTPS persists after restart; budgets available                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | Host-local persistent service failure                                                                   | Cooldown-controlled reboot                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Configuration invalid or budgets exhausted                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Unsafe or repetitive recovery condition                                                                 | Lockout; alert; manual intervention                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**Scope:** This is automated monitoring and guarded recovery, not traffic failover or a high-availability cluster. Future extensions may add protected-host heartbeats, an external probe, or quorum-style evidence correlation without changing the fail-open safety model.

Implementation uses Python, systemd, SMTP, TLS validation, TCP/HTTP checks, persistent state, journal logging, Nginx local health verification, and the host hardware watchdog. Production packaging should include guided installation, rollback, diagnostics, signed updates, and per-environment validation.