Monitoring

- Infrastructure Monitoring & Alerting Plan

Infrastructure Monitoring & Alerting Plan

Executive Summary

This document establishes the architecture, service inventory, and phased rollout plan for comprehensive telemetry, uptime monitoring, and alerting across the self-hosted infrastructure (`ul.drheck.dev`) and external nodes (`rng.drheck.dev`).

---

1. Current Infrastructure Inventory

Primary Host (`ul.drheck.dev`)

- **Hardware:** AMD Ryzen Threadripper PRO 5955WX (16 Cores / 32 Threads), 128 GB RAM, 468 GB NVMe (`/`) with extensive storage pools mounted under `/data`.
- **Edge Proxy:** Nginx reverse proxy with SSL termination and domain routing for `*.drheck.dev`.
- **Rootless Podman Quadlet Fleet (`docker-data`, `/home/docker-data/.config/containers/systemd/`):**
  - **Identity & Security:** Authentik (Server, Worker, LDAP), Vaultwarden, Step-CA, Webshell.
  - **Media, AI & Gaming:** Immich (Server + ROCm ML), Funkwhale, Navidrome, RomM (+ MariaDB), Sopro TTS, Demucs Stem Splitter, SubOCR (ROCm MIGraphX).
  - **Productivity & Docs:** Nextcloud + Collabora CODE, BookStack (+ MariaDB), Penpot (Frontend, Backend, Exporter, Postgres, Redis), Vikunja, WIPStudio (+ MinIO).
  - **Infrastructure & Web Apps:** Anchor, Grill Monitor, YOURLS (+ MariaDB), SControl, DeGoog, AudioMass, BentoPDF, Drawpile, Excalidraw, TLDraw, WebRcade, Wick.
- **Native Systemd Services:** Nginx, HAProxy, Unbound, PostgreSQL, Valkey, Ollama, Forgejo, Jellyfin, Plex Media Server, Kavita, Minecraft (`mc-manager` + `minecraft@*`), Transmission-daemon, CrowdSec, Kanji, Sunshine + Gamescope.

External VPS (`rng.drheck.dev`)

- **Hardware:** Debian 12 (1 GB RAM, 16 GB available on `/home` storage mount).
- **Role:** Off-site canary sentinel, external HTTP/SSL prober, and out-of-band alert dispatcher.

---

2. Monitoring Architecture & Topology

```
                    ┌──────────────────────────────────────────┐
                    │          Off-Site VPS (rng.drheck.dev)    │
                    │  - Uptime Kuma (Blackbox & SSL Prober)    │
                    │  - External WAN/DNS/Port Health Probes    │
                    │  - Independent Alert Routing (ntfy/Pushover)│
                    └──────────────────────┬───────────────────┘
                                           │ Probes *.drheck.dev (HTTPS/IPv6/IPv4)
                                           ▼
┌──────────────────────────────────────────────────────────────────────────────────┐
│  Primary Host (ul.drheck.dev)                                                    │
│                                                                                  │
│  [ Telemetry Exporters ]                                                         │
│   ├── node_exporter         (Host CPU, RAM, NVMe I/O, Network, Systemd)          │
│   ├── cAdvisor              (Per-container CPU, Memory, Network, Restart Loops)  │
│   ├── nginx-prometheus      (Request rates, 4xx/5xx error spikes, upstream latencies)  │
│   ├── postgres_exporter     (DB connections, query latency, lock monitoring)     │
│   └── smartctl_exporter     (NVMe wear, drive temperatures, hardware health)     │
│                                                                                  │
│  [ Time-Series Storage & Dashboards ]                                            │
│   ├── VictoriaMetrics       (High-efficiency TSDB, low memory footprint, PromQL) │
│   └── Grafana               (Unified dashboards & visual panels)                 │
│                                                                                  │
│  [ Alert Engine ]                                                                │
│   └── Alertmanager          (Routes internal metrics -> Telegram / ntfy / Matrix)  │
└──────────────────────────────────────────────────────────────────────────────────┘
```

---

3. Core Component Roles

A. External Canary (Uptime Kuma on `rng`)

- **Purpose:** Detects total site loss, ISP drops, power outages, and certificate expiration before users notice.
- **Why `rng`:** Because `rng` is outside the local network, it accurately detects external DNS, IPv6 routing, and gateway failures that local monitors cannot detect.
- **Configuration:** Probes all public subdomains (`wiki.drheck.dev`, `auth.drheck.dev`, `immich.drheck.dev`, `cloud.drheck.dev`, etc.) on 60-second intervals.

B. Host & Container Telemetry (VictoriaMetrics + cAdvisor + Exporters on `ul`)

- **VictoriaMetrics:** Selected over standard Prometheus due to its significantly lower memory footprint, superior compression for NVMe endurance, and drop-in PromQL compatibility.
- **cAdvisor / Podman Exporter:** Continuously monitors all 41 rootless Podman containers (`user@1100.service` cgroup hierarchy), capturing CPU throttling, memory leaks, and container restart loops.
- **node_exporter:** Monitors host-level thread saturation, memory usage, network interfaces (`eth77`), and disk utilization across mounts.

C. Unified Visualization (Grafana on `ul`)

- **Preconfigured Dashboards:**
  1. *Host Overview:* 32-thread CPU load, RAM allocation, NVMe I/O, network throughput.
  2. *Rootless Podman Fleet:* Container status, memory limits, restart counters, per-service resource breakdown.
  3. *Web Traffic & Edge:* Nginx request rates, response latency percentiles (p95/p99), HTTP status distribution (2xx/3xx/4xx/5xx).
  4. *Database Health:* PostgreSQL and MariaDB active connections, buffer hits, query response times.

---

4. Phased Rollout Plan

Phase 1: External Sentinel (`rng.drheck.dev`)

1. Deploy **Uptime Kuma** under `/home/luke/docker/uptime-kuma` on `rng` using rootless Podman.
2. Configure HTTP(s), TCP, and SSL certificate monitors for all public services on `drheck.dev`.
3. Configure notification webhooks (e.g. ntfy.sh, Telegram, or Gotify) for instant push alerts to mobile devices.

Phase 2: Exporter Deployment (`ul.drheck.dev`)

1. Deploy `node_exporter` as a native systemd unit or container (listening on `127.0.0.1:9100`).
2. Deploy `prometheus-podman-exporter` / `cAdvisor` as a rootless Podman Quadlet reading `/run/user/1100/podman/podman.sock` and `/sys/fs/cgroup`.
3. Add `smartctl_exporter` for continuous NVMe drive telemetry.

Phase 3: Time-Series DB & Grafana Stack (`ul.drheck.dev`)

1. Create rootless Podman Quadlets under `/data/docker/monitoring/` linked into `/home/docker-data/.config/containers/systemd/` with:
   - `victoriametrics` (TSDB storage)
   - `grafana` (Dashboard UI)
   - `vmagent` or Prometheus scraping configuration
2. Configure scrape jobs for `node_exporter`, `cAdvisor`, Nginx metrics, and database exporters.
3. Expose Grafana behind Nginx at `monitor.drheck.dev` (secured with Authentik SSO).

Phase 4: Alert Rules & Thresholds

Define critical alert rules in VictoriaMetrics / Alertmanager:

- **Disk Space:** Warning at >80% utilization; Critical at >90% on `/` or any `/data` mount.
- **Service Outage:** Any service unreachable for > 2 probe cycles (120s).
- **Container Crashes:** Container restart count > 3 in a 10-minute window.
- **Host Resource Saturation:** RAM available < 10% or continuous high load average.

- **SSL Certificates:** Alert if certificate validity < 14 days remaining.

Phase 5: Verification & Drills

1. Perform synthetic service termination drill (e.g. test container stop) to verify alert firing and recovery notification.
2. Verify dashboard graphs and metric retention policies.