GOVERNMENT OF BIHAR // NATIONAL INFORMATICS CENTRE (NIC)

Bihar State NOC — Uptime Kuma SLA Architecture

Executive Technical Dossier & Operations Blueprint (State NOC Perimeter)

PLATFORM STATUS
ONLINE // PORT 3001

Executive Summary: To eliminate blind spots in Bihar State's mission-critical e-governance infrastructure, an enterprise-grade synthetic monitoring platform (**Uptime Kuma**) has been deployed on the Bihar State NOC Server (**STATE-NOC-NODE**). The platform runs 24/7 without external cloud dependencies, autonomously verifying web endpoints, SSL health, and micro-latency across state departments (Mines, Agriculture, Transport, and SDC Core) with **sub-minute anomaly detection and zero-touch auto-healing**.

1. KEY EXECUTIVE VALUE PILLARS

Operational Impact

FLEET AVAILABILITY

`100.0% SLA`

Continuous synthetic probing across all mission-critical department portals every 60 seconds.

DATA SOVEREIGNTY

`100% On-Premise`

No portal telemetry or government data leaves the State WAN/SDC boundary. Hosted entirely on STATE-NOC-NODE.

RESILIENCE & RECOVERY

`< 120s Auto-Heal`

Two-tier autonomous watchdog revives the daemon immediately upon server restart or transient disruption.

2. SERVER TOPOLOGY & DEPLOYMENT ARCHITECTURE

State NOC Perimeter

LAYER	COMPONENT	TECHNICAL SPECIFICATION	OPERATIONAL FUNCTION
Host Server	PAT-SHQ-F02-205	Windows Server / Windows 11 (AMD64)	Core Bihar State NOC intranet management node.
Web Gateway	Microsoft IIS 10.0	FastCGI PHP 8.4 Bridge (Port 80)	Delivers existing State NOC Portal and administrative supervisor.
Monitoring Daemon	Uptime Kuma Core	Standalone Node.js 24.16.0 (Port 3001)	Autonomous non-blocking event-driven synthetic probe kernel.
Data Storage	Embedded SQLite 3	Write-Ahead Logging (WAL Mode)	Zero-latency time-series storage for heartbeats, pings, and incidents.
Security / TLS	Native System CA	`--use-system-ca` Engine Flag	Implicitly trusts Indian CCA / NIC root certs installed in Windows OS.

3. CURRENTLY MONITORED MISSION-CRITICAL FLEET

Live Targets

TARGET PORTAL	DEPARTMENT / AUTHORITY	TARGET ENDPOINT	PROTOCOL	INTERVAL	LIVE STATUS
Khanan Soft Bihar	Mines & Geology Dept	`https://[REDACTED-PORTAL].internal/`	HTTPS GET (200 OK)	60s	OPERATIONAL
ISTP Bihar	Agriculture Department	`https://istp.bihar.gov.in/`	HTTPS GET (200 OK)	60s	OPERATIONAL
VLTS Portal Bihar	Transport Department	`https://vltsportal.bihar.gov.in/`	HTTPS (IIS Auth Handshake)	60s	OPERATIONAL
Bihar State NOC Core	NIC Bihar State HQ	`http://STATE-NOC-NODE/portal_monitor.html`	HTTP GET (Internal LAN)	60s	OPERATIONAL
NOC Edge Services	AdityaSec Production Gateway	`https://adityasec32.systems/`	HTTPS API Endpoint	60s	OPERATIONAL

SANITIZED CASE STUDY • ADITYA KUMAR • STATE NOC SURVEILLANCE

How Uptime Kuma Operates & Manager Briefing Guide

Lifecycle of Probes, Autonomous Recovery, and Stakeholder Talking Points

ARCHITECTURE
SELF-HEALING

4. END-TO-END PROBE LIFECYCLE (HOW PROBING WORKS UNDER THE HOOD)

Execution Mechanics

1 Temporal Schedule
Asynchronous timers trigger lightweight non-blocking synthetic requests without spawning OS threads.

2 Synthetic Probe
Performs full TCP handshake, TLS certificate negotiation, HTTP request, and records round-trip latency.

3 Flapping Filter
If a target fails, it marks state "Pending" and retries 2 times. Eliminates false alarms caused by ISP packet loss.

4 Time-Series Storage
Appends ping and status into SQLite (`kuma.db`) with zero locking delay using Write-Ahead Logging.

5 Live WebSocket Broadcast
Pushes telemetry directly to connected NOC video walls and dashboards over Socket.IO without page refreshing.

5. AUTONOMOUS SELF-HEALING WATCHDOG (ZERO-TOUCH HIGH AVAILABILITY)

Dual-Tier Protection

TIER 1: SCHEDULED TASK WATCHDOG

Integrated into the 2-minute Windows Task Scheduler routine (`portal_monitor_daemon.py`). If `CNI-NOC-KERNEL:3001` fails to answer a health probe, the watchdog automatically issues an API start call to resurrect the daemon within **< 120 seconds**.

TIER 2: PASSIVE FASTCGI AUTO-HEAL

The administrative controller (`kuma_service.php`) on Microsoft IIS actively inspects Windows socket tables. Any status request or NOC user visit checks port 3001 and automatically launches `node.exe` if offline.

6. MANAGER BRIEFING & FREQUENTLY ASKED LEADERSHIP QUESTIONS

Key Talking Points

Q1: "Why do we need Uptime Kuma if our departmental web servers are already running?"

Talking Point: A web server running does not mean the website is working for citizens. A web server can be on while the database is disconnected, an SSL certificate is expired, or the application pool is crashed. Uptime Kuma acts as an external synthetic citizen, constantly validating real HTTP status, SSL expiry, and round-trip latency from outside the portal.

Q2: "Does this software put high load or strain on our server (STATE-NOC-NODE)?"

Talking Point: No. Uptime Kuma is optimized for production high-concurrency with minimal footprint. It consumes only **~165 MB of RAM** and less than **0.5% CPU**, enforced with a strict V8 memory ceiling (`--max-old-space-size=512`).

Q3: "What happens if STATE-NOC-NODE is rebooted for Windows Updates?"

Talking Point: Zero manual intervention is required. The two-tier autonomous watchdog checks the port every 2 minutes. As soon as the server boots, the daemon is revived automatically in the background with all 5 monitors running immediately.

Q4: "How do managers and duty officers access the dashboard?"

Talking Point: Simply open `http://CNI-NOC-KERNEL:3001` in any browser across the NOC network, or click the direct **'Uptime Kuma'** button embedded in the header of our primary Bihar State NOC Portal (`http://STATE-NOC-NODE/portal_monitor.html`).

SANITIZED CASE STUDY · ADITYA JAIN · STATE NOC SURVEILLANCE