Kubernetes Automation & Observability

FROM VISIBILITY TO OPERATIONAL CONFIDENCE

Executive Summary

Kubernetes has become a foundational platform for modern applications, but it has also introduced new operational complexity for network and infrastructure teams. While Kubernetes-native tools provide deep platform metrics, they often lack network-aware context and are difficult for NetOps teams to operationalize.

NetBrain extends its automation and observability platform to Kubernetes environments by integrating Kubernetes health, capacity, application, and security signals into the same workflows used for network operations. The result is **Kubernetes observability and automation that fits naturally into Day-2 operations**, without requiring teams to become Kubernetes experts.

What It Is

The NetBrain Kubernetes Automation Library provides automated monitoring and observability for Kubernetes clusters, focusing on:

- Resource health and utilization
- Application stability and availability
- Capacity management
- Security posture

These capabilities integrate directly with the NetBrain platform, allowing Kubernetes signals to participate in automation, diagnosis, visualization, and proactive operations alongside traditional network data.

Rather than operating as a standalone Kubernetes tool, the automation library enables Kubernetes to become first-class operational context within NetBrain's real-time digital twin.

Why It Matters

Kubernetes environments introduce challenges that traditional network and infrastructure tooling was never designed to handle:

- Highly dynamic pods, services, and nodes
- Ephemeral failures that are difficult to correlate
- Resource contention that impacts application performance
- Limited visibility across network, platform, and service layers

As a result, many organizations experience:

- Longer MTTR for Kubernetes-related incidents
- Increased dependency on specialized platform teams
- Gaps between network troubleshooting and application impact

NetBrain addresses these challenges by **bridging Kubernetes operational data with network intelligence**, enabling faster diagnosis and more consistent operations across hybrid environments.

Who Cares

Network Operations (NetOps)

- Need to understand when Kubernetes issues are network-related
- Require visibility without learning Kubernetes internals
- Benefit from automated diagnosis and contextual visualization

Platform & Cloud Operations

- Need continuous insight into cluster health and capacity
- Want proactive detection of instability before incidents occur
- Require automation that integrates with existing workflows

SRE / Reliability Teams

- Care about application stability and resource efficiency
- Need early indicators of failure patterns
- Benefit from correlation across infrastructure layers

Security & Compliance Teams

- Need visibility into Kubernetes security posture
- Want continuous validation of known risk patterns
- Require audit-friendly, repeatable checks

Core Capabilities

Cluster & Resource Health Monitoring

- Node CPU and memory utilization monitoring
- Pod CPU and memory utilization monitoring
- Detection of nodes in NotReady state
- Identification of pending pods caused by resource constraints

Application Stability & Availability

- Detection of CrashLoopBackOff and OOMKilled events
- Monitoring of container restart spikes
- Liveness and readiness probe failure detection
- Comparison of desired vs. available deployment replicas

Control Plane Health

- etcd leader election status and leader change tracking
- API server request latency monitoring
- Controller manager queue and work duration analysis
- Scheduling latency visibility

Capacity Management

- Pod and node memory capacity thresholds
- Node CPU request vs. allocatable capacity monitoring
- Pod CPU throttling and over-provisioning detection
- Persistent volume disk pressure alerts

Security Monitoring

- Validation of ingress controller versions against known CVEs
- Detection of privileged containers running with elevated access

All of these checks are implemented as automated, repeatable logic that can run continuously or on demand.

How NetBrain Approaches Kubernetes Differently

Unlike Kubernetes-native dashboards or metric collectors, NetBrain:

- Integrates Kubernetes signals into **network-led workflows**
- Uses automation instead of static dashboards
- Correlates Kubernetes health with network context
- Enables consistent operations across on-prem, cloud, and Kubernetes

NetBrain does **not** attempt to replace Kubernetes management platforms. Instead, **it operationalizes Kubernetes for teams responsible for end-to-end service availability**.

Example Use Case

Detecting and Diagnosing Application Instability

A team uses the Kubernetes Automation Library to:

- Continuously monitor pod restarts and CrashLoopBackOff events
- Identify resource pressure causing pod scheduling failures
- Correlate Kubernetes instability with network connectivity paths
- Visualize impact within the NetBrain digital twin
- Trigger follow-up automation or escalation workflows

This approach reduces time spent manually correlating metrics across tools and accelerates root cause identification.

Operational Value

Technical Value

- Faster identification of Kubernetes-related issues
- Reduced dependency on deep Kubernetes expertise
- Consistent diagnostics across environments

Business Value

- Reduced application downtime
- Improved reliability of containerized services
- Lower operational risk as Kubernetes adoption scales

Strategic Value

- Makes Kubernetes operationally accessible to NetOps teams
- Supports hybrid and cloud-first strategies
- Advances NetBrain's vision toward proactive and self-healing operations

Where This Fits In

Kubernetes automation in NetBrain:

- Moving from initial visibility to operational relevance
- Integrating Kubernetes into automation and diagnosis workflows
- Supporting production-scale, Day-2 operations

This represents operational maturity, not a one-time feature addition.

Summary

The NetBrain Kubernetes Automation Library enables organizations to bring Kubernetes environments into their operational workflows with confidence. By combining automated health checks, capacity monitoring, security validation, and network-aware context, NetBrain helps teams move from reactive troubleshooting to proactive Kubernetes operations.