Hawk - UNMS (Unified Network Management System)

Category: Network Performance Monitoring (Q2) V2
Scope: IT and Non-IT Infrastructure Monitoring & Management
Target: Enterprise & Carrier-Grade Networks including North Bound / South Bound Connectivity

Specification & Features supported but not limited to;

1. End-to-End Fault & Performance Monitoring

- Integrated platform supporting network fault and performance monitoring, configuration and change management (NCCM), NetFlow traffic analysis, and dashboard-based reporting with integration capabilities.
- Supports FCAPS framework and comprehensive data visualization.

---

2. Platform Compatibility

- Operates on Linux platforms using open-source databases.
- Fully optimized 64-bit application ensuring efficient server resource utilization.
- Plug-and-play deployment supported.

---

3. Dual-Stack IP and Vendor Independence

- Supports both IPv4 and IPv6.
- Vendor-agnostic monitoring designed for multi-vendor , heterogenous environments.

---

4. Unified Monitoring

- Provides a single platform to monitor networks, servers, applications, and both IT and non-IT IP-enabled devices.

---

5. Scalable Architecture

- Scalable to manage over thousands devices, ensuring future readiness and expandability. 2.5 lacs nodes/devices per device (Hawk)

---

6. Advanced Topological and Path Analysis

- Visual network outage representation on topology maps.
- Historical trend analysis of performance data.
- Multi-hop and hop-by-hop path analysis across on-prem, hybrid, and cloud networks.

- Real-time and historical latency tracking.

---

7. Real-Time Fault Detection

- Near real-time detection and highlighting of anomalies across monitored infrastructure.

---

8. Event Filtering and Correlation

- Includes capabilities for filtering, de-duplication, suppression, and correlation to isolate critical business-impacting events.

---

9. Multi-Level Severity and Notification

- Multiple severity levels with automated event handling.
- Notification through GUI, pop-ups, sound alerts, email, and SMS.

---

10. Rule-Based Alarming System

- Rule engine allows configuration by device group, node, resource, and interface.
- Supports threshold breaches based on average, min, max values.
- Custom alarms, repeat counters, and multiple severity levels supported.
- Custom Thresholds

---

11. Multi-Channel Alerting

- Supports alerts via email, SMS, SNMP traps, batch file execution, pop-up, XML notification, and audio (Buzzer) alerts.

---

12. Traffic Monitoring

- Interface-level traffic utilization tracking.
- Aggregated reports by location, branch, or department.
- Provides min, max, avg bandwidth and throughput metrics.

---

13. Custom Polling Intervals

- Polling frequency adjustable at component/resource/interface level based on criticality.
- Supports sub-second polling intervals.

---

14. Topology Visualization

- Supports various topology views: physical, flat, user-customized, layers, protocols and geo-based maps.

---

15. WAN Monitoring & Link Analysis

- Real-time metrics on latency, bandwidth utilization, and round-trip times.
- Custom threshold configuration and graphical geographic mapping with drill-down capabilities.

---

16. Performance Metrics

- Monitors packet loss, errors, discards, traffic volume, packet count, and response times.

---

17. Infrastructure Health

- Tracks CPU, memory, storage, temperature, fan speed, and power supply across servers and devices.

---

18. Protocol and Service Monitoring

- Supports SNMP, HTTP/S, Ping, SMTP/POP3, WMI, SOAP, REST API, SSH, Telnet, and more.

---

19. Virtualization and Application Monitoring

- Monitors virtual machines, hypervisors, clusters, web/email/database servers, and other application endpoints.

---

20. Syslog Management

- Collects and filters syslogs from devices including firewalls, routers, switches, WLCs, servers, applications, and databases.
- Custom filtering, export, and alert capabilities via email/SMS.

---

21. Flow Capture and Retention

- Captures NetFlow, sFlow, J-Flow, Netstream, IPFIX data from multi-vendor devices.
- No rollups or data loss; supports long-term storage with export formats (CSV, Excel, PDF, HTML, JSON).

---

22. SSL/TLS & Threat Monitoring

- Detects SSL/TLS anomalies including false or expired certificates.
- Compares traffic with known threat signatures (IOC-based and signature-based detection).
- DDoS detection and real-time mitigation reporting.

---

23. Network Traffic Analysis

- Presents traffic usage in a web UI.
- Supports NBAR, CBQoS, and identifies top-consuming users, applications, protocols, countries, ASNs, and routers.

---

24. SLA Monitoring

- SLA definition and breach detection for links, services, and customers.
- Provides breach visibility with configurable thresholds.

---

25. Compliance and Integration

- Supports integration with ITSM tools for ticket automation.
- CLI-based configuration snapshot management, remote firmware upgrades, and vulnerability detection/remediation.
- Session recording and relay for remote CLI sessions.
- Configurable backup schedules and alerting for failed backups.

---

26. Configuration Management

- Tracks configuration changes with version comparisons.
- Approvals for config changes, ITSM integration, and compliance reporting supported.

---

27. IP Address Management

- Centralized management of IPv4/IPv6 address space.
- AD, DHCP, and DNS integration.
- Monitors subnet capacity, IP conflicts, and rogue devices.

---

28. Network Access and Inventory Tracking

- Tracks user login history and access via AD integration.
- Detects new, guest, trusted, and rogue devices.

---

29. System Hardware Requirements

- **Processor:** Dual Intel Xeon 5th Gen or higher
- **Memory:** 64 GB DDR5 ECC (expandable to 128 GB)
- **Storage:** 3×960 GB SSD with RAID 5
- **Power:** Dual redundant hot-swappable PSU
- **Network:** Dual gigabit + Dual 10 Gbps SFP+ (SM fiber)

---

30. Software Compatibility

- **OS Support:** Linux, Windows, macOS, iOS
- **Browser Support:** Chrome, Edge, Firefox, Safari, Opera
- **Database Support:** Oracle, MySQL, PostgreSQL, MS SQL, NoSQL, HANA, Hadoop
- **Cloud Support:** AWS, Azure
- **Deployment:** Public/Private cloud, On-prem, Kubernetes supported

---

31. Reporting and Dashboards

- Online/offline reporting with export in HTML, PDF, Excel, CSV, JSON/XML.
- Custom and scheduled reports with email delivery.
- Dashboards and network diagrams are web-based and Visio-style, drag-and-drop enabled.
- Event and alert management via GUI dashboard.

---

32. Enterprise Enhancements

- RBAC, LDAP, 2FA (Totp), audit trails
- High Availability and disaster recovery support
- Multi-tenant scalability
- Predictive analytics and anomaly detection via AI/ML
- REST APIs with TMF814, etc. SNMP, NetConf, RestConf, GRPC support

- SLA (Mulit-level) monitoring and root-cause analysis

Enterprise compliance and additional enhanced capabilities

✅ AI-Ops Features (AI for IT Operations)

Leverage AI/ML for proactive management, anomaly detection, and predictive analytics:

1. Anomaly Detection & Auto-Healing

- Real-time anomaly detection using ML (e.g., CPU/memory spikes, link failures).
- Auto-remediation via playbooks or scripts (restart services, reroute traffic).

2. Predictive Analytics

- Forecast bandwidth usage and link saturation.
- Predict device failure based on historical trends and logs.

3. Intelligent Alerting

- Noise reduction through alert correlation.
- Event prioritization based on impact score.

4. Root Cause Analysis (RCA) Automation

- AI-based suggestion engine to trace cascading issues.
- Heatmaps for affected systems and probable causes.

5. Intent-Based Networking

- Define desired network outcomes (e.g., “ensure minimum 99.9% uptime”) and let the system adapt configurations automatically.

✅ DevOps Features

Integrate CI/CD pipelines, infrastructure monitoring, and IAC:

1. Configuration as Code (IaC)

- Integrate with tools like Ansible, Terraform for automated config deployment.

2. Pipeline Monitoring

- Observe Jenkins, GitHub Actions, or GitLab CI pipelines.
- Monitor build failures and deploy anomalies.

3. Version Control & Rollback

- Track device config versions and rollback on failures.

4. Integration with DevOps Tools

- API Integration and in-built orchestration with templates.

✅ Connectivity Features: MPLS, GSM, GPRS, Multi-ISP

Enterprise-grade network monitoring requires multi-link, multi-tech support.

1. Link Failover and SLA Monitoring

- Monitor primary (MPLS) and secondary (GSM/GPRS/4G LTE) links.
- ISP-wise link performance tracking and SLA breach alerts.

2. Multi-ISP Routing Insights

- BGP/OSPF route table view per ISP.
- Auto-Routing suggestion engine based on current ISP latency/jitter.

3. SIM/GPRS/GSM Monitoring

- SIM usage dashboards.
- GPRS signal strength and latency tracking.

✅ SD-WAN & SDN Features

Support dynamic WAN policies and virtual networking.

1. Policy-Based Routing Visualization

- Centralized control for site-to-site, site-to-cloud traffic paths.

2. WAN Optimization Insights

- Monitor compression, de-duplication, FEC, application acceleration performance.

3. Virtual Link Performance

- Monitor tunnel health between SD-WAN edges.
- Monitor underlay vs overlay link quality.

4. SDN Controller Integration

- Interface with OpenDaylight, ONOS, or vendor-specific SDN controllers.
- Real-time view of flow-table entries and route maps.

✅ Compliance with IT / Non-IT Monitoring Standards

Be enterprise-compliant across verticals.

1. IT Standards

- SNMP v1/v2/v3, NetFlow/sFlow/IPFIX, Syslog, ICMP, SSH, API-based polling.
- ISO/IEC 9001, 20000, 27001, 27034 & ITILv4 alignment.
- Agile process alignment
- Support for NMS integrations via REST/gRPC.

2. Non-IT Standards

- Support for industrial protocols like Modbus, MQTT, OPC-UA.
- Environmental sensor monitoring (temperature, power, intrusion).
- Railway, power-grid, and smart city standards.

✅ **Other Enterprise-Grade Features**

1. Custom Dashboard Builder

- Business-unit wise views.
- Executive summary dashboards with KPI and SLA stats.

2. Multi-Tenant Support

- Different organizations or departments with strict access separation.

3. Distributed Polling Engines

- Regional polling engines that report to centralized Hawk NMS.

4. High Availability & Disaster Recovery

- Active/Active Or Active/Standby and failover models with DB replication and node syncing.

Core Functionalities

- Unified Dashboard for SNMP, ICMP, HTTP(S), Syslog, Flow, API, and sFlow-based device & service monitoring
- Topology-based device discovery with real-time updates
- Real-time alerting with customizable severity, thresholds, and webhook/email integrations
- Scheduled polling and historical data trend visualization
- Multi-Tenant support with Role-Based Access Control (RBAC)

- Integrated WebSocket channels for live notifications and visualizations

---

AI-Ops & Predictive Intelligence (Enterprise Enhancements)

- Anomaly Detection using ML models (e.g., CPU spikes, bandwidth drifts)
- Predictive Alerts for device health and failure forecasting
- Noise Reduction & Event Correlation engine (deduplicates repeated alerts)
- Root Cause Analysis (RCA) with impact propagation tracing
- Auto-healing Scripts (restart services, reroute traffic, clear cache)
- AI-driven Log Analysis for proactive incident detection
- Learning Engine for dynamic thresholding and auto-baseline creation

---

DevOps-Driven Capabilities

- CI/CD pipeline integration for automated updates/config deployment
- integration for configuration rollbacks and change tracking
- RESTful API access for orchestration with Ansible, Terraform, or custom pipelines
- Webhook support for Slack, Teams, PagerDuty, OpsGenie, etc.
- Containerized deployment via Docker & Kubernetes-ready Helm charts
- Agentless script automation via SSH/SCP or REST APIs

Connectivity & Network Support

- MPLS Monitoring: Label-switched path (LSP) tracking, interface mapping, and latency/jitter monitoring
- GSM/GPRS Device Monitoring: SIM-based gateways, cellular signal quality (RSRP/RSRQ), and data usage
- SD-WAN & Multi-ISP Monitoring:
    - Real-time link failover tracking
    - Latency, jitter, and packet loss metrics per ISP path
    - Application-aware routing visualization
    - SLA-based link selection logic
- SDN Support:
    - OpenFlow controller integration
    - Southbound API monitoring (RESTCONF, NETCONF)

    - Virtual network slice visibility
- VPN/GRE/IPSec Tunnel Monitoring with status and encryption strength alerts

---

Compliance & Interoperability (IT/Non-IT Standards)

- Supports ITU-T, TMF814/854 standards for telecom-grade interoperability
- ISO 27001-aligned access control and audit logging
- 21 CFR Part 11 compliance for pharmaceutical-grade systems
- IEC 62443 for industrial systems and SCADA/PLC integration
- Environmental Monitoring (via Modbus/TCP for temperature, humidity, etc.)
- Vendor-neutral SNMP support with customizable MIB parsers
- Export support in JSON, CSV, XML for third-party integrations

---

Enterprise-Grade Features

- High Availability (HA) & Auto failover support
- Clustered deployment with load balancing
- Multi-Region/Multi-Site visualization support
- LDAP/Active Directory/SSO Authentication support
- Enterprise SLA Dashboard with Mean Time to Resolve (MTTR), Downtime, Uptime %, SLA breach alerts
- Data Retention Policies & Archival Support
- Audit Trails & Forensic-ready logs

Extensibility & Customizations

- Plugin support for third-party integrations (e.g. Microsoft 360, outlook etc)
- Regional Language UI support *
- Worldwide/Nationwide/State-wise/Constituency-wise Geo Map - datacenter visualization – NAVIC, Bharat MAPS integration etc.
- Business Service Mapping to link infra to end-user apps/services