

NetOps.NMF - NetOps Network Monitoring Framework

Solution Overview

NetOps.NMF is highly configurable, flexible, modular and scalable network monitoring framework. It is a DevOps style solution comprised of well-known and best-of-breed open-source software in the field of IT monitoring. These systems are carefully glued together in microservices architecture using container orchestration technologies. With such approach, NetOps.NMF can provide fully customized network monitoring solution, that is tailored-fit for devices and technologies used in the target network environment.

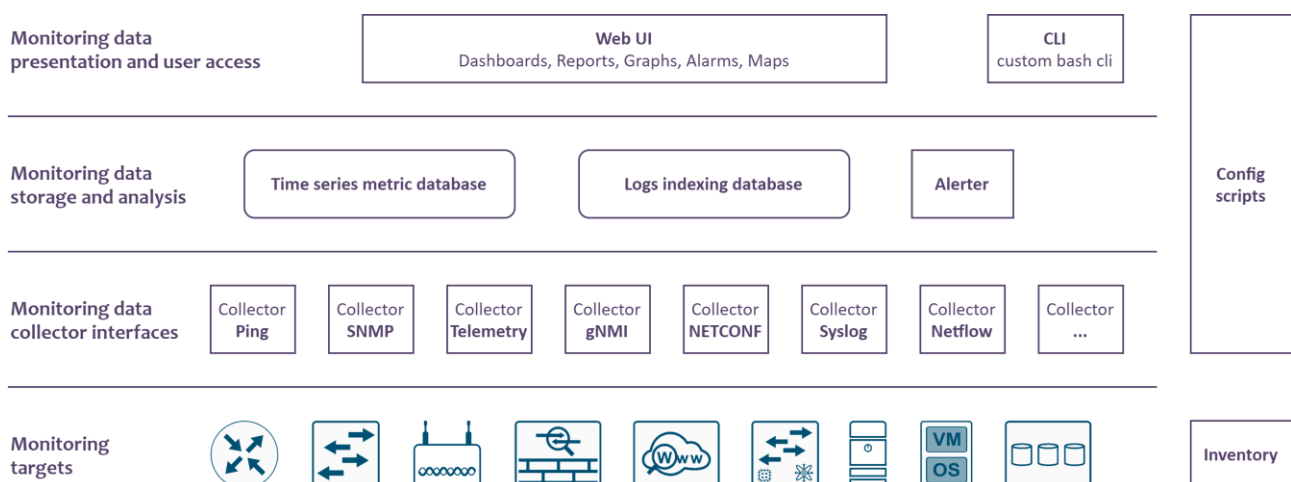
Solution Rationale

Due to exponential network traffic growth in the last decade, network technologies started to evolve toward automation and programmability. The emerging development of SDN and Open Networking technologies brought new network operating systems and programmable interfaces to the reality. To successfully cope with the scalability and versatility requirements of new networks, network departments must align their teams, workflows and mindsets to DevOps principles - their networking counterparts also known as NetDevOps or NetOps.

Single vendor solutions and resulting lock-in are things of the past. Network silos with dedicated network management and monitoring solutions hinder the agility of new services deployment. Separated monitoring applications for campus network, data center, firewalls or Web proxies result in network issue troubleshooting "nightmare". As NetDevOps principles implementation includes network monitoring as one of the most important processes, it requires highly flexible and customizable tools that will fit the needs and specifics of the network.

Solution Architecture

NetOps.NMF enables network operations teams to monitor their various network infrastructure, devices and applications using single system. It integrates various tools in an open and flexible way making it highly configurable and adaptable to any environment, vendor or technology. Since it uses well-known and best-of-breed open-source tools, horizontal and vertical integration with other systems is possible with relatively small development efforts.



All the services that comprise NetOps.NMF are realized as application containers. The system uses container orchestration technology which enables horizontal scaling on multiple physical nodes, while maintaining manageability of the single system.

Collection of the monitoring data is possible from various devices and applications using multiple different collectors. Collectors used by the system include number of well-known collector applications, as well as custom developed daemons where needed. Each collector can communicate with the network devices using one or multiple protocols or interfaces. Support for new protocols and interfaces can be realized by developing custom collectors or developing new input plugins for existing open-source collectors.

Monitoring data in the form of numerical values and logs are stored in time-series database. This provides versatile and easy access to monitoring data with advanced querying capabilities. Other monitoring data in the form of logs which requires advanced indexing are stored in search engine database which is de-facto standard for these kinds of applications.

Web user interface uses well-known state-of-the art general metric visualization tool. It provides advanced querying of data from various databases and sources. Its capability to combine and visualize data from various data sources, makes it as an ideal tool to use as "single pane of glass". It also provides the most comprehensive options for creation of custom dashboards and reports that can fulfil almost any user requirement.

Alarming is realized using a data processing engine for data comparison and correlation. It receives the monitoring data in "real-time" from time-series database and compare it against the set of rules defined in alerting scripts. As a result of comparison, the "Alerter" system will save Alarms in local database. The visualization of alarms can be done using Web UI dashboards or by exporting Alarms to separate dedicated Alarm visualization tool. The Alarm visualization tool can be used for consolidation and deduplication of alarms from multiple sources with simple and effective visualization of the alarms. Additional alerting can be also performed over multiple other destinations (email, webhook or custom scripting).

The NetOps.NMF includes collection of pre-created dashboards that can be reused or adjusted for certain network technologies and needs. It also integrates customizable Linux Bash based CLI (command line interface) for simplified operations and maintenance of the overall solution. All these software components are wrapped-up with custom scripts which translate the configuration from single configuration file and inventory information to all the configuration files and scripts used by every microservice of the framework.

Solution Features and Benefits

Features	Benefits
Monitoring data collection	Data collection with number of well-known collector systems using various protocols: SNMP, NETCONF, Telemetry, gNMI, Syslog, NetFlow, etc.
Monitoring data processing	Configurable regex parsing of syslog messages, provides support for intelligent data ingest. This enables query, search and analysis of CGNAT logs, DHCP accounting logs, RADIUS accounting logs, etc.
Monitoring data storage and retention	Monitoring data storage in time series database and search engine index for long term search, aggregation, analytics and graphing purposes.
Configurable thresholds, alarming and actions	Comparing monitoring data against defined thresholds and rules defined using scripts and alerting to multiple destinations. Closed loop automation can be achieved using local automation scripts or by integration over webhooks or message bus.
Visualization	Using general-purpose visualization tool provides fully customizable dashboards. Extensible visualization plugins provide various ways to present network related monitoring information. Support for multiple data sources enables using the system as single-pane-of-glass for monitoring data from various systems or databases.
Simplified operations	Configurable Bash based CLI provides simplified system operations and maintenance.
High availability	High availability is achievable using at least three servers in cluster and by data replication across databases or database clustering.

Solution Specification

- Network monitoring of multiple vendors
- Microservices container architecture with High Availability support
- Bash based command line interface for OAM
- Supported data collection protocols and formats:
 - Connectivity testing using ICMP Ping
 - SNMP v1, v2c and v3 for metric collection
 - OpenConfig gRPC telemetry
 - JTI over UDP (Juniper Telemetry Interface)
 - NETCONF
 - JSON using REST API
 - Syslog (RFC 3164 and RFC 5424)
 - SNMP Traps v1, v2c and v3
 - NetFlow v5, v9 and IPFIX
- Alerting capabilities to multiple destinations:
 - Email
 - Webhooks, REST API
 - Log, Kafka, MQTT, SNMP trap
 - Alerta, Slack, PagerDuty, OpsGenie
 - Script execution
- Visualizations:
 - Tables
 - Time series graphs
 - Single values statistics
 - Gauge
 - Manually created topology diagrams enriched with monitoring data and thresholds
 - Geographical maps enriched with monitoring data and thresholds

Services and Support

The *NetOps.services* is a company providing consulting services in the field of Network Monitoring and Network Automation. It provides consulting, deployment, configuration, customization and training services for NetOps.NMF solution. The *NetOps.services* provides support services for software configurations, custom scripts and custom code developed by *NetOps.services*. The *NetOps.services* does not provide support services or bug fixing for third-party open-source software used in the NetOps.NMF solution. For this software, users might be able to purchase additional support from respective third-party companies that have developed them.

NetOps.services
info@netops.services
<http://netops.services>

All trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. NetOps.services assumes no responsibility for any inaccuracies in this document. NetOps.services reserves the right to change, modify, transfer, or otherwise revise this publication without any notice.