What is NMIS?

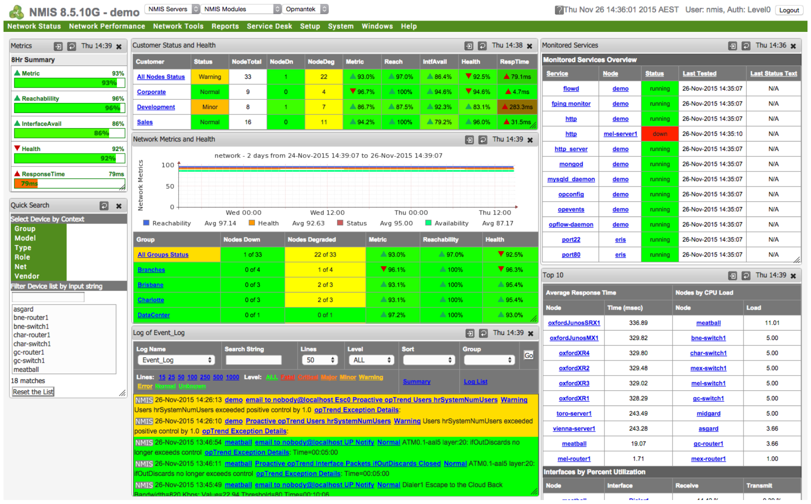
What is NMIS?

NMIS (acronym for Network Management Information System) is an open-source network management system that was first released in 1998. Originally written by Keith Sinclair and with later substantial input from Eric Greenwood, the intellectual property for NMIS was purchased by commercial open source software company Opmantek in early 2011 under a stated commitment to keep "NMIS free and lead the community to rapidly advance the product". NMISv8 was released by Opmantek shortly after and remains free and open source. NMISv9 is currently (as at April, 2020) in the final stages of development. NMIS is a complete network management system which assists with fault, performance and configuration management, providing performance graphs and threshold alerting as well as highly granular notification policies with many types of notification methods.

Additional modules and support provided by Opmantek are available to extend the capabilities of NMIS.

What does NMIS do?

NMIS monitors the status and performance of an organization's IT environment, assists in rectification and identification of faults and provides valuable information for IT departments to plan expenditure and IT changes.



Customer	Status	NodeTotal	NodeDn	NodeDeg	Metric	Reach	IntfAvail	Health	RespTime
All Nodes Status	Warning	33	1	22	▲ 93.0%	▲ 97.0%	▲ 86.4%	▼ 92.5%	▲ 79.1ms
Corporate	Normal	9	0	4	▼ 96.7%	▲ 100%	▲ 94.6%	▼ 94.6%	▲ 4.7ms
Development	Minor	8	1	7	▲ 86.7%	▲ 87.5%	▲ 92.3%	▲ 83.1%	▲ 283.3ms
Sales	Normal	16	0	11	▲ 94.2%	▲ 100%	▲ 79.2%	▲ 96.0%	▲ 31.5ms

Group	Nodes Down	Nodes Degraded	Metric	Reachability	Health
All Groups Status	1 of 33	22 of 33	▲ 93.0%	▲ 97.0%	▼ 92.5%
Branches	0 of 4	1 of 4	▼ 96.1%	▲ 100%	▼ 96.3%
Brisbane	0 of 3	2 of 3	▲ 93.1%	▲ 100%	▲ 95.4%
Charlotte	0 of 3	2 of 3	▲ 93.1%	▲ 100%	▲ 95.4%
DataCenter	0 of 1	0 of 1	▲ 97.2%	▲ 100%	▲ 93.0%

Log Name	Search String	Lines	Level	Sort	Group	
Event_Log		50	ALL			Go

Lines: 15 25 50 100 250 500 1000 Level: ALL Fatal Critical Major Minor Warning Error Normal Unknown Summary Log List

```
NMIS 26-Nov-2015 14:26:13 demo email to nobody@localhost Esc0 Proactive opTrend Users hrSystemNumUsers Warning Users hrSystemNumUsers exceeded positive control by 1.0 opTrend Exception Details:
NMIS 26-Nov-2015 14:26:10 demo Proactive opTrend Users hrSystemNumUsers Warning Users hrSystemNumUsers exceeded positive control by 1.0 opTrend Exception Details:
NMIS 26-Nov-2015 13:46:54 meatball email to nobody@localhost UP Notify Normal ATM0.1-aal5 layer:20: ifOutDiscards no longer exceeds control opTrend Exception Details: Time=00:05:00
NMIS 26-Nov-2015 13:46:11 meatball Proactive opTrend Interface Packets ifOutDiscards Closed Normal ATM0.1-aal5 layer:20: ifOutDiscards no longer exceeds control opTrend Exception Details: Time=00:05:00
NMIS 26-Nov-2015 13:45:49 meatball email to nobody@localhost UP Notify Normal Dialer1 Escape to the Cloud Back Bandwidth=820 Kbps; Value=22.94 Threshold=80 Time=00:10:06
```

Monitored Services Overview

Service	Node	Status	Last Tested	Last Status Text
flowd	demo	running	26-Nov-2015 14:35:07	N/A
fping monitor	demo	running	26-Nov-2015 14:35:07	N/A
http	demo	running	26-Nov-2015 14:35:07	N/A
http	mel-server1	down	26-Nov-2015 14:35:10	N/A
http_server	demo	running	26-Nov-2015 14:35:07	N/A
mongod	demo	running	26-Nov-2015 14:35:07	N/A
mysqld_daemon	demo	running	26-Nov-2015 14:35:07	N/A
opconfig	demo	running	26-Nov-2015 14:35:07	N/A
opevents	demo	running	26-Nov-2015 14:35:07	N/A
opflow-daemon	demo	running	26-Nov-2015 14:35:07	N/A
port22	eris	running	26-Nov-2015 14:35:07	N/A
port80	eris	running	26-Nov-2015 14:35:07	N/A

Average Response Time		Nodes by CPU Load	
Node	Time (msec)	Node	Load
oxfordJunosSRX1	336.89	meatball	11.01
oxfordJunosMX1	329.82	bne-switch1	5.00
oxfordXR4	329.80	char-switch1	5.00
oxfordXR2	329.48	mex-switch1	5.00
oxfordXR3	329.02	mel-switch1	5.00
oxfordXR1	328.29	gc-switch1	5.00
toro-server1	243.49	midgard	5.00
vienna-server1	243.28	asgard	3.66
meatball	19.07	gc-router1	3.66
mel-router1	1.71	mex-router1	1.00

Interfaces by Percent Utilization

Node	Interface	Receive	Transmit

But Why?

NMIS performs multiple network management functions from the OSI Model and International Organization for Standardization FCAPS model, these being - Fault, Configuration, Accounting and/or Administration, and Performance. These metrics provide valuable capabilities and features for fault and performance management, which in turn are useful for many other aspects of network and business management. NMIS is very popular within Telecommunications carrier organizations and Managed Service Providers (MSP's) and is used by IT staff as a key business management and improvement tool.

Features?

The NMIS business rules engine classifies events on their business impact, not just the technical nature. The rules engine is extremely powerful; however, it can be configured in minutes for a network with a small number of devices to hours for networks with large numbers of devices.

NMIS currently supports 10,000 vendors out of the box. The simple set-up allows for network management to occur quickly and can easily integrate new technology.

Operations can see how device performance is impacting the health of a single device, a group of devices or of the whole network. Add opCharts to see these impacts on topological maps.

NMIS measures a baseline of availability, response time and performance, and automatically shows the changes when compared to the previous period baseline. Add in opTrend to intelligently identify outliers to your baselines.

From the largest distributed global environments down to a single office implementation, NMIS handles the data, rules, and presentation. If you add in opHA there is no limit to what you can manage in a single pane of glass.

NMIS allows for customised alert escalation to suit your business. Escalate events based on your organisational structure, operational hours or chain of command. Add opEvents to even automate the event remediation of event management.

How does it work?

NMIS uses a single poll (usually but not necessarily SNMP) for performance and fault data, which reduces the bandwidth of the network management traffic and increase the performance of the network management system. The returning data creates real-time performance monitoring and graphing. When NMIS probes are deployed throughout the network, the network can be managed easily to avoid bottlenecks and enable zero cost redundancy. Both the front and back ends of NMIS are highly extensible and features are easy to add. Custom statics can be gathered for any metric available on a device.

How is it built?

NMIS has been developed in Perl and runs natively on Linux, performing best as a 64-bit multithreaded application. It is commonly used on 64bit Red Hat Enterprise Linux, or other F/OSS equivalents such as CentOS, Debian and Ubuntu. The software is available online as source code (with installer script) or as a Virtual appliance. The Virtual Appliance is compiled as a .OVA image and can be run through any major virtualization product such as VirtualBox or VMWare. It comes with NMIS, Open-AudIT, CentOS and Apache installed and requires no additional configuration.

Licensing

Licensed free of charge under the GNU General Public License. Support contracts provided by Opmantek.

Feature Summary

Performance Management	Faults and Events	Configuration
• Integrated Fault and Performance Management. • Graphs can be produced on the fly. • Graphing period is flexible, graphs can have varying lengths – up to 1 year. • Interactive graphs with drill-down. • Graphing of Interface, CPU, Memory stats. • Interface statistics are returned in utilisation and/or bits per second. • Response time graphed and metrics for health and availability generated from statistics collected. • Threshold engine which send alerts when thresholds are exceeded.	• Integrated Fault and Performance Management. • Sophisticated business rules engine (see heading for Business Rules Engine) • Varying event levels for different device types. • Color coded events, status for at a glance interpretation. • Integrated alerting subsystem • Event levels are set according to how important the device is to the organizations (see Business Rules Engine). • Events are stateful including thresholds, meaning that an event is only issued once. • Integrated logging facility to view NMIS events and syslog messages. • Outage time calculated for each down event • Planned outages can be put in so alerts are not issued.	• Find function which searches interface information for node name, interface name, description, type, IP address, for matching interfaces. • Interface information includes IP address information. • Dynamic handling of ifIndex changes and difficult SNMP interface handling • Checking of changes to device details. • NMIS stores contacts and location information which links to the SNMP sysContact and sysLocation MIBS. • Produces DNS and Host records from the collected IP addressing information • Produces DNS LOC records for "visible" traceroute utilities. • Inventory management –list managed devices by location or type and software revisions
Real-time monitoring	Operational Tools	Management Reporting
• Live base-lining • Live performance monitoring • Live availability monitoring • Live flexible graphs • Live flexible notification conditions • Live alerting	• Diagnostic tools such as ping and traceroute • Produces DNS LOC records for "visible" traceroute utitlities. • And many more	• Powerful out of the box reporting. • Reports to assist in planning and measurements against KPIs. • Live Summary of entire managed environment into a single metric, which indicates reachability, availability, health and response time of all devices being managed. • Summary pages of devices including device information, health graphs, and interface summaries
Extensive list of supported devices	Business Rules Engine	Notification and Escalation
• If it has an IP address, NMIS can manage it and it will leverage the key IP of NMIS. • If it doesn't have an IP address NMIS can probably manage it too! • Support of SNMP v3 v2 and v1 • SNMP traps	• Event levels are set according to how important the device is to the business. • Planned outages – removing alerts during planned outage periods • Policy Based Actions – business actions for people to follow when a fault occurs. • Policy based Escalation • Policy Based Event Handling • Policy based notifications	• Sophisticated business rules engine (see heading for Business Rules Engine) • Escalation subsystem based on device groups which provides high granularity. • Notification engine can handle any "command line" notification method, including email, paging, signs, speakers, etc. • Integrated event manager, allowing a list of active events with an escalation level.

<table>
<tr><td>Distributed Monitoring</td><td>Notification</td><td>Ease of Implementation</td></tr>
<tr><td>• Manage an unlimited number of Nodes
• High level of redundancy
• Single configuration for the system
• Access all information from one place
• Straight forward setup</td><td>• Powerful, out of the box reporting
• Reports for utilisation, outages and more
• Snapshot and dynamic reporting for metrics on all devices and groups of devices.</td><td>• Centralised configuration and storage of information
• Very simple to implement – download the VM</td></tr>
<tr><td colspan="3">Scalability</td></tr>
<tr><td colspan="3">• Performance and Fault data in a single pole
• Extremely efficient monitoring platform
• UI desgined to provide specilized views to assist in “seeing the wood from the trees” in large environments.
• Summary information
• Simple, policy based escalation</td></tr>
</table>