NETWORK MONITORING SYSTEM TOOLS: AN EXPLORATORY APPROACH

Ochin[1], Jugnu Gaur[2]

Faculty of Engineering & Technology, Manav Rachna International University,Faridabad, India

ochin.fet@gmail.com[1], jugnugaur@gmail.com[2]

Phone: 91-129-4198268

***Abstract*--A network is comprises of many things as infrastructure components, network protocols, applications, services, servers, and network infrastructure. Due to the fast development of technologies the complexity level to manage the networks are a challenging job now a days. For large networks it is a tedious task to monitor the entire network manually from different aspects and to correct the faults at its earlier or to prevent effectively the faults to occur. In this paper we have explored three open source network monitoring tools and their comparisons so that as per the requirements individuals or teams can be benefited from.**

Keywords— **Network Monitoring,** network **T**roubleshooting**,** fault detection, QoS, **Open Source Network Monitoring Tools**

I. INTRODUCTION

The term network monitoring describes the use of a system that constantly monitors a computer network for slow or failing components and that notifies the network administrator (via email, pager or other alarms) in case of outages. It is a subset of the functions involved in network management.With the ever-increasing reliance on networkservices for cooperative design applications, there **is** agrowing interest in **an** effective way to monitor networkactivity in order to get the network performance or security situation[1].

A basic method for achieving desired Network reliability and performance is network monitoring [2]where states of a network are frequently monitored.Monitored information can be used to infer quality-of-service(QoS) at a network relating to congestion. Network centric monitoring approaches, where states ofthe network are monitored rather than individual nodes in isolationare important for network management. Network statescan be considered as a collection of nodal states which may correspondto packet losses or delays at the nodes. Network monitorscan reside at all or subset of network nodes. A goal ofnetwork-centric monitoring is to infer states of an entire managednetwork using measurements collected locally at networkmonitors[3].

Steps undertaken in network monitoring are:

1. IT staff configure the tool to monitor critical IT infrastructure components, including system metrics, network protocols, applications, services, servers, and network infrastructure.

2. Configured tool sends alerts when critical infrastructure components fail and recover, providing administrators with notice of important events. Alerts can be delivered via email, SMS, or custom script.

3. IT staff can acknowledge alerts and begin resolving outages and investigating security alerts immediately. Alerts can be escalated to different groups if alerts are not acknowledged in a timely manner.

4. Reports provide a historical record of outages, events, notifications, and alert response for later review.
5. Trending and capacity planning graphs and reports allow you to identify necessary infrastructure upgrades before failures occur.

II. OPEN SOURCE NETWORK MONITORING TOOLS

Here we are exploring three open source network monitoring tools:

A. NAGIOS

Nagios is a powerful monitoring system that enables organizations to identify and resolve IT infrastructure problems before they affect critical business processes[5].

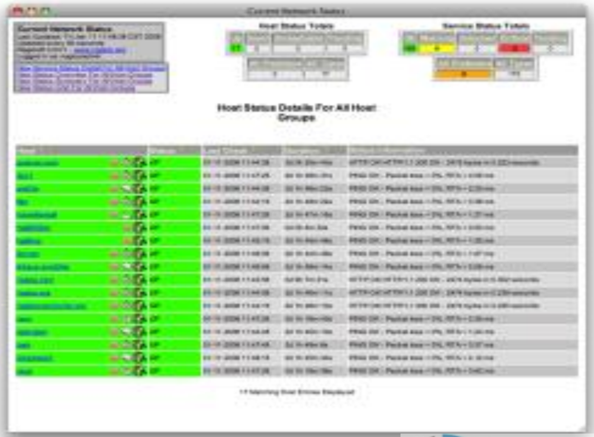


Figure 1: Host Status Details for all host groups

Features of Nagios

◊ Comprehensive Monitoring
◊ Capabilities to monitor applications, services, operating systems, network protocols, system metrics and infrastructure components with a single tool
◊ Powerful script APIs allow easy monitoring of in-house and custom applications, services, and systems Visibility
◊ Centralized view of entire monitored IT infrastructure
◊ Detailed status information available through web interface
◊ Fast detection of infrastructure outages
◊ Alerts can be delivered to technical staff via email or SMS
◊ Escalation capabilities ensure alert notifications reach the right people
◊ Problem Remediation
◊ Alert acknowledgments provide communication on known issues and problem response
◊ Event handlers allow automatic restart of failed applications, services, and services
◊ Proactive Planning
◊ Trending and capacity planning addons ensure you're aware of aging infrastructure
◊ Scheduled downtime allows for alert suppression during infrastructure upgrades
◊ Effective Reporting
◊ Availability reports ensure SLAs are being met
◊ Historical reports provide record of alerts, notifications, outages, and alert response
◊ Third-party addons extend reporting capabilities
◊ Multi-Tenant Capabilities
◊ Multi-user access to web interface allows stake holders to view infrastructure status
◊ User-specific views ensures clients see only their infrastructure components
◊ Extendable Architecture
◊ Integration with in-house and third-party applications is easy with multiple APIs
◊ Hundreds of community-developed addons extend core Nagios functionality
◊ Stable, Reliable, and Respected Platform
◊ Over 10 years of active development
◊ Scales to monitor thousands of nodes
◊ Failover capabilities ensure non-stop monitoring of critical IT infrastructure components
◊ Multiple awards, media coverage and recognition prove Nagios' value
◊ Vibrant Community
◊ An estimated 1 million+ users worldwide
◊ Active community mailing lists provide free support
◊ Hundreds of community-developed addons extend Nagios' core functionality
◊ Customizable Code
◊ Open Source Software
◊ Full access to source code
◊ Released under the GPL license

B. OpenNMS

OpenNMS is an enterprise grade network monitoring and network management platform developed under the free software or open source model. It consists of a community-supported, free-software project as well as an organization offering commercial services, training and support.The goal is for OpenNMS to be a truly distributed, scalable platform for all aspects of the FCAPS (includes Faults, Configuration, Accounting, Performance, and Security) network management model, and to make this platform available to both free software / open-source and commercial applications[6].

Features

⊕ Service polling - determining service availability and latency, including distributed measurement of availability and latency, and reporting on the results
⊕ Data collection - collecting, storing and reporting on data collected from nodes via protocols including SNMP, JMX, HTTP, Windows Management Instrumentation, JDBC, and NSClient
⊕ Thresholding - evaluating polled latency data or collected performance data against configurable thresholds, creating events when these are exceeded or rearmed
⊕ Event management - receiving events, both internal and external, including via SNMP traps
⊕ Alarms and automations - reducing events according to a reduction key and scripting automated actions centered around alarms
⊕ Notifications - sending notices regarding noteworthy events via e-mail, XMPP, or other means
⊕ Other Important aspects of OpenNMS
⊕ OpenNMS is an award winning network management application platform with a long track record of providing solutions for enterprises and carriers.
⊕ While the features list is long and constantly growing, they can be divided into four main areas.

Figure 2 shows the graphs of OpenNMS for HTTP Response Time and SMTP response time.Figure 3 dispalys a view of OpenNMS dashboard.

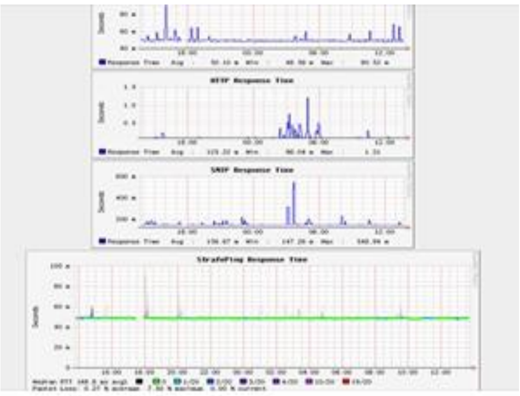
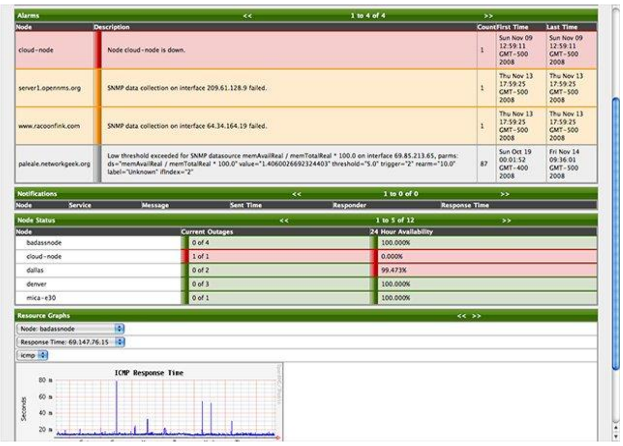


Figure 2:OpenNMS SNMP Graphs: HTTP Response Time, SMTP Response Title



Alarms	<<	1 to 4 of 4	>>	
Node	Description	Count	First Time	Last Time
cloud-node	Node cloud-node is down.	1	Sun Nov 09 12:59:11 GMT-500 2008	Sun Nov 09 12:59:11 GMT-500 2008
server1.opennms.org	SNMP data collection on interface 209.61.128.9 failed.	1	Thu Nov 13 17:59:25 GMT-500 2008	Thu Nov 13 17:59:25 GMT-500 2008
www.racoonfink.com	SNMP data collection on interface 64.34.164.19 failed.	1	Thu Nov 13 17:59:25 GMT-500 2008	Thu Nov 13 17:59:25 GMT-500 2008
paleale.networkgeek.org	Low threshold exceeded for SNMP datasource memAvailReal / memTotalReal * 100.0 on interface 69.85.213.65, parms: ds="memAvailReal / memTotalReal * 100.0" value="1.4060026692324403" threshold="5.0" trigger="2" rearm="10.0" label="Unknown" ifIndex="2"	87	Sun Oct 19 00:01:52 GMT-400 2008	Fri Nov 14 09:36:01 GMT-500 2008

Notifications		<<	1 to 0 of 0	>>	
Node	Service	Message	Sent Time	Responder	Response Time

Node Status	<< 1 to 5 of 12 >>	
Node	Current Outages	24 Hour Availability
badassnode	0 of 4	100.000%
cloud-node	1 of 1	0.000%
dallas	0 of 2	99.473%
denver	0 of 3	100.000%
mica-e30	0 of 1	100.000%

Resource Graphs << >>

Node: badassnode

Response Time: 69.147.76.15

icmp

Figure 3: OpenNMS Dashboard

C. PANDORAFMS

Pandora FMS (for *Pandora Flexible Monitoring System*) is software solution for monitoring computer networks. Pandora FMS allows monitoring in a visual way the status and performance of several parameters from different operating systems, servers, applications and hardware systems such as firewalls, proxies, databases, web servers or routers.

Pandora FMS can be deployed in almost any operating system. It features remote monitoring (WMI, SNMP, TCP. UDP, ICMP, HTTP) and it can also use agents. An agent is available for each platform. It can also monitor hardware systems with a TCP/IP stack, such as load balancers, routers, network switches, printers or firewalls.

Pandora FMS has several servers that process and get information from different sources, using WMI for gathering remote Windows information, a predictive server, a plug-in server which makes complex user-defined network tests, an advanced export server to replicate data between different sites of Pandora FMS, a network discovery server, and an SNMP Trap console.Released under the terms of the GNU General Public License, Pandora FMS is free software[7].

Pandora FMS contains a long list of features including the following highlights.

∇ A new Web console for smartphones.

∇ Better dataserver performance.

∇ More powerful software agents (cron modules, conditional execution, concurrent checks, value propagation and more).

∇ Custom charts from SQL queries in reports.

∇ IPv6 support for ICMP and SNMP modules.

∇ Creation of specific tabs for extensions and a new extension manager.

∇ Support for group hierarchy and new topology maps.

∇ Automatic capture of Agent IP address.

∇ Sound alerts in the web console.

∇ New ReconScript mode for recon server, to use custom scripts to create dynamic monitoring information. A SNMP reconscript is the first application.

∇ Added fullscreen mode in GIS Maps.

∇ Vastly improved massive operations and command line interface.

∇ Special version of software agent for WinNT4.

∇ Implemented UDP server for AGENT REFRESH operation on Unix Agents.

∇ Added the "standby" mode to the alerts, integrated in the new flow of event management.

∇ Improved interface for policy management, including management from command line, policy exclusion list, queue management and much more.

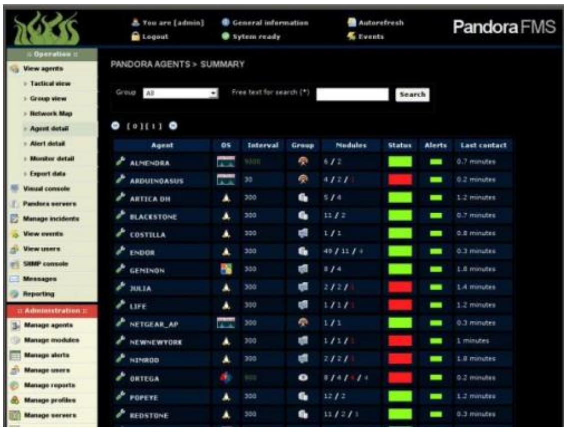
∇ Baseline graphs in HTML, XML and PDF reports.

∇ Distribution and synchronisation of file collections with software agents.

∇ Support for complex scripts in PDF reports (Japanese, Arabic, Hebrew...)

∇ New network maps with group and policy views and the ability to save them.

∇ External authentication for LDAP, ActiveDirectory and other Pandora/Babel/Integria server.



PANDORA AGENTS > SUMMARY

Group All Free text for search (*) Search

[0][1]

Agent	OS	Interval	Group	Modules	Status	Alerts	Last contact
ALMENDRA		300		6 / 2	🟩	🟩	0.7 minutes
ARDUINOASUS		30		4 / 2 / 1	🟥	🟩	0.2 minutes
ARTICA DH		300		5 / 4	🟩	🟩	1.2 minutes
BLACKSTONE		300		11 / 2	🟩	🟩	0.7 minutes
COSTILLA		300		1 / 1	🟩	🟩	0.8 minutes
ENDOR		300		49 / 11 / 4	🟩	🟩	0.3 minutes
GENINON		300		8 / 4	🟩	🟩	1.8 minutes
JULIA		300		2 / 2 / 1	🟥	🟩	1.4 minutes
LIFE		300		1 / 1 / 1	🟥	🟩	1.2 minutes
NETGEAR_AP		300		1 / 1	🟩	🟩	0.3 minutes
NEWNEWYORK		300		1 / 1 / 1	🟥	🟩	1 minutes
NIMROD		300		2 / 2 / 1	🟥	🟩	1.8 minutes
ORTEGA		300		8 / 4 / 4 / 4	🟥	🟩	0.2 minutes
POPEYE		300		12 / 2	🟩	🟩	1.2 minutes
REDSTONE		300		11 / 2 / 1	🟩	🟩	0.3 minutes

Figure 4: Pandora Agents Summary

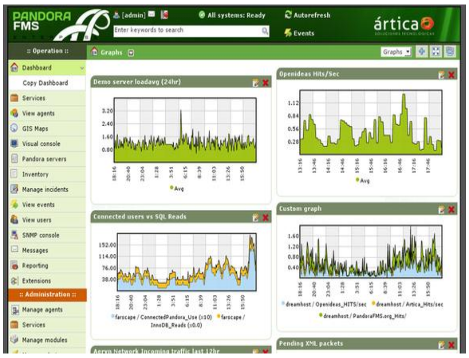


Figure 5:Enterprise dashboard: Average demo server load, connected users, hit/sec,Custom graphs

COMPARISIONS

Here we are representing the comparisons among three open source network monitoring systems with respect to different aspects.

TABLE 1

Name	SNMP	Syslog	Plugins	Triggers / Alerts	WebApp	Distributed Monitoring
OpenNMS	Yes	Yes	Yes	Unknown	Yes	Supported
Nagios	Via plugin	Yes	Yes	No	Via plugin	Supported
Pandora FMS	Yes	Yes	Yes	Yes	Yes	Supported

TABLE 2

Name	IP SLA Reports	Logical Grouping	Trending	Trend Prediction	Auto Discovery	Agent
OpenNMS	Yes	Yes	Yes	Yes	Full Control	Yes
Nagios	Via plugin	Via plugin	Yes	Yes	Full Control	Yes
Pandora FMS	Yes	Yes	Yes	Yes	Full Control	Yes

TABLE 3

Name	Inventory	Data Storage Method	License	Maps	Access Control	IPv6
OpenNMS	Limited	JRobin, PostgreSQL	GPL	Yes	Yes	Limited
Nagios	Via plugin	Flat file, SQL	GPL	Yes	Yes	Yes
Pandora FMS	Yes	MySQL	GPLv2	Yes	Granular	Yes

SLAs	is a feature included in the Cisco IOS Software that can allow administrators the ability to Analyze IP Service Levels for IP applications and services
SNMP	Simple Network Management Protocol is an "Internet-standard protocol for managing devices on IP networks.
Syslog	is a standard for logging program messages It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them.
Logical Grouping	Support arranging the hosts or devices it monitors into user-defined groups.
PostgreSQL	is a relational database that OpenNMS uses to store information about devices on the network, as well as information about events, notifications and outages.
Trending	Provide trending of network data over time.
Trend Prediction	The software feature algorithms designed to predict future network statistics
Auto Discovery	The software automatically discover hosts or network devices it is connected to
Agent	The product rely on a software agent that must run on hosts it is monitoring, so that data can be pushed back to a central server.
Plugins	Architecture of the software based on a number of 'plugins' that provide additional functionality.
Triggers/Alerts	Capable of detecting threshold violations in network data, and alerting the administrator in some form.
Distributed Monitoring	Able to leverage more than one server to distribute the load of network monitoring.
Inventory	Keeps a record of hardware and/or software inventory for the hosts and devices it monitors.
Maps	Features graphical network maps that represent the hosts and devices it monitors, and the links between them.
Access Control	Features user-level security, allowing an administrator to prevent access to certain parts of the product on a per-user or per-role basis.
IPv6	The Internet operates by transferring data in small packets that are independently routed across networks as specified by an international communications protocol known as the Internet Protocol. Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP) that is designed to succeed Internet Protocol version 4 (IPv4).

ACRONYMS/DEFINITIONS

CONCLUSIONS

As network monitoring is essential to find, prevent faults, network failures and performance related issues. Although there is lots of network monitoring tools available now a days. Here we have analyzed and compared three open source tools. Due to open source, these tools are also reducing the cost to company and detailed features presented here will help the teams to choose one that can worthwhile to utilize.

REFERENCES

[1] Bo Yang, Yi Li, Yuehui Chen, Runzhang Yuan', A Flow-based Network Monitoring System Used for CSCW in Design, The 9th Intemational Conference on Computer Supported Cooperative Work in Design Proceedings.

[2] R. Caceres, N. G. Duffield, J. Horowitz, and D. Towsley, "MulticastbasedInference of Network-Internal Loss Characteristics," *IEEE Trans.Inform. Theory*, pp. 2462–2480, Nov. 1999..

[3] I. Widjaja and A. Elwalid, "MATE: MPLS Adaptive Traffic Engineering,"IETF Draft, 1999.

[4] Chuanyi Ji, Anwar Elwalid, Measurement-Based Network Monitoring andInference: Scalability and Missing Information, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 20, NO. 4, MAY 2002.

[5] http://www.nagios.org

[6] http://www.opennms.org

[7]http://www.pandorafms.org