OpenNMS

Kevin Breit

OpenNMS is an open source network monitoring system written in Java licensed under the GPL.

www.opennms.org

Supports monitoring of both network devices (switches, routers) as well as servers and the services which run on them (ex. SSH, HTTP, etc.).

OpenNMS has been used to monitor 80,000 devices according to opennms.org.

Minimum Requirements

- 1 GHz processor
- At least 256 MB RAM, 512 recommended
- 200 MB disk space for program files plus configuration data and interface data (2 MB each)

Installation

- Recommended to use distribution based binaries

Software Requirements

- Java
- PostgreSQL
- JICMP

Getting Started

Start using standard init.d commands.

Log into web interface using http://hostname:8980/opennms/. Be sure holes are poked in firewalls for external access.

By default username and password are admin.

Host Discovery

Discovery finds devices to add to monitoring queue.

Discovery can be configured to use either host based or IP ranges.

Note: OpenNMS uses ICMP pings to do discovery. Gateways often block pings so automatic range discovery may be challenging in this situation. Best I could tell, SNMP sweeps are not an option, but it could possibly be done. Alternative is to hard code interfaces.

Wait...what's an interface?

Interfaces

An interface is an IP address to monitor.

A switch or router with multiple IP addresses assigned to it will show up as multiple interfaces.

OpenNMS can detect whether a server is down based on its interface.

Nodes are made up of interfaces. What is a node?

Nodes

Nodes are devices. Servers, desktop computers, network equipment. They're all nodes.

Configuration

Web Interface

- Pretty good
- Cannot do all configuration and utilize all features through the web interface

Configuration Files

- XML based
- Human readable
- Relatively well documented

This presentation focuses on the web component.

SNMP

SNMP is a common network protocol which pulls system statistics from a device.

Configuration for SNMP is done via snmp-config.xml

Set public string, private string, and IP address ranges to poll SNMP settings.

Examples of data SNMP pulls in OpenNMS:

- Hostname
- Interface usage statistics
- Hard drive usage
- Memory consumption
- Much much more

Net-SNMP is a common software package to allow a Linux device provide SNMP statistics.

Service Monitoring

Monitor not only servers, but the services running on the server. OpenNMS supports a whole lot of services (

Ex. Is HTTP running on 10.1.25.12 on ports 80 and 443?

Event Notification

Monitoring and notification is the heart of a Network Monitoring System.

What is going on in my network and on my servers?

If something bad is happening, I need to know.

Notifications are comprised of a few components:

- Event - Something occurs
- Threshold - Event occurs within a certain range
- Notification - Contacts are notified
- Escalation - Secondary contacts are notified if primary contact doesn't acknowledge event

Kinds of Events

- Network interface is down
- Path to destination is down
- Server CPU is pegged
- Hard drive space reaches a certain level of consumption

OpenNMS is a very powerful application that a simple presentation can't begin to scratch.

Q&A