Open-Source Network Monitoring Software

Network monitoring need not be the province of expensive commercial software. There are many open-source free packages entirely capable of doing the job. We examine 15 of them.

By Roger Burton West
Network Operations
Team Leader

Many organisations want to keep track of machines on their networks; if a service fails, the relevant people should be informed quickly. There is a wide range of commercial software available to do this: HP OpenView, Patrol and Netcool / Omnibus are among the better-known packages. However, these are all very expensive, and tend to require highly-specified machines as dedicated monitoring servers.

The free-software community has produced a number of programs which serve the same task. While they tend not to have such slick graphical interfaces as the commercial offerings, they are generally much less demanding in terms of system resources, typically not even requiring a dedicated server but able to share a machine with other software. They also tend to be more open and extensible than the commercial packages, which is a boon when monitoring your own custom-written services. All the packages described here are supplied in source form, and will run on Linux, FreeBSD, and in most cases Solaris. All are set up by editing text-based configuration files, rather than by a graphical interface.

One important distinction must be drawn between local monitoring of a remote service (such as connecting to a Web server and verifying that it is responding normally) and remote monitoring of a remote service (a process on the server checks available disk space and reports it to the central monitor). This latter is obviously very useful, but is not widely offered; systems that do offer it tend to pay little attention to security, which can cause problems when the servers to be monitored are accessible from the Internet.

NOCOL

NOCOL (Network Operations Centre On-Line) has been in development for some years, and provides a fairly comprehensive set of tests. Development has been slow of late, though it is still active. Most testing of Internet services will be carried out via portmon, which connects to specific ports, sends text and monitors responses. SNMP monitoring is available, but can be rather troublesome to set up.

The principal output is a console application, but Web pages can also be generated; these allow the addition of notes to machines with problems, but not changes to monitoring. Driving a paging system is easily achieved. Remote monitor extensions exist for a range of systems, but again can be troublesome to set up, and security is minimal. There is no network hierarchy, so a router failure leads to a large number of simultaneous alerts. The system must be restarted to add new monitors. Testing is done in parallel for most monitors. The current version is 4.3.

Netsaint

Netsaint (no connection to the SATAN / SAINT security toolkits) is a thorough, expandable system. It comes with an impressive array of monitors (“plug-ins”), which are developed separately from the core code. The range of tests is large, including databases, SNMP, and even games servers; setup of all of these is extremely easy, and a new user can get a working monitor configuration up and running in a couple of hours even on a medium or large network.

Principal output is Web-based, but read-only. To change configuration, setup files must be edited and the monitors restarted. Scalability is fair. Third-party software is available to allow execution of monitoring packages on remote machines. The supplied remote monitor extensions use authentication and strong encryption to secure system data in transit and prevent external access even on non-firewalled systems. There is no console output, but the Web output is usable on text-mode browsers.

The current development code allows for thorough authentication and complex data restriction, making general access to the monitoring Web pages a reasonable proposition. This version also offers parallel testing, which the current formal release does not.

Probably the best feature of Netsaint is the event handler system; this can be used to attempt to restart services that have failed without requiring human intervention. Combined with ssh and suitable key distribution, this is an extremely powerful tool. Network hierarchy is supported for hosts, but not for services on those hosts. The current version is 0.0.4 (0.0.5alpha).

Big Brother

Big Brother is the last of the three “major” monitoring packages. Its output is exclusively Web-based, and dependent on a graphical browser; console browsers are not sufficient. Since it also contains a lot of animated GIFs, it will tend to slow down most browsers; however, where eye candy is a requirement it does a better job than the other, more utilitarian packages reviewed here. The supplied range of monitors is reasonably good, covering most of the standard services, though not SNMP or games. Testing is done in parallel, but there is no hierarchy support and the system must be restarted to add new monitors.

Its remote monitoring is comprehensive and, unlike most of the monitoring packages, includes clients for NT systems. However, remotely-monitored information is exposed to anyone who can connect to the relevant port, as there is no authentication, encryption or IP-based security. BB does have a fully-featured notification system, including acknowledgement and escalation, which is probably the best of any of the programs considered here. Unlike the other packages with Web output, it can drive a remote display server rather than requiring a Web server on its own platform (though this traffic is not encrypted or secured, leading to the possibility of a range of interesting third-party attacks).

Unlike all the other programs mentioned here, which are genuinely free software, BB requires a hefty licence fee for commercial use. This outdated scheme is probably the main reason it is not more popular. The current version is 1.4b.

Mon

Mon is a general-purpose monitoring package, written entirely in Perl. It is highly extensible, and as well as comprehensive built-in SNMP polling can be configured to respond to SNMP traps (or other remotely-generated events). Supplied monitors cover all standard services, and a number of less usual ones.

There is no supplied remote testing, but this can of course be added easily through the modular monitor system.

Mon offers parallel testing with hierarchy support, and has output via Web, console, email or pager software (with a variety of customisable Web interfaces available). It must be restarted to add new services. Services can easily be dropped temporarily from testing via a command-line or Web client, a feature not shared by most of the other programs mentioned here. The current version is 0.38.18.

Angel Network Monitor

Angel is a simple set of Perl programs to check connectivity. It is extensible with little difficulty, and this is a good thing, since the included monitors only check for TCP connectivity, ping, and disk / load via rsh or ssh. No state-change information is maintained; each (cronned) invocation starts afresh. Testing is serial, and no hierarchy is supported. Output is via Web only; no other interface is supplied. The current version is 0.7, but it’s not under active development.

> *“Netsaint appears the best package; it is easy to set up quickly, and has a comprehensive monitor set. However, the lack of parallelising in the current release is a problem.”*

Autostatus

Autostatus is a fast, parallel, hierarchy-based parallel system checker. Output is by Web or email, and email-to-pager software can easily be attached to this. Restarts are required for new services. Testing is by ping or tcpcheck. As in the case of Angel, this offers slightly less functionality than testers written for a specific service. No SNMP or remote monitoring is available, and the system is not designed to allow for its addition. The current version is 1.2beta; again, it's not under active development.

The Event Monitor Project

The Event Monitor Project relies entirely on remote monitoring, and does not attempt to test any functions directly from the monitoring server. While it is very lightweight, the requirement for client software installation (and the lack of security) can cause problems. By default, it monitors disk space, specific processes, kernel logs and network services. It has no hierarchical structure available, requires a restart to add new services, but is extensible to include other remote monitors.

MARS

MARS is written entirely in Java, with the performance, resource requirement and compatibility problems that implies. It has a remote monitoring tool, SPOTS; however, this has no protection from unauthorised access. Supplied monitors are reasonable, but do not include NNTP, telnet or DNS testers. No network hierarchy is available, and the system must be restarted to add new monitors. Output is only available through the Java application, rather than via Web or console access; thus all users must be logged in to the monitoring server itself. No paging support is available.

Netup

Netup is an ICMP reachability tester; it does not support other tests, nor does it support a hierarchical system. However, uniquely among the programs considered here, it does support restarts without loss of state information. Output is via an X11/Tk interface only, but Perl code can be added to the configuration file to send email or take other action on state changes. Note that the main documentation is supplied only in French, though many pages are available in English. The current version is 1.2; not under active development.

OverCR

OverCR is a strictly local monitoring system, written in Perl. It can collect a very wide array of information (disk space, uptime, load, TCP connection status, process data), but has no way of passing this to the outside world. It is best used in combination with one of the other monitoring packages considered here - both Netsaint and Big Brother come with OverCR monitors, and it can easily be combined with ssh for more secure remote polling. The current version is 1.49.08.

> *"Open-source packages tend to be more open and extensible than commercial packages, which is a boon when monitoring your own custom-written services."*

Spong

Spong is a deliberately simple monitoring package written in Perl. It handles both local and remote monitoring, and can output via a Web interface, to command-line tools or by email. Remote monitoring relies on the remote client program sending status updates to the monitoring server; while this removes a large part of the security risk, it does require more thorough configuration of remote machines than might otherwise be needed. Spong allows disabling of service monitoring during extended outages, but does not support hierarchies or parallelised local tests. Spong is fairly easily extensible; a modular interface is supplied, but few examples are given, and the built-in monitors use a separate interface. The current version is 2.6.

PIKT

PIKT is a heavyweight monitoring and remote management tool. It is based on a scripting language, which is optimised for remote distribution of files to groups of heterogeneous platforms. PIKT is somewhat demanding and therefore not an “out-of-the-box” solution to the network monitoring problem. With this in mind, though, PIKT can handle parallel checks very easily, does not require monitor restarts, and can deal with hierarchies; it can generate Web pages, email messages, or drive pager software. It can also be used to maintain consistent access lists and configuration files across multiple platforms. The current version is 1.8.2; not under active development.

JMon

JMon is a remote monitoring package which reports CPU, memory and swap on remote machines. Output is via console only, and configurability is very low. Security is also somewhat poor, with no encryption included or easily added. The current version is 0.3.1; not under active development.

Sysmon

Sysmon is a general-purpose TCP-based tool which supports network hierarchies. Documentation is very scanty, parallel checks are not available, and restarts are required to update the configuration. Checks are not modular, and addition of new monitors will require modification of the source code of core modules. Output is to a console or via email / pager; there is no Web interface. The current version is 0.82.3; not under active development.

NocMonitor

NocMonitor is designed specifically for use on small networks (up to 90 hosts or so). Installation is quick and comparatively painless. Output is via HTML or a Tk application; alerts can be sent by email or other configurable command. Extensibility is good, with the existing checks using a standard interface. Parallel checks are not available, and hierarchies are not supported, but in small networks of the type envisioned this is not necessarily a major problem.

Conclusion

Overall, Netsaint appears the best package; it is easy to set up quickly, and has a comprehensive monitor set. However, the lack of parallelising in the current release is a problem. While the development code is reasonably stable, other changes render upgrading a significant task. NOCOL is also easy to set up, and does offer parallel checking, though the command syntax is somewhat less intuitive. The Web interface feels somewhat cumbersome. mon is also of interest; there are several third-party Web interfaces available, and customising them is easy. However, configuration (even with M4 assistance) is not as convenient as it might be.

The other packages are best used for specific purposes:

- OverCR: as a remote monitor to be plugged into other packages.
- Netup: if only host reachability is important.
- The Event Monitor Project: if hosts are behind a firewall and extensive information is required about them.
- PIKT: if development time is plentiful and many custom tests are required, or a full management system is being set up.
- NocMonitor: for a small network for which monitoring is an urgent requirement.
- Big Brother: if an attractive interface is needed quickly and the commercial-use licence fees are not a concern.

PCNA

Web References

NOCOL
www.netplex-tech.com/software/nocol/

Netsaint
www.netsaint.org

Big Brother
maclawran.ca/sean/bb-dnld/

mon
www.kernel.org/software/mon/

Angel Network Monitor
www.ism.com.br/pagani-ni/angel/

Autostatus
www.angio.net/consult/autostatus/

The Event Monitor Project
www.gsyc.inf.uc3m.es/assman/em/

MARS
www.altara.org/mars.html

Netup
www.pasteur.fr/units/sis/netup/

OverCR
www.molitor.org/overcr/

Spong
monsters.org/pub/spong/

PIKT
pikt.uchicago.edu/pikt/

JMon
www.dsp.sun.ac.za/jjb/jmon/

Sysmon
www.sysmon.org/

NocMonitor
www.nocmonitor.net/

New Reviews from Tech Support Alert

Anti-Trojan Software Reviews
A detailed review of six of the best anti trojan software programs. Two products were impressive with a clear gap between these and other contenders in their ability to detect and remove dangerous modern trojans.

Inkjet Printer Cartridge Suppliers
Everyone gets inundated by hundreds of ads for inkjet printer cartridges, all claiming to be the cheapest or best. But which vendor do you believe? Our editors decided to put them to the test by anonymously buying printer cartridges and testing them in our office inkjet printers. Many suppliers disappointed but we came up with several web sites that offer good quality cheap inkjet cartridges with impressive customer service.

Windows Backup Software
In this review we looked at 18 different backup software products for home or SOHO use. In the end we could only recommend six though only two were good enough to get our “Editor’s Choice” award

The 46 Best Freeware Programs
There are many free utilities that perform as well or better than expensive commercial products. Our Editor Ian Richards picks out his selection of the very best freeware programs and he comes up with some real gems.

Tech Support Alert
http://www.techsupportalert.com