

IPMONITOR

NETWORK MONITORING TOOL

ipMonitor Corporation's ipMonitor V7.5 is a full-featured, sophisticated and cost-effective network watchdog. It scales extremely well and has an amazingly intuitive user interface.

by Barry Nance, Network Testing Labs

Finding a good network monitoring tool that actually monitors everything on your network isn't as easy as you might think – or might need. For instance, Microsoft's MOM software can stand guard over Windows server activity, but it can't track switches, routers and other devices. Similarly, Ipswitch's What's Up Gold can detect device and server outages but can't warn you when a server process or server component is failing.

The perfect network, server and application monitor immediately alerts you when outages occur, pinpoints the root cause of the outage and helps you reestablish communications tout-de-suite. The tool will, in certain situations, even fix the problem for you automatically. An ideal tool can produce useful reports showing utilization trends, outage statistics, Service Level Agreement (SLA) compliance breaches and other information. A perfect tool is easy to use, scales well, integrates with network management systems, handles any and all protocols and supports just about every computing environment.

ipMonitor Corporation claims its new ipMonitor V7.5 product meets these criteria. We decided to put ipMonitor V7.5 to the test in our network lab to verify the vendor's claims.

ipMonitor met or exceeded our expectations in every category, emerging from the tests with flying colors. ipMonitor contains a wealth of features and can closely monitor virtually every networking device, server or activity. It sports a responsive and intuitive user interface, scales well and offers highly useful reports. ipMonitor 7.5 easily wins the Network Testing Labs World Class Award for best network monitoring and alerting tool.

Monitoring, alerting and correcting

ipMonitor keeps watch over devices, applications, databases and servers. For example, it can tirelessly and faithfully monitor Windows server (NT, 2000, XP, 2003), Microsoft Exchange, Microsoft SQL Server, Oracle relational databases, Dell servers and networking equipment, Hewlett Packard servers, Cisco routers, Foundry Networks switches, APC back-up power protection systems and NetBotz environmental monitors. Our tests showed that ipMonitor is specifically geared to help network administrators



maintain high availability, responsiveness and application/server performance quality. The tool can even generate synthetic transactions to ensure critical business applications are operating and behaving normally. The components for monitoring Windows-based servers also keep tabs on Services, event log entries, free disk space, Active Directory, Kerberos and specific key files that you designate. ipMonitor keeps tabs on Unix-based servers via ICMP/ping and via the network protocol streams emitted by the Unix-based servers.

The intelligent ipMonitor components for monitoring devices (infrastructure) measure network activity for such protocols as HTTP, HTTPS, FTP, POP3, IMAP4, ICMP/ping, SNMP, HTML/ASP, SMTP, DNS, Lotus Notes, LDAP, RADIUS, Telnet and SNPP. ipMonitor also supplies a useful and accurate network bandwidth measurement.

Its alerting feature is a strong point in favor of ipMonitor. When the tool detects a Quality of Service (QoS) degradation, a particular pattern of network traffic, activity levels that exceed settable thresholds or a server or application failure, ipMonitor will let you know via e-mail, SMS, pager, wireless device and network broadcast. ipMonitor supports UCP/SMS text messaging. The SMS Text Pager Alert can use UCP (Universal Computer Protocol) to send an Alert to your alphanumeric pager or digital phone with SMS support. It also integrates with your help desk software to issue and track trouble tickets. You can embed scheduling information in its alerts and ipMonitor can escalate alerts to make sure problems do not get overlooked or inadvertently ignored.

Avoiding problems is always a good idea, and ipMonitor's QoS, disk space, valid link, event log and SNMP modules can trigger alerts even before a failure actually occurs.

ipMonitor takes corrective action to solve many types of problems. Its automatic recover feature can run an external program, reboot a server or restart a Service.

Ease of use, reports and scalability

ipMonitor offers an extremely useful network scan (discovery) action for locating applications, servers, devices and services on part or all of a network. The scan feature makes quick work of telling ipMonitor which network entities it should track, and the discovery methods are an accurate, comprehensive and configurable mix of DNS, ICMP/ping, SNMP and TCP/UDP port scanning operations. ipMonitor groups the results by IP address or domain name, and it helpfully suggests what to monitor based on its findings during the scan.

The browser-based Web interface is a highly configurable, responsive and easy to navigate view into ipMonitor.

Designed for large installations consisting of many thousands of monitored entities, ipMonitor's filter interface makes quick work of locating and managing similar objects.



An administrator can easily enable, suspend, disable, delete or add monitored entries to ipMonitor's named groups. It even supports searching via regular expressions.

ipMonitor reports show both real-time and historical data. Live Status reports display the current, up-to-the-minute health and status of servers, applications and devices, while historical reports (for time periods you specify) and recent activity reports (last 24 hours) reveal trends, help with problem follow-up and quantify your network's uptime and availability. The reports detail such information as uptime, response time and failure durations. ipMonitor can send automatically-generated reports to e-mail addresses you specify, and changing the layout and content of reports with ipMonitor's report design feature is child's play.

Impressively, instances of ipMonitor running on a network can coordinate with each other. Even more impressively, ipMonitor boasts a SOAP (Simple Object Access Protocol) interface for managing ipMonitor instances across an enterprise. With just a small computer programming effort (using, for example, .NET, J2EE, perl, C++ or Visual Basic), we found we could easily add, edit, delete and view configuration elements and associated objects throughout ipMonitor's domain of monitored objects. We could also access real-time status information via the SOAP interface.

We were pleasantly surprised to find ipMonitor offers a pop-up window for displaying the XML (Extensible Markup Language) schemas for monitored objects, groups, profiles and alerts. ipMonitor can import and export configuration parameters and their relationships in XML form.

Security is ipMonitor's fort . It sports the use of SSL (Secure Socket Layer), certificates and credentials, password-challenge authentication methods, IP address filters and delegated administrative accounts.

Installation is a simple process. ipMonitor's printed documentation, a 372-page Administrator's Guide, is clear and comprehensive.

Conclusion

ipMonitor has matured into a full-featured, sophisticated network monitoring and alerting tool. When uptime and availability are critical, we recommend you look closely at ipMonitor. It's a highly flexible, comprehensive tool that excels at early problem detection, often fixes problems without human intervention, is robust, reliable and scalable, produces highly useful reports, is easy to use and is priced right.



Testbed and Methodology

We ran the ipMonitor software product on a Windows XP-based Dell Latitude D505 computer equipped with a 1.5 GHz Pentium processor, 512 Mb RAM and 30 Gb hard drive.

The testbed network of six Fast Ethernet segments contained a NetWare 5.0, Windows NT 4.0 or Windows 2000 file server, an Oracle 8i, Microsoft SQL Server or Sybase Adaptive Server database server, a Netscape or Internet Information Server (IIS) Web server and 100 Windows 98, Windows ME, Windows NT, Windows XP, Windows 2000, Macintosh System 8, and Red Hat Linux 6.2 clients. The six-segment network also contained SNMP-aware switches, Cisco routers, T1 Internet links, back-to-back Frame Relay DSU/CSUs and RMON I/II hardware probes. An Agilent Advisor protocol analyzer eavesdropped on the network traffic to reveal both overall utilization and the content detail of network traffic.

In our tests, we primarily looked for the ability to monitor the health and availability of our servers, operating systems, applications and network devices. The ability to resolve a problem automatically was a plus. We tested the sending of problem notifications by pager, e-mail and SNMP alerts (traps). We expected ipMonitor to produce reports that helped establish baselines, show current and historical server, application and operating system problems, identify trends and avoid future problems. Ease of use was a significant criterion.



Report Card

Grade scale is A through F, with F = Failing and A = Perfect

Category and weight (%)	ipMonitor Corporation ipMonitor 7.5
Monitoring and analysis (30%)	A
Notifications and taking action (30%)	A
Ease of use (20%)	A
Reports (10%)	A
Documentation and Installation (10%)	A
Overall score	A

Vendor Details

ipMonitorV7.5

Price: starts at \$995.00 for 500 Monitors

ipMonitor Corporation

15 Gamelin Blvd., Suite 500
Gatineau, Quebec, Canada J8Y 1V4
Tel: 819.772.4772
www.ipmonitor.com



About the Author

Barry Nance is a networking expert, magazine columnist, book author and application architect. He has more than 29 years experience with IT technologies, methodologies and products. Over the past dozen years, working on behalf of Network Testing Labs, he has evaluated thousands of hardware and software products for ComputerWorld, BYTE Magazine, Government Computer News, PC Magazine, Network Computing, Network World and many other publications. He's authored thousands of magazine articles as well as popular books such as *Introduction to Networking (4th Edition)*, *Network Programming in C* and *Client/Server LAN Programming*.

He's also designed successful e-commerce Web-based applications, created database and network benchmark tools, written a variety of network diagnostic software utilities and developed a number of special-purpose networking protocols.

You can e-mail him at barryn@erols.com.

About Network Testing Labs

Network Testing Labs performs independent technology research and product evaluations. Its network laboratory connects myriads of types of computers and virtually every kind of network device in an ever-changing variety of ways. Its authors are networking experts who write clearly and plainly about complex technologies and products.

Network Testing Labs' experts have written hardware and software product reviews, state-of-the-art analyses, feature articles, in-depth technology workshops, cover stories, buyer's guides and in-depth technology outlooks. Our experts have spoken on a number of topics at Comdex, PC Expo and other venues. In addition, they've created industry standard network benchmark software, database benchmark software and network diagnostic utilities.

