

Looking for trouble

You can't be everywhere at once, so by the time you notice a glitch on the network, it's already causing problems. So let MonitorMagic act as your eyes and ears, helping you react to trouble more quickly

BY KAY EWBANK, CONSULTANT EDITOR, ESM

One of the most irritating aspects of being a systems administrator is that by the time a problem is reported to you, it's already disrupting the smooth running of your network. What's worse is the knowledge that in many cases you could have limited the damage to minor inconvenience if you'd seen it in time. There isn't a sensible person-based alternative to this situation – you don't want your users reporting every tiny (and usually imaginary) glitch on the off-chance that one in a thousand will turn out to be a real problem. And you can't be everywhere at once. What you need is some monitoring software to be your intelligent eyes and ears.

MonitorMagic is a network monitor and manager that gives you proactive monitoring across your network. It alerts you to potential problems, and there's an escalation option that will start with one response to a problem, then go through more 'urgent' responses if the problem isn't solved after the specified length of time. The latest version of MonitorMagic includes integrated reporting, 3D

'An escalation option starts with one response to a problem, then goes through more 'urgent' ones if the problem isn't solved in a given time'

graphing, and a command-line monitor that lets you run a command-line utility, batch file, or whatever, and pass the output to MonitorMagic's standard set of alerts and alarms. You also get two free command-line utilities that work with this particular part of MonitorMagic. WebPing lets you check whether a particular web page exists and, if so, whether it is responding correctly. PortPing does a similar thing with a TCP/IP port, letting you know whether the port is open and responding.

You can run MonitorMagic from a single workstation, and there's also a web interface for remote management on other sites. The software supports Windows XP, 2000, NT and .NET. You can choose to have your information logged to a database so you have an event trail, and the devices monitored include SNMP devices so you can control most network resources.

Essentially, MonitorMagic lets you monitor objects on your network. The objects you can monitor include disks as well as a number of software-based items – services, event logs, and performance counters. You can also monitor TCP/IP hosts. Each type of object has its own monitor, and these individual monitors are all managed from the central application.

Obey the rules

MonitorMagic uses both rules and monitor policies so you can achieve the level of checking you prefer. The main way of deciding what you're going to track is by setting up rules. Each monitor can have as many rules as you like, and each rule is designed to check on a particular event. You build rules by entering criteria such as 'available disk space is less than 20 per cent'. You build the criteria in a dialog box where you first enter the value to be checked, choosing from values such as 'computer', 'status', and 'counter', or entering a numeric or text value. You then add an operator – the list contains combinations of equal, greater and less than, contains and does not contain, and you can choose case sensitive or insensitive options. Finally, you enter a limit or reference value.

When a rule is triggered because the event it is checking occurs, MonitorMagic will execute one or more alarm actions of your choice. Typical options include sending an e-mail message so you know that the rule has been triggered, or sending a message to your mobile

phone or pager; restarting the service; or sending an SNMP trap (a network packet that contains data relating to a component of the system sending the trap). Rules can have a number of alarm actions, and you can specify the conditions that will cause the alarm actions to be executed.

Programs that use rules and alarm actions are great once you've set up everything, but doing so can be an immense task. Fortunately, you can set up monitor policies, and MonitorMagic comes with a set of predefined policies to get you started. A monitor policy can be applied to a collection of monitors, and the best way to think about it is as a template with the definition of all the objects to be monitored, the rules and alarms, but without the specific details. You don't need to specify a particular physical or software device – you just specify the things to monitor, such as all the disks, or all the event logs.

When a policy is applied to a particular computer, MonitorMagic looks through the policy and applies the rules and alarm actions for all relevant objects. So if you have a policy that specifies that all the disks should be monitored, MonitorMagic will see which disks are attached to the computer and will apply the rules and alarms to each of the disks.

Setting up policies can be even trickier than setting up specific monitors, so it's probably just as well that MonitorMagic comes with predefined policies. The policies have all the details for services, event and performance counter monitors with settings based on average network sizes. You can add your own custom alarms to the predefined policies, but other than that you use them as they come.

Preventive medicine

Getting an immediate e-mail or message on your pager if things go slightly wrong is a big improvement on ignorance, but it still means you have a problem. To avoid this, MonitorMagic offers a range of reports based on your event logs that might alert you before problems occur. You can view reports for each MonitorMagic service that is connected, and all the possible reports can be viewed and configured from the main MonitorMagic window.

Information from the reports is collected and stored in the MonitorMagic database according to the schedule you specify. Report management is easy enough – you can set up report profiles that apply to multiple computers or to a single machine, and where you're specifying a report profile for multiple computers, it doesn't matter if a particular computer isn't running all the MonitorMagic services for which you're asking for reports. This makes life a lot easier as

you can ask for all the reports on all the computers and MonitorMagic will sort out exactly what information is realistic.

The main problem with the reports, as with all reports collecting information from sources such as event logs, is that you end up with acres of data. All that data is usually stored in a database. You get the choice of using SQL Server, Access, or any ODBC-compliant database manager, and the database can be local or remote. Whichever you go for, the database management software needs to be installed before a database can be created. It is treated as a system data source, and you can choose to connect to an existing database or create a new one. You can also choose to store your data locally then transfer it into the database according to a schedule.

Once in the database, MonitorMagic can use the data for various purposes, including many of the reports and showing graphs of historical data, as well as predicting trends and carrying out analysis.

One of the better ways to examine the health of your system is by viewing MonitorMagic's graphs. You can view both 2D and 3D graphs, and there are options to view either realtime or historical data. When viewing a graph, you can zoom in on a particular time or value. You can also drag and drop items to add more information to the graph, so if you've missed a particular service from your graph, you can add its data when you realise it's missing.

To sum up...

MonitorMagic is easy to set up, comes with pre-configured rules and profiles, and has some attractive graphs and reports. One drawback with this version is that you are limited to collecting data from event logs, but this will be put right in the next release. <

System requirements

Client workstation running Windows NT 4.0, Windows 2000, Windows 98, Windows Me or Windows XP; Pentium processor running at 133MHz; 64Mb RAM; 10Mb disk space. The computer on which MonitorMagic monitor is running requires Windows NT 4.0, Windows 2000 or Windows XP (Server); Pentium running at 133MHz; 64Mb RAM; 16Mb disk space. Optional database system – Access, SQL Server or ODBC compliant.

UK supplier

Pillar Solutions
Tel: 01732 363670
Web: www.pillar-solutions.com

Bottom line

Pros Policy and rule-based network monitor; optional web-based interface.

Cons Current version reports only on event logs.

What's coming next...

The next version of MonitorMagic is close to release, and will extend the reporting facilities and add more policies. The improved report module will give a more extensive range of reports, and enable you to collect and analyse data from a much wider selection of system objects. For example, the new reports will include an overview of the Exchange mail queue length, a report showing the number of attacks on ISA server, and another showing accounts lockouts. The other main addition to the next release is a range of extra policies. Version 5.0 will contain the following new policies: Citrix Metaframe, ISA server, printer spooler, ArcServe and antivirus software (eg Norton and McAfee).