

Problem solved

Rather than wait for users to gripe about a network fault, let AlertCentre keep you informed and resolve potential problems before they occur

BY MIKE JAMES

How do you know that your network and the applications that run on it are working? If you are anything like the 40 per cent of respondents in a recent survey, you don't make any special effort to monitor the workings of your network or your applications; you simply hope that they are all running smoothly. If you want to be the first to know about network and application problems, rather than waiting for a user to tell you, you need some sort of monitoring software. This is precisely what MKS AlertCentre does for you. Put simply, you set up a range of tests that your network and applications have to pass and AlertCentre applies them at specified intervals. If any test fails, you are alerted to the problem by a number of routes.

AlertCentre converts a machine into a monitoring station, which can typically monitor 20–50 servers. Installation is simple and you can choose to use it via the Microsoft Management Console (MMC) or a web browser, possibly running on a remote machine. The web browser interface looks like the MMC interface so swapping between them is simple. Configuration is achieved via the graphical user interface and getting everything correctly set up is easy.

The next task is to select what you want to monitor and when. The biggest problem with monitoring applications in general is that they often need to

'instrument' the servers they are monitoring by installing agents or services. This can cause problems because the very act of modifying the server can make it unstable or reduce its efficiency. AlertCentre monitors servers and resources without using agents. Essentially the monitoring is achieved either using system-provided standard facilities or by determining if the resource is active by attempting to use it. This means you don't have to deploy anything to the machines being monitored.

Covering the basics

Connectivity is fundamental to any network and this can be monitored in a number of ways. The most basic is to set up a 'ping' monitor, which checks that machines can be contacted. Specific access points can also be monitored – HTTP, FTP, POP3, SMTP, IMAP, NetBios Share, DNS and remote access. All of these are monitored by attempted use and this means you have to configure the monitors to access the service. For example, to test an FTP server you have to supply a username, password and select a command to be executed. In most cases the defaults should be sufficient to prove the server is functioning at some level, but further customisation can extend the checking to specific levels of functionality. For example, the FTP server monitor can try to download or upload a specific file.

A second category of monitors can check resource levels and operational states. You can set up monitors on CPU utilisation, disk space, memory usage and Windows performance. You can also check that a file or directory exists and test its current size. You can also check there is sufficient space left on a disk drive. The printer monitor even lets you test toner, paper and error status. Again these monitors work either by trying to use the resource or by using standard system facilities to query their status.

The third group of monitors check whether applications are available and in good health. These take a little more thought to set up effectively. For example, the application log monitor can open, read and extract any field and test that it is equal to a required value. This is very powerful, but to be effective at detecting a problem it depends on you deciding which fields to

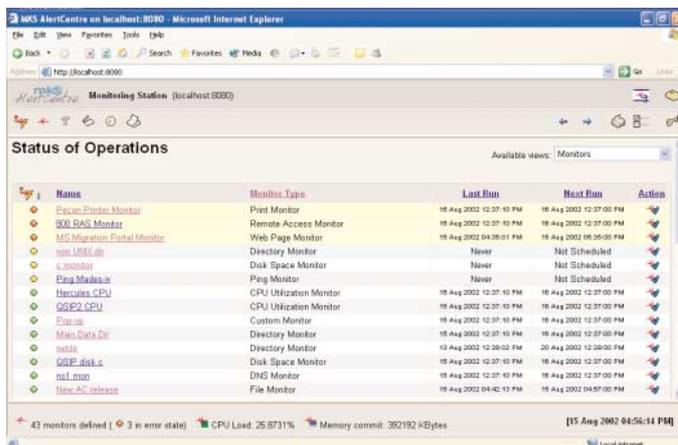


Figure 1: The user interface makes it easy to see the status of monitors

PRODUCT REVIEW

MKS ALERTCENTRE

System requirements

Operating system Windows NT 4.0, 2000, XP Pro, Server 2003.

Processor Minimum CPU speed of 500MHz recommended.

Memory Additional memory of 32–64Mb over operating system requirements is recommended. Memory requirements vary depending on the number of simultaneous monitors running and the frequency of the polling interval.

Supported browsers IE 5.5+, NS 6.0+, Mozilla 1.0+.

For full system requirements, see release notes at http://www.mksoftware.com/docs/rn/relnotes_ac201.asp#hws

UK supplier

You can buy AlertCentre directly from MKS Systems
Tel: 01483 733933
E-mail: uk@mks.com
Web: www.mksoftware.com

or from the Web Store at <http://webstore.mksoftware.com/webstore>

Cost

£3,333 per monitoring station. This includes 12 months' PCS (Preferred Customer Support – unlimited technical support, patches and upgrades and access to information).

Bottom line

Pros An integrated network monitoring tool that doesn't use agents to gather information.

Cons Costly for use with small networks.

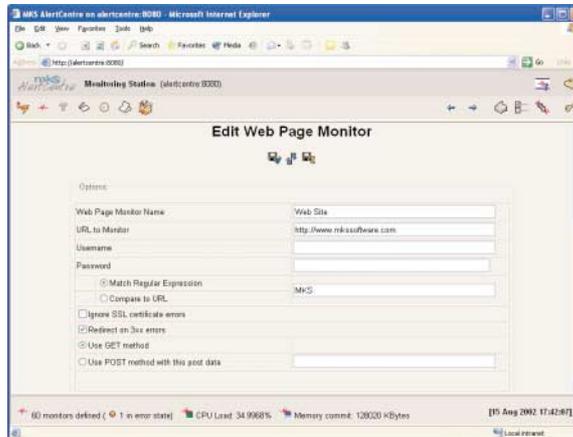


Figure 2: Selecting one of the monitor types takes you on to a page that allows you to create or configure existing monitors

monitor. You can create monitors that will check that a Windows service is running, or access a specific web page, logging on and posting data if necessary and then verifying that the response is correct. The web site link integrity monitor will start from a specified base URL and then recursively follow links to specified hosts so checking they are reachable. The ODBC database monitor will submit an SQL query that you specify and compare the result to a target string. The e-mail monitor will send an e-mail using one SMTP server and check that it is received by another SMTP server by downloading it using POP3 or IMAP.

Magic moments

The monitors described above constitute the basic AlertCentre tools. To make life easier, however, application wizards will automatically build a set of monitors suitable for checking a whole application. Currently, there are three wizards for Exchange, IIS and SQL Server. For example, if you decide to monitor an IIS server a range of monitors for performance counters, sites, disk utilisation and so on are created. In each case the wizard automatically discovers as much about the configuration of the application as possible, so reducing the amount of time the user has to spend entering data.

You can also create a custom monitor. A command-line script can be run and its results compared with a specified exit code or string result. The advantage of integrating the testing script with AlertCentre is that the custom monitor can be managed using the same facilities as the supplied monitors. Any monitor can be scheduled to run at any interval. A number of predefined schedules – daily, every 15 minutes, every hour and weekly – are supplied, but you can easily create your own. Schedules can be set to run monitors at any given daily pattern, or on system startup, or when the system is idle.

Every monitor can be associated with actions that are carried out under a range of monitor-detected errors. You can set an individual action for three different error counts. For example, you could set one action if a monitor returns a single error and another if the monitor returns multiple consecutive errors. You can also trigger an action if the monitor returns a success. The actions can be automatically modified according to the day, date or time. A command can be set to execute before and after the action has been processed. Actions include sending an e-mail or pop-up message, dialling a modem, running a script, rebooting a particular machine, restarting a service, logging the problem to an ODBC database or creating an SNMP event.

Seeing red

From the AlertCentre interface you can see the status of monitors graphically and, to make this easier to interpret, you can group monitors under headings. Monitors that have returned no errors show green; those with problems show amber or red. Hovering the cursor over the indicator displays the reason it is not green in a pop-up. You can also generate a range of reports: uptime, status, errors, schedule and monitor lists.

So who monitors the monitor? The answer is the backup monitoring station. If the primary monitoring station fails, the backup will take over and optionally inform you of the problem. The AlertCentre licence allows you to install it twice: once for the primary and once for the backup monitoring station.

AlertCentre is created from scripts using Perl and a small amount of C/C++ code. It makes use of the MKS Toolkit, which is included so you can extend AlertCentre by writing custom scripts.

Overall, AlertCentre provides an easy-to-use way of monitoring a network and actively testing it and the applications that run on it to ensure they really are working. By bringing monitoring activities together as part of a single tool, you are more likely to cover all the possibilities and detect a network or application problem before users tell you about it. The benefits of using AlertCentre are likely to grow as you develop its configuration to deal with the specific details of your own network setup. <

You can download an evaluation version from <http://www.mksoftware.com/>

Produced by Enterprise Server Magazine (ESM), November 2003. ESM is the only magazine independently owned and produced in the UK that specialises in Windows and Enterprise Server computing. Free subscription available at www.esmag.co.uk

Mike James has more than 20 years of programming experience as a developer and lecturer and has written numerous books on IT-related subjects. You can reach him at editorial@esmag.co.uk