You're monitoring your servers, your network devices are in check and you know exactly what your applications are doing. However, there's a problem. What about your users? You know, the people who pay your wages. It's in your best interest to keep them happy. Just because your server estate is working like a charm, it doesn't mean your users are necessarily also working just as smoothly.

There may be many reasons for this. There could be virus outbreaks on the client machines, users may be having application issues, their operating systems could be performing poorly... the list goes on. Then there's the fact that many of your users may not be of a technical bent, in which case the simplest of problems could send them into a panic. This could have a considerable impact on their work – and on the client machine, too.

With this in mind, it would seem appropriate to extend your monitoring solution to the client machines in addition to your servers and network devices. However, adding this type of monitoring brings its own list of problems. For example, not all monitoring solutions are designed to monitor large numbers of machines. There will also be extra overhead and licensing costs associated with extending your monitoring solution to the desktops.

You have to realise that you will have limited control over desktop machines. Even with strict desktop lockdown policies, the risk of something unexpected happening to a machine is far more likely on a desktop machine, which users have access to, than a server.

However, Microsoft System Center Operations Manager 2007 does away with these problems. Its redesigned architecture is structured to support a large number of agents without causing issues. Not only does it happily monitor your Windows Server estate and allow you to ensure your network devices are online, it also provides the following three separate methods of monitoring your client machines:

- Business-critical client monitoring
- Collective client monitoring
- Agentless exception monitoring (AEM)

Using these three different methods, you can monitor all aspects of your client desktop infrastructure.

Business critical monitoring is designed for those client machines that serve a business-critical function such as machines that run banking applications and basically any machine that would cause business impact in the event of a failure. This type of monitoring requires an agent to be installed and will need a full agent Operations Manager Licence (OML). It will, however, be monitored as though it were a server, which means that the operating system, applications and availability will all be monitored.

This aspect of client monitoring has not changed since earlier versions of Operations Manager, with the only exception being that the latest version of the product...
is capable of scaling to accommodate a very large number of monitored machines. Clients configured in this way can also have Audit Collection enabled to allow security events to be securely collected and stored in an Audit Collection database.

Collective client monitoring is designed to remove the issues associated with collecting data from many thousands of machines. The client management packs support monitoring and reporting for groups of machines, rather than storing all data from each individual client. Each client will require an agent and an OML for this type of monitoring, but the cost of an OML for collective client monitoring is less than the cost of business-critical monitoring for a client.

Collecting data
The way that Operations Manager 2007 deals with performance data from clients is different from previous versions. Performance data forms the majority of operational data and is very large. In previous versions all performance data was collected on a schedule. Now Operations Manager 2007 has introduced the idea of data point collection. This allows data to be collected according to a schedule and the actual value of the data itself. So you can define that data collection will only occur every 15 minutes and only if the performance point reaches 25, 50 and 80 per cent. Regardless of how many data points are recorded, data will only be collected once the performance point hits one of the specified values (Figure 1).

This type of client monitoring also helps when generating reports. As data is aggregated, reports can be generated for groups of machines, allowing large numbers of machines to be included in a single report.

AEM is another new method of client monitoring and it’s the most impressive. It’s based on Microsoft’s Corporate Error Reporting software, which has now been integrated into Operations Manager 2007.

This new type of monitoring allows error data from the Dr Watson engine in Windows 2000 and above machines to be collected by Operations Manager without the need for an agent. It is very simple to configure and clients are configured globally using Group Policy. Application and operating system crash data is collected and, where necessary, can be passed to Microsoft for investigation. If a fix becomes available from Microsoft it is automatically appended to Operations Manager and, in turn, if the client receives the error again a link to the fix is provided.

In addition, reports can be generated to identify application and operating system issues and trends across the environment (Figure 2). These types of reports are particularly useful when rolling out a new update or service pack, for example. Any crashes or application faults will be recorded and can be compared to identify if the new fix is causing the problem. The same method can be adopted to identify whether or not a fix has resolved an application or operating system crash issue.

Operations Manager 2007 offers a real choice in terms of monitoring client machines. With its redesigned architecture, collective monitoring functionality and integration of AEM, it allows clients to be effectively monitored even in the largest of enterprises. If you can combine this additional functionality with business processes and gain the most from the data collected, your users’ experiences of their IT services can be greatly improved.

Andy Dominey is a MOM consultant at 1E. You can reach him at editorial@server-management.co.uk