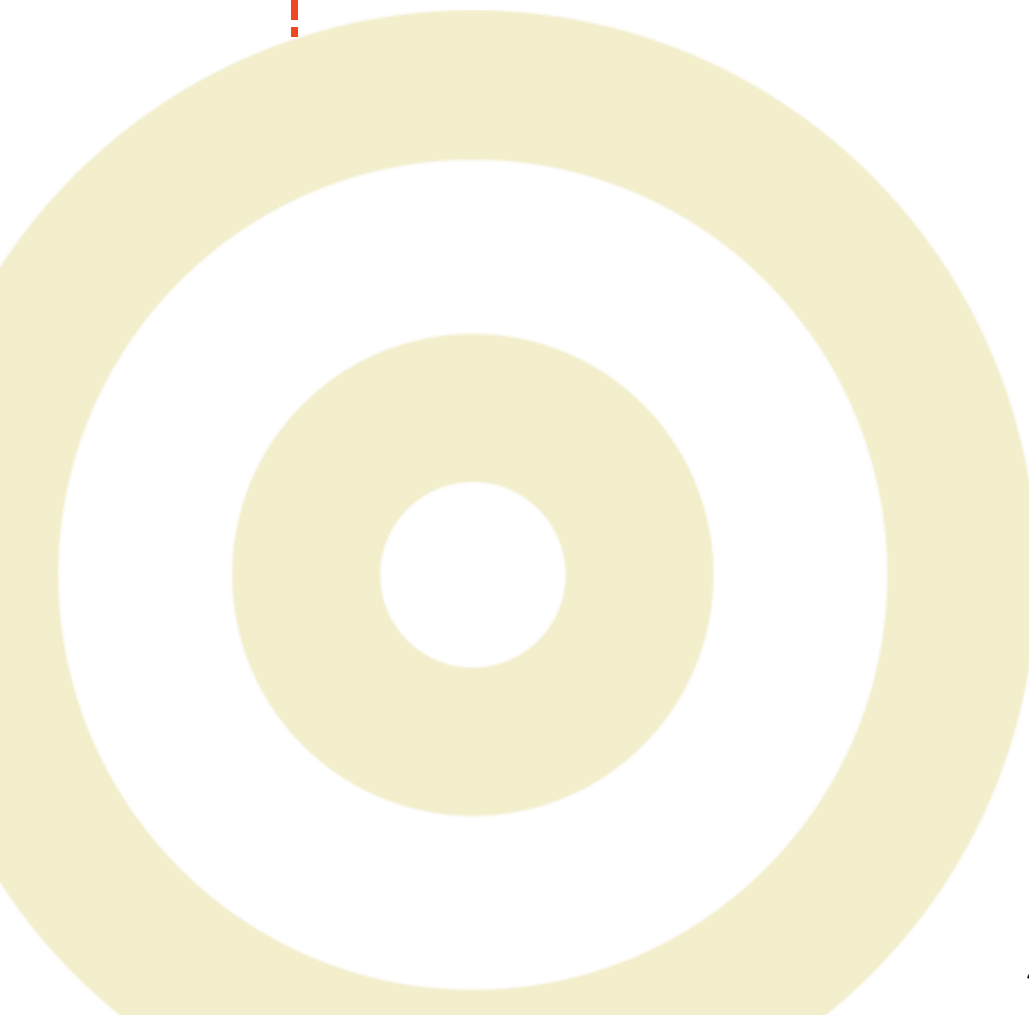


An IT Briefing produced by



Managing Server-Based Applications: The Challenges and How to Deal with Them



Sponsored By:



Managing Server-Based Applications: The Challenges and How to Deal with Them

By Serdar Yegulalp

© 2005 TechTarget

BIO

Serdar Yegulalp is an industry expert and Editor of *The Windows Power Users Newsletter*. He is a frequent contributor to several TechTarget Websites, including SearchWinSystems.com.

This *IT Briefing* is based on an RTO/TechTarget Webcast, “[Managing Server-Based Applications: The Challenges and How to Deal with Them.](#)” To view this Webcast online, please click the link.

This TechTarget *IT Briefing* covers the following topics:

- Executive Summary 1
- What Constitutes a Server Application? 1
- Major Concerns When Monitoring Server Applications. 1
- Local vs. Remote Monitoring 2
 - Server Location 2
 - Bandwidth 2
- Basic Server Monitoring 2
 - Advanced Monitoring Products 3
- Summary 3
- Common Questions. 4

Copyright © 2005 Serdar Yegulalp. All Rights Reserved. Reproduction, adaptation, or translation without prior written permission is prohibited, except as allowed under the copyright laws.

About TechTarget *IT Briefings*

TechTarget *IT Briefings* provide the pertinent information that senior-level IT executives and managers need to make educated purchasing decisions. Originating from our industry-leading Vendor Connection and Expert Webcasts, TechTarget-produced *IT Briefings* turn Webcasts into easy-to-follow technical briefs, similar to white papers.

Design Copyright © 2005 TechTarget. All Rights Reserved.

For inquiries and additional information, contact:
Dennis Shiao
Director of Product Management, Webcasts
dshiao@techtarg.com

Managing Server-Based Applications: The Challenges and How to Deal with Them

Executive Summary

This TechTarget *IT Briefing* addresses the topics to consider when managing server-based applications, as opposed to applications that run locally on a workstation. Specific issues and considerations are discussed, along with methods and tools for monitoring server applications' performance and availability. A section addressing common questions is provided at the end of the document.

What Constitutes a Server Application?

A server application is any application that runs on a server or remote system rather than on a desktop system. Examples include a standalone service like Internet Information Server (IIS), a DNS server, an SMTP server, or SQL Server.

These applications also include Web applications that run on one of these services, such as an ASP application or a Perl script. Another example would be a custom executable script that runs on the service site, usually without user interaction—an application that runs every hour, every day, or every five minutes.

Server applications often interact with networks, but this is not the major criterion in deciding whether an application is a server application—the fact that it runs on a server is the major factor. Another common example of such an application is a script that runs a maintenance process to defragment or perform other system cleanup duties on a server—its main criterion is not interactivity.

Server applications are not as easy to monitor as those on the desktop. Knowing how to manage these applications and ensuring they are running well is a key challenge.

Major Concerns When Monitoring Server Applications

The largest concerns are whether the server and its applications are running correctly, maintaining basic connectivity, and functionality. A familiar example of testing for these concerns is continually pinging a remote server to see if it responds. Another example is having a program running on the same server that tests other programs' responses on that server and reports back. Such a program monitors current server behavior; this approach is useful to find out what is happening at any given moment on a server.

For example, assume an SQL Server is running and you need a quick update on how many simultaneous user transactions the SQL Server is processing. This information is not easily available though the SQL Server itself because it has no built-in user interface, so another tool is required. The choice of tool can provide you with information of varying degrees of depth and complexity: maybe you only need the basics (“is it running?”), or maybe you need more details (“which user connections are causing a blocking condition?”).

Aside from monitoring basic functionality and whether a server is still running, there are three basic reasons to monitor applications:

1. Can performance be improved? If an application is simply functioning, that is not enough if thousands of users are unable to use that application because it is not functioning well enough.
2. How can performance be improved? Knowing that performance can be improved is one thing; knowing how to improve it is another. Statistics are useful to help determine exactly what part of the system may be lagging.

3. Where are the bottlenecks? If statistics show heavy disk activity, for example, the disk subsystem may need to be upgraded or replaced. An overloaded CPU might indicate there is not enough raw processing power to do the needed work.

Monitoring statistics along with basic application functionality shows not only what is running, but how well it is running. With additional information available, IT personnel can always have an eye turned to improving system performance.

Another important reason to monitor is to gather information that allows resolution of future problems. If a performance problem is fixed but the fix is not documented, the next time the problem occurs, the solution may have to be rediscovered. If this solution information is recorded, IT personnel can say “this happened before, this is how we fixed it, and here is how we can fix it again.” Monitoring is not just about fixing current problems but preventing the same problems from occurring in the future, and being proactive against creating situations where they might exist once more.

Local vs. Remote Monitoring

Local monitoring means that any monitoring is taking place on the server itself and then reported outward. Reporting can be in the form of a notification e-mail or a report generated and stored on the server that can be accessed through a Web browser. Remote monitoring is when a console is run on another workstation, and tools on that console monitor the remote system and gather information from it.

The two methods work in fundamentally different ways: local reporting has the advantage of being run independently of the user, in a “hands-off” fashion. We could call this the “set it and forget it” model of monitoring. There is little need for user involvement, but on the other hand, that can be limiting. If there is a system-specific piece of information needed, it can be more difficult to obtain when using this type of tool.

Remote monitoring allows administrators to gather exactly what they need and when they need it. Its disadvantage, however, is that it is essentially disconnected from the system and can only gather what is available to the user through a remote interface.

Server Location

Another major consideration in local vs. remote monitoring is where the server is located and how it is connected. If the server is on the local network, the difference between local and remote monitoring is almost nil because the systems are in the same place. If the server in question is hosted, for example, at a third-party network operation center (NOC), it is a different story. You are not just dealing with your own network anymore; this other network may have its own bottlenecks and blockages that need to be taken into consideration. In such a case, administrators may want to simply test locally on that server and have reports sent out or use the NOC’s monitoring system if available.

Another situation may be remote offices connected via WAN. This situation is somewhat the same as a remotely-hosted server, except you usually have a little more control over how to talk to the remote host.

Bandwidth

Another consideration for local vs. remote management is the amount of bandwidth available to the system administrator. If this administrator is using dial-up and dealing with a tool that requires a great deal of bandwidth, there is a performance mismatch. As a result, the amount of bandwidth the management tool uses should be factored into any purchase decision.

Basic Server Monitoring

One of the most basic monitoring tools is pinging between services. An example of this is IIS when running an ASP application. Microsoft established this function because they were receiving reports from people who had written a badly-coded ASP application that locked up the whole server. No one would have any way of knowing the process was dead without actually checking it. So the IIS master service pings the ASP services to determine if the two are still “talking”. If they are not, then the child process running the ASP application is killed and restarted. This is one example of how one service can monitor another on the same system to see if it is still working: if it is not, then the service can be killed and perhaps an emergency notification can be sent to the system administrator. There are also desktop applications that will ping a remote Web server to see if the Web server is responding. This can be useful when

trying to determine whether a network is down. Sometimes the question is whether the network or the server itself is down. Fortunately, hosting companies often have their own tools that can tell exactly where the problem is—such as a local ping service that checks to see if the server is responding within the host's own network. Administrators should find out exactly how many tools are available across the board and use all of them. The more information you have at your disposal, the better.

The event log on the remote server itself can capture specific events that may be worth knowing—whether alerts are serious or simply minor informational alerts that may indicate something that could become problematic—and forward this information via e-mail or pager.

There are many ways to perform monitoring and many kinds of information that can be obtained. Alerts do not have to be used to alert the admin to disasters, such as having the server go down; they can simply detail issues such as running low on disk space so administrators can keep watch on that particular system.

Advanced Monitoring Products

This section discusses some of the advanced monitoring products available. Microsoft Operations Manager is a large, powerful overall management tool; it may not be the best solution for everybody, however, because of its size and cost.

Advanced monitoring products deal with specific applications such as Exchange or Windows scripting; specific services such as IIS and SQL; and system logs such as Web logs or the system services themselves.

For an “everything in one” approach, Microsoft Operations Manager (MOM) is designed to troubleshoot issues with a broad range of Microsoft applications; because Microsoft wrote both MOM and the applications, they know how to “get under the hood” and obtain detailed answers to specific problems. MOM covers SQL Server 2000, Exchange Server 2003, and Active Directory, among others. It also has the ability to drill down and provide feedback about what might be wrong with, for example, a certain SQL Server database. You not only get information that something is wrong, you get infor-

mation about what might be wrong, how to fix it, and how to avoid it in the future.

MOM can be run from a desktop console or a Web browser. It has provisions for automatically correcting certain conditions. For example, if running low on disk space, an event can be generated to make sure the temp directory (a common dumping ground for applications) is automatically purged. A trial version of MOM is available at no cost from the Microsoft Operations Manager's site, www.microsoft.com/mom.

There are pros and cons to MOM; on the plus side, it is specific to Microsoft applications and powerful enough to provide detailed granularity. The downside is that it is expensive and fairly complicated; it should not be used unless the administrator already knows a great deal about the packages being monitored. If you do not know SQL Server, do not try SQL Server monitoring, because otherwise you are not going to make much sense of the data you are gathering, and you might do more harm than good.

Summary

What is the best way to choose monitoring tools? The single most important rule is to know your needs. If running a simple Web service that does not serve a lot of data, complicated performance monitoring may not be necessary. You may just need to know that the server and its applications are up, which you could determine with anything from a simple ping script to a desktop application like GFI Network Monitor.

If dealing with something more ambitious, however, such as monitoring performance or event logging, take the time to learn the ropes, such as what specific logged events mean and the importance of various metrics. Do not assume the importance of a given event; sometimes what may seem urgent may turn out to be something you can safely ignore.

Begin with current capabilities and address current needs. If the company is not growing quickly, do not worry about upgrading tools and using more sophisticated products. If it is growing explosively, however, choose a product that can also grow—but do not spend large amounts of money for something you are not going to use. Go with what you know is needed now.

Common Questions

Question: If an application on the server only runs intermittently, does it still need to be monitored?

Answer: Yes, although not as aggressively as some other applications. For example, you might have a script that only runs hourly or daily; the admin might not need to know about it unless it fails to run at all. In such a case, they could receive notification by pager or e-mail, or in the case of something that is not really all that important, in an entry in the system log.

The same thing applies to hardware, too. The remote server I manage is monitored for ping by the hosting company. If it stops responding to ping, I get an e-mail notification.

Question: When gathering statistics as part of the monitoring operation, what is a possible sign that the server itself might need an upgrade?

Answer: Aside from CPU load, monitor the amount of disk chatter, or disk activity from the performance counters. That is usually a broad clue as to how the server is handling its particular load. If there is not enough physical memory, the system will begin to swap more aggressively to disk, which will raise the amount of disk activity. There are two main possibilities here: one, the disk system may be having a problem—you may need a bigger disk or a faster controller; two, there is not enough physical memory. Always purchase as much memory as possible when you can. Memory is cheap right now; there is no reason not to. The amount of disk activity is the single most obvious statistic to pay attention to.

Question: If a company is considering having someone else host its server but still wants to monitor it, what kind of monitoring options do hosting centers typically have?

Answer: They have some fairly sophisticated tools. One of the companies I deal with, ThePlanet.Net, has a hosting center with a number of different tiers of monitoring options. The most basic monitoring option is a local ping where they can test every few

minutes if your server is up. That comes free with most of the levels of service. For additional costs, you can add other services such as Cisco firewalls, TippingPoint intrusion/flood detection, and so on. They can also monitor multiple IP addressees; if there are several IP addressees associated on a system, they can ping each one of them in succession to make sure things are running.

Question: What can a company do to ping a remote server if ping has been port-blocked?

Answer: Sometimes, if a server is hosted remotely ping is blocked by the ISP as a way to stop distributed denial-of-service attacks. I mentioned earlier that if your hosting company offers some kind of local ping solution, where the box is pinged locally within their network rather than from outside, use that instead of a remote ping; it is usually more reliable.

People are beginning to move away from ping; it is often aggressively blocked, and it is only a basic “heartbeat” indicator—it does not even describe whether services are up.

Question: If a company installs the free trial version of Microsoft Operations Manager, can they upgrade to the full version without reinstalling?

Answer: Yes. You need to run their selected retail version of the install, which they provide for you. Enter the license number they give you for each of the components: the management server, the consoles, and the database.

Question: What would be some good resources for administrators to learn about monitoring system events and statistics?

Answer: First, there is www.eventid.net, a huge searchable database of Windows system log event IDs. You can get a one-year subscription for \$24 or three months for \$9; the free stuff by itself is very compelling. If you need to dig out the meaning behind various event IDs on a regular basis, your money will be well spent here.

Another is Microsoft itself. If you search Microsoft TechNet for “Windows server performance counters reference,” you will get a complete overview broken down by feature and by object of every single one of the Windows performance counters. You can go to www.microsoft.com and or TechNet, or even do a Google contextual search to find a particular counter.

Those are two major sources that come to mind. The great thing about them is between the two of them there are links to plenty of third-party resources who have even more information.

Do not do anything before you have an idea of what you are going to change and why. So, starting from multiple resources to get more than one opinion is going to help more than just relying on one alone.



About TechTarget

We deliver the information IT pros need to be successful.

TechTarget publishes targeted media that address your need for information and resources. Our network of industry-specific Web sites give enterprise IT professionals access to experts and peers, original content and link to relevant information from across the Internet. Our conferences give you access to vendor-neutral, expert commentary and advice on the issues and challenges you face daily. Practical technical advice and expert insights are distributed via more than 100 specialized e-mail newsletters, and our webcasts allow IT pros to ask questions of technical experts in real time.

What makes us unique

TechTarget is squarely focused on the enterprise IT space. Our team of editors and network of industry experts provide the richest, most relevant content to IT professionals. We leverage the immediacy of the Web, the networking and face-to-face opportunities of conferences, the expert interaction of Webcasts and Web radio, the laser-targeting of e-mail newsletters and the richness and depth of our print media to create compelling and actionable information for enterprise IT professionals. For more information, visit www.techtarget.com.

RTO_08_2005_0002