Monitoring Virtual Desktops

BY GABE KNUTH

When I think of monitoring virtual desktops, I think of all the years I spent trying to find that one magical product that would monitor every single thing in my environment, throw up snazzy alerts, and kick off workflows to fix some of the easier things like resetting a print spooler service. Nothing I ever found was good enough, though, and I tried them all. I was always jealous of the NASA Mission Control-style NOCs in the big data centers that I'd visit, but those giant screens had a higher-level view than I needed in the desktop world.

Therein lies the problem, actually. When most people think about monitoring, they think about servers or networking. To make matters worse, nobody thinks about monitoring before they need it. That means when you have a problem with the network, you're going to look for the monitoring platform with the best networking data (let's face it, the fanciest "dashboard"). It can do other things, but it's made for networking. Then, when you have a server issue, you have two choices: you can try to use your existing platform that was made for networking but can do other things, or you go buy another platform that was made for servers. Then when you have a problem with your databases or desktops, you do the same thing.

brianmadden

TechTarget® Custom Media

A TECHTARGET WHITE PAPER

You end up with either a platform that only kind of works for most things, or you end up with a half-dozen different platforms that only work well in specific scenarios. Even today, when we have more desktops than ever in our data centers—and with that more reliance on virtualization, quality networking, and reliable, fast storage—the monitoring products that we use are likely from a time when we had physical servers that ran dedicated workloads. Even if those platforms have been updated, they're almost assuredly better at some things than others.

That paints a bleak picture, doesn't it? The good news is that there are things you can do to make monitoring easier and more productive for your environment. What follows are the six keys to making monitoring more productive in your environment:

1. Don't wait to get a monitoring platform until you need one.
2. Don't try to find one platform that can do everything.
3. Out-of-band is just as important as in-band.
4. You know about desktop virtualization, so find a monitoring platform that knows it, too.
5. High-level isn't bad, but you still need to monitor all of the other layers.
6. Pretty dashboards are great, but reporting is more important.

Let's explore these a bit more.

1. Don't wait to get a monitoring platform until you need one

The first mistake we make with monitoring is waiting too long. If you're planning a desktop virtualization project, or if you have one running smoothly right now but without any monitoring, now is the time to start looking at them! Waiting until the last second results in knee-jerk reactions that lead to choosing the first product that looks like it will address the specific problem you're having.

Instead, evaluate the potential products now.

2. Don't try to find one platform that can do everything

If there's one thing I've learned about monitoring, it's that you can't possibly find one platform that does everything you want in the way that you want to do it. It may be possible to assemble something that collects every possible data point, but can you sort through it and present it in a valuable way?

The best solution is actually multiple platforms that do an excellent job in their respective areas. You may actually get some value out of the high-level dashboard that turns various colors of the rainbow based on certain conditions, but it doesn't do you any good if you can't chase down the root cause. You may think the catch-all platform you currently have can do that, but ask yourself:

- Does it allow you to drill down to the hypervisor level?
- Does it look at what's happening in your storage?
- Can it watch your database servers and report on queries and execution time?
- Does it look inside the VMs at the individual processes for each user?
- Does it watch the network traffic to see if an application is misbehaving?
- Can it see inside your remote desktop protocol to discover exactly what it is doing?

Odds are your platform can't do all that. Even if it can, the useful data is elusive because it is mixed with everything else. To be successful, you need to have multiple platforms that excel in each of these, and though we're talking about monitoring virtual desktops specifically, this will undoubtedly affect other areas of your business as well.

3. Agentless is just as important as agent-based

When you start looking at monitoring products, you'll notice that they're broken up into two groups: agent-based and agentless. Agent-based platforms use a custom agent installed on every system that's monitored to report back to a central system. Agentless, as you probably figured out, leverages wire data or something else that allows it to perform its monitoring out-of-band.

- Some tap into the network and monitor application traffic that goes by, providing the basis for wire data analytics.
- Some are virtual machines that live on each host, watching the hypervisor and the other virtual machines via hypervisor-specific channels.
- Some are simply servers that reach out to monitored systems via the network and poll the data that the systems have already collected (like WMI or Perfmon data).

When asked which I prefer, my answer is always, "Both!" In fact, it can be helpful to get both a top-down and an inside-out view of your environment when tracking down a problem. For example, an agentless network monitoring solution might alert you to the fact that your printing virtual channel in HDX is way larger than normal, and that it's coming from a specific session. You could then use an agent-based tool to dig deeper and isolate the problem with a specific document or printer driver that a user has.

It's worth keeping in mind that the only truly agentless tools are the ones that watch the network or plug in to the hypervisor and observe systems from the outside. Any other "agentless" monitoring products leverage an agent of sorts, it's just that the "agent" they use comes with Windows in the form of the WMI service or Perfmon. So when you hear that agentless will give you better performance because "you don't install anything," keep in mind that you're just using what's already there. (And come on, what's a tiny agent these days compared to VDAs and antivirus?)

While we're talking about the differences between agent-based and agentless, remember that while many agentless tools that leverage Windows performance data can help get the same CPU/memory/disk information as agent-based products, they can't measure the user experience directly. Agent-based products can do this because they have extra visibility from within Windows. They can see from the application level, and they can also see how the apps, OS, and hardware are working together.

Assembling a solution that uses data from multiple sources also means that you're choosing the best platform for each scenario. For example, using an agentless network product can give you insight into application behaviors that you can't access with an agent-based product, while using a lightweight agent-based product can give you insight into the user experience. Whatever you choose, make sure you're covered from both sides.

4. You know about desktop virtualization, so find a monitoring platform that knows it, too

We all know by now that desktop virtualization is not the same thing as server virtualization, right? Compared to desktops, servers are boring, practical devices that pretty much do the same thing all the time. They're easy to standardize, and they're relatively easy to monitor.

Desktops, on the other hand, have to do a lot more. They have to support all of the crazy things that end users try to do, all of the devices they want to plug in, and other things that we don't have to worry about with servers, like 3-D graphics, incompatible applications, antivirus, and boot/logon storms. And to make matters worse, the users are connecting to this environment via a remote protocol from client devices that can be anywhere in the world!

It makes sense to keep the rather large difference between server and desktop virtualization in mind when looking at monitoring packages. What worked great for you and your servers might not work so well when you add in all the complexities of desktops, even though it looks like it might be fine.

Sure, every monitoring solution might be aware that virtual desktops and protocols exist, but one product's ability to collect and present relevant data might not be the same as another's. That's why it's important to select something that is not only aware of virtual desktops, but offers visibility into what's going on. The ideal set of solutions can give you insight not only into the protocol, but also into the encoding process.

You're probably aware (but if you're not, congratulations on building the best environment ever!) that there's a lot going on inside your HDX, PCoIP, or RemoteFX packet. There is graphical data, keyboard and mouse data, printing, port redirection, drive redirection, USB, and a number of other things being sent back and forth at any given time.

Normally, the desktop virtualization platforms do a great job of manipulating the traffic between the host and client in a way that all the data gets through without drastically affecting the user experience, but we don't keep monitoring around for the "normal" days, do we? When something does go awry, the product that can see inside the protocol is going to alert you that you have an increased amount of drive redirection traffic, whereas the product that's only aware of the protocol's

existence is going to simply tell you that the packets are bigger than normal.

5. High-level isn't bad, but you still need to monitor all the other layers

At the risk of sounding redundant, there is a place for high-level monitoring that can give you an overall impression of the world, but keep in mind that it is just that: an overall impression. High-level is great when everything is green, but when things start happening you're going to want to lean on something else. The workloads we encounter today are different than the ones in the past, and so what we look for in a given situation is also different.

Outages are easy, but slowness, inconsistent performance, and our reliance on more moving parts than ever means that we need visibility into a lot more places, like:

- Hypervisors
- Virtual machine resource consumption
- Virtualization host hardware
- RDSH session information
- Network equipment and configuration
- Active Directory traffic and configuration
- Database queries and traffic
- HTTP payloads for browser or cloud applications

There's no single product that can do all of this, but you can assemble two or three different products that provide you with the high-level view you want 99% of the time and the ability to correlate data from different systems to find the cause of the problem when the time comes.

6. Pretty dashboards are great, but reporting is more important

Monitoring isn't sexy. There's rarely anything that you can point at and say, "Now THAT is a nice monitoring platform!" Vendors know that, too, so they all put a lot of effort into the first thing a customer sees: the dashboard.

We've all been wooed by the pretty colors and blinking lights of a really cool dashboard even though we know that under that dashboard is basically the same information that we could collect via Perfmon. As nice as they are, you rarely spend time looking at them, so why would the product you buy have anything to do with how cool the dashboard looks? You can make a pretty dashboard, but when things start to turn south you're not going to care so much about how pretty the screen is while the building is burning down.

Functionality is king (it has to do what we want, after all), but reporting is next in line for the throne. Good reporting does two things. First, it gives you something that you can hand your boss that shows what a great decision they made in investing in monitoring! Second, it gives you ammunition you need when it comes to planning your next steps in desktop virtualization. You can see how your environment is performing, where your bottlenecks are likely to be, and where you need to allocate funds from next year's budget. You may even be able to identify problems before they happen!

Wrap-up

It's time to change the way we look at monitoring. It's not the most exciting area of IT, but that doesn't mean it should be ignored until the last second. The only way you can be sure to get all the data you need is to pick the right products for each area that you need to monitor. Some are very good at a few areas, but nothing can do it all. If you plan now, you can get the appropriate platforms in the right places so that you can avoid long outages or knee-jerk purchases that amount to a waste of money. Make it a blend of agent-based and agentless, and by all means make sure it's as aware of desktop virtualization as possible.