



Common Pitfalls in Server Virtualization

Last Updated: 08/25/08

Executive Summary

For all its benefits, server virtualization can be difficult to implement and could actually increase your costs and complicate network management. Here are some common pitfalls to look out for and avoid.

Everybody's talking about virtualization and server consolidation these days, and many companies are taking some kind of action, with large enterprises in the lead. Server consolidation through virtualization is a proven way to save money in many ways: less hardware, lower power consumption, less floor space and more.

And that's just server virtualization. There's also storage virtualization, data center virtualization, application virtualization and desktop virtualization, all of which promise significant economic and performance benefits. Without doubt, virtualization is the future of computing, because it decouples computing operating systems and applications from the hardware, lending enormous flexibility and agility to an enterprise's computing system.

For all its benefits, however, server virtualization can be difficult to implement and could actually increase your costs and complicate your life. The objective is to avoid potential pitfalls, many of which are described below.

Poor preparation

Your virtualization project is almost certainly only the first step toward a completely virtualized network that is going to be much different than the hardware-centric system you are used to working with. That's why even small virtualization projects tend to be much more complex than they first appear.

There are implications far beyond simply adding virtual operating systems to a host server to boost computing power. You will face a wide range of issues, from server compatibility to network limitations, software licensing to storage infrastructure and more.

If you don't understand all these issues up front, before the virtual machines start multiplying (and they will multiply), you could find yourself in a desperate race to catch up with proliferating problems. Make sure you and your staff are aware of what it takes to implement, maintain and manage a virtualized infrastructure and avoid the pitfalls noted below. See >> "Server Virtualization: Putting and End to Server Sprawl" and >> "Server Virtualization: Deciding What You Need to Purchase."

Insufficient server capacity

Virtualization does not add computing resources, only usage. Multiple operating systems — even if they are virtual — require substantial processing power, input/output capacity, memory and disk capacity.

To be a good candidate for virtualization a server should have at least two CPUs, 4GB of RAM or more and more than 100GB of available disk space. Servers with less capability could prevent you from gaining the substantial benefits of multiple Virtual Machines (VMs), especially if the server already hosts an input/output intensive application, such as a database.

So, evaluate your hardware to determine whether your CPUs, RAM, and storage are underutilized, and if so, by how much. Your first step toward profitable virtualization might have to be upgrading your servers.

Mismatched servers

If you are virtualizing multiple servers and they use different chip technology (Intel and AMD), you might encounter difficulties with migrating VMs between them. In some cases, you won't be able to migrate VMs without rebooting the server, somewhat mitigating the benefits of virtualization and live migration. It's a good idea to standardize your servers on a single chip manufacturer.

Slow network communications

One of the goals of virtualization, and its primary benefit, is a huge leap in computing capacity for a given amount of hardware. But, latency and insufficient network bandwidth can steal much of the intended gain. So be ready to bolster your network's communications capabilities.

That will probably require some combination of new servers, new switches, network interface cards, and cabling: think 10Gbps Ethernet (and imagine the future 100Gbps Ethernet). Be sure to include the cost of faster communications devices in your virtualization budget.

Slow mechanical disks

Current mechanical disk technology cannot keep up with the read/write demands of multiple servers in high-use periods, so you will experience some latency. One possible solution is storage caching, whereby frequently accessed data is served from high-speed memory instead of mechanical disks. Another solution on the near horizon, is solid state disks, which promise read/write speeds up to 30 times faster than spinning-disk technology.

Too many VMs per host

One of the great things about VMs, and one of the most problematic, is the ease with which they can be deployed and migrated to meet changing needs. If you and your staff aren't careful, however, you could end up with more VMs than you can effectively manage and more than a server can handle without degrading performance. It is a good idea to establish a VM implementation policy that recognizes system and personnel limitations and make sure the entire IT staff adheres to that policy.

Uneven workload distribution

To maximize usage of your data center computing power, you need to really fine-tune the distribution of processing requirements across all your physical servers. That means you need to monitor application usage to detect daily, weekly or monthly peak usage and determine response times and so on. This will enable you to allocate applications accordingly.

There are a number of application performance software tools available for this purpose, but the burden will grow rapidly as more and more VMs are added. Managing — let alone optimizing — even a single server with 10 or more VMs running different operating systems and multiple applications can be very challenging. Fortunately, automated data center management tools, now on the horizon, will help you meet that challenge.

Losing track of applications

Where you once had a clear idea of which applications were running on which servers, you will now find it much more difficult to track applications running on virtual servers. This can really complicate application patching and updates, as well as software licensing.

This is a network management issue. And the larger the virtualized network, the more critical it becomes.

Enterprise virtualization applications now on the market offer strong virtualization management capabilities. They can help IT managers dynamically tag and map all VMs and software applications, enabling efficient patching and updates.

Software licensing restrictions

Historically, software vendors have relied on hardware-based licenses. However, in many cases, that approach will restrict usage in the virtualized environment. Microsoft software licenses, for example, cannot be skirted by installing multiple VMs on a single physical server; each VM will have to be licensed.

Although Microsoft has shifted from installation-based licensing to instance-based licensing to accommodate the needs of virtualization, the restrictions on live migration of VMs to other physical servers can be confusing. Other vendors have simpler licensing terms whereby a single license for a physical server permits installation of unlimited VMs.

Be sure to talk with your vendors about how to address the important licensing issue before you get too far into your virtualization project. If you don't, you might end up paying a sizable penalty for using key applications in your new infrastructure.

Security risks

Virtualization by itself does not enhance your network security. In fact, it could actually increase risk because it can give users a false sense of security, and all the VMs on a server share the vulnerability of the host server. While it's true that a breach on one VM doesn't compromise all the others, it's almost certain that cybercriminals are trying to find ways to penetrate a VM and then escape into the host and from there to your network.

So far, there are no definitive security answers or best practices to help you sort through all the virtualization security issues. However, you should apply all the security basics you've already learned, plus a few common-sense steps.

First, you should harden VMs just as you would the host server. Install antimalware and firewalls, and keep them patched and updated. Next, be sure your virtualization applications are updated and patched. Finally, design your virtualized infrastructure to isolate important data as much as possible.

If you employ network access control (NAC), you might find that it is complicated by virtualization. This is because VMs don't have their own IP addresses, but share the address of the host server.

Virtualization is moving quickly, and CDW is on top of it

Virtualization in all its forms is difficult to even comprehend, especially because new products and technology developments are announced almost daily. Still, it's possible to map out a virtualization approach for your enterprise that lets you take full advantage of current capabilities while also preparing for the future.

CDW's technology specialists have helped hundreds of enterprises successfully implement virtualization across the network infrastructure. We can help you avoid the common virtualization pitfalls while gaining maximum benefits for your organization. Put our experience to work for you. Call your CDW manager or (800) 985-4239 today to find out more.