Virtualization: Why You Shouldn't Jump In Just Yet

by: Nico Favila

Virtualization is the creation of a virtual hardware platform, operating system, storage device or network resource. It is a growing trend in the IT community with the goal of having the IT environment being able to manage itself.

Resource Management & Support

For all of virtualization's benefits – which can be easily found online – there are also concerns which should make you think twice about implementing a virtual environment. Applications that use lots of resources and constant disk and memory access are not suitable in a virtual environment. IT Administrators also have to double-check that what they intend to run or use will work on their chosen virtual environment. While virtualization is gaining ground in the industry, not all software manufacturers offer full-support or offer the license to use their products in a virtual environment since many vendors have not clearly established licensing terms. Having support for such services is important and not having any is a deal breaker.

According to John Enck (Gartner's Vice President for Research), *"Not all workloads are candidates for virtualization, and it isn't always easy to determine which ones are. Also, the cost of virtualization software forces high rates of virtual machine density to achieve return on investment."* A view that most experts share to this day.

Bandwidth

A virtual environment relies heavily on your organization's network bandwidth. Typically, a virtual desktop at its most basic will have the server sending data to the user to refresh mouse movements and keyboard strokes. Multiply the number of virtual desktops to a hundred or more and one will notice that even the basic functions make heavy use of bandwidth. Once users start using applications you can expect bandwidth use to spike even further. The network must be able to handle all the traffic that is coming from many desktops to a single location in the data center. If an organization doesn't have enough bandwidth, virtualization would not be a viable option because it relies on the availability (and lots of it) of said bandwidth to deliver the services the user requires.

Security & Cost

Security for virtual environments is also rather scarce at the moment. In the article *"Seven things that will sink virtualization" by Denise Dubie (Network World),* she states that, *"Such vendors as Altor Networks, Blue Lane Technologies, Catbird and Reflex Security are working to add a layer of security to the virtual environment, but the underlying platform still could suffer an attack, industry watchers point out. The market for virtual security*

products is nascent... Enterprise IT managers have to realize that approaches to securing known environments still can fail, so virtualization presents more opportunity for attackers."

Desktop virtualization can be cost-prohibitive to start while offering a return on investment that is difficult to quantify. With virtual desktop costing 150% to 200% more than traditional PCs according to analysts, IT Administrators have realized that they would also need to calculate for indirect costs when pricing out a project.

Virtualization projects rely heavily upon server redundancy. If your organization hosts all its desktops on one server, your whole user-base is at risk if there is a server outage. Though server clustering and redundant connectivity offers a solution to this problem, one must take into account the network and storage requirements for virtualization that goes with setting up redundant servers. These standby servers must be identical to the primary servers they protect when it comes to network and storage requirements. In what is already an expensive endeavor to undertake, it may become too costly to continue deploying.

Seitz of First American says, *"Typically when doing an ROI against desktops, you don't factor in network and storage costs. You need to break that all down in a per-virtual-machine model. But storage could be a big cost; shared storage is not cheap."*

Virtual Servers, Real Problems

Going hand-in-hand with desktop virtualization is server virtualization. Per Webopedia, it is defined as, *"Server virtualization is the partitioning of a physical server into smaller virtual servers. In server virtualization the resources of the server itself are hidden, or masked, from users, and software is used to divide the physical server into multiple virtual environments, called virtual or private servers."* Server virtualization shares most of the same disadvantages that can be found in desktop virtualization while also exhibiting its own unique set of disadvantages.

Canceled Benefit

Server virtualization also faces physical failures like its desktop counterpart. Run a number of servers on one physical host and if that host goes down, all of those servers goes down, severely hampering business continuity. While this can be rectified by investing in redundant hardware, it also cancels out one of the perceived benefits of virtualization – the reduction of hardware, maintenance and office rental space used. If one has to invest in redundant hardware anyway, it would be more feasible to just invest in physical servers to eliminate such concerns. Office rental space should not be a concern because in a recent study provided by Colliers International/Philippines last year, *"Makati CBD rents were generally steady during 2Q10 with only a modest up-tick in the Grade B market. As of*

2Q10, the average rent for Premium Grade office space was unchanged at P795 per sq m monthly (per net useable area). Average rent for Grade A buildings was also steady at P630 per sq m. On the other hand, Grade B office rents increased marginally to an average of P420 per sq m from P415 per sq m in 1Q10.
Outside Makati, because of expanding demand the incentives given by landlords to tenants last year have been steadily reduced and rental rates are expected to increase by 5% to 10% through to end 2010. Makati will lag such growth." Compared to other rental markets, the Philippines offers really low rates for prime office space.

How well do you want your applications to run? Very-well of course. By having a virtualized server though, it's not easy to ensure that is what you'll get. Just like virtualized desktops require bandwidth, applications running on virtual servers require hardware resources. Applications that have a specific set of hardware requirements when run on a physical server usually need more when they are run on a virtual platform. This makes it crucial to plan for the number of extra resources an application would need to run on a virtual server. An additional challenge to that is almost every application differs on the amount of resources it needs when run in a virtual server. Facing these issues, it may be more beneficial to leave applications running on a physical server than a virtual one.

Different Skills for the Virtual Realm

A new environment requires a new set of skills. While an IT Administrator may have all the necessary skills to run physical servers, those skills don't necessarily translate to a virtual environment. Administrators need to change their train of thought when handling a virtual server simply because it doesn't behave the same. Configuring a physical server to run based on a set of specifications doesn't mean that a virtual version will be configured the same, Administrators first have to use performance monitoring tools to gauge the amount they would need in the virtual environment (multiplied by the amount of virtual servers running on the hardware) to make sure that the hardware is being used to capacity.

Troubleshooting a virtual environment adds more tools to use for admins and more work. In order to see the whole picture of what's happening on the server, you would need access to the virtualization toolset to find out the impact on the virtual machines. The concern here is that these toolsets are not freely available. Also, when it comes to disaster recovery, it is hard to find a tool that supports all the various virtualization solutions, leaving you with different sets of tools for different virtual environments.

Virtual Security?

Security on virtual environments is also quite troublesome. Some of these problems are simply because of the architecture of a virtual environment. If malware infects one server, it will potentially affect all virtual machines hosted on that server rather than just a single machine. Virtualization also makes it easy for users to deploy unsupported systems or

applications, making it harder for the organization to maintain security standards and for admins to know what they are trying to manage. Another worrying concern is a scenario in-which an unauthorized user gets access to a server, that user has access to all virtual servers and machines, making it easy for them to compromise highly sensitive data and disrupt service. Unlike a physical server which usually has limited physical control access as found in most data center set ups, a virtual server is much easily compromised than a physical one.

Virtualization may be the new trend in IT these days, but until the very big problems of security and performance – along with all the other problems one faces in having a virtual environment – are resolved, it just isn't the time to join this trend.