How Virtualization Works and its Effects on IT

Oliver Garraux

Information Technology Fundamentals

Professor Johnson

October 31, 2007

How Virtualization Works and its Effects on IT

Over the last five years, virtualization has become a common topic in IT. Once only available on expensive, high end mainframes, virtualization has become a viable option on Intel/AMD platforms as well, thanks to a variety of software makers, most significantly VMware. As it becomes a more mature technology, virtualization can offer many benefits in a wide range of uses – from data centers, to developers and end-users.

Types of Virtualization

There are several ways to classify virtualization software, based on their capabilities and how they operate. Some vendors use terms to mean slightly different things than other vendors. A virtual machine (also called guest by VMware) is an instance of an operating system that is being virtualized, so that it is running on top of another operating system. The hypervisor (also called virtual machine monitor) is the software that facilitates this by managing and running the virtual machines. VMware also refers to the hardware, operating system, and hypervisor as the host.

Up until the last two years, there have only been two options for virtualization on Intel platforms. The first is full software virtualization, and the second is paravirtualization. Full software virtualization was popularized by VMware in 1998. With full virtualization, the hypervisor software intercepts the CPU instructions that are not capable of being virtualized and rewrites them so that it will work with virtualization.

On Intel/AMD x86 processors, there are different levels or rings that software can be executed at. Ring 0 is used by operating system kernel, where Ring 3 is typically used by user mode software (OSR Staff, 2003) – the applications that run on the operating system kernel. Ring 0 has the least restricted access, where the other rings have more restricted access to the processor. With virtualization, the host operating system kernel runs at Ring 0 in the actual processor. The hypervisor runs at Ring 0 as well because almost all virtualization software uses a kernel driver to interact with the host operating system/processor. However, the guest operating systems cannot run in Ring 0 (Extreme Tech, 2001). Because the guest operating system expects to be running at Ring 0 (as it would be if it were running directly on the hardware without any virtualization), it will use some processor instructions that are not accessible from the “outer” rings where it is being executed. Full virtualization software intercepts these instructions and rewrites them using the kernel driver on the host (which is running in Ring 0) (Brodkin, 2007).

The advantage of full virtualization software is that almost all operating systems can be run in the virtual machine without modification, because the hypervisor is able to modify all of the instructions that cannot be passed directly to the processor. It also does not require any of the actual hardware to specifically support virtualization. However, this does add some overhead performance wise. Full virtualization is slower than some of the other alternatives, but because it does not require hardware support or modification of the guest operating systems it was the first to become popular and was what VMware used to get their start. Most current VMware products can work using full software virtualization, however they also offer support for hardware assisted virtualization, which will be covered later.

Paravirtualization came later on. One of the most popular pieces of paravirtualization software is the open source project Xen. Paravirtualization requires the guest operating system to be modified. So, a guest operating system being run using paravirtualization must “know” that it is being virtualized, whereas guest operating systems being run in full software virtualization do not. Paravirtualization is faster because it the guest operating system is modified to run at Ring 1. The hypervisor does not have to intercept and modify any instructions. Because operating systems must be modified to be paravirtualized, proprietary operating systems like Windows generally cannot be virtualized using this method. Because Windows is proprietary, it is not possible to modify the Windows kernel to run in Ring 1, which is needed by paravirtualization software. Paravirtualization is generally only possible with operating systems whose vendors support it. Because Linux is open source it is possible for it to be modified to work on paravirtualization software. Most Linux distributions support being virtualized with Xen. Novell also supports Xen, and has made it possible to run Netware, their older proprietary operating system, on Xen, to assist those who are moving from Netware to Linux.

Hardware assisted virtualization is a relatively new development. Intel released its first processors supporting their version of hardware virtualization (Intel VT) in late 2005 (Mohamed, 2005). AMD supports hardware assisted virtualization (called Pacifica); however, it is not the same as Intel's. Most software that supports hardware assisted virtualization is compatible with both vendors' types of virtualization.

Hardware assisted virtualization works by allowing the guest operating systems to run at Ring 0. Intel's VT splits Ring 0 into two parts: one which the hypervisor runs in, and another that the virtualized guest operating systems run in (Binstock & Gillespie, 2006). This gives hardware virtualization the advantages of both full software based virtualization and paravirtualization. Any operating system can be virtualized with hardware virtualization. This is because like full software virtualization, the guest operating system does not need to be modified. However, hardware based virtualization is typically faster than full software virtualization, because no CPU instructions have to be rewritten. Nearly all virtualization software either supports or is moving towards hardware based virtualization because of its advantages. Additionally, most of Intel and AMD's new processors support their respective virtualization platforms.

Popular Virtualization Software

There are three major virtualization software vendors: VMware, Microsoft, and XenSource. VMware has three virtualization products. VMware Workstation and VMware Server work very similarly. Both of them run/install in an existing host operating system (both Linux and Windows are supported as host operating systems), and allow you to run virtual machines on top of that OS. They both support hardware assisted virtualization, though currently that support is only "experimental" with VMware Server (VMware, Inc., 2007b). VMware's other major product is VMware ESX, also known as VMware Infrastructure. ESX is primarily designed for virtualizing servers for medium or large businesses. Unlike most other types of virtualization software, ESX does not run on a traditional host operating system. Instead, VMware ESX provides its own small proprietary operating system kernel that does the virtualization. This significantly reduces the overhead, by taking the host operating system basically out of the picture. ESX also supports many advanced features, such as hot migration of running virtual machines (marketed as VMotion) (VMware, Inc., 2007a). All VMware products, including Virtual Infrastructure, now have 64 bit support. This allows virtual machines to have a 64 bit operating system installed on them if the underlying hardware is 64 bit.

Microsoft is also a major vendor in virtualization. Most of their virtualization software can be traced back to Virtual Server and Virtual PC, which were bought from Connectix in 2003 (Fried & Wilcox, 2003). Since 2003, Microsoft has added support for hardware assisted virtualization in Virtual PC and Virtual Server. However, neither of them supports 64bit virtual machines. Most of Microsoft's current efforts appear to be in Windows Server Virtualization, also known as Viridian, which will be released shortly after Windows Server 2008. Windows Server Virtualization will run on top of the Windows Server 2008 Core, a light version of Windows Server 2008 that lacks a GUI. It will require a 64 bit processor that supports hardware virtualization and it will support 64 bit guest operating systems (Goldworm, 2007).

Xen originally supported only paravirtualization. However, it was still popular on Linux because it was open source, and was very useful for running Linux virtual machines on top of a Linux host operating system. The Linux kernel had to be modified to run on Xen; therefore, it was not possible to run Windows on top of Xen because it could not be modified. However, with the advent of processors supporting hardware virtualization Xen has become capable of running Windows and other operating systems as well (Pratt, 2006). Xen still supports paravirtualization. In fact Xen can run paravirtualized operating systems and hardware assisted virtual machines side by side. It is best to use paravirtualization when running Linux virtual machines (or Netware, or any other operating system that supports paravirtualization with Xen) on Xen, because paravirtualization is typically better performance-wise than hardware assisted virtualization (Novell, 2007). Recently, XenSource, the company that supports Xen and sells XenEnterprise, was bought by Citrix. Citrix sells software that allows people to run applications remotely over a network using terminal services (Citrix Systems, 2007).

Impact of Virtualization

As virtualization becomes more common, it is making an impact on many parts of information technology. At the most basic level, it gives organizations a means to consolidate multiple lightly-used servers into one physical server running multiple virtual machines. Replacing multiple servers with one server can reduce the costs related to power usage and cooling, in addition to freeing up space in the data center.

Beyond that, however, virtual machines can be used to isolate multiple applications that before would have been running on a single machine. This could potentially make it easier to manage, because administrators would not have to worry as much about how changes in the operating system install relating to one application will affect other applications running on the same install. Instead, multiple operating system installs can be running on one physical server with virtualization.

Virtualization software can also be helpful in development or testing. Desktop virtualization software like VMware Workstation or Microsoft Virtual PC can let developers test a deployment of an application on a server OS without actually having to have a server to deploy it on. Virtualization is also commonly used by those making demonstrations. They can demonstrate a server operating system from their laptop, without having to rely on network connectivity that may or may not be present where they are presenting. Desktop virtualization software is also extremely useful in lab environments, where students or IT staff practice configuring multiple server virtual machines. Running more than one virtual machine would let them see how the servers interact with each other. For instance, you could set up a cluster of Windows file servers, using a Linux virtual machine as shared storage with iSCSI on a single desktop or notebook computer, without any special hardware.

Virtualization is also being used by software makers as a means of distributing their software. This is becoming especially prevalent for evaluation software and some open source server software. Users can download virtual machines with the software pre-configured making it much faster to evaluate or begin using. For example, on VMware's Virtual Appliance Marketplace, you can download an evaluation version of SQL Server 2005 on Windows Server 2003, provided by Microsoft. You can also download a full version of SSL Explorer, an open source web-based VPN server, pre-configured on a Linux virtual machine (VMware, Inc., 2007c). If this trend continues, it could drastically change the way that server software is packaged and how people deploy that software.

Disadvantages

Many people are hesitant to deploy virtualization, primarily for a few primary reasons. One of these reasons is security. Because the hypervisor controls the operating system and interfaces with hardware, it is a potential target for a root kit or other malware. If a hypervisor is infected by a root kit, it could be completely undetectable from inside the operating systems running on the virtual machines, while still having full access to the hardware and data. There are no known vulnerabilities in hypervisors that would allow this, however many are concerned that it is possible (Radcliff, 2007). There have been proof of concepts that have shown it may be possible for malware to virtualize an operating system (that is not already being virtualized), by themselves, though there is no known malware that does this in the wild. Even if there were, using virtualization software would not necessarily make systems more vulnerable to this. Still, many organizations are specifically not using virtualization for outward facing servers, like web servers, even if they use it for internal servers.

Another downside of virtualization is the complexity that it adds to systems. This makes it more difficult for organizations to manage. Adding another layer of complexity adds another layer of things that can go wrong, and more software that has to be installed and configured. Most virtualization vendors provide their own software to manage virtual machines across multiple servers, though there are third party solutions that do this as well. Many companies may not be considering the management aspects of virtualization as much as they should (Gittlen, 20007). This leads to the third major reason that some people are wary of virtualization, reliability. Putting more operating systems on one server means that a single hardware failure can cause downtime for many systems. This is something that should be taken into account when purchasing hardware to run many virtual machines – invest in redundancy.

In summary, operating systems can be virtualized in three ways: full software virtualization, paravirtualization, and most recently, hardware assisted virtualization. All three major virtualization software providers (VMware, Microsoft, and XenSource) support hardware assisted virtualization in some of their products. Virtualization promises to continue to change the way people run computers, by making it easier to isolate applications and develop software for different platforms. It is even changing the way that some software is distributed and deployed. Virtualization has a few potential pitfalls to go along with its advantages, but it can be a very valuable tool and is an important technology to be aware of.

References

Binstock, A., & Gillespie, M. (2006, April 17). *Intel Virtualization Technology: A Primer.* Retrieved October 26, 2007, from Intel: http://cache-www.intel.com/cd/00/00/22/30/223039_223039.pdf

Brodkin, J. (2007, August 20). The Pluses of Virtualization at the Chip. *Network World , 24* (32), p. 48.

Citrix Systems. (2007, August 15). *Citrix Acquisition of XenSource*. Retrieved October 29, 2007, from Citrix: http://www.xensource.com/PressReleases/Pages/pr081507.aspx

Extreme Tech. (2001, December). *Virtual Machines and VMware Part I*. Retrieved October 21, 2007, from Extreme Tech: http://www.extremetech.com/article2/0,1697,1156611,00.asp

Fried, I., & Wilcox, J. (2003, February 19). *Microsoft Buy to Boost Server Efforts.* Retrieved October 28, 2007, from CNet News: http://www.news.com/2100-1001-985149.html?tag=fd_top

Gittlen, S. (20007, August 20). ADP CTO: Take the Slow Road to Virtualization. *Network World , 24* (32), p. 39.

Goldworm, B. (2007, July 25). *Windows Server 2008 virtualization: Preparing customers.* Retrieved October 29, 2007, from TechTarget: http://searchsystemschannel.techtarget.com/tip/0,289483,sid99_gci1265651,00.html

Mohamed, A. (2005, November 22). *Harware-based virtualisation heralds major revamp for PCs*. Retrieved October 27, 2007, from ComputerWeekly: http://www.computerweekly.com/Articles/2005/11/22/213059/hardware-based-virtualisation-heralds-major-revamp-for.htm

Novell. (2007, March). *An Introduction to Xen Virtualization.* Retrieved 10 20, 2007, from San Diego Linux Users Group: http://sdoss.org/events/Presentations/2007/SDLUG%20and%20XEN.pdf

OSR Staff. (2003, May 08). *What are Rings*. Retrieved October 21, 2007, from OSR Online: http://www.osronline.com/article.cfm?article=224

Pratt, I. (2006, October). *Xen in the Enterprise.* Retrieved October 20, 2007, from Cambridge Computer Laboratory - Xen Architecture: http://www.cl.cam.ac.uk/research/srg/netos/papers/2006-xen-linuxworld-london.pdf

Radcliff, D. (2007, August 20). Virtual System, Real Risk. *Netweork World , 24* (32), pp. 30-31.

VMware, Inc. (2007c). *Virtual Appliance Marketplace*. Retrieved October 30, 2007, from VMware: http://www.vmware.com/appliances/

VMware, Inc. (2007a). *VMWare Infrastructure 3.* Retrieved October 28, 2007, from VMware: http://www.vmware.com/pdf/vi_brochure.pdf

VMware, Inc. (2007b, June 22). *VMware Server Product Datasheet.* Retrieved October 28, 2007, from VMware Server Features: http://www.vmware.com/pdf/server_datasheet.pdf