Virtual Machines Technologies

Mircea Bogdan GAGNIUC
University „Politechnica" Bucharest
Faculty of Automatic Control and Computers
gagniuc.mircea@gmail.com

***Abstract*—The paper is focused on Virtual Technologies, that offer many advantages starting to from reduce hardware costs to increase security systems and workstations. A Virtual Machine is presented, as well as the experimental results.**

***Index Terms*—virtual Technologies, virtual Machine, operating system, benchmark**

I. INTRODUCTION

In 1974th Gerald J. Popek and Robert P. Goldberg in "Formal Requirements for Virtualizable Third Generation" 1 have introduced the term of Virtual Machine. In computer science, a virtual machine (VM) is a software implementation of a machine (computer) that executes programs like a real machine. In the article mentioned, they have established that a virtual machine is an efficient, isolated duplicate of a real machine. In today terminology, virtual machines include systems, which have no direct correspondence to any real hardware.

To determine virtualization requirements, Popek and Goldberg introduce a classification of instructions of an Instruction Set Architecture into three different groups:

- Privileged instructions – are those instructions that trap if the processor is in user mode and do not trap if it is in system mode.
- Control sensitive instructions – are those instructions that attempt to change the configuration of resources in the system.
- Behavior sensitive instructions – are those instructions whose behavior or result depends on the configuration of resources (the content of the relocation register or the processor's mode).
- Based on this classification, Gerald J. Popek and Robert P. Goldberg have defined the virtualization requirements starting from two theorems:

Theorem 1. For any conventional (third generation) computer, a Virtual Machine may be constructed if the set of sensitive instructions for that computer is a subset of the set of privileged instructions.

Intuitively, the theorem states that to build a Virtual Machines i is sufficient that all instructions that could affect the correct functioning of the Virtual Machine (sensitive instructions) always trap and pass control to the Virtual Machine. But this condition, is not sufficient.

A related problem is that of deriving the Instruction Set

Architecture requirements for recursive virtualization, that is, the conditions under which a Virtual Machine that can run on a copy of itself can be built. Popek and Goldberg presents the following (sufficient) conditions:

Theorem 2. A conventional (third generation) computer is recursively virtualizable if it is virtualizable and a Virtual Machine can be constructed for it without any timing dependencies.

Of course, their theory are related to the "third generation architectures" (e.g., IBM 360, Honeywell 6000, DEC PDP-10), but is general enough to be naturally extended to current machines.

Creating an Virtual Machine environment, based on Popek and Goldberg theorems there are three conditions to analyze:

Equivalence

A program running under the Virtual Machine should exhibit a behavior essentially identical to that demonstrated when running on an equivalent machine directly.

Resource control

The Virtual Machine must be in complete control of the virtualized resources.

Efficiency

A statistically dominant fraction of machine instructions must be executed without Virtual Machine intervention.

II. SYSTEM VIRTUAL MACHINES

System Virtual Machines (sometimes called hardware virtual machines) allow sharing a physical machine or part of their resources between different virtual machines. The most important fact and able to generate many advantages is that each of Virtual Machine can run its own operating system. The software layer providing the virtualization is called a virtual machine monitor, hyper-visor, or even virtual machine player.

The main advantages of virtual machines are:

- multiple Operating Systems environments can co-exist on the same computer, *in strong isolation* from each other;

the virtual machine can provide an instruction set architecture that is somewhat different from that of the real machine.

Multiple Virtual Machines each running their own operating system (called G*uest operating system*) are frequently used in server consolidation, where different services that used to run on individual machines in order to avoid interference, are instead run in separate Virtual Machines on the same physical machine.

The original motivation to creating Virtual Machines was the desire to run multiple Operating Systems as it allowed time-sharing a single computer between several single-tasking Operating Systems.

The guest Operating Systems do not have to be all the same, it is possible to run different Operating Systems on the same computer (e.g. Microsoft Windows and Linux, or older versions of an OS in order to support software that has not yet been ported to the latest version, as you can see followed). The use of Virtual Machines to support different guest Operating Systems is becoming popular in embedded systems; a typical use is to support a real-time operating system at the same time as a high-level OS such as Linux or Windows.

Another use is to sandbox an Operating System or an software that is not trusted, possibly because it is a system under development. Virtual machines have other advantages for Operating Systems development, including better debugging access and faster reboots.

The main advantage of Virtual Machines for quality-of-service isolation is a result of incomplete resource isolation provided by most contemporary operating systems. Only Solaris Zones are an alternative that provide strong resource isolation within a single operating system. Zones are not virtual machines, but an example of "operating-system virtualization". This includes other "virtual environments" (also called "virtual servers") such as Virtuozzo, FreeBSD Jails, Linux-VServer, chroot jail and OpenVZ. These provide some form of encapsulation of processes within an operating system. These technologies have the advantage of being more resource efficient than full virtualization; the disadvantage is that they can only run a single operating system and a single version/patch-level of that operating system - so, for example, they cannot be used to run two applications, one of which only supports a newer Operating System version and the other only supporting an older Operating System version on the same hardware.

III. VIRTUALIZATION ON X86 MACHINES.

Virtualization was first implemented more than 30th years ago by IBM as a possibility to partition mainframe computers into separate Virtual Machines. These partitions allowed mainframes to run multiple applications and processes at the same time.

Virtualization was abandoned during the 1980s and 1990s when client-server applications and inexpensive x86 servers and desktops established the model of distributed computing. Instead of sharing resources centrally in the mainframe model, organizations used the low cost of distributed systems to build up their networks and needs. The large acceptance of Windows and Linux as server operating systems in the 1990s, established x86 servers as the industry standard. The growth in x86 server and desktop deployments has introduced new IT infrastructure and operational challenges, which consist in:

Low Hardware Utilization. Typical x86 server deployments achieve an average utilization of only 10% to 15% of total capacity, according to International Data Corporation. Organizations typically run one application per server to avoid the risk of vulnerabilities in one application affecting the availability of another application on the same server.

Increasing Physical Infrastructure Costs. The operational costs to support growing physical infrastructure have steadily increased. Most computing infrastructure must remain operational at all times, resulting in power consumption, cooling and facilities costs that do not vary with utilization levels.

Increasing Information Technologies Management Costs. As computing environments become more complex, the level of specialized education and experience required for infrastructure management personnel and the associated costs of such personnel have increased. Organizations spend disproportionate time and resources on manual tasks associated with server maintenance, and thus require more personnel to complete these tasks.

Insufficient Failover and Disaster Protection. Organizations are increasingly affected by the downtime of critical server applications and inaccessibility of critical end user desktops. The threat of security attacks, natural disasters, health pandemics and terrorism has elevated the importance of business continuity planning for both desktops and servers.

High Maintenance end-user desktops. Managing and securing enterprise desktops present numerous challenges. Controlling a distributed desktop environment and enforcing management, access and security policies without impairing users' ability to work effectively is complex and expensive. Numerous patches and upgrades must be continually applied to desktop environments to eliminate security vulnerabilities.

Due to evident advantages of using Virtual Machines instead of physical machines, the problem of 90th years were using the "popular" x86 machines as "host" operating system for guest Virtual Machines. The problem is generated by the x86 processors architecture, because they did not meet the Popek and Goldberg requirements. That problem is begin to be solved, starting from 2005, when Intel was officially launched Intel Virtualization Technology, which is already available on some Pentium 4 models, Pentium D, Xeon, Core Duo and Core 2 Duo.

Of course, AMD has developed his own AMD Virtualization technology, which is present in AMD Athlon 64, Turion 64, Phenom, Opteron and all their newer processors.

For the future, both processor producers intent to extend virtualization technology from processor to chipse, BIOS, and perhaps, software. For example, Intel already present an technology named Virtualization for Directed I/O which can provide a way of configuring interrupt delivery to individual Virtual Machines for preventing a Virtual Machine from using DMA to break isolation.

A similar technology developed by AMD is I/O Memory Management Unit.

As I describe already, the x86 architecture producers, only in the past of two-three years has begin developing useful technologies for virtualization techniques. But, the user need have determined software developers to solve x86 problems before architecture producers. Therefore, on February 8, 1999, VMware introduced *the first x86 virtualization product*, based on techniques which were filed

for a Patent by Vmware in October 1998.

Due to x86 processor architecture, VMware and similar virtualization software for the x86, must employ sophisticated techniques to trap and virtualize the execution of certain instructions.

Before 2005, when Intel or AMD have announced their technology some, some software producers have tried to develop some techniques based on x86 architecture and Operating Systems of that years[2].

Now, a lot of software is known to conditionally make use of virtualization technology features, like as:

- Microsoft Virtual PC 2007 / supports both Intel VT-x and AMD AMD-V virtualization techniques;
- VirtualBOX supports both AMD-V and VT-x techniques.
- VMware Workstation supports Intel VT-x virtualization.
- XEN, supports Intel VT-x and AMD-V
- Padded Cell - virtual machine technology from Green Hills Software hosted on INTEGRITY real-time operating system, supports Intel VT-x.
- Kernel-based Virtual Machine - a Linux kernel module.

This is a small enumeration for illustrate the actual tendencies in developing Virtual Architectures and Software Techniques based on x86 machines.

IV. Virtual Machines Potential.

Starting from an Intel DualCore Machine running Windows XP with Service Pack 2, I want to illustrate the possibilities which can be useful using virtualization techniques. For this example, I have choose the VMware's Virtual Workstation product (as an initiator of virtualization on x86 architecture).

Like I said, I had use an Intel Dual Core machine, as is describe in Fig 1.

Motherboard:

CPU Type	DualCore Intel Pentium D 820, 2800 MHz (14 x 200)
Motherboard Name	Asus P5GZ-MX (2 PCI, 1 PCI-E x1, 1 PCI-E x16, 2 DDR2 DIMM, Audio, Video, Gigabit LAN)
Motherboard Chipset	Intel Lakeport-G i945GZ
System Memory	1527 MB (DDR2-533 DDR2 SDRAM)
BIOS Type	AMI (11/30/06)

Display:

Video Adapter	Intel(R) 82945G Express Chipset Family (64 MB)
3D Accelerator	Intel GMA 950
Monitor	Plug and Play Monitor [NoDB] (F1NQ750088913)
Monitor	Plug and Play Monitor [NoDB] (F1NQ750088913)

Multimedia:

Audio Adapter	Realtek ALC883 @ Intel 82801GB ICH7 - High Definition Audio Controller [A-1]

Storage:

IDE Controller	Intel(R) 82801G (ICH7 Family) Ultra ATA Storage Controllers - 27DF
IDE Controller	Intel(R) 82801GB/GR/GH (ICH7 Family) Serial ATA Storage Controller - 27C0
Disk Drive	SAMSUNG SP2504C (250 GB, 7200 RPM, SATA-II)
Optical Drive	TSSTcorp DVD-ROM SH-D162C (16x/48x DVD-ROM)
SMART Hard Disks Status	OK

Partitions:

C: (NTFS)	38468 MB (33451 MB free)
D: (NTFS)	200004 MB (145238 MB free)
Total Size	232.9 GB (174.5 GB free)

Input:

Keyboard	Standard 101/102-Key or Microsoft Natural PS/2 Keyboard
Mouse	Microsoft PS/2 Mouse

Network:

Primary IP Address	192.168.0.19
Primary MAC Address	00-1A-92-95-98-C0
Network Adapter	Marvell Yukon 88E8001/8003/8010 PCI Gigabit Ethernet Controller (192.168.0.19)

Figure 1. Description of Host Machine.

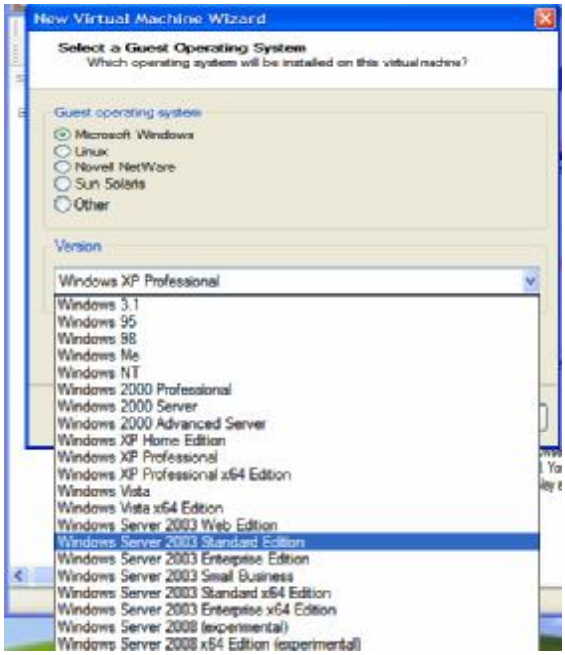

Figure 2. Windows OS capabilities for guest machine.

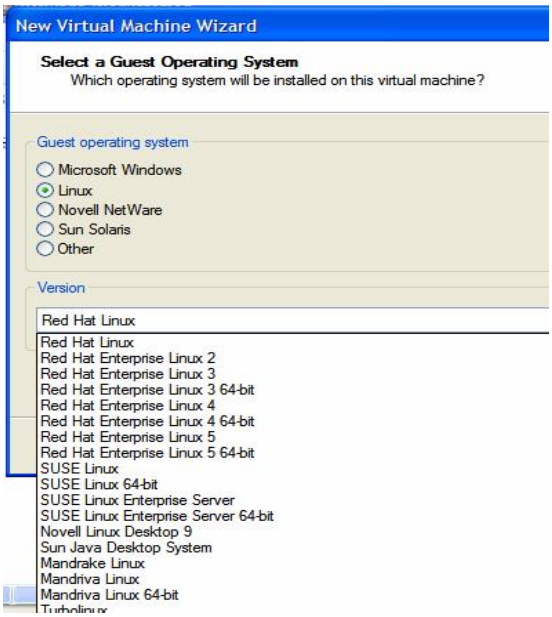

Figure 3. Linux OS capabilities for guest.

As it can see from Fig 1 and Fig 2, VMware offer many possibilities for guest machine's Operating System. In figures illustrated bellow, I have shown only Windows and Linux possibilities of choice. But, VMware offer two more Operating Systems capabilities, like Novell Netware or Sun Solaris.

For my description, I have chosen for the Virtual Machine, the Windows Server 2003 Standard Edition OS.

After this selection, next step is to create the virtual machine. Using Virtual Machine Hardware Tab offered by VMware software, it is easily to understand one of the big advantages for using this technique: we can create a new computer, starting from the host computer, *without any supplemental cost.*

For creating virtual machine, all activities to do is choosing hardware components according to final result needs. In this explained example, the virtual machine is defined as an an Intel Dual Core Machine, with 663 MB, 51 GB HDD (with only one NTFS Partition), with I/O adapters implemented by VMware software. Of course, all I/O devices (Floppy Disk Drives, CD-ROM or DVD-ROM drives, USB Ports) can be added to virtual machine, based on physically existents on host computer.

Now is necessary a comment. The Memory section provides the following information to help user to choose an appropriate amount of memory for the virtual machine: *Guest OS recommended minimum*, is the minimum that the operating system vendor recommends for the operating system to run. *Recommended memory* represent the minimum that VMware recommends for running this virtual machine. If it is allocated more or less memory than is recommended, the Virtual Machine might perform poorly. This recommendation takes into account the amount of memory allocated for all powered-on virtual machines, as described in Memory Tab. *Maximum recommended memory* is the recommendation for best performance when this virtual machine is the *only virtual machine running.* Because starting virtual machine based on host operating system, allocating more memory to this virtual machine can have a negative impact on the host's performance, including the host's ability to run VMware Workstation properly.

So, the first conclusion is that using virtualization techniques needs to configure the host (physically) computer with supplement hardware than a usual machine. Imagine one host computer on which is running simultaneous three new different guest machine: using a simple 1 GB memory RAM host machine, that will established some limits for Operating System guests. And, sharing the only 1 GB memory of RAM for four machines (the host and three guests) this fact certainly will create difficulties for the host machines to operate his one system, or even VMware software.

Another disadvantage determined by using this virtual techniques, is the reduce possibilities to use another video adapter. More exactly, virtual machine has an video adapter emulated by software, any video command being trapped and redirected to host video adapter. Therefore, creating a virtual machine for video purposes will be a mistake, because the virtual hardware will have some limitations from original hardware. About displays, Virtual Machine can use host settings, which is enough for most cases. Selecting this option means that if the Virtual Machine is running on a host that is using one monitor, the virtual machine will see only one monitor. But if the same virtual machine is moved to a different host that is using two monitors, the virtual machine will see two monitors. Another possibility is to specify monitor settings. This option enables user to specify the number of monitors and maximum resolution of any one monitor.

Another virtual component who needs some comments is the Network Adapter. VMware offer many posibilities to set the isolation between host and guest(s) or between guests.

For Virtual Machine, Vmware software create one virtual Ethernet adapter (called VMnet0) who is bridged to an

active Ethernet adapter on the host computer. By default, Workstation automatically bridges VMnet0 to the first available physical Ethernet adapter on the host. Anyway, the software give the user possibility to choose the desire phissycaly Ethernet host adapter to bridge at the virtual Ethernet adapter(s). By network settings, user can make the host computers and guest(s) computer to communicate which other like in a local area network enviroment. This facility is creating another advantages of using virtualization techniques: for different network testing purposes, is more easily and convenient to create and set two ore more Virtual Machines than use of two or more physically computers.

But, the network comunications is not the only posibility to control the isolation between guest and host machines. The software offer an entire options menu to controlling the isolation between machines running on the same host:

The guest isolation features enable user to:

• Copy and paste text and files from the host computer to a Linux, Windows, or Solaris 10 guest, and vice versa.

• Drag and drop files from the host computer to a Linux, Windows, or Solaris guest, and vice versa. User can also drag files from a file manager to an application that supports drag and drop, or from applications such as zip file managers that support drag-and-drop extraction of individual files.

• Copy and paste text and files, or drag and drop files, from one virtual machine to another. It's easy understandable that data communications is very facil between all machines (real or virtual) running in a moment of time.

Even that, there is two more posibility to comunicate between host and guests computers, or only between guests computers. Shared folders, provide another easy way to share files among virtual machines, and between virtual machines and the host. The shared folder panel includes the following settings:

• Folder Sharing can be select as Enabled or Disabled, with two posibilities: until next power off or suspend if you want to enable folder sharing temporarily, until you shut down, suspend, or restart the virtual machine. Or, selecting this option Always, give user permision to enable or disable specific folders in the Folders section permanently.

• Folders Section – Give user the posibility to choose which folders (from host disk partitions) will be share between host and guest(s) computer.

Another usefull posibility to change files between host and guest computer, is the software capabilities to map a virtual disk to a drive on the host as an alternative to using shared folders or copying data back and forth between a Windows guest and host. Using a mapped drive enables user to connect to the virtual disk without having to go into a virtual machine at all. Even if Vmware offer posibility to open files on virtual partitions in modified mode, it is strongly recommended users to leave the check box called Open file in read-only mode selected. This setting prevents user from accidentally writing data to a virtual disk that might be the parent of a snapshot or linked clone. Writing to such a disk could make the snapshot or clone unusable.

Another attention is necesarry because maping a drive to the virtual disk, you will not be able to power on any virtual machine that uses that disk until you disconnect the virtual disk from the host. More than that, take the following considerations into account when mapping a virtual disk:

• it can be mounting volumes formatted with FAT (12/16/32) or NTFS only. If the virtual disk has a mix of partitions (volumes) where, for example, a partition is unformatted or is formatted with a Linux operating system and another partition is formatted with a Windows operating system, you can mount the Windows partition only.

• user can mount a virtual disk that has a snapshot, but if you write to the disk, you can irreparably damage a snapshot or linked clone previously created from the virtual machine.

• you cannot mount a virtual disk if any of its .vmdk files are compressed or have read-only permissions. It is necessary to change these attributes before mounting the virtual disk.

Even with that limitations, there is a lot of posibilities settings for host and guest(s) machines to communicate wich other.

After those settings, the virtual machines can be finalized for creation. The result will be some *.vmx files (for Virtual Machine configuration settings) and *.vmdk for virtual disk partitions. From this, result another advantage of use Virtual Machines techniques: on an real amovable Hard Disk which on is hosted one or more Virtual Machines, which is moved on another computer compatible with VMware, the new host computer can suport and start the guest computers that are already created on Amovable Hard Disk. It is not necessary to describe now, what advantages result from carrying two or more computers, in one only HDD.

Returning to my example, after finished creating an Virtual Machine, next (and final)step was to install and set the Operating System who was chosen for that guest (Windows 2003 Server Standard Edition). The final test was to start simultaneously the host and the guest and trying to benchmark the two systems. Result of that test is shown in Fig. 4.

For benchmark was use the same software, in two situations: first, was benchmarked the host machine, without any software running. Then, after Virtual Machines was starting, both (the host and the guest) was benchmarked with the same software.

The test result shown in Fig 4, demonstrate that two machines can run simultaneosly without any singnificant loss of power for both (real and virtual machine).

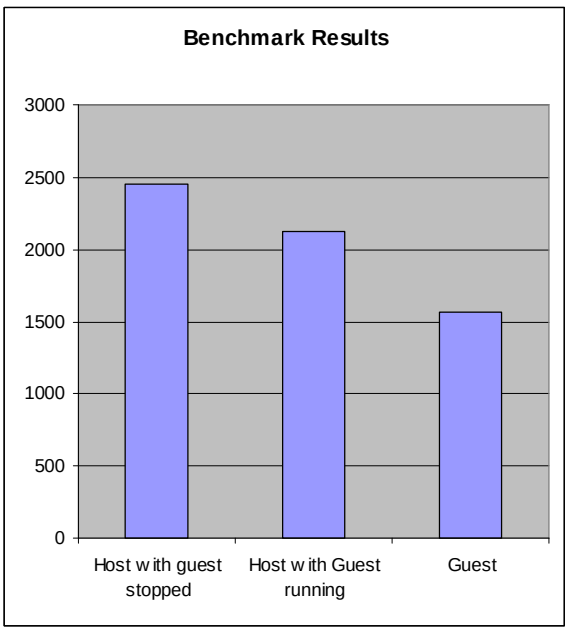

Figure 4.

I. CONCLUSIONS.

As I demonstrate before, using Virtual Technologies offered today by processor architecture producers and software developers, offer many advantages starting to from reduce hardware costs to increase security systems and workstations.

One of the most important advantage of using isolation between host and guest, is that the host is independent of what is happend with the Operating System installed on the guest. Even if guest computer is virused, the Operating system is became instable, the host remain intact. And all this problems can solve with a simple file deletion and creating a new, clean and sure virtual machine. Of course, manipulating without care of file sharing between machines, cand transmit the problems from a machine to another. But, this is an hypotethically option that can be disabling by user.

Another advantage, is the portability of one ore two computers: Vmware can create clones of real machines, which can be copied on different data supports, and carrying and transported easily to another locations, where can be juast starting and use conform desires.

And the most impotant advantage, in my opinion, is the posibility to test any software, any Operating System, without concern about what is happend with the host computer. Using a Virtual Machine, only component who can be damaged is two ore more files from host hard-disk partitions, files which can be deleting and recreating according to user needs.

REFERENCES

[1] Gerald J. Popek and Robert P. Goldberg (1974). "Formal Requirements for Virtualizable Third Generation Architectures". Communications of the ACM 17 (7): 412 –421.

[2] Hardware Requirements for 64-Bit Guest Operating Systems. VMware, Inc. (2007-03-20). Retrieved on 2007-10-10.

[3] Intel Pentium 4 Processor 6xx Sequence and Intel Pentium-4 Processor Extreme Edition Datasheet - Intel.

[4] The Patent was granted as U.S. Patent 6,397,242 on May 28, 2002

[5] VMware Virtual Platform in 1999, Plex86 – a project to support only Linux as a guest operating system, Microsoft Virtual PC and Microsoft Virtual Server.