Virtualization and the Computer Architecture

Rakhi Poonam Verma
Computer Science Department
San Jose State University
San Jose, CA 95192
408-924-1000
rakhipoonam.verma@sjsu.edu

ABSTRACT

In this paper, we study a worthy new direction for computer architecture i.e., virtualization. The computer hardware of today's world was designed and architected for the purpose of running a single operating system and its applications and therefore most of the hardware of such computer would be left underutilized. Virtualization enables the option of running multiple virtual computers on a single physical system. This paper studies about virtualization, importance of virtualization in today's world and various ways, through which virtualization is supported in computer systems. We will also study impact of virtualization on computer architecture. We will see the impact of virtualization on current processors and the different problems with x86 architecture and how these problems are resolved i.e., virtualization extensions for current processors.

1. INTRODUCTION

Virtualization in simple words means to virtualize the underlying hardware and abstract it away from the end user. Virtualization means to create a virtual version of a device or resource, such as a server, storage device, network or even an operating system where the framework divides the resource into one or more execution environments. Virtualization has been in existence in computer world since a long time. For example, partitioning a hard drive is considered virtualization because one drive is represented as two separate hard drives. In virtualization devices, applications and humans interact with the virtual resource as if it were a real single logical resource. It has revolutionized how computer hardware is organized, used and visualized in today's world. [1] With the advent of virtualization, the pace at which computers affect our day to day life has increased dramatically. Virtualization techniques allow us to run multiple operating systems on the same hardware at the same time. This provides a way to use CPU and Memory resources with high utilization rate as compared to a system where only one operating system can run at a time.

2. ADVANTAGES OF VIRTUALIZATION

Virtualization has brought a big boom in the IT industry in terms of resource utilization, high availability, increased security, easier access, etc. with all these things at considerably low cost. Here are some advantages of virtualization [2]:

2.1 Hardware Abstraction

With Virtualization, hardware is nearly completely abstracted from the end user. The service vendors create huge clusters of hardware like storage, compute resources like CPU and Memory, networks etc., at their preferred locations, and then use virtualization techniques to provide access to these clusters to the customers. The customers just ask for their desired resources like 500 GB storage, 2 Core CPU and 5 GB RAM. The customers don't know where their resources are coming from, or where their data or workload is being hosted. This provides the advantage to the vendors to move the workload to some other location, in case some disaster occurs at the original location.

2.2 Ease of Migration

As stated above, the vendors or the customers can migrate or move their workload of virtual machines to different location if some disaster occurs at the original location. If some vendors have multiple datacenters or clusters deployed, then they can move the virtual machines to datacenters which are closer to customer's location to improve performance and user experience.

2.3 Encapsulation of Storage

Vendors can buy large capacity storage and create partitions on them as desired by the customers. This enables simplified system backup and restore, since the whole storage disk can be backed up in a single attempt.

2.4 Ease of Growth

Virtualization provides a simple way to cater to expanding hardware requirements. More hardware can be added to the clusters anytime without the customers knowing. Without virtualization, whenever hardware was added to the cluster, there was always some downtime associated to it. Thus virtualization brings a huge advantage with it, because if the requirements from the customers are increasing at a rapid rate, then adding the required hardware can actually keep up with them without any downtime.

2.5 Improved Monitoring & Troubleshooting

Most virtual environments allow management of all physical hosts through a central console where you can easily compare resource usage and see a history of tasks and events. You can easily make comparisons between physical and virtual servers and perform in-depth analysis and troubleshooting. Since hardware is abstracted from the user, their workloads can be moved to different place without the user's knowing about it. This way, faulty or broken hardware can be fixed/replaced without any downtime in user's services.

2.6 Workload Consolidation

In a single operating system environment without virtualization, most physical boxes are incredibly under-used because of software limitations (such as the need to separate applications or roles from each other). But, with virtualization techniques, the

resource utilization can be increased to more than 80-90% by performing load balancing algorithms. ~2-100 workloads can be placed on a single piece of hardware reducing physical purchases dramatically, as well as lowering energy and cooling costs. Rather than needing to put in a purchase order for a new server, you can have a new virtual machine spun up in minutes.

2.7 Improved Remote Management

Remote Management capabilities allow you to completely manage a machine from a remote location. You can address what would have typically been an on-site visit through a remote console, including resource upgrades, network troubleshooting, power on/off operations, and more. This can greatly increase the efficiency of server management while cutting travel costs and downtime.

3. HOW VIRTUALIZATION WORKS

Virtualization of computer hardware is done by a component called Virtual Machine Monitor (VMM). VMM is the control system at the core of virtualization. It acts as the control and translation system between the VMs and the hardware [3]. Specifically, the monitor sits between OS(s) and the hardware and gives the illusion to the each OS that it controls the machine. But in reality, the monitor is in control of the hardware, and multiplexes, load balances and time slices running OS instructions across the physical resources of the machine. The VMM can be viewed as an operating system for operating systems, but at a much lower level. The design of VMM such that the running OS still thinks that it is interacting with the physical hardware itself. The main challenge of VMM is the efficient controlling of physical platform resources; this includes memory translation and I/O mapping. With the complex, time consuming operations involved to create and run them, virtual machines, until now, showed significant performance reductions compared to dedicated physical machines [4].

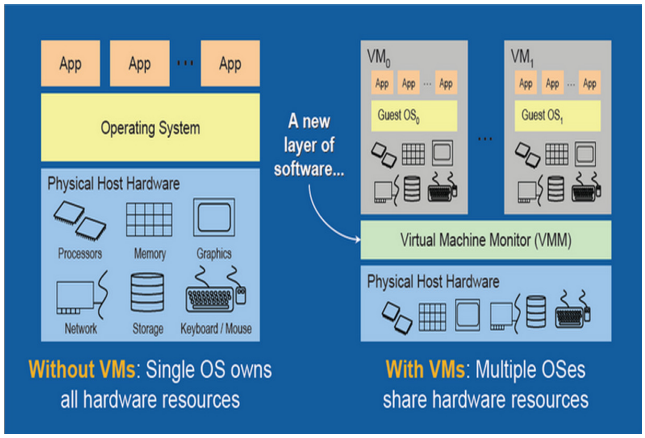

Figure 1 Virtual Machine Monitor [3]

4. THE CHALLENGES IN X86 HARDWARE VIRTUALIZATION

4.1 x86 architecture was not virtualizable

The x86 architecture executed instruction using a Ring architecture with 4 Rings from 0-3. The privileged instruction by the OS were run at Ring level 0 while the user level instructions were run at Ring level 3. To enable virtual environment, there was a need to run instructions in all Ring levels. The main challenge was that since VMM is not an actual OS, how could it run the Ring level 0 commands initiated by guest OS (which thinks that its interacting with hardware directly).

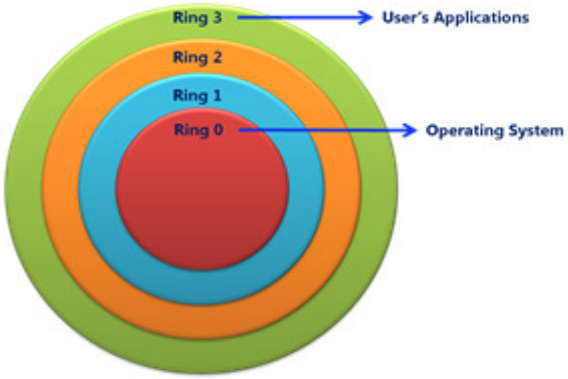

Figure 2 OS Ring based privileges

4.2 x86 architecture had daunting complexity

The x86 architecture was CISC architecture and that too with incredibly large instruction set. The majority of these instructions included legacy support for multiple decades of backwards compatibility. Over the years, it had introduced four main modes of operations (real, protected, v8086, and system management), each of which enabled in different ways the hardware's segmentation model, paging mechanisms, protection rings, and security features (such as call gates). This versatility in instruction set added a huge challenge to support all instructions and operating systems by the VMM.

4.3 x86 machines had diverse peripherals

Although there were only two major x86 processor vendors, the personal computers of the time could contain an enormous variety of add-in cards and devices, each with their own vendor-specific device drivers. Virtualizing all these peripherals was intractable. This had dual implications: it applied to both the front-end (the virtual hardware exposed in the virtual machines) and the back-end (the real hardware the VMM needed to be able to control) of peripherals.

4.4 Need for a simple user experience

The main aim of VMM is to virtualize hardware and abstract it away from the end users. Classic VMMs were aimed to be installed in factories where an expert can install/updated/maintain the software. But, in the modern days, virtualization was becoming a requirement for home users as well. So, a simple solution that could be installed

by anyone was required, otherwise the reach of virtualization would have been restricted [5].

5 OVERVIEW OF INTEL VIRTUAL TECHNOLOGY

Intel was first in providing hardware specifications to VMM vendors that significantly reduced the overhead of VMM operations and greatly improve the speed and abilities of the VMM. Intel® Virtual Technology (Intel® VT) is a specification that has been included in Intel hardware shipped since 2005. It provides a flexible set of hardware primitives to aid VMM software and has the broadest hardware and software support [3].

The advent of Intel VT technology marked the start of support for virtualization in the hardware itself. This simplified the development of virtualization software, since many of the challenges seen above were addressed in the hardware, and the developers could focus more on providing better user experience and flexibility in using the software. Since, hardware began to support virtualization; standardization of the hardware and minimum requirements for virtualization software was done, so that it becomes easy and convenient for the end users to choose between all the available options.

The Intel VT technology had the following advantages:

5.1 Reduce VMM Complexity

As stated earlier, due to diversity in the instruction sets of x86 architecture, and inconsistency between different vendors with x86 architecture of Intel, VMMs got very complicated in order to support all the flavors of hardware available. With Intel VT technology, standardization of hardware to support virtualization was made, which greatly reduced the complexity of VMMs. This Closed hardware “virtualization holes” by design and hence were more efficient and durable.

5.2 Enhance Reliability, Security & Protection

Since hardware now had the support for virtualization natively, the stability, durability and security of VMMs increased greatly, since these can now be controlled in an isolated manner.

5.3 Improve Functionality

Intel’s computer architecture was already supporting a large number of computers in the world with a variety of Operating systems. It also had the facilities to support the variety of I/O peripherals available. By incorporating virtualization into computer architecture, native support for all these existing functionality was provided which became one of the biggest reasons for the wide usage of virtualization.

5.4 Increase Performance

Intel VT technology improved the performance of virtualization software manifold. It eliminated unnecessary transitions to VMM, provided new address-translation mechanisms (for CPU and devices) to improve accessing memory speeds, reduce memory requirements (translated code, shadow tables) etc.

6. INTEL VT HARDWARE SPECS

• VT-x for the IA-32 and Intel®64 Architecture - Available in all Intel-based processors (server, desktop, mobile)

• VT-i for the Intel® Itanium® Architecture - Available in Intel® Itanium® processor-based servers since 2005

• VT-d for Directed I/O Architecture - Intel is working with VMM vendors to deliver software support with systems in 2007.

• Secure Virtualization Core™ Micro-architecture support for Intel® Trusted Execution Technology - A set of hardware extensions that provide creation of multiple separated execution environments (partitions) that help protect the confidentiality and integrity of data stored or created on the PC.

With Intel VT-x, there are two distinct modes of CPU operation: VMX root mode and non-root mode.

• In root mode, the CPU operates much like older generations of processors without VT-x support. There are four privilege levels ("rings"), and the same instruction set is supported, with the addition of several virtualization specific instruction. Root mode is what a host operating system without virtualization uses, and it is also used by a hypervisor when virtualization is active.

• In non-root mode, CPU operation is significantly different. There are still four privilege rings and the same instruction set, but a new structure called VMCS (Virtual Machine Control Structure) now controls the CPU operation and determines how certain instructions behave. Non-root mode is where guest systems run.

The VMCS provides fairly fine-grained control over what the guests can and can't do. For example, a VMM can allow a guest to write certain bits in shadowed control registers, but not others. This enables efficient virtualization in cases where guests can be allowed to write control bits without disrupting the hypervisor, while preventing them from altering control bits over which the hypervisor needs to retain full control. The VMCS also provides control over interrupt delivery and exceptions.

VT-x inherently avoids several of the problems which software virtualization faces. The guest has its own completely separate address space not shared with the hypervisor, which eliminates potential clashes. Additionally, guest OS kernel code runs at privilege ring 0 in VMX non-root mode, obviating the problems by running ring 0 code at less privileged levels. For example the SYSENTER instruction can transition to ring 0 without causing problems. Naturally, even at ring 0 in VMX non-root mode, any I/O access by guest code still causes a VM exit, allowing for device emulation [6].

7. CONCLUSION

In this paper we studied the basics of Virtualization and the big advantages it has. Due to the development of hardware to support virtualization, the reach and benefits of it have increased manifold. Virtualization has added high stability, security, high availability and ease of access to compute resources while reducing cost in all directions. With the development of virtualization technologies by companies like VMware, Amazon, Microsoft etc., it has become really easy to access hardware resources from any part of the world. Any single user or a small startup can now focus more on developing interesting solutions to real world problems than worrying about budgets and hardware maintenance. We mentioned the main challenges that were present

in the legacy x86 architectures that prevented virtualization software from flourishing in the past. Intel's VT technology addressed all these challenges and added support for virtualization in hardware. This gave the virtualization field a big boost which led it to become a huge success and helped the computer industry to make lives of humans far more convenient.

REFERENCES

[1] What is Virtualization? Webpedia. webopedia.com. [Online] [Cited: November 04, 2014.] http://www.webopedia.com/TERM/V/virtualization.html.

[2] E, Justin. Understanding the Benefits of Virtualization. spiceworks.com. [Online] 2013. [Cited: November 06, 2014.] http://community.spiceworks.com/how_to/show/42797-understanding-the-benefits-of-virtualization.

[3] The Advantages of Using Virtualization Technology in the Enterprise. intel Developer Zone. [Online] intel, March 05, 2012. [Cited: November 06, 2014.] https://software.intel.com/en-us/articles/the-advantages-of-using-virtualization-technology-in-the-enterprise.

[4] Virtual Machine Monitors. [Online] University of Wisconsin. [Cited: November 06, 2014.] http://pages.cs.wisc.edu/~remzi/OSTEP/vmm-intro.pdf.

[5] BUGNION, EDOUARD, et al. Bringing Virtualization to the x86 Architecture with the Original VMware Workstation. ACM Transactions on Computer Systems. November, 2012, Vol. 30, 12.

[6] Chapter 10. Technical Backround. virtualbox.org. [Online] Oracle. [Cited: November 06, 2014.] https://www.virtualbox.org/manual/ch10.html.