ACM Word Template for SIG Site

1st Author

2nd Author

Jim Xu

**ABSTRACT**

abs

**Keywords**

keys

# INTRODUCTION

intros

# A literature survey of the topics that contrasts different approaches to the problem

Gerald and Robert, in their article, *Formal Requirements for Virtualizable Third Generation Architectures*, classified two types of hypervisors.(Figure 1)



**Figure 1. two types of hypervisors**

Type-1 is native or bare-metal hypervisor, it runs directly on host hardware to control the underlying hardware as well as manage guest OS. This is a technique where the abstraction layer sits directly on the hardware and all the other blocks reside on top of it. The Type 1 hypervisor runs directly on the hardware of the host system in ring 0. The task of this hypervisor is to handle resource and memory allocation for the virtual machines in addition to providing interfaces for higher level administration and monitoring tools.The operating systems run on another level above the hypervisor. Modern equivalents include Xen, Oracle and Microsoft Hyper-V. Another one is hosted hypervisor (type-2 hypervisor), it runs as a process on the host. Guest OS Virtualization is perhaps the easiest concept to understand. In this scenario the physical host computer system runs a standard unmodified operating system such as Windows, Linux, Unix or MacOS X, and the virtualization layer runs on top of that OS being in effect a hosted application. In this architecture, the VMM provides each virtual machine with all the services of the physical system, including a virtual BIOS, virtual devices and virtual memory. This has the effect of making the guest system think it is running directly on the system hardware, rather than in a virtual machine within an application.VMware is an example of type-2 hypervisors. However, Kernel-based Virtual Machine (KVM) can act as type-1 and type-2 hypervisors at the same time [1].

2.1 Type-1 Hypervisor (native or bare-metal hypervisor)

Xen is a virtual open source project developed by the Computer Laboratory of the University of Cambridge. Xen can safely execute multiple virtual machines on a set of physical hardware, which is extremely close to the operating platform and has the least resources. Xen is known for its high-performance and acquiring less resources, and thus wins a high degree of recognition and support from IBM, AMD, HP, Red Hat and Novell and many other world-class hardware and software manufacturers. Xen, based on X86 architecture, is a virtualization technology that has fastest growing speed, the most stable performance and minimal sources. Novell SUSE Linux Enterprise Server is the first to use Xen virtualization technology. It is particularly suitable for server application integration, which can effectively save operating costs, improve equipment utilization, maximize the use of data center IT infrastructure.

In the Xen environment, there are two main components (Figure 2). One is the virtual machine monitor (VMM), also known as hypervisor. The hypervisor layer is the first layer of hardware that must be loaded first between the hardware and the virtual machine. Once the hypervisor is loaded, you can deploy the virtual machine. In Xen, the virtual machine is called "domain". In these virtual machines, one of them plays a very important role, is domain0, has a very high privilege. Typically, the operating system installed before any virtual machine has this privilege [2].

Domain0 is responsible for some specialized work. Since the hypervisor does not contain any drivers for hardware conversations and interfaces to the administrator, these drivers are provided by domain0. With domain0, administrators can use some Xen tools to create other virtual machines (the Xen term is called domainU). These domainU are also called unprivileged domains. This is because in the x86-based CPU architecture, they will never enjoy the highest priority, while only domain0 can [2].

In domain0, an Xen process is also loaded. This process manages all other virtual machines and provides access to these virtual machine consoles. When creating a virtual machine, the administrator uses the configuration program to talk directly to domain0 [3].

As the Xen approach to virtualization has taken a big step forward, the founders of Xen set up their own company, XenSource, which has been acquired by Citrix later. The goal of XenSource was to provide a complete virtualization solution based on the Xen hypervisor in order to compete with other virtualization products such as VMware. Other companies also have integrated Xen hypervisors in their own products. For example, Linux manufacturers Red Hat and Novell have included their own versions of Xen in their operating systems. Since most of Xen is open source, these solutions for virtualization are very similar.

**2.2 Type-2 Hypervisor (hosted hypervisor)**

VMware (Virtual Machine ware) is a "virtual PC" software company, providing virtualization solutions. VMware virtualization directly introduces a streamlined software layer into the computer hardware or above host operating system. It contains a dynamic and transparent way to allocate hardware resources of the virtual machine monitor. In order to achieve multiple operating systems running on the same physical machine at the same time, sharing hardware resources with each other is applied.

VMware first introduced virtualization technology on x86 computing platform in 1999. VMware virtualization pulled the operating system away from the underlying hardware on which it was running and provided standardized virtual hardware for the operating system and its applications. As a result, a virtual machine can run one or more shared processors at the same time independently.

VMWare products enable to run two or more Windows, DOS, and LINUX systems simultaneously on a single machine. Compared with the “multi-boot” system, VMWare uses a completely different concept. Multi-boot system can only run a system at a time, the system switches need to restart the machine. VMWare is truly “running” at the same time, multiple operating systems on the main system platform, switching to Windows as standard application. And in each operating system you can carry out a virtual partition [4]. The configuration does not affect the real hard drive data, so you can use network interface card to connect several virtual machine into a local area network, which is extremely convenient.



**Figure 2. the Xen(Type-1) architecture**

The software layer contains a virtual machine monitor (or “hypervisor”) that allocates hardware resources dynamically and transparently (Figure 3). Multiple operating systems can run concurrently on a single physical machine, sharing hardware resources with each other. Virtual machines are fully compatible with all standard x86 operating systems, applications, and device drivers because the entire computer, including the CPU, memory, operating system, and network devices, is packaged. You can safely run multiple operating systems and applications on a single computer at the same time, and each operating system and application can access the resources it needs when needed [5].

In all virtualization software technology to optimize and manage the IT environment, VMware virtualization technology has been the most widely used, from the desktop environment to the data center are involved.

**2.3 Type-3 Hypervisors (A combination of type-1 and type-2)**

KVM is a hardware-based virtual machine (VM) implementation proposed by an open-source organization called Qumrant in Israel in October 2006. The Linux 2.6.20 kernel, released in February 2007, is the first time that included KVM. In fact KVM is only part of the virtualization solution, and it needs the underlying processor support for multiple operating systems to provide virtualization processors.

KVM is an open-source Linux native full-virtualization solution based on virtualization extensions (Intel VT or AMD-V) for X86 hardware. In KVM, virtual machines are implemented as regular Linux processes that are scheduled by standard Linux dispatchers; each virtual CPU of the virtual machine is implemented as a regular Linux process. This allows KVM to use the existing functionality of the Linux kernel [6]. As the virtualization hardware to provide a new framework to support the operating system directly in the above operation, without the need for binary conversion, reducing the associated performance overhead, greatly simplifying the VMM design, making VMM performance more powerful. Beginning in 2005, Intel promotes Intel Virtualization Technology in its processor product line, which is called IntelVT technology.

KVM is a software that allows to implement computer-based virtualization in OS Linux and Linux-like systems (Figure 4). For some time now KVM is a part of Linux-kernel, that is why they develop together. It works only in systems with hardware virtualization support on the CPU Intel and AMD. For organization of work KVM uses direct access to a kernel with CPU-specific module (kym-intel or kvm-amd). Moreover, the complex contains a main kernel kvm.ko and elements UI, including popular QEMU. Hypervisor enables to work directly with virtual machines files and disc images from other programs. Isolated space is created for every machine with its own RAM, disk, network access, video card and other devices [7].

In addition to CPU virtualization, memory virtualization is also achieved by the KVM. In fact, memory virtualization is often used by virtual machine to achieve the most complex part. CPU memory management unit MMU is through the form of the page table to run the virtual address into the actual physical address. In virtual machine mode, the MMU's page table must perform two address translations in one query. Because in addition to converting the virtual address of the client program to physical address of the client, it also needs to convert the client physical address into a real physical address. Since KVM is only a simple virtualization module, its memory management is not self-realization, and needs the help of Linux kernel memory management. KVM can use any storage supported by Linux, in the realization of the driver, directly with the help of the Linux kernel to drive any hardware. KVM architecture is very simple, is a module of the kernel. The user provides that to the virtual machine to use through QEMU simulation hardware. A virtual machine is a common Linux process, through the management of this process, you can complete the management of the virtual machine.



**Figure 3. the VMware(Type-2) architecture**



**Figure 4. the KVM architecture**

**2.4 Contrast between different types of hypervisors**

Generally, type-1 hypervisors provide better performance and flexibility than type-2 hypervisors, because it runs directly on hardware and exposes hardware resources to virtual machines (VMs), thus reducing the overhead that caused by the executing hypervisors. Since it is completely independent from the Operating System, one virtual machine or guest operating system do not affect the other guest operating systems running on the hypervisor. The hypervisor is small as its main task is sharing and managing hardware resources between different operating systems, and it allows higher density hardware. However, type-1 hypervisors need particular hardware component to support different operating system, which causes it is hard for manufactured. The strict hardware requirements also make it costly compared to type-2 hypervisors [8].

Type-2 hypervisor is also known as Hosted Hypervisor, because it runs on the original operating system as a process. In this case, the hypervisor is installed on an operating system and then supports other operating systems above it, and that makes it completely dependent on host Operating System for its operations. The host operating system have the privileged control over the hardware access, and guest operating system can be only have a few hardware support. This makes type-2 hypervisors have easy access of different operating systems without changing the host system through restarting machine. On the other hand, while having a base operating system allows better specification of policies, any problems in the base operating system affects the entire system as well even if the hypervisor running above the base OS is secure [8]. That means type-2 hypervisors need a powerful and secure host operating system first.

Typically, a Type 1 hypervisor is more efficient than a Type 2 hypervisor, yet in many ways they both provide the same type of functionality because they both run the same kind of VMs. In fact, you can usually move a VM from a host server running a Type 1 hypervisor to one running a Type 2 hypervisor and vice versa. A conversion may be required, but the process works. Type 1 hypervisors support hardware virtualization. Because they run as an application on top of an operating system, Type 2 hypervisors perform software virtualization [9].

# title

## title

text

# title

## title

text

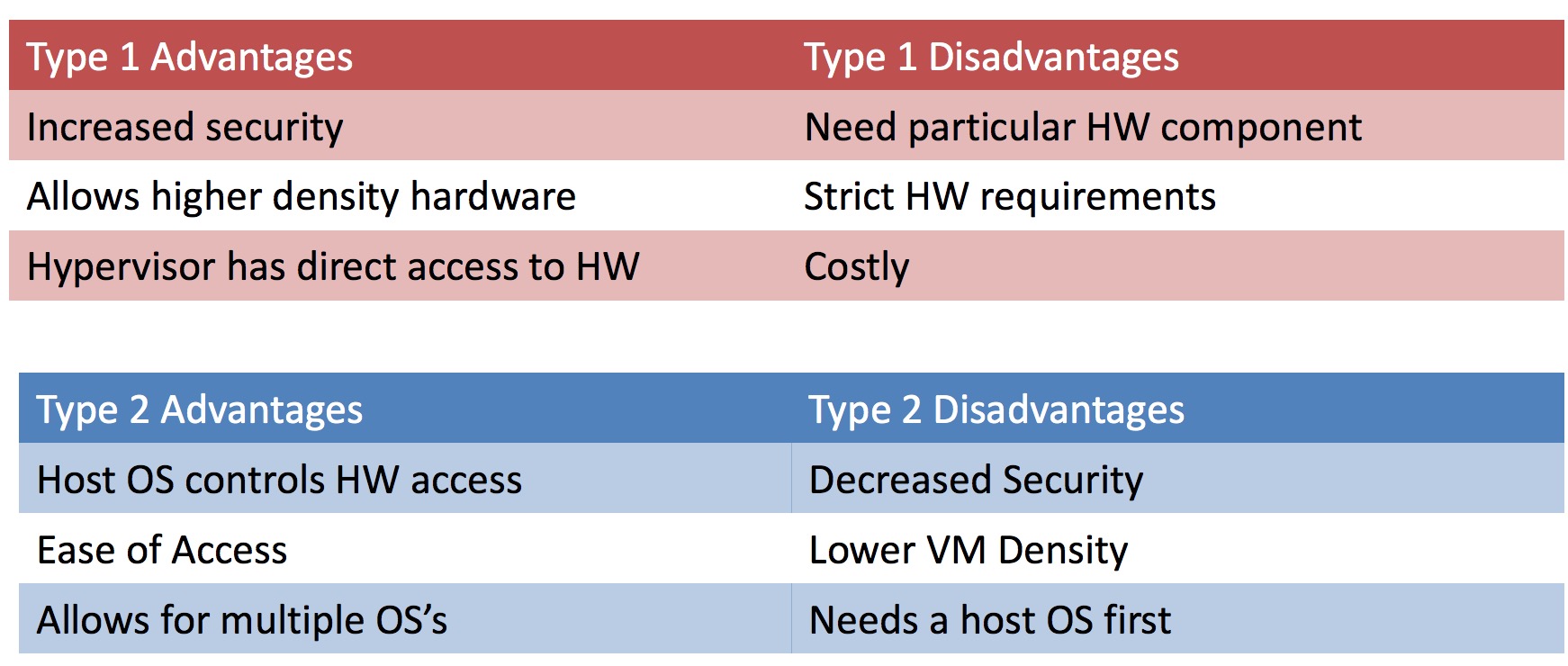


Figure 1. Insert caption to place caption below figure.

.

# REFERENCES

1. Rui Natário. “Full Virtualization Explained” <http://networksandservers.blogspot.com/2011/11/full-virtualization-explained.html>



**Table 1. differences between hypervisors**

1. Gil Neiger, Amy Santoni, Felix Leung, Dion Rodgers, Rich Uhlig. Intel Virtualization Technology: Software-only virtualization with the IA-32 and Itanium architectures, Intel Technology Journal, Volume 10 Issue 03, August 2006.
2. "Xen dom0 support in Lucid - Kernel team discussions - ArchiveOrange". Web.archiveorange.com. Retrieved January 22, 2014.
3. Matthew Palmer (July 13, 2012). "vSwitch the New Battleground for Network Virtualization". Sdncentral.com. Retrieved August 25, 2016.
4. Christian Hammond (January 26, 2016). "A Tribute to VMware Workstation, Fusion, and Hosted UI". ChipLog. Retrieved August 25, 2016.
5. "Red Hat Advances Virtualization Leadership with Qumranet, Inc. Acquisition". Red Hat. 4 September 2008. Retrieved 16 June 2015.
6. "Linux kernel 2.6.20, Section 2.2. Virtualization support through KVM". kernelnewbies.org. 2007-02-05. Retrieved 2014-06-16.
7. Deepak Prasad, “Comparison Type 1 vs Type 2 Hypervisor”. July 01, 2014. http://www.golinuxhub.com/2014/07/comparison-type-1-vs-type-2-hypervisor.html
8. Danielle Ruest. “Virtualization hypervisor comparison: Type 1 vs. Type 2 hypervisors” techtarget. September 2010. <http://searchservervirtualization.techtarget.com/tip/Virtualization-hypervisor-comparison-Type-1-vs-Type-2-hypervisors>

Columns on Last Page Should Be Made As Close As Possible to Equal Length