Virtualization Security

Abhinav Mishra
Scientist C
NIELIT, Gorakhpur, India

Rishabh Mishra
Assistant Professor
DSITM, Ghaziabad, India

Abstract

The recent form of change in working on resources and platform introduced the term virtualization. Virtualization comes with its own merits and challenges. As it hides physical characteristics of the resources and the concept of encapsulation comes into picture. Hypervisor based architecture requires fewer hardware resources and can communicate more efficiently. All major players have introduced their hypervisor based solution to the virtualization. One of the challenges comes with it is the virtualization security.

Keywords- Virtualization, attacks, sniffing, hypervisor, vm, vdi

I. INTRODUCTION

Accessing number of machines from one single host machine is basically server or platform virtualization. Accessed machines are referred as Virtual guest machines and the physical machine on which the machines are hosted is referred as host machine. Later the virtualization expanded its area and it involved resources such as network and memory resources and it is then termed as resource virtualization. Various players have introduced their virtualization software that are drastically being used by the organizations.

Top companies in this field are:-

1) VMware: It dominates the server virtualization market with its Enterprise Virtualization Product VSphere 5.1.
2) Microsoft: Being a new entrant in virtualization race, Microsoft has come up with its Enterprise Virtualization Product Hyper-V.
3) Citrix: Known for its Para virtualized hyper visor Xen, Citrix dominates the desktop virtualization sector.
4) Oracle: Being a database giant Oracle is also offering Enterprise Virtualization Product Vbox

It's the IBM who actually introduced the concept of virtualization in the early 1964 with the development of CP-40 followed by CP [-67]/CMS at Cambridge Scientific Center. Which Is a virtual machine/virtual memory time-Sharing operating system for the IBM System.

But it was VMware who took the lead with its Enterprise Level Virtualization Product VMware Server released on July 12, 2006, a free machine-level virtualization product followed by GSX, ESX and ESXi.

II. HYPERVISOR ARCHITECTURE

Hypervisor/Virtual Machine Monitor is software used to create and run virtual machines. Hypervisors can be categorized into two categories ie. Type-I and Type-II.

A. Type-I Hypervisor

Type-I hypervisor installs directly on the hardware like any other OS and is also known as bare metal hypervisor. It directly controls the physical hardware and manage requests from guest OS. In this environment guest machine operating system/Virtual machine operating system is runs above the hypervisor layer.

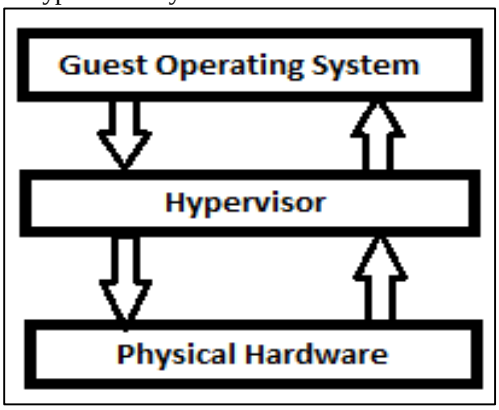


Fig. 1: Type 1 Hypervisor

B. Type-II Hypervisor

Type–II hypervisor does not installs directly on the physical hardware like Type-I hypervisor rather it installs within the conventional OS environment and forms a second software layer above which guest operating systems runs. Hosted hypervisors comes in this category.

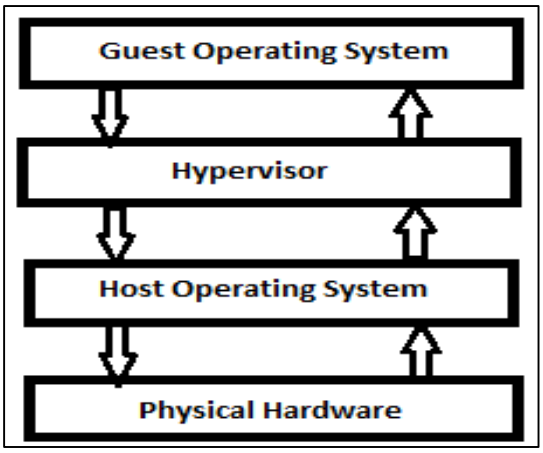


Fig. 2: Type 2 Hypervisor

Depending upon the level of abstraction Virtualization is characterized into three main categories.

1) Full Virtualization

In full virtualization environment Guest Operating System is totally isolated from the Physical hardware layer by the hypervisor. All the OS-to-hardware requests are handled by the hypervisor. Virtual machine OS is totally unaware of being virtualized. This is the most secure virtualization environment.

2) Hardware Assisted Virtualization

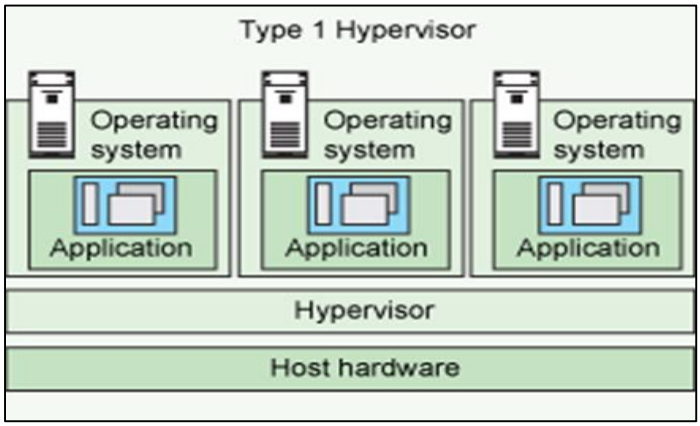
In this type of virtualization environment some specific CPU calls from Guest Operating System/Virtual machine are directly handled by the CPU instead of being translated by hypervisor. This reduces the load on hypervisor by removing the time required to translate system calls and hence increases the performance.

3) Para virtualization

In this type of virtualization, kernel of the guest OS is modified in a way so that the instruction which cannot be virtualized are replaced by the methods so that they can interact directly with the hypervisor. This type of virtualiFzation is mainly seen in Linux environments like Xen, KVM.

III. DIFFERENCE BETWEEN TYPE 1 AND TYPE 2 HYPERVISOR

Type 1 hypervisors run directly on the system hardware. Type 2 hypervisors run on a host operating system that provides virtualization services, such as I/O device support and memory management. Figure 2 shows how type 1 and type 2 hypervisors differ.



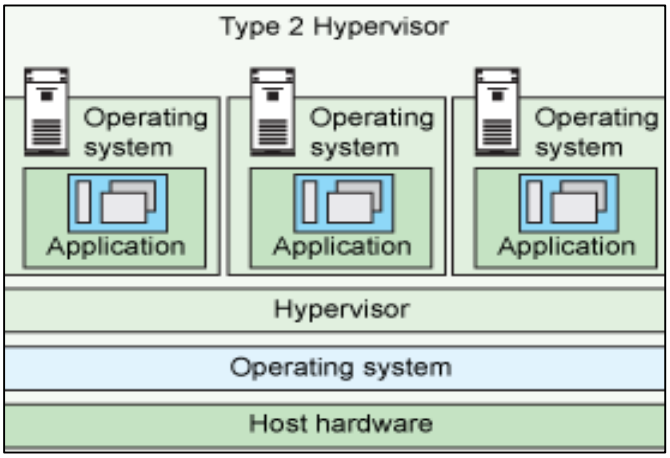


Fig. 3: Difference between Type 1 and Type 2 Hypervisor

IV. FACTORS SHOULD BE EXAMINED BEFORE CHOOSING A SUITABLE HYPERVISOR

One of the best ways to determine which hypervisor meets your needs is to compare their performance metrics. These include CPU overhead, amount of maximum host and guest memory, and support for virtual processors.

But metrics alone should not determine your choice. In addition to the capabilities of the hypervisor, you must also verify the guest operating systems that each hypervisor supports.

If you are running heterogeneous systems in your service network, then you must select the hypervisor that has support for the operating systems you currently run. If you run a homogeneous network based on Windows or Linux, then support for a smaller number of guest operating systems might fit your needs.

All hypervisors are not made equal, but they all offer similar features. Understanding the features they have as well as the guest operating systems each supports is an essential aspect of any hardware virtualization hypervisor selection process. Matching this data to your organization's requirements will be at the core of the decision you make. (To get started with this process, explore the details of each hypervisor).

The following factors should be examined before choosing a suitable hypervisor.

A. Virtual Machine Performance

Virtual systems should meet or exceed the performance of their physical counterparts, at least in relation to the applications within each server. Everything beyond meeting this benchmark is profit.

Ideally, you want each hypervisor to optimize resources on the fly to maximize performance for each virtual machine. The question is how much you might be willing to pay for this optimization. The size or mission-criticality your project generally determines the value of this optimization.

B. Memory Management

Look for support for hardware-assisted memory virtualization. Memory overcommit and large page table support in the VM guest and hypervisor are preferred features; memory page sharing is an optional bonus feature you might want to consider.

C. High Availability

Each major vendor has its own high availability solution and the way each achieves it may be wildly different, ranging from very complex to minimalist approaches. Understanding both the disaster prevention and disaster recovery methods for each system is critical. You should never bring any virtual machine online without fully knowing the protection and recovery mechanisms in place.

D. Live Migration

Live migration is extremely important for users; along with support for live migration across different platforms and the capability to simultaneously live migrate two or more VMs, you need to carefully consider what the individual hypervisor offers in this area.

E. Networking, Storage, and Security

In networking, hypervisors should support network interface cards (NICs) teaming and load balancing, Unicast isolation, and support for the standard (802.1Q) virtual local area network (VLAN) trucking.

Each hypervisor should also support iSCSI- and Fiber Channel-networked storage and enterprise data protection software support with some preferences for tools and APIs, Fiber Channel over Ethernet (FCoE), and virtual disk multi-hypervisor compatibility.

F. Management Features

Look for such management features as Simple Network Management Protocol (SNMP) trap capabilities, integration with other management software, and fault tolerance of the management server — these features are invaluable to a hypervisor.

V. BENEFITS OF VIRTUALIZATION

Virtualization has proven to be a revolutionary technology for Enterprise Networks. Here are some of the benefits offered by Virtualization Technology.

- Virtualization reduces the infrastructure cost by reducing the physical hardware.
- Less hardware leads to less maintenance costs.
- Also known as Green Technology as less physical hardware in data center means less heat and less power consumption.
- More control with Virtual Data Centers.
- Server Deployment is never been an easy task for administrators but with virtualization server machines can be imported, exported or migrated with so much ease.
- Faster Re-deployment and Backups as virtual machines are stored in a file format so it becomes easier for administrators to backup virtual machines in open virtualization formats and recover or redeploy them. Features like snapshot can be used to revert the virtual machines to previous states.
- No Vender Dependencies, with Virtualization it really doesn't matter what physical hardware you use as machine runs in a virtual environment.
- With Snapshots and migration of virtual machines Disaster Recovery becomes easier.
- Features like cloning helps in faster availability as machines can be made available to users with just a click.
- More efficient cloud environment can be made using Virtualization Technology.
- Better utilization of hardware resources like CPU and RAM.
- With virtual switches it becomes easier for network administrators to manage networking.
- With Virtualization one can test any network component as virtual appliances of different network components are easily available.
- Reduced Downtime as virtual machines can be restored easily after a failure.
- High Availability is key feature of virtualization.

VI. CHALLENGES WITH VIRTUALIZATION

Virtualization Technology does offer great benefits but there are many challenges related to this technology.

- Performance- It can virtual networks match up with the performance offered by physical networks? Although virtual appliances for network components like router and switches are available but the question is whether they are efficient enough to replace physical router and switches.
- Networking- Managing virtual networks is easier but requires proper knowledge of virtual networking otherwise wrongly configured networks can lead to performance issues.
- Storage- Companies like VMware, Microsoft and Citrix recommends to use a network storage solution for better performance and availability like SAN but implementing SAN's require skilled personnel's which can lead to extra costs.
- Storage Management- Virtual Machine storage provisioning is to be done with care as over provisioning can lead to wastage of storage space.
- Application Availability- To maintain high availability vm's are migrated from one host to other but during the migration process application becomes unavailable causing problems like shopping cart transaction failures.
- Load Balancing- Care must take while configuring hosts keeping in mind network traffic to avoid bottleneck like situations.
- VM Management- Tools should be there to manage and monitor virtual machines which can again leads to extra cost.
- Application Support- Can virtual machines handle mission critical applications like exchange and database Servers.

So these are some of the challenges that we have to deal with in this virtual technology age.

VII. SECURITY CONCERNS

Virtualized architectures follow two approaches i.e. Bare Metal Hardware Virtualization or Hosted Hardware Virtualization. Although Bare Metal Hardware Virtualization approach is treated as more secure than Hosted Hardware Virtualization approach because hypervisor runs directly on the physical hardware layer and does not relies on underlying OS. Hosted Hardware Virtualization approach relies on the underlying OS as hypervisor runs above the Hosted OS layer causing more security implications.

Here is some more security concerns related to Virtualization Technology:-

- Security Risks due to conventional OS in Hosted Architectures. As they are more prone to attacks.

- Virtual Machine Isolation must be there so that one vm cannot access other vm or address the other vm's resources.
- Guest OS access to host OS should be restricted to prevent users from gaining access to the host operating system.
- Management interfaces should be protected to control access to management consoles or to protect administrative access.
- Skilled personnel's should be employed to minimize the risk of misconfiguration.
- Monitoring of traffic in the virtual network is very much needed to reduce the possibility of attacks. Many virtual appliance
- Patching hypervisor with latest updates to reduce the chances of exploitation of hypervisor vulnerabilities.
- Encryption of traffic between virtual machines or data centers to protect information sniffing.
- Features like cloning, snapshots, and migration needs special attention as if wrongly handled can cause serious problems.
- Configuration of Virtualized architecture is a major security concern as wrongly configured environment can lead to many security implications.
- As all the virtual hardware stores in a file format so file integrity and security becomes an important security concern

So these are some the security concerns related to virtualization technology. Although every hypervisor provider is recommending its own security solutions but that also requires a team of skilled personnel's.
VMware is a market leader offering vSphere as its enterprise virtualization product.

vSphere security provide a guideline on the VMware vCenter and ESXi security. ESXi is widely used virtualization technology which works on three layers: The virtualization layer, virtual machines and virtual networking layers.

These virtual machines can be accessed via an environment provided by the VMware vSphere client either through console of the client application or through web. All virtual machines running on a common virtualization platform are isolated from one another. VMware virtualization layer or VMkernel acts as an interface between Virtual networking layer (which provides the resources to virtual machines) and virtual machines.

Virtualization Security is ensuring prevention from sniffing the information while accessing a virtual machine from host machine. It is an incisive decision to enable virtualization security by encrypting the traffic between guest and host machines. In case of bad configuration, the need for security is necessary. The need is to be aware of Virtual Desktop Infrastructure (VDI). Consolidated data centers also demands extremely tight security as the storage are also provided virtually.

Hypervisor has emerged as a new area of threat to the organization. It is true that no attack has been developed yet which can exploit the hypervisor but it may develop in near future. Virtualization security solutions are provided by number of companies that helps in protecting from external threats and provide security virtualized desktop to end user.

VIII. CONCLUSION

Virtualization is revolutionary technology offering great benefits to different sectors. Introduced a new way of working and provides an extra layer of flexibility and portability. Positive and negative comes together so is the case with virtualization technology as it also has some challenges and security concerns but the thing which matter the most is how efficiently and effectively we can use this technology to gain more benefits. It will be our decisions and innovativeness which decides the future prospects of this technology.

ACKNOWLEDGMENT

The authors are thankful to the E-Security Division of DIT (Department of Information Technology, under Ministry of Communications & Information Technology, Government of India) for sponsoring the activity.

REFERENCES

[1] Edward L. Haletky. Secure Hybrid Cloud Reference Architecture, The Virtualization Practice, LLC(www.virtualizationpractice.com); Version 1.1 (September 2012)
[2] Edward L. Haletky. VMware vSphere(TM) and Virtual Infrastructure Security: Securing the VirtualEnvironment, Prentice Hall PTR; 1 edition (June, 2009)
[3] Trend Micro Deep Security Reference Architecture for the Secure Hybrid CloudEdward L. Haletky Analyst – Virtualization and Cloud Security. The Virtualization Practice Sponsored by Trend Micro
[4] Virtualization Security and Best Practices Rob Randell, CISSP
[5] Virtualization and Risk: Key Security Considerations for Your Enterprise Architecture, McAffe
[6] NIST Guide to Intrusion Detection and Prevention Systems, http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf
[7] Gartner, Radically Transforming Security and Management in a Virtualized World: Concepts, Neil MacDonald, March 14, 2008
[8] VM World News, www.vmware.com/vmworldnews/esx.html
[9] Top Virtualization Security Mistakes(and How to Avoid Them) A SANS Whitepaper – August 2009 , Written by Jim D. Hietala
[10] Secure In-VM Monitoring Using Hardware Virtualization, Institute Eurecom, Sophia Antipolis, France.
[11] http://www.ibm.com/developerworks/cloud/library