An Overview Of Virtualization

Article *in* INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY · December 2006

DOI: 10.24297/ijct.v5i3.3518

CITATIONS
5

READS
3,993

2 authors, including:

Gurjit Singh Bhathal
Punjabi University, Patiala
14 PUBLICATIONS **97** CITATIONS

SEE PROFILE

International Journal of Computers & Technology
Volume 5, No. 3, May -June, 2013, ISSN 2277-3061

An Overview Of Virtualization

Er.Gursimran Singh[1] , Dr.Gurjit Singh Bhathal[2]
E-mail: gursimran51@gmail.com, gurjit.bhathal@gmail.com
[1]Student , Computer Engineering Department, University College of Engineering,
Punjabi University, Patiala
[2]Assistant Professor in Computer Engineering Department,
University College of Engineering
Punjabi University, Patiala

Abstract: This paper presents an overview of virtualization .The first part covers the various Virtualization approaches. The second part covers the requirements for virtualization and its working. The third part covers its applications. In the final part the challenges and security issues are discussed.

General terms: Real World System, Techniques, Encapsulation, Layers, Interfaces, Resources.

Keywords: Virtualization, types of virtualization, Security concerns and challenges for virtualization, Virtual machine monitor.

1. INTRODUCTION

Virtualization is a technique which allows partioning, extending or replacing an existing interface into multiple completely separate virtual interfaces to mimic the behavior of actual interface/system. Virtualization [1][2] can also be defined as the technique that encapsulates the virtual interface (resource or request or application) from the underlying physical delivery of that interface. New virtual interfaces provide an environment which is similar to that of actual system interface.

Virtual Machine Monitor also known as Hypervisor is a software component that provides abstraction for different virtual machines/interfaces running on same system.

Layered Architecture and Types of Interfaces:-

Architecture defines the formal specification and arrangement of a system's interface and logical behavior of the visible resources. Figure 1(A) shows different levels of interfaces, depending on what is virtualized or mimicked [3], we can obtain different form of virtualization as shown in Figure 1(B).

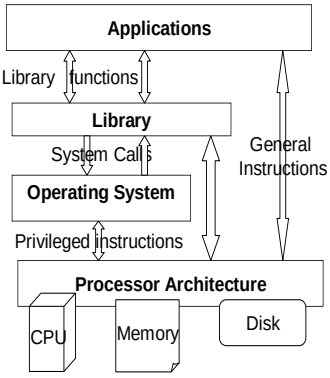


Figure 1(A) Architecture of System before Virtualization

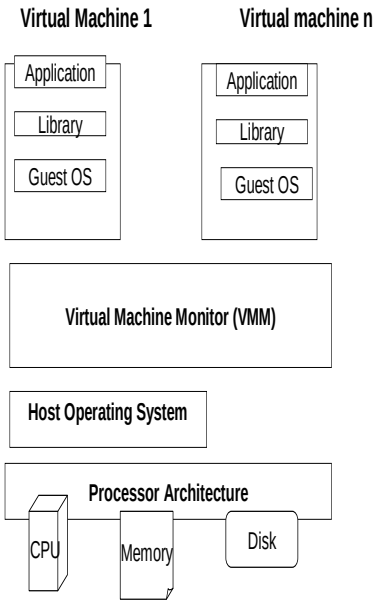


Figure 1 (B) After Virtualization at OS level

International Journal of Computers & Technology
Volume 5, No. 3, May -June, 2013, ISSN 2277-3061

2. VIRTUALIZATION APPROACHES

From the architecture described in above figures we can see that virtualization is possible at different levels [4] which are defined below sequentially:-

2.1. Virtualization at ISA level- This is possible by implementing an emulation of ISA in software. Here by making use of emulation, guest machine's instruction are executed by translating the virtual instruction into native instruction and then their execution on the available hardware. For mimicking the exact behavior of the real world system an emulator has to be able to emulate every instruction that a real system can like reading chips, I/O specific instructions, rebooting etc.

Advantages

- It provides ease of implementation while dealing with multiple platforms.
- It does not enforce stringent binding between the guest and host platforms.
- It provides infrastructural portability and flexibility.

Disadvantages

- Portability comes here at a price of performance.
- Examples: - Boch, Crusoes, Qemu, Bird.

2.2. Virtualization at Hardware Abstraction layer level- In this type of virtualization physical resources are portioned into virtual resources, so that each virtual machine assume that it is using its own resources, but in reality native hardware is used for its computation. For this type of virtualization technology virtual machine must be able to trap every privileged instruction and then pass it to VMM to get CPU's attention.

Advantages

- It cuts down the interpretation latency.
- It provides an efficient and viable use of resources, hence increase performance.
- It provides high degree of isolation.

Disadvantages

- It is not easy to implement.
- It requires mechanism like cod scanning and Dynamic Instruction Rewriting for salient fails.

Examples: - VMware, Denali, Xen, Microsoft Virtual PC, Plex 86, User mode Linux, Cooperative Linux.

2.3. Operating System Level Virtualization-This type of virtualization is developed to reduce the installation overhead required in HAL virtualization. Here virtual machines share the physical resources as well as the operating system on system and uses a virtualization interface layer above the OS layer to present multiple and isolated virtual machine to user. This technique basically provides a replica of operating environment on physical machine, so that difference from the real environment becomes hard to find.

Advantages

- It reduces the overheads like OS installation and network set up etc.
- It provides high performance with simplicity of implementation.

Disadvantages

- It is not as flexible as ISA level.
- It requires careful partioning and multiplexing technique.
- Examples: - Jail, Linux Kernel Mode Virtualization, Ensim.

2.4. Library Level Virtualization- Libraries are basically used to provide an abstraction to users to hide complex operating system details to keep the OS simpler. Applications are programmed using set of APIs provided by group of library functions. This is also known as ABI/API emulation as it implements a different Application Binary Interface and/or a different Application Programming Interface using the underlying system.

Advantages

- It provides user friendly environment without reducing performance.

Disadvantage

- Sometimes it has low Flexibility and degree of Isolation.

Examples: - WINE, LxRun, Visual MainWin.

2.5. Application Level Virtualization- It describes software technologies for applications that encapsulate applications from the underlying OS on which they are executed. Here virtualization is done at application level. Basically application virtualization layer replaces part of the run time environment normally provided by the OS. The layer intercepts all files/registry operation of virtualized application and redirects them to a single virtualized location. This is also known as programming language level virtualization.

Advantages

- It provides high degree of isolation and easy debugging at higher level.
- It helps to run multiple application level operations simultaneously with proper separation.

Disadvantages

- Each application has its own features with that do not allow them to virtualized.

Examples: - JVM, Microsoft.NET CLI, Parrot, Microsoft app V, ThinApp, XenApp.

3. REQUIREMENTS FOR VIRTUALIZATION

Popek & Goldberg [5] define the required condition for a system to have virtualization.

They define Virtual Machine as "An efficient, Isolated Mimic/Replica of Real Machine."

International Journal of Computers & Technology
Volume 5, No. 3, May -June, 2013, ISSN 2277-3061

They define 2 types of **modes**:-

a) **Supervisor Mode**- allows complete access to machine. It is used by OS Kernels & VMMs.

b) **User Mode**- It provides limited access and is generally used by applications.

TRAP is defined as the option which put the processor in a stored state while saving the current state.

Requirement Conditions are defined below:-

a) Privileged Instruction must be superset of Sensitive Instruction set; only then virtualization is possible. In other words privileged instruction must trap only in user mode, not in Supervisor mode.

b) A Control Sensitive Instruction can only change the operating mode. Also VMM should be interacted for accessing system's resources. Non Sensitive Instructions can safely be executed directly.

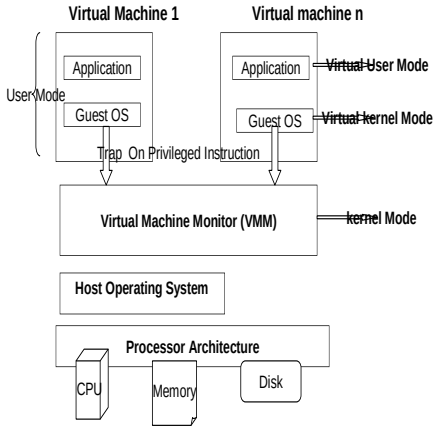
c) Any program run under the VMM should exhibit an effect identical with that demonstration as programming running on original machine.

d) A statistically dominant subset of virtual processor's instruction are executed directly by real processor.

Virtual Machines can be constructed by letting VMM in supervisor mode and virtual machine in user mode.

4. HOW VIRTUALIZATION WORKS

Virtualization is possible only if underlying resources are compatible in doing it. The overall process of virtualization [6] is described below with help of figure



2.

Figure 2: Work Diagram of virtualization

CPU supports both user and kernel mode. The set of instruction that can only be executed in kernel mode are known as sensitive instruction. Examples are- I/O, Change MMU settings etc.

In Operating system a privileged instruction performs a Trap operation when executed in kernel (supervisor) mode.

"Type 1 Virtualization is feasible only if sensitive instruction set is a subset of privileged instruction set."

Unmodified operating system is running in user mode. But it assumes that is running in kernel mode, that's why it is known as virtual kernel mode. Then privileged instruction gets trap.

VMM is a real kernel, upon trapping operation it executes privileged instruction operations or emulates what the hardware would do.

In **Para-virtualization**, operating system is modified to replace all sensitive instructions with hyper calls. OS behaves like a user program making system calls. VMM executes the privileged operation invoked by hyper calls.

5. APPLICATIONS

Virtualization is useful in almost every field. Some applications [2] [4] [7] are defined below:-

5.1. In Software Testing and Evaluation—A Test bed can be created using Virtual machines. Also un-trusted software can be evaluated in virtual machine. So virtual machine is said to be work like "Sandbox" from which the software cannot easily escape out and hence can be tested and evaluated effortlessly.
In Production Applications –Business Applications are placed in virtual machines, so protecting the main server from poorly written and buggy code. Also it provides security by applying principle of least privilege.

5.2. Desktop Virtualization—Application is hosted in a virtual machine or Blade PC (that also include the operating system), so rather than giving employees physical PC, enterprise can give them a personal Virtual machine running on a central server which save expenditure and space as well.

5.3. In Security mechanism— for running an Intrusion Detection System, virtual machines are very good platform. Here they are known as "Honey Pots". Honeypots are unprotected machines that are connected to the Internet. By using these virtual Honeypots, attackers will not be able to go any further than these Honeypots, hence cannot crack the security.

5.4. In Cross Platform and Software Distribution Applications—Applications developed for a specific OS are placed on a virtual machine, but it can be run on another different OS; so it is easy to run incompatible application simultaneously and hence save time. With few configurations changes software installed on one machine can be distributed on another.

5.5. In Debugging and Replaying—VMMs can replay and monitor actions of virtual machines. When a Virtual Monitor is infected with viruses or is attacked by hackers, its action can be

International Journal of Computers & Technology
Volume 5, No. 3, May -June, 2013, ISSN 2277-3061

studied by simply replaying its execution; so it is easy to debug with the virtual machines.

6. CHALLENGES IN VIRTUALIZATION

Virtualization requires some attention during its implementation due to following reasons [8]:-

6.1. Depletion of Resources— while moving from physical hardware to virtual environment often create the performance issues as Virtual Machine saturation cause application network resources depletion at a much faster rate. It also reduces Bandwidth, hence increases Latency.

6.2. Lapse in Application Availability—Virtual machine instances are often migrated from one physical device or location to another single which can cause a lapse in application availability, i.e. whenever resource scheduler moves any data to some different storage, the application may become unavailable during this process and IP addresses also get lost, so availability of application is adversely affected.

6.3. Increase in Cost—Virtualization adds some cost as new hardware and software licenses are required. Also maintenance and storage cost is increased which affect overall cost.

6.4. Limited Sharing of Information—some features of advanced network technologies like switching and VLAN segmentation etc are not integrated with the rest of network as they have tight infrastructure. Hence are not sharable outside the virtual environment.

6.5. Congestion and Over Flow in Storage Network—Data and Files are moved to shared storage in virtual environments; this increases the traffic on the storage network. Also this increases Flooding of data and causes congestion and delay on delivery of data.

6.6. Management Complexity—Management of virtual machines as well as other existing data centers as a single unit is very difficult. Built- in management tools mange only virtual machine platform data. They do not guarantee about external information.

Solution to Above Challenges:-To avoid above discussed problems in virtualization one can make use of Local Traffic Manager (LTM) that offload resources and boosts the performance. Also it manages the session, application availability and proxy connections and their life times.

Also LTM helps in Load Balancing, Caching and Tiering to avoid congestion and un- necessary delay by aggregating capacity and increasing utilization of storage devices. Making use of Automation, WANJet and ESX- aware technologies provide direct integration between virtual machine and data centers. They also provide true application delivery and enable Dynamic Provisioning of resources that simplify the maintenance as single unit.

7. SECURITY ISSUES

Let's have a look on five main principles of security [9] [10] affected by use of Virtualization:

7.1. Confidentiality: Confidentiality is affected in several ways with virtualization. Firstly the logging feature gives the VMM the ability to look inside the virtual machine. This feature can be misused by hackers and crackers. Virtual Machines are transferable between different physical servers, so confidentiality might depend on security of physical servers.

7.2. Integrity: Attackers may manipulate the state of the virtual machines with the help of features like rollback, intervention and Logging.

7.3. Authenticity: As identity of the machine is used for communication purposes, that identity might get changed during migration. If a virtual machine is duplicated, there is no authenticity for any interfaces without original machine.

7.4. Non-Repudiation: If any transaction is stored in a virtual machine in the form of transaction log, transaction may be lost if log is restored. The signature key can also be copied as it is stored in Virtual Machine. Therefore it may affect security.

7.5. Accessibility: Virtualization is not without accessibility. As application sometimes become inaccessible as data is moved to a single location.

In this way we can say that virtualization may cause complexity as there is increase in amount of code, so an increase in bugs affect security adversely. There may be loss of uniqueness, location bounded ness and monotonicity. Isolation and Small Footprints etc have clearly positive effects on security issues. But there is a need to resolve above discussed concerns. Some efforts have already done to resolve them like by Scanning for viruses and Inspecting Virtual machines may distract attackers. Strict Organization of Virtual Infrastructure also helps in protecting Virtual Environment.

8. CONCLUSION

this paper concludes that Virtualization is an important technique that can be used in different environments. Currently, many different approaches are used for virtualization. These approaches can be compared on the basis of parameters like Performance, Robustness, Relationship with host operating system, Portability to multiple guests, Security etc. However all the approaches have some flaws which can be removed in further research. Techniques like Application Virtualization and Para virtualization can be looked promising for future applications. For specific areas selection of proper approach (with their security issues) needs proper care.

9. REFERENCES

[1] Wikipedia contributors. Virtualization, Wikipedia, the Free Encyclopedia,2012.

[2] VMWare Inc. Virtualization Overview White Paper, 2004.

[3] J.E.Smith and R.Nair. The architecture of virtual machines, Computer, IEEE Computer Society Press, Los Alamitos, CA, USA, Volume 38, Issue 5, pp. 32-38 May 2005..

[4] S.Nanda and T.Chiueh. A Survey on Virtualization Technologies, Technical report TR-179, Department of Computer Science, State University of New York, February 2005.

[5] G.J.Popek and R.P.Goldberg. Formal Requirements for Virtualizable Third Generation Architectures, Communications of the ACM, ACM Press, New York, NY, USA, Volume 17, Issue 7, pp. 412-421, July 1974.

[6]Mendel Rosenblum, Tal Garfinkel, "Virtual Machine Monitors: Current Technology and Future Trends," IEEE Computer, pp. 39-47, May 2005.

[7] Flexera software white paper (online) Getting Started with Application Virtualization, 2012.

[8] F5 Virtualization Solutions: www.f5.com/solutions/virtualization, 2008.

[9] G.Dunlap, S.T.King, S.Cinar, M.Basrai, and P.Chen, "Revirt: Enabling intrusion analysis through virtual-machine logging and replay," in In Proceedings of the 2002 Symposium on Operating Systems Design and Implementation (OSDI). New York, NY, USA, pp. 211–224, ACM, 2002.

[10] P.Karger and D.Safford, "I/O for Virtual Machine Monitors: Security and Performance Issues," IEEE Security Privacy, vol. 6, no. 5, pp. 16–23, 2008.

[11] Erik van der Kouwe and Andrew S.Tanenbaum, "Virtual Machines : The state of Art", Vrije University, Amsterdam, 2006.