Chapter 12
An Overview on the Virtualization Technology

Ganesh Chandra Deka
Government of India, India

Prashanta Kumar Das
Government of Assam, India

ABSTRACT

Virtualization technology enables organizations to take the benefit of different services, operating systems, and softwares without increasing their IT infrastructure liabilities. Virtualization software partitions the physical servers in multiple Virtual Machines (VM) where each VM represents a complete system with the complete computing environment. This chapter discusses the installation and deployment procedures of VMs using Xen, KVM, and VMware hypervisor. Microsoft Hyper-v is introduced at the end of the chapter.

INTRODUCTION

Virtualization follows various approaches directly related to the architecture of the Virtual Machine Monitor (VMM) or Hypervisor. In the hosted architecture the VMM runs as an application on the host operating system and relies on it for resource management, system memory devices and drivers. It is also responsible for starting, stopping and managing each virtual machine and also controls access of virtual machines to the physical system resources. Virtualization system that follows this approach is the VMware Workstation. The architecture of VMware Workstation is shown in Figure 1.

In the autonomous architecture, the VMM is placed directly above the hardware. Thus, it is responsible for managing system resources such as CPU, RAM and Hard disk etc. and allocate to different virtual machines. This architecture is more efficient because the VMM has direct access to system resources.

Figure 1. Virtual machine monitor hosted architecture

Figure 2. Virtual machine monitor autonomous architecture
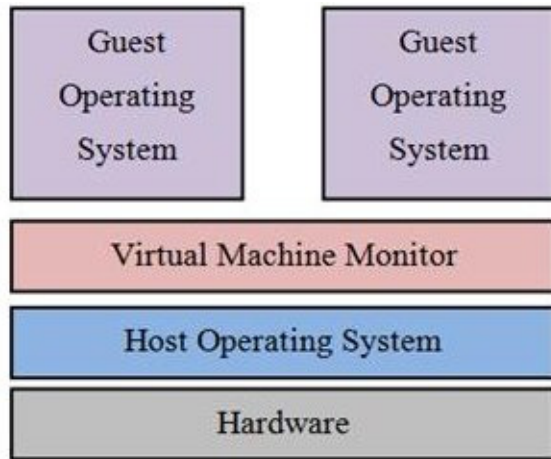
An example of an autonomous architecture is Xen as shows in Figure 2.

The guest operating systems run with limited privileges and doesn't have direct access to hardware. Thus, it is difficult to virtualize some critical operating system instructions because their implementation requires higher privileges.
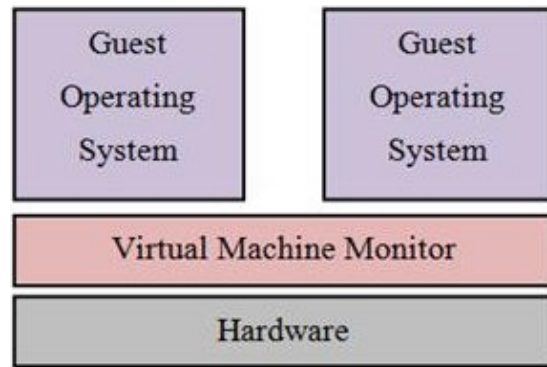
The x86 processor architecture includes four privilege levels (rings). The operating system kernel running at level 0, has the highest privileges. This level provides complete control of system hardware. Simple applications runs on level 3has limited privileges.

Levels 1 and 2 are not used. Thus, in a Virtualization environment the guest operating systems are runs as an application. For this reason some critical instructions that require more privilege cannot be virtualized. Two techniques were followed to solve this problem they are: Full Virtualization and Paravirtualization.

FULL VIRTUALIZATION

Full Virtualization provides total abstraction of the underlying physical system and creates a new virtual system in which the guest operating systems can run. No modifications are needed in the guest OS or application. So, any software that is capable to run in the real system can run without changes in the virtualized environment. In order to execute the critical instructions, a technique known as binary translation is used. In this technique, the software is patched while it runs. For example the critical instructions that cannot run in the virtual environment are replaced by different instructions that can run safely. However, continuous scanning and emulation of critical instructions reduces performance. Some examples of full Virtualization systems are the VMware Workstation and VirtualBox. (see Figure 3)

PARAVIRTUALIZATION

Paravirualization requires modification of the guest operating systems that run on the virtual machines i.e. the guest operating systems are aware that they are running on a virtual machine. The main purpose of paravirtualization is to reduce the time spent in performing critical patches on the guest's unsafe instructions. This is achieved by modifying the client software so it can communicate with the VMM, which run at *ring 0* and has direct access to hardware. So, when an application needs to perform a critical instruction,

Related Content

Big Data Computation Model for Landslide Risk Analysis Using Remote Sensing Data
Venkatesan M.and Prabhavathy P. (2018). *Big Data Analytics for Satellite Image Processing and Remote Sensing (pp. 22-33).*
www.irma-international.org/chapter/big-data-computation-model-for-landslide-risk-analysis-using-remote-sensing-data/200257

Evolution of Fog Computing Applications, Opportunities, and Challenges: A Systematic Review
Hewan Shrestha, Puviyarai T., Sana Sodanapalliand Chandramohan Dhasarathan (2021). *International Journal of Fog Computing (pp. 1-17).*
www.irma-international.org/article/evolution-of-fog-computing-applications-opportunities-and-challenges/284861

Role of Agents to Enhance the Security and Scalability in Cloud Environment
Manisha Malhotraand Aarti Singh (2018). *Critical Research on Scalability and Security Issues in Virtual Cloud Environments (pp. 19-47).*
www.irma-international.org/chapter/role-of-agents-to-enhance-the-security-and-scalability-in-cloud-environment/195340

Performance Evaluation of Routing Metrics in Wireless Multi-Hop Networks
Usman Ashraf, Syed Salman Haider Rizviand Mohammad Faisal Azeem (2016). *Managing and Processing Big Data in Cloud Computing (pp. 85-104).*
www.irma-international.org/chapter/performance-evaluation-of-routing-metrics-in-wireless-multi-hop-networks/143341

Survey on DDoS Attacks and Defense Mechanisms in Cloud and Fog Computing
Deepali Chaudhary, Kriti Bhushanand B.B. Gupta (2019). *Cloud Security: Concepts, Methodologies, Tools, and Applications (pp. 1927-1951).*
www.irma-international.org/chapter/survey-on-ddos-attacks-and-defense-mechanisms-in-cloud-and-fog-computing/224665