happiest minds
The Mindful IT Company
Born **Digital** . Born **Agile**

Operational Risks in Virtualization

Happiest People . Happiest Customers

Contents

Introduction

Virtualization has been defined as a game changing technology for a while. Earlier virtualization was considered useful only for testing and development but over time it has started impacting the entire data-center ecosystem. Decoding complex technical jargon, 'Virtualization' generally refers to server virtualization i.e. partitioning a physical server into various virtual servers. It is a combination of software and hardware engineering where an abstraction of computer hardware makes it possible for a single machine to act as multiple ones. In this scenario, each virtual machine (or server) can run different operating systems, independently interact with other devices, data, applications and users while sharing the resources of a single physical computer.

Why Virtualization ?

Interestingly, virtualization is not only for those who run powerful servers; it has enough benefits and has something for everybody who wants to utilize it.

In traditional physical environments, servers typically run at around 20% of capacity. It is often observed that with multiple servers running simultaneously power and capacity is not utilized fully. Besides multiple servers also take up expensive floor space. Virtualizing servers and desktops can eliminate this waste and result in significant business benefits, including the following:

- Cost containment: It helps reduce the overall hardware footprint as well as hardware costs, floor space, power consumption and management requirements.
- Improved system provisioning: Increases the speed of IT by delivering on demand new capacity to make the entire business more agile and competitive.
- Stability: Given that the virtual machines are completely detached from the hardware, it results in greater resil ience, reduced downtime and better system availability, which in turn enables higher productivity.
- Centralized management: Virtualization is a complex technology that requires skilled deployment and mainte nance; however it also introduces additional tools that allows one to manage systems centrally, reducing administrative and support costs.

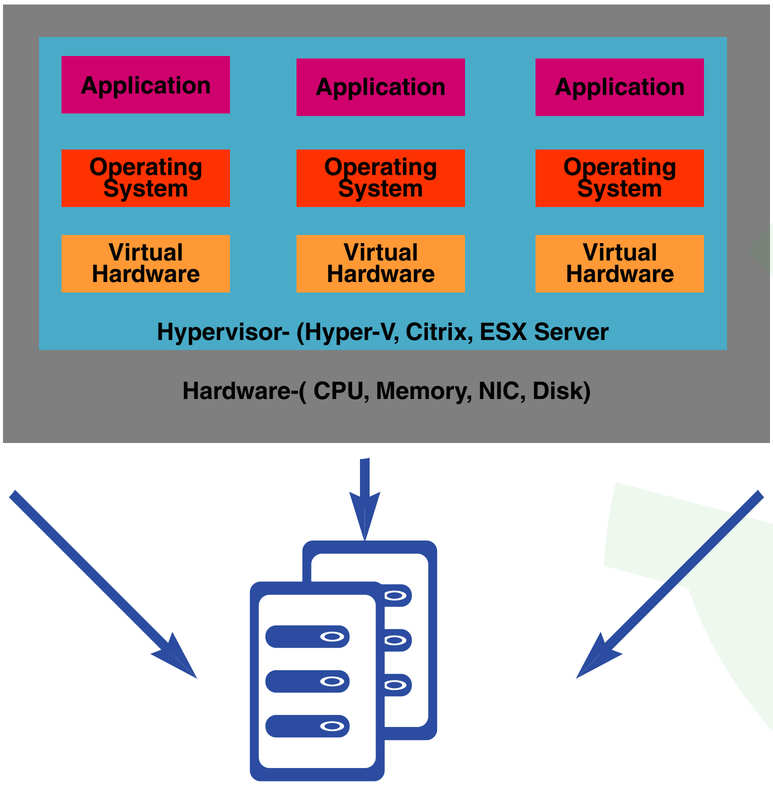

Diagram of a virtualized server

Virtualization is a powerful technology to reduce costs out of the data center while at the same time increasing IT capabilities of the organization. The ability to share all available resources across multiple workloads and to move these workloads across the environment has broken down the silos within IT departments of server, application, network and storage. Companies have started adopting virtualization to a large extent over the last few years.

Virtualization in itself is not insecure but in many cases it is being deployed in a non-secure environment. Through 2012, 60 percent of virtualized servers will be less secure than the physical servers they replace, according to Gartner, Inc. Although Gartner expects this figure to fall to 30 percent by the end of 2015, analysts warned that many virtualization deployment projects are being undertaken without involving the information security team in the initial architecture and planning stages.

Generally security is reviewed and verified when the implementation is done as customers are involved and they closely follow the configurations. Typically most of the vulnerabilities are scanned and fixed prior to the system going live so that a highly secure virtualization is implemented and is ready for operation. But -Does that mean all is well? Traditionally, in a data center there will be one primary and another redundant router/firewall with the same configuration and/or rules to ensure there is a failover capability. In terms of roles there is a L1/L2 role and a device administrator per device and the device manageability is simple. Sometimes during operations, when there is a change in the configuration and/or rules, the same may not mirror/update in any one of the router/firewall. The security risk exposure in these scenarios is thus limited to one device per instance.

In a virtualized data center, there is one physical device with two virtual instances of router/firewall with the same configuration and/or rules to ensure there is a failover capability. In terms of roles there is a L1/L2 role, device administrator and a super admin to distribute the resources (power, processor and memory) to the two virtual instances. Just like it can happen in the traditional data center, at times during operations, a change in the configuration or rule may not mirror/update in any one of the router/firewall virtual instance. The security risk exposure in this scenario is multiplied 3X times by the traditional data center.

Virtualization is a powerful technology tool with various features that enable IT to optimize the resources at hand to meet business requirements at reduced cost within a stipulated timeframe.

However virtualization is not a magic potion. While there are many solutions that are perfect candidates for running virtualization successfully, applications that need a lot of memory, processing power should be ideally left for a dedicated server. Virtualization, like any evolving technology has its fair share of challenges

Risks in Virtualization management

- Resource starvation
- Isolation failure
- Management interface compromise
- Troubleshooting the virtualized machines
- Hypervisor compromise
- Data leakage
- Mis-configured virtual instances [firewalls or networking]
- Compromised VM's
- Managing hypervisor's privileged interfaces

Resource starvation

Virtualization is an on-demand service. There is a calculated risk in allocating all the resources to a virtualization environment; statistics from the past is used to project usage and resources are allocated accordingly. Inaccurate modeling of resources usage - common resources allocation algorithms are vulnerable to:

- **Service unavailability:** Failure in certain highly specific application scenarios which use a particular resource very intensively. Few business process applications will peak whenever there is high volume of transactions and would naturally need more resources to handle the load. Service will be interrupted or unavailable if the resource usage modelling is incorrect.

- **Access control compromise:** When the resources necessary to perform an action are entirely consumed, the action will fail. It is possible to force a system to fail open in the such event of resource exhaustion
- **Economic and reputational losses:** Inaccurate resource forecasting will lead to either excessive or minimal resources procured for the infrastructure. This can result in failure to meet customer demands and/ or financial losses.
- I**nfrastructure oversize:** Excessive provisioning leading to economic losses and loss of profitability
- The inaccurate estimation of resource needs could lead to many budget and schedule collisions.

This risk could be also a consequence of a DDoS attack and of misbehaving applications due to poor application compartmentalization in some virtualization providers' systems.

Isolation failure

Shared resource defines virtualization environment where computing capacity, storage and network are shared between multiple users. There is a consistent risk of failure of mechanisms separating storage, memory, routing and also reputation between different tenants of the shared infrastructure. The impact can be loss of valuable or sensitive data, reputation damage and service interruption for virtualization providers and their clients. Guest-hopping attacks, SQL injection attacks exposing multiple customers' data stored in the same table and side channel attacks cannot be overruled

Management interface compromise

The customer management interfaces of public virtual environments are accessed over internet and they facilitate access to larger sets of resources. Therefore they pose an increased risk especially when combined with remote access and web browser vulnerabilities. This includes customer interfaces controlling a number of virtual machines and most importantly, CP interfaces controlling the operation of the overall virtualization system. Of course, this risk may be mitigated by deeper investment in security by service providers.

Troubleshooting the virtualized machines

Great level of visibility is required for the virtualized machines which was not a concern for organizations during traditional computing times. In the earlier days, if a problem was detected within an application stack, a root cause analysis was done only with respect to the particular application that caused the problem. Considering the highly dynamic nature of virtualized machines these days and the lack of operational silos, any problem with the application stack in VM has to be viewed in a more holistic end-to-end manner.

Without a deep insight into the virtualized environment it is not possible to respond to the various business service needs [storage capacity, network bandwidth I/O connectivity etc;].

Data leakage

Generally, virtual machines are segregated from other machines who share the same host. Every virtual machine is allocated a logical group of resources like memory, processor, storage, network adapter and other resources. One virtual machine cannot access another virtual machine's resources, but they are in the same virtual network. One VM or group of VMs can still be targeted for unauthorized access from other compromised VM.

Some of the threat sources are:

- Data leakage between VM's thru sniffing, spoofing, man-in–the-middle attacks, side channel and replay attacks
- Data leakage through offline images

These require further protection by installing host based firewalls with access control lists managing which VM can talk to which VM within the same host, creating network zones for a logical group of VMs within a host (e.g., development, test & production).

Mis-configured virtual network components

Virtualization lets you run two or multiple instances in one physical device (router or firewall). Basically this enables one physical device to be shared with two or more internal customers within the organization or with different organizations in a shared hosting model. In both the scenarios change management and configuration management plays a crucial role. Lack of consistent change management process and lack of appropriate technical skill set to execute the configuration management will lead to mis-configured virtual instances. This further exposes the virtual machines to unintended parties and can lead to data leakage or destruction.

Compromised VM's

An attacker can use a compromised VM as a bot to gain information and possibly carry out attacks on other VM's running on the hardware components or gather information for future attacks. If the attacker gains access to the operating system, he can access memory that would lead to potential leakage of sensitive information from other VM's and network components. A mis-configured hypervisor may also become a channel for information leakage between hosted virtual components and networks. Isolation of all physical resources (including memory, CPU, network, etc.) is critical to prevent information leakage between VMs and other components or networks on the same host.

Managing hypervisor's privileged interface

Web interfaces to management consoles of hypervisor administration or VM management is a threat source targeted by the attackers. Privileged interfaces (introspection API) of hypervisors are used for management of virtual security appliances (intrusion prevention or detection systems). These interfaces could become another target for exploitation by rogue/misconfigured VMs.

To conclude, virtualization has its benefits and it works if it has been done the right way; wrong implementation of server virtualizations can make backup difficult to manage and more expensive in the long run. As IT needs evolve, Virtualization cannot be seen as an isolated technology to solve a single problem. With users looking at cloud experience IT must offer virtualization solutions that are flexible, agile and can support service based requirements from clients.

About the Author

Vinoth Kumar

Vinoth Kumar - Security Consultant, Governance Risk Compliance practice at Happiest Minds. Vinoth brings with him over 11years of experience in consulting and implementing various Information Security projects in global markets.

About Happiest Minds

Happiest Minds, the Mindful IT Company, applies agile methodologies to enable digital transformation for enterprises and technology providers by delivering seamless customer experience, business efficiency and actionable insights. We leverage a spectrum of disruptive technologies such as: Big Data Analytics, AI & Cognitive Computing, Internet of Things, Cloud, Security, SDN-NFV, RPA, Blockchain, etc. Positioned as "Born Digital . Born Agile", our capabilities spans across product engineering, digital business solutions, infrastructure management and security services. We deliver these services across industry sectors such as retail, consumer packaged goods, edutech, e-commerce, banking, insurance, hi-tech, engineering R&D, manufacturing, automotive and travel/transportation/hospitality.

Headquartered in Bangalore, India; Happiest Minds has operations in USA, UK, The Netherlands, Australia and Middle East.

Business Contact: business@happiestminds.com
Visit us: www.happiestminds.com

Follow us on