Virtualisation

A newsletter for IT Professionals

I. Background of Virtualisation

Virtualisation is the separation of resource or request for a service from the underlying physical delivery of the service. It can dramatically improve the efficiency and availability of resources and applications in your organisation. A common example is computer software gaining access to more memory than physically installed, which is achieved by the partitioning of memory space and background swapping of data to disk storage.

In view of the underutilisation under the old "one server, one application" model, the explosion of the data size, high administration costs for the servers and the incompatibility of different operating system (OS), this gives rise to the need for the virtualisation technology.

Virtualisation technology can be applied to different IT infrastructure layers. The current trend of virtualisation includes server / hardware virtualisation, desktop virtualisation, application virtualisation and virtual infrastructure.

1 Server / Hardware Virtualisation

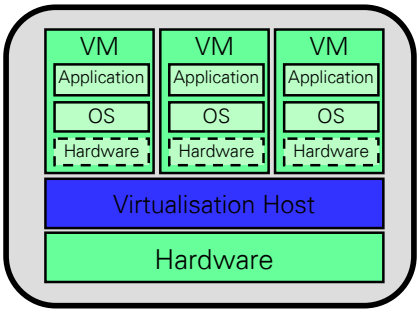

Figure 1 – Server Virtualisation

Server / hardware virtualisation allows a single physical machine to run multiple virtual machines on top of a host operating system or a virtualisation layer. The resources of the single computer are shared across the virtual machines. Each virtual machine emulates a physical computer and has its own CPU, memory, disks and network interface card. In other word, a single physical machine is able to install multiple different OS such as Window, Linux and Unix.

One of the most common approaches to *server virtualisation* is to use hypervisor technology. Hypervisors use a thin layer of code in software to achieve fine-grained, dynamic resource sharing. Hypervisor can be further classified into Type 1 and Type 2. Type 1 hypervisors run directly on the system hardware which are typically the preferred approach for server consolidation because they can achieve higher virtualisation efficiency whereas Type 2 hypervisors run on a host operating system that provides virtualisation services such as I/O device support and memory management. Virtualisation solutions that use a Type 2 hypervisor are also referred to as operating system (OS) virtualisation, and in some environments are called containers.

Reference:
http://www.vmware.com/Virtualization/what-is-Virtualization.html
http://www.microsoft.com/Virtualization/
http://www.vmware.com/technical-resources/advantages/guest-os.html#c133030

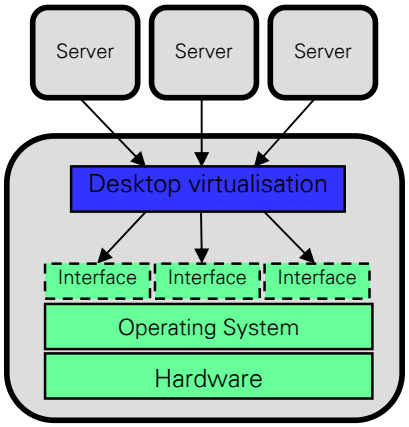

Figure 2 – Desktop Virtualisation

I. Background of Virtualisation (cont'd)

2 Desktop Virtualisation

Desktop virtualisation is also known as *presentation virtualisation*. To run multiple applications, instead of running the applications and displaying the interfaces on the same machine, another option is desktop virtualisation. It enables a client machine to run applications and display interfaces on other corresponding servers through remote desktop.

The major advantage of *desktop virtualisation* is that the management of data and program of each application can be centralised. This saves the installation of the applications on each client machine, and improves efficiency as it decreases the communication overhead between the client and the server.

3 Application Virtualisation

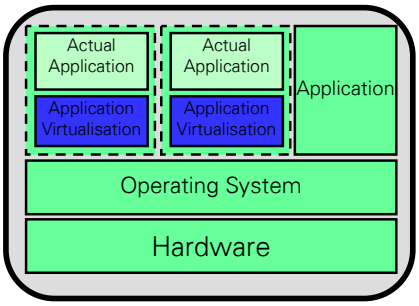

Figure 3 – Application Virtualisation

Apart from the virtualisation of hardware and application interface, the application itself can also be virtualised. Applications may be incompatible to each other when they are run on the same operating system, for instance because of the sharing of specific Dynamic Link Libraries (DLLs) or registry entries.

Application virtualisation is a way to solve the problem. It includes the shared resource and the actual application in a *virtual application*. Resource causing incompatibility is duplicated in each virtual application. Hence, incompatible applications are possible to be run on the same operating system.

4 Virtual Infrastructure – Cloud Computing

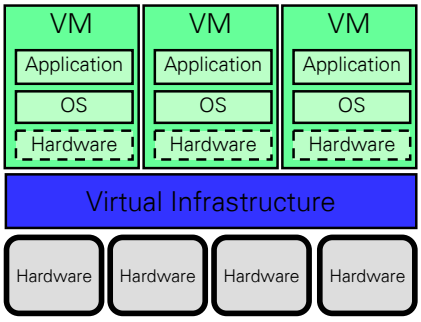

Figure 4 – Virtual Infrastructure

While virtualising a single physical computer by hardware virtualisation is already popular, building a *Virtual Infrastructure* is another way to implement hardware virtualisation.

Servers, storage devices, network bandwidth on the entire infrastructure can be combined into a pool of resources to be dynamically allocated. Virtual machines can be shared over the entire infrastructure, hosting various operating systems and applications.

Case Study

Implement virtualization in UNIX environment

A full refresh of the server environment was completed using 12 x IBM UNIX servers using logical & virtual partitioning which allows the department to run multiple independent servers on a single physical server.

See the article: (http://www.origina.ie/site-map/about-origina/41/93)

Reference:
http://www.vmware.com/Virtualization/what-is-Virtualization.html
http://www.microsoft.com/Virtualization/

I. Background of Virtualisation (cont'd)

Key Benefits Achieved through Virtualisation

1 **Increase efficiency of the existing resources –** Pooling common infrastructure resources and breaking the legacy "one application to one server" model with server consolidation can increase the efficiency and utilisation of the computing resources.

2 **Reduce data centre costs –** Fewer servers and related IT hardware under virtual environment means reduced real estate and reduced power and cooling requirements. In addition, virtualisation technology lets you improve your server to admin ratio, and hence personnel requirements are reduced as well.

3 **Increase availability for improved business continuity –** Under virtualisation, the organisation can securely backup and migrate entire IT virtual environments with no service interruption. This can eliminate or reduce the needs for planned downtime and enable the service to be recovered immediately from unplanned issues.

4 **Gain operational flexibility –** With appropriate hardware configuration, virtualisation able to provide faster server, improve the speed of desktop and application deployment as well as provide dynamic resource management.

5 **Improve desktop manageability and security –** Deploy, manage and monitor secure desktop environments that users can access locally or remotely, with or without a network connection, on almost any standard desktop, laptop or tablet PC.

Industry Story

ITS Virtualization Service
Virtualization as a Service (VaaS) is deployed for departments at the University of Michigan. VaaS offers low cost virtual servers using enterprise class hardware in secured datacenters. Using VaaS virtual servers can yield significant cost savings with numerous benefits and features.

See the article: (http://vaas.umich.edu/benefits.aspx)

Harness the Full Potential of High-Performance IT Hardware
Most x86 computers today operate at a mere 10-15% of their total computing capacity, leaving vast IT resources untapped and unusable. But with virtualisation, you can increase utilisation to as much as 85% by running multiple operating systems on a single computer.

See the article: (http://www.vmware.com/technical-resources/performance/)

Reference:
http://www.vmware.com/Virtualization/what-is-Virtualization.html
http://www.microsoft.com/Virtualization/

II. Risk of Virtualisation in Universities

In view of a numerous benefits of virtualisation, virtualisation technology has recently gained popularity in the marketplace. According to Gartner, percentage of workloads running on virtual machines will jump from 16% to 50% by the end of 2012. Some overseas universities (e.g. Ohio University, Indiana University and Singapore's Insitute of System Science) also deployed virtualisation in their data centres recently for cost-saving purpose. However, universities should consider the risks and vulnerabilities prior to implementing virtualisation technology and examples of these risks are:

1 Inexperienced Staff

The universities only embracing the virtualisation technology not until recently, therefore the universities are less familiar with the implication and risks of the virtualisation technology. The universities' staff are often found to have no or little experience in evaluating the virtualisation products that meet the universities' requirements. However they have to conduct a thorough review of the deployment of the virtualisation tools and applications on the possible effect of security.

Lack of staff expertise may result in mis-configuration of virtual machines, such as unnecessary ports and services. Those vulnerabilities will extend to each instance of the virtual machine that is replicated from that build.

Therefore, it is vital that IT staffs are trained properly on the installation, hardening and maintenance of the virtual machines.

2 Increased Channels for Attack

Hosting multiple virtual machines on a single physical machine increases the attack surface in the virtual environment and the risk of VM-to-VM compromise. Attackers can compromise a single virtual machine first and use the "virtual machine escape" technique to control all virtual machines within the virtualisation host. Moreover, the implementation of virtualisation may be performed by a number of departments and administrative units within universities. The presence of decentralised network within the universities may increase the risk of attacks on virtualised systems.

As a result, appropriate intrusion detection and prevention systems should be implemented to detect malicious activity at the virtual-machine level, regardless of the location of the VM within the virtualisation environment.

3 Change Management Control

With virtualisation, there are often software or firmware updates in place below the operating system. Making changes to the virtualisation host are as simple as editing a file. However, it can impact the virtualisation host, as well the entire virtualisation environment underneath. Dedicated IT security staff within universities may not have relevant knowledge in managing multiple virtual machines instances.

For example, inappropriately applying patches to a virtualisation host that support numerous virtual machines can cause problems and interruptions to production environment, particularly if a system reboot is required.

Moreover, the risk of improper change control process for the virtualised machines is higher especially for the universities that do not currently have an established change management process in place within the universities.

Reference:
http://www.eweek.com/c/a/Virtualization/Server-Virtualization-Adoption-Growing-Rapidly-Gartner-821995/
http://www.vmware.com/files/pdf/partners/security/mcafee-key-security-ent-arch-wp.pdf
http://www.sans.org/reading_room/analysts_program/McAfee_Catbird_Virtualization_Jul09.pdf
http://www.forbes.com/2008/04/09/virtualization-rsa-malware-tech-virtualization08-cx_ag_0409virtual.html?partner=email

II. Risk of Virtualisation in Universities (cont'd)

4 IT Asset Tracking and Management

Since the implementation of virtual machines is comparatively simpler than bringing a physical server online, there is a significant amount of oversight through the asset tracking process. A standard process may not be in place to track and manage the information technology asset in the universities. Difficulty in asset tracking may lead to failure in compliance with licensing requirements and poor asset management.

5 Securing Dormant Virtual Machines

When a virtual machine is offline, any application can still access the virtual machine storage over the network. Virtual machines are therefore susceptible to malware infection. However, dormant VMs do not have the ability to run an antimalware scan agent. To implement virtualisation, universities should first secure these dormant virtual machines and maintain cohesive security in the virtualisation environment.

6 Sharing Data between Virtual Machines

Virtual network traffic between virtual machines on the same physical server never leaves the physical box. Traditional security tools may not be able to analyse and monitoring of the virtual network traffic and confidential or legally protected data can be compromised. To minimise the risk of unauthorised access to the confidential data, the confidential data should be segregated from other non-confidential data, e.g. placing them on a separate physical server.

Statistical Report

2010 State of Virtualisation Security Survey

A recent survey by Prism Microsystems reveals that 48% surveyed IT professionals rank "Lack of Staff Expertise" as a primary inhibitor to effectively securing their virtual environment. Although 86% consider IT security in virtualised environment is as important as the rest of their traditional IT architecture, only around 20% implement virtual-environment specific security solutions, leaving the remaining using existing traditional security solutions (i.e. 58%) or no specific solutions (i.e. 20%) at all.

The top three security concerns on virtualisation are "Potential risk for single point of entry into multiple virtual machines" (i.e. 58%), "Introduction of new virtualisation platform can be attacked" (i.e.57%), and "Risk of unmonitored / invisible machines due to flexible deployment capabilities" (i.e. 53.9%). As for the implementation of security measures for virtualisation environment, less than 30% of respondents have implemented specific security tools to monitor and analyse activities directly from virtualisation layer.

See the article:
(http://www.prismmicrosys.com/documents/VirtualizationSecuritySurvey2010.pdf)

Reference:
http://www.vmware.com/files/pdf/partners/security/mcafee-key-security-ent-arch-wp.pdf
http://us.trendmicro.com/us/solutions/enterprise/security-solutions/virtualization/
http://technology.inc.com/security/articles/200904/virtualization.html

III. Exploitation on Virtualisation

A virtualisation infrastructure represents an additional architectural layer which can suffer from security vulnerabilities and be the target of attacks. Generally, attacks can be categorised into: (1) concealing malicious code activities through detection of virtual machines, (2) denial of service on the virtual machine, and (3) virtual machine escape which is considered to be the most threatening type of attack.

Potential Vulnerabilities in Virtualisation Environment

1 **Concealing malicious code activities through detection of VM –** VM-specific Instructions in the CPU (including the CPUID instruction) would leak information about VM presence. The approaches used to detect the presence of VM or hypervisors usually rely on timing which demands for a comparison to executions without the presence of a hypervisor or require external time sources. Once the hackers detected the existence of VM, they can perform malicious code activities on the virtualisation layer. Malicious codes may alter the behaviour of VM, including refusing to run.

2 **Denial of Service on the Virtual Machine –** Apart from detection, virtual machine can be targets of attacks with the objectives to reduce the availability of VMs. Classical denial of service (DoS) attacks can lead to abnormal termination of VMs or high computational load (e.g. produced through infinite loops) which hinders the interaction of users or administrators with affected VMs.

3 **Virtual Machine Escape –** Virtual machine escape is an exploit that enables a hacker to move from within a virtual machine to the hypervisor, thereby gaining access to the entire computer and all the virtual machines running within it. In other word, the attacker can execute arbitrary code on the host system with the privileges of the virtual machine. This denotes a total compromise.

To minimise the chance of attacks by intruders and safeguard the virtual environment within the organisation, a series of hardening steps for the virtualisation environment have to be in placed properly. In next three sections, some hardening guidelines would be introduced to secure the environment for server virtualisation.

Historical Incident

VMware Multiple Denial Of Service Vulnerabilities
Some VMware products support storing configuration information in VMDB files. Under some circumstances, a malicious user could instruct the virtual machine process (VMX) to store malformed data, causing an error. This error could enable a successful Denial-of-Service attack on guest operating systems.

See the article: (http://ww.securiteam.com/cves/2007/CVE-2007-1877.html)

Reference:
http://www.symantec.com/avcenter/reference/Virtual_Machine_Threats.pdf
http://www.first.org/conference/2008/papers/wimmer-martin-papers.pdf

IV. Hardening Steps to Secure Virtualisation Environment - Server Service Console

All configuration tasks for the VM Server are performed through the Service Console, including configuring storage, controlling aspects of virtual machine behaviour, and setting up virtual switches or virtual networks. A privileged user logged in to the Service Console has the ability to modify, shut down, or even destroy virtual machines on that host. If attackers gain access to the Service Console, they will have access to attribute configuration of the server host. The Service Console is the point of control for server and safeguarding it from misuse is crucial. The following security recommendations or guidelines help to guard against the attacks through Service Console:

1 **Restrict the connection to internal trusted network only –** Restricting the connection to internal trusted network only will help to minimise the chance of the attack via Service Console from untrusted network.

2 **Change the account name of "Administrator" –** Most brute force attacks will use the account name "Administrator" as this default account is not subject to account lockout. To minimise the risk of attacks, user should modify this default account by editing the Local Security Policy.

3 **Block all the incoming and outgoing traffic except for necessary ports –** Service Console firewall should be configured at the high security setting, which blocks all incoming and outgoing traffic except for ports 902, 80, 443, and 22, which are used for basic communication with VM Server in general. This can reduce the risk of the Denial of Service (DoS) attack using the default ports.

4 **Monitor the integrity and modification of the configuration files –** Key configuration files (such as "/etc/profile", "/etc/ssh/sshd_config", "/etc/pam.d/system_auth", "/etc/ntp", "/etc/ntp.conf", "/etc/passwd", "/etc/group", "/etc/sudoers"," /etc/shadow", "/etc/vmware/") should be monitored for integrity and unauthorised tampering to prevent unauthorised modification of key Service Console configuration files. These files should also be securely backed up on a regular basis.

5 **Limit ssh based client communication to a discrete group of ip addresses –** Connectivity of ssh based client communication tools (such as putty, winscp etc.) should be limited to a discrete group of ip addresses belonging to the physical / virtual desktops of the Windows Infrastructure Management Team staff. Limiting the connectivity will be achieved by utilising the /etc/hosts.allow and /etc/hosts.deny files within VMware ESX. The best practice approach to this is to deny access based on subnet range, only allowing access based on ip address exception.

6 **Create separate partitions for /home, /tmp, and /var/log** – Without partitioning for /home, /tmp, and /var/log may experience the Denial of Service (DoS) attack since the root partition may full and unable to accept any more writes.

Reference:
http://xtravirt.com/xd10077
http://technet.microsoft.com/en-us/library/cc264467.aspx
http://download.microsoft.com/download/4/2/9/42995217-e85a-41e9-b530-375a10b800fa/TS_security.doc

V. Hardening Steps to Secure Virtualisation Environment - Virtual Network Layer

The virtual networking layer consists of the virtual network devices through which virtual machines and the Service Console interface with the rest of the network. VM Server such as ESX Server relies on the virtual networking layer to support communications between virtual machines and the users. The virtual networking layer includes virtual network adapters and the virtual switches.

1 **Network breach by user error or omission –** All virtual networks should be labelled appropriately to prevent confusion or security compromises. This labelling prevents operator error due to a virtual machine being attached to a network it is not authorised for or to a network that could allow the leakage of sensitive information. In addition, sensitive networks should be physically segregated from each other by using clusters of physical hosts.

2 **MAC Address spoofing (MAC address changes) –** The "MAC address changes" option should be set to "Reject" in order to protect against MAC impersonation. ESX Server then will not allow requests to change the effective MAC address to anything other than the initial MAC address. The port that the virtual adapter used to send the request is disabled. As a result, the virtual adapter does not receive any more frames until it changes the effective MAC address to match the initial MAC address.

3 **MAC Address spoofing (Forged transmissions) –** The Forged Transmissions option setting affects traffic transmitted from a virtual machine. The "Forged transmissions" option should be set to "Reject", such that the ESX Server will compare the source MAC address being transmitted by the operating system with the effective MAC address for its adapter to see if they match. If the addresses do not match, ESX Server drops the packet. ESX Server intercepts any packets with impersonated addresses before they are delivered, and the guest operating system might assume that the packets have been dropped.

Reference:
http://xtravirt.com/xd10077
http://technet.microsoft.com/en-us/library/cc264467.aspx
http://download.microsoft.com/download/4/2/9/42995217-e85a-41e9-b530-375a10b800fa/TS_security.doc

VI. Hardening Steps to Secure Virtualisation Environment - Virtual Machine

Virtual machines are the containers in which guest operating systems and their applications run. In best practise, all virtual machines are isolated from one another. Virtual machine isolation is imperceptible to the guest operating system. This isolation enables multiple virtual machines to run securely while sharing hardware and ensures both their ability to access hardware and their uninterrupted performance.

1 **Set the resource reservation and limits for each virtual machine –** Resource reservations and limits can protect virtual machines from performance degradation if one of the virtual machines on the Server host is incapacitated by a denial-of-service or distributed denial-of-service (DoS) attack. It is because a resource limit on that machine prevents the attack from taking up so many shared hardware resources and hence minimize the interruption to other virtual machines.

2 **Apply standard infrastructure security measures into virtual infrastructure –** Common security measures such as antivirus agents, spyware filters, intrusion detection systems should be installed and kept up to date including patching in each virtual machine to minimize the general security risk.

3 **Use native remote management services to interact with virtual machines –** Since the VM console allows a user to perform a lot of operations such as power management, it can potentially allow a malicious attacker to bring down the virtual machine. Restricting the connection methodology to VM console by using native remote management services, such as terminal services and ssh only can reduce the possibility of attacks via console.

Reference:
http://xtravirt.com/xd10077
http://technet.microsoft.com/en-us/library/cc264467.aspx
http://download.microsoft.com/download/4/2/9/42995217-e85a-41e9-b530-375a10b800fa/TS_security.doc