

SECURITY IN OPERATING SYSTEM VIRTUALISATION

February 2008

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of, and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR.

Disclaimer: Whilst the Government endeavours to ensure the accuracy of the information in this paper, no express or implied warranty is given by the Government as to the accuracy of the information. The Government of HKSAR accepts no liability for any error or omission arising from or related to the use of the information.

TABLE OF CONTENTS

Summary	2
I. Introduction	3
II. The Management Considerations of Virtualisation	5
Catalysts for Virtualisation.....	5
The Benefits of Virtualisation	6
The Drawbacks of Virtualisation	8
III. Virtualisation for IT Practitioners	10
Deploying Virtualisation.....	10
Security Threats.....	11
IV. Conclusion	12

SUMMARY

While server and desktop PCs continually pose problems for IT managers in terms of manageability, flexibility and security, the isolated execution environments provided by virtual machines are one way of addressing such issues. Another advantage is that virtualisation technology can help organisations protect themselves from accidental data leakage if notebook computers are lost. Pre-built locked-down desktop environments can now be installed in an encrypted folder on a user's notebook computer. With increased hardware support for virtualisation by the major microprocessor vendors, virtualisation products are becoming a practical solution for IT management. In this paper, we discuss the management issues around virtualisation technology, as well as the options available for deploying virtualisation technology in both server and desktop environments.

I. INTRODUCTION

The term “virtual machine” first appeared in academic literature back in the 1960s when researchers first formulated concepts like multi-programming and time-sharing. Early examples of the virtual machine concept can be traced back to the IBM M44/44X project in the 1960s, and later IBM mainframe systems such as IBM 360/67 and VM/370¹. At that time, computing power was a scarce resource, it was important to make good use of limited hardware, and virtualisation technology was developed as one solution.

Virtualisation has been defined as “*a framework or methodology of dividing the resources of a computer into multiple execution environments, by applying one or more concepts or technologies such as hardware and software partitioning, time-sharing, partial or complete machine simulation, emulation, and many others*”². With virtualisation technology, the resources of a computer can be optimised in a way that increases the return on investment. From the user’s perspective, virtualisation provides a way in which more than one operating system can be run on the same physical machine.

Today’s modern hardware is much cheaper, more powerful, and far more abundant compared to the early computers of 1960s and 1970s. But IT management continues to view virtualisation as a good strategy. The driving forces behind today’s server virtualisation technology include:

1. The number of physical servers needed for a specific set of tasks or operations can be reduced;

¹ <http://www.kernelthread.com/publications/virtualization/>

² Same as above.

2. Any physical server consolidation strategy will reduce the space required by hardware in a data centre;
3. Individual applications that are compartmented into dedicated virtual servers can be upgraded more easily, because changes to one application in one virtual server will not affect other applications running on other virtual servers³.

In order to realise virtualisation in practise, a sub-layer of software is needed to control the virtualisation process. This software layer is called the Virtual Machine Monitor (VMM)⁴ or hypervisor. VMMs can be categorised into two types: the first type is a VMM that runs directly on the hardware, and is itself the operating system on which other virtual machines can run. A VMM of this type is sometimes called a type 1 hypervisor (or bare-metal hypervisor). The other type of VMM is one that runs as an application on top of a pre-existing (or host) operating system. For example, when a user runs a virtual Linux machine on their Windows XP desktop PC, Windows XP is referred to as the host operating system, while the virtual Linux (virtual) machine running on top of Windows XP is called the guest operating system. A VMM of this type is sometimes known as a type 2 hypervisor (or hosted hypervisor).

³ http://utilitycomputing.itworld.com/4824/nls_windowsserver050411/page_1.html

⁴ <http://www.kernelthread.com/publications/virtualization/>

II. THE MANAGEMENT CONSIDERATIONS OF VIRTUALISATION

CATALYSTS FOR VIRTUALISATION

As mentioned, virtualisation is not a new idea. Virtualisation software that can support more than one operating system running on the same physical machine has been around for a while, and can be found in older computing platforms, such as Sun Microsystems SPARC workstations. Some years ago, Sun Microsystems provided WABI (Windows Application Binary Interface) to enable Unix users to work with Microsoft Windows applications within several UNIX operating environments running the X Windows System⁵. However, performance was not satisfied because the emulation process relied on software driven programs, with limited CPU processing power.

With today's gigahertz-speed, multi-core CPUs, processing power has increased dramatically, and this has helped accelerate the adoption of virtualisation technologies in the IT market. Vendors such as Intel and AMD have brought virtualisation technology into their processors by developing and introducing multi-core CPUs, which facilitate the running of various operating systems side by side as entirely separate entities. Intel's Virtualisation Technology (or Intel VT) aims to *"give virtualisation software the ability to take advantage of offloading workload to the system hardware, enabling more streamlined virtualisation software stacks and "near native" performance characteristics"*⁶. A number of Intel Core 2 Duo processors already have VT technology integrated into the structure of the chip. AMD has also developed AMD Virtualisation (or

⁵ <http://docs.sun.com/app/docs/doc/802-6306/6ia0mdt48?a=view>

⁶ <http://www.intel.com/technology/platform-technology/virtualization/index.htm>

AMD-V, or Pacifica) technology, achieving the same objective of increasing the performance of virtualised applications⁷.

THE BENEFITS OF VIRTUALISATION

The core benefits of virtualisation include:

1. Trying to manage and account for legacy applications when migrating to a new operating system (OS) is a common problem in IT management. Virtualisation provides a cost effective solution in which critical legacy applications can continue to run in a virtual environment on an interim basis during an OS migration or upgrade process, until more updated solutions are available.
2. Virtualisation provides an environment where technical support staff can rapidly switch to alternate operating systems for problem solving simulations and support issues.
3. The availability of virtual servers provides a cost effective and efficient way for developers to test and debug software on a number of different platforms.
4. Server virtualisation provides an opportunity for physical server consolidation, reducing the space and cost needed to host physical servers in a data centre.
5. Virtualisation also provides a centrally controlled environment that helps protect data security, and reduces concerns regarding the desktop security of home-based or mobile workers.

⁷ http://www.amd.com/us-en/Processors/ProductInformation/0,,30_118_8796_14287,00.html

On top of this, desktop virtualisation provides further advantages in terms of manageability, flexibility and security in the end-user desktop environment.

Manageability

In managing local desktop PCs, each user is usually assigned a desktop computer in which all required applications are installed. To protect company assets from theft and to ensure compliance with policies and regulations, IT managers usually lock-down these desktops by preventing end-users from installing unauthorised applications or changing desktop settings. Corporate policies and standards are enforced, including the installation of virus protection programs, and regular patches of the operating system and system components such as the web browser.

However, achieving a fully compliant, truly homogenous and locked-down desktop environment across the organisation is not easy. With virtualisation technology however, IT support teams can provide a pre-built, secure, locked-down virtual machine that is pre-installed with only approved applications. Users can only access company data via these controlled virtual machines.

Flexibility

While IT managers face continuing manageability and security challenges, end-users like to have more control over their own desktop PCs⁸. On the one hand, IT managers need to maintain security policies and lock desktops to protect sensitive data that can be accessed by the employees. On the other hand, end-users have a tendency to personalise their desktops with favourite wallpapers or even applications. Desktop virtualisation provides a solution that helps solve this dilemma. Using virtualisation technology, IT support teams can provide two (or more) operating systems that can be run on the user's physical PC. While a secure locked-down virtual machine is offered for employees to access company

⁸ http://searchwinit.techtarget.com/originalContent/0,289142,sid1_gci1237943,00.html

data, a second environment can be set up to give users more control over their personal applications and settings. By segregating these two environments, company assets can be protected and end-users have more flexibility to personalise their PCs.

Security

As mentioned, organisations can also use desktop virtualisation to help protect data leakage from lost notebook computers by installing a pre-built locked-down desktop environment within an encrypted folder on the unit⁹. If the notebook is lost, chances of exposing corporate data in the encrypted folder are minimised.

In addition, virtualisation can be an aid in incident handling and disaster recovery. For example, if a Windows server or desktop is infected with rootkits or other malware programs, the only available option is usually to erase and reinstall the OS from scratch. This is a distressing and time-consuming process. But under a virtual environment, the copy of the virtual machine infected with malware can be removed, and a new copy can be downloaded or retrieved from reliable sources. A clean virtual environment can be restored in a short time¹⁰.

THE DRAWBACKS OF VIRTUALISATION

IT managers need to be aware of the following drawbacks when using virtualisation technology:

1. Multiple operating systems must be managed and patched separately.

⁹ http://searchwinit.techtarget.com/originalContent/0,289142,sid1_gci1237943,00.html

¹⁰ <http://www.securityfocus.com/columnists/397/2>

2. Maintenance costs are likely to increase due to the increasing number of operating systems installed on each physical machine.
3. There is an up-front financial investment in purchasing a suitable virtualisation product, as well as additional licence costs for increasing number of operating systems and installed applications across the enterprise.

III. VIRTUALISATION FOR IT PRACTITIONERS

DEPLOYING VIRTUALISATION

As we have pointed out, multiple virtual machines can be hosted directly on one physical hardware system. Usually a virtual machine server is installed first on the physical machine, and then guest operating system images are downloaded and installed onto the host machine. More than one virtual machine can be “powered-up” on the host machine at any one time, and the user can switch to between running virtual machines in the same way one would switch from one Windows application to another. For example, a user can run a virtual Windows XP machine on their Apple Macintosh desktop computer. Typical virtualisation products that support this mechanism are VMware VM server, Microsoft Virtual PC, and Parallels Desktop.

Virtualisation can also be used to help development staff rapidly deploy and test new applications or platforms. Rather than acquiring multiple physical servers to simulate the production environment required for testing, a developer can install multiple virtual machines directly on their desktop PC or server. This can reduce the cost needed to bring together hardware and operating system installations before development and testing environments can be put to good use.

Furthermore, virtualisation can also be helpful for IT support staff who can use the technology to stimulate problems encountered by in-house end-users. Support personnel can answer enquires from users running a variety of applications under various operating systems. Instead of providing a full spectrum of machines running different operating systems for the support person to use, virtual machines installed on a single desktop PC

might provide a convenient way for him or her to select different operating systems or applications as part of their daily support service.

SECURITY THREATS

There is a possibility of bugs or vulnerabilities in the VMM software. For example, a vulnerability in Microsoft Virtual PC has been detected which allows a guest operating system user to run code on the host or in other guest operating systems¹¹. This vulnerability affects nearly all Microsoft Virtual PC versions, and patches need to be applied to address the problem. Another example is an unspecified vulnerability detected in VMware Server in versions prior to 1.0.4. This caused user passwords to be recorded as cleartext in server logs, which could have led to an unauthorised disclosure of information or disruption of service¹².

While there are security advantages offered by desktop virtualisation, the general practice of regularly applying the latest security patches to virtualisation software should be followed.

In addition, virtualisation does not eliminate the normal security vulnerabilities found on any guest operating system. Individual anti-virus software, firewalls and other necessary patch management of host operating systems should be applied and maintained to the required security standards.

¹¹ <http://www.microsoft.com/technet/security/bulletin/MS07-049.msp>

¹² <http://nvd.nist.gov/nvd.cfm?cvename=CVE-2007-5619>

IV. CONCLUSION

Despite its long history, virtualisation technology is still emerging, and large-scale deployment is not yet that common. However, if virtual environments are to be deployed in the enterprise, the following should be noted:

1. Virtual machine environments provide isolation in the sense that different virtual machines appear to be independent coexisting computers. But, the extent of isolation depends on how the underlying virtualisation technology is implemented. As a general rule therefore, operations within a virtual guest operating system should not be configured to affect operations within another guest operating system.
2. In case sensitive data is stored in a virtual machine, standard security best practices should be implemented to protect the integrity of the virtual machine platform. One example is to store the virtual machine in an encrypted folder so that the guest operating system and its data will be automatically encrypted.
3. Similar to other operating systems, virtual machines should be hardened and patches should be applied regularly.

While enjoying the convenience brought about by the coexistence of multiple virtual machines on one physical unit, organisations should regularly review their security policies and measures with regard to virtual machines. New threats are expected to appear as deployment of virtualisation technology becomes more commonplace.