Virtualization 101

A basic guide to virtualization for the small to medium business

Clavister White Paper

Clavister's five-point guide to adopting virtualization

- Redefine the security policy to include the virtualization aspect
- Use virtual security gateways which run inside the virtual infrastructure
- Protect the virtual administration center and only allow access to this from a separate network
- Limit the number of administrators having access to the virtualization administration tools to a minimum
- Evaluate and test the security level on a regular basis. Replicating the production environment in a test environment is easy with virtualization and this should be utilized

Introduction

Virtualization is fast becoming one of the world's boom technologies. Larger enterprises have moved on from believing it is just another buzzword to realizing the real-world savings and benefits that it can bring. Also, smaller organizations have begun to accept that virtualization is not the sole domain of large enterprises with big budgets. The arrival of inexpensive or free virtualization packages has combined with powerful, high performance workstations and servers to place virtualization firmly within the grasp of small to medium sized businesses (SMB).

So what is virtualization? Traditionally, every major application in your business ran on its own independent server so you had individual mail servers, web servers, file servers and so on. The theory was that this segregation would avoid other applications being brought down if one failed, and at the time it was a sensible idea. However, as the years have progressed, technology has improved and servers have become increasingly powerful. Keeping each application on one physical machine now means needless capital expense and an increased management burden. It also results in underuse of hardware capacity, with industry estimates claiming that the average Windows server runs at approximately 15 per cent utilization.

These changes have coincided with the development of software packages that enable you to run many 'virtual' machines inside one server or computer. At its simplest level, virtualization is the splitting or partitioning of a single physical server or computer into multiple distinct and isolated virtual environments that are capable of interaction with other devices, software or networks as if they were separate machines. Conversely, virtualization software can also be used to combine a number of individual physical machines into one single virtual computer.

The process of virtualization masks server resources from server users and that includes the number of physical machines, their identity, processors and operating systems. Each virtual machine becomes a fully functioning computer which can be configured to your networks, installed with your chosen operating system and loaded with software applications.

clavister®

WE ARE NETWORK SECURITY

Benefits of virtualization

By enabling one server to run multiple operating systems and a wider variety of applications, virtualization enables the SMB to use its existing servers to full capacity rather than buying more new equipment. What was previously done by many servers can now be accomplished by just one.

- The obvious first benefit of this is cost saving. You save capital expenditure and support costs because there is no longer any need to buy new machines when your data center runs out of capacity. Implementing virtualization, particularly with the introduction of server blades, can also save valuable office or data center space. This can translate into considerable savings by eliminating the need to re-fit, extend or move offices as your business grows. Having fewer machines also means lower administration and management costs for internal staff or external consultants.
- Because they are not limited to one single operating system on each physical server, companies can use virtual servers to eliminate the cost of managing and upgrading legacy software by migrating existing applications onto virtual machines.
- Electricity bills are smaller and reduced power consumption also brings 'green' benefits with lowered CO2 emissions. Running fewer machines generates less heat which cuts air-conditioning costs and also improves working conditions for staff.
- In addition, considerable time is saved because physical maintenance of a smaller fleet takes fewer hours and the deployment of virtual servers is much less time consuming than the lengthy set-up required for new physical servers. It makes sense to build just one system then deploy it again and again.

It's all excellent news for the SMB wanting to save money and streamline its operations through server consolidation.

Virtualization game plan for the SMB

Virtualization is a multi-step process and time is well spent on the initial planning and preparation.

There are three main groups of virtualization technologies:

- Hardware virtualization presents virtual hardware to the guest operating system with no need for patching or modification.
- Para-virtualization provides a virtual hardware layer which is similar but not identical to the underlying platform.
- OS-virtualization has only one kernel running on each physical system.

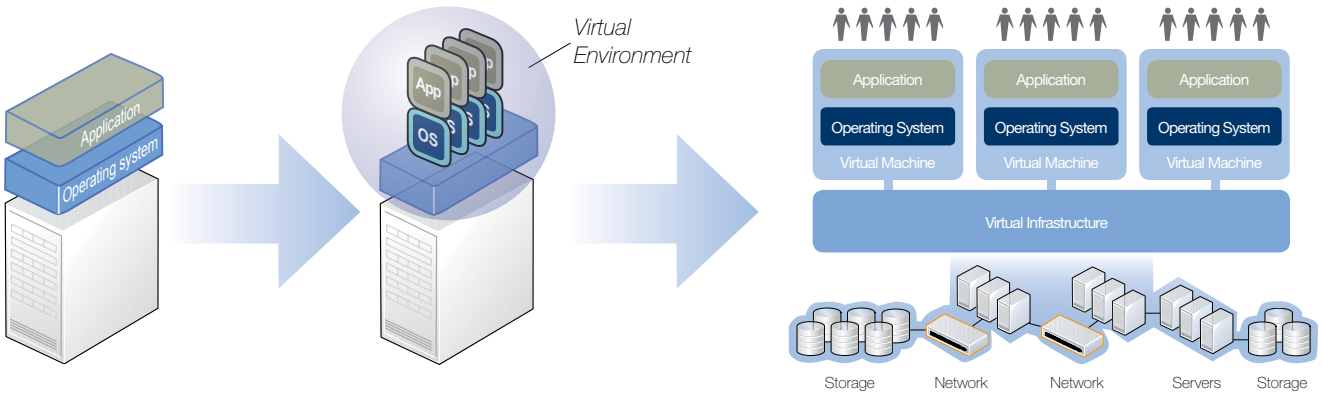
The decision on whether to virtualize or not depends on the complexity of your IT infrastructure so before making this decision, it is important to conduct a broad review of your current IT environment with particular emphasis on server utilization.

It is necessary to identify the physical servers that are suitable for virtualization. Once you have taken an inventory of the data center you must measure the performance of the whole server population. Record each application and what the average processor utilization is. If possible, identify peak utilization levels and how often they occur then note down utilization as a percentage of total CPU capacity. It is important to keep this information for use in the later capacity planning phase of the operation.

Once the performance measurements have been collected, it can be used to decide which physical servers are good virtualization candidates.

Capacity planning is the next stage. You must consider how much computer processing power your current applications need; how much processing power is available and how to distribute the load in the virtual environment. This is where your initial inventory comes in to play.

With all this initial work done, it is time to undertake actual physical to virtual (P2V) migration. There are a number of ways to make physical servers virtual. Each approach can be made to work, but they depend on the resources available in the organiza-



Virtualization allows several operating systems to run on a single machine.

Create shared pools of resources to optimize your infrastructure.

Figure 1: How the virtual environment works

The VSG protects the virtual environment from security threats including inter-VM attacks and external attacks.

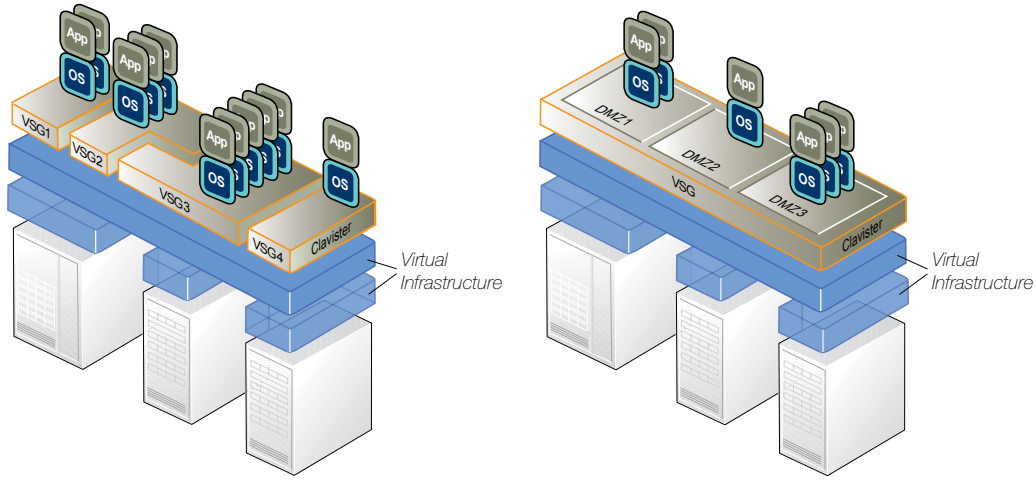


Figure 2: The power of Clavister Virtual Security Gateway (VSG)

tion, your timeframes and budget. Scalability and speed are two of the biggest differentiators among conversion solutions, so it's important to understand your current and future needs. Consider not only how many servers need to be converted straight away but also how many will be converted in the future and whether this will be done individually or in blocks.

It is also important to consider timelines and budgets. Decide if servers can be taken down for conversion during business hours or if this must be done out of hours. Determine how much total down-time is available before the project deadline. Budget is a factor here too because the project may well involve overtime or additional personnel may be needed. Can you afford to extend deadlines if the total required conversion time exceeds the time available?

Personnel and budget questions can't be answered until you determine whether your staff has the skills and time to execute the conversion. Early-generation Physical to Virtual (P2V) conversion tools were complex but fortunately today's packaged conversion solutions are easier to use, automate many previously manual tasks and take less time to execute. Assess your internal IT skills and availability to determine which options are available.

Once you understand your needs it's time to see which of the available solutions is the best match.

There are four possibilities for P2V conversion:

- Free conversion tools from virtualization platform providers. These focus on the conversion aspect and do not attempt to automate much of the overall process so the total time required to prepare, convert and troubleshoot servers can be lengthy.
- Packaged conversion tools and solutions automate many tasks relating to preparation, conversion and post-processing, and often provide a quicker solution.
- Use of boot CDs plus general cloning and copying utilities.
- Outsourcing to a solutions provider is always an option.

Conversion times can go down and success rates go up when physical servers are effectively prepared in advance. Take inventory of configuration settings, licensing details and IP addresses. Install software patches, defrag drives, clean directories, unzip files and conduct other maintenance.

Avoiding some virtualization pitfalls

- Creating new virtual servers unsystematically can easily lead to out-of-control server sprawl. Do not stack too many applications on one host because this can leave them competing for resources and managing your virtual resources among your physical machines can get complicated. Creating new virtual machines can be done so easily and quickly, that it can feel like a free and endless resource. However, when too many virtual servers are added, they can quickly reach the capacity of your physical hosts and complicated server management. It is important to establish standard practices and requirements to justify and control the creation of new virtual servers.
- A major benefit of virtualization is increased resource utilization but too many applications vying for the same resources may leave those applications competing for inadequate processor capacity or network bandwidth. Before moving any applications, take stock of their computing requirements.
- Plan for spikes in demand when allocating resources to your servers and applications to avoid overloading the systems at certain times. Also, don't load physical servers with too many virtual environments because the host physical server will still require maintenance and upgrades. Clustering physical servers and virtual servers is an effective way to avoid physical host server overload.

- You may get cultural resistance from people who have not accepted the dynamic nature of virtualization which means that resources must be shared, as well as the cost of managing or acquiring them. It's important to get stakeholder participation and buy-in early. You can't manage what you can't see and IT departments often have problems understanding what virtual machines (VM) they have and which are active or inactive. To overcome these challenges, discovery tools need to extend to the virtual world by identifying Virtual Machine Disk Format files and how many exist within the environment.
- It is important to map the guest to host relationships in your virtualized environment because it can be difficult to understand which VMs are on which hosts and identifying which business critical functions are supported by each VM.
- Performance bottlenecks can be created if VMs are not configured properly so it is important to maintain a configuration management database to keep control of the current state of each VM.

Securing the virtual environment

A recent survey from international research and consulting organization YouGov[1] shows that more than 40 per cent of IT directors and managers who have implemented server virtualization may have left their IT networks open to attack because they wrongly believed that security was built-in. When companies implement virtualization, it is very dangerous for them to assume that everything is automatically secure when the reality is that they may be facing new security threats.

[1] All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 212 private sector IT or Telecoms Directors and Senior Managers. Fieldwork was undertaken between 22nd - 29th September 2008. The survey was carried out online.

Virtualization now goes beyond merely consolidating physical servers onto one piece of hardware running virtualization software. Full network infrastructure virtualization is offered with network switches, routers and other typical physical applications all managed by the virtualization software. This causes several new challenges and administrators need to consider deploying virtual network security products to manage these challenges.

Most virtualization projects are implemented by the server managers, not the networking or security staff so more focus is often placed on getting the servers running than on ensuring foolproof security.

An SMB may decide it is best practice to follow Peripheral Component Interconnect (PCI) standards and place its firewall and Intrusion Detection & Prevention (IDP) systems in front of the virtual infrastructure. However, many virtual infrastructures have no security between the different virtual servers which knocks out control over the usage of the PCI card data inside the infrastructure. This creates a security problem and opens up the environment to outside interference so a virtual server environment requires new thinking when it comes to network security.

In addition, further security challenges arise with the growth of external communication technologies such as Voice over Internet Protocol (VoIP). This increases network usage, introducing new security challenges.

The effective way to combat these problems is to ensure security, not just in front of the servers but also between the various servers, using professional security gateways designed specifically for running inside the virtual environment.

This security gap can be plugged by Clavister's new operating system, CorePlus 9.10, which brings with it a number of features for traffic optimization including gigabit and IDP traffic shaping,

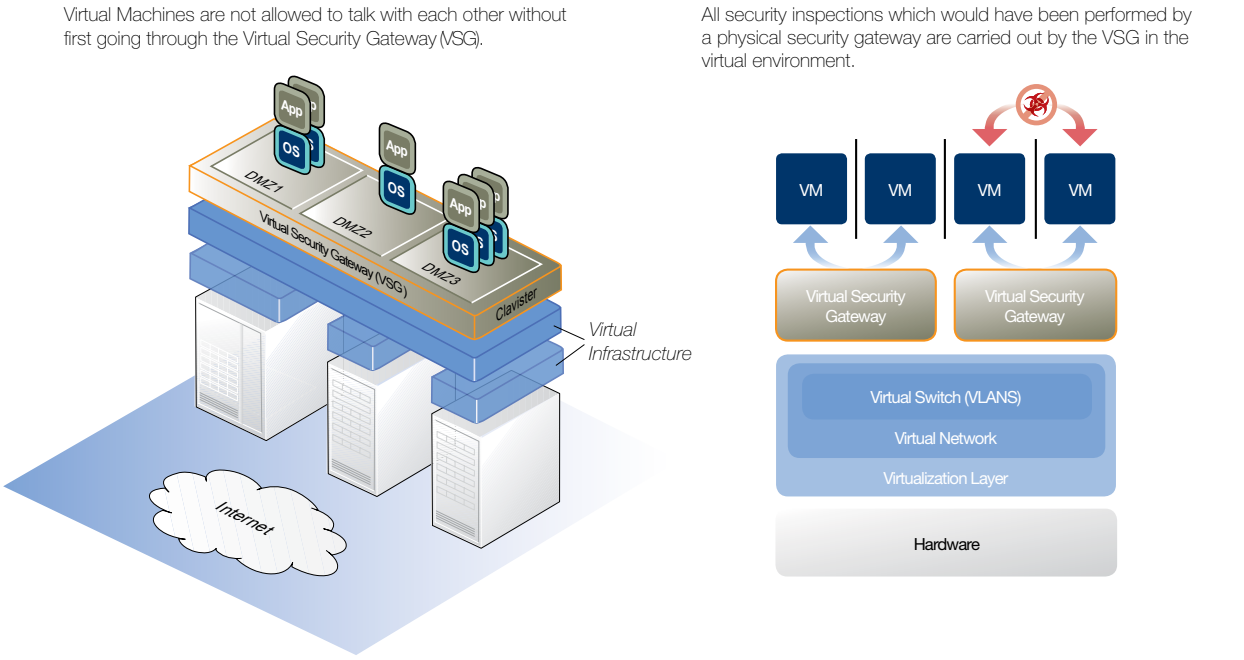


Figure 3: Securing the virtual environment

route load balancing and SLB server monitoring. CorePlus 9.10 can be run as a virtual appliance inside a VM. Virtual security gateways for ESXi (and soon for Xen and other hypervisors) will be offered not only as an alternative to physical appliances but also as a more effective way to protect dynamic virtual infrastructures where multiple applications, or even multiple customers, share the same physical resources.

Clavister CorePlus monitors and shapes network traffic for content filtering, offers intrusion and virus protection and guards against denial-of-service attacks. ISPs, managed service providers and telcos are the company's primary targets. Hosters can sell security services to customers as a premium option. Carriers and cable operators offering virtualized services can deploy specific security gateways for individual customers.

Clavister claims an advantage over many of its direct physical appliance competitors because its OS was built to be portable, although it is targeted primarily at x86 chips and network processors. ASICs can't be virtualized, and more bulky network security operating systems, many of them based on Linux, would require too much RAM and storage to operate effectively within a virtual appliance.

Most security companies do not offer virtual security gateways. Clavister, however, has developed a unique solution that has been designed with virtualization in mind e.g. footprint, RAM/Disk-space. This means that organizations will benefit from fewer security gateways for physical hardware, which is increasingly important for data centers and server farms in respect of both space and power consumption, as well as system safety.

Therefore, companies looking to implement virtualization should not assume that everything is automatically secure when the reality is that they may be facing new security threats, however, SMEs should not be put off adopting virtualization as the benefits far outweigh the challenges.

About Clavister

For over a decade, Clavister has been delivering leading network security solutions, providing commercial advantage to businesses worldwide. The Clavister family of Carrier Telecom Security Systems, unified threat management (UTM) appliances and remote access solutions provide innovative and flexible network security with world-class management and control. Clavister is a recognized pioneer in virtualization and cloud security. This compliments its portfolio of hardware appliances delivering customers the ultimate choice of network security products. Clavister products are backed by Clavister's award-winning support, maintenance and training program. Clavister boasts an unprecedented track record in pioneering network security solutions including the two largest deployments of Virtual Security Gateways in the world to date.

Clavister's solutions are sold through International sales offices, distributors, and resellers throughout EMEA and Asia.

To learn more, visit www.clavister.com.

Clavister Contact Information

Sales Offices
www.clavister.com/about-us/contact-us/worldwide-offices

General Contact Form
www.clavister.com/about-us/contact-us/contact-form

CID: clavister-whp-virtualization-101 (2011/02)

WE ARE NETWORK SECURITY

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com