

Virtualization Management and Security - the Key to a Fully Virtualized Datacenter

All of us are familiar with the benefits of virtualization. Consolidating servers and/or desktops saves on capital costs such as hardware and operating expenses including cooling and electricity. Virtualization can also reduce people costs by simplifying and automating many routine management tasks. There is plenty of empirical evidence that demonstrates dramatic cost reductions with virtualization. One large financial institution has documented \$125M in capital expense and operating cost savings in just a two year period. So if the technology is proven and the cost benefits unequivocal, then why are so few data centers fully virtualized?

Recent surveys indicate performance and scalability are key technical concerns to deploying more applications on a virtual platform. However these surveys also show that main *operational* inhibitor is the ability to secure and manage the virtual infrastructure to the same standards that we have achieved in the physical environment. Unless we can satisfy application owners as well as internal and external auditors that they will have the same level of performance, control and compliance in the virtual world as they now have in the physical one, the goal of a fully virtualized datacenter will be hard to achieve.

Today the virtualization paradigm is at a crossroads. So far the vast majority of applications running in the virtual infrastructure are less critical applications such as test/development, email, Web servers, etc. To fully realize the benefits of virtualization we now must move our most sensitive and "mission critical" applications to the virtual platform.

By definition these types of applications have well defined policies for management and security. Sensitive applications (and their server, network and data storage infrastructure) must be isolated from other less sensitive applications. Virtual servers, networks, and data stores must be protected from internal and external threats in a verifiable and auditable way. Configuration changes must be closely monitored and clear protocols must be enforced before changes to the environment can take place. Performance SLA's must be monitored and strictly adhered to. Compliance with internal and external standards and processes must be closely watched and audited.

In today's physical datacenter we have a host of security and management tools at our disposal to monitor and enforce our organization's standards, policies and procedures. Enterprise Systems Management (ESM) products as well as firewalls, intrusion prevention systems (IPS), VLANs, and other technologies are widely used and well proven. They may not be perfect, but we have come to accept and rely on them.

Some will argue that these tools can be easily extended into the virtual world. However that viewpoint overlooks the many fundamental differences between the virtual datacenter and the physical one. Managing and securing the virtual datacenter requires a different approach and new technologies.

What is so different in the virtual world from the physical one? After all, a Windows server is the same in either environment right? While the a virtual machine running Windows Server may appear the same as a physical machine running the same operating system, there are profound differences.

For one thing, to provision the physical machine requires the purchase of hardware, installing an operating system and other software, racking the hardware, and connecting it to the right network. This process can take hours, days or in some cases weeks depending on the processes in the datacenter. A virtual machine can be provisioned, imaged, and connected to the network with the click of the mouse in mere minutes.

Once the physical machine is mounted in the rack and connected to the right network, it is unlikely to get up and move to another location, another network or another datacenter. Its location on the network can be uniquely identified by its IP or MAC address. A virtual machine is an “on demand” resource that can move from one physical server to another or even from one datacenter to another automatically. IP addresses and MAC addresses can be arbitrary and subject to change depending on configuration.

Management and security tools built for the physical environment have a hard time coping with the dynamic nature of the virtual environment. Tools that manage physical networks expect attributes like IP and MAC addresses to remain constant. In the physical datacenter network and switch configuration is managed separately from server configuration. In a virtual platform networks, switches, and servers are all virtual objects which exist only in software. Because all of these objects are interrelated and highly dynamic, configuration management of the virtual environment is far more challenging.

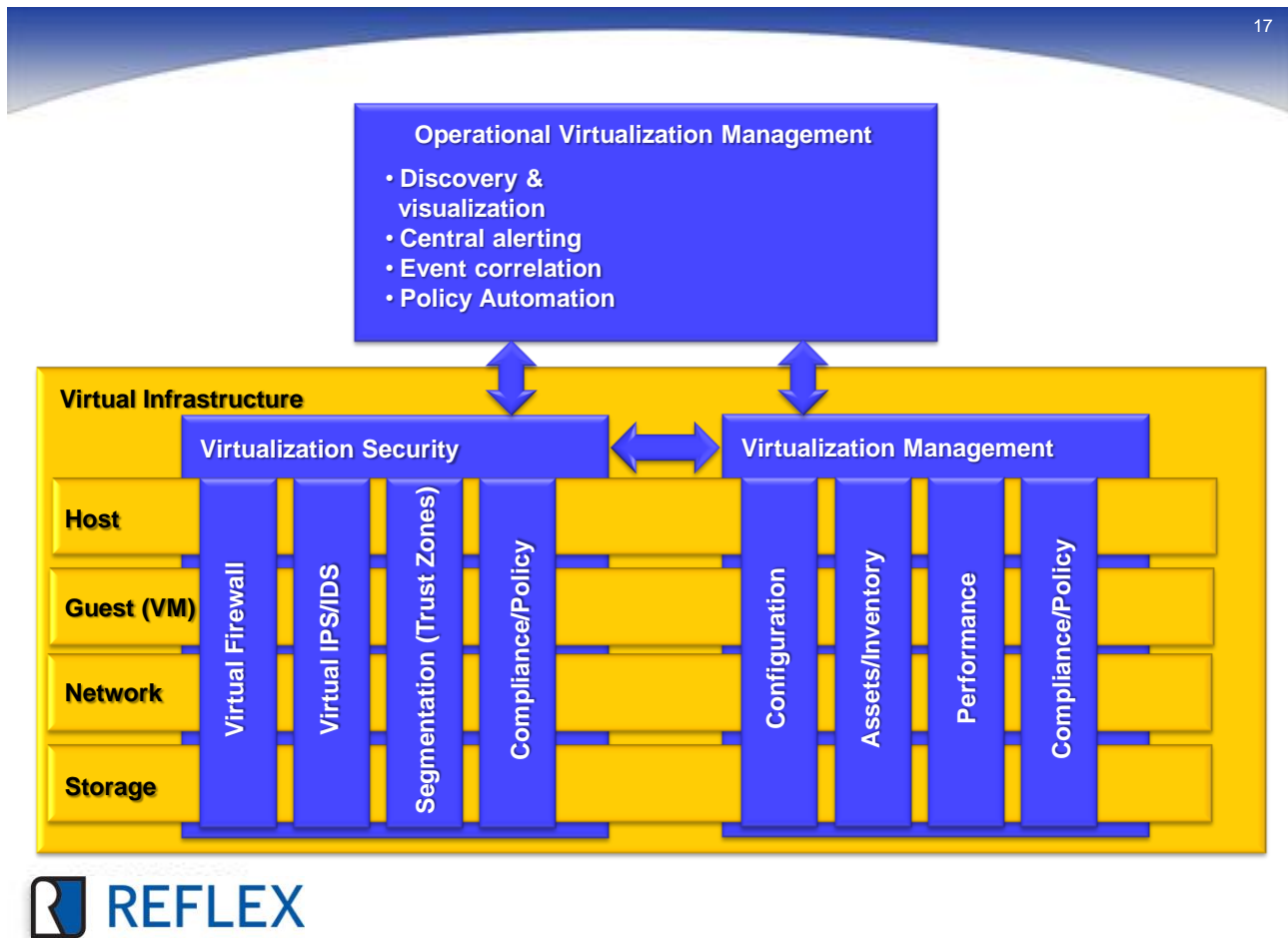
While the dynamic nature of the virtual infrastructure could be viewed as a management and security nightmare, it can also be viewed as an opportunity. Because the virtual environment is so flexible there are many management tasks that can be done better and cheaper or even automated. In fact, with management and security tools designed for the virtual infrastructure, you can achieve even higher levels of datacenter automation and significant operating cost reductions.

For example, ESM tools today assess the software assets installed on a physical server in one of only two ways. They either scan the machine or require an agent to be installed on that machine. Neither approach is ideal. Agents consume CPU cycles and scanning, well lets just say scanning can deliver unpredictable results. Neither approach is viable if you don't have permissions on the subject machine or if the machine is powered off. In the virtual space you can determine precisely what software is installed, who installed it and when it was installed without scanning or using an agent and with orders of magnitude greater speed. You can even obtain this information if the virtual machine is powered off!

Segmentation is another example of where the right virtualization tools can provide more capability, higher automation and lower cost. In today's physical environments we typically achieve separation of applications, servers, and storage with physical switches using VLANs or in some cases physical firewalls. VLANs require expensive physical switches and have a limited number of groups (Zones or Trust Zones) that you can create. Firewalls are also expensive and highly inflexible. If a machine moves from one VLAN to the other it must be manually reconfigured with different IP addresses and possibly different Access Control Lists (ACLs)

If you use VLANs or firewalls to create segmentation in the virtual environment, you will restrict the ability of the virtual infrastructure to dynamically respond to the changing demands of the business. Moving a virtual machine from one host to another will require someone to manually reconfigure the settings on the switch or manually modify firewall rules. Moving a virtual machine from one datacenter to another will require even more extensive manual changes to the firewall, switch or network configuration.

On the other hand, if you use security tools designed for the virtual environment, you can have the potential to create a less complex, flattened network (using less physical switches) divided into as many segments or Trust Zones as you would like - all completely separated in software rather than expensive hardware. With virtual Trust Zones, you can move virtual machines around from host to host or from datacenter to datacenter or even from the datacenter to the public cloud without reconfiguring the network, changing firewall rules or ACLs. This means far less manual involvement and far simpler configuration management. Moreover, virtual Trust Zones are more auditable and better able to meet strict compliance requirements than a hybrid physical/virtual solution.



Copyright 2009 Reflex Systems Inc.

Security is another area which requires tools designed specifically for the virtual environment. Physical security products such as firewalls and IPSs are designed to protect against a wide range of external threats and are designed primarily for the perimeter of the enterprise. Since we can presume the virtual datacenter is protected by these perimeter defenses, virtual security is less external threat driven and more about internal threats, segmentation, policy and compliance.

For example, physical security devices are rarely used to monitor traffic between machines inside the datacenter. Not necessarily because there is no need, but mainly because it is too expensive compared to the risk. In the virtual datacenter it is easy to monitor all traffic between virtual machines with the right tools. Not only is it cost effective, it enables organizations to better manage separation of resources, monitor data loss prevention, and enforce compliance policy.

Take this use case: Payment Card Industry (PCI) policy requires traffic going to and from servers that process credit card data to be encrypted. In the physical world you would have to deploy an IPS on the internal network to detect this. With the right virtual security tools In the virtual datacenter, you can not only detect any violations of this policy at a fraction of the cost of a physical IPS, but you could automatically quarantine the offending machine – actions that would have to be performed manually in the physical world.

Today it is estimated that it requires at least one person to manage and secure every 20 physical servers. With virtualization one person could manage almost 5 times that amount. By using management and security tools designed to take advantage of virtualization one person could manage over 500 servers. Since the largest line item on the IT budget is people, this technology can result in more savings than from server consolidation itself.

Therefore it is time to think outside the box when it comes to management and security for virtualization. Instead of trying to fit a square peg in a round hole by forcing tools designed for the physical datacenter to manage the virtual datacenter, consider tools that understand and leverage the capabilities of virtualization. Next generation tools designed to take advantage of virtualization can make deploying mission critical applications in the datacenter not only possible, but much more cost effective.