



Virtual Machines: They might not hide, but can they run?

By Dan Kusnetzky, Principal Analyst

OVERVIEW

The appearance of virtual systems and virtual resources in the industry standard part of the data center has offered the hope of increased flexibility and reduced costs. It has also introduced challenges that were not part of the operational plans of many organizations.

In my last paper, *Virtual Machines — You Have to See Them to Manage Them*, I explored the issues associated with tracking and monitoring virtual environments. This time, we take the next step. If we fix the visibility challenge, what about the manageability challenge?

It is clear that virtual environments, like physical environments, need to function according to the policies set by the IT administrators. Best practices and execution of policies have become routine when it comes to the management of physical systems and resources. Having succeeded in the physical space, most organizations have chosen to extend these practices as they move applications and systems into virtualized environments. Whether this is enough is yet to be seen. Industry standard systems that support virtual resources are quite different from what's been seen in the past.

WHAT DO ORGANIZATIONS WANT IN A SOLUTION TO THE VIRTUALIZATION MANAGEMENT PUZZLE?

Virtualization introduces new elements to the puzzle of policy management, including the following:

- ☒ Network access to both virtual and physical resources must be controlled. This includes both physical to virtual and virtual to virtual communications.
- ☒ Mingling tasks running the same or different operating systems on the same machine under a single hypervisor has many implications ranging from application performance management to availability/failover management to compliance management.
- ☒ Virtual resources can be created, used and then destroyed much more easily than physical resources. Who manages this process? Who maintains logs for auditing purposes? Physical systems can easily become clogged with “ghosts” from the past that are no longer wanted or needed.
- ☒ It is easily possible for a malicious person to create a rogue copy of a virtual machine to breach security or management procedures. A non-malicious case would be someone putting up a virtual server to support a music or video sharing service. On the one hand, this could lead to theft of critical data. On the other it could lead to legal disputes over the sharing of digital content. Who is responsible for administering organizational policies in this area? Can the organization be certain that all copies of highly proprietary data and applications are accounted for? What is the policy when “extras” are discovered?

IT executives are increasingly facing the fact that there really is no good way of dealing with the following issues:

- Determining what policies are best suited to address the challenges described above
- Having a mechanism to set those policies consistently, throughout the virtual infrastructure
- Insuring and reporting on the success of the policy enforcement in the environment

What is clear is that it is no longer easy to determine either what physical and virtual systems are doing, who they are doing it for or, more importantly, what they are not doing (outages).

EVERYONE IS TALKING BUT, DO THEY HAVE A SOLUTION?

If one does a quick scan of industry announcements, it's easy to see that the suppliers of virtual machine software have focused their efforts on developing tools designed to manage their own hypervisors, not the multitude of virtual machines they enable. The companies focused on providing broad management frameworks have focused on managing physical resources and haven't yet stepped up to managing virtual resources. Knowing what everything is doing on a moment by moment basis can be quite challenging and is likely to require tools that are only now emerging.

If an organization needs to maintain an audit trail of where the computing was done, where the data is and other important data points, they increasingly face a very difficult challenge. Complying with some regulations may be impossible unless there is a structured, well-defined way to track everything. Organizations simply must have a trail of their motion, a history, or a "chain of custody" as they transfer from place to place and from test beds to actual production.

CHARACTERISTICS OF AN IDEAL SOLUTION

To enable proper lifecycle management of this sort, a solution needs to be:

- a) Cognizant of the distinct qualities of the virtual environment
- b) Able to seamlessly incorporate into that environment, through easy deployment and scaling, and ultimately, support multi-platform datacenters
- c) Synergistic with the goals of the environment – and thus not tax the performance of the infrastructure or create bottlenecks.

I suspect that there are many other areas that should be addressed over time.

WHY DON'T TRADITIONAL APPROACHES WORK

The simple answer to this question is that virtual resources are different than physical resources in several important ways. These differences mean that traditional approaches often don't work in a virtual world.

Most organizations don't have standard processes to collect and maintain lifecycle information about virtualized resources. Much of this critical information doesn't really fit into their usual tracking systems.

For example, one simply doesn't install a physical system one morning and retire it that afternoon. Virtual systems are often created, used and then destroyed in a day's time.

Furthermore, it is unlikely that a physical system would be picked up and moved from one side of the datacenter to another several times a day. In a virtual world, this is quite possible. There are many vendors offering orchestration tools that can move virtual systems from one physical machine to another or change it from

being a virtual resource to a physical resource based upon policies or to achieve service level objectives.

Not only is the fundamental data model of traditional tools flawed in these ways, the architecture is equally inappropriate. Fat agents in each virtual machine could be the end of any performance gains made by virtualization. And log files are often not sufficient for generating real-time insight into the environment. The challenge of monitoring virtual environments has many new dimensions of complexity.

It is not clear who would be responsible for virtual resources, as well. Would the system administrators who operate physical systems be also be responsible for the virtual resources that machine might be supporting? Would that job fall to the person in one of the business units who created and is using that virtual system? In the end, without help, administrators really have no reliable way to know what's running, where it's running, and what compatibility issues it may generate.

S U M M A R Y

As organizations increasingly turn to virtual machine technology for both client and server environments, it would be wise to consider the challenges this technology imposes as well as the benefits they may bring. It would also be wise to look at emerging technology not just the technology offered by the traditional suppliers of management frameworks

The Kusnetzky Group recommends that organizations develop a sound, well planned set of processes and procedures to manage these resources. It would also be wise to seek out tools that can automate this process.