

WHITE PAPER

Five Virtualization Pitfalls To Avoid

by Zeus Kerravala, Senior Vice President, Yankee Group

www.xangati.com

Five Virtualization Pitfalls to Avoid

Table of Contents

Introduction – Virtualization Benefits	2
The Reality of Server Virtualization	3
The Five Pitfalls of Virtualization	5
Pitfall 1: Failing to Track Virtual to Physical Communications	5
Pitfall 2: Disregarding Critical Inter-VM Communications	6
Pitfall 3: Assuming IP Storage Configuration is “Plug and Play”	7
Pitfall 4: Keeping Status Quo Service Management/Support Techniques	8
Pitfall 5: Centering Focus only on Your VDI Ecosystem	9
Xangati Solution to Avoid Virtualization Pitfalls	10
Conclusions and Recommendations	11

Introduction - Virtualization Benefits

As a technology category, virtualization has been around about a decade now but it’s only been in the past few years it has become a core technology for more organizations. Although there are numerous technologies that fall under the broader definition of virtualization, the primary focus has been on server virtualization because of the multifaceted value proposition. If deployed correctly, server virtualization will:

- **Improve the utilization of servers.** Servers that are non-virtualized have an average utilization of about 25%. Once virtualization has been deployed, utilization jumps to 70% and in some cases close to 90%.
- **Reduce the number of physical servers.** Running multiple workloads on one server has been a key initiative as organizations look to optimize the amount of data center space used. It’s typical to see consolidation of servers be in the 5:1 up to 10:1 range.
- **Contribute to corporate “green” initiatives.** Server virtualization reduces the number of physical servers needed. This will not only require less physical data center floor space but also use less power and require less cooling to achieve the same workloads.
- **Give a fast ROI.** The current economic environment has put a renewed focus on ROI. Business leaders demand a 12 month or less ROI from almost any technology initiative to be approved. The very nature of virtualization lends itself to rapid ROI, as evidenced by the survey data in Exhibit 1. 26% of respondents revealed that they received an immediate ROI; this immediacy is achieved from avoiding additional hardware purchases. Another 24% indicated an ROI that ranged between one month to one year, which is a necessary condition for technology deployments today.

If your firm has already deployed server virtualization in a production data center, how long did it take to realize an ROI?

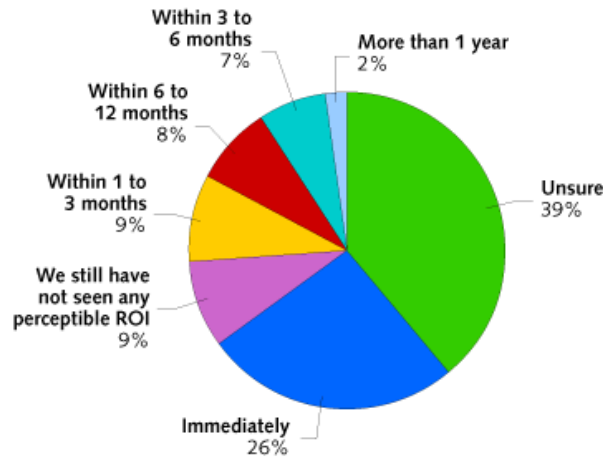


Exhibit 1: The ROI of Server Virtualization

Ultimately though, CIO’s see server virtualization as a core technology that will act as the foundation for other strategic initiatives such as unified computing, cloud computing and desktop virtualization. The value proposition for most companies is so strong many CIO’s can not imagine life without it. A CIO from a major U.S. bank made the comment “I’ll never go back to a non-virtualized environment” at a recent workshop on virtualization.

The Reality of Server Virtualization

Despite the almost unlimited potential of virtualization and incredible industry momentum, server virtualization is still limited in its use within most companies today. The Yankee Group survey data shown in Exhibit 2 paints a rosy picture, where 57% of respondents claim the technology is already deployed for production servers.

Has your organization deployed or plan to deploy server virtualization?

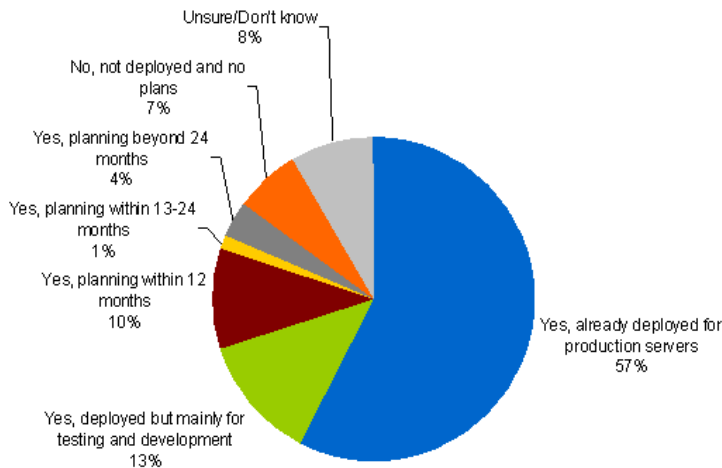


Exhibit 2: Server virtualization appears to be well adopted

However, Exhibit 3 shows that for most organizations, the percentage of servers virtualized ranges only between 1% and 29%. Admittedly, there are some applications that require physical USB keys to operate correctly, or receive continuous data feeds making it near impossible to virtualize these however, these applications make up a mere few percentage points of the overall applications deployed today.

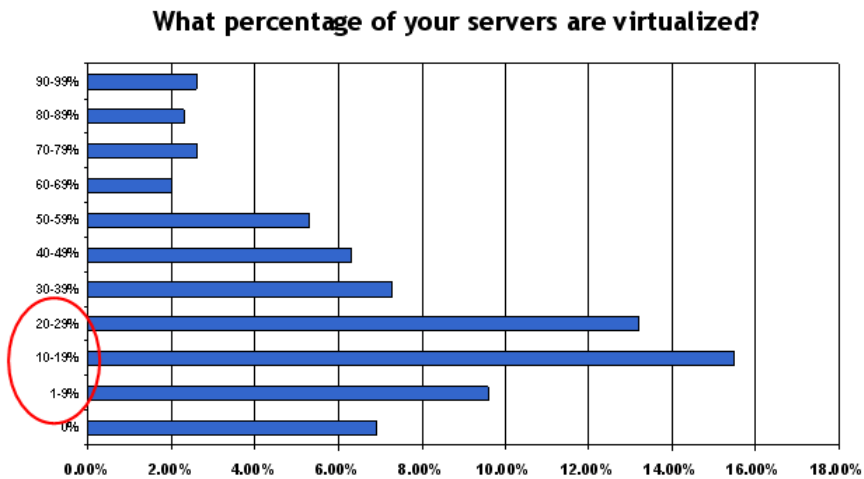


Exhibit 3: Server is still limited in its usage

This begs the obvious question, if the value proposition is so strong and the technology is a foundational requirement to launch other future initiatives, why is adoption still so low? There are a number of reasons why this is, including the following:

- Difficult to understand the impact virtualization has on the network
- Lack of confidence in running mission critical applications on virtualized servers
- Poor understanding of how virtualization impacts the end-user experience
- No single IT domain understands the cross functional areas that actually comprise the data center. In other words, how to manage compute, storage and network resource in conjunction with one another
- Few best practices around large scale deployments of virtualization

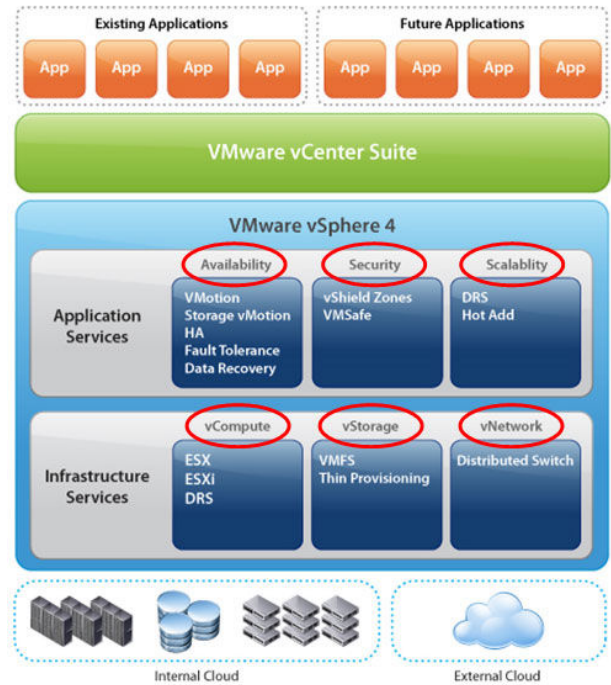
As varied as these problems and others appear to be, the underlying root cause is a lack of manageability and visibility cross all of the physical and virtual domains. Exhibit 4 (next page) depicts a virtual environment and the image shows that while the concept of a virtualized data center is simple, the actual deployment requires knowledge of all areas of IT. Properly maintaining a virtualized infrastructure requires knowledge of availability, security, scalability, compute, storage and networking. These skills are rarely found in a single individual and given the degree of complexity involved require a level of coordination and integrated planning that has yet to be distilled into a set of best practices by the large majority of IT organizations.

The next section will outline the five most common pitfalls associated with wide scale adoption of virtualization and provide some insight as to how better management and visibility can help avoid these most common risks.

The Five Pitfalls of Virtualization

Pitfall 1: Failing to Track Virtual to Physical Communications

Managing across the physical and virtual domains is very difficult – it requires “human” correlation. A virtual workload can exist on one server at one moment and then not be there the next. The VM may have been used to test something and then was shut down or it may have been migrated to another server making it very difficult to know which virtual workloads are running on which physical servers.



(Source: VMware)

Exhibit 4: Virtualization is a complex mesh of data center technologies

This type of complexity is just one example why in a recent survey of data center managers, 85% of the respondents did not feel the legacy products used to manage the physical environment would be sufficient in a virtual environment.

Legacy management software is anchored on static maps and alarms being triggered when devices go down and then again when they come back up. Legacy software leaves blind spots between the infrequent polling intervals and lack of visibility into virtual environments without excessive installation of new probes and agents that still provide little more than element status (red, yellow, green). Effective management of virtual environments requires a deeper understanding of the interplay between the physical and virtual environments. Multiple un-related management products are typically invoked to facilitate “human correlation” when problems need to be identified and resolved. This commonly leads to finger pointing between the IT silos and longer than necessary troubleshooting time.

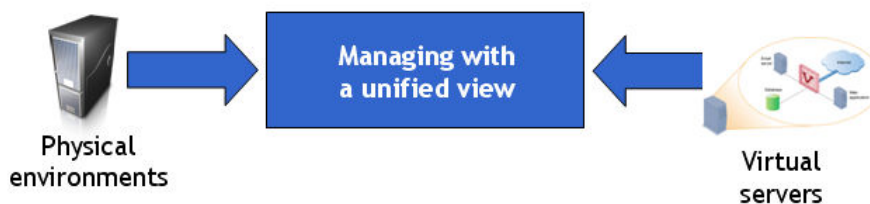


Exhibit 5: Virtualization requires managing a unified view

A management system capable of spanning both physical and virtual domains (Exhibit 5) is a necessity to create the level of visibility required to fully manage a virtual environment. Such visibility will help administrators isolate problems quickly and drastically reduce mean time to repair.

Pitfall 2: Disregarding Critical Inter-VM Communications

Inter-VM communications are invisible to legacy management software and even most new management software. Even VMware's vCenter for managing individual VMs doesn't show VM to VM communications. If you instrument a three tier application within a single hypervisor (Exhibit 6) – how do you investigate a problem? A vSwitch, or virtual switch is a software-based network switch that connects virtual servers and is a critical part of a good server virtualization design. The existence of a vSwitch validates this pitfall as without a vSwitch no visibility into Inter-VM communications is possible. Even with a vSwitch additional tools are required (like Xangati). In fact, the vSwitch has been thought of by many as a panacea to any performance problems in a virtual domain by adding “network capacity” within a physical server so virtual servers can communicate directly unimpeded by the physical realm.

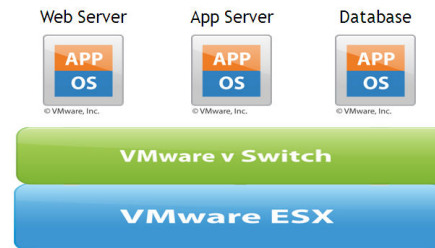


Exhibit 6: Intra-ESX traffic can cover a full N-Tier application - how do you see it?

The vSwitch may be a virtual switch, but it is a network switch and should necessitate the same level of expertise and management one has come to expect with a physical switch. This means the network configuration parameters, policies and other settings on the vSwitch need to be consistent with the physical switching environment (Exhibit 7) and controls need to be in place to ensure this consistency has been maintained before significant communication occurs between virtual servers hosted within the same hypervisor. Otherwise, performance variability will likely exist, variability that will be difficult to unearth in production and that could cost you dearly.

Compounding the complexity is the default visibility “blind spot” that exists for application activity traversing a vSwitch – you just can't see it without special tools. This is why it is essential to look at NetFlow as a strong technology to remove the blind spot. NetFlow feeds key information about communication and application activity without agents or probes. But, you have to study the market carefully to make sure the version of vSwitch you deploy supports NetFlow or whether a third party extension like the Nexus 1000V should be used.

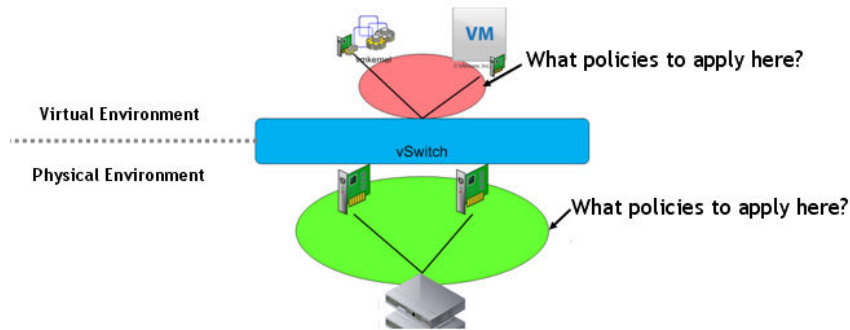


Exhibit 7: The vSwitch spans both the virtual and physical environments

Pitfall 3: Assuming IP Storage Configuration is “Plug and Play”

The ability to move a virtual workload creates a tremendous amount of flexibility for organizations. VM mobility allows IT departments to move a workload, in real time, in the event of a disaster, for maintenance purposes or for performance. However, when the workload moves, network configurations and storage must adapt to the moving VM workload. Establishing network configuration parameters that work properly in this environment is difficult. While emerging “unified computing” systems can help with synchronization of network settings, making sure you have it right is challenging – especially if you are working from historical reports and can’t validate it live.



as additional storage
VMs start moving...

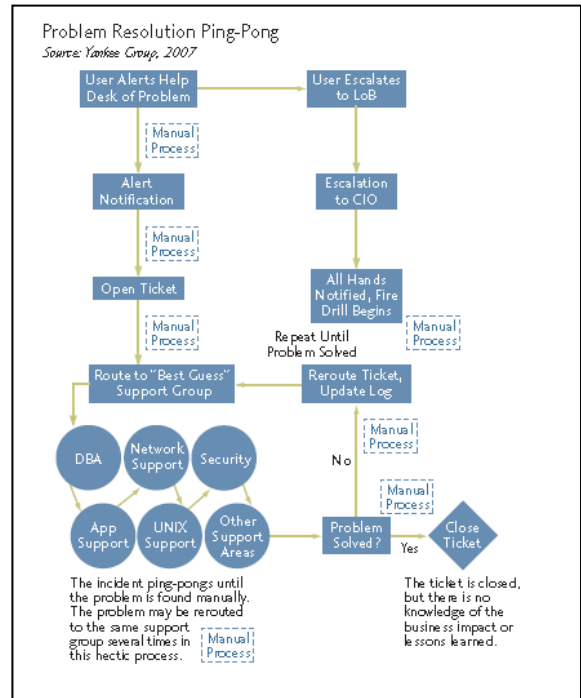
Exhibit 8 shows how simple storage looks to be in the data center. Unfortunately mapping VMs to storage is extremely complex and the adoption of IP based storage is accelerating this complexity. When a VM is moved, performance can suffer immensely and immediately due to a mis-configuration of storage resources for the new VM location. And, unfortunately, mis-configurations in the virtual environment are common. For instance, one federal entity found unsecure traffic in its secure areas – and didn’t know why. It turns out it had improperly configured VLANs which when vMotion moved certain VMs, unsecure traffic was forced through secure areas to get to its assigned IP storage.

One way to solve this problem is to simply replicate storage to every location that may need it. However, the cost of this alone could erode the savings in the consolidation of servers. Additionally, managing this amount of storage can lead to data integrity problems if the storage is not replicated properly. Sure you can use storage vMotion to move the storage a VM uses from host to iSCSI to a SAN or wherever – but how long does it take to move and what impact is this having on performance? Storage can cause your organization significant

problems if proper visibility tools are not put in place. How do you manage something when you aren't sure where it is or what is using it?

Pitfall 4: Keeping Status Quo Service Management/Support Techniques

Forrester reports 75% of problems are reported by end-users through the service desk, not having been detected by infrastructure management solutions. No matter how big the cost savings is for a VM deployment, it can all be for naught if the end-user experience with their applications suffers. If users are no longer able to do their jobs effectively because of poor application performance, the company will suffer. Organizations will not tolerate such a state even with all the great cost savings virtualization promises. Even so, given all of the daily changes taking place and the pitfalls outlined in this paper - how can your IT department be assured that everything will function correctly all or most of the time? The fact is everything won't function correctly and current bottom up management tools (tools looking at the health of individual elements) are not designed to provide the level of end-user experience visibility or communications visibility required to support physical and virtual domains – exacerbating the problem resolution ping pong common in most organizations and illustrated to the right.



IT organizations need to have a way to measure and monitor the end-user experience from the top down or outside in (Exhibit 9) to identify the cause of problems as fast as possible so they can be fixed as fast as possible. As Yankee Group research indicates 90% of the time spent resolving a problem is just identifying the cause of the problem, anything that helps identify the cause of problems will pay dividends quickly. For example the ability to record problems as they arise can be a huge boost as the virtualization team will have real time information to isolate the problem without having to spend hours or days recreating it to find the cause. Top down management approaches providing live visibility and DVR capabilities are therefore critical to successful VM deployments with satisfied users and fast ROI.

90% of problem resolution is identifying the problem
Yankee Group

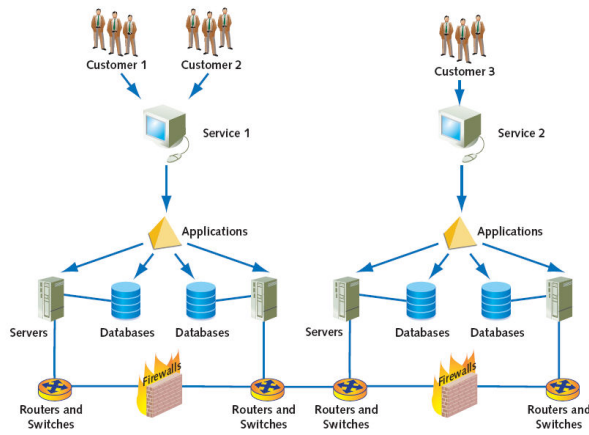


Exhibit 9: Top down management

Pitfall 5: Centering Focus only on Your VDI Ecosystem

If you are implementing VDI (virtual desktop infrastructure or just virtual desktops), you have to look beyond the ecosystem required to implement VDI to everything sharing anything with your VDI implementation.

Why? Because your end-users' desktop experience is over a shared infrastructure – and their experience will be impacted by everything communicating on that shared infrastructure.

VDI splits an end-user desktop into three or more distinct entities – all of which can be adversely affected by something unexpected.



- 1) The monitor and thin client on a physical network that you interact with
- 2) The virtual desktop (VM) in a data center running the desktop OS and office type applications
- 3) The network storage array which stores the files of data that used to be on your desktop and are now separate from the VM

These three entities communicate with each other over your shared network – continuously – with potentially disastrous results due to resource conflicts. Continuous presentation of activity to the thin client means every key stroke, every mouse movement and every click goes over the network to the VM running the OS and desktop applications, with every result going back to be displayed. Any time data is needed files must be accessed over the network as well, and then displayed to the end-user. Traffic is generated regardless if an application is desktop or network-based, with conflicts coming and going in the blink of an eye as hundreds to thousands of people flood your shared network with VDI communications. For your VDI pilot to be successful – you must have visibility into what is happening at all points, and the more live the visibility the better.

Xangati Solution to Avoid Virtualization Pitfalls

Xangati provides a new approach for planning, monitoring and managing your virtualized infrastructure - and avoiding the pitfalls highlighted in this white paper. Below are aspects of the Xangati solution making it uniquely suited to complement the bottom up management solution (e.g., VMware's vCenter) you are probably already using and anxiously awaiting additional new features:

- **Live, video-like visibility:** The only way to see performance hiccups is with live, to-the-second video-like visibility into what end-users, applications, networks and servers are doing – right now. Without this live visibility intermittent performance issues linger. They linger because traditional management solutions based on polling data with 10 to 30 minute polling intervals do not capture the dynamic performance changes that come and go “in the blink of an eye” and wreak havoc on your virtual world.
- **Visibility into each and every device, enterprise-wide, on your virtual and physical infrastructure:** View anything with a presence on your infrastructure, from IP networked devices (e.g., hypervisors, VMs, iSCSI targets, thin clients, VoIP phones, physical servers, etc.), to applications and network interfaces. For each and every one of these elements, Xangati is aware of how they are communicating with the rest of the infrastructure and displays this information live – in essence making it like you are watching its activity on TV. This focus on communications is essential as it shows the relationships between elements within your virtual ecosystem and between your virtual and physical domains. Only through this visibility can you see if elements on your infrastructure are communicating in the way you would expect. And, because everything shown live is also stored historically you can monitor changes in real-time to ensure they work as intended, have not broken something else and enable you to document positive improvements over time.
- **DVR recordings of activity:** In addition to presenting information live the system produces “DVR-like” recordings of any activity, providing full situational awareness at the time of a performance problem. With DVR recordings you do not have to “re-create” the problem to identify the cause as you just rewind and play to see the cause. This saves hours and days with each problem as recreating virtual world problems is often a futile effort. DVR recordings can be triggered in three ways:
 - Xangati user initiated: For example, a VM administrator can create a recording that shows his VM traffic is being slowed down on a bottlenecked WAN interface for a network engineer to review and see what adjustments can be made.
 - Event-driven: If an element is performing outside its normal profile, the system will alert an administrator to the issue and present them with a DVR-recording of what that element was doing at the time of the problem.
 - End-user initiated: End-users use the Visual Trouble Ticket™ portal to initiate recordings when they have slow performance. These recordings show what applications the end user was running, bandwidth being consumed in and out and the latency of their connection. This

way IT has all the information they need to rapidly resolve that performance issue and ensure it was an isolated issue.

- **No agents, no probes:** The Xangati solution uses NetFlow, a data feed supported by both virtual switches and physical routers/switches which eliminates the need for agents or probes. NetFlow summarizes all communications on the network and is pushed effortlessly to the Xangati appliance. In this manner, IT gets comprehensive coverage immediately upon deployment vs. the piecemeal and costly deployment scenarios associated with agents and probes.

Conclusions and Recommendations

Virtualization is a rapidly expanding core technology for companies today seeking lower operating costs and higher asset utilization. However, successful deployments require more than just consolidating a bunch of servers and then treating everything else the same. The flexibility virtualization delivers also creates many pitfalls that can eliminate all of the ROI from a deployment. If your organizations in implementing virtualization, consider the following:

- Virtualization is for more than just server consolidation. Virtualization is an extremely powerful technology that can improve the efficiency and operations of far more than just servers. Consider broadening your use of virtualization after a good understanding of server virtualization is in place.
- Ensure management and visibility products are in place before broadening your use of virtualization. This is the only way to effectively scale virtualization without falling victim to the many pitfalls associated with this technology.
- Choose management solutions that were designed for virtual environments. The management tools that work well in a client server environment are not the ones used to manage mainframes. Similarly, the management tools used to manage virtual environments are different from the ones you have in place today.

About Xangati

Xangati develops virtual management software for today's virtual world. Xangati provides live, video-like visibility into the performance of each and every application, server, network, and end-user device without agents or probes. This live visibility eliminates blind spots left by existing management tools and accelerates savings from virtualization initiatives. For more information, visit www.xangati.com.