

## ***Virtualization: a History and a Future***

Many IT executives today are looking for ways to get the most out of their existing and future infrastructure. One of the directions they are looking at is virtualizing more of the infrastructure. This has gotten a lot of hype in the last couple of years with server hypervisors that enable multiple operating system versions to exist on the same server hardware platform.

While it is tempting to look exclusively at the benefits that virtualized servers provide, the reality is that virtualization also adds layers of complexity to the environment that make it more difficult for tuning the infrastructure for proper performance. In addition, the added layers of abstraction can serve as new gateways for infiltration into the enterprise, which adds another risky security dimension to the picture. IT executives must be aware of how all these virtualization areas impact the enterprise in order to optimally take advantage of their benefits without falling prey to their shortcomings.

### ***The Scope of Virtualization Complexity***

**Networks** were the first infrastructure elements that shared resources for all the protocols, services and applications that run over the top of it.

**Server** virtualization has come into vogue lately with hypervisors and multiple operating system images running on the same physical box.

**Storage** has expanded virtualization with storage area networks (SANs) and network attached storage (NAS).

Finally, **business processes** are being virtualized with the use of service-oriented architectures.

Within each area, virtualization has grown in sophistication. However, there has been much less work in understanding how the virtualization in one domain affects performance and security in the other domains.

There are two problems that are created with these tiers of virtualization:

First, the performance of the overall application becomes nondeterministic.

Second, the different domains of virtualization add layers to the infrastructure that can be exploited for security purposes.

### **Performance Considerations**

From a **performance** perspective, a given SOA application can be built recursively upon sub-services. Each of these services can run on a different server, use different storage, and reside on different network locations in different geographies. When a higher level service requests a lower level service, it does not know *a priori* what server in what location will invoke the requested service. For this reason, it is very difficult to guarantee the performance of any given service. How much network bandwidth is required for services to run properly? How much latency can be tolerated between two services before the end user experience is adversely affected? IT executives must understand the low level details of the elements that compose these services and build the infrastructure in such a way that performance is acceptable within certain bounds.

## **Security Considerations**

In addition to performance difficulties, multiple layers of virtualization create more opportunities for hackers to get access to corporate resources. In general, the greater the complexity the greater the security vulnerability is. While a level of isolation of an operating system from its physical resources has its own security benefits, if a machine is compromised, then every operating system and application running on that machine is at risk. So, if there were previously ten applications running on ten separate systems and one got compromised, the one system is at risk, now, one application or system getting compromised could affect 10 systems. In this way, virtualization has a higher business risk associated with its use.

## **A Federated Approach to Virtualization Management**

The key way of tackling the complexity associated with virtualization is through federalization. Each sub-system should be focused on managing what it is best designed for. Network management systems should continue to focus on optimizing and running the corporate network. Systems management solutions should fine tune server performance. Security systems should be focused on firewalls, intrusion prevention, identity management, and so on. However, there should be a central system that establishes the overall enterprise management framework, and this higher level policy should be distributed to the domain-specific systems for enforcement. The parameters of enforcement should be general enough to go to sub-systems, and these sub-systems can then enforce policies in a domain-specific fashion.

The process for centralized control and distributed enforcement should occur in phases:

- Business Requirements Definition;
- Infrastructure Assessment & Analysis (has a special requirement base);
- Architecture Design;
- Infrastructure Implementation;
- Policy Establishment;
- Policy Enforcement

In Business Requirements Definition, the line of business manager should state the requirements for application performance in business terms: business throughput, transaction latency, application availability, etc. As these requirements are being defined, infrastructure domain owners should be assessing their existing domains to see what measurements can be performed to measure and enforce those business requirements in their domain.

Once the requirements definition and assessment are completed, IT executives can work on building an architecture that pulls together the capabilities from the different IT domains, understanding as well the collective limitations, to arrive at an architecture that cohesively blends the domain-specific elements together in order to manage the whole operation. Individual elements can then be built by domain specific experts, adhering to the higher level requirements without having

to worry about the details of implementation in different domains that are not germane to the domain specific implementer. In this way, parallel development can go on in different domains while the previous high-level coordination guaranteed the appropriate metrics of performance were established to ensure global optimization.

It should be understood that there will be times when building the infrastructure that performance priorities will be in conflict. The network will want to prioritize one application packet, while the identity management system will have a different priority packet to service. At the same time, a back end database may be prioritizing a completely different query. There will always be conflicts, but if application priorities are made at a global level, effective compromises can usually be made with the minimum expenditure of additional resources.

Once systems are built, they have to be managed. The policies that manage individual elements must come from a business and application focused central hierarchy. Only the business owner knows best what applications should have priority for execution in the enterprise. In addition, only the business owner knows how much he is willing to spend to mitigate certain security risks and what the appropriate corporate security policies should be.

However, once these policies are established, the enforcement of those policies the enforcement of those policies should be done locally, with domain specific tools and domain specific enforcement mechanisms. For example, the business owner can say application x must have 100 percent availability and the environment must be capable of supporting 20,000 transactions a day. From this business level policy, network managers can appropriately set network resource reservation levels and database managers can establish database query priorities with domain-specific commands that meets these requirements.

### **Dynamic Requirements**

Business must constantly respond to changes in the marketplace. Some of these changes are relatively slow, such as the move from strictly internal combustion powered cars to hybrid cars, some are more moderately paced, like the shift to buying downloadable music from buying it on discs, and still others are rapid changes, such as price spikes in the cost of petroleum products. How effectively an organization can respond to these changes is dictated, in part, by the organization's ability to change its IT systems. Consider some of the roles IT applications play in adapting to market changes:

- As partnerships are formed with other business, financial systems must be changed to accommodate new compensation models
- Following mergers, IT infrastructures must be integrated to accommodate combined business operations

- Downward price pressures drive process re-engineering and the adoption of greater automation
- Outsourcing of operations may require changes to network infrastructure, security policies and practices, and hardware configurations
- In addition to these common business dynamics, there are the expected but unpredictable events, such as natural disasters, that can disrupt operations and shift priorities.

### **Areas of Caution**

Of those familiar with virtualization, most are deploying it in servers, but a few are venturing into other areas as well. "Virtualization tends to be deployed for multiple reasons and tends to deliver multiple outcomes," said Rogers. The primary areas where virtualization is being used beyond servers include disaster recovery and storage. Other areas are being targeted as well. Virtual storage, on the other hand, he says is an obvious next step in virtualization efforts.

Rogers said test and development and infrastructure are common areas CIOs move to first. The key to success, however, is implementing one area at a time to ensure you have it under control before you move on.

Agility, after all, means the ability to move quickly in a new direction. Just be aware that the new direction may not be where you intended to go. Consider resurrecting the adage "look before you leap" but this time such wisdom applies more to where you go with virtualization rather than whether you should deploy it at all.

VM growth is no different than server growth. It may be easier and cheaper, but from the OS management viewpoint, you're doing the same thing. Likewise, the availability of your services is also in danger. Running five VMs on a single piece of hardware means that a hardware failure takes out five servers instead of one. VMWare and Citrix XenServer can both be clustered and run from shared storage, such that a hardware failure will result in the VMs immediately (instantly, even) being migrated to other servers. The problem is that VMotion requires the most expensive VMWare license, and a VirtualCenter server. Shared storage isn't as big of an issue these days with iSCSI, but it's still another aspect that must be configured.

The point is: dealing with VM sprawl is no different than dealing with scaling up to support more physical servers. Use whatever mechanisms are available on your given platforms, and do it right. A VM is, and always will be, just another server.

## Out vs. Up

I'd like to first spend some time talking about the philosophical difference between scaling "out" and scaling "up." Some applications can be scaled up, that is they can be run on faster hardware to support more transactions. We also call this "scaling vertically." Say we have a database server that can handle one million requests per second but, due to new demands, we need the database to handle at least two million per second. Databases are well suited for scaling up, since bottlenecks are frequently RAM and CPU.

Scaling out (horizontally) means to add more servers and spread the load across multiple machines. In the database example, this may be extremely difficult, since all database servers will need to use the same data and it will have to be replicated. Scaling out application servers, however, is a common practice. Before deciding whether to scale up or out, you must realize that scaling out presents its own problems. Web applications require session data so that a load-balanced cluster of servers will have the same state. A common example is authentication: if a user is authenticated with one server, and the load balancer decides to serve that user's next request (page click) via another server, it could fail to recognize the user is logged in.

Here are a few questions to ask before deciding that scaling out is the right solution:

- Does the application operate properly in a load- balanced environment?
- Will the application scale up to serve enough users without load balancing?
- Can I run many instances of the same application in an automatable and manageable way?

If you find yourself in the situation of having to scale up because of application limitations, you probably shouldn't be using virtualization at all. An application that requires its own server is not a candidate for virtualization. The overhead of virtualization, as small as it may be these days, will contribute to limiting your performance. Furthermore, you will gain none of the benefits of virtualization, such as consolidation and migration between physical servers, because the application must run on its own dedicated server anyway. The migration argument, in case of a hardware failure, is a weak reason to use virtualization since failover setups can easily be configured between two physical servers.

### **Rethink infrastructure barriers**

Gain greater business advantages from virtualization. Virtualization brings newfound freedom and flexibility to your infrastructure. Where it was once rare for several applications to run on one server, it's now commonplace. Workloads are no longer inextricably tied to the infrastructure where they are first deployed. Your infrastructure needs to be designed to let you capitalize on these new possibilities.

Ultimately, you need an infrastructure that lets you free the untapped potential of your data center—one that is built, managed and organized to take full advantage of virtualization. Built-in virtualization lets you capitalize on virtualization quickly. A modular infrastructure helps you flexibly use resources as business needs change. And advanced infrastructure management lets you create a self-optimizing infrastructure that helps you continuously put unused capacity and resources to work, where and when they are needed, to meet business requirements.

### **HP Server Example**

HP Integrity servers with the HP Virtual Server Environment and HP-UX 11i deliver mission-critical virtualization integrated with high availability right out of the box. HP ProLiant servers and HP BladeSystem are designed for virtualization, providing consistent, reliable performance and ease of management. The HP infrastructure management portfolio encompasses the core server management capabilities of HP Systems Insight Manager and the HP Insight Control Environment for deploying, monitoring and controlling ProLiant servers. Building on top of these is HP Insight Dynamics – VSE, the world's first integrated solution that lets you continuously analyze and optimize your physical and virtual resources in exactly the same way. It provides a single toolkit that delivers the freedom and flexibility of virtualization across your infrastructure. Meanwhile, the HP BladeSystem and its Virtual Connect architecture virtualizes the connection between blade servers and the storage and network resources they are connected to, so you can make server changes in real time, independent of storage and network connections. With Virtual Connect, you can wire everything once, and then add, replace or recover servers in minutes.

Storage is a key part of the equation. You'll want to implement a storage architecture that pools and shares your storage resources, designed for virtualization, with network storage or a shared storage solution. For example, the HP StorageWorks Enterprise Virtual Array (EVA) aggregates and automates array management tasks to manage more storage capacity with fewer resources and the HP StorageWorks XP Disk Array lets you virtualize nearly 250 petabytes on many storage systems behind it—whether from HP, or from third parties—and operate them as one pool of storage.

### **Rethink applications and IT operations management**

Leverage virtualization to improve business services. Better business outcomes are driven by better business services. The key is to dynamically link business services to the physical and virtual resources that deliver those services, and then manage the services in real time leveraging best practices for business service management, business service automation and IT service management. With the right processes, tools and virtualization technologies, and a proactive approach to management, you can improve the quality of business services and keep your infrastructure closely aligned with business goals and priorities.

### **How HP can help**

HP provides business service management and automation capabilities to give you greater insight into your virtual and physical environment and help you gain greater control from a business services perspective. We facilitate this by looking first at applications and business services. We then work virtualization into a strategic framework established with best practices for business service automation and IT Service Management. Along the way, we help you weave virtualization into IT governance, your existing policies and procedures, enabling consistency of and control over operations for virtual and physical resources alike, for all applications and business services. We do this in practical terms, with infrastructure and business service management tools that are optimized for both virtual and physical environments. In these efforts, we make use of our extensive portfolio of management software and service management services. HP Server Automation software, for example, provides a single solution for managing and automating configuration activities across heterogeneous physical and virtual servers. HP Operations Manager software, meanwhile, helps your IT staff improve its efficiency by aggregating server, storage and network performance data from physical and virtual infrastructures to detect and isolate service problems before they affect the business.

### **Rethink client architectures**

Enhance reliability, security and management with virtualization. The potential benefits of virtualization don't stop at the doors of your data centers. Client virtualization has emerged as a key way to achieve greater return on your overall client investment by improving the reliability, security, manageability and flexibility of your computing infrastructure. This occurs by replacing traditional, dispersed personal computers with centralized computing resources in your data center. End users access these resources through highly reliable thin clients with enhanced security features.