NETGEAR®
Connect with Innovation™

Whitepaper

Server Virtualization

A Game-Changer For SMB Customers

Introduction

Everyone in the IT world has heard of server virtualization, and some stunning achievements by datacenter and Enterprise customers have been trumpeted in the press. Larger companies face massive logistical and financial problems with server sprawl, power, cooling and support. Server virtualization can address these issues and also transform testing and development environments while radically changing business continuity and disaster recovery practices. But in the Small and Medium sized Business (SMB) market, where the "datacenter" may be an IT closet with a handful of servers and a collection of inherited networking components, backup arrangements and informal practices, is there a similar benefit?

Market Definition

Small Business	5-75 users
Medium Business	76-500 users

Simply put, server virtualization is the ability to run multiple concurrent operating systems on the same hardware platform. In most cases, as little as 10% of the available processing power and resources of modern hardware platforms are utilized by a single operating system or single set of applications. That's a lot of wasted investment in hardware that isn't doing anything.

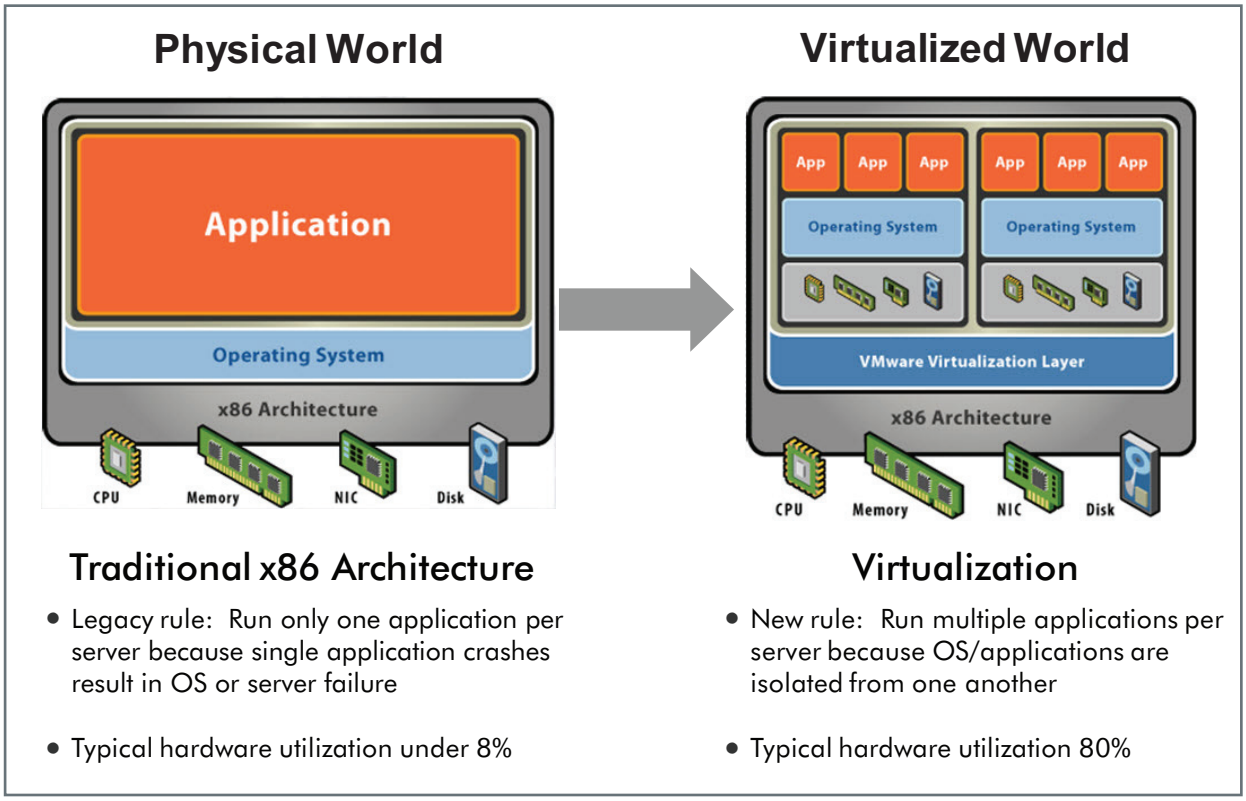

Figure 1. Virtualization Architecture

A virtual server environment lets a software package (a hypervisor) assign hardware resources to virtual machines. Broadly, instead of 5 servers each at 10% use, I now have one server with higher utilization. In addition to reducing the number of servers used, virtualization also increases flexibility. More virtual machines can be added (or removed) as needed, with no interruption and no downtime. In a nutshell, server virtualization separates the hardware from the processing power, letting administrators manage and adjust each independently.

There are five essential components for a virtualized infrastructure:

- Software (Virtualization software like VMware, Hyper-V or XenSource)
- Server hardware (a standard 1U platform like Dell, HP or IBM or a blade server)
- Storage (networked, preferably unified with both NAS and SAN capability)
- Switches (1GE or 10GE Ethernet, managed for best traffic control)
- Security (protection from external intrusion or unmitigated traffic disruptions)

Feature	Benefit
Server Consolidation	Better resource utilization, lower power usage, less cooling
Dynamic Provisioning	Greater flexibility for applications and storage
Workload Management	Improved quality of service (QoS)
Workload Isolation	Higher availability/security (if something crashes, it's isolated)
Mixed Production and Test	Try new things on the fly with no risk
Mixed OS types/releases	No more dedicated legacy servers and apps
Cheap Dedicated Servers	Make new VMs as needed, no purchasing or setup required
Separate storage and processing	Add or remove capacity and servers on demand

Table 1. Feature/Benefit Table

Software (Hypervisors)

There are three main players in the hypervisor world: VMware, Microsoft and Citrix. A hypervisor allows multiple virtual machines on the same hardware platform and provide the management interface between each virtualized operating system and the underlying CPU, memory and IO resources (like network and storage).

In an SMB environment, no-cost hypervisors with limited scalability make adoption financially painless, and future growth can be delivered through licensed feature upgrades. Advanced instances include options for planning, migration, management and control of the entire virtualized infrastructure. Third parties may offer software and hardware tools to ensure robust levels of redundancy, recovery time and granular recovery points.

It is important to note that in this case "free" does not mean "weak." Even the lowest-end hypervisor offerings are applicable for SMB customers and affordable solutions can be built to address business continuance, backup and restore, and disaster recovery challenges.

Virtual machines often revolutionize disaster recovery because they can be packaged up as files and copied offsite for simple disaster recovery, as in the sample diagram below.

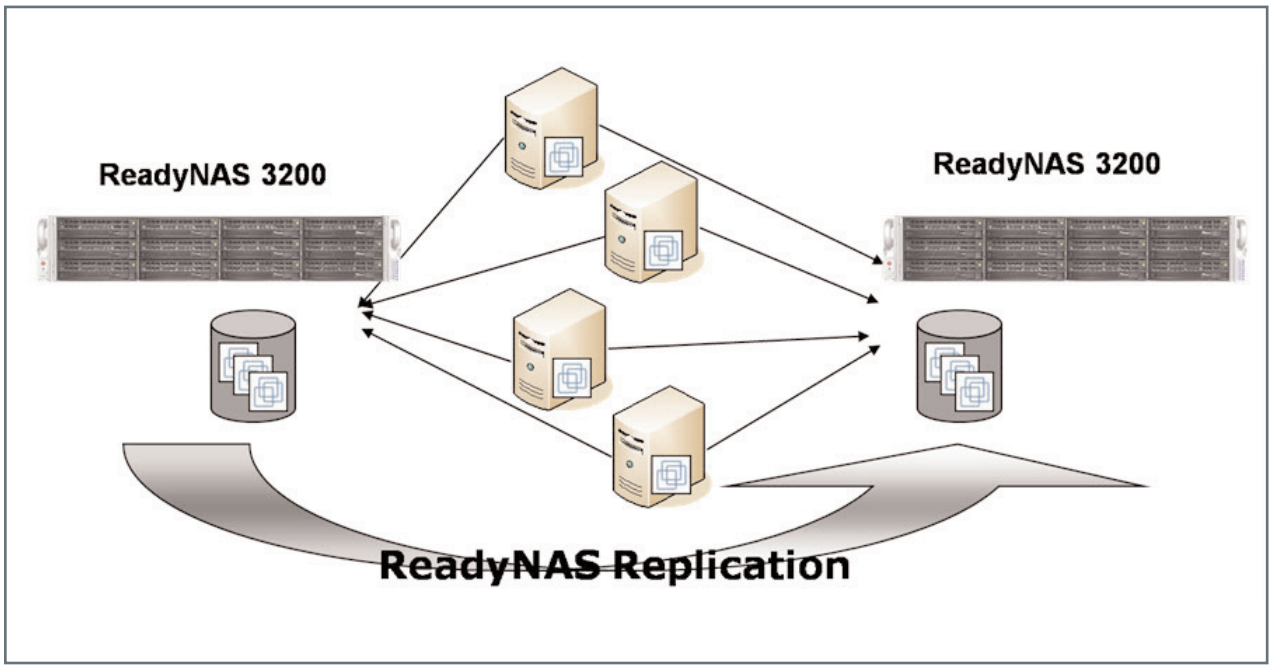

Figure 2. ReadyNAS® Replication

Vendor	VMware		Microsoft			Citrix
Product	**ESX**	**ESXi**	**Server**	**Windows Hyper-V R2**	**Hyper-V R2**	**XenServer**
Version	4	4	2.0.1	2	2	5.5
Cost	Fee-based	Free	Free	Cost of the OS version	Free	Free
Virtual Disk Format	VMDK format	VMDK format	VMDK format	VHD format	VHD format	VHD format
NFS Support	Yes	Yes	Host OS dependent	No	No	Yes
iSCSI Support	Yes	Yes	Host OS dependent	Yes	Yes	Yes
Snapshot VMs	Yes	Yes	Yes	Yes	Yes	Yes
Move VMs	VMotion	VMotion	No	Live Migration	Live Migration	XenMotion

Table 2. Product Comparisons

Most modern operating systems and applications function with a name-brand hypervisor, but if in doubt check with your application vendor. Modern hypervisor software also includes useful physical-to-virtual (P2V) tools that simplify the initial conversion tasks from physical servers to Virtual Machines (VMs).

Intelligent and affordable network storage and switch products can be used with any hypervisor to transform a small business IT environment. Let's look at the specifics of a complete solution.

Servers

Given the increasing importance of the remaining server(s), best practices include upgrading to a sturdy server hardware platform to host the new VMs. Minimum hardware recommendations or hardware certifications are available from the top hypervisor vendors. And even though hypervisors include memory management features, as a general rule the amount of physical memory installed should reflect the combined requirements of the various operating systems and applications that will be virtualized. If there were four individual servers requiring 2G of RAM each, then the virtual host server should be configured with 8GB. This will avoid memory swapping to disk and possible performance issues at a later date

Storage

The true power of virtualization is unlocked through network storage. Features like high availability (VMware HA), load balancing (Hyper-V Live Migration) and site recovery options (VMware SRM), require shared network storage. When the storage is centralized, virtual machines can connect to their own capacity and then migrate, while still running, between server platforms. Load balancing can be automated, letting operating systems move between host servers based on set policies, so the load is balanced and hardware investment is maximized - on the fly. If a virtual machine crashes, it can be simply started on another host at the touch of a button. High availability options can incorporate remote sites for disaster recovery purposes by replicating VMs to another location and using a new hardware platform to host them remotely.

A unified storage system allows the greatest flexibility. With both NAS and SAN functions in your storage, file servers can be eliminated entirely and moved directly to NAS, while application servers can be converted to VMs over your protocol of choice – NFS, iSCSI, or both. NETGEAR® ReadyNAS® unified storage systems are certified to operate with many virtualization vendors, ensuring compatibility and support.

Reliability is important but many SMBs are bound by cost realities. ReadyNAS® systems have field replaceable parts, so if dual power supplies are cost prohibitive, systems can still be recovered quickly, on site.

For a superb example of a Microsoft Hyper-V installation with offsite replication, refer to the Headlands Asset Management success story. This customer reduced physical servers by 50% while replacing older high-end storage, reducing capital, operational maintenance costs and rack space by 80%. In addition they adopted an off-site disaster recovery solution using the built-in ReadyNAS® software tools at no additional cost.

Switching

Network infrastructure is absolutely critical to a virtual environment, because no VM can function without access to network resources. Switching infrastructure on a physical external network must be fast enough to handle an increase in network traffic, reliable, powerful enough to manage traffic, QoS and security, and affordable for SMB customers. NETGEAR® ProSafe® managed switches have a lifetime warranty and provide the network infrastructure to connect to physical servers, clients, network storage and other resources with flexibility and easy management software.

- 10GE connections & Link aggregation for higher throughput/performance
- Fail over port configuration for reliability
- VLANs to help separate backup, NAS or SAN traffic
- Network traffic management for overall performance improvement

Read how NETGEAR® Provides Reliable IT Infrastructure for Public Library System.

Security

With any new technology there will always be new threats and security concerns associated with it. Virtualization is no exception. In October 2007, Gartner predicted that through 2009, 60 percent of production virtual machines (VMs) will be less secure than their physical counterparts. Below are some of the top security threats surrounding virtualization:

- Virtualization Specific Attacks
- Traditional Threats
- Management Responsibilities
- VM Sprawl
- Virtual Machine Segmentation

One aspect of the threats listed above which most organizations have more experience dealing with is traditional threats. This is a good starting point in securing a virtualized environment as many VM targeted threats still come in the network through traditional means such as spam and malformed Web pages. For years, servers and end user PCs have been attacked by a multitude of online threats.

Millions of unique malware programs are created each year. Such malware is "pulled" onto user desktops through Web pages and spam emails. Because virtual machines are essentially "real" machines but with the physical aspect of them removed, they are just as vulnerable to these attacks as their physical counterparts. Most threats do not differentiate between virtual and physical machines. Spam will hit a mail server regardless of whether or not it is a VM.

Virtual machines can get infected by executing virus code. Only this time, not only the VM itself is at risk, but also the hypervisor plus all the machines above it. Once the hypervisor itself is compromised, all is lost. All data and applications on the guest VMs are now at risk. All this time, the guest VMs are oblivious to the attack.

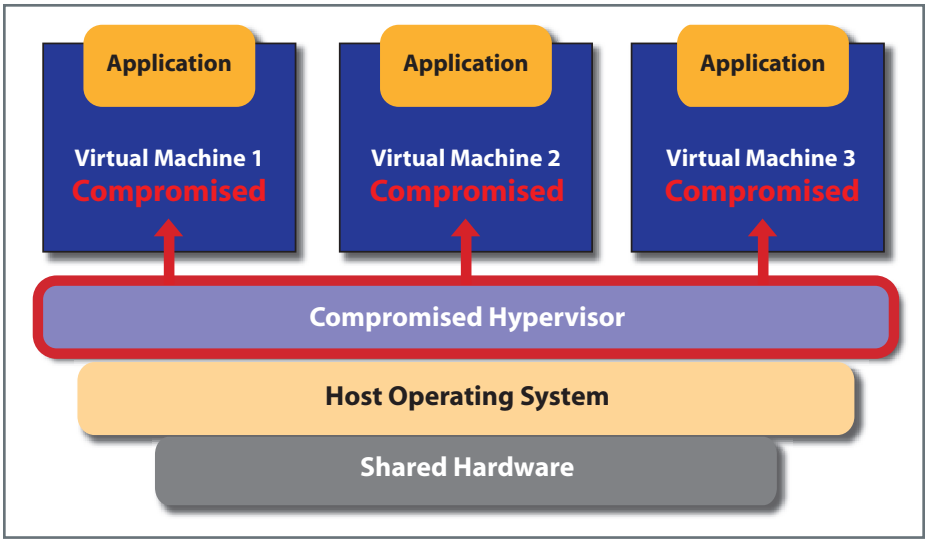

Figure 3. Compromised Hypervisor and VMs

Traditional security measures and policies must be followed through more than ever. Anti-virus software must be deployed on each VM and especially on the host system itself. Access rights need to be clearly defined for each virtual resource. Optimally, a layered gateway security solution will be deployed at the network gateway. Intrusion prevention systems can thwart non-malware based attacks such as SQL injections. Anti-spam and Web filtering will prevent users from being exposed to malware carried through Web and email. For the malware that manages to bypass these layers, gateway anti-malware scanning should detect and remove the file before it reaches server or end user machines.

Whether an environment is completely or partially shifted from physical to virtual, preserving the resources from malicious activity remains paramount. Look for products that reduce IT cycles, and cover both internal and external threats (malware, viruses, Trojans, spam and bad URLs). There's no point in simplifying your network infrastructure if it is still plagued by traditional security risks.

NETGEAR® ProSecure® security appliances protect networks from millions of security threats originating from multiple vectors, both internal and external. For a good case study, read about the retailer J Peterman and their experience with NETGEAR® switching, storage and security products.

Read how NETGEAR® ProSecure® UTM25 Offers Retailer "Uncommonly Good" Threat Protection.

Conclusion

SMBs can achieve the same virtualization results as big companies on a more appropriate scale, using products and services that are available in the right size and price point. While larger firms have traditionally created lower-end products for smaller businesses, there is an inherent conflict of interest that may doom the products to weakness or premature irrelevance. Only NETGEAR® offers the products and partnerships to provide four of the five critical components: servers, software, storage, switching and security. For more information or to contact a NETGEAR® reseller, please visit www.netgear.com

For more information or to contact a NETGEAR reseller, please visit www.netgear.com.

ReadyNAS®

PROSECURE® SECURITY ARCHITECTURE BY NETGEAR®

PROSAFE®