



WHITE PAPER

The Benefits of Virtualizing Remote and Branch Offices

Sponsored by: VMware

Gary Chen
September 2014

IDC OPINION

Remote offices and branch offices, like retail stores, bank branches, or manufacturing plants, are crucial assets in company operations and have unique infrastructure challenges. The major challenge is that these locations are geographically distributed, with few or no IT staff members available. This situation can be exacerbated by often difficult operating conditions such as unreliable wide area network (WAN) Internet connections.

Server virtualization technology can play a key role in modernizing remote office infrastructure, just as it has in the past decade for datacenters, radically improving those operations. Remote and branch offices can benefit from the agility, availability, and standardization that virtualization can provide when properly implemented.

Beyond solving typical IT operational problems, virtualization will play a key role in enabling business transformation. Today, companies must change the way they do business and interact with customers because technology is changing customer expectations. For example, a retail store may have to integrate an application like mobile checkout, offer in-store location-based services, and provide customer access through social networks. Parts of these connected, intelligent services will need to run on store premises. Thus remote and branch offices will need a flexible and fast software-based/virtual infrastructure to provision and manage these applications, which can change frequently.

SITUATION OVERVIEW

Remote office and branch office infrastructure can have unique needs compared with datacenters when organizations consider the latest IT. These satellite offices can play a significant role for many types of businesses. They are often the critical "endpoints" for a business, conducting crucial activities such as customer checkout at a retail store, financial transactions at a bank branch, or manufacturing product at a factory. The overall challenge with remote and branch offices is the physically distributed nature of these sites. In addition, many sites may have few or no IT staff members present. Further, environmentally harsh and chaotic operating conditions may exist at remote sites, particularly for manufacturing and other industrial-oriented operations. Other IT departments may have the same challenges with branches as they do with a centralized datacenter but must solve these challenges in a very different environment because of staffing and resource availability.

Some of the issues IT staff must deal with are:

- **Availability:** IT services must be made highly available at each location, as downtime even in one location can impact a business' top and bottom lines. Yet high availability can be a challenge for remote offices and branch offices. From a location standpoint, many remote sites don't have the controlled physical facilities of a traditional datacenter. Unlike a traditional datacenter, many remote offices house their server equipment in small backrooms and closets where heat and humidity, and potentially dust, dirt, or other contaminants, are constant concerns. From a systems point of view, high availability has traditionally involved expensive and complex hardware and software, making it difficult to justify and apply to a broad set of workloads. Even with the proper hardware and software, remote and branch offices are highly dependent on the WAN connection, creating a single point of failure. Further, if a centralized server were to go down, the impact would be magnified (e.g., if hundreds of stores in a retail chain all relied on that one server). Thus sites will run certain workloads on-premises so that those workloads can run independently, allowing key activities to continue, such as retail stores selling goods, manufacturing plants making products, or hospitals administering patients.
- **Regulatory/corporate policy compliance and security:** All enterprises deal with security as a major threat. While datacenters have always been natural targets, remote and branch offices are important targets as well that must be protected. In fact, many hackers have found sites such as retail stores to be "soft targets" with attractive rewards, as witnessed by the recent spate of point-of-sale hacks in several large store chains. Further, many industries now must comply with a variety of stringent regulatory rules regarding IT operations and security, such as PCI for merchants dealing with credit cards and HIPAA for the privacy of medical records. Implementing defensive measures like intrusion prevention systems and antimalware tools is one aspect of compliance, which has many dimensions. Proper configuration management is essential in maintaining secure, consistent, and compliant configurations over time.
- **Data protection:** In today's digital world, data is being created at an enormous rate. It's also something unique and critical to a company, something that can never be recreated once lost. Much of the digital data today is generated at remote sites, such as customer accounts at a bank branch or patient records at a doctor's office. Sometimes, this data is part of a centralized system, but with independent systems, the data could be stored locally during the day's operations and then replicated to a central location each night.

How Virtualization Can Address Remote Office and Branch Office Challenges

According to IDC's Server Virtualization Tracker, the overall industry average of virtual machine (VM) density today is about 10 VMs per server. At the high end, datacenters are running 20-30+ VMs per server. On the low end of the average, such as small and medium-sized businesses (SMBs) and remote offices and branch offices, it's common to see only 5-7 VMs per server.

Many remote and branch office sites have only a couple of low-end tower form factor servers with one to two CPUs and internal direct-attached disks. More advanced sites could have a small networked storage appliance or RAID setup, and most will be connected by a perhaps unreliable WAN connection. Unlike servers in most datacenters, these servers often run in less-than-optimal conditions, such as a backroom IT closet. For example, with manufacturing companies, servers could potentially be located out on the plant floor – harsh conditions for computer electronics.

Virtualization has become standard in the datacenter, with 30% of new server shipments being virtualized today, according to IDC. However, remote and branch offices can be overlooked when organizations embark on virtualization projects. Granted, many remote and branch offices have very modest server footprints, so consolidation would not be a major benefit. However, consolidation is not to be overlooked in a company that has a very large number of sites, such as a large retail chain, as the savings can add up quickly. But even in the datacenter, virtualization's benefits have progressed well beyond consolidation. The improved operations will benefit remote and branch offices the most. Virtualization significantly improves the overall deployment and management of systems and also makes infrastructure services such as availability and networking more robust. IDC data shows that virtual machines are much more likely to have advanced infrastructure services attached to them because of the greater ease and cost efficiency of implementing these services in the virtual domain.

Virtualization can address IT concerns at remote and branch offices in the following ways:

- **Availability:** A certain level of availability is inherent with VMs. With the hardware abstracted from the software and VMs stored as a file, virtual servers can be easily moved to and booted on any spare server with a hypervisor. In the physical world, differences in hardware, drivers, and image portability make this much more difficult. Further, having standby capacity is much more economical as physical servers don't have to be dedicated for it. Moreover, virtualization software can offer advanced tools and automation to improve high availability further by detecting failures and automatically restarting VMs on a different server. Advanced tools also allow VMs to be moved while running, allowing servers to be evacuated for maintenance and restored again as workloads run uninterrupted. Since all this happens in the virtual domain and is software controlled, it can be done remotely without physical access to the systems.
- **Configuration management:** Centralized management consoles are standard for VM deployments, and virtualization software provides tools to help manage configurations for better compliance and security. The management software allows standardized configurations for both the hypervisor host and the guest virtual machines. Hypervisor host configurations can be set and then pushed down to remote bare metal servers. VMs are installed through "golden master" templates, ensuring that the same image is used each time for consistent VM configurations. Then, monitoring tools in the console can monitor configurations over time and alert administrators if something changes. VM snapshots can be used to roll back VMs to prior states in the case of unexpected configuration changes or even security breaches and data corruption.
- **Data protection:** While backups can be done in the traditional way, through the OS on virtualized servers, virtualization can also offer an easier way to do backups by centralizing them through the hypervisor. Since the hypervisor controls the execution of VMs, it can also access the VM data, allowing it to back up VMs without any guest VM having to be configured with an agent. An agent may be used, however, to add additional functionality like application-aware backups. The ability to snapshot live VMs also allows for nondisruptive and consistent backups.
- **Network isolation:** Software-based virtual network switches are embedded in hypervisors to allow VM networking, which can be leveraged to let administrators easily create multiple isolated networks. This is often a prerequisite in many regulated environments to enhance security. Configuring multiple isolated networks is much easier using virtual networks compared with isolating physical networks. Also, virtual networks are easier to reconfigure dynamically than traditional physical networks.

VMWARE PROFILE

VMware has released new editions of vSphere (vSphere Remote Office Branch Office Standard and Advanced editions) specifically designed for the remote and branch office customer. These editions offer features, pricing, and licensing tailored for the remote office and branch office market. The product is licensed per VM, and vCenter Server must be purchased separately. vSphere Remote Office Branch Office Standard edition includes virtualization features such as:

- **vMotion:** Allows VMs to be migrated to a different physical server while running, eliminating application downtime from planned server maintenance
- **High availability:** Automatically restarts VMs on a different server in the event of an unplanned server failure
- **Data protection:** Backup for VMs delivered as a virtual appliance (It can restore directly to a host without dependence on vCenter Server and quiesce the VDP appliance for long-term retention purposes.)
- **Replication:** Replicates VMs continuously to a second copy, delivering multiple point-in-time snapshots for more granular recovery
- **Fault tolerance:** A higher level of availability, allowing a VM to keep running in the event of failure, without having to restart it (Two VMs running on different servers are kept in continuous sync, and if one dies, the other picks up immediately and transparently.)
- **Storage vMotion:** Live migrates VM disk files across storage arrays, allowing storage maintenance or migration with no downtime

The Advanced edition also includes:

- **Distributed switch:** The distributed switch is a virtual network switch that logically encompasses multiple vSphere servers. It allows easier network configuration and management while also providing advanced network features that remote offices and branch offices need, such as the ability to segregate in-scope and out-of-scope workloads on the same physical box and enhanced network monitoring for regulatory compliance.
- **Host Profiles and Auto Deploy:** Host Profiles helps manage the configuration of vSphere hosts by capturing host-level configuration settings and saving them as a template to configure other vSphere hosts. It also monitors hosts for configuration changes and alerts administrators if deviations are found. When firmware upgrades or other events that require storage, network, or security configuration changes on multiple hosts in a cluster occur, administrators can edit the host profile and apply it across the cluster for consistent configuration updates. Auto Deploy can automate the deployment of vSphere software to physical hosts.

FUTURE OUTLOOK

The entire IT industry is being impacted by a new style of IT. This includes new application architectures and development methods, hardware advances like converged infrastructure, and cloud-style delivery of services. Remote and branch offices will also be affected by these changes:

- **New applications:** As businesses take on more modern applications to adapt to a more technologically oriented customer, the architecture and development of these applications are also changing. Applications are increasingly built in an agile style, where apps are deployed much faster and more often in a continuous manner to accommodate the rapidly changing needs of business. These applications assume an agile virtualized or cloud infrastructure that can handle a high rate of change. This virtualized or cloud infrastructure is becoming increasingly important as customers interact directly with these applications, for example, in a store or a bank branch.
- **Converged infrastructure:** Today, remote and branch office hardware is a disjointed collection of servers, storage appliances, and networking infrastructure. Converged infrastructure integrates servers, storage, and networking into a single highly optimized appliance. As a result, remote and branch office administrators have fewer endpoints to manage and are able to manage the entire infrastructure through a single interface. Further, many of these converged infrastructure devices have a low-power and small footprint design, which fits in well with typical remote and branch office physical environments.
- **Cloud:** The largest overall change in IT today is the impact of cloud. Remote and branch offices will be impacted by cloud in several ways. First, workloads may be moved off-premises and into a public or private cloud. However, there are many challenges in doing so, which are discussed in the section that follows. Second, the infrastructure at the remote or branch office itself may become a "mini" private cloud (as a logical extension of the datacenter private cloud) as this infrastructure is virtualized and put under the control of a cloud system.

Will Workloads Move from Remote/Branch Offices and into the Cloud?

The cloud has already made a huge impact on IT and datacenters, and many customers will be examining its usefulness for remote and branch offices. The most futuristic scenario is a "zero footprint" setup, where everything is run in the cloud, with nothing to manage at the remote site. This would obviously centralize infrastructure and eliminate the challenges of managing a distributed environment, which is certainly appealing. However, IDC believes that many workloads will still need to be run on remote and branch office premises for a variety of reasons.

The primary challenges to using remote cloud services at a remote or branch office site are the speed, latency, and reliability of the WAN connection upon which external cloud services rely heavily. The WAN becomes a choke point and a single point of failure. While buying better WAN services would certainly help, that is not always an option. Many sites, like retail store locations or manufacturing plants, are in areas with average to poor Internet service, with few options for improved service. Many remote offices and branch offices today don't have redundant WAN connections, and WAN redundancy can be deceiving. While the network connection to the remote site itself may have multiple redundant paths, locality and provider monopolies often funnel these connections to the same network back end, which still leads to a single network dependency.

While noncritical workloads, such as those run perhaps just once a day or once a week, could be run in the cloud, other critical applications that are run continuously would not be a good fit. Many applications

designed to run on the LAN would encounter numerous problems running over the WAN. Take, for example, a manufacturing control system at a plant. It makes more sense to run the control system next to the devices being controlled. Running a control system remotely would be quite risky because any WAN disruption would halt factory production. Further, the latency, even on a good WAN connection, introduces performance problems and also exposes the system to security risks by going over the Internet. There is no benefit in running this type of system remotely. Another similar example is a retail point-of-sale system in a store. A lot of burden would be put on the network if the back-end system was remote, with every transaction requiring a lengthy WAN round-trip. Such systems are normally run locally, with some noncritical parts of the application connecting back to the datacenter or a cloud, but are still able to run independently to allow the store to function autonomously.

In some scenarios, like a corporate branch office with information workers, there may be workloads that could be more effectively centralized, particularly considering the mobility trends already transforming user behavior. Information workers tend to have viable options to reestablish connectivity should their primary network access point become unavailable for any reason.

The best approach is to examine each workload for its appropriateness for cloud given its specific requirements and the available remote site infrastructure and WAN. IDC believes some existing remote and branch office workloads could be pushed out to a public or private cloud, but the majority will continue to run locally for the foreseeable future because of the previously discussed reasons of availability, security, and performance.

CHALLENGES/OPPORTUNITIES

Challenges

- **Remote and branch office infrastructure life cycle:** Remote and branch office infrastructure often has lengthy life cycles. Virtualization has compelling benefits, but implementing virtualization may require much more than simply purchasing software licenses. It will likely require significant planning and investment from customers.
- **Hypervisor competition:** VMware's competitors have improved over time and may offer virtualization alternatives while also targeting the remote office/branch office market.

Opportunities

- **Targeting remote and branch offices:** The remote and branch office market is often overlooked for virtualization, and creating specific editions and tailored pricing and licensing may help VMware gain traction in this market versus competitors that don't have remote and branch office editions.
- **XP and Windows Server 2003 end of life:** Support for XP ended this year, and Windows Server 2003 end of life is slated for 2015. These platforms are popular in remote and branch offices, and their end will likely trigger a refresh cycle that can cause administrators to consider other infrastructure changes like virtualization.
- **Business transformation:** As businesses deal with a rapidly changing environment, with pressures to engage in areas such as mobile applications, social media, and the Internet of Things (IoT), companies will be driven to (re)build infrastructure that is more agile and responsive to accommodate new applications required to support the business. Virtualization and cloud are key enablers of business agility.

CONCLUSION

Remote offices and branch offices are undergoing a transformation similar to that of datacenters. The increased pressure on all areas of business, from datacenters to remote and branch offices, is driving the adoption of technologies like virtualization that can increase agility.

VMware, an established virtualization vendor in the datacenter, is recognizing the need for virtualization beyond the datacenter and into scenarios like remote and branch offices. As small extensions of large enterprises, remote and branch offices have unique needs, and VMware has created products with remote and branch office-specific feature sets and pricing/licensing to address these needs. As enterprises look to further expand their virtualization footprints to remote sites, VMware's vSphere Remote Office Branch Office editions deserve consideration.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data – Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2014 IDC. Reproduction without written permission is completely forbidden.

