

WHITE PAPER

Simplifying Remote and Branch Office Management with VMware



Contents

- Introduction..... 1**
- Remote and Branch Offices Present Unique IT Challenges..... 1**
- Extending Virtualization Beyond the Data Center.....2**
- Why Choose VMware For Remote and Branch Offices?2**
 - VMware Infrastructure 3 Simplifies IT Management.....2
 - VMware Infrastructure 3 Ensures Business Continuity.....4
 - VMware Infrastructure 3 Reduces Costs5
- Deployment Approaches6**
 - Centralized Deployment.....7
 - Distributed Deployment9
 - Option 1: Manual Failover Using Replication at the Remote Office 10
 - Option 2: Automatic Failover Using VMware HA at the Remote Office 12
 - Option 3: Load-Balanced using VMware VMotion and DRS at the Remote Office..... 13
 - Loss of WAN Connectivity in Distributed Deployments 15
- Conclusion 15**
- Additional Resources 16**
- Appendix: Third-Party Components..... 17**
 - Optimizing Network Performance with WAN Acceleration..... 17
 - Leveraging Replication Software for Manual Failover and Disaster Recovery 18
 - Improving Data Protection with Centralized Backup..... 19
 - Cost-Effective Alternatives to Physical Shared Storage.....20

Introduction

Virtualization is rapidly transforming the way organizations manage their remote and branch office IT infrastructures. Physical servers and desktops residing outside the data center have traditionally been hard to manage, difficult to protect and costly to maintain. By extending virtualization beyond the data center, organizations gain increased visibility and control over IT resources in remote locations. They can also rapidly deploy new servers and desktops in the form of virtual machines in minutes and scale to the growing needs of their remote and branch offices in a cost-effective manner.

VMware virtualization solutions deliver significant benefits for remote and branch office management, including:

- Streamlined management and rapid provisioning.
- Improved service levels and availability.
- Lowered IT hardware and operational costs.

Remote and Branch Offices Present Unique IT Challenges

Today's IT infrastructure is increasingly distributed and difficult to manage. Many critical business applications now reside outside the data center in places such as retail stores, bank branches, manufacturing plants, medical clinics and warehouses. Because these locations are connected by a corporate network to a central data center, they are commonly known as remote or branch offices¹. Physical servers and desktops residing in remote and branch offices are often hard to manage, difficult to protect and costly to maintain for a variety of reasons, including:

- **Lack of onsite IT expertise:** Often, remote and branch offices do not have enough servers or desktops to justify hiring an onsite IT administrator. They must rely on centralized IT support or expensive third-party support contracts. The need for support personnel to troubleshoot remote servers and desktops in person not only extends service downtime but also drives significant support costs. In cases of new workload requests or new employee additions, administrators must provision servers and desktops at headquarters, and then ship them to the remote office. This process leads to lengthy turnaround times and high costs. Lack of onsite IT staff also means that the task of managing backups and rotating tapes falls upon non-technical office personnel. Although tape backups are affordable, they are error-prone, susceptible to theft or loss, and labor-intensive to maintain, making them less than ideal for remote offices with minimal staff.
- **Lack of standardization:** The distributed nature of remote offices makes it difficult for IT organizations to enforce consistent deployments across all sites. The lack of standardization also makes it difficult for IT staff to meet demand for new applications, support legacy applications, and perform routine upgrades and maintenance in the remote offices. Without a standardized hardware platform, it can be costly and difficult to provide a disaster recovery strategy for the remote office environments.

¹ The terms "remote office", "branch office", and "remote site" are used interchangeably throughout this whitepaper to refer to any location connected by a corporate network to a central data center. These include, but are not limited to: retail stores, bank branches, manufacturing plants, medical clinics, warehouses, distribution centers, call centers, embassies, hotels, restaurants, etc

- **Limited space and IT budget:** Remote offices are rapidly running out of space to accommodate new workloads, and existing physical servers at these sites are not efficiently utilized. Limited space and budget make it prohibitive to invest in redundant hardware components and specialized business continuity solutions. As a result, single points of failure create the risk for significant service downtime. Protecting a remote office from site failure has typically required duplicating remote office infrastructure in the data center and has therefore been cost and space prohibitive for most organizations.

Extending Virtualization Beyond the Data Center

Remote and branch offices have under-utilized servers that are ideal for virtualization and consolidation. By abstracting the operating system from the hardware on which it's running, VMware® Infrastructure 3 allows remote offices to collapse standard office IT infrastructure (e.g. email, file, print, proxy and firewall servers) into a single virtualized environment for easier management and protection. Standardization upon a virtual platform allows organizations to meet new business needs in remote offices without purchasing additional hardware or hiring more IT staff, thereby reducing the total cost of ownership.

VMware Infrastructure 3 provides a set of capabilities that make remote IT environments more serviceable, available and efficient than physical hardware alone. IT administrators can leverage the remote management capabilities in VMware® VirtualCenter to monitor and maintain high levels of service across multiple remote and branch offices – all from a central point of view. VMware® High Availability (HA) brings easy, automated failover to the remote office environment, while VMware® vMotion and VMware® Dynamic Resource Scheduler (DRS) eliminates planned downtime in these locations. By using VMware® Update Manager to automate patch management, IT administrators can protect remote offices against security vulnerabilities and reduce the management complexity associated with patching remote servers.

IT departments can add a higher degree of security and control by using VMware® Virtual Desktop Infrastructure (VDI) to host complete desktop environments for remote office users in virtual machines. In addition, this simplifies and streamlines desktop management, reducing costs while providing end users access to their personalized desktops anywhere, anytime, using any device.

Why Choose VMware For Remote and Branch Offices?

VMware Infrastructure provides a proven remote and branch office management solution used by organizations of all types and sizes worldwide. Customers who have used VMware virtualization solutions in their remote and branch offices have realized the following benefits.

VMware Infrastructure 3 Simplifies IT Management

A virtual infrastructure simplifies IT management in a number of ways:

- **Standardized deployment:** By removing the dependency between hardware and software, virtualization allows IT administrators to deploy hardware-independent virtual machines from templates, without worrying about disparate hardware in remote offices. As a result, all remote office servers and desktops are guaranteed to match the current best practice for security and configuration. Establishing a standardized deployment platform across all remote and branch office environments simplifies troubleshooting,

patch management, hardware refresh cycles, upgrades, migrations and legacy operating system support.

- **Centralized management:** VMware VirtualCenter offers centralized management capabilities that allow administrators to organize, monitor and configure the entire IT environment through a single interface. By using VMware VirtualCenter to manage distributed resources in remote offices, central IT staff can minimize setup and support trips to the remote office. Servers and desktops can be upgraded, patched and backed-up from a single central location, increasing the success rates while reducing IT maintenance and support costs.
- **Rapid provisioning:** VMware Infrastructure 3 enables central IT staff to manage more workloads and scale for future business growth because it simplifies labor and resource intensive IT operations. Central IT staff can instantly provision and deploy new applications and desktops in the form of virtual machines to meet new remote office needs, without requiring additional hardware. Virtual machines can also be built and distributed as plug-and-play virtual appliances for rapid deployment to remote offices. Not only does this decrease the time it takes remote offices to get software up and running, but it also decreases potential support issues related to incorrectly configured software or hardware.

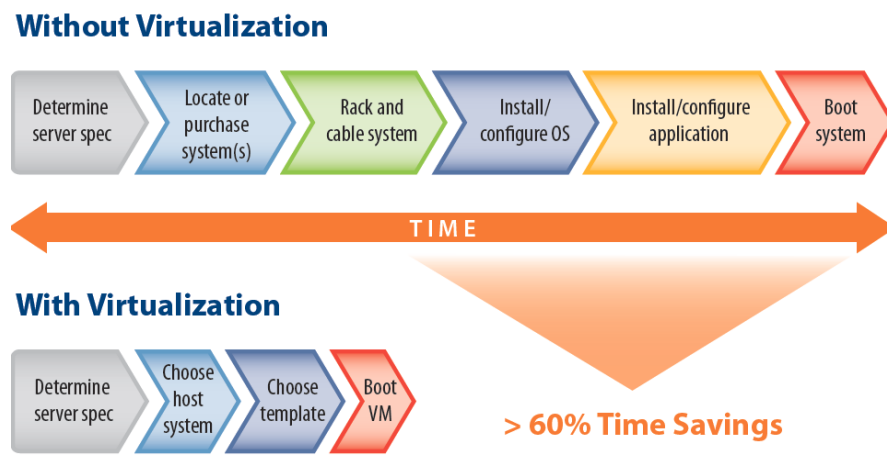


Figure 1. Virtualization accelerates the server provisioning process by as much as 60 percent.

- **Server consolidation:** Consolidating existing workloads onto fewer physical servers improves utilization of existing IT assets, contains server sprawl, and allows room for future growth. Administrators can easily add new workloads to existing servers as virtual machines, without consuming additional physical hardware space in the remote office.
- **Simplified IT operations:** Because VMware® ESX Server 3i is integrated directly into server hardware, remote offices can move from booting a server to running virtual machines in a matter of minutes. The automatic configuration capability in ESX Server 3i simplifies IT operations and eliminates the need to have special IT skills at the remote site for installing and configuring new systems.

VMware Infrastructure 3 Ensures Business Continuity

Businesses can improve service continuity by eliminating downtime and accelerating system recovery:

- **Improved service and availability:** Limited IT staff in remote offices need solutions that do not require manual intervention or frequent testing. When hardware fails at a remote site, VMware HA technology can rapidly recover and restart virtual machines on a secondary server, thereby reducing the amount of unplanned downtime at the remote site. Consolidating servers in space-constrained remote offices also reduces the chance of systems overheating and lowers the likelihood of a component failing.
- **Reliable disaster recovery:** VMware Infrastructure 3 encapsulates a complete system into a small set of files to make it easy to replicate and backup entire virtual machines from remote offices to the data center. Unlike a physical environment, a virtualized remote office does not need to duplicate remote office infrastructure in the data center for disaster recovery; it only needs the capacity to host virtual machines and a recent copy of those virtual machines.

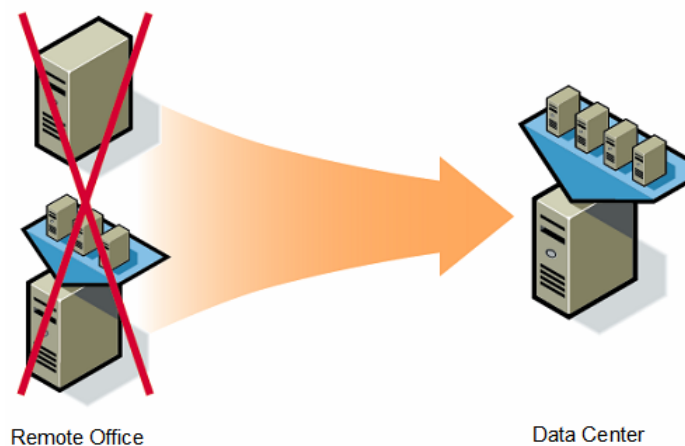


Figure 2. A virtual infrastructure enables recovery of physical and virtual machines in the remote office to virtual machines on any hardware in the data center.

- **Improved end user Service Level Agreements:** Using a VDI solution for desktops ensures continuous availability of end-user personalized desktops. VMware Infrastructure 3, which runs the virtual desktops for remote users, makes it possible to eliminate planned downtime for upgrades and patches because desktops all run on server hardware that can be moved instantly from one server to the other, without service interruption for the desktop end user. Additionally, it enables end users in remote offices to access their personalized desktops anywhere, anytime, from multiple devices.

VMware Infrastructure 3 Reduces Costs

Virtualization leads to reduced costs in a number of areas:

- **Reduced hardware costs:** Because new applications can be added as virtual machines to the remote office without requiring additional hardware, organizations can lower hardware costs upfront and when adding new workloads.
- **Reduced operating costs:** Consolidated workloads and better hardware utilization in the remote office let organizations reduce cooling, energy and real estate costs significantly in remote IT environments.
- **Reduced administration costs:** VMware HA automatically restarts virtual machines when hardware fails, eliminating the need for costly support visits or third-party support contracts. By centralizing and automating key server management tasks (such as server provisioning, patch management, etc.), and automatically load balancing between systems with VirtualCenter, organizations have realized significant productivity gains. It reduces the number of administrators required and frees staff to focus on other important IT initiatives.

Deployment Approaches

Depending on business needs and network reliability, physical servers running VMware Infrastructure 3 can be deployed centrally in a data center or locally in the remote office.

- Centralized deployment:** In a centralized deployment, VMware Infrastructure 3 consolidates remote office IT infrastructure onto a virtual platform *in the data center*, and remote offices access server and desktop workloads over a secure network connection. This option is ideal for organizations with reliable, high-bandwidth, low-latency network links, or organizations who have implemented a wide-area data services solution for application acceleration across the Wide Area Network (WAN).
- Distributed deployment:** In a distributed deployment, VMware Infrastructure 3 consolidates remote office IT infrastructure onto a virtual platform *in the remote office*, and a central IT staff manages server and desktop workloads remotely from the data center. This option is ideal for organizations with unreliable network links, or organizations that require physical servers to be located close to the end-user.

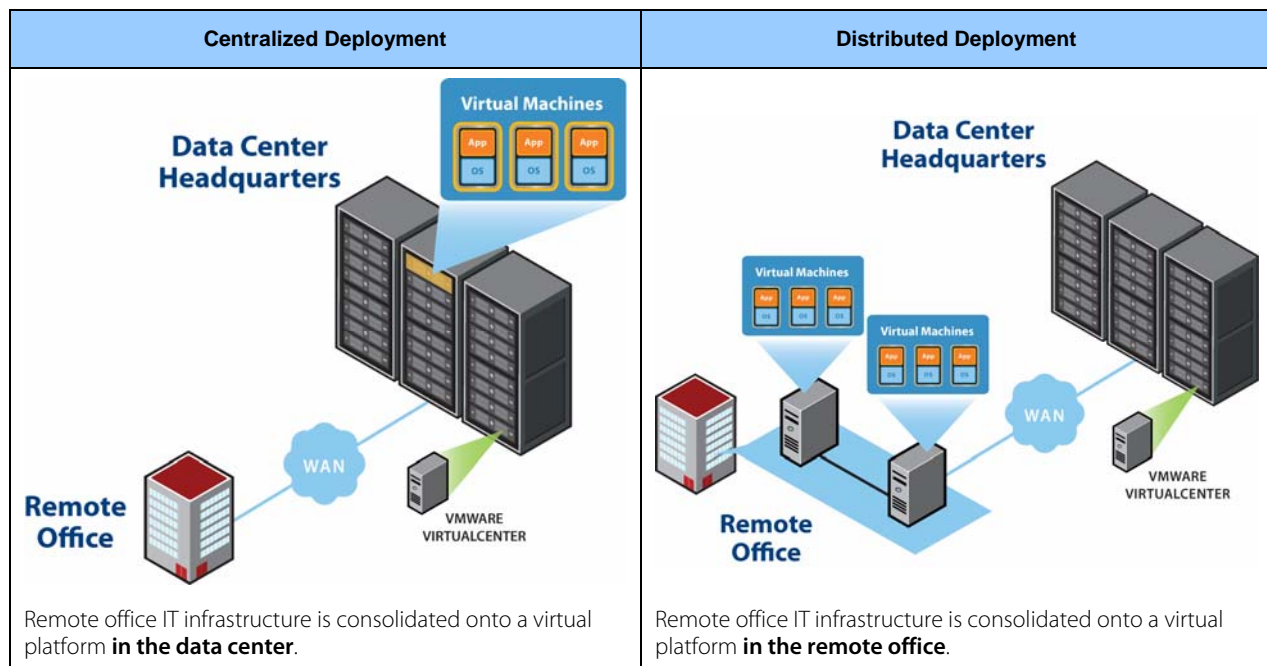


Figure 3. Deployment approaches for a virtual infrastructure include centralized and distributed deployment scenarios.

Centralized Deployment

Organizations with reliable, high-bandwidth, low-latency network links to remote offices, or organizations who have implemented a wide-area data services solution for application acceleration across the WAN, can manage and standardize server and desktop environments in the corporate data center, where administrators can perform backups, upgrades and complete maintenance. Administrators can pull servers and desktops out of the remote office, convert them into virtual machines using VMware® Converter and host them on the virtual infrastructure behind a secure firewall in the data center. End users in remote offices can then access server and desktop workloads over the network. Administrators can enforce strict control over access to virtual machines by delegating customizable roles and permissions to authorized administrators and end users.

A centralized approach to deployment maximizes consolidation ratios, ensures security and minimizes management complexity. Because the remote office IT infrastructure is located in the data center, IT staff with technical expertise can offer more responsive and better support to end-users in remote locations. Additionally, remote office services can leverage data center resources, including high-end servers, storage and networking, as well as existing data center disaster recovery and backup plans. Centralized deployment not only enhances security and compliance, but local backups can be performed in the data center at LAN speeds.

Since end users must access workloads over the WAN, a centralized deployment will increase network traffic between the remote site and the data center. Application performance will depend on application type, network bandwidth and distance between the site and the data center. Wide-area data services solutions or WAN acceleration products can help alleviate performance issues.

Typical architecture components

The components of a typical centralized deployment scenario include:

- **VMware Infrastructure 3 Enterprise (in the data center):** Provides virtual infrastructure for server consolidation and standardization.
- **Thin clients or PCs (in the remote office):** Provides desktop virtualization, if desired.
- **Remote client software (in the remote office):** Provides desktop virtualization, if desired.
- **Third-party WAN acceleration:** Optimizes network performance (see Appendix for additional details).

Customer case study: Greenebaum Doll & McDonald, PLLC

Greenebaum Doll & McDonald is a US-based business law firm with approximately 200 legal professionals. The law firm has branch offices in Kentucky, Ohio, Tennessee and the District of Columbia, each with multiple servers and highly confidential data. By consolidating branch office servers with VMware Infrastructure 3 into its data center, the company eliminated two-thirds of its physical branch office servers and increased data security. Using Steelhead™ appliances from Riverbed, the law firm accelerated disaster recovery traffic and increased its network capacity 2.5x, on average. File transfers that once took six hours now take 20 minutes. "To make it even better," said Mandi Turner, director of IT at Greenebaum, Doll & McDonald, "we still get the daily benefits of improved performance at our branch offices for our attorneys and other professionals."

Many organizations have deployed a **virtual desktop infrastructure** solution to move sensitive data normally stored on a remote office PC **into the corporate data center** to maintain data integrity and meet regulatory compliance requirements (e.g. HIPAA, Sarbanes-Oxley, and Gramm-Leach-Bliley). VMware VDI is ideal for offsite facilities used for development, call centers, back order processing or other transaction-based tasks that require confidential information and intellectual property to be stored and maintained securely in the corporate data center.

Customer case study: IntelliRisk Management Corporation

IntelliRisk Management Corporation (IRMC) performs collections and accounts receivable for all major banks and credit cards in the United States. Desktop tasks were time-consuming and inflexible, making it time-intensive to add desktops for new customers. Using VMware Infrastructure 3, users have remote access over RDP to virtual desktops residing on hosted ESX servers in a central data center. With desktop systems hosted and running on reliable thin clients, administrators benefit from simplified desktop management and administration as well as the flexibility to respond to the business needs. New desktop PCs can be set up in just eight minutes, and administrators can modify call center setup and add and change users more readily, because the desktops now reside in hardware-independent virtual machines. IT staff that previously had to provide support on location can manage remote sites from the data center, further reducing costs. It is quicker and easier to upgrade and manage the desktop images from a central location.

Distributed Deployment

While most organizations would prefer to centralize their IT infrastructures, network reliability or functionality requirements may prohibit some from doing so. By deploying VMware Infrastructure 3 in the remote office, organizations can maintain a local IT infrastructure and manage it from the central data center. By hosting virtual machines locally in the office, the remote office can continue business operations, even if network connectivity to the data center is lost. Desktop virtualization can also be added locally if the virtualized servers and storage possess enough processing capacity for the desktop workloads.

Virtualizing workloads at the remote site offers optimal application performance and responsiveness. Although technical expertise will remain geographically distant from the remote office IT infrastructure, central IT staff will be able to leverage VMware VirtualCenter for automating server maintenance tasks and monitoring resources. These remote management capabilities minimize the need to troubleshoot remote servers and desktops in person.

Depending on the criticality of the applications being used, different remote office environments will require different levels of availability. The following design approaches demonstrate how to achieve the desired level of availability in each remote site.

	Option 1: Manual Failover	Option 2: Automatic Failover	Option 3: Load-Balanced
Availability	Manual Failover (leveraging Third-Party Replication Software)	Automatic Failover (leveraging VMware High Availability)	
Resource Management			VMware DRS, Storage VMotion, VMotion
Software	VI3 Foundation + Third-Party Replication	VI3 Standard	VI3 Enterprise
Hardware	Two physical servers + Internal Storage	Two physical servers + Shared Storage	Two or more physical servers + Shared Storage

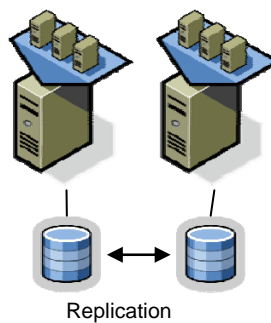
Table 1. Distributed Deployment Options

Option 1: Manual Failover Using Replication at the Remote Office

Ideal for: Budget and space-constrained environments.

Solution overview: A remote office can attain the basic benefits of virtualization at a low cost by consolidating existing servers down to one or two physical servers running VMware Infrastructure 3 Foundation. By replicating virtual machines between the two VMware ESX Server hosts, the remote office can achieve manual failover if either server fails. By using internal storage, the remote office avoids the costs and challenges associated with managing shared storage at a remote office.

Note: Alternatively, organizations can choose to invest in shared storage or a virtual storage appliance to avoid the time lag associated with using replication between the two servers.



Typical Architecture Components:

- **VMware Infrastructure 3 Foundation**
 - **VMware ESX Server:** Installed in the remote office to partition servers.
 - **VMware VirtualCenter:** Runs in the data center and connects over the network to distributed hosts for centralized management.
- **Two physical servers with internal storage:** Installed in the remote office.
- **Third-party replication:** Occurs between physical servers in the remote office (see Appendix for details on third-party replication).

Note: For remote offices that choose to deploy only one server at the remote site, administrators can use asynchronous replication (host or guest-based) or centralized backup between the remote server and the data center to ensure application availability and disaster recovery. If a server fails or a disaster occurs, applications can be served from the datacenter over the WAN, allowing the remote office to continue operating with minimal disruption. Again, the use of wide-area data services or WAN acceleration can help by ensuring that recovery time is as short as possible among sites.

Customer case study: Kennedys Law

Kennedys Law is one of the leading dispute resolution law firms in London. They have offices in Spain, Dubai, Hong Kong and New Zealand and associated offices in the rest of the world. When the company needed to set up a new office IT infrastructure overseas in Sydney, Australia, they turned to VMware for a solution to significantly cut down the installation time.

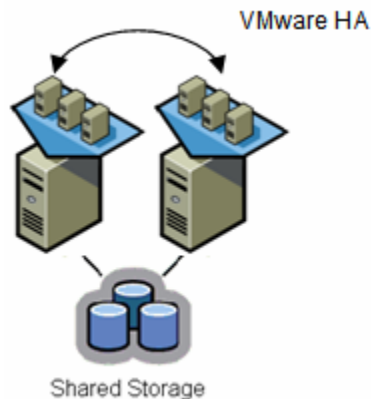
Setting up the specialist applications used in the legal environment would have been time-consuming, and resources to support the roll-out were limited. "By using virtual machines and VMware we were able to get this built locally and far quicker than if we were relying on physical hardware," Taking the virtual approach has meant that we saved about 50 percent of the overall project costs, as well." Using VMware, experienced staff at the head office built virtualized servers in the UK and shipped them to Australia, where the installation," said Ian Lauwerys, IT Director at Kennedys Law. The process was completed by a local partner. Using virtual machines ensures that there is no downtime for applications, even in the event of a physical hardware failure. The Sydney office is now equipped to support over 75 staff members.²

² Read more about Kennedys Law's branch office deployment at http://www.vmware.com/files/pdf/customers/ss_kennedys_1007.pdf

Option 2: Automatic Failover Using VMware HA at the Remote Office

Ideal for: Environments needing automatic failover (<2 minutes of downtime).

Solution overview: Adding shared storage allows a remote office to leverage the automatic failover capabilities in VMware Infrastructure 3 Standard. By using two physical servers running VMware Infrastructure 3 Standard connected to shared storage, a remote office can use VMware HA to monitor and automatically restart virtual machines on the secondary server if one server fails. Having redundant host-bus adapters, dual power supplies, redundant fan kits and multiple network interface cards further minimizes potential points of failure.



Typical architecture components:

- **VMware Infrastructure Standard**
 - **VMware ESX Server:** Installed in the remote office to partition servers.
 - **VMware VirtualCenter:** Runs in the data center and connects over the network to distributed hosts for centralized management.
 - **VMware HA:** Used in the remote office to automatically restart virtual machines on a secondary server in cases of a hardware failure.
- **Two physical servers with shared storage:** Installed in the remote office.

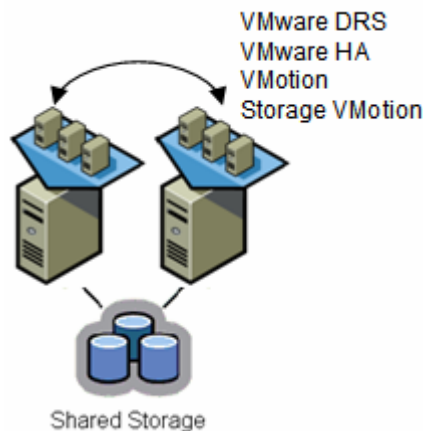
Customer case study: Global Pharmaceutical Company

With over 300 sites and 100,000 employees scattered across the globe, developing and deploying a coherent IT strategy was a huge challenge for a Global Pharmaceutical Company (GPC). A typical remote office at GPC had seven to 10 servers hosting different types of applications – for instance, e-mail, directory, anti-virus, and file and print services. GPC wanted to reduce the capital and operational costs associated with hosting these applications. Thus, they set out to create a standardized remote office “virtual application pack” based on VMware Infrastructure 3 and six applications – Microsoft® Exchange®, Active Directory, SMS, antivirus, file and print services, and EMC® Avamar® Virtual Edition. By virtualizing their remote office servers, GPC reduced the number of servers in their remote offices by up to 78percent. Due to the remote locations of its sites and the great distance between its data center and sites, a server failure risked creating long downtimes for its remote office employees. By using VMware HA, GPC is able to limit potential downtime to less than 10 minutes.

Option 3: Load-Balanced using VMware VMotion and DRS at the Remote Office

Ideal for: Environments needing highest levels of availability and performance.

Solution overview: By using two or more physical servers running VMware Infrastructure 3 Enterprise connected to shared storage, a remote office can eliminate planned downtime with VMware VMotion and “Maintenance Mode,” a feature of VMware DRS. As in Option 2, VMware HA typically limits unplanned downtime to less than two minutes. Additionally, remote offices running applications that have different resource requirements (e.g. transaction, manufacturing control systems, accounting systems, etc.) can take advantage of automatic load balancing across servers, ensuring maximum performance and resource utilization. Having redundant host-bus adapters, dual power supplies, redundant fan kits and multiple network interface cards further minimizes potential points of failure.



Typical architecture components:

- **VMware Infrastructure 3 Enterprise**
 - **VMware ESX Server:** Installed in the remote office to partition servers.
 - **VMware VirtualCenter:** Runs in the data center and connects over the network to distributed hosts for centralized management.
 - **VMware HA:** Used in the remote office to automatically restart virtual machines on a secondary server in cases of hardware failure.
 - **VMware DRS:** Reduces unplanned downtime by automatically migrating running applications away from servers that cross utilization thresholds.
 - **VMware VMotion:** Allows for live migration of virtual machines across hosts in the remote office.
- **Two or more physical servers with shared storage:** Installed in the remote office.

Customer case study: Engen Petroleum

Engen Petroleum is one of the world's most advanced fuel technology companies. The company is a distributed organization with 2,500 users. It maintains approximately 1,250 service stations in South Africa as well as a central office that is responsible for six remote offices. These remote offices have no IT support staff.

Following years of rapid growth, Engen experienced a rapid increase in the number of servers its IT department had to deploy, manage and maintain, resulting in rising support and maintenance costs, lack of space and low server utilization. To curb server growth and streamline IT management processes, Engen rolled out VMware ESX Server at each of its remote offices to run a wide variety of applications, including Microsoft Exchange, Citrix and SQL. VMware VirtualCenter performs remote management from the data center. Engen decreased downtime using VMware VMotion to keep services running during hardware servicing. In addition to curbing server sprawl in its remote offices, Engen also cut maintenance costs by 50 percent and reduced server provisioning time from seven hours to 15 minutes. According to Nick Lain, systems engineer at Engen, "We used to face a significant challenge in the delivery of new systems to remote offices, due to the lack of infrastructure flexibility, remote management tools and local IT staff. Thanks to VMware, we are now able to manage servers at six remote locations from a central point."³

³ Read more about Engen Petroleum's branch office deployment at <http://www.vmware.com/pdf/engen.pdf>

Loss of WAN Connectivity in Distributed Deployments

In Distributed Deployments, losing WAN connectivity to VMware VirtualCenter will not disrupt business operations in the remote office. Because the basic function of virtualization is provided by the ESX Server hosts in the remote office, the virtual machines will continue to run. VMware HA will continue to protect remote office virtual machines, as VMware HA functionality does not depend upon VirtualCenter once it has been configured. Automatic load balancing of virtual machines (via VMware DRS) will halt temporarily while VirtualCenter connection is unavailable (as VMotion is initiated by VirtualCenter), but will automatically resume once the connection is re-established.

The following table summarizes the impact of VirtualCenter downtime on a VMware Infrastructure 3 environment.

Component or Functionality		Impact of VirtualCenter Downtime
Virtual Machine		Continue to run; management through direct connection to ESX Server only.
ESX Server		Continue to operate; management through direct connection only; cannot modify host inventory.
VMotion		No function
VMware DRS		No function
VMware HA	Restart VM	Continues to operate, i.e. VMs will be restarted on other host if ESX Server fails.
	Admission Control	No function
Performance & Monitoring Statistics		Historical record will have gap during time of outage; real-time statistics can be viewed per host or VM by connecting directly to the host.

Table 2. Impact of VMware VirtualCenter downtime on remote offices.

Additionally, organizations can further protect themselves from failure of the VirtualCenter server, the entire datacenter or simply from the datacenter being disconnected by replicating the VirtualCenter database to another site. Administrators can configure a second VirtualCenter to automatically reach out to all ESX servers and update their VirtualCenter configurations (IP address for VirtualCenter).

Conclusion

Organizations with remote and branch office infrastructure need reliable and cost-effective solutions that can scale with the growing needs of their remote and branch offices. With a VMware Infrastructure solution, IT organizations can reduce the cost and complexity of managing remote and branch office environments, while delivering higher levels of flexibility, availability and protection. By virtualizing either at the remote office or back to the data center, organizations can leverage existing data center IT and personnel resources, thereby reducing cost, effort and downtime.

To learn more about remote and branch office solutions with virtual infrastructure, visit us on the Web at <http://www.vmware.com/solutions/remotefice>. If you are ready to implement remote office solutions in your environment, VMware Professional Services and our global network of solutions providers can help you develop a customized plan for virtualizing your remote offices. Email us at sales@vmware.com or call us at 1-877-4VMware to get started.

Additional Resources

File / Print / DNS Servers: Getting Started with Virtual Infrastructure:

http://www.vmware.com/pdf/file_print_dns_wp.pdf

Making Your Business Disaster Ready with Virtual Infrastructure:

http://www.vmware.com/pdf/disaster_recovery.pdf

Reducing Server Total Cost of Ownership (TCO) with VMware:

<http://www.vmware.com/pdf/TCO.pdf>

VDI – A New Desktop Strategy:

http://www.vmware.com/pdf/vdi_strategy.pdf

Appendix: Third-Party Components

A complete Remote and Branch Office solution may also include other design elements that compliment, extend or leverage the core features of VMware Infrastructure virtualization platform. The following sections provide examples of third-party components that complement VMware's remote office solutions. These product listings are not meant to be all-inclusive.

Optimizing Network Performance with WAN Acceleration

Organizations can improve application performance and avoid costly bandwidth upgrades by using WAN acceleration to overcome bandwidth limitations and network latency in their existing WAN links. WAN acceleration technologies can be added to VMware's remote and branch office solutions in both the Centralized and Distributed Deployment approaches for improving disaster recovery traffic, application performance over the WAN and remote management.

- **Cisco:** Cisco® Wide Area Application Services (WAAS) reduces congestion on the WAN by combining application acceleration and Cisco Wide Area File System (WAFS) with a variety of WAN optimization techniques, including compression, redundancy elimination, transport optimizations, caching and content distribution. The Cisco Integrated Services Router bundles all networking capabilities required for a remote site into a single device, including Cisco WAAS functionality.
- **Riverbed:** Riverbed® Steelhead™ appliances and Steelhead Mobile software are powered by the Riverbed Optimization System, which combines patent-pending data reduction, TCP optimization, application-level latency optimizations, and remote office file and management functionality. This provides for LAN-like speeds in copying virtual machines and data, and enables quick set up of a remote or branch office. Riverbed products are in use with VMware deployments today and require no customized configuration.

Leveraging Replication Software for Manual Failover and Disaster Recovery

Host-based replication can be used in combination with manual failover at the remote office (as in Distributed Deployment: Option #1) for additional levels of availability. In scenarios where VMware HA is being used for automated failover at the remote office (as in Distributed Deployment: Option #2), guest-based continuous replication can be a cost-effective way to replicate critical data from within virtual machines to centralized datacenters hundreds of miles away for disaster recovery.

Host-based replication can be used when performance SLA's are moderate. For demanding performance requirements and lowest Recovery Time Objective and Recovery Point Objective, organizations should consider off-host replication via array-based or storage network-based replication with WAN acceleration. The replication load is handled by the storage processors within the storage arrays in the remote office and disaster recovery sites (connected by a WAN). Synchronous replication improves data integrity but presents a potential performance bottleneck. Asynchronous replication accepts a higher potential of inconsistent data in exchange for increased performance.

Below are examples of replication recovery approaches that work with VMware Infrastructure.

- **CommVault:** With CommVault® Continuous Data Replicator (CDR), changes are captured as they occur and are moved over the WAN from the remote office to the central site in small portions. This helps preserve WAN bandwidth during crucial business hours and enables more granular recovery options since data is captured continuously. Once the changes are at the central site, snapshots are taken of the central site replica on a scheduled basis to create discreet recovery points. Because of the continuous nature of the replication and the snapshotting, it is possible to keep many points in time available for recovery, rather than only the traditional daily backup copy.
- **Double-Take Software:** Double-Take Software provides a set of products which allow the data from each virtualized server to be replicated in real-time to a target virtual or physical server. Double-Take for Virtual Systems installs within each VM and provides continuous replication and automated application failover. Double-take for VMware Infrastructure provides replication at the ESX Server host level, protecting entire VMs to a second physical host and allowing easy recovery of the entire virtual machine.
- **EMC:** EMC® Replistor provides asynchronous replication of open and closed files, directories and registry keys for Microsoft Windows environments over unlimited distances via LAN/WAN connectivity. Whether protecting VMware VirtualCenter or Microsoft applications such as Exchange and SQL Server with Microsoft VSS integration, EMC RepliStor offers manual and automated failover and failback for protecting business critical data. In the case of a disaster, EMC Replistor ensures users stay connected to their applications and data at a secondary location.
- **NetApp:** NetApp® ReplicatorX™ is a heterogeneous replication software that can replicate data and system drives. In an environment where remote or branch offices are looking for the benefits of centralized data services, administration and security of their local data, ReplicatorX can be used for disaster recovery, cloning of production data for development and test, analytics or reporting, and data migration.

Improving Data Protection with Centralized Backup

Organizations able to lose up to one day of data may choose not to invest in replication for disaster recovery and instead, backup complete virtual machine (.vmdk) files to headquarters. Not only does centralized backup ensure organization-wide consistency in data retention and disaster recovery protection, but it also reduces the amount of unmanaged and unprotected data sitting at each remote office. Centralized backup solutions today use data de-deduplication and compression technologies to reduce the backup windows and the amount of backup data that needs to be stored onsite or sent over the network. Organizations can choose to combine WAN acceleration technologies with their current backup software, or use an all-in-one centralized backup solution.

- **CA:** CA XOSoft and CA ARCserve fully integrate cross-platform WAN-optimized replication, application failover, traditional backup and continuous data protection. This integration allows for consolidation of backups from multiple branch office servers into a central data center location with low deployment and staffing overhead, while simultaneously delivering the benefits of disaster recovery and continuous application availability. CA ARCserve VCB integration also enables the solution to take full advantage of the virtualized environment.
- **CommVault:** CommVault's Simpana software suite provides multiple ways to protect remote office data. Through the Galaxy Backup and Recovery product, traditional remote office backups for file and database data over WAN connections are supported. These backups can include both local and remote copies of the data managed on a scheduled basis with initial and secondary copies created at different times and to different media types (disk to disk, tape) in any combination.
- **Data Domain:** Data Domain's Global Compression high-performance de-duplication and local compression technology reduces the volume of virtual machine (.vmdk) backup data to be stored by up to 40x. Cutting network bandwidth requirements up to 99percent, the Data Domain solution enables offsite vaulting for disaster recovery across the WAN.
- **EMC:** EMC® Avamar identifies redundant sub-file data segments within and across servers, desktops and remote offices worldwide. As a result, Avamar reduces the traditional backup load – which can be as much as 200 percent of primary data moved weekly – down to as little as 2percent. Avamar de-duplicates data *before* it is transferred across the network or virtual infrastructure, dramatically reducing virtual machine backup times and shared resource consumption. Avamar provides efficient, encrypted, replication across sites, eliminating the need to manage and ship tapes for disaster recovery. EMC Avamar Virtual Edition is deployed as a virtual machine and leverages existing shared storage and server resources
- **HP:** HP® Data Protector™ Software automates high performance backup and recovery, from disk or tape, over unlimited distances, to enable 24x7 business continuity and improve IT resource utilization. Centralized multisite management capabilities enable organizations to automate routine tasks and easily implement changes. Synthetic full and virtual full backup reduces the time and resources needed to perform backups. By using "pointers" rather than duplicating data (Virtual Full) or automated backup object consolidation into a single full on tape (Synthetic Full), HP Data Protector Software provides an 'Incremental forever' feature, thereby reducing the data volume dramatically. This enables organizations to perform both local and remote backups in the most efficient manner while providing the flexibility of disk to disk/disk to tape/tape mirroring combinations.

- **NetApp:** NetApp® Snapshot™ / SnapRestore™ technology enables near-instantaneous, space-efficient, server-free backups and recovery of data, applications and virtual machines deployed in remote or branch offices. From a disaster recovery perspective, SnapMirror and SnapVault can be used to transmit these local backups to a centralized facility with efficient data line usage due to NetApp de-duplication solution. Beyond these solutions which are available on the entire NetApp® FAS Series family, replication from StoreVault to FAS Series is also available for remote locations needing an entry-level storage platform.
- **Symantec:** Symantec® NetBackup integrates Symantec's PureDisk deduplication technology to ensure that redundant backup information is only stored once across the entire backup environment, consolidating desktops and laptops, remote offices and data centers. This global approach to deduplication has commonly yielded 50-500X data deduplication rates when compared to traditional backup methods.
- **Vizioncore:** Vizioncore® vRanger is a hot backup solution for VMware Infrastructure that takes a full image backup and restores it to any VMware ESX Server for rapid recovery. A full bare-metal backup image provided by vRanger includes the entire operating system and data volumes, as well as the configuration settings for the virtual machine being backed up. Images can be sent as compressed files over a WAN to support disaster recovery strategies. vRanger reduces the size of the original virtual machines (.vmdk file) by an average of 50percent. Because vRanger is VMware VirtualCenter aware, IT administrators can manage remote office backups using the same VirtualCenter interface that is used to manage the virtual machines.

Cost-Effective Alternatives to Physical Shared Storage

A traditional physical shared storage system may exceed the budget, space or IT management capabilities of some remote or branch offices. For these offices, virtual storage appliances are a viable alternative to purchasing and managing physical shared storage. Virtual storage appliances encapsulate internal disk storage of a series of VMware ESX Servers, aggregate it, and present it back to the VMware ESX Servers as an iSCSI shared storage cluster. This enables the remote office to leverage VMware shared storage features, such as VMware HA, VMware DRS, VMware VMotion technology, and VMware Consolidated Backup.

- **LeftHand Networks:** LeftHand Networks Virtual SAN Appliance (VSA) for VMware ESX Server enables high availability and remote data replication without the cost and additional hardware of a physical SAN. The VSA is LeftHand Networks full featured open iSCSI SAN software, SAN/iQ®, integrated into a certified Virtual Appliance supported on VMware ESX Server. The VSA allows remote/branch offices to combine server virtualization and storage virtualization on the same server hardware. The SAN/iQ VSA replicates data across the ESX Server nodes using patented Network RAID capability to provide continuous data availability in the event of a network, disk, processor, or entire server failure at the remote/branch site. Utilizing as few as two servers, remote/branch offices can enable all the enterprise class features and remote management once considered out of reach for small offices. Using the VSA's Remote Copy capability, remote/branch sites can copy data over WAN links to the Data Center Headquarters for a simple, cost effective backup and disaster recovery.



VMware, Inc. 3401 Hillview Ave Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2008 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,961,806,
6,961,941, 6,880,022, 6,397,242, 6,496,847, 6,704,925, 6,496,847, 6,711,672, 6,725,289, 6,735,601,
6,785,886, 6,789,156, 6,795,966, 6,944,699, 7,069,413, 7,082,598, 7,089,377, 7,111,086, 7,111,145,
7,117,481, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,268,683, 7,275,136, 7,277,998,
7,277,999, 7,278,030, 7,281,102, 7,290,253; patents pending.

