WHITE PAPER

VMware Infrastructure and CA XOsoft's WANSyncHA

Building a Cost-effective and Robust DR System

Contents

Introduction 1

The Importance of Business Continuity 1

The Increasing Expense and Complexity of DR Planning 1

An Introduction to the Technologies 3

VMware Infrastructure 3

VMware ESX Server 4

The Complete VMware Infrastructure Solution 6

High Availability Benefits of VMware Infrastructure 9

CA XOsoft's WANSyncHA 9

The Basic System 10

Protection from Corruption with CDP 11

Automated Testing with Assured Recovery 11

A Summary of Benefits 13

The Combined Solution 14

The Need for a Layered Solution 14

Outline of the Solution 15

Sample Scenarios 16

Conclusion 20

About VMware 21

About CA XOsoft 21

Introduction

You can combine two very powerful solutions, VMware Infrastructure and CA XOsoft's WANSyncHA, to provide a multi-layered disaster recovery solution that covers a wide array of contingencies, is extremely cost-effective, and provides an unusually high degree of robustness and simplicity.

The Importance of Business Continuity

The expansion of IT systems to power more and more mission-critical business processes is fueling both an increase in the importance of business continuity (BC) and disaster recovery (DR) planning and a corresponding increase in the difficulty of providing DR coverage that is both cost-effective and robust. Any time the IT systems that power a business's core processes are disrupted, the negative business impact is extremely serious: from revenue loss when customers cannot reach your business systems or be serviced to productivity loss when employees are unable to work to longer-term costs of damaged reputation, such as the loss of investor confidence resulting in decreasing stock valuations, and future lost opportunities due to defecting customers.

While a particular business may consider the likelihood of a major disaster insignificant, the picture can change when the entire range of potential disruptions is considered, from virus attacks to fiber cuts to application errors to simple administrator and user errors. Considered together with the potential cost to the business, the risk easily becomes quite significant. If a major disaster occurs, the very existence of the business is threatened.

The Increasing Expense and Complexity of DR Planning

To exacerbate the problem, IT systems are becoming more important, more numerous, and more complex. Increases in the productivity and effectiveness of business processes that arise from the application of new technologies tend to lead to a rise in the expectations of customers, management, employees and investors. As a result, what was once a significant advance in capabilities quickly becomes just a new baseline against which day-to-day performance is measured. The scope of these systems is also increasing from just a few critical servers to larger and larger numbers of web servers, application servers, database servers, and so on.

The problem of protecting these systems is twofold:

First, as illustrated in Figure 1, providing the best business continuity protection for servers is an expensive proposition. As availability requirements increase, so does the cost of purchasing and maintaining the required solutions.

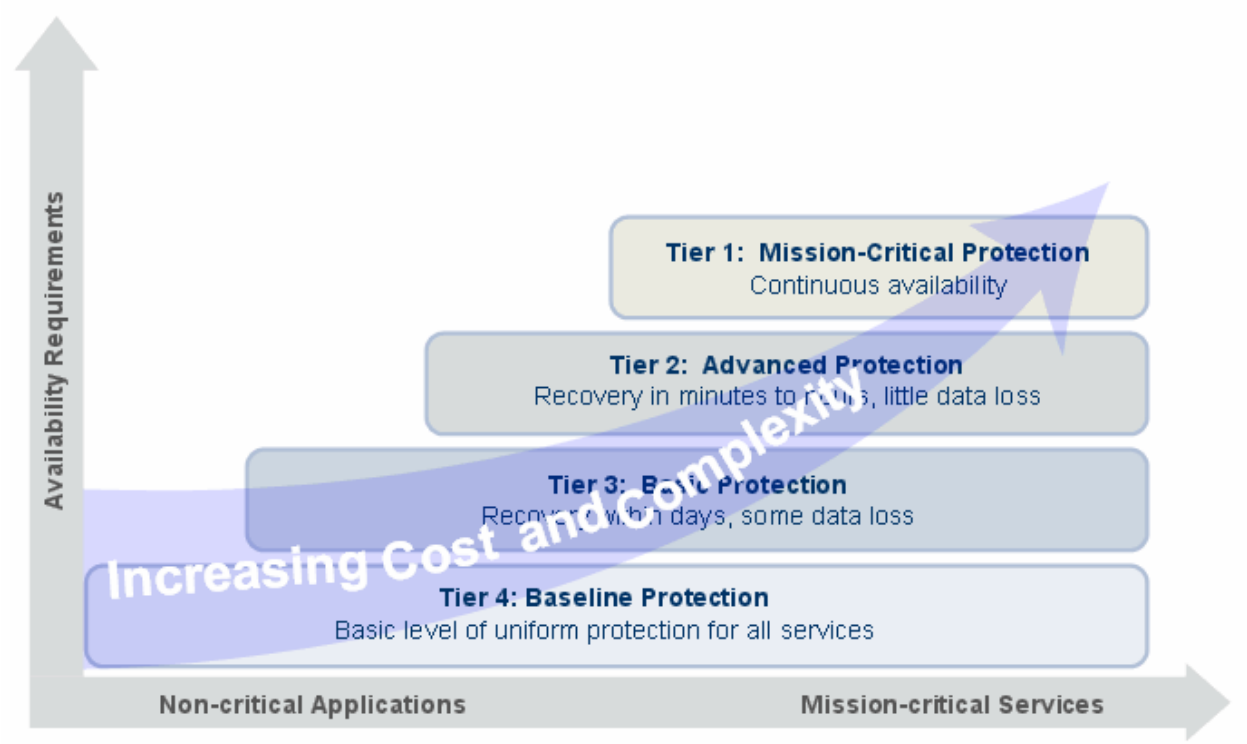

Figure 1: Increasing cost and complexity of advanced protection

Second, increasing numbers of servers and systems and increasing availability requirements on those systems are effectively increasing the numbers of systems that fall into the top tiers of Figure 1. These increased numbers lead to increased complexity. Some complexity arises from the need to install and maintain large numbers of duplicate systems, with all the attendant management issues, such as performing regular upgrades in sync with production systems, and infrastructure issues, such as heat and power management problems. Additional complexity arises as well because higher-availability solutions most often do not replace lower levels of protection. Rather, they are added on top of existing protection methods in order to augment their capabilities; having an automatic switchover solution doesn't mean that you stop making backups.

As the numbers of protected servers increase, however, a further source of complexity arises because of potential failures in the DR systems themselves. With just a few servers, the likelihood is low that the backup systems will have a problem at the same time that the main site goes down. With larger numbers of systems, however, that likelihood increases until, at some point, it becomes a virtual certainty. Thus, there is a new problem with the robustness of the DR solution due simply to the sheer number of systems being protected.

In summary, as the numbers of servers requiring high availability protection increase, organizations face increasingly complex and expensive solutions that are decreasingly robust.

This is the problem that this paper addresses. In the next few sections, the paper will introduce the individual technologies from which a solution can be built. Following that, it discusses how these two powerful technologies can be combined to produce a DR solution for mission critical servers that is both cost-effective and highly robust.

An Introduction to the Technologies

This section introduces the two technologies. The goal is to convey a basic understanding of what each technology does, how it works, and what advantages it brings to the IT environment.

VMware Infrastructure

Infrastructure is what connects physical IT resources to your business and its key processes. VMware Infrastructure accomplishes exactly the same thing as physical infrastructure, but in a dramatically flexible and cost-effective way. At the core of VMware Infrastructure is the powerful ESX Server (see the section entitled *ESX Server*). VMware Infrastructure transforms industry standard servers and their attached networks and storage into flexible pools of resources that administrators can *dynamically map* to your business needs. The result: decreased costs and increased efficiencies and responsiveness.

Virtualization has already changed the way IT resources are managed. Storage virtualization technology, such as Storage Area Networks (SANs), abstracts the physical storage resources and hides the details of the physical disk drives on which files reside, while managing the security and backup of the data transparently. Similarly, network virtualization in the form of Virtual LANs allows a logical networking topology to be overlaid on a physical topology, increasing flexibility to secure and isolate network traffic.

VMware Infrastructure provides a broad virtualization capability that includes network, storage, and processing resources. It allows administrators to deploy applications and services on any server and easily move between servers when needed.

VMware Infrastructure treats the IT infrastructure as a pool of computer, storage and networking power and provides management tools to take advantage of this pool of resources. As a result, IT infrastructure is more manageable, more efficient, and more easily serviceable - at a lower cost.

VMware ESX Server

Virtualization is a layer of abstraction between physical hardware resources and the operating system and applications that make use of them. By decoupling the OS from the underlying hardware, ESX virtualization enables multiple *virtual machines* to run simultaneously on a single physical set of hardware, thus providing far better resource utilization and flexibility.

As illustrated in Figure 2, each virtual machine is a true representation of an x86 computer, complete with processor, memory, networking interfaces and storage devices. It is important to note that the VMware virtualization layer gives each virtual machine direct access to the underlying x86 processor. This is a key distinction from hardware emulation approaches since it means that a virtualized solution is able to match the performance of a traditional server with all hardware dedicated to a single instance of the OS.

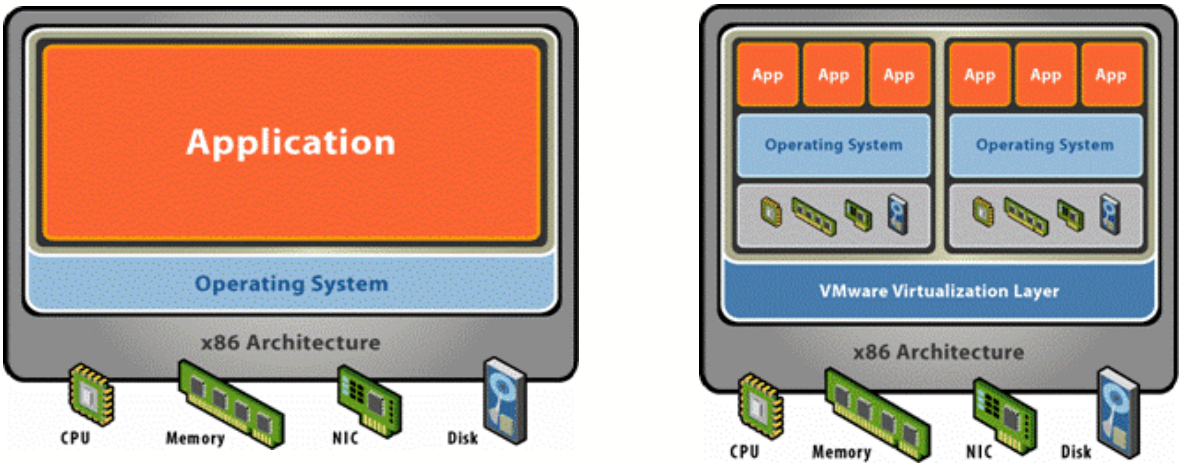

Figure 2: With virtualization and without virtualization

Virtual machines are a well proven concept. They were developed to allow multiple users to share the very expensive resources of mainframe systems safely. VMware applied the virtual machine concept to lower-cost hardware platforms in order to solve the more recent problems of server proliferation and server resource under-utilization that arose from the need to run critical applications within dedicated operating systems. VMware's unique technology can virtualize x86 systems efficiently so that multiple unmodified x86 operating systems and applications can run simultaneously in a true virtual environment with excellent performance.

ESX Server uses a "bare metal" architecture. A host operating system does not need to be installed for ESX to work. In fact, ESX Server is a light-weight operating system that is installed directly on the hardware. Because ESX Server removes the need for a host operating system, virtualization is more efficient.

Virtualization brings three key classes of benefits, as illustrated in Figure 3.

Partitioning for Improved Resource Utilization

Virtual machines allow a single physical computer to be divided into separate *partitions*, each of which can run its own operating system and application stack concurrently with the others. In fact, the virtual machines can run completely different operating systems and software because each is allocated its own storage, memory, and networking interfaces, with the underlying virtualization layer allocating the shared physical resources between virtual machines. The networking and storage features of virtual machines allow them to be networked exactly as would real physical machines, so that they may be joined in clusters for high availability or isolated on separate networks for security purposes.

Because partitioning allows multiple OSs to operate simultaneously on the server, it improves hardware resource usage dramatically. With a typical ratio of about four to eight running virtual machines per physical CPU (and other hardware resources), hardware usage can be increased substantially without sacrificing overall performance. More effective usage in turn translates into reduced operating costs and better returns on hardware investment.

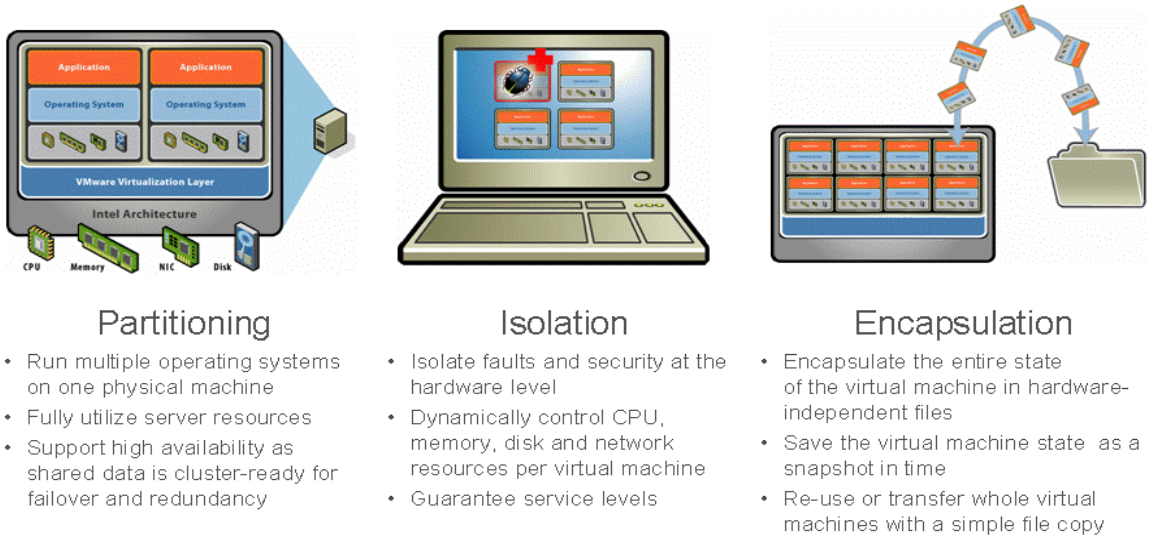

Figure 3: Three key properties of virtualization

Isolation for Improved Security

The process that manages the concurrent execution of each virtual machine on the host system hardware uses the hardware protection features of the CPU to *isolate* the virtual machines from each other and from the monitor, resulting in strong separation of one operating environment from another, since there is no shared component. All the sharing takes place at the virtualization layer.

The implication of isolation is that applications in one virtual machine can encounter failures without any effect on other virtual machines. Indeed, the U.S. National Security Agency spent over a year attempting to hack from one virtual machine to another and were unable to find any weaknesses to exploit, leading the NSA to approve VMware technology for running insecure off-the-shelf software on their secure machines.

By isolating faults and security at the hardware level and dynamically controlling CPU, memory, disk and network resources for each virtual machine, VMware's virtualization technology removes end user objections to server consolidation because it allows IT administrators to guarantee service levels and security even in a shared-resource environment.

Encapsulation for Improved Manageability

Encapsulation means that the complete state of a virtual machine – memory, disk storage, I/O device, CPU state, and virtual hardware configuration – is all stored in a small set of files. These files are hardware independent, so a virtual machine image can be moved from one physical server to another and will run with no changes necessary as long as the VMware virtualization layer is present, even if the physical servers are from different manufacturers.

An *encapsulated* virtual machine can represent just the configuration and disk state or can be a snapshot of the entire state of a *running* machine at a point in time. Such an encapsulated machine image can saved and reverted to at any time. By storing the image in machine-independent files, you gain the ability to copy, save, and move virtual machines wherever and whenever you need them simply by copying a directory of files.

The Complete VMware Infrastructure Solution

While ESX Server is a key component of VMware Infrastructure, many other components are included in order to deliver a true virtual infrastructure solution. VMware Infrastructure allows server, storage and network resources to be managed like a shared utility and provisioned to different business units and projects without a need to worry about the underlying hardware differences and limitations.

Additional components included are the VMware Virtual Machine File System (VMFS), a high-performance cluster file system for virtual machines; the Virtual Symmetric Multi-Processing (SMP) capability that allows a virtual machine to use multiple physical processors simultaneously; the VirtualCenter Management Server, which provides a central point for configuring, provisioning and managing the entire virtualized IT infrastructure; and the VI Client and VI Web Access, which provide an interface to allow administrators and users to connect remotely to the management server or individual ESX Server installations (see Figure 4).

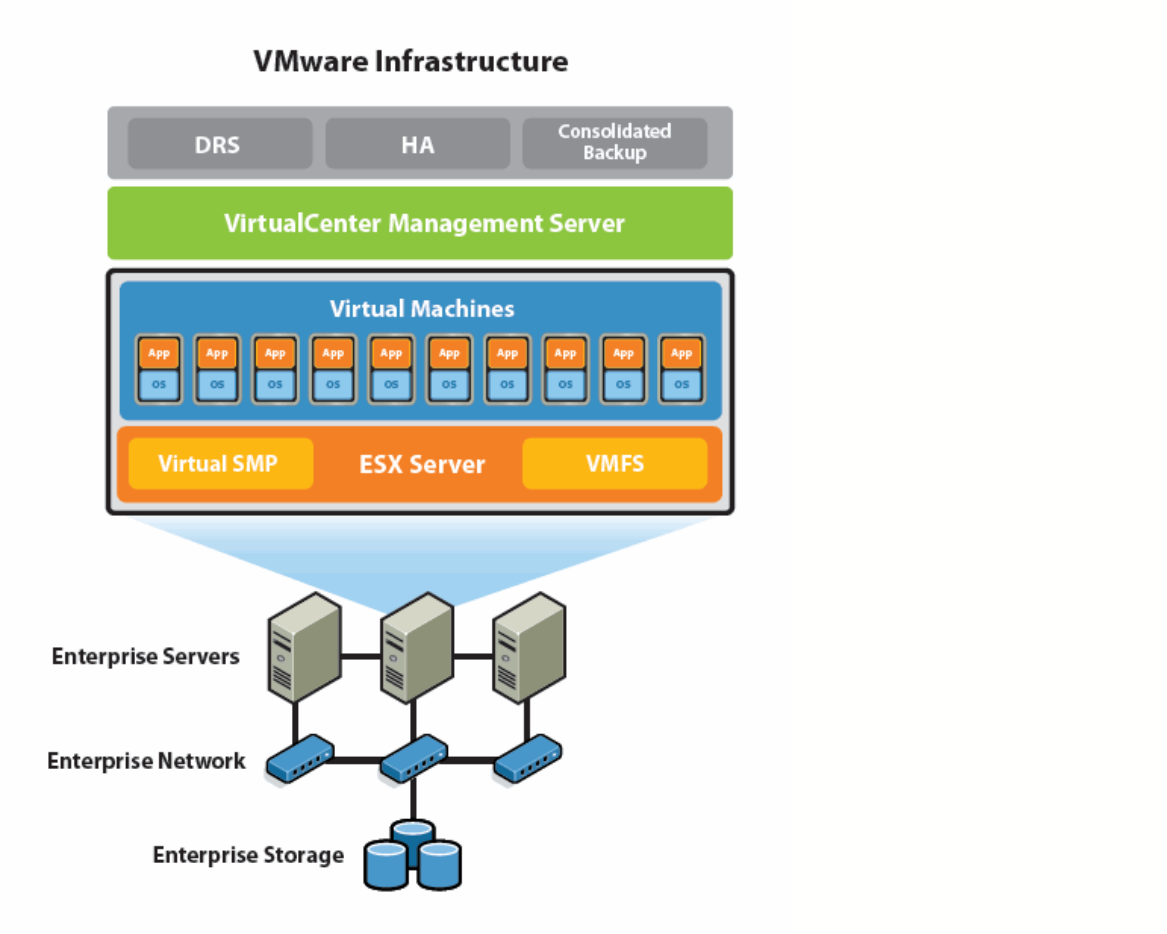

Figure 4: VMware Infrastructure architecture

In addition to this basic infrastructure, VMware Infrastructure also offers several unique capabilities in support of truly dynamic mapping of resources to needs. The first is VMware VMotion™, an advanced capability that enables *live* migration of a running virtual machine from one physical server to another with zero downtime, continuous service availability, and complete transaction integrity. In an enterprise networked storage environment, virtualization lets system administrators think of their computing resources as "pools." The boundary of a physical system becomes irrelevant since virtual machines can use any physical resource in the pool when preset policy conditions are met. This easy movement of virtual machines from one physical server to another enables IT organizations to maximize availability and resource usage. Moreover, the administrator can automate all of this based on configurable policies.

High Availability Benefits of VMware Infrastructure

The VMware Infrastructure enables customers to create resource pools from their existing hardware within the data center and to create virtual machines that use these pools. Once provisioned, virtual machines can be moved freely from one server to another in the resource pool, as long as certain configurable service level and availability conditions are satisfied. VMware HA (VMHA) enables customers to deploy a local high availability solution so that if one server in a resource pool fails virtual machines running on that server are restarted on another server.

Because VMHA agents are already installed on the ESX Server, minimal setup is required. All ESX Servers in the resource pool can host their own virtual machines and still accept new VMs if one server fails. VMHA constantly monitors capacity usage and reserves spare capacity so as to restart virtual machines. VMHA is OS agnostic and easy to manage. VMHA agents are part of the ESX Server and don't install on the guest OS. It does not matter what OS the virtual machines are running. Since there are no agents to be installed on virtual machines, there is no need to manage agents in each virtual environment. It is important to note that VMHA can move virtual machines in case of server failure, but not software failure in the virtual environments themselves.

CA XOsoft's WANSyncHA

The second technology component of the joint solution presented in this paper is CA Xosoft's award-winning WANSyncHA product. WANSyncHA is a hardware-independent business continuity solution that integrates several powerful technologies to provide continuous availability of your mission-critical application servers through a wide range of disasters, from server failure to data corruption to the loss of an entire site.

WANSyncHA is much more than a data protection solution. Restoring data after a problem occurs is just the first step in getting your critical business processes operational. Therefore, the focus of WANSyncHA is on protecting the *application,* not just the data.

This application focus means first that CA XOsoft has integrated into a single product *all* the technologies required to ensure the continuity of your IT services, including data replication, automated push-button or fully automatic switchover of the application server over a LAN *or* WAN, application-aware status monitoring, integrated continuous data protection as a guard against data corruption, and completely non-disruptive automatic testing of your disaster recovery system, all in a system that sets the standard for ease of configuration and management.

In addition, CA XOsoft has developed application-specific WANSyncHA solutions for major applications like Microsoft Exchange, Microsoft SQL Server, Oracle, Microsoft IIS web servers, Blackberry Server, file servers, and other applications on both 32- and 64-bit Windows servers, Windows clusters, and Linux, AIX and Solaris servers. These out-of-the-box solutions dramatically reduce deployment and management complexity by automatically detecting application data and configurations, auto-configuring appropriate defaults tailored to the application, and in several cases even automatically configuring your DR server to match the production system's configuration.

The Basic System

Figure 5 illustrates how WANSyncHA works. Here, the production application, such as an Exchange or database server or cluster, is located at the main data center in San Francisco – this is the system that is normally used by clients. A second server, called a *replica,* is located at a backup facility in New York – this second server is normally passive, but is available to take over the function of the production server in the event that becomes necessary.

Underlying the WANSyncHA solution is powerful asynchronous host-based software replication that transfers changes to application data as they occur to a standby replica server, which may be located nearby on the same subnet or at any distance over a WAN link. The replication system ensures the integrity of the replicated data, which may be emails, database updates, file operations, etc. All operations are performed byte-for-byte in exactly the same order they occurred on the production server, making it an appropriate solution for databases and other applications where preserving write order is vital. Thus, the replica server always maintains an exact

copy of the state of the production server just a few seconds earlier. The lag arises because WANSyncHA uses asynchronous replication in order to eliminate distance restrictions on the location of the replica server. WANSyncHA even supports cross-platform replication between different operating systems, e.g., from Windows to Linux, where appropriate.

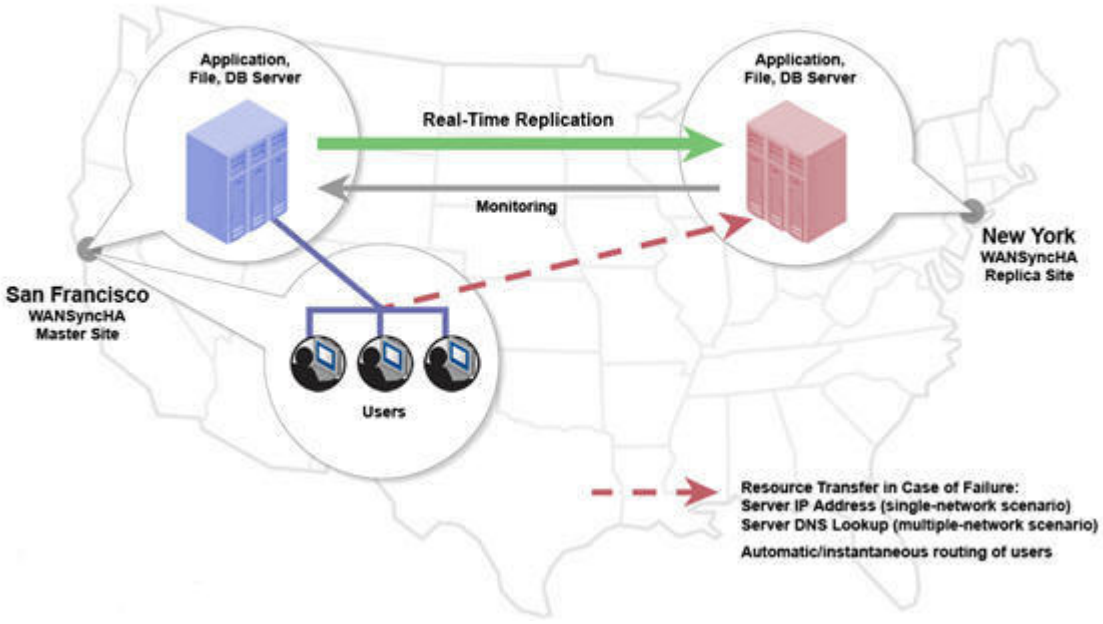

Figure 5: Schematic of WANSyncHA

At the same time that data is replicated, WANSyncHA continuously monitors the state of the production server. Much more than a simple ping, the system monitors both the accessibility of the server and the state of the application, including checking that all necessary application services are running and that the application data registers as valid.

In the event a problem with the production server is detected, WANSyncHA alerts the administrator – alerts can be configured to be sent via the GUI event window, email, system logs, and other means. If it is necessary to have the replica site take over servicing users, a fully automated switchover can be triggered either automatically by WANSyncHA or with a single push of a button by an administrator, depending on how you choose to configure the system. In either case, once triggered, WANSyncHA starts the application on the replica server and perform all actions necessary to redirect users to that server. No client-side configuration is necessary, and the entire process takes just a few minutes – essentially the time required to start the application on the replica server.

Once the production system and site are back up and running, the two sites can be resynchronized simply by restarting the WANSyncHA scenario. Once synchronization is complete, the application can be switched back with the same push of a button – there is no need for time-consuming and complex reconfiguration to prepare for switchback.

Protection from Corruption with CDP

Continuous data protection (CDP) refers to the ability to recover data not just to certain isolated previous states captured, for example, in a daily or weekly backup or snapshot, but to recover the data back to *any point in time*. XOsoft pioneered the development of true, continuous CDP back in 2002 through its *rewind technology* and it remains a core capability built into WANSyncHA.

CDP provides the extra layer of protection needed to recover not just from server or storage failure, but from data corruption as well. Any time that data corruption occurs due to human error, a virus, or a software error,

the corruption is, of course, replicated to the secondary server too. If the error causes the production server to become unavailable, all the backup systems will be unavailable as well, for the same reason.

With WANSyncHA's rewind capability, however, it is still possible to recover: the data on the replica server need only be rewound to a time *before* the corruption event occurred, and the server can then be recovered. With CDP, both data loss and time to recovery are minimized.

Automated Testing with Assured Recovery

No matter how well a solution is tested when it is installed, it may fail to work later as a result of changes in the IT environment such as hardware replacements, software upgrades, network reconfigurations, or simply the growth of the dataset size. It is vital therefore that your business continuity systems be regularly tested if you are to continue to have confidence in them.

The problem is that testing is disruptive and expensive. Even the most basic test requires some disruption to application availability and IT staff time and, if the test fails, your organization faces real downtime and is left unprotected while the issue is resolved.

The ideal, illustrated in Figure 6, is a way to test the application on the replica server that takes over the production server responsibilities if switchover occurs, and perhaps even to switch over one or more test users, but to do this in a way that does not impact either the availability of the production server or the safety that the DR system is designed to provide.

In a nutshell, this is what Assured Recovery does.

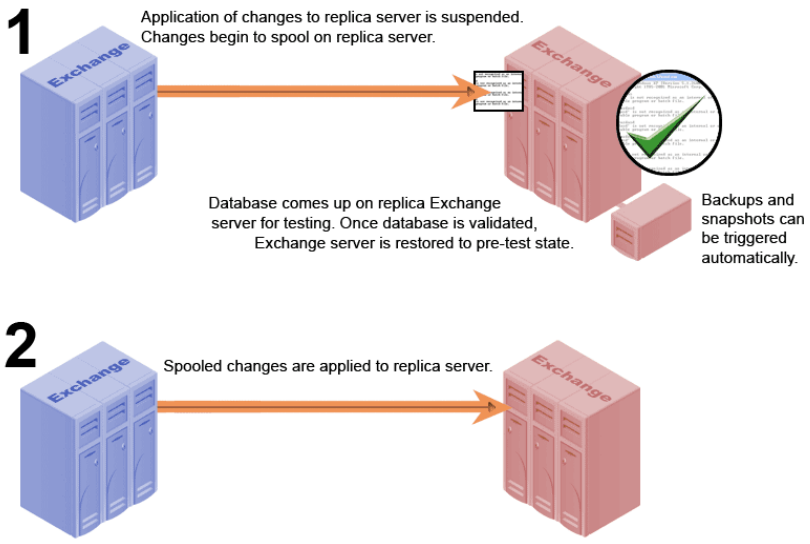

Figure 6: Assured Recovery at work

You can configure testing to occur automatically on a scheduled basis as often as once an hour, or you can perform it manually at any time. In either case, when testing begins, the changes that are replicated to the secondary server are temporarily stored there in a spool directory – note that the capture and transfer of changes from the production server does *not* stop at any point.

As a first step, the application is started on the replica server. For many applications, including email and databases, starting the application causes data to be written, taking the replica server out of sync with the production server. Assured Recovery addresses this problem through XOsoft's CDP technology, which is used after the test completes to restore the replica data to the precise state that existed when testing started.

Once the application is running, tests are performed. The simplest possible test, the one performed "out of the box," is simply for AR to start the application, verify that all services start and all databases properly mount, and

then shut the application down. Scripts can be registered to perform additional customized testing. Fully interactive testing is allowed as well In the case of Exchange, for example, the administrator can interactively switch over a single test user to the replica server, using the same technology that is used in a real switchover, test out the system by sending and receiving several emails, and then switch the test user back to the production server.

This is a true test of the replica system, the kind of test that ordinarily could be done only by stopping replication during the test, and then resynchronizing the data, an approach that is time-consuming, involves user downtime, and risks the system by leaving it unprotected during the test. With Assured Recovery, there is no impact on the production system, on users, on the network, or on the level of protection. If the production server fails during the test, switchover occurs as soon as the test is completed.

Once testing is done, Assured Recovery can trigger a backup or snapshot of the just-validated data automatically, providing support for offsite backups without the cost or complexity of transporting tapes or for backup consolidation of branch office servers to a single central site.

A Summary of Benefits

In summary, WANSyncHA provides several layers of automated business continuity protection either within a single site or across geographically distant locations: continuous replication to ensure minimal data loss, automated monitoring and switchover to ensure minimal downtime, CDP to protect against accidental or malicious data corruption, and fully automated and non-disruptive testing that can be performed daily or even more often to ensure that the solution remains solid even in a dynamic environment.

In addition to the sophisticated functionality of WANSynchHA, the solution is extremely easy to install and manage. The product can be installed on a fully operational system with no application or user downtime. Wizards guide the administrator through remote installation, including simultaneous installation on multiple servers, and through the creation of new scenarios. Finally, a simple and flexible GUI management console enables all scenarios of all types throughout the enterprise to be managed from a single point or distributed across several different points, as best fits the needs of the organization.

The Combined Solution

Each of the technologies discussed in the previous section individually provides powerful and highly cost-effective support for maintaining continuous availability of applications that support critical business processes. As the number of systems that require high availability protection increases, though, a solution sufficiently broad to cover all major contingencies on all servers becomes increasingly expensive and decreasingly robust. This is where a combination solution built on both CA XOsoft's WANSyncHA and VMware Infrastructure enables a new approach to high availability that reduces total costs, reduces complexity, and provides increased robustness.

The Need for a Layered Solution

It is important to emphasize the tremendous importance in any effective disaster recovery solution of using multiple layers of protection. There are two key reasons for this. First is the need to mitigate the risk of any single point of failure. With large numbers of servers under protection, the likelihood that any single point of vulnerability will be hit can become quite high. The second reason is that a layered approach allows the strengths and weaknesses of particular solutions to complement one another. A shared-storage cluster, for example, is a powerful high availability solution, but not against site-wide disaster. A tape backup provides a final layer of protection against catastrophic data loss, but is inadequate to provide up-to-the minute data protection. Adding replication and cross-site switchover covers the gap between the two solutions effectively. The combination of all three provides effective protection against a much broader range of potential problems than can any single one of them.

We can divide the overall problem into three basic components.

The first component consists of local solutions at a production site such as the high availability features of VMware Infrastructure, to ensure high availability through a variety of localized problems, such as the failure of a single server or a single component of a system. Regardless of the local solutions used, however, an additional layer of protection is needed against site-wide disaster.

The second component of an overall solution, then, is a technology to carry high availability protection offsite. This may be straight data replication, either continuous or periodic, or, if there is a need for rapid recovery, it may be a full replication and application switchover. In the latter case, the production systems being protected must, of course, have replica systems at the disaster recovery site ready to take over.

As the number of systems you are protecting grows, a third component is becoming increasingly important, namely, a need for effective protection against *the failure of the DR systems themselves,* as well as a way to reduce the cost of maintaining a large number of duplicate systems.

Our discussion covers all three components.

Virtualization is one of the key decisions that IT administrator must make. Depending on the need, the primary as well as secondary DR site can be virtualized. Most customers can benefit from virtualization at both sites. In this case, called virtual-to-virtual DR, consolidation and HA benefits are available at the primary and secondary sites. VMware Infrastructure also allows load-balancing, thus improving application performance and availability at both sites.

Sometimes customers prefer to implement virtualization only at the secondary site, especially if the primary site already exists and a secondary site is being added for DR purposes only. In this case, called physical-to-virtual DR, applications and operating systems run on physical servers at the primary site, whereas they run in a virtual environment at the secondary site. This implementation allows customers to virtualize their environment according to their own schedule, without disrupting the primary site at all. Moreover, when the secondary DR site is virtualized, you already have the skills and knowledge framework to implement virtualization in production when the time is right

Outline of the Solution

The solution approach combines key capabilities of the CA XOsoft and VMware technologies.

- **Virtual Infrastructure for Effective Resource Utilization**

  The VMware Infrastructure Distributed Resource Scheduler technology improves the use of hardware resources, reduces power and cooling requirements, and significantly eases the management of the servers. With policy based load-balancing enabled, resources are used optimally and efficiently. Virtualization-enabled hardware consolidation can be achieved only at the primary site, only at the secondary site or at both sites. Simply changing the consolidation ratio (virtual machines per server) allows customers to save on the hardware cost of replicating the entire hardware environment of the primary site.

- **WANSyncHA for Replication and Switchover**

  WANSyncHA provides distance-independent data replication, continuous data protection, application monitoring, and automated failover to ensure fast, seamless recovery of all mission-critical IT applications in the event of a failure at the primary site, including accidental or malicious data corruption.

- **Assured Recovery for Regular Recovery Testing and Offsite Backup**

  Assured Recovery allows your organization to conduct daily or even more frequent tests of the recoverability of your applications at your disaster recovery site. In addition, integration with snapshot and backup means that you can produce offsite backups of validated data without the additional cost and complexity of transporting tapes.

- **VMware Infrastructure for High Availability**

  VMware Infrastructure's high availability features such as VMware HA, support for redundant network and storage connectivity, and fault isolation protect server infrastructure against hardware failures. When VMHA is implemented at the primary and/or secondary site, the organization can recover quickly and keep the servers/applications available through component failures.

Sample Scenarios

Virtualization of disaster recovery site resources can be of benefit even if only a few critical servers are protected. Figure 7 and Figure 8 illustrate multiple standalone servers or a combination of cluster and standalone servers can easily be replicated to a reduced set of hardware at a DR site.

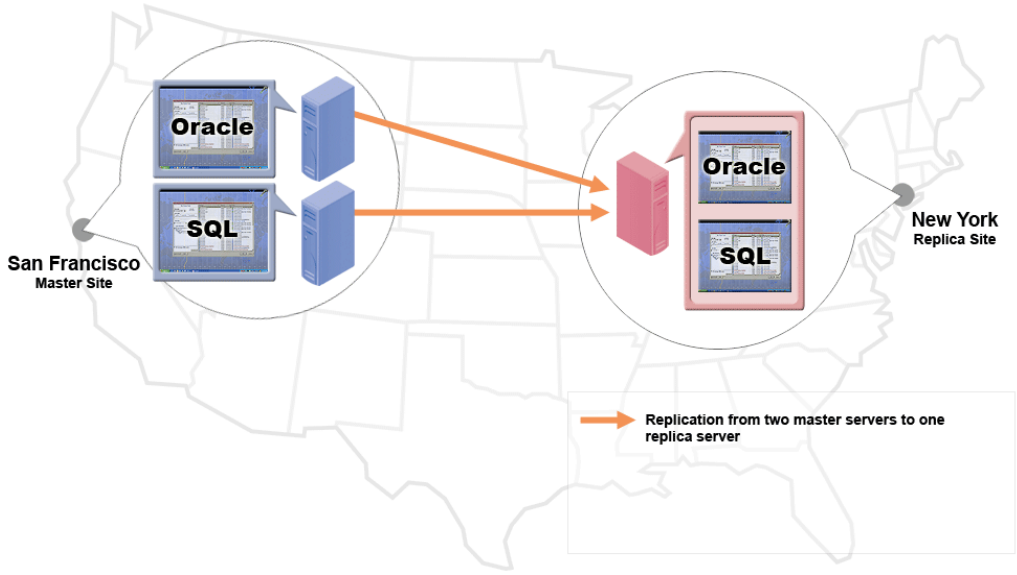

Figure 7: Basic DR virtualization

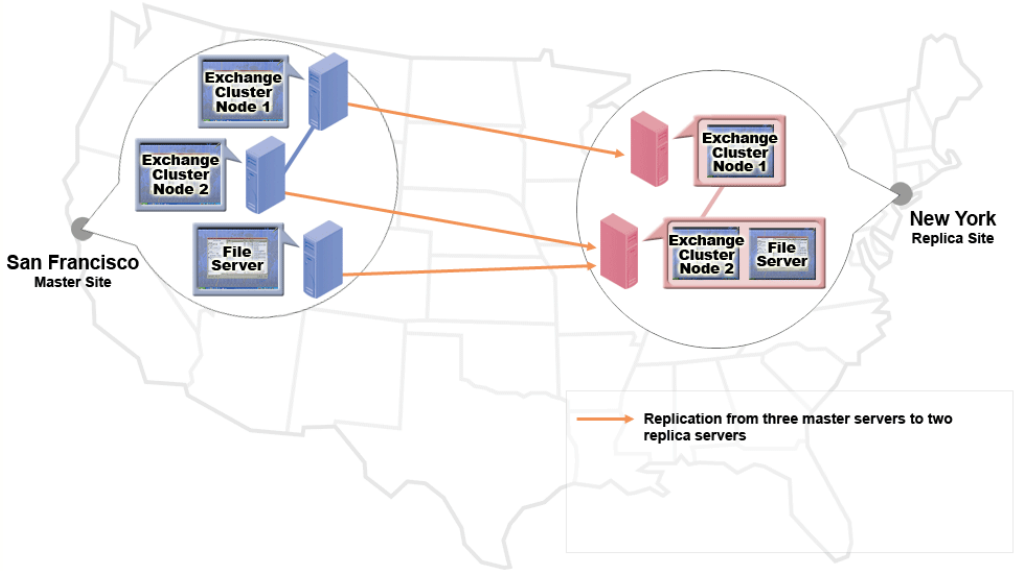

Figure 8: DR virtualization of a combination of standalone and cluster servers

The real power of VMware Infrastructure is manifested when large number of systems require protection. Figure 9 shows fourteen physical servers on the production site, 3 two-node clusters plus 8 standalone servers, replicating to a single 3-node cluster at the DR site while preserving the exact cluster/standalone configuration of the servers at the main site.

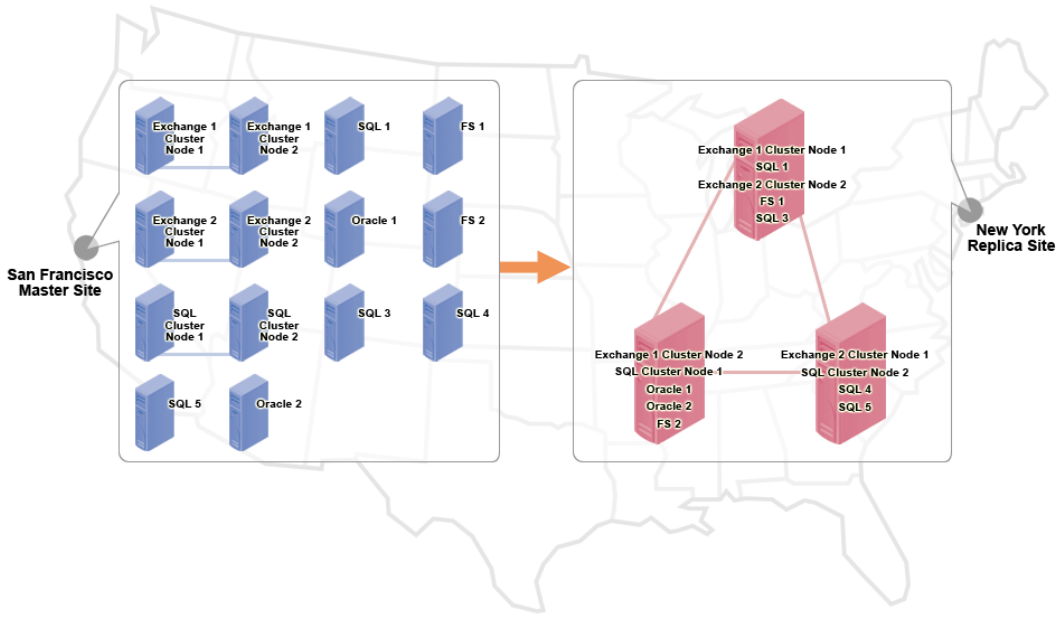

Figure 9: The power of physical to virtual virtualization

Figure 10 shows a virtualization configuration that is virtual to virtual in which both production and disaster recovery sites are virtualized illustrating the full power of virtualization.

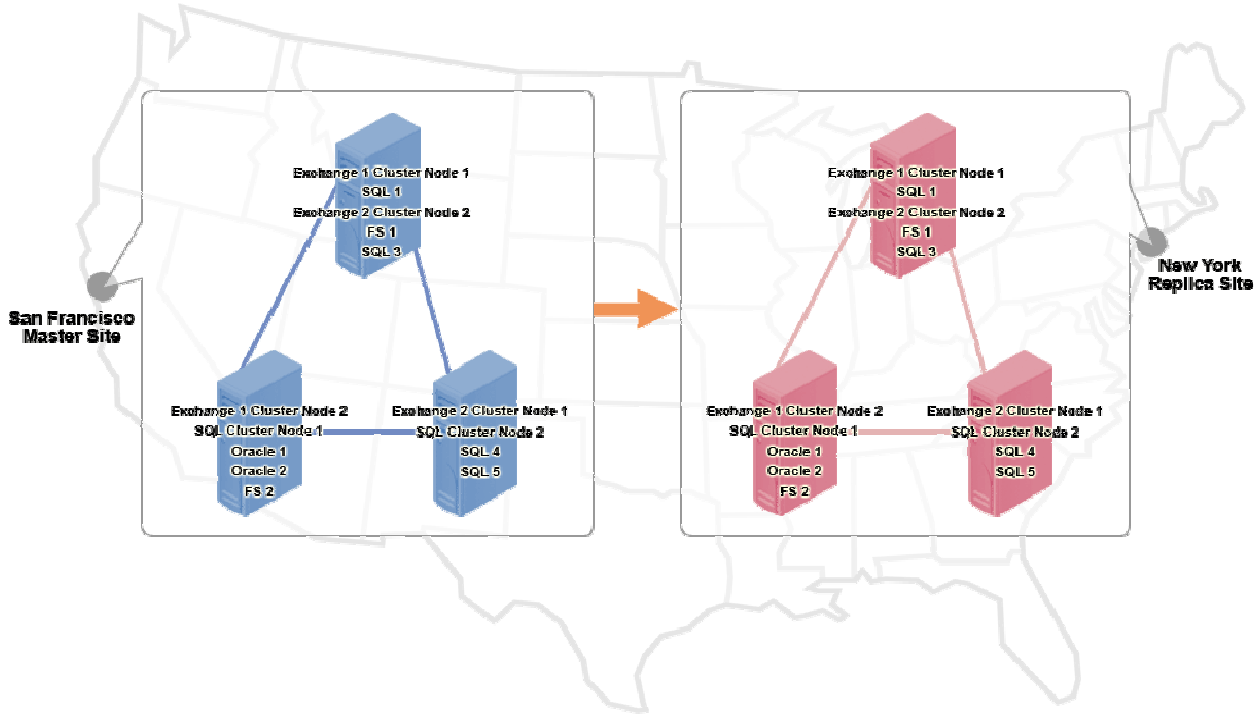

Figure 10: Virtual to virtual virtualization

Additionally, the high availability capabilities of VMware Infrastructure provide powerful additional protection at the DR site. Figure 11 illustrates the use of VMHA to recover failed virtual servers and *all* their applications to other resources – unlike traditional application clustering, switchover is not restricted to a single clustered application.

Finally, the ability to capture the running state of a virtual machine in a small set of files that can be copied locally to independent storage provides yet another level of protection against server *or* storage failure at the DR site.

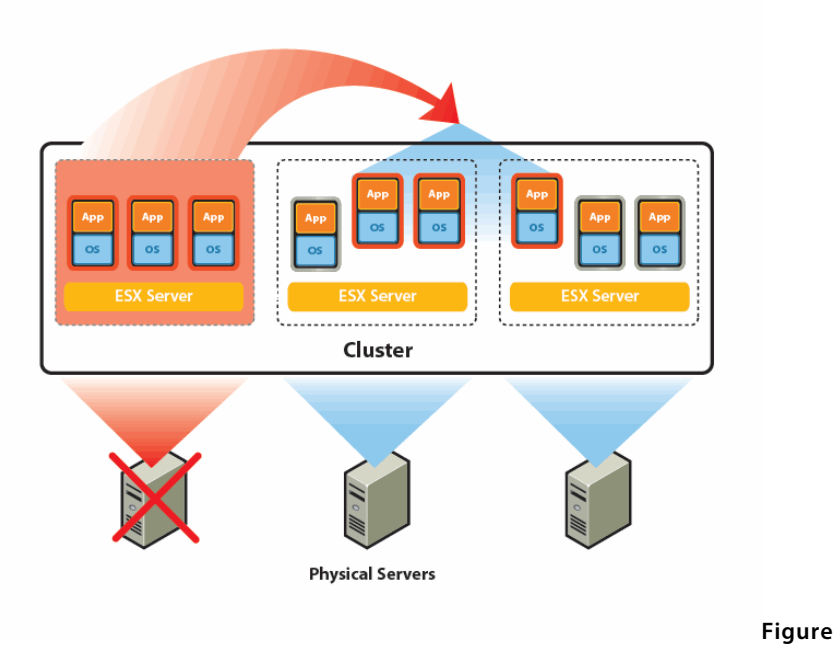

Figure 11: VMHA at work

Conclusion

By employing WANSyncHA to provide high-availability protection for mission-critical servers through switchover to a DR site that is powered by VMware Infrastructure, organizations can reduce costs dramatically at the same time that they significantly increase the robustness of the overall solution. This new solution enables organizations to gain multiple powerful layers of protection, including

- Over-the-WAN replication and switchover
- Regular recovery testing without disruption.
- Continuous data protection against corruption
- VMHA for simple, cost-effective local clustering of DR-site servers
- Virtual machine snapshot and copy for rapid alternative recovery at the DR site

The combination of the two technologies offers an antidote to the out-of-control growth in cost and complexity of disaster recovery and business continuity protection as it is extended to growing numbers of critical servers.

About VMware

VMware® was founded in 1998 to bring virtual machine technology to industry-standard computers. VMware delivered its first product, VMware Workstation, in 1999 and entered the server market in 2001 with VMware GSX Server and VMware ESX Server. With the groundbreaking launch of VMware VirtualCenter and VMware VMotion™ in 2003, the company established itself as the leader in virtual infrastructure technology by introducing a new category of data center capabilities. In 2004 the company extended the capabilities of virtual infrastructure to the enterprise desktop with the introduction of VMware ACE. With the launch of VMware Player in late 2005 and VMware Server in early 2006, VMware introduced the first free commercially available virtualization products for users new to virtualization. In June 2006, VMware introduced VMware Infrastructure 3, the industry's first complete infrastructure virtualization suite to deliver comprehensive virtualization, management, resource optimization, application availability and operational automation capabilities in an integrated offering.

Please visit http://www.vmware.com.

About CA XOsoft

CA has extended its storage management portfolio with the acquisition of XOsoft, Inc. The acquisition enables CA to offer a complete recovery management solution that allows customers to reduce the risk of data loss, reduce the time spent on backups and accelerate recovery of critical business services. CA will integrate XOsoft's products with BrightStor ARCserve Backup to deliver a complete solution for protecting and recovering critical applications. Using XOsoft's patented technology, CA also will develop a next-generation information protection platform to unify and simplify enterprise recovery operations.

XOsoft develops and markets Continuous Application Availability software solutions that minimize application downtime and accelerate time to recovery.

Founded in 1999, XOsoft is a leading provider of continuous application and information availability solutions that fully address business continuity, disaster recovery, continuous data protection and content distribution needs. XOsoft products ensure uninterrupted access to all types of file and application servers, including Microsoft Exchange, Microsoft SQL, Microsoft IIS, and Oracle, and allow instantaneous recovery from any type of disaster.

Please visit http://www.caxosoft.com.

VMware, Inc. 3145 Porter Drive Palo Alto CA 94304 USA Tel 650-475-5000 Fax 650-475-5001 www.vmware.com

vmware®