

Business Continuity and Disaster Recovery with CA Recovery Management and VMware Infrastructure

CA Recovery Management Team



Table of Contents

Executive Summary		SECTION 4: CONCLUSIONS	16
SECTION 1: CHALLENGE	2	SECTION 5: REFERENCES	16
The Importance of Flexible, Cost-effective BC and DR			
The Increasing Expense and Complexity of Data Recovery			
SECTION 2: OPPORTUNITY	4		
Reducing Cost and Complexity			
VMware Infrastructure			
VMware ESX Server			
VMware Infrastructure Components That Support BC and DR			
CA Recovery Management			
Maximizing Availability for Virtualized Servers			
SECTION 3: BENEFITS	15		
Protecting Physical and Virtual Servers Across the Enterprise			

Executive Summary

Challenge

The expansion of IT systems to support the growth of mission-critical business processes and services is fueling two parallel trends. One is the increase in the deployment of new applications and the provision of access to them and their information in ways that are economical, flexible, fast and well managed. The other is an increase in the implementation of business continuity (BC), disaster recovery (DR) and high availability (HA) initiatives aimed at safeguarding these applications. As such, many organizations are particularly challenged with simultaneously supporting and protecting their growing farms of mission-critical business applications with cost-effective BC and DR programs.

Opportunity

Organizations need powerful and affordable solutions for maintaining continuous availability of applications that enable critical IT processes via data protection, business continuity and high availability, necessitating broad coverage of all major contingencies on all servers. To address these difficult issues, a new and combined offering from CA and VMware provides a novel, integrated approach to application and server provisioning. This approach reduces total cost and complexity, while increasing application availability and augmenting information safety.

Benefits

CA Recovery Management and VMware Infrastructure help you effectively respond to the challenges and opportunities of business-critical computing. Specifically, the combined solution leverages the strengths of two powerful software management systems to:

- Enable you to rapidly and economically deploy physical and virtual servers
- Provide a multi-layered disaster recovery system that addresses a wide array of contingencies
- Help organizations of any size to reduce management complexity, operating costs and power and cooling requirements, all while increasing server and application availability and reliability

The Importance of Flexible, Cost-effective BC and DR

Today, organizations of all sizes and types depend heavily upon their IT resources to survive and thrive in an increasingly competitive marketplace, which is why they require the ability to rapidly and economically deploy BC solutions to protect the technologies that run their mission-critical applications.

Any time the IT systems that power core business processes are disrupted, the negative impacts and risks multiply quickly and can include:

- Reduced revenues when clients and partners cannot reach key business systems or services
- Diminished productivity because employees are unable to work
- Decreased stock valuations from a lack of investor confidence
- Lost opportunities due to defecting customers

And while you may consider the likelihood of a major disruption highly improbable, the picture changes when you allow for the entire range of potential causes, such as:

- Viruses, Trojan horses, and worms
- Fiber cuts
- Application faults
- Administrator and user errors

Individually and together, these risks represent significant threats to your operations — and identify events from which you sometimes never recuperate. If a major disaster occurs, the very existence of your business is in jeopardy — especially if recovery takes days or weeks — rather than minutes or hours.

But, providing cost-effective and robust BC coverage is not a simple task. After all, enterprises must be able to deploy new applications and servers swiftly and inexpensively, manage them effectively, defend them against unplanned downtime and ensure that they can recover quickly from disruptions.

These requirements are fueling the growth of virtualization. In fact, at many enterprises, reducing the number of physical servers to be managed directly results in more effective support of BC and DR initiatives, according to market-watchers The Aberdeen Group. In a recent survey of more than 300 IT and business decision-makers, The Aberdeen Group found that a significant portion of the respondents attributed improvements in BC, DR and application availability directly to virtualization.¹ And, this link underscores the business value of maximizing protection and resiliency for virtualized systems.

The Increasing Expense and Complexity of Data Recovery

In spite of, or perhaps because of, virtualization IT systems are becoming more numerous and complex. As improvements in productivity and business processes arising from the use of new technologies often lead to rising expectations for customers, management, employees and investors, significant advances quickly become the new baseline against which day-to-day performance is measured. In turn, this pushes the expectations of these supporting systems to provide continuous application and data accessibility. In other words, the sheer increase from just a few critical servers to larger numbers of application, content, database, web and other specialized servers complicates management and protection for IT.

Specific problems around safeguarding these systems are twofold. First, as illustrated in Figure A, providing even the most basic business continuity protection for servers can be an expensive proposition. As availability requirements increase, so does the cost of purchasing and maintaining associated and necessary solutions.

Second, as the number of servers increases, so do the availability requirements placed on these systems. As shown in Figure A, this likewise increases the number of systems that fall into the top tiers of protection, amplifying complexity. Added complexity also comes from the need to install and maintain a significant numbers of duplicate systems with all of the attendant management issues. These include the need to perform regular upgrades in sync with (and without disrupting access to) production systems, as well as infrastructure issues, such as heating and power management problems.

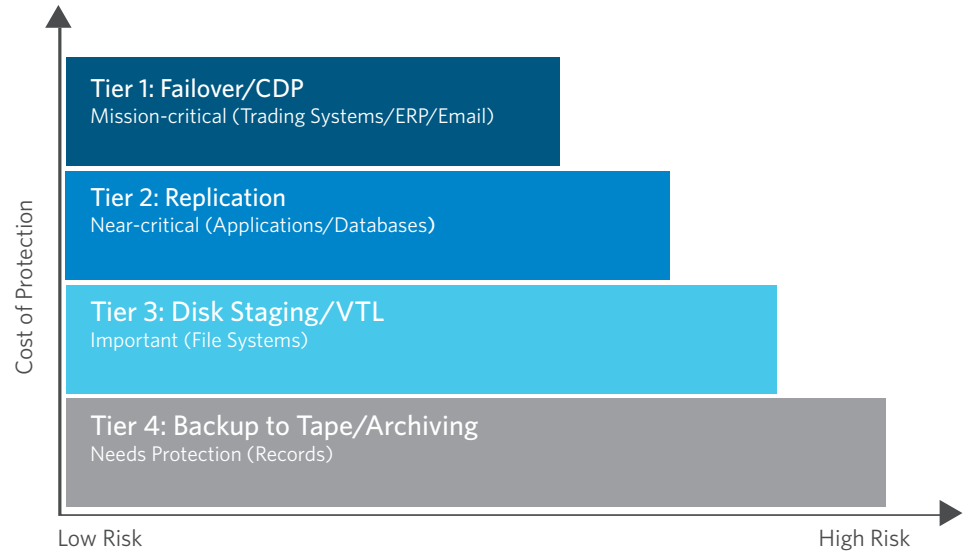
And, complexity is further exacerbated because high availability systems and processes do not typically reduce necessary protection levels, but are usually added to adequately augment them. For example, backups remain essential, even with a new switchover system in place.

And finally, another source of complexity arises from potential failures in the DR systems themselves and by virtue of the amount of servers being protected. With just a few servers, probability is low that backup systems will experience a problem at the same time that the primary site goes down. With a larger number of systems, however, that likelihood increases until, at some point, it becomes a near certainty. And, the growing use of virtual servers is dramatically accelerating the magnitude of this challenge at many organizations.

In summary, as the number of servers requiring BC and DR increase, so do the cost and complexity of deploying and managing protection solutions. But, this does not imply that organizations gain greater resilience to disasters with more involved solutions. And in fact, many experts maintain that you place yourself at greater risk due to the very nature of the complexity.

FIGURE A

THE COST OF BC PROTECTION INCREASES ALONG WITH RISK



SECTION 2: OPPORTUNITY

Reducing Cost and Complexity

By removing the traditional limitations of physical infrastructures, VMware Infrastructure allows you to deploy dynamic real-time infrastructures that are agile and can easily adapt to changing business needs. And, you can leverage VMware Infrastructure in conjunction with CA Recovery Management to economically deploy a flexible and dynamic BC, DR and high availability solution that addresses these unique — and dynamic — requirements.

VMware Infrastructure

As shown in Figure B, virtual infrastructure is that which links physical IT resources to your business and its key processes, providing the same connection that the physical infrastructure does but in a more flexible and cost-effective manner.

Virtualization is a layer of abstraction between physical hardware resources, the operating system and the applications that make use of them. By decoupling the operating system from the underlying hardware, virtualization enables multiple virtual machines (VMs) to run simultaneously on a single physical set of hardware and provides far better resource utilization and agility.

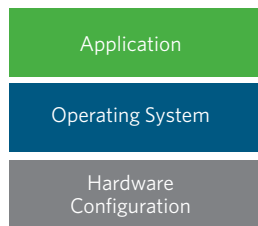
VMware Infrastructure transforms industry-standard physical servers, their attached networks and storage media into flexible bands of resources that administrators can dynamically map to various business needs. The result: decreased costs, increased efficiencies and enhanced responsiveness.

Moreover, VMware Infrastructure allows administrators to deploy applications and services on any server and easily move between them when necessary. Specifically, VMware Infrastructure treats the IT infrastructure as a pool of computer, storage and networking power and provides comprehensive and universal management tools to leverage that pool. As a result, the IT infrastructure becomes more manageable, more efficient and more easily deployable and serviceable — *all at a lower cost*.

VIRTUALIZATION DECOUPLES SOFTWARE AND HARDWARE ELEMENTS FROM THE SERVER ARCHITECTURE

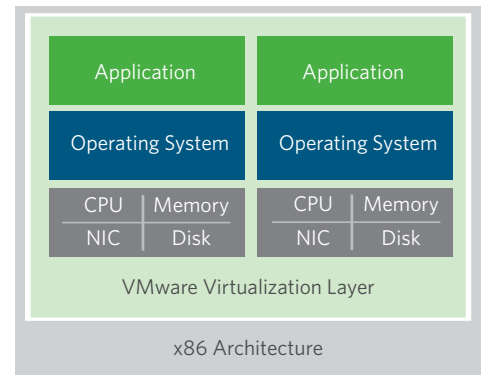
FIGURE B

Before Virtualization



- Software tied to hardware
- Single operating system image per machine
- One application workload per operating system

After Virtualization



- Multiple workloads per machine
- Software independent of hardware
- System, data and applications are files

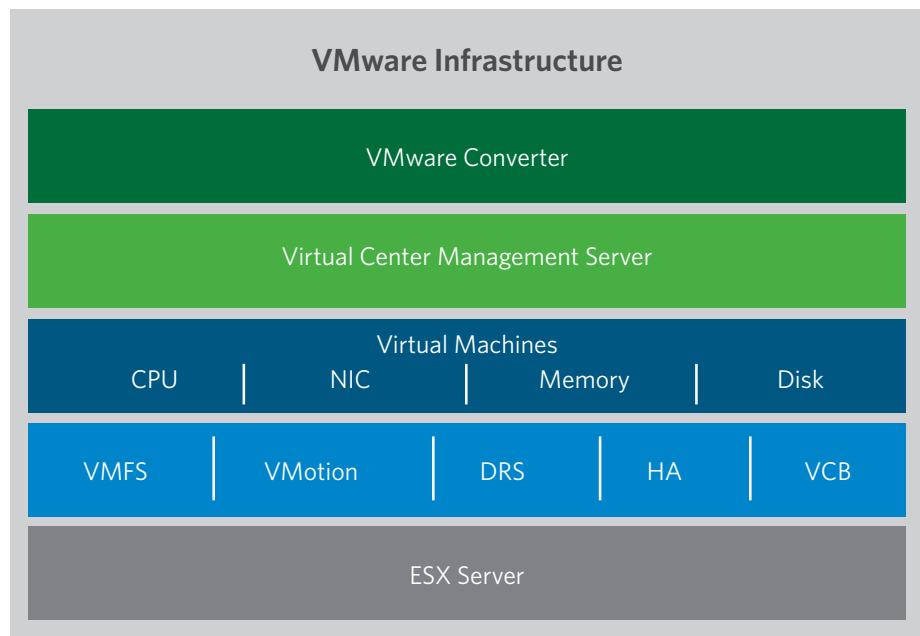
VMware ESX Server

At the core of VMware Infrastructure is the ESX Server; software that powers the virtualization features of the solution. As illustrated in C, each virtual machine is a true representation of an x86 computer — complete with processor, memory, networking interfaces and storage devices.

The VMware virtualization layer offers each VM direct access to the underlying x86 processor, which is a critical distinction from hardware emulation approaches because it means that the solution is able to match the performance of a traditional server with all hardware dedicated to a single copy of the operating system.

FIGURE C

THE VMWARE INFRASTRUCTURE ARCHITECTURE IS BASED ON MAINFRAME TECHNOLOGY



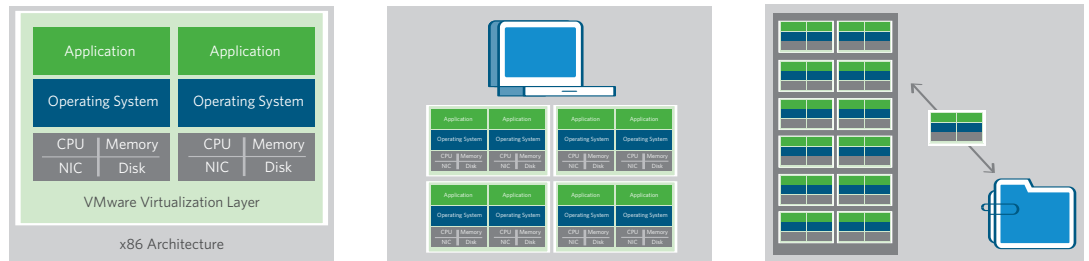
Virtual machines are a well-proven concept first deployed on mainframes, and VMware applied the very same VM model to lower-cost hardware platforms to help address the more recent problems of server proliferation and server resource under-utilization. These issues arose from the growth of highly distributed, loosely coupled IT and business infrastructures and as a result of the need to run critical applications atop dedicated, often disparate operating systems. Thus, VMware's unique technology can efficiently virtualize x86 systems 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, which means that a host operating system does not need to be installed for ESX to work. In fact, ESX Server is the VMware kernel that installs directly on the hardware. This kernel is also known as the “virtualization layer” that provides the hardware abstraction for server virtualization. Moreover, because ESX Server removes the need for a host operating system, its brand of virtualization is more efficient.

As illustrated in Figure D, virtualization offers three key classes of features; partitioning, isolation and encapsulation. And, a brief exploration of these features helps explain in detail how virtualization can assist you in improving resource utilization and server security and manageability.

THE THREE BENEFITS OF VIRTUALIZATION ARE IMPROVED RESOURCE UTILIZATION AND SERVER MANAGEABILITY AND SECURITY

FIGURE D



Partitioning

- Run multiple operating systems on one physical machine
- Fully utilize server resources
- Support high availability as shared data is cluster ready for failover and redundancy

Isolation

- Isolate faults and security at the hardware level
- Dynamically control CPU, memory, disk and network resources per VM
- Guarantee service levels

Encapsulation

- Encapsulate the entire state of the VM in hardware-independent files
- Save the VM state as a snapshot in time
- Re-use or transfer whole VMs with a simple file copy

PARTITIONING FOR IMPROVED RESOURCE UTILIZATION

With VMware, 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, with VMware, the VMs 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 among virtual machines. And, the networking and storage features of VMs 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 operating systems to run simultaneously on a server, it dramatically improves hardware resource usage. With a typical ratio of about four to eight VMs running per physical server, hardware utilization can be significantly increased without sacrificing overall performance. And, more effective usage, in turn, translates into reduced operating costs and better returns on your hardware investment.

ISOLATION FOR IMPROVED SECURITY

The VMware 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 VMs from one another and from the monitor, resulting in strong separation of one operating environment from another. Moreover, here is no common component, which means all sharing takes place at the virtualization layer.

The advantage of isolation is that applications in one virtual machine can encounter failures without affecting other virtual machines. By separating faults and security at the hardware level and dynamically controlling CPU, memory, disk and network resources for each VM, VMware's virtualization technology removes end-user objections to server consolidation. More importantly, VMware Infrastructure allows IT administrators to guarantee service levels and security — even in a shared-resource environment.

ENCAPSULATION FOR IMPROVED MANAGEABILITY

To VMware, encapsulation means that the complete state of a VM — including related memory, disk storage, I/O device, CPU state and virtual hardware configuration information — is stored in a small set of files. And, these files are hardware independent. Therefore, a VM image can be moved from one physical server to another and will run without modification as long as the virtualization layer is present. This is true 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 specific point in time. Such an encapsulated image can be saved and reverted to at any time. And by storing the image in machine-independent files, IT staff can copy, save and move virtual machines wherever and whenever needed — simply by copying a directory of files.

VMware Infrastructure Components That Support BC and DR

While ESX Server is a key component of VMware Infrastructure, many others must also be added in order to deliver a true virtual infrastructure solution. Thus, VMware Infrastructure offers several unique capabilities in support of truly dynamic mapping of resources to needs, as well as BC and DR, including VMware VMotion and VMware High Availability (HA).

VMware VMotion is 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. This easy movement of VMs from one physical server to another helps IT organizations to maximize availability and resource usage.

Another important component is VMware HA, which helps to keep virtualized environments and their supported applications and services highly available in the face of failures or threats. If a physical server in a resource pool fails, virtual machines running on that server are restarted on another server. This high availability function constantly monitors and manages capacity utilization and reserves spare capacity to restart virtual machines when needed.

VMware HA is operating system-agnostic and easy to manage, and because it is part of the ESX Server software it does not need to be installed on the guest operating system. (It is important to note that VMware HA can move VMs in case of physical server failure, but not application failure in the virtual environments themselves.)

CA Recovery Management

CA Recovery Management is a solution that offers several powerful options for protecting servers provisioned and managed with VMware Infrastructure, including traditional backup (D2D2T), with over the WAN data replication, “push-button” or automated failover, continuous data protection (CDP) and the industry’s first fully automated DR testing option.

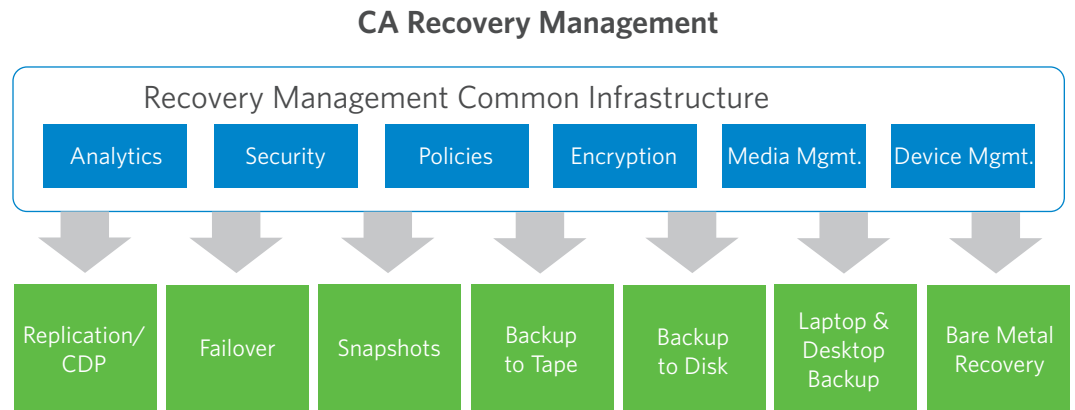
Because CA Recovery Management uniquely combines powerful data protection technologies, it provides you with multi-layered protection of business-critical data and applications. And as shown in Figure E, the solution also simplifies and automates both the security and recovery of data in multi-vendor, multi-platform heterogeneous storage and server environments.

Finally, the software focuses on protecting applications and services — not just data — and incorporates all the technologies required to ensure continuity of IT services. Plus, it is a solution that allows organization to safeguard their critical applications and data according to their value to their business.

Under this solution platform, CA Recovery Management integrates CA ARCserve® Backup for comprehensive high-performance backup, along with CA XOsoft™ products for continuous application availability and disaster recovery. It does so with a single, centralized interface that allows IT administrators to easily review backup policies, data replication and recovery options across small or large distributed server farms.

More importantly, CA Recovery Management builds upon VMware’s Infrastructure to extend the benefits and capabilities of both solutions, thereby providing you the ability to build cost-effective and flexible BC and DR solutions for your environment.

To help, CA has developed application-specific solutions for major applications like Microsoft Exchange Server, Microsoft SharePoint Server, Microsoft SQL Server, Oracle, Microsoft Internet Information Server (IIS) Web servers, Research In Motion (RIM) Ltd. 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 offerings 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, automatically creating a standby application to match the production system.



Maximizing Availability for Virtualized Servers

Figure F illustrates how CA XOsoft™ High Availability™ works to make and keep virtual servers highly available, regardless of the type of threat. 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 it becomes necessary.

Underlying this solution is a powerful asynchronous host-based software replication engine that transfers changes of 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 and ensures the integrity of the replicated data, including emails, database updates, file operations and other content.

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 is due to the use of asynchronous replication in order to eliminate distance restrictions on the location of the secondary system.

As it performs data replication, the CA XOsoft High Availability software continuously monitors the state of the production server. More than a simple ping, the system checks both the accessibility of the server and the state of the application and in order to ensure that all necessary application services are running and the application data registers as valid.

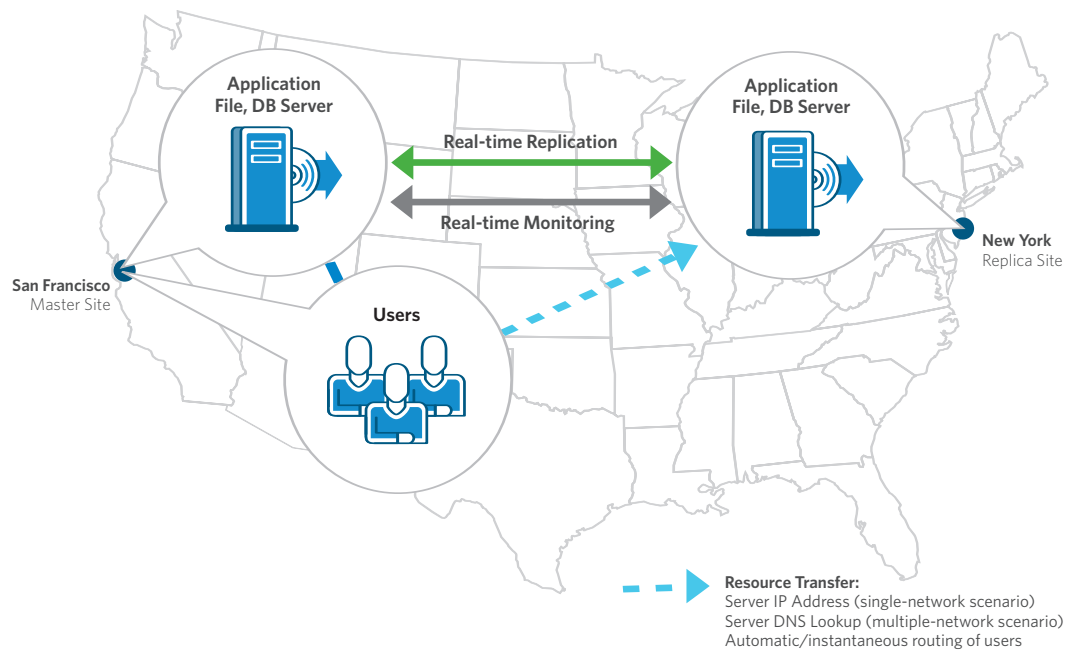
When the system detects a problem with the production server, CA XOsoft alerts the IT systems administrator. Alerts can be sent via the GUI event window, email, system logs or other means. If the replica site must take over servicing users, a fully automated transparent switchover can be triggered automatically or with a single push of a button by the IT administrator — depending on how you choose to configure the system.

In either case, once the change is triggered, CA XOsoft initiates the application on the replica server and performs all the necessary actions to redirect users to that server. No client-side configuration is necessary and the entire process takes just a few minutes — and just the time required to start the application on the secondary server.

Once the production system and site are back up and running, the two servers can be resynchronized via the same process. And 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 changeover.*

FIGURE F

CA XOSOFT HIGH AVAILABILITY KEEPS VIRTUAL SERVERS CONTINUOUSLY AVAILABLE



GUARDING AGAINST DATA CORRUPTION

A backup server is of no value if it stores corrupted data, which can be unintentionally replicated along with valid data. But because CA XOssoft Continuous Data Protection (CDP) features true CDP technology, it captures and replicates all changes, thereby allowing you to go back to any point in time to recovery data. This type of CDP technology gives you flexible recovery point objectives that are not isolated to previous states of backups (daily, weekly) or snapshots. Without doubt, CDP gives you an extra layer of protection; it lets you recover not just from server or storage failures, but from data corruption, as well. If data corruption occurs due to human error, a virus or a software error, the affected data is replicated on the secondary server. If the error causes the production server to go down, all backup systems will also be unavailable and for the same reason.

With CA XOssoft's Rewind capability, it is still possible to recover. The data on the replica server need only be "rewound" to a time immediately before the corruption event occurred, allowing valid data to be recovered. This capability provides you with greater control over your recovery point objectives (RPOs) and your recovery time objectives (RTOs.)

AUTOMATING TESTING

No matter how well a solution is tested when it is installed, it may fail later because of changes in the IT environment. These changes may include hardware replacements, software upgrades, network reconfigurations, or simply the growth of the dataset size and a gamut of threats a server may be exposed to, such as Active Directory or DNS issues. It is vital, therefore, that your IT administrators regularly test business continuity systems to ensure their continued integrity.

The problem is, testing is disruptive and expensive. Even the most basic check requires some disruption to protection and IT staff time and to application availability for users. For this reason testing is performed all too infrequently, leaving potential issues with standby systems unnoticed until a real failure occurs. And when this happens, full recovery can take days, weeks or longer, casting doubt upon an enterprise's very ability to survive. According to various industry pundits, as many as 50 percent of companies that experience a sustained outage never fully recover and go out of business.

The ideal solution, illustrated in Figure G, is a way to test the application on the replica server that takes over the production server's responsibilities if a switchover occurs. IT administrators may want to shift one or more test users in a way that does not impact the availability of the production server or compromise the safety the DR system provides.

CA XOssoft™ Assured Recovery™ option provides an automated disaster recovery testing capability that helps you ensure successful recovery in the event of an unavoidable disaster. CA XOssoft Assured Recovery is not testing through simulation. Rather, it is a technology that allows you to perform a real test of your disaster recovery server by running the actual standby application — even modifying data — without impacting your production environment or disrupting protection in any way. This option can be used with CA XOssoft™ Replication™ or CA XOssoft High Availability and provides out-of-the-box support for Microsoft Exchange, SQL Server and IIS web servers, as well as Oracle database servers. And, support for other applications or advanced customization can be easily added through simple scripts or batch files. Regardless, both manual and fully automated scheduled testing is performed without any disruption to production users or interrupting real-time data protection.

You can configure CA XOssoft Assured Recovery to schedule automated testing as often as once an hour, or activated manually at any time. In either case, when testing commences a point-in-time, a snapshot copy is taken of the production data that resides on the replica without interrupting the replication process or impacting the replica server in anyway.

As a first step, the application is started on the replica server at which point CA XOssoft Assured Recovery proceeds to verify that all services start and all databases properly mount (the simplest test that can be performed right out of the box). Furthermore, IT administrators can also create and register scripts to perform additional and customized testing. And fully interactive testing is also allowed. For example, in the case of Exchange, an IT administrator can interactively switch over a single test user to the replica server using the same processes as in a real switchover, test the system by sending and receiving several emails, then when testing is completed, switch the test user back to the production server.

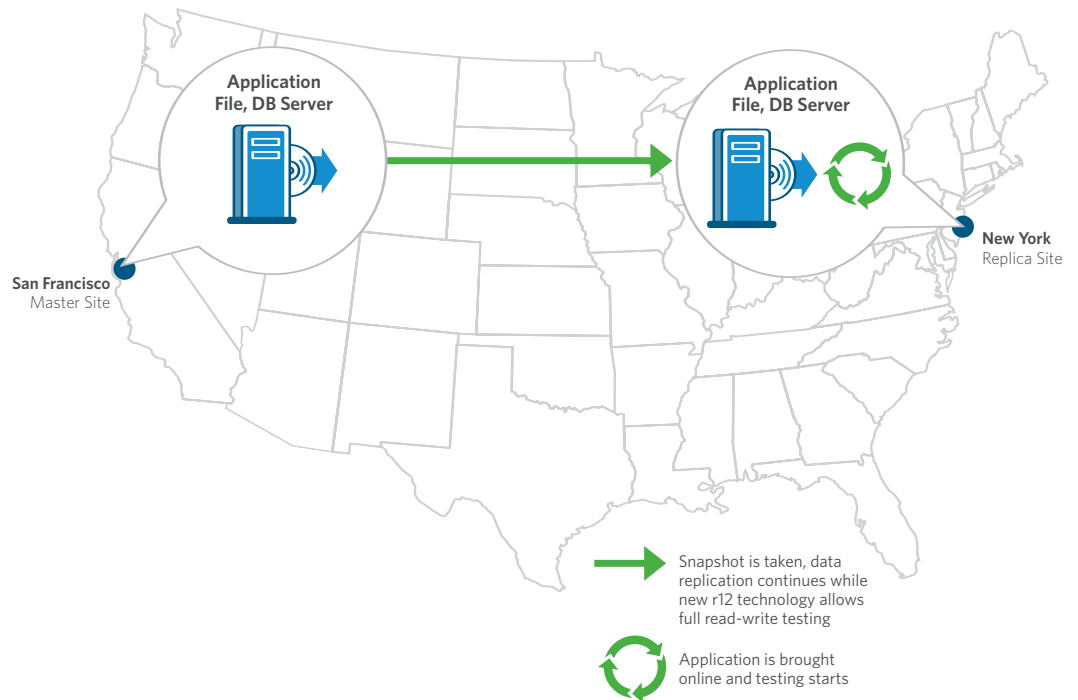
For many applications, including email and databases, starting the application causes data to be written and takes the replica server out of sync with the production server. This is not a problem with CA XOssoft Assured Recovery, however, because it uses a snapshot copy of the production data that later gets discarded to perform its testing. As such, it uses less space and allows you to test using live information. While this is a true test of the replica system, it could ordinarily not be performed unless you stopped replication during the test and then resynchronized the data, an approach that is time-consuming, involves user downtime and risks the system by leaving it unprotected during the test. But with CA XOssoft 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.

And once testing is completed, the software allows you to automatically trigger a backup or VSS snapshot of the newly validated data. CA XOssoft Assured Recovery supports any backup software, including the fully integrated CA ARCserve Backup, allowing you to eliminate your backup window on your production servers by taking backups off the replica and providing support for offsite backups without the cost or complexity of transporting tapes. And although Assured Recovery is not required to initiate backups from the replica server, it is considered a best practice to backup a known good recoverable version of your data and to ensure a greater level of security for recovery efforts.

Also important to note is that CA ARCserve Backup seamlessly integrates with VMware's Virtual Consolidated Backup (VCB) capability, which helps you further reduce the complexity of backups in virtual environments.

FIGURE G

CA XOSOFT ASSURED RECOVERY TESTS PRODUCTION DATA ON THE REPLICA SERVER



Protecting Physical and Virtual Servers Across the Enterprise

CA Recovery Management solutions complement the management and protection features of VMware Infrastructure to offer powerful protection and recovery of your physical and virtual servers across the entire enterprise. These features make the combined solution ideally suited to ensure comprehensive business continuity and disaster recovery while delivering on the promise of easy management, reduced costs and decreased complexity.

Moreover, the technologies work seamlessly and synergistically to provide more benefits than possible with either solution alone, including:

VIRTUAL INFRASTRUCTURE FOR EFFECTIVE RESOURCE UTILIZATION VMware Infrastructure technology improves the use of hardware resources, reduces power and cooling requirements and significantly eases server management. With policy-based load balancing enabled, resources are used optimally and efficiently. Virtualization-enabled hardware consolidation can be implemented at the primary site only, at the secondary site only or at both sites. And by simply changing the consolidation ratio of VMs per physical server, you can eliminate the cost of replicating the entire hardware environment at the primary site.

SEAMLESS REPLICATION AND SWITCHOVER CA Recovery Management provides distance-independent data replication, CDP, application monitoring and automated failover. These features, when combined with those of VMware Infrastructure, help 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.

AUTOMATED DR TESTING AND OFFSITE BACKUP CA Recovery Management allows organizations to conduct daily or even more frequent tests of application recoverability at a remote disaster recovery site. In addition, integration with snapshot and backup means that IT can produce offsite backups of validated data without the additional cost and complexity of transporting tapes.

REDUNDANT CONNECTIVITY VMware HA features support for redundant network and storage connectivity with fault isolation that protects the server infrastructure from hardware failures. When VMware HA is implemented at the primary and/or secondary site, you can recover vital business processes quickly and keep your servers and applications available through component failures.

SECTION 4: CONCLUSIONS

Enterprises can employ CA Recovery Management solutions to provide business continuity and disaster recovery protection for mission-critical servers through switchover to a DR site that is powered by VMware Infrastructure. Using this approach, you can dramatically reduce costs, while significantly increasing the robustness of your overall IT infrastructures and BC/DR initiatives.

The combined solution enables you to deploy and manage physical and virtual servers — and the applications, services and information they support — economically and flexibly. The solution also offers multiple and powerful layers of protection, including:

- Over-the-WAN replication and switchover
- Automated DR testing without disruption
- CDP to protect against data corruption
- VMware HA for simple, cost-effective local clustering of DR site servers
- VM snapshot and copy features for rapid alternative recovery at the DR site

As such, the combination of VMware Infrastructure and CA Recovery Management counteracts the rising cost and complexity of BC/DR and IT resource provisioning as business-critical IT infrastructures change. Even more important, the solution can help build and evolve highly available, affordable, energy-efficient, resilient and secure computing foundations for sustained business growth.

SECTION 5: REFERENCES

The Aberdeen Group, September 2007. *Are You Protected? Virtualization and Business Continuity*.

To learn more about CA Recovery Management and VMware Infrastructure, visit ca.com/recovery and vmware.com.

Notes

CA (NYSE: CA), one of the world's leading independent, enterprise management software companies, unifies and simplifies complex information technology (IT) management across the enterprise for greater business results. With our Enterprise IT Management vision, solutions and expertise, we help customers effectively govern, manage and secure IT.

MP327470308

Learn more about how CA can help you transform your business at [ca.com](https://www.ca.com)

