

Using Replication and Virtualization for Business Continuity

Table of Contents

Executive Summary	3
<hr/>	
SECTION 1: CHALLENGE	7
The Obstacles to Business Continuity	7
Key Challenges for Maintaining Business Continuity	7
Data Replication Technologies	9
Requirements for Effective Data Replication	10
Server Virtualization Technologies	12
Requirements for Effective Virtualization Deployments	15
Summary of the Challenge	17
<hr/>	
SECTION 2: OPPORTUNITY	17
Using CA Technologies to Maintain Business Continuity	17
CA XOssoft Replication	17
CA XOssoft High Availability	19
CA XOssoft Assured Recovery	21
CA ARCserve Backup	22
<hr/>	
SECTION 3: BENEFITS	26
Benefits of CA Technologies for Business Continuity	26
<hr/>	
SECTION 4: CONCLUSIONS	29
<hr/>	
ABOUT CA	BACK COVER

Copyright © 2008 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. To the extent permitted by applicable law, CA provides this document "As Is" without warranty of any kind, including, without limitation, any implied warranties of merchantability or fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document including, without limitation, lost profits, business interruption, goodwill or lost data, even if CA is expressly advised of such damages.

Executive Summary

Challenge

Organizations face a number of challenges to business continuity and application availability, such as volumes of data and application complexity, demands for round-the-clock operations, and server proliferation. Data replication can meet many of these challenges, but must be properly used and meet certain standards, if it is to be of benefit. Server virtualization is becoming widely used because of benefits such as reduced hardware and power costs, but needs its own protection technologies. Virtualization can also be an important recovery management and business continuity technology, if used with appropriate management and backup tools.

Opportunity

CA XOssoft™ technologies support your business continuity and application availability goals through replication and failover tools, and through support for server virtualization. CA replication and virtualization support technologies are included in:

- CA XOssoft Replication r12, which provides continuous data protection
- CA XOssoft High Availability r12, which provides data protection and application failover
- CA XOssoft Assured Recovery r12, which provides automatic disaster recovery testing

Additional virtualization support technologies are included in: CA ARCserve® Backup r12, which provides secure permanent data backups and disaster recovery tools.

Benefits

CA XOssoft™ Replication, CA XOssoft High Availability, and CA XOssoft Assured Recovery provide a range of benefits to help meet the requirements for effective data replication, such as:

- Protection against site unavailability
- Timely replication of data and prevention of data loss
- Reduction in backup overhead and provision of simple recovery procedures

CA XOssoft Replication, CA XOssoft High Availability, and CA ARCserve Backup® also provide a range of benefits to help meet the requirements for effective virtualization deployments, such as:

- Provision of cost-effective virtual system platforms
- Reduction of management complexity and simple backup and restore procedures for virtual machines
- Reduction in overhead and impact of virtual machine backups

The Obstacles to Business Continuity

Organizations are becoming more reliant on computer systems to support continuous business operations. Organizations also require resilient systems, which enable rapid recovery in the event of system failure and provide continuous business operations. Data replication and server virtualization technologies can help to support your business continuity objectives, but also have their own challenges to successful deployment.

Key Challenges for Maintaining Business Continuity

There are various key challenges that all organizations face when designing strategies to maintain business continuity and improve application availability, including increasing volumes of data, system and application complexity, availability, backup, and regulatory compliance.

DATA GROWTH

Email, file storage, and database storage requirements have increased as the cost of disk storage has reduced. The explosion in data growth has led to increased pressure on IT operations such as backup, trial restore operations, and disaster recovery testing. For some organizations, requirements for system availability have further reduced the time that is available to perform maintenance operations such as backup.

SYSTEM AND APPLICATION COMPLEXITY

System complexity has increased significantly with the requirement to support multiple operating systems, applications, and software to perform maintenance tasks such as backing up and restoring data.

Geographically dispersed applications, such as email systems that are hosted across geographically dispersed locations, present significant challenges for backup, restore, disaster recovery, and regular maintenance tasks.

REDUCING DOWNTIME

By minimizing the amount of system downtime when recovering from significant data loss events, IT departments can manage risk and reduce the effect that data loss has on their organization when a significant event occurs.

Recovery management has become more difficult as systems and applications have become more complex, data volumes have increased, and the number of servers has increased. Organizations require recovery tools that enable them to recover data quickly and easily, without needing to acquire additional support from external sources to complete the task. By providing backup tools that are easy to use and that provide the ability to restore data quickly, you can significantly reduce downtime for your organization.

ROUND-THE-CLOCK OPERATIONS

Business demands for round-the-clock operations can mean significant challenges for system administrators. Administrators must ensure that all of the necessary data is backed up and also ensure that the files are in a consistent state for future restore operations. The safest way to back up a file is to ensure that no one is accessing it during the backup period, however, this may require taking an application, file system, or database offline while the backup takes place. It is not always practical to take a system offline while a backup takes place, especially during automated backup operations.

SERVER PROLIFERATION

To support business requirements for new applications and services, the number of servers that are used within organizations has grown significantly. In addition, many software vendors recommend that you deploy their application onto dedicated hardware, so following these recommendations has led to further server growth. The proliferation of physical

servers in many organizations has led to significant increases in costs due to hardware support, power, cooling, and physical hosting requirements. To reduce operating costs, organizations have embraced virtualization technologies.

Virtualization offers the opportunity to support rapid business growth through easy and rapid deployment of servers and to benefit from increased server hardware utilization, while maintaining server performance. By using virtualization to align your storage infrastructure to your application requirements, you can help to reduce the operational cost of resource management and administration. Faster deployment and complete system recovery enable you to achieve improvements in the recovery and protection of your critical business data by using virtualization technology. However, virtualization requires different techniques to manage systems and meet high availability and disaster recovery requirements, so these techniques are often complex to implement and require significant effort from skilled IT staff.

BACKUP MANAGEMENT

You must ensure that you conduct regular backups for your systems, applications, and data, and that you can use these backups to recover in the event of a major catastrophe. By creating a single central data center for all of your servers and applications, you can remove the problems of performing remote backups. However, the cost of providing sufficient bandwidth for all of your users in remote locations may be prohibitive.

REGULATORY REQUIREMENTS

Organizations have experienced an increase in regulations that they must comply with. This increase in regulations has had a significant impact on IT operations with requirements to provide historical data; this has increased the need for more efficient archiving, recovery, and accessibility of data. Compliance requirements can be particularly costly and cumbersome to implement. Software that enables your organization to help meet compliance regulations can save significant time, effort, and money.

Data Replication Technologies

Data replication is one of the key recovery management techniques that can be used to help support your organization's business continuity objectives. Replicating data can help you to recover quickly from a single point of failure. By replicating data, you can maintain a copy of the critical data and use this copy to restore data rapidly in the event of a server or site failure. Replication is typically used in conjunction with more traditional backups, where replication is used to provide rapid access to recent data, and backups are used to create permanent archival copies.

You can replicate data by a number of methods including:

- Clustered server solutions that provide high availability.
- Bulk file copying between locations that provides timed snapshots for a point-in-time recovery solution.
- Asynchronous real-time data replication that copies changes in data from one server to another as the changes happen. Asynchronous replication can be used to provide continuous data protection (CDP).

Requirements for Effective Data Replication

Data replication is a powerful technique for protecting data and applications, but to be useful and provide effective tools to maintain business continuity and maximize application availability, certain requirements must be met, such as cost-effectiveness, environmental protection, timeliness, protection of data against loss, system and application consistency, awareness of overheads, and using simple recovery procedures.

COST-EFFECTIVE IMPLEMENTATION

The cost of providing replica hardware for replications and backup may be prohibitive for some organizations. For example, clustered solutions, although providing high availability, can be costly to implement and manage.

PROTECTION AGAINST SITE PROBLEMS

Any replication technology you use must be able to provide protection against site problems, such as power outage, flood, or fire. So, as well as protecting your sites by providing uninterruptible power supplies (UPS) and backup power sources, flood defenses, and fire control systems, you must also protect your data by ensuring that copies of data are maintained at more than one site. Server clustering, for example, although providing high availability, does not protect against site unavailability.

TIMELY REPLICATION

To provide CDP, you must ensure that you replicate data as soon as it changes. If there is a delay in data replication and the primary copy of the data is lost, your changes also are lost. By providing near immediate replication of changes, you can ensure that you provide CDP for your organization. Bulk copying, for example, provides a point-in-time recovery solution, but due to data changes between snapshots, this replication method inevitably means some data loss occurs when data corruption or accidental deletion takes place.

DATA LOSS

In the event of data loss, you must recover your system to the point-in-time when all of the data was present. This requires that you restore from your last available backup, which you may have taken the previous day, or that you use CDP to enable you to rewind your replicated data to just before the point when data loss occurred. However, you also need protection against data corruption, because corrupt data that is replicated becomes a corrupt backup. True CDP can rewind the replication process to a point-in-time just before the data corruption occurred. Some high availability solutions, such clustering, provide little protection against data corruption or data loss.

SYSTEM AND APPLICATION CONSISTENCY

You can replicate data relatively simply by copying files, however, this form of replication is only sufficient for basic document files that change infrequently. Complex applications, such as database and email solutions, require you to copy the entire application in a consistent state to ensure you can recover data in the event of loss or corruption. Replicating applications while they are running may involve copying open log files, databases, and other configuration settings. If you cannot copy this data while it is in use by the application, you require a solution that can replicate the changes byte by byte across the network to your replica server while your applications are running. An additional challenge for many organizations is to provide replication for database and complex distributed applications that span multiple sites.

Replication solutions must also offer the option to use replicated application data to provide high availability for applications through application failover technologies.

NETWORK AND PROCESSOR OVERHEAD

If you replicate data from one server to another, you must consider the volume of traffic that must be copied across the network and the method that the replication uses to copy the files. A simple file copy takes a copy of the entire file across the network each time a change occurs. For large files, a solution that copies only changes to files is preferred, a process often described as *delta replication*.

Even using delta replication, you must consider the number and frequency of changes that are made to a file and the implication of copying this data across your network. For organizations that have distributed applications across multiple sites, the use of delta replication can enable data to be copied across the wide area network (WAN) to a backup site, where backups are then performed offline. Even though delta replication has the advantage of minimizing network traffic, it is often difficult to predict the volume of changes

that are replicated across the WAN and, therefore, it is difficult to predict the bandwidth that is required to provide resilience in the event of data loss at the primary location.

Traditional backup operations require all of the data to be copied to backup media within a particular time interval, known as *the backup window*. This can result in an intensive period of high-level server processor utilization and file input/output (I/O). Delta replication can reduce the impact that backup operations can have on server and system performance. By copying only file changes as they happen, the volume of data that must be copied is reduced and is not concentrated in a particular time of day.

SIMPLE RECOVERY PROCEDURES

One important measure of the success of any recovery management strategy is how easy it is to recover particular data files or complete applications. Replication can provide simple tools for the recovery of lost or corrupt data, and if combined with application failover, can provide simple procedures that provide near-instantaneous deployment of standby systems. Your standby systems can provide your organization with valuable disaster recovery time so that you can rebuild your production servers, restore applications from backup media, and resynchronize data with the standby server before failing back to the production system.

For many organizations, the additional hardware, infrastructure, and management costs that are required to deploy replica and standby servers can be prohibitive. Similarly, using hardware-based methods to replicate data to disaster recovery sites to protect against local site unavailability is often too expensive and complex to implement.

Server Virtualization Technologies

Server virtualization creates virtual machines (VMs) that operate as if each were a separate server with its own operating system. VMs enable a single physical computer to be divided into separate partitions, each of which can run its own operating system and applications concurrently with others. The VMs can run different operating systems and software because each has its own virtual storage locations, memory spaces, and networking interfaces and the underlying virtualization layer manages system resource sharing between virtual machines. This partitioning dramatically improves hardware resource utilization and enables a single host computer to support multiple replica or standby systems.

COST-EFFECTIVE SYSTEM PLATFORM

Virtualization can provide significant advantages for business continuity by lowering hardware requirements. In many cases, the provision of a temporary limited service is the priority, so standby systems need not necessarily be at the same hardware specification as, or be complete hardware duplicates of, your production servers. Because server virtualization can provide replication and backup services at minimal hardware cost, your investment will have bought you time to repair or replace your production systems.

Virtualization technology helps reduce the number of physical servers that are required to support business continuity and disaster recovery processes, and can result in follow-on savings in several key areas:

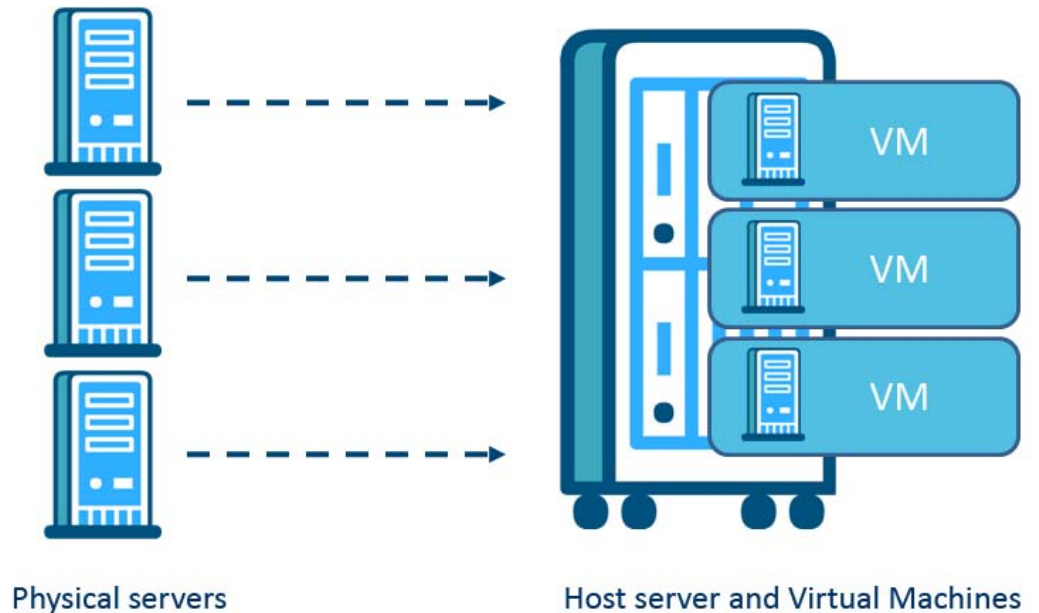
- **Power** - The costs of the power itself, together with associated power infrastructure costs, such as UPSs
- **Cooling** - The costs of installing and running air conditioning systems in your server rooms
- **Floor space** - The costs of providing floor and rack space for your servers

Using virtualization, some organizations may be able to use their existing geographical locations as recovery sites for different parts their business. For instance, a site in Germany may be able to act as a disaster recovery site for operations in France. Virtualization can enable an organization to provide cost-effective disaster recovery solutions without investing in a dedicated disaster recovery site.

USING VIRTUALIZATION FOR DISASTER RECOVERY

FIGURE A

One of the most significant server virtualization benefits for many organizations is the ability to replicate multiple physical servers to a virtual environment to create a cost-effective disaster recovery solution.



SIMPLIFIED MANAGEMENT

Virtualization also makes infrastructures flexible and potentially easier to manage. When business processes and services are independent of the hardware they run on, it is easy to move them to other hosts while performing system maintenance or while moving labs and data centers. However, virtualization does also incur its own additional management requirements, such as the need to ensure that effective disaster recovery plans are in place for your host servers. If you do not protect your host servers properly, the loss of a single host can lead to multiple VMs becoming unavailable.

To help maintain the availability of VMs, many organizations make use of other virtualization technologies, such as Storage Area Networks (SANs) and virtual local area networks (VLANs). SANs abstract physical storage resources and hide the details of the physical disk drives on which files reside, while managing the security and backup of the data transparently. Using SANs for data storage means that a replacement VM can be brought online and have access to the same data as the offline VM. Similarly, VLANs enable a logical networking topology to be overlaid on a physical topology, which increases your flexibility to secure and isolate network traffic.

Requirements for Effective Virtualization Deployments

Server virtualization is an important technology that can provide cost-effective and flexible recovery management tools and can help you to maintain business continuity and to provide effective disaster recovery. However, because virtualization involves multiple VMs running on single hosts, and uses a virtualization layer to provide access to resources such as file systems, there are specific backup and recovery requirements that must be met for virtualization to become a benefit to your organization, and not a risk to your business operations.

SIMPLE BACKUP IMPLEMENTATION

The requirement to deploy software to every virtual server is significant for organizations with many virtual servers; backup solutions that are able to benefit from virtual servers running on the same hardware can provide significant advantages. For example, tools that run on the host computer, or that access shared data on SANs, do not typically require installation on all VMs on that host.

LOW BACKUP OVERHEAD

Traditional support by using backup agents that are installed and configured within each virtual server, provides these benefits:

- Server, application, and file level recovery
- Familiar deployment tools, because deployment is exactly like deployment to physical servers and desktop computers.

However, the traditional approach has its own problems:

- Performance is adversely affected by backup because creating copies from VMs is disk and network I/O intensive, and resources on the host computer can become a bottleneck and impact VM performance.
- Software overhead is increased because software maintenance must be performed on each virtual server, not just on each host computer. This reduces some of the benefits of deploying virtualization for server consolidation.

One alternative is to backup the host computer. This enables fast server-level recovery of the virtual host, and protects the virtualization layer and management consoles. However, such an approach is not application aware, and makes it complex to restore individual virtual hosts or particular virtualized applications that are running on those hosts. There may also still be a significant performance impact during the backup process.

LOW BACKUP IMPACT

Virtual server configurations and data are stored as files on a hard disk. A simple method to backup virtual servers is to close the virtual server down and to backup the virtual server file. The advantages of this backup method are that you:

- Create a complete copy of your virtual server that you can restore rapidly.
- Reduce the complexity of backup.
- Increase the speed of backup.

However, there are also some disadvantages, which include the requirement to take servers offline to perform the backup and that there is a significant storage requirement for large image backup files.

SIMPLE RESTORE PROCEDURES

To maintain an effective virtualized environment you must be able to easily and rapidly restore VMs if there is a problem with a live production VM, or when using a VM as a temporary replacement for a crashed or unavailable physical server.

Summary of the Challenge

Replication and virtualization are potential solutions to many of today's data management and protection challenges. However, replication and virtualization also bring their own challenges that must be met, if organizations are to successfully exploit the potential of these technologies.

Using CA Technologies to Maintain Business Continuity

CA technologies help to maintain business continuity and application availability through replication and failover, and through support for server virtualization. CA replication and virtualization support technologies are included in:

- CA XOssoft Replication r12, which provides true CDP for data and applications.
- CA XOssoft High Availability r12, which includes all of the features in CA XOssoft Replication, and adds application failover.
- CA XOssoft Assured Recovery r12, which provides automatic disaster recovery testing.

Additional virtualization support technologies are included in:

- CA ARCserve Backup r12, which, including its associated Backup Agents, creates and manages secure permanent data backups and provides bare-metal disaster recovery tools, so that a computer without any operating system or application software is restored to a previously backed up state.

CA XOssoft Replication

CA XOssoft Replication provides data replication between live (master) servers and backup (replica) servers. CA XOssoft Replication features meet the following key requirements for an effective replication-based recovery management solution:

- **Cost-Effective Implementation** – The replica server hardware does not need to match the hardware that is used on the master server. The master and replica can run on different operating system versions; CA XOssoft Replication r12 supports Windows Server 2003 and Windows Server 2008, and other versions are available for non-Windows operating systems.
- **Protection against Site Problems** - Low bandwidth data transfer over both LAN and WAN connections is optimized. After an initial synchronization between the master server and the replica server, the CA XOssoft replication engine only sends file changes back to the replica server. This reduces the bandwidth that is required for daily backups of remote data and applications, and means that CA XOssoft Replication can provide effective protection against site problems through the use of offsite data replicas.
- **Timely Replication** - Real-time replication transfers changes from a master server to a standby replica server, so that the most recent data is always available for recovery purposes. CA XOssoft Replication uses block-level replication of changes that are made to files rather than replicating the entire file.
- **Prevent Data Loss** - True CDP for data and applications includes the ability to rewind data to a particular point-in-time. CA XOssoft Replication complements backup and snapshot solutions and enables reliable and fast data rewind.
- **System and Application Consistency** – A range of built-in *scenarios* provide sets of tested settings for configuring replication for particular applications. These scenarios support applications such as Microsoft Internet Information Services (IIS), Microsoft SQL Server, and Microsoft Exchange, and ensure that even complex applications are consistently replicated, including all relevant application data, configuration, and log files. CA XOssoft Replication also includes scripting support, so that custom applications can be properly replicated.
- **Network and Processor Overhead** – The replication engine used by CA XOssoft Replication does not have significant processor requirements for either the master or replica servers, so that normal replication does not have a significant performance impact on your production servers. There is low overhead on network bandwidth, because only file changes are sent back to the replica server. You can also reduce, or remove, the potentially high processor and network bandwidth requirements of

traditional backup windows by using continuous low bandwidth replication to your central data center and then using traditional backup methods to back up the replica servers. CA XOssoft Replication includes an *assessment mode* that enables you to measure the amount of bandwidth that is required to replicate data, prior to implementation.

- **Simple Recovery Procedures** - Rewind journals store any I/O operational information that results in modifications being made to a file. By using the rewind journal, it is possible to undo I/O operations, and rewind one or many files to any previous point-in-time. This can help to make it easy to recover lost or corrupt files.

CA XOssoft Replication features also help you to exploit and protect virtual servers, by enhancing the key benefits of server virtualization and meeting the key requirements for an effective virtualization deployment:

- **Cost-Effective System Platform** - The hardware does not have to be the same, so you can easily replicate data from physical servers to virtual servers, which provides a cost-effective replication platform.
- **Simple Backup Implementation** - CA XOssoft Replication is easily installed on a VM to provide full replication to a virtual replica server.
- **Low Backup Overhead** - Copying large volumes of data from VMs during traditional backups is I/O intensive, and can result in significant disk and network overhead, and affect VM performance. Data replication and CDP used in CA XOssoft Replication has a much lower impact, through continuous copying of delta changes, rather than a nightly full copy done by backup.

CA XOssoft High Availability

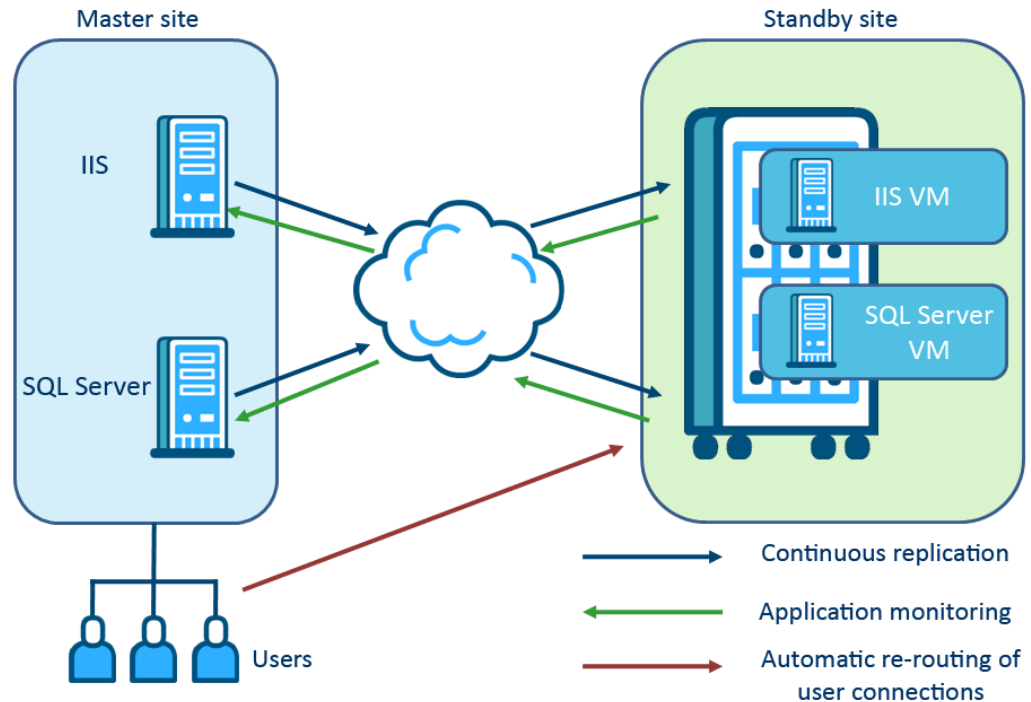
CA XOssoft High Availability r12 adds application failover functionality to the replication tools that are provided by CA XOssoft Replication. CA XOssoft High Availability features meet the following key requirements for an effective replication-based application failover solution:

- **Cost-Effective Implementation** - Is hardware agnostic, like CA XOssoft Replication, so does not require any particular hardware for the master and replica (standby) servers. You can use any combination that makes sense to your business:
 - Physical to Physical (including multi-processor to single processor)
 - Physical to Virtual
 - Virtual to Virtual
 - Microsoft Cluster to Microsoft Cluster
 - Microsoft Cluster to Virtual or Physical
- **Protection against Site Problems** - Uses the same replication engine as CA XOssoft Replication, and works well over WAN connections. You can also monitor the health of remote production servers.
- **Timely Replication** - Uses the CA XOssoft Replication engine, so after application failover the most recent data is always available on the standby server.
- **System and Application Consistency** - Provides additional scenario settings, to ensure reliable replication and failover for applications such as IIS, Microsoft SQL Server, and Microsoft Exchange.
- **Simple Recovery Procedures** - Uses the same technologies for both data replication and for manual or automatic failover of applications and servers. Automatic failover uses sophisticated test criteria, known as *is-alive* testing. This means that CA XOssoft High Availability can provide resilient applications for your users through automatic detection of failed servers and redirection of clients to replica servers.

USING VIRTUALIZATION FOR APPLICATION FAILOVER

FIGURE B

CA XOsft High Availability can be deployed in a virtual server environment to provide cost-effective application failover.



CA XOsft High Availability features also help you to exploit and protect virtual servers, by meeting the following key requirements for effective server virtualization:

- **Cost-Effective System Platform** – 100 percent hardware independent, so you can configure failover from a physical server to a virtual server, and depending on your application requirements, you may be able to consolidate your standby servers so that several physical master servers are configured to failover to a single host computer that is running multiple virtual standby servers.
- **Simple Backup Implementation** – Easily installed on a VM to provide full application failover to a virtual standby server.

CA XOsft Assured Recovery

The CA XOsft Assured Recovery option is available for CA XOsft Replication and CA XOsft High Availability, and provides automatic disaster recovery tests to ensure that your replicated data and applications are recoverable. CA XOsft Assured Recovery helps to meet these replication requirements:

- **Prevent Data Loss** – After the assured recovery test completes, you can use the Windows Volume Shadow Copy Service (VSS) to generate a snapshot of your data and application to provide additional protection for your critical data and enable a restore point. VSS snapshots enable you to create a point-in-time image copy of data on a volume, so you can quickly restore individual files or entire volumes in the event of system failure or data corruption.
- **System and Application Consistency** – During the assured recovery tests, replication is temporarily paused while the replica data and application are checked to ensure recoverability and data consistency. The testing is performed on the replica

server, so there is no impact on your production environment and, on completion of the test, replication continues without the need to resynchronize data.

- **Simple Recovery Procedures** – By combining replication with the VSS snapshot backups that are generated by CA XOsoft Assured Recovery, you can easily recover to a known point-in-time by using a verified and checked copy of your data and application. You can mount snapshots, and use familiar drive letter-based access, to enable you to drag and drop data for fast recovery of snapshot-based data.

CA XOsoft Assured Recovery features also help you to exploit and protect virtual servers, by meeting the following key requirement for effective server virtualization:

- **Low Backup Impact** – Automatically created VSS snapshots can be used to enable low impact backups, where it is the snapshot that is backed up rather than the live shared file system.

CA ARCserve Backup

CA ARCserve Backup is a comprehensive backup solution that can integrate with a range of applications and operating systems. CA ARCserve Backup uses a single management console to monitor, configure, and report on backup and restore tasks for your physical and virtual environment, and helps to simplify backup and restore operations. To backup virtual servers, CA ARCserve Backup can make use of snapshot technologies to help meet the challenge of effective virtualization.

SNAPSHOTS AS BACKUPS

A snapshot is copy of a computer system at a particular point-in-time, which includes all of the data and may include BIOS configuration. Snapshot technology is available for both physical computers, through Windows operating system snapshots, and virtual machines. In the virtual environment, by using some virtualization tools you can take multiple incremental snapshots.

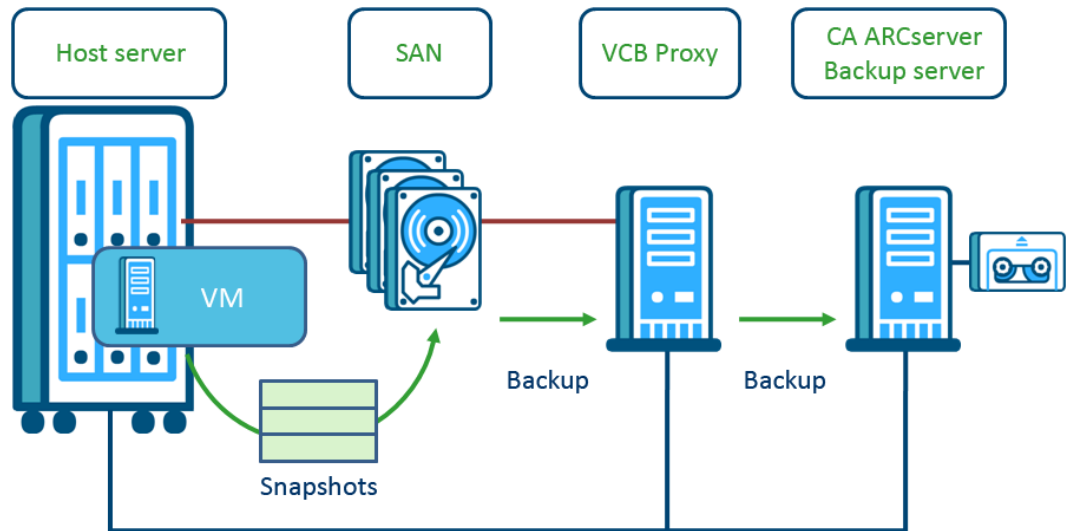
VMWARE CONSOLIDATED BACKUP

VMware Consolidated Backup (VCB) is part of the VMware Infrastructure, and is integrated with VMware ESX Server and VMware VirtualCenter Server. VCB uses VMware snapshots to protect VMs and data. By using VCB you can offload VM backup activity to a dedicated backup proxy system and the proxy system can access and mount VMware snapshots for backups. VCB provides the underlying technology for effective VM backup, but does not itself include backup software or backup management tools. You use the CA ARCserve Backup Agent for VMware with VCB, which works with the backup and restore functionalities that are provided by CA ARCserve Backup to protect your VMs.

USING VMWARE CONSOLIDATED BACKUP

FIGURE C

VMware Consolidated Backup enables VMs to be backed up from SAN-based snapshots.



VIRTUAL SERVER/HYPER-V

Microsoft Virtual Server 2005 SP2, and the new Hyper-V virtualization that is supported in Microsoft Windows Server 2008, use VSS snapshots to create point-in-time copies of VMs and data. By using VSS, you can create a shadow copy that includes only the changes that have occurred since a full shadow copy was last completed, so the copy only takes up a small percentage of the overall volume size. A hardware snapshot performs a full copy of a volume; this is an exact copy of the volume so the copy requires the same amount of disk space as the volume.

Microsoft Virtual Server and Hyper-V use VSS writers to ensure that VMs are backed up to a consistent state when the shadow copy backup request is processed. When you create the shadow copy, a VSS writer suspends writes to a volume to ensure that files selected for backup remain in a consistent state. For Windows virtualization, VSS support is provided through the Microsoft Virtual Server 2005 Writer and Microsoft Hyper-V Writer.

CA ARCserve Backup supports VSS through the Agent for Open Files and the Enterprise Option for VSS Hardware Snap-Shot. CA ARCserve Backup VSS support is automatically installed when you install the Agent for Open Files.

CA ARCSERVE BACKUP AND VIRTUALIZATION

CA ARCserve Backup enhances support for VMware virtual infrastructure by providing online virtual server backup through the CA VMware backup agent, which makes use of VCB to create a VMware snapshot backup. The CA ARCserve VMware Agent uses VCB to:

- Reduce the load created by backup tasks on your ESX server.
- Remove the requirement for a backup agent on every virtual server.
- Use a SAN rather than the LAN to improve the backup process.
- Provide backup support for virtual servers that are not powered on.
- Enable full image or file level backup.
- Discover VMs from the VCB Proxy.

CA ARCserve Backup enhances support for Microsoft Virtual Server and Hyper-V by using the CA ARCserve Backup Windows VSS Agent to:

- Remove the requirement for a backup agent on every virtual server.
- Provide backup support for virtual servers that are not powered on.
- Enable full image backup.

- Discover VMs from host computer.

CA ARCserve Backup features also help you to exploit and protect virtual servers, by meeting the following key requirement for effective server virtualization:

- **Simplified Management** – CA ARCserve Backup includes integrated antivirus scanning, which ensures virus-free backups and eliminates the need to scan live VMs for viruses. For VMware-based VMs, backups can be managed at multiple levels:
 - VCB Proxy
 - VMware ESX Server or VirtualCenter
 - Virtual Machine
 - Data volume
- **Simple Backup Implementation** – CA ARCserve Backup Agents ensure that there is minimal software to deploy and maintain. For example, one CA ARCserve Backup Agent for VMware license covers all of the VMs on a VMware ESX server. Using CA ARCserve Backup and CA XOssoft Replication together provides simplified backups because the CA XOssoft scenario appears as a backup source in CA ARCserve Backup.
- **Low Backup Overhead** – The VCB-based backup used by CA ARCserve Backup Agent for VMware is fast, and supports incremental and differential backups. Similarly, VSS backups are also faster than using traditional backup agents in each running VM.
- **Low Backup Impact** – VCB-based backups have low impact on the running VMs, because snapshots rather than live VMs are accessed, and the backup takes place over the SAN. Similarly, VSS backups do not access data on the live VMs.
- **Simple Restore Procedures** – Using the Disaster Recovery tools in CA ARCserve Backup it is easy to restore physical servers to a *bare-metal* virtual server, which results in reduced downtime and reduced disaster recovery costs, and gives you time to fix problems on the physical primary server. The CA ARCserve Backup Agent for VMware supports granular or full restores and also supports simplified restores to original data locations.

SECTION 3: BENEFITS

Benefits of CA Technologies for Business Continuity

By using data replication and server virtualization technologies, you can help your organization to meet the key challenges for business continuity and application availability. By using CA replication, failover, and backup solutions you can ensure that you make the most effective use of your investments in replication and virtualization. You do not need to modify your existing environment to exploit these technologies, and replication and backup integration enables you to deploy high availability and disaster recovery simultaneously.

CA XOssoft Replication, CA XOssoft High Availability, and CA XOssoft Assured Recovery provide the following benefits to help meet the requirements for effective data replication:

- **Management of costs** - CA replication solutions are simple to implement, cost-effective, and easy to manage and maintain. You do not need to re-engineer your applications or IT infrastructure to provide a highly available solution for your organization. CA XOssoft Replication and CA XOssoft High Availability can run on any hardware that is supported by Windows Server 2003 or Windows Server 2008.
- **Protection against site problems** - CA XOssoft Replication and CA XOssoft High Availability provide effective data replication and application failover, even over WAN links, so they enable high availability and disaster recovery solutions that protect against site unavailability.

- **Timely Replication** - CA XOssoft Replication and CA XOssoft High Availability use real-time replication to transfer changes from the master to the replica server, so that the most recent data is always available for recovery.
- **Prevention of data loss** - CA XOssoft Replication and CA XOssoft High Availability use CDP and data rewind to help eliminate or reduce downtime for your applications and data. CA XOssoft Assured Recovery adds the automatic creation of VSS snapshots, for point-in-time recovery from tested backups.
- **Maintenance of system and application consistency** - CA XOssoft Replication and CA XOssoft High Availability application scenarios provide tested replication and failover settings to help to ensure system and application consistency. CA XOssoft Assured Recovery snapshots provide backups from a known consistent and verified state.
- **Reduction of network and processor overhead** - The CA XOssoft Replication and CA XOssoft High Availability replication engine does not have significant processor requirements and because only file changes are sent back to the replica server, there are also low network bandwidth requirements. The assessment mode enables you to plan for the amount of bandwidth that will be required to replicate data.
- **Use of simple recovery procedures** - CA XOssoft Replication and CA XOssoft High Availability enable rapid data and application recovery in the event of system failure or data corruption, by use of simple data rewind and recovery of single or multiple files. Application failover that uses CA XOssoft High Availability can be initiated manually or automatically. Data from snapshot backups can be easily restored by mounting the snapshot as a logical drive.

CA XOssoft Replication, CA XOssoft High Availability, and CA ARCserve Backup provide the following benefits to help meet the requirements for effective virtualization deployments:

- **Provision of cost-effective system platforms** - CA XOssoft Replication and CA XOssoft High Availability are hardware agnostic, so you can easily use VMs as replica and standby servers, and consolidate several physical master servers to failover to a single host computer that is running multiple virtual standby servers.
- **Reduction of management complexity** - CA ARCserve Backup can use integrated antivirus scanning to ensure virus-free backups and eliminate the need to scan live VMs. VMware-based backups can be managed at the VCB Proxy, the host server, the VM, or the data volume.
- **Implementation of simple backup procedures** - CA XOssoft Replication can be used to provide replication for a VM, and CA XOssoft High Availability can be used to enable VM failover to a physical server or other VM. A single CA ARCserve Backup Agent license covers all of the VMs on a host computer, and CA XOssoft scenarios appear as a backup source in CA ARCserve Backup.
- **Reduction in backup overhead** - CA XOssoft Replication and CA XOssoft High Availability can be used to provide data replication in VM environments, so that backups are performed through continuous copying of delta changes. VCB-based backups that are used by the CA ARCserve Backup Agent for VMware are fast and support incremental and differential backup operations. VSS backups of Virtual Server and Hyper-V VMs are also faster than using traditional backup agents.
- **Reduction in backup impact** - CA XOssoft Assured Recovery can create VSS snapshots that can be used to enable low impact backups, where it is the snapshot that is backed up rather than the live shared file system. The use of VSS backups also reduces the impact of backups on live Virtual Server and Hyper-V VMs. CA ARCserve Backup VCB-based backups have low backup impact because VMware snapshots are accessed and the backup takes place over the SAN.
- **Implementation of simple restore procedures** - CA ARCserve Backup Disaster Recovery tools enable you to easily restore physical servers to a bare-metal virtual

server. The CA ARCserve Backup Agent for VMware supports granular or full restores, and also supports simplified restores to original data locations.

SECTION 4: CONCLUSIONS

Organizations face a number of challenges to business continuity and application availability. These challenges include the volumes of data generated and application complexity, demands for round-the-clock operations, server proliferation, and regulatory requirements for data protection and storage.

Replication and virtualization are potential solutions to many of these data management and protection challenges. However, replication and virtualization technologies also have their own requirements, and if the challenge of these requirements is not met, many organizations will fail to successfully exploit the potential of data replication, continuous data protection, application failover, and server virtualization technologies.

CA XOssoft replication solutions and CA ARCserve Backup technologies can help you to maintain business continuity and application availability through effective use of replication and failover, and through support for server virtualization.

To learn more about the CA XOssoft and CA ARCserve Backup architecture and technical approach, visit ca.com/xosoft and ca.com/arcserve.