

---

# Adopting Server Virtualization for Business Continuity and Disaster Recovery

*CA ARCserve® Backup and CA XOSoft™ Replication and High Availability Software with Hyper-V™ Technology—  
A Powerful Combination*

---

This white paper is for informational purposes only. MICROSOFT AND CA MAKE NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Document published May 2009



UNIFYING THE ENTERPRISE



# Contents

- Introduction .....2
- What is Hyper-V? .....2
- What is the most important consideration in moving workloads and applications from a physical environment to a virtual environment? .....2
- What is CA ARCserve Backup? .....3
- What are CA XOsoft Replication and CA XOsoft High Availability? .....4
- Why companies are adopting Hyper-V for their virtualization infrastructure.....5
  - Reliable Disaster Recovery Support.....6
  - Environmentally Responsible Technology.....6
- Considerations in implementing virtualization.....6
  - Determining Application Requirements .....6
  - Determining the Architecture of Your Virtualized Server Environment.....7
  - Determining Hardware Resource Requirements .....7
    - Processor Resources..... 8
    - Memory Resources..... 8
    - Storage Resources ..... 8
    - High-Performance Hardware Requirements..... 8
  - Determining Backup, Disaster Recovery (DR), and Business Continuity (BC)\High Availability (HA) Requirements.....8
    - Backups That Use Native Applications..... 9
    - Guest-Level Backups..... 9
    - Hypervisor-Level Backups ..... 10
  - Determining High-Availability Requirements .....10
    - High Availability within a Data Center..... 10
    - High Availability Across Data Centers ..... 11
- Implementing backups of Hyper-V environments using CA ARCserve Backup.....12
  - Full Weekly Backup with Daily Differential Backups** .....12
  - Image-Level VM Restores and Granular Folder\File-Level Restores** .....13
  - Multiple Remote Office Backup**.....13
  - Physical to Virtual Server Migration** .....14
- Establishing a high-availability data recovery site by using Hyper-V and CA XOsoft High Availability ..15
  - Basic High-Availability Scenario: Two Virtual Machines on a Single Physical Machine** .....15
  - Large-Scale High-Availability Scenario: Physical-to-Virtual Environment with Advanced Data Recovery**.....16
- Conclusion .....16

## Introduction

In today's competitive business environment, your IT infrastructure must accommodate rapidly changing business needs and unforeseen problems with minimal impact on day-to-day operations. But this level of flexibility, scalability, and high availability can be expensive and difficult to deploy and maintain, especially for small and midsize businesses. No matter what size your business is, in today's economic climate, having an IT infrastructure that includes a cost-effective business continuity (BC) and disaster recovery (DR) solution is a necessity. Downtime of mission-critical applications can cause irreparable harm to any-size business. Server virtualization is now a mainstream technology within small, midsize, and large organizations - not just for early adopters - and requires the same levels of protection as physical servers.

Server virtualization technology helps significantly reduce overall IT capital expense and operational costs. Hyper-V™ virtualization technology, a feature of the Windows Server® 2008 operating system, is an enterprise-class virtualization solution that can be quickly deployed in any business environment. By using Hyper-V with BC/DR solutions from CA such as CA ARCserve® Backup, CA XOssoft™ Replication, and CA XOssoft High Availability, you can build an IT infrastructure with robust business continuity and disaster recovery capabilities to protect mission-critical applications and data while reducing total cost of ownership (TCO).

## What is Hyper-V?

Hyper-V is the next-generation hypervisor-based server virtualization technology. Available as an integral feature of Windows Server 2008, it enables you to implement server virtualization with ease. You can use Hyper-V to make the best use of your server hardware investments by consolidating multiple server and application roles as separate virtual machines (VMs) running on a single physical machine. With Hyper-V, you can also efficiently run multiple different operating systems—Windows®, Linux, and others—in parallel, on a single server, and fully leverage the power of x64 computing. And with more and more cores getting added to a CPU, the adoption of virtualization is going to increase at a faster pace than ever before.

## What is the most important consideration in moving workloads and applications from a physical environment to a virtual environment?

Given the benefits of virtualization, when you want to move your workloads or applications into virtualized infrastructure, some of the top considerations of your backup\storage administrator would be “How do I protect the data in the virtualized infrastructure? How do I make sure that there is minimum impact on the existing backup processes? How do I make sure that my existing restores or recoveries processes don't change? How do I make sure I know the backups of my data in the virtual infrastructure is backed up and restored in the most efficient way?” How do I limit my risk with more virtual servers residing on a single physical server now?

These are some of the questions all storage\backup administrators will have in their mind as they see more servers getting virtualized.

## What is CA ARCserve Backup?

CA ARCserve Backup offers world-class data protection for distributed servers, databases, and applications running in both physical and virtual environments, including Hyper-V. This high-performance solution combines innovative D2D2T (disk-to-disk-to-tape) backup with powerful, integrated antivirus and encryption tools, making it one of the most secure out-of-the-box backup solutions offered. It is a solution that delivers reliable data protection for a wide range of operating environments and includes the following critical features:

- **Data deduplication** reduces disk storage for backups, increases recovery points, and reduces recovery time objective (RTO)
- **Granular file and folder restores from image-level VM backups** provide the ability to perform a full VM restore or a granular file or folder restore from a single VM backup.
- **Powerful dashboard with storage resource management reporting** provides a single-pane-of-glass view through which administrators can monitor and manage storage resources and backups. The dashboard displays statistics regarding recovery points of physical and virtual machines, CPU, memory, disk, network cards, volume utilization, volume fragmentation, and server OS and service pack levels.
- **Scalability and flexibility features** give users the choice to multistream, multiplex, back up to disk, back up to tape, or back up to disk to tape. This provides complete flexibility and choice of approach to best meet specific backup requirements and to minimize the backup window.
- **Security with password key management for encryption** enables administrators to easily secure data without the burden of memorizing passwords. CA ARCserve Backup has flexible role-based administration and supports complete auditing capabilities to reduce administrative efforts.
- **Extensive Microsoft® application and OS support** is available for a wide range of Microsoft applications including Microsoft SQL Server®, Microsoft Exchange Server, Microsoft Office SharePoint® Server, Microsoft Hyper-V Server, and all Windows, Unix, and Linux operating systems.

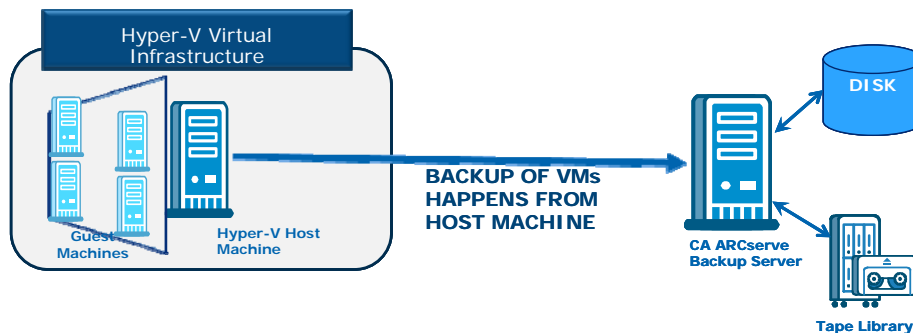
All of these features, along with its affordable, flexible, and simple licensing structures, make CA ARCserve Backup a value leader in the market delivering enterprise-class data protection for a wide range of operating environments. Suitable for companies of all sizes, it offers leading-edge backup and data protection technology that efficiently and cost-effectively helps reduce the costs of protecting business-critical data and applications running on both virtual and physical servers. Certified across an extensive range of industry platforms and applications, it provides compatibility and support for heterogeneous environments.

### Protection of your virtual server Infrastructure

CA ARCserve Backup integrates with Microsoft Hyper-V Servers starting with complete integration within the user interface—no scripting required! Some of its salient features are:

- **Auto discovery and protection of VMs.** With the flexible nature of the virtual infrastructure, virtual machines can appear and disappear dynamically, creating the potential for missed backups if the backup administrator does not realize these changes have occurred. To avoid this problem, CA ARCserve Backup has automatic discovery of VMs to help ensure that they are all backed up regardless of how the environment changes.
- **Granular file/folder restores.** One-step granular file recovery process allows restoration of individual files and directories from an image-level backup of the VM directly from the backup media. This requires just one full VM image backup; from that one backup it is possible to restore either the full VM or granular file restores.
- **Fast and efficient restores.** When a granular file/folder restore is required, CA ARCserve Backup uses a patent-pending technology to restore the granular files/folders directly from the backup media to the VM without staging. This ensures extremely fast and efficient restoration of the data.
- **Flexibility and reduced storage requirements.** They support mixed backups for weekly full backup and daily incremental or differential backups.

- **Small backup window.** Using multiple, controlled data streams, CA ARCserve Backup can simultaneously back up data from multiple VMs across multiple Hyper-V servers to disk or to tape, thus helping to reduce the backup window and improve backup efficiencies.
- **No change in processes.** Backing up a virtual infrastructure is as simple as backing up any physical machine. There are no custom scripts—it simply works out of the box.
- **Quick disaster recovery of physical servers to virtual servers.** Achieve quick and efficient disaster recovery into a virtual machine from the backups of your physical servers.
- **Migration.** CA ARCserve Backup also aids in the migration of production applications from physical to Windows Server 2008 Hyper-V virtual servers.



## What are CA XOssoft Replication and CA XOssoft High Availability?

CA XOssoft software products provide both business continuity and disaster recovery capabilities to help ensure that critical business systems, applications, and data are always available—even in the face of planned and unplanned outages.

The CA XOssoft product family includes CA XOssoft Replication and CA XOssoft High Availability for both physical and virtual server environments like Hyper-V. They also include support for a wide range of operating systems and applications. Both products provide:

- **Real-time host-based data replication** across the LAN or WAN between production servers and remote replica servers for data protection and continuous application availability.
- **Continuous data protection (CDP) with "Rewind"** for fast recovery time after accidental or malicious data loss or damage.
- **CA XOssoft Assured Recovery®**, included with both CA XOssoft products, for fully automated disaster recovery testing to help ensure recovery readiness, with no disruption to the production or DR environment. Optional VSS snapshots may be performed after system validation for backup.
- **Web-based centralized management** and no-reboot deployment and maintenance to make CA XOssoft easy to deploy and manage with no impact to the production environment.
- **Extensive Microsoft application and OS support** to protect a wide range of applications including Microsoft SQL Server, Microsoft Exchange Server, and Microsoft SharePoint Server, Microsoft Hyper-V Server, and most Windows operating systems. Oracle and Blackberry Enterprise Server are also supported.

CA XOssoft High Availability adds:

- Real-time server monitoring

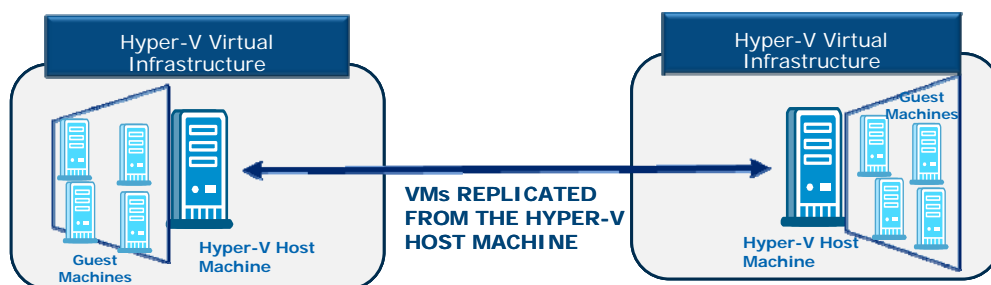
- Scheduled and automated instantaneous failover
- Push-button fail-back

Like CA ARCserve Backup, all of these features, combined with its affordable, flexible, and simple licensing structures, make CA XOssoft a value leader in the market delivering enterprise-class data protection. Suitable for companies of all sizes, it offers leading-edge replication, failover, and DR-testing technology that efficiently and cost-effectively helps reduce the costs of protecting business-critical data and applications running on both virtual and physical servers. Certified across an extensive range of industry platforms and applications, it provides compatibility and support for heterogeneous environments.

### Protection and use of your virtual server infrastructure

CA XOssoft integrates easily with your Microsoft Hyper-V Servers. Some of its salient features include:

- **P2V, V2V, and V2P replication.** Provides the protection of applications and data running on Hyper-V Servers and also allows the use of Hyper-V Servers for replica or failover servers to help you reduce overall BC/DR costs.
- **Independent replication and high availability.** Offer flexibility of multiple guest operating systems/applications running on a Microsoft Hyper-V Server to another Hyper-V Server without the requirement of installing CA XOssoft on each of the guest operating systems. This enables broader protection and simplifies CA XOssoft deployment, improving IT productivity and reducing risk.
- **System state and registry synchronization.** Helps you protect and more quickly restore the Windows Operating System through periodic, scheduled snapshots stored on the replica server
- **Data migration.** Enables migration from physical to virtual servers or from x86 to x86-64 platforms using a native 64-bit replication solution.
- **Any-to-any replication.** Allows you to pick and choose your server and storage vendors and products on both production and replica environments, to help keep DR costs low.
- **No reboot install and maintenance.** Help eliminate disruption to the production environment.
- **Linux and UNIX® replication.** Provides data protection for organizations with heterogeneous environments.
- **Integrated backup with CA ARCserve Backup.** Allows for quick and easy VSS snapshot backup off the replica server, eliminating any impact to your production servers.



## Why companies are adopting Hyper-V for their virtualization infrastructure

The following are some of the benefits of Hyper-V:

### Integrated Management Tools

- Integrated with System Center, monitoring and planning tools help businesses to see where they can use virtualization to enhance their infrastructure.
- Integration with management and monitoring tools make it possible for administrators to monitor the status of all physical and virtual machines so that they can diagnose and address maintenance issues before they become major problems.
- Hyper-V integrates with industry-standard server management tools through the DMTF standards.

### Improved System Management Efficiency

- Administrators can use Hyper-V tools to change many aspects of the virtual machine configuration without shutting down the virtual machine.
- Hyper-V can be monitored and management solutions can immediately alert administrators if the performance of a Web server is reduced because of increased server workload.
- Hyper-V can be configured to manage other Hyper-V Servers and their hosted virtual machines.

### Reliable Disaster Recovery Support

- Hyper-V supports server clustering to balance system workload over several physical or virtual machines and to minimize the potential impact of server failure.
- Quick Migration makes it possible for administrators to automatically or manually move virtual machines between physical servers with little downtime.
- CA Recovery Management products are integrated with Hyper-V to provide a complete backup copy of each VM/hypervisor and an off-site replica for failover in the event of a local disaster.
- Hyper-V reduces the costs associated with replica servers used to provide HA for business-critical applications.

### Environmentally Responsible Technology

- Server consolidation means a smaller impact on the power grid because server consolidation can save power, rack space, storage, and cabling. This helps organizations that are implementing green initiatives to develop smaller and more cost-effective data centers.

## Considerations in implementing virtualization

As with any deployment of new server technology, introducing virtualization into an enterprise computing environment is a complex task. The goal in deploying virtualization is to replicate the current end-user environment while reducing costs and maintaining performance. In this section, we will review some of the system requirements to evaluate before you plan your migration to a virtual machine environment.

### Determining Application Requirements

Before deploying your virtualization solution, it is a good idea to create an inventory of the end-user applications that your organization relies on. This inventory should include the following information for each application:

- All software and hardware dependencies, including device drivers and maximum memory usage
- The software version
- The division or department that owns the application
- The level of support provided for the application by the manufacturer

The Microsoft Assessment and Planning Tool (MAP) provides agentless inventory functionality. It is available free of charge on the Microsoft Web site<sup>\*</sup>. With MAP, you can generate reports that can help you to determine which systems and workloads are good candidates for virtualization.

## Determining the Architecture of Your Virtualized Server Environment

There are three general approaches to deploying your virtual machine environment. The first is to deploy to all data centers, servers, and workstation and portable computing platforms at once. The main benefit of this approach is that virtualization tools and administrative practices are applied consistently throughout the organization. This provides standardized administrative support that reduces the complexity of IT maintenance tasks and their associated costs. The risk is that it is a much larger deployment that has a higher likelihood of causing business disruptions.

The second approach is to deploy to hubs. Hubs are groups of virtual machines, users, and domains in a central physical location that connect to satellite locations. Hub-based deployment starts at the hub and extends to the satellite locations. This design also benefits from the standardization of administrative support, but hubs can also be used as a test bed in deploying virtual machine technology to a small number of servers before the full deployment. The disadvantage of this approach is that the deployment is not performed across the entire organization at one time. Several smaller deployments increase the amount of system downtime at the hub, which increases the risk of business disruption.

The third approach is to gradually deploy to the entire environment, one location at a time. This deployment method can be performed in environments with or without hubs. This is the least-costly of the three approaches and provides the opportunity to test the new environment before deploying it to the rest of the organization. However, decentralized deployment methods such as this have the highest risk of business disruption, are the most complex to administer, and limit the benefits of virtualization to only those areas of the organization that have been deployed.

## Determining Hardware Resource Requirements

Virtualization technology places heavy processing loads on server-computer hardware and requires state-of-the-art server performance. Consider the size and design of your organization's virtual machine environment when making decisions about how much to invest in newer, high-performance hardware resources.

The following is the server hardware to which it is important to pay particular attention in this assessment:

- Processor architecture and configuration
- Memory
- Storage
- High-performance hardware, such as storage area network (SAN) hardware
- Network cards and infrastructure

Corporate security issues will often determine whether a virtual machine environment will be deployed on a physical server. Take this into consideration as well when determining the hardware resources that you will use in your virtual machine deployment.

---

\* <http://www.microsoft.com/downloads/details.aspx?FamilyId=67240B76-3148-4E49-943D-4D9EA7F77730&displaylang=en>

## **Processor Resources**

Each server virtualization product has its own requirements for processor resources. It is a good idea to plan your investment in processor number and speed to match the requirements of the virtual workloads running on the physical server. Add a buffer amount to maximize the capacity of your system—tools such as MAP can help you estimate this. The risk in failing to do this accurately is that one or more of the virtual machines that you host may exceed the processing capacity of the physical server and degrade the performance of all the virtual machines.

## **Memory Resources**

Most virtualization technologies make it possible for you to control the amount of memory that an application can use. To determine the optimal amount of memory, test your application on the virtual machine before deployment. Put greater than normal demands on the application. Here again, the MAP tool can help you determine appropriate test workloads.

Adding a memory buffer to a virtual machine is not recommended because it will limit the number of virtual machines you can host on a physical server. Your application inventory will be useful in determining the memory requirements of your virtual machine environment.

## **Storage Resources**

In determining the storage needs of your virtual machine environment, you will need to consider the capacity and performance capability of your storage system and whether it will be direct-attached or shared storage. Direct-attached storage is one or more disk storage devices that are uniquely accessible by each host server. Shared storage is storage that is accessible by more than one host server. Shared storage is usually implemented by a SAN, which is a networked group of disk storage devices that the server system accesses by Fibre Channel (FC) or the Internet small computer system interface (iSCSI) protocol, which makes high-speed SCSI storage access possible over conventional network hardware. Direct-attached storage is generally cheaper and SAN storage is faster.

Determine which of these storage methods to use in your deployment based on your performance requirements, cost considerations, your backup requirements, your virtual machine architecture, and the type of data that you will be storing.

## **High-Performance Hardware Requirements**

Support for high-performance hardware such as specialized storage devices like optical jukeboxes and tape libraries may be limited or non-existent in certain virtualization environments. For example, Hyper-V does not currently support host bus adapter (HBA) hardware mapped to a virtual machine that is not the parent partition. Verify that the manufacturer of your virtualization technology supports your high-performance hardware and test the interoperability of your hardware with your virtualization server environment before deployment. Note that you can get better performance and handling when specialized storage devices are accessed by the virtualization host rather than by the virtual machine.

## Determining Backup, Disaster Recovery (DR), and Business Continuity (BC)\High Availability (HA) Requirements

The most common strategies that are used in organizations to protect data today fall into two categories: backup and high availability.

Backups, typically used as a core component of any disaster recovery solution, can be performed in a number of ways. The most common method today involves using dedicated backup software like CA ARCserve Backup to perform periodic backup to disk or tape and archiving for long-term storage or regulatory compliance. Backups can be scheduled and implemented using a combination of full, differential or incremental strategies as well as leveraging Microsoft VSS Snapshot technology to ensure data integrity.

It's always a good practice to ensure that the backup images or replicated data is indeed restorable or recoverable. This is not only useful for compliance purposes but also gives peace of mind that in the event of a problem, you can restore or recover the data reliably and quickly. Both CA ARCserve Backup and CA XOSoft provide this functionality out of the box, conducting periodic Disaster Recovery testing without any manual intervention.

You should consider a vendor like CA whose solutions can protect your data across the entire spectrum of recovery points all the way from backing up data every day, using hourly replication, or continuous replication, or implementing high availability of business-critical data.

There are three common data backup methods: backups that use native applications, guest-level backups, and hypervisor-level backups.

### Backups That Use Native Applications

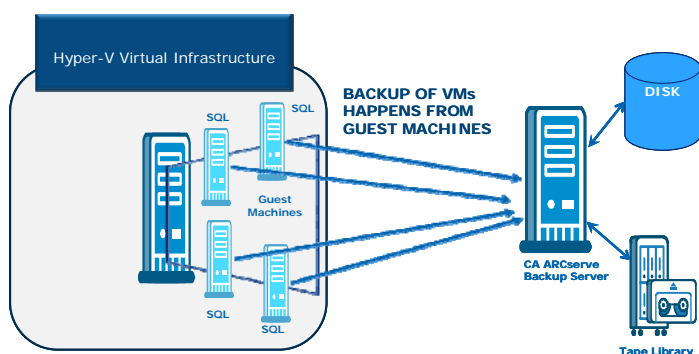
It is possible to use custom scripts to back up applications like Microsoft SQL Server, Exchange Server, or SharePoint Server. But the complexity of managing and maintaining the backup images on disk or tape using custom-built scripts is costly, inefficient, and often prohibitive. More importantly, debugging the details of why backups on certain applications failed and tracking all the different recovery points for different data could easily become complicated and difficult to manage.

CA ARCserve Backup not only offers out-of-the-box backup of Microsoft applications, but it also provides an easy way of tracking backup images on disk or tape. Using a policy-based approach, a copy of the disk-to-tape backup provides simple-to-use, point-in-time restores of applications and automatically restores the full backup image, the differential backup image, and the transaction log backup images. The administrative dashboard provides a single view of the historical trends of your application server backup, for troubleshooting and storage resource management. Overall, for backup and restoration of applications like SQL Server, Exchange Server, SharePoint Server, and file servers, it is often more efficient and cost-effective to use a dedicated backup solution with an integrated application agent like CA ARCserve Backup.

### Guest-Level Backups

In this method, you install a third-party backup agent, such as CA ARCserve Backup, on each virtual machine that will be protected. You then use the backup agent to establish a backup schedule for each server and identify and select the volumes, files and folders, and databases, etc. that will be backed up. Other than the ability to provide centralized scheduling and administration, there is no interaction between the backup processes of each virtual machine—each virtual machine is treated like a physical server for backup purposes.

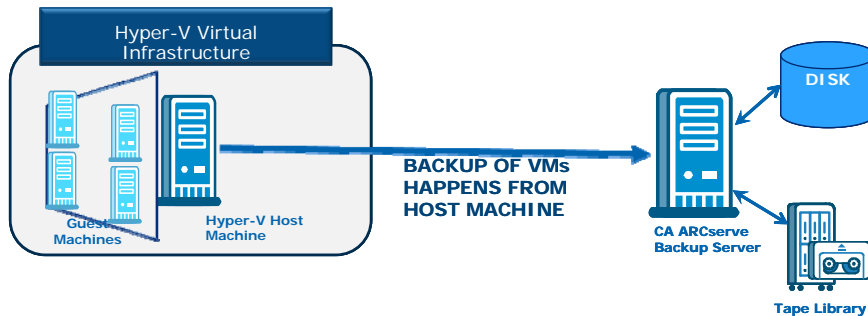
The advantage of this approach is that you can do granular file/folder restores. This is because you are treating a virtual machine just like any other physical machine and doing the backups of files and folders from within the VM. The disadvantage of this approach is that it would be slow to recover a full VM. This specific problem can be addressed by doing hypervisor-level host-based backups.



## Hypervisor-Level Backups

In this method, you deploy a third-party backup agent such as CA ARCserve Backup agent for virtual machine on the Hyper-V host machine. You can then configure the backup server to do an online backup of these VMs by taking a VSS snapshot of the VMs, thus ensuring the integrity and consistency of the data inside each of the VMs.

Doing hypervisor-based backup has an advantage that the entire VM can be backed up. This helps in the quick recovery of the entire virtual machine in case of a disaster or the need to clone a VM. Moreover, using CA ARCserve Backup's unique patent-pending capabilities, you can also achieve granular restores of files and folders from the full image-level VM backup. What this means is that you can do both types of restores from just one image-level backup of the VMs from the Hyper-V host, thus increasing the operational efficiency of managing virtual machine backups and restores.



Refer to the section titled “Implementing backups of Hyper-V environments using CA ARCserve Backup” later in this document for use scenarios corresponding to these backup methods.

## Determining High-Availability Requirements

In most computing environments, a two-tiered approach to assessing and deploying high-availability solutions is necessary. Because of its central location, a data center cannot always provide the level of business continuity that an organization requires. Brownouts, power failures, and catastrophic storage device failures within a data center can result in a complete loss of the data that is hosted at that site. To minimize these risks, you may want to deploy an additional level of failover protection between data centers.

This section assesses the difference between the high-availability requirements *within* data centers and the requirements *between* data centers.

### High Availability within a Data Center

There are three basic approaches to implementing this tier of high availability. Each approach is appropriate for a specific type of server or application, so you will likely use a combination of these methods in your solution.

- **Network Load Balancing (NLB).** This approach involves distributing the network traffic that is being sent to an application across a group of copies of that application that are running on different servers. If one server fails, the traffic that is sent to the application instance that is running on that server is redirected to the copies that are running on the other servers. The network traffic load is redistributed across the remaining application copies and servers by using a load-balancing algorithm. This is particularly useful for stateless application instances.
- **Application-Specific Clustering.** A server cluster is server software that is installed on separate physical servers and is configured to operate as a single server. The server cluster shares server configuration data, access to storage devices, and load-balancing operations.

When one of the physical or software servers fails, the remaining servers in the cluster reassign to the operational servers the tasks that are performed by the defunct server. Some mission-critical enterprise server applications—for example, Microsoft SQL Server and Microsoft Exchange Server—can operate as a server cluster. These server applications are said to be “cluster aware.”

- **Host Clustering.** Virtual machine configurations that do not have cluster-aware software can use host clustering to implement high availability. In this approach, several physical servers that host virtual machine operate as a cluster. When one of the physical servers fails, the operations that are performed by all of the virtual machines that are hosted on that server computer are moved to the other physical servers in the cluster. The level of system availability that host clustering provides is not as high as with application-specific clustering, because the operating systems or applications deployed on the hosted virtual machines are not cluster aware. With Hyper-V, a configuration with host clustering provides for planned and unplanned downtime. During unplanned downtime, the virtual machines will be restarted on the target node within the cluster, and during planned downtime the virtual machines will be transferred statefully from one cluster node (physical server) to another node.

### High Availability Across Data Centers

Server virtualization technology makes it possible to run a cluster of virtual machines on one physical server. This is a way to implement a high degree of system usage for relatively little cost. An optimal high-availability solution is where the data and operations of a cluster of physical servers at the primary site are replicated in an identically configured cluster of standby virtual machines at a remote backup site. When the primary site becomes unavailable, data center operations are quickly transferred over a wide area network (WAN) from the primary site to a standby site in a process called *failover*.

Network load-balancing and clustering technologies protect only the data that a server cluster manages, so software that manages data protection between clusters is necessary. Also, not all applications are cluster-aware and not all operating systems support clustering. CA has developed two software products to address these limitations of conventional clustering technology—CA XOssoft Replication and CA XOssoft High Availability.

To accommodate this critical business continuity need, companies of all sizes may leverage two powerful technologies. Data replication with manual and automated failover provides offsite data protection and continuous application availability (HA). Continuous data protection, often referred to as CDP, enables organizations to protect data between their scheduled backups and instantaneously rewind their data back to a known good point-in-time before a data corruption event from accidental or malicious damage.

- **Replication and Failover.** In simple terms, data replication technology such as that provided by CA XOssoft Replication software, keeps a primary/production server synchronized with a failover/replica server by copying the data and all subsequent changes from one to the other, in either an ongoing real time or scheduled manner. The failover server is typically housed at a remote location for disaster recovery purposes, The replica server also maintains the same operating systems and applications as the production server. If the production server becomes unavailable for any reason, the replication software allows an administrator to reverse-replicate back to the production server after it has been repaired or replaced. Alternatively, the administrator can manually failover or redirect users to the replica server, application, and data. For high availability (HA), the replication technology also includes real-time server monitoring and failover options that will automatically start all applications on the replica/failover server and redirect users—with no manual intervention required. The process is transparent to users who typically continue to work as if nothing has happened. These critical capabilities are provided by solutions such as CA XOssoft High Availability software. A key component of any replication solution is an automated testing capability, especially one that may be scheduled for periodic testing and one that will not impact the production environment

or halt the replication process. Both CA XOssoft solutions include CA XOssoft Assured Recovery that provides this must-have capability.

- **Continuous Data Protection (CDP).** CDP technology captures every change made to files in a journal or log file and allows administrators to use a wizard-like GUI to quickly and easily rewind to a known good point-in-time before a data corruption event. CDP provides full data protection for periods of time between your backup jobs. Both CA XOssoft solutions include built-in CDP that is performed on the replica server to ensure that there is no impact to the production server or users. Together, Replication with manual or automated failover and CDP offer organizations a powerful business continuity solution to complement any backup solution. Microsoft provides a Hyper-V VSS writer that can be used to protect virtual machines in a **consistent state**. If the virtual machines are running Windows operating systems that support VSS and if Hyper-V Integration Components are installed in the guest operating system, the Hyper-V VSS writer is capable of communicating with the guest VSS framework to put guest applications in a consistent state for backup. CA XOssoft uses the VSS framework to detect the snapshot point and inserts a bookmark to indicate the point where the data is consistent.

## Implementing backups of Hyper-V environments using CA ARCserve Backup

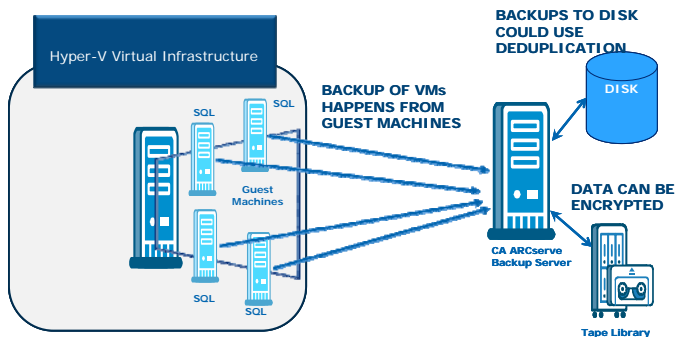
Now let's go through multiple scenarios on how you could back up the Hyper-V infrastructure using CA ARCserve Backup.

### Full Weekly Backup with Daily Differential Backups

A small organization is running Microsoft SQL Server, Exchange Server, and SharePoint Server on a Hyper-V virtualized server. They need to perform a backup of each application as quickly and easily as possible because IT staff is limited in number and experience.

By deploying the CA ARCserve Backup Agents for Microsoft SQL Server, Exchange Server, and SharePoint Server in each of the VMs, application consistent backup can be quickly and easily performed. The administrator can use the CA ARCserve Backup server console to submit Grandfather-Father-Son (GFS) backup jobs, selecting each of the VMs for backup. The administrator may select from the several backup options available such as multiplexing all of the data from multiple sources to a single tape drive, multistreaming while backing up to tapes, or encrypting the data while backing up to tape. Multiplexing and multistreaming help reduce the backup window, and encryption allows you to ensure all data is encrypted on tape. For disk-to-disk-to-tape (D2D2T) backup, the administrator first backs up to disk using data deduplication, and then specifies the policy to copy the data to tape. Since data deduplication decreases disk space utilization, data can be retained on disk for longer periods without adversely impacting storage resources.

The CA ARCserve Backup dashboard keeps track of the status of backups in progress, tracks recovery points, and monitors disk and volume fragmentation. Data can be restored from either disk or from tape. CA ARCserve Backup provides point-in-time restores and automatically chooses the necessary full backup, differential backup, or transaction logs for restores. If using encryption, CA ARCserve Backup remembers the passwords required to restore the data for you.

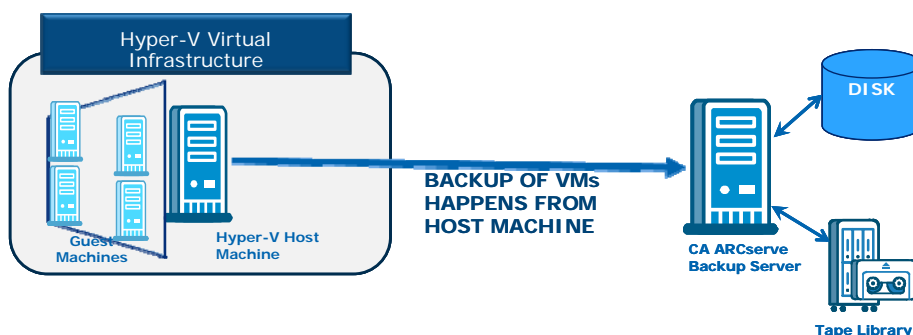


## Image-Level VM Restores and Granular Folder/File-Level Restores

In this scenario, an organization's backup strategy requires the administrator to perform complete VM restore for some VMs for Disaster Recovery, while being able to perform a granular file/folder restore on other VMs.

To accomplish this goal, the administrator installs the CA ARCserve Backup agent for the VM on the Microsoft Hyper-V Server. The agent will discover the VMs, publish them into the CA ARCserve Backup server, and perform the backups. By using the agent deployment tool on the CA ARCserve Backup server, the administrator can deploy the CA ARCserve Backup agent for VM on each of the VMs of the Hyper-V Server. The agent is installed from the central location simultaneously to multiple VMs. Please note that this agent is NOT used to move data—it is used to get a small piece of metadata during backup, which is used later for granular restores. This agent can also be used when you are performing granular files/folders restores.

Now the administrator can select the appropriate VMs and submit the backup job—all from a central CA ARCserve Backup console. This ensures full Image VM restores and granular file/folder restores. The CA ARCserve Backup Dashboard helps you by presenting statistics on backups, encryption, recovery points, trending analysis of backups, and many more SRM style reports on disk, volume, CPU, NIC, memory, and many other key data components.



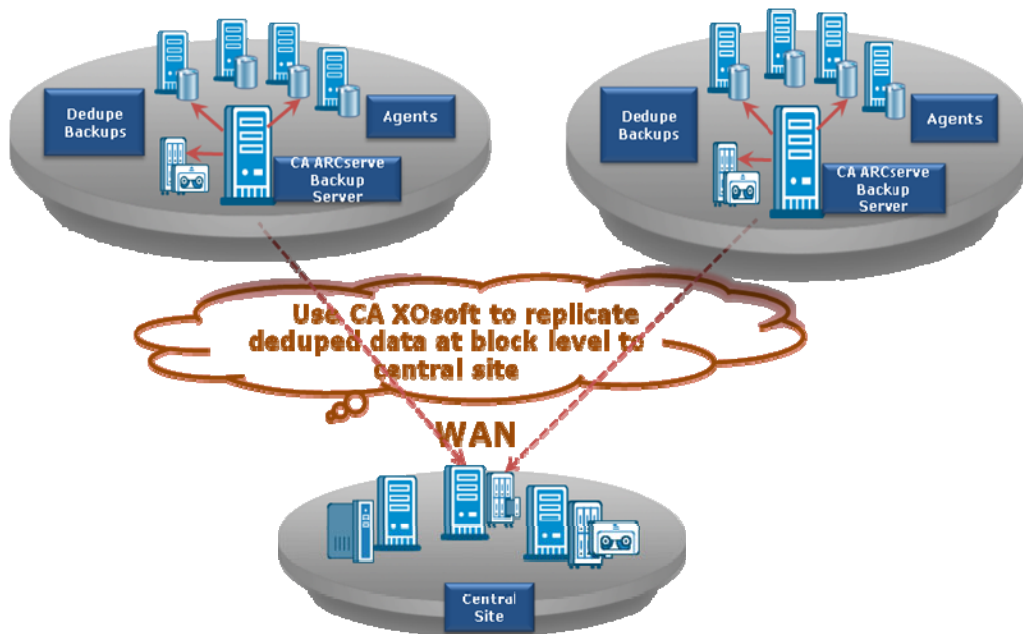
## Multiple Remote Office Backup

A midsize organization has multiple remote branch offices (ROBO), each with different backup requirements. Each office has multiple physical machines, some of which are under consideration for migration to virtual machines to reduce costs. There is a mix of both physical and virtual machines at some of the offices. The organization's backup/restore requirements are typical of

organizations of this size. To reduce backup costs and support from employees at each office, the decision has been made to perform backup to disk and eliminate all tapes at each ROBO. To improve recovery point objectives (RPO), the backup strategy includes the establishment of multiple recovery points at each ROBO for fast, granular restores and to reduce the probability of having to restore data from the central office. Restoration will be performed locally at the ROBO. Finally, all ROBO data must be made available at the central data center in case of a ROBO disaster.

Each ROBO will use CA ARCserve Backup to protect all the VMs and physical servers using backup to disk and deduplication. Since deduplication offers very high data compression, it affords frequent recovery points on disk at the ROBO offices. Deduplication can increase the number of recovery points with minimal disk utilization. According to a variety of sources, approximately 95% of all data recovery scenarios involve granular file/folder restores. Even with deduplication, these restores are usually very fast and efficient. This is due to the unique CA ARCserve Backup capability allowing granular file/folder restores from a full VM backup.

CA XOssoft Replication can be used to replicate the deduplicated data on disk at the ROBO site to the central data center. The central data center not only works as a ROBO DR site but by moving data to tapes it also provides long-term retention of data for compliance. In case deduplicated data is lost at a ROBO location, CA XOssoft Replication can be used to reverse-replicate the deduplicated data back to the ROBO location. In case the entire ROBO location is lost, deduplicated data at the central data center can be restored to VMs and shipped to a new ROBO location.



## Physical to Virtual Server Migration

An organization would like to quickly and easily perform physical to virtual server migration. CA ARCserve Backup allows you to perform Bare Metal Recovery of a physical server onto a virtual machine using the CA ARCserve Backup Disaster Recovery Option. Bare Metal Recovery (BMR) of a physical machine to a virtual machine also enables far faster recovery (within an hour) of an entire physical machine into a virtual machine providing minimal end-user downtime.

## Establishing a high-availability data recovery site by using Hyper-V and CA XOssoft High Availability

Before virtualization technology became generally affordable, physical server clustering was the standard way to implement high availability. Because hardware server technology is usually proprietary, these high-availability solutions were costly to implement, maintain, and scale. Deploying a high-availability solution that uses virtualization technology involves converting many of the physical servers to virtual machines. Newer and faster physical servers are often deployed to host the virtual machines.

This process of *server consolidation* provides the same level of availability as physical server clusters, with the following advantages:

- Fewer physical servers mean reduced power costs and requirements for cooling systems and floor space.
- Virtual machines can be easily moved between physical servers without reconfiguration or shutting them down. This process is known as *quick migration*.
- After a system failure, virtual machines can be quickly restored from backups and restarted. Administrators can restore manually or configure maintenance tools to automate the process.
- The hardware configuration of the physical servers can be modified without changing the configuration of the hosted virtual machines.
- Processing loads can be quickly reallocated between virtual machines to respond to changing use demands.

The following are two use-case scenarios where Hyper-V and CA XOssoft High Availability are used to administer high-availability clusters in high-availability contexts. The scenarios illustrate how high-availability clusters can be constructed from different configurations of physical and virtual machines. Some of the advantages and disadvantages of each scenario are included.

### **Basic High-Availability Scenario: Two Virtual Machines on a Single Physical Machine**

A small, budget-conscious, startup company can afford only one physical machine but requires the application high availability provided to SQL Server 2008 when run in a Microsoft Cluster Services (MSCS) environment. The physical machine runs Windows Server 2008 and Hyper-V and hosts two virtual machines running a clustered SQL Server 2008 and Failover Cluster. The virtual machines share a single SQL Server 2008 database. The virtual machines are managed by Failover Cluster as a cluster so that should the first virtual machine (active node) fail, the second virtual machine (passive node) gains control of the shared resources and keeps the SQL Server available for applications and users.

While this scenario fulfills the minimum requirement for a high-availability cluster, it does not protect against physical hardware failures or a site outage (or a software data corruption). The physical machine is a single point of failure because when it fails, the entire high-availability configuration also fails. Other advantages that clusters normally offer, such as planned physical server maintenance outages, are not possible. This configuration is most useful for quickly testing different high-availability cluster configurations using a minimum of hardware. The more complete solution would be to use CA XOssoft High Availability to enable automatic failover to a remote server providing continuous application availability.

## Large-Scale High-Availability Scenario: Physical-to-Virtual Environment with Advanced Data Recovery

In this scenario, the company has eliminated the physical server as a single point of failure by purchasing four more physical servers and two SANs. All of the physical servers run Windows Server 2008, Failover Cluster, and CA XOssoft High Availability. The first two physical servers host SQL Server 2008, the second two servers host Exchange Server 2007, and the fifth server runs Hyper-V. The first four share access to the first SAN, where all of the server application data is stored. The four physical servers at the main site are configured as primary servers, and the fifth is the standby server.

The standby server resides in a second corporate office and hosts four virtual machines—two running SQL Server 2008 and the others running Exchange Server 2007. Each virtual machine runs Failover Cluster and CA XOssoft High Availability. The second SAN is also deployed in this office as a backup storage device, and all of the virtual machines share access to it. All of the physical servers and SANs are connected by high-speed Ethernet over a WAN.

Here high-availability is maintained within the cluster as well as established across the WAN between the physical servers and the virtual machines. If either the SQL Server or Exchange Server fails on a primary server, the Failover Cluster switches server operations over to the SQL Server or Exchange Server running on the other primary server. In the event that the entire cluster of primary servers fails, CA XOssoft High Availability switches server operations to the corresponding virtual machine on the standby server.

In addition, the company's IT administrators use CA XOssoft Assured Recovery to periodically test the disaster recovery capabilities of the applications on the standby server, to provide scheduled off-host backups, and to implement continuous data protection for the data.

This approach provides several advantages to the basic high-availability scenario:

- A high level of failover protection is provided for the two server applications that are running at the main site.
- Data redundancy between the two SANs is supported.
- By using virtualization, the company does not need to purchase four more physical servers at the second site as backups for the primary servers at the main site. This saves hardware and maintenance costs.
- This solution is more scalable. If an additional physical server or another server application is deployed at the main site, another virtual machine can be hosted as a backup on the fifth server.
- Integrated CA XOssoft tools result in reduced system maintenance costs.
- Assured recovery and continuous data protection help ensure the recoverability of your data.

## Conclusion

Server virtualization reduces the cost of implementing recovery management solutions and improves optimization of computing resources. However, if the deployment is not planned properly, much of the efficiencies that are gained from server virtualization can be lost.

For this reason, as part of the plan, companies should consider reliable recovery management solutions that work well in both physical and virtual environments and that provide robust system management tools. CA ARCserve Backup and CA XOssoft High Availability and Replication products offer world-class technology for protecting file and application servers that are running in physical and virtualized environments such as Hyper-V.