White Paper

The Convergence of Backup & Replication

Real Answers for Today's Business & IT High Availability Requirements

October 2006

Table of Contents

Executive Summary

The needs of business today extend far beyond the data protection provided by traditional backup and restore — they require full 24/7/365 protection for true business continuity. In an increasingly competitive business environment, accessibility and availability of information is often the differentiator between success and failure.

In this paper we will briefly review the new realities of business continuity and disaster recovery for businesses today. These realities give rise to new requirements for effective data protection and recovery management, requirements that go beyond simply protecting data and aggregating a variety of point solutions. Instead, what is required is an integrated recovery management system that provides the ability to balance costs and risks through policies that reflect real business priorities. This system must be able to make use of the entire range of recovery technologies from archival storage of long-term data to continuous application availability through replication, CDP and automated failover.

The combined capabilities of BrightStor® ARCserve® Backup and CA XOsoft™ WANSync™ application availability platforms represent a significant step toward fulfilling these requirements. Already today the integration of the two products offers key benefits like the elimination of backup windows and consolidation of branch office backups.

CA XOsoft Today and Beyond

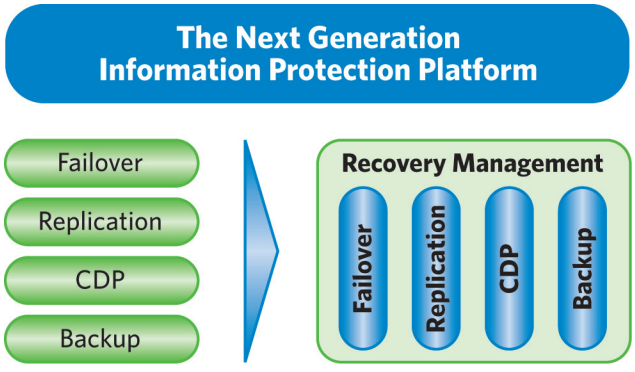


Figure 1. Next Generation Recovery Management under a Single Unified Platform.

"Today we combine previously autonomous solutions into a single platform that spans the continuum of data protection needs (RTO and RPO) and aligns information protection with business requirements."

— Mat Dickson, VP of Product Development, BrightStor Recovery Management, CA

Business Continuity Today

There is a growing shift of focus in data protection from restore and recovery — the ability to find and reinstate data that has been lost or damaged — to real business continuity — the ability to continue operating the core functions of the business through and after a disaster with little or no disruption. This change of focus leads to significantly different requirements and demands new kinds of data and application protection technologies to support it.

There are a variety of factors that are driving this shift, including the increasing cost of both downtime and of inadequate response to disasters, the growing importance of information, and the increasingly distributed nature of IT operations. In the end, traditional approaches have become too limited to address the full range of recovery needs.

According to various industry analysts over 70% companies go out of business after a major fire — data loss being the primary reason.

The Cost of Failure is High

The bottom line is that the cost of not having the right recovery capabilities in place for business critical applications to ensure adequate business continuity is very high.

A study of 80 large organizations by Infonetics Research found that overall downtime costs averaged an astounding 3.6% of annual revenues.[1] Also various industry analysts regularly site studies that estimate that downtime for mid-sized organizations running Microsoft Exchange can cost thousand of dollars per hour, while large e-commerce sites like Amazon and eBay can easily see these hourly downtime costs soar into hundreds of thousands of dollars.

The ultimate cost is going out of business, and unfortunately many companies are forced to pay this high cost.

More than 40% of businesses never re-open their doors after a disaster according to various Industry Analysts reports

The Importance of Information is Growing

Information has always been a core component of business value and competitive advantage, but the importance of digital information has exploded. There are many interrelated factors that have driven this trend, including:

- Increasing IT penetration into core business processes
- Explosive data growth and consequent increase in the complexity and expense of managing data
- Increasing IT penetration into business infrastructure, like communication (email, IP telephony, IM, etc.)
- Radically growing customer power through increased information access
- Growing government compliance requirements (HIPAA, SOX)
- Increasing demand for transparency
- 24x7 remote access & file sharing

For most business today access to information and to the applications that manipulate it are critical to normal operations. When key IT applications and storage are down, the business is down.

It's No Longer Just about the Data Center

According to a recent report by Nemertes Research more than 90% of employees are located at branch office facilities. Even more strikingly, the number of employees working away from their direct management has increased by 800% in the past five years.[2] The expansion of branch office facilities and distributed operations is expected to continue for the foreseeable future.

Decentralized operations present serious IT challenges, particularly in backups, distribution and consolidation of content, and security. Ongoing expansions of branch operations coupled with the explosive growth of data in both size and importance to business translate to a similar growth in complexity of backup, management and recovery of data in highly distributed organizations.

Of particular importance is the issue of backing up critical business data across branch offices. It is clearly not cost-effective for most organizations to maintain sophisticated IT personnel at every location to ensure the integrity of local backup operations. Neither is it safe to place the burden on non-IT staff, for whom performing and verifying backups are unwanted and burdensome tasks. If these tasks are skipped or performed inadequately, however, critical corporate data is put at risk.

Traditional Approaches Alone Are Inadequate

In traditional IT organizations the focus is on backup alone, primarily to tape. New technologies like disk-to-disk and disk-to-disk-to-tape backup systems have alleviated some shortcomings of traditional tape backup systems, but remain inadequate to deal with the full range of requirements for maintaining availability of critical data and applications. Significant issues associated with traditional tape backup and vaulting solutions include:

- Security risks and expense of transporting tapes
- Application downtime due to backup windows
- Limited recovery granularity (i.e., increased risk of data loss)
- Long recovery times
- Complexity of managing and ensuring the integrity of tape backups

IT organizations today can no longer afford to leave these issues unaddressed. It is time for a new approach.

[1] Source: "Large Companies Lose 3.6% of Annual Revenue to Network Downtime", Infonetics Research, February 11th, 2004

[2] Source: "No Easy Fix for Branch Office Blues" by James Rogers, Byte and Switch, June 21, 2006

Requirements for a More Effective Solution

Dealing with today's requirements for 24 X 7 X 365 access to IT resources demands an updated approach to data protection, one that is focused on recovery rather than backup, and one that enables your business to balance the costs and capabilities of your recovery strategies, and the actual value and risks of the systems they are designed to protect.

The Enterprise Strategy Group (ESG), storage analyst firm, has recently introduced the 3DR framework for thinking about data protection.

In this framework, the 1DR level is disk-based and local — ESG believes all recoveries should originate here. 2DR is also disk-based and targeted at disaster recovery — it is an exact replica of the data stored at a different geographical location to be used to recover from a complete outage of the primary data location.

Finally, 3DR is maintaining duplicate copies of unique, critical data on tape in a safe storage location — it is for the worst case and is not intended for normal recovery.

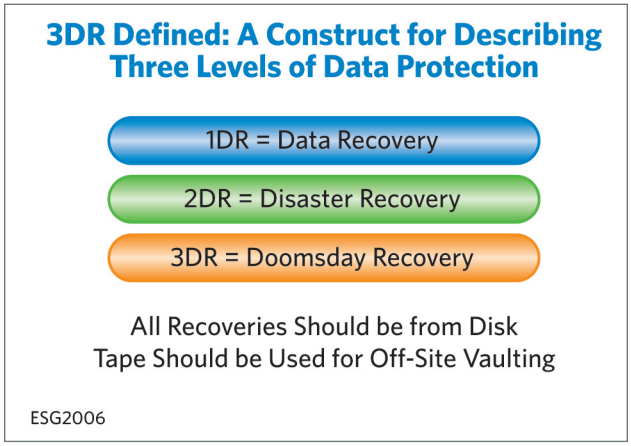


Figure 2. ESG's Multilayer Data Protection Model.[3]

The key idea in both cases is that organizations need to implement different levels of data protection to address different recovery requirements, depending on business priorities and the particular data and where it is in the data life cycle. In addition, effective protection requires layering solutions, from mainstream technologies like RAID, tape backup, and snapshots for basic data protection to technologies like online replication, continuous data protection (CDP) and automated application failover for rapid recovery and minimized data loss.

Figure 3 below presents a similar mapping of technology to data type and recovery requirements.

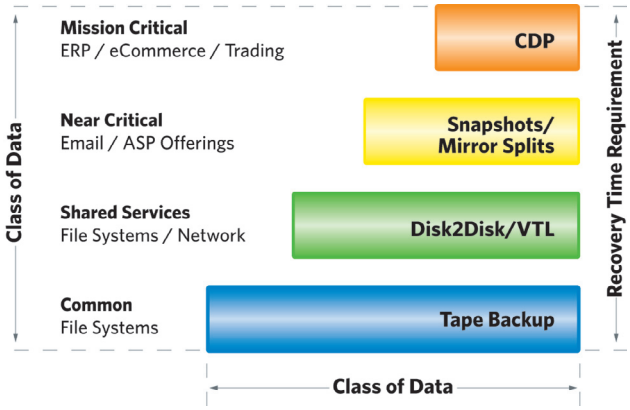


Figure 3. Data Classification Model for RTO and RPO.

More generally, an adequate overall recovery approach should be simple to manage and provide the flexibility to balance risk and cost appropriately. It must offer a full range of methods to address different requirements for minimum data loss (or RPO — recovery point objective) and maximum time to recovery (or RTO — recovery time objective), and should be application aware to best tailor functionality to business needs.

An Integrated Recovery Management System

In summary, what is required is an integrated recovery management solution that offers a range of choices based on business needs and costs, from basic long-term data storage for 3DR doomsday recovery to true continuous application availability for mission-critical 24 X 7 operations. Because recovery requirements are tied to the business value of the data and application, it is necessary that this recovery management solution be an integral part of a system that unifies the administration of all components of data management under a single umbrella, bringing recovery management together with information and resource management in a single administrative environment.

[3] Source: "The New Data Protection Story" presentation by Heidi Biggar, Enterprise Strategy Group, Inc., 2006, p. 35

The system must offer good data and process classification granularity that enables business policies to be tied directly to data management policies in order to provision appropriate recovery schemes. Moreover, such a recovery management system must fully integrate high-availability and continuous data protection (CDP) technologies for rapid recovery together with traditional backup/archive scheme, all controlled by policies driven by the classification assigned to given data. At the same time, enterprise-wide management and reporting will offer organizations flexible and granular control of their information, resource and recovery management.

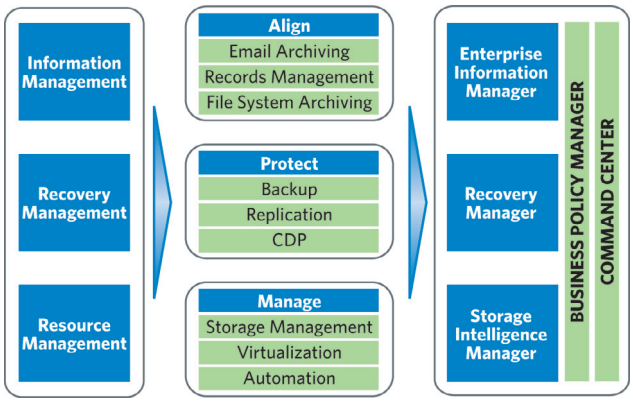


Figure 4. The vision of an Integrated Data Management System.

- **Customizable Classification.** Classification of data and processes must be based on actual business requirements in order to permit explicit tradeoffs between cost and specific recovery objectives. Classification should be able to incorporate information on business processes, applications, data lifecycle, and architecture at all relevant levels of detail.
- **Multilayer Protection.** Effective risk mitigation requires the ability to build multiple layers of protection that incorporate a variety of technologies, including local and remote tape backup, D2D systems, online replication, automated application failover, CDP and others.
- **Verifiability.** An adequate recovery management system must provide the ability to monitor system status at all times and should integrate regular testing of recovery systems.

"Backup management software isn't enough any more. We need to flesh it out with failover, replication and CDP."

— Bob Davis, SVP and General Manager, Storage Business Unit, CA

The BrightStor CA XOsoft Integrated Solution

CA's Integrated Recovery Management — A New All-In-One Solution

The combination of BrightStor ARCserve Backup and CA XOsoft WANSync platform for continuous data protection and application availability provides tremendous capability today and lays a foundation for a comprehensive Recovery Management solution for protecting and recovering critical applications and services.

BrightStor ARCserve Backup already provides customers with high-performance disk-to-disk (D2D), disk-to-tape (D2T), disk-to-disk-to-tape (D2D2T), backup encryption and integrated antivirus protection; multiplexing and snapshot backup and recovery capabilities. CA XOsoft WANSync complements these by adding continuous data protection, replication and automated application failover. The combined solution already delivers the ability to align information protection solutions with business requirements across the full range of data protection needs for both speed of recovery and maximum allowable data loss (RTO and RPO).

Going forward, closer integration of the BrightStor ARCserve and CA XOsoft WANSync technologies will yield an integrated Recovery Management solution that can automate data recovery management through policies driven by data and process classification.

Many vendors offer point solutions for backup, replication and recovery, but without integration system complexity remains high and reliability limited. The combination of products already offers a significant level of integration through the CA XOsoft™ Assured Recovery™ technology for both automated testing and validated backup using BrightStor ARCserve Backup.

The result:
A solution that allows effective balancing of risk and cost to tip the scales toward:

- Lower risk of data and business opportunity loss
- Lower total cost of ownership
- Simplified data and recovery management
- Recovery solutions aligned with business needs

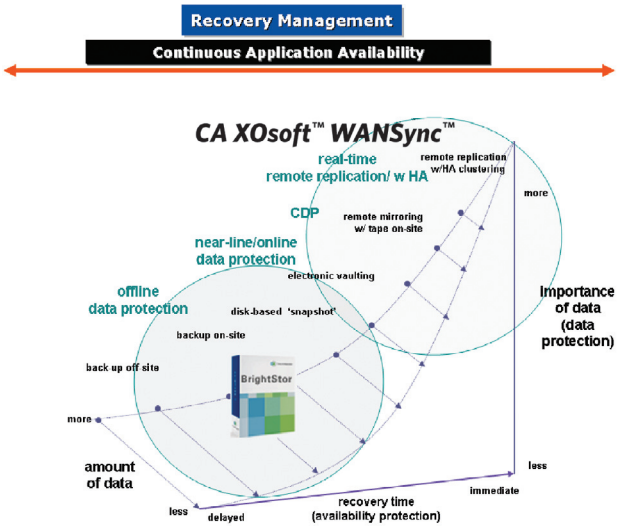


Figure 5. Integrating data recovery choices based to business needs and cost.

Together, BrightStor ARCserve Backup and CA XOsoft WANSync enable you to address the full range of your data protection needs.

The core capabilities of the combined technologies include:

- High-performance D2D, D2T and D2D2T backup and snapshots
- Backup encryption and integrated antivirus protection
- Build-in device and media management
- Real-time replication of files and databases as they change
- The ability to rewind to any previous point in time to recover from corrupted data (continuous data protection — CDP)
- Automatic failover of an application to a standby server at another location and push-button failback of the application once the production server is restored
- Real-time consolidation of data from branch offices to a central datacenter (centralized backup / data consolidation)
- Non-disruptive, fully automated testing of the disaster recovery replica server

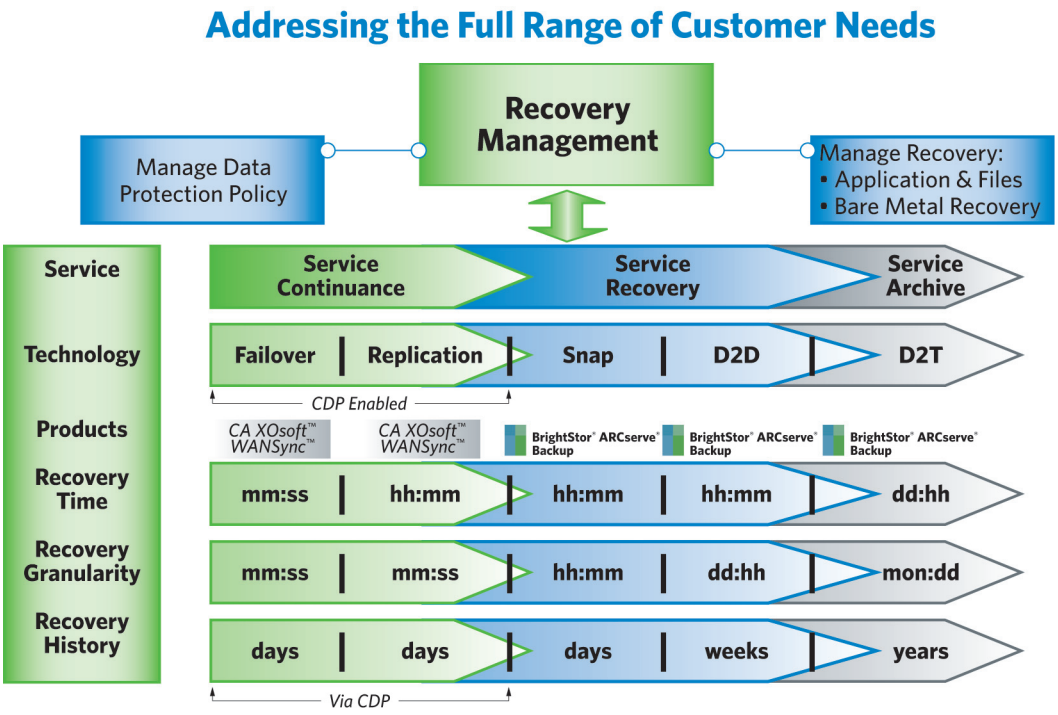


Figure 6. Choose the right technology based on your requirements.

"It is all about the benefit of choices...you can deploy HA replication and still have the benefits of archive..."

— Mat Dickson, VP of Product Development, BrightStor Recovery Management, CA

Phase I Integration — Backup Windows and Branch Offices

The combination of BrightStor® and CA XOsoft™ technologies provides a foundation for a variety of exciting future developments, but there are also very significant new capabilities that arise from the integration of the two products today. Two that are of particular interest are: the ability to employ a disaster recovery replica server to provide an easy offsite backup while eliminating the backup window from the production server, and the ability to consolidate backups from distributed branch offices at a single central location for reduced cost and improved security and manageability.

Using DR Replication to Address Backup

Real-time data replication is a mature disaster recovery technology that can add an important layer of protection to traditional backup solutions. An over-the-WAN asynchronous replication product like CA XOsoft WANSync, provides the ability to maintain an always-up-to-date copy of your critical application data at a secure secondary site.

It seems natural to try to use the copy of the data at a secondary site to perform an offsite tape backup. Unfortunately, replicated data does not naturally lend itself to use for backups or snapshots since there is no way to ensure that the data is in a consistent, backup-ready state at the time a backup is taken. The CA XOsoft Assured Recovery product has unique patent-pending technology which removes this limitation.

CA XOsoft Assured Recovery is designed to allow in-depth testing of the recoverability of the application on the replica server without any disruption to the production server, to the replication process, or to the automated failover protection mechanisms that are in place in case of a disaster.

Backups are Performed off the Replica Server, hence maintaining Continuous Application Availability.

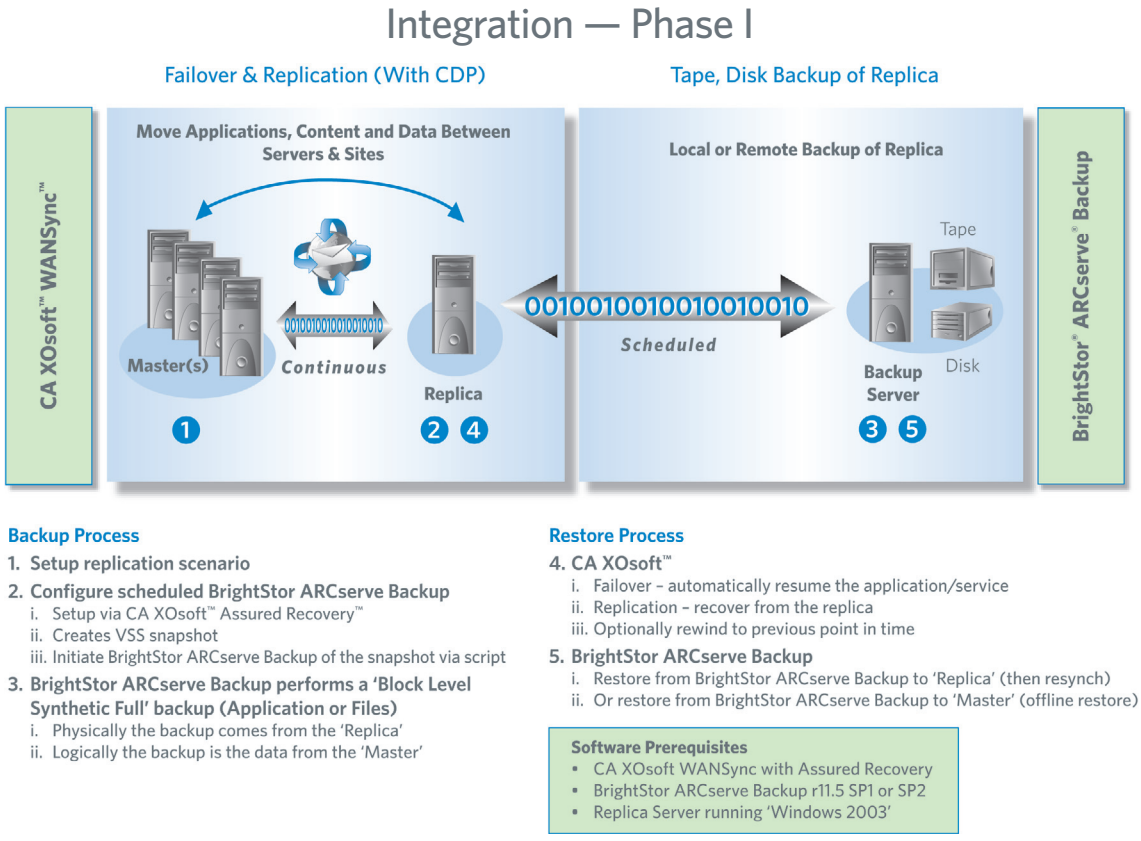


Figure 7. Integrating Replication, CDP with Traditional Backup.

In CA XOsoft Assured Recovery, application of replicated changes on the replica data is temporarily suspended and the application (Exchange, MS SQL Server or Oracle) is started and tested in a fully automated fashion. Manual testing can also be enabled or custom scripting can expend automated testing to virtually any application or database. In effect, CA XOsoft Assured Recovery allows the replica server to remember the state of application data exactly as it was when application of changes was suspended so that, after testing, the data can be returned to that state and replication continued normally. At no point is the production server impacted, nor is it left unprotected, since changes continue to be replicated to the disaster recovery server throughout.

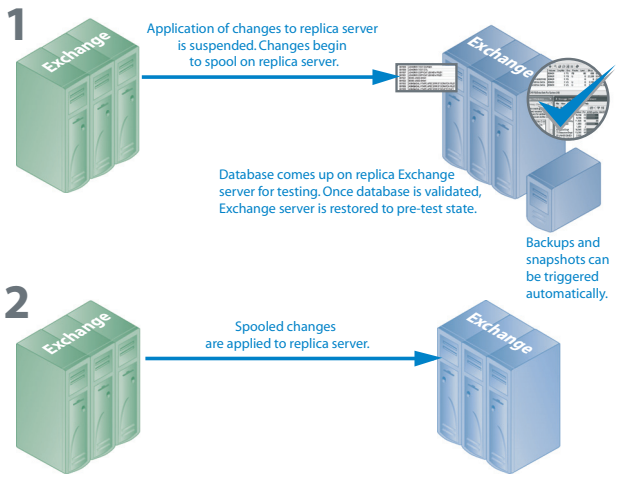


Figure 8. CA XOsoft™ Assured Recovery™ Process Validates Replicas Data followed by automatic Backups and Snapshots.

Once testing is complete, CA XOsoft Assured Recovery has the ability to automatically trigger a backup or snapshot of the just-validated data on the replica server. In effect, this architecture gives you two layers of protection at once: remote replication for disaster recovery (optionally with automated application failover) and a **fully validated offsite backup** with no impact on your production server.

Branch Office Backup Consolidation

In the case of branch offices, an architecture comprised of CA XOsoft WANSync and CA XOsoft Assured Recovery together with BrightStor ARCserve Backup allows the creation of backup replicas of branch office servers at a central data center for a double benefit: disaster recovery and continuous application availability capabilities for your branch office servers together with centralized consolidated backups of multiple branch offices at a single facility, thus significantly reducing the need for sophisticated IT support at every location. In addition, the solution mitigates the security risk with tape transport and offsets existing tape media and handling costs.

This is a significant improvement over the islands of mini-data centers managing critical enterprise data in seclusion that are typical for branch office situations.

Asynchronous Replication Technology Enables:

- Real-Time Consolidation
- Centralized Backup
- Multiple Backup Locations for DR
- CDP for Rapid Recovery

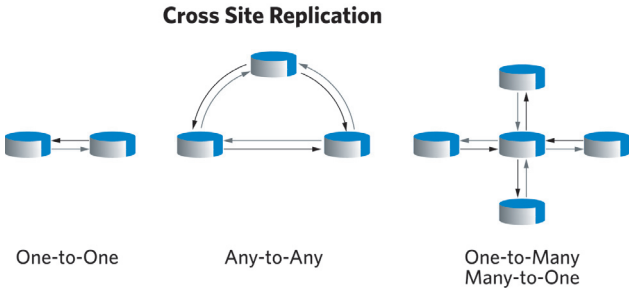


Figure 9. Distributed Multilevel Replication.

The CA XOsoft WANSync platform is also an ideal solution for distributing reference content to internal users throughout a distributed enterprise, such as price lists, policies, sales materials, manuals, news and other relevant information. By allowing content to be maintained in a single central repository with automatic delivery of any changes to target servers throughout the organization either immediately or on a scheduled basis, CA XOsoft™ WANSyncCD easily eliminates the problem of out-of-sync field and branch office data.

BrightStor/CA XOsoft Integration at a Glance

Combining the Best of Breed Award Winning Solutions

The new combined CA XOsoft family of solutions covers the complete range of customer needs for recovery management, from high performance backup and backup management to continuous data protection, online replication, and over-the-WAN automated failover.

The combined offering brings immediate benefits in security, productivity and control, as well as the ability to truly tailor the recovery solution to the specific needs of your business.

Here are just a few of the specific benefits of the new product set.

- Multilayer protection — flexible RPO & RTO
- Choice of the right protection method(s) based on business criticality of the data
- Validated backup with CA XOsoft Assured Recovery
- Synthetic full backup for reduced bandwidth requirements and faster recovery of data from backup media
- Integrated CDP for faster recovery and reduced data loss
- Eliminate the need for IT specialists in branch offices through backup consolidation
- Eliminate backup windows and strain on production servers
- Securely manage removable media in a dedicated location with IT professionals
- Minimize media transportation
- Manage data consistently in line with corporate policies
- Protect current hardware and software investments

New Equations for Recovery Managment

Integrated Backup & Assured Recovery	=	**Time Savings**
Real Time Replication & Integrated CDP *(Real-time Protection for Business Continuity)*	=	**Business Savings**
Backup Consolidation & Remote Management	=	**People Savings**
End-to-End Reliability	=	**PRICELESS**

Looking Forward

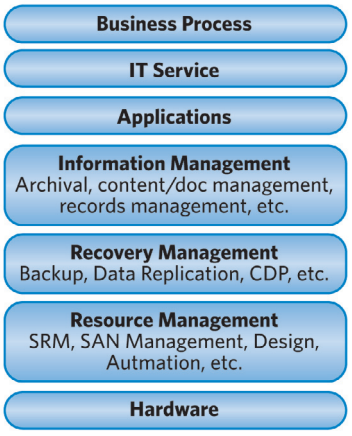
Today the combined CA XOsoft offerings deliver solutions for the entire range of critical backup and recovery issues by combining traditional backup with replication, integrated CDP and automated application failover.

The Future of Recovery Management

Policy-based interface maps technologies to requirements according to business requirements at all points in the information value chain.

Future integration efforts will build on this foundation to provide a truly integrated system of information, resource, and recovery management by providing a policy-based management environment that allows classification of all the elements necessary to manage, protect and align information, data and resources with business objectives, from low-level hardware management all the way up to the core processes of your business.

The Information Value Chain



For additional white papers visit us at:
www.ca.com/xosoft

Quality System
Quality Endorsed Company
ISO 9001
Lic. 2443

CA XOsoft

MP308451006