Computer Associates International, Inc.
One Computer associates Plaza
Islandia, NY 11749
631-342-6000

Darwin's Groceries, Inc.
One Darwin Center
New York, NY 11011

Re: Request for Information – Data Protection through Replication

Dear Sir,

Thank you for providing Computer Associates International, Inc. ("CA") with the opportunity to respond to your above referenced Request for Information ("RFI"). As the world's leading independent software and services supplier, CA welcomes the opportunity to provide software products and services responsive to your needs. Accordingly, we are pleased to submit our attached proposal.

Computer Associates International is one of only three independent software vendors in the world that has generated more than $1 billion in operating cash flow for five years in a row. With over 26 years of successes, Computer Associates has proven again and again that it is a solid company, evidenced by CA's long-term service, support and ongoing product enhancements.

CA also holds the distinction of being the first and only enterprise software company that is ISO 9001:2000 certified. ISO 9001:2000 certification demonstrates that CA's entire organization is focused on delivering solutions and services of the highest quality. The coveted certification followed a comprehensive audit of CA offices in 40 countries by Quality Assurance Services, an independent agency authorized to determine whether companies have met the exacting standards set by the International Standards Organization.

Please be advised that the information contained in our response to the RFI is furnished at this time for the sole purpose of permitting you to make a considered technical and commercial evaluation of CA's proposal.

If you have any questions regarding this proposal or if any supplemental information may be desired, please contact me directly at (631) 342-6000, email jane.salesperson@ca.com.

Sincerely,

Jane Salesperson
Sales Executive

Table of Contents

EXECUTIVE SUMMARY **5**

THE BRIGHTSTOR REPLICATION MANAGEMENT SOLUTION **9**

AVAILABILITY OF CRITICAL DATA 11
Causes of server downtime 11
THE CASE FOR CLUSTERING, MIRRORING AND HIGH-AVAILABILITY 12
Clustering 12
Data mirroring 12
High-availability 13
BRIGHTSTOR HIGH AVAILABILITY 13

BRIGHTSTOR HIGH AVAILABILITY – SPEED AND SECURITY **15**

KEY TERMINOLOGY 15
A SIMPLE BRIGHTSTOR HIGH AVAILABILITY INSTALLATION 16
SYNCHRONIZATION 18
REPLICATION 19
FAILOVER 21
REINSTATEMENT 23
BRIGHTSTOR HIGH AVAILABILITY MANAGEMENT 23

PUTTING BRIGHTSTOR HIGH AVAILABILITY TO WORK **25**

PLANNING FOR BRIGHTSTOR HIGH AVAILABILITY 25
Hardware and Software Requirement 25
Server loading, both current and planned 26
Access to servers 26
Control over applications and services 27
PROTOCOLS 27
OPERATIONAL CONSIDERATIONS 27
The drives and folders to be replicated 28
NTFS security 28
Replication of shares 28
Handling a communications failure 28
Alerting 29
Critical levels of free disk space 29
Primary server identification 29
Failover and reinstatement scripts 29

BRIGHTSTOR HIGH AVAILABILITY WAN FAILOVER **30**

CONFIGURING FOR A FIREWALL ENVIRONMENT 31

CONCLUSION **33**

BRIGHTSTOR STORAGE RESOURCE MANAGER -- 33

PRODUCT OVERVIEW – BRIGHTSTOR SRM 34
BRIGHTSTOR SRM COMPONENTS 35
ARCHITECTURAL PLAN 37
System Components 37
Supported Operating Systems and File Systems 39
CA's Architecture Recommendations 41

BRIGHTSTOR PORTAL -- 42

OVERVIEW 44
SOFTWARE COMPONENTS 44
ARCHITECTURAL PLAN 44
Components 44

BRIGHTSTOR ENTERPRISE BACKUP -- 47

SPECIFIC TARGET ENVIRONMENT 48
SYSTEM REQUIREMENTS 48
Windows: 48
UNIX: 48

DARWIN'S GROCERIES RFI QUESTIONS AND RESPONSES 57

DARWIN'S GROCERIES RFI QUESTIONS AND RESPONSES 57

EXECUTIVE SUMMARY

As the amount of enterprise data has grown, efficient data protection management has become a priority. All the planning and maintenance in the world cannot prevent a server or application crash. Statistics show that it is not a question of *if* systems will fail, but *when*. Such failures can shut down a production infrastructure and your business. System downtime all too often results in lost business opportunities, dissatisfied clients and damage to your reputation. In today's time-critical, web-enabled marketplace, it is imperative that critical business continues uninterrupted.

The foundation of Computer Associates' proposed BrightStor Replication Management Solutions is based on technologies that combine replication, storage monitoring, traditional backup and restore and central management of all storage processes via a web browser.

By identifying the threats and the risks they represent to your business, you can use the business value of the data as the selection criteria to identify appropriate recovery solutions in each scenario. This approach simplifies the disciplines of Disaster Recovery and the IT aspects of Business Continuity. Risk Mitigation demands experience in managing networks, system, applications, and security. CA is uniquely experienced to provide state-of-the-art Risk Management solutions through its offerings in the BrightStor suite of products. In today's ultra-competitive and cost-conscious world, even the smallest parts of a business can impact the top and bottom lines. And when something is as central to an organization's performance and survival as its data and the storage that contains it, efficiency, or lack of it can have a major impact. Innovative BrightStor management solutions bring efficiency to all aspects of today's storage environments, enabling enterprises to truly streamline their operations through in-depth storage knowledge and advanced administration capabilities.

BrightStor High Availability from Computer Associates International, Inc. (CA) helps enable continuous business operations and is a necessary component of any data protection and availability plan. Once critical data is defined, it is automatically replicated to a secondary server in real time—ensuring nonstop access even if a server suffers catastrophic damage. BrightStor High Availability continuously protects

data by automatically replicating any changes and updates to the secondary server as they occur. This powerful solution can automatically detect services and/or server failures and instantly switch end users to the secondary server, whether local or remote. The secondary server assumes the complete identity of the primary, including its host name and IP address, as well as continuing to process its normal workload. The entire failover process occurs in real time and is completely transparent to the end user.

The BrightStor Storage Resource Manager industry leading cross-platform SRM solution enables organizations to centrally manage distributed storage assets in heterogeneous environments from a single global view. Computer Associates continues to refine and enhance the BrightStor Storage Management Solution Suite today based on input from clients and incorporates industry developments and standards.

The BrightStor Replication Management Solutions is as outlined in this response is designed to enable storage management without boundaries; data is viewed as a business-critical asset to be managed regardless of location or platform. Valuable data assets on mainframes, mid-range systems and even desktops, SAN, NAS or DAS connected, can be viewed and managed from one centralized point. Our vision is to help companies like Darwin's Groceries make storage management simply another part of your overall systems management thereby increasing efficiency and reducing storage management costs. With CA's legacy in systems management as well as storage, CA is uniquely positioned to provide its experience and best practices for Darwin's Groceries.

Darwin's Groceries has shared information with CA about their current storage environment and operations including challenges and desired outcome. The proposed solution should include mechanisms or functionality for:

- Hosting replicated data on storage platforms or topologies that do not replicate on a one-for-one basis storage platforms located in the production environment, thereby enabling greater flexibility and lower cost for the overall recovery strategy
- Monitoring the on-going performance of the replication strategy

- Testing the replication strategy without disrupting normal application or storage operations
- Securing data from eavesdropping or unauthorized access during the replication process and after "fail over" of application access to the replicated data set
- Scaling readily in response to increases or decreases in the volume of data to be replicated
- Culling from replicated data duplicate and/or non-critical data as well as data or files containing virus signatures or other malicious software code
- Automated techniques for optimizing data transfers across WAN interconnects of varying bandwidth and for optimizing WAN interconnects for best possible cost-efficiency

Summary: Darwin's Groceries wishes to securely replicate mission critical data from all remote offices to their central site and then ensure availability of the central site to an alternate central location. It wishes to increase span of control including the ability to manage more with less and still ensure future application availability.

A software based replication strategy that is hardware agnostic would mean that Darwin's Groceries could fill storage demand with existing storage assets rather than having to buy new storage capacity and would also be able to maximize the value of future planned purchases. BrightStor High Availability will provide the replication functionality required by Darwin's Groceries to replicate data in real-time to the central location. Darwin seeks repeatable automated processes for capacity planning that would assist in bringing applications on-line faster and facilitate just-in-time purchasing. The BrightStor Storage Resource Manager will provide the management tool necessary to automate routine tasks at the central location while providing information on enterprise-wide storage capacity, allocation, usage, trending and forecast to help Darwin's Groceries improve storage utilization. Once data has been tracked and filtered for duplication by the BrightStor Storage Resource Manager product, the data can be replicated via BrightStor High Availability to the alternate central site.

BrightStor Enterprise Backup at the central location will provide local backup and restore functionality at the central and alternate central sites.

The BrightStor Portal will then facilitate a "single pane of glass" to view all storage processes from anywhere on the network via a web browser.

We have learned that Darwin's Groceries is seeking a solution that is a technical "fit", is proven in the field, and from a company that shares a commitment and strategy for storage management that is compatible with Darwin's Groceries vision. The benefits Darwin's Groceries can derive from CA's BrightStor Replication Management Solutions are numerous. The complexity and size of Darwin's Groceries environment presents challenges that the CA Solution addresses through the breadth of system and storage platforms supported and the hierarchical architecture for scalability. CA's BrightStor Replication Management Solution would provide Darwin's Groceries the ability to manage their storage environment to ensure "right data at the right time on the right media".

Computer Associates has proposed a comprehensive solution to address Darwin's Groceries business and technical requirements in the storage arena. All solution components discussed above and outlined in the response are fully integrated from CA.

CA is confident that Darwin's Groceries will find our response both meets and exceeds your technical and business requirements. The CA response is focused to complement and leverage Darwin's Groceries current storage and infrastructure investments, provide quantifiable cost reductions, and provide an open foundation for new investments in technology.

CA welcomes the opportunity for Darwin's Groceries to leverage our BrightStor Storage Management technologies as well as our best practice experience to solve your immediate business requirements.

THE BRIGHTSTOR REPLICATION MANAGEMENT SOLUTION

This document follows a distinct progression and flow. It can best be characterized through the following logical steps:

- Darwin's Groceries needs and initial assessment
- CA's proposed solution to address these needs
- In depth product information relevant to Darwin's Groceries needs
- Request For Information questions and answers
- CA Solution summary

The intent of this document is to provide Darwin's Groceries with a proposed solution that will address the current environment needs as well as provide a solid foundation for future growth.

The proposed BrightStor Storage Resource Management Solution will help Darwin's Groceries reduce costs through increased utilization, increased span of control with the ability to manage more with less and to insure future application availability.

The proposed BrightStor Storage Replication Management Solution provides a highly scalable management infrastructure that can be deployed in a departmental or geographical fashion and still allow for global, enterprise wide manageability. As the components are installed across the enterprise, all of the gathered data and managed systems can be made available in both local offices and data centers. Having all of the information about Darwin's Groceries storage infrastructure available in a single management console allows for quick and easy data correlation, which simplifies policy creation.

BrightStor Portal is the Executive Dashboard for the storage environment, enabling organizations to have a central view and central access to their storage operations, the "single pane of glass". BrightStor High Availability serves as the foundation of the BrightStor Storage Replication Management Solution. Real-time replication of data from the smaller stores to the central location can be accomplished via block level delta transfers which eliminates the need for huge data transfers that saturate connections at specific times. It also assures that in the event of

server failure all data is immediately accessible via IP Spoofing once redirected. The BrightStor SRM Solution is used to gather data regarding the logical portion of the storage environment. The BrightStor SRM Solution starts with a top down view of the entire storage environment, yet allows for drill down into individual servers and volumes to see key utilization details. These details allow the organization to become more efficient and cost effective by understanding the nature of the data, the criticality of the data to operations, and associating it to the proper media or removal. The BrightStor SRM Solution can also be used to prevent out of space conditions for critical applications, operations, or users by setting thresholds on disk utilization, disk space by user or department, and many other numeric attributes. These thresholds can then be used for alerting and automation. The data gathered by BrightStor can also be used to view trends in storage usage and generate forecasts on the same.

All of this information generated by BrightStor can be presented up to the BrightStor Portal for a single point of administration. All statistics and data can be viewed and manipulated using a web browser by the storage administrators. In addition a subset of this information can be offered up to local or departmental storage administrators, based on the needs of that administrator. The tight integration of the BrightStor SRM Solution allows for seamless management of the entire storage infrastructure.

Using BrightStor High Availability as the foundation, BrightStor Portal as the management console and SRM as the data "monitor", the BrightStor Replication Management Solution gives a comprehensive view of the enterprise from a logical point of view. BrightStor Enterprise Backup will protect data at the central and remote sites by offering a combination of traditional tape as well as backup to disk functionalities for faster access to mission critical applications. It is imperative that mission critical databases have the ability for lightning fast restores from disk vs. the slower tape method.

The integration of the BrightStor Replication Management Solution components is extremely valuable to the management of any storage environment. Over the past several years, CA has made significant strides to tightly integrate our solutions. We continue that effort today to bring even tighter integration through the consolidation of our technologies and central consoles.

The Server Resilience Problem

Availability of Critical Data

Many organizations concentrate most or all of their critical corporate data on a relatively small number of servers. The security of this data can be assured using state-of-the-art backup technology, such as BrightStor Enterprise Backup or BrightStor ARCserve Backup. However, there is still a real problem in providing continuous availability because of the significant time it takes to repair a failed server and bring it back into service. In cases where it is imperative that critical business continues uninterrupted, a new class of solution is clearly required.

Causes of server downtime

An unprotected server represents a single point of failure. Data residing on such a server and business processes executing on it are vulnerable to hardware faults, software crashes, operator error, power failure and many other potential causes of server outage. Recovering from an outage typically involves repairing or replacing hardware, restoring data from backup tapes or even rebuilding the server. Although some of these recovery actions can be very efficient, for example if the BrightStor Enterprise Backup or BrightStor ARCserve Backup Disaster Recovery Option is employed, the server could still be unavailable to provide the services to it's customers for some hours. Without a disaster recovery facility, the recovery of a server could be days.

It is true that some causes of server downtime can be minimized, for example by using redundant hardware, multiple network connections, RAID systems, and so on. However, the cost of these measures, if implemented effectively, can escalate rapidly, and the server still remains a single point of vulnerability.

Recent developments have seen a proliferation of data and server protection solutions each with their own advantages and meeting specific market needs.

The Case for Clustering, Mirroring and High-Availability

Clustering

A particularly effective way of protecting a mission critical server is to duplicate the entire machine and distribute the load. Known as clusters, these are tightly-coupled groups of co-located servers typically sharing a dedicated communication medium and multi-port disk system.

Clustering technology like that of Microsoft's Cluster Services provide high availability. This tends to be categorized in the 99.999% availability range. The main strength of clustering is in providing scalability by dynamic load sharing, coupled with application failover.

The maximum benefit of cluster load balancing is gained only by using cluster-aware applications, which is a sector still not fully exploited by many software products. Furthermore, since they are co-located, an external incident affecting one server is likely to affect the whole cluster, instantly cutting availability to zero.

Implementing clustering technology requires a sizable investment in the hardware. Typically cluster member servers should be identical and the shared storage aspect can be very expensive. This type of technology can often be discounted due to budgeting constraints.

Data mirroring

Typically categorized as 99% availability, this is another effective way of protecting valuable server data. Data mirroring or dynamically replicating data from a principal server to another secondary server, ensuring an exact replica of the data is available. These loosely-coupled associations of servers need not be co-located, can communicate over shared IP network connections, and are self-contained (for example, they do not require expensive multi-port disk systems).

Simple data mirroring does not offer the dynamic load-sharing capability of clusters, but is far more resilient to external events, and can be optimized to provide rapid response to server outage. Minimal data protection can be obtained with a pair of loosely-coupled servers by arranging for critical disks on the main server to be mirrored across existing network connections to a secondary server.

While this does give a degree of data redundancy, it does not in itself provide a stand-in capability and is unlikely to offer real-time protection. Typically, data is not replicated until a file is closed, which could mean that a busy database, remaining open for long periods, would have no effective protection.

A server crash or network failure will render the applications on the primary server unavailable, and although the data may be intact on the secondary server, users cannot gain access without administrator intervention. Databases stop being updated, e-mail servers cease and web servers are inaccessible.

High-availability

To protect mission critical data and ensure essential applications are continuously accessible requires a solution that, in addition to dynamically and efficiently mirroring data, allows a standby server to assume the role of the principal server should it become unavailable for whatever reason.

Typically used as part of a disaster recovery solution, high-availability differs from clustering in that it uses existing hardware and network infrastructures without the need for dedicated systems. In addition, the standby server can be located anywhere on the network – on a LAN or WAN.

High-availability improves on simple data mirroring by ensuring critical applications are always available to users. Rather than passively replicating data to a standby server, high-availability proactively monitors the principal server and will transparently switch users to the standby server should the principal become unavailable. Unlike data mirroring, high-availability performs this automatically and without intervention.

BrightStor High Availability

BrightStor High Availability is a software product developed by Computer Associates to provide high server availability for the Microsoft Windows 2000 and 2003 operating system. It is just one component in the BrightStor family of data protection solutions. BrightStor High Availability allows servers to be loosely coupled using existing network connections and requires no special-purpose hardware. It fulfills three major design objectives:

- The stand-in for a failed server can be up and available within moments of detection,
- The operational impact in terms of server and network overhead is minimized, and
- Data integrity is preserved.

BrightStor High Availability also provides extremely fast synchronization of the servers, allows the stand-in server to process other tasks (both before and after it stands in), allows a single server to stand in for more than one main server, and offers powerful but intuitive single-point management of an entire network of BrightStor High Availability equipped servers.

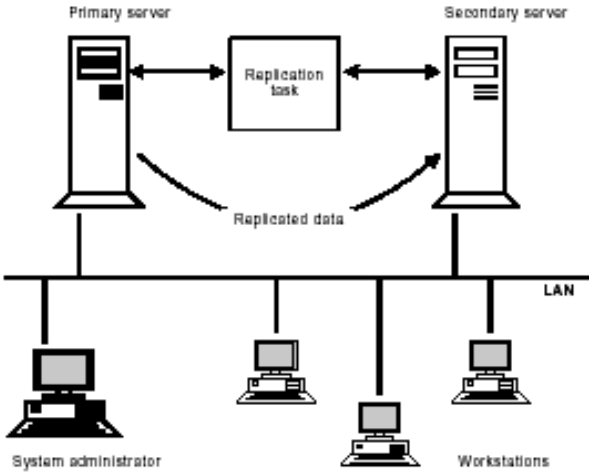
BRIGHTSTOR HIGH AVAILABILITY – SPEED AND SECURITY

Key Terminology

BrightStor High Availability attaches special meaning to the following terms:

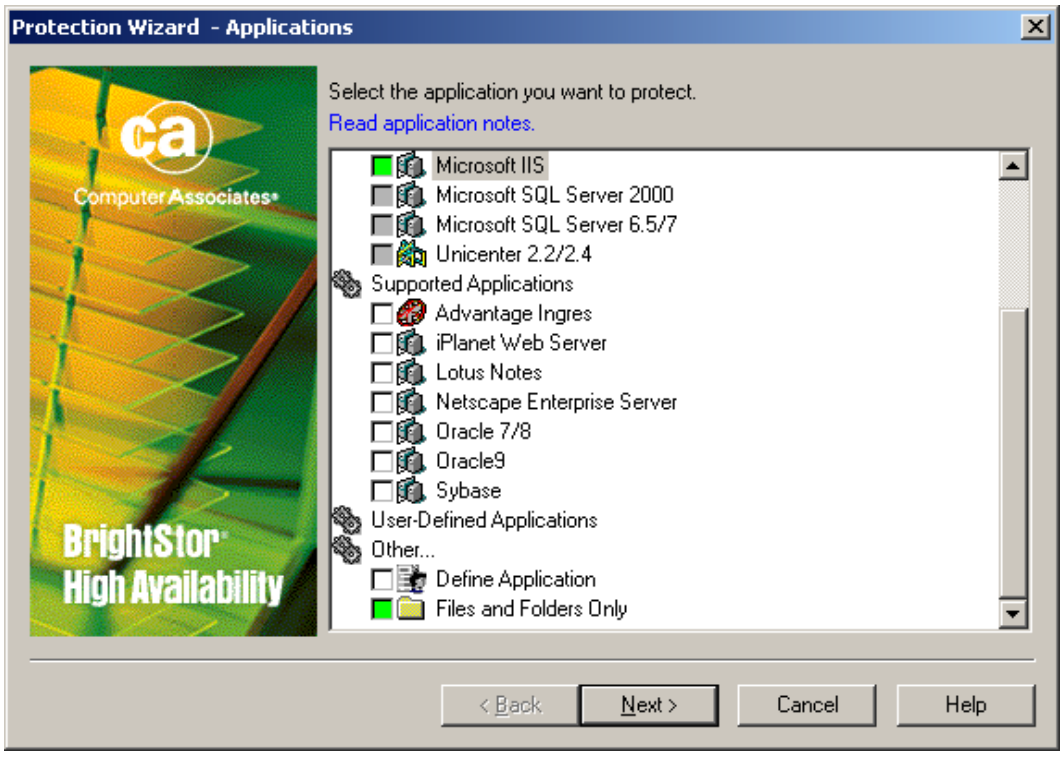
Primary server	A Windows 2000 server being protected by BrightStor High Availability.
Secondary server	A Windows 2000 server that is providing protection to one or more primary servers.
Synchronization	The processes by which those parts of the primary and secondary server file systems that are to be replicated (see below) are made identical. Also referred to as '**static replication**'.
Replication	More correctly known as '**dynamic replication**'. The process by which individual changes occurring to the file system on the primary server are mirrored on the secondary server. During normal running this is a continuous process.
Workload	A workload is a defined criteria which designates what data is to be replicated, where the data will be replicated to, what applications will be failed over and what criteria will initiate a failover.
Failover	The process by which a secondary server stands in for a failed primary server.
Reinstatement	The process by which a repaired primary server resynchronizes its data and reacquires control from a secondary that has been standing in for it.

A Simple BrightStor High Availability Installation



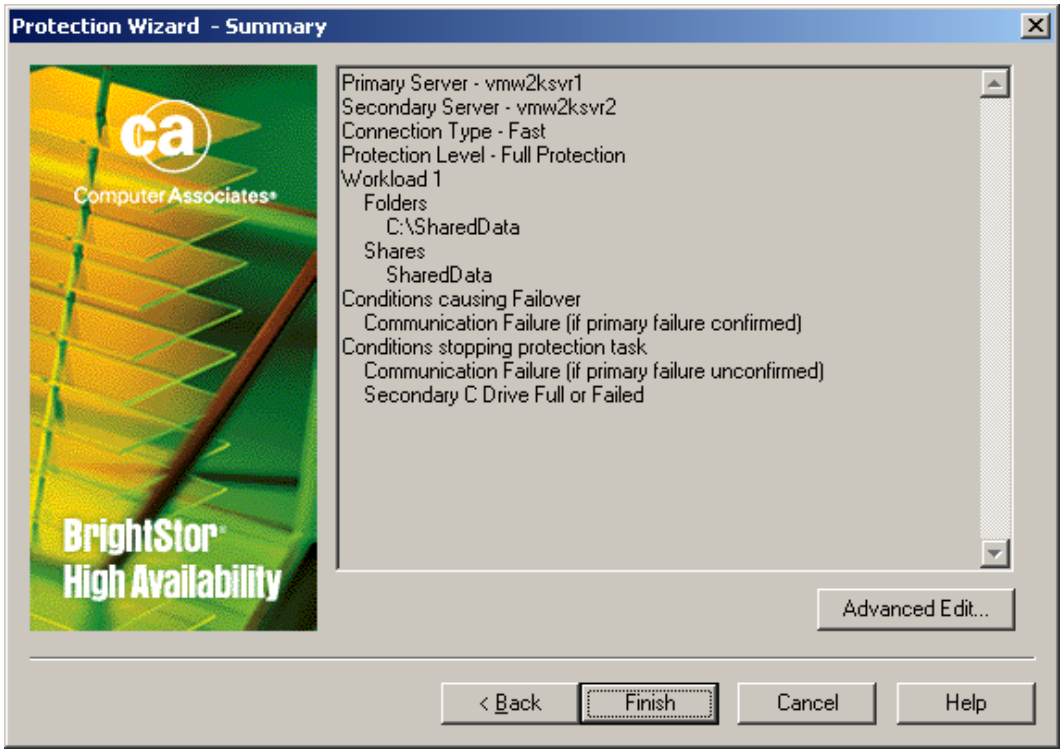
The diagram above shows a simple BrightStor High Availability installation in which a secondary server is protecting a single primary server, with a single LAN connecting the two and hosting a number of client workstations.

In setting up this installation, the system administrator installed BrightStor High Availability on both the primary and the secondary servers, and chose to install the BrightStor High Availability Manager component on their own workstation (it is recommended to be installed on the primary and/or secondary). The primary and secondary servers do not need to be identical, although they do need to be sized appropriately in terms of processor, RAM and hard disk capacity. Clearly the secondary server must have sufficient capacity to run its own native workload (if any) in addition to the workload that it inherits from the primary after failover. Guidance on sizing and configuring the servers is provided later in this document.



After installation, the system administrator configured BrightStor High Availability by creating a protection task using the Protection Wizard which is part of the BrightStor High Availability Manager program. The protection task defines the primary and secondary servers, the failover criteria, various replication settings and one or more workloads (the parts of the primary file system that are to be replicated to the secondary).

The screenshot on the next page shows the final page of the Protection Wizard.



Synchronization

Once installation and configuration are complete, the protection task can be started. Its first job is to ensure that the primary and secondary file systems are synchronized (or, more correctly, those parts of the primary file system that constitute the workload are accurately mirrored on the secondary). In a new installation, this entails copying files from the primary to the secondary over the network connection. The existing directory structure is replicated accurately, as are file attributes and security information. BrightStor High Availability is able to replicate from NTFS to NTFS or FAT, and from FAT to NTFS or FAT. However, it is important to note that if an NTFS system is replicated to a FAT system, it is not possible to retain all attribute and security data. Therefore we highly recommend the use of NTFS on the stand-in server.

The initial synchronization process typically requires large amounts of data to be transferred, and although BrightStor High Availability uses high-performance protocols, this phase can be time-consuming. Unlike some other products, however, BrightStor High Availability lets you continue using the primary and secondary servers while synchronization

takes place. Files that are open and in use on the primary are replicated accurately using the proven open file technology provided by CA's Backup Agent for Open Files (BAOF), a special version of which is automatically installed at the same time as BrightStor High Availability. (If a full copy of BAOF is already present, this will be used instead.)

Under some circumstances, synchronization occurs when some or all of the primary files already exist on the secondary server. BrightStor High Availability uses special algorithms to determine whether these pre-existing files are genuinely identical without having to transfer their contents across the network. This dramatically speeds up the synchronization process. In addition, BrightStor High Availability can determine whether a pre-existing file on the secondary, while not identical, is sufficiently similar to allow just portions of its contents to be transferred. For example, if a one Gigabyte file on the primary differs from its replica on the secondary by only one bit, BrightStor High Availability will transfer only the tiny fraction of the data required to achieve true synchronization. This contrasts favorably with other products, which typically transfer the whole file, and provides yet another performance advantage.

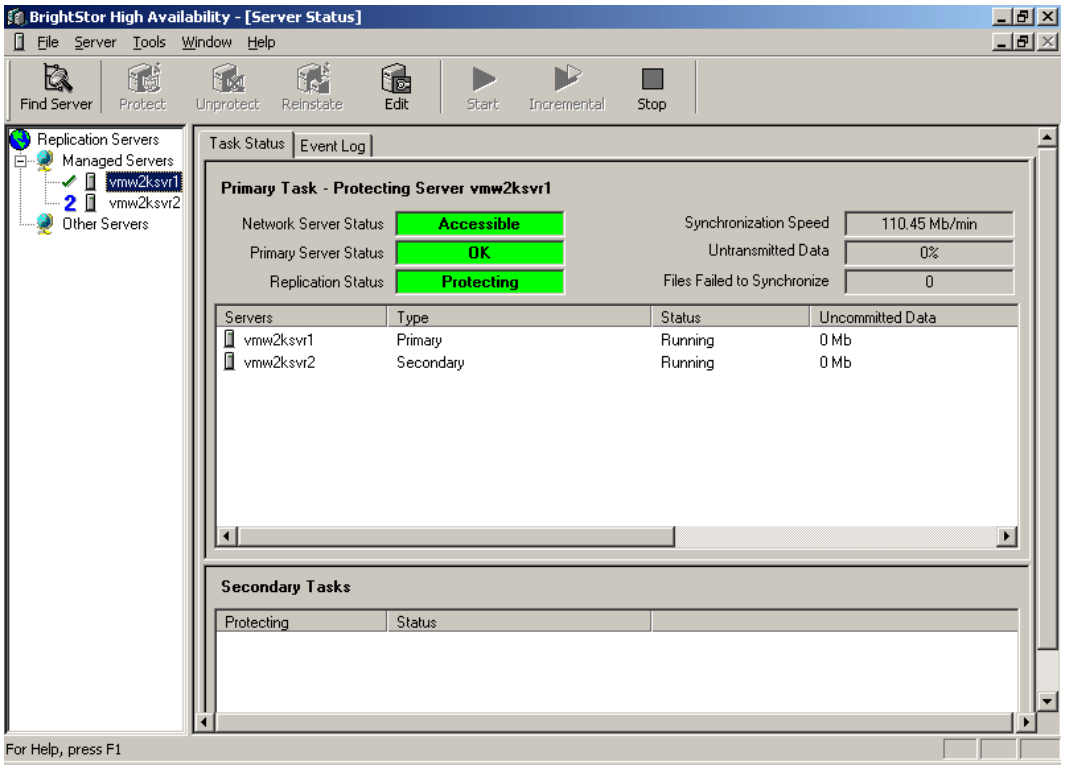
Replication

When synchronization is complete, the primary server is fully protected: the secondary contains an up-to- date set of replicated files, and is able to stand in for the primary at any time. Of course, as changes occur to files on the primary, they are replicated immediately to the corresponding files on the secondary. This occurs in real time.

BrightStor High Availability is unique in that it takes special precautions to preserve transactional integrity. It applies a Write Inactivity Period to files for which changes are pending: if this period expires, without any further write operations, BrightStor High Availability commits the pending changes, on the basis that they constitute a single transaction, and should be applied together. This technique, already field proven in Backup Agent for Open Files, prevents apparent corruption of replicated files on the secondary server. For example, the primary might crash mid-way through a series of write operations forming a single transaction. If each write operation were committed on the secondary as it happened, the replica of the database might exhibit inconsistency or corruption if it were brought into use following failover. BrightStor High Availability

avoids this by delaying commitment of the writes until the transaction is complete. If, during periods of extreme file write activity, the inactivity period does not occur, BrightStor High Availability commits pending changes after a configurable Maximum Hold Time. Any error in determining transaction boundaries is rectified automatically (via the Write Inactivity Period) as soon as normal activity resumes.

The following screenshot shows the protection status screen, which is part of the BrightStor High Availability Manager program.



Replicated files on the secondary server are subject to the same Windows security as the originals on the primary (provided the primary and secondary file systems are compatible). BrightStor High Availability also takes steps to prevent the replicas from being altered or deleted, unless of course failover has occurred. It is perfectly feasible to use the replicated files as the basis for system backup, possibly in conjunction with a full copy of Backup Agent for Open Files on the secondary server.

Failover

During normal running, BrightStor High Availability continuously monitors the state of the primary server, looking for conditions that can cause it to initiate a failover. These conditions include:

Permanent loss of contact with the primary server. This can have a variety of causes, including hardware and software crashes, power outage, and network malfunction. The secondary server monitors a regular 'heartbeat' sent out by the primary. If a number of consecutive heartbeats are missed, BrightStor High Availability assumes loss of contact (the precise period can be configured as it depends, among other things, on the network speed). Optionally, it can then obtain more detail by using an independent serial connection between the primary and secondary servers, and by 'pinging' other pre-selected network nodes, such as a default gateway. In this way, BrightStor High Availability obtains sufficient information to determine whether loss of the heartbeat (as detected by the secondary) is due to genuine failure of the primary, or is caused by problems purely local to the secondary. This information, in conjunction with a policy set by the system administrator, enables BrightStor High Availability to assess the severity of the failure, and whether or not to fail over.

For example, complete failure of the primary warrants failover, whereas a network problem close to the secondary would not, because users logged-in to the primary would almost certainly still be in contact with it. Avoidance of 'false' failovers is an important and unique feature of BrightStor High Availability. Note that even if failover does not occur, loss of contact means that the protection task must be stopped until the problem is resolved.

Critically low disk space on the primary server. The system administrator can configure the drives to be monitored, and the level of free space that is to be regarded as critical. BrightStor High Availability can also monitor free disk space levels on the secondary server, and raise an alert and/or suspend the protection task if critical levels are reached.

On command from the system administrator: This feature is useful if planned maintenance or upgrade is required. The primary server can be taken out of service with little or no disruption. To help the system

administrator control the failover process, BrightStor High Availability offers a set of prepared script files that execute automatically at key stages during failover. These scripts are on the primary server both before and after failover, and on the secondary server both before and after failover. The system administrator would typically set the scripts up to ensure that services are shut down on the primary and started up on the secondary, so providing the correct environment for running applications and servicing client workstations.

After failover, BrightStor High Availability ensures that:

- The replicated file system is available on the secondary server for use by services, users and applications.
- All file system shares originally referencing protected folders on the primary server are switched to point to their stand-in counterparts on the secondary server (the system administrator can fine-tune this behavior).
- The secondary server is available for connection under the same original name as the primary server (the primary is given a temporary new name so that no conflicts occur either if it is still running, or after it restarts).
- The secondary server optionally inherits the IP addresses originally owned by the primary (the primary is given a temporary new address to avoid conflicts).

The net effect is that in most cases users and applications continue functioning, without interruption, and without requiring a new login. Some older applications that were not designed for resilience may require the user to retry a file operation before continuing as normal. Note that it is ***not*** necessary to restart the secondary server to achieve failover.

Reinstatement

When the primary server has been repaired and is ready to go back into service, the system administrator initiates the reinstatement process, using the wizard interface provided by the BrightStor High Availability Manager. Reinstatement can start immediately, or can be scheduled to start at a pre-selected time.

The main steps are to:

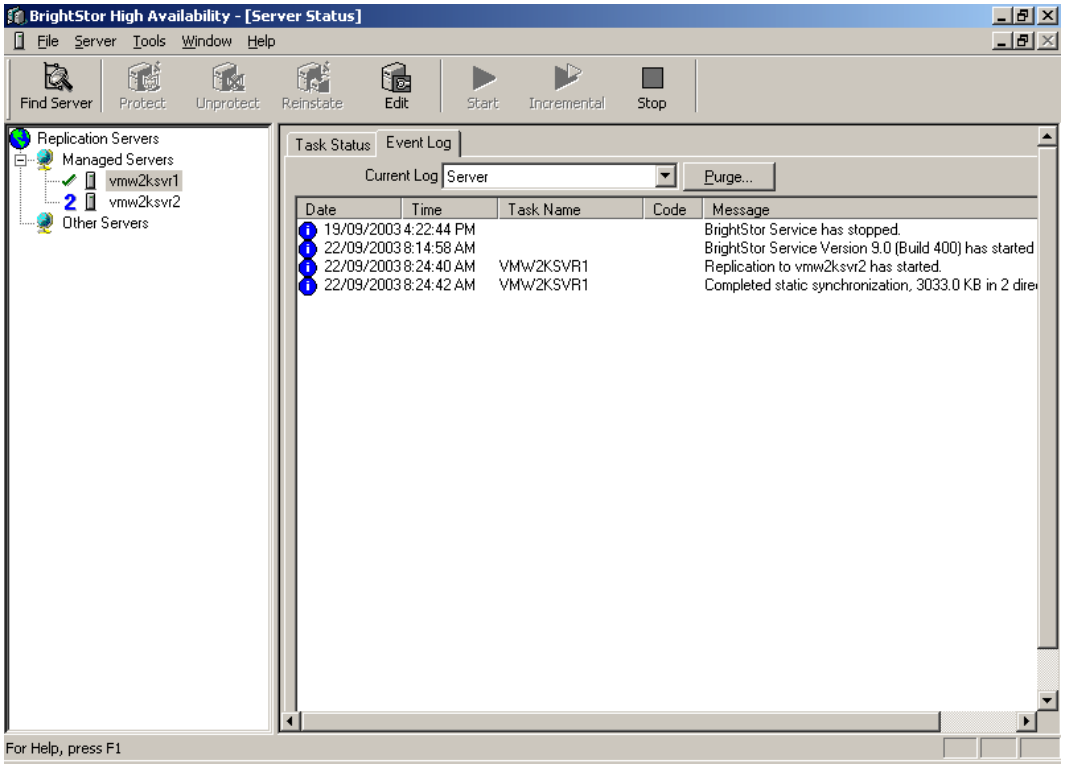
- Optionally issue a warning message to logged-in users.
- Synchronise the primary file system with the secondary so that changes that occurred while the secondary was standing in are not lost. BrightStor High Availability heavily optimises this re-synchronization (see the discussion of synchronization above) so that the absolute minimum amount of data is transferred back to the primary. This leads to relatively fast reinstatement and reduced network traffic.
- Execute pre-reinstatement scripts on both the primary and the secondary server. These might typically be used for closing down services, and are fully configurable.
- Restore file shares and IP addresses to the primary server.
- Execute post-reinstatement scripts on both primary and secondary servers, possibly to start up the services etc. needed for users and applications.
- Optionally restart the protection task, for continued protection.

CA's recommended approach is to advise users of the service and schedule the reinstatement with a server restart.

BrightStor High Availability Management

The Manager component can be installed on the primary and/or secondary server, or on a completely separate Windows system. It gives the system administrator complete control over all BrightStor High Availability operations on any accessible servers, using a combination of Wizards (for creating replication tasks and for initiating reinstatement) and Explorer-like status windows. The Manager program also provides an event log showing all BrightStor High Availability related events, classified according to their severity.

The screenshot on the next page shows a sample BrightStor High Availability event log.



BrightStor High Availability is fully integrated with the CA Alert Manager, which means that alerts can be sent via a range of different media, including e-mail, fax, pager, Unicenter Event Management Console, etc.

PUTTING BRIGHTSTOR HIGH AVAILABILITY TO WORK

This section provides more detail on:

- How to deploy BrightStor High Availability into a typical corporate LAN/WAN environment
- What planning is required
- What the operational considerations are
- How a little time invested pre-deployment will pay large dividends in server application resilience

Planning for BrightStor High Availability

Hardware and Software Requirement

Processor	Intel architecture 486 or higher
System memory	32 MB RAM
Operating system	Microsoft Windows 2000 and Windows Server 2003
Other products by Computer Associates	BrightStor High Availability also uses Backup Agent for Open Files, and the Alert service. If a product is not present on the target computer, or if the current version is out of date, a new version is installed by the BrightStor High Availability setup program.
Disk space	A typical installation requires 12.4 MB. To install the Console and Alert only, you need 10.3 MB. However, computers that will act as stand-in servers must also have enough disk space to hold any replicated data.
Network	TCP/IP

protocol	

Before starting to deploy BrightStor High Availability, it is important to understand the existing network: where the servers are, what applications they are running, how they are interconnected, and where the vulnerabilities lie. Networks both new and old typically exhibit weak spots where a single server failure could affect the smooth running of the entire enterprise. This is where BrightStor High Availability can help most.

In taking stock of an existing network, the following are likely to be important areas:

Server loading, both current and planned

Assess the applications running on each server and their interdependencies, together with the load that they place on their respective servers. This helps to identify the business-critical servers requiring the protection of BrightStor High Availability, and forms the basis for defining and sizing the secondary servers. The secondary server will need sufficient RAM, processing power and disk capacity to handle both its own and its inherited workloads, both now and into the future. The primary server can also benefit from having additional RAM to cope with periods of heavy network congestion, when BrightStor High Availability may need to provide temporary buffering of file changes. The system administrator can fine-tune the amount of RAM that is made available to BrightStor High Availability for this purpose.

Access to servers

Determine how the key servers are connected, both to each other and to the user community. Identify strategic logical locations for primary and secondary servers, so that users can still get effective access to their server applications, even after failover. The BrightStor High Availability Administrator Guide provides in depth detailed information on how to plan the network topology.

Consider also that placing the primary and secondary in separate physical locations might provide extra protection against external events. The system administrator can still control both servers (indeed any number of BrightStor High Availability servers) from their own workstation via the locally installed BrightStor High Availability Manager.

Assess current and planned network bandwidth requirements, taking into account any extra load during server synchronization. The link between the primary and secondary servers should offer as high a bandwidth as possible. Make adequate provision for the different routing of traffic that might occur when the secondary server is standing in.

Control over applications and services

The secondary server may need applications or services (such as a database engine or Web server) to be started prior to standing in for the primary. In normal use, the secondary may not need the database engine to be active and consuming system resources or software licenses.

As part of the planning process, consider what applications, services, etc. should be closed down and/or started up on both the primary and secondary servers before and after failover or reinstatement. BrightStor High Availability provides pre-configured scripts for many of the popular applications as well as generic templates allowing the system administrator to define his or her own scripts to control these events.

Protocols

BrightStor High Availability supports TCP/IP transport between the primary and the secondary servers. In the case of user workstations and their connection to the primary server (and secondary following failover), TCP/IP is the supported protocol.

In the case of a TCP/IP installation, server IP addresses must be static, and not allocated by DHCP. The BrightStor High Availability Administrator Guide provides more information on TCP/IP protocol and configuration recommendations.

Operational Considerations

BrightStor High Availability has been designed so that you can 'set and forget'. Once effectively deployed, there is no particular need to monitor the BrightStor High Availability Manager screen or be concerned with the protection status. However, our recommendation is to implement event management with notifications.

BrightStor High Availability does this by constantly monitoring the state of the primary and secondary servers, responding to changing situations in a planned, predefined manner and alerting the administrator to these events.

Understanding what BrightStor High Availability considers when performing a protection task and defining these parameters in the setup process will optimize the protection of your network. These parameters include:

The drives and folders to be replicated

BrightStor High Availability can protect individual folders and exclude certain file types such as .bak and .tmp files. Choosing only the most critical folders will reduce the system and network resources required.

NTFS security

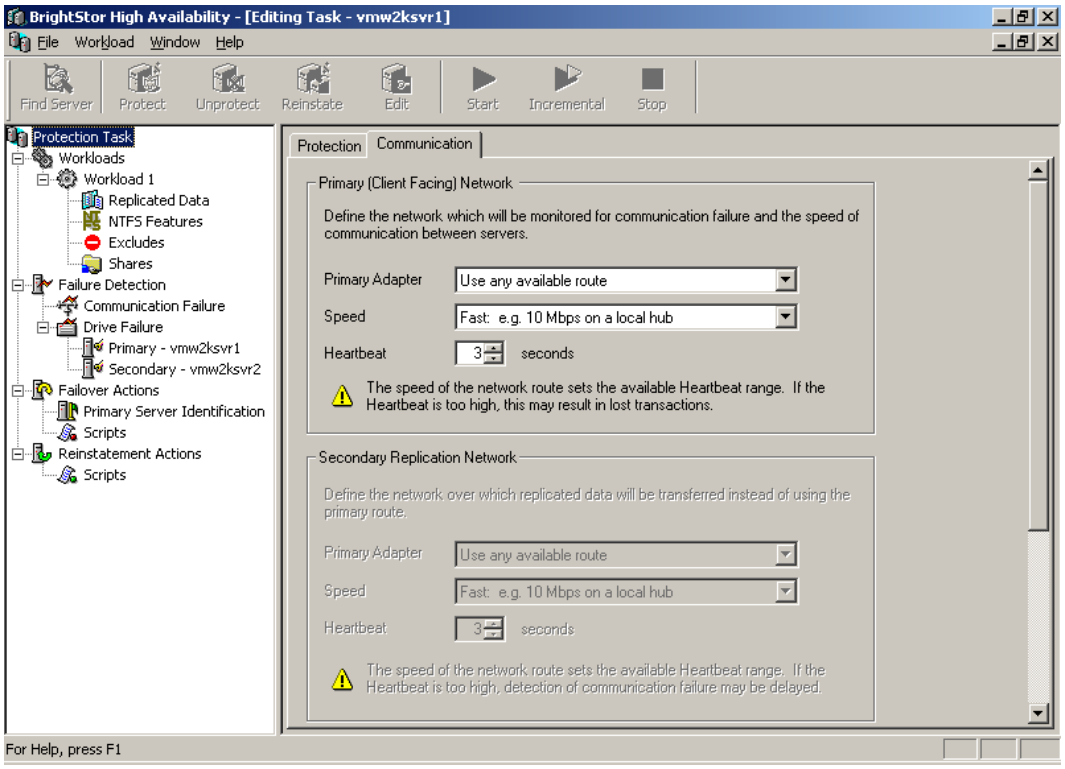
BrightStor High Availability can use either NTFS security descriptors when the primary and secondary are in the same domain, security names when they are not, or, if replicating to a FAT partition, no security. Note that if the primary and secondary servers are in different domains, it is necessary to ensure that all user accounts are present on both servers.

Replication of shares

These will only be implemented on failover and new ones added after set-up can be included or excluded.

Handling a communications failure

BrightStor High Availability can either stop the replication task, fail over immediately or try to confirm primary failure by using a dedicated serial connection and/or 'pinging' other nodes in the network. A comprehensive set of configuration options is available, as illustrated by the following screenshot.



Alerting

To make use of the extensive alerting options provided by CA Alert (installed as part of BrightStor High Availability), it is necessary to enable and configure this feature.

Critical levels of free disk space

BrightStor High Availability offers two action states. The first is a level below which it will broadcast an alert. The second is when it actions the failover or stops the protection task.

Primary server identification

On failover, the primary server will assume a new name for identification purposes. The default is *primaryservername*-FAIL, although this is configurable. Note that some applications are sensitive to the computer name and allowance should be made for this.

Failover and reinstatement scripts

A unique feature of BrightStor High Availability is the ability to run pre-defined scripts on any of eight phases. Specifically, these are pre- and post-failover and pre- and post-reinstatement on both the primary and

secondary servers. Here are some examples of how this feature could be used:

Pre failover on the primary server	Scripts to close down applications currently running and warn users that failover is imminent.
Post failover on the primary server	A script to start a BrightStor ARCserve Backup process.
Post failover on the secondary server	Scripts to start up applications previously running on the primary, such as a database engine or service.
Pre reinstatement on the primary server	Scripts to start up applications previously running on the secondary server.
Post reinstatement on the primary server	Scripts to check the integrity of synchronized data and warn users that reinstatement has occurred.

BRIGHTSTOR HIGH AVAILABILITY WAN FAILOVER

There are currently two methods to support failover across a subnet and both of these require working network connectivity including a Dynamic Name Resolution method (DDNS or WINS) and ICMP ECHO enabled (i.e. ping works correctly) between the Primary and Secondary BrightStor High Availability Servers.

The two methods will be referred to as:-

Local Area Mobility (LAM)—A function built into certain versions of Cisco IOS.

Floating Subnet—A method that hosts the primary machine and reconfigures the routers at failover and reinstatement in order to move control of the floating subnet between the routers.

The **Local Area Mobility** solution relies on proprietary functions built into Cisco hardware. You must have Cisco routers to use this method. Once you configure the routers, the setup of the task completes with very little differences to a standard task. This includes very few changes to the configuration of the primary and secondary servers. This method is ideal for protecting existing servers.

The **Floating Subnet** solution is more generic. It relies on the ability of the router to handle multi-netted networks and to modify the running configuration via telnet from scripts run at failover and reinstatement. This scenario should work with routers from other manufacturers (currently this has only been tested with Cisco equipment). You need to have a spare subnet free within your organisation for the primary to belong to. There are also more steps involved in the setup of the failover task, including editing scripts and text files specifically for your environment. The configuration of routers, however, is easier than the LAM method. The Floating Subnet solution is better suited to protecting new servers introduced to the network. This is because the implications of changing the IP address of an existing server can be difficult for certain configurations or applications.

Configuring for a Firewall Environment

In order to set up BrightStor High Availability on a firewall, you need to follow the rules described below. Many rules will already be in place as a result of the normal running of a Microsoft domain. The only ports that are explicitly required are the BrightStor High Availability data transfer ports and those are also listed below.

Name Resolution Ports 53 or 1512—This applies from the primary and secondary servers to the name resolution server. BrightStor High Availability requires the correct configuration and operation of a name resolution protocol. In order for this to work, DDNS updates or WINS updates need to be let through the firewall to the DDNS/WINS server on port 53/1512 (whichever you use).

Active Directory Ports 445 or 389—This applies from the primary and secondary servers to the Active Directory G.C. server. Active Directory updates are done from the BrightStor High Availability servers. These updates need to be allowed through on port 445 or 389. Windows

tries to use port 445 first. If there is no reply on 445, then Windows tries LDAP on 389.

RPC Ports 137 138 139 + Ports above 1000—This applies from the primary and secondary servers to each other. RPC calls are made between the primary and secondary servers. The initial RPC dialogue is done through ports 137/138/139. The actual RPC conversation takes place by design on random negotiated ports above 1000 (to restrict the range of these negotiated ports see Microsoft TechNet article 154596).

BrightStor High Availability Data Transfer Ports 6080 - 6085—This applies from the primary and secondary servers to each other and to any manager computer. The data transfer and internal communications between BrightStor High Availability servers and managers are done using a block of 5 addresses starting at 6080. You can move this base address with a registry key.

Further details on BrightStor High Availability failover across a WAN are included in the full application note, which accompanies BrightStor High Availability.

CONCLUSION

In summary, BrightStor High Availability provides unprecedented levels of availability for mission-critical business running on key Windows servers. Its unique combination of high availability, high performance and high security make it an obvious choice for all organizations that value business continuity.

Storage Resource Management

MANAGE STORAGE RESOURCES EASILY AND SEAMLESSLY WITH POWERFUL SOLUTIONS

BrightStor Storage Resource Manager --

BrightStor Storage Resource Manager (BrightStor SRM) is the industry's leading cross-platform SRM solution. It enables organizations to centrally manage distributed storage assets in heterogeneous environments from a single global view on one workstation. Wherever your business-critical data is stored - across Windows (2003, XP, 2000, NT), NetWare, UNIX and/or Linux (Intel & Mainframe) environments - BrightStor Storage Resource Manager can easily identify and manage your networked storage resources.

Its analysis, reporting, monitoring, storage classification, threshold-based automation, scheduling, event-oriented alerting, and remote task execution functions help you take comprehensive control of your storage environment. You can reduce the time and money spent on managing storage in your enterprise, ensures storage high-availability, and maximizes the use of your existing resources.

BrightStor SRM's automation capabilities eliminate routine tasks while providing information on enterprise-wide storage capacity, allocation, and usage. In addition, BrightStor SRM enables centralized management of critical storage resources like backup and database applications including

BrightStor Enterprise Backup & ARCserve, Alexandria, Tivoli Storage Manager, Oracle databases, and messaging/collaboration application such as Microsoft Exchange.

PRODUCT OVERVIEW – BRIGHTSTOR SRM

BrightStor SRM offers a single comprehensive solution that helps create a consolidated view of all networked storage resources across multiple platforms within your enterprise. Providing a central storage management facility, BrightStor SRM significantly simplifies the tasks you typically perform to gather storage related to these four basics questions:

- Where data is located?
- How data is organized?
- When data is needed?
- How data is used?

BrightStor SRM offers centralized analysis, reporting, monitoring, logical objects grouping, event-oriented to threshold alerting and automation, and remote task execution by giving you tighter control of your storage resources by offering the following features:

- **Centralized Management.** A global view of storage resources; cross-platform navigation; application management for backup/recovery, databases, and messaging/collaboration; and remote task execution.

- **Storage Classifications.** Logical grouping of storage objects, as well as storage charge-back capabilities that span from the open systems through Mainframe with BrightStor CA-Vantage Storage Resource Manager for OS/390 & z/OS Systems.

- **Exception-Based Management.** Threshold-based automation and notification; desired state management of storage; and notification of space allotment/quota breaches.

- **Advanced Visualization.** Discovery and identification of storage resources; rapid visual identification of storage trends; comprehensive reports; and identification of active storage consumers.

- **Capacity Planning.** Assessments of storage growth patterns needed in preparation for future needs such as SAN migration, server consolidation, or storage optimization; historical data analysis; and planning and implementation of storage management best practices

- **Backup Services and Planning.** Support for BrightStor Enterprise Backup, BrightStor ARCserve, Alexandria, and Tivoli Storage Manager; backup-window strategy analysis and optimization; backup verification, administration, and failure minimization; and maximized reclamation and utilization of storage space.

- **Event Management.** Event-based automation; event-triggered notification and alerting; and event monitoring and reporting.

- **Storage Policy Management.** Uniform policy application across any defined logical group, as well as enforcement of storage policies with automation capabilities.

- **Policy-based Automation.** Resource conditions are automatically monitored and appropriate actions are performed based on user-defined events or thresholds as defined in storage policies. The comprehensive automation system can be leveraged across all storage objects. For example, an administrator may want to archive data older than six months when a disk is 80% full. This scheduled job can be driven through BrightStor SRM or another application to check the disk every 12 hours and automatically archive the specified data once the threshold has been reached. The comprehensive GUI-based automation system can be leveraged across all storage objects.

BRIGHTSTOR SRM COMPONENTS

BrightStor SRM is composed of the following software components:

Application Server – The Application Server (AS) is the main component of BrightStor SRM and it interacts with all other components. The AS performs all these operations transparent to the user. Administrators will have no need to directly interface with the AS for any task other than initial configurations and/or troubleshooting.

The Windows Client – The Windows Client is the primary interface to BrightStor SRM. It provides access to the following major functions of BrightStor SRM:

- Registration of network, BrightStor ARCserve, BrightStor Enterprise Backup, TSM, Oracle, Microsoft objects.
- Browsing of network contents.
- Definitions of BrightStor SRM construct.
- Definitions and execution of services and procedures.
- Processing of the results of service execution (viewing, printing, exporting various format)

Monitor – The state of executing services can be viewed through the BrightStor SRM Monitor. Within the Monitor display, services are separated into activities services and procedures, service on hold, services that have completed operation, and services error.

Database – The BrightStor SRM database contains information about network objects such as domains, computers, volumes, and users, as well as information about other objects that are managed by BrightStor SRM. This information is collected by the BrightStor SRM data collection services from managed objects.

The Database also includes services and constructs created by the storage manager, which describe the management tasks to be performed and the resources available to perform those tasks.

Agent – A platform-specific software component installed and executed on the Application Servers or a managed computer on Windows, UNIX and Linux Operating Systems. The Agents are distributed across the network and collect information about storage assets and their consumption on all managed computers. High-level summary information is stored in the BrightStor SRM database for subsequent use in monitoring and reporting.

Note: Not all managed servers and applications will require an agent. Some use OBDC as an interface for data collection such as Oracle and TSM.

Automation & Utilities – BrightStor SRM has the capability to schedule and execute operations automatically. When BrightStor SRM starts, the Scheduler creates and execution schedule of all services and procedures defined in the BrightStor SRM database. When new service or

procedures defined, it is immediately scheduled for execution. The actual execution is initiated according to defined timing condition and depends on resources available at that particular moment. Every service scheduled for execution appears in the BrightStor SRM monitor display.

BrightStor SRM uses an internal construct called *job* to execute services. A job is the translation of a service request into a set of executable steps. Jobs are not visible to the user, but understanding how BrightStor SRM uses jobs can help explain the principles on which the scheduling of service execution is based. A job is comprised of *tasks*. A task is a program that performs a portion of the job's work.

All jobs are input to the Scheduler, which checks their timing conditions and determines the time interval within which the next execution of the job must take place.

ARCHITECTURAL PLAN

BrightStor Storage Resource Manager can monitor Direct Attached and SAN Attached disks. It also has the capability to manage specific applications within your environment. (See BrightStor SRM Architectural Diagram)

System Components

BrightStor Storage Resource Manager comprises the following systems components:

- Application Server
- Client Agent
- Management Console

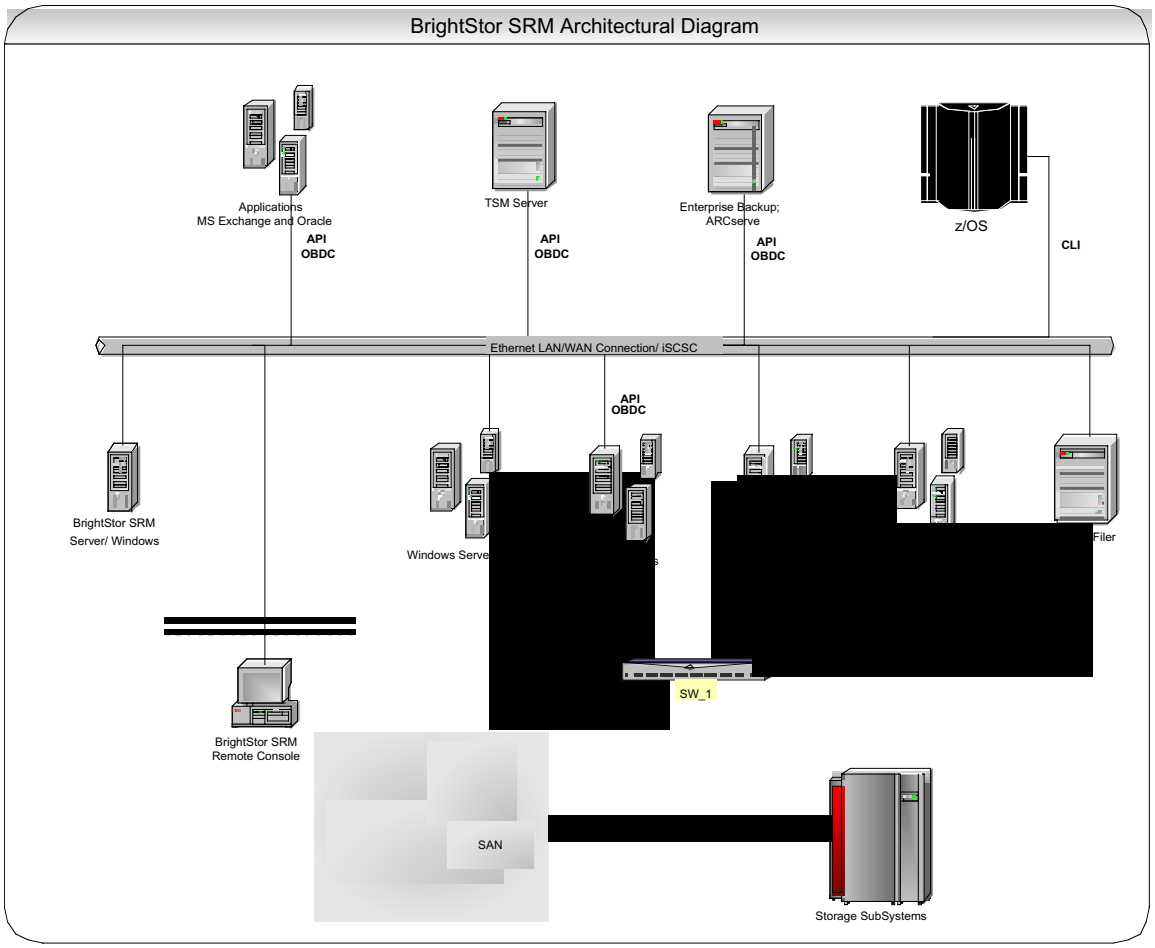
Application Server – In our Best Practice and experience, the Application Server should be installed on a dedicated server consisting of the following configuration:

- Windows Class Server/ Pentium 466 MHz (Minimum); Pentium 880 MHz of higher is recommended
- Estimated 256 MB RAM Server (Minimum); 512 MB or higher is recommended
- 2 GB Free Hard Drive Space

Agents – Based on Best Practices, Client Agents should be installed on any server that requires the management of direct attached and SAN attached disk resources. The Client Agents perform file and volume level scans on all disk volumes that appear to be mapped to those servers. For example, if the LUN ID of a portion of disk residing in a SAN Array is bound to a Windows class server by the Host Bus Adapter and assigned by the Windows Volume Manager as a local drive (such as S:\), then that disk would be scanned as if it was really just another volume inside the server.

These tasks are dictated by a job that is being executed on the Application Server. Some Client Agents will contain a component called a Launcher. The Launcher is used to distribute workload from a job running on the Application Server and delivers specific components of a job to the Client Agent. The Launcher can be found on Windows class machines that have either a Client Agent or an Application Server component installed.

Management Consoles – One or more management console may be installed on any Windows server class machine or workstation that can remotely connect to the Application Server. Alternatively, you can use Terminal Services to log into any Application Server on your network via a web browser.



Supported Operating Systems and File Systems

Managed Computers

- Windows XP, 2003
- Windows 2000
- Windows NT 4.0
- Network Appliance, Data ONTAP 6.0
- Windows Powered NAS
- Linux Powered NAS
- NetWare 3.x, 4.x, 5.x, 6.0
- AIX 4.1, 4.2, 4.3, 5.1
- Solaris 2.7, 2.8/8, 2.9/9
- Linux Kernel 2.2 and 2.4
- HP-UX 10.20, 11.0, 11i

Unix File Systems

- AIX
  - jfs with the default Logical Volume Manager (LVM) supplied by the operating system)
- HP-UX
  - Veritas Logical Volume Manager
  - hfs using one file system per disk, utilizing the hfs primitive partitioning scheme
  - vxfs using SAM as the default volume manager supplied by the operating system
- Linux
  - Traditional file system
- Solaris
  - Veritas Logical Volume Manager
  - Traditional file system, without Volume Manager support

Supported Applications via API or ODBC Connectivity

- BrightStor Enterprise Backup 10.5 (SP1, SP2, or SP3) on Windows
- BrightStor Enterprise Backup 10.5 (SP1, SP2, or SP3) on UNIX
- ARCserve 2000 on Windows
- ARCserve 9 on Windows
- ARCserve 7.0 for NetWare
- ADSM 3.1/TSM 3.7, 4.1, 4.2 and 5.1 (AIX or MF connection with TCP/IP)
- BrightStor Portal via iSponsor
- BrightStor SAN Manager v1.1
- Microsoft Exchange 5.5
- Oracle 8.0, 8.1 and 9.0 (monitored per instance or SID)
- Alexandria 4.5

Please note: Applications and databases that are not listed above can also be monitored in a volume-level capacity by performing file level scans against a list of file extensions. This data can be collected and aggregated across specific servers, a group of servers or across your entire Storage Landscape.

CA's Architecture Recommendations

Based on our experience and Best Practices, CA suggests spreading out the deployment of Application Servers to provide the maximum ease of use and ability to scale for future growth.

The points that will determine the method(s) of deployment are as follows:

- File Level Scans will be performed on a minimal interval
- Each Oracle Database will only have one instance managed
- Network segments are electronically close together based on all the servers being located in the same physical data center.

New features of BrightStor SRM v6.4

Currently, the new features of BrightStor SRM v6.4 will include:

New Device/Software Support

- RAID Array Support
  - Hitachi Freedom Storage (Lightning & Thunder)
  - EMC Symmetrix, including EMC Symmetrix DMX
  - IBM Enterprise Storage Server (ESS) Shark
- Storage-Centric View of Applications
  - New Application Support
  - SAN Management:
    - BrightStor SAN Manager support

Enhanced Application Support

- Messaging/Collaboration:
  - Microsoft Exchange 2000
- Enterprise Storage Automation:
  - BrightStor Portal - Dynamic Instrumentation Sponsor (iSponsor)
- Backup/Recovery management:
  - Tivoli Storage Manager v5.1 (Also available in SRM 6.3, Service Pack 2)
  - New backup reporting features such as event reporting, file space monitoring, and more.
- Support for new releases of platforms
  - Windows .NET server (both 32 and 64 bit versions)
  - NetWare 6

- Linux on S/390
- HP-UX 11i (Also available in SRM 6.3, Service Pack 2)
- Microsoft Server Cluster Support (MSCS)

New Features Summary

- Intelligent agent software installation and un-installation.
- Improved business-driven information views.
- Enhanced automation including management services such as threshold-activated applications invocation to address storage performance events.
- Enterprise storage object automatic discovery and registration enhancements.
- Policy-defined asynchronous and synchronous data collection and file query enhancements.
- Enhanced, wizard-based service builder.
- Enhanced integrated reporting.
- Managed object communication enhanced using TCP/IP and HTTP/HTTPS via Instrumentation Gateway (iGateway) technology.

For the latest list of supported features coming to BrightStor SRM v6.4, please visit our web site located at: http://www.cai.com/solutions/enterprise/storage/brightstor_srm_beta/about.htm

BrightStor Portal MANAGING eBUSINESS STORAGE

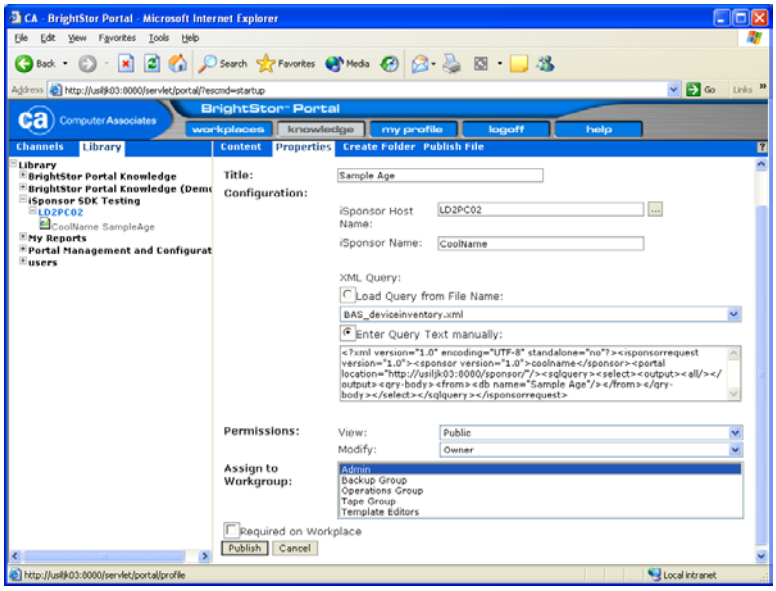
BrightStor Portal --

By consolidating, integrating and reporting application data and operational information from the mainframe to the desktop, BrightStor Portal creates a powerful, end-to-end storage management environment that eliminates conventional platform boundaries.

Support for a wide range of storage platforms and management tools, and the ability to integrate solutions and data from a variety of third-party products, result in a single point of management and control that spans multiple platform environments and storage architectures, from direct-attached, to SAN and NAS.

Operational integration with BrightStor Enterprise Backup and BrightStor ARCserve Backup, and visualization and reporting of information and activity from BrightStor Storage Resource Manager, provide a single point of command and control for multiple BrightStor solutions.
Portal technology offers a flexible, role-based, fully customized view of essential information, applications and tasks, accessible from anywhere on the network. Standard configurations for a range of job types are built in, or users can create their own configurations through unique menus and user preferences.

These features and capabilities provide a management platform that deals effectively with the challenges posed by today's widely networked, heterogeneous storage assets.



OVERVIEW

From a customer perspective, an ideal solution is a management tool that provides a single, customizable view of the complete storage environment via aggregation, normalization and correlation of information providing efficient and intelligent policy-based management. BrightStor SRM can publish all of its content to the BrightStor Portal where storage administrators can then use to get a complete view of the entire storage landscape.

SOFTWARE COMPONENTS

Management Console – The BrightStor Portal Management Console provides a single point of integration to collect, report and visualize all the elements of your Storage environment. Administrators have the capability to create customized Web-based front ends for up to 50 users per Management Console, where each user may have the capability to customize their own Storage Management Workspace.

iSponsor – The BrightStor Portal consists of a Management Console and iSponsors. These iSponsors allow you to communicate to an element within your Storage ecosystem. This element can be an application sitting on a server or an element that send it's information to an iSponsor residing on a client machine that acts as a proxy to collect this information. The iSponsor then transmits that data to the BrightStor Portal so that the data can be viewed by everyone with a secured access to the published information.

The BrightStor Portal may also be used in the capacity of a "command center" by as launching in-context applications that allows for the management for heterogeneous components throughout the Storage Landscape.

ARCHITECTURAL PLAN

Components

The BrightStor Portal is comprised of the following components:

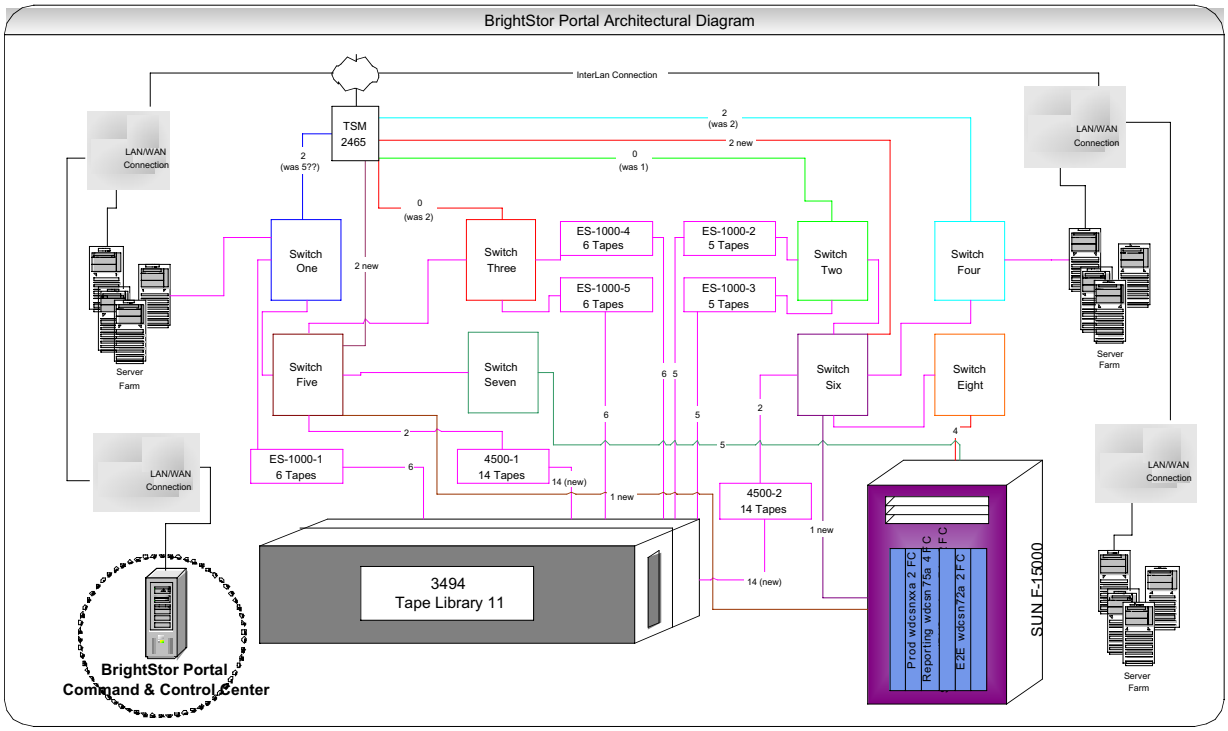
- Management Console
- iSponsors

Management Console – Based on best practices, the Management Console may be installed on a single platform. This can accommodate up to 50 concurrent user connections. The requirements are as follows:

- Windows Class Server/ Pentium 466 MHz (Minimum); Pentium 880 'MHz of higher is recommended
- Estimated 512 MB RAM Server (Minimum); 1 GB or higher is recommended
- 4 GB Free Hard Drive Space (Allows for the multiple BrightStor SRM servers to publish their information to)
- MS-SQL 2000, Service Pack 3

iSponsors – The iSponsors are to be installed on a computer system that meet the following criteria:

- Has a corresponding application to be monitored by the deployed iSponsor
- That are electronically close to the device to be managed where the iSponsor on the installed computer acts as a proxy to collect specific information from that storage element.



Here is a list of current iSponsors that CA has developed for the BrightStor Portal:

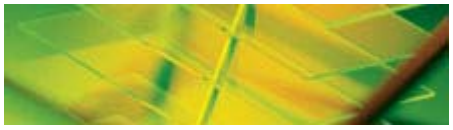
		Platform/Version					
Application	**Version**	**Windows**	**NetWare**	**Solaris**	**AIX**	**Tru64**	**HP-UX**
BrightStor Storage Resource Manager	6.3, 6.2	2000					
BrightStor SAN Manager	1.1	2000					
BrightStor Enterprise Backup	10.5	2003, 2000, NT4		2.9, 2.8, 2.7	5.1, 4.3.3, 4.3.2	In Progress	In Progress
	10	2000, NT4		2.9, 2.8, 2.7	5.1, 4.3.3, 4.3.2		
BrightStor ARCserve Backup	9.0, 7.0/2000	2000	6.0, 5.0 *				
	6.6.1	2000, NT4					
BrightStor Mobile Backup	4	2003, 2000, NT4					
	3.5	2000, NT4					
Legato NetWorker	6.1.2, 6.1.1, 6.0.3, 6.0.1	2000, NT4		2.9, 2.8, 2.7	5.1, 4.3.3, 4.3.2		11,11i
Veritas NetBackup	4.5, 3.4	2000, NT4		2.9, 2.8, 2.7	5.1, 4.3.3, 4.3.2		11,11i
Veritas Backup Exec	8.x, 9.0	2000, NT4					

Tivoli Storage Manager	5.1, 4.5 *	2000, NT4		2.9, 2.8, 2.7, 2.6 *	5.1, 4.3.3 *		11i *
Network Appliance Filers	All	2003, 2000, NT4					
SNIA CIM/SMI-S Providers		2000					

For the latest list of CA developed and partner developed iSponsors, please visit our web BrightStor Portal support site at: http://support.ca.com/public/brightstor-portal/infodocs/bsportal-isponmatrix.html

BrightStor Enterprise Backup v 10.5
HIGH PERFORMANCE ENTERPRISE DATA PROTECTION

BrightStor Enterprise Backup --



BrightStor Enterprise Backup v10.5 delivers manageability and complete data protection in a comprehensive, centralized backup and recovery solution for enterprises with UNIX and/or Windows-centric environments. Through extensive setup and administrator operations tools, it combines maximum ease-of-operation with record-setting, benchmarked backup and recovery performance, unlimited scalability and rock-solid reliability for the enterprise. BrightStor Enterprise Backup v10.5 features integration with leading storage management products and solutions, including BrightStor Portal, BrightStor Storage Resource Manager, and BrightStor ARCserve Backup and competing product environments; it also has built-in integration with off-site vaulting service providers to be part of an overall corporate disaster recovery solution.

BrightStor® Enterprise Backup v10.5 has been significantly enhanced to deliver optimum reliability, superior manageability and industry-best cross-product integration and recovery performance. These combine to give the enterprise customer the most efficient to manage and highest performance solution in the industry. The built-in capability to manage BrightStor ARCserve Backup and competing solutions provides unique investment protection and multi-product management efficiencies as well as a flexible, virtually painless migration path to an enterprise-wide BrightStor Enterprise Backup solution.

SPECIFIC TARGET ENVIRONMENT

- Enterprise-class organization including data center and departmental/remote environments.
- Organizations with UNIX and/or Windows-centric computing environments
- Customers with multi-terabyte, mission-critical applications
- Large networked storage environments
- Financial, Healthcare and other organizations with government-mandated data archive/retention requirements

SYSTEM REQUIREMENTS

Windows:

Operating System: Microsoft Windows 2003 Server (all editions), 2000 (all editions), XP, NT 4.0 SP6 or higher
CPU: 500 MHz Processor
RAM: 512 MB
Disk Space: 500 MB

UNIX:

Operating System: Sun Solaris 2.6, 2.7, 2.8, 2.9; IBM AIX 4.32/3, 5L (32/64-bit); HP-UX 11.0/11i; HP/Compaq Tru64 4.0 e/f/g, 5.0/5.1/5.1A
CPU: Solaris-Sparc Ultra 10 or higher, AIX-IBM RS6000 or higher, TRU64-Compaq Alpha Server or Workstation, HP-UX 9000 Server or Workstation

RAM: 256 MB
Disk Space: 980 MB

New and updated features include:

- Built-in capability to manage BrightStor® ARCserve® Backup v9 environments and ability to manage, monitor and report on competing backup/recovery solutions

- BrightStor Storage Resource Manager integration capability

- Enterprise-wide reporting and monitoring via built-in BrightStor Portal technology

- Off-site vaulting capability and integration with vaulting service providers

- Improved cross-platform management and enhanced command line interface capabilities

- Windows Server 2003 certification and support for all editions, and integrated Microsoft VSS "snapshot" support

- Basic Microsoft SQL Agent and Microsoft SQL Agents with HDS and HP "snapshot" integration

- Added cross-platform Oracle SAN support and Sun Solaris 9 support

- Record-setting Microsoft SQL database recovery and backup performance via integrated support for HDS and HP hardware "snap-shot" support (benchmarked as fastest multi-terabyte SQL database recovery and backup in the industry)

- Added DB2 Agent, Advantage™ Ingres® Enterprise Relational Database Agent and high-performance Exchange Agent add-on

- Job "pre-flight" check for Windows and UNIX platforms eliminating virtually all job failures

- NDMP v4 support and additional NAS support enhancements including support for Microsoft's NAS technology

S = Sun Solaris
H = HP-UX
T = TRU 64
A = AIX

FEATURE	W	S	H	T	A	DESCRIPTION	BENEFIT
Master Setup	x	x	x	x	x	Single, centralized installation and setup program for base product, options and agents, including remote install and setup (and software delivery option for Unicenter® users)	Efficient, easy-to-perform installation and setup saves significant time, increasing productivity

FEATURE	W	S	H	T	A	DESCRIPTION	BENEFIT
Management of BrightStor ARCserve Backup v9 Environments	x					Seamlessly manage BrightStor ARCserve Backup v9 environments from within BrightStor EB	Industry's only efficient path from departmental-level solution (BrightStor ARCserve Backup) to centralized, enterprise-wide solution (BrightStor EB); customer leverages BrightStor ARCserve Backup investment and migrates servers to BrightStor EB at desired pace
Cross-Platform Reporting and Management Using BrightStor Portal Technology	x	x			x	Centralized, cross-platform BrightStor EB and BrightStor ARCserve Backup reporting and monitoring across the entire enterprise	Simplifies management and delivers significantly easier operation by allowing administrators to remotely manage and monitor multiple BrightStor EB servers and devices
Off-Site Vaulting Support	x	x	x	x	x	Support for policy-based exporting and importing of tapes to and from off-site storage vaults	Simplifies off-site media resource management by providing policy-based automation

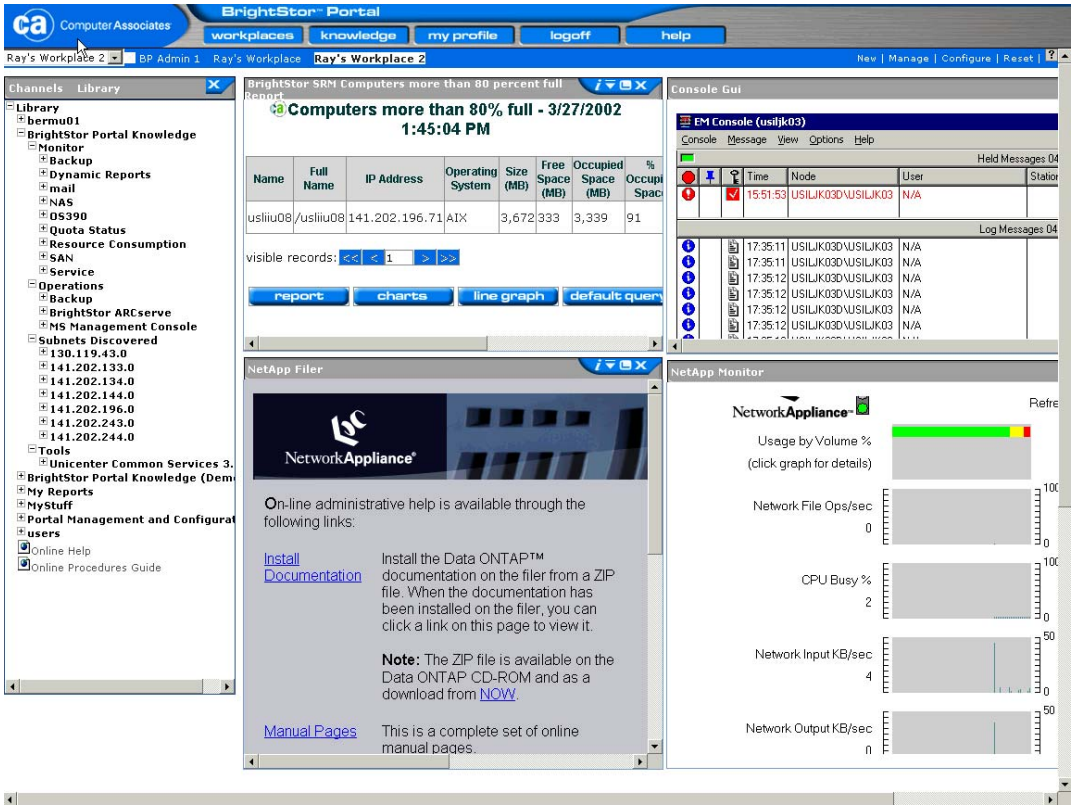
FEATURE	W	S	H	T	A	DESCRIPTION	BENEFIT
Microsoft SQL Agents Integrated with HDS ShadowImage and HP "snap-shot" Management	x					New BrightStor EB database agent to backup/restore MS SQL Server 2000 on Hitachi and HP XP Disk Arrays using their respective hardware "snap-shot" technologies	Record-setting backup and recovery performance for multi-terabyte Microsoft SQL databases with virtually zero impact on SQL production environment during backup/restore operations
Enhanced Lotus Notes Agent	x					Provides support for incremental rotation jobs, point-in-time recovery option, open file agent and improved performance	Improves Lotus Notes efficiency and agent performance by 400%
Agent and Tape Compatibility for BrightStor Enterprise Backup v10.0 and BrightStor ARCserve Backup v9	x					BrightStor EB v10.5 can use BrightStor EB v10.0 and BrightStor ARCserve Backup v9 Agents as well as read their tapes	Provides a flexible, efficient migration option and cost savings/postponement for upgrades
Job "Preflight Check"	x	x	x	x	x	Enables the administrator to "pre-discover" and eliminate issues with scheduled jobs	Increases backup success rate by helping to eliminate any potential problems with scheduled jobs relating to security,

FEATURE	W	S	H	T	A	DESCRIPTION	BENEFIT
						before the jobs run	network connection and media availability
Unicenter® Network and Systems Management Integration	x					Can direct BrightStor EB to perform backup jobs synchronously and communicate job status	Provides efficient workload management for Unicenter and BrightStor® environments
Microsoft Windows Server 2003 and VSS Support	x	x	x	x	x	BrightStor EB v10.5 is Windows Server 2003 certified on all editions and supports VSS "snap-shot" functionality	As the first enterprise-class backup/recovery product to be Windows .NET Server 2003 ready, BrightStor EB provides immediate protection for servers on this new platform and leverages the high performance VSS technology
Calendar-Based Scheduling	x	x	x	x	x	An advanced, calendar-based interface for scheduling backups and defining rotation schemes	Enables easy customization of backup strategies
Easy-to-Use Wizards	x	x	x	x	x	Includes wizards that simplify backup,	Simplifies operations and shortens the learning curve for

FEATURE	W	S	H	T	A	DESCRIPTION	BENEFIT
						restore, job status and device management operations	new administrators
Backup to Disk/Staging to Disk	x	x	x	x	x	Backs up jobs to disk-based storage if data backup or retrieval times are critical; also can stage data to disk prior to tape backup	Provides fast backups and restores from disk-based storage, and enables higher availability using staging to disk
Multi-Streaming	x	x	x	x	x	Offers simultaneous device use within the same job	Provides added flexibility when scheduling jobs and increased performance during backups
Bare-Metal Disaster Recovery	x	x				The server, applications and data can be recovered without reinstalling the operating system or application	Quickly brings mission-critical and revenue-generating servers back online
Integrated Virus Scanning and Cure	x					Scans the data for viruses during backup and copy operations; with the cure option, infected files	Assures protection of critical data without a separate virus protection solution

FEATURE	W	S	H	T	A	DESCRIPTION	BENEFIT
						are automatically cured during a backup without user intervention	
Field Certification Device Support	x	x	x	x	x	CA has certified field engineers with the required skills and tools to easily qualify and add support for unsupported tape drives, tape libraries and various SAN devices	Enables customers to get the industry's fastest, most efficient use of new devices with BrightStor EB
Serverless Backup	x	x				Leverages the industry standard SCSI extended copy command to remove backup loads from the application and file servers	Significantly improves backup performance in SAN environments
EMC Timefinder Integration (including for Oracle)	x	x	x			Provides 24 x 7 application availability while assuring complete data protection without impacting business operations	Reduces the cost typically associated with traditional Oracle data management strategies and application downtime

Powerful BrightStor Portal technology is included with BrightStor Enterprise Backup v10.5, enabling centralized, enterprise-wide reporting and management for CA and 3rd party solutions (including competing backup/recovery products).



DARWIN'S GROCERIES RFI QUESTIONS AND RESPONSES

Architecture

1. Please describe the components or elements of the solution you are describing to Darwin's Groceries. This should include:

a. How you will deliver data replication across an 80-mile distance with, optimally, only five minutes of difference between production and recovery data sets. If a greater delta (difference in data) will be produced by your solution, explain why this is the case and what Darwin might be able to do to address the situation.

Since BrightStor High Availability performs real-time delta replication of data at the block level, we should meet or exceed the five minute requirement. The only exception would be downed links or infrastructure interruptions which could delay all write commits. See additional detail in the BrightStor High Availability section.

b. How you will enable the transition (fail-over) of application access from the production storage infrastructure to the remote backup infrastructure (optimally) within 30 minutes of an unplanned interruption in access to, or proper operation of, production storage.

BrightStor High Availability provides for application failover across subnets (LAN and WAN) for multiple applications. See additional detail in the BrightStor High Availability section.

c. How you will provide security for Darwin Grocery data from the point of creation, during transport, and while stored on production and recovery platforms.

BrightStor High Availability can use either NTFS security descriptors when the primary and secondary are in the same domain, security names when they are not, or, if replicating to a FAT partition, no security. Note

that if the primary and secondary servers are in different domains, it is necessary to ensure that all user accounts are present on both servers. See additional detail in the BrightStor High Availability section.

d. How your solution can be subjected to tests without disruption of normal operations.

CA recommends testing in a controlled environment or by using dedicated test servers at different locations. Once testing has completed in a controlled environment and exact metrics collected based on the WAN topology, a production test can be performed as outlined in the additional detail in the BrightStor High Availability section.

e. Details of the specific support of your solution for various storage infrastructure components deployed in the Darwin Groceries headquarters data center.

The BrightStor Replication Management Solution is comprised of:

- BrightStor High Availability
- BrightStor Storage Resource Manager
- BrightStor Portal
- BrightStor Enterprise Backup

Hardware platform and Operating System is detailed in the product specific are above.

f. Details of the specific support of your solution for the operating system and application software environments used at Darwin Groceries HQ.

The BrightStor Replication Management Solution is comprised of:

- BrightStor High Availability
- BrightStor Storage Resource Manager
- BrightStor Portal
- BrightStor Enterprise Backup

Hardware platform and Operating System is detailed in the product specific are above.

g. Details of any topology or hardware changes required (or recommended) to implement or facilitate the benefits of your proposed solution.

None

h. Details of any changes to wide area networks that are required (or recommended) to implement or facilitate the benefits of your proposed solution.

None

i. Details of management capabilities provided as part of your solution, specifically for verifying the proper operation of your solution, alerting Darwin IT managers to error conditions, optimizing the solution for cost-efficient operation especially in terms of WAN costs, and providing audit trails.

To make use of the extensive alerting options provided by CA Alert (installed as part of BrightStor High Availability), it is necessary to enable and configure this feature. This will provide SNMP, email, pager notification and should be integrated to the BrightStor Portal to receive alerts for central management. The BrightStor SRM product will monitor volume levels and perform trending at the central site and report information to the Portal. This information will allow Darwin to project data growth as well as replication needs in the future.

2. Deployment Issues:

a. Describe the factors that impact the rollout of your solution and discuss the implementation timeframe you anticipate for Darwin Groceries if it selects your solution.

Computer Associates recommends that the implementation of the BrightStor Solutions is completed in the following order:

- Assessment and Planning
- Design and Architecture

- Implementation

A Project Manager will be assigned throughout the Assessment, Planning and Implementation phases in order to manage assist the client through each of the BrightStor Solution implementation.

Factors that Darwin Groceries needs to consider during the environment assessment phase are as follows:

- Systems specified in the environment meet the minimum product system requirements.
- The systems are update to date with operating system and application maintenance.
- Information System Administrators are made available for interviews during environment assessment phase.
- The BrightStor Solution implementation team is granted administrative level access to the systems specified for the BrightStor Solution installation.

b. Describe how your solution can be scaled to meet the increasing volume of data generated by Darwin Groceries over time.

The BrightStor SRM product maintains constant metrics on all relevant file systems to help address and manage the increase in volume. While the increase in volume is inevitable as the business grows, spending can be managed far enough in advance to budget required storage purchases.
m

c. Describe any implementation support services that you offer, including consulting, training, customization, etc. Identify specifically the duration of services (e.g., the length of training) and any additional expense associated with these services.

CA Technology Services offers both customized and packaged services to meet your needs. From Assessments to Implementations, to Migration assistance, CA Technology Services offers the right assistance at the right time to shorten your deployment cycle, maximize your productivity and accelerate Darwin Groceries ROI. Our consulting teams work closely

with CA Education to provide seamless implementation consulting that builds on the knowledge your staff acquires in our training curriculum. Outside our standard service packages, it is expected that Darwin Groceries would require a customized implementation delivery package. We would require further discussion with Darwin Groceries in order to scope the requirement with consideration of your staff expertise as well as potential inclusion of one of our BrightStor business partners bringing additional domain expertise. A customized service delivery plan would then be tailor leveraging superior methodologies and best practices to ensure successful Darwin Groceries implementation of the integrated enterprise technology solution we have proposed.

3. Solution Pricing:

a. Describe you pricing methodology.

The way Computer Associates licenses our solutions is such an important element of our business model that we have named it: FlexSelect Licensing. We use the phrase "Our software sold your way" to describe our flexibility and open approach to doing business that differentiates us from the competition. Our FlexSelect licensing offers a variety of installment plans consisting of up front perpetual licenses to month-to-month subscriptions.

b. Calculate the cost to Darwin Groceries for your proposed solution including optional components and services.

For this proposal, the components need it are the following:

- BrightStor High Availability
  150 Smaller Stores
  10 corporate sites servers
  5 central site servers
- BrightStor SRM
  1 Application Server
  6 managed server licenses
- BrightStor Enterprise Backup
  1 Base product
  1 tape Library option
  6 Client Agents
  1 Oracle Agent

- BrightStor Portal (Included in Enterprise Backup)

The cost of the solution is based on MSRP of the products including 1 year of maintenance that includes upgrade protection and technical support from CA.

The cost of the solutions is 467,000 USD
Implementation costs approximately 250,000 USD. This may vary after having detail discussions with Darwin Groceries

c. Identify maintenance or other recurring costs to Darwin after it has implemented your solution.

At this time there are no other recurring costs. But a further discussion will be needed in order to determine if there are other costs involved

d. Identify any third-party components you have included in your solution and their cost to Darwin Groceries.

None.

4. Benefits:

a. Describe how your enhanced data protection solution may be differentiated from a tape backup-and-restore solution from the standpoint of

i. Shrinking backup windows
ii. Reduced time to data (restore) time
iii. Overall solution dependability
iv. Overall solution cost

This solution provides the advantage to select the replicated server to be the backup target, allowing the administrators to create a backup job without affecting the performance on the primary server. Also the administrators don't have to worry about the restore operation and even can be scheduled for maintenance operations. This solution is hardware independent so there are no necessity of having any special requirements and because the pricing, it can be implemented as an alternate solution of Clustering

b. Remote disk-to-disk mirroring, one approach for data protection, has always carried with it two deficits in Darwin's view: hardware lock-in and high

expense, especially in terms of WAN bandwidth and management. Explain how your solution addresses these concerns.

With the proposed solution, there's no need to have the same hardware in the two replicated sites and the solution allows many to one servers, so the cost implicated with hardware drops dramatically. For WAN bandwidth it will be necessary to have a infrastructure with enough capacity and it will need to be upgrade it for fulfilling the solution.

c. Darwin wants a comprehensive business case to offer to management for the solution it selects, one offering not only risk-reduction, but also cost-savings and business-enablement value. Can you describe benefits in each of these categories that derive from your solution?

Risk Reduction, Cost Saving and business enablement value Analysis

BrightStor High Availability is a comprehensive high-availability solution for Windows NT/2000 environments. It maintains business continuity by protecting the applications that are running on your mission-critical Microsoft windows servers. This is achieved by replicating the application data to an alternative server and then by providing access to that data in the event of failure of the application that is being protected.

Application data is synchronized between two servers in real-time with CA patented technology that ensures both data integrity and transactional integrity while maximizing the synchronization performance.

BrightStor High Availability checks the status of each of the process on the primary machine. If any of these processes fails or if the entire machine fails then a failover to the secondary machine will be automatically initiated. This means that if the application being protected suffers a failure, BrightStor High Availability ensures that the users still have access to the application and its data by effectively mimicking the application onto the secondary server, achieving non-stop access to the data and application, thus protecting your servers against Application failures, OS crashes or network disruptions.

BrightStor HA provides high availability of applications by causing the secondary to assume the identity of the primary in the event of failure and by starting the required application services on the secondary. This function is called "failover".

While a secondary server is taking over the tasks of the primary, a charge recorder keeps track of all of the data blocks that change. This ensures that when the primary server is again available the resynchronization can take place as optimally as possible.

Key Features

- Automated Application Support
  - During the install process common installed applications are identified and can be automatically assigned for failover.
  - And of course any application can be configured for protection
- Enhanced failover
  - By checking the status of each individual process associated with a protected application failover can be initiated accurately in the event of an application fail
- Enhanced Synchronization
  - Synchronization technology ensures that complete transactions are replicated.
  - Intelligence is used to ensure that all critical data associated with the protected applications or complete servers are kept in a consistent state.
- Enhanced failback
  - Making use of Computer Associates File Change recorder technology BrightStor High Availability ensures that during a fail over all changed data is tracked to ensure the fastest possible fail back when the primary is being reinstated.
- WAN enabled failover
  - BrightStor High Availability has been enhanced to allow failover over wide area networks. This is accomplished by using technology to allow IP Failover across subnets

To be able to value a high availability solution a customer must be able to understand the following:

- Quantify the business cost of downtime

- Understand the potential causes of downtime

To quantify the business cost of downtime a customer must be able to :

- Identify technology dependencies
- Calculate the cost of downtime

From the above information it is quite clear that a compelling business reason exists for you to consider a high availability solution.

Our solution today focuses on Microsoft Windows. In this space the predominant applications are as follows:

- Microsoft Internet Server
- Microsoft SQL
- Microsoft Exchange
- Oracle
- Lotus Notes

5. Market Viability

a. Describe how your solution compares with comparable solutions in the market today. (We encourage specific and explicit comparisons to competitive products.)

The BrightStor suite's strength is in managing a complex storage environment.

As customers are starting to realize that they can use what comes with operating systems for volume management & file systems, the market for stand-alone infrastructure solutions is disappearing. However this adds the complexity of multiple management components. The BrightStor Portal delivers a unique central point of management allowing the centralization of both CA BrightStor components AND third party solutions from hardware (array management tools) to software (Veritas, Legato, Tivoli). This is a unique value for BrightStor.

Today customers use the replication provided by the array vendors to actually move the data from primary to backup sites. However, Darwin Groceries' requirement for mixing hardware vendors inevitably leads to software as the solution for this. Thus we provide BrightStor High-Availability as a solution for replicating data across sites.
BrightStor High Availability provides both the ability to replicate data and to manage the failover of applications. The key strengths to this solution are:

- many to one allows a single recovery server to provide backup for many servers
- no shared storage required (no single point of failure)
- multiple method of identifying the loss of original server

BrightStor Enterprise Backup is included to provide the most fastest and most effective backup on the planet. Unique in its' ease of use, BrightStor Enterprise Backup leads the industry in delivering the fastest speeds for the least CPU overhead, while simplifying the use of advanced technologies like hardware snapshot, Serverless backup, NDMP backup, etc. The ability to centralize reporting from itself, BrightStor ARCserve Backup and third-party solutions from software companies like Veritas and hardware companies like Tivoli and Legato/EMC is unique in a backup/recovery solution. This is provided to allow customers like Darwin Groceries the ability to update an environment to BrightStor Enterprise Backup as a standard without having to "rip 'n' replace" all servers in one day. Products can be replaced as their maintenance expires while still having a centralized point for backup management.

b. Describe your business model and financial performance to assuage consumer concerns about their investment and your prospects for longevity.

Computer Associates Intl. is the world leader in enterprise and storage software (IDC August 2003). With revenues exceeding $3.1B in FY 2003 and a staff of over 15,000 employees, CA is committed to customer satisfaction. CA delivers that through strong, proven technology, flexible licensing, quality solutions and dedicated service.

CA has maintained its position of technological and business leadership for over 27 years. The Company has obtained more than 200 patents worldwide and has more than 900 patent applications pending. CA is also the first and only global enterprise software company to meet the exacting standards of global ISO 9001:2000 certification. CA's innovative FlexSelect licensing model empowers customers to dynamically apply CA's best-in-class technologies to their business challenges as required, and to define acquisition terms that are best suited to their needs. CA Technology Services complements CA's technologies with expertise and experience that customers can leverage to maximize the value they realize from their investments in CA and third-party solutions.

c. Identify key factors Darwin should consider in its business decision to select and deploy your solution.

By working with CA, Darwin Groceries can be assured that not only will we help you solve the problems that are bedeviling you at the moment, but that we are committed to extending our lead in storage management in the completeness of our offering, in multi-platform support, through integration of storage management functions and integration of storage management with enterprise management.

Four essentials that are unique to CA:

1) *The return on investment* – we believe that our combination of products provides the surest and most profound ROI for Darwin Groceries's storage management dollar. The immediate capacity gained, the long-term optimization that our products enable and the flexible pricing alternatives that we offer make CA's BrightStor product line the best solution for storage management.

2) *Our breadth of solution* – Computer Associate's comprehensive suite of data and storage management solutions ensure that all of the diagnostic, analytical and management of your storage environment can be done using complete, consistent information in an integrated view. Not only do our storage management applications cover both data and infrastructure management, but they are

3) *Our neutrality vis-à-vis hardware* – CA is the only hardware independent company with a complete suite of management applications, so our agenda is to solve the management issues regardless of how much it slows your hardware investments. Our ongoing focus is on ensuring that your data is protected and hence the continuity of your business and that your storage investment is serving you as effectively as possible.

4) *Our internationally recognized commitment to quality* – Though our ISO 9001 certification makes CA the only enterprise management software company to have achieved this acknowledgement, our dedication to quality extends to the service we provide, enabled by the large, skilled group of CA technologists committed to supporting your storage management objectives.

Darwin Groceries has a sophisticated environment that can benefit immediately from the information, control and acumen that CA products and support staff can enable. These gains will be recognized in cost savings from deferred hardware purchases, greater span of control by your storage administrators, and better performance from your storage infrastructure. As Darwin Groceries looks at its long term strategic reliance on effectively managing data and the storage environment, Computer Associates will continue to lead the way in providing centralized, automated On-Demand Storage. The fundamental goals of on-demand storage are to dynamically align storage capacity with changing business priorities while increasing the efficiency with which storage resources are used.