



Computer Associates®

White Paper

Advanced Data Protection and Storage Management Strategies for Microsoft Exchange

Including:

- Protecting Microsoft Exchange and Keeping It Available
- Management, Capacity Planning and Reporting
- Email Regulatory Compliance Requirements
- Migrating to Microsoft Exchange 2003

Computer Associates International, Inc. Authors:
Steven A. Menges, BrightStor® Product Marketing Manager
Jack Zito, Manager, BrightStor Development
Josh Eddy, Product Manager, BrightStor
Paul Ignatius, Senior Vice President, BrightStor Development
Christopher Evans, Manager, Technology Services

April 2004

Introduction	3
Protecting Microsoft Exchange and Keeping It Available	3
Business Challenge	3
Solution Options	4
Offline ("Cold") Backup and Restore	4
Online ("Hot") Backup and Restore	4
Snapshot-Based Backup and Restore	5
Software-Based Snapshot	5
Hardware-Based Snapshot	5
Disaster Recovery (DR)	6
Server Disaster	6
Natural Disaster	6
Real-Time Replication	6
CA's BrightStor® Solutions for Exchange	6
Management, Capacity Planning and Reporting	7
Business Challenge	7
Solution Options	7
Storage Resource Management	8
SAN Design	9
SAN Management	9
Duplicate File Reduction	9
CA's BrightStor Solutions for Exchange	9
Email Regulatory Compliance Requirements	10
Business Challenge	10
Solution Options	10
CA's BrightStor Solutions for Exchange	10
Migrating to Microsoft Exchange 2003	10
Business Challenge	10
Solution Options	11
CA's BrightStor Solutions for Exchange	11
Conclusion	11
Appendix A: BrightStor® ARCserve® Backup Agent for Microsoft Exchange Premium Add-on — Message- and Document-Level Technical Detail	A1
Appendix B: Technical Detail — BrightStor® ARCserve® Backup Agent for Microsoft Exchange — Database Level	B1
Appendix C: Technical Detail — Snapshot Technologies and Microsoft Exchange	C1
Appendix D: Government Regulations	D1
Appendix E: Migrations to Microsoft Exchange 2003 — Best Practices and Other Tips	E1
Appendix F: Complexis Corporation Scenario and BrightStor® Product Solutions	F1

Introduction

Email is perhaps the most significant new business tool created in the past 20 years. It enables never before seen communication efficiencies and record-keeping for organizations of all sizes and types. Rapid growth in email software (and its dominant vendor, Microsoft Exchange) and storage requirements have brought with it unique new challenges for email administrators and IT managers.

With 2.5 billion messages sent every day (IDC), email has surpassed telephone, fax and overnight delivery as the most important method of business communication and information exchange today. Downtime is no longer an acceptable inconvenience—it is an interruption that affects virtually everyone in the organization. Downtime negatively affects productivity and even a small lapse in availability can result in lost revenue.

Despite the growing importance of email, the complexity, cost and time required to plan and implement a true highly available, data protection strategy for Microsoft Exchange (Exchange) often have prevented or delayed the decision to do it. Organizations know they need 100% protection, the highest availability and the fastest possible recoverability, but tackling this complex challenge is a daunting task. The “strategy” of hoping it will not go down and hoping the existing backup solution will provide adequate recovery to prevent your business from being harmed by an outage is an unnecessary risk and burden for IT to bear.

This white paper explains and addresses key challenges faced by IT organizations and email administrators as they manage and protect Exchange environments, including:

- Protecting Exchange and keeping it available
- Managing explosive email growth
- Meeting regulatory compliance requirements
- Migrating to Exchange 2003

When formulating a strategy for protecting Exchange, it is important to understand the true total cost of ownership (TCO) of the solution(s) you are considering. The TCO of a solution includes all the required hardware and software, one-time consulting and implementation costs, the cost of all ongoing administrator cycles to manage the solution, any periodic costs for follow-up consulting and so on.

The TCO also includes the time and effort required to manage the vendor or group of vendors supplying the software solutions discussed in this paper. This TCO should be weighed against the business value of data (and the business costs/impacts of the data being inaccessible for minutes, hours or days).

A primarily three time zone (8 a.m.–8 p.m. ET) shop will likely have very different needs and requirements than a global enterprise with stakeholders covering five continents. Similarly, certain manufacturing companies would not be noticeably impacted by a scheduled two-hour blackout with Exchange being unavailable, while organizations depending on so-called “knowledge” workers would be severely impacted by even a two-hour brownout in which data is available, but the system is running well below required performance metrics. The drill of getting a good understanding of acceptable brownout and blackout thresholds for your organization is a very worthwhile exercise to help ensure that your strategy fits your needs and expenses are minimized as much as possible.

We will now look at the four key challenges listed above and outline the solution options to meet these challenges. In the “Appendices,” we go into more detail about the topics discussed in the paper and detail a customer scenario example and the solution choices made to best address your needs and environment.

Protecting Microsoft Exchange and Keeping it Available

Business Challenge

Because Exchange has become a critical business application, its data must be protected and available to the users who rely on it. Rapid growth in users and required storage capacity, coupled with constant changes in hardware and software technology, make it a challenge to keep Exchange truly protected and available. Despite these challenges, the ever-present risk of data loss makes protection and availability a necessity.

To keep data protected and available, a backup and restore solution is a necessity. The desired level of “availability” will differ depending upon the needs of your organization and, of course, there are cost impacts as you move up the availability scale.

The need for 24 x 7 x 365 is fast becoming a business reality for some. Organizations that need this level of availability and accessibility cannot tolerate scheduled downtime (blackouts), and cannot even afford the extended periods of slow system response (brownouts), caused by traditional backup methods. The other key element in "availability" is how quickly an organization can recover from a physical disaster in its data center. Off-site storage of backups typically comes into play here along with advanced replication technologies. Automatically replicating data locally and/or remotely can minimize blackout time, but obviously requires significantly more hardware and software.

Solution Options

Offline ("Cold") Backup and Restore

Offline or "cold" backup is the traditional method used to back up Exchange. It typically involves shutting down the Exchange server(s) during non-business hours and then using a basic backup technology to back up the database(s), logs, security credentials (Active Directory or other) and so on to one or more tapes. It is the lowest cost solution and is relatively easy to administer. High performance technology called multistreaming enables backup and recovery data to be transmitted in multiple streams using multiple tape drives simultaneously in a multi-drive library. This enables high-performance backup and recovery of large databases in high throughput environments by maximizing throughput and utilizing the full capability of as many drives as possible. Multiplexing technology can also provide higher performance and media minimization for some environments (typically lower throughput environments), by enabling multiple data sources to simultaneously be backed up to a single tape drive to maximize the capability of that drive.

If your organization can tolerate scheduled blackouts, then a cold backup solution will meet your needs and keep costs at a minimum.

Online ("Hot") Backup and Restore

Online or "hot" backup technology enables you to back up Exchange while it is up and available to users. Online backup solutions back up the files not in use (the same way as with a cold backup), and log any open files so the changes to those files are

backed up as soon as they become stable. During restores, the application knows how to bring all the data back efficiently.

Online or hot backup can be done in two ways: a full database/storage group-level backup; or a more granular backup at the folder/mailbox level (this is sometimes referred to as "brick-level" backup).

With a "full" or database-level backup, hot backup can also differ from a cold backup in the sense that a set of logs captured later after the full backup can be applied to the full backup data to recover the Exchange server to a later point in time. The logs contain a copy of all changes (transactions) that occurred since last full backup. For example, if a hot database backup occurs at 5:30 a.m. and you have logs detailing the changes from 5:30 a.m. through 11:30 a.m., you can restore the 5:30 a.m. full database backup and apply the logs of the changes which occurred between 5:30 a.m. and 11:30 a.m. This enables you to recover your Exchange server to a 11:30 a.m. status even though your last full database backup occurred at 5:30 a.m.

Hot backup does affect the performance of Exchange, and slow performance or brownouts are a common nuisance for users during the backup window. Performance during brownouts should be part of the decision criteria for this type of solution as well as overall backup and restore performance, which determines the length of brownouts and time to recover.

Advancements in this technology include the flexibility to backup and restore at a more granular level than the entire database, including the mailbox/folder/brick level, and even message/document level. These advancements offer the flexibility to do more frequent backups of higher priority items and they can drastically backup and restore times vs. always having to back up and/or restore the entire Exchange database. These do not affect the performance of Exchange as much as a full, database-level backup, but there is still a brownout effect. Other recent advancements include the flexibility to filter out unwanted folders (like your "Sent" or "Spam" folder) or types of files (.mp3, .mov and so on) from the backup set; in addition, the flexibility to do incremental or differential backups of just the changes since a previous backup can dramatically reduce backup times.

For more information on flexibility and granularity options like mailbox- or document-level backup and restore, see Appendix A. For more information on database-level backup and restore technology, see Appendix B.

Snapshot-Based Backup and Restore

The emergence of point-in-time or snapshot copy technology further reduces the brownout window to a few minutes or seconds. It involves briefly freezing the data set and taking a quick snapshot of it.

This snapshot can be used as the backup copy or be backed up (migrated) to another disk or tape device. Snapshot-based backup and restore can be complex and include the coordination of many elements, including the:

- Application to be protected (such as Exchange, Microsoft SQL Server, Oracle and so on)
- File system and operating system
- Creation and maintenance of the snapshot (changes from vendor to vendor and technology to technology)
- Performing of a backup and restore operation with the snapshot data

The two key types of snapshot technologies are software-based snapshot and hardware-based snapshot, and they are detailed below. Not all non-CA backup and restore solutions are designed to leverage these technologies for Exchange, so be sure to verify what is supported by the vendors you are considering if you want snapshot-based protection for Exchange.

Software-Based Snapshot

Software-based snapshot technology has been developed by a variety of vendors to instantly “copy” file systems and, in some cases, applications like Exchange, for the purposes of high-performance, low-impact backup or duplication. A software-based snapshot is really an instantaneous set of pointers (or bitmap), made to the original data set as it was at the designated point-in-time. As the original data set changes, the pointers to data that has changed then replicate the original data, enabling the point-in-time restore. Because of the way it works, software-based snapshot copies typically only take up a small fraction of the disk space of the original data set.

Microsoft Windows Server 2003 includes

Microsoft’s software snapshot technology called Volume Shadow Copy Services or VSS, and this technology is designed for use with Exchange 2003 and file systems. Select leading backup and restore software vendors (like CA’s BrightStor®), worked extensively with the prerelease VSS code so their products integrate with and fully leverage this powerful Microsoft technology for doing backup and restore of Exchange. Support for this technology in backup and restore solutions may be via a VSS agent of some type or it may be built into an existing agent, as it is in the BrightStor® ARCserve® Backup Agent for Open Files.

One limitation of software-based snapshots is that the snapshot bitmap is created on, and must stay within, a particular server.

Hardware-Based Snapshot

Hardware-based snapshot technology comes from a disk array hardware vendor or storage virtualization provider (HDS, EMC, HP and so on), and will only work with their own arrays. It consists of doing a full, point-in-time snapshot copy of the data set to another one of the vendor’s disk arrays (or another section of the same disk array). This snapshot copy can then be used as the backup copy for restores or it can be backed up/migrated to another disk or tape device for longer-term retention or archival use. Since the snapshot is an exact full copy of the original data set, it will double the required disk space for the first snapshot copy and so on.

The interface to generate hardware snapshots varies from vendor to vendor, and, to fully leverage this type of technology for applications like Exchange in a backup and restore solution, backup software vendors must integrate, test and certify their products with the application, operating system and the hardware snapshot technologies of the disk array vendors. This is a detailed, time-consuming process that results in even higher levels of data availability. Microsoft Windows Server 2003’s VSS framework contains technology to make the required three-way integration seamless and efficient for applications like Exchange 2003.

For more information on both kinds of snapshot technology and how it can be leveraged by backup and restore solutions, see Appendix C.

Disaster Recovery (DR)

Server Disaster

When an Exchange server goes down, the process of getting it back up and running can be very cumbersome and time-consuming. Tasks may include getting the operating system and its settings reinstalled, reinstalling the Exchange application and restoring the Exchange data itself. Just getting the server operating system back and in working order can take several hours per server. Solutions that automate and/or speed up one or more of these server DR tasks can significantly reduce the time needed.

Natural Disaster

The most common (and typically lowest cost), strategy for preparing for a major physical or “natural” disaster is to have a data protection solution that creates, tracks and manages backup tapes. These tapes (and/or copies of them) can be stored in a tape library, locally outside the library (for manual insertion for restores), or sent to a third-party off-site vault or “hot” site until a restoration is needed. When needed, these off-site tapes can be recalled and the data restored. Off-site vaulting services typically offer several on-demand tape return plans ranging from guaranteeing tapes can be brought from their vaults back to your location in one to two hours through 24 hours or more, with the return time guarantee determining the monthly base cost of the plan.

Another alternative to mitigate the risk of physical disaster is replicating critical data to another location through using real-time replication technology or remote/transportable hardware snapshots. These technologies (described in the next section), enable the highest levels of data availability but also may have a significant hardware, and in some cases software and administration, cost.

Real-Time Replication

The level of highest availability can be achieved via continuous or “real-time replication” technologies with intelligent failover capability. By having Exchange servers replicated in this way, a hardware or operating system failure will not cause the blackouts or brownouts that normally cripple Exchange users and therefore organizations as a whole.

Several types of solutions exist for real-time replication with failover for Exchange. These include simple local and/or remote Windows/Exchange server high-availability replication as well as various server “clustering” solutions for Exchange. Key differences include hardware/software cost, required consulting services and overall ease of administration.

Organizations without in-house server clustering expertise should carefully consider the total investment costs of a clustered solution vs. any incremental benefits of clustering over a simple Windows/Exchange replication with failover solution. The key is to properly quantify costs vs. benefits for your particular organization.

CA's BrightStor® Solutions for Exchange

CA offers the following BrightStor® products for protecting Exchange:

- **BrightStor® ARCserve® Backup for Windows**
- **BrightStor® ARCserve® Backup Agent for Microsoft Exchange**
- **BrightStor® ARCserve® Backup Agent for Microsoft Exchange Premium Add-on**
- **BrightStor® ARCserve® Backup Agent for Open Files**
- **BrightStor® ARCserve® Backup Disaster Recovery Option**
- **BrightStor® Enterprise Backup Media Management/Vaulting Option**
- **BrightStor® High Availability**

**Note: BrightStor® Enterprise Backup solutions also provide the listed BrightStor® ARCserve® Backup functionalities.*

BrightStor ARCserve Backup Agent for Microsoft Exchange provides both hot backup capabilities at a database level and brick level. BrightStor ARCserve Backup Agent for Open Files enables a non-transportable backup solution using VSS technology. BrightStor ARCserve Backup Agent for Microsoft Exchange Premium Add-on enables advanced hot database backup technologies as well as provides an excellent message level restore solution with advanced enterprise features

In addition to these solutions, CA offers leading solutions for Exchange in security (eTrust™) and infrastructure management (Unicenter®). For more information on these solutions, please visit: **ca.com/exchange** or contact a CA sales representative.

Management, Capacity Planning and Reporting

Business Challenge

As demonstrated thus far, data is not protected until it has been backed up and/or replicated, and can be restored quickly. Similarly, messaging and communications services are only available and uninterrupted when there is underlying storage capacity to support the Exchange database that stores the email messages.

Understanding what is happening in your Exchange environment can be a big challenge. Knowing the past, current and future storage capacity allocation, availability and usage growth patterns are important to efficient capacity planning and Exchange storage management. Many organizations loosely track Exchange storage vs. capacity, and purchase and provision storage based on those estimates. Unfortunately, that often leads to two unacceptable scenarios: purchasing storage too early (losing the time value of that money), and/or reaching maximum capacity unexpectedly causing a crisis purchase/provision cycle. Either way, business is negatively impacted and money is wasted.

Being able to easily report on your Exchange environment is also a daunting task when there are multiple Exchange servers in addition to the various platforms and applications involved. Administrators may rely on spreadsheets or homegrown scripts to track the storage metrics of the Exchange servers. This is time-consuming and prone to error, and it is knowledge that is easily lost when an employee leaves.

Lacking up-to-date information, storage administrators often over-allocate storage capacity or incessantly add capacity to Exchange servers to accommodate growth. This leads to expensive and unnecessary spending on hardware and the inability to facilitate just-in-time requisition of storage hardware.

Based on CA's internal research, most organizations are operating at below 30% of utilization for their distributed data storage. That means that less than 30% of the storage that they have paid for is of business use and that more than 70% of existing capacity is taken up by data of questionable value (meaning it is duplicate data, a year or more old, unused space or data that has no owner). Yet 100% of data is typically backed up. The mainframe world typically has storage utilization rates of 80% or higher, and that technology and the

expertise behind it is just now becoming available in the open systems world, including Windows and Exchange.

When it comes to the overall performance of an Exchange environment and, more importantly, how it performs from the perspective of the users, organizations often lack key information about what is actually happening. If an Exchange server goes down, an administrator will know and can react appropriately but, for example, the administrator often does not know whether certain Exchange data throughput is lower than usual, or he knows it is lower than usual but does not know why it is lower. Chances are that throughput may be affected by certain switch ports in the storage area network (SAN) or supporting disk capacity that is below the recommended threshold necessary for optimal server performance. Without such knowledge, your administrator has no way to load balance the Exchange bandwidth for optimal performance or even know that load balancing is necessary to solve a performance problem. The lack of administrators having this key information results in the same, all too common problem: poor performance and availability of Exchange.

In response to Exchange's increased business importance, Exchange data is being increasingly stored on SANs to take advantage of their characteristics such as performance, availability and the ability to centralize resources. Being able to visualize, manage and monitor this newer type of infrastructure is a key to helping ensure the availability and performance of Exchange systems utilizing it. The promise of high-performance, lower-cost SAN storage cannot be realized without the expertise and tools to properly manage, monitor and report on them.

Solution Options

To meet these challenges, you need effective, efficient storage management tools. You need storage resource management and SAN design and management solutions that can handle the complexities of your complete storage environment and give you the information you need to efficiently manage your storage as well as your Exchange environment. In a more complex environment that includes multiple vendors, you will likely need these types of solutions to efficiently manage all the different hardware and software elements of your environment both today and tomorrow as it evolves and new hardware and software are introduced into it.

Storage Resource Management

Storage resource management (SRM) as a discipline is defined differently by different industry experts, vendors and so on. For the purposes of this white paper, we will leverage the more broad CA definition SRM that encompasses most, if not all the characteristics of the others. With regard to Exchange, that definition of SRM means the SRM solutions should:

- **Increase productivity** by proactively identifying storage trends and forecasting capacity needs. It quickly identifies, prioritizes, and automatically preempts and addresses storage-related problems, such as out-of-space issues, before performance problems arise.
- **Automatically gather information** about Exchange servers and visually present the information in clear and centralized charts, graphs and tables.
- **Respond faster to evolving business needs** by providing useful information about objects tracked by the solution's user properties, capacity and quota management details. Some solutions even have problem-remediation properties that can automatically correct problems before detrimental events get out of control.
- **Protect investments** by pinpointing unusual trends in the data transfers, success or failure rates, percentage of capacity used and much more.
- **Contain costs** before they get out of control. You can spend far less time and money managing the Exchange storage resources that you have already purchased.

A top SRM solution should provide a variety of management features and tools to help you realize the benefits described above, including:

Detailed Monitoring and Analysis of Exchange Data Protection Strategy

Any SRM solution should centrally monitor and report on all Exchange servers through access to the Active Directory catalog and Exchange servers to provide a complete picture of related storage objects including server, folder and mailbox status as well as storage capacity utilization and availability properties.

In-Depth Reporting on Exchange

Reporting is key to efficient management and a good SRM solution should have a variety of out-of-the-box, predefined reports that deliver the flexible access to information on networked storage resources in addition to the Exchange objects. There should be a powerful query engine and reporter to help customize the reports, which can be automatically executed and distributed in a variety of formats, including delimited text files, PDF, HTML, XML, MDB or ODBC-compliant databases.

Comprehensive Reporting on Exchange Server and Objects

The data collected from multiple Exchange servers, databases, folders and mailboxes should be accessible via a centralized management console. There should be a comprehensive view with proactive information on the Exchange environment, helping you maximize the availability of your messaging and collaboration system.

Backup Failure Detection and Alerting

Your SRM solution should automatically alert IT staff of an Exchange server backup failure and its frequency. The cause of a failure is determined by investigating the details as well as trending the status of backups. It alerts staff to conditions that may jeopardize the backup process. The solution verifies the successes and failures of backing up Exchange so that an organization's backup strategy can be better planned.

Automatic Control of Networked Storage Environment

Your solution should have the capability to maintain the desired state of the Exchange environment through threshold-based and event-driven automation. With this type of state-of-the-art solution, you can define the desired Exchange state by setting the thresholds or events to monitor. Then you can define the actions to be performed when thresholds or events are reached and the software does the rest. When thresholds are met or predefined events occur, it should automatically perform the actions designated and provide problem alerts.

Automatic Allocation of Storage Capacity to Exchange Servers

Automation tools are the latest technology to leverage and with them, storage capacity can be automatically allocated from the abstracted storage pool to the Exchange server host upon the breach of the storage capacity threshold. Dynamic capacity provisioning helps ensure that Exchange will never run out of space and messaging services will not be disrupted.

SAN Design

One of the most prevalent mistakes plaguing early adopters of SAN technology was not having the tools necessary for proper design of their SANs. Often relying on a particular hardware vendor for the expertise, they were completely reliant on that vendor for design, upkeep, upgrades and all consulting services related to the SAN, both short-term and long-term. Unless you are comfortable completely outsourcing the design and long-term upkeep of your SAN to a third party, you need to look at independent tools which enable flexibility in design and upkeep of your SAN investments.

SAN Management

Health monitoring, topology mapping and storage network management of Exchange servers

A top SAN management solution can automatically discover, map and monitor servers that host the Exchange application. These server hosts and shared storage resources can be monitored for its health and availability in the SAN environment.

SAN management solutions should discover the SAN infrastructure to visualize the topology, inter-connectivity and status of all the key components, such as disk arrays, switch fabrics and server connectivity, that are critical to the continued operation of Exchange.

Flexible views of the infrastructure should be available to provide the information you need to understand this complex environment and relate it to your business. The environment status is displayed through in many intuitive ways to help different levels of administration and management understand the impact of failures or problems. Failures and problems are visually displayed in:

- **Business Process Views™**, which allow you to logically group discovered objects to define business-critical units and processes. If a critical event happens to any device in the storage network, you can see the immediate impact of the problem on the business.

- **Zone Views**, which allow you to view zone membership with support for administering zones and zonesets
- **Logical Volume Views**, which allow you to view logical volumes per node, logical volumes per storage device and the correlation of logical storage to hardware
- **Business-Centric Views**, which allow you to relate storage devices to their business units such as HR, Finance, Sales and more
- **Device-Centric Views**, which allow you to logically group storage devices by type or location, including Tape, Disk, Rack 5, Closet 11 and more
- **Path Visualization**, which displays all valid routes to storage devices
- **Visual Display of Health Status**, which color codes health status
- **Asset Reporting**, which graphically displays device information

Through a flexible event management system, automatic responses to repair, alert and/or escalate are also available.

Duplicate File Reduction

One way to minimize storage costs for Exchange is to employ a solution that supports “single instance storage” for backup/archive. This technology enables you to store only one copy of messages and attachments that exist in multiple mailboxes or folders in your Exchange environment.

CA's BrightStor Solutions for Exchange

CA offers the following solutions to help improve your storage resource management:

- **BrightStor® Storage Resource Manager**
- **BrightStor® Storage Resource Manager Option for Microsoft Exchange**
- **BrightStor® SAN Designer**
- **BrightStor® SAN Manager**
- **BrightStor ARCserve Backup** (to support single instance storage)

In addition to these solutions, CA offers best-of-breed solutions for Exchange in infrastructure management (CA's Unicenter). For more information on these solutions, please visit: ca.com/exchange.

Email Regulatory Compliance Requirements

Business Challenge

From the SEC to the FDA to the U.S. Congress, government entities have recently put additional requirements on how business information is stored, protected and accessed. Many of these regulations are considerably more stringent than standard business practices, requiring a retooling of IT processes and systems. After the rules were introduced with multiyear timelines, businesses concentrated on more immediate issues. However, due to impending deadlines, the risks of noncompliance and specter of enforcement are fast becoming a reality for businesses.

According to the new laws, the U.S. government considers email a business record, thus raising its retention and accessibility requirements from its previously ordinary treatment. Rather than being purged on a regular basis, emails have new preservation requirements that introduce various IT problems. Often containing sensitive information, business email has special protection and retention requirements and must be treated differently.

See Appendix D for more detail on government regulations.

Solution Options

Many of the major regulations affecting email have a few requirements in common. They obligate the organization to have the ability to produce business-related documents, often explicitly listing electronic communications as a business document to retain and produce. Other regulations explicitly require disaster recovery and off-site vaulting/archiving solutions.

One way of retaining email using a company's existing infrastructure is through the well-understood and mature technology of backup and restore. Most companies already have a backup solution and infrastructure in place, and it is an inexpensive solution to protect all email by backing it up to economical media.

The ability to retain the email for the correct time period is just as critical, so you need to be able to set the retention period on the email-containing media. A media management solution can be used to set the retention periods, helping to ensure that critical emails are not lost or overwritten.

According to HIPAA and the Federal Continuous Operations Mandate, certain businesses and government agencies must have a disaster recovery plan. The ability to resume essential operations and

recover critical information is compulsory. Clearly, email communications can be essential, considering the amount and types of information that are often held on email servers. Those affected by the regulations should make disaster recovery or "bare-metal restore" of critical email systems and data part of their overall disaster recovery plan.

The common denominator for most regulations is that business data such as business email must be "protected and available." This translates into having reliable, secure backup and recovery, server disaster recovery and off-site vaulting/archiving solutions to enable compliance (along with sufficient security to protect email from threats).

The backup/archive solution should also have the capability to search or "query" emails based on the subject of the message. This will enable faster response to compliance related inquiries.

These requirements can be met with the data availability solutions described above; organizations need to understand which are the most appropriate for their particular needs and requirements.

CA's BrightStor Solutions for Exchange

CA offers the following solutions to help meet your regulatory compliance requirements:

- **BrightStor ARCserve Backup for Windows**
- **BrightStor ARCserve Backup Agent for Microsoft Exchange**
- **BrightStor ARCserve Backup Agent for Microsoft Exchange Premium Add-on**
- **BrightStor ARCserve Backup Agent for Open Files**
- **BrightStor ARCserve Backup Disaster Recovery Option**
- **BrightStor Enterprise Backup Media Management/Vaulting Option**
- **BrightStor High Availability**

Migrating to Exchange 2003

Business Challenge

Most businesses today are running Exchange v5.5 and/or Exchange 2000, meaning they could benefit from the many new features contained in Exchange 2003. However, the thought of upgrading/migrating key applications has made many organizations delay this process as long as possible. With Microsoft's dropping of Exchange 5.5 support upon us, many organizations now have an immediate need to migrate as quickly, efficiently and painlessly as possible.

Many organizations are also looking at possibly consolidating Exchange servers at the same time to reduce administration requirements and improve performance. The two main challenges in a server consolidation environment are availability and a small or nonexistent maintenance window due to the size and number of databases hosted.

When looking at any tool related to Exchange, be sure the vendor has a good development relationship with Microsoft; this helps ensure that all new Microsoft technology is immediately supported and that the products work together efficiently.

Solution Options

The good news is that new Microsoft and third-party technologies have made it possible to perform relatively painless migrations to Exchange 2003 and even efficiently consolidate Exchange servers. Some backup and restore applications will seamlessly enable migration via their capability to back up Exchange 5.5/2000 servers and restore the information to newly upgraded Exchange 2003 servers. This compatibility feature also solves a potentially sticky problem for previously archived 5.5/2000 data which may be stored in offline racks, at an off-site vault and so on.

Some server consolidation projects attempt to merge many databases into one large one as when combining data marts into a single global data warehouse. For these projects, the size and uptime requirements of the merged database often justify the use of the snapshot technologies detailed earlier in this document. Some backup and recovery solutions enable you to restore/migrate individual mailboxes and others to new locations; this feature can be very handy for load balancing and other migration/consolidation projects.

Other consolidation projects attempt to re-host many individual databases on a centralized hardware infrastructure to take advantage of the high-end hardware and professional management available in a data center. In these cases, snapshot technology should be considered based on the aggregate size of all the databases and the fact that backing up one database using conventional means may affect the operations of other databases. Snapshot addresses both of these issues by making it possible to complete a full restore of a very large database in a matter of minutes, allowing you to perform backups quickly and with minimal impact to online users.

Some SRM tools can assist with the consolidation strategy as well as perform some of the key tasks involved with the migration itself.

CA's BrightStor Solutions for Exchange

CA offers the following solutions to help you with Exchange migrations and consolidations:

- **BrightStor ARCserve Backup for Windows**
- **BrightStor ARCserve Backup Agent for Microsoft Exchange**
- **BrightStor ARCserve Backup Agent for Microsoft Exchange Premium Add-on**
- **BrightStor ARCserve Backup Agent for Open Files**
- **BrightStor ARCserve Backup Disaster Recovery Option**
- **BrightStor Enterprise Backup Media Management/Vaulting Option**
- **BrightStor High Availability**
- **BrightStor Storage Resource Manager**
- **BrightStor Storage Resource Manager Option for Microsoft Exchange**
- **BrightStor SAN Designer**
- **BrightStor SAN Manager**

Conclusion

Exchange is a mission-critical application and its availability and reliability are necessary to deliver a competitive advantage. In this paper we have examined four key areas related to management and protection of your Exchange environment and detailed solution options for meeting your business challenges.

- Protecting Exchange and keeping it available
- Managing explosive email growth
- Meeting regulatory compliance requirements
- Migrating to Exchange 2003

The large, growing Exchange databases in organizations today challenge IT departments to rapidly backup the data with minimal disruption to business operations. Further, the 24 x 7 business world is forcing the backup window to be reduced or eliminated. Bringing a system offline or affecting its ability to serve the business while a backup takes place is often unacceptable because data and application availability has a direct impact on customer service, back-office operations and costs.

The solution or solutions you choose should meet your particular needs and enable complete protection, highest availability, rock-solid reliability and lowest overall storage TCO. Your first step should be to clearly identify your recovery, backup and archive requirements so you can focus on the right set of technologies to meet those requirements (see Figure 1). You should then carefully look at the solutions that meet your requirements and compare them. As we discussed earlier, helping ensure you understand the entire TCO, including required consulting, vendor management and so on.

High-performance, relatively low-cost technologies for Exchange are readily available; an integrated solution set like CA's BrightStor family of storage management solutions can reduce TCO even further by cutting back on required administrator cycles and vendor management costs. By also leveraging CA's integrated eTrust security and Unicenter infrastructure management solutions for Exchange, IT managers can get best-of-breed solutions from a single trusted source. Since these CA products are designed to work together and offer ease-of-management, they also give the customer the lowest overall TCO (see Figure 2).

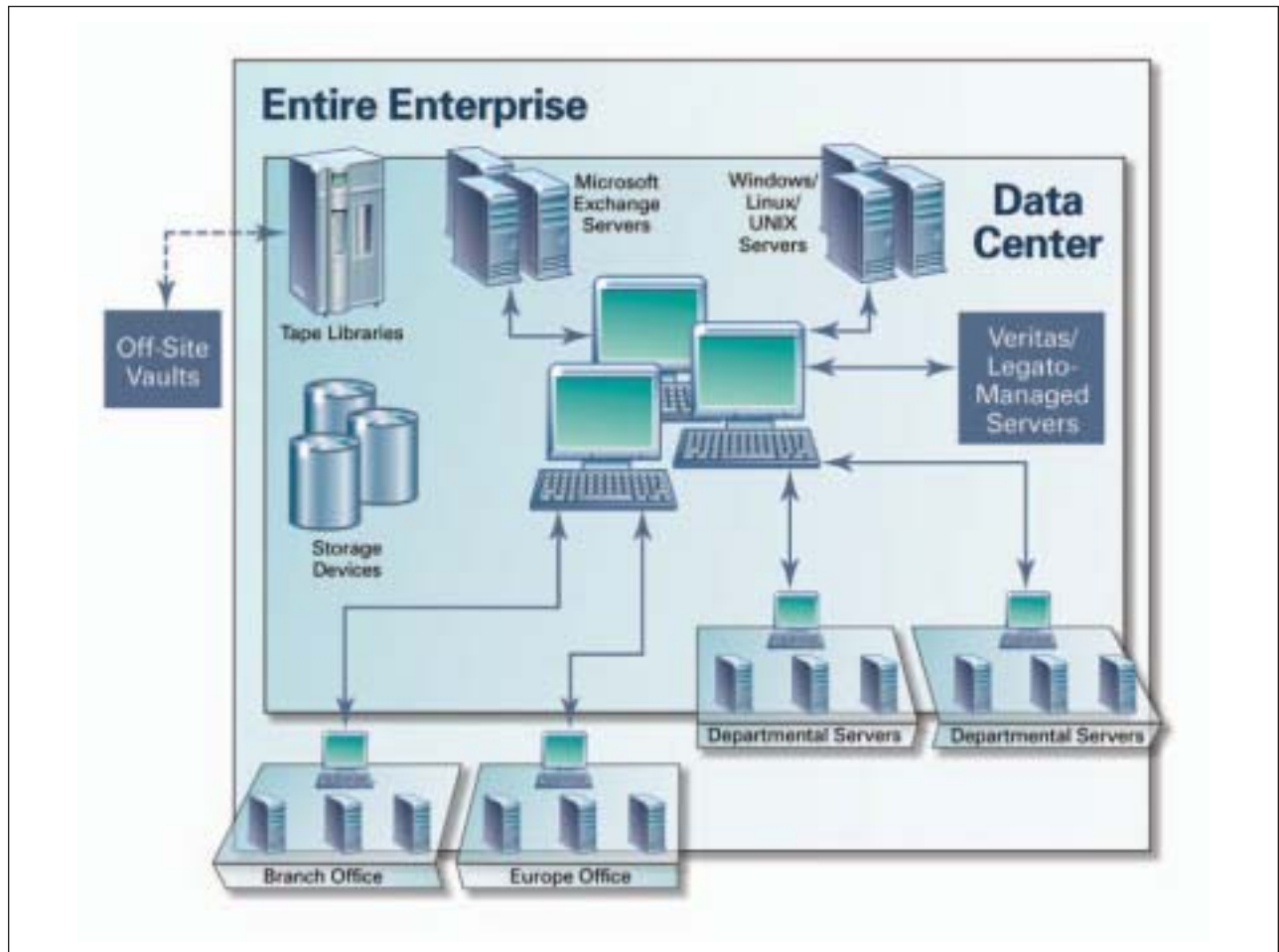


Figure 1. Many enterprises today include a data center, a departmental server, off-site vaulting and multiple consoles for administration.

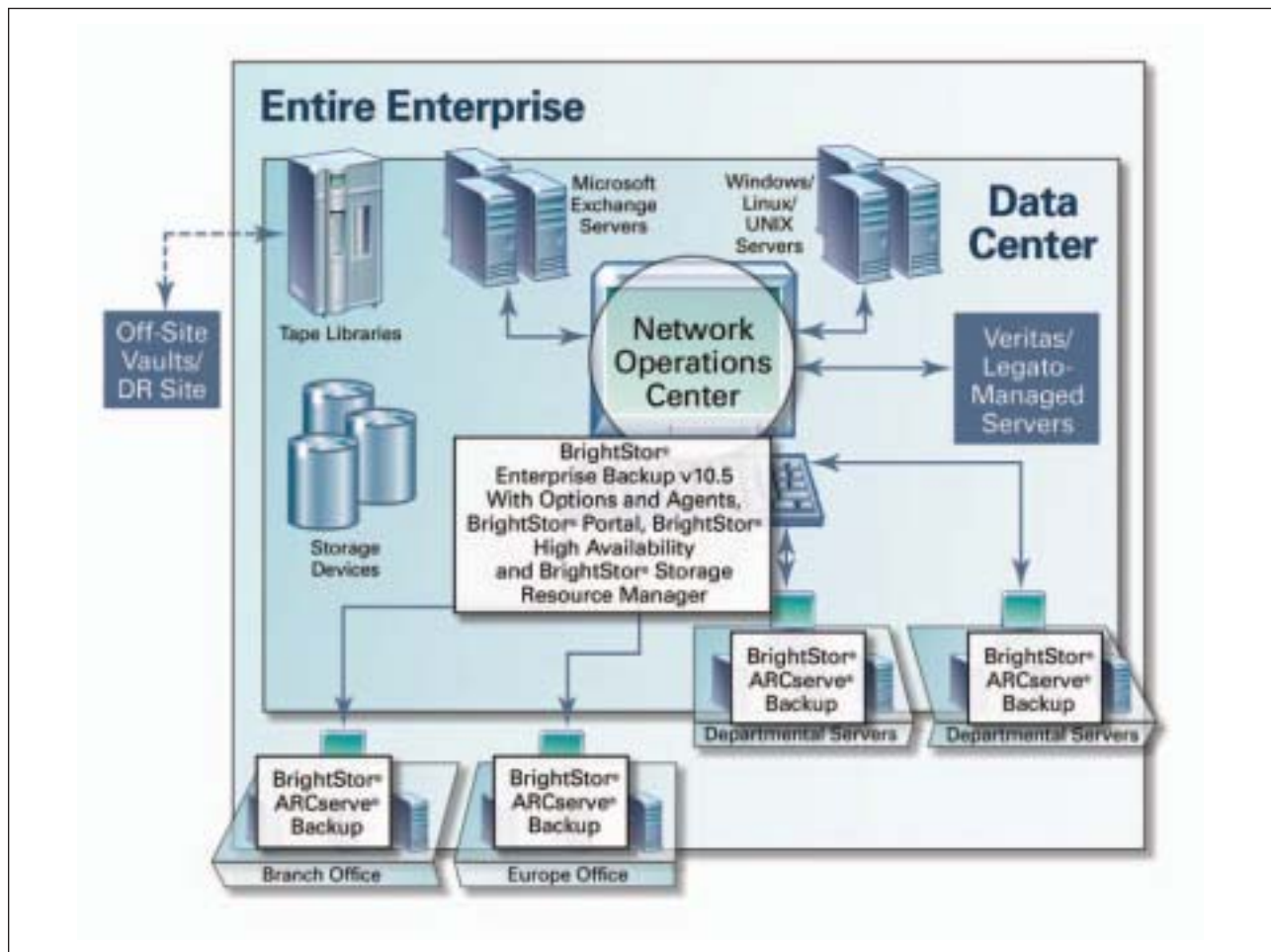


Figure 2. An integrated family of solutions can centralize and simplify management and protection.

Whether you are worried about fines and other penalties associated with regulatory noncompliance, or you just want to get control of your Microsoft

Exchange availability and protection problems and save some budget dollars, there are now excellent tools available to help you achieve your objectives.



Computer Associates®