

Complete Online Exchange Server Data Protection

VERITAS Backup Exec™ 10 *for Windows Servers*

Agent for Microsoft Exchange Server

TABLE OF CONTENTS

Executive Summary	3
What's New:	3
Product Highlights	3
Why Protect Microsoft Exchange Server?	4
Why Do You Need the Backup Exec Agent For Exchange?	4
Protecting Exchange Server.....	5
Introduction.....	5
Application Protection	6
Business Needs and Requirements	6
Options.....	6
Deployment Guidelines.....	7
Database Protection.....	7
Business Needs and Requirements	8
Options.....	10
Data Protection Deployment Guidelines.....	11
Mailbox or Message-Level Protection.....	11
Business Needs and Requirements	12
Options.....	13
Deployment Guidelines.....	13
Other Exchange Solutions From VERITAS.....	14
Summary	15

EXECUTIVE SUMMARY

Companies today are facing the ever-increasing challenge of protecting and managing the explosive growth of valuable data. E-mail, now the predominant method of exchanging ideas, generates huge amounts of information that must be immediately available to users to ensure continued business communication. The loss of a single message may generate hours of unnecessary and frustrating labor for administrators and can lower productivity or even slow down progress within organizations.

VERITAS Backup Exec Agent for Microsoft Exchange Server is the fastest and most flexible way available to protect Exchange 5.5, Exchange 2000, and Exchange 2003 Server data while the application is online. Providing full backup and restore of all Exchange Server components, including embedded objects, attributes, and all Outlook components, the Agent for Microsoft Exchange Server also gives administrators the flexibility to perform individual mailbox backup with selective restore down to the individual message.

WHAT'S NEW:

- **Restore automatically mounts the database upon completion and perform a consistency check:** This ensures a valid database is brought online quickly when using traditional or snapshot backups.
- **Recovery storage groups:** This performs mailbox or message-level restores from a full traditional backup without requiring the installation of a separate Exchange 2003 server.

Key Benefits

- Helps safeguard the integrity of critical corporate Exchange 5.5, Exchange 2000 and/or Exchange 2003 Server data.
- Incorporates online nondisruptive Exchange Server database protection as part of everyday backup routines, which increases the chance of data recovery and minimizes data loss without inhibiting daily activity.
- Protects individual mailboxes, giving administrators the ability to perform granular restores down to a single message.

PRODUCT HIGHLIGHTS

- Protects Exchange data down to the individual storage group, database, or mailbox with full, incremental, copy, or differential backups
- Protects multiple databases on a single Exchange 2000 or Exchange Server 2003 server
- Transparently integrates online "hot" Exchange Server 5.5, Exchange 2000, and Exchange Server 2003 server backups within regularly scheduled network backup routines
- Relocates any database to another server or storage group with move-database (MDB) relocation
- Uses automated data staging to quickly backup and recover Exchange Server databases or transaction logs by staging backups to disk or RAID system before a nightly full or differential to tape
- Eliminates backing up redundant file copies sent to large numbers of users via single-instance storage of attachments. Reduces time required to perform mailbox backups and reduces the amount of media required to protect the Exchange environment
- Protects individual databases within a storage group
- Supports cluster failover in a Microsoft Cluster Server or VERITAS Cluster Server environment, improving fault tolerance
- Provides LAN-free Exchange Server backup, supporting storage area networks (SAN); the SAN Shared Storage Option increases backup and recovery performance over a fibre-channel or iSCSI network
- Uses the native Exchange Server Backup APIs and Messaging APIs for reliable Exchange protection
- Uses single-pass restore, supporting one-step restore of backups created using the Exchange Server 2003 VSS writer when used with the Backup Exec Intelligent Disaster Recovery Option
- Supports off-host backup using the Advanced Disk-based Backup Option (ADBO) to eliminate the backup window, freeing the Exchange Server to serve its users 24x7x365 and perform backups at any time. See the ADBO white paper for details.

WHY PROTECT MICROSOFT EXCHANGE SERVER?

Messaging applications have become key communication tools for businesses of all sizes. Today, messaging is a common and vital form of communication, often replacing the phone as the preferred mechanism for exchanging information in the business world. It is a more efficient and cost-effective way to disseminate information of all types (such as text, image, video, and even voice) to fellow employees and business associates anywhere in the world. In fact, many companies consider their messaging servers to be mission-critical and are among the first servers to recover after a disaster.

Microsoft Exchange Server™ is a stable enterprise-messaging platform, with advanced features to ensure the high availability of this critical service. Since its introduction in 1996, Microsoft Exchange Server has garnered 47.5% of the messaging server market, according to a December 2002 Ferris Research report.

To maintain the availability of Microsoft Exchange and protect its data stores, a working and thoroughly tested data protection and recovery plan, as well as reliable data-protection software, are essential. Together, they ensure the timely recovery of the Exchange Server system environment, user configuration data, and/or message content. The objective is to help minimize downtime for the enterprise messaging environment and to provide the quickest possible data recovery in the event of a system crash, database corruption, loss of a single mailbox, or other data loss.

This white paper addresses several aspects of an Exchange Server data protection plan, focusing on how VERITAS Backup Exec 10 *for Windows Servers* and the Backup Exec Agent *for Microsoft Exchange Server* can meet the needs of this plan. It also introduces several other VERITAS products that enhance Exchange Server data protection and availability.

WHY DO YOU NEED THE BACKUP EXEC AGENT FOR EXCHANGE?

Protecting a large application server such as Microsoft Exchange requires careful thought and planning to meet the availability needs of your company and its budget. The most common method of formalizing these needs is the implementation of service level agreements (SLAs). These agreements are contracts between the users and providers (such as IT departments) that outline such factors as expected services, acceptable downtime, and response time for problem resolution. It is critical that you understand these factors during the design phase of your Exchange deployment, as they can heavily influence the resources you will need to support the plan.

The basic rule of thumb for data protection is that the higher the requirement for availability, the higher the cost. The chart below shows the various technology stops along the way to higher availability. Notice that the cornerstone of any availability solution is backup, and choosing a reliable backup product should be paramount because it may be the last line of defense against data loss. VERITAS Backup Exec, together with the Agent for Microsoft Exchange Server, easily meets the criteria for fast, flexible, and reliable Exchange Server data protection. In fact, Backup Exec has supported Microsoft Exchange since its introduction in 1996 (and has supported the Windows Server operating systems since their introduction in 1992), providing established experience and proven reliability in the Exchange Server market.

In addition to offering Backup Exec, which supports baseline availability for Exchange Servers, VERITAS also offers other products that support Exchange deployments up to the highest levels of availability.



PROTECTING EXCHANGE SERVER

INTRODUCTION

With most database applications like Exchange Server, data protection can be divided into two main objectives: (1) preparing for a disaster recovery where all data (the Windows operating system, Exchange Server application, and its database) is destroyed, and (2) preparing for the restoration of all or some of the application's database data.

Disaster recovery preparation includes protecting the Windows operating system and system state, the Exchange Server application directory, and database backups of Exchange. (For details on protecting the Windows operating system, see the VERITAS white paper "Data Protection for Windows Servers.")

As all user data is contained in the Exchange Server databases, protecting them is the main objective. Exchange Server provides several methods to backup and restore this data, but consider the pros and cons of each to ensure you achieve your data protection goals.

There are two basic ways to backup Exchange Server data at the database and mailbox levels. Database backup is mandatory, as restoring a database is the only way to retrieve all of the Exchange Server data in times of disaster. Mailbox backup is optional for most companies, but it is highly advantageous when the data protection requirements demand fast recovery of specific mailbox or public folder data.

Data protection for Microsoft Exchange can be divided into three major categories:

- **Application (Exchange Server) protection (required for disaster recovery):** This includes backup and recovery of Exchange Server's application files, clustering support for Exchange, and disaster recovery procedures to recover the entire application.
- **Database protection (required for disaster recovery):** This includes the protection of the Exchange Server data using methods such as backup and restore of database volumes in the Exchange Server storage groups and databases.
- **Mailbox protection (optional protection):** This includes techniques for the granular protection of Exchange data down to individual mailbox data, including mail message and attachments, for quick retrieval.

APPLICATION PROTECTION

At the application-protection level, the focus is to protect the Exchange Server application files and settings, along with presenting some options to protecting the entire application.

Business Needs and Requirements

Backing up the host server for Exchange: Since Exchange Server runs on Windows 2000 or Windows 2003, protecting the underlying Windows operating system and Exchange Server's files and settings are very important for a timely disaster recovery. This includes backing up all files on the volumes that Windows and Exchange are installed on and backing up the Windows system state, which contains critical Exchange Server configuration information. The backup schedules of this data should coincide with the backups of Exchange Server data (outlined below), creating a consistent set of data for an easier disaster recovery.

Backup Exec Advantage

Backup Exec easily protects Windows files, the Windows system state, Exchange Server files, Exchange database, and Exchange mailbox backups within a single schedulable job. Or you can break these tasks into multiple jobs if your environment, performance needs, schedule, or data-retention periods demand. If disaster occurs to your Exchange server, the Backup Exec Intelligent Disaster Recovery (IDR) option can help you quickly bring Windows back to life in preparation of recovering Exchange.

Backing up the Active Directory: For Exchange Servers running Active Directory (AD), following the above guidelines backup the Exchange host server will automatically backup the AD database with the system state backup. (If the Exchange Server is not running AD, backup the system state on a server running AD.) Schedule the AD backups as close to the backups of Exchange Server data as possible to create a consistent data set around the most recent server and operating system settings.

Backup Exec Advantage

Protecting the Active Directory in Backup Exec is as simple as clicking a checkbox. By simply selecting "System State" on a Windows Server 2000 or Shadow Copy Components (which include the system state) on a Windows 2003 Server in the Windows server's backup selections, Backup Exec will backup all critical Windows operating system data, including Active Directory, the cluster database, registry, and boot and system files. On recovery, Backup Exec lets you restore all or selected parts of the system state.

Options

Protecting clustered Exchange Servers: An enterprise-level feature of Exchange Server is its tight integration with Microsoft Cluster Services (MSCS) or VERITAS Cluster Server. Clustering technology offers the huge benefit of clustering two or more Windows 2000 and Windows 2003 servers (called nodes) to serve as one highly available server in case one server becomes unavailable. With clustering technology, Exchange Server presents itself as one virtual server that can represent all the servers in the cluster. To properly protect a clustered Exchange installation, the backup application must be able to target the virtual server, so if one Exchange server becomes unavailable, the backup and restore operations can continue.

Backup Exec Advantage

Backup Exec fully supports up to a 32-node clustered installation of Exchange on Windows 2000 and Windows Server 2003 with VERITAS Cluster Server (the maximum number of nodes for MSCS is eight). If Backup Exec is running in the same cluster as Exchange, Backup Exec can automatically restart database backups that were interrupted because of a failover and restart Exchange Mailbox backups at the point where the backup was interrupted.

Deployment Guidelines

- Disaster recovery tip: To restore a consistent snapshot of backup data during disaster recovery, a good strategy is to coordinate the full backups of the Windows operating system files, Exchange Server application files, and the Windows system state with the full backups of the Exchange Server database. Follow this strategy for differential or incremental backups of files and database backups, as well. At least backup the Windows system state with each Exchange database backup, since this will not add much time to your backup and will provide higher protection for disaster recovery later.
- Avoid making the Exchange Server a domain controller. For disaster recovery, it is much easier to restore Exchange if you don't have to first restore the Active Directory or primary domain controller.
- Exchange 2000 and Exchange Server 2003 create an Installable File System driver that shows up as an M: volume on the Exchange Server. Do not select this volume for backup, as the data cannot be restored.
- Do not install Exchange onto a domain that does not have at least two domain controllers. Database replication is not possible with only one domain controller in a domain. If the domain controller fails and corrupts the Active Directory, transactions not included in the last backup may not be recoverable. By contrast, if you have at least two domain controllers in a domain, databases on the failed domain controller can be updated using replication to fill in missing transactions after the database backups have been restored.
- Disable **Write Cache** on the SCSI controller. Windows does not use buffers, so when Exchange (or other applications) receives a write-complete notice from Windows, the write-to-disk has been completed. If **Write Cache** is enabled, Windows responds as though a write-to-disk has been completed, even though it has not, and will provide this incorrect completion information to Exchange (or other applications). The result could be data corruption if the system crashes before the write operation is actually completed.

DATABASE PROTECTION

Exchange Server has two main databases for user information: the information store and the directory.

The information store is where user data is stored. This store is comprised of a public and a private database. All public folder data is stored in the public database. All user mailboxes are stored in the private database. To provide better support for scalability, clustering, and backup, Exchange Server 2000 and 2003 let the information store be split into several storage groups of databases serving specific users. Each storage group can be protected individually, and transaction logs between databases in the group can be shared, providing more-flexible data protection.

The directory is the database of users (recipients) in Exchange. In Exchange 5.5 and earlier, the directory was part of Exchange itself. With Exchange 2000 and Exchange 2003, the application uses Active Directory for the user database. Therefore, Exchange 2000 and Exchange 2003 must run on Windows 2000 or Windows 2003 in an environment where Active Directory is used. Although data in the directory doesn't change as much as the information store, it is critical that the directory be protected in same backup schedule as the information store to maintain consistency between users and their data.

Exchange uses shared transaction logs for each database in a storage group, allowing highly granular protection of Exchange via incremental or differential backups of the logs. Transaction logs are files containing a running log of changes to a database. To recover from error or corruption, Exchange can replay these logs back into the database up to the last successful transaction. The Exchange server can generate quite a few transaction logs very quickly if the Exchange server is busy. To control log growth, frequent incremental or full backups are required, since Exchange Server deletes the log files after these backups. Exchange Server offers a Circular Transaction Log mode in which Exchange uses a small group of transaction logs that are overwritten in a rotation. While this requires less log space, it does *not* allow incremental or differential backups of the Exchange Server. In addition, Circular Log Transaction mode prevents recovery of Exchange up to the point of failure. Recovery can be performed only to the point of the last full or copy backup.

Business Needs and Requirements

Online “hot”) backup of the Exchange message databases: Because of message’s mission-critical nature, Exchange must always be available. To ensure this availability, the Backup Exec Exchange agent performs an online backup of Exchange databases that backup applications can interact with. This allows several backup methods:

- **Full backup:** This backs up the selected database and the associated transaction logs, then deletes the logs after backup. Full backups are the foundation backup type that you can base complex and scalable backup schemes on. If given a choice of only one method of backup, choose a full one.
- **Incremental backup:** This backs up the transaction logs for the associated database and deletes them after backup. The advantage is that this method backs up the least amount of data and therefore has the smallest impact on the Exchange Server. Another advantage is that it helps conserve log file space. The disadvantage is that all incremental backups must be restored consecutively after restoring a full backup. For example, if full backups are performed Sunday and incremental backups are performed during the weekdays, then five sets of data (one full backup and four incremental backups) are needed to recover from a disaster on Friday. Incremental backups save time during a backup but can add time during a restore when compared to differential backups.
- **Differential backup:** This backs up the transaction logs for the associated database and does not delete the logs. The differential method cumulatively backs up all changed data (logs) since the last full or incremental backup. The main advantage to using differential backups occurs during restore: You have to restore only the full backup and the last differential backup (since it is cumulative). For example, if full backups are performed Sunday and differentials during the weekdays, then only two sets of data (one full backup and one differential backup) are needed to recover from a disaster on Friday. The disadvantages to the differential method are that it requires more disk space for logs and more data is backed up compared to incremental backups. Differential backups add time for a backup but save time during a restore when compared to incremental backups.
- **Copy backup:** This backs up the selected database and the associated transaction logs. This method is good for making a copy of the database without disturbing any full, incremental, or differential backup scheme currently in use.

Note: You can use Exchange Server 2003 VSS writer support to take snapshots supporting all backup types listed above (differential and incremental backup types require Exchange Server 2003 SP1). You can use this functionality for disaster recovery with the Backup Exec Intelligent Disaster Recovery option for single-pass restores of entire Exchange environments.

The Exchange Server backup scheme that works best for each organization is based on the size of the environment; the number of transactions processed each day, and the service level agreement with users. To decide which backup methods to use, consider the following:

- **In small office environments** with relatively small numbers of messages passing through the system, a daily full backup at night will provide sufficient data protection and the quickest recovery.
If log file growth becomes an issue, use incremental backups at midday to provide an added recovery point and manage the log file growth for you automatically.
- **In medium and large environments** many shops run full backups on the weekend and incremental backups during the week or intraday. If you have sufficient disk space for a week’s worth of log files, consider implementing differential backups during the week. Mix the backup types within the day or week, but keep the scheme as simple as possible to make disaster recovery manageable.
- **In large environments,** you have several options:

- Consider implementing Exchange storage groups if using Exchange 2000 or 2003. Back up each storage group on a separate schedule or in parallel to separate tape devices for better performance if your server can handle the input/output (I/O) traffic. For example, separate mailbox users by department or last name into two storage groups that could be backed up by with two high-performance tape drives to reduce your backup window. Implementing storage groups provides greater flexibility and performance while adding complexity to Exchange Server administration; see the Exchange Server documentation for guidelines for correctly implementing this feature.
- Consider implementing off-host backup solutions. Off-host backup solutions create hardware snapshots the can be split from the production Exchange server, eliminating any backup window, and mounted on the backup server to perform a high speed SAN backup that can be performed as frequently as desired. See the VERITAS “Advanced Disk-Based Backup Option” white paper for complete details.

Hot backup of the key management service (KMS) database and site-replication service (SRS) databases: If these services databases have been deployed, include them into the Exchange Server backups. (They are normally very small.) Both will be protected using the same backup method that you selected for Exchange database.

Backup Exec Advantage

Backup Exec fully supports all the required database backups described here and all the associated backup methods. It also lets an administrator easily view, select, and create jobs for protecting this data. Backup Exec 10 for Windows Servers offers “guide me” wizards to help you determine which backup method is best.

The Backup Exec Exchange agent leverages the latest VSS writer backup capabilities offered with Exchange Server 2003 and extends this support to include NAS configuration support, legacy API backup, mailbox (MAPI) backup with single-instance message attachment backup, individual database backup, differential backup, copy backup, incremental backup, site-replication service (SRS) protection, and key management service (KMS) protection. For restores, the Backup Exec Exchange agent provides additional functionality, including recovery storage group restore (for 2003 restore targets), individual database restore, automatic re-creation of user accounts and mailboxes for mailbox (MAPI) restore, automatic commit on restore, automatic loss restore, automated scheduled database dismount before restore, automated database mount after restore, and redirected application-level restore at both the server and mailbox level.

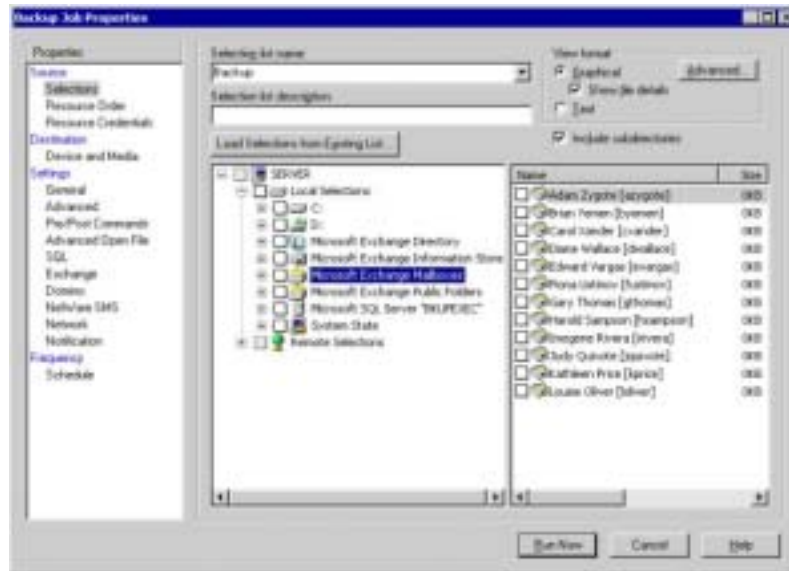
In these environments, you must use traditional backup methods to protect Exchange Server 2003:

- Individual database backup, OR
- Cluster configuration data protection, OR
- NAS configuration data protection, OR
- Mailbox and message-level data protection

In these environments, you should *not* use Exchange VSS Writer to protect Exchange Server 2003:

- Not running Windows Server 2003 operating system, AND
- Not configured in a cluster, AND
- Not configured using NAS, AND
- Not performing mailbox or message-level backup

Note: Mixing traditional Exchange Agent backups (differential, incremental, and copy backups) with Exchange Writer backups in an Exchange Server 2003 protection scheme on Windows Server 2003 is neither recommended nor supported. However, mailbox backups may be combined with either protection method to facilitate the retrieval of individual messages.



Backup Exec clearly displays all Exchange Server data and allows easy integration of database or mailbox backups into the backup scheme.

Options

Off-line backup of Exchange: An off line, or cold, backup of Exchange is simply a backup of data while Exchange Server services are not running. Therefore, all the Exchange Server files and databases are closed and can easily be backed up reliably with normal file backup. The main advantage of a cold backup presents itself during disaster recovery, since all of Exchange can be easily restored in one pass because it was backed up as simple files. However, the major disadvantage of a cold backup is the downtime Exchange users face while the backup occurs, since Exchange must be down the entire time it takes to backup its databases. A backup of this type could take hours.

VERITAS Advantage

While few customers choose to perform cold backups of Exchange because of the downtime incurred, VERITAS offers Backup Exec Advanced Disk-Based Backup, an enterprise-class Exchange solution. This product lets customers use volume mirroring technology, either from VERITAS (including SFW and FlashSnap) or from a hardware snapshot provider, to logically copy Exchange Server 2003 databases running on Windows Server 2003 to another server by breaking the mirror and mounting it on the second server so that cold backups can be performed without slowing the Exchange application or the end users. (See support.veritas.com for a complete list of supported hardware snapshot providers for Backup Exec for Windows Servers.) This offers the advantages of very-low-impact database backup, offering almost instant recovery and easier disaster recovery. See the "Other Exchange Solutions from VERITAS" section below for more details on the Backup Exec Advanced Disk-Based Backup Option.*

Backup of Exchange data on clients: Exchange users can store message data locally on their computers. This provides them tremendous flexibility, but it prevents the IT department from fully protecting that data through Exchange database or mailbox backups. Furthermore, there are two strong shifts in enterprises today that exacerbate this problem. The first is the proliferation of remote users with laptop computers and the second is IT organizations putting space limits on Exchange server mailboxes, which forces the Exchange user to store mailbox data locally. This combination adds up to more critical message data at much higher risk of being lost or stolen, which again, is not protected by Exchange server or mailbox backup methods. To protect this data,

enterprises must use backup procedures of several Outlook files — the Personal Message Store (PST), Offline Message Store (OST), and the Personal Address Book (PAB) — on a regular basis.

VERITAS Advantage

To help solve the need for desktop and laptop data protection, VERITAS offers the new Backup Exec Desktop and Laptop Option (DLO). DLO is an automated solution to protect this crucial remote message data stored in end user PST files along with all other data on the computer. DLO will automatically backup your PST messaging data whether you are using Outlook while attached or unattached to the network. DLO will send only changes to your files to minimize the amount of network traffic and reduce the amount of time required to protect user data. All changes are sent in real time or, when disconnected from the network, changes are cached on disk and sent to the target network share when the user re-establishes a connection to the network

Data Protection Deployment Guidelines

- Locate transaction log files on a separate physical disk from the database. This is the single most important configuration affecting the performance of Exchange. This configuration also has recovery implications, since transaction logs provide an additional recovery resource.
- Disable circular logging. Circular logging minimizes the risk that the hard disk will be filled with transaction-log files. But, if a solid backup strategy is in place, transaction log files are purged during the backup anyhow, freeing disk space. If circular logging is enabled, transaction log histories are overwritten, incremental and differential backups of storage groups and databases are disabled, and recovery is possible only up to the point of the last full or copy backup.

MAILBOX OR MESSAGE-LEVEL PROTECTION

Protecting the Exchange Server at the mailbox or message level largely buys the user a great convenience to restore Exchange data at a very granular level (such as message, calendar item, or note). The usual reason to perform mailbox backups is to allow easy restoration of message data for regulatory, legal, or emergency reasons (such as corporate audit, subpoena, or an executive deleting critical files). Backup Exec has added single-instance storage of attachments that eliminates the need to create multiple copies of redundant data. This feature can dramatically reduce the time required to back up mailboxes and the amount of media required to protect these mailboxes.

Although mailbox backups can make it very fast and convenient to restore data, they come at a higher cost than database backups for the following reasons:

- Mailbox backups must be performed in addition to Exchange Database backups. They should not be used as part of your disaster recovery scheme. Restoring all mailboxes is not the same as restoring the entire database because mailbox backups do not include metadata and the Exchange internal single-instance storage information.
- Mailbox backups are much slower than database backups. While Exchange Server provides backup vendors with high performance APIs to protect the database, there no high-speed APIs for mailbox backups. The few backup vendors that have crafted mailbox and message-level backup solutions use the same messaging API (MAPI) to back up data as an Exchange client (Outlook). The difference in transfer rates between mailbox and database full backups can be huge, as database backups can easily be higher than 10Mbps, while mailbox backups are typically no faster than 3Mbps. Using incremental and differential backup techniques on mailbox backups can significantly cut down on backup time.
- Mailbox backups duplicate information backed up with Exchange database backups. Because mailbox data can contain *many* entries, mailbox backups result in larger catalog sizes and greater tape usage.

Business Needs and Requirements

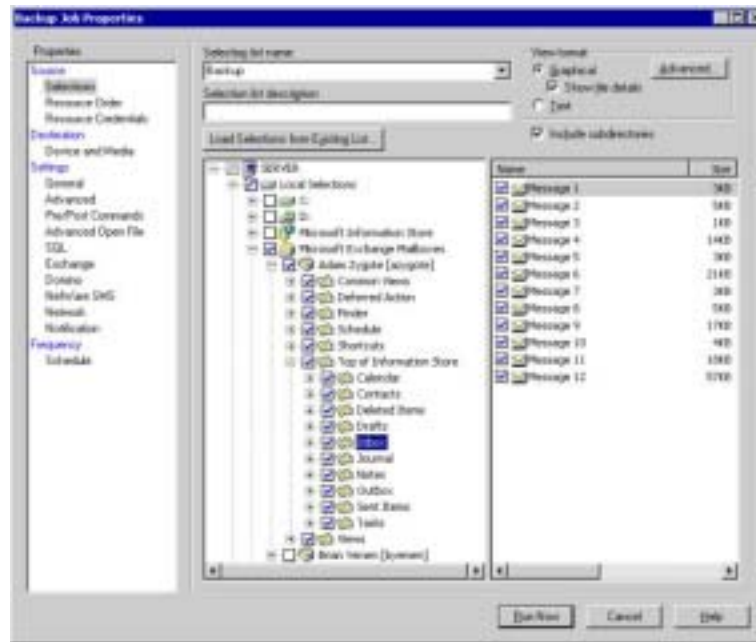
Off-host backup: Has your company come up against the limits of your backup windows for your Exchange server? If yes, review the VERITAS “Advanced Disk-Based Backup” white paper that covers in detail how you can eliminate your dependency on backup windows as your Exchange servers continue to grow.

Online protection of specified Exchange mailboxes: Companies requiring fast and highly granular restores of Exchange information store data can benefit greatly from implementing mailbox-level backup. Given the mailbox-backup limitations stated earlier, only mailboxes that have a high chance of needing this capability should be selected for backup.

Hot backup of specified public-folder data: Like mailbox protection, some companies require fast and granular protection of specific public-folder data. Backing up public-folder data comes with the same advantages and limitations of mailbox backups, so be sure to choose the data that truly needs this support.

To meet this challenging backup need and improve the speed of this backup type, VERITAS has added several features to Backup Exec Exchange that support both mailbox and public-folder data:

- **Single-instance backup of attachments:** VERITAS recognized that the bulk of the Exchange data is composed of attachments to messages. To improve the speed of mailbox backups, Backup Exec now uses single-instance backup of any type of Exchange data attachments such as messages and calendar entries. During the backup of selected mailbox data, Backup Exec will back up attachments only once, even though the attachment may be associated with several messages in the selected mailboxes. This speeds backup and reduced storage space. However, single-instance storage of attachments on all messages takes significant processing time, so it is generally faster to simply back up the multiple copies of the attachments.
- **Incremental and differential backup method extensions:** as it does for the incremental and differential backup methods for the Exchange Database, Backup Exec offers the same method extensions for mailbox and public-folder backups.
- **Global exclusion of mailbox and public-folder data:** Exchange mailboxes can contain *large* amounts of data that does not need to be backed up. Instead of having to specifically select what you do want to back up across hundreds of mailboxes, Backup Exec lets you globally exclude data from all selected mailboxes in one easy method. Examples of this might be deleted items, sent items, calendar, views, journal, tasks, or specific folder names. Wildcards are supported in mailbox or folder names.
- **Automatic re-creation of user accounts and mailboxes on restore:** When a previously backed-up mailbox is deleted, Backup Exec can easily re-create the mailbox upon restoration of any data from the mailbox. This feature is very convenient for instances when a mailbox has been accidentally deleted.
- **Easy selection of mailbox and public-folder data:** Mailbox backup is tightly integrated with Backup Exec: Simply select mailbox data for backup or restore via wizards or the graphical interface — just like any other data.
- **Reliable and complete mailbox protection:** When comparing mailbox-level backup solutions, it is wise to test the mailbox restore to ensure that *all* mailbox data is restored, including views, Outlook flags, and HTML messages. Backup Exec reliably backs up all mailbox data by default and lets you exclude what you don’t want.



With Backup Exec, you can easily select the Exchange Mailbox data you want to back up. Similar views of message data are presented for public folders and when selecting data for restore.

Options

Exchange Server 2003 has added a feature called Recovery Storage Groups (RSG) to simplify mailbox restores from database backups. RSGs let administrators retrieve granular data components, such as mailbox and message data, from database backups without requiring installation of a separate Exchange recovery server, as is still required with Exchange Server 2000. RSGs can be used only with mailbox databases, not with public folders. The mailbox or message-level data can be extracted from the RSG and restored into the existing datastore.

Backup Exec Advantage

Administrators now have the flexibility to choose the backup and restore strategy that is optimized to best meet their SLAs. Administrators may opt to perform mailbox-level backups for some employees such as senior manager and use the RSG strategy to retrieve individual mail messages for Exchange Server 2003 users that are protected using full information-store backups. Administrators can now also mix media types to protect mailbox-level data. Administrators may now want to set up back up to disk for mailbox-level backups to improve performance, reducing the backup window for mailbox backups. In addition to the ability to back up to disk, Backup Exec now includes disk-staging features so disk-based backups can be copied to tape on a schedule you set — not simply after the disk backup. This gives you the flexibility of keeping disk-based backups around for quick restore while protecting your data on tape.

Deployment Guidelines

- Back up mailbox data to disk:** If mailbox backups are mainly needed for short-term emergency restore cases, consider backing up mailbox data to disk and expiring the data within a short time or overwriting the data at the next mailbox backup. This method has the advantages of not taking up a tape drive resource with a slow backup and of allowing very quick restores of data without interrupting a tape drive.

OTHER EXCHANGE SOLUTIONS FROM VERITAS

Backup Exec is just one of many VERITAS solutions that support Exchange Server. VERITAS develops and sells several solutions that keep Exchange Server highly available (through clustering, replication, and snapshot management), slim and trim (hierarchical storage management), and backed up. Be sure to read the VERITAS white paper "Microsoft Exchange without Interruption" to review how these products can work together in the enterprise.

- **VERITAS Backup Exec Advanced Disk-Based Backup Option:** This option, when used with the Backup Exec Exchange Agent, can dramatically improve your overall Exchange server data-protection strategy. Administrators now can create a mirror of their Exchange data, break off the mirror, and mount it on their backup server, performing backup locally and then resynchronizing the mirror with the Exchange server at the end of the backup. This powerful feature has the ability to eliminate dependencies on backup windows and not slowing your Exchange servers during backup.
- **VERITAS Replication Exec:** VERITAS Storage Replicator™ delivers automatic, real-time data replication to Microsoft Windows Server environments, including Exchange Server. Whether needed for real-time disaster protection or for many-to-one backup centralization, VERITAS Storage Replicator handles even the most demanding replication jobs on the Windows NT, Windows 2000, and Windows 2003 platforms.
- **VERITAS Enterprise Vault:** Enterprise Vault lowers costs and saves time. It helps consolidate Exchange servers by letting more virtual data reside in the Exchange information store, eliminating the need to continually purchase additional servers for Exchange. Enterprise Vault saves time by reducing the amount of older data in the Exchange databases, so users can back up and recover systems much faster than without Enterprise Vault.
- **VERITAS NetBackup:** VERITAS NetBackup™ DataCenter delivers mainframe-class data protection for the largest Unix, Windows, and NetWare enterprise environments, especially for corporate data centers. NetBackup DataCenter provides the most advanced media management available, including dynamic tape sharing, and offers optional database agents such as Exchange Server to enable online, nondisruptive backup of mission-critical applications.
- **VERITAS Cluster Server:** This is the industry's leading open-systems clustering solution. It eliminates both planned and unplanned downtime, facilitates server consolidation, and effectively manages a wide range of applications, including Exchange Server, in heterogeneous environments. Supporting up to 32 nodes, VERITAS Cluster Server has the power and flexibility to protect everything from a single critical database instance to very large multi-application clusters in networked storage environments.

SUMMARY

Microsoft Exchange Server has quickly risen to the mission-critical status in many companies, so keeping it highly available and protecting its data is a requirement. Like many enterprise database solutions, there are several methods of backing up the Exchange Server data, which can make the administration of the backup process very complex. To tackle this problem, you need to create a data-protection plan and select a reliable backup product that suits your environment. Briefly, the steps are:

1. Determine your Exchange Server service level agreement (SLA) needs.
2. Research the Exchange Server solutions and determine which best suits the needs in your SLA.
3. Create a data-protection plan that outlines how the solutions will work with your plan.
4. Implement the plan and closely monitor the results.

Because Exchange Server implementations can scale to very large and complex installations, you may need to consider consulting services to ensure that your implementation is scalable and can be easily recovered in case of disaster.

Regardless of the size or complexity of your Exchange Server, the VERITAS Backup Exec Agent *for Microsoft Exchange Server* offers a highly reliable and easy-to-use solution to protect your data at either a database level or mailbox level. When disaster strikes, the Backup Exec Intelligent Disaster Recovery Option can help get your Exchange Server back up and running fast. When fast is not fast enough, VERITAS offers several other solutions to keep your Exchange Server available at a higher state than restore utilities can offer.

VERITAS Software Corporation
Corporate Headquarters
350 Ellis Street
Mountain View, CA 94043
650-527-8000 or 866-837-4827

For additional information about VERITAS Software, its products, or the location of an office near you, please call our corporate headquarters or visit our Web site at www.veritas.com.