

Complete Online Exchange Server Data Protection

VERITAS Backup Exec™ 10 *for Windows Servers*

Agent for Microsoft Exchange Server

TABLE OF CONTENTS

Executive Summary	3
<i>What's New:</i>	3
<i>Product Highlights</i>	3
Why protect Microsoft Exchange Server?	4
Why Do you Need the Backup Exec Agent For Exchange?	4
Protecting Exchange Server	5
<i>Introduction</i>	5
<i>Application Protection</i>	6
Business Needs or Business Requirements	6
Options.....	6
Deployment Guidelines.....	7
<i>Database Protection</i>	7
Business Needs or Business Requirements	8
Options.....	10
Data Protection Deployment Guidelines.....	11
<i>Mailbox or Message Level Protection</i>	11
Business Needs or Business Requirements	13
Options.....	14
Deployment Guidelines.....	14
Other Exchange Solutions From VERITAS.....	15
Summary	16

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 can automatically dismount the database when you start restore and mount upon completion** – ensures valid database is brought on line quickly when using traditional or snapshot backups.
- **Integrated Snapshot protection with consistency check** – Leveraging Microsoft VSS technology to provide on-host or off-host backup from consistent snapshot image.
- **Leverage Recovery Storage Groups** – perform mailbox or message level restores from a full, incremental or differential 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.
- Protection of individual mailboxes gives administrators the ability to perform granular restores down to a single message.

PRODUCT HIGHLIGHTS

- Protect Exchange data down to the individual storage group, database, or mailbox with full, incremental, copy or differential backups
- Supports the protection of multiple databases on a single Exchange 2000 or Exchange Server 2003 server
- Transparently integrate online “hot” Exchange Server 5.5, Exchange 2000, and Exchange Server 2003 server backups within regularly scheduled network backup routines
- Relocate any database to another server or storage group with move database (MDB) relocation
- Single instance storage of attachments eliminate backing up redundant copies of files sent to large numbers of users. This reduces the time required to perform mailbox backups and reduces the amount of media required to protect the Exchange environment
- Protect individual database within a Storage Group
- Automated Data Staging – quickly backup and recover Exchange Server databases or transaction logs by staging backups to disk or RAID system prior to a nightly full or differential to tape
- Supports cluster fail-over in a Microsoft Cluster Server or VERITAS Cluster Server environment, providing improved fault tolerance
- LAN-Free Exchange Server backup – Supports storage area networks (SAN), with the SAN Shared Storage Option increasing 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
- Off-Host Backup is supported in conjunction with the Advanced Disk-based Backup Option (ADBO) to eliminate the backup window which frees up the Exchange Server to serve its users 24x7x365 and perform backups at any point in time. For details on ADBO, reference the ADBO white paper.

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 of disseminating information of all types (text, image, video and even voice) to fellow employees and business associates located anywhere in the world. In fact, many companies consider their messaging servers “mission critical” and are among the first servers to recover after disaster.

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

In order to maintain the availability of Microsoft Exchange and protect its data stores, a working and thoroughly tested data protection and recovery plan and reliable data protection software are essential. Together, they ensure the recovery of the Exchange Server system environment, user configuration data and/or message content in a timely fashion. 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 forms of data loss.

This white paper will address several aspects of an Exchange Server data protection plan, focus in 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, and introduce 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 in order 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. These agreements are contracts between the users and providers (e.g., 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 regarding data protection is the higher the requirement for availability, the higher the cost will be. The chart on the next page illustrates this concept and shows the various technology stops along the way toward higher availability. Notice that the cornerstone of any availability solution is backup, and choosing a reliable backup product should be paramount since 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 supported 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 a base line level of availability for Exchange Servers, VERITAS also develops several other products which support Exchange deployments up to the highest levels of availability. This white paper will briefly introduce these products.



PROTECTING EXCHANGE SERVER

INTRODUCTION

With most database applications like Exchange Server, data protection can be divided into two main objectives; preparing for a disaster recovery where all data (Windows operating system, Exchange Server application, and its database) is destroyed, and 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. While this white paper will briefly outline the data disaster recovery preparation steps to protect the Exchange Server application files, you should read the following Backup Exec White Paper which focuses on protecting the Windows Operating System: "Data Protection for Windows Servers".

Since 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 in order to 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 back 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.

In summary, data protection for Microsoft Exchange can be divided into three major categories which support the objectives outlined above:

- **Application (Exchange Server) Protection (Required for DR)** – 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 DR)** – this includes the protection of the Exchange Server data using methods such as backup and restore of database volumes within the Exchange Server storage groups/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. Listed below are a few requirements, options, and guidelines to protecting Exchange.

Business Needs or Business Requirements

Backup 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, Windows System State, Exchange Server files, Exchange Database, and Exchange Mailbox backups within a single schedulable job...or you can break these tasks up 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 performing a disaster recovery of Exchange.

Backup the Active Directory – For Exchange Servers running Active Directory (AD), following the guidelines stated above to backup the Exchange host server would automatically backup the AD database with the System State backup. If the Exchange Server is not running AD, then select to backup the System State on a server running AD. Attempt to schedule the AD backups as close to the backups of Exchange Server data 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 System State) on a Windows 2003 Server within the Windows server's backup selections, Backup Exec will backup all critical Windows operating system data, which includes Active Directory, Cluster DB, Registry, boot and system files.

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" which can actually represent all of the servers in the cluster. To properly protect a clustered Exchange installation, the backup application must be able to target the Virtual Server, so that if one Exchange server becomes unavailable, the backup and restore operations can continue.

Backup Exec Advantage

Backup Exec fully supports up to an 32-node clustered installation of Exchange on Windows 2000 and Windows Server 2003 with VERITAS Cluster Server (8 is currently the maximum number of nodes MSCS offers). 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.

** Restart of backups is limited to restart after the last device backed up completely. For Example, if multiple Exchange Storage Groups are selected for traditional backup (SG1, SG2, SG3), and SG1 gets backed up completely, and BE is in the middle of backing up SG2 when the failover occurs, on restart we will only back up SG2 and SG3. Mailbox backups can also leverage checkpoint restart if single instance storage of attachments is not selected.

Deployment Guidelines

- Disaster Recovery Tip: In order 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 too. If this cannot be accomplished, 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 a higher degree of protection for a disaster recovery later.
- Avoid making the Exchange Server a Domain Controller. For disaster recovery purposes, 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 into 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, some transactions may not be recoverable if they were not included with the last backup. With 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, and will provide this information to Exchange (or other applications) incorrectly. The result could be data corruption if there is a system crash before the operation is actually written to disk.

DATABASE PROTECTION

Exchange Server has two main databases for user information – the Directory and Information Store.

The Information Store is where user data is stored. This Store is actually 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 allows the Information Store to be split into several Storage Groups of databases serving specific users. Each Storage Group can be protected individually and shares transaction logs between databases within the Group, thus providing a more flexible data protection scheme.

The Directory is the database of users (recipients) within Exchange. In Exchange v5.5 and earlier, the Directory was part of Exchange. 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 within the Exchange databases.

Exchange uses shared transaction logs for each database within a Storage Group, allowing the protection of Exchange in a highly granular manner 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. As you can guess, 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 types of backups. Exchange Server offers a Circular Transaction Log mode that causes Exchange to use a small group of transaction logs that are overwritten in a circular pattern. While this has the benefit of requiring less log space since it overwrites the oldest log file in a circular manner, it also has the major disadvantage of **not** allowing 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 only be performed to the point of the last “full” or “copy” backup.

Business Needs or Business Requirements

Hot (on-line) Backup of the Exchange Message Databases – Since it has been established that messaging applications are considered very important and even mission critical to some businesses, it is critical that Exchange is always available. To meet this need, the Backup Exec Exchange agent offers a method of performing an on-line or hot backup of Exchange databases which backup applications can interface with. This interface allows several backup methods such as:

- **Full Backup** – Backs up the selected database and the associated transaction logs, then deletes the logs after backup. Full backups are the foundation backup type which complex and scaleable backup schemes can be based on. If given a choice of only one method of backup choose a full.
- **Incremental** – Backs up the transaction logs for the associated database and deletes them after backup. The advantage of the incremental method is that it 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 incrementals must be restored consecutively after restoring a full backup. For example, if full backups are performed Sunday and incrementals during the weekdays, then 5 (1 full + 4 incremental) sets of data would be needed to recover from a disaster on Friday. Put another way, Incremental backups save time during a backup, but can add time during a restore when compared to differential backups.
- **Differential** – Backs up the transaction logs for the associated database, but logs are not deleted. The differential method cumulatively backs up all changed data (logs) since the last full or incremental backup. The main advantage to using differential backups is during restore: you only have to restore the full backup and the last differential backup (since they are cumulative). For example, if full backups are performed Sunday and differentials during the weekdays, then only 2 (1 full + 1 diff) sets of data would be needed to recover from a disaster on Friday. The disadvantages to the differential method are that it requires more log disk space and more data is backed up vs. incrementals. Put another way, differential backups add time for a backup, but mostly saves time during a restore when compared to incremental backups.
- **Copy** – 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/Differential backup scheme currently in use.

NOTE: Exchange Server 2003 VSS writer support can be leveraged to take snapshots offering support for all* backup types listed above. This functionality can be used for disaster recovery purposes in conjunction with the Backup Exec Intelligent Disaster Recovery option for restores of entire Exchange environments.

The Exchange Server backup scheme that will work 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 when a recovery is required. 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 - 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, then consider implementing differential backups during the week. Mix the backup types inter-day or inter-week, but it's best to keep the scheme as simple as possible to make disaster recovery manageable.

*Differential and incremental backup types require Exchange Server 2003 SP1

- **In large environments –**

- 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 which could be backed up by with two high performance tape drives to reduce your backup window. Implementing Storage Groups enables 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 provide the benefit of creating hardware snapshots that 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 Advanced Disk-based Backup Option white paper for complete details.

Hot Backup of the Key Management Service Database and Site Replication Service Databases – If these Services Databases have been deployed, then include them (each is normally very small) into the traditional Exchange Server backups***. Both will be protected using the same backup method that you selected for Exchange Database.

Backup Exec Advantage

Backup Exec fully supports all of the required database backups above and all of the associated backup methods. It also allows an administrator to easily view, select, and create jobs for protecting this data. Backup Exec 10 for Windows Servers offers “Guide Me” wizards to help the user determine which backup method is best for them.

Backup Exec Exchange agent leverages the latest snapshot (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, site replication service (SRS) protection and key management service (KMS) protection with traditional backups. On the restore side, Backup Exec Exchange agent provides additional functionality over and above the VSS writer by offering recovery storage group restore (for 2003 restore targets), individual database restore, automatic recreation 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.

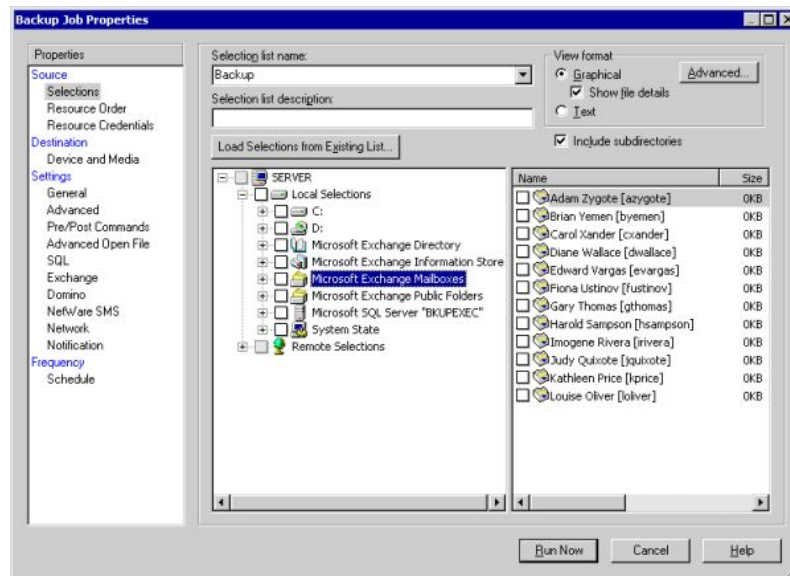
***Snapshot backups (leveraging VSS) do not support Site Replication Service Databases, individual Exchange databases, Mailbox backup or NAS devices. Site Replication Databases are dynamically recreated when full Exchange databases are restored.

Environments where you must use traditional backup methods to protect Exchange Server 2003:

- Individual database backup OR
- NAS configuration data protection OR
- Mailbox and message level Data protection OR
- SRS backups OR
- Leverage Recovery Storage Groups for restore OR
- Not running Windows Server 2003 operating system OR

Note: Intermixing of traditional Exchange Agent backups (differential, incremental or 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 in 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 of 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 and there are no log files to replay. However, there are major disadvantages of a cold backup. One disadvantage is the downtime Exchange users face while the backup and restore occurs, since Exchange must be “down” the entire time it takes to backup or restore its databases...a backup or restore of this type could take many hours. Another is that restores cannot leverage Recovery Storage Groups to perform partial restores.

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 allows customers to use volume mirroring technology, either from VERITAS (SFW, 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 impacting the Exchange application or the end users. 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.

*see support.veritas.com for a complete list of supported hardware snapshot providers for Backup Exec for Windows Servers.

Backup of Exchange data on Clients – Exchange users have the ability to store message data locally on their computers. This ability provides users with tremendous flexibility. Users can store their message data locally so that they utilize many Exchange features while detached from the network (remote user). While this gives the user many advantages, it plagues the IT department with a large problem since the data cannot be entirely protected

by 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 has the effect of forcing the Exchange user to store mailbox data locally on the laptop or desktop.

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 employ backup procedures of several Outlook files on a regular basis. Briefly, these files are the Personal Message Store (PST), Offline Message Store (OST), and the Personal Address Book (PAB).

VERITAS Advantage

To help solve the need for desktop/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 even if you are using Outlook while attached or unattached to the network. DLO will only send over 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 over in real time or, when disconnected from the network, changes are cached on disk and when the user re-establishes a connection to the network changes are sent to the target network share.

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, thus 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 only possible 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 (e.g., message, calendar item, note, etc). The usual reasons for performing Mailbox backups are to allow easy restoration of message data for regulatory, legal or emergency reasons such as corporate audit, subpoena, and the CEO deleting critical files. Backup Exec has added single instance storage of attachments which eliminate creating multiple copies of redundant data. This feature can dramatically reduce the time required to backup mailboxes and the amount of media required to protect these mailboxes. An additional benefit of MAPI backups of mailbox and message data is in cases where data is comprised by virus attacks. After the Exchange Server is patched with the latest virus definitions, when data is restored from a MAPI backup, the Exchange Server will capture and remove any infected messages rather than simply restoring the entire datastore with infected messages.

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 meta-data 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, this is not the case with Mailbox backups. The few backup vendors that have crafted mailbox/message level backup solutions are using the same Messaging API (MAPI) to backup 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 10MB/second, Mailbox backups are typically no faster than 3 MB/sec. 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. In addition, because mailbox data can contain MANY entries, it follows that mailbox backups will result in larger catalog sizes and greater tape usage.

Business Needs or Business Requirements

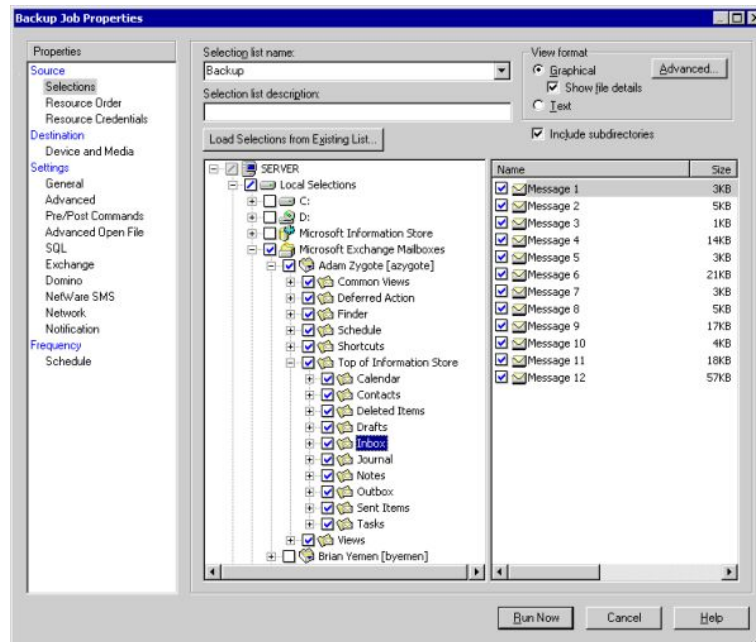
Off-Host Backup – Has your company come up against the limits of your backup windows for your Exchange server? If you can answer “yes”, I would strongly recommend that you review the Advanced Disk-based Backup white paper which discusses in detail how you can eliminate your dependency on backup windows as your Exchange servers continue to grow as you increase employees and the increased use and dependency on email.

On-Line 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 above, 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 into Backup Exec Exchange support for both mailbox and Public Folder data. Here are the highlights.

- **Single Instance Backup of Attachments** – VERITAS recognized that the bulk of the Exchange data are attachments to messages. To improve the speed of mailbox backups, Backup Exec now employs single instance backup of any types of Exchange data attachments such as messages, calendar, etc. During the backup of selected mailbox data, Backup Exec will only backup attachments once, even though the attachment may be associated with several messages in the selected mailboxes. In addition to the speed enhancements, less data needs to be transferred and thus less backup media is used. Generally, performing single instance storage of attachments on all messages isn’t worth the processing time, as the decision to backup message data has a fixed time cost, thus it is generally faster to simply backup the small pieces of data vs. making a single instance storage of an attachment decision for every item backed up.
- **Incremental & Differential Backup Method extensions** – Like the Incremental & Differential backup methods for the Exchange Database, Backup Exec offers these methods for mailbox and Public Folder backups.
- **Global Exclude of Mailbox and Public Folder Data** – Exchange Mailboxes can contain large amounts of data which do not need to be backed up for your purposes. Instead of having to specifically select what you do want to backup across hundreds of mailboxes, Backup Exec allows you to 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 Recreation of User Accounts and Mailboxes on Restore** – In instances where a previously backed up mailbox is deleted for some reason, Backup Exec can easily recreate the mailbox upon restore of any data from the mailbox. This feature is very convenient for instances when 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 GUI – 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 ALL mailbox data is restored, including views, Outlook flags, and HTML messages. Backup Exec reliably backs up all mailbox data by default and gives you the ability to exclude what you don’t want.



With Backup Exec, you can easily select the Exchange Mailbox data you want to backup. 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 (differential, incremental, copy, etc.), traditional database backups. RSGs allow administrators to 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 only be used with mailbox databases and not with public folders. The mailbox or message level data can be extracted from the RSG and restored into the existing data store.

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 traditional backups for some employees such as senior managers and use the RSG strategy to retrieve individual mail messages for Exchange Server 2003 users that are protected using traditional full information store backups. Administrators can now also mix media types to protect mailbox level data. Administrators may now want to set up backup to disk for mailbox level backups to improve performance, reducing the backup window for mailbox backups. In addition to the ability to backup to disk, Backup Exec now includes disk staging features to allow disk based backups to 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

- Backup 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 frame or “overwriting” the data upon the next Mailbox backup. This method has the advantages of not taking up a tape drive resource with a slow data rate backup and 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 which support Exchange Server. VERITAS develops and sells several solutions that keep Exchange Server highly available (clustering, replication, snapshot management), slim and trim (hierarchical storage management), and backed up. See below for a list of these products, but 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 in conjunction with the Backup Exec Exchange Agent, can have a dramatic impact on your overall Exchange server data protection strategy. Administrators now have the ability to create a mirror of their Exchange data, break off the mirror and mount it on their backup server performing backup locally and then re-syncing 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 impacting 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 many-to-one backup centralization, VERITAS Storage Replicator handles even the most demanding replication jobs on the Windows NT and Windows 2000 and Windows 2003 platforms.
- **VERITAS Enterprise Vault** – Enterprise Vault lowers costs and saves time. It helps consolidate Exchange servers by allowing more virtual data to 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, allowing users to 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. VERITAS NetBackup DataCenter provides the most advanced media management available, including dynamic tape sharing, and offers optional database agents like Exchange Server, to enable online, non-disruptive backup of mission critical applications.
- **VERITAS Cluster Server** - is the industry's leading open systems clustering solution which 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 features 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, therefore keeping it highly available and protecting its data is not an option. 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 which outlines how the solutions will work with your plan
4. Implement the plan and closely monitor the results

This white paper only covered the high-level considerations of an Exchange Server data protection plan and how you should implement the backup solution. Since 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.