

Planning a  
Microsoft  
Exchange Server  
Data Protection  
Strategy  
Using Version 8.0 of  
Backup Exec™  
for Windows NT/2000



BUSINESS WITHOUT INTERRUPTION™



## Table of Contents

1. Introduction .....	1
2. Introduction to Microsoft Exchange Server .....	1
3. Data Protection Considerations .....	2
Exchange Server Protection .....	2
Loss or Corruption of the Information Store .....	3
Mailbox Level Protection .....	3
Critical Exchange Files .....	3
Key Exchange Data Files.....	4
Client Database Files .....	4
Transaction Logs.....	6
Previously Committed Logs .....	6
“Checkpoints” and Checkpoint Files .....	7
Reserved Logs .....	7
Circular Logging Considerations.....	8
Review of Key Planning Items .....	8
4. Exchange Data Protection Tools.....	8
Microsoft Windows NT/2000 Backup .....	8
Backup Exec™ for Windows NT/2000.....	8
Microsoft Exchange Agent for Backup Exec for Windows NT .....	8
Intelligent Disaster Recovery™ Option for Windows NT.....	9
5. Backing up the Exchange Server.....	9
Online vs. Offline Backup.....	9
Backup Job Types .....	10
Normal (Full).....	10
Copy .....	10
Incremental .....	10
Differential .....	10
Recommended Exchange Server Backup Process .....	10
Full Server Protection.....	11
Exchange Application Backup.....	11
6. Protecting User Mailboxes .....	12
Remote User Mailbox Protection.....	12
7. Recovering Exchange Servers .....	13
General Exchange Server Restore Requirements .....	13
Online Information Store Recovery to Original Exchange Server .....	14
Recovery to a Different Exchange Server Machine.....	14
8. Recovering User Mailboxes .....	15
Recovering Mailboxes from a Mailbox Backup .....	15
Restoring a Mailbox from an Offline Copy of the Information Store .....	16
Prepare the Recovery Machine .....	16
9. Conclusion .....	18
10. General Disaster Recovery Considerations .....	18

### Whom to contact

If you have questions regarding Backup Exec, please contact:

VERITAS® Software Corp.  
North American Sales Headquarters  
400 International Parkway  
Heathrow, FL 32746  
1-800-327-2232 (US and Canada)  
407-531-7501 (Outside the US)

## 1. Introduction

Messaging applications have become a ubiquitous communication tool 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. 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.

In order to maintain the Exchange system's availability and protect its data stores, a working, tested Data Protection plan is essential. A good data protection plan will help ensure the recovery of the Exchange system environment, user configuration data and/or message content in a timely fashion. The objective is to help minimize downtime for your enterprise messaging environment and to provide the quickest possible data recovery in the event of a system crash, database contamination, loss of a single mailbox, or other forms of data loss. For those of you who have worked through live data recovery events, such a time is not conducive to learning but a time for executing tried and trusted operating procedures and techniques.

This paper will discuss the Exchange data stores requiring protection and provide the information needed to design an Exchange Data Protection Strategy. The focus will be on those issues that must be taken into consideration when planning for an Exchange recovery and provide guidelines for implementing some of the more common data protection strategies. It was written for the administrator responsible for maintaining the messaging environment's availability and assumes the reader has a working knowledge of the Windows NT/2000 operating system and Microsoft Exchange Server administration practices. The paper also assumes that you are running Version 4.0 or (higher) of Windows NT/2000, Version 5.0 (or higher) of Microsoft Exchange Server and Version 7.3 (or higher) of VERITAS Backup Exec™ Agent for Microsoft Exchange.

## 2. Introduction to Microsoft Exchange Server

Microsoft Exchange is a client-server, Windows NT/2000 systems-level application that is designed to provide a high level of integrity for your messaging environment. In small companies this environment may consist of a single Exchange Server and a few Exchange or Outlook Clients all connected in a small LAN. In large scale corporate environments, multiple Exchange Servers will be deployed throughout the enterprise and work together to provide a seamless messaging system over LAN and WAN connections that are capable of supporting thousands of both local and remote users located around the world.

Exchange Server is a business critical messaging and collaboration application that major corporations depend on to enhance productivity and enable enterprise wide employee communications. With the introduction of Microsoft Exchange 5.5, it is rapidly becoming the platform of choice for business critical messaging needs. Since its introduction in 1996, Exchange has become the messaging standard in over 50% of Fortune 500 corporations. Exchange Version 5.5 builds on a proven foundation to add key features in the following major areas:

- **Improved Scalability**, unlimited storage capacity in the enterprise edition and native support for SMP enables hosting of thousands of users per server, while single-instance message store maximizes disk utilization.
- **Higher Performance**, native implementations of Internet standards such as MAPI, POP3 IMAP4 reduces the burden placed on the server while providing message delivery to a wide variety of mail clients.
- **Increased Availability and Reliability**, built-in clustering support and transaction-based updates to the data stores ensure that message delivery is reliable.
- **Enhanced Security**, tight integration with Windows NT/2000 logon and password expiration, coupled with support for the latest encryption standards mean your communications are secure when traveling over the Internet.
- **Improved Administration**, integration with the Windows NT/2000 directory and performance monitoring tools, teamed with least cost routing and remote administration services reduce your total cost of ownership.

Users have come to expect 7 day/24 hour availability of their messaging system; however, many organizations have inadequate Exchange maintenance and or disaster recovery capabilities in place. The combination of users' high expectations and the administrators' often interrupted driven work environment, has made comprehensive disaster

recovery plans more critical than ever. In order to protect the integrity and availability of the Exchange system some understanding of how the various components of the system operate is essential.

While this paper will not attempt to replace the need for new administrators to attend professional Microsoft Exchange administration classes, it will give a high level view of Exchange with a focus on how its operation and configuration influences data recovery. Due to the high degree of integration with the Windows NT/2000 operating system and the complex enterprise wide configurations possible in a large scale environment, an understanding of the system's basic operation is needed to define a plan that will best meet the needs of your organization.

### **3. Data Protection Considerations**

Before designing a specific data protection strategy for your environment, it is important to understand how your end-user client's interact with the Exchange environment and what level of protection you need to provide to each Exchange Server being protected. In addition, since Microsoft Exchange Server uses several Windows NT/2000 services and Windows NT/2000 Security for authentication, Windows NT/2000 operating system backup and restore must be tightly integrated with your Microsoft Exchange Server backup and restore strategy. You should also determine the service levels to be provided to users' individual mailboxes and who is responsible for providing that protection.

Remember that users expect the mail system to be there when they need it and quickly panic when they have lost this critical communications link. Panic turns to frustration or even anger when they are informed of extended outages and/or that some messages have been permanently lost. VERITAS provides a variety of products and options to help minimize your effort and reduce the level of complexity to a manageable level. We will reference these products throughout the paper in the context of where they would provide added value in the data backup and recovery process.

When planning an Exchange data protection strategy, there are several types of potential data loss or error conditions that need to be considered. The loss of an entire Exchange Server, data store loss or corruption, and the loss of a single client's mailbox store or messages. Our first priority is to protect the Exchange Servers as their loss will directly effect your messaging system's availability. When considering protection strategies for the server we have two primary concerns, the loss of the entire server and the loss or corruption of the Information Store. After ensuring the Exchange Servers are protected we must determine the level of protection offered to individual mailboxes. Considerations for each of these will be discussed in the following sections.

#### **Exchange Server Protection**

Exchange Server should be deployed on a dedicated Windows NT/2000 server whenever possible. The demands placed on the Windows NT/2000 system resources when providing messaging services to an organization are high and throughput will be highest when there are no conflicts with other applications' systems. In addition, the tight integration of Exchange and Windows NT/2000 may require that you rebuild your Windows NT/2000 server as part of the Exchange recovery process, which would require that you interrupt all applications running on the server while Exchange is being restored. By dedicating one or more servers to Exchange you will simplify the data protection process and enable more flexibility in your recovery options.

In large environments, it is common to find multiple Exchange Servers running as part of a single enterprise environment. In this situation, recovery in particular becomes more complex. While these scenarios are discussed in more detail throughout the paper, the following should be considered prior to designing your Exchange Data Protection Strategy.

- If dedicated servers are being used for Exchange Server, keep all server environments in sync by applying upgrades and maintenance for both Windows NT/2000 and Exchange Server to all servers in the production environment.
- Decide whether to provide a locally attached tape device to each server or share a tape library among multiple servers and then use the same equipment throughout your Exchange environment.
- Be sure to perform Windows NT/2000 Systems Backup policies on all Exchange Servers so you can recreate the Windows NT/2000 environment exactly when required. Do not rely on using 'similar' spare Windows NT/2000 system configurations as a backup system for production Exchange Server recovery. Windows NT/2000 Registry and Security information must be exactly the same as the server it was replacing in support of certain recovery situations.

## **Loss or Corruption of the Information Store**

While less severe than a full server loss, a recovery from loss or corruption of the Information Store is the most common form of recovery you will be performing in support of Exchange. By carefully planning a backup strategy to include frequent online backups of the Information Store and Exchange Directory Store, you will be able to rapidly restore both individual user mailboxes and the full Exchange Server information base more easily. Section five of this document discusses the various options available to you for protecting these databases without disrupting the end users access to the system.

The decision on whether to use full backup processes only or to use either Incremental or Differential backup techniques to augment your full backup (also referred to as "normal backup") routine is generally based on the following criteria. In small office environments with relatively small numbers of messages passing through the system, a nightly full backup either online or while Exchange is down will provide good data protection and the quickest recovery. If log file growth becomes an issue, consider using differential online backups at midday to provide an added recovery point and manage the log file growth for you automatically.

In large environments, the Incremental backup process should be used to provide more frequent recovery point options throughout the day and manage log file growth. Many shops run full backups on a weekly basis, preferring to run Incremental backups throughout the week to keep backup run time to a minimum. The trade-off with these techniques occurs at recovery time when you must not only recover from the full backup process but each and every Incremental backup process as well. What will work best for you will be based on the size of your environment, number of transactions processed each day and the expectations of your users when a recovery is required.

For fastest recoveries consider the following backup options in recovery priority sequence:

- Full Backups run as frequently as possible, no less than once a day.
- Full Backups daily with Differential Backups used at regular periods throughout the day, for example at lunchtime or every four hours.
- Full Backups every few days (no less than weekly) with frequent Incremental jobs in between each full backup.
- No matter which model you choose to follow, consider maintaining an Exchange Recovery Server that is kept up to date with the production servers and can be used to recover individual mailboxes or messages for those users who keep their mailbox data on the production Exchange Server.

## **Mailbox Level Protection**

First, think about how your users access the system. Do you allow client configurations to vary according to individual needs or have you standardized the majority of your client configurations? Does the server support a mobile user base or senior company executives who require additional levels of protection? Will the Exchange/Outlook Client be configured to move or copy messages to a Personal Message Store (PST) located on the client system? The client's PST may be placed on a server as a volume mapped in the user's file directory and be backed up by that server's backup job. Without a local PST, a client's messages are stored on the Exchange Server Information Store which centralizes mailbox level protection but places the burden of database management and protection on the administrator.

For mobile users the Exchange Client's offline mode is used to allow for periodic remote connection to the server, at which time the client will send outgoing mail and download copies of new messages to the Offline Message Store (OST) for reading at a convenient time without requiring server availability. While this provides great flexibility for the "road warrior," it may place the burden for individual mailbox protection on the end user, depending on whether the messages were moved or copied to the client's PST. When messages are 'moved' to the client machine, they are deleted from the Exchange Server's data store. If your clients are using an OST, then management is simplified because the OST is a 'snapshot' of your messages that are stored in the Information Store database, leaving the original messages intact on the server. These issues will be covered in more detail in section six, "Protecting User Mailboxes," and section eight, "Recovering User Mailboxes."

## **Critical Exchange Files**

Before looking at specific data protection strategies, a discussion of the key Exchange files will help to frame your understanding of the various processing options available to you. There are two main types of data stores to be backed up, user data and configuration data. Microsoft Exchange Server stores user message data in the Information Store

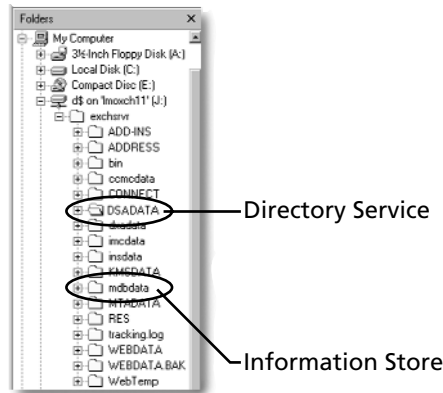
and one or more sets of transaction logs. The Information Store manages two databases, the Private and the Public Information Stores. The Private Store database is named PRIV.EDB and the Public Store is named PUB.EDB. For a client, Exchange message data and objects are either stored on the Exchange Server, a general purpose server or on the client's machine in a Personal Message Store (PST) or in an Offline Message Store (OST), while mail addresses are stored in the Personal Address Book (PAB).

Microsoft Exchange Server configuration data is stored in the Microsoft Exchange Directory (DIR.EDB), the Windows NT Registry, and in various subdirectories under the Microsoft Exchange Server installation path – and potentially paths created by running the Microsoft Exchange Performance Optimizer. The Public and Private Information Stores and the Directory Service on a Microsoft Exchange Server each have transaction logs reflecting the transactions directed at that database. These logs are used during the data recovery process for roll-forward operations after restoring Exchange files to the point of the last good backup.

Because transactions are cached in RAM and written to the log file prior to commitment in the database, the database files on a running Exchange server are always in an “in-flight” state. Therefore the most current state of a database consists of the data already committed to the EDB file and the transactions still residing in the server's cache prior to database commitment. If you lose a database and don't replay the transaction logs after a restore, you will have a database that is missing information even if a backup had been completed just prior to the outage. Your data protection plan must ensure that the database and its log files are always synchronized. The best way to do this is to allow Backup Exec™ to manage the log files for you. Section five of this document, “Backing up the Exchange Server,” will discuss log file management in more detail.

### Key Exchange Data Files

Transparent to the end-user, Microsoft Exchange Server maintains several database files or “stores.” These data points need to be considered in your procedures and are categorized below. We have used the default Exchange Server installation path of \exchsrvr; however, their exact location may be changed by the administrator.



**Directory Service Location**  
\exchsrvr\dsadata\DIR.EDB

**Information Store Locations**  
Private  
\exchsrvr\mdbdata\PRIV.EDB

Public  
\exchsrvr\mdbdata\PUB.EDB

### Client Database Files

Depending on how your Exchange Clients have been configured, there are several databases that may reside on the client system. The most critical is the PST and it should be backed up on a regular basis to ensure that client mailboxes can be recovered under certain circumstances. Client PST file data protection needs to be coordinated between the user and the administrator based on the type of client configuration in use. If all users are configured such that their messages are copied to the local PST, leaving the original message in the server's database, then protection is simplified as the Exchange Server's Information Store backup will also protect the client's mailboxes. If you support mobile clients or other users configured such that they have local PST files and download their messages using the move option, then the messages are deleted from the server Information Store after they have been downloaded. (Note: Deleted messages may still be recoverable in Exchange 5.5's deleted message archive, for the period of time specified by the administrator, after which they are purged from the system.) In this case the user's PST file must be backed up to ensure mailbox data loss is kept to a minimum. Responsibility for local PST backup must be considered as part of the Exchange Data Protection plan.

### **PST (Personal Message Store)**

If users store PST's on local drives, and local drives are not being backed up, you may be out of luck in the event that the PST becomes corrupted. If PST's are stored on file servers (i.e. home directories), be sure to include them in each file servers' backup routines. Recovery in this case is as simple as restoring the PST and adding the PST to an existing user profile. Make sure users realize that if they password protect his or her PST and then forget the password, there is no way to recover the password and therefore the data in the PST file. In the event a PST file becomes damaged, running the SCANPST program can usually repair it.

### **OST (Offline Message Store)**

The OST is used to support some remote client configurations. When the client logs on to Exchange, the system will synchronize the information in their account on the server with the client's OST. For example, new messages are downloaded and any messages in the client's "Send" folder will be uploaded to the server for delivery. OST data is at risk when changes have been made to the local OST and they have not yet been replicated up to the server-based store. Normally, the synchronization process is run at initial login to Exchange and optionally during the shutdown process. If a user machine crashes, a new OST can be created on the replacement machine and all server-based information can be sent down to the OST file via the Exchange synchronization process.

### **PAB (Personal Address Book)**

Personal Address Book files are used to store the users contact mail addresses for associates not included in the system wide Global Address List. The PAB can be stored in a file server directory or on their local drive. Since most file servers are backed up regularly, any server based PAB files can also be backed up. The risk of PAB data loss occurs when users store the PAB file locally and do not arrange for a backup. This can cost an employee many hours of work and lost productivity to replace the PAB entries. Ensure that a user's PAB is backed up by the user if it is not stored on a file server that is protecting these files for the user.

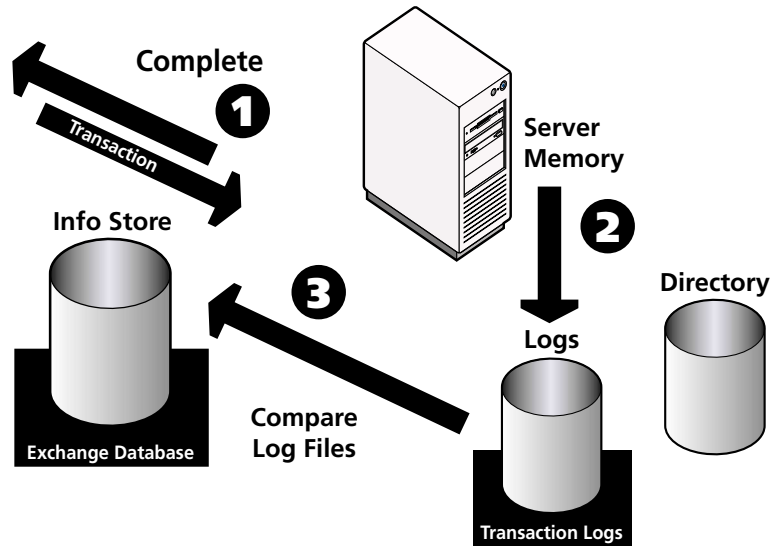
### **Using SCANPST.EXE to Repair PST and OST Files**

The SCANPST program, also known as the Inbox Repair Tool, will repair both PST and OST files. This tool is similar to the MMF check capability in MS Mail and is installed in the Microsoft Exchange client subdirectory by default. SCANPST will perform a variety of checks on the file selected. During repair, you have the option to backup the existing file prior to making the repair; however, this will require that you have up to 2x the available disk space of the PST or OST file size. Use this tool to try and correct a corrupted database prior to falling back to a complete restore of the file from a recent backup as some data may be lost if it was created after the last backup had been run.

### **Transaction Logging and the Exchange Database**

Microsoft Exchange database technology implements log files to accept, track and maintain the integrity of each Exchange transaction. All message transactions are written first to log files in memory. After this has been accomplished, the "transaction complete" signal is sent to the initiator of the request allowing that process to continue servicing other requests. However, in most cases, remember, the transaction has not been committed to the appropriate database. A background function in Exchange is responsible for managing the commission of transactions in memory to the respective database files and updating the checkpoint record to reflect the current state of the system and guide the transaction recovery process after a database restore.

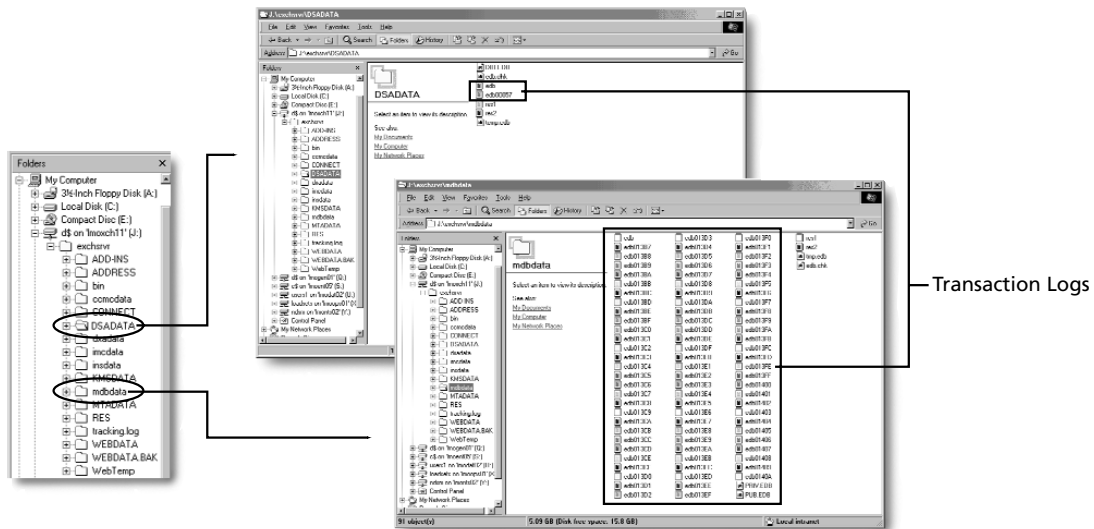
The two-phase commit process is used to provide maximum performance to clients using the system. During a recovery, if you have either backed up the logs or the logs are still intact, they can be used to recover message transaction data in the event that a hardware failure corrupts the Information Store or Directory Service database files. To help ensure recovery, it is best if log files are kept on a separate physical disk drive from the actual Information Store and Directory Service database files. If the database files are damaged, they can be restored and those transactions recorded in the logs can be "played" back to the restored file bringing the database back to its most current state.



## Directory Service and Information Store Control Files

### Transaction Logs

Transaction logs, by default, are stored in the following Exchange Server directories: Information Store logs are kept in \exchsrvr\mdbdata and Directory Service logs are in \exchsrvr\dsadata. Each subdirectory contains an EDB.LOG file that is the current transaction log file for the respective service. Both the Information Store subdirectory and the Directory Service subdirectory usually contain a separate set of .LOG files (unless circular logging, described below, is enabled). Log files are always allocated to be 5,242,880 bytes in size. If log files do not reflect this exact size, they are most likely damaged. Since transactions are first written to the EDB.LOG files and then later written to the actual database, the most current state of a database is a combination of the uncommitted transactions in the transaction log file and the records already written to the .EDB database file. When the EDB.LOG files are filled with transaction data, they are renamed and a new EDB.LOG file is created.



### Previously Committed Logs

EDB.LOG files are renamed and accumulate in the original subdirectory. The log files are named in a sequential numbering order, for example EDB00014.LOG, EDB00015.LOG, and so on using hexadecimal suffixes to form unique names. Backup Exec online backup processing purges previously committed log files at the completion of the backup process. Online mode, Normal (Full) Backup or Incremental Backup jobs will delete log files only if every transaction in the log has been committed. There may be several versions of previous logs with

uncommitted transactions during a backup and online backup processing will never purge these as they will be required during most forms of Exchange Server recovery.

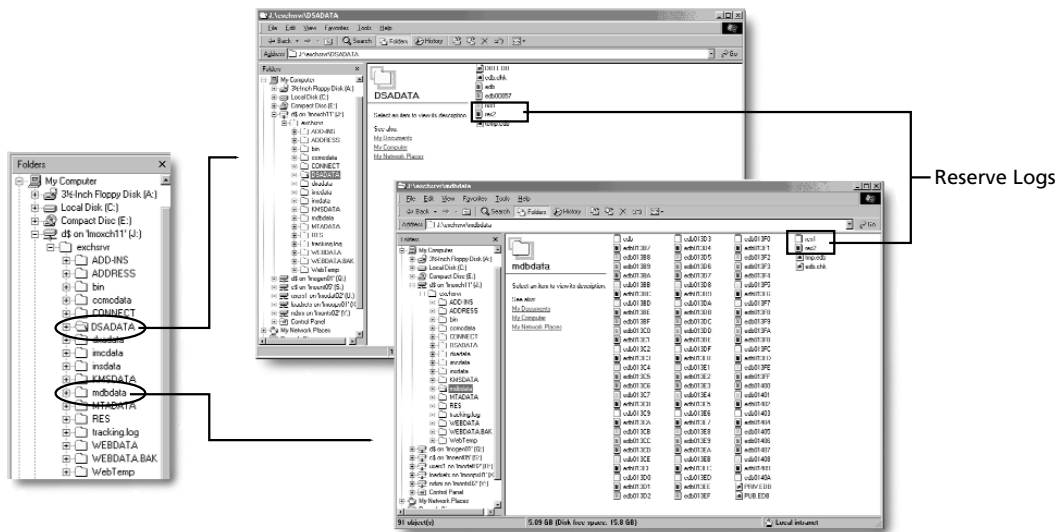
When Circular Logging is enabled, histories of Previous Logs are not maintained and therefore log files are not purged by any backup operation. For this reason, Incremental and Differential on-line backups, which only process log files, are not supported when Circular Logging is enabled. When Exchange's services are normally shut down, all transactions in the log files will be committed to the respective database file before the shutdown is completed. Log files should never be manually purged while Exchange services are running. It is best to allow the backup process to manage them and ensure the integrity of the Exchange System is maintained.

### “Checkpoints” And Checkpoint Files

A checkpoint (EDB.CHK is the file name) record is maintained to track the current transaction commit status within the Exchange System. In the background, when all transactions in the current checkpoint have been committed to disk, the checkpoint record will be updated and the next set of in-process transactions will be processed. It's very important to note that the log files, even though they have been committed to disk, are still needed for proper online backup processing. Never delete log files manually unless you are purposely resetting the state of Exchange to a previous, fixed point in time using offline backup and recovery processes. Checkpoint files are used for managing the recovery of transaction logs into their respective database files. The Information Store and the Directory Service maintain separate checkpoint files. Whenever a transaction is written to the database file from the transaction log, the checkpoint file is updated with information specifying which transaction was successfully committed. During recovery, Microsoft Exchange Server start-up determines which transactions have not yet been committed to the respective file by reading the checkpoint file or by reading the transaction log files directly. The Information Store and Directory Service read their checkpoint files during startup and any transactions that have not been committed are played into the database files from the log files.

### Reserved Logs

The Directory Service and Information Store services independently maintain two reserve files, RES1.LOG and RES2.LOG. These LOG files are normally empty and are rarely used. They are stored in the MBDATA and DSADATA directories. If the Directory Service and/or Information Store is in the process of renaming the EDB.LOG file and creating a new one and there is not enough disk space to create the new EDB.LOG file, then the reserve log files are used. This is a fail-safe mechanism that is only used in the event of an emergency. These files are used to store transactions that may be “in-flight” during a premature shutdown of Exchange when disk space for new logs is unavailable. When this occurs, an error will be sent to the respective service and the shutdown process will start. The service will flush any transactions in memory that have not yet been written to a transaction log into the RES1.LOG and, if necessary, the RES2.LOG. When this is completed, the respective Exchange service will shut down and record an abnormal termination event in the Windows NT/2000 event log.



### **Circular Logging Considerations**

Database Circular Logging is a mechanism that uses transaction log technology but does not maintain a series of transaction log files. Instead, a fixed number of log files are maintained and eventually overwritten as the available log space is fully utilized. When transactions in log files have been committed to the database, the existing log files are reused and this process destroys old transaction records. Circular logging is enabled by default and the settings can be changed from the Microsoft Exchange administrator program. Once a change is made, you must restart the affected Exchange service (database). VERITAS recommends turning off the circular-logging feature to provide the most flexibility during a recovery.

When Circular Logging is not enabled, log files will accumulate until an on-line Normal (Full) or Incremental backup is performed. Therefore the advantage of enabling circular logging is that it helps to manage disk space and prevents the build up of additional transaction log files. The drawback is that in high transaction environments log files may be overwritten in between backup operations reducing the options an administrator has during a subsequent recovery. When a recovery is performed after the log records have been over written, some loss of transactions will likely occur as the Exchange System will not be able to recover those records.

### **Review of Key Planning Items**

- What service level commitment is in place regarding message system availability?
- What is the time and duration of regularly scheduled Exchange Server maintenance?
- Will you be incorporating Exchange Data Protection with the Windows NT/2000 Server protection processes?
- Are all key Exchange files being protected and do you have a recovery plan for each one?
- Will you be using the Database Circular Logging feature?
- Do you need to support user mailbox backup and recovery?
- Do you need to support mobile users localized personal information stores?

## **4. Exchange Data Protection Tools**

### **Microsoft Windows NT/2000 Backup**

An enhanced version of the Windows NT/2000 NTBACKUP.EXE program ships with Microsoft Exchange Server. This integrated backup solution, provided by VERITAS, is included as a built-in component of Microsoft's BackOffice business applications. Because of this integrated backup solution, Microsoft Exchange Server and the new NTBACKUP.EXE provide live, online backup of the Microsoft Exchange Information Store and Directory Service without interruption to the messaging system. NTBACKUP.EXE also provides file-based backup services and will back up the Windows NT/2000 registry.

### **Backup Exec for Windows NT/2000**

Backup Exec for Windows NT/2000 (BENT) is a high performance, complete data management solution for Windows NT/2000 networks. BENT offers a 32-bit client /server design to provide fast, reliable backup and restore capabilities for servers and workstations across a network. In addition, you may add a robust set of optional features to the base product that add advanced capabilities to your data management arsenal. Autoloader and Fibre Channel device support, Windows NT/2000 server disaster recovery and agents for network operating platforms, as well as Windows NT/2000 applications are examples of optional components.

The VERITAS Backup Exec family is part of an integrated solution designed to cover all your data management needs. When used to protect Exchange Application Servers, Backup Exec provides a system that is fully integrated with both Windows NT/2000 and the Exchange application to ensure that you are providing the most complete protection available, now and in the future. Backup Exec uses Microsoft developed APIs and technology extensively so you can be assured that your data protection strategy will be able to support Exchange Server's future enhancements.

### **Microsoft Exchange Agent for Backup Exec for Windows NT/2000**

The VERITAS Backup Exec Agent for Microsoft Exchange Server integrates Exchange Server data protection into network backup routines. The on-line support allows users to protect Exchange Servers while active. The entire Information Store (IS), Directory Service (DS), Message Transfer Agent (MTA), and System Attendant remain in service

during on-line backup. The agent also supports mailbox or 'bricked' backup to enable individual mailbox protection.

Advantages of using the mailbox support over competitive solutions include: higher performance; complete mail attachment protection, including embedded messages and objects; restoration of the original mailbox and message attributes; and complete recovery of important options such as Outlook flags, internet headers, tracking options, and message flags.

**Exchange Cluster Support** – Version 7.3 (or higher) of Backup Exec for Windows NT/2000 provides the capability to backup and restore Microsoft Exchange Cluster Server properly. All backup and restore jobs must target the virtual server, and each node in the cluster needs a license of the Microsoft Exchange Agent for Backup Exec for Windows NT/2000 as well as a license of the Agent Accelerator for Windows NT/2000.

In addition, users can backup all network and Exchange Servers to the same media, reducing the costs of having dedicated media for Exchange Server backup. The Backup Exec Exchange Agent allows users to completely protect their Exchange Server, including all Windows NT/2000 shares. Data restores can be redirected to any Exchange Server on the network and the Exchange Agent uses Backup Exec's extensive alerts.

### **Intelligent Disaster Recovery™ Option for Windows NT/2000**

The perfect compliment to backup and restore, Intelligent Disaster Recovery™ (IDR) from VERITAS works in conjunction with Backup Exec for Windows NT/2000 to provide complete protection for the Windows NT/2000 Server hosting your Exchange application. While traditional backup is great at protecting application data and your Windows NT/2000 file system from loss, it is not always able to provide the fastest most complete method of recovering a lost Windows NT/2000 server. Before Backup Exec can recover data, you must have an operational Windows NT/2000 system. Intelligent Disaster Recovery Option provides a valuable alternative to manual Windows NT/2000 system recovery procedures.

IDR provides a simple, automated process for preparing for and executing a full local or remote Windows NT/2000 server recovery that reduces the time, cost and risk associated with manual efforts. IDR can quickly perform the task of rebuilding a server with the identical configuration of the operating system, user profiles, and maintenance updates as was present on the original lost server. And because it is fully integrated with Backup Exec, IDR can trigger the recovery of your application specific data right to the point of the last full or Incremental backup run. When used as part of your Exchange data protection plan, IDR will protect the closely coupled inter-relationship between Exchange Server and the underlying Windows NT/2000 Server operating platform.

## **5. Backing up the Exchange Server**

There are two basic backup methods that can be used to protect your Exchange Server online and offline. Online Backup uses Exchange API's to protect key data files while Exchange is running and available to users. Offline Backup refers to protecting the system after Exchange Services have been shutdown.

### **Online vs. Offline Backup**

Microsoft Exchange Server "Offline" backup is a file-based backup scheme requiring the Exchange services to be stopped. You simply run the NTBACKUP program supplied with Windows NT/2000 or Backup Exec program to backup all Exchange files on the Exchange Server. The main limitation to "Offline" backup is that the Exchange service is interrupted for end-users and you can't perform Incremental or Differential backups. The best time to use the offline Full backup process is when you wish to snap-shot the entire Windows NT/2000 Exchange Server such as before moving to a new release level of either the Windows NT/2000 operating system or Exchange itself. Be sure to include all drives and directories when performing a full offline backup on a server. A convenient feature of Microsoft Exchange Server is the ability to backup databases without interrupting service to end-users. Microsoft Exchange Server "Online" backup requires that all Microsoft Exchange Core Services remain running. During the Full or Copy backup operation, data is read from the .EDB files. If a transaction is made to a part of the .EDB file that has already been backed up, it is recorded in a .PAT (patch) file. If a transaction is made to a part of the .EDB file that has not yet been backed up, it is simply processed as usual and does not need to be written to the patch file. A separate .PAT file is used for each Exchange database, PRIV.PAT, PUB.PAT, and DIR.PAT. These .PAT files will only be present during the online backup process, as Exchange dynamically creates them at the start of the backup process. If some large transactions are in progress, the Exchange "Online" backup process creates a TEMP log file to store these transactions.

Whether you are performing an “Offline” or “Online” backup, you have the option to include the Windows NT/2000 registry in the backup job. You should always select this option and back up your entire Exchange Directory Tree to help ensure a successful recovery in a wide variety of data loss situations.

### **Backup Job Types**

#### **Normal (Full) – Processes both Database & Logs** (Flushes fully committed log files)

Any subsequent Incremental and Differential backup jobs are given their context as a result of the transaction logs being purged. Making a Full backup of one or more Microsoft Exchange Server results in backing up the entire Information Store and/or Directory Service databases as well as their associated transaction logs. Once the databases and transaction logs are backed up, the committed transaction logs are deleted. Full backup jobs should be run on a regularly scheduled basis, such as weekly.

#### **Copy – Processes Databases & Logs** (Does not flush log files)

The Copy backup method is similar to the full backup except that the transaction logs are not flushed after being backed up. Leaving the logs intact means that there is no context marking for subsequent Incremental or Differential backup runs. It is used to snap-shot the databases at a given point in time without impacting other backup routines. Use the Copy method to make a complete backup of the Microsoft Exchange Server without disturbing the state of ongoing Incremental or Differential backups. Copy backups are rarely used with Exchange, but may be useful as an emergency backup of Exchange that will not impact your normal backup schedules. Copy backups should be run with Exchange offline in order to ensure a fixed point in time recovery of the system.

#### **Incremental – Processes Logs Only** (Flushes fully committed logs)

Backing up one or more Microsoft Exchange Server using the Incremental backup method backs up only the transaction logs associated with each Exchange database selected. The Incremental backup process does not backup the Exchange databases themselves and runs in much less time than a full backup operation. Only new transactions written to the log files since the last Full backup or last Incremental backup are processed. The committed .LOG files are then purged from disk, setting the context for the next backup job.

Incremental backups are used to backup the Exchange System in between the full backup jobs. Incremental backups should be run frequently to provide granularity at recovery time and at least on a nightly basis. It is recommended that you do not let too much time elapse between Full Backups when using the Incremental process as excessive recovery times will result. In a recovery, you will need to restore your last Full Backup file set and restore each Incremental file set before the restore process is complete.

Note that an Incremental backup cannot be performed when circular logging is enabled.

#### **Differential – Processes Logs Only**

Like the Incremental, this backup type copies the log files associated with the Information Store and/or Directory Service since the last Full (Normal) backup was performed and leaves all log files intact. Note: You shouldn't mix Differential and Incremental backups inbetween Full Backup runs. Use one or the other in conjunction with the full backup process to create a complete backup cycle for Exchange. The primary trade-off between these two backup types is the time frames required for both backup and recovery. The Differential Backup run will increase over time as Exchange creates more log files. However, in a recovery, you will only need to restore from your last full backup tape set and the last Differential tape set.

Your Exchange Backup cycle should begin with a Full Backup and use multiple Incremental or Differential Backup runs to collect new and changed data in between Full Backup jobs. For example, run full backups every Weekend and Incremental or Differential backups on Monday through Friday.

Note that a Differential backup cannot be performed when circular logging is enabled.

### **Recommended Exchange Server Backup Process**

Two backup methodologies are required to ensure complete protection of the Exchange environment. The first is used to protect the entire operating platform in the event of a hardware failure or natural disaster that requires the emergency recovery of the whole server. The offline full backup method will be used to protect your Windows NT/2000 operating environment and should be rerun after major modifications are made to the Windows NT/2000 system. The second method is designed to protect your Exchange application data and will be used to provide for the recovery of the Exchange Information Store, Directory Service and selected user's mailbox data.

## Full Server Protection

Recovering a Windows NT/2000 Exchange Server from bare hardware is a time consuming and exacting process. Before you can recover Exchange's custom configuration settings, application-related executables and the application data itself, you must have an exact version of the Windows NT/2000 system up and running. Due to the variables and potential for an extended outage when something goes wrong, we suggest using the Intelligent Disaster Recovery Option for Windows NT/2000 to automate most of the process, including the ability to restore the application specific data files right up to the point of your last backup.

Used in conjunction with a full offline backup of the Windows NT/2000 Server, IDR's wizard allows the emergency recovery process to be consistently applied to one or more lost Exchange Servers. Complete instructions are provided for creating the emergency restore diskettes in the Backup Exec for Windows NT/2000 administrator's Guide. This type of severe outage is often handled differently so we will not go into detail on how to recover the Windows NT/2000 Server in this paper. In many shops, standby servers are ready to be deployed for each major operating platform being used to support mission critical applications in the network.

Remember, regardless of your specific procedure for performing a bare metal recovery, you will need a complete full backup of each Exchange Server to complete your Exchange recovery. Specify a full backup for this job, selecting the root directory of each local drive and check the backup Windows NT/2000 Registry Option. You do not need to include the Exchange Information Stores or Directory Service files as they will be protected using an online backup. Even though the Information Store and Directory Service can be backed up on-line, files in directories being accessed by other Microsoft Exchange Servers for Windows NT/2000 services, such as the DXA or PCMTA services, should be backed up in offline mode when the respective services are stopped.

## Exchange Application Backup

The Exchange Agent allows you to run online backups to protect the application from the more common forms of data loss. This process can be run more frequently to provide greater levels of granularity during a recovery due to the fact that Exchange Services are not interrupted to the users. It is a good idea, however, to run your application backups at a time of day when user activity is the lowest. For this process, there are two Exchange databases to be backed up in each job type: the Information Store and the Directory Store.

After installing the Exchange Agent you will be able to view icons for the Exchange Servers running in your network from your Backup Server. You can select the icons for the Information Store and Directory databases by opening the Backup Exec "Backup Selection Tab." Select Backup on the toolbar and verify that the default backup options are correct. To change the defaults, go to the General and Advanced backup tabs and make any required changes. See the Backup Exec Administrator's Guide for more details.

Once you have set up the job, you can run it immediately, schedule the execution at a future date and time or save the definition you created for usage in the future. If individual mailboxes are selected as part of an Exchange backup, you will only be able to select the full backup method from the Backup Options Tab in Backup Exec. For this reason, it is recommended to run individual mailbox backups as a separate job (see section six for more details). You will need to set up a job for each type of backup you wish to run and schedule them appropriately. For example:

Backup Type	SUN	MON	TUE	WED	THU	FRI	SAT
Full	X			X			NONE
Incr/Differential		X	X		X	X	NONE

In general, the duration between full backup runs when using Incremental jobs in between can be longer than when using the Differential backup type. This is due to the longer run times experienced for the differential. In all cases, your file selection criteria should be the same as when you built the full backup job. If backup run times are not an issue, the fastest recovery will be provided by running a full backup every night. Also note that in addition to selecting the Information Store and Directory databases, you should include the Windows NT/2000 Registry and the security files located in directory \EXCHSRV\SECURITY.

## 6. Protecting Individual User Folders and Mailboxes

With Backup Exec 7.2 (and higher) and the enhanced version of the Exchange Agent installed, administrators have two options for protecting centrally managed folders and mailboxes. In essence, the procedures created for protecting the server will also backup the mailbox data as it is contained in the Exchange Information Store. However, administrators also have the option of backing up individual mailboxes or folders within a mailbox separately, which makes recovery a much easier process. Backup Exec's Backup Selection Tab will include a "Microsoft Exchange Mailboxes" icon for each Exchange Server on the network. If desired, this icon can be expanded to allow the selection of any number of mailboxes and/or one or more folders within a mailbox, for inclusion in the backup job. Once you have completed mailbox selection, select backup job options such as target device settings and schedule the job.

**Exchange Mailbox Server-Centric View** – This feature, available only in version 7.3 of Backup Exec, makes it possible to change the view of the Exchange mailboxes to allow the user to select either a Site view or Server view of their mailboxes. When you select to use the Server view, only mailboxes that belong to the selected server will be displayed under the Microsoft Exchange Mailboxes share of the server in the backup selection window. Using a server-centric view allows a user to configure mailbox backup and restore easier.

Mailbox selection can be added to your server protection jobs, but it is important to note that mailbox level support will significantly slow down the backup process due to the requirement that Exchange Server 'walk through' each mailbox to copy the data out of the Information Store. Note: Backing up either the Information Store database or all individual mailboxes will provide a complete backup of Exchange mailbox data. However, the latter is not a recommended option for large accounts as the process used for mailbox backup is much slower and does not support Incremental backup processing. In addition a backup of every mailbox will not process certain configuration information or support a full Exchange Server recovery. A good practice is to set up a separate job solely for mailbox level protection and then select only those mailboxes that require the fastest level of recovery available, such as key executives.

Note: If individual mailboxes are selected, only the full backup type will be allowed by Backup Exec. Do not allow individual mailbox jobs to run at the same time as your Online Exchange Server backup jobs or severe performance degradation will result.

Before you can select mailboxes or folders for backup, a mailbox profile must exist that the Backup Exec service account can use to access the Exchange Server on which the mailboxes reside. The preferred Windows NT/2000 account for that mailbox must be the Backup Exec service account. The profile describes the mail services you need to access and the Messaging Application Programming Interface (MAPI) providers that enable access to those specific mail services. You may set up permission using the Exchange Administrator function to allow the Backup Exec Profile to backup all mailboxes on the Exchange Server by editing the Exchange Server Properties Tab. Another option is to set up Exchange Mailbox backup permissions only for the individual user mailboxes to be backed up. For complete instruction of setting up these profiles refer to the Backup Exec Administrators Guide and the Microsoft Exchange Agent section.

### Individual Message Restore

No matter how many administrative safeguards are put in place, the accidental deletion of important messages by a user is inevitable. The restoration of a single message from backup set would be a great benefit to today's administrators. However, companies today need to preserve the security of sensitive data and therefore must manage who has access to this important information. Still, from time to time, the need to restore a single message arises.

Administrators can temporarily restore a second "Inbox" folder to a given mailbox, and allow the user to retrieve the lost message from the previously protected folder. To perform this operation, the user's mailbox must have been previously backed up individually. Then, simply restore the user's "inbox" folder taking care to uniquely rename the folder so as not to affect the users current "Inbox" folder. Since the renamed folder will not exist in the destination mailbox, the uniquely named folder will be created. The user will now see a second folder where they may retrieve the lost message. Once the message is retrieved to the user's "Inbox", the secondary "inbox" folder should be deleted.

### Remote User Mailbox Protection

For your mobile users who elect to have mail delivered to a PST stored on their local hard drive, other considerations are needed to preserve the mailbox information. The full server and mailbox backup processes discussed above will not protect these users' PST data. As discussed earlier, a local PST with the "move mail" delivery option enabled

relocates mail to the client and deletes the messages from the Exchange Server's Information Store. In this configuration you and the user have several options for protecting their mailbox.

- Change their message delivery mode to 'copy' from 'move'- this option allows Exchange Server to retain a copy of the delivered message, in addition to sending a copy on to the local PST. This option allows the administrator to provide a minimum level of protection. The accuracy of Server Level backups for this user's information will be limited to the time of the last 'synchronization' process between the local client and the server. Any outgoing mail waiting to be delivered or changes to the user's Personal Address Book (PAB) will not be protected.
- Change their client configuration to use an OST instead of a local PST. This option is very similar to a configuration where the PST is setup to use the 'copy message' option as described above. The last 'synchronization' process between the local client and the server will limit the accuracy of the Server Level backups. Any outgoing mail waiting to be delivered or changes to the user's Personal Address Book (PAB) will not be protected.
- Move the PST to a file server volume mapped as a drive to the clients local system. This option will suffice for a user who is on the network most of the time and not subject to extended periods of remote usage such as the sales person who downloads mail before leaving on a trip. In this case, client PST data can be protected as part of the file server's regular backup protection schedule.
- Provide a local backup procedure for the user to protect their mailbox PST. Windows 95, 98 and Windows NT/2000 have backup programs that come with the system and can be used to protect the PST after the Exchange or Outlook Client has been completely shutdown. An alternative to local backup is to have the user simply copy the PST to a file server before disconnecting from the network and after shutting down their Exchange Client.
- An additional option available for local client Exchange data protection is the usage of a centralized, client data protection solution such as VERITAS' Telebackup. Telebackup employs dedicated servers and intelligent data reduction technology to fully protect the desktop environments in your enterprise. Telebackup can be used to protect local PST files; however, due to restrictions in the Windows operating system and the dynamic nature of Exchange, users will have to shutdown the Exchange Client during the backup.

## 7. Recovering Exchange Servers

There are several different Exchange Server restore scenarios to be considered. The correct restore process depends on the type of problem you are trying to recover from. Have you suffered some form of loss or contamination in the Information Store, or have you lost the Exchange Server or an attached hard drive? You must also consider the type of backup operation you used, whether it was online or offline. We will review the various processes and detail some additional considerations that you must be aware of in several cases. NOTE: Your best defense is periodic testing of the various recovery plans you have designed. You will learn how to anticipate and solve problems caused by your own unique set of environment and configuration variables. The following should only be used as a planning guide. Do not wait for an outage to 'test' your recovery plans.

### General Exchange Server Restore Requirements

- Before starting restore operations, the Microsoft Exchange System Attendant (SA) service must be running on the computer to which you are restoring Exchange information.
- You must be in the local administrator's group on every Exchange Server that you are restoring the Information Store and Directory Store Databases.
- If you are redirecting the restore of Exchange Server components to different Microsoft Windows NT/2000 machines, the Microsoft Exchange System Attendant must be running on each target computer.
- Restores of the Microsoft Exchange Directory to an Exchange Server other than the original are not supported Only Information Store data can be restored to a different computer. In most cases, the directory will be rebuilt as part of the Exchange start-up process.

## **Online Information Store Recovery to Original Exchange Server**

This is the simplest form of Exchange Server Recovery to execute. To perform this recovery, you will need to restore the Information Store and Directory from your online backup runs. Remember to start with your most recent full backup file set and continue to restore each Incremental file set in the order in which they were created. If you used the Differential backup type, then simply restore the last Differential backup file set after completing the full backup restore operation. Once the restores have completed, restart the Exchange Services using the sequence specified at the end of section below.

## **Recovery to a Different Exchange Server Machine**

This section discusses issues with restoring a Microsoft Exchange Server to a different physical machine, such as when the old machine was lost or when you wish to migrate Exchange to a more powerful server. Note that this is a special case since Microsoft Windows NT/2000 is reinstalled and a new Registry is created. This will require that a new Windows NT/2000 S.I.D. (security identifier) be created for the recovery machine in the domain as outlined below. Keep in mind that if only a hard drive was lost and replaced in the same machine, the Windows NT/2000 Registry can be restored from a backup (as it will still be the same physical machine) and a new S.I.D. should not be created.

There are a number of situations where it may be necessary to do a full restore of the Exchange Server Databases. Depending on your environment it may be necessary to restore the Windows NT/2000 SAM database. Microsoft Exchange automatically adds two accounts upon initial installation of the software: the Windows NT service account and the Windows NT/2000 account that was logged on during the installation. While both these accounts receive special privileges during installation, only the Windows NT/2000 account S.I.D. that was originally used to install Exchange is needed to restore the Exchange Directory Service. The Exchange Directory Service will not be accessible unless this S.I.D. exists in the Windows NT/2000 environment.

Note: If for any reason there are no Domain Controllers of the original domain available, it is necessary to restore the Windows NT/2000 Primary Domain Controller SAM.

- You will need the following to perform the recovery operation:
- A full backup of the Information Store and Directory.
- Replacement PC with, at least, the same hardware level and capacity as the original production server.
- Access to the original Windows NT/2000 SAM (Security Accounts Manager).
- Microsoft Exchange Installation Code.
- Windows NT/2000 Server and Windows NT/2000 Service Pack installation codes.
- Microsoft Exchange Server Production Server configuration sheet.

A full server recovery is defined as the ability to restore an original production Microsoft Exchange server such that all Windows NT/2000 security and configuration information, as well as Microsoft Exchange configuration and data are recovered. This will allow users to log on to their mailbox accounts upon re-deployment using their current passwords. The full server recovery requires both the IS and DS to be restored. Remember that Microsoft Exchange uses Windows NT account S.I.D. information in object properties within the Exchange Directory, so there are two key conditions for a successful Directory Service restore.

- The DS must be restored to a Windows NT/2000 machine with the same Site, Organization AND Server name as the original production server.
- The recovery server must belong to the domain in which the original Microsoft Exchange Server was installed.

A full server disaster recovery involves three machines. Two of these will already be in production and the third is the targeted Exchange recovery machine. One required machine is the Primary Domain Controller and the other is a Backup Domain Controller that may also be one or more existing Exchange Servers. Note: whenever possible, Exchange Servers should not be used as PDC's.

The reason for requiring a PDC and BDC to re-create the Exchange Server is due to the way Exchange uses the Windows NT/2000 Security Accounts Manager (SAM) database to provide authentication to directory objects. Let's say, for example, there is one Microsoft Exchange Server in a site and this server also acts as a PDC. Nightly backups are

being performed and the server crashes needing to be replaced. A hot backup PDC with Microsoft Exchange can be built from scratch and you can restore all Exchange IS and DS files. When Exchange is started, it expects all security properties in Directory Objects to match the Windows NT/2000 SAM for the user accounts. Since the machine was rebuilt as a PDC, a new Windows NT/2000 SAM was created. The restored Exchange Directory will not match up with the SAM objects and you will not be able to start Exchange or access the administrator program.

A better alternative is to dedicate a PDC and use one or more Exchange Servers as a BDC. When you lose the production Exchange Server, rebuild a Windows NT/2000 domain controller on the recovery server using the same name as the crashed Exchange Server. Be sure to install all the same service packs as was on the original server. When this machine is connected to the domain as a BDC, the PDC provides it with a copy of the SAM from the domain in which the production Exchange Server resided. Remember to first delete the old computer name – BDC definition – from the PDC and then add it again during the BDC install using the Server Manager. Each machine gets a unique S.I.D. when added to a domain and a new one will be assigned to the recovery machine.

Then install Microsoft Exchange Server using the same Site and Organization Name, allowing Exchange to create the Microsoft Exchange Server name using this information with the new machine name. If you are recovering a server and joining an existing site during the re-installation, refer to the Microsoft Exchange Administration guide for more details. After this, restore the Information Store and Directory from the last set of production server backups server and restart the system. When restarting the system, it is best to restart services from the server command line and wait for each service to complete before starting the next one. The proper sequence for service restart is as follows:

- Start Microsoft Exchange System Attendant
- Start the Directory Service
- Start the Information Store Service
- Start the Message Transfer Agent and then your connection managers in any order.

## 8. Recovering User Mailboxes

There are several options available to you for recovering an individual user mailbox. Once again, your options will be limited by the client configuration used or the type of backup you will be using for the recovery. As stated earlier, if your user is having mail delivered to a PST stored on their client system, then they are responsible for the recovery. They can restore the PST and PAB, if needed, from a local backup or a file server backup if they stored the PST on a mapped server drive. If they did not perform any local backups and no file server backups are available, their data is lost.

If their client configuration keeps messages and other objects in the Exchange Server Information Store, then you have one of two options. Recover the mailbox from an offline restored version of the IS or recover their mailbox from a mailbox backup, assuming their mailbox was individually selected for back up in a Backup Exec Job. While the individual mailbox backup and recovery is very useful for key executives, the performance associated with the backup process does not make it practical for protecting large numbers of users in this manner. See section six for more information.

### Recovering Mailboxes from a Mailbox Backup

This is the easiest recovery of all and Backup Exec allows you to select entire mailboxes and/or one or more specific folders of a mailbox. Due to current MAPI restrictions, individual messages in folders cannot be individually selected for a restore. When messages in folders being restored to an existing mailbox location and a message with the same name already exists, then the restored message does not replace the existing message, it is added to the target folder. Therefore after a mailbox or folder restore, let your users know that duplicate messages may exist in their mailbox.

To perform a mailbox restore, expand the Exchange Server's directory display in the Backup Exec restore options dialog box, file selection tab, just as you did when selecting the mailboxes for backup within the backup dialog. The Exchange Server hosting the mailbox should be up and running and you should have the appropriate access as already described. You may also redirect one or more folders or an entire mailbox to another mailbox, provided the destination mailbox already exists and it has an associated user account profile. When the restore completes, the recovered mailbox/folders will have been added to the existing mailbox structure, rather than the target mailbox.

As stated, mailbox level backup and recovery is not practical for protecting large numbers of users, nor should it be considered a replacement for the aforementioned server level protection strategies. An alternative to mailbox level restore is the ability to restore individual user mailboxes from the server level Information Store backups you are performing as part of your overall Exchange Server protection strategy.

### **Restoring a Mailbox from an Offline Copy of the Information Store**

In the event that a single mailbox, not protected by the individual mailbox backup process, needs to be recovered, you can still recover a mailbox for the user. This might be necessary due to accidental deletion of an entire mailbox or a portion of the data stored within the user's mailbox, such as a folder or message. In these cases, you can still recover the data for the user from a full Information Store backup. The procedure used will be the same for any Exchange Server's mailbox recovery, regardless of the production Exchange Servers name. In a centrally managed organization, it is a good idea to have an 'offline' Exchange Server standing by for this purpose.

**Caution:** Please note that this process should NOT be performed on an Exchange Server that is in the production environment. As noted below, the procedure calls for restoring the IS database to a standby Exchange Server that is installed using the same Site and Organization name as the production site. Be sure to create a new site with these parameters and do not select 'Join an Existing Site' when performing setup.

For this procedure, you must restore the entire Information Store and then retrieve data from the desired mailbox and deliver the PST to the user in question. In short, prepare an Exchange Server running Windows NT/2000 Server and install Exchange with the same Site and Organization name as the production server that contained the mailbox to be recovered. Then restore the Information Store from a backup tape, logon with Exchange administrator privileges and assign the Windows NT/2000 administrators ID access to the desired mailbox. Restore mailbox data to a PST file and attach the PST to the desired user profile.

The following are required for this process:

- A dedicated server with enough capacity to restore the entire Information Store database.
- A recent backup of the Private Information Store database.
- Microsoft Exchange Client and Exchange Server installation codes.
- Windows NT/2000 and the appropriate Windows NT/2000 Service Pack installation codes.

### **Prepare the Recovery Machine**

Prepare a non-production recovery server. A good idea is to have this machine running and available at all times with the correct levels of Windows NT/2000 already installed to match your production environment. The machine can be installed as a Windows NT/2000 BDC or member server. Make sure there is adequate disk space for the IS to be restored and that you have a tape drive attached that is compatible with your production environment.

Create a New Exchange Site (do not Join an Existing Site). The machine should be a stand-alone server and not be joined to your production Exchange environment. Remember, you are using the same site and organization name and your production environment will be compromised if you join the existing site. Logon to Windows NT/2000 as the administrator and install Microsoft Exchange using the same Site and Organization name as the production server you will be restoring. The server name of the recovery machine does not matter for this procedure, as the server itself will not be put into production.

Install the Microsoft Exchange Client on the recovery server and start Backup Exec. This procedure assumes a tape from an online backup is being used for the restore. If an offline backup tape is to be used, do not direct Backup Exec to start the Exchange Services following the restore. After the restore completes, start the Exchange Directory Service, execute the command "isinteg-patch", and then start the IS Service. Start these services one at a time allowing each to complete before starting the next one.

Note: it is best to start these services from the Windows NT/2000 command line, as you will have a better indication of progress than if using the Exchange Administrator user interface. It may take 20 minutes or more for the Directory Service to complete its startup.

•Perform the following steps:

- Make sure the Exchange System Attendant is running.
- Insert the appropriate Backup Tape in the drive.
- Logon to the recovery domain as the administrator.
- Start Backup Exec and catalog the tape in your drive.
- Go to the Restore Dialog and on the Restore Information screen select Entire Network and then the Server name of the Exchange Server being restored.
- Select the correct ORG\SITE\SERVER\Information Store Icon and run the restore.

After the restore completes:

- Logon to the recovery server using the Windows NT/2000 Administrator ID.
- Run the Exchange Administrator program.
- Run the DS/IS Consistency Adjustment.
- Select the Exchange recipient's container and double click on the desired mailbox name.
- From the mailbox's General Tab, select the Primary Windows NT/2000 Account button.
- Select the option 'Existing Windows NT/2000 Account' and click okay.
- From the 'Add User or Group' screen, select Administrator and click add.
- Select okay on the User Property screen.
- From the Exchange Client program group, run Microsoft Exchange Services and configure a profile for the desired user.
- Add a personal folder to that profile.
- Run the Microsoft Exchange Client.
- Highlight the "Mailbox UserName" on the left panel and select the first folder or item in the list on the right.
- From the pull down menu select: Edit; Select All and then File; Copy.
- In the copy screen highlight the Personal Folder and select okay. All data will be copied to the PST File.
- Copy the PST to the destination location on the production Exchange Server.
- Add the PST to the User's Profile on the Production Server and notify the user the mailbox is restored.

Be sure to test this procedure on a regular basis, particularly after you have modified the recovery server configuration to match any changes to Windows NT/2000 or Microsoft Exchange in the production environment. Also, you can perform this process with a server online to the production servers because the server name does not need to match the name of the Production Exchange Server being restored. That match is only required when you are performing a Full Server recovery to replace a failed server in production. Be certain, however, that the recovery server is NOT performing DS Replication with the production Exchange Servers as serious Directory Service problems will effect your entire production Exchange environment.

## 9. Conclusion

Exchange Data Protection is a critical aspect of maintaining a healthy messaging environment for your users. While the number of configuration and deployment options tend to complicate the administrator's responsibilities, planning data protection as part of your Exchange implementation rollout will greatly simplify your ability to maintain a highly available Exchange environment for your users. In large enterprises with multiple Exchange Servers working together over a WAN, be sure that each local administrator understands their responsibility and the impact a faulty server recovery can have on the entire environment.

Perhaps even more important than early planning is the need to run frequent tests of each recovery scenario you have documented. This is the only way to be sure you have the ability to rapidly restore service after an unexpected outage. Be sure to test and simulate Exchange Server Information and Directory Store data loss, the loss of an entire Exchange Server, and the loss of an entire site, when more than one Exchange Servers may be effected. Be creative when testing and pick a random administrator not normally involved in Exchange to follow your documented procedures. You will learn a lot about how prepared you are from these tests and you may also find that in a real recovery situation, things will go better than you had expected as a result.

## 10. General Disaster Recovery Considerations

**Dedicate Recovery Equipment And Build A Recovery Lab** – It is important to dedicate hardware. Don't fall into the trap of allowing test equipment to become production equipment without replacement. Make sure that the recovery equipment is always in working order and available at a moment's notice. What tends to happen is that companies purchase recovery equipment, install some "test only" software and then become dependent on this equipment for production use. In short, keep recovery equipment in a dedicated mode. Another reason to build a lab is for recovery purposes. Note that it is more cost effective for an organization to maintain one recovery server with sufficient disk space. To achieve this you will require up to 2X the disk space of the largest production server Information Store database for recovery and database de-fragmenting using the EDBUTIL utility. Review the Environment. When placing production servers, inspect the area when deploying servers. Make sure that the environment will be receptive. Is there enough power? If possible, dedicate power lines for your equipment. Review existing amperage and new amperage requirements. Make sure the servers are not placed under fire sprinklers. Also be sure to locate servers in a physically secure location and ensure that the room temperature is acceptable. The robustness of Microsoft Exchange Server can be compromised by failure to perform basic preventive maintenance routines when deploying servers.

**Deploy an Un-interruptible Power Supply (UPS ) And Test It Periodically** – Don't take the approach that if the Microsoft Exchange-based server "goes" due to a power outage, all other servers will go too. Make sure that you are UPS protected. In some cases, computer rooms are supposedly UPS protected when in fact some outlets have not been included or just overlooked. If you do not have a dedicated UPS, make sure that you speak with the local electricians or operations personnel and perform a test. It is wise not to make assumptions. Users will hold you accountable and not the person or paperwork that said the outlets were UPS protected. Also note that UPS system batteries can wear out every 3 years or so and require replacement.

**Publish A Microsoft Exchange Server Maintenance Window** – A Microsoft Exchange-based server is no different than a car that requires oil changes and check-ups. Unlike mainframes, servers often get overlooked when it comes to scheduling downtime for maintenance. It is a simple formula: planned maintenance generally reduces unplanned downtime. It is important to set user expectation levels by publishing a maintenance window, especially when users expect 7day/24hr. service. Maintenance is inevitable since the nature of the data processing business includes service pack updates, software upgrades, and hardware upgrades. Although rare, it might be necessary to take down the Information Store service in order to reduce the size of store files using EDBUTIL.

**Create And Verify Daily Backups** – This is a very critical step in disaster recovery. It sounds simplistic but you can only recover data if you have a valid backup. It is often "assumed" that backup tapes are being swapped and that data is being properly backed up. It should be a daily routine to review all back up logs and to follow up on any errors or inconsistencies. Furthermore, Full (Normal) backups reset and remove transaction logs resulting in free disk space. This is not an issue if circular logging is enabled. If circular logging is not enabled and daily Full backups are failing, transaction logs will not be purged and can fill up the entire transaction log disk drive. Failure to verify that your backups are being completed successfully is one of the most common mistakes made.

**Standardize Tape Backup Formats** – Recovery equipment must be compatible with production tape equipment. If you deploy a new type of tape drive, make sure that you equip recovery equipment with a compatible model. You should also test reading and restoring production tape backups on the tape drive used for recovery.

**Create A Disaster Kit** – Planning ahead will reduce the time to recovery. You will find that a significant portion of recovery time in tests is spent trying to locate information or disks needed to configure your recovery system. It is critical to build a kit that includes items such as: operating system configuration sheet, hard drive partition configuration sheet, RAID configuration, hardware configuration sheet, EISA/MCA configuration disks, Microsoft Exchange configuration sheet, Windows NT/2000 emergency repair diskette, and the Microsoft Exchange Performance Optimizer settings sheet.

**Keep Solid Records Of All Configuration Done To The Production Server** – This will be necessary when configuring the recovery server. Records include Windows NT/2000 tuning settings, path information, protocol addresses, Microsoft Exchange connector configuration, and so on. These records should be part of the disaster recovery kit discussed above.

**Take A Proactive Approach To Monitoring The Information Store** – Monitor the growth of the Information Store and server performance and be prepared with a plan to remedy these issues. Windows NT/2000 disk space alerts can be set up as well to monitor remaining disk space. Performance Monitor objects exist for the Information Store and should be used.

**Check Windows NT/2000 Event Logs Daily** – It is best to take a proactive approach and review logs regularly. This can help you identify problems before they have an impact. Extensive logging is available in Microsoft Exchange and this should be leveraged. Logging tools are available on the Microsoft Exchange Server Technical Resource CD-ROM.

**Perform A Periodic Fire Drill** – This is to measure your ability to recover from a disaster and to certify your disaster recovery plans. Conduct this in a test environment and simply attempt a complete recovery. Be sure to use data from production backups. During this process it is best to record the time it takes to recover. This information will assist you in determining time to recovery in a real disaster recovery situation. Most administrator's experience that up to 1/3 of the recovery time can be spent in preparing and getting the correct tools in place to complete the job. For maximum effect, provide no notice to your staff that you are performing a drill. This will provide the most valuable experience that you will have in your disaster recovery planning.

**Devise An Archiving Plan** – An archiving plan will allow end users to move server-based messages into local store files. This will help reduce the size of the server based Information Store. Have users store PSTs on local drives or on a separate disk or server from that of the Information Store. Dedicate a file server for PST archiving if required. Otherwise, data will be reduced in the Store but added to another area of the same disk or logical drive. The hit will be greater since PST storage maintains messages in both RTF and ASCII format. Note also that disk space limits cannot be set on PST files. Be sure to include all sensitive data in backup strategies, including end user PST files. Use encryption when creating .OST and .PST files.

**Consider Maintaining Off-Site Tapes And Equipment** – Due to legal and/or security issues, certain companies opt not to send backup tapes to a third party off-site location. An alternative to this is to send tapes to an off-site location within the same company.

**Determine Downtime Cost** – This is useful when justifying the purchase of recovery equipment. There are different models for calculating the per hour downtime cost and this varies per business. Some calculations include Lost Orders Per Hour, Delayed Financial Transactions, and the cost of Delayed Time Sensitive Market Decisions.

**Microsoft Exchange Configuration Considerations** – If possible, avoid configuring the Microsoft Exchange-based server as a PDC or BDC. If the Microsoft Exchange-based server is not the PDC, you don't need to worry about promotions and demotions of Domain Controllers in a recovery situation. If the Microsoft Exchange-based server is a member server and not a PDC or BDC, additional memory overhead for the domain SAM will not be required; however, for remote offices, companies can save money by having the local Microsoft Exchange-based server provide authentication (BDC) and messaging services. Note that for a proper Directory Service restore, access to the original SAM is required. Never install a Microsoft Exchange-based server in a domain that does not have a BDC.

**Locate Transaction Log Files On Separate Dedicated Physical Disk** – Transaction logs provide an additional mechanism for recovery. Aside from this, it is the single most important aspect that can influence the performance of your Microsoft Exchange-based server. If you run the Microsoft Exchange Optimizer utility, it will automatically locate the files.

**Locate Information Store (IS) On RAID5 Stripe Set** – Since the Information Store uses random access, this provides superior performance. Furthermore, RAID5 provides an added level of recoverability.

**Mirror Or RAID5 the Operating System Partition** – This provides redundancy for the underlying operating system.

**Use Hardware RAID And MIRRORING When Possible** – Use hardware RAID5 wherever possible so that a disk drive failure can be remedied real-time by plugging in a replacement drive. Software RAID requires reconfiguration to add a new drive when bringing the system back to its original configuration following a failure. System partitions should be mirrored or RAID5 for redundancy.

**If Possible, Disable Circular Logging** – By default, Microsoft Exchange Server is configured with circular logging enabled. While Circular Logging can help conserve disk space, there are drawbacks. Specifically, Incremental and Differential backups are disabled. With Circular Logging off, log files will accumulate on the transaction log disk drive. When you run a Full backup from Backup Exec or the Windows NT/2000 Backup utility, transaction logs that are no longer needed (have been committed to disk) are automatically deleted. If a solid backup strategy is in place, transaction log files will be purged on a regular basis thus freeing up disk space.

**Place Limits On Information Store Attributes Early To Set User Expectations And To Properly Size Servers** – Configure mailbox storage limits and maximum age of server based messages. Also limit MTA message sizes and the size of messages that users can send.

**Configure The MTAs Accordingly** – Configure the MTA frequency such that queues are cleared quickly. This prevents queued messages from accumulating in the Information Store. Also, design a redundant MTA path so that messages keep flowing in the event of a link outage. It is important that MTAs are able to keep up with the traffic that flows through them to reduce messages in the store and for timely message delivery.

**Equip Servers With Sufficient disk Space** – Off-line maintenance and repair routines require up to 2x the disk space of the database file being administered with the EDBUTIL utility.



**VERITAS Software**  
**Corporate Headquarters**  
**1600 Plymouth Street**  
**Mountain View, CA 94043**

**North American Sales Headquarters**  
**400 International Parkway**  
**Heathrow, FL 32746**  
**800-327-2232 or 407-531-7501**  
**407-531-7730 Fax**

**Global Locations**

**United Kingdom**  
**44-(0)870-2431000**  
**44-(0)870-2431001 Fax**

**France**  
**33-1-41-91-96-37**  
**33-1-41-91-96-38 Fax**

**Germany**  
**49-(0)69-9509-6188**  
**49-(0)69-9509-6264 Fax**

**South Africa**  
**27-11-448-2080**  
**27-11-448-1980 Fax**

**Australia**  
**1-800-BACKUP**  
**612-8904-9833 Fax**

**Hong Kong**  
**852-2575-2576**  
**852-2893-2727 Fax**

**Japan**  
**81-3-5532-8217**  
**81-3-5532-0887 Fax**

**Malaysia**  
**603-715-9297**  
**603-715-9291 Fax**

**Singapore**  
**65-488-7596**  
**65-488-7525 Fax**

**China**  
**011-8610-62638358**  
**011-8610-62638359 Fax**

**Electronic communication**

**E-Mail:**  
**[sales@veritas.com](mailto:sales@veritas.com)**

**World Wide Web:**  
**<http://www.veritas.com>**

90-00988-910 • NT01-2KEXCWPR-9903

© 1999 VERITAS Software Corp. All rights reserved. VERITAS and the VERITAS logo are registered trademarks of VERITAS Software. Backup Exec, Client Exec and Intelligent Disaster Recovery are registered trademarks or trademarks of VERITAS Software Corp. All other names and trademarks are the property of their respective owners. Specifications and product offerings subject to change without notice. Printed in USA. January 2000.