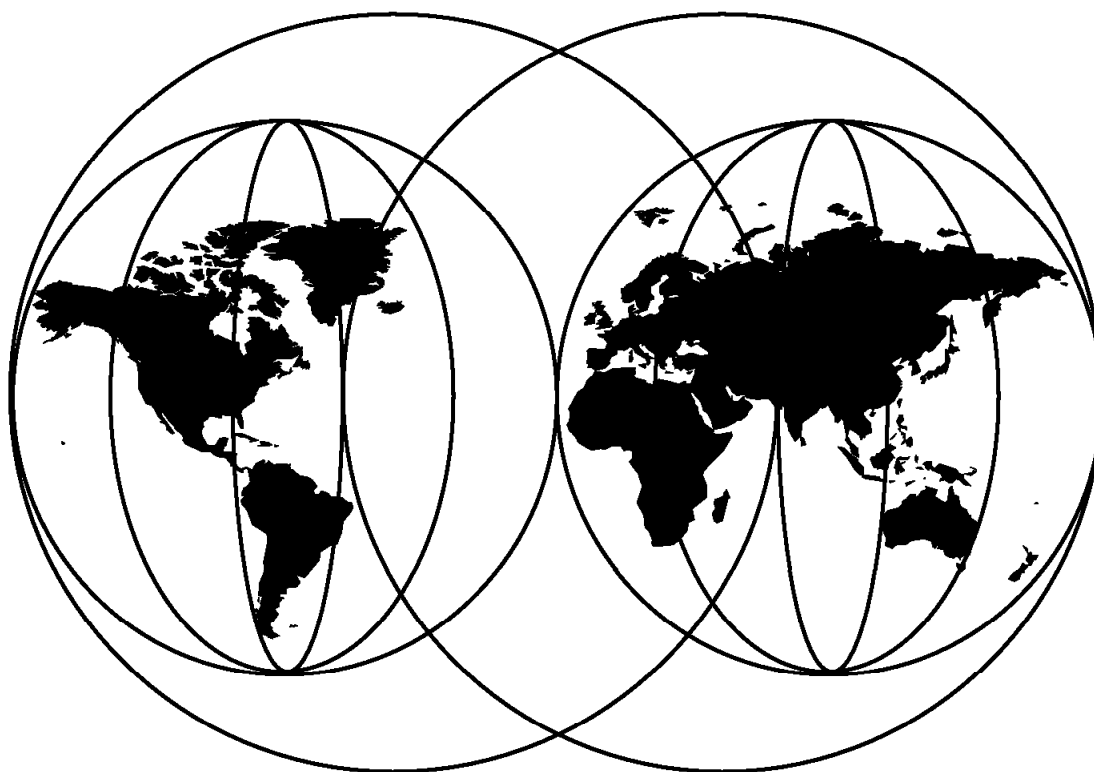


Using ADSM to Back Up and Recover Microsoft Exchange Server

*Chris Barnes, Petra Jobst, Alex Osuna, Miklos Werner,
Patrick Randall*



International Technical Support Organization

<http://www.redbooks.ibm.com>



International Technical Support Organization

SG24-5266-00

**Using ADSM to Back Up and Recover
Microsoft Exchange Server**

November 1998

Take Note!

Before using this information and the product it supports, be sure to read the general information in Appendix F, "Special Notices" on page 91.

First Edition (November 1998)

This edition applies to:

- Version 3, Release 1 of ADSTAR Distributed Storage Manager for MVS, Program Number 5655-A30, for use with the MVS and OS/390 operating system
- Version 3, Release 1 of ADSTAR Distributed Storage Manager for AIX, Program Number 5765-C43, for use with the AIX operating system, Version 4
- Version 3, Release 1 of ADSTAR Distributed Storage Manager for HP-UX, Program Number 5639-D92
- Version 3, Release 1 of ADSTAR Distributed Storage Manager for Sun Solaris, Program Number 5639-D91
- Version 3, Release 1 of ADSTAR Distributed Storage Manager for Windows NT, Program Number 5639-C59, for use with the Windows NT operating system

Comments may be addressed to:

IBM Corporation, International Technical Support Organization
Dept. QXXE Building 80-E2
650 Harry Road
San Jose, California 95120-6099

When you send information to IBM, you grant IBM a non-exclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

© **Copyright International Business Machines Corporation 1998. All rights reserved.**

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

Contents

Figures	v
Preface	vii
The Team That Wrote This Redbook	vii
Comments Welcome	viii
 Chapter 1. Backing Up Microsoft Exchange Server: An Overview	1
1.1 Microsoft Exchange Server Components and Windows NT Backup	1
1.1.1 Microsoft Exchange Server Components	1
1.1.2 Windows NT Backup Program	2
1.2 Microsoft Exchange Server and ADSM	3
1.2.1 Offline Backup to ADSM with the Backup/Archive Client	4
1.2.2 Online Backup to ADSM with the ADSMConnect Agent	4
1.3 Scope of This Book	5
 Chapter 2. Backup: Installation, Setup, and Day-to-Day Operation	7
2.1 Microsoft Exchange Server Services and Outlook Client Data	7
2.1.1 Microsoft Exchange Server Core Components	7
2.1.2 Files Maintained by the Outlook Client	8
2.2 ADSM Offline Backups of Microsoft Exchange Server	10
2.2.1 Automating with the ADSM Command Schedule	11
2.2.2 Backing Up Database Copies	13
2.3 ADSM Online Backup of Microsoft Exchange Server	15
2.3.1 Data Backed Up by ADSMConnect Agent for Microsoft Exchange Server	15
2.3.2 Data Not Backed Up by ADSMConnect Agent for Microsoft Exchange Server	16
2.3.3 Defining the Location of Files Maintained by the Outlook Client	17
2.3.4 Supported Environments	18
2.3.5 Microsoft Exchange Server Database Transaction Logs	18
2.3.6 ADSM Management Class	22
2.3.7 Microsoft Exchange Server Information Store Maintenance	24
2.3.8 Client Options File Recommendations	25
2.3.9 Performance Settings	29
2.3.10 Capacity Planning	31
2.3.11 Detecting Performance Bottlenecks	33
2.3.12 Windows NT Event Viewer	38
2.3.13 Windows NT Accounts	41
2.3.14 ADSMConnect Agent Log File Setup and Use	43
2.3.15 ADSMConnect Agent Scheduling and Maintenance	47
 Chapter 3. Database Recovery	51
3.1 Restoring Databases from Offline Backups	51
3.2 Restoring Databases from Online Backups	54
3.2.1 Requirements for Successful Recovery	55
3.2.2 NT Machine Security	55
3.2.3 NT Machine Security and Full Server Recovery	55
3.2.4 Procedure to Restore a Full Server	56
3.3 Restoring Individual Mailboxes	60
3.3.1 Using the Deleted Item Recovery Option	61
3.3.2 Using an Existing Personal Folder	65

3.3.3 Using an Existing Offline Folder	65
3.3.4 Restore to a Spare Server	67
3.3.5 Public Folder Recovery	70
3.4 Microsoft Exchange Server Disaster Recovery Planning	71
3.4.1 Preparation	71
3.4.2 Microsoft Exchange Server Internet Mail Connector: Backup and Restore	73
3.5 Validating the Recovery	74
Appendix A. Information Store Considerations	77
A.1 Size	77
A.2 Use of Personal Folders (PSTs)	77
A.2.1 Advantages	77
A.2.2 Disadvantages	78
A.3 Clean Mailbox	78
Appendix B. Sample Offline Archive Command File	79
Appendix C. Adding a New ADSM Management Class	81
Appendix D. Unattended Setup Scripts for Microsoft Exchange Server	83
D.1 Setup Script to Install Microsoft Exchange Server at an Existing Site	83
D.2 Setup Script to Install Microsoft Exchange Server at a New Site	83
Appendix E. Sample Scripts and Command Files	85
E.1.1 Sample Command File to Install ADSM Scheduler	85
E.1.2 ADSMConnect Agent Backups	85
E.1.3 ADSMConnect Agent Backups and Central Logging	86
E.1.4 ADSMConnect Agent Backups, Central Logging, and Log Pruning	87
E.1.5 Perl Script for Deleting Old ADSMConnect Agent Backups	88
Appendix F. Special Notices	91
Appendix G. Related Publications	93
G.1 International Technical Support Organization Publications	93
G.1.1 ADSM Redbooks	93
G.1.2 Tivoli Redbooks	93
G.2 Redbooks on CD-ROMs	94
G.3 ADSM Product Publications	94
G.4 ADSM Online Product Library	94
G.5 Tivoli Publications	95
How to Get ITSO Redbooks	97
How IBM Employees Can Get ITSO Redbooks	97
How Customers Can Get ITSO Redbooks	98
IBM Redbook Order Form	99
Index	101
ITSO Redbook Evaluation	103

Figures

1.	Microsoft Exchange Server Components	2
2.	Microsoft Exchange Server Online Backup with the Windows NT Backup Command	3
3.	Microsoft Exchange Server and ADSM Overview	4
4.	Files Maintained by the Outlook Client	8
5.	The Outlook Bar	9
6.	Exclude Statements from the ADSM BAclient dsm.opt File	12
7.	ADSM Schedule to Archive Dumped Database Files	15
8.	Microsoft Exchange Server Databases	16
9.	Microsoft Windows Mail Profile	17
10.	Transaction Log Processing	19
11.	Circular Logging	20
12.	Circular Logging Settings	21
13.	Circular Logging Status	22
14.	ADSM Backup Copy Group Properties	23
15.	IS Maintenance Properties	24
16.	Node Properties	27
17.	ADSM Node Registry Entry	28
18.	Sample Client Options File	29
19.	Performance Buffers	30
20.	Exchange Agent Settings: Performance	30
21.	Command Line Example: Buffer Utilization	31
22.	Windows NT Performance Monitor	33
23.	dsmacct.log File Accounting Record	34
24.	EXCSCHED.LOG	35
25.	ADSMConnect Agent for Microsoft Exchange Server GUI	36
26.	Query Node Example	37
27.	Select node_name Example	38
28.	System Log: Event Detail	39
29.	Event Viewer: Application Log	39
30.	Application Event Log: Event Detail Information	40
31.	Application Log: Event Detail-Error	40
32.	Local Group Properties: Administrators Group	42
33.	Services Startup Properties	43
34.	Sample EXCDISM.LOG File	43
35.	ADSMConnect Agent Default Activity Log File	44
36.	Output from ADSMConnect Agent Backup	47
37.	Scheduler Client Session Timeout	50
38.	Windows NT Control Panel: Services	51
39.	ADSM Backup/Archive Client Retrieve	52
40.	Select DIR.EBD, PRIV.EDB and PUB.EDB for Retrieve	53
41.	Default Modify Retrieve Options	53
42.	Default Destination for Retrieved Objects	54
43.	Windows NT Machine Security	56
44.	Full Server Recovery Steps	57
45.	Deleting the Old Machine Account	58
46.	Creating New Site	58
47.	Start Microsoft Exchange Server System Attendant	59
48.	Start Microsoft Exchange Server Restore of Information Store and Directory	60
49.	Permanent Deletion of Messages	61

50.	Deleted Item Retention Time	62
51.	Recovering Deleted Items	63
52.	Registry Update for Deleted Item Recovery	64
53.	Access to Other Users' Mailboxes	65
54.	Preparation to Work Offline	66
55.	Steps to Restore to Spare Server	67
56.	Start Microsoft Exchange Server Restore of Information Store	69
57.	Consistency Adjustment after Database Restore	70
58.	Public Information Store Instances Tab	71
59.	Microsoft Exchange Server Distribution List Properties	74
60.	Microsoft Exchange Server Client Permissions on Public Folders	75
61.	Microsoft Exchange Server Information Store Site Configurations	76
62.	Microsoft Exchange Server Message Tracking Center	76
63.	Clean Mailbox Configuration	78

Preface

This redbook describes the experiences of using ADSM to back up Microsoft Exchange Server. We cover offline backup using the ADSM Backup/Archive client and online backup using the ADSMConnect Agent for Microsoft Exchange Server. We demonstrate how ADSM can be used to protect typical Microsoft Exchange Server implementations against failures ranging from simple user errors to site disasters.

This book will be especially useful for ADSM and Microsoft Exchange Administrators who need to understand the backup and recovery considerations associated with ADSM and Microsoft Exchange Server.

The Team That Wrote This Redbook

This redbook was produced by a team of specialists from around the world working at the International Technical Support Organization, San Jose Center.

Patrick Randall is a Distributed Storage Software Specialist at the International Technical Support Organization, San Jose, California. He has written eight redbooks on ADSM, teaches IBM classes worldwide on all areas of distributed storage, and is a consultant in disaster and business recovery. Before joining the ITSO in July 1996, Patrick worked in IBM UK's Business Recovery Services as a Solutions Architect.

Chris Barnes is a Technical Support Specialist at Bankers Trust Australia. He has 12 years of experience in network operating systems. Chris has an Electronics and Electrical Engineering Certificate from Sydney Technical College. He is a Certified Microsoft and Novell Engineer. His areas of expertise include the design and support of Microsoft Windows NT and Microsoft Exchange Server installations.

Petra Jobst is a Senior IT Specialist in IBM Global Services, in the United States. She has been in the computer industry for 11 years and has worked for IBM for 9 years in New York. Petra's areas of expertise include ADSTAR Distributed Storage Manager and AIX. She has worked extensively in problem determination, critical situation management, and project management.

Alex Osuna is a Consulting IT Specialist for the IBM Advanced Technical Support group in San Jose, California, USA. He has worked for IBM for 18 years. Alex is an IBM ADSM and Microsoft Certified Professional. His areas of expertise are in support of the ADSM MVS and Windows platforms. Alex has published 12 Washington System Center flashes on ADSM.

Miklos Werner is a Business Recovery Consultant in Germany. He has worked at IBM for 14 years, initially in application development projects and in the education area. For the last two years Miklos worked on storage management issues in different customer projects. He holds a degree in mathematics. His areas of expertise include storage management with ADSM.

Thanks to the following people for their invaluable contributions to this project:

Maggie Cutler

IBM International Technical Support Organization, San Jose Center

Del Hoobler
IBM ADSM Agent Development, Endicott, NY

Chris Zaremba
IBM IGS ADSM Agent Development, Endicott, NY

Phil Chissell
National Power PLC Development, Swindon, UK

Comments Welcome

Your comments are important to us!

We want our redbooks to be as helpful as possible. Please send us your comments about this or other redbooks in one of the following ways:

- Fax the evaluation form found in "ITSO Redbook Evaluation" on page 103 to the fax number shown on the form.
- Use the electronic evaluation form found on the Redbooks Web sites:

For Internet users	http://www.redbooks.ibm.com/
For IBM Intranet users	http://w3.itso.ibm.com/

- Send us a note at the following address:
redbook@us.ibm.com

Chapter 1. Backing Up Microsoft Exchange Server: An Overview

The Microsoft Exchange Server is software for handling mail, organizing meetings, and managing the enterprise directory. In this chapter we describe the Microsoft Exchange Server components and the native Windows NT method of backing them up. We then outline two methods of backing up Microsoft Exchange Server with ADSM:

- Offline backup to ADSM (with the Microsoft Exchange Server services stopped)
- Online backup to ADSM with the ADSMConnect Agent for Microsoft Exchange Server

In 1.3, "Scope of This Book" on page 5, we detail what is and is not covered in this book.

1.1 Microsoft Exchange Server Components and Windows NT Backup

In this section we outline the major components and functions of Microsoft Exchange Server and describe the default method of using the Windows NT Backup command to back up the Microsoft Exchange Server

1.1.1 Microsoft Exchange Server Components

As shown in Figure 1 on page 2, Microsoft Exchange Server consists of the following core components:

- An information store, which includes two database files:
 - A public database that contains public folders and is the central place for sharing information among users. Public folders can be replicated to other Microsoft Exchange Server public information stores.
 - A private database containing all messages in users' mailboxes. Users' mailboxes cannot be replicated.
- A directory database, under control of the directory service, which contains an organization's recipients (users), distribution lists, servers, and messaging infrastructure. The directory database is replicated to all servers in an organization. Nevertheless, it contains unique information about each server and cannot be restored from another server.
- The message transfer agent (MTA), which is the service responsible for submitting, routing, and delivering messages between other Microsoft Exchange Server MTAs and connectors.
- The system attendant service, which is responsible for a number of administrative functions such as:
 - Assisting with the operation of server monitors
 - Checking messaging connectors
 - Checking directory replication
 - Building routing tables
 - Generating e-mail addresses
 - Logging message tracking information

- Assisting in the generation of the offline address book for mobile users

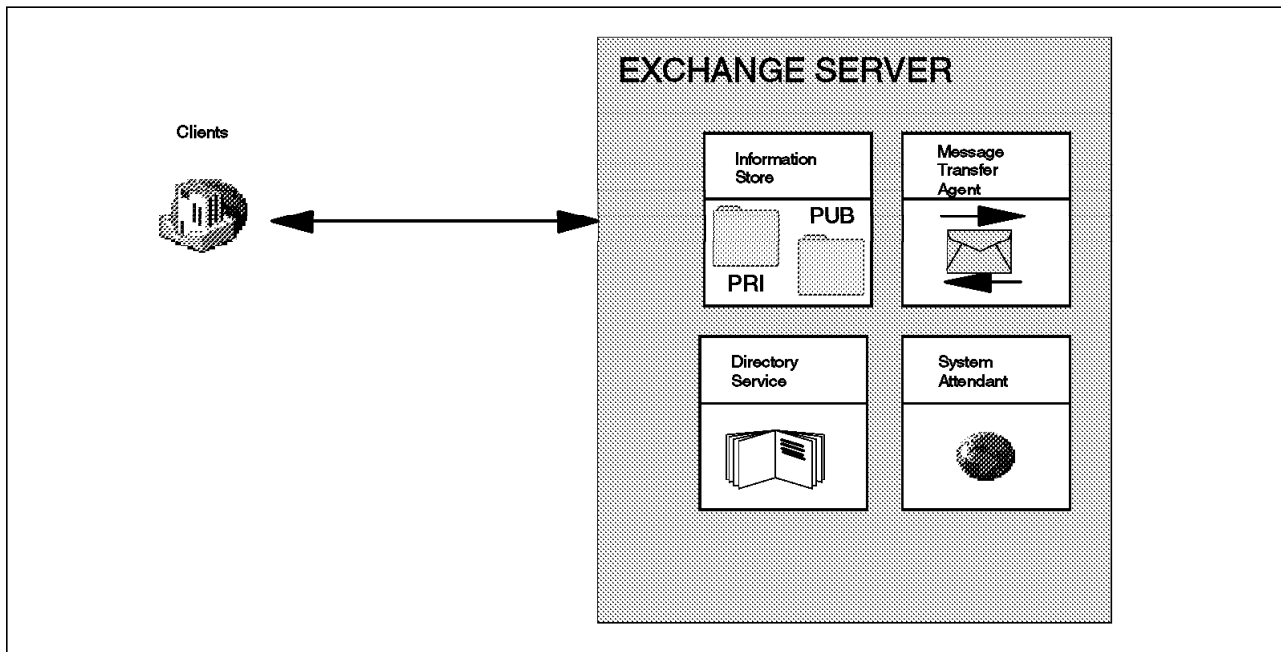


Figure 1. Microsoft Exchange Server Components

1.1.2 Windows NT Backup Program

As shown in Figure 2 on page 3, you can use the Windows NT backup program to back up Microsoft Exchange Server online, that is, without stopping the Microsoft Exchange Server services. The output must be directed to a supported local tape device. This option is not covered in this book. You can find more information in the Microsoft Exchange Server online help.

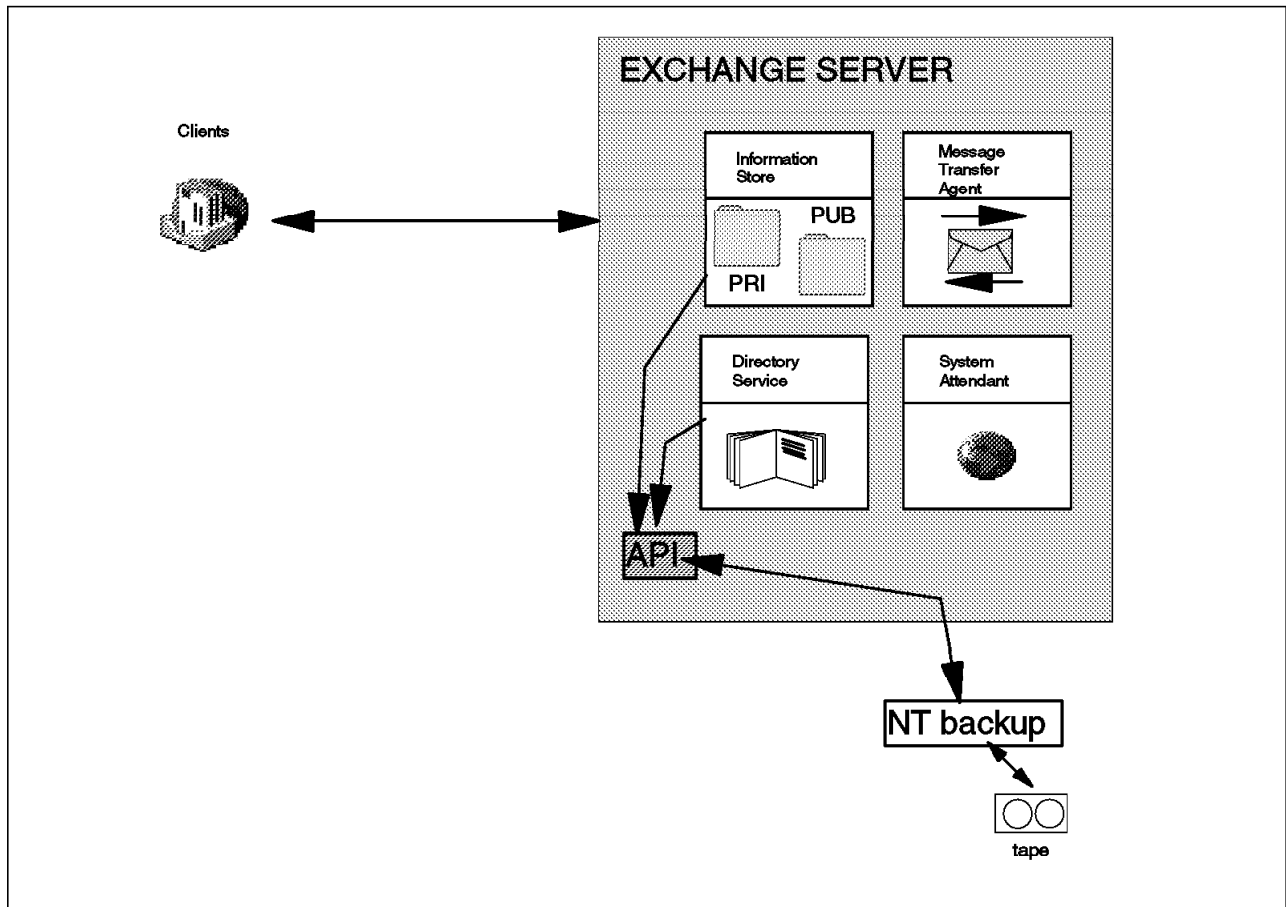


Figure 2. Microsoft Exchange Server Online Backup with the Windows NT Backup Command

1.2 Microsoft Exchange Server and ADSM

As shown in Figure 3 on page 4, Microsoft Exchange Server can be backed up to ADSM either offline through the standard backup archive client or online through the Microsoft API and the ADSMConnect Agent.

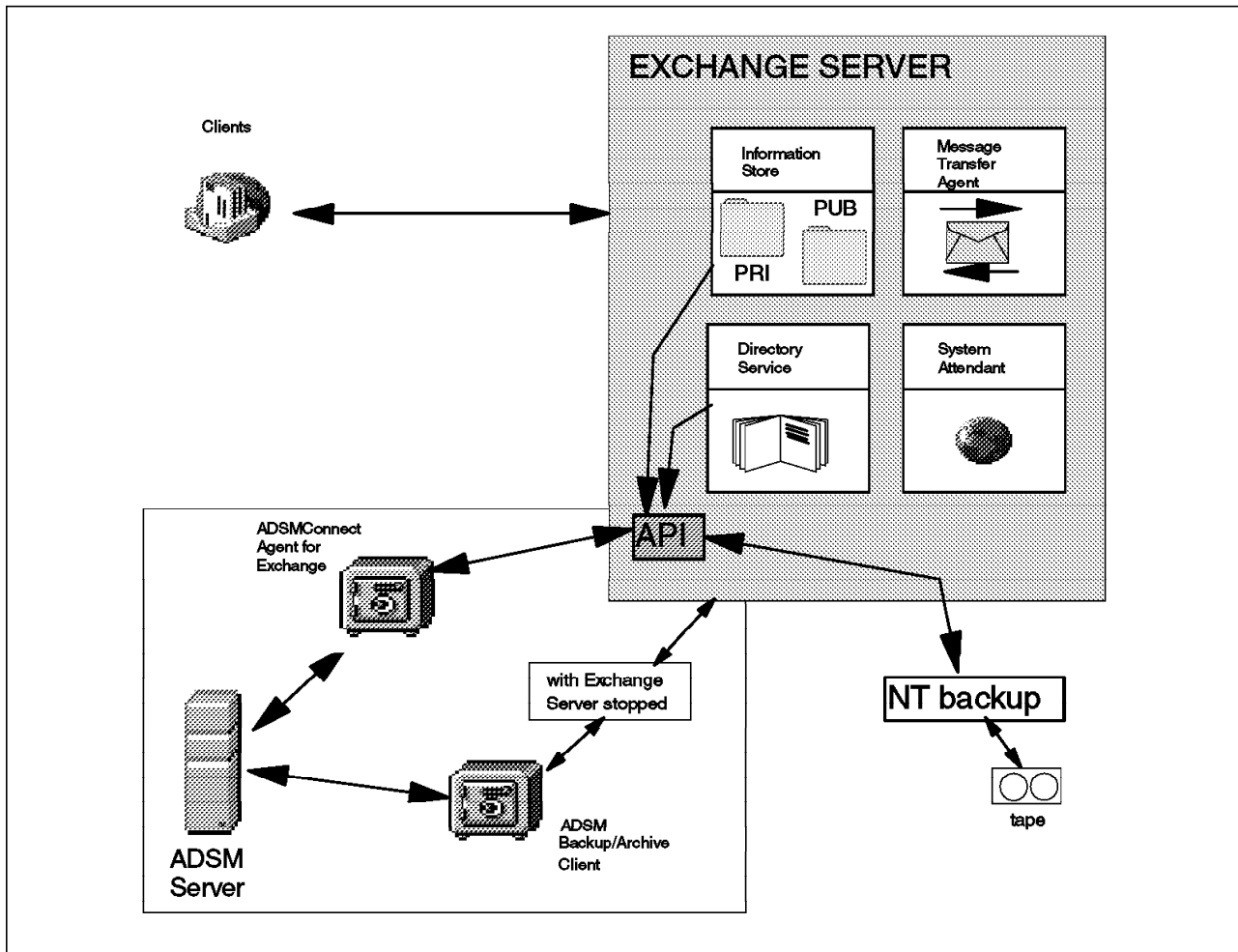


Figure 3. Microsoft Exchange Server and ADSM Overview

1.2.1 Offline Backup to ADSM with the Backup/Archive Client

If it is possible to stop the Microsoft Exchange Server to back it up, you can use the standard ADSM backup/archive client to back up the files associated with the server. You can stop the Microsoft Exchange Server services and run ADSM BAclient archive. The entire offline backup procedure can be automated with a command file that can be scheduled to run at a certain time.

If a backup window is not available, it is possible to keep a second local copy of the database and schedule the ADSM archive while the Microsoft Exchange Server database is up and running.

These options are explored further in 2.2, "ADSM Offline Backups of Microsoft Exchange Server" on page 10.

1.2.2 Online Backup to ADSM with the ADSMConnect Agent

The ADSMConnect Agent helps protect and manage Microsoft Exchange Server data by making it easy to do the following actions:

- Perform full, copy, differential, and incremental backups of the Microsoft Exchange Server directory and information store databases

- Restore a full directory or information store database and any number of associated transaction logs
- Delete a directory or information store database backup from ADSM storage
- Back up the Microsoft Exchange Server databases to any ADSM server, with drag-and-drop ease
- Set ADSM options regarding connection information to ADSM servers
- Set ADSM options regarding security and performance
- Obtain online context-sensitive, task, and concept help
- View online documentation for the Exchange Agent
- Launch other ADSM and related system applications
- Automate scheduled backups

This backup method is explored further in 2.3, “ADSM Online Backup of Microsoft Exchange Server” on page 15.

1.3 Scope of This Book

In this book we discuss using ADSM to back up Microsoft Exchange Server.

Windows NT supplies a utility program, NTBACKUP, to perform online backups to a supported local tape device. We do not cover NTBACKUP in detail in this book, but more information about it is available in the Microsoft Exchange Server online help.

Some organizations have planned down times, which may be necessary or even acceptable. If planned down times are an option in your organization, see 2.2, “ADSM Offline Backups of Microsoft Exchange Server” on page 10 on how to use the ADSM backup/archive client for Windows NT to perform an offline backup of Microsoft Exchange Server.

If an offline backup is not an option and/or distributed tape management, as with NTBACKUP, is not desirable, see Chapter 2, “Backup: Installation, Setup, and Day-to-Day Operation” on page 7 for using the ADSMConnect Agent for Microsoft Exchange Server to back up and recover a production environment.

We address different recovery scenarios with the ADSMConnect Agent for Microsoft Exchange Server. Information about using ADSM to recover Windows NT, a Microsoft primary domain controller (PDC), or a Microsoft backup domain controller (BDC) is documented in *Windows NT Backup and Recovery with ADSM* (SG24-2231-00).

Although we address using the ADSMConnect Agent for disaster recovery of a Microsoft Exchange Server, we do not discuss the recovery of the ADSM server. Information about server recovery is available in other IBM Redbooks and other IBM ADSM manuals and documentation, depending on the platform on which the ADSM server is running.

We installed and tested the Microsoft Exchange Server on a member server within a Microsoft Windows NT domain. The Microsoft Exchange Server was not configured as a PDC or BDC nor was it running any virus scan programs. We used Transmission Control Protocol/Internet Protocol (TCP/IP) for communications.

The Microsoft Exchange Server clients in our environment ran Microsoft Outlook. We provide some information about these clients in 2.1, “Microsoft Exchange Server Services and Outlook Client Data” on page 7 because they are part of the Microsoft Exchange Server environment, but we do not discuss their recovery.

Chapter 2. Backup: Installation, Setup, and Day-to-Day Operation

In this chapter we explain how to install, set up, and prepare for day-to-day operations of Microsoft Exchange Server. We cover:

- Microsoft Exchange Server core components and files maintained by the Outlook client.
- Offline backup using the ADSM backup/archive client
- Online backup using the ADSMConnect Agent for Microsoft Exchange Server

2.1 Microsoft Exchange Server Services and Outlook Client Data

In this section we discuss the Microsoft Exchange Server Core Components and files maintained by the Outlook client

2.1.1 Microsoft Exchange Server Core Components

The following four components are implemented as Window NT services, installed by the Microsoft Exchange Server setup.exe program, and required for a functioning Microsoft Exchange Server:

- **Directory service**

The directory service manages information about the organization of Microsoft Exchange Server. The information in the directory includes addresses, mailbox information, distribution lists, the public folder hierarchy, and other servers. Microsoft Exchange Server administrators maintain the directory. The directory information is stored in the DIR.EDB database file. The directory is automatically replicated to all servers within in the organization.

- **Information store**

The information store service maintains the server-based private (user mailboxes) and public folder information. The private and public information stores are in two separate databases, PRIV.EDB and PUB.EDB. The information store also replicates public folders, enforces storage limits, and delivers messages to users on the same Microsoft Exchange Server.

- **Message transfer agent**

The MTA service is responsible for submitting, routing, and delivering messages between other Microsoft Exchange Server MTAs and connectors.

- **System attendant**

The system attendant service is responsible for a number of functions:

- Assists with the operation of server monitors
- Checks messaging connectors
- Checks directory replication
- Builds routing tables
- Generates e-mail addresses
- Logs message tracking information
- Assists in the generation of the offline address book

2.1.2 Files Maintained by the Outlook Client

As shown in Figure 4, the Outlook client stores configuration and messaging data in files that are not part of the Microsoft Exchange Server information store. These files must be included in backup schedules.

2.1.2.1 Offline Folders

Offline folders are files that are replicated copies of the Microsoft Exchange Server based mailbox. They are commonly referred to as OST files because of their default extension. OST files are used by mobile users when not connected to the Microsoft Exchange Server. They enable a mobile user to work offline and periodically synchronize local data with the server-based mailbox. The first time you configure and use an offline folder, an OST file is created on the local file system, and the server-based mailbox is replicated. When working offline, you work in your offline mailbox exactly as you do with your mailbox on the server. When you connect to the Microsoft Exchange Server, changes are sent to the server-based mailbox, and any new messages on the server are replicated to the OST file.

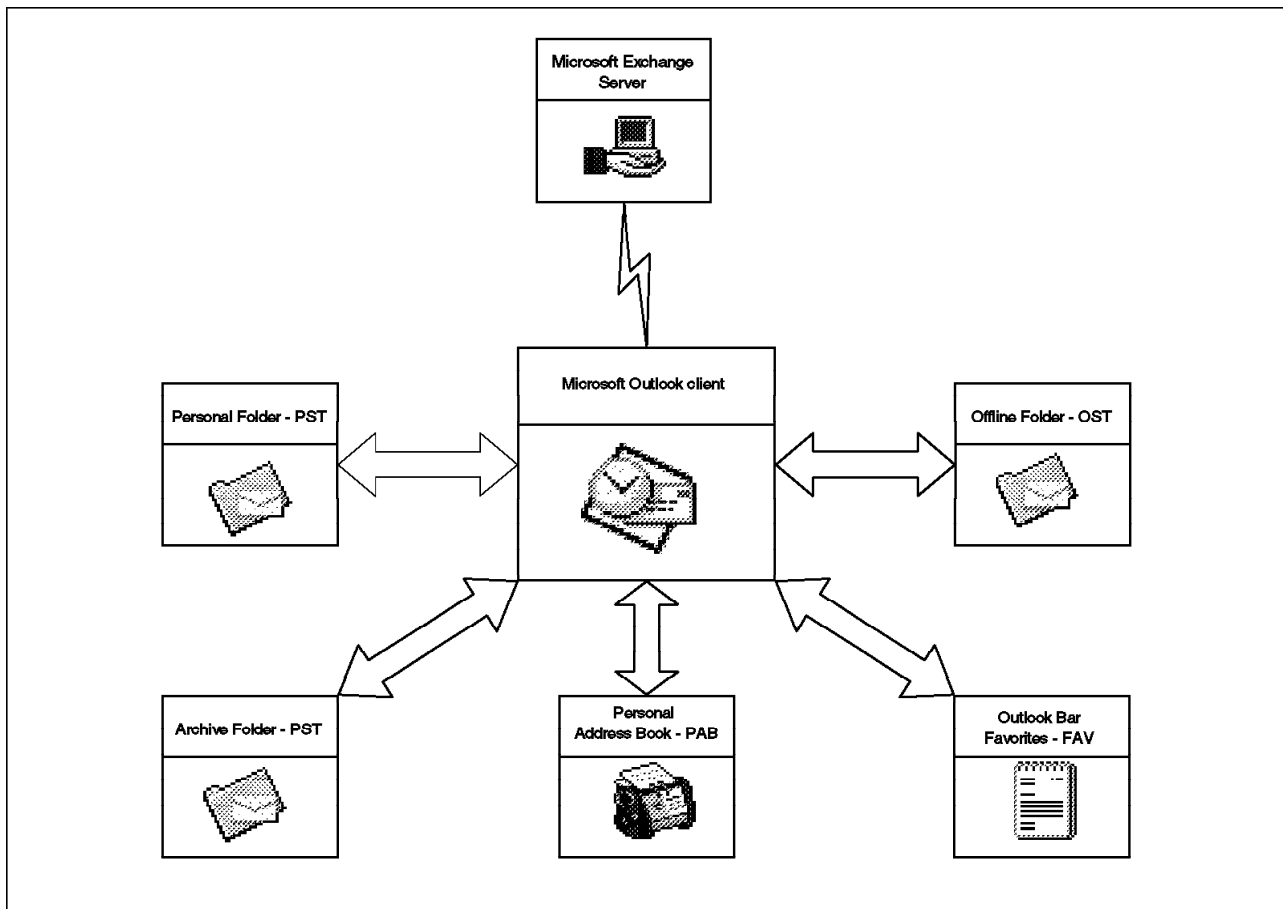


Figure 4. Files Maintained by the Outlook Client

2.1.2.2 Personal Folders

Personal folders are files you can create to store messaging data on a file system outside the server-based mailbox. They are commonly referred to as PST files because of their default extension. You can define as many PSTs as you like. You can copy, delete, rename, and move a PST as you can any other file.

2.1.2.3 Personal Address Book

Personal address book is a file that contains a list of e-mail addresses and distribution group information as compiled by a user. Personal address book files are commonly referred to as PAB files because of their default extension.

2.1.2.4 Archive Folders

Archive folders are files created by the archive process in the Outlook client. They are PST files, and it is common for each user to have one archive file called archive.pst. An identical folder structure is created between the archive file and server-based mailbox.

When you archive, items within the server-based mailbox are copied to the archive file and then removed from the server-based mailbox.

2.1.2.5 Outlook Bar Favorites File

The Outlook bar favorites file contains configuration settings. When you customize the Outlook bar within the Outlook client, the changes are automatically saved to a file called <profile_name>.FAV. This file is unique for each user and cannot be copied to another user.

Figure 5 shows the Outlook Bar that you can customize.

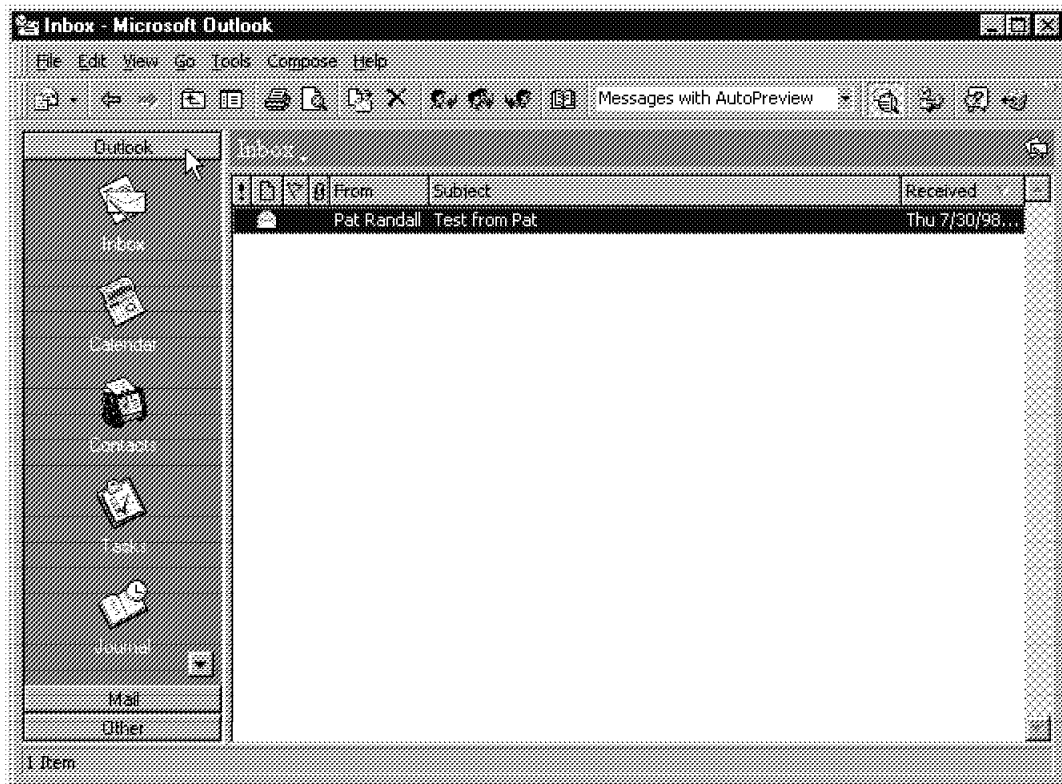


Figure 5. The Outlook Bar

2.2 ADSM Offline Backups of Microsoft Exchange Server

As shown in Figure 2 on page 3, you can use the Microsoft Exchange Server standard backup/archive client to back up to ADSM when it is stopped and offline. If your operations do not require 24x7 availability and offline periods are easily scheduled, the ADSM windows backup client may be the more economical choice as you do not have to purchase the ADSMConnect Agent license.

If you try to back up the Microsoft Exchange Server while the Exchange services are running, several critical files will be in an open state. Depending on the ADSM settings, the ADSM backup/archive client for Windows NT will make several attempts to back up the Microsoft Exchange Server database files, but eventually these backups will fail and the errors will be logged in the DSMSCHED.LOG and DSMERROR.LOG client files. Below is an example of the errors:

```
00:14:30 ANS1228E Sending of object 'C:\exchsrvr\mdbdata\PRIV.EDB' failed
00:14:30 ANS4007E Error processing 'C:\exchsrvr\mdbdata\PRIV.EDB': access to the object is denied
00:14:31 Normal File--> 9,445,376 C:\exchsrvr\mdbdata\PUB.EDB ** Unsuccessful **
00:14:31 ANS1228E Sending of object 'C:\exchsrvr\mdbdata\PUB.EDB' failed
00:14:31 ANS4007E Error processing 'C:\exchsrvr\mdbdata\PUB.EDB': access to the object is denied
00:14:31 Normal File--> 1,056,768 C:\exchsrvr\mdbdata\tmp.edb ** Unsuccessful **
00:14:31 ANS1228E Sending of object 'C:\exchsrvr\mdbdata\tmp.edb' failed
00:14:31 ANS4007E Error processing 'C:\exchsrvr\mdbdata\tmp.edb': access to the object is denied
```

If you choose to use the ADSM backup/archive client for Windows NT to back up the Microsoft Exchange Server, you must first stop the Exchange server services, and then issue the ADSM command to back up the Microsoft Exchange Server database. If you choose to do an offline backup, consider these items first:

- Database size, which equates to down time
- ADSM archive function
- Automating the stop and start of the Exchange services
- Scheduling
- Error checking
- Backups are not incremental

A large Microsoft Exchange Server database, with many users and many document attachments, equates to down time for backing it up. You could stop the Exchange services, copy the database files to another location, and quickly restart the services. However, this approach requires an extra step, perhaps more automation and error checking, as well as additional disk space on the server for the copies of those database files.

For several reasons, we used the ADSM archive action, instead of an ADSM selective or incremental backup:

- If you schedule a regular ADSM backup for the Microsoft Exchange Server database files, the ADSM backup/archive client options file must contain an include statement for those files. Therefore, other ADSM backups against the same drive will result in error messages, like those in the above example.

Note

You could schedule a selective backup for the Microsoft Exchange Server database and then another selective backup for other Windows NT files. A selective backup however, is different from an incremental backup because a selective does not check to see that the file has changed. This changes the active-inactive synchronization in ADSM and distorts what ADSM records as actual changed files on your server.

- Excluding the database files is easier. Regular incrementals can run, and the Microsoft Exchange Server database can be specified in a separate archive operation.
- You can specify a unique description for archives that will enable you to easily identify it.
- Archives are managed by the RETVer parameter, referenced as the "Length of time to retain archive version" in the ADSM Administrative GUI. Therefore, the files do not have to be deleted, for old copies to be removed, and if the file name changes for some reason, they are not deleted according to the specified backup copy group rules.

Every time the offline backups are run, the Exchange services must be stopped before the ADSM backup/archive action is invoked. All of the commands for performing these functions can be placed in a command file and then scheduled. You have several options for automating this, depending on how customized you would like your implementation, and how many additional resources you have:

- You could implement all of the NET STOP, NET START, and ADSM ARCHIVE commands in a single command file, which could be started by a schedule.
- You can stop the Exchange services, copy the database files to local disk, then immediately bring the Exchange services back up, leaving the ADSM ARCHIVE to be scheduled at any convenient time.

2.2.1 Automating with the ADSM Command Schedule

In this example, we assumed that ADSM would archive only Microsoft Exchange Server database files. Other Windows NT files, including the registry, would be backed up with separate ADSM incremental schedules.

We installed and configured the ADSM backup/archive client for Windows NT on the Microsoft Exchange Server. To avoid error messages during the incremental backups, we added four exclude statements in the ADSM BAclient options file, dsm.opt. You can add the exclude statements while configuring other options for the ADSM client. See Figure 6 on page 12.

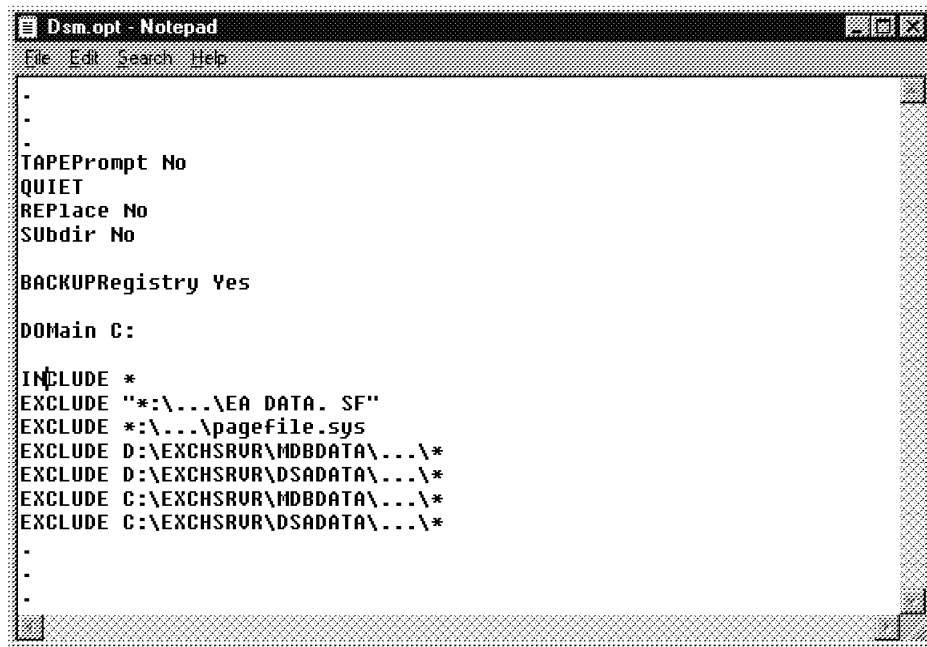


Figure 6. Exclude Statements from the ADSM BAclient dsm.opt File

For more information on about installing and configuring the ADSM BAclient, see *ADSTAR Distributed Storage Manager: Installing the Clients Version 3 Release 1* (SH26-4080).

We created a command file to:

1. Stop all Microsoft Exchange Server services
2. Archive the Microsoft Exchange Server database files
3. Start all Microsoft Exchange Server services

Before we ran the ADSM ARCHIVES against the Microsoft Exchange Server database files, we stopped the Exchange services. We implemented the following commands:

1. NET STOP MSEXCHANGEMTA
2. NET STOP MSEXCHANGEIS
3. NET STOP MSEXCHANGEDS
4. NET STOP MSEXCHANGESA

We then set up a series of ADSM ARCHIVE schedules.

We added two simple ADSM ARCHIVE commands to archive all of the Microsoft Exchange Server database and redirect any output to EXCHOUT.LOG:

```
DSMC ARCH C:\EXCHSRVR\DSADATA\*. * > C:\ADSM\BACLIENT\EXCHOUT.LOG
DMSC ARCH C:\EXCHSRVR\MBDDATA\*. * >> C:\ADSM\BACLIENT\EXCHOUT.LOG
```

Because the Exchange services are stopped before ADSM ARCHIVES run, all information in the logs is committed to the Microsoft Exchange Server databases. Therefore we did not archive the log files. However, the logs are open files, so we excluded them in the ADSM BAclient options file.

If you have any subdirectories beneath DSADATA and MBDDATA, add a -SUBDIR=YES parameter. You can also specify a -DESCRIPTION= parameter, if you want to specifically identify each group of archived files. For more

information about the ADSM backup/archive client ARCHIVE command, see *ADSTAR Distributed Storage Manager: Using the Microsoft Windows Backup-Archive Clients Version 2* (SH26-4056).

If you choose to configure a unique ADSM management class for the Microsoft Exchange Server archives, use the -ARCHMC option. Otherwise, the archives fall under the rules of the default management class. For more information about ADSM management classes, see the ADSM Administrator's Guide for your server platform.

Once the archives completed, we restarted the Microsoft Exchange Server database, using these NET START commands:

1. NET START MSEXCHANGESA
2. NET START MSEXCHANGEDS
3. NET START MSEXCHANGEIS
4. NET START MSEXCHANGEMTA

To automate the restart, place all of these commands into a single command file (see Appendix B, "Sample Offline Archive Command File" on page 79.)

Note

Centralized error checking is not implemented in this example. If, for some reason, the NET STOP commands do not complete, the command file will not complete properly and the ADSM archives will generate errors. Messages will be logged in the EXCHOUT.LOG and the DSMERROR.LOG file, but the ADSM schedule is a command schedule, and, as long as the EXCHARCH.CMD is successfully started, the schedule will list the outcome as completed.

2.2.2 Backing Up Database Copies

This example assumes that the Windows NT server running the Microsoft Exchange Server has additional disk space, enough to accommodate a second copy of the database. We configured the ADSM backup/archive client with the same exclude statements as we used in the first example, and any additional management class definitions you want to make would again apply. This example does the following:

1. Stops all Microsoft Exchange Server services
2. Copies the Microsoft Exchange Server database files to an alternative location on the same server
3. Starts all Microsoft Exchange Server services
4. Executes an ADSM ARCHIVE on the copies of the database

The ADSM operation was again an archive; however, it ran after the Microsoft Exchange Server database was restarted. Because the two operations are separate, you can schedule them separately. We defined a command file to run NET STOP against all Exchange services, copy the database files to an alternative location, and restart the Exchange services with the NET START commands. We used the same NET STOP and START commands as in the first example but replaced the DSMC ARCHIVE with the following copy commands:

```
COPY C:\EXCHSRVR\DSADATA\*.* E:\DUMPS\DSA\  
COPY C:\EXCHSRVR\MDBDATA\*.* E:\DUMPS\MDB\
```

Note

As in the first example, we did not copy the log files, because that information was committed to the Microsoft Exchange Server database when the Exchange services were stopped.

We then scheduled the command file, EXCHDUMP.CMD, using the Windows NT AT command:

```
AT 01:00AM /EVERY:MONDAY,TUESDAY,WEDNESDAY,THURSDAY,FRIDAY,SATURDAY,  
SUNDAY C:\EXCHDUMP.CMD
```

The AT command schedules commands and programs to run at a specified time and date on the local Windows NT machine. You must enter this command as one line, and the Windows NT Schedule service must be running to use the AT. For more information about the NT AT command, see the Windows NT online help.

Note

In both examples, automating with the ADSM command schedule and backing up database copies, the commands can be placed in a command file and scheduled to run under the ADSM scheduler service, the NT AT command, or any other scheduling mechanism you want to use. The important factor is logging the output for error detection. In both examples we provide some ideas for capturing output or logging error messages.

In our test environment, the least amount of activity on Microsoft Exchange Server was between 01:00 and 04:00, so we scheduled the copy at 01:00 and began the ADSM archives at 02:00, long after the Exchange services have been restarted.

We configured four ADSM ARCHIVE schedules for each of the dump directories. ADSM allows only one object to be configured in an ADSM ARCHIVE, so you have to set up four schedules. You can create a separate command file with the DSMC ARCHIVE commands, as in the first example, and schedule it with an ADSM COMMAND schedule, or even the NT AT command. However, the error logging will not be as centralized as with an ADSM ARCHIVE schedule.

We included several OPTIONS in our schedules:

- VERbose explicitly writes all of the activity to the DSMSCHED.LOG.
- DELetefiles deletes the files from the local disk after archiving them.

If you want to keep a copy on the local disk, and instead remove the files from the previous day, you have to put the appropriate delete commands in the command file before the copy commands.

- DESCription adds the specified description to the archive, so the files are easily identified.

Figure 7 on page 15 is an example of a schedule to archive the Microsoft Exchange Server Directory copy located in the E:\DUMPS\DSA\ directory.


```
adsm> query schedule exch_dom daily_arch_msexch_dir format=detailed
```

```
Policy Domain Name: EXCH_DOM
Schedule Name: DAILY_ARCH_MSEXCH_DIR
Description: One of four daily schedules to archive
              MExchange dumped database
Action: Archive
Options: -ve -del -desc='Daily Archive Directory'
Objects: E:\DUMPS\DSA\*
Priority: 1
Start Date/Time: 08/10/1998 02:00:00
Duration: 1 Hour(s)
Period: 1 Day(s)
Day of Week: Any
Expiration:
Last Update by (administrator): ADMIN
Last Update Date/Time: 08/10/1998 11:16:50
```

Figure 7. ADSM Schedule to Archive Dumped Database Files

We scheduled the other three directories with similar schedules, spacing the start times at 15-min intervals. For more information about setting up ADSM client schedules and scheduling them, see the ADSM Administrator's Guide for your server platform.

2.3 ADSM Online Backup of Microsoft Exchange Server

The ADSMConnect Agent for Microsoft Exchange Server can use the Microsoft API to back up components of the Microsoft Exchange Server without stopping the service. In this section we discuss some issues to consider when you install, set up, or operate the ADSMConnect Agent for Microsoft Exchange Server.

2.3.1 Data Backed Up by ADSMConnect Agent for Microsoft Exchange Server

The ADSMConnect Agent can perform an online backup of:

- The directory service, ..\dsadata\dir.edb
- The transaction logs for the directory service, ..\dsadata*.log
- The private information store, ..\mdbdata\priv.edb
- The public information store, ..\mdbdata\pub.edb
- The transaction logs for the information store, ..\mdbdata*.log

Figure 8 on page 16 shows an overview of Microsoft Exchange Server databases backed up by the ADSMConnect Agent for Microsoft Exchange Server.

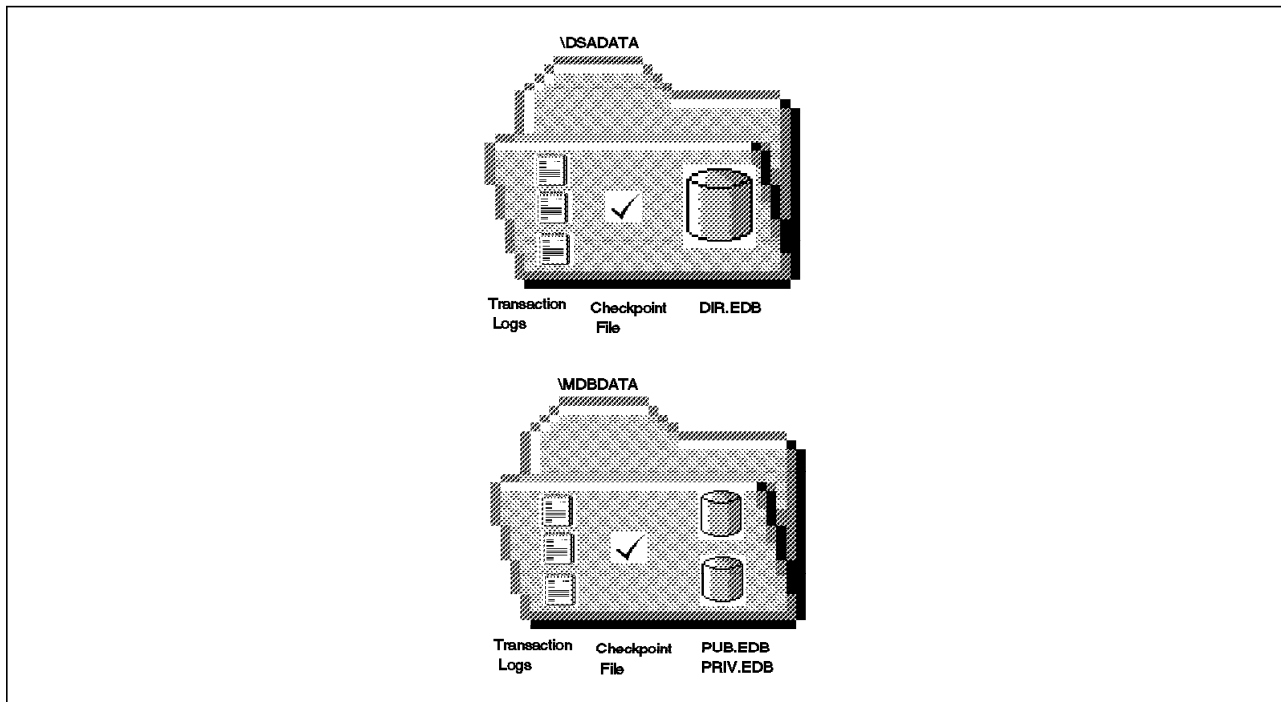


Figure 8. Microsoft Exchange Server Databases

Note

There is one checkfile for the directory and one for the combined information stores. The private and public information stores share the same transactional log files.

2.3.2 Data Not Backed Up by ADSMConnect Agent for Microsoft Exchange Server

The ADSMConnect Agent does not back up files maintained by the Outlook client. The following files must be backed up by the ADSM Windows client:

- PST files
- PAB files
- Archive files (PST)
- FAV files

The ADSMConnect Agent does not back up files or configuration data for the following Microsoft Exchange Server services:

- Microsoft Exchange Server Key Management Service files
- All Microsoft Exchange Server message connector configurations, including the Internet Mail Connector.

The Microsoft Exchange Server Key Management Service requires a backup to be made when the service is stopped. We describe a method of backing up the Internet Mail Connector configuration in 3.4, "Microsoft Exchange Server Disaster Recovery Planning" on page 71.

The following files are not backed up or restored by the ADSMConnect Agent, they are re-created by the Exchange services after a restore:

- The checkpoint file for directory service, `..\dsadata*.chk`
- The checkpoint file for the information store, `..\mdbdata*.chk`

2.3.3 Defining the Location of Files Maintained by the Outlook Client

A Microsoft Windows mail profile is built from the settings in the mail and fax icon on the control panel.

Figure 9 shows the GUI to the Microsoft Windows mail profile after you open the mail and fax icon on the control panel.

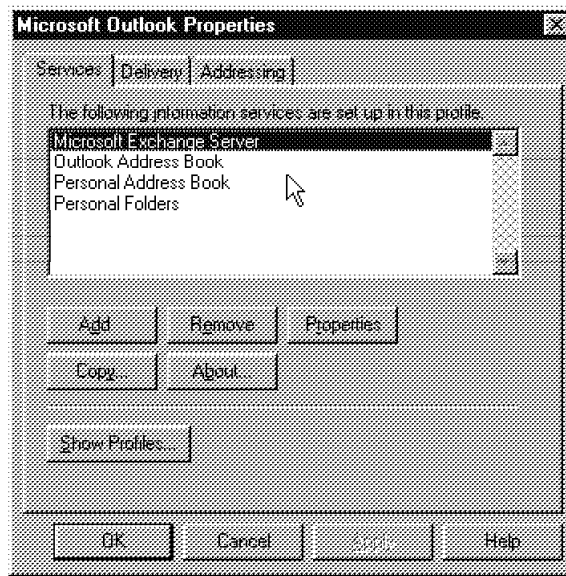


Figure 9. Microsoft Windows Mail Profile

Every user requires a mail profile for connection to Microsoft Exchange Server. You can automate the creation of the mail profile with the `newprof.exe` program and the `outlook.prf` configuration file. By creating an `outlook.prf` for all users connected to your Microsoft Exchange Server, you can define a standard operating environment for the Outlook client. With the `outlook.prf` file you can define numerous Outlook client configuration options. Here is an example of the property values in `outlook.prf` that enable you to control the location of Outlook client data files:

- `DefaultArchiveFile=h:\outlook\archive.pst`
- `OfflineFolderPath=c:\outlook\offline.ost`
- `PathToPersonalFolders=h:\outlook\perstore.pst`
- `PathToPersonalAddressBook=h:\outlook\peradd.pab`

For each of the above property values there is a corresponding property type that must match. For more information about creating and editing the `outlook.prf` files refer to Microsoft Knowledge base article Q172073.

After you have created a customized `outlook.prf` files you can use it with the `newprof.exe` program to generate the Microsoft Windows mail profile, as in this example:

```
c:\program files\windows messaging\newprof.exe -p c:\winnt\outlook.prf -s  
-x -z
```

For more information about the use of newprof.exe, refer to Microsoft Knowledge base article Q145905.

The location of the Outlook FAV file is configured within the Windows NT registry for each user. For more information about configuring the location of the FAV file, refer to Microsoft Knowledge base article Q167397.

2.3.4 Supported Environments

- Hardware
 - Intel 486 or higher
 - 32 MB of memory or higher; at least 64 MB recommended
 - At least 8 MB of free disk space
- Operating Systems
 - Microsoft Windows NT 3.51
 - Microsoft Windows NT 4.0
 - We recommend that you apply the latest Microsoft Windows NT service packs.
- Communication protocols
 - TCP/IP
 - IPX/SPX
 - NetBIOS
 - Named Pipes
- Microsoft Exchange Servers
 - 4.0
 - 5.0
 - 5.5
- ADSM Server Versions
 - Version 2
 - Version 3
- ADSMConnect scheduling
 - V2 Baclient
 - V3 Baclient

2.3.5 Microsoft Exchange Server Database Transaction Logs

The Microsoft Exchange Server, like most database-based applications, uses transaction logs to hold uncommitted data or data that has not been written to the database. After data is committed to the database, the checkpoint is advanced in the transaction log to identify committed and uncommitted data. Incremental and differential backups can be done any time after a full backup by backing up the transaction log (see Figure 10 on page 19). Thus any updates to the database since the last full backup can be captured by using the

uncommitted portion of the transaction log. The ADSMConnect Agent for Microsoft Exchange Server uses incremental backups and full database backups to restore the database to a point in time equivalent to the last incremental backup. The ADSMConnect Agent for Microsoft Exchange Server can store multiple point-in-time full and incremental backups of the database.

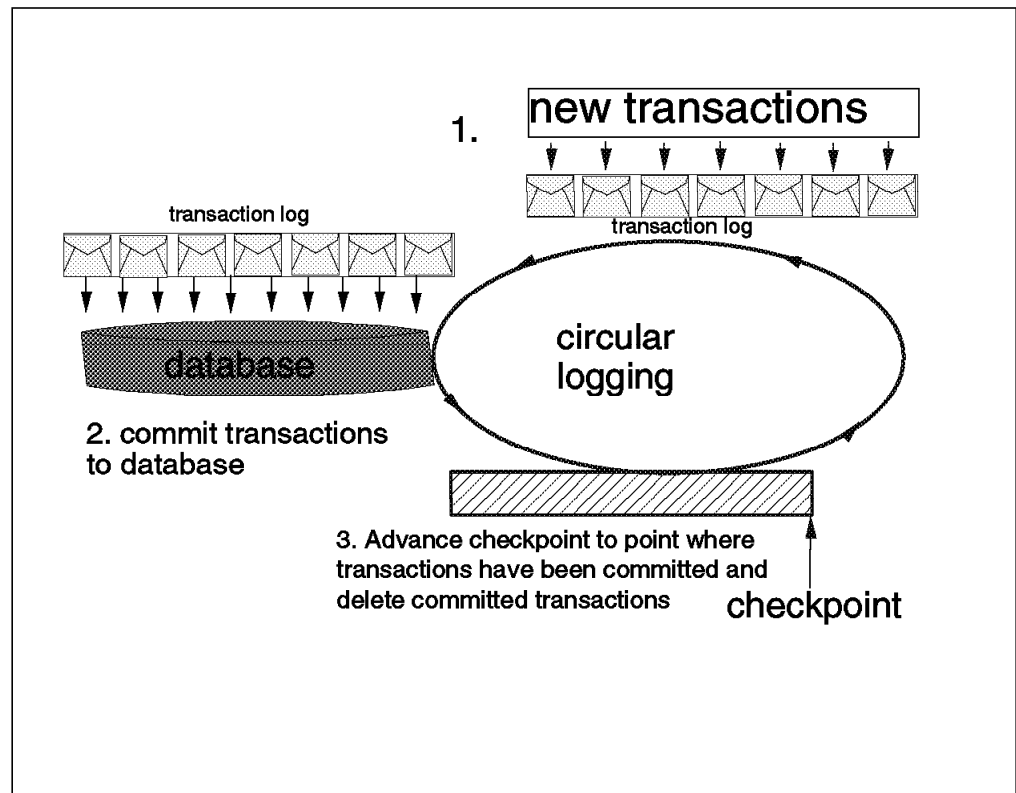


Figure 10. Transaction Log Processing

2.3.5.1 Microsoft Exchange Server Circular Logging

With Microsoft Exchange Server you can use circular logging (see Figure 11 on page 20), which deletes the committed portion of the transaction log up to the checkpoint and thus helps to keep the size of the transaction log small.

Note

Because the committed portion of the transaction log is no longer available, incremental or differential backups cannot be done, only full backups. Keep in mind that full database backups take more time and can increase network and server resource utilization. These factors determine the frequency of full backups and the currency of data recovery.

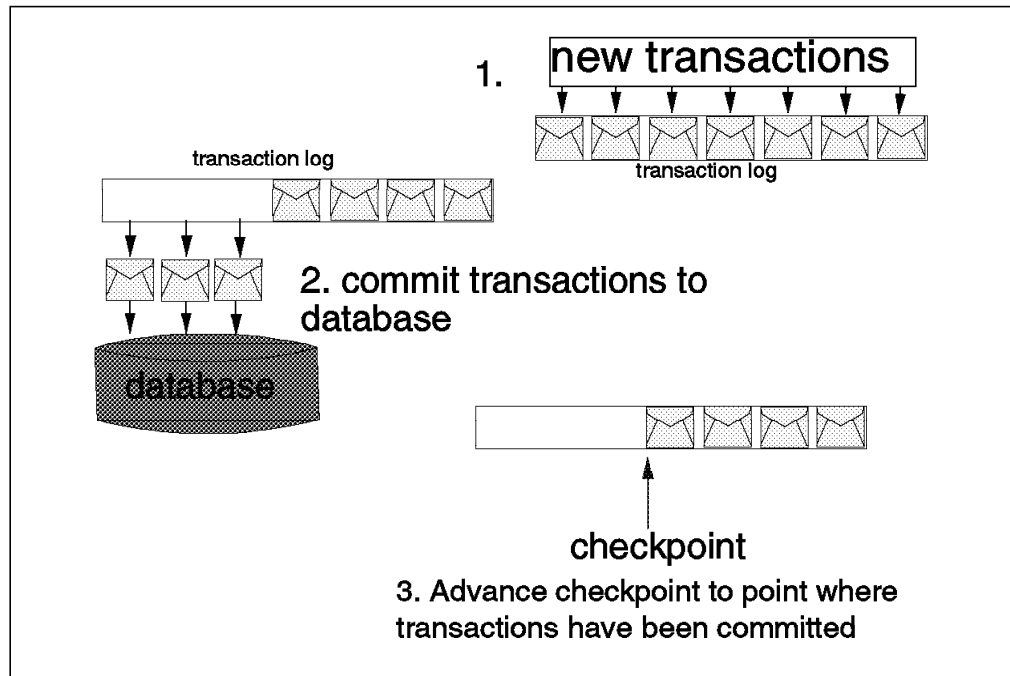


Figure 11. Circular Logging

Circular logging is enabled by default. To determine the status of circular logging on the Microsoft Exchange Server, go to the Properties window and click on the **Advanced** tab as shown in Figure 12 on page 21. You can also determine the status of circular logging through the ADSMConnect Agent for Microsoft Exchange Server. After you start the ADSMConnect Agent for Microsoft Exchange Server and select the database, the status of circular logging is displayed. In addition, if circular logging is enabled, as shown in Figure 13 on page 22, the incremental and differential options are grayed out.

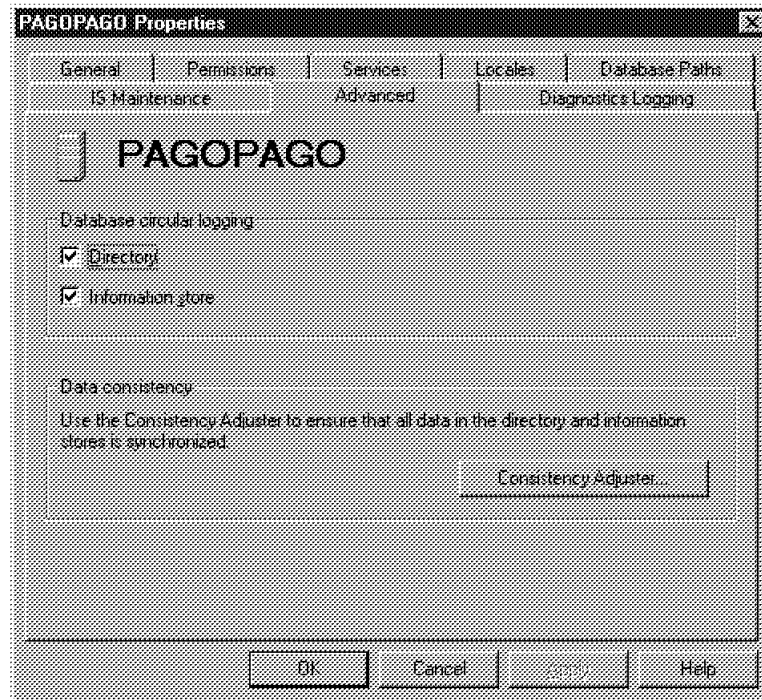


Figure 12. Circular Logging Settings

Recommendation

We recommend that you change circular logging from the default of enabled to *disabled* to allow incremental and differential backups, which take less time and reduce network and server resource utilization. Disabling Circular logging also allows for more frequent backups, thereby providing a more up-to-date recovery capability.

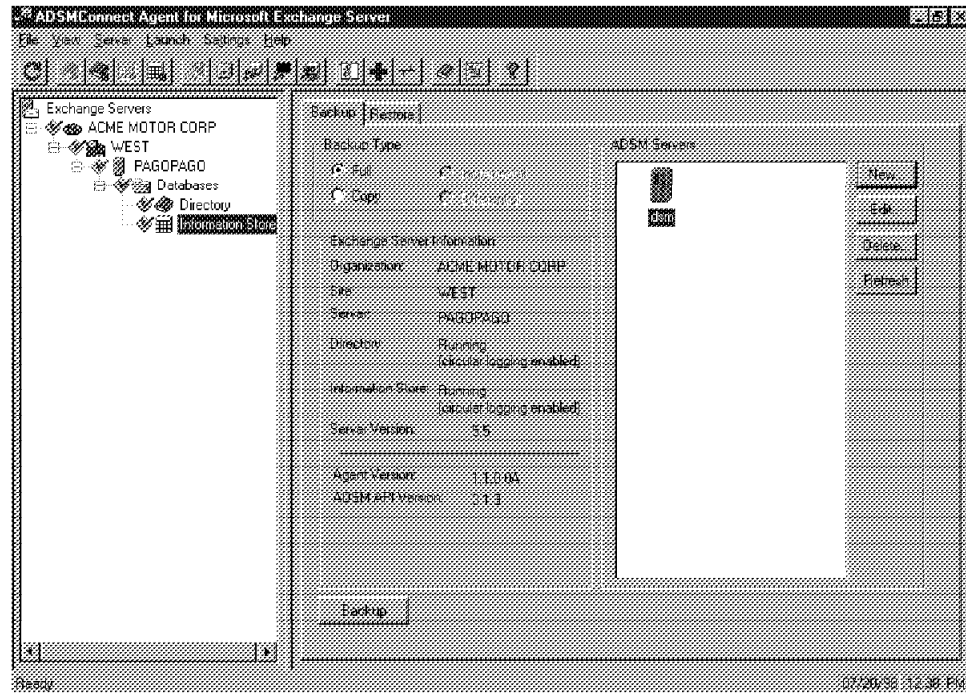


Figure 13. Circular Logging Status

2.3.6 ADSM Management Class

Once you have installed the ADSMConnect Agent for Microsoft Exchange Server and configured the ADSMConnect Agent `dsm.opt` file to communicate with the ADSM server, be sure that the ADSMConnect Agent, which is also an ADSM client, is registered with the ADSM server. See the *ADSTAR Distributed Storage Manager: ADSMConnect Agent for Microsoft Exchange Server Installation and User's Guide* (SH26-4071).

The *ADSMConnect Agent Installation and User's Guide* recommends a separate ADSM management class, because certain requirements for the ADSMConnect Agent for Microsoft Exchange Server are likely different from those for most ADSM clients. We created a separate ADSM domain for the Microsoft Exchange Servers in our environment. By keeping the servers in a separate ADSM domain from other clients, we could leave one default management class in place for all servers. Later, we found it necessary to define a different destination storage pool for a single, new Exchange server. We added another ADSM management class, `EXCH_MC_TAPE`, to the existing ADSM Exchange policy domain and specified the new management class at the bottom of the `dsm.opt` file for that Exchange ADSM node:

```
Include * EXCH_MC_TAPE
```

We used the default values for the ADSM backup copy group definitions and specified a tape device in the destination storage pool. If you require the Microsoft Exchange Servers to remain in an existing ADSM domain, simply add a management class, as we did in the above example, and specify it in all of the Exchange ADSM client `dsm.opt` files.

For an example of how to add a management class to an existing policy domain and policy set, see Appendix C, “Adding a New ADSM Management Class” on page 81. The example uses the ADSM administrative GUI, which is supplied with the ADSM backup/archive client for Windows NT Version 3.

Because the ADSMConnect Agent does not use an archive copy group, we did not define one. Be aware that if you do not define an archive copy group, the ADSM server generates a warning message when you validate and activate the policy set:

```
ANR1554W DEFAULT Management class EXCH_MC in policy set
EXCH_DOM EXCH_POL does not have an ARCHIVE copygroup: files will not
be archived by default if this set is activated.
```

In addition, because the ADSMConnect Agent does not use most of the parameters in the backup copy group, we left all of them at the defaults, except for VERDELETED and the Destination Storage Pool. You must set VERDELETED to zero, so that the objects backed up by the ADSMConnect Agent will be marked inactive and deleted when they are meant to be deleted by the ADSMConnect Agent delete function. *The ADSTAR Distributed Storage Manager: ADSMConnect Agent for Microsoft Exchange Server Installation and User's Guide* lists the management class parameters, which are unnecessary for the ADSMConnect Agent, and provides more explanation about the VERDELETED parameter and deletion. Figure 14 shows the backup copy group properties for EXCH_MC_TAPE. Note that the VERDELETED option is referred to as “If client data is deleted” in the GUI.

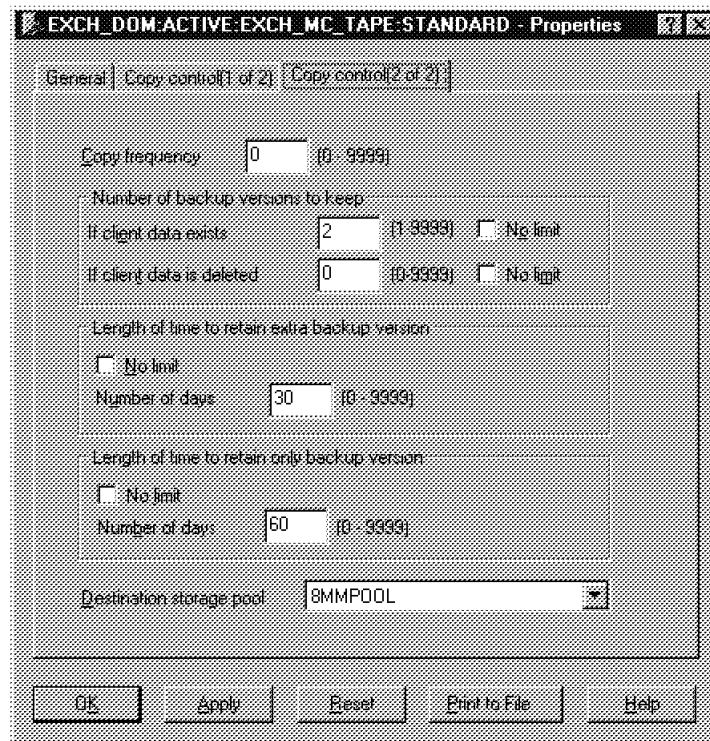


Figure 14. ADSM Backup Copy Group Properties

2.3.7 Microsoft Exchange Server Information Store Maintenance

For database efficiency the Microsoft Exchange Server performs scheduled online maintenance tasks, including deleting public folder messages and cleaning up indexes that exhibit a poor locality of reference on the information store. During scheduled maintenance, information store response could be affected. With this in mind, consider scheduling the maintenance tasks during periods of low activity. You can access the information store maintenance schedule through the Server Properties IS Maintenance tab (see Figure 15).

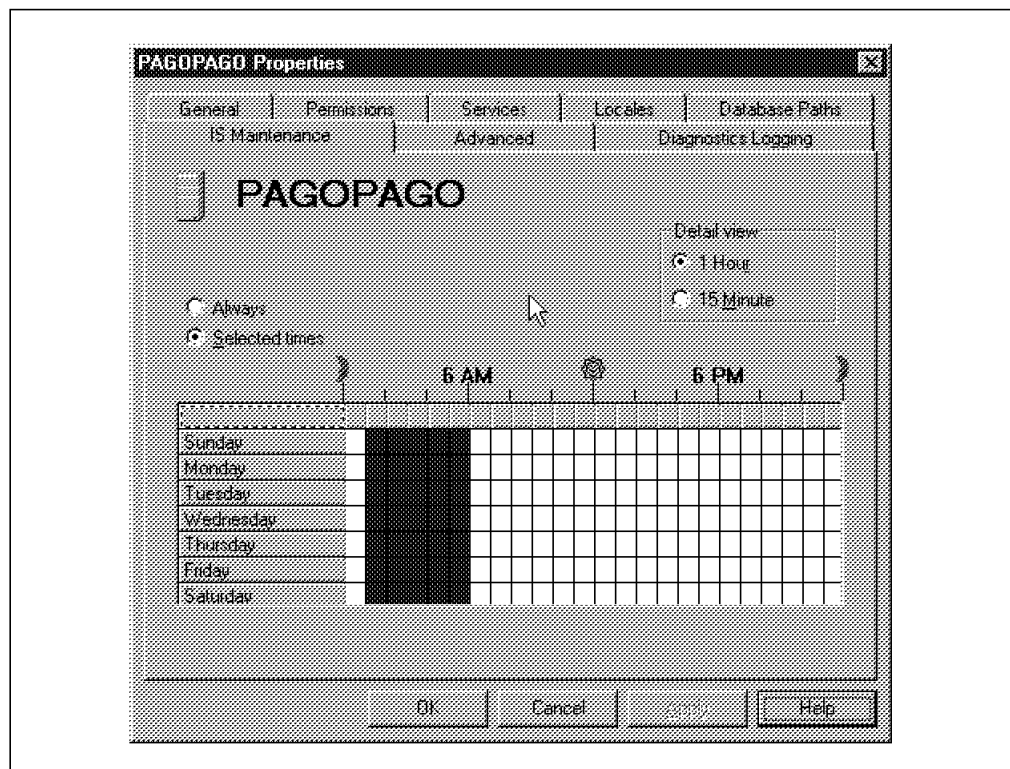


Figure 15. IS Maintenance Properties

Note

Selecting **Always** on the Server Properties window will invoke information store maintenance every 15 min and could affect the performance of the Microsoft Exchange Server and ADSMConnect Agent for Microsoft Exchange Server. Use the **Selected Times** checkbox instead and define a schedule.

Recommendation

Do not define the information store maintenance schedule to coincide or overlap with the ADSM backup client or ADSMConnect Agent for Microsoft Exchange Server schedules.

2.3.8 Client Options File Recommendations

In this section we cover some of the client options file entries that will affect the performance or operation of the ADSMConnect Agent for Microsoft Exchange Server.

2.3.8.1 *.OPT File

The default client options file for the ADSMConnect Agent for Microsoft Exchange Server is dsm.opt. You create several option files with the file type of .OPT to facilitate different ADSM servers or different options. You can specify which options file to use through the ADSMConnect Agent for Microsoft Exchange Server GUI, the command line, or the command file used with the ADSM scheduler. In our environment we used WINNT.OPT for the Windows NT ADSM server and AIX.OPT for the AIX ADSM server. Keep in mind that the ADSM API always reads the dsm.opt. Therefore any options appearing in dsm.opt file that do not appear in the Exchange Agent options file will be in effect.

2.3.8.2 TCPWindowSize

If you specified a COMMMethod of TCP/IP, the TCPWindowSize option specifies the size of the TCP sliding window for your client. A large window size can improve communication performance but uses more memory. It enables frames to be sent before an acknowledgment is received. If you observe transmission delays, increasing the TCPWindowSize may increase throughput.

Recommendation

TCPWindowSize 64

2.3.8.3 TCPBufsize

If you specified a COMMMethod of TCP/IP, use the TCPBufsize option to specify the size of the ADSM buffer that the ADSM API uses to transfer data to and from TCP/IP. A large buffer can improve communication performance but requires more memory.

Recommendation

TCPBufsize 32

2.3.8.4 TCPCLIENTAddress

If you use server-prompted scheduling you must specify TCPCLIENTAddress for the ADSMConnect Agent for Microsoft Exchange Server. If you use more than one scheduler service, as we recommend, use the same TCPCLIENTADDRESS in both the Windows NT backup client and the ADSMConnect Agent for Microsoft Exchange Server options files:

```
tcpclienta adsm.sanjose.ibm.com
```

2.3.8.5 TCPCLIENTPort

If you use server-prompted scheduling, you must specify TCPCLIENTPort for the ADSMConnect Agent for Microsoft Exchange Server. If you use more than one scheduler service, as we recommend, then you should use different values for TCPCLIENTPort in both the Windows NT backup client and the ADSMConnect Agent for Microsoft Exchange Server options files:

```
tcpclientp 1502
```

Note

Server-prompted scheduling is supported only with TCP/IP communication. By default the ADSMConnect Agent for Microsoft Exchange Server uses the client polling schedule mode.

2.3.8.6 NodeName

If you have installed the ADSM backup client for Microsoft Windows NT to back up your operating system and applications, we recommend that you specify a NodeName in the ADSMConnect Agent for Microsoft Exchange Server client options file that is different from the NodeName specified in the ADSM Windows backup client options file. Specifying a separate NodeName has the following benefits:

- Eases central scheduling tasks
- Allows customization of policy domain and management class specific to Microsoft Exchange Server nodes
- Separates Microsoft Exchange Server backup data from file backup data

2.3.8.7 COMPRESSION

The COMPRESSION option is valid only if the ADSM administrator allows the node to decide whether or not compression should be used (see Figure 16 on page 27). Some considerations for the use of the COMPRESSION option are:

- Reduced ADSM server storage pool space
- Reduced network utilization
- Increased ADSM client CPU utilization
- Increased ADSM client memory utilization

Recommendation

We recommend that you avoid using compression if possible. Although compression reduces ADSM server storage pool space and network utilization, it generally reduces client throughput.

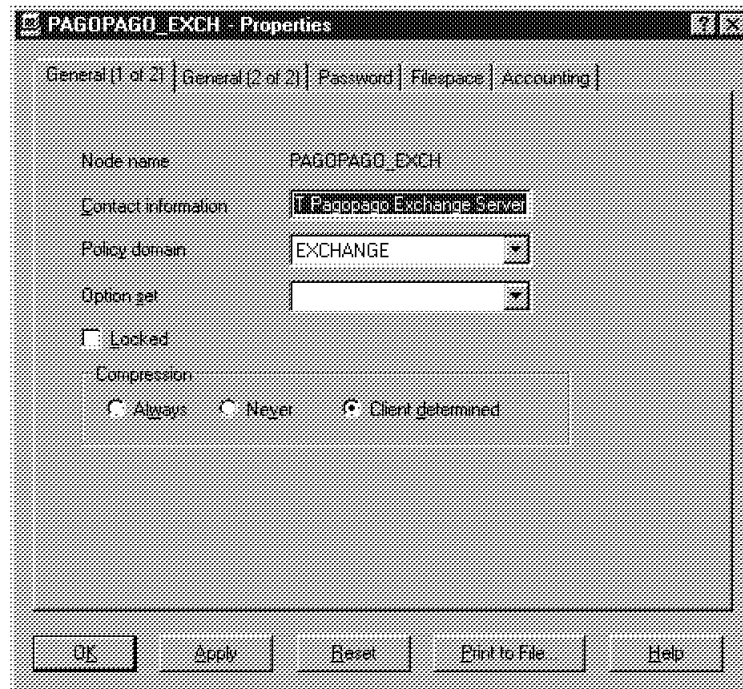


Figure 16. Node Properties

2.3.8.8 PASSWORDAccess Generate

We recommend that you use PASSWORDAccess Generate for the ADSMConnect Agent for Microsoft Exchange Server to facilitate unattended operations. You have to register the ADSMConnect Agent for Microsoft Exchange Server nodename and provide an initial password. During the initial connection, you are prompted to provide the password. After the initial logon, the current password is encrypted in the Windows NT registry (see Figure 17 on page 28) so that authentication occurs without intervention. In addition, a new password is generated and encrypted automatically when the ADSM server expires the current password.

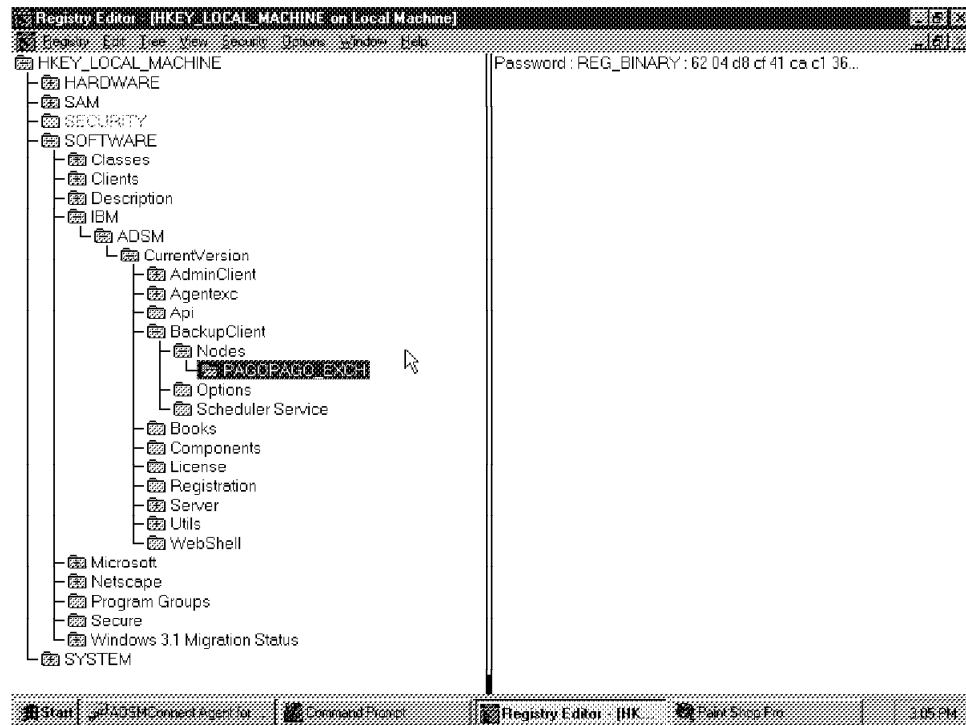


Figure 17. ADSM Node Registry Entry

2.3.8.9 *EXC_MOUNTWait

The *EXC_MOUNTWait option controls whether the ADSMConnect Agent for Microsoft Exchange Server waits for tape mount requests to be resolved on the ADSM server or terminates the current operation when the ADSM server indicates that it will have to wait for a tape mount in order to complete the operation. During a backup operation, ADSM might issue a prompt to place a tape volume in a drive. Also, during a restore operation, the data you want to recover might be on a tape not currently mounted by the server. In this case, an ADSM operator or autochanger must take time to mount the particular tape. During that time, the ADSMConnect Agent for Microsoft Exchange Server continues to show activity and wait for an ADSM server operation to complete. If you specify *EXC_MOUNTWait YES, the ADSMConnect Agent for Microsoft Exchange Server waits for a tape to be mounted before it continues. If you do not specify this option, the operation ends. The EXC_MOUNTWait option is preceded by an asterisk (*) because it is a unique option of the ADSMConnect Agent for Microsoft Exchange Server, and the asterisk allows it to be ignored by the ADSM API but recognized by the ADSMConnect Agent for Microsoft Exchange Server.

Recommendation

We recommend that you specify a value of yes for the *EXC_MOUNTWait option.

2.3.8.10 TAPEPROMPT

*EXC_MOUNTWait requires TAPEPROMPT YES. In order for the

*EXC_MOUNTWait option to be honored, the ADSM TAPEPROMPT option must be set to yes in the client options file. By default the TAPEPROMPT setting is set to yes. If TAPEPROMPT is changed to no, the *EXC_MOUNTWait parameter will have no effect. The ADSM API will always wait for a media mount.

2.3.8.11 Sample Client Options File

In our test environment we used the options file shown in Figure 18.

COMMMethod	TCPip
TCPPort	1500
TCPServeraddress	kindu
TCPWindowSize	64
tcpbuffsize	32
txnbytelimit	25600
NODename	pagopago_exch
COMPRESSION	Off
PASSWORDAccess	Generate
TAPEPrompt	Yes
SCHEDMODE	Prompted
TCPCLIENTPORT	1502
*EXC_MOUNTWait	Yes

Figure 18. Sample Client Options File

2.3.9 Performance Settings

The Exchange Agent is a multithreaded application that uses asynchronous execution threads to transfer data between the ADSM API and the Microsoft Exchange Server. Multiple data buffers are used to allow one thread to send or receive data on the ADSM API and another thread to send or receive data on the Microsoft Exchange Server simultaneously (see Figure 19 on page 30).

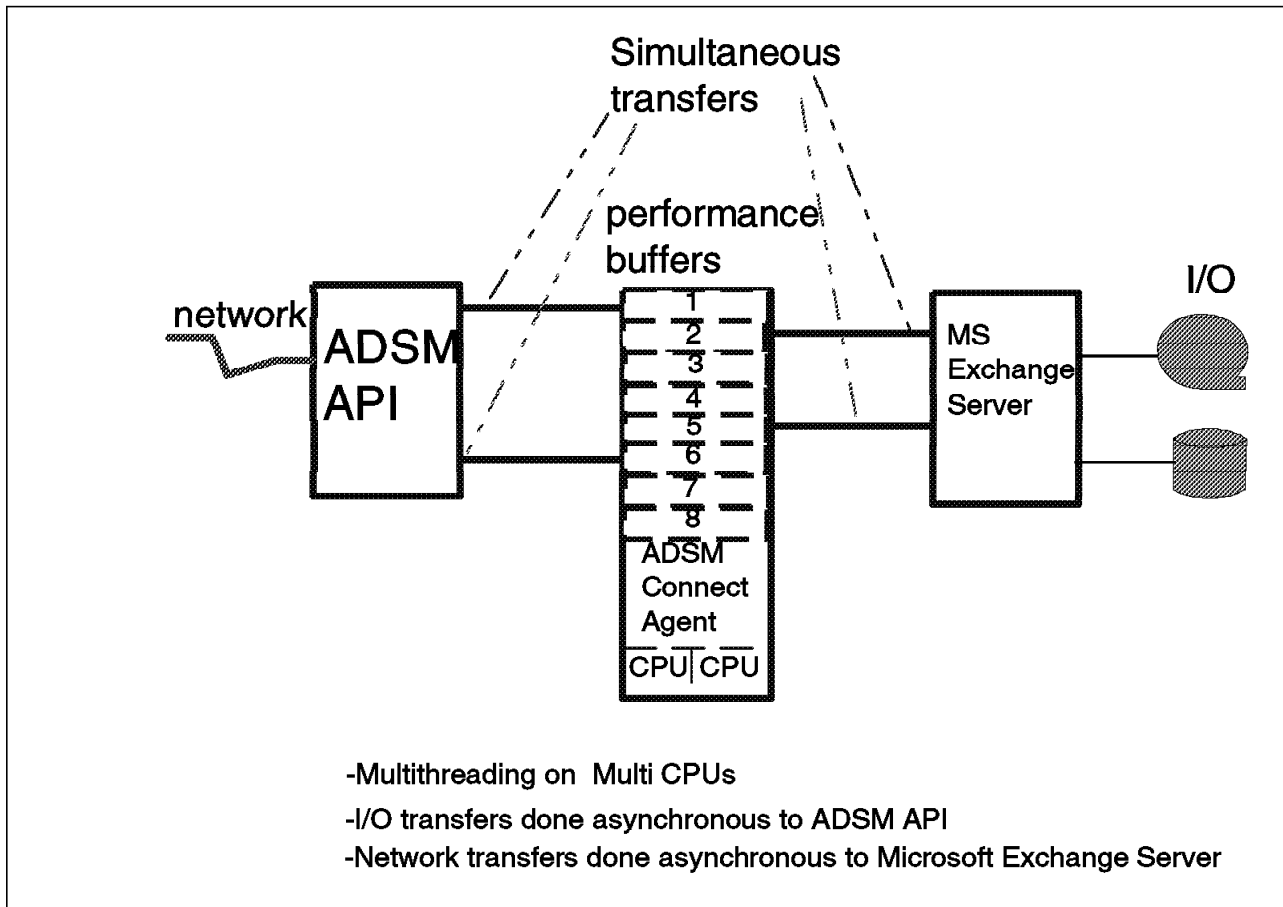


Figure 19. Performance Buffers

You specify the number of buffers that can be configured through the Exchange Agent Settings dialog (see Figure 20).

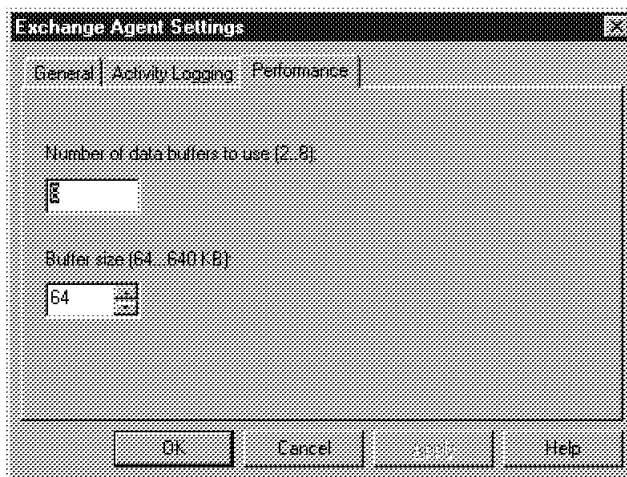
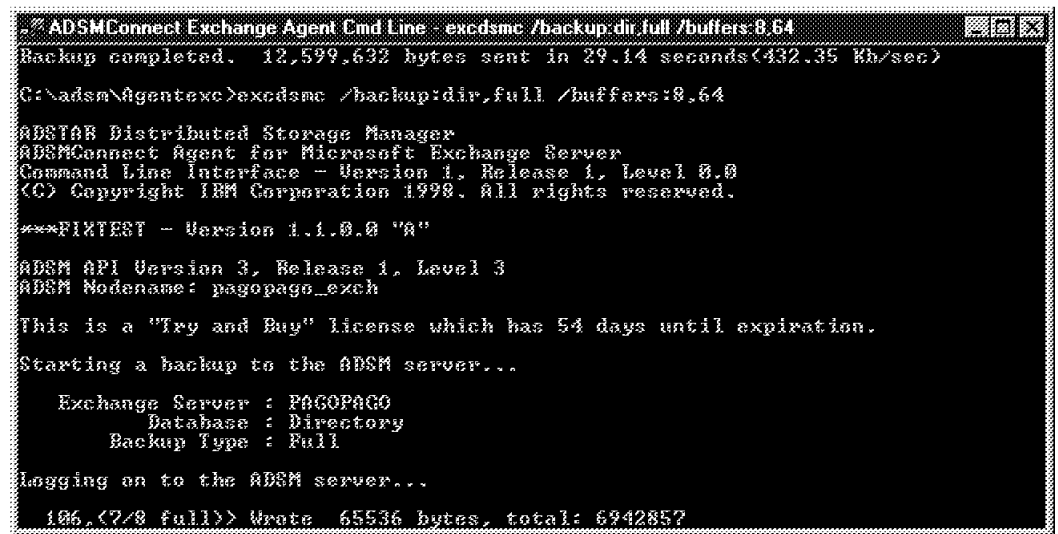


Figure 20. Exchange Agent Settings: Performance

The asynchronous operations allow both the ADSM API and Microsoft Exchange Server to transfer at an optimum rate without delaying one another. The buffers help mitigate some of the limiting factors in data throughput, such as communication and media wait. If multiprocessors are available, the ADSMConnect Agent for Microsoft Exchange Server can maximize its multithreading capability and perform simultaneous thread execution on multiple processors. You can see the number of buffers in use during a restore while operating from the command line (see Figure 21). The default setting is 2.

Recommendation

We recommend that you specify a value greater than 2 for the number of data buffers to use.



```
ADSMBConnect Exchange Agent Cmd Line - excdsmc /backup:dir,full /buffers:8,64
Backup completed. 12,599,632 bytes sent in 29.14 seconds(432.35 Kb/sec)
C:\adsm\Agentexc>excdsmc /backup:dir,full /buffers:8,64
ADSTAR Distributed Storage Manager
ADSMConnect Agent for Microsoft Exchange Server
Command Line Interface - Version 1, Release 1, Level 0.0
(C) Copyright IBM Corporation 1998. All rights reserved.
***FIXTEST - Version 1.1.0.0 "A"
ADSM API Version 3, Release 1, Level 3
ADSM NodeName: pagopago_exch
This is a "Try and Buy" license which has 54 days until expiration.
Starting a backup to the ADSM server...
    Exchange Server : PAGOPAGO
      Database : Directory
    Backup Type : Full
Logging on to the ADSM server...
106,(7/8 full)>> Wrote 65536 bytes, total: 6942857
```

Figure 21. Command Line Example: Buffer Utilization

You also set the buffer size in the Exchange Agent Settings dialog (see Figure 20 on page 30). The default setting of 64 is optimal for most installations, but some installations may benefit by increasing this value. Test the buffer size value in your own environment to determine what is best for your installation.

2.3.10 Capacity Planning

Our Performance Evaluation Laboratory has determined that throughput over a network can be expected to reach saturation at around 80% of its rated capacity. Thus the following are rule-of-thumb throughput maximums that can be obtained for given a network:

4 mb Token ring - 0.4 MB/sec	1.4 GB/hr
10 mb Ethernet - 1.0 MB/sec	3.4 GB/Hr
16 mb Token ring - 1.6 MB/sec	5.5 GB/Hr
25 mb ATM - 2.5 MB/sec	8.6 GB/Hr
100 mb Ethernet - 10.0 MB/sec	34 GB/Hr
100 mb FDDI - 10.0 MB/sec	34 GB/Hr
155 mb ATM - 15.5 MB/sec	53 GB/Hr

The throughput maximums give you a starting point to work *Down* from when you try to estimate the elapsed time for backups or restores. Some of the factors that reduce the ability to transfer data at maximum throughput are:

- Network traffic or load
- Network delay due to routers or switches
- Exchange Server resource utilization
- ADSM server application overhead
- ADSMConnect Agent for Microsoft Exchange Server and ADSM API application overhead
- Media wait
- Resource utilization on the ADSM server
 - CPU
 - memory
 - Disk
- Resource utilization on the ADSMConnect Agent for Microsoft Exchange Server and ADSM API
 - CPU
 - memory
 - Disk

To determine your network and resource capabilities, create a large test file over 50 MB. Transfer this file to the ADSM server and document elapsed time and kilobytes per second. Transfer the same file from the ADSM server to the Windows NT machine and document elapsed time and kilobytes per second. Convert kilobytes per second to gigabytes per hour with the following formula:

$$\text{Throughput(GB/hr)} = \text{Throughput(KB/sec)} * (3600 / 1048576)$$

These measurements should be done several times for validation. They will give you an estimate of your data transfer capabilities, excluding the overhead of the ADSM server application, ADSMConnect Agent for Microsoft Exchange Server, Exchange Server activity, and the ADSM API.

2.3.11 Detecting Performance Bottlenecks

After successful setup and operation of the ADSMConnect Agent for Microsoft Exchange Server, often the next step is to determine service requirements such as backing up data within the specified backup window or restoring within a specified time. To meet these service requirements you must identify performance bottlenecks for resolution.

2.3.11.1 Windows NT Performance Monitor

If the elapsed time of your backups and restores is not as expected, you can use the Windows NT Performance monitor (see Figure 22) to determine whether the problem exists within the Windows NT server and its resources.

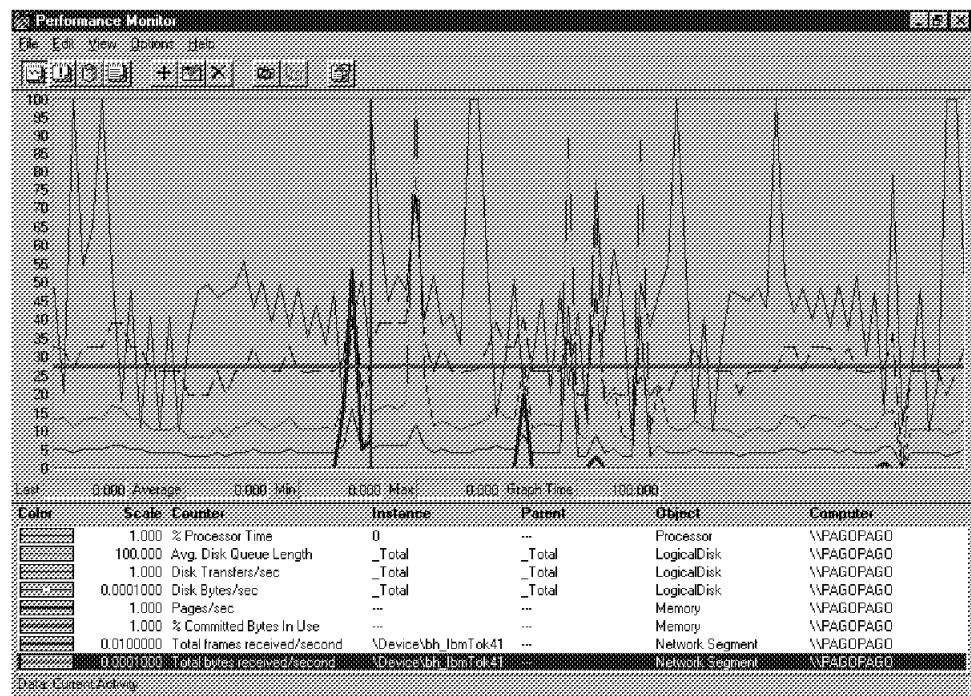


Figure 22. Windows NT Performance Monitor

2.3.11.2 ADSM Server dsmacnt.log File

When accounting is set to on, the server creates a session resource usage accounting record whenever a client node session ends. At installation accounting is set to off. You can set accounting to on by entering the following on the ADSM administrative command line:

```
set accounting on
```

For ADSM servers excluding MVS and AS/400, accounting records are stored in the dsmacnt.log file in the directory from which the server is started. (For MVS and AS/400 see the respective administrative reference manuals for the location

of the accounting records.) The dsmacnt.log file contains accounting records that can be viewed directly or read into a spreadsheet program (see Figure 23 on page 34).

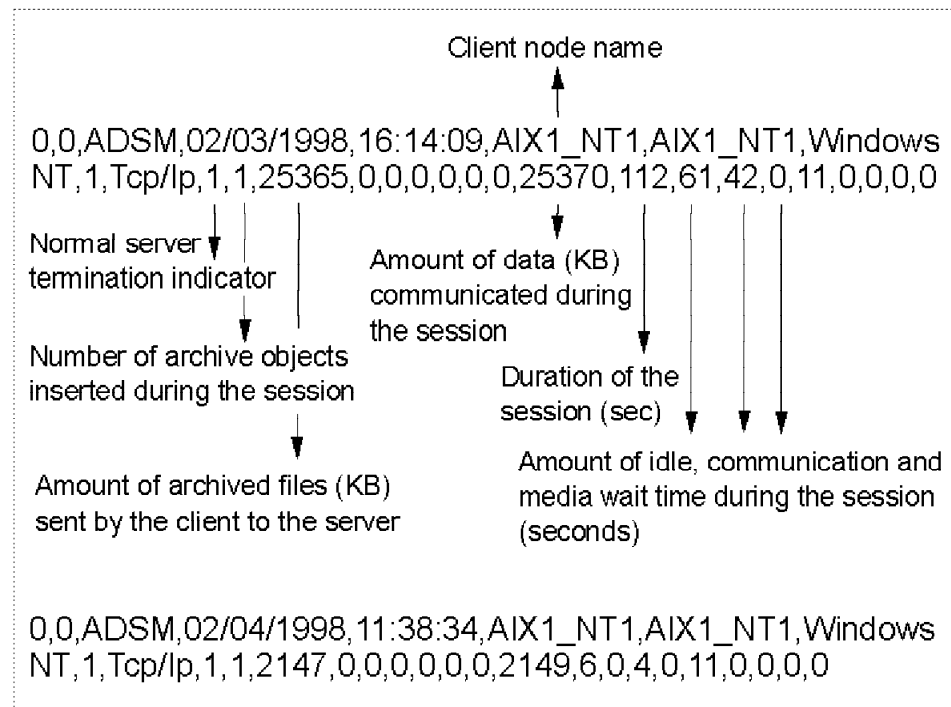


Figure 23. dsmacnt.log File Accounting Record

The dsmacnt.log file remains open while the server is running and accounting is set to on. It continues to grow until you delete it or prune old records from it. To close the file for pruning, either temporarily set accounting to off from the ADSM administrative command line or halt the server.

The dsmacnt.log provides an ADSM server perspective in determining what is occurring between the ADSM server and ADSM client. The accounting records indicate whether the delays are outboard on the ADSM client or network or inboard on the ASDM server.

The key fields in the accounting record are:

Field Description

- 20 Amount of data, in kilobytes, communicated between the client node and the ADSM server during the session
- 21 Duration of the session, in seconds
- 22 Amount of idle wait time in seconds during the session, when the server was idle waiting for a request from the client. An excessive value indicates a problem in the client.
- 23 Amount of communications wait time in seconds during the session when the server was waiting to receive expected data from the client or waiting for the communication layer to accept data to be

sent to the client. An excessive value indicates a problem in the communication layer or the ADSM client.

- 24 Amount of media wait time in seconds during the session when the server was waiting for removable volumes to be mounted.

Using the above fields, you can determine the:

- Aggregate throughput rate in kilobytes per second = field 20 / field 2
- Network throughput in kilobytes per second = field 20 / (field 21 - (field 22 + field 23 + field 24)).

If elapsed time is a concern and no delays are indicated in the media wait, communication wait, or idle wait, investigate the ADSM server and its resources for any bottlenecks.

2.3.11.3 DSMSCHED.LOG or EXCSCHED.LOG

You can use the DSMSCHED.LOG or EXCSCHED.LOG located on the client to determine the data throughput when a schedule is used (Figure 24). The total number of bytes transferred, elapsed time, and kilobytes per second for scheduled sessions are logged.

```
ADSTAR Distributed Storage Manager
ADSMConnect Agent for Microsoft Exchange Server
Command Line Interface - Version 1, Release 1, Level 0.0
(C) Copyright IBM Corporation 1998. All rights reserved.
***FIXTEST - Version 1.1.0.0 "A"
ADSM API Version 3, Release 1, Level 3
ADSM Nodename: pagopago_exch
Starting a backup to the ADSM server...
  Exchange Server : PAGOPAGO
    Database : Directory
    Backup Type : Incremental
Logging on to the ADSM server...
  1,(1/2 full)> Wrote 61543 bytes, total: 61543
  2,(1/2 full)> Wrote 65536 bytes, total: 127079
  3,(1/2 full)> Wrote 65536 bytes, total: 192615
  .
  .
161,(1/2 full)> Wrote 8192 bytes, total: 10485925
162,(1/2 full)> Wrote 0 bytes, total: 10485925
163,(0/2 full)> Wrote 0 bytes, total: 10485925
```

Figure 24. EXCSCHED.LOG

2.3.11.4 ADSMConnect Agent for Microsoft Exchange Server GUI

If you are doing manual backups or restores from the ADSM GUI client, the number of bytes transferred and elapsed time are displayed at completion (see Figure 25). You can calculate the throughput by dividing kilobytes by elapsed time.

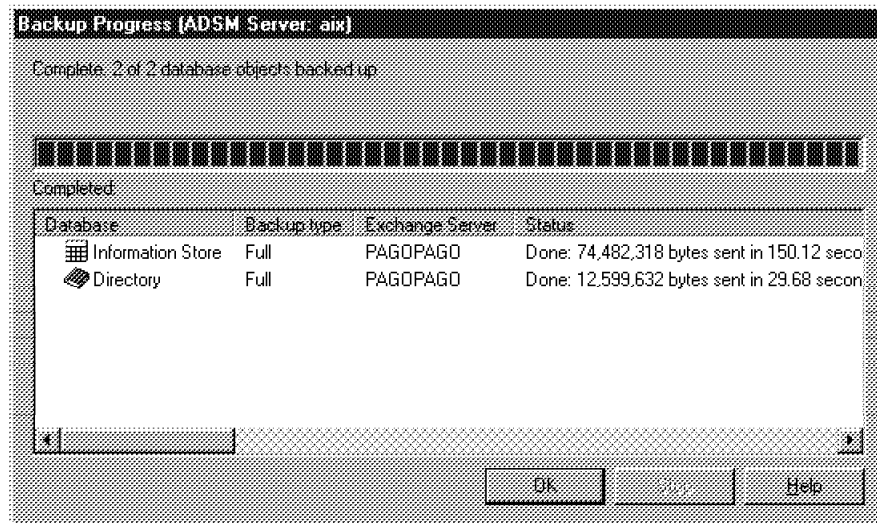


Figure 25. ADSMConnect Agent for Microsoft Exchange Server GUI

2.3.11.5 ADSMConnect Agent for Microsoft Exchange Server Command Line

After you execute a restore or backup from the command line:

```
excdsmc /backup:dir,full /quiet
```

the total number of bytes transferred, elapsed time, and kilobytes per second for the session are displayed (see Figure 24 on page 35).

2.3.11.6 Database Queries

Although the ADSM database does not keep historical information similar to the accounting records, it does keep information for the last session for each node. You can display this information in one of two ways from the command line:

```
Q Node Nodename f=d
```

seeFigure 26 on page 37

```

adsm> q node pagopago_exch f=d

Node Name: PAGOPAGO_EXCH
Platform: WinNTDB
Client OS Level: 4.00
Client Version: Version 3, Release 1, Level 0.3
Policy Domain Name: STANDARD
Last Access Date/Time: 08/11/1998 13:48:50
Days Since Last Access: <1
Password Set Date/Time: 08/11/1998 13:44:22
Days Since Password Set: <1
Invalid Sign-on Count: 0
Locked?: No
Contact: adsm
Compression: Client's Choice
Archive Delete Allowed?: Yes
Backup Delete Allowed?: Yes
Registration Date/Time: 07/21/1998 14:05:00
Registering Administrator: ADMIN
Last Communication Method Used: Tcp/Ip
Bytes Received Last Session: 85.07 M
Bytes Sent Last Session: 2,776
Duration of Last Session (sec): 140.00
Pct. Idle Wait Last Session: 5.00
Pct. Comm. Wait Last Session: 27.86
Pct. Media Wait Last Session: 0.00
Optionset:
URL:
Node Type: Client

```

Figure 26. Query Node Example

```
select * from nodes where node_name='NODENAME'
```

See Figure 27 on page 38

```

adsm> select * from nodes where node_name='PAGOPAGO_EXCH'

      NODE_NAME: PAGOPAGO_EXCH
      PLATFORM_NAME: WinNTDB
      DOMAIN_NAME: STANDARD
      PWSET_TIME: 1998-08-11 13:44:22.000000
      INVALID_PW_COUNT: 0
      CONTACT: adsm
      COMPRESSION: CLIENT
      ARCHDELETE: YES
      BACKDELETE: YES
      LOCKED: NO
      LASTACC_TIME: 1998-08-11 13:48:50.000000
      REG_TIME: 1998-07-21 14:05:00.000000
      REG_ADMIN: ADMIN
      LASTSESS_COMMETH: Tcp/Ip
      LASTSESS_RECVD: 89197220
      LASTSESS_SENT: 2776
      LASTSESS_DURATION: 140000
      LASTSESS_IDLEWAIT: 7000
      LASTSESS_COMMWAIT: 39000
      LASTSESS_MEDIWAIT: 0
      CLIENT_VERSION: 3
      CLIENT_RELEASE: 1
      CLIENT_LEVEL: 0
      CLIENT_SUBLEVEL: 3
      CLIENT_OS_LEVEL: 4.00
      OPTION_SET:
      AGGREGATION: YES
      URL:
      NODETYPE: CLIENT

```

Figure 27. Select node_name Example

2.3.12 Windows NT Event Viewer

The Windows NT Event Viewer logs errors, warnings, and success or failure of tasks. Event logging starts automatically when Windows NT is started. The Event Viewer is useful for investigating problems when you are running the ADSMConnect Agent for Microsoft Exchange Server. It assists you in determining the time and type of failure and whether or not the failure is related to the application, operating system, or hardware.

2.3.12.1 System Log

The System log logs events related to Windows NT system components and device drivers. You can use the System Log to determine whether a system component or driver used by the ADSMConnect Agent for Microsoft Exchange Server failed or had an error resulting in an ADSMConnect Agent for Microsoft Exchange Server failure or error (see Figure 28 on page 39).

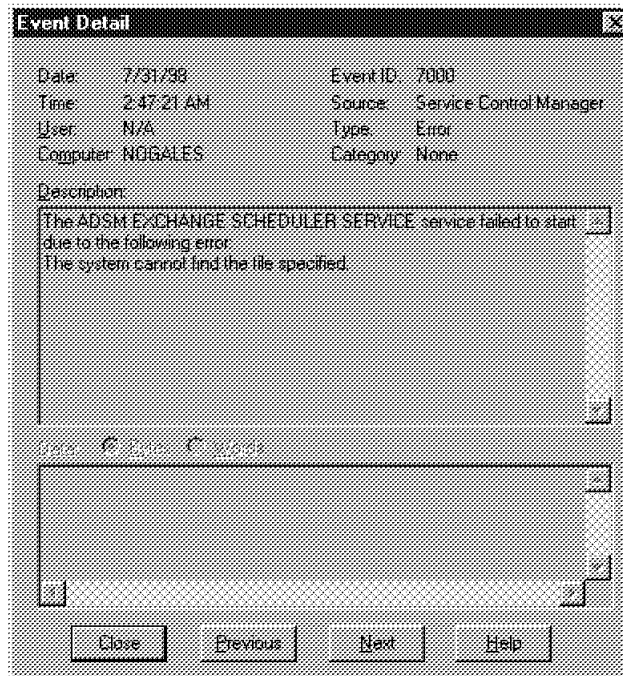


Figure 28. System Log: Event Detail

2.3.12.2 Application Log

The Application log (see Figure 29) logs events as determined by the application developers.

Date	Time	Source	Category	Event	User	Co
8/4/98	9:40:30 AM	AdsmClientService	None	4100	SYSTEM	PA
8/4/98	9:40:29 AM	AdsmClientService	None	4103	SYSTEM	PA
8/4/98	9:40:29 AM	AdsmClientService	None	4097	SYSTEM	PA
8/4/98	9:38:21 AM	AdsmClientService	None	4099	Guest	PA
8/4/98	9:38:21 AM	AdsmClientService	None	4099	Guest	PA
8/4/98	9:38:10 AM	AdsmClientService	None	4097	SYSTEM	PA
8/4/98	9:36:50 AM	MSExchangeIS	PubMTA Connections	2000	N/A	PA
8/4/98	9:36:44 AM	MSExchangeIS	PubMTA Connections	2000	N/A	PA
8/4/98	9:22:41 AM	ESE97	Logging/Recover	102	N/A	PA
8/4/98	9:22:40 AM	ESE97	Logging/Recover	104	N/A	PA
8/4/98	9:21:50 AM	ESE97	Logging/Recover	102	N/A	PA
8/4/98	9:09:17 AM	ESE97	Logging/Recover	104	N/A	PA
8/4/98	9:09:09 AM	ESE97	Logging/Recover	105	N/A	PA
8/4/98	9:09:09 AM	ESE97	Database Page C	118	N/A	PA
8/4/98	9:09:04 AM	ESE97	Logging/Recover	102	N/A	PA
8/4/98	9:06:21 AM	ESE97	Logging/Recover	102	N/A	PA
8/4/98	9:06:21 AM	ESE97	Logging/Recover	104	N/A	PA
8/4/98	9:05:51 AM	ESE97	Logging/Recover	102	N/A	PA
8/4/98	9:05:40 AM	ESE97	Logging/Recover	104	N/A	PA
8/4/98	9:05:40 AM	ESE97	Logging/Recover	104	N/A	PA
8/4/98	9:05:32 AM	ESE97	Logging/Recover	102	N/A	PA

Figure 29. Event Viewer: Application Log

Although the ADSMConnect Agent for Microsoft Exchange Server does not directly log events to this log, the Microsoft Exchange Server logs problems and

informational messages that occur during the backup or restore operation with ADSMConnect Agent for Microsoft Exchange Server (see Figure 30 on page 40 and Figure 31 on page 40).

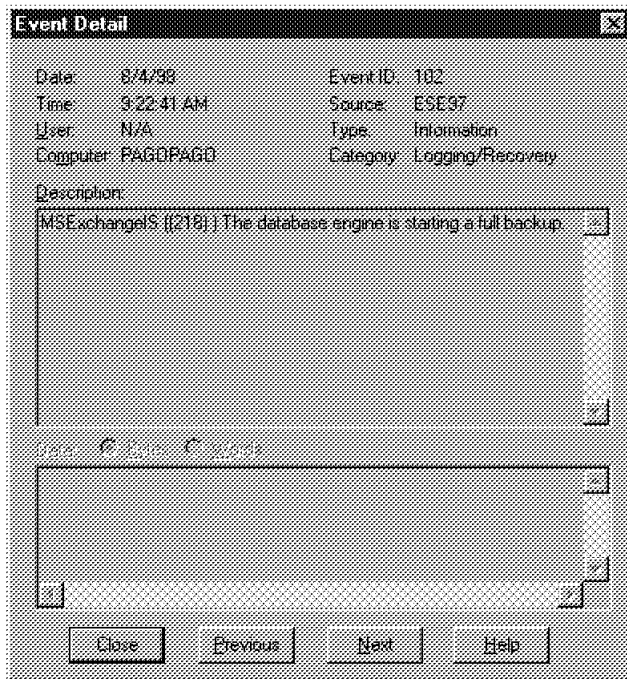


Figure 30. Application Event Log: Event Detail Information

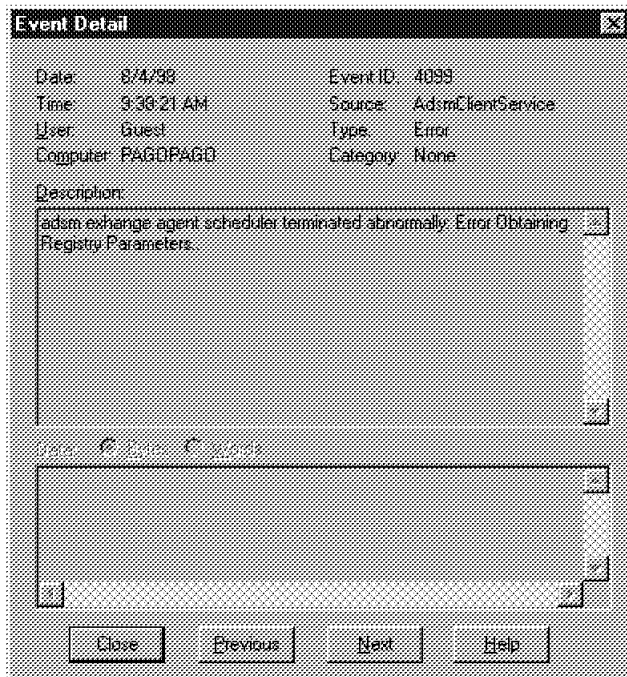


Figure 31. Application Log: Event Detail-Error

2.3.12.3 Security Log

The Security log logs events related to logon attempts and indicates whether or not they were successfully authenticated. In addition the Security log logs events related to resource use and objects.

2.3.13 Windows NT Accounts

2.3.13.1 Microsoft Exchange Server Site Services Account

The Microsoft Exchange Server must have a site services account for operation. The account is specified at installation. When the Microsoft Exchange Server services start up, they are authenticated by the domain controller. The account must have the following user rights:

- Restore files and directories
- Log on as a service
- Act as part of the operating system

Recommendation

We recommend that the site service account have a password that never expires.

2.3.13.2 Account for Manually Operating the ADSMConnect Agent for Microsoft Exchange Server

To run the ADSMConnect Agent for Microsoft Exchange Server GUI or command line from a Windows NT machine with Microsoft Exchange Server installed, you must be logged on with an account that is part of the local machine's, administrators group (see Figure 32 on page 42). This account gives you user rights or permissions to the following activities, which are key to operating the ADSMConnect Agent for Microsoft Exchange Server GUI or command line:

- Running ADSMConnect Agent for Microsoft Exchange Server
- Backing up and restoring files
- Local logon
- Accessing the Microsoft Exchange Server Administrator
- Starting or stopping Microsoft Exchange Server services
- Permission to read and write from the NT registry

If you are not running as "Exchange Site Services Account" not only do you have to have local "Admin" authority, but you must also have been granted the proper "Exchange Server" rights through the Exchange Administrator program.

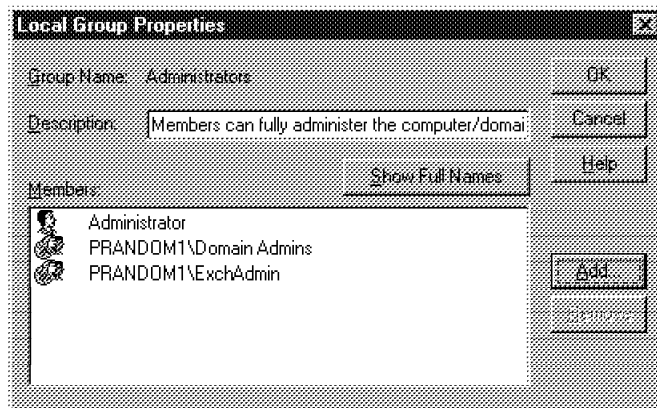


Figure 32. Local Group Properties: Administrators Group

Recommendation

We recommend that you not use the service account used by the Microsoft Exchange Server for manual operations of the ADSMConnect Agent for Microsoft Exchange Server. This prevents any accidental change to the service account that may prevent the Microsoft Exchange Server services from starting and additionally isolates backup operators from accessing the entire Microsoft Exchange organization.

2.3.13.3 Accounts for Using the ADSM Scheduler Service for the ADSMConnect Agent for Microsoft Exchange Server

In order for the ADSM scheduler service for the ADSMConnect Agent for Microsoft Exchange Server to start up with the system, the service Startup type must be set to automatic (see Figure 33 on page 43). Assuming that the latest ADSMConnect Agent for Microsoft Exchange Server maintenance has been applied, the account used to log on must be the system account or an account within the local machine's administrators group (see Figure 32). By default the system account is used (see Figure 33 on page 43). These accounts give you user rights or permissions for the following activities, which are required for successful operation of the ADSM scheduler service.

- Running the ADSMConnect Agent for Microsoft Exchange Server
- Backing up and restoring files
- Logging on as a service
- Backing up and restoring the Microsoft Exchange Server databases

If you are not running as "Exchange Site Services Account" not only do you have to have local "Admin" authority, but you must also have been granted the proper "Exchange Server" rights through the Exchange Administrator program.

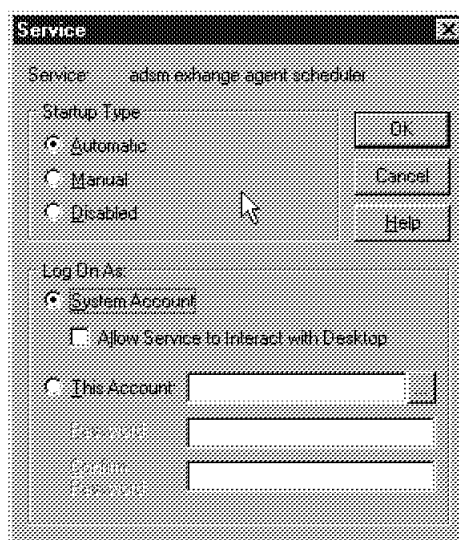


Figure 33. Services Startup Properties

2.3.14 ADSMConnect Agent Log File Setup and Use

The ADSMConnect Agent for Microsoft Exchange Server uses several types of logs to determine the outcome of the backups and restores as well as to help you figure out any problems that have occurred.

By default, the ADSMConnect Agent creates two logs in the AGENTEXC directory or in the directory where the ADSMConnect Agent is installed:

- ADSMConnect Agent information or activity is logged in excdsm.log
- ADSM API error messages are logged in dsiererror.log

When you use the ADSMConnect Agent to run backups at the client, you monitor ADSM backup activity with EXCDSTM.LOG on that Microsoft Exchange Server (see Figure 34), and the DSIERROR.LOG provides information on related errors.

```
08/04/1998 16:00:09,COMMAND LINE : excdsmc /adsmquerydb
08/04/1998 16:00:09,ANSI302E (RC2) No objects on server match query
08/04/1998 16:09:26,=====
08/04/1998 16:09:26,COMMAND LINE : excdsmc /adsmquerydb
08/04/1998 16:31:30,=====
08/04/1998 16:31:30,COMMAND LINE : excdsmc /adsmquerydb
08/04/1998 16:37:52,=====
08/04/1998 16:38:24,BACKUP(GUI) - Database: Directory,Type: Full,
Actual bytes: 13,648,208,3,648,208,Secs: 31.34,Kb/Sec: 435.50,
Exchange server: SCANDIUM,ADSM server: dsm,Status: Done: 13,648,208
bytes sent in 31.34 seconds(435.50 Kb/sec),
```

Figure 34. Sample EXCDSTM.LOG File

By default, when you work at the client, EXCDSTM.LOG always documents the ADSMConnect Agent activities. You can modify the logging by changing a

parameter in the ADSMConnect Agent for Microsoft Exchange Server GUI. Click on **Settings**, then **Preferences**, then **Activity Logging**. See Figure 35 on page 44.

To change the activity log filename via the command-line client, use the `"/LOGFILE:filename"` option.

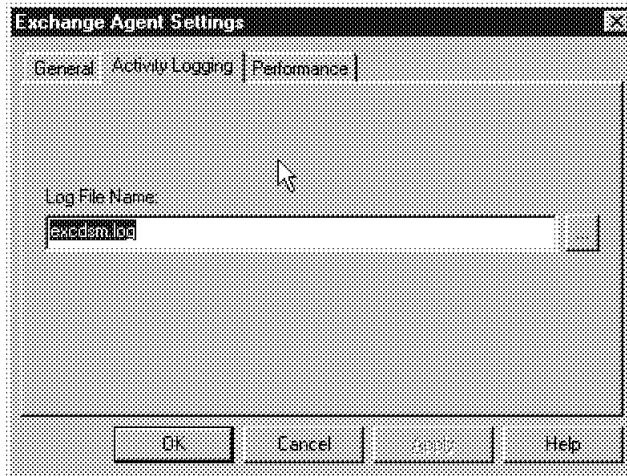


Figure 35. ADSMConnect Agent Default Activity Log File

In our environment, we set up and used additional types of logging through customization and scripting. Below we discuss what we did to set up unique logging and to prepare to automate the backups for the ADSMConnect Agent for Microsoft Exchange Server.

2.3.14.1 ADSM Scheduler Service

The ADSM Version 3 backup/archive client for Windows NT comes with a utility to install the ADSM scheduler as a Windows NT service to allow scheduled ADSM operations to run for that ADSM Windows NT client. You use DSMCUTIL.EXE to customize the ADSM service and automate the ADSM scheduler service installation. Details on how to use the DSMCUTIL.EXE command are documented in DSMCUTIL.TXT in the Baclient directory.

When ADSM scheduled operations run for the Windows NT client, two log files are created in the same Baclient directory from where it runs: DSMSCHEDED.LOG and DSMERROR.LOG. You can also schedule an ADSM command schedule to run the ADSMConnect Agent backups. If you choose to schedule these with the same ADSM service as the backup/archive client uses, the same DSMSCHEDED.LOG and DSMERROR.LOG files can be used to log information about the scheduled operations. However, we do not recommend this.

The alternative is to install a separate ADSM scheduler service for the ADSMConnect Agent, as we did in our environment. The main benefit of installing a separate ADSM scheduler is keeping the Microsoft Exchange Server backup activity separate from that performed by the ADSM backup/archive client. Consider these other benefits:

- Improved management of the ADSMConnect Agent activities
- Improved problem determination, by getting to the right information quickly
- Ability to organize and capture ADSMConnect Agent log files in a central location

- Assurance that scheduled backups for the ADSM backup/archive client and ADSMConnect Agent will not miss because of overlapping schedules

Note

In a TCP/IP environment, creating a separate ADSM scheduler service for the ADSMConnect Agent client also requires a separate NODENAME and use of a separate TCP/IP port. This is especially important when you are also running ADSM backup/archive client schedules.

We installed the scheduler, using the DSMCUTIL.EXE program, which comes with the ADSM backup/archive client for Windows NT Version 3. We specified a unique name for this scheduler, as well as a schedule log and error log for the output from scheduled operations.

Throughout our testing, we did not see many messages logged in EXCHERROR.LOG. We created EXCHERROR.LOG by using the /ERRORLOG parameter when we installed the scheduler service. If you are familiar with the ADSM backup/archive client, be aware that not all error messages you are used to seeing logged in DSMERROR.LOG will be logged in the log created with the DSMCUTIL /ERRORLOG parameter. For example, we found that error messages having to do with TCP/IP were not logged in our EXCHERROR.LOG:

```
08/05/1998 10:33:14 TcpFlush: Error 10053 sending data on Tcp/Ip socket 956.
08/05/1998 10:33:14 sessSendVerb: Error sending Verb, rc: -50
08/05/1998 10:33:14 TcpFlush: Error 10053 sending data on Tcp/Ip socket 956.
08/05/1998 10:33:14 TcpFlush: Error 10038 sending data on Tcp/Ip socket 4294967295.
08/05/1998 10:33:14 sessSendVerb: Error sending Verb, rc: -50
```

However, messages having to do with busy ports were logged in EXCHERROR.LOG:

```
08/05/1998 13:33:04 Re-trying bind with any port after finding default
                    port number in-use.
08/05/1998 13:33:04 Obtained new port number on which to listen.
```

Below is a sample of the command we used to install a separate ADSM scheduler service for the ADSMConnect Agent. It assumes that the ADSM backup/archive client is installed in the C:\ADSM\ directory:

```
DSMCUTIL INSTALL /NAME:"ADSM MExchange Scheduler"
/OPTFILE:C:\ADSM\AGENTEXC\DSM.OPT /NODE:SCANDIUM_EXCH
/PASSWORD:SCANDIUM_EXCH /SCHEDLOG:C:\ADSM\AGENTEXC\EXCHSCHED.LOG
/ERRORLOG:\ADSM\AGENTEXC\EXCHERROR.LOG
```

The entire command must be entered as one line.

Note

The *ADSTAR Distributed Storage Manager: ADSMConnect Agent for Microsoft Exchange Server Installation and User's Guide* states that only the Microsoft Exchange Server Exchange site services account can run the ADSMConnect Agent. Therefore the service account for the ADSM Scheduler Service must be that same userid. However, this requirement has changed. The code change is documented and available from a fixtest located on the ADSM anonymous server, index.storsys.ibm.com/adsm/fixtest/agents/ntexch/v1r1/. For more information, download the readme file for this fixtest, IC20843A.readme.ftp.. For our tests, we applied the fixtest and did not define the site services account in the service account of the ADSM scheduler service.

If you are not running as "Exchange Site Services Account" not only do you have to have local "Admin" authority, but you must also have been granted the proper "Exchange Server" rights through the Exchange Administrator program.

To automate the installation of a separate ADSM scheduler service, put the command in a command file, but be aware that you have to customize variables for the /NODE and /PASSWORD parameters, according to your environment and the degree of automation you want. For a sample of our command file, see E.1.1, "Sample Command File to Install ADSM Scheduler" on page 85.

2.3.14.2 Additional Logging with Automated Batched Backups

To have the ADSM scheduler service perform scheduled backups of the Microsoft Exchange Server you also have to use the command line executable that comes with the ADSMConnect Agent for Microsoft Exchange Server, EXCDSMC.EXE.

To use the scheduling function of ADSM to run a backup, using the ADSMConnect Agent, we created a command schedule at the ADSM server to run a command, or script, file at the client, the Microsoft Exchange Server. Two sample command files are provided as part of the ADSMConnect Agent for Microsoft Exchange Server installation:

```
excfull.smp  
excincr.smp
```

We modified these two files slightly and implemented them in the ADSM command schedule, specifying two new log files to obtain information about that operation.

In the Exchange Agent directory, AGENTEXC, the EXCDSM.LOG is automatically created and logs Exchange Agent information by default. In our command files, we used the /LOGFile:logfilename option to specify EXCHFULL.LOG for full backups and EXCHINCR.LOG for incremental, or transaction log, backups:

```
EXCDSMC /BACKup:DIR,FULL /LOGFile&GML.C:\ADSM\AGENTEXC\EXCHFULL.LOG
```

We decided to use EXCHFULL.LOG for backups of both the directory and the information store.

The last log file we created was for output from the backup operations. Typically this information would go to standard out, or the console of the Exchange server,

if, for example, the command was run from the command line. See Figure 36 on page 47.

```
C:\adsm\Agentexc>excdsmc /back:dir,full

ADSTAR Distributed Storage Manager
ADSMConnect Agent for Microsoft Exchange Server
Command Line Interface - Version 1, Release 1, Level 0.0
(C) Copyright IBM Corporation 1998. All rights reserved.

***FIXTEST - Version 1.1.0.0 "A"

ADSM API Version 3, Release 1, Level 3
ADSM Nodename: scandium_exch

Starting a backup to the ADSM server...

    Exchange Server : SCANDIUM
        Database : Directory
        Backup Type : Full

Logging on to the ADSM server...

    244,(0/2 full)> Wrote      0 bytes, total: 15745360

Backup completed.  15,745,360 bytes sent in
                   35.19 seconds(447.39 Kb/sec)

C:\adsm\Agentexc>
```

Figure 36. Output from ADSMConnect Agent Backup

We decided to use the hostname or computername of the Microsoft Exchange Server for the output file. We specified the output file in a command file as follows:

```
EXCDSMC /BACKup:DIR,FULL /LOGFile&GML.C:\ADSM\AGENTEXC\EXCHFULL.LOG >>
C:\ADSM\AGENTEXC\SCANDIUM.OUT
```

This command must be entered as one line.

In addition to all of the ADSM log files, the Microsoft Exchange Server logs information to the Windows NT event log, which you should also consider when performing problem determination. For more information see 2.3.12, “Windows NT Event Viewer” on page 38.

2.3.15 ADSMConnect Agent Scheduling and Maintenance

We used a wide array of logging in setting up the ADSMConnect Agent for Microsoft Exchange Server to perform ADSM scheduled backups. Although the ADSMConnect Agent does not currently provide built-in central administration, the command line interface does provide a great deal of flexibility for customizing regularly scheduled backups.

In E.1.3, “ADSMConnect Agent Backups and Central Logging” on page 86, we provide a sample command file for performing the full backups described in 2.3.14, “ADSMConnect Agent Log File Setup and Use” on page 43. The incremental command file was set up in the same way except for the names of the log files. We decided to leave the ADSMConnect Agent activity log files in the same directory where the agent was installed.

Consider the following points when setting up your environment for automated ADSMConnect Agent backups of the Microsoft Exchange Server:

- Naming conventions for log files
- Centralized log file collection
- Log file pruning
- Deleting old backups
- Strategy for keeping old backups

We defined the output logs with the computername of the Microsoft Exchange Server to enable us to collect the output from all Microsoft Exchange Servers in our site and review the servers collectively for any output errors. For any further investigation of problems, we could go to those individual Microsoft Exchange Servers. We created a share at a central utility server used for administrative purposes and set a variable in the backup command file so that we could write the output logs to that server.

Once we began backing up, it was necessary to prune all of the log files we created. During our project log file pruning did not exist in the ADSMConnect Agent for Microsoft Exchange Server, so we added three more statements to the command file to use an OLDLOGS directory and delete old logs after archiving them:

1. Move an existing log by the name of EXCHFULL.ARC to the OLDLOGS directory.
2. Rename EXCHFULL.LOG to EXCHFULL.ARC in the ADSMConnect Agent directory.
3. Issue an ADSM BAclient ARCHIVE -DELETEFILES on the OLDLOGS directory.

This method maintains the last and current activity logs and enabled us to go back to even older copies if necessary.

We would implement something similar for the DSIERROR.LOG, and the logs created by the scheduler would be handled with the same options available in the BAclient:

```
SCHEDLOGRetention  
ERRORLOGRetention
```

Because the output log was routed to a central location, we handled its pruning there.

For an example of our backup command file, which includes the above steps for cleaning up the logs, see E.1.4, “ADSMConnect Agent Backups, Central Logging, and Log Pruning” on page 87.

ADSM designates the ADSMConnect Agent backups as *backup objects*, and this affects how the objects will be expired, or removed, from ADSM. See 2.3, “ADSM Online Backup of Microsoft Exchange Server” on page 15 for more information about the ADSM management class for ADSMConnect Agent.

Because of the way the ADSMConnect Agent for Microsoft Exchange Server works, we had to invoke it to delete old objects. For example, once we determined what we no longer needed to retain, we used the following command

from the command line interface to delete an old full backup of the Microsoft Exchange Server information store:

```
EXCDSMC /ADSMDElete IS,19980804163042.FULL
```

The database name, IS, and the object name, 19980804160849.FULL, are the two required parameters. The object name includes the year (1998), the month (08), the day (04), and the time (160849 or 16:08:49), followed by the type of backup, FULL. We identified the object name, by first issuing this query:

```
EXCDSMC /ADSMQUERYDB&GML.IS
```

Here is the output from the query command:

DB	Type	Size	Date	Time	ADSM Object Name	Org.Site.Server

With this output, we could identify the correct backup to delete, but we could not create a simple command file to obtain the object name and then feed it into the EXCDSMC /ADSMDEL command.

During the project, we located a Perl script posted on the ADSM discussion forum, ADSM-L@VM.MARIST.EDU. See E.1.5, “Perl Script for Deleting Old ADSMConnect Agent Backups” on page 88. We did not write the script, nor do we support it, but we include it for your information.

Because the Perl script was posted in a public forum, the Perl executable is required to run it. We obtained the script and tested it in our environment. You might want to use this or a similar script by adding a CALL statement to the bottom of the backup command file so that every time a full backup is run, the the last step will be to delete the oldest backups:

```
CALL PERL EXC_LIST_OLD_DBS.PL <DAYS>> IN.TXT OUT.TXT
```

Before implementing this script or any script to delete old copies of the backups, first consider your strategy for keeping Microsoft Exchange Server backups. How long you are required to keep backup copies will determine not only how you implement your automation for deleting old copies but also what the DASD, or disk, requirements will be. Consider how often you require a full backup of the directory and how often you require information store full and incremental backups or whether you need incremental backups at all. This information will be important when you define the ADSM schedules. For more information about defining ADSM schedules, see the ADSM Administrator’s Guide for your server platform.

It is possible to get scheduler timeouts when you use the ADSM scheduler with the Exchange Agent; for an example see Figure 37 on page 50.

```

08/05/1998 00:18:05 ANR0406I Session 7283 started for node PTLEXM01
>(WinNT) (Tcp/Ip 10.1.3.196(3404)).
>
>08/05/1998 00:18:07 ANR0406I Session 7284 started for node PTLEXM01
>(WinNTDB) (Tcp/Ip 10.1.3.196(3406)).
>
>08/05/1998 00:33:20 ANR0482W Session 7283 for node PTLEXM01 (WinNT)
>terminated - idle for more than 15 minutes.
>
>08/05/1998 01:05:01 ANR2578I Schedule EXCHG_DAILY in domain EXCHANGE
>for node PTLEXM01 has missed its scheduled start up window.
>
>08/05/1998 01:21:37 ANR0406I Session 7307 started for node PTLEXM01
>(WinNT) (Tcp/Ip 10.1.3.196(4080)).
>
>08/05/1998 01:21:38 ANR2576W An attempt was made to update an event
>record for a scheduled operation which has already been executed -
>multiple client schedulers may be active for node PTLEXM01.
>08/05/1998 01:21:38 ANR0403I Session 7307 ended for node PTLEXM01
>(WinNT).
>
>08/05/1998 01:21:38 ANR0406I Session 7308 started for node PTLEXM01
>(WinNT) (Tcp/Ip 10.1.3.196(4081)).
>
>08/05/1998 01:21:38 ANR0403I Session 7308 ended for node PTLEXM01
>(WinNT).
>
>08/05/1998 01:21:51 ANR0403I Session 7284 ended for node PTLEXM01

```

Figure 37. Scheduler Client Session Timeout

In this case, message ANR2576W is related to IC21388, TCPFLUSH error 10054 is due to the fact that the scheduler client session timed out (message ANR0482W) while it was waiting for the Exchange Agent to complete the backup. Similarly, message ANR2578I indicates that the scheduled event was missed because the scheduler client session had timed out. You can avoid these messages by changing the command file used to launch the Exchange Agent to START EXCDSMC rather than invoking it directly. This change causes the command file to return to the scheduler after launching the command rather than waiting for it to complete. In this case, you would see the scheduler session complete (and indicate successful completion) very quickly after start of the event, but the Exchange Agent session would continue to run as normal. Be aware though that the successful completion of the scheduled event simply means that the agent was started. You still have to check the agent log file to confirm success of the Exchange Agent backup.

Chapter 3. Database Recovery

In this chapter we explain how to recover from both offline and online backups. We cover the recovery of individual components and full servers and complete disaster recovery.

3.1 Restoring Databases from Offline Backups

In this section we explain how to recover from the backup method described in 2.2, "ADSM Offline Backups of Microsoft Exchange Server" on page 10. To recover archives of the Microsoft Exchange Server database, using the ADSM backup/archive client, you must first shut down the database by stopping the Microsoft Exchange Server services.

We discuss retrieving the Microsoft Exchange Server directory and information Store and repairing the information Store after an offline restore. We then show how to restart the Microsoft Exchange Server.

Once you have identified the need for an ADSM retrieve, you have to decide which files and dates are appropriate for the retrieve.

To stop the Microsoft Exchange Server services, you can run a command file or use the Services window (see Figure 38).

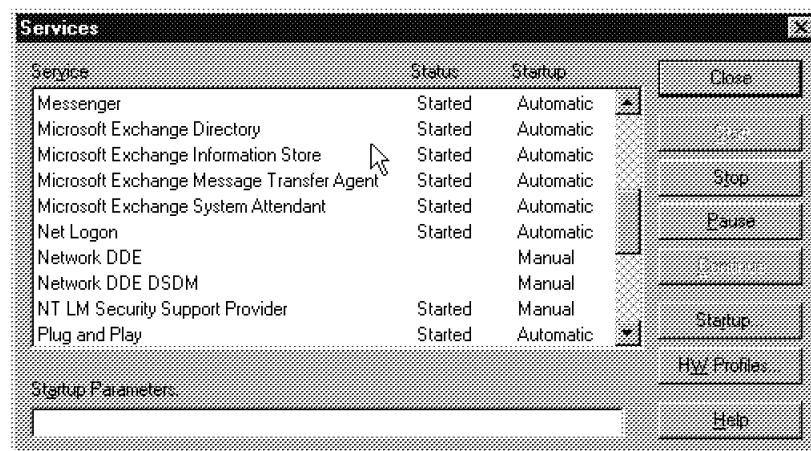


Figure 38. Windows NT Control Panel: Services

Follow the same order as noted in 2.2, "ADSM Offline Backups of Microsoft Exchange Server" on page 10:

1. Microsoft Exchange Message Transfer Agent
2. Microsoft Exchange Information Store
3. Microsoft Exchange Directory
4. Microsoft Exchange System Attendant

We installed and configured the ADSM backup/archive client for Windows NT on the Microsoft Exchange Server. In our environment, the ADSM client was installed in the C:\ADSM\ directory. From the ADSM client, which is the Microsoft Exchange Server requiring the recovery, invoke the ADSM

backup/archive client Version 3 GUI, and click on **Retrieve**. Click on the plus sign (+) next to the ADSM client name, and the archives listed by the description fields we used in 2.2, “ADSM Offline Backups of Microsoft Exchange Server” on page 10. See Figure 39.

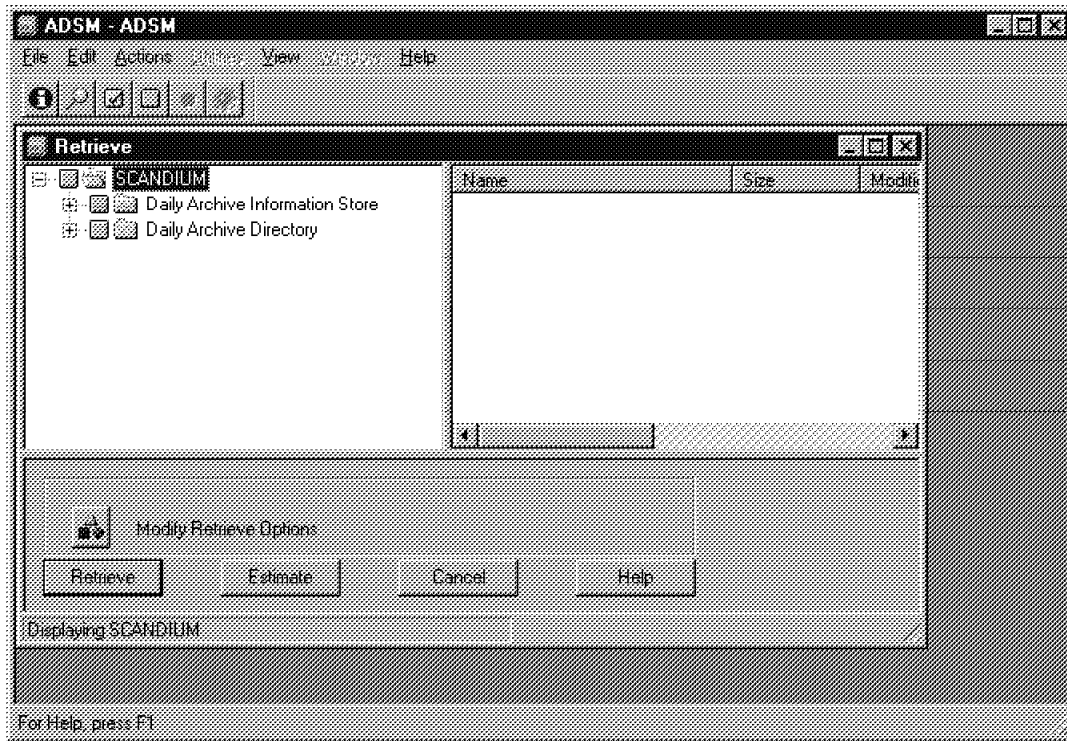


Figure 39. ADSM Backup/Archive Client Retrieve

First we selected the latest version of the directory, DIR.EDB, and then we selected the latest version of the information store, PRIV.EDB, and PUB.EDB.

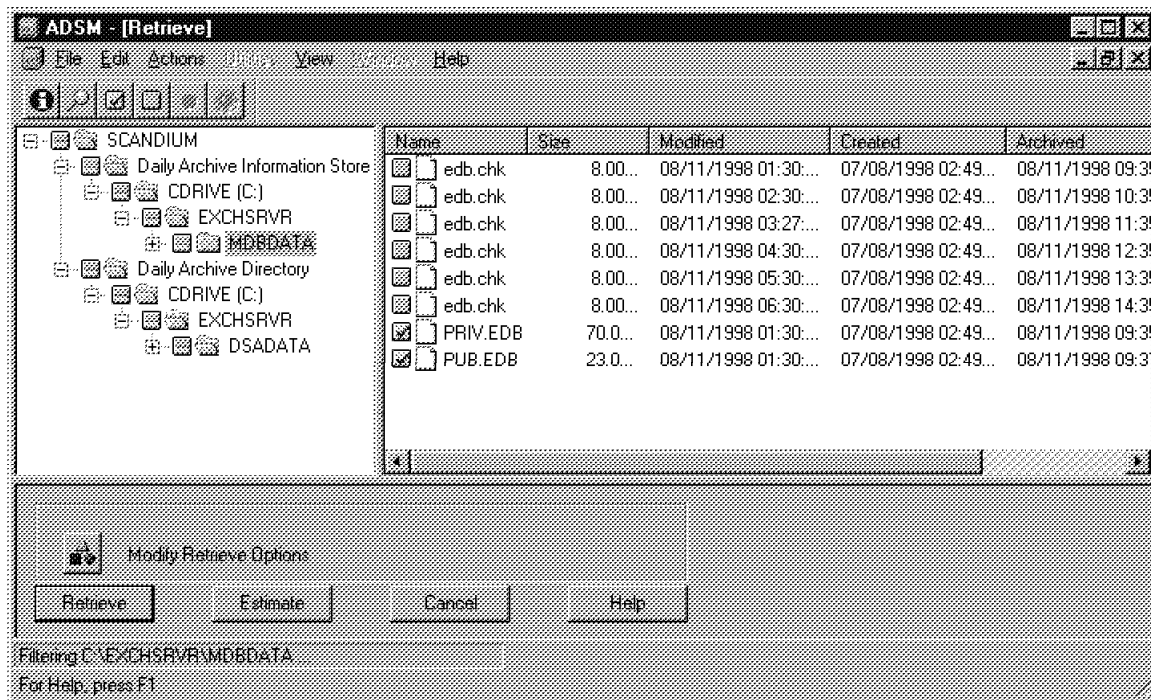


Figure 40. Select DIR.EDB, PRIV.EDB and PUB.EDB for Retrieve

Before starting the retrieve, we checked some of the ADSM options:

1. We clicked on **Modify Retrieve Options** on the ADSM backup/archive client Retrieve window to get to the Retrieve Options window (Figure 41).

Note that the default options specify that all the files and directories from the selected group will be retrieved. In addition, the files that already exist will be skipped.

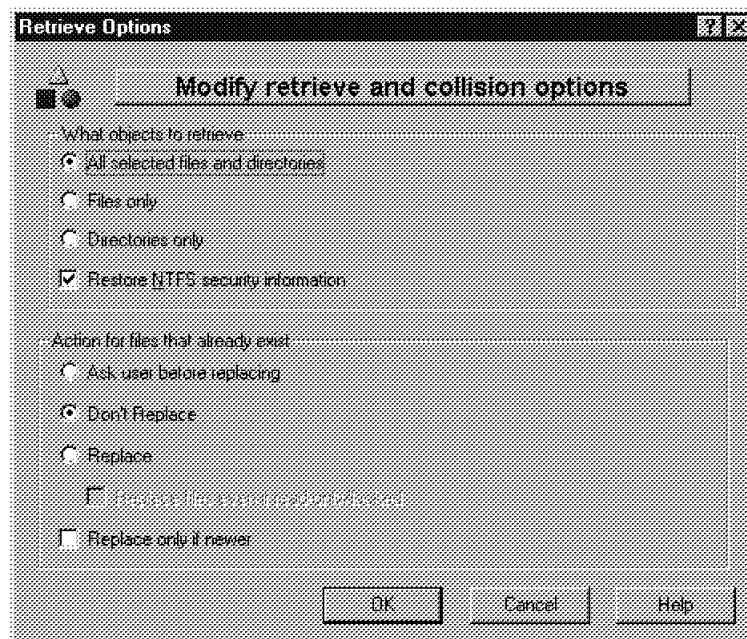


Figure 41. Default Modify Retrieve Options

In our example, the directories exist, but the files no longer exist on the disk, so we changed the *What objects to retrieve* parameter to **Files only**.

2. We clicked on **Retrieve** on the ADSM backup/archive client Retrieve window to get the Retrieve Destination window (Figure 42).

Note that the default options specify that the files will be retrieved to the original location.

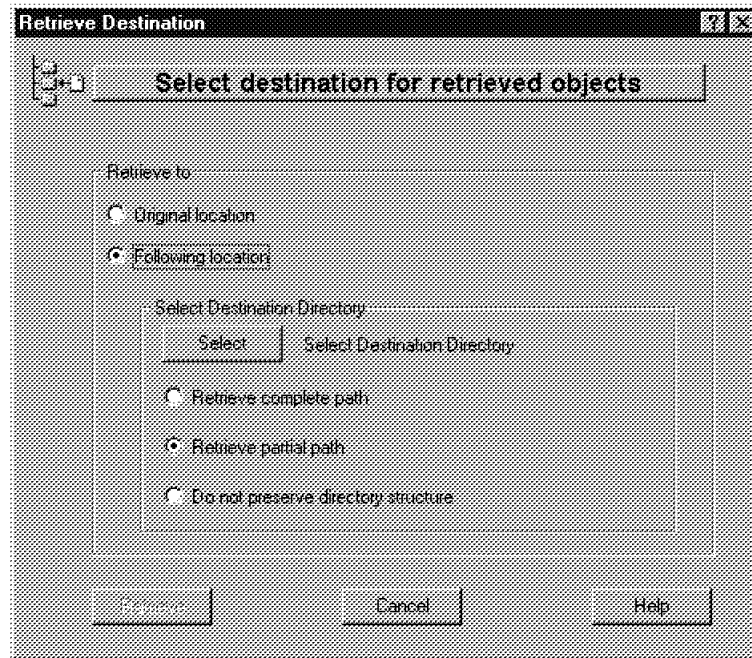


Figure 42. Default Destination for Retrieved Objects

After completing the retrieve, we issued the Microsoft Exchange Server command to repair the information store. This repair is necessary after an offline information store restore or, in this case, retrieve. Before issuing this command, we had to start the directory service:

1. NET START MSEXCHANGEDS
2. C:\EXCHSRVR\BIN\ISINTEG -PATCH

For more information about the ISINTEG command, see the Microsoft Exchange Server online help.

At this point, the Microsoft Exchange Server is ready to be started and tested for a proper restore. For the things we do to check for a valid restore, see 3.5, "Validating the Recovery" on page 74.

3.2 Restoring Databases from Online Backups

If a Microsoft Exchange Server is destroyed or must be moved to new hardware, full server recovery is required. We define full server recovery as the ability to recover the information store and directory to a new machine. After the recovery all clients should be able to log on. In this section we describe the requirements for a full server recovery, explain NT machine security within a domain and its implication for full server recovery, and present the procedure for recovering Microsoft Exchange Server databases.

3.2.1 Requirements for Successful Recovery

To successfully restore a Microsoft Exchange Server directory, two essential conditions must be met:

- The Microsoft Exchange Server directory must be restored to a Windows NT machine that has the same site, organization, and NT server name as the production server.
- The new server must be able to access the same NT domain where Microsoft Exchange Server was originally installed.

3.2.2 NT Machine Security

All security-related activities in a Windows NT environment are based on security identifiers (SIDs). All user accounts and machine accounts obtain an SID at the time they are created. The SID is a unique number representing the account. It can never be changed.

Windows NT machines use the SID to establish membership within the Microsoft Windows NT domain. An authentication process occurs between each Windows NT machine and the domain controller. The result of a successful authentication is the establishment of a secure channel between the Windows NT machine and the domain controller.

3.2.3 NT Machine Security and Full Server Recovery

In case of full server recovery you have to build a new Windows NT machine on replacement hardware with the same machine name you are attempting to restore. The same machine name is required to be able to restore Microsoft Exchange Server directory. If you set up a new Windows NT machine with a machine name that exists in a domain, there will be two different SIDs for the machine. Therefore you will not be able to join this new machine with the domain - (see Figure 43 on page 56). Building the new Windows NT machine creates a new SID for the machine account.

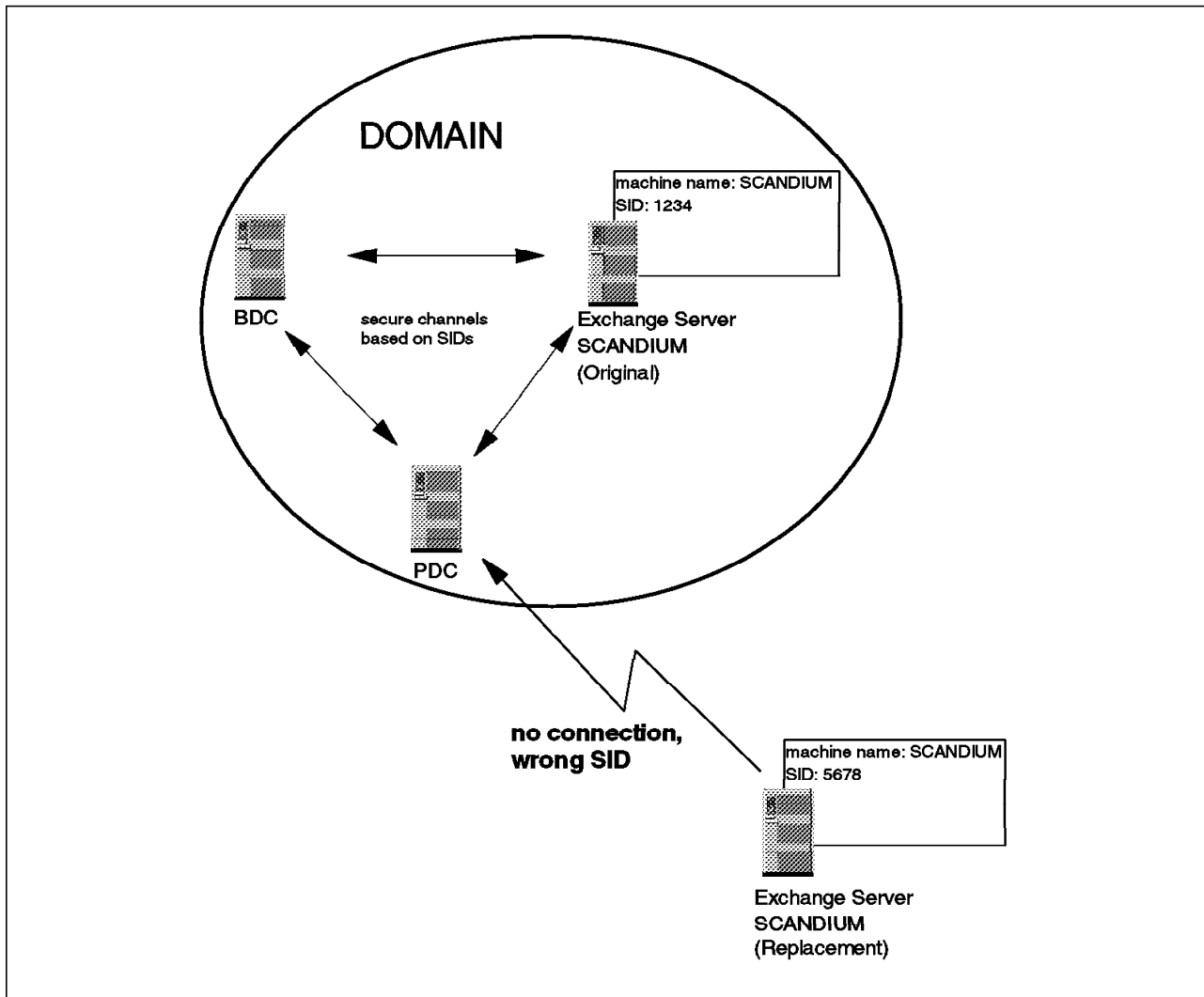


Figure 43. Windows NT Machine Security

3.2.4 Procedure to Restore a Full Server

Figure 44 on page 57 shows the necessary steps for a full server recovery. We describe these steps in this section.

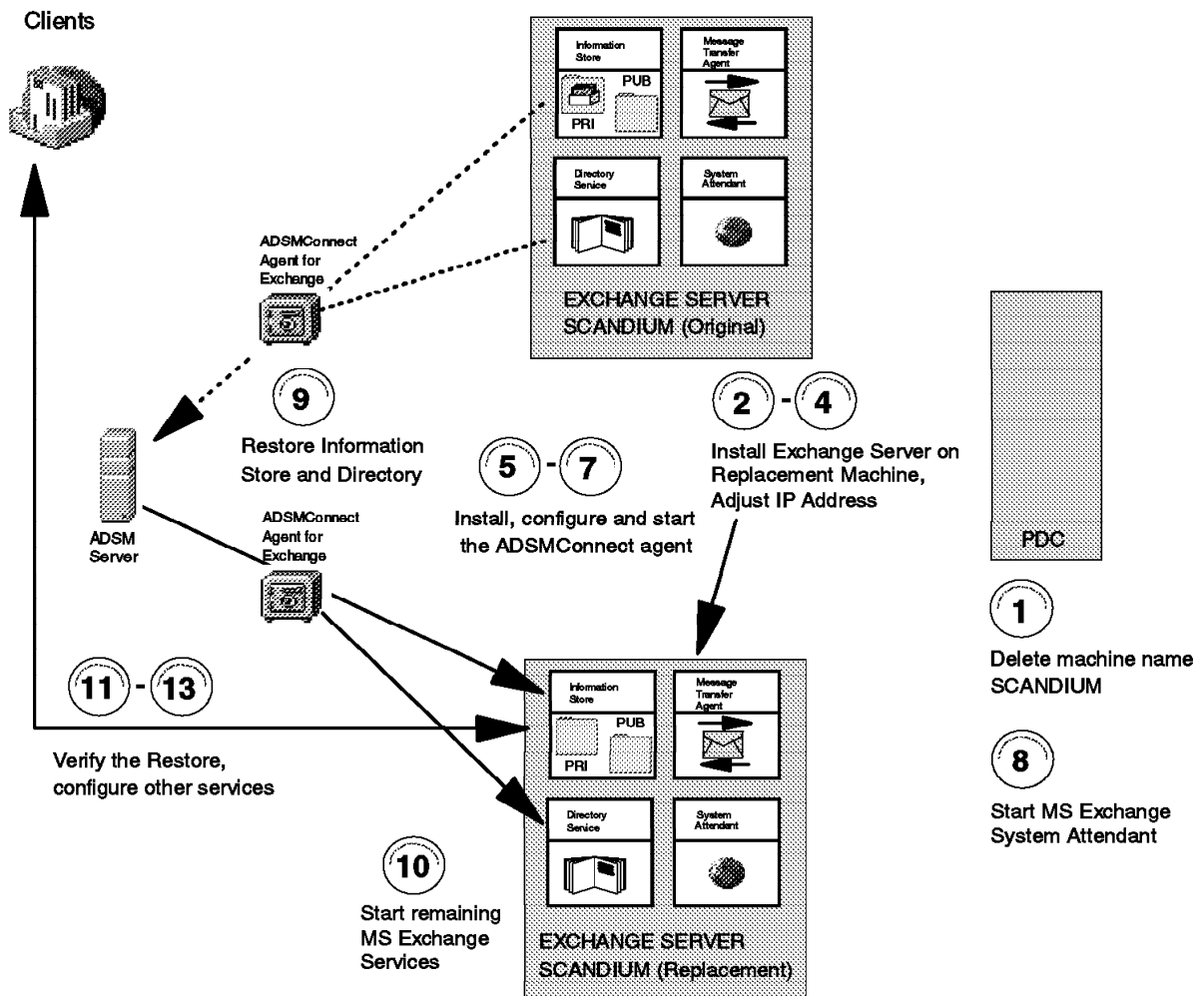


Figure 44. Full Server Recovery Steps

To complete the restore process we provided the following information on the Microsoft Exchange Server configuration sheet:

NT (NetBIOS) Name:	SCANDIUM
MS Exchange Organization Name:	ACME Motor Corp
MS Exchange Site Name:	West
MS Exchange Service Account:	EXCHSERVICE
MS Exchange Service Acct PW:	EXCHSERVICE

Follow these steps to restore the Microsoft Exchange Server information store and directory on new hardware:

1. Delete the old machine name from the NT domain, using the Server Manager program. Select the machine and press the **delete** key. See Figure 45 on page 58.

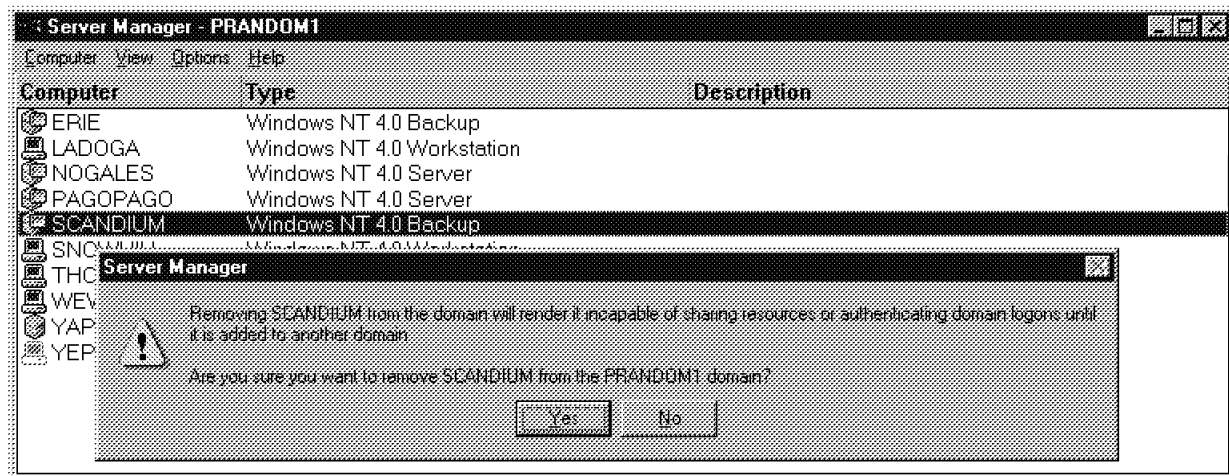


Figure 45. Deleting the Old Machine Account

2. Build a new Windows NT server with the required service packs on equivalent hardware to the production server. Specify an NT machine name that is the same as the original production machine. Join the NT domain (which will automatically add a new unique SID).
3. In a TCP/IP environment, ensure that client workstations can resolve the machine name of the replacement server. Assign the IP address of the original server to the replacement server or change the DNS entry for the machine name of the replacement server.
4. Install Microsoft Exchange Server, using the Setup /R command. The /R option tells the setup program to install Microsoft Exchange Server without starting services or initializing the directory.

Create a new site (do not join an existing site) with the same site and organization name as the production system. See Figure 46.

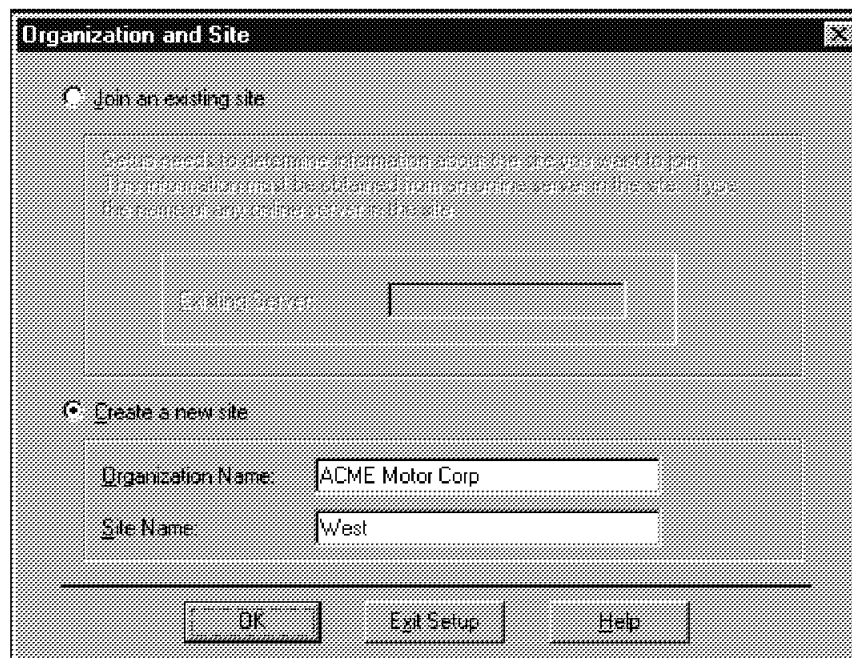


Figure 46. Creating New Site

Use the same Microsoft Exchange Server service account as used in the original site.

As a precaution set all Microsoft Exchange Server services to start up manually. You do not want the server to begin replicating with other servers until the information store and directory have been restored.

5. Install the ADSMConnect Agent.

After this preparation you are ready to restore.

6. Configure the ADSMConnect Agent. The ADSMConnect Agent dsm.opt file must use the nodename used by the Microsoft Exchange Server you are attempting to recover.

7. Start the ADSMConnect Agent.

You need the ADSM client password of the ADSMConnect Agent for the restore process. If you do not know the client password, you can either:

- Use the ADSM scheduler service configuration utility, DSMCUTIL SHOWPW, if it is available at the original machine, to display the password. For details on how to use *DSMCUTIL*, see DSMCUTIL.TXT in the backup client directory.

or

Set a new client password for the ADSMConnect Agent from an ADSM administrator client.

8. From the Control Panel Services applet start the Microsoft Exchange System Attendant, which is required by ADSMConnect Agent for restore operations. See Figure 47.

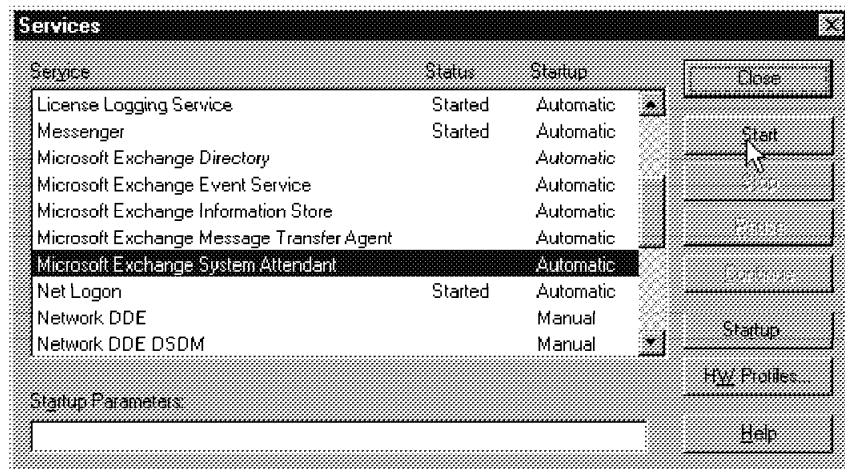


Figure 47. Start Microsoft Exchange Server System Attendant

9. Restore the information store and directory. Select the latest full backup and all more recent incremental backups for both the information store and the directory. See Figure 48 on page 60.

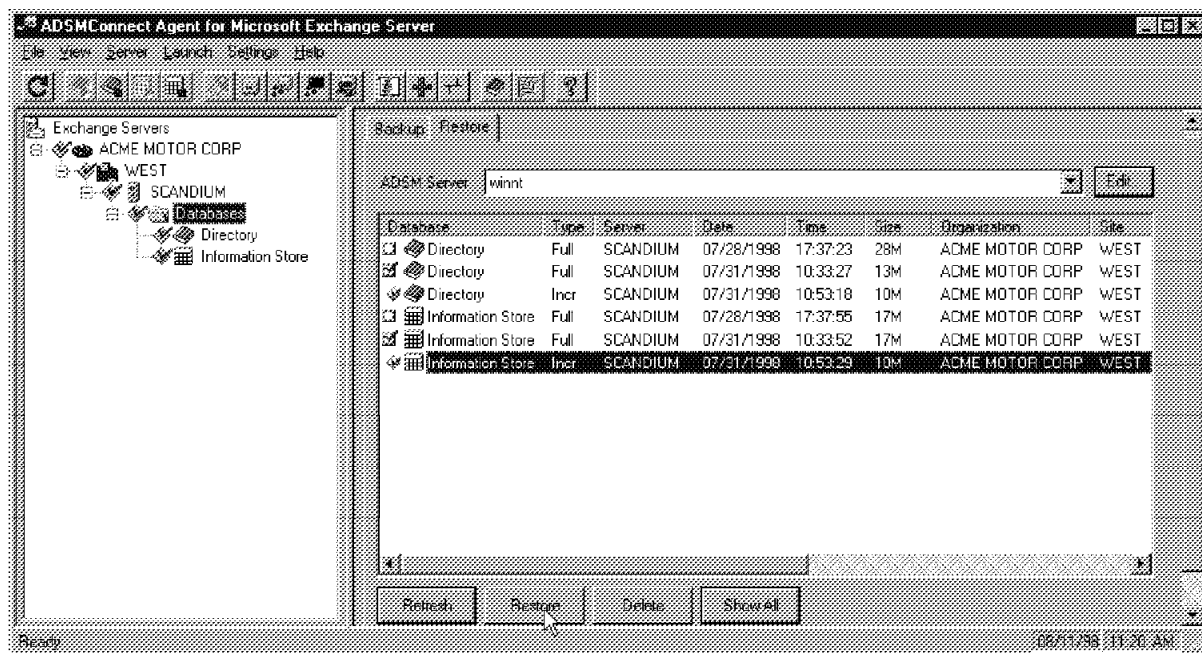


Figure 48. Start Microsoft Exchange Server Restore of Information Store and Directory

10. Start the remaining Microsoft Exchange Server services from the Control Panel Services applet.
11. From within Microsoft administrator verify that all mailboxes have a Windows NT domain account association.
12. Check that client workstations can connect and access mailboxes.
13. Create and configure any other services that were in the production system.

3.3 Restoring Individual Mailboxes

User mailboxes are contained within the information store. It may be necessary to recover lost or deleted data from mailboxes in some circumstances, such as when:

- A user's mailbox has been inadvertently deleted.
- Individual messages have been lost.

Unfortunately there is no Microsoft Exchange Server API to extract portions from the backup of the information store database files. Therefore it is not possible to recover individual messages or even a user's mailbox directly from a backup of the information store without first restoring the entire information store.

Needless to say, you must handle the deletion of a complete Microsoft Exchange Server mailbox very carefully.

Note

We recommend that you save the user's mailbox in a PST file before deleting it. For a definition of PST files, see 2.1.2.2, "Personal Folders" on page 9.

You can choose among four different restore techniques depending the nature of the data loss. We describe the techniques below, going from the easiest to the most difficult.

3.3.1 Using the Deleted Item Recovery Option

A new feature of Microsoft Exchange Server 5.5 is the ability to recover deleted items from existing user mailboxes and public folders. Using the deleted item recovery option is the simplest way of recovering individual messages.

Deleting an item moves it to the Deleted Items folder. A deletion in the Deleted Items folder discards the item permanently. In Figure 49 all items in the Deleted Items folder are deleted.

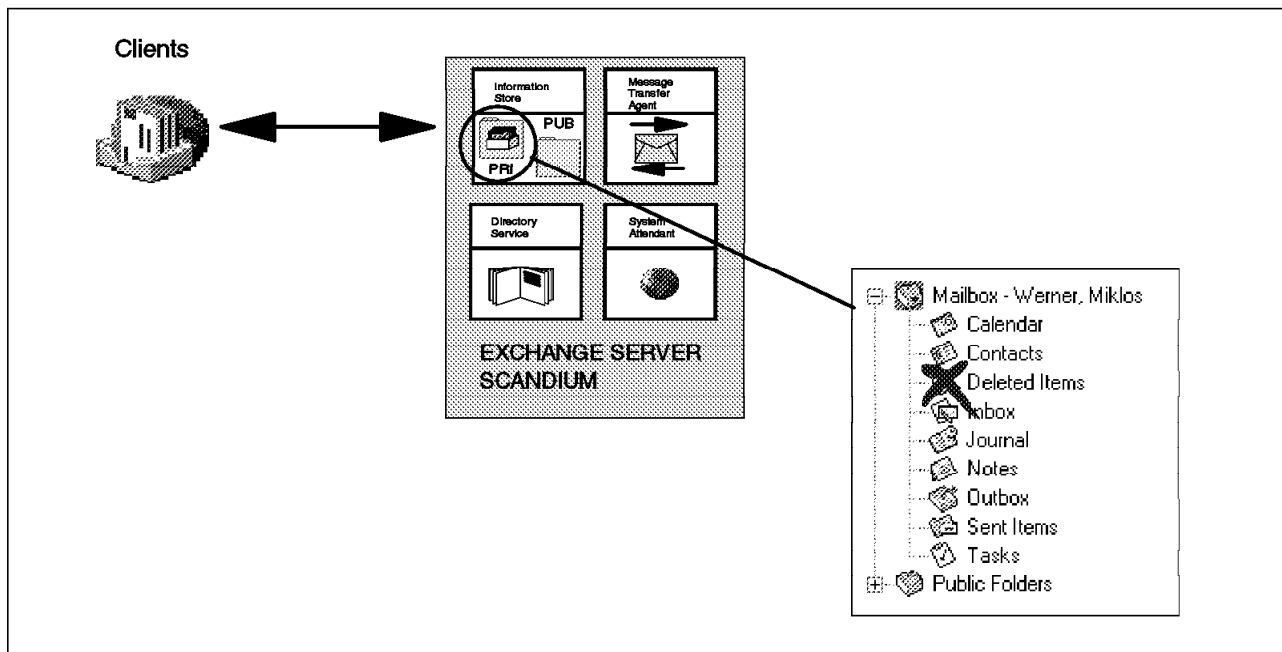


Figure 49. Permanent Deletion of Messages

There are two prerequisites for successful recovery:

- You need Microsoft Outlook Version 8.03 or above. (In this book we refer to the product as the *Outlook client*.)
- The date of loss or inadvertent deletion must be within the *deleted item retention time*. This value is controlled by the Exchange administrator on the Properties page of each server's private and public information store (see Figure 50 on page 62). The deleted item retention time must be set separately for the private information store and the public information store.



Figure 50. Deleted Item Retention Time

3.3.1.1 Recovering Deleted Items

With the Outlook client, users have access to their permanently deleted items within the predefined *deleted item retention time*. By clicking on Recover Deleted Items on the Outlook bar you get the complete list of your recoverable items. See the Deleted Items window in Figure 51 on page 63.

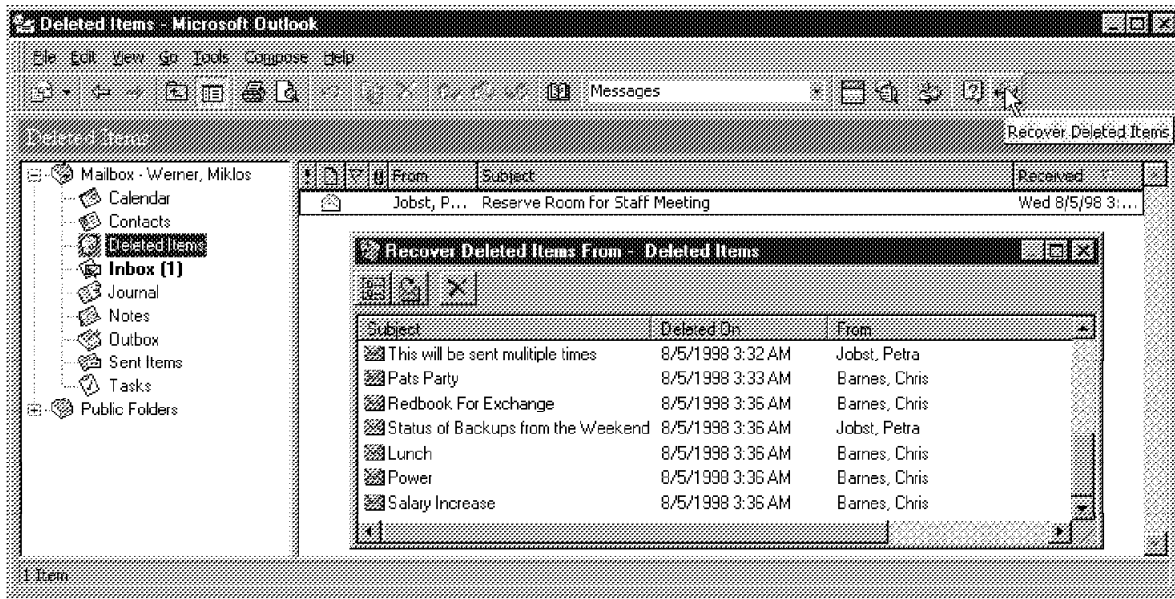


Figure 51. Recovering Deleted Items

Recovering deleted items moves them back to the Deleted Items folder.

3.3.1.2 Recovering Deleted Items for a User

If you want to recover deleted items for a user, you must add an additional Registry key at the Outlook client. This modification also allows deleted item recovery from all folders of any user's server-based mailbox. Modifying the Windows NT registry using the regeditor may result in serious damage to the operating system, so use extreme caution when making any changes.

At your workstation follow these steps:

1. Using the Regedt32.exe program, locate the key:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Exchange\Client\Options
2. Select **Edit** and then **Add Value**.
3. Add a value of DumpsterAlwaysOn.
4. Select data type of **REG_DWORD**.
5. Select data of 1.

Figure 52 on page 64 shows the result of the above operation.

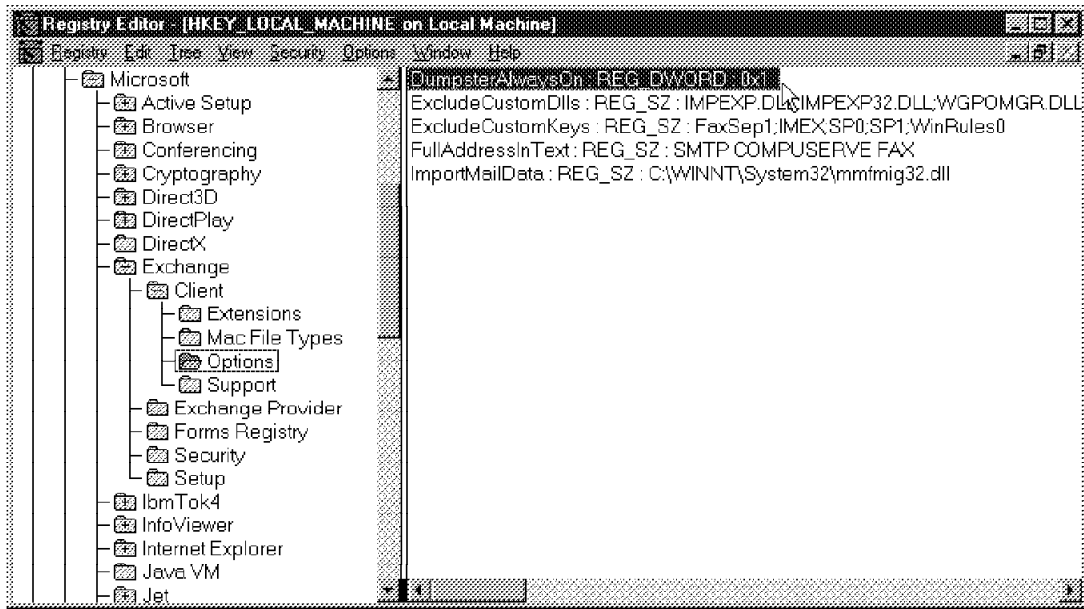


Figure 52. Registry Update for Deleted Item Recovery

At the Outlook client prepare the access to the mailbox of another user:

1. From the Tools menu, select **Services** and double-click on **Microsoft Exchange Server**.
2. Select the **Advanced** tab and then **Add** to add the required user mailbox to the profile.

Now you have access to the mailbox of the selected user and can complete the recovery of any deleted items. See Figure 53 on page 65.

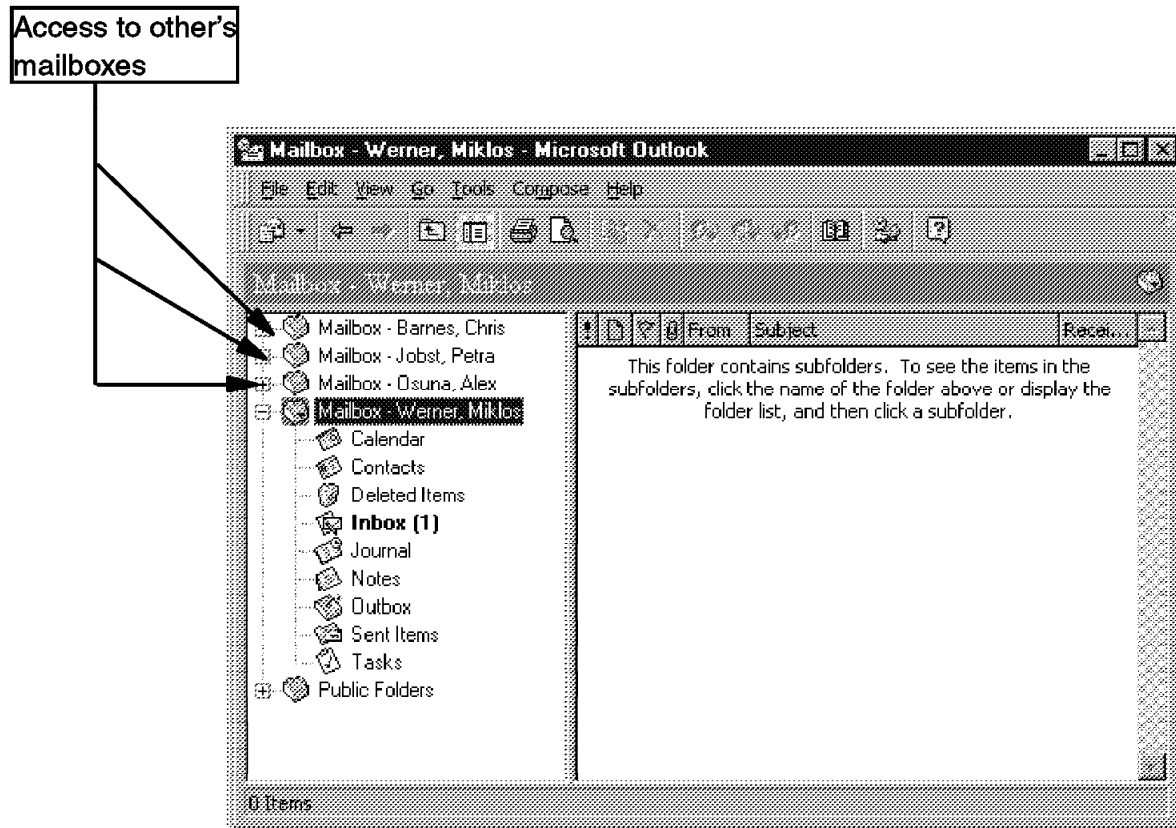


Figure 53. Access to Other Users' Mailboxes

3.3.2 Using an Existing Personal Folder

A PST file is located on a file system of choice. It can therefore be used to copy a server-based mailbox to removable media (export) and install that mailbox on another machine which is not connected to the first server (import).

If a Microsoft Exchange Server mailbox is deleted, users who have a copy of their existing mailbox in a PST file may be able to recover a server-based mailbox.

Use the import and export functions of Microsoft Exchange Server clients for these activities. These functions are described in the Microsoft Outlook client's Online Help.

3.3.3 Using an Existing Offline Folder

If a Microsoft Exchange Server mailbox is deleted, users with an offline folder (for the definition see 2.1.2.1, "Offline Folders" on page 8) may be able to recover mailbox data.

Attention

Some settings in the user's Outlook client environment may cause an automatic replication at start time. This replication would synchronize the offline and server-based versions of the mailbox and thereby overwrite the offline storage file.

Therefore **do not start** the Outlook client for the user.

Follow these steps to recover data from the OST file:

1. Configure the profile to work offline. On the Mail and Fax icon on the Control Panel, double-click on **Microsoft Exchange Server** and click on **Work offline and use dial-up networking**. See Figure 54.

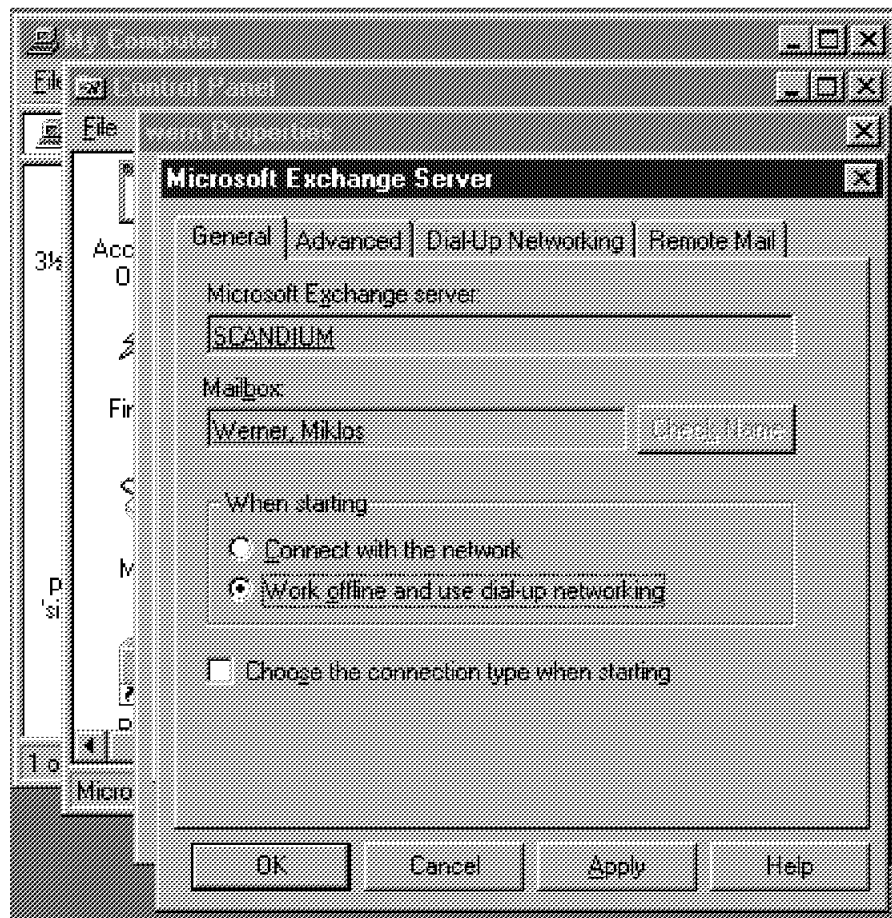


Figure 54. Preparation to Work Offline

2. Start up the Outlook client.
3. Select **File** and then **Import and Export**.
4. Export the offline mailbox to a PST file (for details see 3.3.2, "Using an Existing Personal Folder" on page 65).
5. Use the recovered data within the PST file to restore to a new server-based mailbox.

3.3.4 Restore to a Spare Server

If a Microsoft Exchange Server mailbox is deleted and neither an OST nor a PST file exists, you have to restore the information store to a spare machine. See Figure 55.

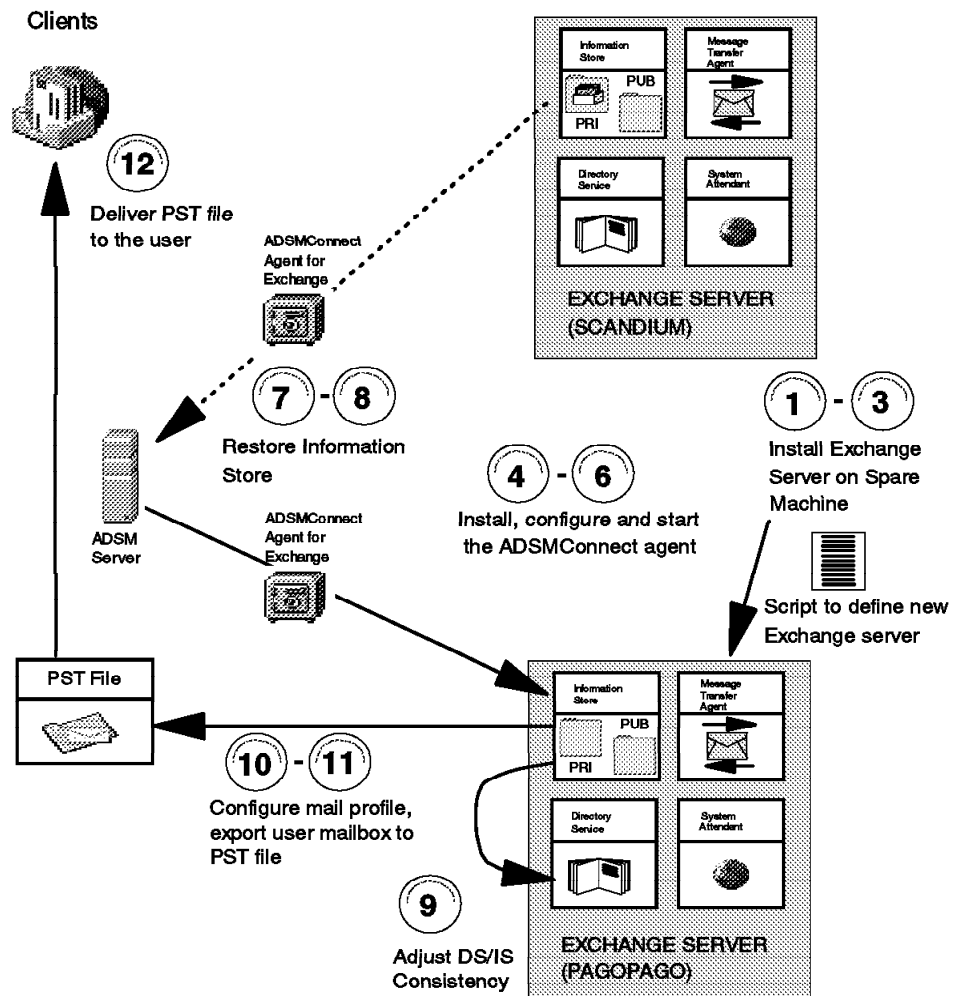


Figure 55. Steps to Restore to Spare Server

The spare machine could be used to restore any server-based mailbox within the entire organization. The spare machine can also contain installation code (software distribution of Microsoft Exchange Server and service packs) so that in the event of a disaster a full recovery server can be created.

To prevent any interaction with the production system, we recommend using a nonproduction service account to install Microsoft Exchange Server, restore databases, and export mailbox data to a PST file.

You must first set up and configure the spare server. You could do this in advance to be prepared for the restore. Follow these steps to prepare the spare server:

1. Build a spare Windows NT member server with the required service packs. There should be enough disk space to restore the entire information store.

2. Install Microsoft Exchange Server and create a new site with the same site and organization name that was used on the server from which you are restoring the mailbox.

Note

We suggest creating unattended installation scripts for the Microsoft Exchange Server within your organization to expedite the build process. For the sample scripts we used in our environment, see D.2, "Setup Script to Install Microsoft Exchange Server at a New Site" on page 83.

3. Install the Outlook client on the spare machine. This action will also install the Microsoft Exchange Server client if you need it in your environment. The Microsoft Exchange Server client is started from this executable:

c:\Program Files\Windows Messaging\exchng32.exe

4. Install the ADSMConnect Agent.

After this preparation you are ready to restore.

5. Configure the ADSMConnect Agent. The ADSMConnect Agent dsm.opt file must use the nodename used by the Microsoft Exchange Server you are attempting to recover.

6. Start the ADSMConnect Agent.

You need the ADSM client password of the ADSMConnect Agent for the restore process. If you do not know the client password, you can either:

- Use the ADSM scheduler service configuration utility, DSMCUTIL SHOWPW, if it is available at the original machine, to display the password. For details on how to use *DSMCUTIL*, see DSMCUTIL.TXT in the backup client directory.

or

- Set a new client password for the ADSMConnect Agent from an ADSM administrator.

7. Select the **Restore** tab and use the **Show All** button to display all possible restores. See Figure 56 on page 69.
8. Select the **Information Store** only (do not restore the directory), and click on the **Restore** button to start the restore process.

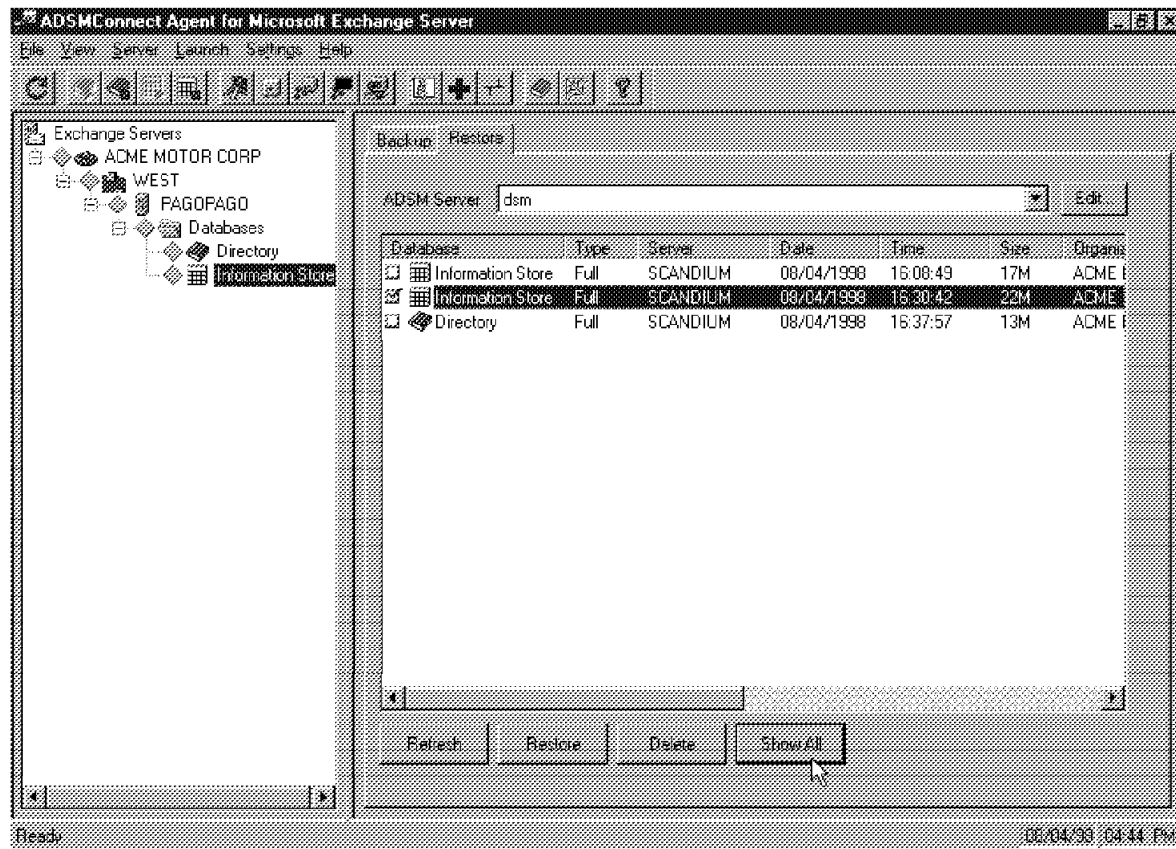


Figure 56. Start Microsoft Exchange Server Restore of Information Store

Note:

The SCANDIUM directory is displayed on the Restore window, but you cannot restore it to a Windows NT machine with a different NetBIOS name.

We restored the information store from SCANDIUM onto the PAGOPAGO server. When you click on the ADSMConnect Agent GUI **Refresh** button, you get an informational message because the ADSMConnect Agent checks the ADSM server for all possible PAGOPAGO restores done on a nodename of SCANDIUM. Use the **Show All** button to display all available restores of the SCANDIUM server.

9. From the Exchange Administrator execute the **DS/IS Consistency Adjustment**. This action creates a directory entry for all mailboxes within the information store.

To execute the DS/IS Consistency Adjustment, follow these steps:

- a. Select the server object.
- b. Choose **Properties** from the File menu.
- c. Select the **Advanced** tab.
- d. Select the **Consistency Adjuster** button.
- e. Ensure that Filter is set for All inconsistencies.

Figure 57 on page 70 shows the DS/IS Consistency Adjustment window before consistency adjustment starts.



Figure 57. Consistency Adjustment after Database Restore

10. Configure a mail profile for the user by selecting the Mail and Fax icon on the Control Panel.
11. Execute Microsoft Outlook and then export the server-based mailbox to a PST file. The size of the exported PST file may be very large depending on the amount of data within the user's server-based mailbox.
12. Deliver the PST file to the user through the network, tape, or disk.

3.3.5 Public Folder Recovery

If you have to restore a public folder, you can follow the same procedure as for a single mailbox restore. In the Exchange Administrator program, ensure that you add all required public folders to Folders on this Information Store (see Figure 58 on page 71). Select the properties of the public information store and select the **Instances** tab.

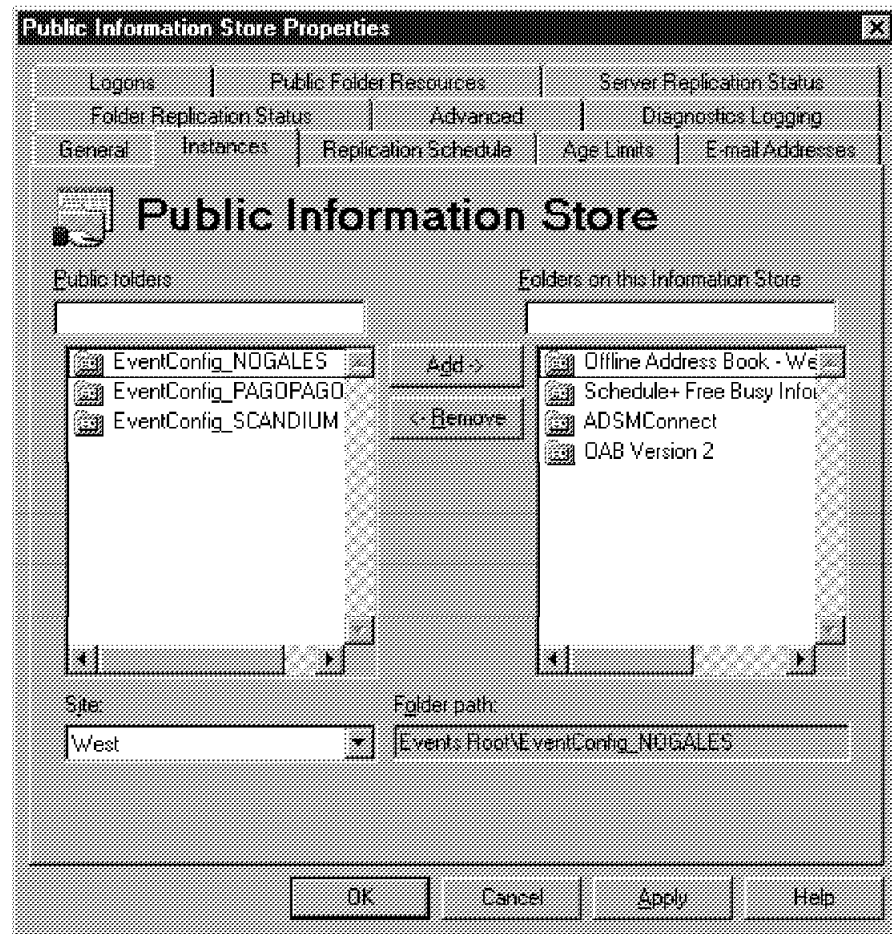


Figure 58. Public Information Store Instances Tab

3.4 Microsoft Exchange Server Disaster Recovery Planning

We define disaster recovery as the ability to recover from a situation where the Microsoft Exchange Server has been destroyed. As Microsoft Exchange Server clients are an essential component of the overall messaging architecture, they should be able to log on without modification after the server is recovered. In this section we outline the procedures for recovering the Microsoft Exchange Server in the event of a disaster.

3.4.1 Preparation

In preparation for disaster recovery we recommend that you complete the following steps in advance:

1. Create a server configuration sheet (see Table 1 on page 73) for every Microsoft Exchange Server and store them offsite. Server configuration sheets contain essential documentation that facilitate the recovery. They should be updated when any changes are made.
2. Build a recovery machine with sufficient disk space equal to that of the production data.
3. In a multiserver environment decide whether all servers within the same physical location will need to be recovered. Store required mailboxes on one

or more production servers, which will be recovered in the event of a disaster.

4. Limit the size of server-based mailboxes to ensure that databases do not grow to the point where it will be impossible to restore them.
5. Store tapes offsite.
6. In a test environment using the production data, record the actual time needed to complete a full recovery.
7. Place all production servers in a clean, air-conditioned, and physically secure environment.
8. Replicate public folder data to offsite servers.
9. Back up the configuration of Microsoft Exchange Server Internet Mail Connector and store it offsite. See 3.4.2, "Microsoft Exchange Server Internet Mail Connector: Backup and Restore" on page 73.

Table 1. Microsoft Exchange Server Configuration Sheet

Item	Description	Item	Description
NT (Netbios) Name		Exch Version	
Computer Model		Exch Org Name	
Serial Number		Exch Site Name	
Asset Number		Exch Srv Account	
CPU		Exch Srv Acct Pass	
RAM		Exch Connectors	
Network Interface #1		Perfwiz # Users	
IP Address		Perfwiz Server Type	
Subnet Mask		Perfwiz Org Users	
Default Gateway		Perfwiz Mem Usage	
Network Interface #2		Path to PRIV.EDB	
IP Address		Path to PUB.EDB	
Subnet Mask		Path to DIR.EDB	
Default Gateway		Path to IS Logs	
Hard Disk Config		Path to DS Logs	
NT Server Ver & SP		Path to MTA Files	
NT Server Role		Path to IMC Files	
NT Domain Name			
NT Install Directory			
NT Swap File			
NT Protocols			

3.4.2 Microsoft Exchange Server Internet Mail Connector: Backup and Restore

The Microsoft Exchange Server Internet Mail Connector is a Windows NT service that connects the Microsoft Exchange Server organization to the Internet. With the large increase of Internet mail flowing in and out of most companies, the Internet Mail Connector has become an important and essential messaging component.

The setup and configuration of the Microsoft Exchange Server Internet Mail Connector is extensive in large environments. Without some method of backing up and restoring the configuration of the Microsoft Exchange Server Internet Mail Connector, it is a time-consuming process.

Microsoft Exchange Server is distributed with a utility that allows you to back up and restore the configuration of the Microsoft Exchange Server Internet Mail Connector. The utility, imccopy.exe, is located on the Microsoft Exchange Server distribution in the following location:

`\server\support\utils\i386\imccopy.exe`

The command to back up the Internet Mail Connector configuration is:

`imccopy -save all <filename.txt>`

The command to restore the Internet Mail Connector configuration is:

```
imccopy -restore all <filename.txt>
```

The resulting configuration file should be backed up and stored offsite. For more information about imccopy.exe, see the Microsoft Exchange Server distribution in the following location:

\server\support\utils\readme.doc

3.5 Validating the Recovery

To validate the recovery of the Microsoft Exchange Server after a full server restore, check that:

- The Microsoft Exchange Server mailbox is associated with a primary Windows NT account.
- Distribution lists contain members.
- There are permissions on public folders.
- Windows NT Application Log reports no errors.
- The ADSM error logs report no errors.
- Messages are flowing to other servers within the same site and to external messaging systems such as the Internet.

You can verify that the distribution lists have the correct members by going to the Microsoft Exchange Administrator and selecting a distribution list (see Figure 59).



Figure 59. Microsoft Exchange Server Distribution List Properties

Use the Microsoft Exchange Administrator and review Client Properties on the selected public folder to verify that client permissions have not changed (see Figure 60).

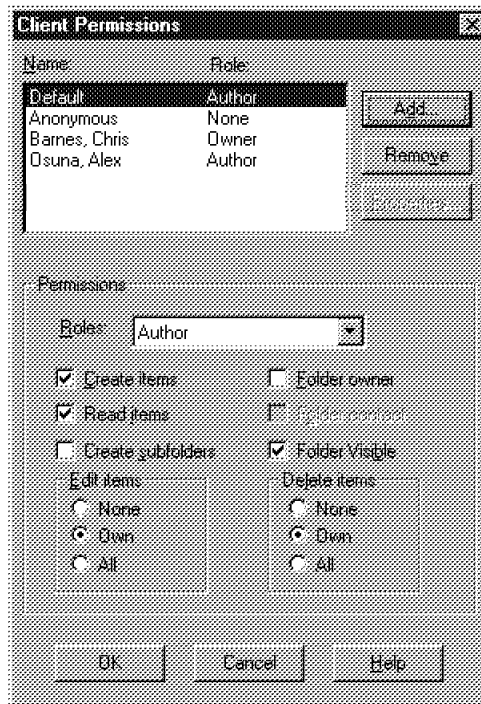


Figure 60. Microsoft Exchange Server Client Permissions on Public Folders

The Windows NT Event Viewer provides information about any errors that may have occurred as a result of the recovery of the Microsoft Exchange Server (see 2.3.12, “Windows NT Event Viewer” on page 38) for more information.

In the same way, ADSM messages are logged to whichever error logs you have set up. If you did not configure any specific logs, the default logs are found in the directory where the ADSMConnect Agent is installed:

EXCDISM.LOG
DSIERROR.LOG

For more information about setting up logging in the ADSMConnect Agent for Microsoft Exchange Server, see 2.3.14, “ADSMConnect Agent Log File Setup and Use” on page 43.

To determine whether messages are flowing correctly within the site or to external sources, turn on message tracking for the MTA site configuration, information store site configuration (see Figure 61 on page 76), and any additional connectors. Send a test message that uses configured connectors. Go to the Message Tracking Center (see Figure 62 on page 76) in the Microsoft Exchange Administrator to determine the results of your test messages.

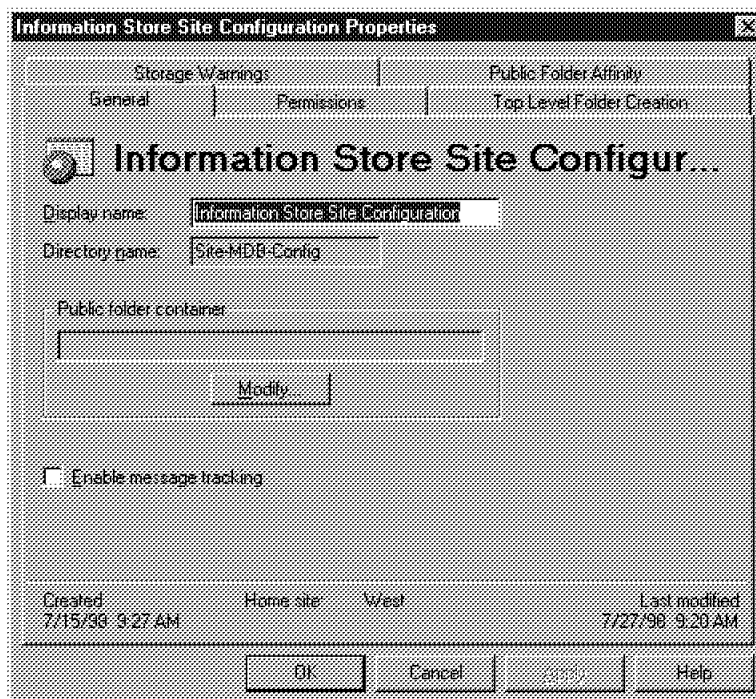


Figure 61. Microsoft Exchange Server Information Store Site Configurations

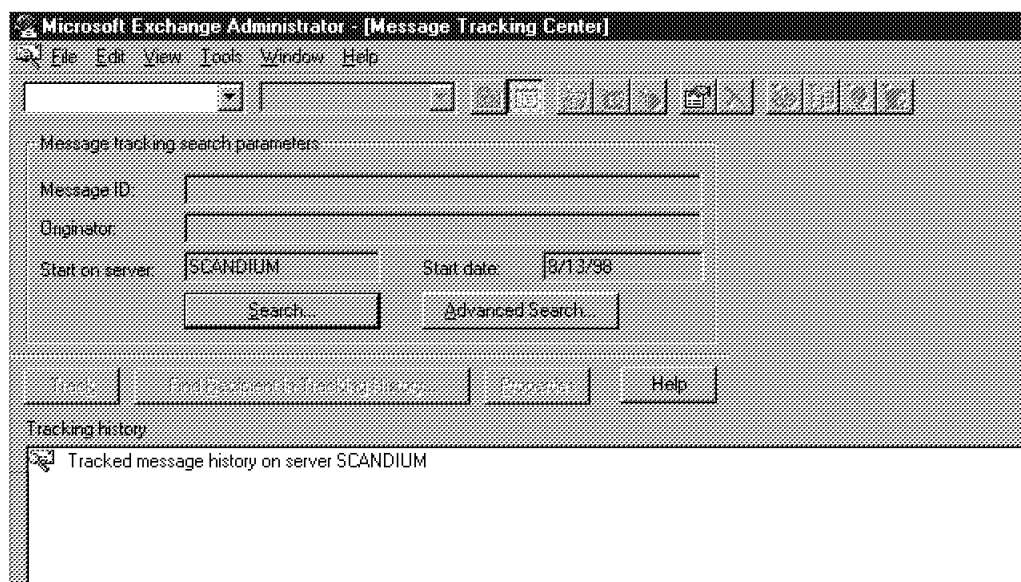


Figure 62. Microsoft Exchange Server Message Tracking Center

A Microsoft document entitled "XADM: How To Verify Exchange Online Backups" explains what to do to validate a backup. This method of validating a restored Microsoft Exchange Server involves restoring to a test server, validating the restore with certain commands, and checking for errors. This information can be found in the Microsoft Knowledge Base Article Q179308.

Appendix A. Information Store Considerations

In this appendix we discuss the size of the Microsoft Exchange Server information store and the methods to use to manage it.

A.1 Size

The Microsoft Exchange Server information store size is limited only by hardware in Version 5.5 enterprise and above. As the number of users increases, the Microsoft Exchange Server information store grows. Administrators should consider the effects of very large information stores and consolidate all users onto a few servers. The factors to be taken into account are:

- The time it takes to back up and restore the information store
- The ability to recover from a disaster
- The backup window timeframe available
- The expectations of users with regard to the amount of time it will take to recover the Microsoft Exchange Server
- The performance of backup hardware
- The performance impact of the Microsoft Exchange Server during an online backup
- The mean time between failures when using large disk storage for Microsoft Exchange Server databases
- The risk of consolidating all users onto a single server in the event of a system outage

The ADSMConnect Agent should be tested in your environment to ascertain the time frame to back up and restore your information store.

A.2 Use of Personal Folders (PSTs)

Users can implement local archiving of messages at the client. Microsoft Outlook clients can use the Archive feature to either automatically or selectively move messages out of the server-based mailbox into a PST file. The older Microsoft Exchange Server clients can implement the use of PST files to selectively move messages out of the server-based mailbox. PST files should be stored on a filesystem that is backed up.

A.2.1 Advantages

- PST files can be password protected.
- PST files can be encrypted and compressed.
- PST files can be copied, deleted, and moved between filesystems.
- Users can keep large information stores that far exceed the limits applied by the Microsoft Exchange Server administrator for the server-based mailbox.

A.2.2 Disadvantages

- Password protection of PST files can be easily broken.
- Single instance storage of messages is lost and will require additional space on other filesystems.
- Cannot be accessed through Outlook Web Access (HTTP) or Outlook Express (POP3/IMAP4) clients.
- Information within PST files cannot be shared with other users simultaneously.
- Requires additional filesystem space, backup, and configuration considerations.

A.3 Clean Mailbox

With the release of service pack 1 for Microsoft Exchange Server Version 5.5 an improved Clean Mailbox tool is available in the Microsoft Exchange Server Administrator program (see Figure 63). The updated Clean Mailbox is accessible on the Tools menu. Clean Mailbox can delete messages from selected mailboxes of Microsoft Exchange Server clients. Cleaning mailboxes can help decrease the size of the information store.

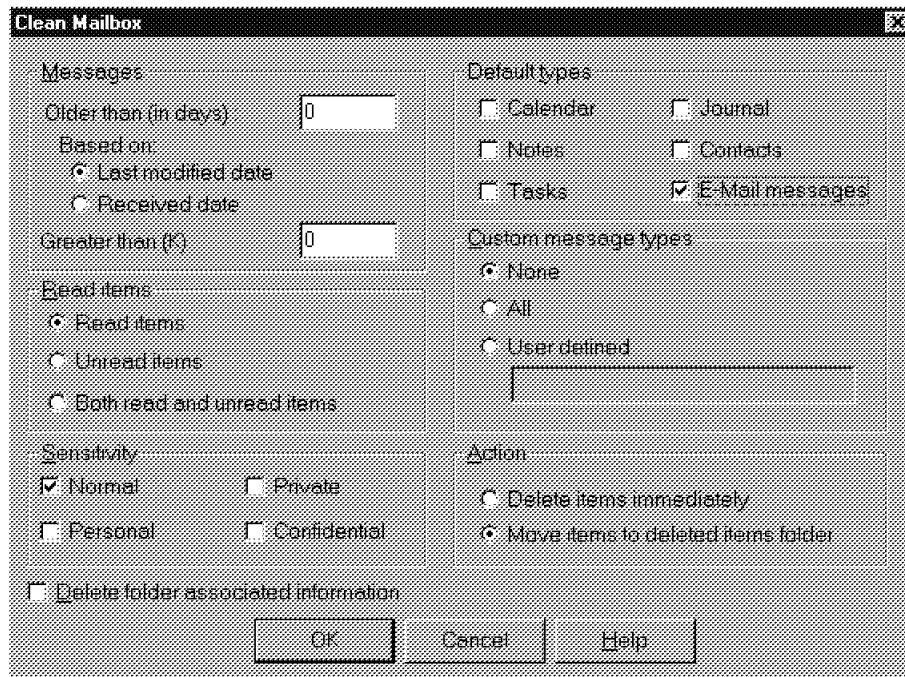


Figure 63. Clean Mailbox Configuration

Appendix B. Sample Offline Archive Command File

```
@ECHO OFF
rem *****
rem * This command file, C:\EXCHARCH.CMD, is specified as the OBJECT
rem * parameter in an ADSM Command Schedule. Once the ADSM schedule
rem * starts, EXCHARCH.CMD will run, and the NET STOP commands will
rem * quiesce the Microsoft Exchange Server, DSMC ARCH will archive
rem * the directories
rem * where the Exchange database exists, and the NET START commands
rem * will then restart the Exchange services.
rem * This script assumes that the ADSM client is installed in
rem * C:\ADSM\ directory. The -SU=Y is specified to include any files
rem * in any subdirectories beneath the archived directories.
rem * The -DESC= is specified to help easily identify the Microsoft Exchange Server
rem * Directory, Information Store with a label.
rem * Schedule information will be logged in
rem * C:\ADSM\BACLIENT\DSMSCHED.LOG and ADSM errors will be logged in
rem * C:\ADSM\BACLIENT\DSMERROR.LOG. The output file,
rem * C:\ADSM\BACLIENT\EXCHOUT.LOG, specified below, for output from
rem * the DSMC ARCHIVE command.
rem *****
C:
CD \

rem *****
rem * Stop the Microsoft Exchange Server services in the proper order:
rem * Microsoft Exchange Message Transfer Agent
rem * Microsoft Exchange Information Store
rem * Microsoft Exchange Directory service
rem * Microsoft Exchange System Attendant
rem *****
NET STOP MSEXCHANGEMTA
NET STOP MSEXCHANGEIS
NET STOP MSEXCHANGEDS
NET STOP MSEXCHANGESA

rem *****
rem * Run the ADSM Archives. Note that these commands are each written
rem * on one line.
rem *****
CD \ADSM\BACLIENT

DSMC ARCH -SU=Y -DESC="Daily Archive Directory" C:\EXCHSRVR\DSADATA\*
> C:\ADSM\BACLIENT\EXCHOUT.LOG
DSMC ARCH -SU=Y -DESC="Daily Archive Information Store"
C:\EXCHSRVR\MBDDATA\* >> C:\ADSM\BACLIENT\EXCHOUT.LOG

rem *****
rem * Start the Microsoft Exchange Server services in the proper order.
rem *****
NET START MSEXCHANGESA
NET START MSEXCHANGEDS
NET START MSEXCHANGEIS
NET START MSEXCHANGEMTA
```

Appendix C. Adding a New ADSM Management Class

This example uses the ADSM Administrative GUI from the ADSM for Microsoft Windows NT Intel Client Version 3 and lists the steps for adding a management class to an existing ADSM policy set and domain.

1. Bring up the ADSM Administrative GUI.
2. Expand **Policy Domains**.
3. Expand **Policy Sets**.
4. Double-click on **Management Classes**.
5. Locate the appropriate **Policy Domain Name** and highlight an existing management class.

When you are copying, select the latest one added, so you can copy all the previously defined copy groups to the new management class.

6. Click on **Edit** and then **Add** from the title bar.
7. Change the **Management class name** and the **Description**.
8. Be sure **Copy all copy groups** is selected, then click on **Add**.
9. Return to the Component Tree window and expand **Management Class**.
10. Double-click on **Backup Copy Group**.
11. Double-click on the item that corresponds to the management class you just created.
12. Make appropriate changes for the ADSMConnect Agent client.

You may leave the default values in place. Be sure the *If client data is deleted* has a value of zero.

13. Click on **OK**

The Archive Copy Group is not used by the ADSMConnect Agent for Microsoft Exchange Server; therefore, we will not update it.

14. Return to the Component Tree window and double-click on **Policy Sets**.
15. Locate the appropriate **Policy Domain Name** and highlight the **Policy Set**, other than **Active**, which was last to be activated. This will already include the other active management classes.
16. Click on **File** and then **Validate** from the title bar.
17. Click on **Validate** in the Policy Sets - Validate window.

If no **Archive Copy Group** was created, you will see an error message about this.

18. If there are no other messages, click on **OK**.
19. Leave the same policy set highlighted and click on **File** and then **Activate** from the title bar.
20. Click on **Activate** in the Policy Sets - Activate window.
21. Click on **OK**.
22. Go back to the Backup Copy Group window

You may have to refresh the window to see the change.

23. Click on **View** and then **Refresh Now** from the title bar.

You should see the new management class you just created with a **Policy Set Name** of **Active**.

24. Double-click on the management class object, and verify that the information is correct, as you just added it.

Appendix D. Unattended Setup Scripts for Microsoft Exchange Server

The sample scripts in the appendix can be used conjunction with the Microsoft Exchange Server setup program to install without user intervention. This setup method is helpful when installing a number of Microsoft Exchange Servers with the same configuration. It is not meant for full server recovery, which requires the use of the /R command line switch. Modification of these scripts is required for each Microsoft Exchange Server site and services account. Information about unattended setup can be found in Microsoft Knowledge Base article Q168490. Additional sample scripts can be found on the Microsoft Exchange Server CD in the ..\server\support\batsetup\setup directory.

D.1 Setup Script to Install Microsoft Exchange Server at an Existing Site

```
[Product ID]
cdkey=xxx-xxxxxxx

[Paths]
ServerDest=c:\exchsrvr

[Components]
Services=TRUE
Administrator=TRUE
MSMailConnector=FALSE
cc:Mail=FALSE
X400=FALSE
Active Server Components=FALSE
Sample Applications=FALSE
Books Online=FALSE
Event Service=FALSE

[Site]
ExistingServerName=SCANDIUM
[ServiceAccount]
AccountPassword=exchservice

[Licensing]
PerSeat=TRUE
```

D.2 Setup Script to Install Microsoft Exchange Server at a New Site

```
[Product ID]
cdkey=xxx-xxxxxxx

[Paths]
ServerDest=c:\exchsrvr
AdminDest=c:\exchsrvr

[Components]
Services=TRUE
Administrator=TRUE
MSMailConnector=FALSE
cc:Mail=FALSE
X400=FALSE
```

Active Server Components=FALSE
Sample Applications=FALSE
Books Online=FALSE
Event Service=FALSE

[Site]
SiteName=West

[Organization]
OrganizationName=ACME Motor Corp

[ServiceAccount]
AccountName=prandom1\exchservice
AccountPassword=exchservice

[Licensing]
PerSeat=TRUE

Appendix E. Sample Scripts and Command Files

E.1.1 Sample Command File to Install ADSM Scheduler

```
@ECHO OFF
rem *****
rem * After installing the ADSM Backup/Archive Client version 3, use
rem * this script, which invokes the ADSM scheduler installation
rem * utility, DSMUTIL.EXE to install a scheduler for the ADSMConnect
rem * Agent for Microsoft Exchange Server, and then issues the
rem * Microsoft NT NET START command to start the service.
rem * This script assumes that the ADSM client is installed in
rem * C:\ADSM\ directory. The ADSMConnect Agent NODENAME follows the
rem * naming convention of HOSTNAME or COMPUTERNAME, followed by an
rem * underscore (_) and EXCH, and the ADSMConnect Agent PASSWORD is
rem * the same as the nodename. The ADSMConnect Agent Scheduler has
rem * a name of, the bar "ADSM MExchange Scheduler", the schedule log
rem * has a name of, C:\ADSM\AGENTEXC\EXCHSCHED.LOG, and the error log
rem * has a name of, C:\ADSM\AGENTEXC\EXCHERROR.LOG.
rem *****
set ba_dir=C:\ADSM\BACLIENT
set exc_dir=C:\ADSM\AGENTEXC
set cl_name=%computername%_exch
set cl_pwd=%cl_name%
c:
cd %ba_dir%
rem *****
rem * The following command is written on one line.
rem *****

dsmcutil install /NAME:"ADSM MExchange Scheduler"
/OPTFILE:%exc_dir%\dsm.opt /NODE:%cl_name% /PASSWORD:%cl_pwd%
/AUTOSTART&GML.yes /SCHEDLOG:%exc_dir%\exchsched.log
/ERRORLOG:%exc_dir%\excherror.log

net start "ADSM MExchange Scheduler"
```

E.1.2 ADSMConnect Agent Backups

```
@ECHO OFF
rem *****
rem * MODIFIED excfull.smp sample command file for a full online backup
rem * of Microsoft Exchange Server using ADSMConnect Agent. This
rem * command file, C:\ADSM\AGENTEXC\SCRIPTS\EXCHFULL.CMD, is specified
rem * as the OBJECT parameter in an ADSM Command Schedule. Once the
rem * ADSM schedule starts, EXCHFULL.CMD will run, invoking the
rem * ADSMConnect Agent command line backup.
rem * This script assumes that the ADSMConnect Agent for Microsoft
rem * Exchange Server is installed in C:\ADSM\AGENTEXC directory.
rem * The ADSM Schedule Service was previously installed with certain
rem * log designations. Schedule information will be logged in
rem * C:\ADSM\AGENTEXC\EXCHSCHED.LOG, certain ADSM errors will be
rem * logged in C:\ADSM\AGENTEXC\EXCERROR.LOG. ADSM API errors will
rem * be logged in C:\ADSM\AGENTEXC\DSIERROR.LOG and ADSMConnect
rem * Agent activity will be logged in C:\ADSM\AGENTEXC\EXCHFULL.OUT
rem * for both Directory and Information Store full backups. The
```

```

rem * output file, C:\ADSM\AGENTEXC\SCANDIUM.OUT, will document the
rem * output from the backup commands after being updated with the
rem * date and time.
rem *****

SET EXC_DIR=C:\ADSM\AGENTEXC
C:
CD %exc_dir%

rem *****
rem * Put a date and time stamp in the output log file.
rem *****

DATE < NUL >> %exc_dir%\SCANDIUM.OUT
TIME < NUL >> %exc_dir%\SCANDIUM.OUT

rem *****
rem * Execute the ADSMConnect Agent commandline to perform full backups
rem * on the Microsoft Exchange Server Directory and Information Store.
rem *****

%exc_dir%\EXCDSMC /BACK:DIR,FULL /LOGF:%exc_dir%\EXCHFULL.LOG >>
%exc_dir%\SCANDIUM.OUT

%exc_dir%\EXCDSMC /BACK:IS,FULL /LOGF:%exc_dir%\EXCHFULL.LOG >>
%exc_dir%\SCANDIUM.OUT

```

E.1.3 ADSMConnect Agent Backups and Central Logging

```

@ECHO OFF
rem *****
rem * MODIFIED EXCHFULL.CMD command file for a full online backup
rem * of Microsoft Exchange Server using ADSMConnect Agent. This
rem * command file, C:\ADSM\AGENTEXC\SCRIPTS\EXCHFUL2.CMD, is specified
rem * as the OBJECT parameter in an ADSM Command Schedule. Once the
rem * ADSM schedule starts, EXCHFULL.CMD will run, invoking the
rem * ADSMConnect Agent command line backup.
rem * This script assumes that the ADSMConnect Agent for Microsoft
rem * Exchange Server is installed in C:\ADSM\AGENTEXC directory.
rem * The ADSM Schedule Service was previously installed with certain
rem * log designations. Schedule information will be logged in
rem * C:\ADSM\AGENTEXC\EXCHSCHED.LOG, certain ADSM errors will be
rem * logged in C:\ADSM\AGENTEXC\EXCERROR.LOG. ADSM API errors will
rem * be logged in C:\ADSM\AGENTEXC\DSIERROR.LOG and ADSMConnect
rem * Agent activity will be logged in C:\ADSM\AGENTEXC\EXCHFULL.OUT
rem * for both Directory and Information Store full backups. The
rem * output file, SCANDIUM.OUT, is created at another server, LADOGA,
rem * which is a utility server used for multiple administrative
rem * purposes, including central logging. LADOGA has a share drive,
rem * \\LADOGA\CENTLOG\, with create access for everyone. SCANDIUM.LOG
rem * will document the output from the backup commands after being
rem * updated with the date and time.
rem *****

SET EXC_DIR=C:\ADSM\AGENTEXC
SET CENT_LOG=\\LADOGA\CENTLOG\
C:
CD %exc_dir%

```



```

rem *****
rem * Put a date and time stamp in the output log file.
rem *****

DATE < NUL >> %cent_log%\SCANDIUM.OUT
TIME < NUL >> %cent_log%\SCANDIUM.OUT

rem *****
rem * Execute the ADSMConnect Agent commandline to perform full backups
rem * on the Microsoft Exchange Server Directory and Information Store
rem * and send the output to the share drive located at utility server,
rem * LADOGA.
rem *****

%exc_dir%\EXCDSMC /BACK:DIR,FULL /LOGF:%exc_dir%\EXCHFULL.LOG >>
%cent_log%\SCANDIUM.OUT

%exc_dir%\EXCDSMC /BACK:IS,FULL /LOGF:%exc_dir%\EXCHFULL.LOG >>
%cent_log%\SCANDIUM.OUT

```

E.1.4 ADSMConnect Agent Backups, Central Logging, and Log Pruning

```

@ECHO OFF
rem *****
rem * MODIFIED EXCHFULL.CMD command file for a full online backup
rem * of Microsoft Exchange Server using ADSMConnect Agent. This
rem * command file, C:\ADSM\AGENTEXC\SCRIPTS\EXCHFUL3.CMD, is specified
rem * as the OBJECT parameter in an ADSM Command Schedule. Once the
rem * ADSM schedule starts, EXCHFULL.CMD will run, invoking the
rem * ADSMConnect Agent command line backup.
rem * This script assumes that the ADSMConnect Agent for Microsoft
rem * Exchange Server is installed in C:\ADSM\AGENTEXC directory.
rem * The ADSM Schedule Service was previously installed with certain
rem * log designations. Schedule information will be logged in
rem * C:\ADSM\AGENTEXC\EXCHSCHED.LOG, certain ADSM errors will be
rem * logged in C:\ADSM\AGENTEXC\EXCERROR.LOG. ADSM API errors will
rem * be logged in C:\ADSM\AGENTEXC\DSIERROR.LOG and ADSMConnect
rem * Agent activity will be logged in C:\ADSM\AGENTEXC\EXCHFULL.OUT
rem * for both Directory and Information Store full backups. The
rem * output file, SCANDIUM.OUT, is created at another server, LADOGA,
rem * which is a utility server used for multiple administrative
rem * purposes, including central logging. LADOGA has a share drive,
rem * \\LADOGA\CENTLOG\, with create access for everyone. SCANDIUM.LOG
rem * will document the output from the backup commands after being
rem * updated with the date and time.
rem * Then the local log file will be copied and deleted, so that only
rem * the last backup and the current backup activities will be on the
rem * local disk. Old copies are archived and deleted by the ADSM
rem * BAClient.
rem *****

SET EXC_DIR=C:\ADSM\AGENTEXC\
SET CENT_LOG=\\LADOGA\CENTLOG\
SET OLD_LOG=C:\ADSM\AGENTEXC\OLDLOGS\
SET ADSM_DIR=C:\ADSM\BACLIENT\

C:
CD %exc_dir%

```

```

rem *****
rem * Put a date and time stamp in the output log file.
rem *****

DATE < NUL >> %cent_log%\SCANDIUM.OUT
TIME < NUL >> %cent_log%\SCANDIUM.OUT

rem *****
rem * Execute the ADSMConnect Agent commandline to perform full backups
rem * on the Microsoft Exchange Server Directory and Information Store
rem * and send the output
rem * to the share drive located at utility server, LADOGA.
rem *****

%exc_dir%\EXCDSMC /BACK:DIR,FULL /LOGF:%exc_dir%\EXCHFULL.LOG >>
%cent_log%\SCANDIUM.OUT

%exc_dir%\EXCDSMC /BACK:IS,FULL /LOGF:%exc_dir%\EXCHFULL.LOG >>
%cent_log%\SCANDIUM.OUT

rem *****
rem * Copy the ADSMConnect Agent old log file to OLDLOGS
rem * directory, and rename
rem * the current log file to EXCHFULL.ARC. Then run ADSM ARCHIVE with
rem * delete option on the old log file in OLDLOGS directory.
rem *****

MOVE %exc_dir%\EXCHFULL.ARC %old_log%\
REN %exc_dir%\EXCHFULL.LOG EXCHFULL.ARC
CD %adsm_dir%
DSMC ARCH -DELETEFILES %old_log%\*.*

```

E.1.5 Perl Script for Deleting Old ADSMConnect Agent Backups

Place a call statement at the bottom of your backup command file, specifying the Perl executable, perl; this filename: exc_list_old_dbs.pl; the days, <days>; the input file, in.txt; and the output file, out.txt.

Note

The Perl script reproduced here was copied from an original file transmission. The font is small so that you can see the script exactly as it should look. We obtained the script from a public forum during the project. We did not write the script, and we do not support it.

```

#!/perl.exe
#
#   exc_list_old_dbs.pl
#
#   This script generates a list of exchange databases which are
#   greater than $ARGV[0] days old and writes them to
#   a temporary file

# allow window to be specified as a parameter

if ($ARGV[0]) { $w=$ARGV[0]; } else { $w=7; }

$start=0;

open (OUT,">$ARGV[2]") || die "ERROR: can't open \"$ARGV[2]\" \n";
open (IN,"$ARGV[1]");

```

```

# evaluate 7 days ago date string

@days=(31,28,31,30,31,30,31,31,30,31,30,31);
(@now)=localtime(time);

# check numbers for 0 padding and millenium

if ( $now[5]=~ /\^9[89]$/ ) { $now[5]= ~s/\^/19/; }
elsif ( $now[5]=~ /\^[0..9][0..7]$/ ) { $now [5]=~s/\^/20/; }

# note above should be valid for 100 yrs or until the year is 4 digits

if (length($now[4]+=1)==1) { $now[4]=~s/\^/0/; }
if (length($now[3])==1) { $now[3]=~s/\^/0/; }

# decide if year is a leap year
# if a year is exactly divisible by 4 and NOT exactly divisible
# by 100 but is divisible by 400

if (($now[5]%4==0 && $now[5]%100!=0)||($now[5&rb rk.%100==0 && $now [5]%400==0))
{ $days[1]=29; }

# now derive 7 days ago marker

if ($now[4]== '01' && $now[3] < '07') {
    $ago7=($now[5]-1).'12'.sprintf("%02.2d",31-$w+$now[3]);
}
elsif ($now[3] < '08') {
    $ago7=$now[5].sprintf("%02d%02d",$now[4]-1,$days[$now[4]-2]-$w+$now[3]);
}
else { $ago7=$now[5].$now[4].sprintf("%02d",$now[3]-$w); }

# process each line of adsm report and write old logs to OUT

while (<IN>) {
    if (/^-----/) { $start = 1; next; }
    if ($start && /\^[a-zA-Z]/) {
        chop;
        (@fields)=split(/[ ]+/);
        ($m,$d,$y)=split('/', $fields[3]);
        $testnum=$y.$m.$d;
        if($testnum<$ago7) {
            $cut=join(' ', $fields[0] ,',', $fields[5&rb rk.,"\\n");
            push(@array,$cut); }
        }
    }
}
print OUT @array;
close OUT;
close IN;

exit 0;

# end of script

```

Appendix F. Special Notices

This publication is intended to help administrators of Microsoft Exchange Server use ADSM to back up and recover their data. It can also be used by ADSM administrators seeking an understanding of how ADSM can be used with Microsoft Exchange Server. The information in this publication is not intended as the specification of any programming interfaces that are provided by ADSM. See the PUBLICATIONS section of the IBM Programming Announcement for ADSM for more information about what publications are considered to be product documentation.

References in this publication to IBM products, programs or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM product, program, or service is not intended to state or imply that only IBM's product, program, or service may be used. Any functionally equivalent program that does not infringe any of IBM's intellectual property rights may be used instead of the IBM product, program or service.

Information in this book was developed in conjunction with use of the equipment specified, and is limited in application to those specific hardware and software products and levels.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM Corporation, Dept. 600A, Mail Drop 1329, Somers, NY 10589 USA.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Any pointers in this publication to external Web sites are provided for convenience only and do not in any manner serve as an endorsement of these Web sites.

The following terms are trademarks of the International Business Machines Corporation in the United States and/or other countries:

ADSTAR®
AIX/6000®
DATABASE 2

AIX®
AS/400®
DB2®

HACMP/6000
LAN Distance®
MVS® (logo)
MVS/ESA
RS/6000
SQL/DS

IBM®
Magstar
MVS/DFP
NetView®
S/390®
StorageSmart

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

Java and HotJava are trademarks of Sun Microsystems, Incorporated.

Microsoft, Windows, Windows NT, and the Windows 95 logo are trademarks or registered trademarks of Microsoft Corporation.

PC Direct is a trademark of Ziff Communications Company and is used by IBM Corporation under license.

Pentium, MMX, ProShare, LANDesk, and ActionMedia are trademarks or registered trademarks of Intel Corporation in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Limited.

Other company, product, and service names may be trademarks or service marks of others.

Appendix G. Related Publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this redbook.

G.1 International Technical Support Organization Publications

For information on ordering these ITSO publications see "How to Get ITSO Redbooks" on page 97.

G.1.1 ADSM Redbooks

Book Title	Publication Number
General Topics	
ADSM Concepts	SG24-4877
ADSM Version 2 Presentation Guide	SG24-4532
ADSM Version 3 Technical Guide	SG24-2236
A Practical Guide to Network Storage Manager	SG24-2242
ADSM Advanced Implementation Experiences	GG24-4221
Using ADSM Hierarchical Storage Management	SG24-4631
Client Disaster Recovery: Bare Metal Restore	SG24-4880
Server Books	
ADSM Server for Windows NT Configuration and Recovery Examples	SG24-4878
Getting Started with ADSM/6000	GG24-4421
ADSM for AIX: Advanced Topics	SG24-4601
AIX Tape Management	SG24-4705
ADSTAR Distributed Storage Manager/6000 on 9076 SP2	GG24-4499
ADSM for MVS: Recovery and Disaster Recovery	SG24-4537
ADSM for MVS: Using Tapes and Tape Libraries	SG24-4538
Getting Started with ADSM/2	GG24-4321
ADSM for OS/2: Advanced Topics	SG24-4740
Setting Up and Implementing ADSTAR Distributed Storage Manager/400	GG24-4460
ADSM/VSE Implementation Guide	SG24-4266
Specific Client Books	
Getting Started with ADSM NetWare Clients	GG24-4242
Getting Started with ADSM AIX Clients	GG24-4243
ADSM API Examples for OS/2 and Windows	SG24-2588
Windows NT Backup and Recovery with ADSM	SG24-2231
ADSM with Other Products	
ADSM Reporting with SAMS:Vantage	SG24-5271
Using ADSM to Back Up Databases	SG24-4335
Using ADSM to Back Up Lotus Notes	SG24-4534
Hierarchical Storage Management for NetWare: ADSM and AvailHSM Implementation	SG24-4713
Using ADSM to Back Up OS/2 LAN Server and Warp Server	SG24-4682
Backup, Recovery, and Availability with DB2 Parallel Edition on RISC/6000	SG24-4695

G.1.2 Tivoli Redbooks

Book Title	Publication Number
TME 10 Cookbook for AIX Systems Management and Networking Applications	SG24-4867
Understanding Tivoli's TME 3.0 and TME 10	SG24-4948

G.2 Redbooks on CD-ROMs

Redbooks are also available on CD-ROMs. **Order a subscription** and receive updates 2-4 times a year at significant savings.

CD-ROM Title	Subscription Number	Collection Kit Number
System/390 Redbooks Collection	SBOF-7201	SK2T-2177
Networking and Systems Management Redbooks Collection	SBOF-7370	SK2T-6022
Transaction Processing and Data Management Redbook	SBOF-7240	SK2T-8038
Lotus Redbooks Collection	SBOF-6899	SK2T-8039
Tivoli Redbooks Collection	SBOF-6898	SK2T-8044
AS/400 Redbooks Collection	SBOF-7270	SK2T-2849
RS/6000 Redbooks Collection (HTML, BkMgr)	SBOF-7230	SK2T-8040
RS/6000 Redbooks Collection (PostScript)	SBOF-7205	SK2T-8041
RS/6000 Redbooks Collection (PDF Format)	SBOF-8700	SK2T-8043
Application Development Redbooks Collection	SBOF-7290	SK2T-8037

G.3 ADSM Product Publications

Book Title	Publication Number
ADSM V3R1 Messages	GC35-0271
ADSM V3R1 AIX Quick Start	GC35-0273
ADSM V3R1 AIX Administrator's Guide	GC35-0274
ADSM V3R1 AIX Administrator's Reference	GC35-0275
ADSM V3R1 MVS quick Start	GC35-0276
ADSM V3R1 MVS Administrator's Guide	GC35-0277
ADSM V3R1 MVS Administrator's Reference	GC35-0278
ADSM V3R1 AIX License	SC35-0283
ADSM V3R1 MVS License	GC35-0284
ADSM V3R1 Windows NT Administrator's Guide	GC35-0292
ADSM V3R1 Windows NT Administrator's Reference	GC35-0293
ADSM V3R1 Windows NT License	SC35-0294
ADSM V3R1 Windows NT Quick Start	GC35-0295
ADSM V3R1 Using the UNIX Backup-Archive Client	SH26-4075
ADSM V3R1 Using the OS/2 Backup-Archive Client	SH26-4076
ADSM V3R1 Using the Novell NetWare Backup-Archive Client	SH26-4077
ADSM V3R1 Using the Microsoft Windows Backup-Archive Client	SH26-4078
ADSM V3R1 Installing the Clients	SH26-4080
ADSM V3R1 Using the Application Programming Interface	SH26-4081
ADSM V3R1 Trace Facility Guide	SH26-4082
ADSM V3R1 Client Reference Cards	SX26-6019
ADSM V3R1 Using the OS/2 Lotus Notes Backup Agent	SH26-4084
ADSMConnect for Oracle7 Backup on AIX Installation & User's Guide	SH26-4061
ADSMConnect for Oracle Backup on Sun Solaris Installation and User's Guide	SH26-4063
ADSMConnect for Lotus Notes on Windows NT Installation and User's Guide	SH26-4065
ADSMConnect for Lotus Notes on AIX NT Installation and User's Guide	SH26-4067
ADSMConnect for Microsoft SQL Server Installation and User's Guide	SH26-4069

G.4 ADSM Online Product Library

CD-ROM Title	Publication Number
ADSM V3R1 MVS Online Product Library	SK3T-1396

G.5 Tivoli Publications

Book Title	Publication Number
TME 10 Tivoli/Plus for ADSM User's Guide	GC31-8405
Tivoli/ADE Documentation Kit Volume 1	SK2T-6062
Tivoli/ADE Documentation Kit Volume 2	SK2T-6063
Tivoli/ADE Documentation Kit Volume 3	SK2T-6064
Tivoli/ADE Documentation Kit Volume 4	SK2T-6065

How to Get ITSO Redbooks

This section explains how both customers and IBM employees can find out about ITSO redbooks, CD-ROMs, workshops, and residencies. A form for ordering books and CD-ROMs is also provided.

This information was current at the time of publication, but is continually subject to change. The latest information may be found at <http://www.redbooks.ibm.com/>.

How IBM Employees Can Get ITSO Redbooks

Employees may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Redbooks Web Site on the World Wide Web**

<http://w3.itso.ibm.com/>

- **PUBORDER** — to order hardcopies in the United States

- **Tools Disks**

To get LIST3820s of redbooks, type one of the following commands:

```
TOOLCAT REDPRINT
TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET SG24xxxx PACKAGE
TOOLS SENDTO CANVM2 TOOLS REDPRINT GET SG24xxxx PACKAGE (Canadian users only)
```

To get BookManager BOOKs of redbooks, type the following command:

```
TOOLCAT REDBOOKS
```

To get lists of redbooks, type the following command:

```
TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT
```

To register for information on workshops, residencies, and redbooks, type the following command:

```
TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1998
```

- **REDBOOKS Category on INEWS**

- **Online** — send orders to: USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (<http://www.redbooks.ibm.com/redpieces.html>). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

How Customers Can Get ITSO Redbooks

Customers may request ITSO deliverables (redbooks, BookManager BOOKs, and CD-ROMs) and information about redbooks, workshops, and residencies in the following ways:

- **Online Orders** — send orders to:

In United States:
In Canada:
Outside North America:

IBMMAIL
usib6fpl at ibmmail
caibmbkz at ibmmail
dkibmbsh at ibmmail

Internet
usib6fpl@ibmmail.com
lmannix@vnet.ibm.com
bookshop@dk.ibm.com

- **Telephone Orders**

United States (toll free)
Canada (toll free)

1-800-879-2755
1-800-IBM-4YOU

Outside North America
(+45) 4810-1320 - Danish
(+45) 4810-1420 - Dutch
(+45) 4810-1540 - English
(+45) 4810-1670 - Finnish
(+45) 4810-1220 - French

(long distance charges apply)
(+45) 4810-1020 - German
(+45) 4810-1620 - Italian
(+45) 4810-1270 - Norwegian
(+45) 4810-1120 - Spanish
(+45) 4810-1170 - Swedish

- **Mail Orders** — send orders to:

IBM Publications
Publications Customer Support
P.O. Box 29570
Raleigh, NC 27626-0570
USA

IBM Publications
144-4th Avenue, S.W.
Calgary, Alberta T2P 3N5
Canada

IBM Direct Services
Sortemosevej 21
DK-3450 Allerød
Denmark

- **Fax** — send orders to:

United States (toll free)
Canada
Outside North America

1-800-445-9269
1-403-267-4455
(+45) 48 14 2207 (long distance charge)

- **1-800-IBM-4FAX (United States) or (+1)001-408-256-5422 (Outside USA)** — ask for:

Index # 4421 Abstracts of new redbooks
Index # 4422 IBM redbooks
Index # 4420 Redbooks for last six months

- **On the World Wide Web**

Redbooks Web Site
IBM Direct Publications Catalog

<http://www.redbooks.ibm.com/>
<http://www.elink.ibm.link.ibm.com/pbl/pbl>

Redpieces

For information so current it is still in the process of being written, look at "Redpieces" on the Redbooks Web Site (<http://www.redbooks.ibm.com/redpieces.html>). Redpieces are redbooks in progress; not all redbooks become redpieces, and sometimes just a few chapters will be published this way. The intent is to get the information out much quicker than the formal publishing process allows.

IBM Redbook Order Form

Please send me the following:

Title	Order Number	Quantity

First name	Last name
------------	-----------

Company

Address

City	Postal code	Country
------	-------------	---------

Telephone number	Telefax number	VAT number
------------------	----------------	------------

• Invoice to customer number _____

• Credit card number _____

Credit card expiration date	Card issued to	Signature
-----------------------------	----------------	-----------

We accept American Express, Diners, Eurocard, Master Card, and Visa. Payment by credit card not available in all countries. Signature mandatory for credit card payment.

Index

Special Characters

*exc_mountwait 28

A

accounting records 33
ADSM ARCHIVE 11
ADSM command schedule, automating 11
ADSM overview 4
archive copy group 23
archive files 16
archive folders 9
ARCHIVE schedules 12
archives 13
AT command, scheduling with 14

B

backup command 1
backup/archive client 4
buffer size 31

C

capacity planning
 accounting records 33
 communications wait 34
 data throughput 35
 database queries 36
 idle wait 34
 network 31
 performance bottlenecks 33
 performance monitor 33
 server perspective 34
 system log 38
central logging 86
circular logging 19
client options
 *exc_mountwait 28
 compression 26
 nodename 26
 passwordaccess generate 27
 TAPEPROMPT 29
 tcpbuffsize 25
 tcpclientaddress 25
 tcpclientport 26
 tcpwindowsize 25
client options file 25
client options recommendations
 different versions 25
client password 68
communication protocols 18
communications wait 34

components 1
compression 26
configuration 8
configuration file, IMC 74
configuration sheet 71
core components 7

D

data throughput 35
database copies, backup 13
database files 11
database queries 36
database recovery
 full server 56
 individual mailboxes 60
 introduction to 51
 machine security 55
 new hardware 54
 new site 58
 NT server names 55
 offline backups 51
 online backups 54
 requirements 55
 retrieve options 53
day-to-day operation 7
deleted item recovery 61
deletefiles 14
deleting old backup copies 49
deleting old backups, PERL script 88
description 14
directory database 1
directory service 1, 7, 15
 online backup 17
disaster recovery planning
 configuration sheet 71
 multiserver environment 71
 public folder replication 72
 recovery machine 71
 server-based mailboxes 72
 tapes offsite 72
DNS entry 58
DS/IS consistency adjustment 69
DSMCUTIL SHOWPW 59
DSMCUTIL.EXE 44
DSMERROR.LOG 10
DSMSCHED.LOG 10, 35

E

event viewer 75
EXCDISM.LOF file, sample 43
exchange services 17
exclude statements 12

EXCSCHED.LOG 35

F

FAV files 16
files 8
full server restore 56

I

idle wait 34
imccopy 74
include statement 10
incremental backups 11
information store 1, 7
 clean mailbox 78
 maintenance 24
 online maintenance 24
 personal folders 77
 size 77
information store considerations 77
information store restore 60
installation 7
installation scripts 68
internet mail connector
 configuration backup 73
 service description 73

K

key management 16
key management service files 16

L

log file setup 43
log files 48
log pruning 87

M

machine security 55
mail connector 16
mail profile 17
management class, adding 81
management class, adding new 23
management class, default 22
management class, separate 22
message connector 16
message transfer agent 1, 7
modifying logging 43
MTA service 7
multiserver environment 71

N

NET START 11
NET START commands 13
NET STOP 11

new hardware 54
nodename 26
NT backup program 2
NT server names 55

O

objects, expiring 48
offline address book 2
offline archive command file 79
offline backup 1, 4, 7
offline backups with ADSM 10
offline folders 8
offline periods 10
online backup 1, 4, 7, 15
 directory service 15
 Microsoft Exchange Server 15
 private information 15
 public information 15
 transaction logs 15
online maintenance 24
operating systems 18
OPTIONS, scheduling 14
OST files 8
outlook bar favorites 9
outlook client
 archive folders 9
 configuration 8
 core components 7
 data 7
 directory service 7
 files 8
 information store 7
 message transfer agent 7
 offline folders 8
 OST files 8
 outlook bar favorites 9
 personal address book 9
 personal folders 9
 system attendant 7
outlook client, spare machine build 68

P

PAB files 16
passwordaccess generate 27
performance monitor 33
performance settings
 buffers 29
personal address book 9
personal folders 9
point-in-time backups 19
policy domain 15
private database 1
private information 15
PST files 16, 60
public database 1
public folder replication 72

public information 15

Q

query schedule 15

R

recovery machine 71
regeditor 63
registry update 64
requirements for recovery 55
restoring individual mailboxes 60

S

scheduled operations 44
scheduler service 44
scheduling and maintenance 47
separate ADSM scheduler service 44
server perspective 34
server properties 24
server-based mailboxes 72
setup 7
spare server, restoring mailboxes to 67
START EXCDSMC 50
subdirectories, backup 12
supported environments
 ADSM server versions 18
 adsmconnect scheduling 18
 communication protocols 18
 exchange servers 18
 hardware 18
 operating systems 18
system attendant 1, 7
system log 38

T

TAPEPROMPT 29
tapes offsite 72
tcpbuffsize 25
tcpclientaddress 25
tcpclientport 26
tcpwindowsize 25
transaction logs 15, 18

U

unattended setup scripts 83
uncommitted data 18
user mailbox recovery
 consistency adjustment 70
 database restore 70
 deleted items 61
 PST file 70
 server object 69

V

validating the recovery 74
verbose 14
VERDELETED 23

ITSO Redbook Evaluation

Using ADSM to Back Up and Recover Microsoft Exchange Server
SG24-5266-00

Your feedback is very important to help us maintain the quality of ITSO redbooks. **Please complete this questionnaire and return it using one of the following methods:**

- Use the online evaluation form found at <http://www.redbooks.ibm.com>
- Fax this form to: USA International Access Code 914 432 8264
- Send your comments in an Internet note to redbook@us.ibm.com

Which of the following best describes you?

☐ **Customer** ☐ **Business Partner** ☐ **Solution Developer** ☐ **IBM employee**
☐ **None of the above**

Please rate your overall satisfaction with this book using the scale:
(1 = very good, 2 = good, 3 = average, 4 = poor, 5 = very poor)

Overall Satisfaction _____

Please answer the following questions:

Was this redbook published in time for your needs? Yes_____ No_____

If no, please explain:

What other redbooks would you like to see published?

Comments/Suggestions: **(THANK YOU FOR YOUR FEEDBACK!)**

