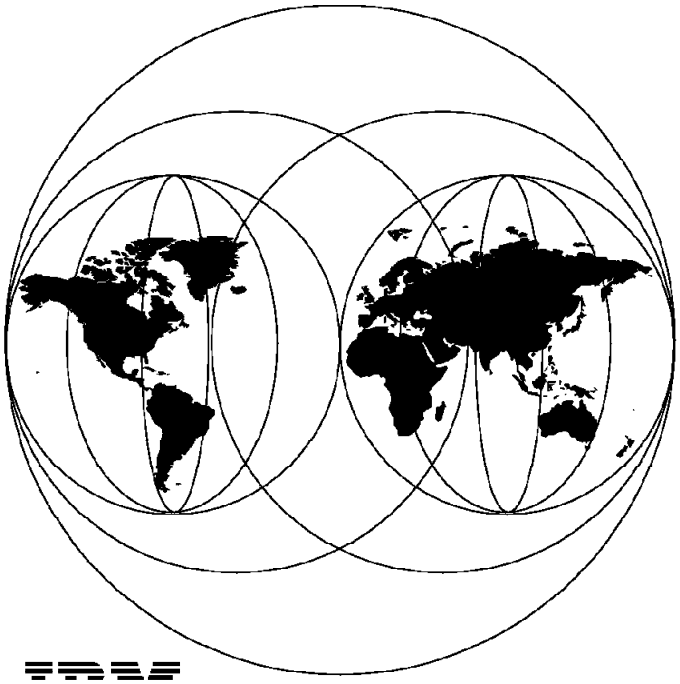
Using ADSM to Back Up OS/2 LAN Server and Warp Server

SG24-4682-00

March 1996



IBM

International Technical Support Organization
San Jose Center

Using ADSM to Back Up OS/2 LAN Server and Warp Server

SG24-4682-00

March 1996

Take Note!

Before using this information and the products it supports, be sure to read the general information under “Special Notices” on page xv.

First Edition (March 1996)

This edition applies to Versions 1 and 2 of ADSM for AIX, Program Numbers 5765-203 and 5765-564; Versions 1 and 2 of ADSM for MVS, Program Numbers 5648-020 and 5655-119; ADSM for VM, Program Number 5648-020; ADSM for OS/2, Program Number 5622-112; ADSM for OS/400, Program Numbers 5737-197 for OS/400 Version 2 Release 3, 5763-SV1 for OS/400 Version 3 Releases 0.5 and 1, and 5716-SV for OS/400 Version 3 Release 6; ADSM for VSE/ESA, Program Number 5686-073; ADSM for HP-UX, Part Number 14H0260 (5871-AAA); and ADSM for SUN Solaris, Part Number 28H2189 (5871-AAA).

Order publications through your IBM representative or the IBM branch office serving your locality. Publications are not stocked at the address given below.

An ITSO Technical Bulletin Evaluation Form for reader′s feedback appears facing Chapter 1. If the form has been removed, comments may be addressed to:

IBM Corporation, International Technical Support Organization
Dept. 471 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.

Abstract

This book describes how to use ADSTAR Distributed Storage Manager (ADSM) to back up OS/2 LAN Server and OS/2 Warp Server. We discuss both LAN Server Entry and Advanced and describe how to back up FAT, HPFS, and 386 HPFS files and directories. Integration of ADSM with the LAN Server BACKACC and RESTACC backup and restore utilities is described. We present several scenarios showing you the step-by-step LAN Server backup and restore process. Three sample scripts for automating LAN Server backup are included.

We discuss the new OS/2 Warp Server Backup/Restore utility, which is based on Personally Safe “n” Sound (PSnS), and how it can be used as an ADSM API application. We compare using OS/2 Warp Server Backup/Restore and the ADSM Backup/Archive client. We include a detailed scenario showing you the step-by-step process for using OS/2 Warp Server Backup/Restore as an ADSM API application.

This document is written for system, storage, and LAN administrators who want to back up their LAN and OS/2 Warp servers to ADSM. This document applies to any ADSM server platform.

(184 pages)

Contents

Figures

Tables

Special Notices

This publication is intended to help IBM, customer, vendor, and consultant personnel back up LAN Server and OS/2 Warp Server systems by using ADSTAR Distributed Storage Manager (ADSM). 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, 500 Columbus Avenue, Thornwood, NY 10594 USA.

The information contained in this document has not been submitted to any formal IBM test and is distributed AS IS. The information about non-IBM (VENDOR) products in this manual has been supplied by the vendor and IBM assumes no responsibility for its accuracy or completeness. 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.

Reference to PTF numbers that have not been released through the normal distribution process does not imply general availability. The purpose of including these reference numbers is to alert IBM customers to specific information relative to the implementation of the PTF when it becomes

available to each customer according to the normal IBM PTF distribution process.

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

ADSTAR	Advanced Function Printing
AFP	AIX
BookManager	DATABASE 2
DB2/2	IBM
MVS (logo)	OPERATING SYSTEM/2
Operating System/2	OS/2
SystemView	WebExplorer

The following terms are trademarks of other companies:

C-bus is a trademark of Corollary, Inc.

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

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

Microsoft, Windows, and the Windows 95 Logo are trademarks of Microsoft Corporation.

Other trademarks are trademarks of their respective companies.

Preface

This document describes how to use ADSTAR Distributed Storage Manager (ADSM) to back up OS/2 LAN Server and OS/2 Warp Server. We discuss both LAN Server Entry and Advanced and explain how to back up FAT, HPFS, and 386 HPFS files and directories. Integration of ADSM with the LAN Server BACKACC and RESTACC backup and restore utilities is described. We present several scenarios showing you the step-by-step LAN Server backup and restore process. Three sample scripts for automating LAN Server backup are included.

We discuss the new OS/2 Warp Server Backup/Restore utility, which is based on Personally Safe and Sound, and how it can be used as an ADSM API application. We compare using OS/2 Warp Server Backup/Restore and the ADSM Backup/Archive client. We include a detailed scenario showing you the step-by-step process for using OS/2 Warp Server Backup/Restore as an ADSM API application.

This document is written for system, storage, and LAN administrators who want to back up their LAN and OS/2 Warp servers to ADSM. This document applies to any ADSM server platform.

How This Document Is Organized

The document is organized as follows:

- Chapter 1, “LAN Server V4.0”

  This chapter provides an overview of LAN Server V4.0 and the LAN Server Entry and LAN Server Advanced versions. We describe the base network operating system functions, such as clients, file systems, and communications support. We discuss the different types of system and operational LAN data that might be on a LAN Server system and explain how the LAN backup and restore utilities, BACKACC and RESTACC, can be used in conjunction with ADSM to protect that data.

- Chapter 2, “LAN Server V4.0 Backup and Recovery Scenarios”

  In this chapter we show sample LAN Server V4.0 backup and recovery scenarios that use ADSM with the LAN Server utilities.

  First we give a short overview of the test environment we used for the scenarios. Then we show five scenarios that use the ADSM graphical user interface (GUI), providing step-by-step procedures for you to follow. The five scenarios detail backup and recovery of:

  – LAN Server Entry operational data

- LAN Server Advanced operational data
- LAN Server Advanced directory size limits
- LAN Server Entry domain control database (DCDB)
- LAN Server Entry entire partition

We conclude with a realistic approach that you would implement in a customer environment: automatic backup. We provide three sample scripts to automate LAN Server backup. These sample scripts are detailed in A.4, “LAN Server Backup Scripts” on page 151, and provided on the diskette in the back of this book. The three scripts detail backup and recovery of:

- LAN Server Entry
- LAN Server Advanced with 386 HPFS drives
- LAN Server Advanced with 386 HPFS drives and directory size limits

- Chapter 3, “OS/2 Warp Server”

  In this chapter we discuss the backup and recovery services provided for OS/2 Warp Server. OS/2 Warp Server provides a new Backup/Restore utility based on Personally Safe “n” Sound (PSnS). There are three alternatives for OS/2 Warp Server backup and restore:

  - Warp Server Backup/Restore
  - Warp Server Backup/Restore as an ADSM API application with any ADSM server
  - ADSM backup/archive client

  We compare all three alternatives and discuss for which environments each alternative or combination of alternatives may be most appropriate. We also explain how to convert from one alternative to another.

- Chapter 4, “Using Warp Server Backup/Restore As an ADSM API Application”

  In this chapter we explain how to use OS/2 Warp Server Backup/Restore as an ADSM API application.

  We discuss the backup and recovery of an HPFS shared data area (C:\RESOURCES\SHAREDDATA) that resides on the OS/2 Warp Server. The data is backed up to ADSM media.

Related Publications

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

- ADSM Publications
  - *ADSM Online Product Library CD-ROM*, SK2T-8714

    All of the ADSM publications are available in online readable format on the CD-ROM listed above. The ADSM library is also available on the following CD-ROMs:

    - *MVS Base Collection Kit*, SK2T-0710
    - *VM Base Collection Kit*, SK2T-2067
    - *OS/2 Base Collection Kit*, SK2T-2176
    - *AIX Base Collection Kit*, SK2T-2066
    - *AS/400 Base Collection Kit*, SK2T-2171
    - *IBM SystemView for AIX*, SK2T-1451

    Please note that the ADSM AIX and MVS server books and the client books listed are the Version 2 books; the library is restructured for Version 2.
  - *ADSM: General Information*, GH35-0131
  - *ADSM: Licensed Program Specification for AIX*, GH35-0132
  - *ADSM: Licensed Program Specification for MVS*, GH26-4038
  - *ADSM: Licensed Program Specification for VM*, GH35-0115
  - *ADSM: Licensed Program Specification for OS/2*, GH26-4012
  - *ADSM: Licensed Program Specification for ADSM V3R6 for OS/400*, GH26-4015-02
  - *ADSM: Licensed Program Specification for VSE*, GH26-4026
  - *ADSM: Licensed Program Specification for SUN Solaris*, GH26-4021-02
  - *ADSM: Licensed Program Specifications for HP-UX*, GH26-4017-02
  - *ADSM: Installing the AIX Server and Administrative Client*, SH35-0136
  - *ADSM: Installing the MVS Server and Administrative Client*, SH26-4043
  - *ADSM: Installing the OS/2 Server and Administrative Client*, SH26-4014

- *ADSM: Installing the OS/400 Server and Administrative Client*, SH26-4016-01
- *ADSM: Installing the VSE Server and Administrative Client*, SH26-4029
- *ADSM: Installing the SUN Solaris Server and Administrative Client*, SH26-4024
- *ADSM: Installing the HP-UX Server and Administrative Client*, SH26-4020

- *ADSM: Administrator's Guide for AIX*, SH35-0134
- *ADSM: Administrator's Guide for HP-UX*, SH26-4018
- *ADSM: Administrator's Guide for MVS*, SH26-4039
- *ADSM: Administrator's Guide for OS/2*, SH26-4003
- *ADSM: Administrator's Guide for OS/400*, SH26-4008-01
- *ADSM: Administrator's Guide for SUN Solaris*, SH26-4022
- *ADSM: Administrator's Guide for VM*, SH35-0117
- *ADSM: Administrator's Guide for VSE*, SH26-4027

- *ADSM: Administrator's Reference for AIX*, SH35-0135
- *ADSM: Administrator's Reference for HP-UX*, SH26-4019
- *ADSM: Administrator's Reference for MVS*, SH26-4040
- *ADSM: Administrator's Reference for OS/2*, SH26-4004
- *ADSM: Administrator's Reference for OS/400*, SH26-4009-01
- *ADSM: Administrator's Reference for SUN Solaris*, SH26-4023
- *ADSM: Administrator's Reference for VM*, SH35-0130
- *ADSM: Administrator's Reference for VSE*, SH26-4028
- *ADSM: Messages*, SH35-0133

- *ADSM: Device Configuration*, SH35-0137
- *ADSM: Installing the Clients*, SH26-4049
- *ADSM: Using the UNIX Hierarchical Storage Management (HSM) Clients*, SH26-4030
- *ADSM: Using the UNIX Backup/Archive Clients*, SH26-4052

- *ADSM: Using the OS/2 Backup/Archive Clients*, SH26-4053
- *ADSM: Using the DOS Backup/Archive Clients*, SH26-4054
- *ADSM: Using the Microsoft Windows Backup/Archive Clients*, SH26-4056
- *ADSM: Using the Novell NetWare Backup/Archive Clients*, SH26-4055
- *ADSM: Using the Apple Macintosh Backup/Archive Clients*, SH26-4051
- *ADSM: Using the Lotus Notes Backup Agent*, SH26-4047
- *ADSM: Client Reference Cards*, SX26-6013

- OS/2 LAN Server
  - *OS/2 LAN Server Network Administrator Reference Volume 3: Network Administrator Tasks*, S10H-9682
  - *OS/2 LAN Server Problem Determination Guide*, S10H-9685
  - *OS/2 LAN Server Commands and Utilities*, S10H-9686
  - *OS/2 LAN Server Programming Guide and Reference*, S10H-9687
- OS/2 Warp Server (online books)
  - *Tell Me About It*
  - *OS/2 Warp Server Backup/Restore User's Guide*

International Technical Support Organization Publications

- ADSM redbooks
  - *ADSM Presentation Guide*, GG24-4146
  - *ADSM Version 2 Presentation Guide*, SG24-4532
  - *ADSM Implementation Examples*, GG24-4034
  - *ADSM Advanced Implementation Examples*, GG24-4221
  - *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
  - *Getting Started with ADSM/6000*, GG24-4421
  - *ADSM for AIX: Advanced Topics*, SG24-4601
  - *Getting Started with the NetWare Client*, GG24-4242
  - *Getting Started with the AIX/6000 Client*, GG24-4243

- *ADSM Hierarchical Storage Management for AIX Clients*, SG24-4631
- *ADSM API Examples for OS/2 and Windows*, SG24-2588
- *Using ADSM to Back Up Databases*, SG24-4335-01
- *Using ADSM to Back Up Lotus Notes*, SG24-4534
- *AIX Storage Management*, GG24-4484
- *Easy Access to Host Data with Distributed File Manager*, GG24-4427
- *ADSM/VSE Implementation*, GG24-4266
- *Setting Up and Implementing ADSM/400*, GG24-4460
- *AIX Storage Management Products Comparison*, GG24-4495
- *ADSM/6000 on 9076 SP2*, GG24-4499
- *ADSM for OS/2: Advanced Topics*, SG24-4740 (in press)
- *Hierarchical Storage Management for NetWare: Implementing ADSM and NetSpace*, SG24-4713 (in press)
- *AIX Tape Management*, SG24-4705 (in press)
- *Backup, Recovery, and Availability with DB2 Parallel Edition on RISC/6000 SP*, SG24-4695 (in press)

• OS/2 LAN Server

- *The IBM OS/2 LAN Server Version 3.0 System Recovery Considerations*, GG24-4043
- *Inside LAN Server 4.0*, SG24-4428-01

• OS/2 Warp Server

- *Inside OS/2 Warp Server, Volume 1: Exploring the Core Components*, SG24-4602
- *Inside OS/2 Warp Server, Volume 2: Using SystemView Backup/Recovery and Advanced Print*, SG24-4702 (in press)

• Related ITSO Sold Bills of Form

- *Storage Software: Distributed Storage Management*, SBOF-6311
- *OS/2 LAN and Distributed Systems*, SBOF-6335

A complete list of International Technical Support Organization publications, known as redbooks, with a brief description of each, may be found in:

International Technical Support Organization Bibliography of Redbooks, GG24-3070.

How Customers Can Get Redbooks and Other ITSO Deliverables

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

- **IBMLINK**

  Registered customers have access to PUBORDER to order hardcopy and to REDPRINT to obtain BookManager BOOKs.

- **IBM Bookshop** — send orders to:

  usib6fpl@ibmmail.com (USA)
  bookshop@dk.ibm.com (Outside USA)

- **Telephone orders**

  1-800-879-2755 (USA)
  354-9408 (Australia)
  359-2-731076 (Bulgaria)
  42-2-67106-250 (Czech Republic)
  593-2-5651-00 (Ecuador)
  03-69-78901 (Israel)
  905-627-1163 (Mexico)
  064-4-57659-36 (New Zealand)
  027-011-320-9299 (South Africa)
  0256-478166 (UK)
  32-2-225-3738 (Belgium)
  1-800-IBM-CALL (Canada)
  45-934545 (Denmark)
  01805-5090 (Germany)
  0462-73-6669 (Japan)
  31-20513-5100 (The Netherlands)
  507-639977 (Panama)

- **Mail Orders** — send orders to:

  IBM Publications
  P.O. Box 9046
  Boulder, CO 80301-9191
  USA

  IBM Direct Services
  Sortemosevej 21,
  3450 Allerod
  Denmark

- **Fax** — send orders to:

  1-800-445-9269 (USA)
  32-2-225-3478 (Belgium)
  905-316-7210 (Canada)
  593-2-5651-45 (Ecuador)
  03-69-59985 (Israel)
  31-20513-3296 (The Netherlands)
  507-693604 (Panama)
  0256-843173 (UK)
  359-2-730235 (Bulgaria)
  42-2-67106-402 (Czech Republic)
  07032-15-3300 (Germany)
  0462-73-7313 (Japan)
  064-4-57659-16 (New Zealand)
  027-011-320-9113 (South Africa)

- **1-800-IBM-4FAX (USA only)** — ask for:

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

- **Direct Services**

  Send note to softwareshop@vnet.ibm.com

- **Redbooks Home Page on the World Wide Web**

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

- **E-mail (Internet)**

  Send note to redbook@vnet.ibm.com

- **Internet Listserver**

  With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

How IBM Employees Can Get Redbooks and ITSO Deliverables

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

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

- **GOPHER link to the Internet**

  Type GOPHER
  Select IBM GOPHER SERVERS
  Select ITSO GOPHER SERVER for Redbooks

- **Tools disks**

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

  ```
  TOOLS SENDTO EHONE4 TOOLS2 REDPRINT GET GG24xxxx PACKAGE
  TOOLS SENDTO CANVM2 TOOLS REDPRINT GET GG24xxxx PACKAGE (Canadian users only)
  ```

  To get lists of redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS REDBOOKS GET REDBOOKS CATALOG
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ITSOCAT TXT PACKAGE
  TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET LISTSERV PACKAGE
  ```

  To register for information on workshops, residencies, and redbooks:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ITSOREGI 1996
  ```

  For a list of product area specialists in the ITSO:

  ```
  TOOLS SENDTO WTSCPOK TOOLS ZDISK GET ORGCARD PACKAGE
  ```

- **Redbooks Home Page on the World Wide Web**

http://w3.itso.ibm.com/redbooks/redbooks.html

- **ITSO4USA category on INEWS**
- **IBM Bookshop** — send orders to:

  USIB6FPL at IBMMAIL or DKIBMBSH at IBMMAIL

- **Internet Listserver**

  With an Internet E-mail address, anyone can subscribe to an IBM Announcement Listserver. To initiate the service, send an E-mail note to announce@webster.ibmlink.ibm.com with the keyword subscribe in the body of the note (leave the subject line blank). A category form and detailed instructions will be sent to you.

Enclosed Sample Diskette Missing

If the diskette in the back of the redbook is missing or not readable, you can obtain a copy from either your IBM representative or the ITSO ftp server.

IBM employees can obtain the package of materials accompanying this publication by typing the following command from their local VM user IDs:

```
TOOLS SENDTO USDIST MKTTOOLS MKTTOOLS GET ADSMLANS PACKAGE
```

To obtain the samples from the accompanying diskette from the ITSO anonymous FTP server, *ftp.almaden.ibm.com*, issue the following commands from the */redbooks* directory:

```
cd SG244682
binary
get ADSMLANS.SCR
ascii
get READ.ME
```

Acknowledgments

This project was designed and managed by:

Cyndie Behrens
International Technical Support Organization, San Jose Center

The authors of this document are:

Chris Jarvis
IBM New Zealand

Mike McIntyre
IBM Canada

This publication is the result of a residency conducted at the International Technical Support Organization, San Jose Center.

Thanks to the following people for the invaluable advice and guidance provided in the production of this document:

Jim Bells
IBM Canada

Oscar Cepeda
International Technical Support Organization, Austin Center

Maggie Cutler
Technical Editor

Dave Derk
IBM San Jose

Michael Fabianski
IBM Warwick

Wim Fabri
IBM Belgium

Bruce Nash
IBM Warwick

Toshi Shimizu
International Technical Support Organization, Austin Center

Horace Tang
IBM San Jose

Uwe Zimmerman
International Technical Support Organization, Austin Center

Chapter 1. LAN Server V4.0

This chapter provides an overview of LAN Server V4.0 and the LAN Server Entry and LAN Server Advanced versions. We describe the base network operating system functions, such as clients, file systems, and communications support. We discuss the different types of system and operational LAN data that might be on a LAN Server system and explain how the LAN backup and restore utilities, BACKACC and RESTACC, can be used in conjunction with ADSM to protect that data. In Chapter 2, “LAN Server V4.0 Backup and Recovery Scenarios” on page 39 steps you through the LAN Server backup and restore scenarios we implemented and provide some scripts for automating the process.

LAN Services:

LAN Server is a network operating system that enables you to share a system′s resources with other Ethernet or token-ring networked systems, using either NetBIOS or TCP/IP. The resources that can be shared include:

- Data areas (files and directories)
- OS/2 applications
- Windows applications
- DOS applications
- Printers
- Serial devices, such as modems and plotters

The systems that participate in the LAN can be defined as either servers, requesters, or peer systems. Servers are systems that share their resources with multiple LAN systems. Requesters are systems that use the resources shared by servers. Peer systems are a special type of pseudo servers that can share their resources with requesters, but only one requester can access the shared resource at one time. A LAN system can have dual roles, that is, it can act as both a LAN server and LAN requester, or a peer system and a LAN requester. For example, a system, server 1, can share a resource such as a printer while also accessing a data area located on another system, server2, as shown in Figure 1 on page 2.

Peer systems with OS/2 LAN Requester can only have one requester share a resource at a time. OS/2 Peer-to-Peer in OS/2 Warp Connect can have multiple requesters share a resource.

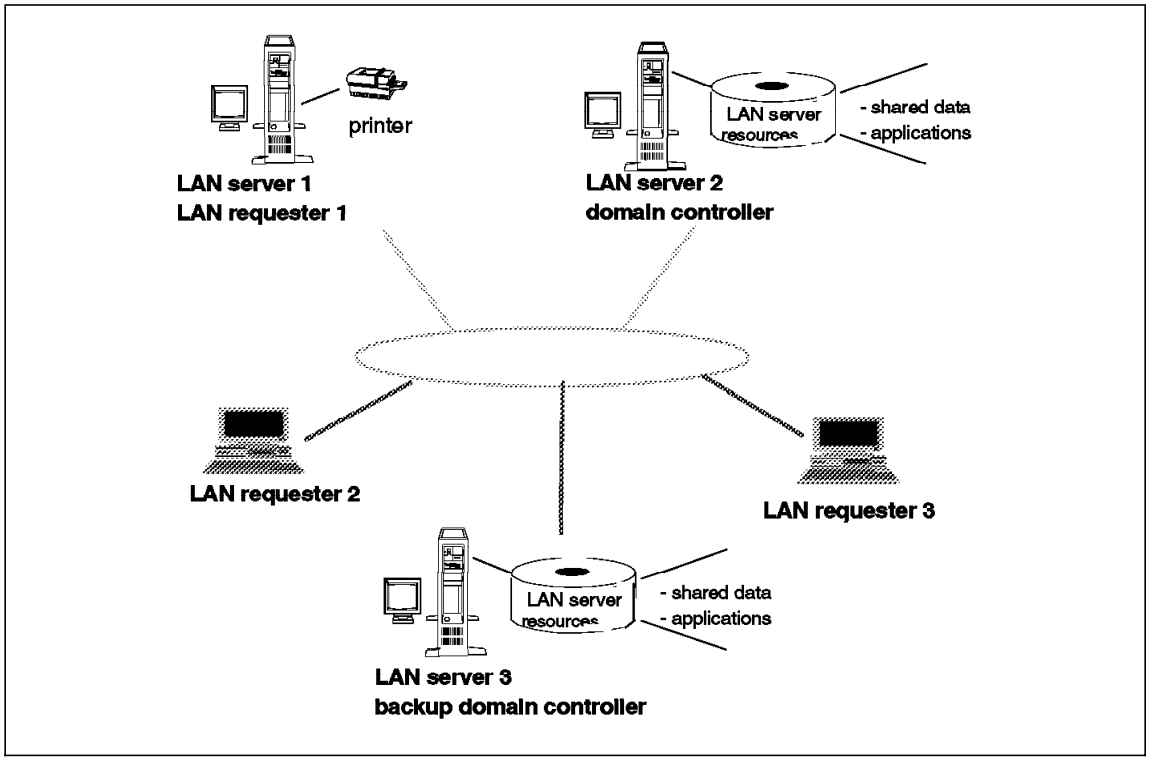


Figure 1. Single Domain LAN

With LAN Server you do not log on to each individual server. Instead you log on to the LAN Server environment, which may consist of a single server or multiple servers. This environment is called the *domain*. A domain is a group of servers that provides resources to requesters. The requesters do not have to know the physical server location of the resources. This allows for more transparent change of a resource if it is moved to a different server.

A domain always has a primary server called the *domain controller*. The domain controller maintains information about LAN users, groups, and resources. When a user logs on to the LAN, the domain controller processes the request and allocates the user access to the user's defined domain resources (this may include access to multiple resources across multiple servers). Other LAN servers can be defined as either a backup domain controller or an additional server. A backup domain controller

maintains a backup copy of the user, group, and resource information so that it can process logon requests if the domain controller is either unavailable or busy. An additional server has no special responsibilities other than sharing its resources.

1.1 LAN Server Versions and Components

Both the LAN Server Entry and LAN Server Advanced versions of LAN Server provide server and requester components that support a large variety of operating environments, as shown in Table 1. They also provide interoperability with OEM products and previous versions of LAN Server, as shown in Table 2 on page 4. The requester components coexist with the Novell NetWare requester, enabling you to log on and concurrently access resources from both LAN Server servers and NetWare servers.

Table 1. LAN Server V4.0 Components and Their Supported Operating Environments

LAN Server Component	Operating Environments
LAN Server	OS/2 V2.1 or higher IBM approved equivalent
OS/2 LAN Requester	OS/2 V2.1 or higher IBM approved equivalent
DOS LAN Services, previously known as DOS LAN Requester	IBM DOS V3.3, V5.0, V6.1, V6.3 MS-DOS V3.3, V5.0, V6.0, V6.2 IBM approved equivalent

Note

Some LAN Server functions require OS/2 V2.11.

IBM provides LAN Server V4.0 certification testing for OEM hardware and operating systems. You can find information about tested and certified OEM platforms on Prodigy and Compuserv OS/2 forums.

DOS LAN Services also supports the Windows environment when Windows V3.1 or higher is loaded onto a supported operating environment.

Table 2 (Page 1 of 2). LAN Server V4.0 Client/Server Interoperability: Requester Support for Server Logon and Resource Access

	PCLP V1.3	**LS V1.0**	**LS V1.2**	**LS V1.3**	**LS V2.0**	**LS V3.0**	**LS V4.0**	**WS**	**LM**	**MAC**
PCLP V1.31	√	√	√	√	√	√	√	√		
OS/2 LR V1.0		√								
DOS LS V1.0		√								
OS/2 LR V1.2			√	√	√	√	√			
DOS LS V1.2			√	√	√	√	√			
OS/2 LR V1.3			√	√	√	√	√			
DOS LS V1.3			√	√	√	√	√			
OS/2 LR V2.0			√	√	√	√	√	√	√	√
DOS LS V2.0			√	√	√	√	√	√	√	√
OS/2 LR V3.0			√	√	√	√	√	√	√	√
DOS LS V3.0			√	√	√	√	√	√	√	√
OS/2 LR V4.0			√	√	√	√	√	√	√	√
DOS LS V4.0			√	√	√	√	√	√	√	√
LM Requester					√	√	√	√	√	
MAC Requester					√	√	√	√	√	√
WFW					√	√	√	√		

Table 2 (Page 2 of 2). LAN Server V4.0 Client/Server Interoperability: Requester Support for Server Logon and Resource Access

	PCLP V1.3	LS V1.0	LS V1.2	LS V1.3	LS V2.0	LS V3.0	LS V4.0	WS	LM	MAC
Windows 3.x shipped with WS					√	√	√	√		
Windows 95 shipped with WS					√	√	√	√		
NT Requester							√	√		

Note:

PCLP = Personal Computer LAN Program.

LM = Microsoft LAN Manager.

LR = LAN Requester.

LS = LAN Server.

MAC = Macintosh AppleShare.
An additional program, LAN Server for Macintosh, is required on the server to support interoperability between LAN Server and Macintosh AppleShare environments.

WFW = Microsoft Windows for Workgroups.

WS = OS/2 Warp Server

Some restrictions may apply. Please see IBM OS/2 Warp Server announcement letter 296-056 for details.

LAN Server addresses a wide variety of network sizes and complexities, from small workgroups, to departmental networks, to the corporate network, by supporting dedicated and nondedicated servers through its two versions. LAN Server Entry provides base network operating system functions that you would commonly use in a workgroup or departmental network. It is typically recommended for dedicated domain controllers and print servers. LAN Server Advanced provides both base and specialized network operating system functions that you would commonly use in large, specialized, or complex networks. It is typically recommended for file servers and application servers because the 386 high performance file

system (HPFS) provides improved performance. For more information on these products refer to 1.2, “LAN Server Entry” on page 6, and 1.3, “LAN Server Advanced” on page 11.

1.2 LAN Server Entry

LAN Server Entry is designed to be used as either a nondedicated or dedicated server. It provides base network operating system functions such as:

- Resource sharing
- Support for multiple clients
- An object-oriented GUI
- Support for multiple file systems—file allocation table (FAT) and HPFS
- Access control profiles (ACPs)

  The terms *ACP* and *access control list* (ACL) can be used to refer to the security permissions for a LAN Sever resource.
- Support for remote initial program load (IPL) of multiple types of clients
- LAN messaging
- Communications support, including TCP/IP
- Adapter autosense

1.2.1 Resource Sharing

LAN Server Entry provides sharing of server or peer system resources with requesters. The resources that can be shared include:

- Data areas (files and directories)
- OS/2 applications
- Windows applications
- DOS applications
- Printers
- Serial devices, such as modems and plotters

as shown in Figure 2 on page 7.

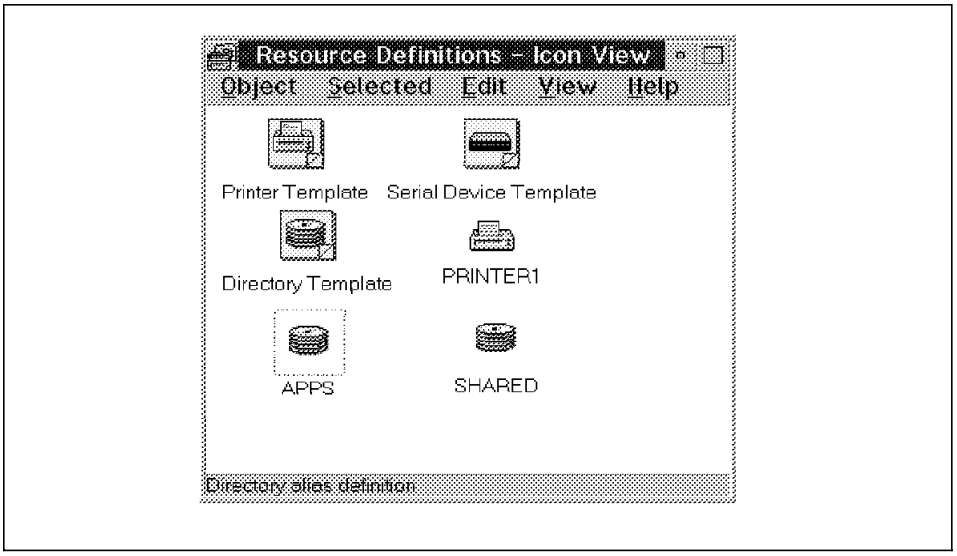


Figure 2. Types of LAN Server Entry Shared Resources

1.2.2 Multiple Clients

LAN Server Entry supports OS/2, Windows, DOS, Microsoft LAN Manager, Macintosh AppleShare, Windows for Workgroups, and Windows NT requesters. An additional program, LAN Server for Macintosh, is required on the server to support interoperability between LAN Server and Macintosh AppleShare environments.

1.2.3 Object-Oriented GUI

Object-oriented GUI interfaces are provided for both administrators and OS/2, Windows, and DOS requesters. The GUI enables administrators to quickly and easily create, change, and delete users, groups, resources, and assignments by using GUI notebooks and drag and drop techniques. The GUI enables requesters to access domain resources quickly and easily and administer their own user IDs and passwords.

Figure 3 on page 8 shows the LAN Server Administration-Icon View Window, the main administration GUI window.

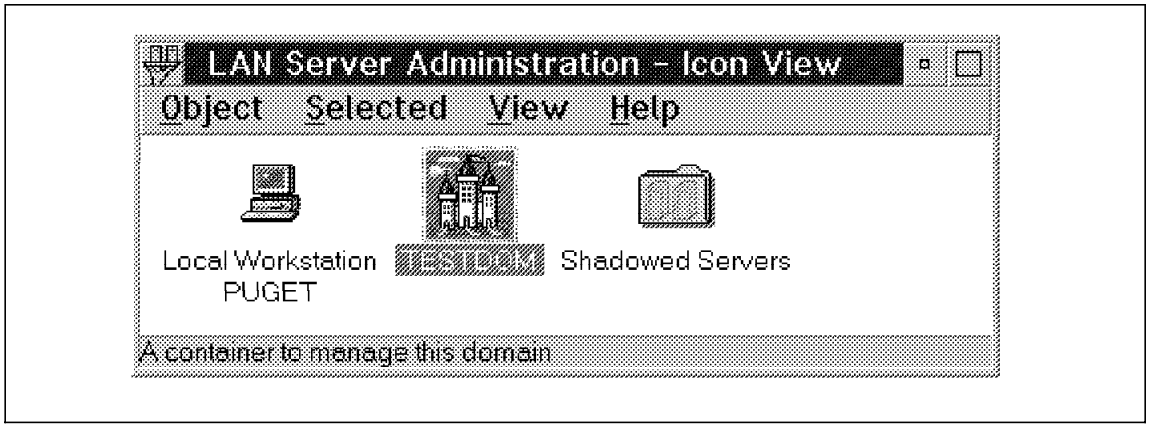


Figure 3. LAN Server Administration-Icon View Window

1.2.4 Multiple File Systems

LAN Server Entry supports the following file systems:

- FAT

  A FAT file system uses a single table, located at the beginning of the disk, to allocate disk space for a file and to locate and chain together parts of a file that may be scattered among different sectors. FAT supports 8.3 file names; that is, a maximum of eight characters can be used for the main file name, and a maximum of three characters can be used for the extension. The file name cannot contain spaces; for example, MY FILE.DAT is not a valid file name, whereas MY_FILE.DAT is. OS/2, Windows, and DOS support the FAT file system.

- HPFS

  An HPFS uses tables located near each file (in the file′s fnode) to allocate and track the distribution of files across the disk. It supports long file names (up to 254 characters) that can contain spaces and nonalphanumeric characters. HPFS also supports hotfixing, which allows it to automatically reroute data from a bad to a good data sector. The HPFS is fully supported by OS/2. It can also be accessed by DOS and Windows requesters from LAN Server redirected drives. DOS and Windows only support 8.3 file names. If HPFS files have been created with long file names, DOS and Windows programs can see and use the data files, but they will not see the correct file name because it is truncated at either the first space or after the first 8 characters.

1.2.5 Access Control Profiles

ACPs enable you to define security permissions for a LAN resource that uniquely identify who can access the resource and their level of authority. Permissions can be defined at a user, group, or universal level. The access permissions that you can specify are:

- None
- Read
- Write
- Create
- Delete
- Execute
- Attributes
- Permissions

Figure 4 on page 10 shows that the D:\RESOURCES\SHAREDDATA directory has been given Read access permission from MAINTENANCE and all permissions (ACDPRWX) from SUPERVISOR.

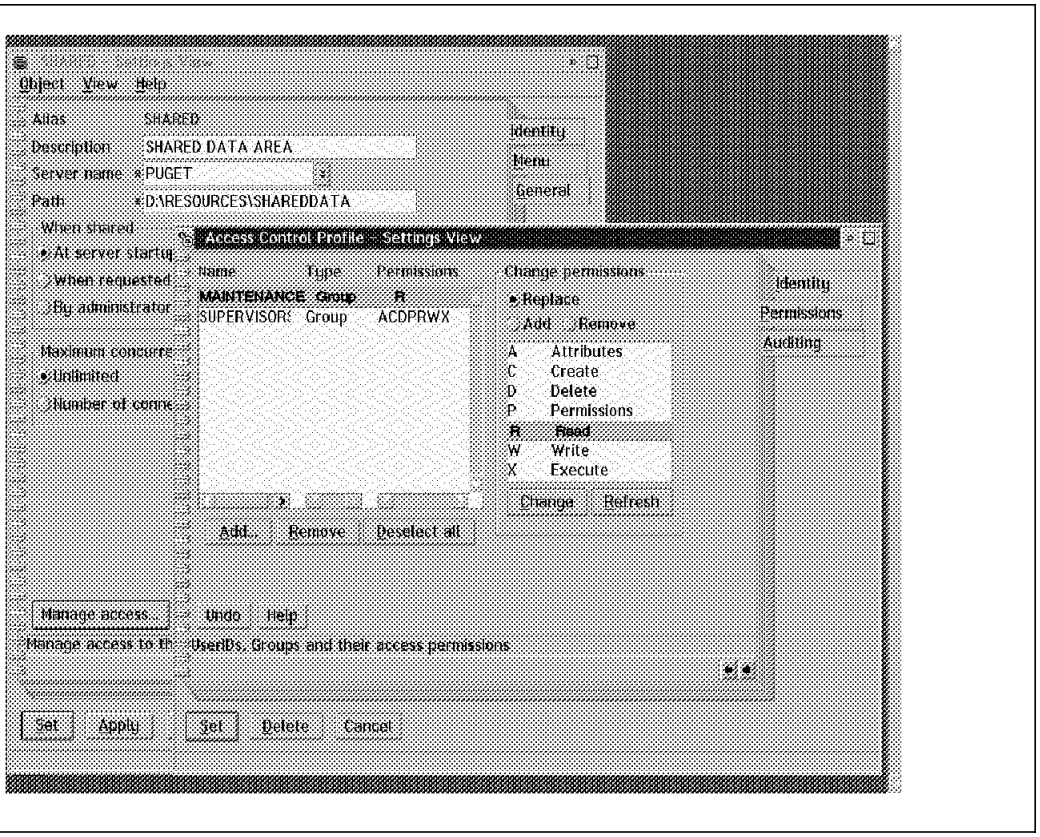


Figure 4. Sample ACP Definition

An ACP is specified for a directory. If a new subdirectory is created, it receives the same ACP as its parent directory. This propagation of ACPs is called *inheritance*. HPFSs and FAT file systems do not directly support inheritance; they rely on LAN Server to provide this function. Therefore, if you are using LAN Server Entry and create a directory locally at the server, that directory will not inherit an ACP. To ensure that all directories have associated ACPs, create the directories remotely (from a remote LAN requester that is using redirected drives). Conversely, to ensure the removal of ACPs, delete the directories remotely.

Files in an HPFS or FAT file system inherit permissions from the directory. You must use the NET ACCESS command to add ACP protection for files.

The 386 HPFS of LAN Server Advanced provides both local and remote inheritance functions for directory creation and deletion. You can also specify file permissions separately from directory permissions. Therefore

multiple files in the same directory can have different permissions. For more information about the 386 HPFS refer to 1.3.1, “386 HPFS” on page 12.

Users cannot access directory resources that do not have an associated ACP, unless an ACP is defined at the drive level, such as C:.

1.2.6 Remote Initial Program Load

Remote IPL enables the use of diskless systems, or systems that do not have the requester installed, as requesters. When the remote system is IPLed, it contacts the domain controller, which then downloads the appropriate IPL files. OS/2, Windows, and DOS requesters can be IPLed remotely.

1.2.7 LAN Messaging

LAN messaging provides simple-to-use inter-LAN communication between LAN Server requesters without the complexity of e-mail. It enables you to:

- Send and receive messages
- Save messages in a log file
- Add and delete messaging names
- Forward messages to another requester

1.2.8 Communications Support, Including TCP/IP

LAN Server supports Multi-Protocol Transport Services (MPTS), which provides NetBIOS, TCP/IP, NETBIOS over TCP/IP, IPX/SPX, and IEEE 802.2 SNA communications support.

1.2.9 Adapter Autosense

Adapter autosense is provided as part of the installation program. It enables the installation program to detect the type of LAN adapter installed in the system and automatically select the correct drivers (if available).

1.3 LAN Server Advanced

LAN Server Advanced provides increased performance, security, availability, and control while still supporting the base network operating functions as discussed in 1.2, “LAN Server Entry” on page 6. It is designed with higher performance file system access, increased architectural limits for larger workloads, and fault tolerance. LAN Server Advanced provides the following additional functions:

- 386 HPFS
- 386 HPFS directory size limits

- Symmetric multiprocessing (SMP) support
- Fault tolerance (including disk mirroring and duplexing)
- Local security for 386 HPFS

1.3.1 386 HPFS

386 HPFS provides improved performance over HPFS and FAT because it runs at ring zero within the OS/2 operating environment. Thus LAN Server Advanced has extremely fast access to very large disk volumes and optimizes server performance when many files are simultaneously open. This optimized high performance file system incorporates fault tolerant features and increased architectural limits that support larger workloads.

386 HPFS offers increased security because it provides both local and remote ACP inheritance functions for directory creation and deletion. You can also separately specify file permissions so that files in the same directory can have different permissions. For more information about inheritance, refer to 1.2.5, “Access Control Profiles” on page 9.

1.3.2 386 HPFS Directory Size Limits

386 HPFS directory size limits provide increased control because they allow directory level management of server disk space. An administrator can define the maximum size that a directory (including its subdirectories) can grow to and set warning thresholds to inform either a single user or multiple users that they are about to exceed the directory size limit. Directory size limits are only provided for 386 HPFS.

Figure 5 on page 13 shows the LAN Server administrator GUI window, Directory Size Limits, used to define directory size limits. In this example a directory size limit of 54 KB is set.

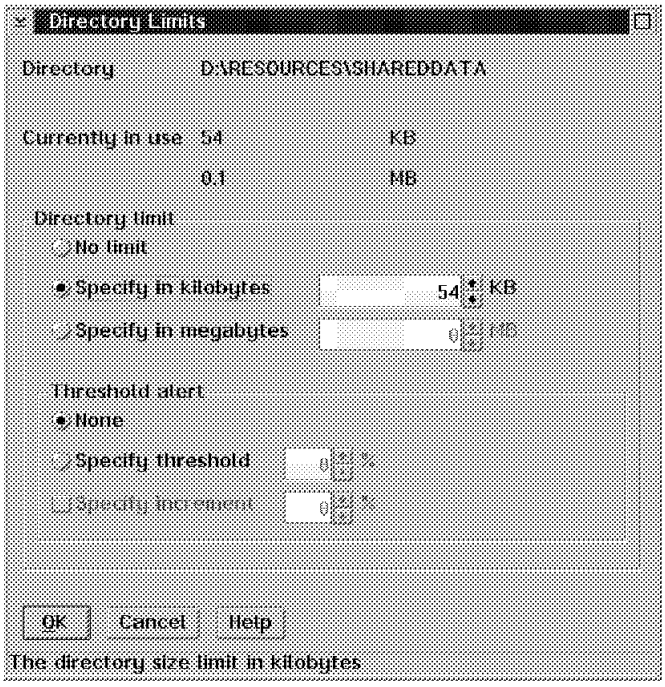


Figure 5. Directory Size Limit Definition

1.3.3 Symmetric Multiprocessing Support

SMP support provides increased performance because it enables you to run LAN Server Advanced on certified SMP hardware that provides two, four, or eight processors.

1.3.4 Fault Tolerance

Fault tolerance offers increased availability because it protects against data loss when hard disk failures occur by providing:

- Disk mirroring

  Disk mirroring is the duplication of a partition of one disk drive volume on another disk drive volume. This technique provides protection against errors caused by a faulty disk.

- Disk duplexing

  Disk duplexing is a special type of disk mirroring where each physical disk is attached to a separate disk controller. This technique provides

protection against errors caused by either a faulty disk or a faulty disk controller.

- Fault monitoring and reporting

  Fault monitoring detects errors that occur during hard disk read and write operations and issues an alert when critical errors are encountered.

- Error correction

  Error correction is performed by the fault tolerance monitor utility. If potential disk errors are detected during system startup, the utility automatically attempts to verify or compare all sectors on both the primary and secondary partitions of the mirrored drives to correct any inconsistencies or errors.

- Support for hot-swappable disks in a disk array

  Support for hot-swappable disks enables you to replace a faulty disk without powering off the LAN Server system.

Figure 6 shows an example of the disk mirroring and disk duplexing fault tolerance capabilities. Disk F is being mirrored because its copy is on the same controller. Disks C and E are being duplexed because their copies are on a different controller.

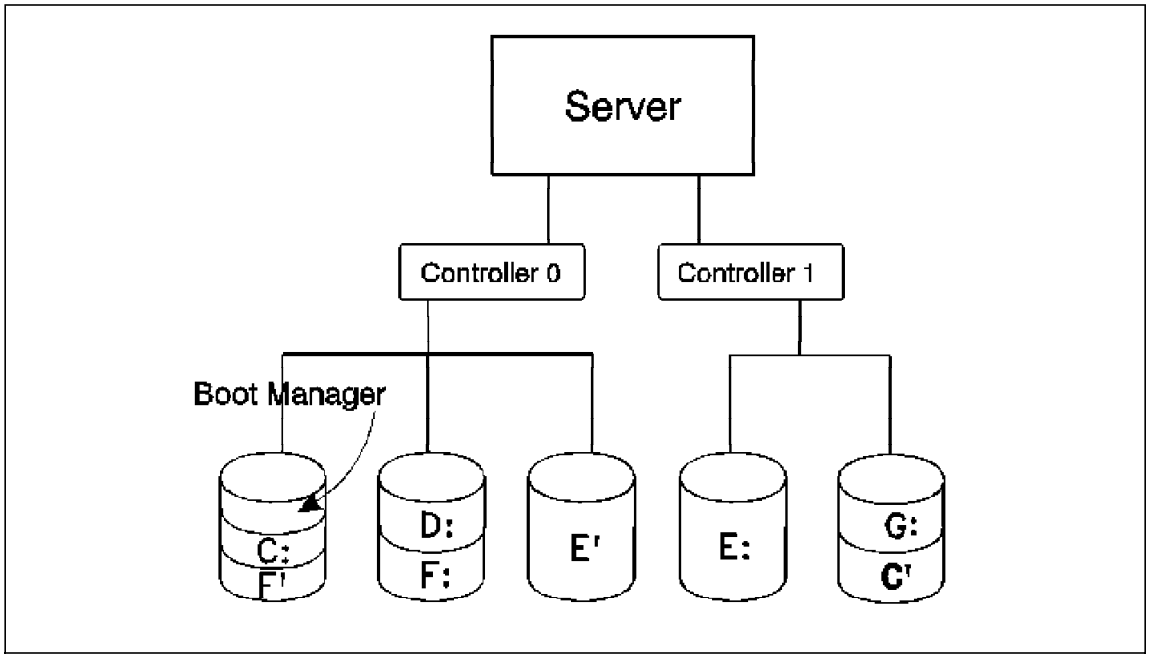


Figure 6. Fault Tolerance Administration

1.3.5 Local Security for 386 HPFS

Local security for 386 HPFS provides increased security as it extends access restrictions to users working locally at the server. It protects all files on the server 386 HPFS partitions from unauthorized access.

You can also increase security by placing the LAN Server in a badge access or locked room and using power-up and lockout passwords. This security measure does not require implementation of the local security feature.

1.4 LAN Utilities

LAN Server provides a variety of utilities for:

- Backup and restore

  The utilities commonly used during LAN Server backup and restore are BACKACC and RESTACC. We look at these utilities in detail, including how to use them with ADSM in 1.6.1.1, “LAN Server Backup and Restore Utilities” on page 22.

- Migration

  LAN Server provides utilities that help you migrate from previous versions of LAN Server and when changing from a file system that does not contain ACPs (FAT) to a file system that does (386 HPFS).

- Multimedia

  386 HPFS supports a hard disk format that is especially suited for use with multimedia software. The multimedia HPFS disk format helps with the storage and readability of large files because it stores files in contiguous blocks that are at least 256 KB. The multimedia format is unreadable to previous versions of HPFS and 386 HPFS.

  You select the multimedia format when you format a new 386 HPFS disk, but if a disk is already formatted, LAN Server provides a utility, MMUTIL, to apply or remove the multimedia format on an HPFS disk that is already in use. Thus there is no need to back up, reformat, and restore the disk. Another utility, PROFILER, analyzes and adjusts disk organization to ensure that it is suitable for multimedia format.

- Scheduling

  LAN Server provides a scheduling utility, AT, which can schedule commands to be run at the LAN Server server. Administrative authority is required.

- Licensing

LAN Server provides a license tracking utility, LTU, to help you keep track of requesters on a network and the software installed on each of the requesters. LTU finds and lists the requesters logged on or using resources on a specified domain, lets you specify the software installed on each requester, and displays a report of how many and what type of licenses you should have.

LAN Server Entry and LAN Server Advanced provide many of the same utilities; however, some utilities are more applicable to one environment than another.

1.5 LAN Data

LANs are complex environments that incorporate many types of data such as:

- LAN Server programs
- Resource definitions
- User definitions
- Group definitions
- ACP definitions
- LAN applications
- User data files
- Printer definitions and queues
- Serial definitions and queues

Data can be categorized as either system or operational data. System data is located on a single server and is vital to the operation of the LAN Server environment. Operational data can be located either on single or multiple servers and/or peer systems and is vital to user operations.

If the LAN provides critical user resources, a disaster recovery plan that incorporates periodic data backup and restore should be maintained to enable you to recover your data or systems with a minimum of downtime and impact on users. As part of your disaster recovery plan, determine the different types of system and operational data and the procedures required to back up and restore each type of data.

The ADSM client can be loaded on LAN Server server and peer systems to provide easy-to-install facilities that enable you to back up both your system and operational data. ADSM also provides you with the ability to schedule

automated backups, which you may choose to kick off during quiet network periods.

We look at the system and operational data and the LAN Server backup and restore utilities in more detail. For each type of data, we discuss our recommendations for using ADSM for backup and restore.

Note

There are no restrictions on running an ADSM server and/or client on a LAN Server server or LAN Server requester, provided that there is adequate processing power, memory, and disk space. However, if you use NetBIOS for ADSM communications, both LAN Server and ADSM use NetBIOS resources and you must increase the NetBIOS names, network control blocks (NCBs), and sessions defined in the MPTS configuration.

Both the ADSM V2R1 level 0.2 backup/archive and administrative clients (GUI and CLI) require:

- An additional name
- An additional session
- Two additional NCBs

If you have more than one client, that is, more than one backup/archive or administrative client, you still only require one additional name, one additional session, and two NCBs, because generally only one client or administrator will be active at one time.

The ADSM V1R2 level 0.9/1.9 server requires:

- An additional name
- Additional sessions equivalent to either the NETBIOSSESSIONS parameter defined in the DSMSERV.OPT file or the MAXSESSIONS parameter if the NETBIOSSESSIONS parameter has not been specified
- Two additional NCBs for each additional ADSM session

The ADSM server level is always presented as two numbers. The first number, level 0.9 in our environment, pertains to the level of the generic ADSM server code that is common across ADSM platforms. The second number, level 1.9 in our environment, pertains to the level of the platform-specific code.

1.5.1 System Data

The majority of LAN Server system data is on the domain controller. Other servers also have some system data, such as the base LAN Server program files and backup copies of the LAN definition files. However, the domain controller is the primary repository for system data and is responsible for the distribution and synchronization of the data with other servers.

LAN Server system data includes:

- LAN Server program files

  The LAN Server program files are copied to the server during installation. They reside in the IBMLAN directory structure.

- IBMLAN.INI

  The IBMLAN.INI file contains the LAN parameters used to define the server and requester resources and their behavior.

- PROTOCOL.INI

  The PROTOCOL.INI file contains the configuration and binding information for the system protocol and network adapter drivers.

- ACPs

  LAN Server Entry uses either the HPFS or FAT file system, both of which store resource ACPs in the NET.ACC file. LAN Server Advanced supports the 386 HPFS, HPFS, and FAT file systems. When either HPFS or FAT is used, all ACPs are stored in the NET.ACC file. When 386 HPFS is used, only printer, serial port, and volume ACPs are stored in the NET.ACC file; file and directory ACPs are stored in the file system.

  For more information about ACPs and the 386 HPFS, refer to 1.2.5, “Access Control Profiles” on page 9, and 1.3.1, “386 HPFS” on page 12.

- NET.ACC

  The NET.ACC file is a critical LAN Server file that is unique to each server. It acts as the user accounts database.

  When you use LAN Server Entry or LAN Server Advanced with either the HPFS or a FAT file system, the NET.ACC file contains server-unique information, LAN user IDs, group IDs, passwords, and ACPs.

  When you use LAN Server Advanced with 386 HPFS, the NET.ACC file contains server-unique information, LAN user IDs, group IDs, passwords, and all ACPs except file and directory ACPs. The 386 HPFS stores the file and directory ACPs in the file system. This improves server performance when a user accesses a file or directory because the

server does not have to swap between disk areas to first determine the user's access rights and then provide access to the file or directory.

The NET.ACC file may become corrupted if the server is not properly shut down; for example, if there are system or environmental problems, such as a fluctuating power supply. Symptoms of a problem with your NET.ACC file include user IDs, group definitions, and ACPs that cannot be created or changed, disappearing logon assignments, and the inability of a user to access resources or log on.

- Domain control database

  The domain control database (DCDB) is a directory structure located on the domain controller. It contains files describing and controlling the current domain. The DCDB contains file, device, application, and machine definitions, as well as remote IPL images and user profiles, as described in Table 3.

Table 3. Domain Control Database Directory Structure

Subdirectory	**Contents**
\DATA	DCDB and ACPs
\FILES	*.CMD or *.BAT files for external files resources
\DEVICES	*.CMD or *.BAT files for external serial device resources
\PRINTERS	*.CMD or *.BAT files for external printer resources
\APPS	*.CMD or *.BAT files to start applications
\IMAGES	*.img or *.def files for remote IPL
\LISTS	DOS LAN Services list files
\USERS\user ID	User profiles for each user ID that contain: • Private applications • Public applications • Logon assignments • Logon profile

- HPFS386.INI

  The HPFS386.INI file contains the initialization parameters for the 386 HPFS. The initialization parameters include those that specify directory size limits.

- NET.AUD

  The NET.AUD file contains the following audit log information for the server:

  - Requests for session connection
  - Requests for logon and logoff
  - Share requests
  - Logon limit violations
  - Changes to the user and group accounts database
  - Changes to the access control database

  This information can be used for accounting, security, network use analysis, and problem determination.

- 386 HPFS directory size limits

  The 386 HPFS directory size limits feature is available only with LAN Server Advanced for the 386 HPFS. The size limitations associated with each directory are stored in the file system.

1.5.2 Operational Data

LAN Server operational data is on the server or peer system that is sharing the resource.

Operational data includes:

- Shared data areas

  Shared data areas include files and directories, which are typically text, executable, and command files.

- LAN applications

  LAN applications include files and directories, which are typically text, executable, command, and application customization files. Depending on the application they may also include database or specialized licensing directories and files.

  Specialized applications, such as Lotus Notes and DB2/2 databases, require special procedures for backup and recovery. Two detailed redbooks describe ADSM backup and recovery of these specialized applications:

  - *Using ADSM to Back Up Lotus Notes* (SG24-4534)
  - *Using ADSM to Back Up Databases* (SG24-4335-01)

- Home directories

Home directories include files and directories, which are typically text, command, and application customization files.

- Spooler queues

  Spooler queues are typically a single directory with transient printer files.

Operational data generally has ACPs associated with it. To ensure that you can fully restore operational data, back up both the data and its associated ACPs. For information on backing up ACPs, refer to 1.6.4.4, “Access Control Profiles” on page 33.

1.6 LAN Server Backup and Recovery

LAN Server incorporates data that is accessed at different times in different ways. Some data is accessed only during server initialization, other data is accessed only as required, and yet other data is accessed during system startup and not released until system shutdown. To ensure a comprehensive server backup, all data must be made available for backup at some point in time regardless of the system access requirements. A comprehensive backup of your LAN Server environment can be difficult because LAN Server keeps several of its system files in a continuous open and locked state. However, both LAN Server and ADSM provide specialized support for the backup of these files.

Let us look at the LAN Server backup utilities (BACKACC and RESTACC), using ADSM to directly back up and restore LAN Server, and a comparison of using ADSM directly or in conjunction with BACKACC and RESTACC. Let us state up front that, overall, we recommend using ADSM in conjunction with the LAN Server BACKACC and RESTACC utilities.

We finish this section by looking at ADSM backup of LAN Server from a different perspective: how to use ADSM to back up the system and operational data described in 1.5, “LAN Data” on page 16.

1.6.1 LAN Server Support

To enable you to back up and restore LAN Server open files, locked files, and ACP information, LAN Server provides the BACKACC and RESTACC utilities. The LAN Server documentation recommends that you use these utilities when backing up your LAN Server environment because many data backup and recovery programs do not support the direct backup and recovery of locked files.

If you are using the LAN Server Advanced local security feature, you must use the BACKACC and RESTACC utilities because its automated recovery process is based on them.

The local security feature protects local system files from unauthorized access even if LAN Server is not initialized because the feature is activated at system startup. The local security feature initializes the user account subsystem and accesses the NET.ACC file. If the NET.ACC file is corrupt or missing, it automatically attempts to copy the BACKACC-created NETACC.BKP file on top of the corrupted NET.ACC file (see 1.6.1.1, “LAN Server Backup and Restore Utilities” for details on how BACKACC works). A successful copy enables the local security initialization to continue. A failure of the copy causes the system to boot without local security.

1.6.1.1 LAN Server Backup and Restore Utilities

Figure 7 on page 23 shows the overall BACKACC and RESTACC process. The process differs according to the type of file system. BACKACC is used for both LAN Server Entry and Advanced; RESTACC is required only for 386 file systems and thus only for LAN Server Advanced.

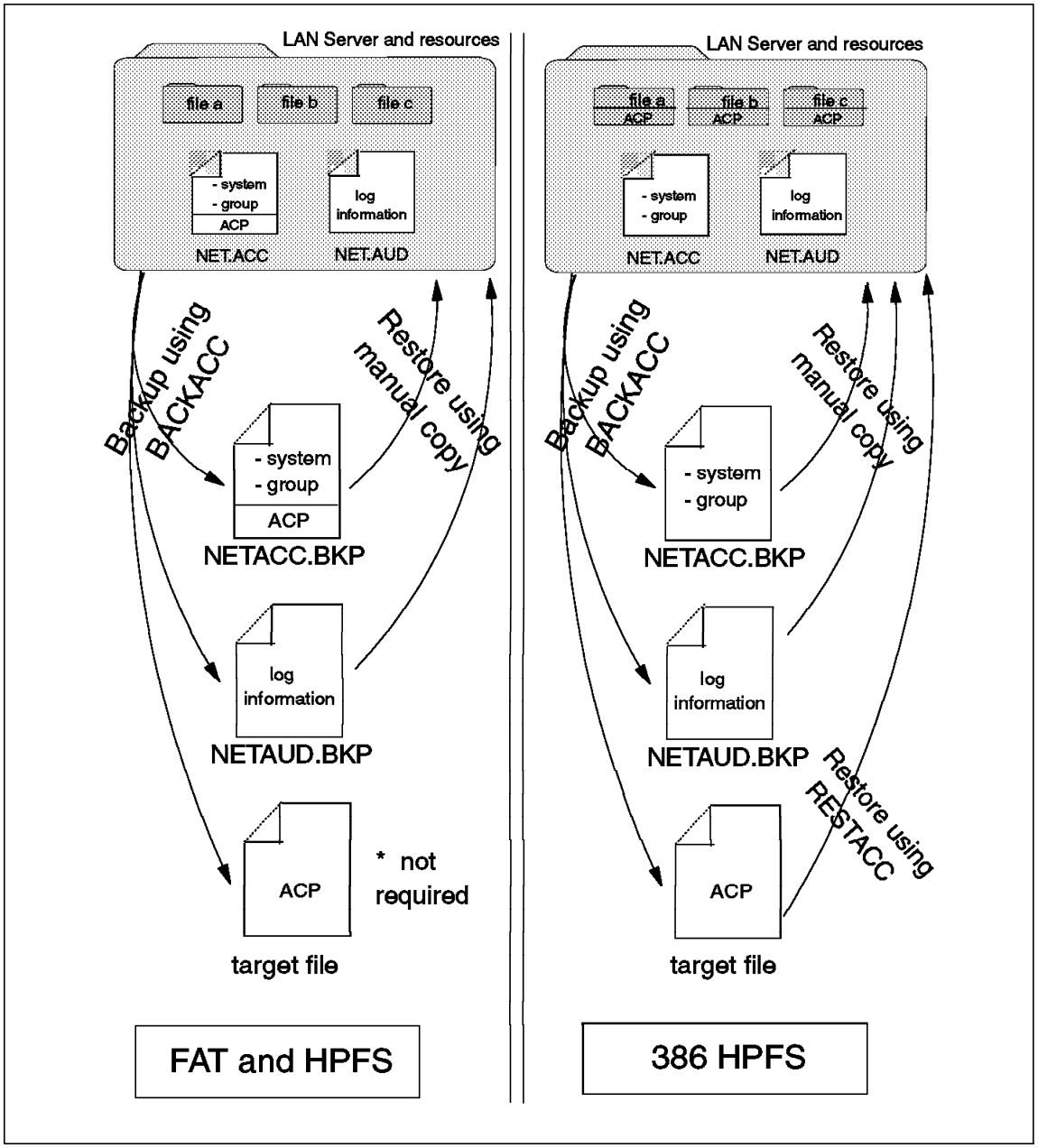


Figure 7. BACKACC and RESTACC Process

The invocation of BACKACC differs according to the type of file system. Because LAN Server Entry stores its ACPs in the NET.ACC file, BACKACC can be run once to back up all ACPs. Because LAN Server Advanced with

386 HPFS stores the ACPs in the file system, BACKACC must be run for each disk drive partition with ACPs.

Let us look at BACKACC and RESTACC in more detail.

BACKACC: This utility, as shown in Figure 7 on page 23:

- Backs up the NET.ACC file to the NETACC.BKP file and places it in the same directory as the NET.ACC file (IBMLAN\ACCOUNTS)
- Backs up the NET.AUD file to the NETAUD.BKP file and places it in the same directory as the NET.AUD file (IBMLAN\LOGS)
- Backs up the ACPs for files and directories to the specified target directory and file. This is not required for FAT and HPFS file systems because the ACPs are in the NETACC.BKP file.
- Deletes ACPs for nonexistent directories.

Figure 8 shows the BACKACC command syntax,

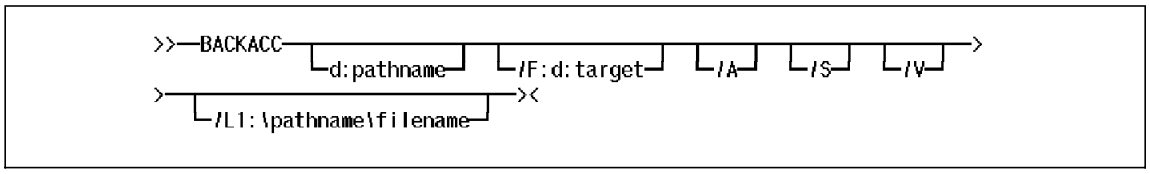


Figure 8. BACKACC Command Syntax

where:

- **d:\pathname**

  Is the path to the directory and files whose permissions are being backed up.

- **/F:d:\target**

  Is the target path and file that the BACKACC utility uses to store the access control information.

- **/A**

  Is an informational parameter telling the BACKACC utility to update the target file instead of overwriting it.

- **/S**

  Is an informational parameter telling the BACKACC utility to back up ACPs for the specified directory and all descendant subdirectories.

- **/V**

Is an informational parameter telling the BACKACC utility to display the names of the access control files as they are being backed up.

- **/L1:\pathname\filename**

  Is an optional parameter telling the BACCACC utility where the LAN CID utility should write its log.

Note

You do not have to stop the server to run the BACKACC utility.

For more information about ACPs and the NET.ACC and NET.AUD files, refer to 1.2.5, “Access Control Profiles” on page 9, and 1.5.1, “System Data” on page 18.

RESTACC: RESTACC restores ACPs for 386 HPFS file system resources backed up using the BACKACC utility, and deletes ACPs for nonexistent directories.

As you can see in Figure 7 on page 23, to restore the NET.ACC and NET.AUD files, you just manually copy the backups, NETACC.BKP and NETAUD.BKP. You **do not** use RESTACC.

Note

When recovering lost data and its associated ACPs, ensure that you restore the data before running the RESTACC utility. You must restore the data because RESTACC determines that ACPs are no longer required if the data they point to no longer exists.

Figure 9 shows the RESTACC command syntax,

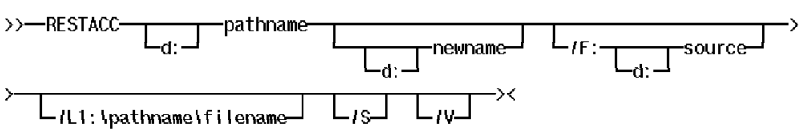


Figure 9. RESTACC Command Syntax

where:

- **d:\pathname**

Is the path to the directory and files whose permissions are being restored.

- **d:\newname**

  Is an optional parameter specifying the path to the file or directory that is to receive the permissions for the file or directory associated with pathname.

- **/F:d:\source**

  Is the source path and file that the RESTACC utility uses to restore the access control information.

- **/L1:\pathname\filename**

  Is an optional parameter telling the BACCACC utility where the LAN CID utility should write its log.

- **/S**

  Is an informational parameter telling the BACKACC utility to restore ACPs for the specified directory and all descendant subdirectories.

- **/V**

  Is an informational parameter telling the BACKACC utility to display the names of the access control files as they are being restored.

Note

You do not have to stop the server to run the RESTACC utility.

1.6.2 ADSM Support

ADSM provides backup and restore support for both files and directories.

1.6.2.1 Files

ADSM supports the direct backup of LAN Server data files and system files that are open and locked during server operation.

To back up ACPs for FAT and HPFS files and directories, you must back up the NET.ACC or, preferably, the NETACC.BKP file. ADSM does not back up ACPs for FAT and HPFS files and directories at an individual file and directory level.

ADSM does back up and restore local 386 HPFS files and directories and the ACPs stored within them. Optionally you can turn off ADSM ACP support by using the SKIPLANSERVERACP=YES parameter either on the ADSM backup command or in the DSM.OPT file. This parameter informs ADSM

that it should not request the ACP information when backing up files and directories from 386 HPFS drives. SKIPLANSERVERACP improves backup performance when using ADSM in conjunction with the LAN Server BACKACC utility, because BACKACC captures the ACP information so ADSM does not have to capture it. The ability to skip backing up ACPs is available with the ADSM for OS/2 V1R2 L0.6 client, but it is undocumented. If you use the SKIPLANSERVERACP option, check that it is still available and known by the same name when upgrading to future levels of ADSM.

We strongly recommend that you use the SKIPLANSERVERACP option exclusively. Do not turn SKIPLANSERVERACP on and off between backups. If you change the status of SKIPLANSERVERACP, all files that contain ACP data are rebacked up when the next incremental backup occurs. The rebackup could result in the back up of very large amounts of data and premature expiration of older versions of files stored on the ADSM server. We also recommend using the SKIPLANSERVERACP option in the DSM.OPT file instead of on ADSM commands.

Note

ADSM does not support the backup and restore of ACPs associated with local or remote (net used) FAT and HPFS drives.

ADSM does not support the backup and restore of ACPs associated with remote 386 HPFS network drives, that is, net used drives.

1.6.2.2 Directories

ADSM provides full backup, restore, and ACP support of populated (nonempty) directories, using a variety of backup and restore selection methods. For example, you can back up directories by using the ADSM incremental, incremental by date, file specification, or directory tree back up methods.

ADSM provides support for ACPs and the backup of empty subdirectories when you use using the incremental backup method. It provides support for ACPs and the restoration of empty subdirectories when you use the subdirectory path method. If you choose to back up or restore directories by using any other method, ADSM will not process empty directories. This is an important consideration when backing up and restoring file structures that may contain empty subdirectories, such as the LAN Server DCDB.

Note

If a directory and its contents are deleted, and ADSM is used to recover the directory and data, all associated ACPs will be restored.

If the contents of a directory are deleted but the directory is not, and ADSM is used to recover the data, all ACPs associated with the data will be recovered, but the ACPs associated with the directory will not be recovered. Directory ACPs are recovered only when a directory is newly recreated during restore from the ADSM backup copy.

1.6.2.3 LAN Server Administration during ADSM Backups

We recommend that you not schedule system data backups to occur while you are performing LAN administration, as such backups cause many critical system files to be open and unavailable for backup.

Critical system files could be backed up if you have specified dynamic serialization in your backup copy group. However, they would be fuzzy backups and, when restored, they may not mirror the state of the actual file before the disaster occurred.

1.6.3 Should You Use ADSM Directly or with LAN Server BACKACC?

If you are using ADSM to back up and recover your LAN Server environment, you can back up and restore LAN Server open files and ACPs by using one of two methods: ADSM in conjunction with the LAN Server utilities (BACKACC, RESTACC) or ADSM direct backup and restore. The backup and recovery steps for each method depend on the server file system. HPFS and FAT file systems store their ACP data in the NET.ACC file, whereas 386 HPFS stores its file and directory ACP information within the file system. The advantages and disadvantages of using ADSM directly or in conjunction with the LAN Server BACKACC and RESTACC utilities are summarized in Table 4 on page 29, Table 5 on page 29, Table 6 on page 30, and Table 7 on page 31.

Overall, we recommend using ADSM in conjunction with the LAN Server utilities.

Note

Neither ADSM nor the LAN Server utilities support the direct restoration of files that are open and locked by LAN Server during run time.

Table 4. HPFS and FAT File System Backup and Recovery Using ADSM Directly

Backup	Advantages
• Direct ADSM backup of LAN Server files and directories Recovery • Direct ADSM restore of LAN Server files and directories	• Single-step backup and restore process Disadvantages • A full restore of the NET.ACC file is required because ACP information is not saved at the file level. Updates to the NET.ACC file are lost when the backed up NET.ACC file is restored over an existing NET.ACC file. • Does not provide any additional housekeeping facilities, such as the detection and deletion of old ACP definitions

Table 5. HPFS and FAT File System Backup and Recovery Using ADSM with LAN Server BACKACC Utility

Backup	Advantages
• BACKACC utility to back up NET.ACC and NET.AUD files • ADSM backup of LAN Server files, directories, and BACKACC-produced files Recovery • ADSM restore of LAN Server files, directories, and BACKACC-produced files	• Provides additional housekeeping facilities, such as the detection and deletion of old ACP definitions Disadvantages • Two-step backup process • Requires that additional files be backed up (for example, NET.BKP)

Table 6. 386 HPFS Backup and Recovery Using ADSM Directly

Backup	Advantages
• Direct ADSM backup of LAN Server files and directories (including ACPs in the file system) Recovery • Direct ADSM restore of LAN Server files and directories (including ACPs)	• Single-step backup and restore process Disadvantages • Does not provide any additional housekeeping facilities, such as the detection and deletion of old ACP definitions • The time required to back up each file or directory increases significantly because ADSM must separately request the file and directory data from the ACP information. For each file and directory backup, ADSM must make two requests to the LAN Server application programming interface (API), one for the file and directory data and one for the ACP information. • You must manually create the NETACC.BKP file for local security feature automated recovery.

Table 7. 386 HPFS Backup and Recovery Using ADSM and LAN Server BACKACC and RESTACC Utilities

Backup • BACKACC utility to back up NET.ACC and NET.AUD files and ACPs • ADSM backup of LAN Server files, directories, and BACKACC-produced files Recovery • ADSM restore of LAN Server files, directories, and BACKACC-produced files • RESTACC utility to restore file and directory ACPs to the file system	Advantages • Provides additional housekeeping facilities, such as the detection and deletion of old ACP definitions • Window required to back up files and directories can be reduced if you use the SKIPLANSERVERACP option. • Creates the NETACC.BKP file for local security automated recovery Disadvantages • Two-step backup process • Two-step restore process • Requires that additional files be backed up (for example, NETACC.BKP) • Additional backup time required to run the BACKACC utility. The time required is directly proportional to the number of files and directories. If you have a large or complex file system, the time to run BACKACC increases.

When deciding which backup and recovery process to implement for your LAN Server environment, consider:

- The current backup and recovery process you have today

  If the established process schedules and uses the LAN Server utilities and you are happy with it, you may not want to change it.

- Which file systems are implemented within your environment

  If you have HPFS and FAT file systems and are not adding and deleting files remotely, you might generate a lot of ACP information in the

NET.ACC file that is no longer valid. You should periodically delete this invalid data, using the LAN Server utilities. Therefore, you may want to use the LAN Server utilities for backup and recovery.

- The size of your backup window

  With a 386 HPFS, you will require a longer backup window if you are using ADSM directly rather than in conjunction with the LAN Server utility. The backup window may be significant if you have a lot of disk space or a complex file and directory structure.

- Whether you have implemented local security

  If you have implemented local security, ensure that you have a NET.ACC file backup, that is, NETACC.BKP, and that it is located in the IBMLAN\ACCOUNTS directory.

Overall, we recommend using ADSM in conjunction with the LAN Server utilities.

1.6.4 Using ADSM to Back Up and Restore LAN Server System Data

Now that we have described in detail how to use ADSM with and without the LAN Server backup utilities, let us look at LAN Server backup from a different perspective. We look at the LAN server system data described in 1.5.1, “System Data” on page 18, and explain how to use ADSM to back it up.

1.6.4.1 LAN Server Program Files

LAN Server program data includes files and directories that reside in the IBMLAN directory. Most files are not open or locked during normal LAN Server processing.

A sample scenario of LAN Server program file back up and restore is discussed in 2.6, “LAN Server Entry Entire Partition” on page 70.

1.6.4.2 IBMLAN.INI

The IBMLAN.INI file resides in the IBMLAN directory and is accessed by the LAN Server server and requester components during startup. After startup the file is not accessed again. ADSM can back up IBMLAN.INI at any time other than initial server or requester startup.

A sample scenario of LAN Server program files (such as IBMLAN.INI) backup and restore is discussed in 2.6, “LAN Server Entry Entire Partition” on page 70.

1.6.4.3 PROTOCOL.INI

The PROTOCOL.INI file resides in the IBMCOM directory and is initially read during system startup. The PROTOCOL.INI information is then stored in memory so that any other applications that require protocol resources or network adapter information can access the information. After system startup, PROTOCOL.INI is closed and thus available for ADSM backup.

1.6.4.4 Access Control Profiles

The location of ACPs depends on the file system used. ACPs can be in the NET.ACC file or the file system itself.

If ACPs are in the NET.ACC file, they are backed up and restored as part of the NET.ACC backup and restore process. For more information about this process, refer to 1.6.4.5, “NET.ACC.”

If ACPs are in the file system itself, the LAN Server BACKACC utility should be used before ADSM backup, and the RESTACC utility should be used after ADSM restore (for 386 HPFSs). For more information about the BACKACC and RESTACC utilities, refer to 1.4, “LAN Utilities” on page 15.

Sample scenarios of LAN Server Entry and LAN Server Advanced ACP backup and restore are discussed in 2.2, “LAN Server Entry Operational Data” on page 41 and 2.3, “LAN Server Advanced Operational Data” on page 58.

1.6.4.5 NET.ACC

The NET.ACC file resides in the IBMLAN\ACCOUNTS directory. It is accessed by the server during startup and is subsequently kept open and locked until LAN Server is stopped or the system is shut down. Therefore the NET.ACC file is not usually available to backup utilities. However, ADSM can back up the NET.ACC directly because it can handle the type of LAN Server lock used for the file (we do not recommend using ADSM to back up the NET.ACC file directly, however). LAN Server provides the BACKACC utility to back up the NET.ACC to a target file. You can then back up the target file by using ADSM.

To correct a suspected NET.ACC problem you could immediately restore it by using your ADSM backup copy. However, if you have made changes to your LAN Server definitions (such as adding users or resources) since your last backup, you lose these updates and must manually add them to the restored NET.ACC file. To restore the NET.ACC to its most current state, and to avoid or keep manual updates to a minimum, we recommend trying each of the following three recovery options in order. If one of the recovery options is successful, you do not have to proceed to the next recovery

option. In other words, you should not start your recovery procedure with ADSM restore option 3; try options 1 and 2 first.

1. Run the CHKDSK utility.

   This utility checks the status of a hard disk partition and optionally fixes any minor errors that it encounters. The CHKDSK.COM program is located in the root directory on OS/2 diskette 2. When running the CHKDSK program against the OS/2 boot hard disk partition, the OS/2 boot must be performed from maintenance diskettes.

2. Run the LAN Server Entry FIXACC utility.

   When LAN Server updates the NET.ACC file, it sets on an “in use” flag. If a condition occurs that prevents LAN Server from completing the update, LAN Server may leave the flag on and consider the NET.ACC file unusable, even though there may be only one bad record. The FIXACC utility reads the unusable NET.ACC file and builds a new file that does not have the “in use” flag set to on.

3. Replace the corrupted NET.ACC file with the ADSM backup of the NETACC.BKP file produced by the BACKACC utility.

   Note

   When replacing the NET.ACC file, you must ensure that LAN Server, or any other program that also uses the NET.ACC file, such as Database Manager for OS/2, is not running on the system. The NET.ACC file cannot be restored while any of these programs are active.

Sample scenarios of the NET.ACC file for LAN Server Entry and LAN Server Advanced backup and restore are discussed in 2.2, “LAN Server Entry Operational Data” on page 41 and 2.3, “LAN Server Advanced Operational Data” on page 58.

1.6.4.6 Domain Control Database

The DCDB data resides in the IBMLAN directory and includes files and directories. These files are accessed by the server when a user launches a LAN application from his or her public applications folder, when a remote system is IPLed, or when a user logs on to the LAN. The DCDB files are neither open nor locked during normal LAN Server processing and are thus available for ADSM backup.

If you do not have external serial devices, files, or printer resources, or if you do not use command or .BAT files to invoke your shared LAN applications, you may have empty directories within your DCDB. Even though these directories are empty, LAN Server attempts to access them

during initialization. If these directories are not available, LAN Server reports an error.

If you choose to use the ADSM incremental backup method, ADSM recognizes and backs up both full and empty directories. If you use ADSM selective backup by file specification or directory tree, ADSM only backs up directories that contain files. To ensure that you have a full DCDB backup, you must complete at least one incremental backup. Conversely, to support the restoration of empty subdirectories, you must use the subdirectory path restore option rather than either the file specification or directory tree option.

Note

When LAN Server is installed and the DCDB is initialized, LAN Server automatically associates default ACPs with the DCDB. To ensure that you can fully restore the DCDB, you must back up the DCDB files and directories (both full and empty) and their associated ACPs.

A sample scenario of a DCDB for LAN Server Entry back up and restore is discussed in 2.5, “LAN Server Entry Domain Control Database” on page 66.

1.6.4.7 HPFS386.INI

The HPFS386.INI file resides in the IBM386FS directory and is accessed by OS/2 during system startup, and by LAN Server during server startup. After startup the file is not accessed again. It is closed and available for ADSM backup.

1.6.4.8 NET.AUD

The NET.AUD file resides in the IBMLAN\LOGS directory. If LAN Server accounting is activated, NET.AUD is accessed by the server during startup and is subsequently kept open and locked until LAN Server is stopped or the system is shutdown. Therefore the NET.AUD is not usually available to backup programs. However, ADSM can back up NET.AUD because it can handle the type of LAN Server lock used for the file. LAN Server provides BACKACC to back up the NET.AUD to a target file. You can then back up the target file by using ADSM. This is the approach we recommend.

When restoring the NET.AUD file, use ADSM to restore the target file produced by the BACKACC utility, ensure that LAN Server is not running on the system, delete the corrupted NET.AUD file, and restore the backup copy in its place.

1.6.4.9 386 HPFS Directory Size Limits

The directory size limits are kept within the file system, and they are accessed each time data is written to the directory. Directory size limits are accessed to check whether writing the data will exceed the preset alert threshold or limit. The directory size limits information is generally neither open nor locked during normal LAN Server processing.

LAN Server does not provide any utilities to back up directory size limits, nor does the ADSM server V1R2 level 0.9/1.9 or ADSM OS/2 client V2R1 level 0.2, which we used in our environment. However, the directory size limits are available through LAN Server APIs. The NetDASDEnum or Net32DASDEnum LAN Server APIs return a list of directories that have had directory size limits applied to them. They also return other related information, such as the limit applied to each directory, the space used, and the alert and incremental threshold values. The NetDASDAdd and Net32DASDAdd APIs invoke the directory size limit function, placing a limit on the disk space that can be used within a directory tree.

To back up the directory size limits, you have to write two small applications. One application backs up the directory size limits by querying LAN Server for the directories that have limits associated with them as well as the information related to each directory. This application then saves this information to a file that ADSM can back up. The second application is used during the restore procedure to interrogate the file produced by the first backup application to determine the directories that have limits associated with them as well as the information related to each directory. This restore application then restores this information to LAN Server.

Two such sample applications, BACKDLIM and RESTDLIM, are provided in A.5, “LAN Server Directory Size Limits Backup and Restore” on page 157 and on the diskette in the back of this book. They were written by Will Fabri from IBM Belgium. They are simple applications that back up and restore directory size limits with ADSM, but you could add more elaborate commands that return processing complete and error messages.

1.6.5 Using ADSM to Back Up and Restore LAN Server Operational Data

Now let us look at how to use ADSM to back up the LAN Server operational data described in 1.5, “LAN Data” on page 16.

1.6.5.1 Shared Data

Shared data includes files and directories. Typically shared data can be backed up at any time regardless of the processes being run on the local system. However, it is possible that a user might access a file that is scheduled to be backed up. To avoid this situation, schedule your shared

data backups during either quiet network periods or maintenance windows when users should not be accessing LAN resources.

In the event that a user accesses a file at the time it is scheduled to be backed up, ADSM decides whether or not to back up the file on the basis of the backup copy group serialization set by the ADSM administrator. At the end of the backup, ADSM detects whether a file has changed since it initially read the file attributes. If ADSM detects that the file has changed, it might:

- Not back up the open file (static serialization)
- Back up the open file (dynamic serialization)
- Retry backing up the open file several times. If the file is closed on any of the retry attempts, it backs it up (shared static serialization).
- Retry backing up the open file several times. If the file is still open after all attempts, it backs it up anyway (shared dynamic serialization).

With the dynamic and shared dynamic serialization options, you have the potential for a “fuzzy” backup.

1.6.5.2 LAN Application

LAN application data includes files and directories. As each application is unique in the services it provides, the mechanism it uses to provide its services, and the operating environment it uses, you cannot assume that you can use ADSM to directly back up all application files at any given time.

If an application has its own backup utilities and procedures, it is best to use them in conjunction with ADSM. You can usually use the application backup utilities to create a backup to a file and then use ADSM to back up that file. Some application utilities are updated to use the ADSM API, so that the backup can be sent directly to ADSM without creating an intermediate file. Check each application′s documentation for its ADSM support. If you are unsure, contact the vendor or try a test ADSM backup and recovery scenario. Be careful not to overwrite any production data during your test.

Examples of OS/2 applications that are updated to use the ADSM API are DB2/2 and Lotus Notes. For detailed information about ADSM backup of Lotus Notes, see *Using ADSM to Back Up Lotus Notes* (SG24-4534). For detailed information about ADSM backup of DB2/2, see *Using ADSM to Back Up Databases* (SG24-4335-01).

1.6.5.3 Home Directory

Home directory data includes files and directories. Typically home directory data can be backed up at any time, regardless of the processes being run on the local system. However, it is possible that a user might access a file

that is scheduled to be backed up. To avoid this situation, schedule your shared data backups during either quiet network periods or maintenance windows when users should not be accessing LAN resources.

In the event that a user accesses a file at the time it is scheduled to be backed up, ADSM decides whether or not to back up the file on the basis of the backup copy group serialization set by the ADSM administrator. ADSM detects, at the end of the backup, if the file has changed since ADSM initially read the file attributes. If ADSM detects that the file has changed, then the backup copy group serialization options are used.

1.6.5.4 Spooler Queue

The spooler queue is a directory that can be backed up at any time regardless of the processes being run on the local system. Typically, you would not back up the printer files within the spooler queue because they are transient files generated by users using shared LAN data and applications. If a user′s “printout” is lost, it can generally be re-created, provided that the user still has access to the same data and applications.

Chapter 2. LAN Server V4.0 Backup and Recovery Scenarios

In this chapter, we show sample LAN Server V4.0 backup and recovery scenarios that use ADSM with the LAN Server utilities.

First we give a short overview of the test environment we used for the scenarios. Then we show five scenarios that use the ADSM graphical user interface (GUI), providing step-by-step procedures for you to follow. The five scenarios detail backup and recovery of:

- LAN Server Entry operational data
- LAN Server Advanced operational data
- LAN Server Advanced directory size limits
- LAN Server Entry DCDB
- LAN Server Entry entire partition

We conclude with a realistic approach that you would implement in a customer environment: automatic backup. We provide three sample scripts to automate LAN Server backup. These sample scripts are detailed in A.4, “LAN Server Backup Scripts” on page 151, and provided on the diskette in the back of this book. The three scripts detail the automated backup and recovery of:

- LAN Server Entry
- LAN Server Advanced with 386 HPFS drives
- LAN Server Advanced with 386 HPFS drives and directory size limits

2.1 Test Environment

We used the same LAN Server, user, group, resource, access control, and directory size limit definitions for each scenario. These definitions are representative of those found in typical workgroup, departmental, and corporate LAN environments. For more information about the ACPs, domain definitions, and system software levels, see Appendix A, “LAN Server Test Environment and Scripts” on page 139.

Note

Although for our scenarios we installed most LAN Server components on the server, we did not configure these components:

- Fault tolerance
- Remote IPL
- Local security
- Replication

Figure 10 depicts the LAN Server environment we used for testing. We used dual boot (two C drives) to accommodate our Warp Server scenarios. We had all of the LAN Server data on one partition (D drive), so that we could access it no matter which C drive we used to boot. In a typical customer environment, you would probably have all system data on one partition (ADSM, MPTS/2, and LAN Server) and all user data (LAN Server resources) on another partition.

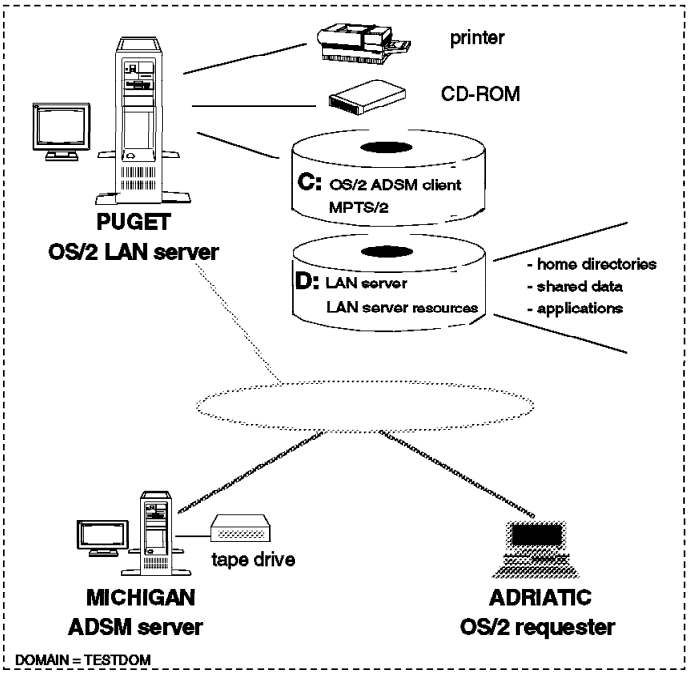


Figure 10. LAN Server Test Environment

2.2 LAN Server Entry Operational Data

This scenario shows the backup and recovery of operational data (shared data) that resides on a LAN Server Entry domain controller. The data area uses HPFS; therefore the shared data ACPs are kept in the NET.ACC file. Files are restored with the correct ACPs provided that the NET.ACC file is available and not damaged.

> **Note**
>
> For maximum recoverability we recommend that you back up the NET.ACC file at the same time that you back up the shared data area.

In this scenario we back up the D:\RESOURCES\SHAREDDATA shared data file. We assume that the NET.ACC, NETACC.BKP, and NETAUD.BKP files in the SHAREDDATA directory have been corrupted. These files must be restored from backup and the NET.ACC file replaced.

For information about the NET.ACC, NETACC.BKP, and NETAUD.BKP files refer to 1.5.1, “System Data” on page 18, and 1.6, “LAN Server Backup and Recovery” on page 21.

This scenario is representative of the steps you would take to back up and restore a variety of operational data (such as home directories) when using either an HPFS or a FAT file system.

2.2.1 Backup

Backup of the shared data area is a three-step process where you:

1. Back up the NET.ACC file, using the LAN Server BACKACC utility program
2. Back up the shared data
3. Back up the files produced by the BACKACC utility.

2.2.1.1 NET.ACC

As the NET.ACC file is kept open and locked by the server during run time, it cannot be directly backed up by many backup utilities. Its backup depends on the type of lock used by LAN Server and what the backup utility can recognize. ADSM can back up the NET.ACC file directly, although we do not recommend that approach. See 1.6.3, “Should You Use ADSM Directly or with LAN Server BACKACC?” on page 28 for more details.

To back up the NET.ACC file we recommend using the BACKACC utility provided with LAN Server. For more information about the BACKACC utility refer to “BACKACC” on page 24

Run the BACKACC utility.

At a command prompt type:

BACKACC /V

The BACKACC utility displays the file names that have been backed up, as shown in Figure 11.

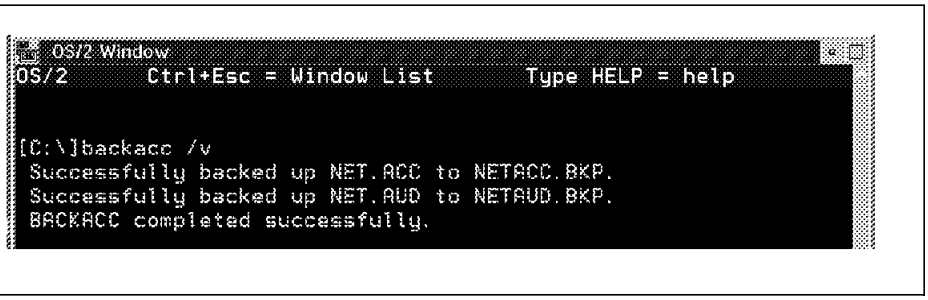


Figure 11. BACKACC Messages

BACKACC creates the following files:

- D:\IBMLAN\ACCOUNTS\NETACC.BKP
- D:\IBMLAN\LOGS\NETAUD.BKP

2.2.1.2 Shared Data

Now we back up the shared data area, D:\RESOURCES\SHAREDDATA, and all of its descendant subdirectories:

1. From your OS/2 desktop, double-click on the **ADSM Client** icon, as shown in Figure 12.

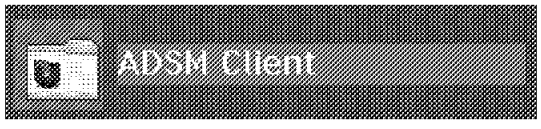


Figure 12. ADSM Client Icon

The ADSM Client folder is displayed, as shown in Figure 13 on page 43.

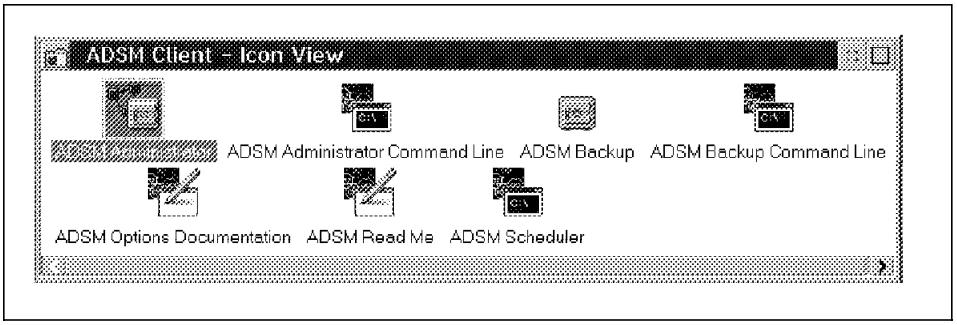


Figure 13. ADSM Client Folder

2. Double click on the **ADSM Backup** icon.

   The Password Entry window is displayed, as shown in Figure 14.

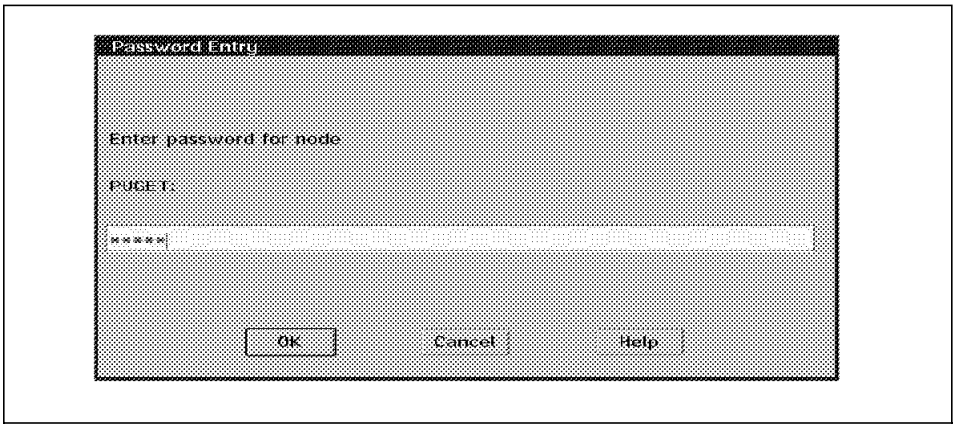


Figure 14. Password Entry Window

3. Enter the node password.
4. Select the **OK** button.

   The Drive Information window is displayed, as shown in Figure 15 on page 44.

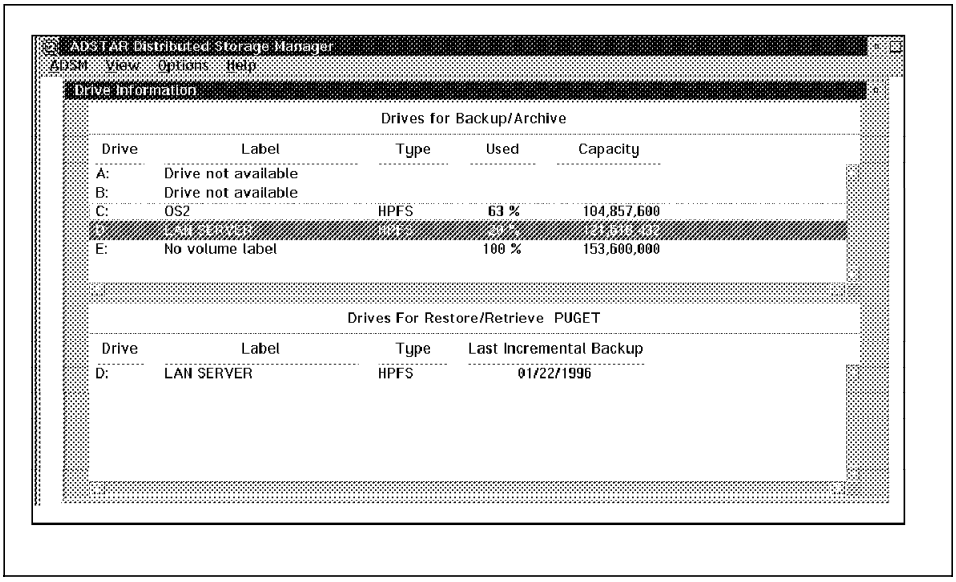


Figure 15. Drive Information Window

5. Under the Drives for Backup/Archive section, select the LAN Server drive, D.
6. Select **ADSM** from the action bar.
7. Select **Backup** from the pull down menu.

   A side menu is displayed, as shown in Figure 16 on page 45.

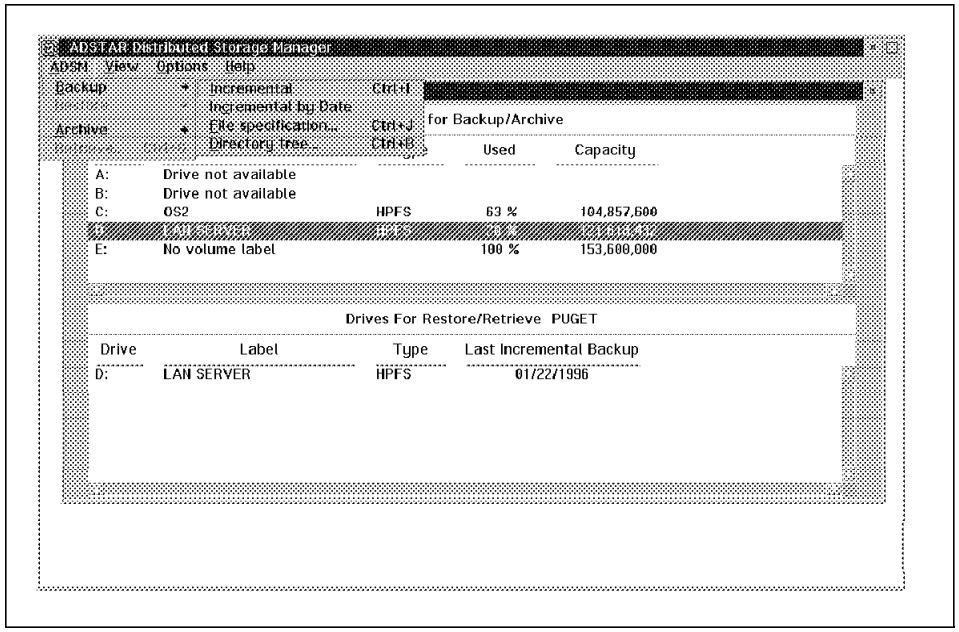


Figure 16. ADSTAR Distributed Storage Manager Window: Shared Data Backup

8. Select **File specification** from the side menu.

Note

This backup method does not capture empty subdirectories. At least one incremental backup is required to capture empty subdirectories. You could back up the shared data directories and files by using the incremental, incremental by date, or directory tree method if you prefer.

The Backup by File Specification window is displayed, as shown in Figure 17 on page 46.

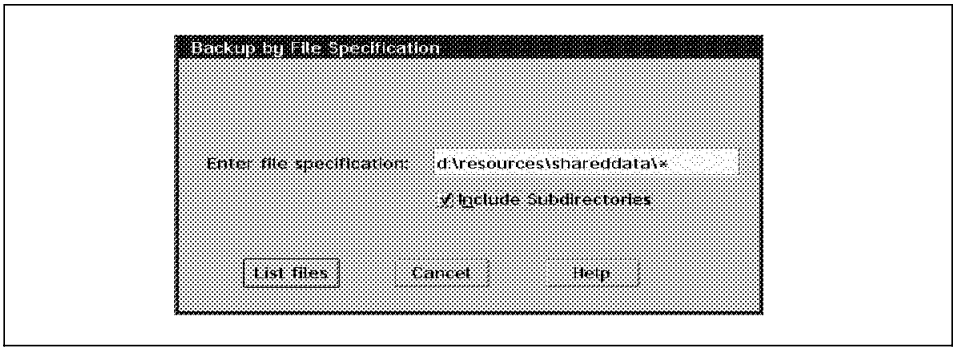


Figure 17. Backup by File Specification Window

9. Enter d:\resources\shareddata* in the **Enter file specification** field.

   If your D drive is very large or has many directories and files, you may encounter an ADSM error indicating that the list box is full or there is a system memory error because the ADSM GUI reserves 64 KB for this information. In this situation use the ADSM command line interface (CLI) because it uses memory to process and display this data.

   Note

   Ensure that you include the slash and wildcard at the end of your path specification, otherwise ADSM will not find any files or subdirectories. Neglecting to include the slash and wildcard causes the following ADSM errors:

   - ANS2036W No files found for file specification entered
   - ANS2318W Incorrect file specification entered

10. Check the **Include Subdirectories** check box.
11. Select the **List files** button.

    The Backup by File Specification window is displayed, as shown in Figure 18 on page 47.

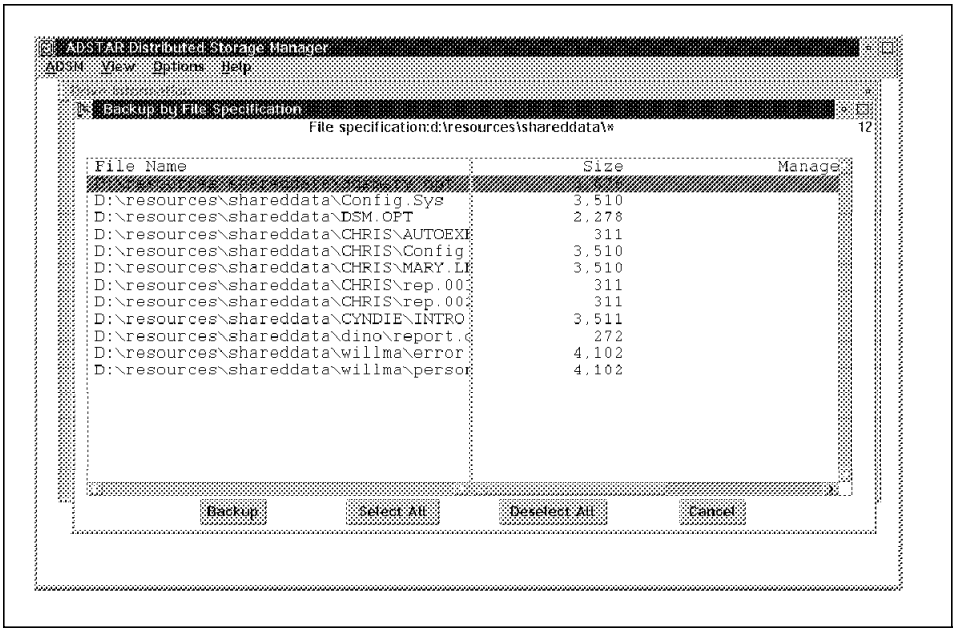


Figure 18. Backup by File Specification Window

12. Select the **Select All** button.
13. Select the **Backup** button.

    The Mount Wait window may be displayed, as shown in Figure 19.

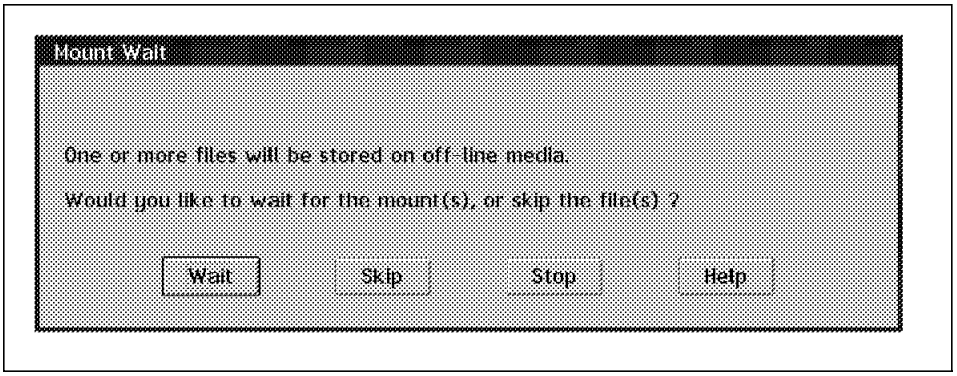


Figure 19. Mount Wait Window

14. Select the **Wait** button.

    Once the offline media have been loaded and ADSM has completed the backup, the Selective backup completed message box is displayed, as shown in Figure 20 on page 48.

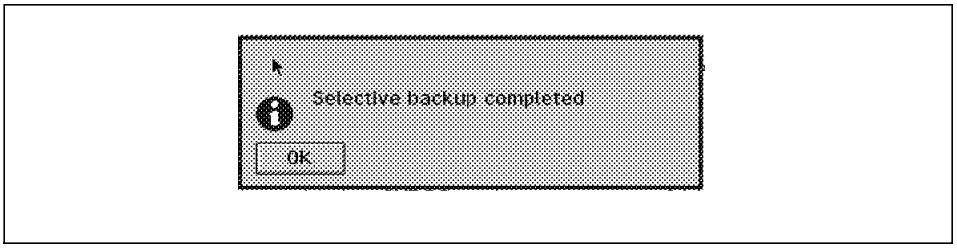


Figure 20. Selective Backup Completed Message Box

15. Select the **OK** button.

    The Backup Status window is displayed, as shown in Figure 21.

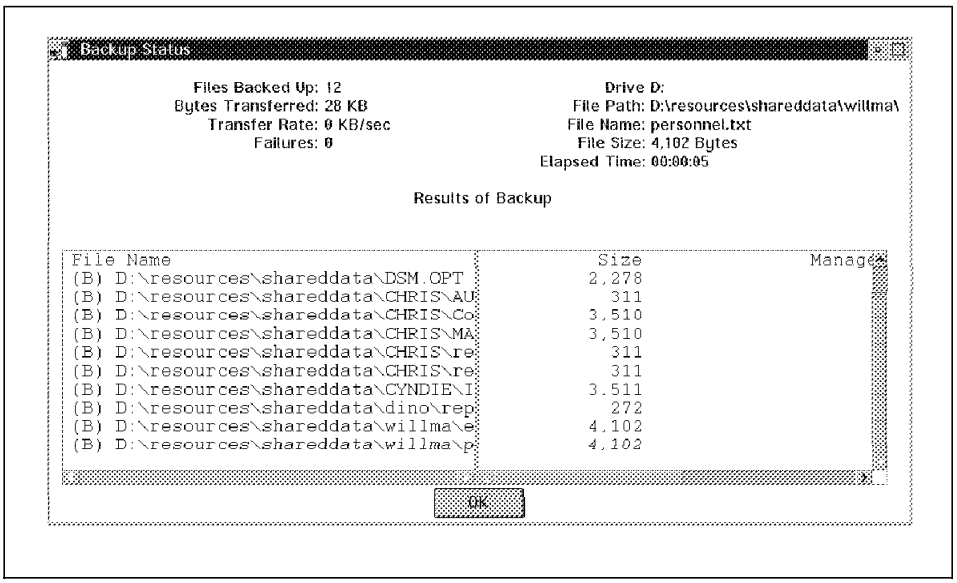


Figure 21. Backup Status Window

16. Select the **OK** button.

    The Backup by File Specification window is displayed.

17. Select the **Cancel** button.

    The Drive Information window is displayed.

2.2.1.3 NETACC.BKP and NETAUD.BKP

Now we back up the files produced by the BACKACC utility: NETACC.BKP and NETAUD.BKP.

1. Follow steps 1 - 7 in 2.2.1.2, “Shared Data” on page 42.

2. On the ADSTAR Distributed Storage Manager Window (Figure 17), select **Directory Tree** from the side menu.

> **Note**
>
> You could back up the files by using the file specification method if you prefer.

The Selective Backup by Directory Tree window is displayed, as shown in Figure 22.

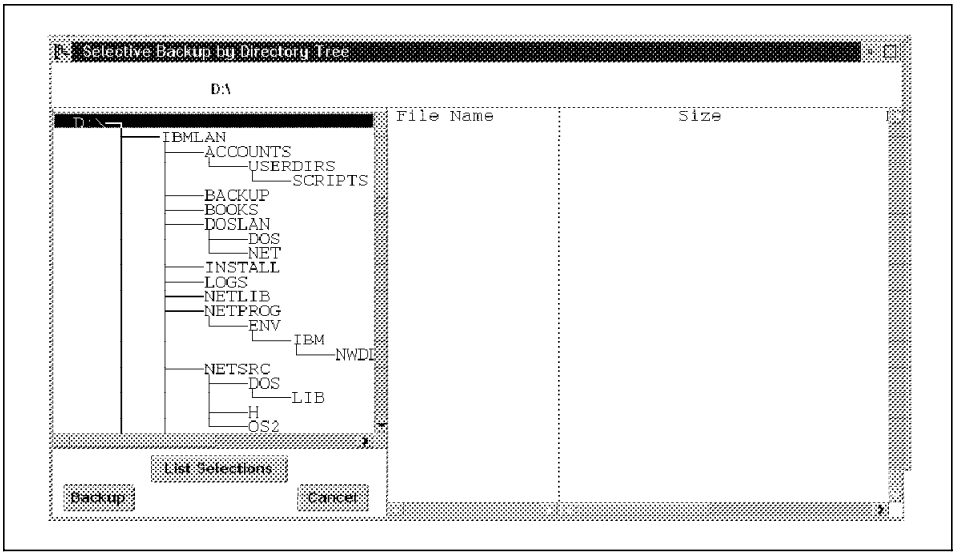


Figure 22. Selective Backup by Directory Tree Window

3. Double-click on the IBMLAN directory and then the ACCOUNTS directory. Select the D:\IBMLAN\ACCOUNTS\NETACC.BKP file. Double-click on the LOGS directory and select the D:\IBMLAN\LOGS\NETAUD.BKP file, as shown in Figure 23 on page 50.

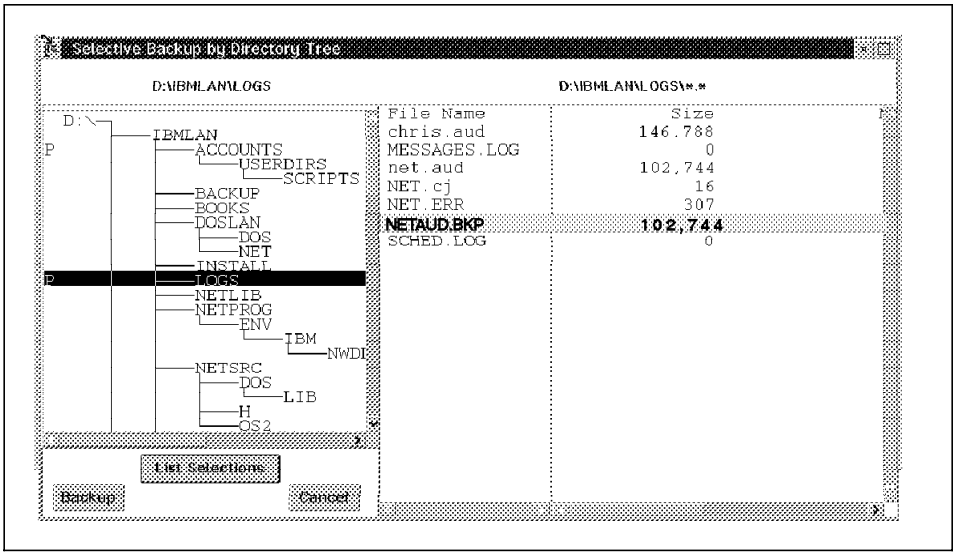


Figure 23. Selective Backup by Directory Tree Window Selections

4. Select the **List Selections** button.

   The Selected Files for Backup window is displayed, as shown in Figure 24, with both the NETAUD.BKP and NETACC.BKP files selected.

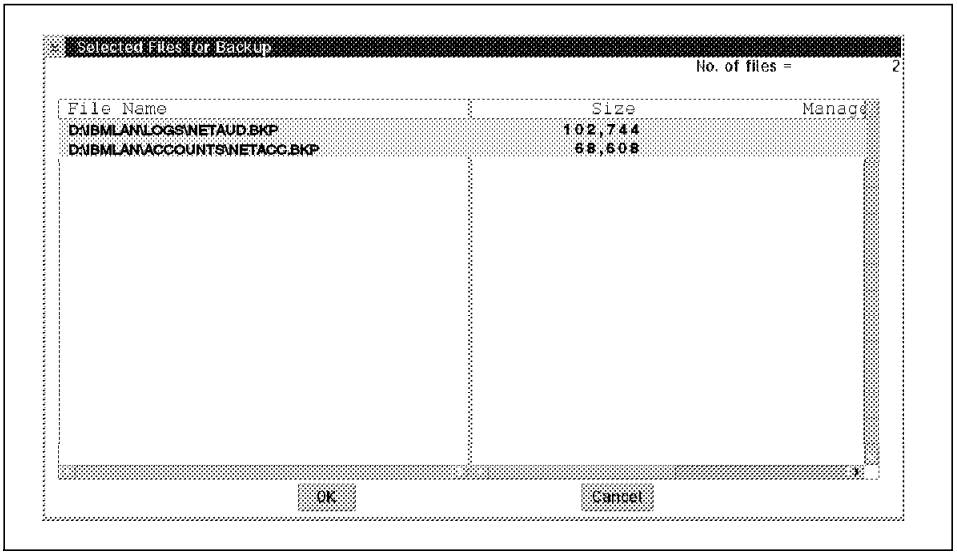


Figure 24. Selected Files for Backup Window

5. Select the **OK** button.

The Selective Backup by Directory Tree window is displayed (not shown).

6. Select the **Backup** button.

   The Mount Wait window may be displayed (not shown).

7. Select the **Wait** button.

   Once the offline media have been loaded and ADSM has completed the backup, the Selective backup completed message box is displayed (not shown).

8. Select the **OK** button.

   The Selective Backup by Directory Tree window is displayed (not shown).

9. Select the **Cancel** button.

   The Drive Information window is displayed (not shown).

2.2.2 Recovery

Recovery of the shared data area is a three-step process where you:

1. Recover the shared data
2. Recover the files produced by the BACKACC utility program
3. Replace the corrupted NET.ACC file

2.2.2.1 Shared Data

First we recover the shared data area, D:\RESOURCES\SHAREDDATA, and all of its descendant subdirectories:

1. From your OS/2 desktop, double-click on the **ADSM Client** icon.

   The ADSM Client folder is displayed.

2. Double-click on the **ADSM Backup** icon.

   The Password Entry window is displayed.

3. Enter the node password.
4. Select the **OK** button.

   The Drive Information window is displayed, as shown in Figure 25 on page 52.

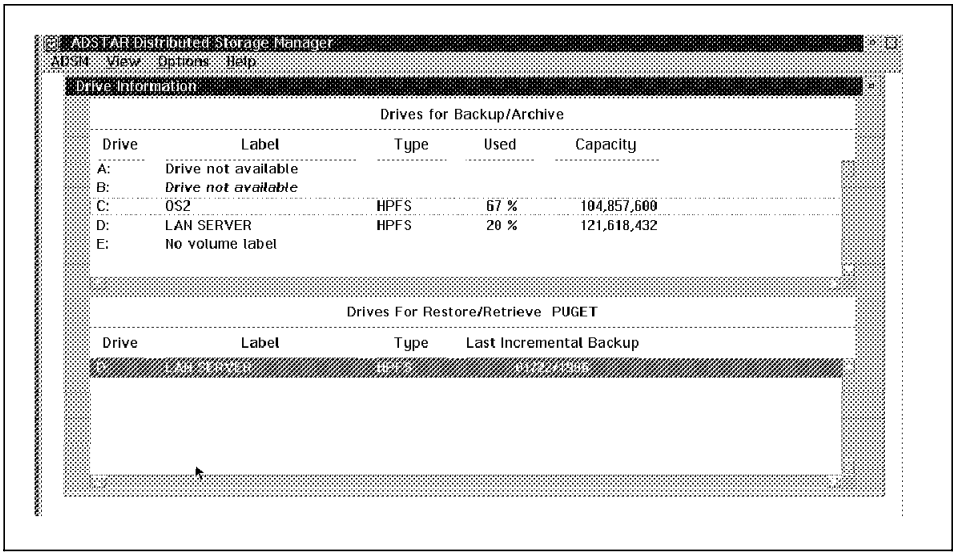


Figure 25. Drive Information Window

5. Under the Drives For Restore/Retrieve section, select the LAN Server drive, D.
6. Select **ADSM** from the action bar.
7. Select **Restore** from the pull-down menu.

   A side menu is displayed, as shown in Figure 26.

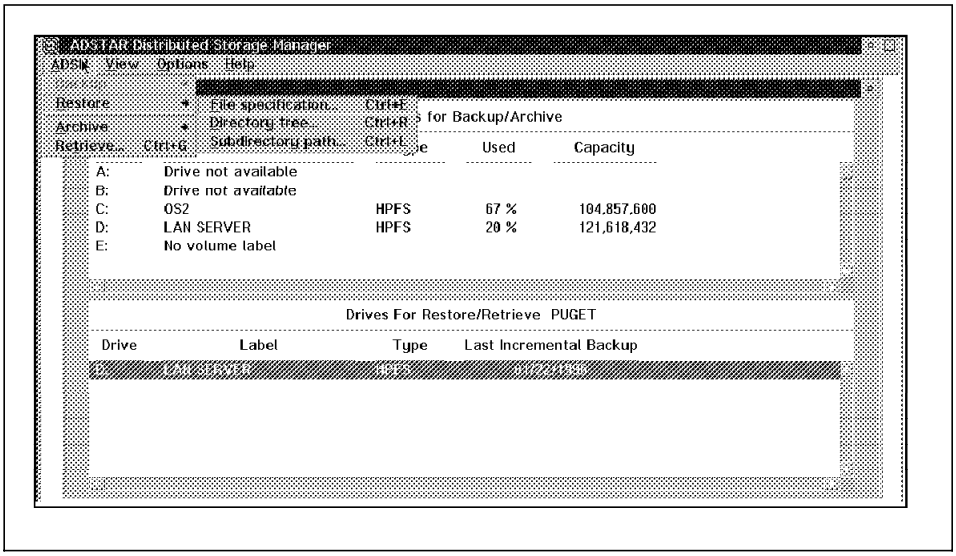


Figure 26. ADSTAR Distributed Storage Manager Window: Shared Data Restore

8. Select **Subdirectory path** from the side menu.

> **Note**
>
> You could recover the shared data directories and files by using either the file specification or directory tree method if you prefer. The subdirectory path method ensures that empty directories and their ACPs are properly restored.

The Restore Subdirectory Path window is displayed, as shown in Figure 27.

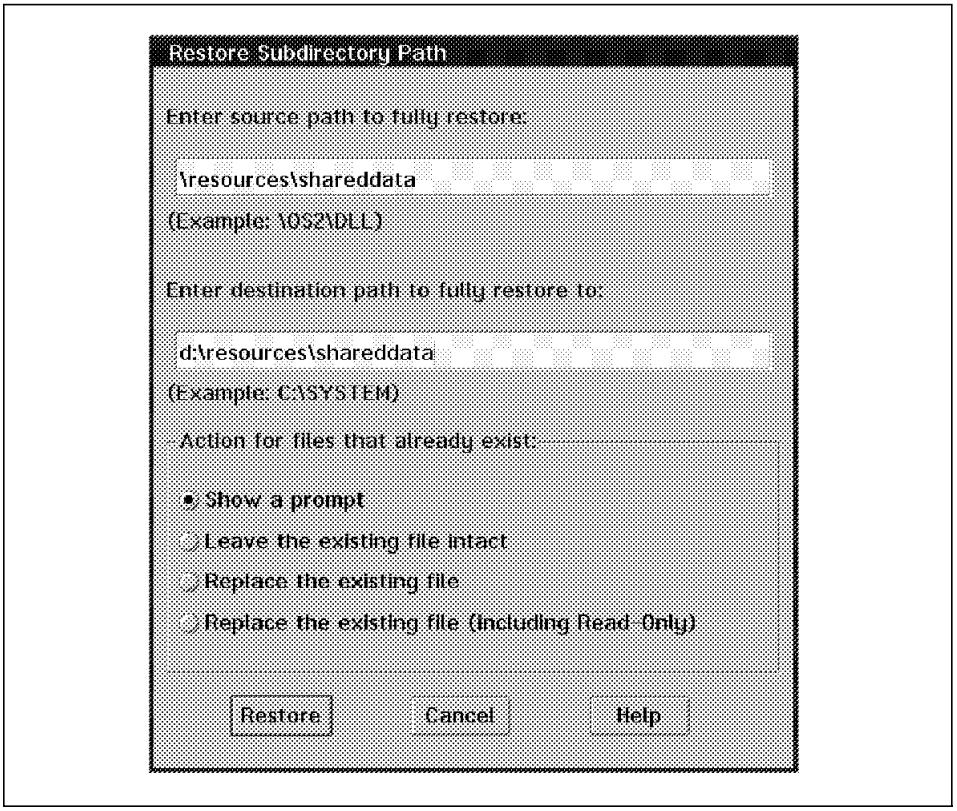


Figure 27. Restore Subdirectory Path Window

9. Recover the shared data directories and files to their original location:
   a. Enter \resources\shareddata in the **Enter source path to fully restore** field.
   b. Enter d:\resources\shareddata in the **Enter destination path to fully restore to** field.

c. Select the **Show a prompt** radio button from the **Action for files that already exist** options.

10. Select the **Restore** button.

    The Mount Wait window may be displayed.

11. Select the **Wait** button.

    The Wait message box is displayed, as shown in Figure 28.

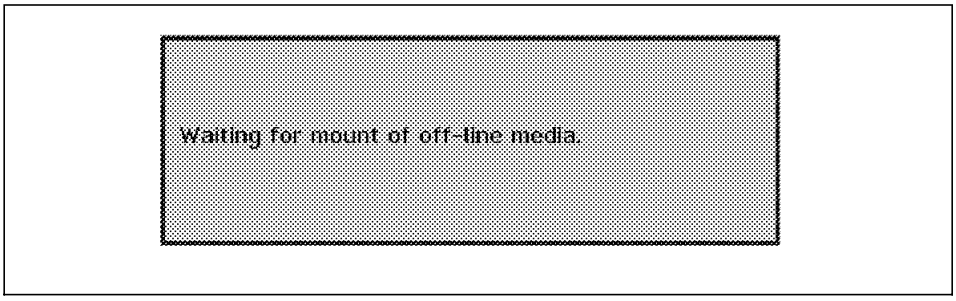


Figure 28. Wait Message Box

Once the offline media have been loaded and ADSM has completed the restore, the Restore completed message box is displayed, as shown in Figure 29.

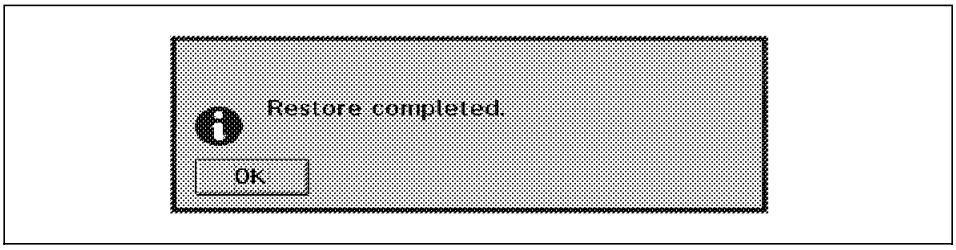


Figure 29. Restore Completed Message Box

12. Select the **OK** button.

    The Restore Status window is displayed, as shown in Figure 30 on page 55.

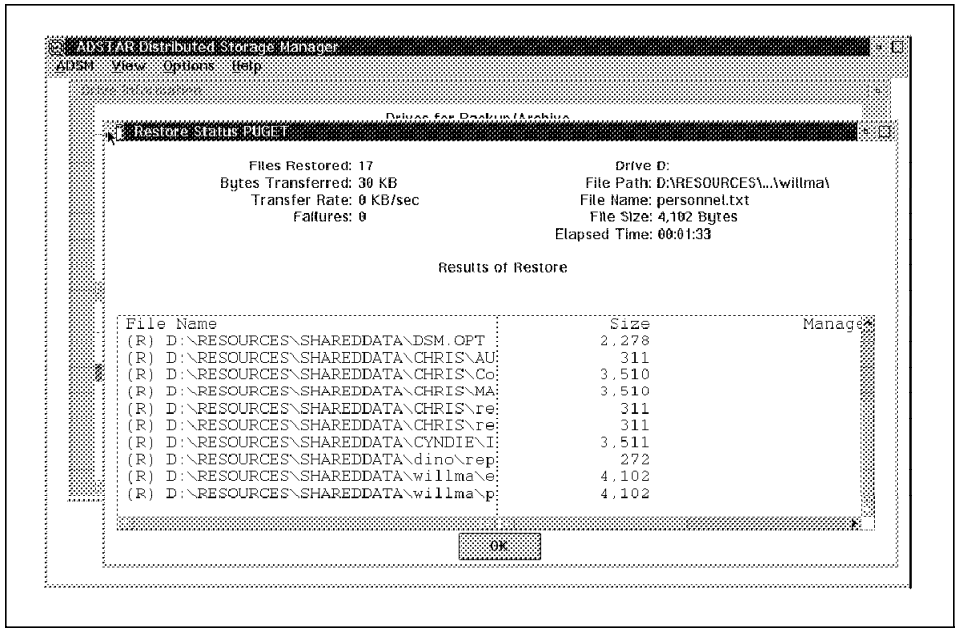


Figure 30. Restore Status Window

13. Select the **OK** button.

    The Restore by File Specification window is displayed.

14. Select the **Cancel** button.

    The Drive Information window is displayed.

2.2.2.2 NETACC.BKP and NETAUD.BKP

Next we recover the files produced by the BACKACC utility: NETACC.BKP and NETAUD.BKP.

1. Follow steps 1 - 7 in 2.2.2.1, “Shared Data” on page 51.
2. On the ADSTAR Distributed Storage Manager window (Figure 17), select **Directory tree** from the side menu.

   Note

   You could restore the files by using the file specification method if you prefer.

   The Restore by Directory Tree window is displayed.

3. Double-click on the IBMLAN directory and then the ACCOUNTS directory and select the D:\IBMLAN\ACCOUNTS\NETACC.BKP file. Double-click

on the LOGS directory and select the D:\IBMLAN\LOGS\NETAUD.BKP file.

4. Select the **List Selections** button.

   The Selected Files for Restore window is displayed (not shown), showing both the NETACC.BKP and NETAUD.BKP files selected.

5. Select the **OK** button.

   The Restore by Directory Tree window is displayed (not shown).

6. Click on **Restore**.

   The Restore Parameters window appears, as shown in Figure 31.

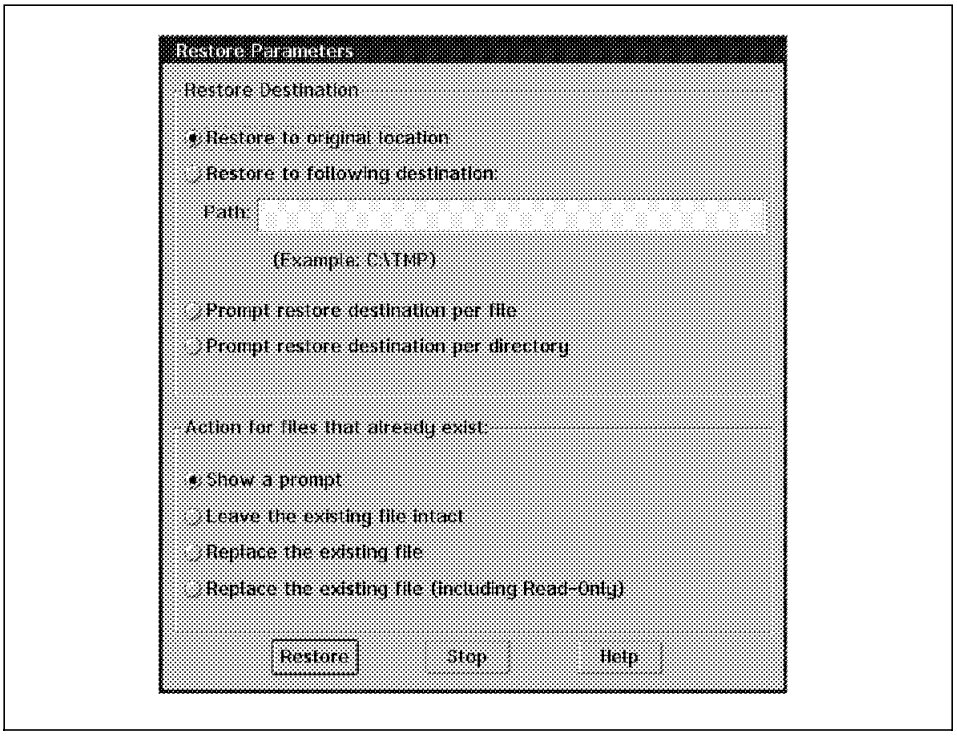


Figure 31. Restore Parameters Window

7. Select the **Restore to original location** radio button and click on **Restore**. When the restore completes, a completion window appears (not shown).

8. Click on **OK**.

   The Restore Status window appears (not shown). Click on **OK** The Restore by Directory Tree window is displayed (not shown).

9. Click on **Cancel**.

The Drive Information window is displayed (not shown).

2.2.2.3 NET.ACC

We assume that the NET.ACC file has been corrupted and neither the CHKDSK nor FIXACC utility can fix it. The ADSM backup of the NETACC.BKP file has been restored and is now used to replace the corrupted NET.ACC. (For information about the other NET.ACC recovery options refer to 1.6.4.5, “NET.ACC” on page 33.)

Here are the steps to recover the NET.ACC file:

1. Stop the server.

   Issue at a command prompt: NET STOP Server

2. Stop the requester.

   Issue at a command prompt: NET STOP Requester

3. Disable the server from automatically starting at system startup.

   Issue at a command prompt:

   RENAME STARTUP.CMD STARTUP.OLD

4. Disable any other programs that may use the NET.ACC file from automatically starting at system startup.

   Be aware that programs can be automatically started at system startup if you are using the STARTUP.CMD file, the startup folder, or the SET AUTOSTART parameter or RUN statement in the CONFIG.SYS file.

   Note

   Other programs, such as Database Manager for OS/2, also use the NET.ACC file. The NET.ACC file cannot be restored while any of these programs are active.

   An alternative method to steps 1 - 4 is to boot from diskette.

5. Shut down the system by selecting Shut down from the OS/2 LaunchPad.

6. Restart the system by pressing the CTRL, ALT, and Delete keys simultaneously.

7. Replace the NET.ACC file with the NETACC.BKP file.

   Issue at a command prompt:

   COPY NETACC.BKP NET.ACC

   You can do a direct copy as both files reside in the D:\IBMLAN\ACCOUNTS directory.

Perform the same process to recover the NET.AUD file; copy the NETAUD.BKP file over the NET.AUD file. NETAUD.BKP and NET.AUD both reside in the D:\IBMLAN\LOGS directory.

8. Reenable the server to automatically start at system startup.

   Issue at a command prompt:

   RENAME STARTUP.OLD STARTUP.CMD

9. Reenable any other programs that may use the NET.ACC file so that they automatically start at system startup.
10. Shut down the system by selecting Shut down from the OS/2 LaunchPad.
11. Restart the system by pressing the CTRL, ALT, and Delete keys simultaneously.

2.3 LAN Server Advanced Operational Data

This scenario describes the backup and recovery of operational data (shared data) that resides on a LAN Server Advanced domain controller. The data area uses 386 HPFS; therefore the shared data ACPs are kept with each file or directory. Files are restored with the correct ACPs provided that the ACPs have been backed up.

Note

For maximum recoverability we recommend that you back up the NET.ACC at the same time that you back up the shared data area.

In this scenario we back up the D:\RESOURCES\SHAREDDATA shared data area. We assume that the NET.ACC, NETACC.BKP, NETAUD.BKP, and SD140196.ACL files in the SHAREDDATA directory have been corrupted. These files must be restored from backup, the NET.ACC replaced, and the ACPs resurrected.

For information about the NET.ACC, NETACC.BKP, NETAUD.BKP, and SD140196.ACL files refer to 1.5.1, “System Data” on page 18 and 1.6, “LAN Server Backup and Recovery” on page 21.

This scenario is representative of the steps you would take to back up and restore a variety of operational data (such as home directories) when using 386 HPFS.

2.3.1 Backup

Backup of the shared data area is a three-step process where you:

1. Back up the NET.ACC file, using the LAN Server BACKACC utility program
2. Back up the shared data
3. Back up the files produced by the BACKACC utility.

2.3.1.1 NET.ACC and ACP

We recommend that you use BACKACC to back up the NET.ACC file. For more information about the BACKACC utility refer to “BACKACC” on page 24.

Run the BACKACC utility.

At a command prompt type:

```
BACKACC D:\RESOURCES\SHAREDDATA /F:D:\RESOURCES\BACKUP\SD140196.ACL /S /V
```

The BACKACC utility displays the names of the backed up access control files.

BACKACC creates the following files:

- D:\IBMLAN\ACCOUNTS\NETACC.BKP
- D:\IBMLAN\LOGS\NETAUD.BKP
- D:\RESOURCES\BACKUP\SD140196.ACL

2.3.1.2 Shared Data

Next we back up the shared data area, D:\RESOURCES\SHAREDDATA, and all of its descendant subdirectories. Follow steps 1 - 17 in 2.2.1.2, “Shared Data” on page 42.

2.3.1.3 NETACC.BKP, NETAUD.BKP, and ACP

Next we back up the files produced by the BACKACC utility: NETACC.BKP NETAUD.BKP, and SD140196.ACL (the target file we specified on the BACKACC command for the ACP definitions).

1. Follow steps 1 - 7 in 2.2.1.2, “Shared Data” on page 42.
2. On the ADSTAR Distributed Storage Manager window select **Directory tree** from the side menu.

> **Note**
>
> You could back up the files by using the file specification method if you prefer.

The Selective Backup by Directory Tree window is displayed.

3. Double-click on the IBMLAN directory and then the ACCOUNTS directory and select the D:\IBMLAN\ACCOUNTS\NETACC.BKP file. Double-click on the LOGS directory and select the D:\IBMLAN\LOGS\NETAUD.BKP file. Double-click on the RESOURCES directory and then the BACKUP directory and select the D:\RESOURCES\BACKUP\SD140196.ACL file.
4. Select the **Backup** button.

   The Mount Wait window may be displayed (not shown).
5. Select the **Wait** button.

   Once the offline media have been loaded and ADSM has completed the backup, the Selective backup completed message box is displayed.
6. Select the **OK** button.

   The Selective Backup by Directory Tree window is displayed.
7. Select the **Cancel** button.

   The Drive Information window is displayed.

2.3.2 Recovery

Recovery of the shared data area and ACPs is a three-step process where you:

1. Recover the shared data
2. Recover the files produced by the BACKACC utility program
3. Replace the NET.ACC file and resurrect the directory and file ACPs

2.3.2.1 Shared Data

First we recover the shared data area, D:\RESOURCES\SHAREDDATA, and all of its descendant subdirectories. Follow steps 1 - 14 in 2.2.2.1, “Shared Data” on page 51.

2.3.2.2 NETACC.BKP, NETAUD.BKP, and ACP

Next we recover the files produced by the BACKACC utility.

1. Follow steps 1 - 7 in 2.2.2.1, “Shared Data” on page 51.
2. On the ADSTAR Distributed Storage Manager window select **Directory tree** from the side menu.

> **Note**
>
> You could restore the files by using the file specification method if you prefer.

The Restore by Directory Tree window is displayed (not shown).

3. Double-click on the IBMLAN directory and then the ACCOUNTS directory and select the D:\IBMLAN\ACCOUNTS\NETACC.BKP file. Double-click on the LOGS directory and select the D:\IBMLAN\LOGS\NETAUD.BKP file. Double-click on the RESOURCES directory and then the BACKUP directory and select the D:\RESOURCES\BACKUP\SD140196.ACL file.
4. Follow steps 4 - 9 in 2.2.2.2, “NETACC.BKP and NETAUD.BKP” on page 55.

2.3.2.3 NET.ACC Replacement and ACP Resurrection

We assume that the NET.ACC file has been corrupted and neither the CHKDSK nor FIXACC utility can fix it. The ADSM backup of the NETACC.BKP file has been restored and is used to replace the corrupted NET.ACC file.

For information about the other NET.ACC recovery options refer to 1.6.4.5, “NET.ACC” on page 33.

The SD140196.ACL file and the RESTACC utility are used to resurrect the shared data ACPs.

Here are the steps to replace the NET.ACC file and resurrect the ACPs:

1. Stop the server.

   Issue at a command prompt: NET STOP Server
2. Stop the requester.

   Issue at a command prompt: NET STOP Requester
3. Disable the server from automatically starting at system startup.

   Issue at a command prompt:

   RENAME STARTUP.CMD STARTUP.OLD
4. Disable any other programs that may use the NET.ACC file from automatically starting at system startup.

   To automatically start programs at system startup use the STARTUP.CMD file, the startup folder, or the SET AUTOSTART parameter or RUN statement in the CONFIG.SYS file.

Note

Other programs, such as Database Manager for OS/2, also use the NET.ACC file. The NET.ACC file cannot be restored while any of these programs are active.

An alternative method to steps 1 - 4 is to boot from diskette.

5. Shut down the system by selecting Shut down from the OS/2 LaunchPad.
6. Restart the system by pressing the CTRL, ALT, and Delete keys simultaneously.
7. Replace the NET.ACC file with the NETACC.BKP file.

   Issue at a command prompt:

   COPY NETACC.BKP NET.ACC

   You can do a direct copy as both files reside in the D:\IBMLAN\ACCOUNTS directory.

   Perform the same process to recover the NET.AUD file; copy the NETAUD.BKP file over the NET.AUD file. The NETAUD.BKP and NET.AUD files both reside in the D:\IBMLAN\LOGS directory.
8. Resurrect the shared data ACPs, using the RESTACC utility.

   At a command prompt type:

   RESTACC D:\RESOURCES\SHAREDDATA F:D:\RESOURCES\BACKUP\SD140196.ACL /V

   RESTACC displays a command completed successfully message.

   RESTACC resurrects the ACPs for the D:\RESOURCES\SHAREDDATA area directory, files, and its descendant subdirectories.
9. Reenable the server so that it automatically starts at system startup.

   Issue at a command prompt:

   RENAME STARTUP.OLD STARTUP.CMD
10. Reenable any other programs that may use the NET.ACC file so that they automatically start at system startup.
11. Shut down the system by selecting Shut down from the OS/2 LaunchPad.
12. Restart the system by pressing the CTRL, ALT, and Delete keys simultaneously.

2.4 LAN Server Advanced Directory Size Limits

This scenario describes the backup and recovery of a LAN Server Advanced directory that has a 20 MB directory size limit, a 90% alert threshold, and a 1% incremental threshold. The directory is restored with the correct directory size limits provided that both the directory and its size limits have been backed up correctly.

ADSM does not currently support the backup of directory size limits. Therefore, two sample applications (BACKDLIM and RESTDLIM) have been created to assist in the backup and recovery of this information. The applications are written in C and use the LAN Server APIs. (Many thanks to Wim Fabri, IBM Belgium, for creating and sharing these applications!)

The BACKDLIM and RESTDLIM code is included in A.5, “LAN Server Directory Size Limits Backup and Restore” on page 157, and on the diskette in the back of this book.

In this scenario the directory to be recovered is D:\RESOURCES\SHAREDDATA\CYNDIE.

2.4.1 Backup

Back up of the directory and its directory size limits is a three-step process where you:

1. Back up the directory size limits using the BACKDLIM utility program
2. Back up the directory
3. Back up the output file produced by the BACKDLIM utility

2.4.1.1 Directory Size Limits

First we back up the directory size limits and put the results in the LIMITS.BKP file.

Run the BACKDLIM utility. At a command prompt type:

```
BACKDLIM D:\RESOURCES\BACKUP\LIMITS.BKP D:\
```

The BACKDLIM utility copies the LAN Server directory size limits to a file. This process creates D:\RESOURCES\BACKUP\LIMITS.BKP.

The directory size information for the CYNDIE directory, as captured in the LIMITS.BKP file, is:

```
"D:\resources\shareddata\CYNDIE" 20480 90 1
```

2.4.1.2 Directory

Next we back up the directory, D:\RESOURCES\SHAREDDATA\CYNDIE, and all of its descendant subdirectories:

1. Follow steps 1 - 8 in 2.2.1.2, “Shared Data” on page 42.
2. In the Backup by File Specification window (Figure 18), enter D:\RESOURCES\SHAREDDATA\CYNDIE* in the **Enter file specification** field.

   Note

   This backup method does not capture empty subdirectories. At least one incremental backup is required to capture empty subdirectories.

3. Follow steps 10 - 17 in 2.2.1.2, “Shared Data” on page 42.

2.4.1.3 LIMITS.BKP

Next we back up the file produced by the BACKDLIM utility: LIMITS.BKP.

1. Follow steps 1 - 7 in 2.2.1.2, “Shared Data” on page 42.
2. On the ADSTAR Distributed Storage Manager window (Figure 17), select **Directory tree** from the side menu.

   Note

   You could back up the files by using the file specification method if you prefer.

   The Selective Backup by Directory Tree window is displayed (not shown).
3. Double-click on the RESOURCES directory and then the BACKUP directory and select the D:\RESOURCES\BACKUP\LIMITS.BKP file.
4. Select the **Backup** button.

   The Mount Wait window may be displayed (not shown).
5. Select the **Wait** button.

   Once the offline media have been loaded and ADSM has completed the backup, the Selective backup completed message box is displayed (not shown).
6. Select the **OK** button.

   The Selective Backup by Directory Tree window is displayed (not shown).
7. Select the **Cancel** button.

The Drive Information window is displayed (not shown).

2.4.2 Recovery

Recovery of the directory and its size limits is a three-step process where you:

1. Recover the directory
2. Recover the output file produced by the BACKDLIM utility: LIMITS.BKP
3. Resurrect the directory size limits

2.4.2.1 Directory

First we recover the directory, D:\RESOURCES\SHAREDDATA\CYNDIE, and all of its descendant subdirectories:

1. Follow steps 1 - 8 in 2.2.2.1, “Shared Data” on page 51.
2. Recover the directory, subdirectories, and files to their original location. On the Restore Subdirectory Path window (Figure 28):
   a. Enter \RESOURCES\SHAREDDATA\CYNDIE in the **Enter source path to fully restore** field.
   b. Enter D:\RESOURCES\SHAREDDATA\CYNDIE in the **Enter destination path to fully restore to** field.
   c. Select the **Show a prompt** radio button from the **Action for files that already exist** options.
3. Follow steps 10 - 14 described in 2.2.2.1, “Shared Data” on page 51.

2.4.2.2 LIMITS.BKP

Next we recover the output file produced by the BACKDLIM program: LIMITS.BKP

1. Follow steps 1 - 7 in 2.2.2.1, “Shared Data” on page 51.
2. On the ADSTAR Distributed Storage Manager window (Figure 17), select **Directory tree** from the side menu.

   Note

   You could restore the files by using the file specification method if you prefer.

   The Restore by Directory Tree window is displayed.
3. Double-click on the RESOURCES directory and then the BACKUP directory and select the D:\RESOURCES\BACKUP\LIMITS.BKP file.

4. Follow steps 4 - 9 in 2.2.2.2, “NETACC.BKP and NETAUD.BKP” on page 55.

2.4.2.3 Directory Size Limit Resurrection

Use the LIMITS.BKP file and the RESDLIM program to resurrect the directory size limits.

> **Note**
>
> RESTDLIM adds directory size limits only to directories that do not have any current limits associated with them, for example, a directory that has been deleted and is then restored from an ADSM backup. RESTDLIM does not work if you have restored the directory over the existing directory.

Resurrect the directory size limits, using the RESTDLIM utility. Issue at a command prompt:

```
RESTDLIM D:\RESOURCES\LIMITS.BKP
```

The directory size limits for D:\RESOURCES\SHAREDDATA\CYNDIE are restored.

> **Note**
>
> You do not have to stop the server to run the RESTDLIM utility.

2.5 LAN Server Entry Domain Control Database

This scenario describes the backup and recovery of a LAN Server Entry DCDB. The DCDB is comprised of files and directories that reside in the \IBMLAN\DCDB directory on the domain controller. The files and directories have ACPs associated with them. Files are restored with the correct ACPs provided that the NET.ACC file is available and not damaged.

> **Note**
>
> For maximum recoverability we recommend that you back up the NET.ACC file at the same time that you back up the DCDB.

In this scenario the DCDB is located in the D:\IBMLAN\DCDB directory. We assume that the DCDB files are corrupted, but the NET.ACC files and ACPs are intact.

Note

If you are backing up and recovering the DCDB of a LAN Server Advanced server running 386 HPFS, follow the same backup and restore procedures as in this scenario, but additionally use the BACKACC utility to capture the ACPs and the RESTACC utility to restore the DCDB ACPs to the file system.

This DCDB recovery scenario also assumes that only one primary domain controller exists, with no backup domain controller, and that LAN Server DCDB replication is not used. LAN Server DCDB supports replication of the database to a backup domain controller. If the primary domain controller fails, LAN Server automatically switches to a backup domain controller.

2.5.1 Backup

Backup of the DCDB is a three-step process where you:

1. Back up the NET.ACC file, using the LAN Server BACKACC utility program
2. Back up the DCDB
3. Back up the files produced by the BACKACC utility

2.5.1.1 NET.ACC

We recommend using the BACKACC utility to back up the NET.ACC file. For more information about BACKACC refer to “BACKACC” on page 24.

Run the BACKACC utility. At a command prompt type:

```
BACKACC /V
```

The BACKACC utility displays the backed up access control file names.

BACKACC creates the following files:

- D:\IBMLAN\ACCOUNTS\NETACC.BKP
- D:\IBMLAN\LOGS\NETAUD.BKP

2.5.1.2 DCDB Area

Next we back up the DCDB area, \IBMLAN\DCDB, and all of its descendant subdirectories:

Note

The ADSM incremental backup method is used to ensure that the backup captures both the full and empty DCDB subdirectories.

1. Follow steps 1 - 7 in 2.2.1.2, “Shared Data” on page 42.
2. On the ADSTAR Distributed Storage Manager window (Figure 17), select **Incremental** from the side menu.

   The Mount Wait window may be displayed.
3. Follow steps 14 - 17 in 2.2.1.2, “Shared Data” on page 42.

2.5.1.3 NETACC.BKP and NETAUD.BKP

Next we back up the files produced by the BACKACC utility: NETACC.BKP and NETAUD.BKP.

1. Follow steps 1 - 7 in 2.2.1.2, “Shared Data” on page 42.
2. On the ADSTAR Distributed Storage Manager window (Figure 17), select **Directory tree** from the side menu.

   Note

   You could back up the files by using the file specification method if you prefer.

   The Selective Backup by Directory Tree window is displayed (not shown).
3. Double-click on the IBMLAN directory and then the ACCOUNTS directory and select the D:\IBMLAN\ACCOUNTS\NETACC.BKP file. Double-click on the LOGS directory and select the D:\IBMLAN\LOGS\NETAUD.BKP file.
4. Select the **Backup** button.

   The Mount Wait window may be displayed (not shown).
5. Select the **Wait** button.

   Once the offline media have been loaded and ADSM has completed the backup, the Selective backup completed message box is displayed (not shown).
6. Select the **OK** button.

   The Selective Backup by Directory Tree window is displayed (not shown).
7. Select the **Cancel** button.

The Drive Information window is displayed (not shown).

2.5.2 Recovery

Recovery of the DCDB is simple because the NET.ACC file and ACPs are not corrupted.

If you suspect a corrupted NET.ACC file, follow the processes outlined in 2.2.2.2, “NETACC.BKP and NETAUD.BKP” on page 55, and 2.2.2.3, “NET.ACC” on page 57.

Here are the steps to recover the DCDB:

1. Stop the server.

   Issue at a command prompt: NET STOP Server

2. Stop the requester.

   Issue at a command prompt: NET STOP Requester

3. Disable the server from automatically starting at system startup.

   Issue at a command prompt:

   RENAME STARTUP.CMD STARTUP.OLD

4. Disable any other programs that may use the NET.ACC file from automatically starting at system startup.

   Note

   Other programs, such as Database Manager for OS/2, also use the NET.ACC file. The NET.ACC file cannot be restored while any of these programs are active.

   An alternative method to steps 1 - 4 is to boot from diskette.

5. Shut down the system by selecting Shut down from the OS/2 LaunchPad.

6. Restart the system by pressing the CTRL, ALT, and Delete keys simultaneously.

7. Recover the DCDB, D:\IBMLAN\DCDB, and all of its descendant subdirectories, including all empty subdirectories.

   Follow steps 1 - 8 in 2.2.2.1, “Shared Data” on page 51.

8. Recover the DCDB files and subdirectories to their original location:

   a. Enter \IBMLAN\DCDB in the **Enter source path to fully restore** field.

   b. Enter D:\IBMLAN\DCDB in the **Enter destination path to fully restore to** field.

c. Select the **Show a prompt** radio button from the **Action for files that already exist** options.

9. Follow steps 10 - 14 in 2.2.2.1, “Shared Data” on page 51.
10. Reenable the server so that it automatically starts at system startup.

    Issue at a command prompt:

    RENAME STARTUP.OLD STARTUP.CMD
11. Reenable any other programs that may use the NET.ACC file so that they automatically start at system startup.
12. Shut down the system by selecting Shut down from the OS/2 LaunchPad.
13. Restart the system by pressing the CTRL, ALT, and Delete keys simultaneously.

2.6 LAN Server Entry Entire Partition

This scenario describes the backup and recovery of a LAN Server Entry disk partition that contains LAN Server system and operational data.

In this scenario, OS/2, MPTS/2, and the ADSM client are located on the C drive, whereas LAN Server and the LAN resources are located on the D drive. A hard disk failure resulted in the loss of all of the data on the D drive.

Note

If you are backing up and recovering the D drive of a LAN Server Advanced server running 386 HPFS, follow the same backup and restore procedures described in this scenario, but additionally use the BACKACC utility to capture the ACPs and the RESTACC utility to restore the D drive ACPs to the file system.

2.6.1 Backup

Backup of the D drive is a two-step process where you:

1. Back up the NET.ACC file, using the LAN Server BACKACC utility program
2. Back up the D drive files and directories

2.6.1.1 NET.ACC

We recommend using BACKACC to back up the NET.ACC file. For more information about the BACKACC utility refer to “BACKACC” on page 24.

Run the BACKACC utility. At a command prompt type:

BACKACC /V

The BACKACC utility displays the backed up access control file names.

BACKACC creates the following files:

- D:\IBMLAN\ACCOUNTS\NETACC.BKP
- D:\IBMLAN\LOGS\NETAUD.BKP

2.6.1.2 D Drive

Next we back up the D drive and all of its descendant subdirectories:

1. Follow steps 1 - 8 in 2.2.1.2, “Shared Data” on page 42.
2. On the Backup by File Specification window (Figure 18), enter D:* in the **Enter file specification** field.

   An incremental backup may be easier than a GUI backup by file specification.

   If your D drive is very large or has many directories and files, you may encounter an ADSM error indicating that the buffer is full because the ADSM GUI reserves 64 KB for this data. In this situation, use the ADSM CLI because it uses memory to process and display the data.
3. Follow steps 10 - 17 in 2.2.1.2, “Shared Data” on page 42.

Note

You do not have to separately back up the NETACC.BKP, NETAUD.BKP, and DDRIVE140196.ACL files because they are backed up as part of the D drive backup.

2.6.2 Recovery

Recovery of the D drive is a three-step process where you:

1. Replace and configure the hardware
2. Recover the D drive files and subdirectories
3. Recover the NET.ACC file

2.6.2.1 Replace and Configure Hardware

First we replace the disk that failed and make it available to the system:

1. Disable the server from automatically starting at system startup.

   Issue at a command prompt:

RENAME STARTUP.CMD STARTUP.OLD

2. Disable any other programs that may use the NET.ACC file from automatically starting at system startup.

> **Note**
>
> Other programs, such as Database Manager for OS/2, also use the NET.ACC file. The NET.ACC file cannot be restored while any of these programs are active.
>
> An alternative method to steps 1 - 4 is to boot from diskette.

3. Shut down the system by selecting Shut down from the OS/2 LaunchPad.
4. Restart the system by pressing the CTRL, ALT, and Delete keys simultaneously.
5. Replace the faulty hard drive.
6. Power on the system.
7. Create a new logical partition on the new hard drive, using OS/2 utility FDISKPM.
8. Shut down the system by selecting Shut down from the OS/2 LaunchPad.
9. Restart the system by pressing the CTRL, ALT, and Delete keys simultaneously.
10. Format the new partition with HPFS, using the OS/2 FORMAT command.

    Issue at a command prompt:

    FORMAT D: /FS:HPFS

    Label the volume with the same name as that of the failed disk.

2.6.2.2 D Drive

Next we recover the D drive and all of its descendant subdirectories:

1. Follow steps 1 - 8 in 2.2.2.1, “Shared Data” on page 51.
2. Recover the D drive files and subdirectories to their original location. On the Restore Subdirectory Path window (Figure 28):
   a. Enter \ in the **Enter source path to fully restore** field.
   b. Enter D:\ in the **Enter destination path to fully restore to** field.
   c. Select the **Show a prompt** radio button from the **Action for files that already exist** options.
3. Follow steps 10 - 14 in 2.2.2.1, “Shared Data” on page 51.

2.6.2.3 NET.ACC

Next we replace the NET.ACC file, using the ADSM backup of the NETACC.BKP file:

1. Replace the NET.ACC file with the NETACC.BKP file.

   Issue at a command prompt:

   COPY NETACC.BKP NET.ACC

   You can do a direct copy, as both files reside in the D:\IBMLAN\ACCOUNTS directory.

2. Reenable the sever so that it automatically starts at system startup.

   At a command prompt issue:

   RENAME STARTUP.OLD STARTUP.CMD

3. Reenable any other programs that may use the NET.ACC file to automatically start at system startup.

4. Shut down the system by selecting Shut down from the OS/2 LaunchPad.

5. Restart the system by pressing the CTRL, ALT, and Delete keys simultaneously.

2.7 Automatic Backup of OS/2 LAN Server V4.0 and Operational Data

In this section we describe how to set up ADSM for automatic backup of OS/2 LAN Server V4.0 and the operational or user data. We assume that the ADSM for OS/2 server and client software is installed with the appropriate storage pools, communication methods, and policies. Although we used an ADSM for OS/2 server in our test environment, you can use any ADSM server platform.

For more details and examples of REXX command scripts, see *The IBM OS/2 LAN Server Version 3.0 System Recovery Considerations* (GG24-4043).

2.7.1 ADSM Client Setup

To automate ADSM backup of a LAN Server client, you must select and customize one of the three sample scripts described below. You then must update the ADSM client options file, DSM.OPT.

2.7.1.1 REXX Command Scripts

Sample REXX command scripts were written to back up OS/2 LAN Server's NET.ACC with the BACKACC command and directory size limits with the BACKDLIM program. BACKACC is an OS/2 LAN Server utility, and BACKDLIM is a C program executable written by Wim Fabri from IBM Belgium.

Our sample REXX command scripts check for successful execution of the BACKACC and BACKDLIM commands. If successful, an ADSM INCREMENTAL command is executed to add the drive partition where OS/2 LAN Server is installed to the domain of drives for ADSM incremental backup. If not successful, a failure message is sent to the LAN administrator's workstation asking him or her to review the BACKACC.LOG and BACKDLIM.LOG log files. If not successful, the drive partition where OS/2 LAN Server is installed is not added for ADSM incremental backup. Not adding the drive partition prevents ADSM from creating backups of OS/2 LAN Server that are incomplete or in error.

Below are the sample REXX command scripts. Choose a script that closely matches your OS/2 LAN Server environment. Review the comments in the REXX command script you choose and make the necessary updates.

- LANSRVE.CMD is for use with LAN Server Entry. The backups produced could be used for the recovery steps described in 2.2, "LAN Server Entry Operational Data" on page 41, 2.5, "LAN Server Entry Domain Control Database" on page 66, and 2.6, "LAN Server Entry Entire Partition" on page 70.
- LANSRVA.CMD is for use with LAN Server Advanced and 386 HPFS drive partitions. The backups produced could be used for the recovery steps described in 2.3, "LAN Server Advanced Operational Data" on page 58.
- LANSRVAL.CMD is for use with LAN Server Advanced and 386 HPFS drive partitions and directory size limits. The backups produced could be used for the recovery steps described in 2.4, "LAN Server Advanced Directory Size Limits" on page 63.

  The REXX command scripts are shown in A.5, "LAN Server Directory Size Limits Backup and Restore" on page 157. They are also included on the diskette in the back of this book.

2.7.1.2 DSM.OPT Updates

The DSM.OPT file must be updated to invoke the REXX command script and set up some backup options. The DSM.OPT updates you must make are:

- Make sure there is a NODENAME option to identify your ADSM client workstation to the ADSM server.
- Add a DOMAIN option to specify the drives to include for incremental backup. Do not add the drive where LAN Server is installed. The REXX command script adds the LAN Server drive for incremental backup if the BACKACC and BACKDLIM commands are successful.

- If using an ADSM V1 server and its central scheduler (and an ADSM for OS/2 V2 client), add a PRESCHEDULECMD option to execute the REXX command script before ADSM executes the scheduled ADSM action. The REXX command script is executed to do the LAN Server backups and, if successful, adds the LAN Server drive for ADSM incremental backup. However, a second incremental backup of the operational data drives is performed if you set up the ADSM scheduler action as incremental. This second backup is performed because both our REXX script and the ADSM scheduler are set up to execute an ADSM incremental backup command. To avoid a second ADSM incremental backup, define a no-op ADSM scheduled action such as ARCHIVE and an OBJECTS option of a nonexistent file.

  With an ADSM V2 server, you can define a scheduled action of COMMAND to run the REXX command script. You cannot use this new V2 COMMAND option with V1 servers. Therefore, with V1 servers the only way to simulate scheduling a command is to use the PRESCHEDULECMD option as described above.

  Alternatively, other schedulers, such as the OS/2 LAN Server AT command or SystemView′s Event Scheduler, could be used to execute the REXX command scripts. The PRESCHEDULECMD option would not be added to DSM.OPT if one of these alternative scheduling choices is used. The PRESCHEDULECMD option is required only with the ADSM V1 server example when you choose to use the ADSM central scheduling facility.

  Optionally add INCLUDE and EXCLUDE statements for OS/2 LAN Server. The default ADSM policy has a STANDARD management class with a copy group of two backup versions. We defined another management class, SYSTEM, with more backup versions and longer retention periods. We added INCLUDE statements to assign certain OS/2 LAN Server files and directories to this SYSTEM management class.

  We added an EXCLUDE statement for the NET.ACC file because we did not want to directly back up the NET.ACC file. The REXX command script uses the BACKACC command with ADSM to back up the NET.ACC file. It is possible to back up the NET.ACC file directly with ADSM if the management class copy group serialization is dynamic. ADSM would back up the file while it is open, and potentially being updated by OS/2 LAN Server. Therefore, our automatic backup scripts use the recommended method of BACKACC in conjunction with ADSM.

Here is part of the DSM.OPT file used in our environment:

```
*  Setting the nodename.
*  --------------------------------------------------------
   NODENAME PUGET

*  Drives to be included for incremental backup.
*  Drive D where OS/2 LAN Server is installed is backed up
*  with the DSMC INCREMENTAL -DOMAIN="D:" command within the
*  REXX script executed with the PRESCHEDULECMD option.
*  --------------------------------------------------------
   DOMAIN E:

*
*  INCLUDE and EXCLUDE list for OS/2 LAN Server.
*  SYSTEM is a management class defined for system data.  It has
*  more backup versions and longer retention periods defined than the
*  STANDARD management class.  If you would reinstall OS/2 LAN Server
*  in a recover situation, then uncomment the EXCLUDE for
*  D:\IBMLAN\...\*.  The order of search is from the bottom up until
*  a match is found.
*  --------------------------------------------------------
* EXCLUDE  D:\IBMLAN\...\*
   INCLUDE  D:\IBM386FS\HPFS386.INI SYSTEM
   INCLUDE  D:\IBMLAN\IBMLAN.INI SYSTEM
   INCLUDE  D:\IBMLAN\ACCOUNTS\* SYSTEM
   INCLUDE  D:\IBMLAN\DCDB\...\* SYSTEM
   INCLUDE  D:\IBMLAN\LOGS\* SYSTEM
   EXCLUDE  D:\IBMLAN\ACCOUNTS\NET.ACC  * BACKACC is used instead.

*  A command that ADSM should process before running a schedule.
*  --------------------------------------------------------
   PRESCHEDULECMD "D:\ADSMCMDS\LANSRVE.CMD"
```

2.7.2 ADSM Server Setup

You must perform the following ADSM Server actions before using the ADSM automatic backups. You can use either the ADSM administrator GUI or commands. The ADSM commands are fully documented in the *ADSM: Administrator's Reference for OS/2* manual.

- Create a nodename at the ADSM Server, using the ADSM REGISTER NODE command, to match the NODENAME option in the DSM.OPT file on the ADSM client. Ensure that the client node password matches the -PASSWORD= parameter on the DSMC INCREMENTAL command in the REXX command script that will be executed with DSM.OPT file option PRESCHEDULECMD.
- Optionally use the ADSM DEFINE MGMTCLASS command to create a management class, such as SYSTEM, with the extra backup versions

and longer retention periods than the STANDARD management class. This new SYSTEM management class will be used for the OS/2 LAN Server backups. The management class name must match the management class assigned with the INCLUDE statements in the DSM.OPT file on the ADSM client.

- Define an ADSM schedule, using the ADSM DEFINE SCHEDULE command. For ADSM V1 servers, define an ACTION of ARCHIVE and an OBJECTS option of a nonexistent client file. For ADSM V2 servers, define an ACTION of COMMAND.
- Associate the client node with the backup schedule, using the ADSM DEFINE ASSOCIATION command.

2.7.3 Running an ADSM Scheduled Backup

Now you are ready to run scheduled ADSM backup. From an OS/2 window on the ADSM client, type the following command:

```
DSMC SCHEDULE
```

You are be prompted for the ADSM client node password. After responding with a correct password, a message is displayed stating the number of minutes before the scheduled ADSM backup begins. Monitor the ADSM backup to ensure that it completes with no problems.

You could add the DSMC SCHEDULE -PASSWORD= command to the STARTUP.CMD file so that the client scheduler is started at OS/2 bootup. Another alternative is to create a command file with the DSMC SCHEDULE -PASSWORD= command. Then create a program object icon in your ADSM folder or OS/2 desktop to execute this command file. You could then start your ADSM client scheduler by clicking on this icon.

You could use standard output redirection to save additional messages from what usually is logged in the DSMSCHED.LOG file. A single > will overwrite and a double >> will append to the SCHED.LOG file.

```
DSMC SCHEDULE>>C:\ADSM\SCHED.LOG
```

Note: The ADSM for OS/2 V2 client has new DSM.OPT options of PASSWORDACCESS and PASSWORDDIR. If you add PASSWORDACCESS GENERATE to the ADSM client DSM.OPT file, an encrypted password is stored in a file with a PWD extension when you initially reply with the ADSM client's password. When the ADSM server expires the client node's password, a generated password is automatically stored in the encrypted password file. The PASSWORDDIR option is the directory location of this encrypted password file. If you do not want to have passwords in REXX

command files, but you do want to run ADSM incremental backups unattended, you could implement PASSWORDACCESS GENERATE after your initial ADSM scheduled backup test completes successfully.

Another alternative is not to use security at all by using the SET AUTHENTICATION OFF command on the ADSM server.

Chapter 3. OS/2 Warp Server

In this chapter we discuss the backup and recovery services provided for OS/2 Warp Server. OS/2 Warp Server provides a new Warp Server Backup/Restore utility based on Personally Safe “n” Sound (PSnS). As shown in Figure 32 on page 80, there are three alternatives for OS/2 Warp Server backup and restore:

- Warp Server Backup/Restore
- Warp Server Backup/Restore as an ADSM API application with any ADSM server
- ADSM backup/archive client

We compare all three alternatives and discuss for which environments each alternative or combination of alternatives may be most appropriate. We also explain how to convert from one alternative to another.

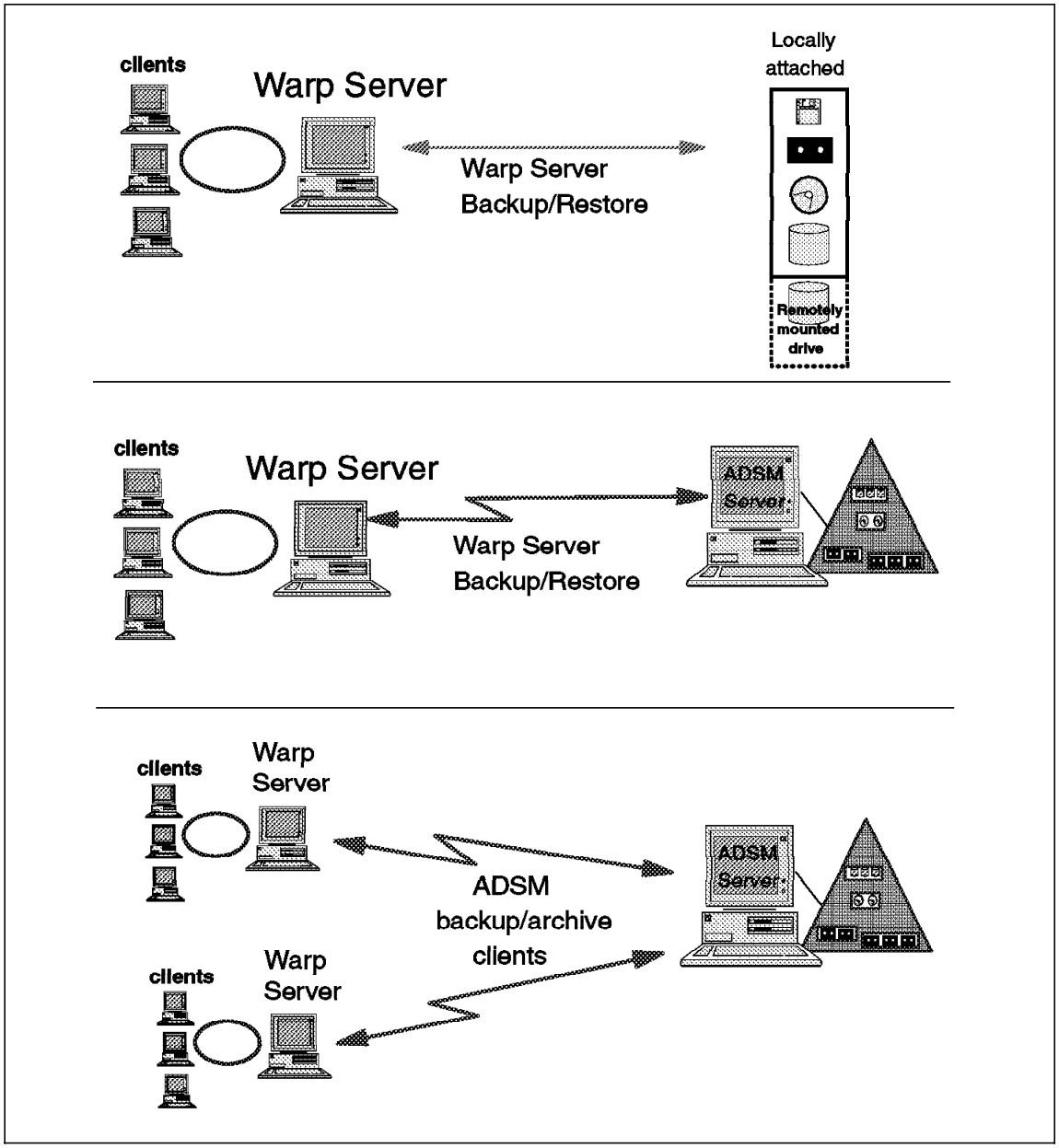


Figure 32. OS/2 Warp Server Backup amd Restore Alternatives

The reference materials used for this chapter include the OS/2 Warp Server online library books entitled “Tell Me About It” and “OS/2 Warp Server Backup/Restore User’s Guide.”

3.1 Overview

OS/2 Warp Server is a business server that addresses a wide variety of environments, from small workgroups, to departmental LANs, to corporate networks. It provides an integrated platform for the application server environment as well as a complete set of traditional file and print services.

OS/2 Warp Server provides a suite of services to uniquely customize your server for your environment. It uses OS/2 Warp for its base services and then allows you to selectively install and customize the services you require, as shown in Figure 33. You can choose to install all services at one time or add or delete services at a later date as the needs of your environment change.

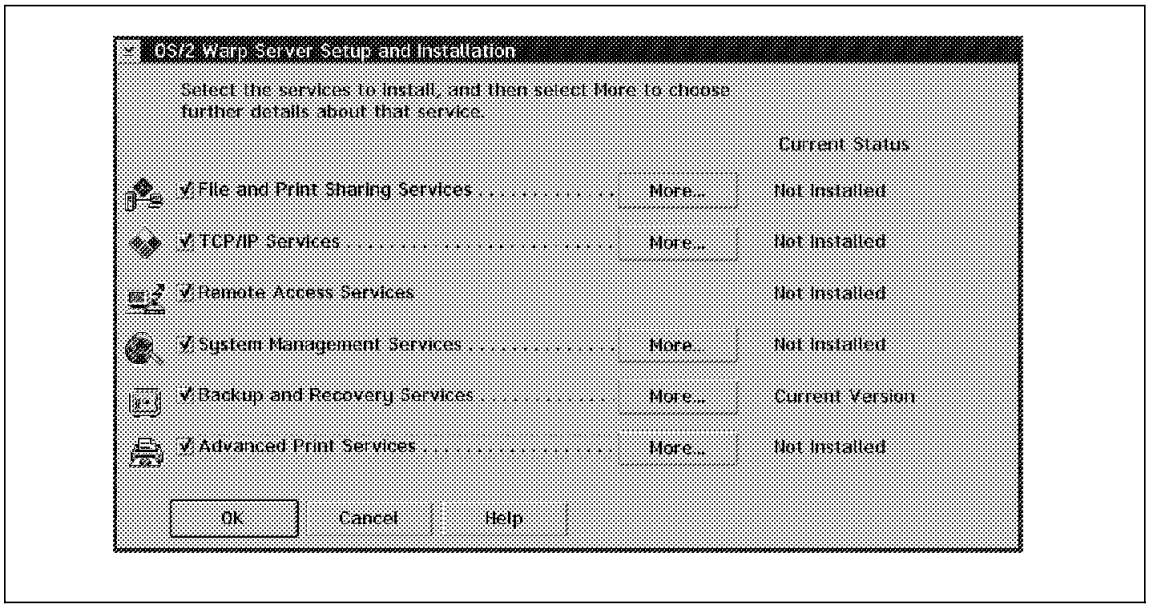


Figure 33. OS/2 Warp Server Optional Services

OS/2 Warp Server provides these services:

- File and print sharing

  OS/2 Warp Server's file and print sharing services are based on IBM LAN Server V5.0, a network operating system for sharing data, applications, printers, and serial devices across a LAN. These services can coexist and interoperate in a LAN environment with previous versions of LAN Server. You can read more about LAN Server in Chapter 1, "LAN Server V4.0" on page 1.

- TCP/IP

OS/2 Warp Server′s TCP/IP services provide TCP/IP communications and popular TCP/IP applications, such as the WebExplorer and NewsReader/2. With TCP/IP services you can establish your own internal internet and/or connect to the global TCP/IP network (Internet) and the World Wide Web (WWW).

- Remote access

  OS/2 Warp Server′s remote access services are based on IBM LAN Distance Connection Server, an application that enables several remote systems to simultaneously dial in to your LAN environment and access LAN resources.

- System management services

  OS/2 Warp Server′s system management services are based on IBM SystemView for OS/2, an application for managing individual systems or groups of managed systems on your LAN. We describe how to use SystemView for OS/2 in *ADSM for OS/2: Advanced Topics* (SG24-4740; in press).

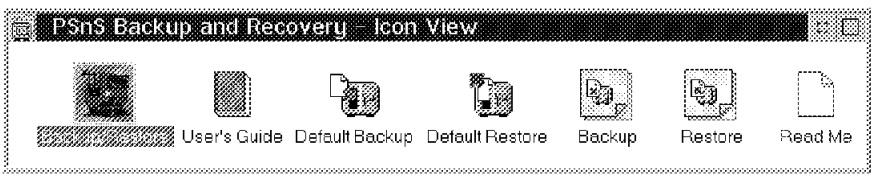
- Backup and recovery

  OS/2 Warp Server′s backup and recovery services are based on IBM′s PSnS, an application that enables you to make backups of your data to safeguard your system against loss of information. You can use OS/2 Warp Server Backup/Restore as an ADSM API application with any ADSM server.

- Advanced print

  OS/2 Warp Server′s advanced print services are based on IBM Print Services Facility/2 for OS/2, an application that supports additional print file and server types and automatically performs data stream transformations to convert the data in your document to the type of data required by the printer you are using.

3.2 Backup and Recovery Services



Your OS/2 Warp Server system comprises many types of information, suc as system data, application data, and user data, all of which are important to the smooth running of your system. OS/2 Warp Server provides features to safeguard your system against the possible loss of this data by enabling you to quickly and easily define and implement multiple backup strategies through a user-friendly GUI (as shown in Figure 34), quick start guides, and hints.

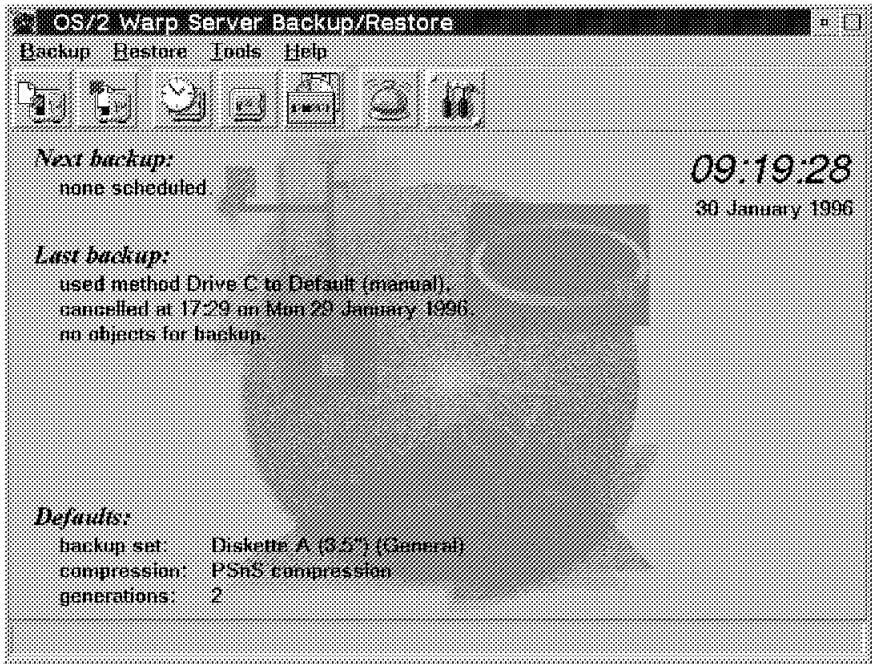


Figure 34. OS/2 Warp Server Backup/Restore Window

Backup strategies are implemented through the definition of backup sets and backup methods, as explained in more detail in 3.2.3, “Backup Strategies” on page 87. Once you have designated how backups are initiated (either manually or scheduled) and where they are stored, OS/2 Warp Server Backup/Restore manages the backup and retrieval for you, thus releasing you from the burden of manually cataloging and organizing your backup media. OS/2 Warp Server Backup/Restore manages the data through the creation of index files that contain such information as the backup set data inventory, data storage location, and number of data versions to be kept. The index files are backed up and kept with your data files (backup set), thus ensuring that your data is recoverable even if a disk drive crashes.

Let us look at OS/2 Warp Server Backup/Restore in more detail, including the backup data types supported, backup storage devices supported, backup and restore strategies, and disaster recovery support. In 3.3, "OS/2 Warp Server Backup/Restore and ADSM" on page 97, we look at how to use OS/2 Warp Server Backup/Restore with ADSM.

3.2.1 Backup Data Types

OS/2 Warp Server data can be distributed across multiple drives and drive types and may have system or security information associated with it. OS/2 Warp Server Backup/Restore provides backup support for:

- Locally attached hard drives
- Remotely attached hard drives
- 386 HPFS formatted drives
- HPFS formatted drives
- FAT formatted drives
- Long file names
- Extended attributes
- ACPs

3.2.2 Backup Storage Devices

OS/2 Warp Server Backup/Restore supports a wide variety of fixed and removable media storage devices, such as:

- Diskette drives

  Diskettes must be formatted with the FAT file system.

- Locally attached hard drives

  Hard drives can be formatted with either the 386 HPFS, HPFS, or FAT file systems.

- LAN alias hard drives

  OS/2 Warp Server Backup/Restore supports any OS/2 Warp Server or LAN Server network drives to which your OS/2 Warp Server system has access. These network drives can be formatted with either the 386 HPFS, HPFS, or FAT file systems.

- Remotely attached hard drives

  Remote drives are supported only if they are made available to the OS/2 Warp Server system through a logical drive letter and are compatible with the FAT file system.

- Tape drives

OS/2 Warp Server Backup/Restore supports a wide variety of SCSI II tape drives. Refer to B.1, “OS/2 Warp Server Device Support” on page 163 for a list of currently supported devices.

- Optical drives

  OS/2 Warp Server Backup/Restore supports any read/write optical drive supported by OS/2 Warp Server. Optical disks can be formatted with either the 386 HPFS, HPFS, or FAT file systems.

- ADSM media

  OS/2 Warp Server Backup/Restore recognizes ADSM as a backup and restore facility that provides access to storage devices. OS/2 Warp Server Backup/Restore regards ADSM as a unique type of storage device that enables you to access all ADSM devices. It treats the ADSM device as a single, fixed volume that is accessed through a communications link. The ADSM server actually stores data in a hierarchy of one or more physical storage volumes, as defined by the ADSM administrator. ADSM assumes responsibility for managing and protecting the backup data associated with the OS/2 Warp Server Backup/Restore ADSM storage device.

OS/2 Warp Server Backup/Restore refers to the media associated with removable media storage devices as *volumes*. It provides facilities to name the volume and query the backup sets, control files, and free space on the volume.

3.2.2.1 Backup Storage Device Configuration

When OS/2 Warp Server Backup/Restore is installed, it automatically scans your system for suitable storage devices and, if possible, configures them as shown in Figure 35 on page 86.

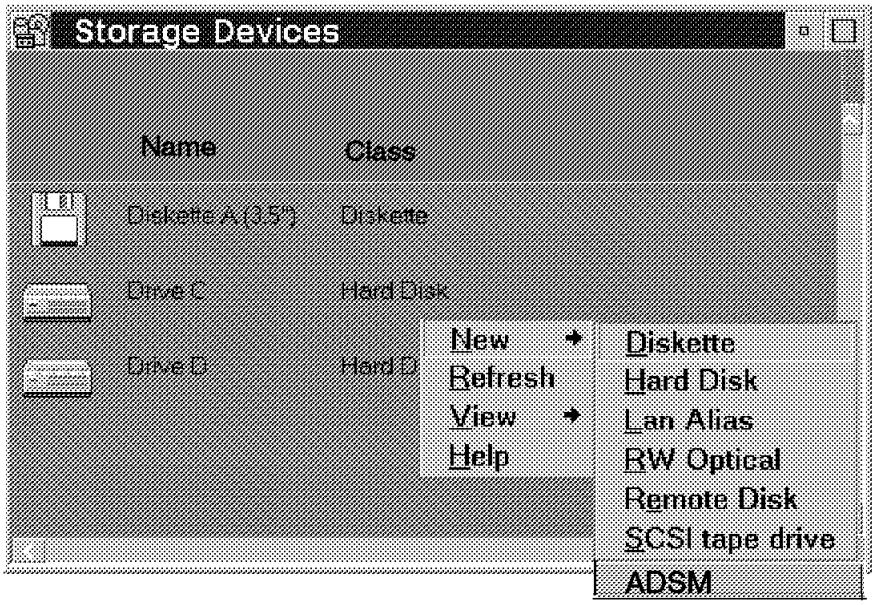


Figure 35. Storage Devices Window

Alternatively, you can manually configure the storage device settings. The settings information required differs among storage devices but may include the:

- Drive letter

  The drive letter is the physical drive letter for locally attached hard drives and the logical drive letter for LAN or remotely attached hard drives.

- Parent directory for all backup paths

  The parent directory is the main directory that backup sets access to create their own subdirectories and subsequently use to store backup data.

- Server name

  The server name is the name of the OS/2 Warp or LAN Server system to which the remote hard drive is attached.

- Alias

  Alias is the name of the OS/2 Warp or LAN Server alias that points to the remote hard drive.

- Drive letter for index files

  The drive letter for index files is the drive letter that an optical storage device can use for backup of index files. You can back up index files to diskettes, rather than using a separate optical disk.

- Adapter

  The adapter is the SCSI adapter number to which your SCSI tape device is connected.

- Unit number

  The unit number is the SCSI number of your tape device.

3.2.3 Backup Strategies

When setting up your OS/2 Warp Server system, analyze the types of data that it encompasses and the impact on users if the data is not available. You can determine the importance of your data and group it into different backup and restore priorities. You may find that you require multiple backup strategies to address unique data requirements. For example, application development data may change frequently and require backup more often than the end-of-month reports. OS/2 Warp Server Backup/Restore implements backup strategies through the definition of backup sets and backup methods, as shown in Figure 36 on page 88.

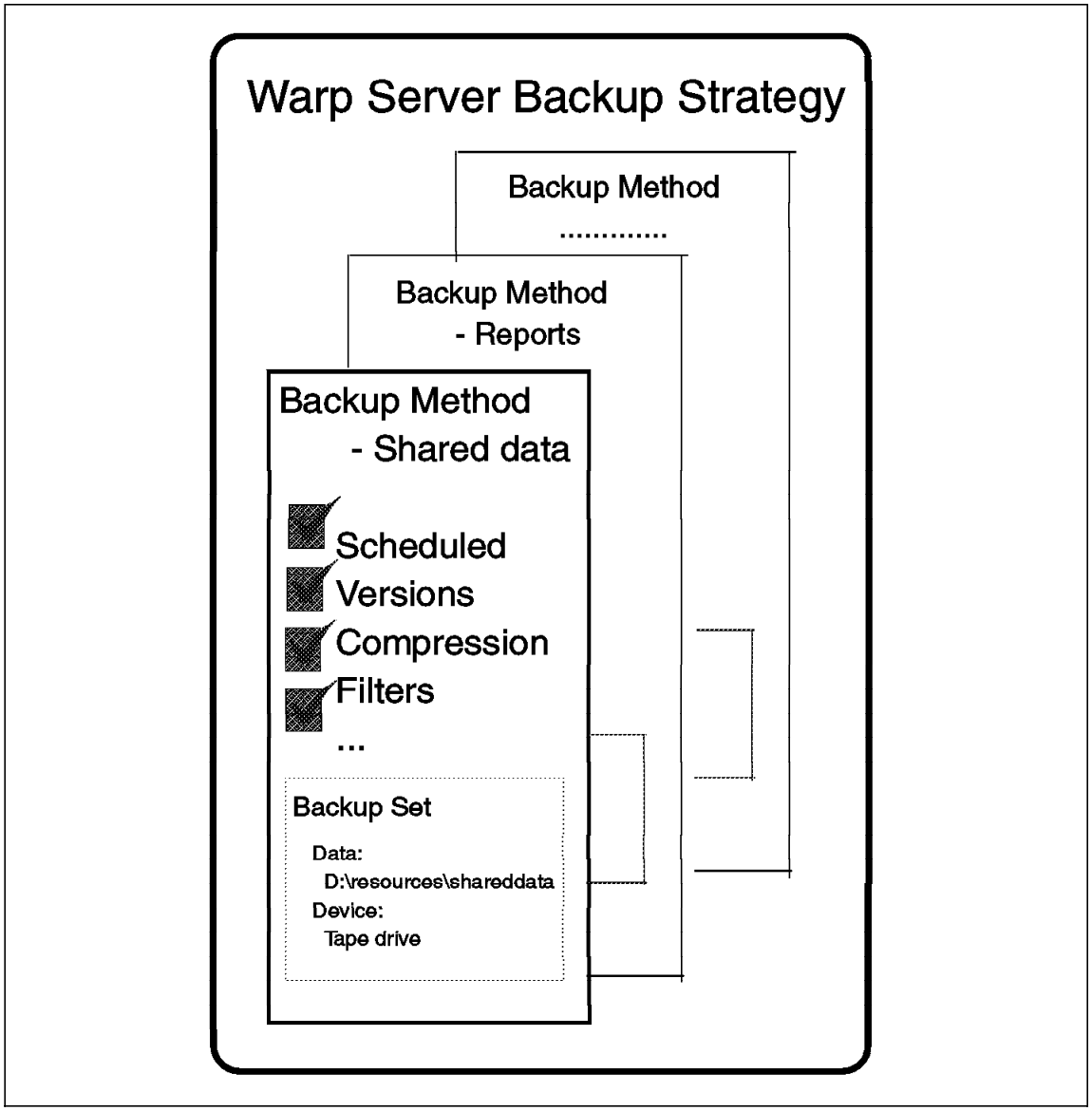


Figure 36. OS/2 Warp Server Backup Strategy

3.2.3.1 Backup Set Definition

A backup set is a logical collection of files that are backed up to a specific storage device. When you define a new backup set you must specify a unique backup set name, the storage device on which to store the data, and the settings to be used for the storage device. The settings information required differs among storage devices but may include:

- Whether you want to verify backups

  OS/2 Warp Server Backup/Restore can be set up to verify that the data actually written to the storage device is correct. Although verification provides backup confirmation, it affects the backup time for your data.

- Whether you want to back up index files

  OS/2 Warp Server Backup/Restore can be set up to automatically back up the backup set index files with the data.

- Whether you want the storage device to ask for media

  This option is available only for removable volume storage devices such as diskette, optical, and tape devices. If your system is set up for multimedia, that is, you have a sound card, PSnS will say, “Please insert a diskette”; if you do not have a sound card you will just hear a bleep.

- The backup path

  You are prompted for the backup path if you back up to a fixed-volume storage device. The path specified must be a subdirectory of the path defined by the settings for the storage device. This setting may not be changed after the backup set is created.

- Whether you want to check the drive before requesting a tape

  OS/2 Warp Server Backup/Restore can be set up to check the drive for a suitable volume before prompting you to insert a tape. This setting is useful for scheduled backups to a tape storage device.

3.2.3.2 Backup Set Operation

You can perform actions against a backup set after creating it, as shown in Figure 37 on page 90. The actions include:

- Viewing the backed up data

  You can view the backed up data and its backup information, using the OS/2 Warp Server Backup/Restore GUI, the View log facility (which records all files backed up and restored for a backup set), or the View backed up data facility (which displays a tree view of files in the backup set). The tree view also enables you to review all of the versions of an object (if you define reviewing all versions as an option in your backup set), drop an object, and drop a folder.

- Transfer out

  Transfer out exports a backup set so that it can be archived or used on a different system. If you want to use a transferred-out backup set on another system, you must first perform a transfer-in action.

- Empty

Empty deletes the data held in a backup set, but not the backup set itself.

- Delete

  Delete deletes both the data held in a backup set and the backup set itself.

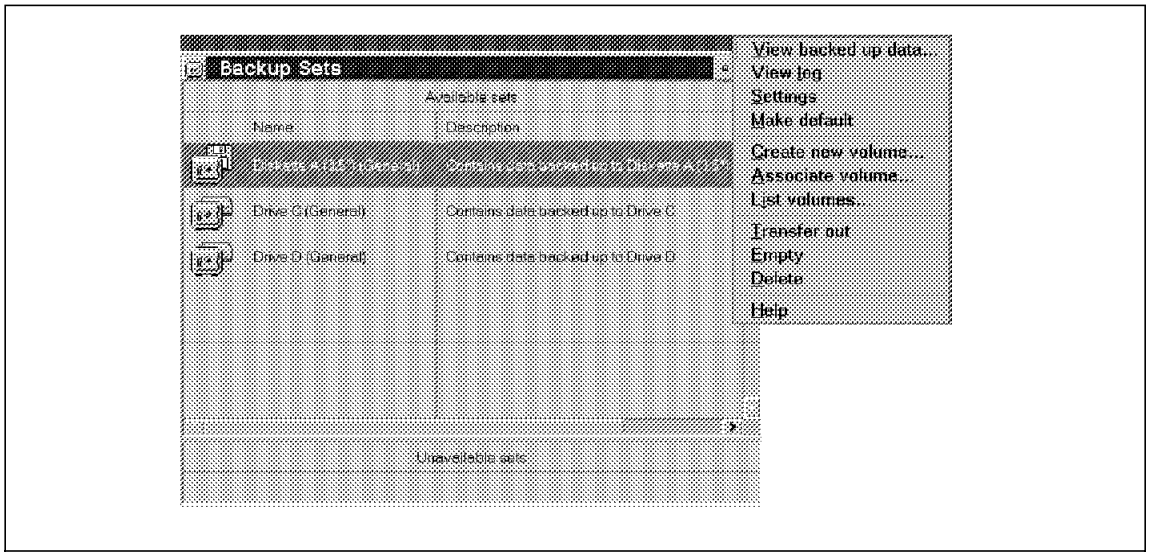


Figure 37. Backup Sets Window

Backup sets are associated with backup methods.

3.2.3.3 Backup Method Definition

Backup methods control the actual backup procedure, as shown in Figure 38 on page 91. Backup methods define:

- The data to be backed up

  The data to be backed up is specified by selecting a source directory and using file filters to filter out unwanted files. Filters can be defined in two ways: tree-based filters, which enable you to graphically view and select files and folders, and rule-based filters, which provide a list of rules either to include or exclude specific files and folders. You can customize the default rule-based filter by adding, deleting, and editing the rules.

- How the data is backed up

  You define how the data is to be backed up by specifying whether you want to perform a full or incremental backup, the type of compression, and the number of backup generations to keep. You can customize your

environment by customizing existing rulebooks and creating your own rulebooks.

- Where the data is backed up to

  You define the destination backup set.

The GUI is designed so that you can see the backup or restore logic flow through the connecting *pipes*. In this example, we choose to back up the C drive and its subdirectories, using PSnS compression to the default backup set. We also want to preview the list of files before the backup occurs.

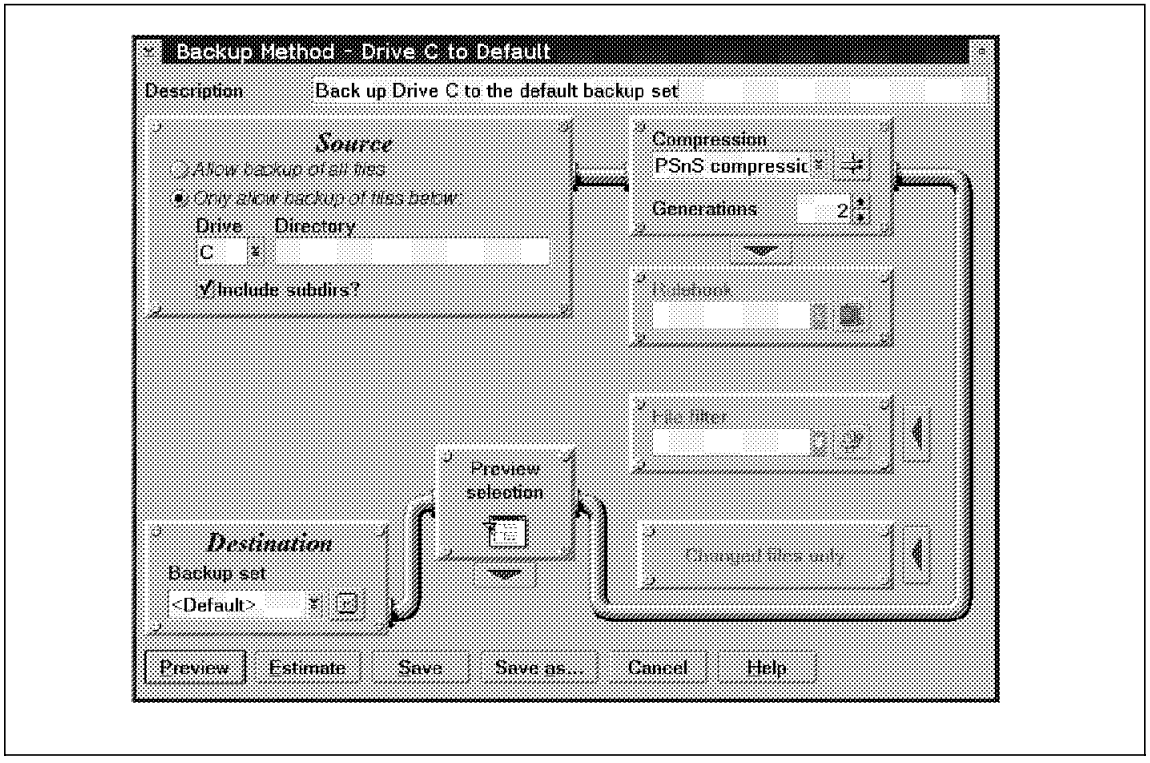


Figure 38. Backup Method Window

3.2.3.4 Backup Method Operation

After defining a backup method you can:

- Preview

  Preview presents you with a tree view of all objects that are selected. You can deselect objects that you do not want to back up.

- Estimate now

Estimate now determines the total amount of data to be backed up and estimates the time the backup will take. The time estimate is based on information about previous backup times to the same storage device.

- Use now

  Use now runs the backup method immediately and captures statistical information on the backup process, such as the amount of data processed, the time taken to perform the backup, the average data rate, and the remaining space on the media.

3.2.3.5 Backup Invocation

Backups can be initiated either manually or as a scheduled event. Scheduled events run a specific backup method at a particular time. There are many types of scheduled events, as shown in Figure 39 and described below.

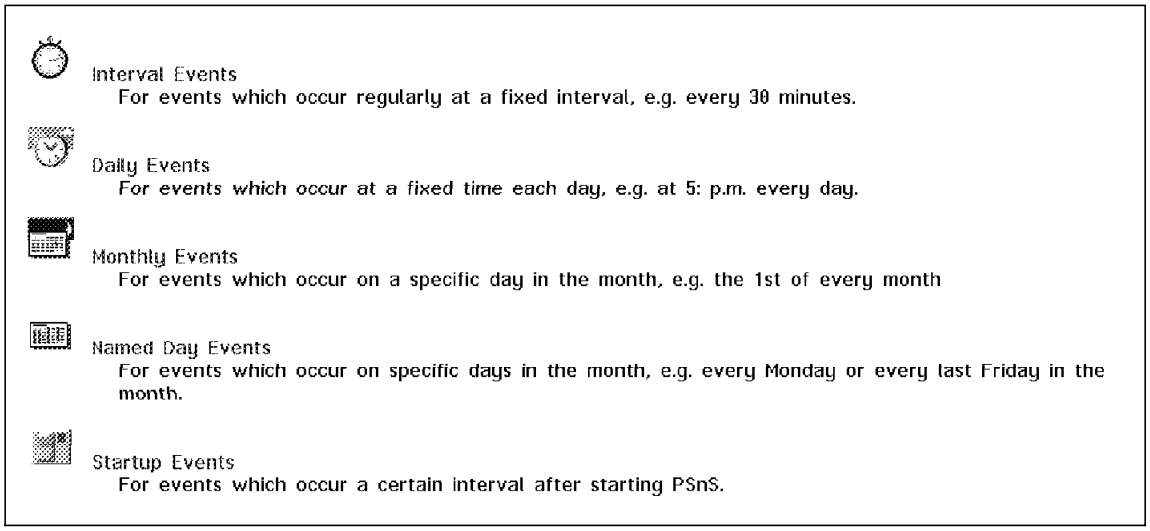


Figure 39. Types of Scheduled Events

- Interval events

  Interval events occur at a regular, fixed interval, for example, backing up transaction data every 2 hours.

- Daily events

  Daily events occur at a fixed time each day, for example, backing up shared user data at 2 a.m. every morning.

- Monthly events

Monthly events occur on a specific day of the month, for example, backing up the end-of-month processing on the first day of every month.

- Named day events

  Named day events occur on specific days of the month, for example, backing up employee time sheets on the last Friday of every month.

- Startup events

  Startup events occur at a certain interval after starting OS/2 Warp Server Backup/Restore, for example, backing up your OS/2 Warp Server desktop whenever the server is booted. If OS/2 Warp Server Backup/Restore is initialized as part of the boot process, you can schedule the desktop backup to occur 5 minutes after OS/2 Warp Server Backup/Restore has been started.

A scheduled event is automatically activated. If you want to delay the start of an event or temporarily stop the processing of an event, you must deactivate it. When you want to start the processing of the event again, you must reactivate it.

Users can be audibly notified of specific events by sounds, through the association of audio files with certain processes, such as the start of a scheduled backup, the successful completion of a backup, or the unsuccessful completion of a backup, as shown in Figure 40 on page 94.

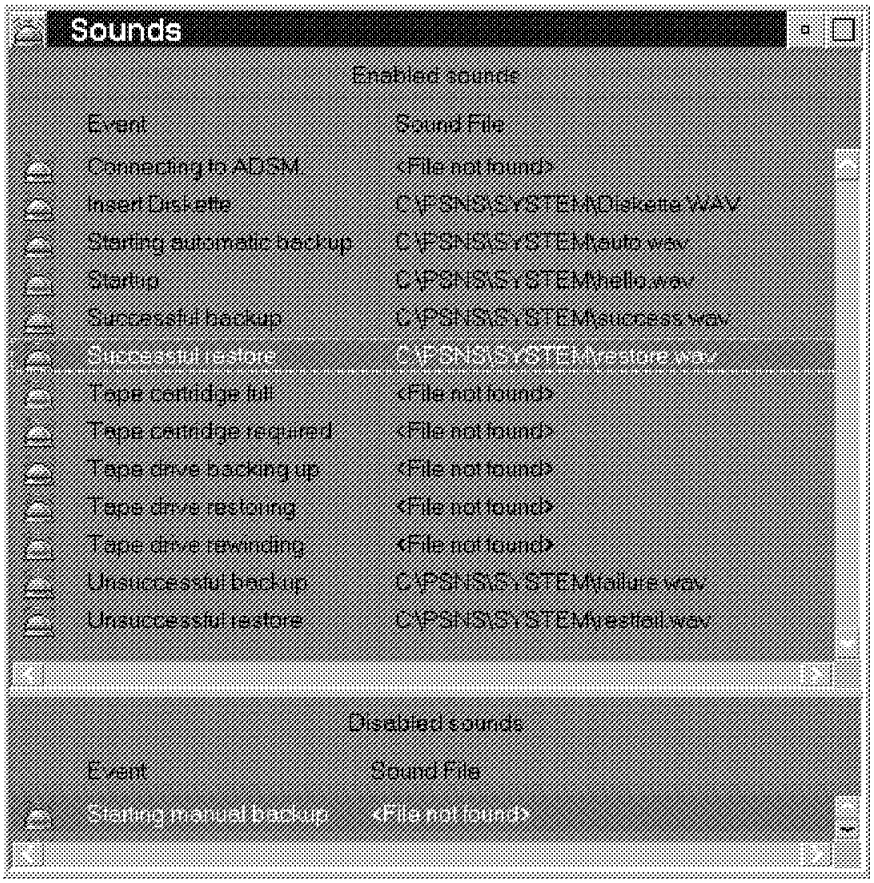


Figure 40. Sounds Window

3.2.4 Restore Strategy

OS/2 Warp Server Backup/Restore restores data that has been backed up on your system or transferred from another OS/2 Warp Server system. You must define a restore method to restore data.

3.2.4.1 Restore Method Definition

Restore methods control the actual restore procedure, as shown in Figure 41 on page 95. They contain such information as:

- The data to be restored

  To specify the data available to be restored, select all backup sets or a specific backup set. You can restore any of the files, or you can restore

particular files by specifying a directory, file name, or file pattern, for example, *.PRE. You can also specify whether subdirectories are to be restored.

- The versions of the data to be restored

  If your backup method specifies that multiple versions of the data are to be saved, you must specify which version to restore. You can restore the most recent version or the version closest to a specific date and time.

- Where the data is to be restored

  You can restore data to either its original location and name or a new location and/or a new name.

In our example, we chose to restore any file, but only the most recent version, to its original location and name. We also selected to preview the list of files before the restore.

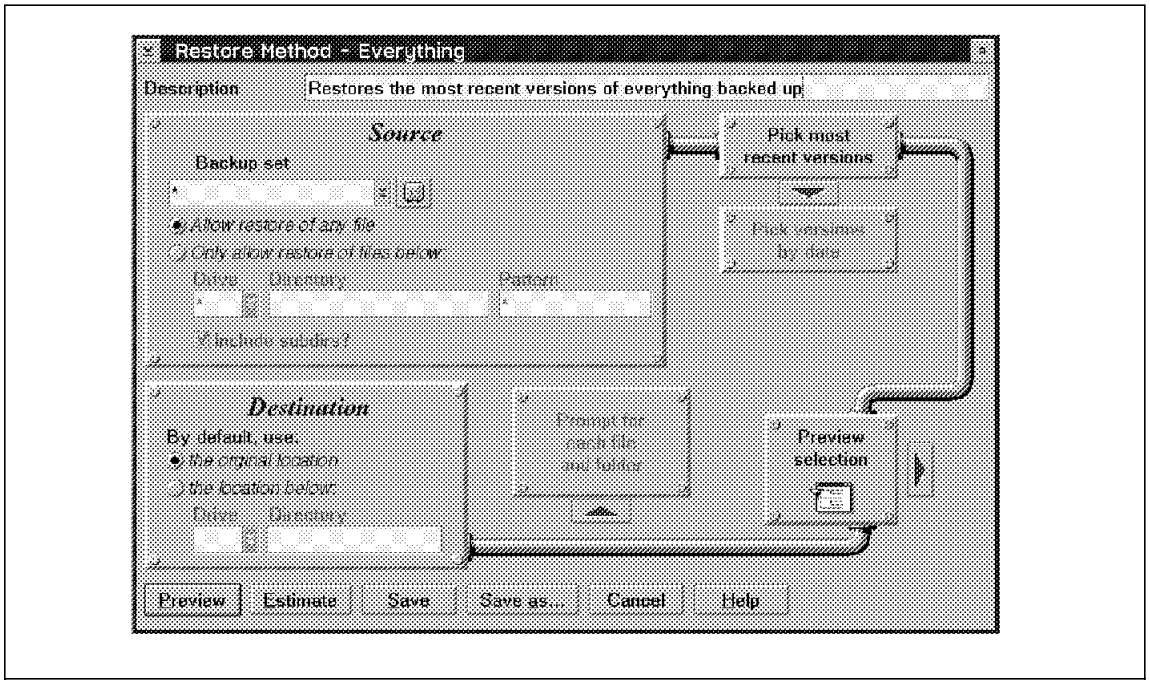


Figure 41. Restore Method Definition

3.2.4.2 Restore Method Operation

After defining a restore method you can:

- Preview

Preview presents you with a tree view of objects that are selected. You can deselect objects that you do not want to restore.

- Estimate now

  Estimate now determines the total amount of data to be restored and estimates the time the restore will take. The time estimate is based on information about previous restore times from the same storage device.

- Use now

  Use now runs the restore method immediately and captures statistical information on the restore process, such as the amount of data processed, the time taken to perform the restore, and the average data rate.

Users can be notified of specific events by sound, through the association of audio files with certain processes, such as insertion of a volume, the successful completion of a restore, or the unsuccessful completion of a restore.

3.2.5 Disaster Recovery Support

OS/2 Warp Server Backup/Restore recognizes that specific system data, if lost, prevents your system from starting and therefore prevents you from restoring other data. OS/2 Warp Server Backup/Restore provides a disaster recovery guide, as shown in Figure 42 on page 97. This guide describes how to create recovery diskettes that are specific to your system. The recovery diskettes are bootable diskettes that contain OS/2 Server Backup/Restore program files and information about your storage devices. After booting from these diskettes, OS/2 Warp Server Backup/Restore can restore other backed up data, and you can check, format, and repartition system hard drives and boot sectors.

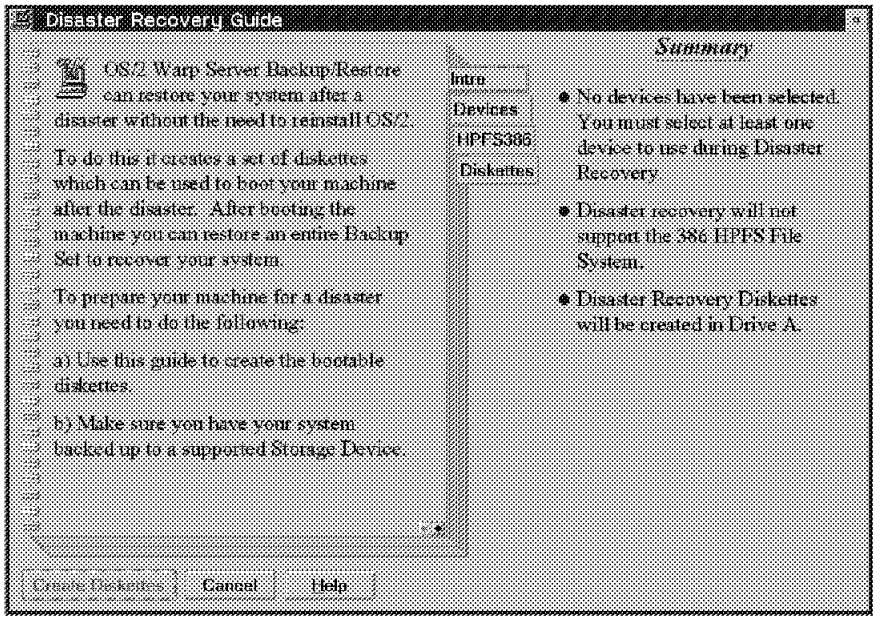


Figure 42. Disaster Recovery Guide

3.3 OS/2 Warp Server Backup/Restore and ADSM

OS/2 Warp Server is a business server that addresses a wide variety of environments, from small workgroups, to departmental LANs, to corporate networks. IBM recognizes that each environment has different backup and recovery requirements. Rather than providing separate products that address each environment, IBM provides a Backup/Restore utility with OS/2 Warp Server that can be extended or integrated to participate in larger or more complex networks by using the powerful backup and restore features of ADSM.

3.3.1 OS/2 Warp Server Backup Alternatives

When installing and configuring OS/2 Warp Server Backup/Restore, you can define the interaction you require with other ADSM systems. As shown in Figure 32 on page 80, this interaction can range from an OS/2 Warp Server Backup/Restore environment where you do not have access to any ADSM systems, to an environment where you have OS/2 Warp Server Backup/Restore coexisting with your ADSM systems and utilizing their storage facilities, to an environment where ADSM takes full responsibility for

the backup/restore management for your Warp Server. Let us look at each alternative in detail and the environments for which they are best suited.

3.3.1.1 OS/2 Warp Server Backup/Restore without ADSM

In an environment that uses OS/2 Warp Server Backup/Restore without ADSM, OS/2 Warp Server Backup/Restore is responsible for the backup and recovery of your OS/2 Warp Server system and data. Backup can be placed on:

- Diskette drives
- Locally attached hard drives
- LAN alias hard drives
- Remotely attached hard drives
- Locally attached manual change tape drives
- Locally attached manual change optical drives

3.3.1.2 OS/2 Warp Server Backup/Restore As an ADSM API Application

In an environment that uses OS/2 Warp Server Backup/Restore as an ADSM API application, OS/2 Warp Server Backup/Restore is responsible for the definition and operation of the backup and recovery of your OS/2 Warp Server system and data. Backups can be placed on:

- Diskette drives
- Locally attached hard drives
- LAN alias hard drives
- Remotely attached hard drives
- Locally attached manual change tape drives
- Locally attached manual change optical drives
- ADSM media

After data is associated with the ADSM storage media, OS/2 Warp Server Backup/Restore releases control of the data, and ADSM assumes responsibility for managing and protecting it. ADSM can move the data between its physical storage volumes, depending on the data hierarchy and migration thresholds defined.

3.3.2 ADSM Backup/Archive Client

In an environment that uses an ADSM backup/archive client, ADSM is responsible for the backup and recovery of your OS/2 Warp Server system and data. Backups can be placed on ADSM server:

- Hard drives
- Manual tape drives
- Automated tape libraries
- Manual optical drives
- Automated optical libraries
- LAN-attached optical drives

ADSM also provides a suite of other facilities such as:

- Automated backup to multiple storage volumes
- Support for multiple backup/restore clients
- Definition of data storage hierarchies
- Automated storage management of backup data through the definition of migration thresholds
- Transparent restoration of backup data to clients other than the original client (this does not require a transfer-out and transfer-in process)
- Security services which ensure that only authorized systems can back up or restore data
- Both command and GUI user and administrative interfaces that facilitate automation
- Support for APIs that enable you to automate, create, and customize backup/restore routines specific to your environment
- Direct integration with applications such as Lotus Notes and DB2/2, for more extensive and customized application backup
- Support for a wide range of backup/restore client and server platforms.

3.3.3 Positioning

In a workgroup environment you typically have a small number of servers, a small amount of data to manage, and a knowledgeable user who assumes administrative responsibilities. OS/2 Warp Server Backup/Restore is ideal for such an environment because it is available on OS/2 Warp Server systems and integrated with other system services. OS/2 Warp Server Backup/Restore provides backup and restore facilities for its system and operational data. These facilities can be extended to other servers that OS/2 Warp Server can access through either LAN alias or logical drive definitions. It provides quick start guides, hints, default backup and restore routines, and a user-friendly GUI for quick and easy setup of backup, restore, and disaster recovery procedures.

If other platforms are added to your environment, OS/2 Warp Server client backups are required, your environment grows, or the amount of data increases, you may find that it is difficult and time consuming to manage each OS/2 Warp Server system individually. In addition your backup data may no longer fit on a single tape or optical disk, so someone must be present during large backups. In these circumstances, consider using ADSM as an integral part of your backup/restore strategy because it provides support for:

- Multiple ADSM clients
- A wide variety of client and server platforms
- Centrally initiated backup and restore operations for all clients
- The definition of data storage hierarchies

Remember

The most successful backup strategies are simple, require little or no human intervention, and store data in the most secure place possible.

3.3.3.1 OS/2 Warp Server Backup/Restore or ADSM?

If your environment contains OS/2 Warp Server systems and you have access to an ADSM server, you may find it difficult to choose the appropriate storage media and backup/restore application. When you are evaluating your options, ask yourself these questions:

- Which data should I back up?
- When or how often should the backup occur?
- Is the backup larger than a single volume?
- Do I have a trained LAN administrator onsite and available?
- Is unattended backup desirable?
- How quickly do I have to access my data?
- To which storage media do I have access?
- Do I have access to an ADSM server?
- Which communications methods can I use to access the ADSM server?
- How large is and what is the speed of the communications pipe I have between my system and the ADSM server?
- How long will it take to back up my data?
- Do I have a large enough backup window to accommodate the data flow?

By asking these questions you may find that, because of the nature of your environment and backup/restore strategy, either OS/2 Warp Server Backup/Restore or the ADSM backup/archive clients is more appropriate for you. If you have access to both environments, however, you will probably want to use some features of both applications. For example:

- The speed and size of your communication links may dictate that you back up only the most sensitive and critical daily files, such as end-of-day processing files, to the ADSM server, and back up the less critical files, such as daily letters, locally.
- If you have good access to an ADSM server, you can base your backup/restore processes on it but use the OS/2 Warp Server Backup/Restore features as part of your system disaster recovery plan.

3.3.3.2 Features Comparison

OS/2 Both Warp Server Backup/Restore and ADSM support many types of file systems, storage devices, and file management services, as indicated in Table 8, Table 9, Table 10 on page 102, Table 11 on page 102, Table 12 on page 103, and Table 13 on page 103.

Table 8. OS/2 Warp Server Backup/Restore and ADSM Interfaces

	OS/2 Warp Server Backup Restore	**ADSM**
GUI	√	√
CLI		√
API		√

Table 9 (Page 1 of 2). OS/2 Warp Server Backup/Restore and ADSM Storage Devices

	OS/2 Warp Server Backup Restore	**ADSM**
Diskette drive	√	
Local hard drive	√	√
Remote hard drive	√	√
Manual tape drive	√	√

Table 9 (Page 2 of 2). OS/2 Warp Server Backup/Restore and ADSM Storage Devices

	OS/2 Warp Server Backup Restore	ADSM
Automated tape library		√
Manual optical drive	√	√
Automated optical library		√
LAN-attached optical drive		√

Table 10. OS/2 Warp Server Backup/Restore and ADSM File Systems and Attributes

	OS/2 Warp Server Backup Restore	ADSM
FAT	√	√
HPFS	√	√
386 HPFS	√	√
Extended attributes	√	√
ACPs	√	√

Table 11 (Page 1 of 2). OS/2 Warp Server Backup/Restore and ADSM Client Support

	OS/2 Warp Server Backup Restore	ADSM
Backup from multiple clients		√
Backup from multiple client platforms	√	√ *
Restore to multiple clients		√

Table 11 (Page 2 of 2). OS/2 Warp Server Backup/Restore and ADSM Client Support

	OS/2 Warp Server Backup Restore	ADSM
Cross-client restore		√

Note:

* ADSM supports a much greater number of client platforms than OS/2 Warp Server Backup/Restore.

Table 12. OS/2 Warp Server Backup/Restore and ADSM Management Features

	OS/2 Warp Server Backup Restore	ADSM
Support for data hierarchies		√
Support for automated data migration		√
Local management facilities	√	√
Central management facilities		√
Security facilities		√
Information and error logs	√	√
System disaster recovery facilities	√	√
CID enabled	√	√

Table 13 (Page 1 of 2). OS/2 Warp Server Backup/Restore and ADSM Backup Features

	OS/2 Warp Server Backup Restore	ADSM
Support for incremental backup	√	√
Support for selective backup	√	√
Manually initiated backups	√	√

Table 13 (Page 2 of 2). OS/2 Warp Server Backup/Restore and ADSM Backup Features

	OS/2 Warp Server Backup Restore	ADSM
Support for multiple versions	√	√
Support for compression	√	√
Scheduled backups	√	√
Scheduled backups of all clients		√
Direct application support (for example, Lotus Notes and DB2/2)		√

3.3.4 Converting from OS/2 Warp Server Backup/Restore to ADSM

You cannot migrate backup versions from OS/2 Warp Server Backup/Restore to ADSM. Even if you use OS/2 Warp Server Backup/Restore as an ADSM API application to store the backup data in ADSM server storage, you cannot use the ADSM backup/archive client to restore the backups. ADSM application clients and backup/archive clients are not interoperable. If you back up using an application client, you must restore using the application client. If you back up using a backup/archive client, you must restore using a backup/archive client.

Therefore, it is important to read 3.3.3, “Positioning” on page 99 and make the proper decision for your present and future environment. There are three possible scenarios for converting from OS/2 Warp Server Backup/Restore to ADSM, as shown in Figure 43 on page 105:

- From OS/2 Warp Server Backup/Restore to ADSM backup/archive clients (A)
- From OS/2 Warp Server Backup/Restore to OS/2 Warp Server Backup/Restore with ADSM (B)

  In this case, OS/2 Warp Server Backup/Restore is an ADSM application client. It uses the ADSM API.
- From OS/2 Warp Server Backup/Restore with ADSM to ADSM backup/archiv clients (C)

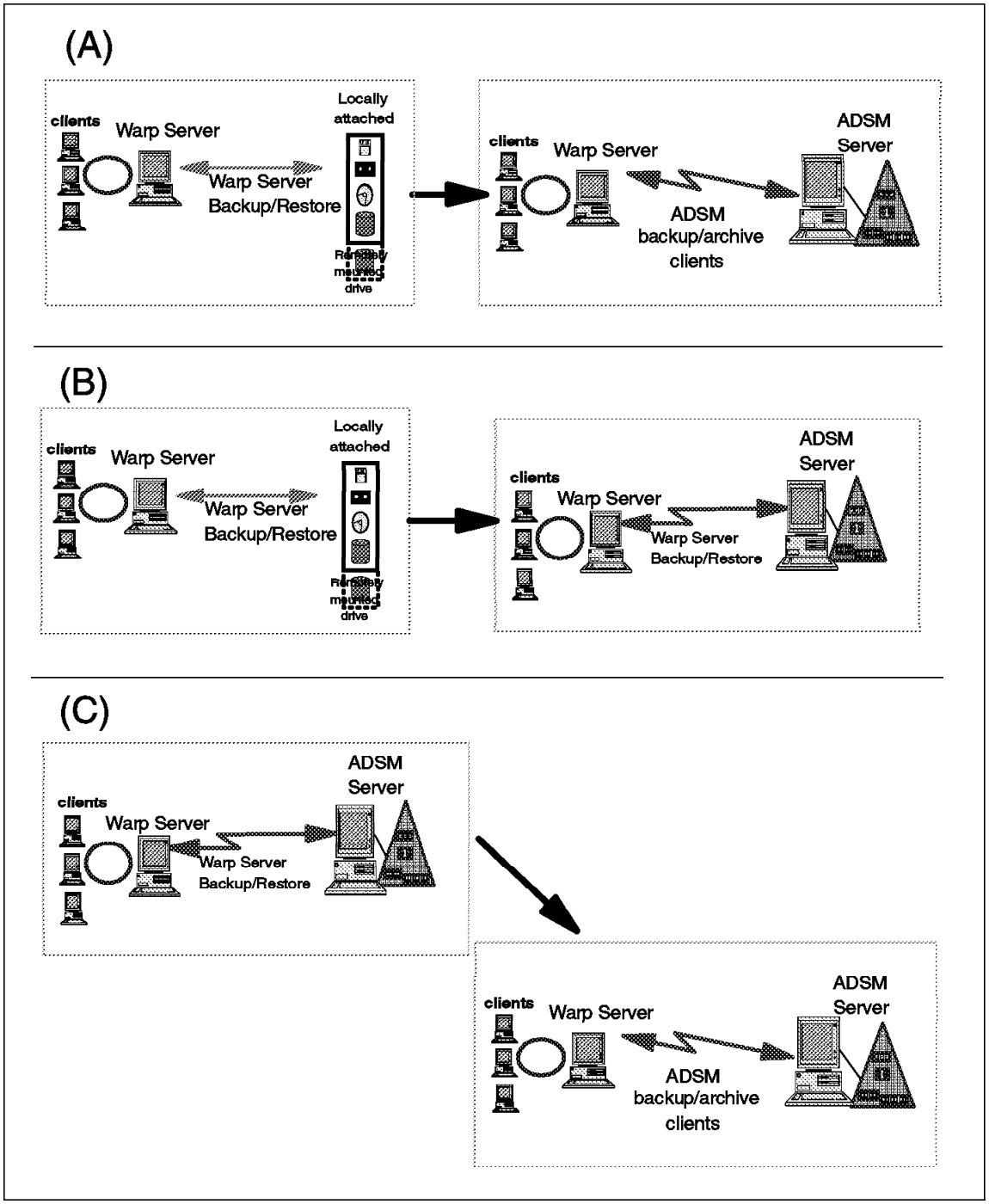


Figure 43. Converting from OS/2 Warp Server Backup/Restore to ADSM

For each scenario there are two conversion approaches: *coexistence* and *immediate conversion*.

3.3.4.1 Coexistence

OS/2 Warp Server Backup/Restore can coexist with the ADSM backup/archive client. You can keep previous data versions on OS/2 Warp Server Backup/Restore media and at the same time back up new data to ADSM. This is a gradual, cleanup approach to free up disk, tape, or optical media.

For scenarios A and C, you would start any future backups from the ADSM backup/archive client. For scenario B, you would start any future backups to the OS/2 Warp Server ADSM backup set. You would keep OS/2 Warp Server Backup/Restore for some time just in case you have to restore files and directories that have been erased from the workstation or if you want to restore older backup versions.

After your new backup method has been running for a while, you can delete the backup copies stored by your old backup method. You could use OS/2 Warp Server Backup/Restore to view the backup sets directory tree structures from the Backup Sets window, and click on a chosen part of the directory tree with the right mouse button to Drop the entire directory and all subdirectories. Another option is to delete the entire backup set from the Backup Sets window by clicking on the backup set with the left mouse button and then clicking with the right mouse button to use the Delete action.

3.3.4.2 Immediate Conversion

You may want to convert to the new backup method immediately as a quick cleanup approach to free up disk, tape, or optical media.

For scenarios A and C, you would start any future backups from the ADSM backup/archive client. For scenario B, you would start any future backups to the OS/2 Warp Server ADSM backup set. However, you would not keep the older backup method, using just OS/2 Warp Server Backup/Restore; instead you would immediately determine which files and directories have been erased on the workstation so that they can be re-created and rebacked up with the new backup method. You would restore these files and directories using OS/2 Warp Server Backup/Restore and then reback them up to ADSM. After the backup to ADSM is successful, you can delete all of the OS/2 Warp Server Backup/Restore backup sets.

Chapter 4. Using Warp Server Backup/Restore As an ADSM API Application

In this chapter we explain how to use OS/2 Warp Server Backup/Restore as an ADSM API application.

We discuss the backup and recovery of an HPFS shared data area (C:\RESOURCES\SHAREDDATA) that resides on the OS/2 Warp Server. The data is backed up to ADSM media.

Figure 44 depicts the LAN environment we used for testing.

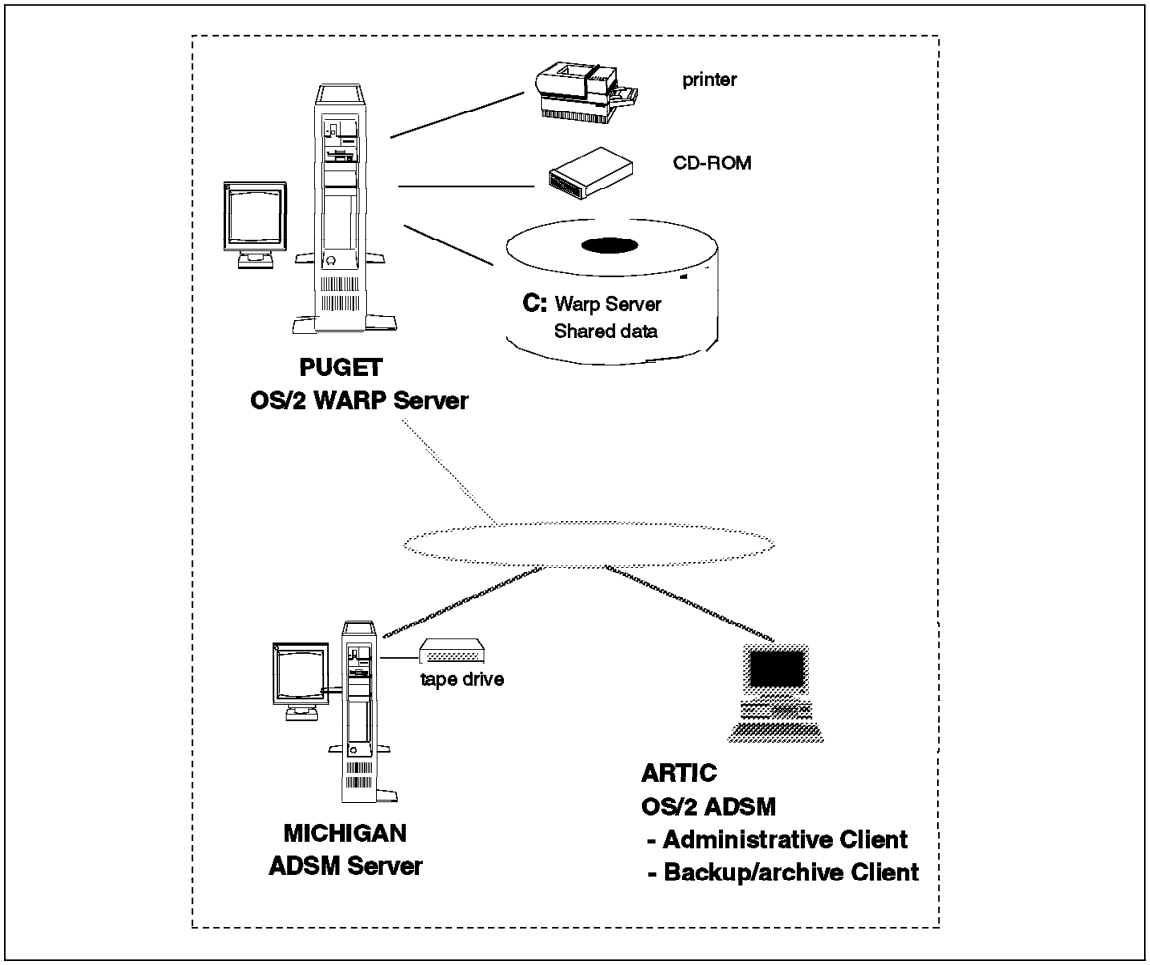


Figure 44. LAN Testing Environment

4.1 Backup

The backup of the shared data area is a six-step process:

1. Configure the ADSM server to recognize OS/2 Warp Server Backup/Restore.
2. Configure OS/2 Warp Server Backup/Restore for ADSM media support.
3. Define a backup set that uses ADSM storage media.
4. Define a backup method that backs up the shared data to the ADSM backup set.
5. Run the backup method.
6. Check the backup log.

4.1.1 Configure the ADSM Server

Configure the ADSM Server to recognize the OS/2 Warp Server Backup/Restore system:

1. From your ADSM Administration system desktop, double-click on the **ADSM Client** icon, as shown in Figure 45.

Figure 45. ADSM Client Icon

The ADSM Client folder is displayed, as shown in Figure 46.

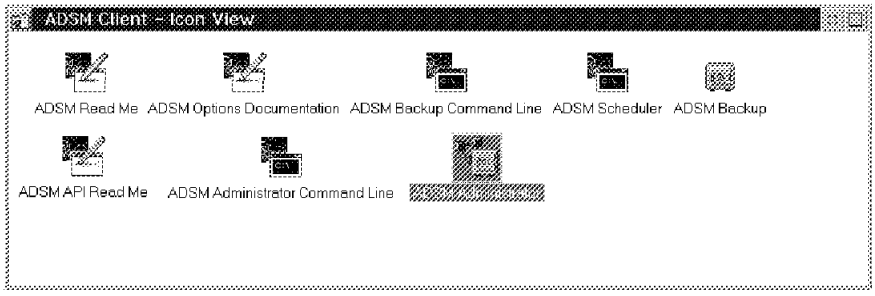


Figure 46. ADSM Client Folder

2. Double-click on the **ADSM Administrator** icon.

The Product Information window is displayed.

3. Select the **OK** button.

   The ADSM Administration - Logon window is displayed.

4. Enter an administrator name and password.

5. Select the **Logon** button.

   The ADSTAR Distributed Storage Manager (Administration) window is displayed, as shown in Figure 47.

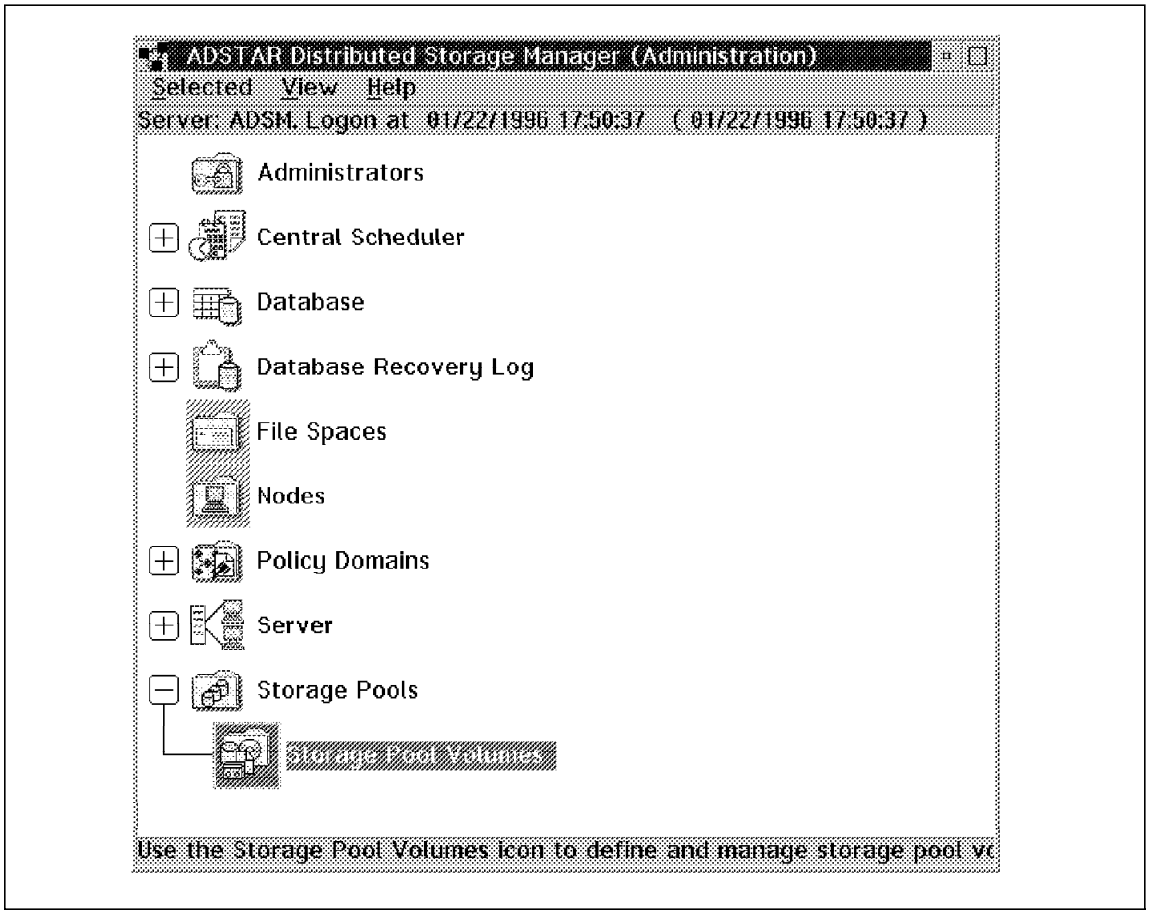


Figure 47. ADSTAR Distributed Storage Manager (Administration) Window

6. Double-click on the **Nodes** icon.

   The Nodes window is displayed.

7. Select **Edit** from the menu bar.

8. Select **Add** from the pull-down menu.

   The Node - Add notebook is displayed, as shown in Figure 48.

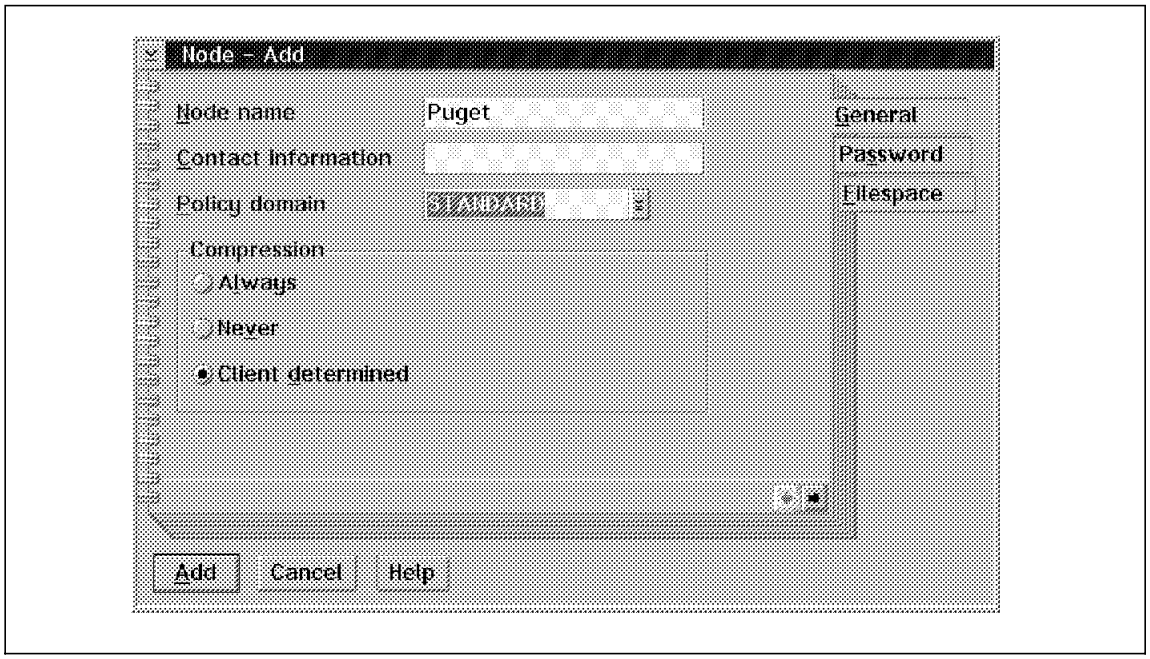


Figure 48. Node - Add Notebook

9. Define the OS/2 Warp Server Backup/Restore system:
   - Enter Puget in the **Node name** field.
   - Select STANDARD from the **Policy domain** list box.
   - Select the **Client determined** radio button from the **Compression** options.
   - Click on the Password tag. On the Password notebook page enter a password in the **Password** field.
   - Reenter the password in the **Reenter Password** field.
   - Click on the Filespace tag. On the Filespace notebook page check the **Can delete archive data** checkbox
   - Check the **Can delete backup data** checkbox
10. Select the **Add** button.

    The Nodes window is displayed, as shown in Figure 49 on page 111.

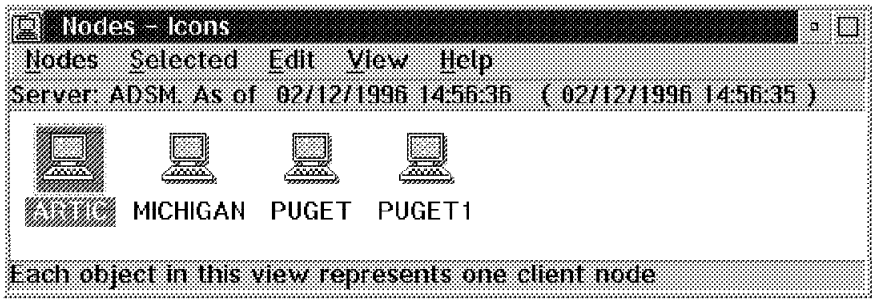


Figure 49. Nodes - Icons Window

11. Double-click on the Nodes icon at the top left of the window.

    The ADSTAR Distributed Storage Manager (Administration) window is displayed.

Note that we set up a PSnS management class and backup copy group that differs from the standard ADSM OS/2 client defaults. The PSnS backup copy group (Figure 50 on page 112) only keeps one backup version if the file exists on the client and no backup versions if the file is deleted on the client, as shown in Figure 51 on page 113. The standard default backup copy group keeps two backup versions if the file exists on the client and one backup version if the file is deleted.

We used a different backup copy group because PSnS uses a different object name each time it sends a file to the ADSM server through the ADSM API. PSnS keeps track of the different versions of a file it sends to ADSM. From ADSM′s point of view, each file it receives from PSnS is a completely different file. Because of PSnS′s naming scheme, letting ADSM keep multiple versions of the same file would waste space. PSnS only uses active files on ADSM. This will become clearer when we look at how the PSnS data is stored on the ADSM server (see Figure 73 on page 129).

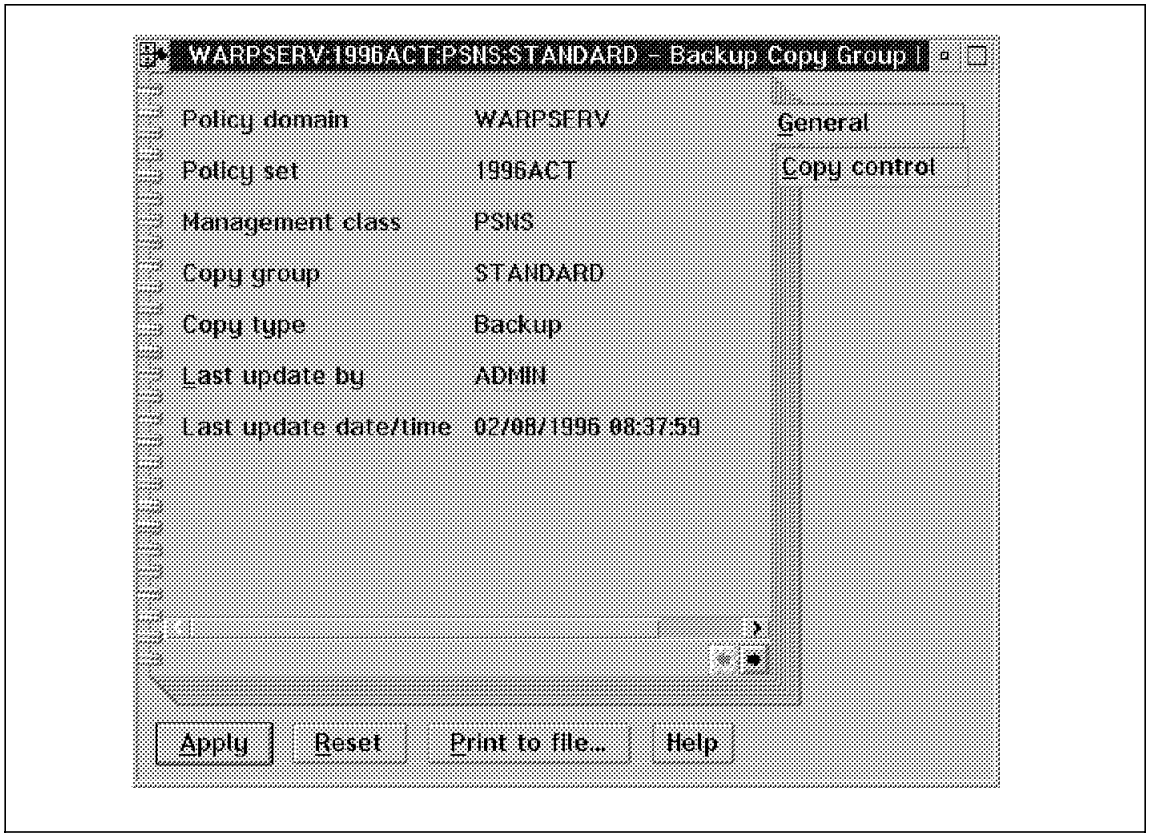


Figure 50. PSnS Backup Copy Group: General Notebook Page

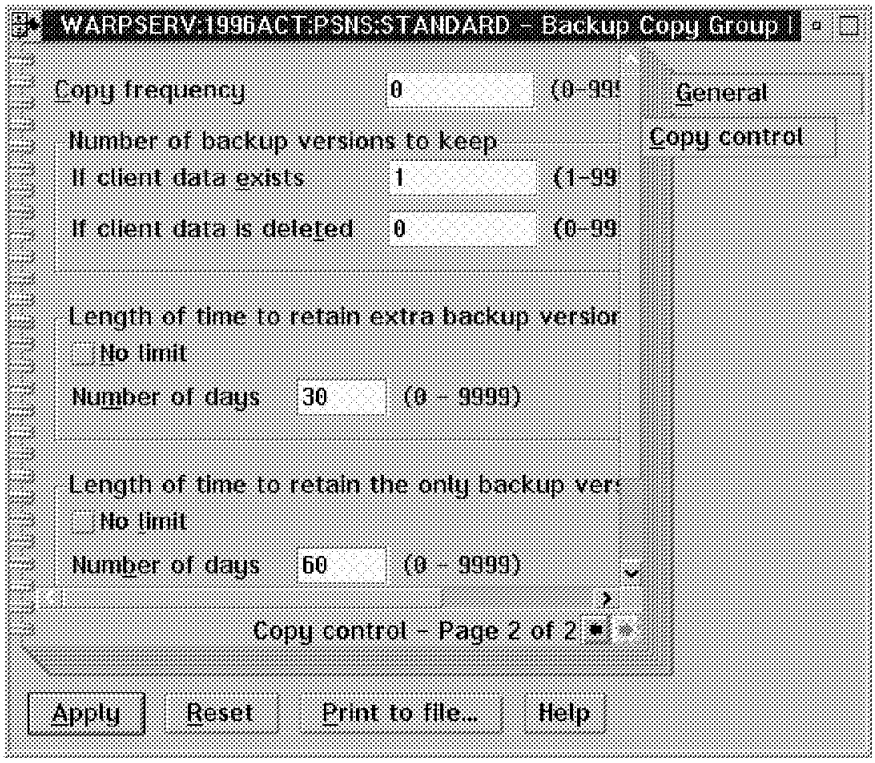


Figure 51. PSnS Backup Copy Group: Copy Control Notebook Page

4.1.2 Configure OS/2 Warp Server Backup/Restore

Configure the OS/2 Warp Server Backup/Restore system for ADSM media support:

1. From your OS/2 Warp Server desktop, double-click on the **PSnS Backup and Recovery** icon, as shown in Figure 52.

Figure 52. PSnS Backup and Recovery Icon

The PSnS Backup and Recovery folder is displayed, as shown in Figure 53 on page 114.

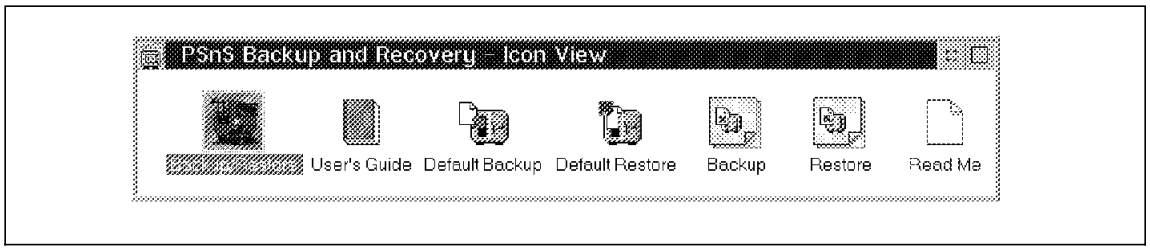


Figure 53. PSnS Backup and Recovery Folder

2. Double-click on the **Backup/Restore** icon.

   The OS/2 Warp Server Backup/Restore window is displayed, as shown in Figure 54.

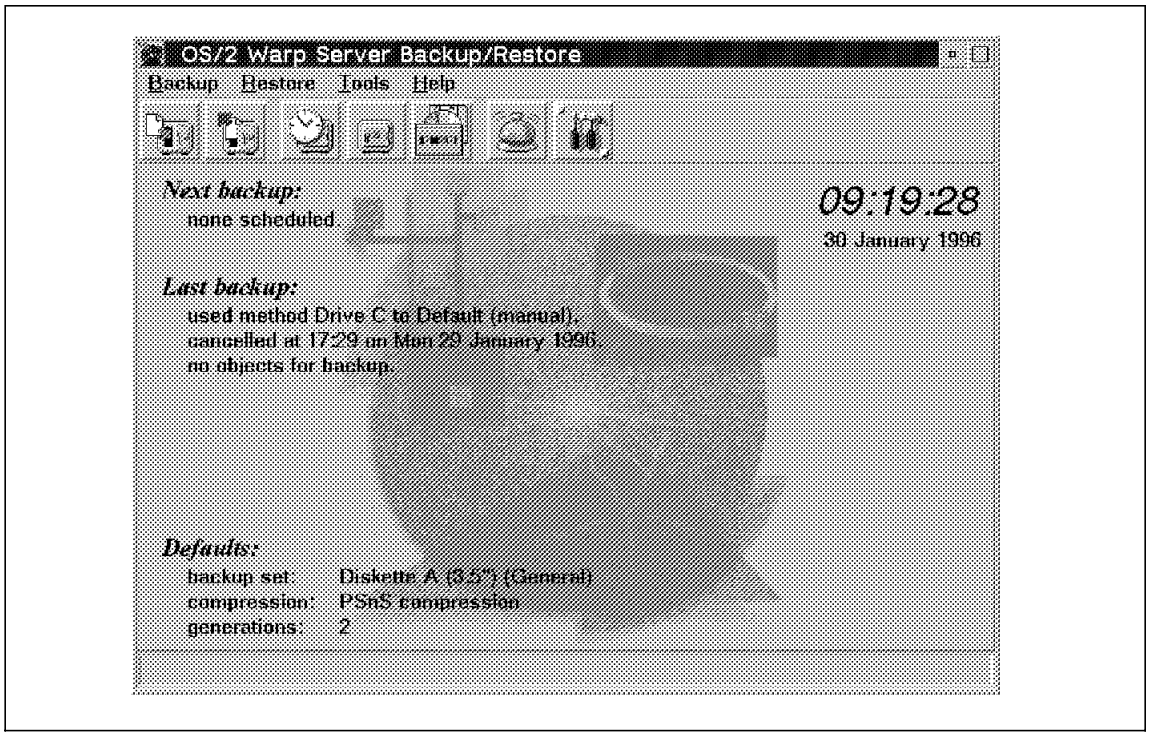


Figure 54. OS/2 Warp Server Backup/Restore Window

3. Select **Tools** from the menu bar.
4. Select **Storage Devices** from the pull down menu.

The Storage Devices Window is displayed, as shown in Figure 56 on page 116.

5. Click with your right-hand mouse button on an unpopulated area of the window.

   The Storage Devices pop-up is displayed, as shown in Figure 55.

6. Click on **New**.

   A side menu is displayed, as shown in Figure 55.

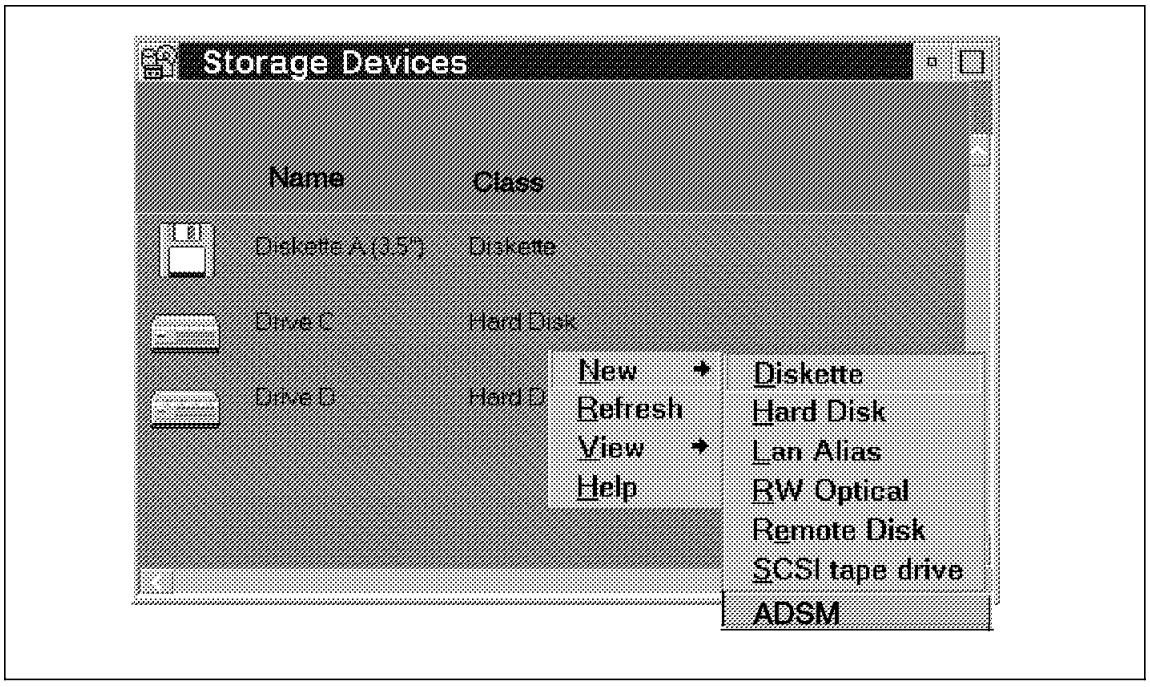


Figure 55. Storage Devices Window before Adding ADSM

7. Select **ADSM** from the side menu.

   The Storage device - ADSM window is displayed, as shown in Figure 56 on page 116.

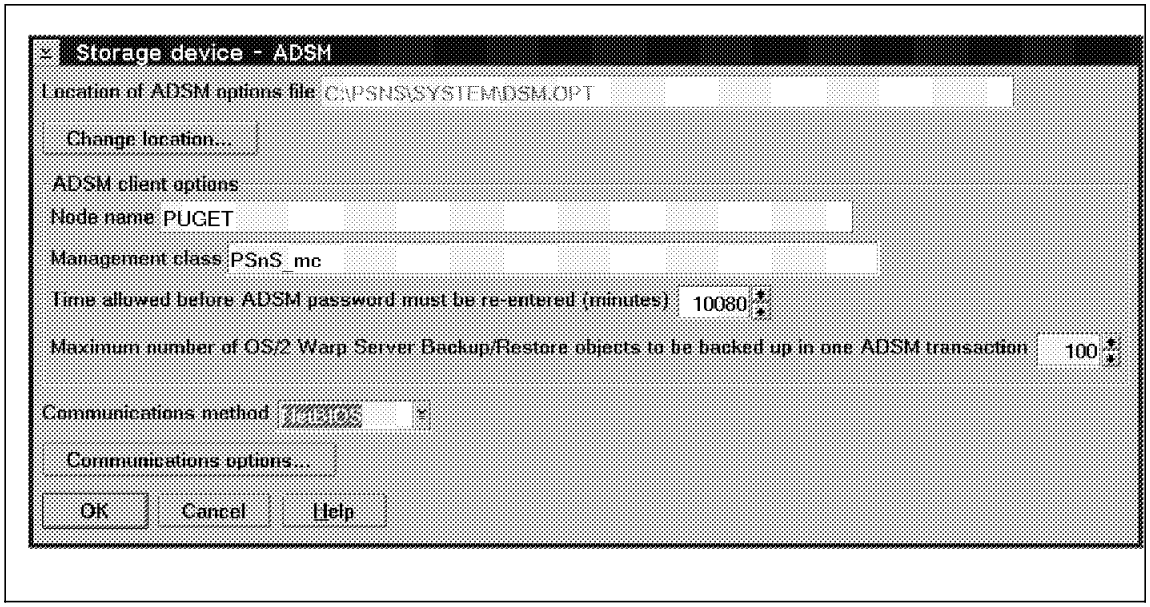


Figure 56. Storage Device - ADSM Window

8. Define the ADSM client options required to connect to ADSM Server Puget through NetBIOS:
   - Enter PUGET in the **Node name** field.
   - Enter the management class we defined for PSnS data, PSnS_mc, in the **Management class** field.
   - Accept the default settings for Time allowed before ADSM password must be re-entered (minutes) and Maximum number of OS/2 Warp Server Backup/Restore objects to be backed up in one ADSM transaction.
   - Select NetBIOS from the **Communications method** list box.
   - Click on the **Communications options** button.

     The ADSM configuration - NetBIOS options window is displayed, as shown in Figure 57 on page 117.

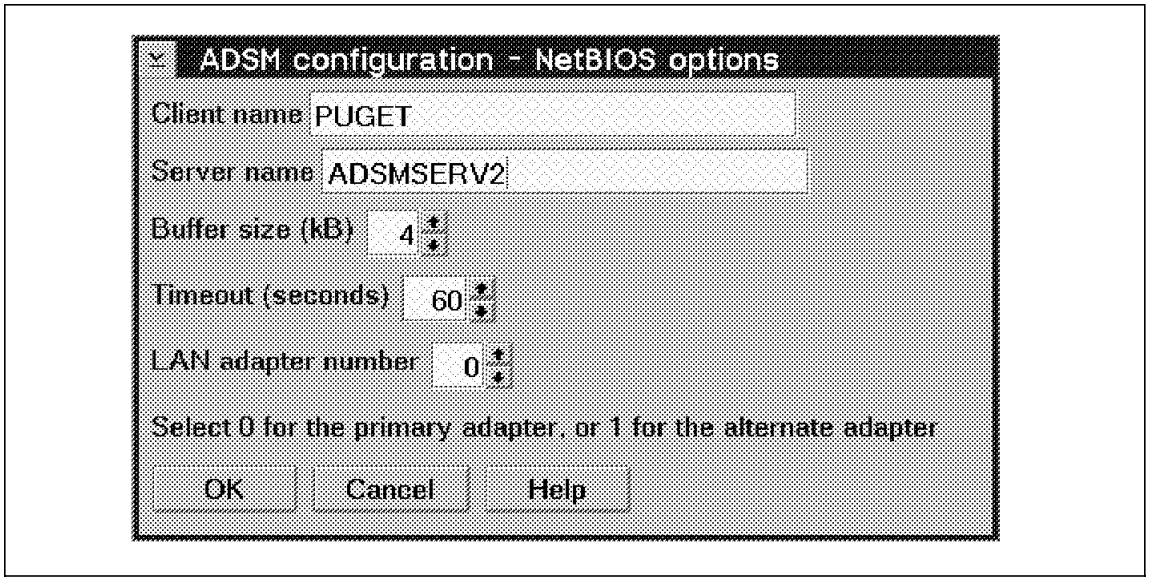


Figure 57. ADSM Configuration - NetBIOS Options Window

9. Define the OS/2 Warp Server Backup/Restore client, and ADSM Server information:
   - Enter PUGET in the **Client name** field.
   - Enter ADSMSERV2 in the **Server name** field.
   - Accept all other default settings.

   Note

   This process updates the DSM.OPT file in the PSNS\SYSTEM directory. To see the changes made to the DSM.OPT file as a result of this configuration, refer to B.2, "OS/2 Warp Server DSM.OPT Options File" on page 166.

10. Select the **OK** button.

    The Storage device - ADSM window is displayed.

11. Select the **OK** button.

    The Storage Devices window shown in Figure 58 on page 118 displays a storage device called ADSM with a storage class of ADSM Client.

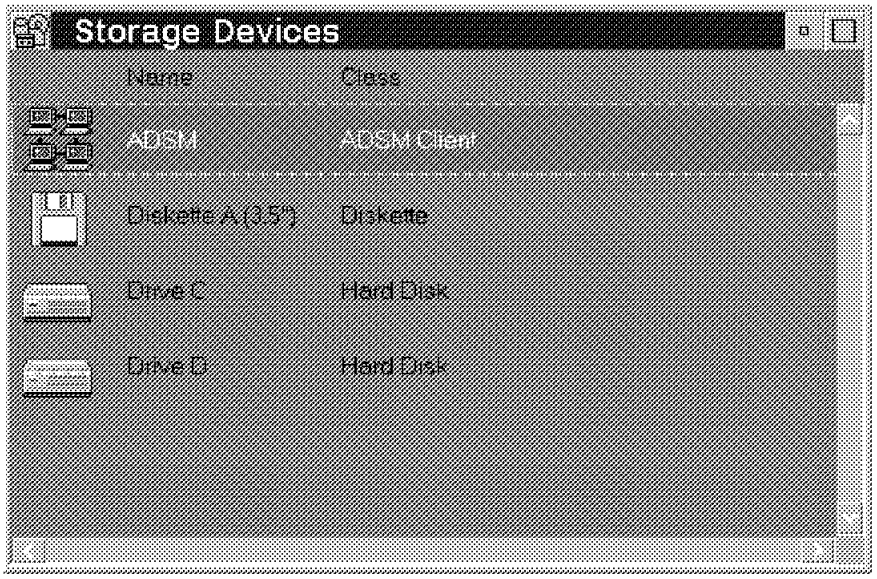


Figure 58. Storage Devices Window after Adding ADSM

12. Double-click on the **Storage Devices** icon at the top left of the window.

    The OS/2 Warp Server Backup/Restore window is displayed.

4.1.3 Define a Backup Set

Define a backup set called ADSM that uses ADSM storage media:

1. Select the OS/2 Warp Server Backup/Restore window.
2. Select **Tools** from the menu bar.
3. Select **Backup Sets** from the pull-down menu.

   The Backup Sets window is displayed, as shown in Figure 59 on page 119.
4. Click with your right-hand mouse button on an unpopulated area of the window.

   The Backup Sets pop-up is displayed, as shown in Figure 59 on page 119.

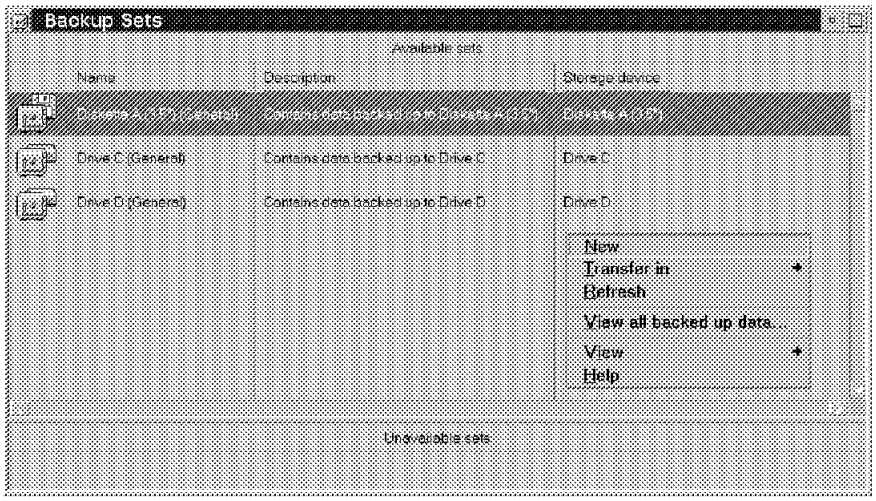


Figure 59. Backup Sets Window before Adding ADSM

5. Click on **New**.

   The New Backup Set window is displayed, as shown in Figure 60.

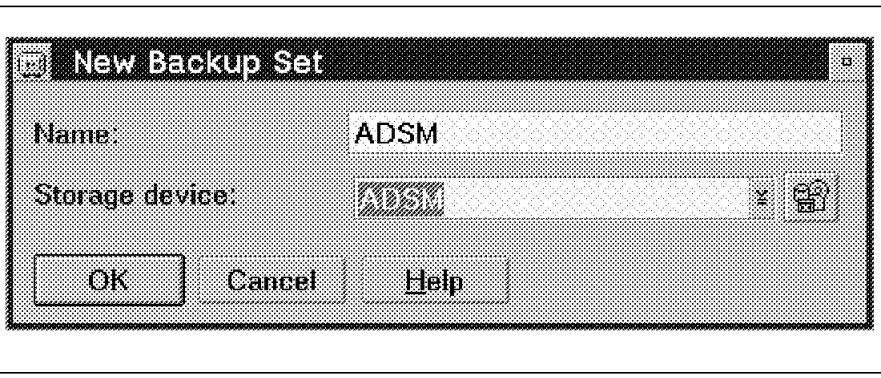


Figure 60. New Backup Set Window

6. Define backup set ADSM that uses ADSM storage media:
   - Enter ADSM in the **Name** field.
   - Select ADSM from the **Storage device** list box.
7. Select the **OK** button.

   The Backup Set Settings - ADSM window is displayed, as shown in Figure 61 on page 120.

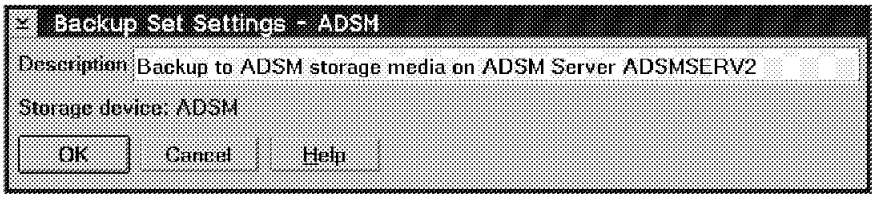


Figure 61. Backup Set Settings - ADSM Window

8. Enter Backup to ADSM storage media on ADSM Server ADSMSERV2 in the **Description** field.
9. Select the **OK** button.

   The Backup Sets window shown in Figure 62 displays a backup set called ADSM that uses a storage device called ADSM.

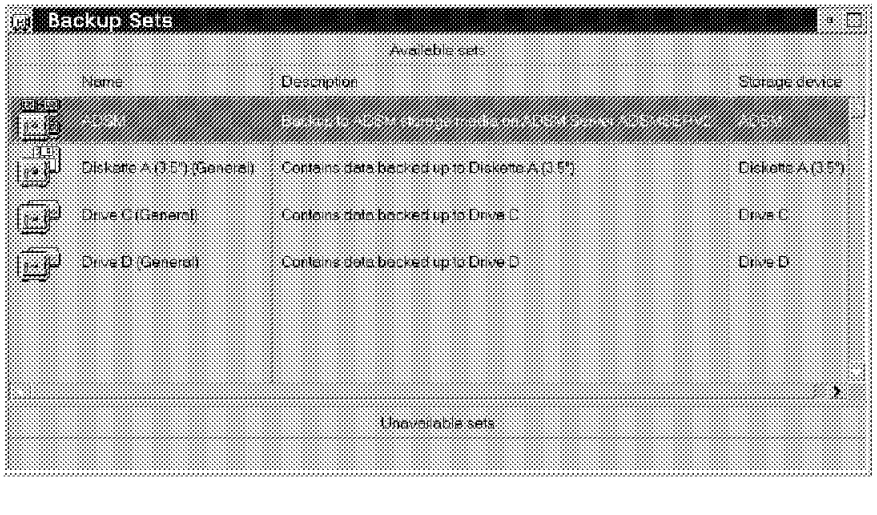


Figure 62. Backup Sets Window after Adding ADSM

10. Double-click on the **Backup Sets** icon at the top left of the window.

    The OS/2 Warp Server Backup/Restore window is displayed.

4.1.4 Define a Backup Method

Define a backup method called SD2ADSM that backs up the C:\RESOURCES\SHAREDDATA shared data by using the ADSM backup set:

1. Select the OS/2 Warp Server Backup/Restore window.

2. Select **Tools** from the menu bar.
3. Select **Backup Methods** from the pull-down menu.

   The Backup Methods window is displayed, as shown in Figure 63.
4. Click with your right-hand mouse button on an unpopulated area of the window.

   The Backup Methods pop-up is displayed, as shown in Figure 63.

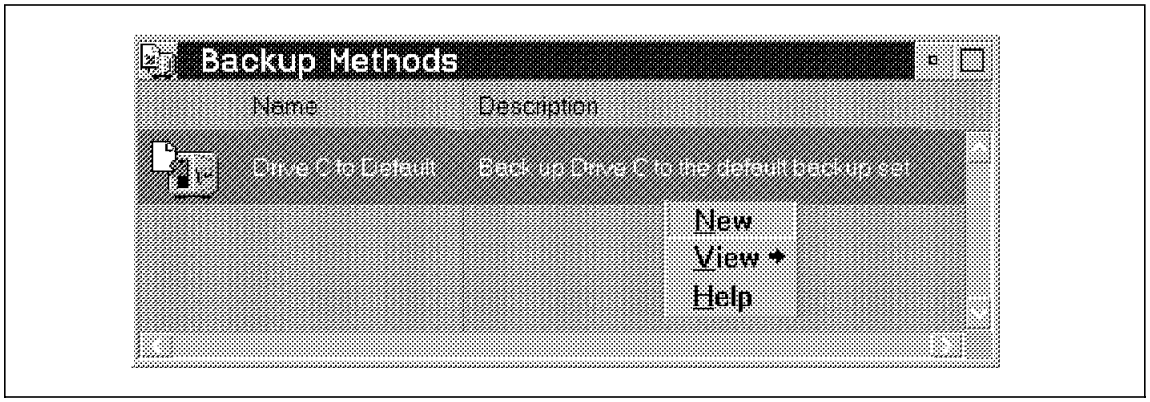


Figure 63. Backup Methods Window before Defining a New Backup Method

5. Click on **New**.

   The default Backup Method - Untitled window is displayed, as shown in Figure 64 on page 122.

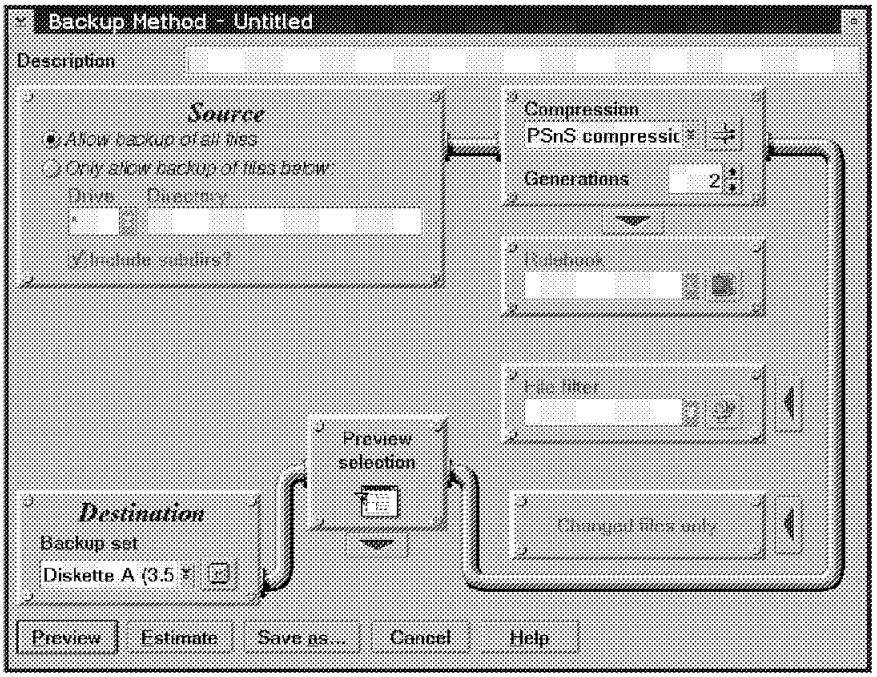


Figure 64. Backup Method - Untitled Window

6. Back up the C:\RESOURCES\SHAREDDATA shared data area to the ADSM backup set. The information you provide in this step appears in the Backup Method - SD2ADSM window (Figure 67 on page 124).
   - Enter PUGET shared data area C:\RESOURCES\SHAREDDATA in the **Description** field.
   - Select the **Only allow backup of files below** radio button from the **Source** options.
   - Select C from the **Drive** list box.
   - Enter RESOURCES\SHAREDDATA in the **Directory** field.
   - Check the **Include subdirs?** check box.
   - Select no compression from the **Compression** list box.
   - Enter 4 in the **Generations** field.
   - Select the **Preview selection** option.
   - Select ADSM from the **Backup set** list box.
7. Select the **Save as** button.

The Save as window is displayed, as shown in Figure 65 on page 123.

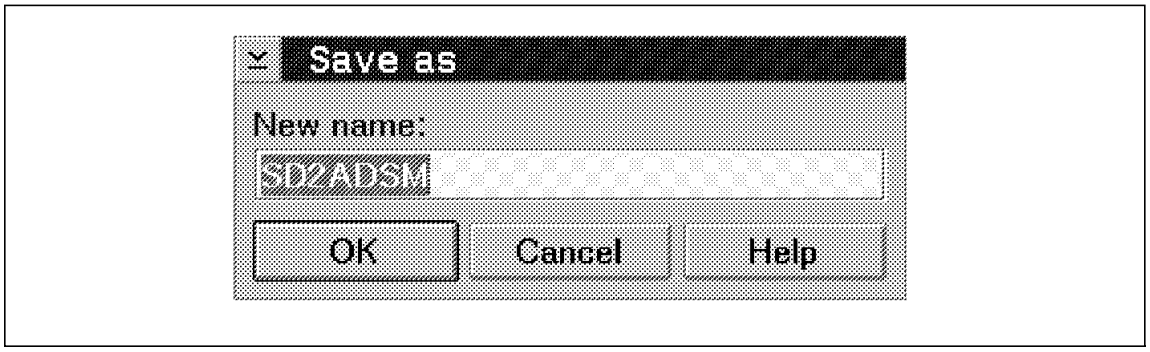


Figure 65. Save As Window

8. Enter SD2ADSM in the **New name** field.
9. Select the **OK** button.

   The Backup Methods window is displayed.
10. Double-click on the Backup Methods icon at the top left of the window.

    The OS/2 Warp Server Backup/Restore window is displayed.

4.1.5 Run the Backup Method

Run the SD2ADSM backup method:

1. Select the OS/2 Warp Server Backup/Restore window.
2. Select **Tools** from the menu bar.
3. Select **Backup Methods** from the pull-down menu.

   The Backup Methods window is displayed, as shown in Figure 66.

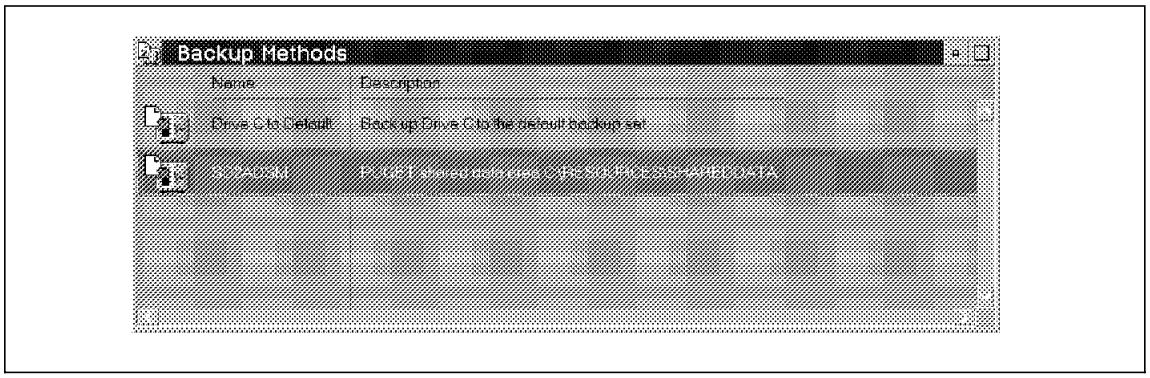


Figure 66. Backup Methods Window after Defining a New Backup Method

4. Double-click on the SD2ADSM icon.

   The Backup Method - SD2ADSM window is displayed, as shown in Figure 67.

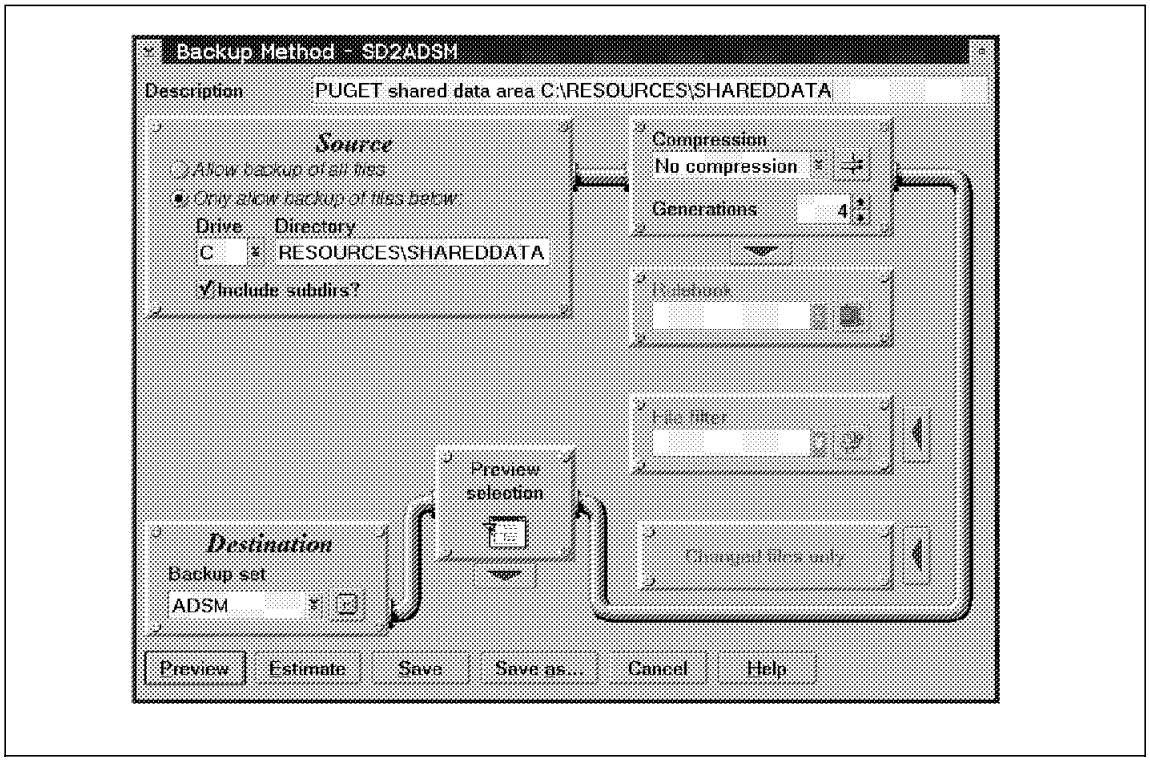


Figure 67. Backup Method - SD2ADSM Window

5. Select the **Preview** button.

   The Backup Preview - SD2ADSM window is displayed, as shown in Figure 68 on page 125.

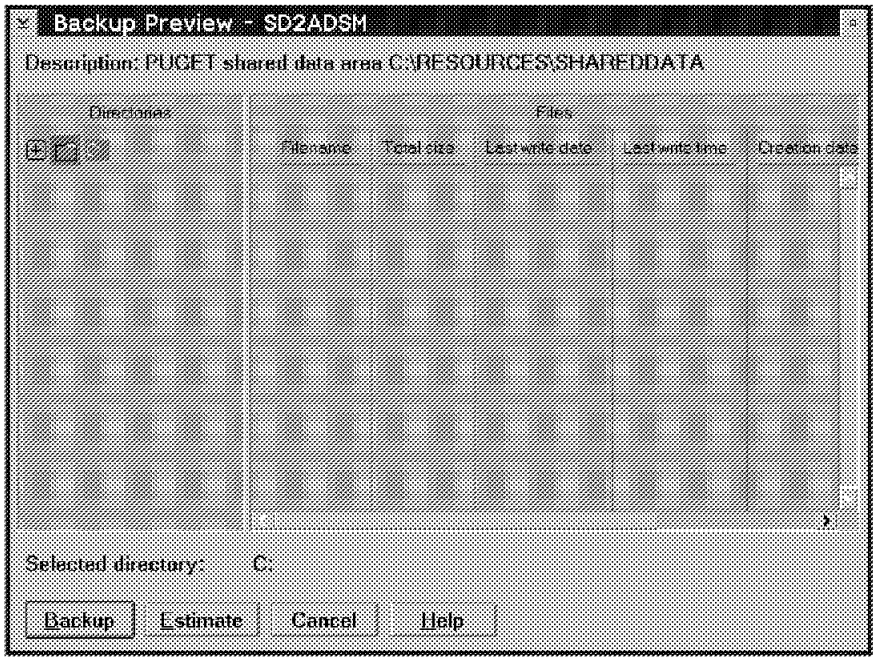


Figure 68. Backup Preview - SD2ADSM Window before Selecting Directories for Backup

6. Show the directories to be backed up:
   - Click on the + icon next to C icon.
   - Click on the + icon next to the RESOURCES icon.
   - Click on the + icon next to the SHAREDDATA icon.

   The C:\RESOURCES\SHAREDDATA files and subdirectories that are to be backed up are displayed and marked with checkmarks, as shown in Figure 69 on page 126.

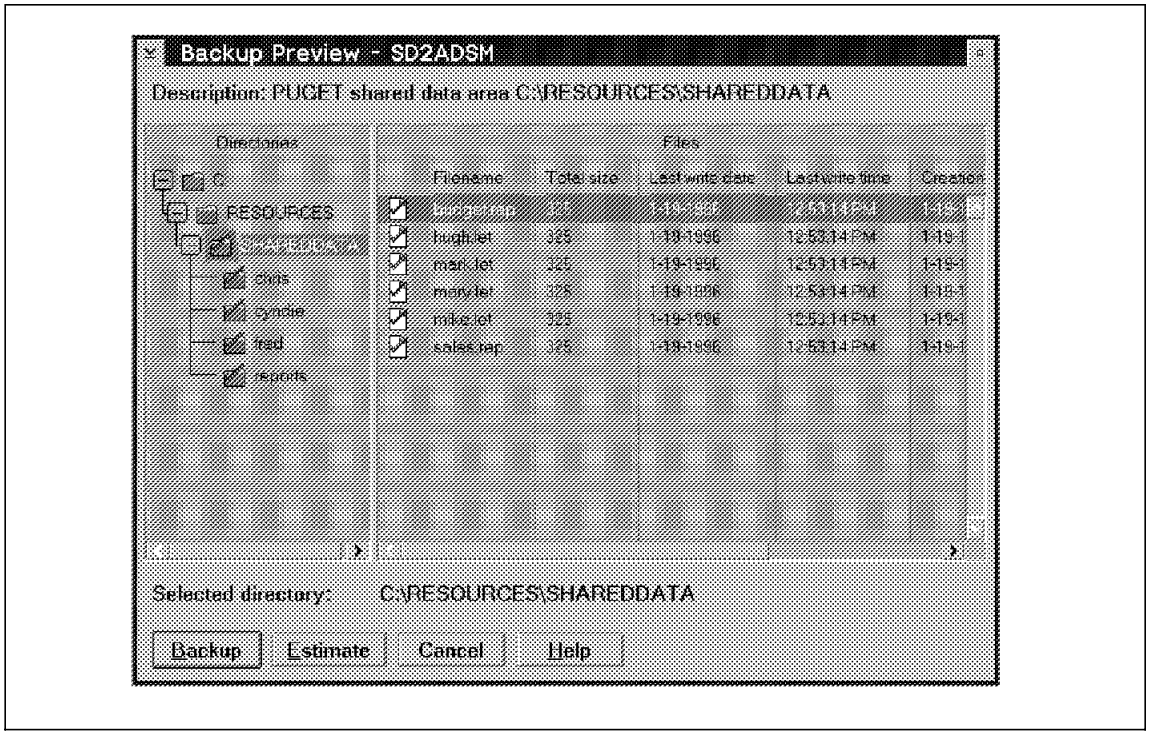


Figure 69. Backup Preview - SD2ADSM Window after Selecting Directories for Backup

7. Select the **Backup** button.

   The Backup Progress - SD2ADSM window is displayed, as shown in Figure 70 on page 127.

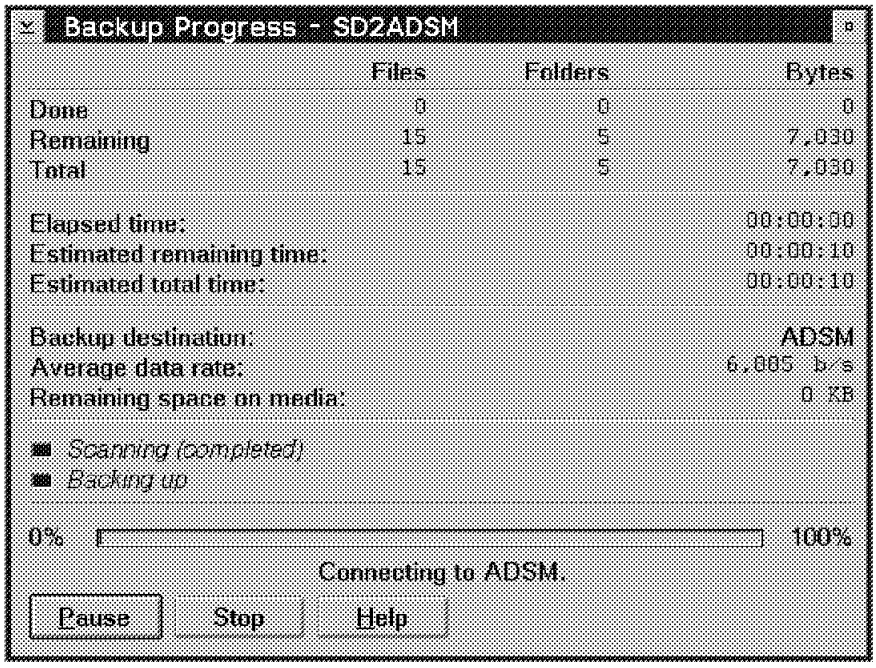


Figure 70. Backup Progress - SD2ADSM Window

Note

If you receive an error the first time you try to back up to ADSM, check that all communication options in DSM.OPT are correct. PTR0324 fixed a known problem but did not make it into the golden OS/2 Warp server code.

The Enter password for ADSM node window is displayed, as shown in Figure 71.

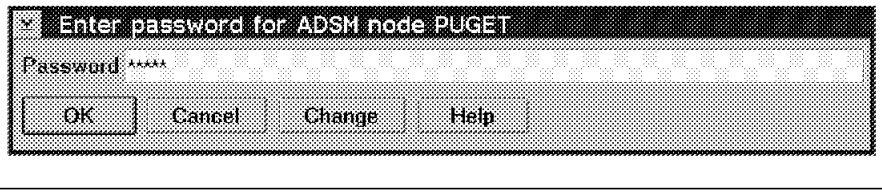


Figure 71. Enter Password for ADSM Node Window

8. Enter the password in the **Password** field.

9. Select the **OK** button.

   The Backup Progress - SD2ADSM window is displayed, as shown in Figure 72 This window disappears at the completion of a successful backup and the Backup Method - SD2ADSM window is redisplayed. Figure 72 shows the Backup Progress - SD2ADSM window after approximately 90% of the selected files have been backed up to ADSM.

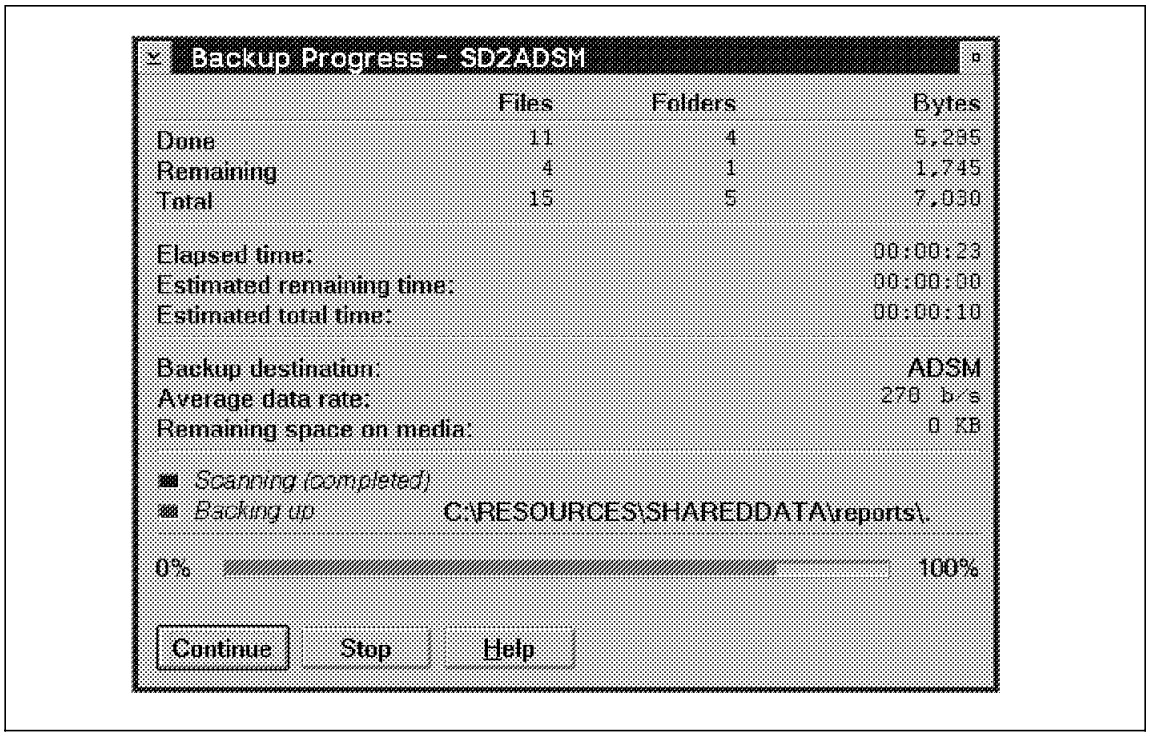


Figure 72. Backup Progress - SD2ADSM Window: 90% of Files Backed Up

The backup creates two ADSM application client file spaces for node PUGET on the ADSM Server, as shown in Figure 73 on page 129. One file space, PSnS_data_311FA1AA, is created for the C:\RESOURCES\SHAREDDATA data and the other, PSnS_indices_311FA1AA, is created for the Warp Server Backup/Restore indexes that are backed up with the shared data.

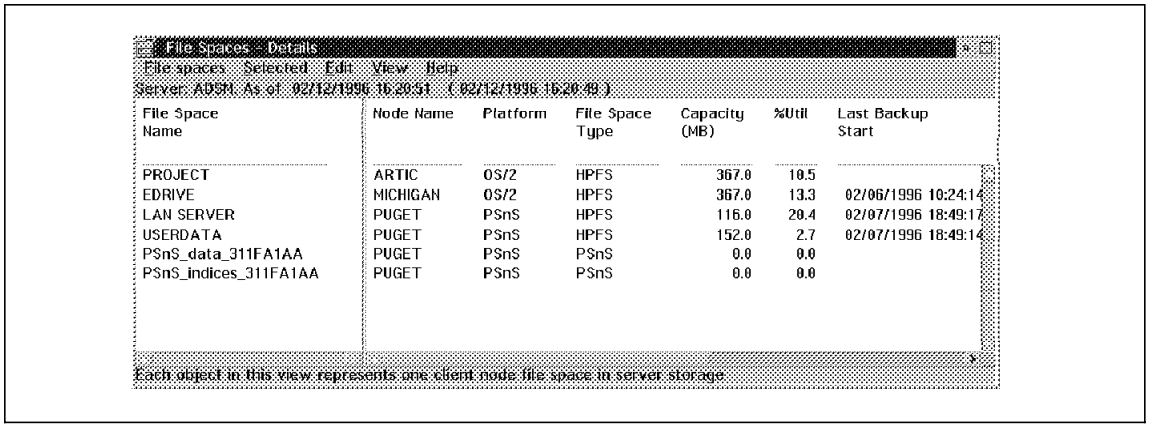


Figure 73. File Spaces - Details Window

If you issue these ADSM administrative commands:

```
query content D:\ADSMSERV\BACK01.DSM node=PUGET filespace=PSnS_data_311FA1AA
query content D:\ADSMSERV\BACK01.DSM node=PUGET filespace=PSnS_indices_311FA1AA
```

you can see the files that ADSM has stored in the two PSnS filespaces. For the output of these query content commands see B.3, “Sample ADSM Filespace Listings for OS/2 Warp Server” on page 170.

10. Double-click at the top left of the window to close the window.

    The Backup Methods Window is displayed.

11. Double-click at the top left of the window to close the window.

    The OS/2 Warp Server Backup/Restore window is displayed.

4.1.6 Check the Backup Log

Check that the backup method SD2ADSM ran correctly.

1. Select the OS/2 Warp Server Backup/Restore window.
2. Select **Tools** from the menu bar.
3. Select **Backup Sets** from the pull-down menu.

   The Backup sets window is displayed.

4. Click with the right-hand mouse button on the **ADSM** icon.

   The ADSM pop-up is displayed, as shown in Figure 74 on page 130.

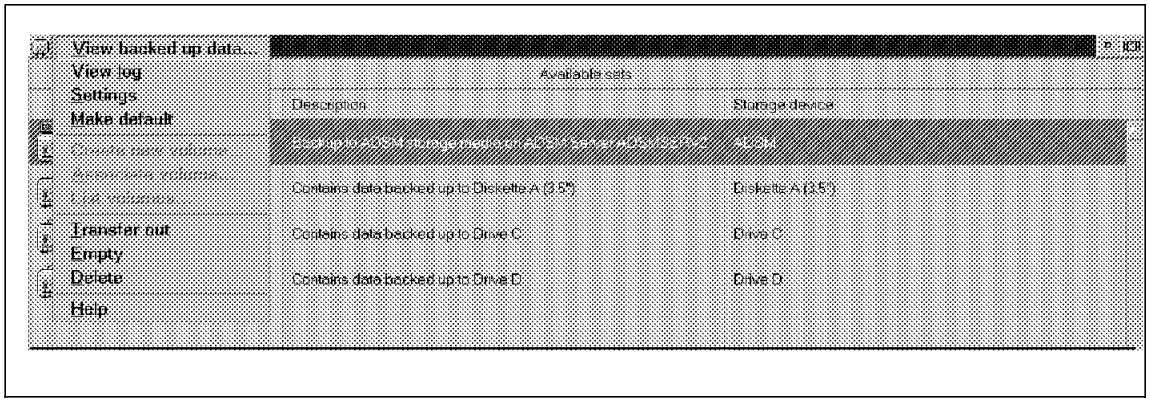


Figure 74. Backup Sets Window

5. Select **View log**.

   The Backup Set Log - ADSM window is displayed, as shown in Figure 75.

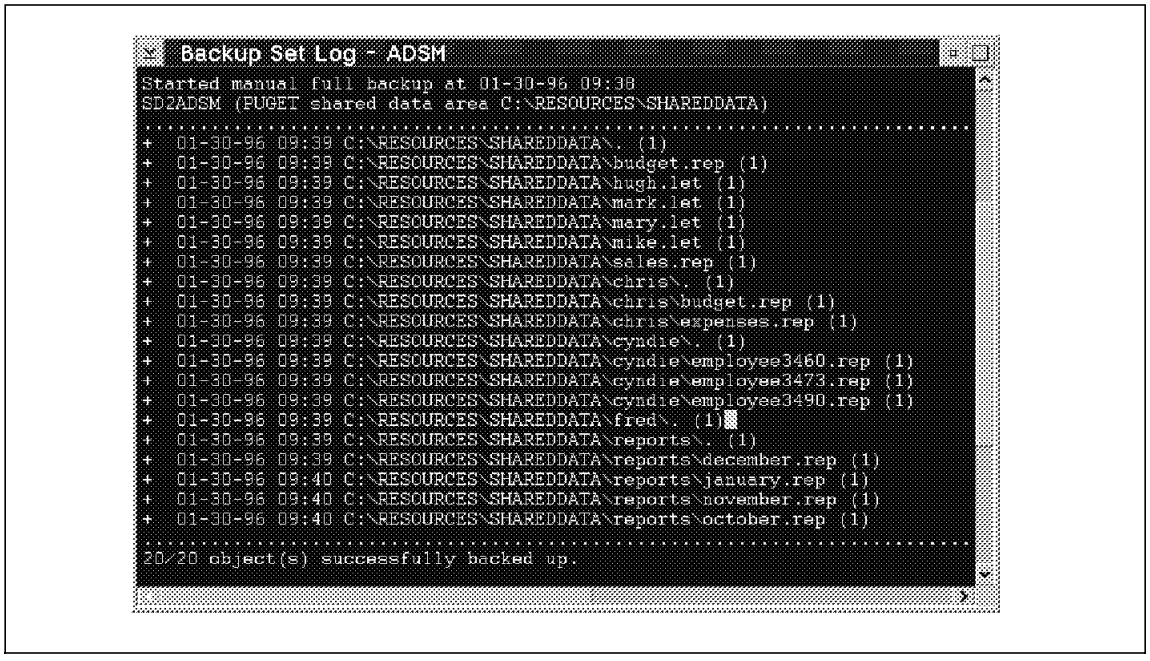


Figure 75. Backup Set Log - ADSM Window after Backup

6. Check that the shared data and subdirectories were successfully backed up.
7. Double-click at the top left of the window to close the window.

The Backup Sets window is displayed.

8. Double click on the Backup sets icon at the top left of the window to close the window.

   The OS/2 Warp Server Backup/Restore window is displayed.

4.2 Restore

Recovery of the shared data area is a three-step process, where you:

1. Define the restore method.
2. Run the restore method.
3. Check the restore log.

4.2.1 Define the Restore Method

Define a restore method called ADSM2SD that restores the C:\RESOURCES\SHAREDDATA shared data area from ADSM media:

1. Select the OS/2 Warp Server Backup/Restore window.
2. Select **Tools** from the menu bar.
3. Select **Restore Methods** from the pull-down menu.

   The Restore Methods window is displayed, as shown in Figure 76.

4. Click with your right-hand mouse button on an unpopulated area of th window.

   The Restore Methods pop-up is displayed, as shown in Figure 76.

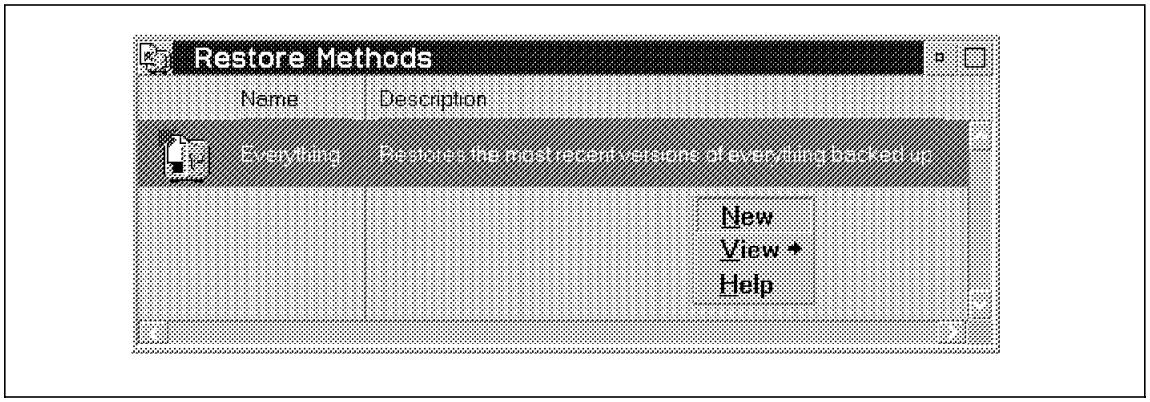


Figure 76. Restore Methods Window before Defining a Restore Method

5. Click on **New**.

The default Restore Method - Untitled window is displayed, as shown in Figure 77 on page 132.

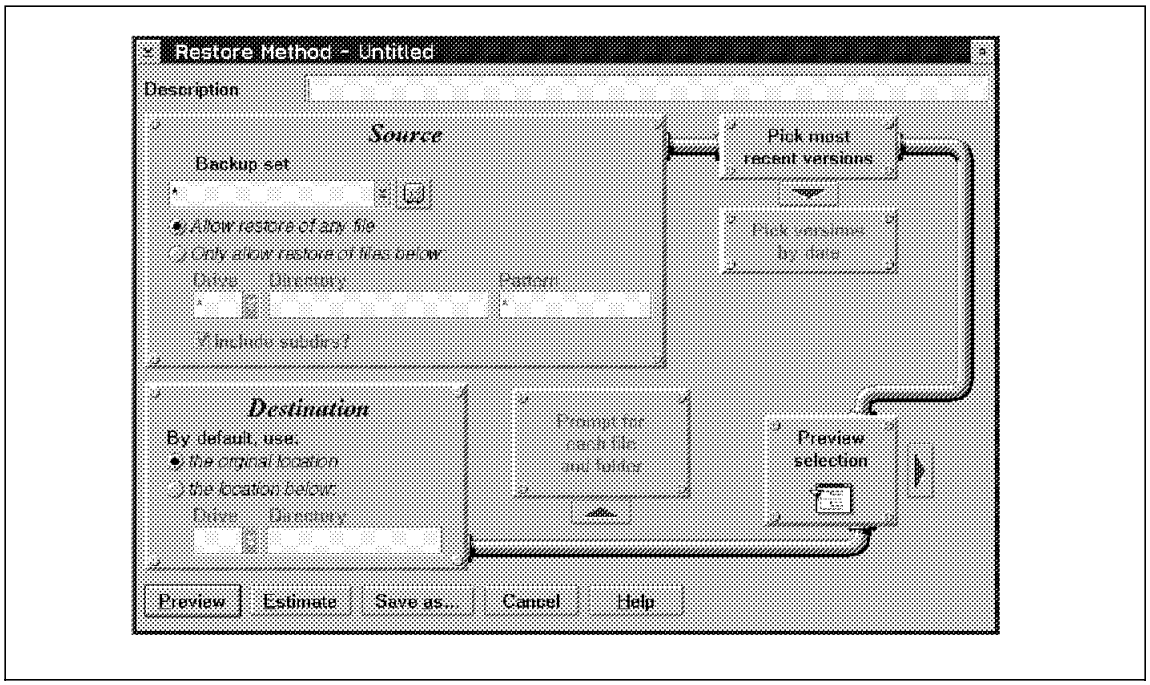


Figure 77. Restore Method - Untitled Window

6. Restore the C:\RESOURCES\SHAREDDATA shared data area to its original location. The information you provide in this step appears in Figure 79 on page 134.
   - Enter PUGET shared data area C:\RESOURCES\SHAREDDATA in the **Description** field.
   - Select ADSM from the **Backup set** list box.
   - Select the Allow restore of any file radio button from the **Source** options.
   - Select the **Pick most recent versions** option.
   - Select the **Preview selection** option.
   - Select the **original location** radio button from the **Destination** options.
7. Select the **Save as** button.

   The Save as window is displayed.
8. Enter ADSM2SD in the **New name** field.

9. Select the **OK** button.

   The Restore Methods window is displayed.

10. Double-click on the Restore Methods icon at the top left of the window.

    The OS/2 Warp Server Backup/Restore window is displayed.

4.2.2 Run the Restore Method

Run the ADSM2SD restore method:

1. Select the OS/2 Warp Server Backup/Restore window.
2. Select **Tools** from the menu bar.
3. Select **Restore Methods** from the pull-down menu.

   The Restore Methods window is displayed, as shown in Figure 78.

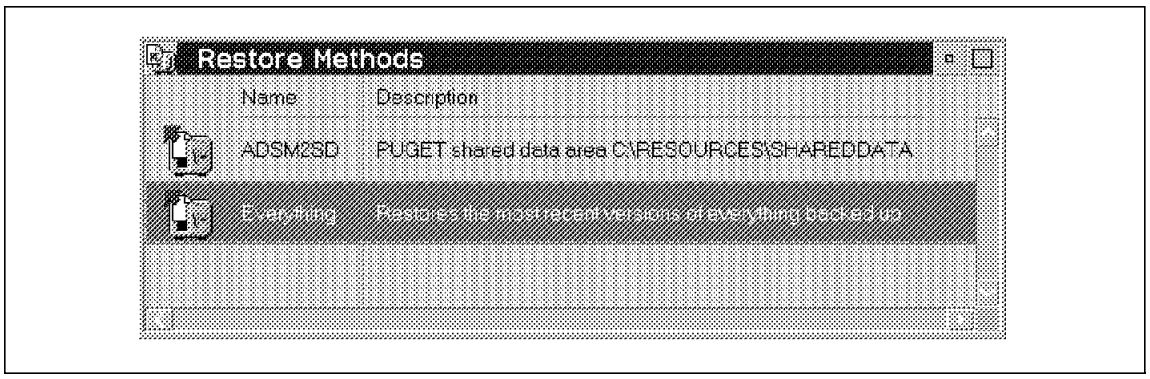


Figure 78. Restore Methods Window after Defining a Restore Method

4. Double-click on the **ADSM2SD** icon.

   The Restore Method - ADSM2SD window is displayed, as shown in Figure 79 on page 134.

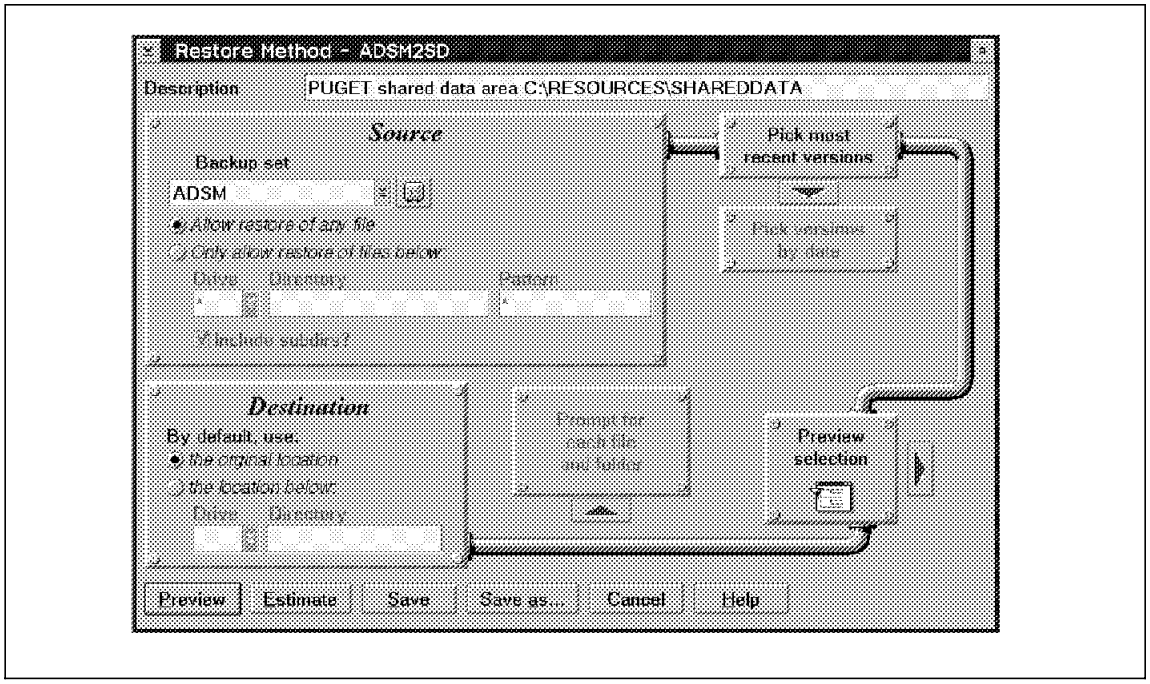


Figure 79. Restore Method - ADSM2SD Window

5. Select the **Preview** button.

   The Restore Preview - ADSM2SD window is displayed, as shown in Figure 80 on page 135.

6. Show the directories to be restored:

   - Click on the + icon next to C icon.
   - Click on the + icon next to the RESOURCES icon.
   - Click on the + icon next to the SHAREDDATA icon.

   The C:\RESOURCES\SHAREDDATA files and subdirectories that are to be restored are marked and displayed, as shown in Figure 80 on page 135.

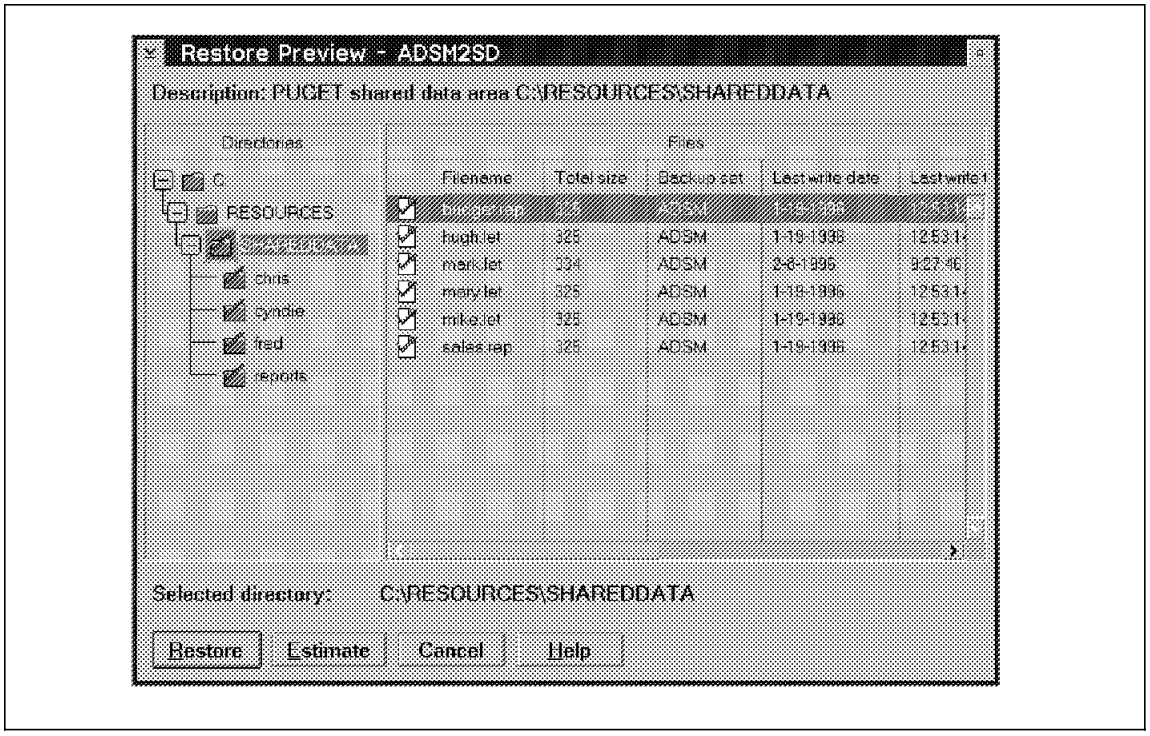


Figure 80. Restore Preview - ADSM2SD Window

7. Select the **Restore** button.

   The Restore Progress - ADSM2SD window is displayed, as shown in Figure 81 on page 136.

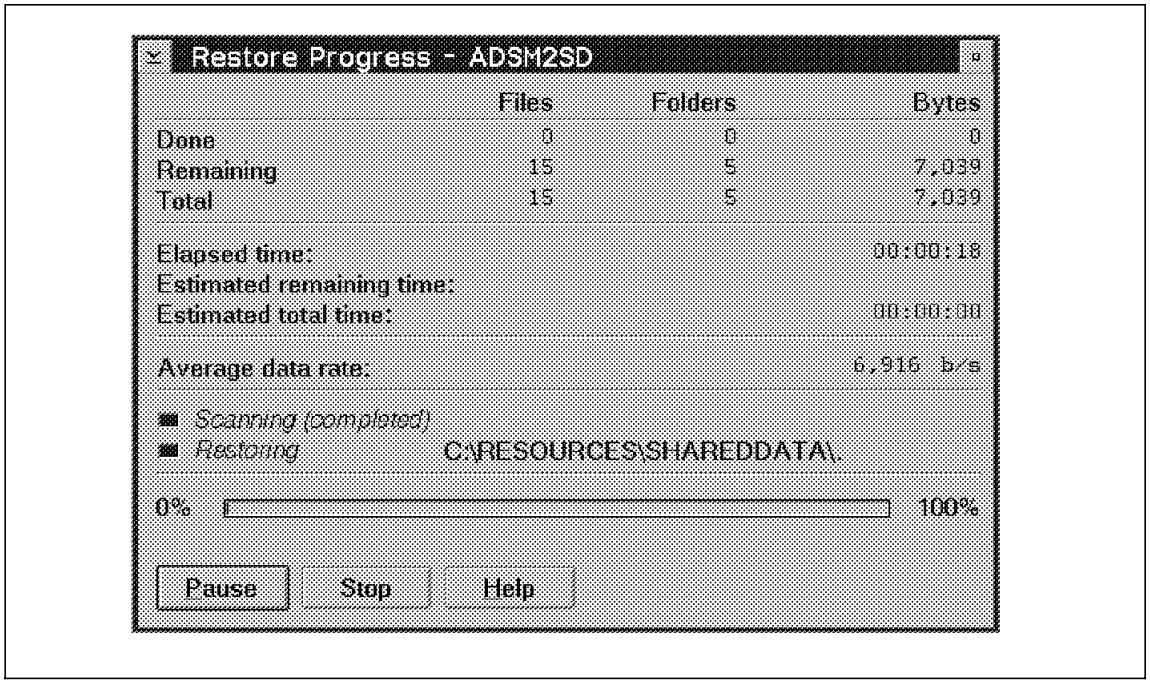


Figure 81. Restore Progress - ADSM2SD Window

The Enter password for ADSM node window is displayed (not shown).

8. Enter the password in the **Password** field.
9. Select the **OK** button.

   The Restore Progress - SD2ADSM window is displayed. This window disappears at the completion of a successful restore.

   The Restore Method - ADSM2SD window is displayed.
10. Double-click at the top left of the window.

    The Restore Methods Window is displayed.
11. Double-click at the top left of the window.

    The OS/2 Warp Server Backup/Restore Window is displayed.

4.2.3 Check the Restore Log

To check that the ADSM2SD restore method ran correctly:

1. Select the OS/2 Warp Server Backup/Restore window.
2. Select **Tools** from the menu bar.
3. Select **Backup Sets** from the pull-down menu.

The Backup Sets window is displayed.

4. Click with the right-hand mouse button on the **ADSM** icon.

   The ADSM pop-up is displayed.

5. Select **View log**.

   The Backup Set Log - ADSM window is displayed, as shown in Figure 82.

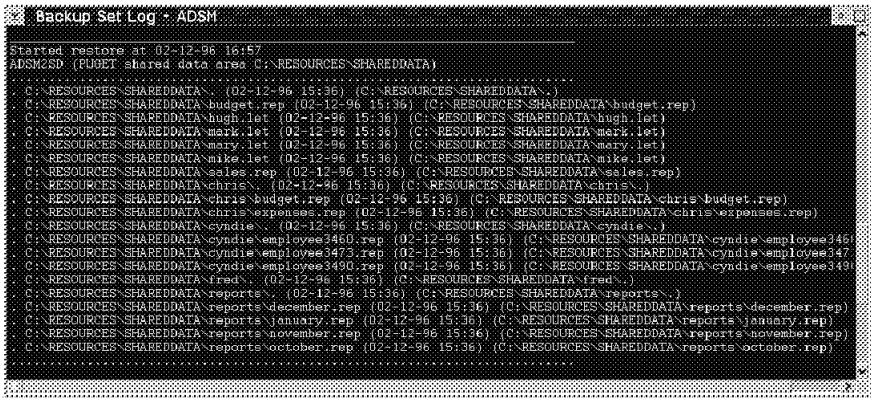


Figure 82. Backup Set Log - ADSM Window after Restore

6. Check that the files and subdirectories were successfully restored.
7. Double-click at the top left of the window.

   The Backup Sets window is displayed.

8. Double-click at the top left of the window.

   The OS/2 Warp Server Backup/Restore window is displayed.

Appendix A. LAN Server Test Environment and Scripts

This appendix contains the LAN Server:

- Test environment ACPs
- Test environment domain information
- Test environment system levels
- Backup scripts
- Directory size limits backup and restore scripts, BACKDLIM and RESTDLIM

A.1 Access Control Profiles

Here is a sample of the ACPs for our LAN Server test environment. We show a subset of the ACPS, in particular, those for the D: drive.

```
Resource  Permissions                          Permissions
-------------------------------------------------------------------------------
D:\IBMLAN\DCDB       ( Audited - FAILURE:ALL )
          *GUESTS:R                            *USERS:R

D:\IBMLAN\DCDB\APPS       ( Audited - FAILURE:ALL )
          *GUESTS:R                            *USERS:R

D:\IBMLAN\DCDB\DATA       ( Audited - FAILURE:ALL )
          *GUESTS:R                            *USERS:R

D:\IBMLAN\DCDB\DEVICES       ( Audited - FAILURE:ALL )
          *GUESTS:R                            *USERS:R

D:\IBMLAN\DCDB\FILES       ( Audited - FAILURE:ALL )
          *GUESTS:R                            *USERS:R

D:\IBMLAN\DCDB\PRINTERS       ( Audited - FAILURE:ALL )
          *GUESTS:R                            *USERS:R

D:\IBMLAN\DCDB\USERS\BARNEY
          BARNEY:RWCXDAP

D:\IBMLAN\DCDB\USERS\BARNEY\BATCH
          BARNEY:RWCXDAP

D:\IBMLAN\DCDB\USERS\FRED
          FRED:RWCXDAP
```

```
D:\IBMLAN\DCDB\USERS\FRED\BATCH
          FRED:RWCXDAP

D:\IBMLAN\DCDB\USERS\WILLMA
          WILLMA:RWCXDAP

D:\IBMLAN\DCDB\USERS\WILLMA\BATCH
          WILLMA:RWCXDAP

D:\IBMLAN\DOSLAN\DOS       ( Audited - FAILURE:ALL )
          *GUESTS:R                          *USERS:R

D:\IBMLAN\DOSLAN\NET       ( Audited - FAILURE:ALL )
          *GUESTS:R                          *USERS:R

D:\IBMLAN\NETPROG       ( Audited - FAILURE:ALL )
          *GUESTS:R                          *USERS:R

D:\IBMLAN\REPL\IMPORT\SCRIPTS
          *ADMINS:RX                         *USERS:RX

D:\RESOURCES\APPS       ( Audited )
          *MAINTENANCE:RWX                   *SUPERVISORS:RWX

D:\RESOURCES\APPS\EMT4PMWP       ( Audited )
          *MAINTENANCE:RWX                   *SUPERVISORS:RWX

D:\RESOURCES\HOMEDIR\BARNEY
          BARNEY:RWCXDAP

D:\RESOURCES\HOMEDIR\FRED
          FRED:RWCXDAP

D:\RESOURCES\HOMEDIR\WILLMA
          WILLMA:RWCXDAP

D:\RESOURCES\SHAREDDATA       ( Audited )
          *MAINTENANCE:R                     *SUPERVISORS:RWCXDAP
          BARNEY:(none)
```

A.2 Domain Definitions

Here are the domain definitions, including user IDs and group definitions, for our LAN Server test environment.

```
TESTDOM

User accounts for \\PUGET
-------------------------------------------------------------------------------

User ID                          BARNEY
Full Name
Comment
User's comment                   Barney Rubble
Parameters
Country code                     000 ( System Default)
Privilege level                  USER
Operator privileges              None
Account active                   Yes
Account expires                  Never

Password last set                01-15-96 09:24am
Password expires                 Never
Password changeable              01-15-96 09:24am
Password required                Yes
User may change password         Yes

Requesters allowed               All
Maximum disk space               1000 KB
Preferred logon server           Domain controller
Logon script
Home directory                   H:\PUGET\D$\RESOURCES\HOMEDIR\BARNEY
Last logon                       Never

Logon hours allowed              All

Group memberships                *MAINTENANCE
                                 *USERS

Logon assignments for BARNEY:
   APPS        X:
   CDROM       I:
   SHARED      S:
   PRINTER1    LPT3
Applications assigned to BARNEY:
   EMT4PMWP    PUBLIC

User ID                          FRED
Full Name
Comment
User's comment                   Fred Flinstone
Parameters
Country code                     000 ( System Default)
```

```
Privilege level                 USER
Operator privileges             None
Account active                  Yes
Account expires                 Never

Password last set               01-15-96 09:23am
Password expires                Never
Password changeable             01-15-96 09:23am
Password required               Yes
User may change password        Yes

Requesters allowed              All
Maximum disk space              1000 KB
Preferred logon server          Domain controller
Logon script
Home directory                  H:\PUGET\D$\RESOURCES\HOMEDIR\FRED
Last logon                      01-15-96 10:35am

Logon hours allowed             All

Group memberships               *MAINTENANCE
                                *USERS

Logon assignments for FRED:
   APPS        X:
   CDROM       I:
   SHARED      S:
   PRINTER1    LPT3
Applications assigned to FRED:
   EMT4PMWP    PUBLIC

User ID                         GUEST
Full Name
Comment
User's comment
Parameters
Country code                    000 ( System Default)
Privilege level                 GUEST
Operator privileges             None
Account active                  Yes
Account expires                 Never

Password last set               01-12-96 01:45pm
Password expires                Never
Password changeable             01-12-96 01:45pm
Password required               No
User may change password        Yes
```

```
Requesters allowed              All
Maximum disk space              Unlimited
Preferred logon server          Domain controller
Logon script
Home directory
Last logon                      Never

Logon hours allowed             All

Group memberships               *GUESTS

Logon assignments for GUEST:
   None
Applications assigned to GUEST:
   None

User ID                         PUGET
Full Name
Comment                         System ID
User's comment                  System ID
Parameters
Country code                    000 ( System Default)
Privilege level                 USER
Operator privileges             None
Account active                  No
Account expires                 01-01-80 12:00am

Password last set               01-12-96 01:45pm
Password expires                Never
Password changeable             01-12-96 01:45pm
Password required               No
User may change password        Yes

Requesters allowed              All
Maximum disk space              Unlimited
Preferred logon server          Domain controller
Logon script
Home directory
Last logon                      Never

Logon hours allowed             All

Group memberships               *SERVERS
                                *USERS

User ID                         USERID
Full Name
Comment
```

```
User's comment                  Default User ID
Parameters
Country code                    000 ( System Default)
Privilege level                 ADMIN
Operator privileges             None
Account active                  Yes
Account expires                 Never

Password last set               12-12-89 09:43am
Password expires                Never
Password changeable             12-12-89 09:43am
Password required               Yes
User may change password        Yes

Requesters allowed              All
Maximum disk space              Unlimited
Preferred logon server          Domain controller
Logon script
Home directory
Last logon                      01-15-96 09:18am

Logon hours allowed             All

Group memberships               *GROUPID
                                *ADMINS

Logon assignments for USERID:
   None
Applications assigned to USERID:
   None

User ID                         WILLMA
Full Name
Comment
User's comment                  Willma Flinstone
Parameters
Country code                    000 ( System Default)
Privilege level                 ADMIN
Operator privileges             None
Account active                  Yes
Account expires                 Never

Password last set               01-15-96 09:26am
Password expires                Never
Password changeable             01-15-96 09:26am
Password required               Yes
User may change password        Yes
```

```
Requesters allowed                All
Maximum disk space                5000 KB
Preferred logon server            Domain controller
Logon script
Home directory                    H:\PUGET\D$\RESOURCES\HOMEDIR\WILLMA
Last logon                        01-15-96 11:57am

Logon hours allowed               All

Group memberships                 *SUPERVISORS
                                  *ADMINS

Logon assignments for WILLMA:
   APPS        X:
   CDROM       I:
   SHARED      S:
   PRINTER1    LPT3
Applications assigned to WILLMA:
   None

*******************************************************************************


Group Accounts for \\PUGET
-------------------------------------------------------------------------------

Group ID     ADMINS
Comment

Members
-------------------------------------------------------------------------------
USERID                   WILLMA

Group ID     GROUPID
Comment      Default Group ID

Members
-------------------------------------------------------------------------------
USERID

Group ID     GUESTS
Comment

Members
-------------------------------------------------------------------------------
GUEST
```

```
Group ID     LOCAL
Comment

Members
--------------------------------------------------------------------------------

Group ID     MAINTENANCE
Comment      Bedrock Maintenance Crew

Members
--------------------------------------------------------------------------------
BARNEY                   FRED

Group ID     SERVERS
Comment      System ID - Server

Members
--------------------------------------------------------------------------------
PUGET

Group ID     SUPERVISORS
Comment      Maintenance Crew Supervisors

Members
--------------------------------------------------------------------------------
WILLMA

Group ID     USERS
Comment

Members
--------------------------------------------------------------------------------
BARNEY                   FRED                     PUGET

********************************************************************************


Alias definitions for \\PUGET
--------------------------------------------------------------------------------

Alias:                          APPS
Description:                    LAN Applications
Server:                         \\PUGET
Path:                           D:\RESOURCES\APPS
When Shared:                    At server startup
Maximum number of users:        No limit
```

```
Alias:                          CDROM
Description:                    CDROM E Drive
Server:                         \\PUGET
Path:                           E:\
When Shared:                    At server startup
Maximum number of users:        No limit

Alias:                          PRINTER1
Description:                    Printer attached to LPT1
Server:                         \\PUGET
Print spooler queue:            IBMNULLP
When Shared:                    At server startup
Maximum number of users:        No limit

Alias:                          SHARED
Description:                    Shared data area
Server:                         \\PUGET
Path:                           D:\RESOURCES\SHAREDDATA
When Shared:                    At server startup
Maximum number of users:        No limit

*******************************************************************************

Public Application definitions for \\PUGET
-------------------------------------------------------------------------------

Details for public application EMT4PMWP:

Remark                           Disk image utility
Type                             OS/2
Interface                        PM
Location                         APPS\EMT4PMWP (remote)
Command line                     EMT4PMWP.EXE
Working Directory                (none)
Prompt for parameters            No
Redirections                     0

*******************************************************************************
```

A.3 System Levels

This section lists the software levels we used in our LAN Server test environment. We issued the OS/2 SYSLEVEL command to obtain the following software level listing:

```
C:\GRPWARE\SYSLEVEL.WCB◄OS/2 WARP Connect without WIN-OS2
Version 3.00     Component ID 562267100
Current CSD level: IP08000
Prior   CSD level: IP08000

C:\OS2\SYSLEVEL.EPW◄IBM OS/2 First Failure Support Technology/2
Version 1.20     Component ID 562119400
Current CSD level: WR00485
Prior   CSD level: WR00480

C:\OS2\INSTALL\SYSLEVEL.GRE◄IBM OS/2 32-bit Graphics Engine
Version 3.01     Component ID 562260100
Type WC
Current CSD level: XR03004
Prior   CSD level: XR03004

C:\OS2\INSTALL\SYSLEVEL.OS2◄IBM OS/2 Base Operating System
Version 3.01     Component ID 562260100
Type WC
Current CSD level: XR03004
Prior   CSD level: XR03004

C:\OS2\INSTALL\SYSLEVEL.SDS◄Distributed SOM Framework
Version 2.01.1     Component ID 96F8647DS
Current CSD level: SM20004
Prior   CSD level: SM20003

C:\OS2\INSTALL\SYSLEVEL.SEM◄SOM Event Management Framework
Version 2.01.1     Component ID 96F8647EM
Current CSD level: SM20004
Prior   CSD level: SM20003

C:\OS2\INSTALL\SYSLEVEL.SIR◄SOMobjects Interface Repository Framework
Version 2.01.1     Component ID 96F8647IR
Current CSD level: SM20004
Prior   CSD level: SM20003

C:\OS2\INSTALL\SYSLEVEL.SRK◄SOM Run-time Kernel
Version 2.01.1     Component ID 96F8647RK
Current CSD level: SM20004
Prior   CSD level: SM20003

C:\OS2\INSTALL\SYSLEVEL.SUC◄SOMobjects Taligent Collection Classes
Version 2.01     Component ID 96F8647UC
Current CSD level: SM20004
Prior   CSD level: SM20003
```

```
C:\OS2\INSTALL\SYSLEVEL.SUT◄SOMobjects Utility Classes
Version 2.01.1     Component ID 96F8647UT
Current CSD level: SM20004
Prior   CSD level: SM20003

D:\IBMCOM\SYSLEVEL.TRP◄IBM OS/2 LAN Adapter and Protocol Support
Version 2.60.2     Component ID 562246103
Current CSD level: WR08000
Prior   CSD level: WR08000

D:\IBMLAN\SYSLEVEL.REQ◄IBM OS/2 LAN Requester
Version 4.00     Component ID 562246101
Current CSD level: IP08000
Prior   CSD level: IP08000

D:\IBMLAN\SYSLEVEL.SRV◄IBM OS/2 LAN Server
Version 4.00     Component ID 562246100
Current CSD level: IP08000
Prior   CSD level: IP08000

D:\IBMLAN\BOOKS\SYSLEVEL.LSR◄IBM OS/2 LAN Server/Requester Product
Version 4.00     Component ID 562246100
Current CSD level: IP08000
Prior   CSD level: IP08000

D:\IBMLAN\DOSLAN\NET\SYSLEVEL.DLS◄IBM DLS - DOS LAN Services
Version 4.00     Component ID 562246102
Current CSD level: IP08000
Prior   CSD level: IP08000

D:\IBMLAN\RPL\IBMCOM\SYSLEVEL.TRP◄IBM OS/2 LAN Adapter and Protocol Support
Version 2.60.2     Component ID 562246103
Current CSD level: WR08000
Prior   CSD level: WR08000

D:\IBMLAN\RPL\IBMLAN\SYSLEVEL.REQ◄IBM OS/2 LAN Requester
Version 4.00     Component ID 562246101
Current CSD level: IP08000
Prior   CSD level: IP08000

D:\IBMLAN\RPL\IBMLAN\SYSLEVEL.SRV◄IBM OS/2 LAN Server
Version 4.00     Component ID 562246100
Current CSD level: IP08000
Prior   CSD level: IP08000

D:\IBMLAN\RPL\IBMLAN\NETPROG\SYSLEVEL.SIR◄SOMobjects Interface Repository Framew
ork
Version 2.01     Component ID 96F8647IR
```

```
Current CSD level: SM20004
Prior   CSD level: SM20003

D:\IBMLAN\RPL\IBMLAN\NETPROG\SYSLEVEL.SRK◄SOM Run-time Kernel
Version 2.01     Component ID 96F8647RK
Current CSD level: SM20004
Prior   CSD level: SM20003

D:\IBMLAN\RPL\IBMLAN\NETPROG\SYSLEVEL.SUC◄SOMobjects Taligent Collection Classes
Version 2.01     Component ID 96F8647UC
Current CSD level: SM20004
Prior   CSD level: SM20003

D:\IBMLAN\RPL\IBMLAN\NETPROG\SYSLEVEL.SUT◄SOMobjects Utility Classes
Version 2.01     Component ID 96F8647UT
Current CSD level: SM20004
Prior   CSD level: SM20003

D:\IBMLAN\RPL\MPTN\SYSLEVEL.MPT◄IBM OS/2 Socket/Multi-Protocol Transport Service
s
Version 1.00     Component ID 562246103
Current CSD level: WR08000
Prior   CSD level: WR08000

D:\IBMLAN\RPL\MUGLIB\SYSLEVEL.MUG◄IBM OS/2 User Profile Management
Version 4.00     Component ID 562246104
Current CSD level: WR08000
Prior   CSD level: WR08000

D:\IBMLAN\RPL\MUGLIB\SYSLEVEL.UPE◄IBM OS/2 User Profile Management - Extended
Version 4.00     Component ID 562246105
Current CSD level: IP08000
Prior   CSD level: IP08000

D:\MPTN\SYSLEVEL.MPT◄IBM OS/2 Socket/Multi-Protocol Transport Services
Version 1.00     Component ID 562246103
Current CSD level: WR08000
Prior   CSD level: WR08000

D:\MUGLIB\SYSLEVEL.MUG◄IBM OS/2 User Profile Management
Version 4.00     Component ID 562246104
Current CSD level: WR08000
Prior   CSD level: WR08000

D:\MUGLIB\SYSLEVEL.UPE◄IBM OS/2 User Profile Management - Extended
Version 4.00     Component ID 562246105
Current CSD level: IP08000
Prior   CSD level: IP08000
```

ADSM software levels do not get displayed using the syslevel command. An ADSM dsmc query file command (or similar command) displays the current ADSM client and server levels. Here are the ADSM software levels:

- ADSM OS/2 backup/archive client, Version 2 Release 1 Level 0.2
- ADSM OS/2 administrative client, Version 2 Release 1 Level 0.2
- ADSM for OS/2 server, Version 1 Release 2 Level 0.9/1.9.

A.4 LAN Server Backup Scripts

This appendix shows the three REXX command scripts that correspond to scenarios in 2.7.1.1, “REXX Command Scripts” on page 73:

- LAN Server 4.0 Entry
- LAN Server V4.0 Advanced with 386 HPFS drive partitions
- LAN Server V4.0 Advanced with 386 HPFS drive partitions and directory size limits

The scripts are also included on the diskette in the back of this book.

A.4.1 REXX EXEC for LAN Server V4.0 Entry, LANSRVE.CMD

```
/* REXX command file for LAN Server V4.0 Entry.                          */
/*                                                                       */
/* To do a BACKACC for LAN Server Entry.                                 */
/* Record messages in BACKACC.LOG and send a message to the LAN administrator*/
/* if BACKACC fails.                                                     */
/*                                                                       */
/* Update the drive letter for logfile= and -DOMAIN= to where OS/2 LAN Server*/
/* is installed.  Change MICHIGAN to your LAN Administrators workstation name*/
/* and update TESTSRV to your server name on the NET SEND command.      */
/* Update -PASSWORD= for the ADSM client node on the DSMC INCREMENTAL    */
/* commands if you want to run in unattended mode.                  .    */
/*                                                                       */
/* You may want to remove the -QUIET parameter on the DSMC INCREMENTAL   */
/* command for the initial backup test to see all the messages on the ADSM   */
/* client scheduler window.  Then add -QUIET back afterwards.            */
/*                                                                       */
/* A workstation name should be used instead of a user name that may not be  */
/* logged on and the NET SEND would fail.  The message is logged into    */
/* d:\IBMLAN\LOGS\MESSAGES.LOG if the MESSENGER service is started.      */
/* The LAN Administrator can check this MESSAGES.LOG for past BACKACC    */
/* failure messages in case a message popup window was not noticed.      */

logfile = 'D:\IBMLAN\LOGS\BACKACC.LOG'
ADDRESS CMD 'BACKACC /V 2>'logfile
```

```
saverc = RC
/*                                                                  */
/* If BACKACC executes successfully, then add the D drive where OS/2 LAN     */
/* Server is installed to the domain of drives in DSM.OPT to be backed up.   */
/*                                                                  */
/* If BACKACC fails, then send a message to the LAN Administrator and don't  */
/* add the D drive to the incremental backups.  This is to prevent ADSM      */
/* from creating new backup versions for potentially incomplete backup copies*/
/* of NETACC.BKP and NETAUD.BKP.                                    */
/*                                                                  */
IF RC <> 0 THEN  /* check for BACKACC error. */
  DO
    CALL WriteLog logfile, saverc
    NET SEND MICHIGAN BACKACC FAILED ON SERVER TESTSRV. CHECK BACKACC.LOG.
    'DSMC INCREMENTAL -PASSWORD=PUGET -QUIET -TAPEPROMPT=NO'
  END
ELSE             /* BACKACC executed successfully. */
  DO
    CALL WriteLog logfile, saverc
    'DSMC INCREMENTAL -DOMAIN="D:" -PASSWORD=PUGET -QUIET -TAPEPROMPT=NO'
  END

EXIT

/* Write a message with the date and time BACKACC executed and the resulting */
/* return code to BACKACC.LOG.                                      */
/*                                                                  */

WriteLog:
parse arg logfile, saverc

dateis = DATE(S)
datemsg = SUBSTR(dateis,1,4)]]"-"]]SUBSTR(dateis,5,2)]]"-"]]SUBSTR(dateis,7,2)
logtext = 'BACKACC executed with a RC ='
message = datemsg TIME(N) logtext saverc]]'.'
CALL LINEOUT logfile, message

RETURN
```

A.4.2 REXX EXEC for LAN Server V4.0 Advanced with 386 HPFS, LANSRVA.CMD

```
/* REXX command file for LAN Server V4.0 Advanced with 386 HPFS drives.      */
/*                                                                  */
/* To do a BACKACC for LAN Server Advanced with 386 HPFS.  Backup ACPs       */
/* for each drive partition that is 386 HPFS.                       */
/* By default a ACLBAKd.ACL file is used, where d is the drive letter of the */
/* drive in which ACPs have been backed up.  This file is stored in         */
```

```
/* d:\IBMLAN\ACCOUNTS where OS/2 LAN Server is installed.                    */
/* Record messages in a BACKACCx.LOG for each drive and send a message to    */
/* the LAN administrator if a BACKACC fails.                                 */
/*                                                                           */
/* Update the -DOMAIN= parameter on the DSMC INCREMENTAL commands to where   */
/* OS/2 LAN Server is installed.                                             */
/* Change MICHIGAN to your LAN Administrators workstation name and update    */
/* TESTSRV to your server name on the NET SEND commands.                     */
/* Update -PASSWORD= for the ADSM client node on the DSMC INCREMENTAL        */
/* commands if you want to run in unattended mode.                           */
/*                                                                           */
/* You may want to remove the -QUIET parameter on the DSMC INCREMENTAL       */
/* commands for the initial backup test to see all the messages on the ADSM  */
/* client scheduler window.  Then add -QUIET back afterwards.                */
/*                                                                           */
/* A workstation name should be used instead of a user name that may not be  */
/* logged on and the NET SEND would fail.  The message is logged into        */
/* d:\IBMLAN\LOGS\MESSAGES.LOG if the MESSENGER service is started.          */
/* The LAN Administrator can check this MESSAGES.LOG for past BACKACC        */
/* failure messages in case a message popup window was not noticed.          */
/*                                                                           */
/* Update lan_drive = variable to where OS/2 LAN Server is installed.        */

CALL RxFuncAdd 'SysLoadFuncs', 'RexxUtil', 'SysLoadFuncs'
CALL SysLoadFuncs

lan_drive = 'D:\'

BACKACC_RC = 0

dMap = SysDriveMap('C:', 'LOCAL')
i = 1
DO WHILE (WORD(dMap,i) <> '')
  drive = SUBSTR(WORD(dMap, i),1,1)
  logfile = lan_drive]]'IBMLAN\LOGS\BACKACC']]drive]]'.LOG'
  ADDRESS CMD 'BACKACC ']]drive]]':\ /S /V 2>'logfile
  rcb = RC
  CALL WriteLog logfile, rcb
  IF rcb <> 0 THEN  /* check for BACKACC error. */
    BACKACC_RC = rcb
  i = i + 1
END

/*                                                                           */
/* If BACKACC executes successfully, then add the LAN Server drive to the    */
/* domain of drives in DSM.OPT to be incrementally backed up.                */
/*                                                                           */
/* If BACKACC fails, then send a message to the LAN Administrator            */
```

```
/* and don't add the LAN Server drive to incremental backups.               */
/* This is to prevent ADSM from creating new backup versions for potentially */
/* incomplete backup copies of NETACC.BKP, NETAUD.BKP and ACLBAKd.ACL.      */
/*                                                                          */

IF BACKACC_RC <> 0 THEN  /* check for BACKACC error. */
  DO
    NET SEND MICHIGAN BACKACC FAILED ON SERVER TESTSRV. CHECK BACKACCx.LOG.
    'DSMC INCREMENTAL -PASSWORD=PUGET -QUIET -TAPEPROMPT=NO'
  END
ELSE             /* BACKACC executed successfully. */
  'DSMC INCREMENTAL -DOMAIN="D:" -PASSWORD=PUGET -QUIET -TAPEPROMPT=NO'

EXIT

/* Write a message with the date and time BACKACC executed and the resulting */
/* return code to BACKACCx.LOG.                                             */
/*                                                                          */

WriteLog:
parse arg logfile, saverc

dateis = DATE(S)
datemsg = SUBSTR(dateis,1,4)]]"-"]]SUBSTR(dateis,5,2)]]"-"]]SUBSTR(dateis,7,2)
logtext = 'BACKACC executed with a RC ='
message = datemsg TIME(N) logtext saverc]]'.'
CALL LINEOUT logfile, message

RETURN
```

A.4.3 REXX EXEC for LAN Server V4.0 Advanced with 386 HPFS and Directory Size Limits, LANSRVAL.CMD

```
/* REXX command file for LAN Server V4.0 Advanced with 386 HPFS drives that  */
/* have directory limits.                                                   */
/*                                                                          */
/* To do a BACKACC for LAN Server Advanced with 386 HPFS.  Backup ACPs       */
/* for each drive partition that is 386 HPFS.                               */
/* By default a ACLBAKd.ACL file is used, where d is the drive letter of the */
/* drive in which ACPs have been backed up.  This file is stored in         */
/* d:\IBMLAN\ACCOUNTS where OS/2 LAN Server is installed.                   */
/* Record messages in a BACKACCx.LOG for each drive and send a message to   */
/* the LAN administrator if a BACKACC fails.                                */
/*                                                                          */
/* To do a BACKDLIM to backup directory limits on 386 HPFS drives.          */
/* By default a BACKDLMd.BKP file is used, where d is the drive letter of the*/
/* drive in which directory limits have been backed up.  This file is stored */
/* in d:\IBMLAN\ACCOUNTS where OS/2 LAN Server is installed.                 */
```

```
/* Record messages in BACKDLMx.LOG for each drive and send a message to     */
/* the LAN administrator if a BACKDLIM fails.                               */
/*                                                                          */
/* Update the -DOMAIN= parameter on the DSMC INCREMENTAL command to where   */
/* OS/2 LAN Server is installed.                                            */
/* Change MICHIGAN to your LAN Administrators workstation name and update   */
/* TESTSRV to your server name on the NET SEND commands.                    */
/* Update -PASSWORD= for the ADSM client node on the DSMC INCREMENTAL       */
/* commands if you want to run in unattended mode.                          */
/*                                                                          */
/* You may want to remove the -QUIET parameter on the DSMC INCREMENTAL      */
/* commands for the initial backup test to see all the messages on the ADSM */
/* client scheduler window.  Then add -QUIET back afterwards.               */
/*                                                                          */
/* A workstation name should be used instead of a user name that may not be */
/* logged on and the NET SEND would fail.  The message is logged into       */
/* d:\IBMLAN\LOGS\MESSAGES.LOG if the MESSENGER service is started.         */
/* The LAN Administrator can check this MESSAGES.LOG for past BACKACC       */
/* failure messages in case a message popup window was not noticed.         */
/*                                                                          */
/* Update lan_drive = variable to where OS/2 LAN Server is installed.       */
/* Update dlimpath = variable to the directory path where the BACKDLIM      */
/* executable file is.                                                      */

lan_drive = 'D:\'
dlimpath = 'D:\UTILS\'
dlimout = lan_drive]]'IBMLAN\ACCOUNTS\'


BACKACC_RC = 0
BACKDLIM_RC = 0

dMap = SysDriveMap('C:', 'LOCAL')
i = 1
DO WHILE (WORD(dMap,i) <> '')
  drive = SUBSTR(WORD(dMap, i),1,1)

/* BACKACC for each 386 HPFS drive partition.                               */
/*                                                                          */
  logfile = lan_drive]]'IBMLAN\LOGS\BACKACC']]drive]]'.LOG'
  ADDRESS CMD 'BACKACC ']]drive]]':\ /S /V 2>'logfile
  rcb = RC
  CALL WriteLog logfile, rcb
  IF rcb <> 0 THEN  /* check for BACKACC error. */
    BACKACC_RC = rcb

/* BACKDLIM for each 386 HPFS drive partition with directory limits.        */
/*                                                                          */
```

```
  logfile = lan_drive]]'IBMLAN\LOGS\BACKDLIM']]drive]]'.LOG'
  ADDRESS CMD dlimpath]]'BACKDLIM ']]dlimout]]'BACKDLM']]drive]]'.BKP ',
  ]]drive]]':\ 1>'logfile
  rcb = RC
  CALL WriteLog logfile, rcb
  IF rcb <> 0 THEN  /* check for BACKACC error. */
    BACKDLIM_RC = rcb
  i = i + 1
END

/*                                                                  */
/* If BACKACC and BACKDLIM executes successfully, then add the LAN Server    */
/* drive to the domain of drives in DSM.OPT to be incrementally backed up.   */
/*                                                                  */

/* If BACKACC or BACKDLIM fails, then send a message to the LAN Administrator*/
/* and don't add the LAN Server drive to incremental backups.               */
/* This is to prevent ADSM from creating new backup versions for potentially */
/* incomplete backup copies of NETACC.BKP, NETAUD.BKP, ACLBAKd.ACL and       */
/* BACKDLMd.BKP.                                                    */
/*                                                                  */
/* Check for BACKACC or BACKDLIM errors.                            */
IF (BACKACC_RC <> 0 ] BACKDLIM_RC <> 0) THEN
  DO
    IF BACKACC_RC <> 0 THEN
      NET SEND MICHIGAN BACKACC FAILED ON SERVER TESTSRV. CHECK BACKACCx.LOG.
    IF BACKDLIM_RC <> 0 THEN
      NET SEND MICHIGAN BACKDLIM FAILED ON SERVER TESTSRV. CHECK BACKDLMx.LOG.
    'DSMC INCREMENTAL -PASSWORD=PUGET -QUIET -TAPEPROMPT=NO'
  END
ELSE             /* BACKACC and BACKDLIM executed successfully. */
  'DSMC INCREMENTAL -DOMAIN="D:" -PASSWORD=PUGET -QUIET -TAPEPROMPT=NO'

EXIT

/* Write a message with the date and time BACKACC or BACKDLIM executed       */
/* and the resulting return code to BACKACCx.LOG or BACKDLMx.LOG.            */
/*                                                                  */

WriteLog:
parse arg logfile, saverc, command

dateis = DATE(S)
datemsg = SUBSTR(dateis,1,4)]]"-"]]SUBSTR(dateis,5,2)]]"-"]]SUBSTR(dateis,7,2)
logtext = command]]' executed with a RC ='
message = datemsg TIME(N) logtext saverc]]'.'
CALL LINEOUT logfile, message
```

```
RETURN
```

A.5 LAN Server Directory Size Limits Backup and Restore

This section includes the LAN Server Directory Size Limits Backup and Restore programs written by Wim Fabri of IBM Belgium, as discussed in 2.4, “LAN Server Advanced Directory Size Limits” on page 63. Some sample directory size limits backup output is also included.

A.5.1 Directory Size Limits Backup Program, BACKDLIM.C

This section details the the BACKDLIM utility C code used to query the LAN Server Advanced directory size limits. It calls the LAN Server Net32DASDEnum API. (Alternatively the NetDASDEnum API could be used.) The Net32DASDEnum API returns a list of directories that have had directory size limits applied to them and other related information, such as the limit applied to each directory, the space used, and the alert and incremental threshold values for each directory. BACKDLIM then creates an output file detailing this information.

```
  /* BACKDLIM.C */
  /* 21/01/96        */


#include <stdio.h>
#define INCL_DOSMISC
#include <os2.h>
#define PURE_32
#include <netcons.h>
#include <neterr.h>
#include <dasd.h>


struct dasd_info_0 * buf;
unsigned short buflen;
unsigned long ulEntriesReturned;
unsigned long ulEntriesAvail;
unsigned short rc,rc2;

main(int argc, char *argv·“, char *envp·“)
{
   long i;


   FILE * file;
   char * path;
   char msgbuf·3000“;
```

```
   unsigned long msglength;


   if (argc<2) {
      printf("usage : backdlim outfile ·path"\n");
      exit(0);
   } /* endif */

   if (argc==3) {
      path=argv·2";
   } else {
      path=NULL;
   } /* endif */

   buf=malloc(64*1024-1);
   buflen=64*1024-1;
   rc=Net32DASDEnum(NULL,path,1,0,buf,buflen,&ulEntriesReturned,&ulEntriesAvail);
   if (rc) {
      rc2=DosGetMessage(NULL,0,msgbuf,sizeof(msgbuf),rc,"net.msg",&msglength);
      printf("%s\n",msgbuf);
      rc2=DosGetMessage(NULL,0,msgbuf,sizeof(msgbuf),rc,"neth.msg",&msglength);
      printf("%s\n",msgbuf);
   } else {
      if (ulEntriesReturned==0) {
         printf("No directory limits defined for this path,
                 output file will be empty\n");
      } /* endif */
      file=fopen((const char *)argv·1",w");
      for (i=0;i<ulEntriesReturned ; i++) {
         fprintf(file,"\"%s\"",buf·i".d0_resource_name);
         fprintf(file," %ld",buf·i".d0_max);
         fprintf(file," %d",buf·i".d0_thresh);
         fprintf(file," %d\n",buf·i".d0_delta);
      } /* endfor */

      fclose(file);
   } /* endif */

}
```

A.5.2 Directory Size Limits Backup Program, BACKDLIM: Sample Output File

This section provides a sample output file created by the BACKDLIM utility. Each LAN Server Advanced directory that has a directory size limit is listed on a separate line. Each entry includes the:

- Full path and directory name

- Maximum allowed disk space specified for the directory (in KB)
- Initial alert threshold. This specifies the point at which an alert should be generated indicating that disk space for the specified directory is becoming full. This is recorded as a percentage of the total directory limit space; for example, 80 would indicate that an initial alert should be generated when the directory becomes 80% full.
- Incremental alert threshold. This specifies the point at which further alerts should be generated indicating that the disk space for the specified directory is still increasing. This is recorded as a percentage of the total directory limit space.

```
"D:\resources\shareddata\BARNEY" 20480 90 1
"D:\resources\shareddata\BETTY" 20480 90 1
"D:\resources\shareddata\CHRIS" 20480 90 1
"D:\resources\shareddata\CYNDIE" 20480 90 1
"D:\resources\shareddata\FRED" 20480 90 1
"D:\resources\shareddata\reports\jan" 10240 10 0
"D:\resources\shareddata\reports\feb" 10240 10 0
"D:\resources\shareddata\reports\mar" 10240 10 0
"D:\resources\shareddata\sales\letters" 51200 60 10
"D:\resources\shareddata\WILLMA" 20480 90 1
```

A.5.3 Directory Size Limits Restore Program, RESTDLIM.C

This section includes the RESTDLIM utility C code used to restore LAN Server Advanced directory size limits that were backed up with the BACKDLIM utility. It interrogates the output file created by the BACKDLIM utility to determine the directories that have had directory size limits applied to them, the size limititation specified, and the alert and incremental threshold values. It calls the LAN Server Net32DASDAdd API. (Alternatively the NetDASDAdd API could be used.) The Net32DASDAdd API invokes the directory size limit function, which places a limit on the amount of disk space that can be used within each specified directory tree.

Note

This utility will add directory size limits only to those directories that do not have any current limits associated with them. This is the case if a directory has been deleted and you have restored it from an ADSM backup. The function of this utility could be extended to include the detection and deletion of existing directory size limits through the implementation of other LAN Server APIs.

```
  /* RESTDLIM.C */
  /* 21/01/96        */


#include <stdio.h>
#define INCL_DOSMISC
#include <os2.h>
#define PURE_32
#include <netcons.h>
#include <neterr.h>
#include <dasd.h>


struct dasd_info_0 info_buf;
struct dasd_init_0 init_buf;

main(int argc, char *argv·“, char *envp·“)
{
   unsigned short rc,rc2;
   FILE * file;
   char line·1000“;
   char path·100“;
   char msgbuf·3000“;
   unsigned long msglength;
   unsigned long max;
   unsigned char thresh;
   unsigned char delta;
   char max_string·20“;
   char thresh_string·10“;
   char delta_string·10“;

   if (argc<2) {
      printf(”usage : restdlim infile\n”);
      exit(0);
   } /* endif */

   file=fopen((const char *)argv·1“,”r”);
   if (file==NULL) {
      printf(”Could not open file %s”,argv·1“);
      exit(1);
   } /* endif */
   while (fgets(line,1000,file)!=NULL) {
      sscanf(line,”\”%·–\”“\” %s %s %s”,path,max_string,thresh_string,delta_string);
      info_buf.d0_resource_name=path;
      info_buf.d0_max=atoi(max_string);
      info_buf.d0_flag=DASD_VALIDATE_LIMIT_OFF;
      info_buf.d0_thresh=atoi(thresh_string);
```

```
      info_buf.dO_delta=atoi(delta_string);
retry:rc=Net32DASDAdd(NULL,0,&info_buf,sizeof(info_buf));
      if (rc) {
         if (rc==NERR_DASDNotInstalled) {
            printf("not enabled,enabling\n");
            init_buf.iO_CtlFlag=DASD_CTL_INSTALL;
            init_buf.iO_Drive=path·0";
            rc=Net32DASDCtl(NULL,0,&init_buf,sizeof(init_buf));
            if (rc) {
               rc2=DosGetMessage(NULL,0,msgbuf,sizeof(msgbuf),
                                    rc,"net.msg",&msglength);
               printf("%s\n",msgbuf);
               rc2=DosGetMessage(NULL,0,msgbuf,sizeof(msgbuf),
                                   rc,"neth.msg",&msglength);
               printf("%s\n",msgbuf);
               exit(1);
            } /* endif */
            goto retry;
         } else {
            rc2=DosGetMessage(NULL,0,msgbuf,sizeof(msgbuf),
                                rc,"net.msg",&msglength);
            printf("%s\n",msgbuf);
            rc2=DosGetMessage(NULL,0,msgbuf,sizeof(msgbuf),
                               rc,"neth.msg",&msglength);
            printf("%s\n",msgbuf);
            exit(1);
         } /* endif */
      } /* endif */
   } /* endwhile */


}
```

Appendix B. OS/2 Warp Server

This appendix contains the following sections:

- OS/2 Warp Server storage device support
- OS/2 Warp Server DSM.OPT options file
- Sample ADSM filespace listings for Warp Server

B.1 OS/2 Warp Server Device Support

This section lists the SCSI II tape drives supported by OS/2 Warp Server Backup/Restore. This list was accurate at the time the book was written. Since then, support for additional drives may have been added. If you are using OS/2 Warp Server and are interested in using a tape drive that is not mentioned in this list, contact your IBM representative to determine whether the device is supported.

Note

Although OS/2 Warp Server Backup/Restore uses the same tape device drivers as ADSM, it supports only manual tape drives, whereas ADSM supports both manual and automated drives and libraries.

If you require automated backup of data to multiple tapes, base your backup strategy on ADSM rather than OS/2 Warp Server Backup/Restore.

Table 14, Table 15 on page 164, Table 16 on page 165, and Table 17 on page 166 list the locally attached tape drives that OS/2 Warp Server Backup/Restore supports. **Note:** The OS/2 Warp Server Backup/Restore tape device driver supports SCSI II hardware only.

Table 14 (Page 1 of 2). OS/2 Warp Server Backup/Restore 8 mm Tape Drives

Device Name	Supported Formats	Estimated Capacity
ANDATACO ENCORE 8205	8200, 8200C	2.3 GB*
ANDATACO ENCORE 8505	8200, 8200C, 8500, 8500C	5.0 GB*
CYBERNETICS CY8205	8200, 8200C	2.3 GB*

Table 14 (Page 2 of 2). OS/2 Warp Server Backup/Restore 8 mm Tape Drives

Device Name	Supported Formats	Estimated Capacity
CYBERNETICS CY8500	8200, 8500	5.0 GB
CYBERNETICS CY8505	8200, 8200C, 8500, 8500C	5.0 GB
DYNATEK HSB 2300	8200, 8200C	2.3 GB*
DYNATEK HSB 10.0	8200, 8200C, 8500, 8500C	5.0 GB*
DYNATEK HSB 5000	8200, 8200C, 8500, 8500C	5.0 GB*
EXABYTE 8200	8200	2.3 GB
EXABYTE 8205	8200, 8200C	2.3 GB*
EXABYTE 8205XL	8200, 8200C	3.5 GB* w/ XL tape
EXABYTE 8500	8200, 8500	5.0 GB
EXABYTE 8500C	8200, 8200C, 8500, 8500C	5.0 GB*
EXABYTE 8505	8200, 8200C, 8500, 8500C	5.0 GB*
EXABYTE 8505XL	8200, 8200C, 8500, 8500C	7.0 GB* w/ XL tape
IBM 3532-023	8200	2.3 GB
IBM 3445-001	8200, 8200C, 8500, 8500C	5.0 GB*
SUN 8505XL	8200, 8200C, 8500, 8500C	7.0 GB* w/ XL tape
TTI CTS-8000H	8500, 8500C	5.0 GB*
TTI CTS-8519H	8200, 8200C, 8500, 8500C	5.0 GB* **

Note: :.

* Greater capacity might be achieved with compression

** OS/2 Warp Server Backup/Restore supports mirrored mode operations only.

Table 15 (Page 1 of 2). OS/2 Warp Server Backup/Restore 4 mm Tape Drives

Device Name	Supported Formats	Estimated Capacity
HP 35470A	DDS1	2.0 GB

Table 15 (Page 2 of 2). OS/2 Warp Server Backup/Restore 4 mm Tape Drives

Device Name	Supported Formats	Estimated Capacity
HP 35480A	DDS1, DDS1C	2.0 GB*
HP C1553A	DDS1, DDS1C, DDS2, DDS2C	4.0 GB*
HP Jetstore 2000e	DDS1	2.0 GB
HP Jetstore 5000e	DDS1, DDS1C	2.0 GB*
IBM 3440-001	DDS1, DDS1C	2.0 GB*
IBM (74G8632/8191339)	DDS1, DDS1C, DDS2, DDS2C	4.0 GB*
IBM (74G8631/8191359)	DDS1, DDS1C, DDS2, DDS2C	4.0 GB*
IBM 4326NP/RP	DDS1, DDS1C, DDS2, DDS2C	4.0 GB*
WANGDAT 3300DX	DDS1, DDS2	4.0 GB
WANGDAT 3400DX	DDS1, DDS1C, DDS2, DDS2C	4.0 GB*
SONY SDT5000	DDS1, DDS1C, DDS2, DDS2C	4.0 GB*

Note:

* Greater capacity might be achieved with compression.

Table 16. OS/2 Warp Server Backup/Restore QIC Tape Drives

Device Name	Supported Formats	Estimated Capacity
IBM 3450-001	QIC120, QIC150, QIC525, QIC1000	1.19 GB
TECMAR QT525ES	QIC525	525 MB
WANGTEK 5525ES	QIC525	525 MB

Table 17. OS/2 Warp Server Backup/Restore DLT Tape Drives

Device Name	Supported Formats	Estimated Capacity
Quantum DLT 2000	DLT10, DLT10C	10 GB*
Quantum DLT 4000	DLT10, DLT10C, DLT20, DLT20C	20 GB*

Note:

* Greater capacity might be achieved with compression.

B.2 OS/2 Warp Server DSM.OPT Options File

This section describes the default ADSM client options file, DSM.OPT, provided by OS/2 Warp Server Backup/Restore before and after configuration of ADSM storage media. This DSM.OPT file resides in the PSNS\SYSTEM subdirectory.

B.2.1 Before OS/2 Warp Server Backup/Restore Configuration

```
************************************************************
* ADSTAR Distributed Storage Manager
*
* Sample client options file for the PSnS ADSM device interface
*
************************************************************


*  Setting Nodename
*  ------------------------------------------------------

  NODENAME                  PSnS_node


*  Setting Options for the IPX/SPX Communication Method
*  ------------------------------------------------------
* COMMMETHOD                IPXspx
*    IPXSERVERADDRESS         ipx_serveraddress
*    IPXBUFFERSIZE            4
*    IPXSOCKET                8522


*  Setting Options for the Named Pipes Communication Method
*  ------------------------------------------------------
* COMMMETHOD                NAMEdpipes
*    NAMEDPIPENAME            \pipe\dsmserv


*  Setting Options for the NETBIOS Communication Method
*  ------------------------------------------------------
* COMMMETHOD                NETBIOS
*    NETBIOSNAME              client_name
*    NETBIOSSERVERNAME        server_name
*    NETBIOSBUFFERSIZE        4
*    NETBIOSTIMEOUT           60
*    LANADAPTER               0


*  Setting Options for the PWSCS Communication Method
*  ------------------------------------------------------
* COMMMETHOD                PWScs
*   SYMBOLICDESTINATION       server


* COMMMETHOD                PWSCS
*   TPNAME                    server
*   PARTNERLUNAME             target_lu
*   CPICMODENAME              mode_name
*   CPICBUFFERSIZE            15


* COMMMETHOD                PWScs
*   NODENAME                  node_name
```

```
*  Setting Options for the SNA LU 6.2 Communication Method
*  ------------------------------------------------------
* COMMMETHOD                SNAlu6.2
*   SYMBOLICDESTINATION       server


* COMMMETHOD                SNAlu6.2
*   TPNAME                    server
*   PARTNERLUNAME             target_lu
*   CPICMODENAME              mode_name
*   CPICBUFFERSIZE            15


*  Setting Options for the TCP/IP Communication Method
*  ------------------------------------------------------
* COMMMETHOD                TCPip
*    TCPSERVERADDRESS         tcp_address
*    TCPPORT                  1500


*  Setting Options for the 3270 Communication Method
*  ------------------------------------------------------
* COMMMETHOD                3270
*   3270LOGICALTERMINALID     A
*   3270HOSTCOMMAND
*   3270BUFFERSIZE            4000
*   3270HOSTCMDPAUSE          1
*   3270HOSTTIMEOUT           10
*   3270CHECKSUM              YES


*  Setting default management class
*  --------------------------------
  INCLUDE * PSnS_mc


*  Setting National Language options
*  ---------------------------------
   LANGUAGE                 AMENG
   DATEFORMAT               1
   TIMEFORMAT               1
   NUMBERFORMAT             1
```

B.2.2 After OS/2 Warp Server Backup/Restore Configuration

```
*************************************************************************
* ADSM configuration file produced by OS/2 Warp Server Backup/Restore v5.00
* Mon Jan 29 11:33:17 1996
*************************************************************************

NODename PUGET

COMMmethod NETBios

* Configuration data for 3270 communications
* 3270Logicalterminalid A
* 3270HOSTCOmmand
* 3270HOSTENdcommand
* 3270Buffersize 4000
* 3270HOSTCMDPause 1
* 3270HOSTTimeout 10
* 3270Checksum Yes

* Configuration data for PWSCS communications
* SYMbolicdestination server
* TPname server
* PARtnerluname target_lu
* CPICMOdename mode_name
* CPicbuffersize 15

* Configuration data for SNA LU 6.2 communications
* SYMbolicdestination server
* TPname server
* PARtnerluname target_lu
* CPICMOdename mode_name
* CPicbuffersize 15

* Configuration data for TCP/IP communications
* TCPPort 1500
* TCPServeraddress tcp_address
* TCPBuffsize 8
* TCPWindowsize 16

* Configuration data for NetBIOS communications
NETBIOSNAME    PUGET
NETBIOSSERVERNAME    ADSMSERV2
NETBIOSBuffersize 4
NETBIOSTimeout 60
LANAdapter 0

* Configuration data for IPX/SPX communications
* IPXServeraddress ipx_serveraddress
* IPXSOcket 8522
* IPXBuffersize 4

* Configuration data for Named Pipes communications
* NAMEdpipename \pipe\dsmserv
```

```
* INCLUDE statement for default management class
INclude * PSnS_mc

* Options which OS/2 Warp Server Backup/Restore has left from
  your previous configuration
   LANGUAGE                AMENG
   DATEFORMAT              1
   TIMEFORMAT              1
   NUMBERFORMAT            1
**********************************
* End of configuration data
**********************************
```

B.3 Sample ADSM Filespace Listings for OS/2 Warp Server

The listing below is the output of the ADSM administrative command:

```
query content D:-ADSMSERV-BACKO1.DSM node=PUGET filespace=PSnS_data_311FA1AA
```

```
Node Name   Type   Filespace    Client's Name for File
                   Name
----------  ----   ----------   --------------------------------------
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\00000001\1\ .
                    _311FA1AA
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\00000001\0\
                    _311FA1AA    budget.rep
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\00000001\0\
                    _311FA1AA    hugh.let
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\00000001\0\
                    _311FA1AA    mark.let
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\00000001\0\
                    _311FA1AA    mary.let
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\00000001\0\
                    _311FA1AA    mike.let
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\00000001\0\
                    _311FA1AA    sales.rep
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\chris\00000001\-
                    _311FA1AA    1\ .
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\chris\00000001\-
                    _311FA1AA    0\ budget.rep
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\chris\00000001\-
                    _311FA1AA    0\ expenses.rep
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\cyndie\00000001-
                    _311FA1AA    \1\ .
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\cyndie\00000001-
                    _311FA1AA    \0\ employee3460.rep
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\cyndie\00000001-
                    _311FA1AA    \0\ employee3473.rep
PUGET       Bkup   PSnS_data-   \RESOURCES\SHAREDDATA\cyndie\00000001-
```

```
                  _311FA1AA    \0\ employee3490.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\fred\00000001\1\
                  _311FA1AA    .
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\reports\0000000-
                  _311FA1AA    1\1\ .
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\reports\0000000-
                  _311FA1AA    1\0\ december.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\reports\0000000-
                  _311FA1AA    1\0\ january.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\reports\0000000-
                  _311FA1AA    1\0\ november.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\reports\0000000-
                  _311FA1AA    1\0\ october.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\00000002\1\ .
                  _311FA1AA
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\00000002\0\
                  _311FA1AA    budget.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\00000002\0\
                  _311FA1AA    hugh.let
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\00000002\0\
                  _311FA1AA    mark.let
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\00000002\0\
                  _311FA1AA    mary.let
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\00000002\0\
                  _311FA1AA    mike.let
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\00000002\0\
                  _311FA1AA    sales.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\chris\00000002\-
                  _311FA1AA    1\ .
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\chris\00000002\-
                  _311FA1AA    0\ budget.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\chris\00000002\-
                  _311FA1AA    0\ expenses.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\cyndie\00000002-
                  _311FA1AA    \1\ .
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\cyndie\00000002-
                  _311FA1AA    \0\ employee3460.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\cyndie\00000002-
                  _311FA1AA    \0\ employee3473.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\cyndie\00000002-
                  _311FA1AA    \0\ employee3490.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\fred\00000002\1\
                  _311FA1AA    .
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\reports\0000000-
                  _311FA1AA    2\1\ .
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\reports\0000000-
                  _311FA1AA    2\0\ december.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\reports\0000000-
```

```
                  _311FA1AA    2\0\ january.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\reports\0000000-
                  _311FA1AA    2\0\ november.rep
PUGET       Bkup  PSnS_data-   \RESOURCES\SHAREDDATA\reports\0000000-
                  _311FA1AA    2\0\ october.rep
```

The listing below is the output of the ADSM administrative command:

```
query content D:-ADSMSERV-BACK01.DSM node=PUGET filespace=PSnS_indices_311FA1AA

Node Name   Type   Filespace    Client's Name for File
                   Name
----------  ----   ----------   ------------------------------------
PUGET       Bkup   PSnS_indi-   \PSNS\SYSTEM\311FA1AA\ sofa.bed
                    ces_311F-
                    A1AA
PUGET       Bkup   PSnS_indi-   \PSNS\SYSTEM\311FA1AA\ setinfo.psm
                    ces_311F-
                    A1AA
PUGET       Bkup   PSnS_indi-   \PSNS\SYSTEM\311FA1AA\ 00000003.nod
                    ces_311F-
                    A1AA
PUGET       Bkup   PSnS_indi-   \PSNS\SYSTEM\311FA1AA\ 00000004.nod
                    ces_311F-
                    A1AA
PUGET       Bkup   PSnS_indi-   \PSNS\SYSTEM\311FA1AA\ 00000005.nod
                    ces_311F-
                    A1AA
PUGET       Bkup   PSnS_indi-   \PSNS\SYSTEM\311FA1AA\ 00000006.nod
                    ces_311F-
                    A1AA
PUGET       Bkup   PSnS_indi-   \PSNS\SYSTEM\311FA1AA\ 00000007.nod
                    ces_311F-
                    A1AA
PUGET       Bkup   PSnS_indi-   \PSNS\SYSTEM\311FA1AA\ log
                    ces_311F-
                    A1AA
PUGET       Bkup   PSnS_indi-   \PSNS\SYSTEM\311FA1AA\ nodes
                    ces_311F-
                    A1AA
PUGET       Bkup   PSnS_indi-   \PSNS\SYSTEM\311FA1AA\ setinfo.end
                    ces_311F-
                    A1AA
```

List of Abbreviations

ACP	access control profile
ACL	access control list
ADSM	ADSTAR Distributed Storage Manager
APA	all points addressable
API	application programming interface
CID	configuration, installation, and distribution
CLI	command line interface
DCDB	domain control database
DLT	digital linear tape
FAT	file allocation table
GUI	graphical user interface
HPFS	high-performance file system
IBM	International Business Machines Corporation
IPL	initial program load
ITSO	International Technical Support Organization
LAN	local area network
LM	Microsoft LAN Manager
LS	LAN Server
LR	LAN Requester
LTU	license tracking utility
MPTS	Multi-Protocol Transport Services
NCB	network control block
PCLP	Personal Computer LAN Program
QIC	quarter inch cartridge
SMP	symmetric multiprocessing
REXX	Restructured Extended Executor
WFW	Windows for Workgroups

Index

Numerics

A

B

C

D

F

H

I

L

M

N

O

P

R

S

T

W

Printed in U.S.A.