

NetWorker
AA-RDHKA-TE

Disaster Recovery Guide

Restricted Rights: Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

Licensed to Digital Equipment Corporation, Maynard Massachusetts

Copyright © 1998, Legato Systems, Inc.
All rights reserved.

Digital Equipment Corporation makes no representations that the use of its products in the manner described in this publication will not infringe on existing future patent rights, nor do the descriptions contained in this publication imply the granting of licenses to make, use, or sell equipment or software in accordance with the description.

Possession, use, or copying of the software described in this publication is authorized only pursuant to a valid written license from DIGITAL or an authorized sublicensor.

The following are trademarks of Digital Equipment Corporation:

DEC, DIGITAL, OpenVMS, TruClusters, and the DIGITAL logo.

Adobe, Acrobat, and Acrobat Reader are registered trademarks of Adobe Systems Incorporated. AIX, IBM, OS/2, and RISC System/6000 are registered trademarks of International Business Machines Corporation. EXABYTE, EXB10i, EXB-60, EXB-120, EXB-8200, and EXB-8500 are trademarks of Exabyte Corporation. Hewlett-Packard, HP, and HP-UX are registered trademarks of Hewlett-Packard Corporation. Informix is a registered trademark of Informix Software, Inc. Intel is a registered trademark of Intel Corporation. IRIX is a trademark of Silicon Graphics, Inc. Legato NetWorker is registered trademark of Legato Systems, Inc. Mac and Macintosh are registered trademarks of Apple Computer, Inc. Microsoft, Microsoft Exchange Server, MS-DOS, Windows, Windows95, and Windows NT are registered trademarks of Microsoft Corporation. NetWare is a registered trademark, and UnixWare is a trademark of Novell, Inc. NFS, Sun, and SunOS are trademarks, and Solaris is a registered trademark of Sun Microsystems, Incorporated. Oracle is a registered trademark, and Oracle7 and Oracle8 are trademarks of Oracle Corporation. SCO is a registered trademark of Santa Cruz Operations, Inc. StorageTek is a registered trademark of Storage Technology Corporation. UNIX is a registered trademark in the United States and other countries licensed exclusively through X/Open Company Ltd. X Window System is a trademark of the Massachusetts Institute of Technology.

All other trademarks and registered trademarks are the property of their respective holders.

Operating System: Windows NT and UNIX.

Software: NetWorker for Windows NT and NetWorker for UNIX

Date: July 1998

Order Number: AA-RDHKA-TE

Contents

Preface	7
Conventions.....	8
Chapter 1: Introduction.....	9
Preparing for Disaster.....	11
Disaster Recovery Requirements	11
Important Information	12
Bootstrap Information.....	12
Windows NT and UNIX.....	13
NetWare	13
Bootstrap Save Set ID.....	14
How to Find the Bootstrap for Windows NT	14
How to Find the Bootstrap for UNIX	14
NetWare	15
Disk Information	15
Windows NT	16
UNIX	16
NetWare	18
Disaster Recovery Choices	18
Restoring the Operating System.....	18
Complete Installation	20
Partial Installation	20
Recovery with Autochangers	21
Autochanger Addition and Configuration.....	22
How to Recover with an Autochanger for Windows NT and UNIX	22
How to Recover with an Autochanger for NetWare.....	24

Contents

Recovery with a Stand-alone Drive	25
How to Recover with a Stand-alone Drive for Windows NT and UNIX	25
How to Recover with a Stand-alone Drive for NetWare	26
Chapter 2: Disaster Recovery for Windows NT	27
Requirements.....	27
Requirements for Replacing the Hardware	28
Requirements for Reinstalling the Operating System.....	28
Requirements for Reinstalling NetWorker	28
Recovery for a Corrupted Operating System and Partitions	29
REPAIRDISK Directory	30
Backing Up and Recovering the REPAIRDISK Directory	30
Back Up the REPAIRDISK Directory.....	30
How to Use the NetWorker Administrator Program	31
How to Use the NetWorker User Program	31
How to Eliminate the REPAIRDISK Directory From Backups.....	31
How to Prepare for Recovering the Repair Disk Data	32
How to Recover the Repair Disk Data.....	32
How to Recover the Repair Disk Data from the Command Line.....	33
How to Recover the Operating System with the Repair Disk	33
Critical Data Recovery	34
How to Recover Critical Data	34
Operating System Recovery	34
How to Prepare for Recovering the Operating System	35
How to Recover the Operating System	36
NetWorker Software Recovery	37
How to Prepare for Recovering NetWorker Software.....	38
How to Recover NetWorker Clients and Storage Nodes.....	38
How to Recover NetWorker Indexes and Configuration Files	39
Using the mmrecov Command.....	40
Recovery from Clone Volumes.....	43

How to Rename the Configuration Files Directory	44
How to Complete the Recovery of the NetWorker Server Data	45
Recovery to a New Server.....	45
DIGITAL Alpha NT Considerations.....	47
Microsoft Cluster Server Support	47
Backing Up Cluster Data.....	48
How to Recover Cluster Data.....	48
How to Recover the Cluster Database.....	49
How to Recover a Cluster Server.....	51
Chapter 3: Disaster Recovery for UNIX.....	53
Requirements for Replacing the Hardware	54
Requirements for Reinstalling the Operating System	54
Requirements for Reinstalling NetWorker.....	54
Critical Data Recovery	55
How to Recover Critical Data	55
Operating System Recovery.....	56
How to Prepare for Recovering the Operating System	56
How to Recover the Operating System.....	58
NetWorker Software Recovery	58
How to Prepare for Recovering NetWorker Software	59
How to Recover NetWorker Clients and Storage Nodes	60
How to Recover NetWorker Indexes and Configuration Files.....	61
Using the mmrecov Command	62
Recovery from Clone Volumes	65
How to Rename the Configuration Files Directory	66
How to Complete the Recovery of the NetWorker Server Data	67
Recovery to a New Server.....	68
Chapter 4: Disaster Recovery for NetWare.....	71
NetWare Terminology for Backup and Restore.....	71

Contents

New Disaster Recovery Assistance in NetWare 4.11/IntranetWare	72
Disaster Recovery Preparation	73
NetWorker Indexes and Configuration Files Recovery	74
Recover from a Disaster Command	75
Non-SYS Volume Recovery.....	77
Recovering a Non-SYS Volume	77
Full Server Recovery on a Single Server Network.....	77
SYS Volume Recovery on a Single Server Network.....	78
SYS Volume Recovery on a Multiple-Server Network	81
SYS Volume Recovery on a NetWare 4.10 Server	81
SYS Volume Recovery on a NetWare 4.11 or IntranetWare Server	85
Nonreplicated Partition Recovery	88
Network-wide Disaster Recovery	88
Recovery to a New Server	90
Moving NetWorker to a New Server with No Changes.....	90
Moving NetWorker to a New Server with Changes	90
Reregistering NetWorker	91
Appendix A: Win95 Client Recovery.....	93
Glossary	95
Index	103

Preface

The *NetWorker Disaster Recovery Guide* stresses the importance of preparing for a disaster, whether it is for a single system or an entire network. Using NetWorker to back up your data is an excellent way to begin. However, you must also consider how to recover your data and systems if a disk crashes or an entire system is lost. If you back up your data regularly and implement the planning procedures outlined in this guide, you are well prepared to recover from a disaster.

For instructions about configuring and administering the administration program for NetWorker, refer to the *NetWorker Administrator's Guide* that pertains to your platform. To learn how to recover files and filesystems and perform manual backups with the appropriate NetWorker program, refer to the online help.

About This Guide

This guide is for system administrators who are responsible for performing backups and recovers and for maintaining the safety of the data on the network.

The instructions in this guide act as general guidelines to follow because every system, network, and disaster recovery situation is unique.

This guide includes the following information:

- Descriptions of different types of disasters
- Platform-specific information that prepares you for a disaster
- Choices to consider while performing a disaster recovery
- Step-by-step instructions for recovering from a disaster for each of the following major server platforms: Windows NT[®], UNIX[®], and NetWare[®]

Conventions

This guide uses the following typographic conventions and symbols to make information easier to access and understand.

- **boldface** – Indicates DOS or UNIX line commands. For example:
Run the **jbconfig** command to add and configure the autochanger.
- *italic* – Indicates directory pathnames, files, machine names, new terms defined in the Glossary or a chapter, and words or ideas that require emphasis. For example:
Rename the original `\nsr\res` directory to `\nsr\res.orig`.
- `fixed-width` – Represents examples and information displayed on the screen. For example:
`media waiting: recover waiting for 8mm 5GB tape
volume name`
- `Pull-down_menu>Command>Command` – Depicts a path or an order to follow for making selections in the GUI. For example:
`Volume>Change Mode>Appendable`
- `fixed-width, boldface` – Represents commands and text you type exactly as shown. For example:
`% dkinfo sd0a`
- `fixed-width, boldface italic` – Represents commands and text you type for which you need to substitute a variable. For example:
`C:\win32app\nsr\bin scanner -B \\. \Tape0`



Important: Important information and cautionary notes that prevent you from making a mistake.

Chapter 1: Introduction

This chapter contains concepts, procedures, and information that help you prepare for recovering data after a disaster. It is important that you develop a plan for recovering from a disaster where valuable data, a disk, or an entire system has been destroyed.

This chapter addresses disaster recovery issues for Windows NT, UNIX, and NetWare systems. Most information applies to all three platforms; platform-specific information is clearly marked. These examples are meant to be generic, but might use conventions and protocols that apply to a platform other than your own. However, these examples still apply to your platform even though the protocols or conventions might not.

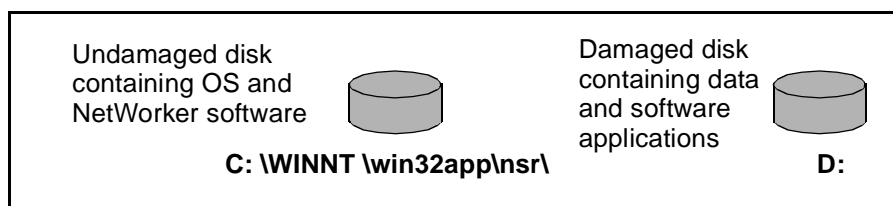
Different Types of Disasters

Typically, the four types of disasters you might experience are as follows:

- Critical data other than the operating system (OS) or the NetWorker software is damaged or destroyed. This disaster applies to both NetWorker clients and servers.

In the example shown in Figure 1 on page 9, a NetWorker client for Windows NT has two disks. The disk containing the operating system and NetWorker software is still operational, but the second disk, containing critical client data, was destroyed by a disk crash. To recover from this disaster, use the NetWorker recover program to recover the lost applications and data.

Figure 1. Critical Data is Lost on a Secondary Disk

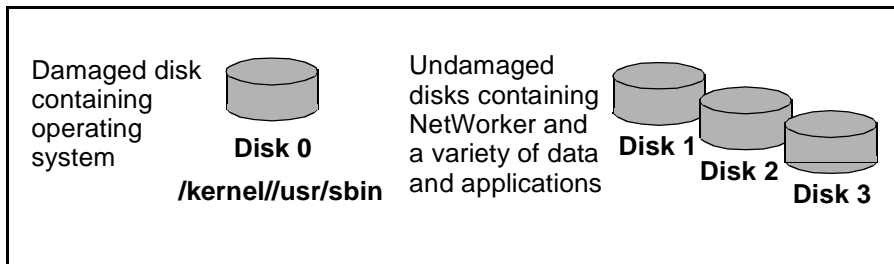


Different Types of Disasters

- In Figure 2, the operating system has been damaged or destroyed. This situation can occur on NetWorker clients and servers.

In the example, a NetWorker server for UNIX has several physical disks. A power outage corrupted the filesystem on Disk 0, which destroyed the operating system. To recover from the disaster, you need to replace the disk, reinstall the operating system, and if necessary, the NetWorker software. Then use NetWorker to recover the lost server configuration and any data that was lost when the operating system was destroyed.

Figure 2. Disk Containing Operating Software is Damaged

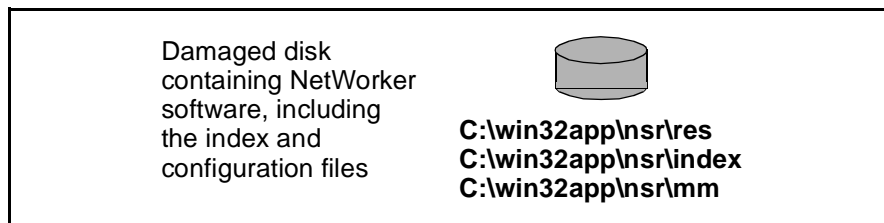


Important: In a situation where the operating system was destroyed, you must always reinstall the operating system, reinstall NetWorker, and then use NetWorker to recover the remainder of your data. You cannot recover data backed up by NetWorker without reinstalling the operating system and NetWorker software first.

- In Figure 3, the directory on the server that contains the NetWorker software and the online indexes and configuration files has been damaged or destroyed. The operating system is assumed to be running on a different disk than the NetWorker software. This situation only applies to NetWorker servers.

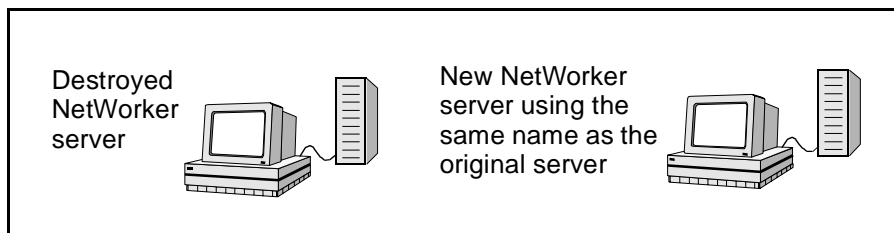
In the example, a single disk on a NetWorker for Windows NT server contains the NetWorker software and the index and configuration files. To recover from a disaster of this type, recover the contents of the bootstrap save set.

Figure 3. Disk Containing NetWorker Indexes is Damaged



- In the example in Figure 4, the NetWorker server has been destroyed. To recover from this disaster, you need to recover all the data to a new system *by the same name*. This applies only to NetWorker servers.

Figure 4. NetWorker Server is Destroyed



Disaster recovery procedures for NetWorker for NetWare systems include additional instructions for recovering the NDS tree on both single-server and multiple-server networks. See “Chapter 4: Disaster Recovery for NetWare” on page 71 for more information.

Preparing for Disaster

Not only do you need to back up important data on a daily basis, you need to develop and test a plan for recovering your data if a disk crashes or you lose critical data. The more time and effort you invest in creating and testing your plan, the better prepared you are if disaster strikes.

Disaster Recovery Requirements

If you have included your NetWorker server and clients in a scheduled backup, you are well on your way to being prepared for a disaster. With each server backup, NetWorker creates a special save set called the *bootstrap* essential for recovering from a disaster.

Along with the bootstrap information, you should also keep accurate records of your network, system configurations, and maintain a safe location for all your original software.

Important Information

The severity of the destroyed or lost data determines the number of procedures you need to perform. To accomplish the most comprehensive disaster recovery, you need the following items:

- Original operating system media and patches
- Original NetWorker media
- Device drivers and media device names
- Filesystem configuration
- IP addresses and hostnames
- NDS topology (NetWare 4.x only)
- Bootstrap information
- Enabler and authorization codes (under certain circumstances)

To recover from a disaster where you need to reinstall the operating system, you have two choices. You can perform a complete installation where you reinstall all the operating system files and recreate any special configurations. Or, you can perform a partial reinstall of the operating system and wait to recover the system configuration files with NetWorker after your system is functional. If you have an autochanger, you can either configure and use the autochanger during the recovery, or use the drive in the autochanger as a stand-alone device.

Important Information

Use the procedures in this section to collect bootstrap and disk configuration information necessary to perform a disaster recovery.

Bootstrap Information

During each scheduled backup of the backup server, NetWorker creates a special save set named *bootstrap*, essential to perform a successful disaster recovery. The bootstrap contains the NetWorker server file index, media database, and configuration files.



Important: NetWorker does not save the bootstrap information during a manual backup; NetWorker only saves it during a scheduled save.

For UNIX and Windows NT systems, NetWorker prints or saves to a file the most recent bootstrap information that includes dates, locations, and save set ID numbers. See Figure 5 for an example of the bootstrap information generated each time NetWorker performs a scheduled backup. Make sure you

store the bootstrap printout or electronic file in a safe place. For NetWare systems, you use a special command to extract the bootstrap data from a backup volume.

Figure 5. Bootstrap Information for UNIX and Windows NT Systems

```
August 20 03:30 1996 NetWorker bootstrap information Page 1
date      time      level ssid      file record volume
8/19/96  2:29:08  9      1148868949 56  0      mars.005
8/20/96  2:52:25  9      1148868985 77  0      mars.001
```

The bootstrap displays a listing of the bootstrap save sets backed up for the past month.

For specific instructions about recovering NetWorker server indexes and configuration files, see “How to Recover NetWorker Indexes and Configuration Files” in the chapter that pertains to the system you are recovering.

Windows NT and UNIX

For Windows NT and UNIX systems, you can also perform scheduled backups of the NetWorker server indexes by using the **savegrp** command. Using this command also sends the bootstrap information to a printer or electronic file. For example:

```
# savegrp -O -c server-name
```

To use the **savegrp -O** command, you must be *root* on the NetWorker server for a UNIX system or Administrator on a Windows NT system.

For information about printing or saving bootstrap data to a file, refer to the section “Bootstrap Notification” in the *Administrator’s Guide*.

NetWare

NetWorker for NetWare does not need to print or save the bootstrap data to a file. Instead, you use the Recover from a Disaster command to locate the bootstrap data on a backup volume. See “Recover from a Disaster Command” on page 75 for more information.

Important Information

Bootstrap Save Set ID

The most efficient way to recover the bootstrap is to make sure you save the bootstrap information prior to a disaster. However, if you do not have the information, you must scan the most recent backup volume to find the save set ID (save set ID or ssid) of the most recent bootstrap. Use the **scanner -B** command for Windows NT and UNIX systems because it always finds a valid bootstrap. Use the Recover from a Disaster command to locate the bootstrap data on the backup volumes for NetWare systems.

How to Find the Bootstrap for Windows NT

For Windows NT systems, after you locate the bootstrap with the most recent date, run the **mmrecov** command, and supply the save set ID and file number displayed by the **scanner** command.

Use the following steps to find the most recent save set ID for a Windows NT system:

1. Place the most recent media used for scheduled backups in the server device.
2. In the Command Prompt window, change to the directory where you originally installed NetWorker, typically, `\win32app\nsr`.
3. Use the **scanner -B** command to locate the most recent bootstrap, for example:

```
C:\win32app\nsr\bin scanner -B \\.\Tape0
```

The **scanner -B** command displays the latest bootstrap save set information found on the backup volume, as illustrated below:

```
scanner: scanning 8mm tape mars.006 on \\.\Tape0
scanner: Bootstrap 1148869870 8/11/96 6:29:58 mars.006,
file 88
```

How to Find the Bootstrap for UNIX

For UNIX systems, after you locate the bootstrap with the most recent date, run the **mmrecov** command, and supply the save set ID and file number displayed by the **scanner** command

Use the following steps to find the most recent save set ID for a UNIX system:

1. Place the most recent media used for scheduled backups in the server device.
2. At the system prompt, change to the directory where you originally installed NetWorker, typically, `/usr/sbin`.

3. Use the **scanner -B** command to locate the most recent bootstrap on the media, for example:

For SunOS™ systems:

```
/usr/etc/scanner -B /dev/nrst8
```

For Solaris® systems:

```
/usr/sbin/scanner -B /dev/rmt/0hbn
```

For AIX® systems:

```
/usr/bin/scanner -B /dev/rmt0.1
```

For HP-UX® 9.x systems:

```
/usr/networker/bin/scanner -B /dev/rmt/0mnb
```

For HP-UX 10.x systems:

```
/opt/networker/bin/scanner -B /dev/rmt/0mnb
```

For DIGITAL™ UNIX systems:

```
/usr/bin/scanner -0B /dev/rmt0h
```

The **scanner -B** command displays the latest bootstrap save set information found on the backup volume, as illustrated below:

```
scanner: scanning 8mm tape jupiter.001 /dev/rmt/0hbn
scanner: Bootstrap 1148869870 of 8/21/96 7:45:15
located on volume jupiter.001, file 88
```

NetWare

NetWorker for NetWare does not need to print or save the bootstrap data to a file. Instead, use the Recover from a Disaster command to locate the bootstrap data on a backup volume. See “Recover from a Disaster Command” on page 75 for more information.

Disk Information

It is recommended that you take an additional precautionary step to help you recover from loss of critical data: before a disaster recovery, find out how each disk on your network is partitioned and formatted and print and save this information. If a disk is damaged or destroyed during a disaster, use the disk information to recreate the disk exactly as it was prior to the disk crash. Do the same for each system NetWorker backs up, unless the systems are consistent in disk and filesystem layout.

Important Information



Important: When you recreate your disk configuration, you need to have partitions large enough to hold all the recovered data. Make the partitions at least as large as they were before to the crash.

Windows NT

Before a disaster, copy the information that appears in the Windows NT Disk Administrator window, including the size of the partitions, the formatting methods, and the drive letters the partitions are assigned to.

UNIX

Use the **df** command to find out how the NetWorker server disks are partitioned and mounted. See Figure 6 for an example of the output generated by the **df** command. Use the appropriate operating system command to print disk partitioning information. Do the same for any NetWorker clients that have local hard disks.

- For DIGITAL UNIX, use the **df** command
- For Advanced File System (AdvFS) domains, use the **ls -lR** command on */etc/fdmns*
- For Solaris, use the **df** and **prtvtoc** command
- For AIX, use the **df** and **lslv** commands or the Logical Volume Manager in the System Management Interface Tool (SMIT)
- For HP-UX, use the **df** command

Figure 6. Example of df Command

Filesystem	kbytes	used	avail	capacity	Mounted on
/dev/dsk/c0t3d0s6	480919	414138	18691	96%	/usr
/dev/dsk/c0t3d0s0	1251422	183449	942833	17%	/
swap	208112	380	207732	1%	/tmp
/dev/dsk/c0t3d0s5	96031	12799	73632	15%	/var

The following **dkinfo** command examples give you information about how each disk is partitioned for a SunOS system:

```
% dkinfo sd0a
      SCSI CCS controller at addr f8800000, unit # 24
      1151 cylinders 9 heads 80 sectors/track
      33120 sectors (46 cyls)
      starting cylinder 0
```



```
% dkinfo sd0b
1151 cylinders 9 heads 80 sectors/track
197280 sectors (274 cyls)
starting cylinder 46
```

The **prtvtoc** command example in Figure 7 displays information about the partitions for each disk on a Solaris system. The device name is the “raw” device corresponding to the device name used for the output from the **df** command.

Figure 7. Output of the prtvtoc Command.

```
* /dev/dsk/c0t3d0s0 partition map
*
* Dimensions:
*   512 bytes/sector
*   80 sectors/track
*   19 tracks/cylinder
*  1520 sectors/cylinder
*  3500 cylinders
*  2733 accessible cylinders
*
* Flags:
*   1: unmountable
*  10: read-only
*
*
* Partition  Tag  Flags   First   Sector   Last
*          0   2   00      0     2663040 2663039  /
*          1   3   01    2663040 261440  2924479
*          2   5   00      0     4154160 4154159
*          5   7   00    2924480 205200  3129679  /var
*          6   4   00    3129680 1024480  4154159  /usr
```

The **lslv** command example in Figure 8 gives you information about the logical volumes on an AIX system.

Disaster Recovery Choices

Figure 8. Output of the lslv Command.

```
OUTPUT of $ lslv hd6
LOGICAL VOLUME:    hd6
LV IDENTIFIER:    00004421b56f747b.1
VG STATE:        active/complete
TYPE:            paging
MAX LPs:         128
COPIES:          1
LPs:             8
STALE PPs:       0
INTER-POLICY:    minimum
INTRA-POLICY:    middle
MOUNT POINT:     N/A
MIRROR WRITE CONSISTENCY: off
EACH LP COPY ON A SEPARATE PV?: yes
VOLUME GROUP:    rootvg
PERMISSION:      read/write
LV STATE:        opened/syncd
WRITE VERIFY:    off
PP SIZE:         4 megabyte(s)
SCHED POLICY:    parallel
PPs:             8
BB POLICY:       non-relocatable
RELOCATABLE:     yes
UPPER BOUND:     32
LABEL:           None
```

If a disk is damaged, you can restore it and recover the filesystems to their original state, using the hardcopy information from these disk information commands.

NetWare

Make a printed record of the disks and partition sizes for your NetWorker for NetWare server, using a standard NetWare utility such as MONITOR or INSTALL. This information helps you recover from a potential disaster much more smoothly, especially if you want to rebuild the server disk exactly as it was before the disaster.

For Novell Directory Services (NDS), document the NDS tree topology and the location of server objects, partitions and replicas and bindery context settings. Use the DOS NETADMIN program or the Windows NWAdmin program to determine the names and locations of the server objects. Use the NetWare DSREPAIR program to check on partitions and replicas. Display or print the NetWare *autoexec.ncf* file to locate the bindery context settings.

Disaster Recovery Choices

You have several options for recovering the operating system and whether you want to use an autochanger or a stand-alone drive. This section outlines the differences so you can decide which methods best suit your situation.

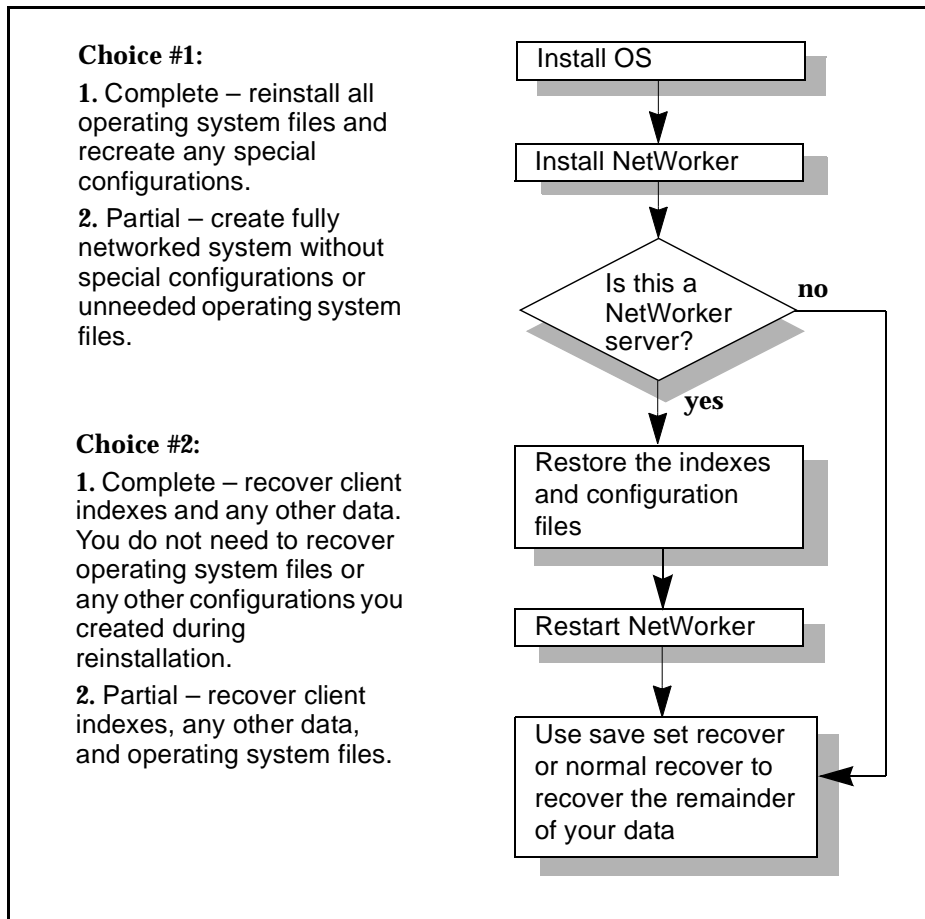
Restoring the Operating System

You can use one of two methods for recovering the operating system during a disaster recovery: complete or partial. When you perform a complete reinstallation, you install all operating system files and recreate any unique configurations that existed before you lost data or experienced a disk crash. To

perform a partial reinstallation, install the minimum number of files and make the minimum number of configurations necessary for creating a fully operational networked system. Then, later, recover the remaining operating system and configuration files using NetWorker.

Figure 9 illustrates the steps for recovering from a disk crash where you lost the operating system, NetWorker software, and server indexes and configuration files. It also outlines the two choices you have for reinstalling the operating system.

Figure 9. Recovering the Operating System



Performing a disaster recovery for NetWorker servers and clients is very similar, except on client systems you do not need to recover the server indexes and configuration files.

Complete Installation

In some cases, it might be faster to perform a complete reinstallation of the operating system, especially if you install the operating system from a CD and have very few special configurations to recreate. Depending on the speed of your backup device and network, it could potentially take longer to recover the remainder of your files and configurations using NetWorker during the disaster recovery procedure.

For UNIX systems, if you use a device with a default configuration that is not directly supported by the operating system, you also need to modify the device configuration files during installation:

- For Solaris systems, you might need to modify the `/kernel/drv/st.conf` file to support a DLT tape drive.
- For SunOS systems, modify the `/usr/sys/scsi/targets/st_conf.legato.h` file.
- For AIX systems, use SMIT to configure the devices.
- For HP-UX systems, you must reconfigure the control port for the device robotics. Enter `lsdev -d spt` to get the major number for the driver. Then enter `ioscan -f` to view a list of devices and `mknod /path/of/device c spt-major-number 0xIITL00`. Then enter `jbinfo` to verify the configuration.

For a Windows NT system, you might need to reinstall the software device driver. For a NetWare system, you need to load the SCSI driver and its ASPI driver.

When you recover the remainder of your data, you can decide whether you want to replace the operating system files you just reinstalled with the operating system files backed up by NetWorker. If you want to guarantee that you have the same configurations prior to the disaster, replace the files and configurations you created during the installation.

Partial Installation

On the other hand, a partial installation might get your NetWorker server up and running more quickly, so you can concentrate on continuing the disaster recovery. Later, you can recover the remainder of your operating system files using NetWorker. You will especially save time if you have a large number of clients and devices on the network that need to be configured; it will take you time to find IP addresses, hostnames, and recreate configurations.

Furthermore, if you wait to recover the remainder of the operating system files with NetWorker, you will be assured that the server, clients, and devices will be reconfigured exactly as they were prior to the disaster.

If you choose to do a partial install, you need to perform the following tasks:

- If necessary, select a domain for the system.
- Install the basic operating system files and device driver software.
- Make sure the system communicates properly over the network.

For UNIX systems, after you reinstall the operating system, whether you did a complete or partial installation, run the **tar** command to verify that the tape drive is functioning properly. For a Windows NT system, use the Backup Utility in the Administrative Tools window. For NetWare systems, use SBackup, the backup application that comes bundled with the NetWare operating system.

Recovery with Autochangers

This section explains how to use your autochanger during a disaster recovery where you have lost, at a minimum, the NetWorker server indexes and configuration files. Typically, the configuration files reside in the following directories:

- Windows NT systems - *C:\win32app\nsr\res*
- UNIX systems - */nsr/res*
- NetWare systems - *SYS: NSR\RES*

The configuration files include the *nsrjb.res* file, which contains autochanger configuration information.

This section assumes that you have lost the NetWorker server indexes and configuration files on the original server, or you are moving NetWorker and need to recover the existing index and configuration files to the new server.

For more information, see “Operating System Recovery” NetWorker Software Recovery” and “How to Recover NetWorker Indexes and Configuration Files” in the chapter that pertains to your operating system.

The programs that recover the indexes and configuration files do not recognize autochangers. Consequently, you need to use the autochanger as if it were a stand-alone drive for that portion of the recovery. Use the autochanger’s control panel to mount and unmount the necessary backup volumes.

After recovering the indexes and configuration files, all the original autochanger configuration files are back in place. You can now use the autochanger to recover the remainder of your data.

Disaster Recovery Choices



Important: If you did not lose the server indexes and they are over 30 days old, you must reenable the server and autochanger to use the autochanger during a disaster recovery.

The rest of this section describes the issues that might influence your choices for using the autochanger or just the drive located inside the autochanger and how to recover the server's indexes and configuration files.

Autochanger Addition and Configuration

If you choose to recover with an autochanger, review these issue about recovering data prior to restoring the server indexes and configuration files:

- If the autochanger has more than one drive, use the first drive for recovery.
- You cannot use the full functionality of the autochanger while restoring the server indexes and configuration files. Neither **mmrecov** for Windows NT and UNIX nor the Recover from a Disaster command for NetWare support autochangers; these commands only support stand-alone devices.
- The robotic device does not locate, load, and mount volumes automatically. You must use the NetWorker Mount and Unmount buttons and the autochanger control panel to mount and unmount volumes. If you use the autochanger control panel, NetWorker does not have a record of where the volumes have been moved, so inventory the autochanger contents after you complete the recovery.
- When you recover the server indexes and configuration files, you recover the autochanger configuration files as they existed during the last backup, including the inventory of the autochanger. If you moved backup volumes inside the autochanger during the disaster recovery, the location of the volumes probably no longer matches the recovered inventory contents. After the recover operation, inventory the autochanger.

How to Recover with an Autochanger for Windows NT and UNIX

Follow these instructions to perform a disaster recovery with an autochanger:

1. If necessary, reinstall the operating system and NetWorker software. During installation, use the same pathname for the indexes that you previously used and backed up.
2. Run the **jbconfig** command to add and configure the autochanger.

3. Issue the **nsrjb -vHE** command. This command resets the autochanger for operation, ejects backup volumes, reinitializes the element status, and checks each slot for a volume. If the **-E** option is not supported for your autochanger, use the **sjielm** program (for example, */etc/LGTOusesi/sjielm* on Solaris) to initialize element status.

If a volume is loaded in the drive, it is removed and placed into a slot. This operation might take a few minutes to complete.

If you receive an error, typically the robotic device is having trouble finding a slot for a volume it has removed from the drive. Try moving some backup volumes around to make room for the volume, or, if possible, remove the volume from the robotic arm and manually place it in a slot.

4. Locate your bootstrap data, either an electronic file or hardcopy. With this information, determine which volumes are necessary for recovering the server indexes and configuration files.
5. Enter the **nsrjb -I** command to inventory the contents of the autochanger, to help you determine whether the volumes required for recovering the bootstrap are inside the autochanger. Chances are the volume currently loaded in the drive contains the most current bootstrap.

If you want to speed up this process, issue the command with the **-S** flag and list only the slots where you think the required backup volumes reside. This saves you from having to inventory the entire autochanger contents. You must list the slots in order (for example, "**nsrjb -I -S 1-3**"). If you want to inventory slots out of order, (for example 1, 3, and 6,) you must issue the **nsrjb -I -S** command separately for each slot. All the volumes currently loaded in the autochanger are marked with an asterisk because you have not yet recovered the media index.

6. Load the appropriate volume by entering the following command:

```
nsrjb -l -S slot -f device-name
```

where *slot* is the slot where the first volume is located and *device-name* is the *pathname* of the first drive. You can also use the NetWorker Mount button.

7. Enter the **mmrecov** command. If the bootstrap spans across more than one volume, NetWorker prompts you to load another backup volume.
8. Enter the **nsrjb -u** command to unmount the volume after the indexes have been recovered. You can also use the NetWorker Unmount button.

```
nsrjb -u -S slot -f device-name
```

9. Shut down NetWorker.

Disaster Recovery Choices

10. Rename `\nsr\res` to `\nsr\res.orig`.

11. Rename the `\nsr\res.R` directory to `\nsr\res`.

When you recover and rename the `\nsr\res` files, you replace the configuration files you created when you reinstalled and configured the autochanger. This step ensures that you have all your configurations that existed on the last backup, prior to the disaster.

12. Restart NetWorker.

After the server indexes and configuration files are recovered, you have a fully functioning autochanger. Inventory the contents of your autochanger, especially if you manually moved volumes as part of the disaster recovery.

How to Recover with an Autochanger for NetWare

When you reinstall NetWorker for NetWare during a disaster recovery, NetWorker automatically searches for any devices attached to the server. If NetWare detects an autochanger, NetWorker automatically adds and configures the device. At this point, you can use the NetWorker interface to move volumes around in the autochanger.

Use the following procedure to perform a disaster recovery with an autochanger:

1. If necessary, reinstall the operating system and NetWorker software. During installation, use the same pathname for the indexes that you previously used and backed up.
2. Locate the backup volume needed for recovering the NetWorker server indexes and configuration files. Typically, it is the last volume you backed up to and is probably loaded in the drive.

If you can't locate the volume needed to begin the recover, inventory the autochanger contents to help you find the backup volume containing the most recent bootstrap data. NetWorker displays an error message that states the volumes are not in the media database. Ignore the message, and proceed with the disaster recovery.

3. After loading NetWorker and mounting the backup volume with the bootstrap data, switch to the NetWare system console, and load the NetWorker Utilities program.
4. Use the Recover from a Disaster command in the NetWorker Utilities program to recover the NetWorker server indexes and configuration files.
After you recover the indexes and configuration files, you should have a fully functioning autochanger.

5. Exit NetWorker Utilities, then stop and restart NetWorker (be sure to unload all of the associated NLM files). This process restores NetWorker to its original configuration – passwords, administrator privileges, backup groups, and schedules.

After you recover the server indexes and configuration files, you have a fully functioning autochanger. With the disaster recovery complete, inventory the contents of your autochanger.

Recovery with a Stand-alone Drive

If you choose to recover with a drive in the autochanger, review these issues about recovering data prior to restoring the indexes and configuration files:

- If the autochanger has more than one drive, use the first drive for recovery.
- You must manually mount the backup volumes required for recovering the server indexes and configurations files.
- If you remove backup volumes from the autochanger cartridge used for recovering the NetWorker indexes and configuration files, put them back in the same slots when you finish.

How to Recover with a Stand-alone Drive for Windows NT and UNIX

Use the following instructions to perform a disaster recovery using just a drive inside the autochanger for a NetWorker for Windows NT or UNIX server:

1. If necessary, reinstall the operating system and NetWorker software. If you need to reinstall the NetWorker software, use the same pathname for the indexes that you previously used and backed up.
2. Locate your bootstrap data, either an electronic file or hardcopy. With this information, determine which volumes are necessary for recovering the server indexes and configuration files.
3. Manually mount the appropriate volume into the drive.
4. Enter the **mmrecov** command.
5. Shut down NetWorker.
6. Rename the original `\nsr\res` directory to `\nsr\res.orig`.
7. Rename the recovered `\nsr\res.R` directory to `\nsr\res`.
8. Restart NetWorker.
9. Issue the **nsrjb -vHE** command. This command resets the autochanger for operation, ejects backup volumes, reinitializes the element status, and checks each slot for a volume. If a volume is loaded in the drive, it is

Disaster Recovery Choices

removed and placed into a slot. This operation might take a few minutes to complete.

10. Inventory the autochanger contents by using the **nsrjb - I** command or use the Inventory command in the administrator program.

After you recover the server indexes and configuration files, you should have a fully functioning autochanger.

How to Recover with a Stand-alone Drive for NetWare

When you use just the drive inside the autochanger for disaster recovery, you can either load and unload backup volumes manually, or you can use the control panel on the front of the autochanger.

Use the following procedure to perform a disaster recovery using the drive located in the autochanger for a NetWorker for NetWare server:

1. If necessary, reinstall the operating system and NetWorker software. If you need to reinstall the NetWorker software, use the same pathname for the indexes that you previously used and backed up.
2. Manually mount or use the autochanger's control panel to load the appropriate volume into the drive.
3. After loading NetWorker and mounting a backup volume, switch to the NetWare system console, and load the NetWorker Utilities program.
4. Use the Recover from a Disaster command in the NetWorker Utilities program to recover the NetWorker server indexes and configuration files.
5. Exit NetWorker Utilities, then stop and restart NetWorker. This process restores NetWorker to its original configuration – passwords, administrator privileges, backup groups, and schedules. At this point, you should have a fully functioning autochanger.
6. Inventory the autochanger contents.

Continue using NetWorker to recover the remainder of your lost data, including the client indexes.

Chapter 2: Disaster Recovery for Windows NT

Use the information in this chapter to determine which disaster recovery procedures you should follow for NetWorker for Windows NT servers and clients. However, it is important that you read and follow the procedures in Chapter 1 before you ever need to recover from a disaster. Chapter 1 explains how to prepare for recovering from a disaster and defines basic terms, procedures, and concepts used throughout this guide.

This chapter includes procedures for recovering from the following kinds of disasters:

- Corrupted operating system and partitions
- Loss of a drive or partition that contains critical data other than the operating system or NetWorker software
- Loss of the operating system
- Loss of a drive or partition that contains NetWorker software, which typically includes the NetWorker indexes and configuration files
- Loss of an entire NetWorker server to the extent that you need to recover to a new system
- Loss of cluster data, database, or server

It is difficult to provide step-by-step instructions for performing a disaster recovery for a specific situation, because every situation is unique. The examples in this chapter are designed to give you *general principles* to recover from a disaster and to help you understand the procedures.

Requirements

While performing any of the disaster recovery procedures included in this chapter, keep in mind the requirements listed in this section. Fulfill the requirements pertinent to the disaster recovery procedure you are following.

Requirements

Requirements for Replacing the Hardware

If hardware becomes damaged or destroyed, use the following selections to install and configure your new system hardware correctly:

- Ensure that the replacement disk is as large or larger than the original disk.
- When replacing the hardware, use the same type of controller, driver, and SCSI ID used prior to the disaster.
- Re-create the same size or larger disk partitions on the new disk/system.
- Format the disk partitions using the same formats used by the original disk (for example, FAT, NTFS, HPFS).
- Assign the same drive letters to each partition used prior to the disaster.

Requirements for Reinstalling the Operating System

If the operating system is damaged or destroyed, adhere to the following list when you reinstall Windows NT:

- Reinstall the same version of Windows NT.
- Reinstall Windows NT in the same directory where it originally resided.
- Use the same system name, TCP/IP hostname, and DNS domain name.
- Reinstall any Microsoft Service Packs or Hotfixes that existed prior to the disaster.
- Reinstall the device and SCSI drivers.
- Make sure all network protocols are working properly.
- After reinstalling Windows NT, reboot your system, and log on as Administrator. Check the Event Viewer to make sure no errors occurred during startup. Also make sure that all the devices are recognized by the operating system.

Requirements for Reinstalling NetWorker

Fulfill the following requirements to ensure successful reinstallation of NetWorker. Refer to the *Quick Start Guide* for installation instructions.

- Reinstall the same version of the NetWorker software.
- Reinstall NetWorker on the same drive and directory where it originally resided.
- Reinstall any patches that you installed prior to the disaster.

- For NetWorker servers, you will have to run additional procedures to retrieve the NetWorker server indexes and configuration files. See “Recover NetWorker Indexes and Configuration Files” on page 39 for information.
- For NetWorker clients or storage nodes, see “How to Recover NetWorker Clients and Storage Nodes” on page 38.

Recovery for a Corrupted Operating System and Partitions

NetWorker automatically backs up repair disk data generated by the Microsoft Repair Disk utility. The Repair Disk utility makes copies of important operating system files, including Registry, configuration, and boot-up files. NetWorker uses these files to speed up and simplify the process of repairing a damaged operating system.

If you do not use NetWorker to back up the repair disk data, you need to run this utility regularly to ensure that you have the most current operating system files backed up to a floppy disk. However, performing this process manually can make it difficult to maintain the repair disk data.

NetWorker simplifies this task during each scheduled backup by automatically starting the Repair Disk utility. The utility generates the repair disk data and copies it to the system's local disk in the *%SystemRoot%\repair* directory. NetWorker then backs up and stores information about this data in a NetWorker index directory named *REPAIRDISK*. See Figure 10 on page 30 for an example of the *REPAIRDISK* directory that appears in the Recover window of the NetWorker User program.

During each scheduled backup, NetWorker also starts and backs up the *client_name.txt* diagnostic report. This report is a text file, generated by the Microsoft Diagnostics utility, that summarizes system configurations. The diagnostic report includes information about the operating system version, software drivers, memory allocation, and addresses of the devices attached to the system. NetWorker saves the diagnostic report with the repair disk data in the *%SystemRoot%\repair* directory. NetWorker backs up the contents of the *%SystemRoot%\repair* directory and uses the data to create an Emergency Repair Disk.

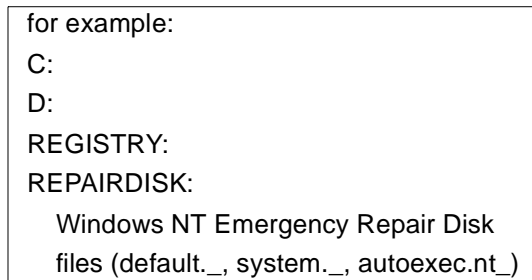
If the Emergency Repair Disk is inadequate for a successful recovery, you might need to use the original Windows NT CD-ROM and Setup disks to reinstall the entire operating system. In this case, the information in the diagnostics report can be useful for reconfiguring the damaged system.

Note: NetWorker for Windows NT release 5.1 only supports the Diagnostic utility on systems running Windows NT 4.0 or later.

REPAIRDISK Directory

The *REPAIRDISK* directory contains the Windows NT Emergency Repair Disk subdirectory that holds Registry, configuration, and boot-up files, as well as the text file generated by the Diagnostics utility. Figure 10 illustrates the *REPAIRDISK* directory, which is under root in the browse window of the NetWorker User program.

Figure 10. Location of the REPAIRDISK Directory



for example:
C:
D:
REGISTRY:
REPAIRDISK:
 Windows NT Emergency Repair Disk
 files (default._, system._, autoexec.nt_)

Backing Up and Recovering the REPAIRDISK Directory

You need to take special precautions for backing up and recovering repair disk data for NetWorker servers. Ideally, you would have two NetWorker servers, each acting as the other's backup server. When you have two NetWorker servers, each backing up the other, you can recover from a disaster using the Emergency Repair Disk as explained in the previous section.

If you only have one NetWorker server, you need to take extra precautions. It is strongly suggested that you run the Microsoft Repair Disk and Diagnostic utilities regularly to ensure that you always have the most current system information. If you do not back up the data regularly and the NetWorker server suffers a disk crash, you cannot access the repair disk data from the backup volume because the operating system and NetWorker software are inoperable.

Back Up the REPAIRDISK Directory

NetWorker automatically generates and backs up the contents of the *%SystemRoot%\repair* directory during scheduled backups to media using the Administrator program. However, if you prefer, you can manually back up the contents of the *%SystemRoot%\repair* directory with the NetWorker User program. The following sections describe both methods.

How to Use the NetWorker Administrator Program

To back up the repair disk data for a group of clients, follow these steps:

1. Select the Configure tab in the Server window to make the Configure window active.
2. Click Clients to open the Clients window.
3. Right-click any client listed, and select Edit from the pop-up menu.
4. To back up the repair disk data on a client, you can either select Save Set All or select a save set that includes the REPAIRDISK: directory (note the colon at the end of REPAIRDISK). By default, Save Set ALL is listed, which backs up all the files for the clients in the group, including the repair disk data. If Save Set All is not listed, add REPAIRDISK:.
5. Add the client to a group and save your changes.
6. Click Manage Groups to open the Group window.
7. Right-click the group to which the client belongs, and select Start from the pop-up menu. After the group has completed, right-click the group to which the client belongs, and select Details from the pop-up menu. The REPAIRDISK: backup should be listed under Successful Save Sets.

How to Use the NetWorker User Program

To back up the repair disk data manually, follow these steps:

1. Double-click the NetWorker User icon to open the NetWorker User program.
2. Click the Backup speedbar button to open the Backup window. NetWorker displays the system's directory structure in the Backup window, including the *REPAIRDISK* directory.
3. Select and mark the *REPAIRDISK* directory for backup. The directory contains no files; the files are generated during backup.
4. Click the Start speedbar button. The Backup Status window opens and displays the progress of the backup.

How to Eliminate the REPAIRDISK Directory From Backups

If necessary, you can eliminate the *REPAIRDISK* directory and its contents from scheduled NetWorker backups by fulfilling these requirements in the NetWorker Administrator program:

- Do not list All or the *REPAIRDISK* save set in the Save Set list box of the Client Edit dialog box.

Recovery for a Corrupted Operating System and Partitions

- Do list all the client's other save sets individually, except for the *REPAIRDISK* directory, in the Save Set list box to ensure that you back up all other data.

How to Prepare for Recovering the Repair Disk Data

To prepare for recovering the repair disk data (located in the *REPAIRDISK* directory), you need to create an Emergency Repair Disk. By default, you recover the repair disk data on the backup media to a floppy disk in drive A of the system performing the recovery. The floppy disk used to create the Emergency Repair Disk must be properly formatted and have sufficient disk space. Although you can relocate the recovered repair disk data to any media your system supports, it is recommended that you use floppy disks, which are readily available and easily transferred from system to system.

To fulfill the requirements to perform a directed recover of repair disk data, follow these steps:

1. Format a 1.44 MB or larger floppy disk.
2. Start NetWorker Administrator and select the Configure tab in the Server window to make the Configure window active.
3. Click Clients to open the Clients window.
4. Right-click the name of the client whose repair disk data you want to recover, and select Edit from the pop-up menu. Select the Remote tab at the top of the Edit Client window.
5. To recover the repair disk data of another client you must add your hostname to the Remote Access List of the client whose repair disk data you are attempting to recover.

How to Recover the Repair Disk Data

The instructions in this section assume that you have a fully functional NetWorker server, and that the NetWorker Administrator and NetWorker User programs are installed and operational.

Use the NetWorker directed recover feature in the NetWorker User program to restore the repair disk data to the client with the damaged operating system. Both the client you are performing the recovery *for* and the client you are performing the recovery *to* must support the NetWorker repair disk feature.

To perform a directed recover, follow these steps:

1. Insert a formatted floppy disk in drive A.
2. Start the NetWorker User program.

3. Select Directed Recover from the Operations menu to open the Source Client dialog box.
4. Select the client you want to recover the data *from* in the Source Client dialog box, and click OK. The Destination Client dialog box appears.
5. Select the client you want to recover the data *to* in the Destination Client dialog box, and click OK. This is the system with the floppy disk in the disk drive and is usually the system initiating the recovery.
6. Select and mark the *REPAIRDISK* directory, and click the Start speedbar button.

NetWorker creates the Emergency Repair Disk by recovering the client's repair disk data to the disk in drive A.

7. Print the diagnostic report from drive A. You need this report only if you cannot successfully reinstall the operating system with the Emergency Repair Disk.

How to Recover the Repair Disk Data from the Command Line

To recover the repair disk data at the command line, follow these steps:

1. Insert a blank formatted floppy disk in drive A:
2. Open an MS-DOS window.
3. Change to the NetWorker directory (by default, *%SystemDrive%\win32app\nsr\bin*).
4. Enter the **recover** command at the command prompt:

```
recover -s client-name REPAIRDISK:\
```

How to Recover the Operating System with the Repair Disk

To recover the system with the damaged operating system using the Emergency Repair Disk, follow these steps:

1. Locate the original Windows NT operating system Setup disks and CD-ROM. You need to use these in conjunction with the Emergency Repair Disk to fully recover the client's operating system.
2. Move to the system with the damaged operating system.
3. Beginning with the first disk, insert the Setup disks in drive A.
4. Respond appropriately to the Windows NT Setup script.
5. Press [R] to choose "Repair damaged Windows NT operating system."

Critical Data Recovery

6. Insert the Emergency Repair Disk. If the Emergency Repair Disk is sufficient to recover the operating system, continue with the installation.

If the Emergency Repair Disk is not sufficient, you receive a message indicating the operating system is damaged beyond repair. In this case, stop and begin again by reinstalling the entire operating system. Use the diagnostic report to provide answers to some of the system configuration questions asked during the installation.

7. Follow the remainder of the install program instructions while reinstalling the Windows NT operating system.

Critical Data Recovery

The following example assumes the disk containing the operating system and NetWorker software is still operational, but another disk containing critical data has been lost. The example applies to both Windows NT NetWorker servers and clients.

If the disk is damaged beyond repair, replace it with a new disk of the same size or larger than the original disk. The disk must be large enough to hold all the data you plan to recover.

How to Recover Critical Data

To recover the critical data, follow these steps:

1. Install the replacement disk. Make sure the operating system recognizes the new disk.
2. Use the saved disk partition information to re-create the disk partitions with the same structure as the original disk. Reformat each partition on the disk with the same filesystems it had before (for example, FAT, NTFS, or HPFS). See "Disk Information" on page 15 for additional information.
3. After creating and formatting the partitions on the replacement disk, use Save Set Recover or the normal recovery procedure in the NetWorker User program to recover the lost data.

For an explanation about the best recovery method for your lost data, see the *NetWorker Administrator's Guide*.

Operating System Recovery

This example assumes a disk containing the operating system has been damaged or completely destroyed. You need to replace the damaged disk and reinstall the operating system. If the disk was not completely destroyed and

either the operating system or NetWorker is still operational, use only the steps in this section that apply to your situation. Instructions in this section apply to NetWorker servers and clients, unless otherwise specified.

How to Prepare for Recovering the Operating System

To prepare for recovering the operating system for either a NetWorker server or client, follow these instructions:

1. Replace the damaged disk if necessary. Make sure the replacement disk is as large or larger than the original disk.
2. Use the saved disk partition information to re-create the disk partitions with the same structure as the original disk. Format each partition on the disk with the same filesystems as before (for example, FAT, NTFS, or HPFS). See “Disk Information” on page 15 for additional information.
3. Reinstall the operating system in the same directory where the operating system originally resided, using the original software and accompanying documentation. Use the same system name, TCP/IP hostname, and DNS Domain name used prior to losing the operating system.



Important: Install the Windows NT operating system into a workgroup. Do not install the server in a Domain. When you recover the Registry later in this procedure, the server is returned to its original Domain after the recovery is complete and you restart the system.

You can choose to fully configure the operating system now, or you can install the minimum number of files and make the minimum number of configurations required to create an operational networked system. See “Restoring the Operating System” on page 18 for more information.

4. Install and configure the SCSI controller and tape device drivers.
5. Reinstall the Microsoft Service Pack if it was installed prior to the disk crash.
Note: If you installed the Microsoft Service Pack Four on a Windows NT 3.51 system, you must also install its patch provided by Microsoft to recover your files. The patch is described in Microsoft document Q149857 *MoveFile_Delay_Until_Reboot*. Download the patch (SMSS.EXE) from the Microsoft anonymous ftp server.
6. Reboot the system, and log on as Administrator.

7. Reinstall the NetWorker software in the same location in which it originally resided. Refer to the *Quick Start Guide* for instructions. Reinstall any NetWorker patches you had installed prior to the disaster.

You might have several different releases of NetWorker software; reinstall the same release that was running prior to the disaster or a later release. The release must equal to or later than the release used for the backups.

You must reinstall NetWorker even if it already exists on another drive to ensure that the correct Registry entries occur and the program shortcuts are added to the Start menu.

If you specify a path to an existing NetWorker setup during the reinstallation, the installation program should discover the existing `\nsr\res\servers` file and use it to update your Windows NT system to use the existing copy of NetWorker.

NetWorker servers only: When you reinstall the NetWorker server software, NetWorker automatically rediscovers indexes and configuration files if they are not corrupted.

NetWorker clients only: The client system is now ready to recover its data from the NetWorker server.

How to Recover the Operating System

To recover the Windows NT operating system, follow these steps:

1. Start the NetWorker User program.
2. Click the Recover speedbar button to open the Recover window. NetWorker displays the system's directory structure.
3. Select and mark the Registry for recovery.
4. Click the Start speedbar button to begin the recovery.
5. Boot the system once the recovery is completed.
6. Log on as Administrator.
7. Select all remaining data for recovery.
8. If you are using Windows NT 3.51, deselect the following file before you recover the data: `%SystemRoot%\system32\smss.exe` where `%SystemRoot%` is the path to your Windows NT installation. This file can cause the recover to fail if installed before Service Pack 4.
9. Click the Start speedbar button to begin the recovery.

The Windows NT system should be restored to its status prior to the disk crash. Check the Microsoft Event Viewer for system or application errors.

NetWorker Software Recovery

The following example for recovering the NetWorker binaries assumes a disk containing the NetWorker software has been damaged or completely destroyed. This example also assumes that the Windows NT operating system is installed and operating properly.

The set of instructions you need to follow in this section depend upon which system you lost (server, client, or storage node) and the extent of the damage. Refer to the following list of disaster recovery scenarios to determine which set of instructions apply to your situation.

- If you are recovering NetWorker clients and storage nodes, you need to follow the instructions in these sections:
 - “How to Prepare for Recovering NetWorker Software” on page 38
 - “How to Recover NetWorker Clients and Storage Nodes” on page 38
- If you are recovering a NetWorker server that lost its indexes and configuration files, you need to follow the instructions in these sections:
 - “How to Prepare for Recovering NetWorker Software” on page 38
 - “How to Recover NetWorker Indexes and Configuration Files” on page 39
 - “How to Rename the Configuration Files Directory” on page 44
 - “How to Complete the Recovery of the NetWorker Server Data” on page 45
- If you are recovering a NetWorker server from clone volumes, you need to follow the instructions in these sections:
 - “How to Prepare for Recovering NetWorker Software” on page 38
 - “Recovery from Clone Volumes” on page 43
 - “How to Rename the Configuration Files Directory” on page 44
 - “How to Complete the Recovery of the NetWorker Server Data” on page 45
- If you are recovering NetWorker to a new server, you need to follow the instructions in “Recovery to a New Server” on page 45.
- If you are recovering cluster servers, data, or databases, follow the instructions in these sections:
 - “How to Recover a Cluster Server” on page 51
 - “How to Recover Cluster Data” on page 48
 - “How to Recover the Cluster Database” on page 49

How to Prepare for Recovering NetWorker Software

Before you can restore NetWorker configuration files and/or indexes, you must reinstall the NetWorker software from the original media on the damaged system.

To reinstall the NetWorker software, follow these instructions:

1. Replace the damaged disk if necessary. Make sure the replacement disk is as large or larger than the original disk.
2. Use the saved disk partition information to re-create the disk partitions with the same structure as the original disk. Format each partition on the disk with the same filesystems it had before (for example: FAT, NTFS, or HPFS). See “Disk Information” on page 15 for additional information.
3. Reinstall the NetWorker software in the same location in which it originally resided. Refer to the *Quick Start Guide* for installation instructions. Reinstall any NetWorker patches you had installed prior to the disaster.

NetWorker servers only: You do not need to reload the license enablers if the `\nsr\res` directory (configuration files) still exists. If the `\nsr\res` directory was destroyed, the license enablers are recovered when you recover the configuration files.

You might have several different releases of NetWorker software; reinstall the same release that was running prior to the disaster or a later release. The release must equal to or later than the release used for the backups.

NetWorker servers only: If you back up to an autochanger and want to use it during the remainder of the disaster recovery, add and configure the autochanger with the `jbconfig` command after installing NetWorker. See “Recovery with Autochangers” on page 21 for more information.

If this system is a server, continue with the disaster recovery by restoring the NetWorker indexes and configuration files. See “How to Recover NetWorker Indexes and Configuration Files” on page 39 for instructions.

If this system is a NetWorker client or storage node, continue following the instructions in “How to Recover NetWorker Clients and Storage Nodes”.

How to Recover NetWorker Clients and Storage Nodes

To recover clients and storage nodes, you simply need to reinstall the NetWorker client software and recover their configuration files, using the NetWorker User program. All client and storage node binaries for NetWorker for Windows NT are contained in the client package.

The NetWorker clients and storage nodes, similar to NetWorker servers, each have a `\nsr` directory that contains special configurations created during the initial installation. During the disaster recovery procedure, you will recover the `\nsr` directory, which restores the clients and storage nodes to their status prior to the disaster.

To recover a NetWorker client or storage node, follow these steps:

1. Log on as Administrator.
2. Start the NetWorker User program.
3. Click the Recover speedbar button to open the Recovery window. NetWorker displays the system's directory structure in the Recover window.
4. Select and mark the NetWorker directory for recovery (the default location is `\win32app\nsr`).
5. Click the Start speedbar button to begin the recovery.
6. Either restart the system once the recovery is completed, or stop and restart the NetWorker Remote Exec Service by using the Windows NT Service Control panel.

The NetWorker client or storage node should be restored to its status prior to the disk crash.

How to Recover NetWorker Indexes and Configuration Files

These steps only apply to NetWorker servers; because only servers store and maintain the indexes and configuration files. Use the `mmrecov` command to recover the NetWorker indexes and configuration files that reside in the `\nsr` directory.

If the operating system and the NetWorker software were also destroyed, you must reinstall them prior to recovering the `\nsr` directory contents. See "Operating System Recovery" on page 34 and "NetWorker Software Recovery" on page 37.

When you use the `mmrecov` command to recover the `\nsr` directory, you recover the contents of three important directories:

- `\nsr\mm` (media manager) directory – contains the NetWorker media index that tracks all the NetWorker backup volumes and their save sets.
- `\nsr\index\server-name` directory – contains the server index, which has a list of all the server files that were backed up prior to the disaster. The server index includes information about the client indexes, for example,

where they are located and how to recover them. Later, after you complete the recovery of the server index, you can use the NetWorker User program to recover the client indexes.

- `\nsr\res` directory – contains special NetWorker configuration files. The `nsr.res` file includes the list of clients that belong to the server, customized client configurations or selections, and device and registration information. The `nsrjb.res` file includes the location of the backup volumes in the jukebox and label template information. Unlike the server index, the contents of this directory cannot be reliably overwritten while NetWorker is running. Therefore, **mmrecov** recovers the `\nsr\res` directory as `\nsr\res.R`, which you rename later.

Using the mmrecov Command

Use **mmrecov** to recover the NetWorker server index and configuration files in the `\nsr` directory. Information in this section applies only to NetWorker servers.

The **mmrecov** command prompts you for the bootstrap save set identification number (ssid or save set ID). If you followed the recommended procedures to prepare for loss of critical data or a disk crash, you have a copy of the bootstrap file (either hardcopy or an electronic file) with the name of the backup media you need and the bootstrap save set ID.

In the following example, ssid “20076” is the most recent bootstrap backup:

```
August 20 03:30 1996 NetWorker bootstrap information Page 1
date      time      level  ssid   file   record  volume
8/08/96   7:44:38   full   19987  5      0       mars.004
8/09/96   6:12:09   full   20008  48     0       mars.005
8/10/96   6:14:23   full   20072  63     0       mars.006
8/11/96   6:29:58   full   20076 130    0       mars.006
```

If you do not have this information, you can still recover the indexes by finding the ssid using the **scanner -B** command. (See “Bootstrap Save Set ID” on page 14.)

With the operating system and NetWorker software in place, recover the indexes and configuration files from the backup media:

1. Find the bootstrap information, which you need for the next two steps.
2. Retrieve the backup media that contains the most recent backup named bootstrap and load it into the server’s backup device.

3. Use the **mmrecov** command to extract the contents of the bootstrap save set. For example:

```
D:\win32app\nsr\bin>mmrecov
mmrecov: Using mars.digital.com as server
NOTICE: mmrecov is used to recover the NetWorker server's
on-line file and media indexes from media (backup tapes or
disks) when either of the server's on-line file or media
index has been lost or damaged. Note that this command
will OVERWRITE the server's existing on-line file and
media indexes. mmrecov is not used to recover NetWorker
clients' on-line indexes; normal recover procedures may be
used for this purpose. See the NetWorker Administrator's
Guide, Windows NT Version, for more details.

\\.\Tape0
\\.\Tape1
What is the name of the device you plan on using
[\\.\Tape0]?
Enter the latest bootstrap save set id []: 20076
Enter starting file number (if known) [0]: 130
Enter starting record number (if known) [0]: 0
Please insert the volume on which save set id 20076 started
into \\.\Tape0. When you have done this, press <RETURN>:
Scanning \\.\Tape0 for save set 20076; this may take a
while...
scanner: scanning dlt7000 tape mars.006 on \\.\Tape0
D:\win32app\nsr\res\nsr.res
D:\win32app\nsr\res\nsrjb.res
D:\win32app\nsr\res\nsrlla.res
D:\win32app\nsr\res\
nsrmmdbasm -r D:\win32app\nsr\mm\mmvolume\
D:\win32app\nsr\mm\
nsrindexasm -r D:\win32app\nsr\index\mars.digital.com\db\
D:\win32app\nsr\index\mars.digital.com\
D:\win32app\nsr\index\
```

NetWorker Software Recovery

```
D:\win32app\nsr\  
D:\win32app\  
D:\  
mars.digital.com: 68 records recovered, 0 discarded.  
scanner: ssid 20076: scan complete  
scanner: ssid 20076: 1.2 MB, 12 file(s)  
\\.\Tape0: mount operation in progress  
\\.\Tape0: verifying label, moving backward 2 file(s)  
\\.\Tape0: verifying label, moving backward 1 file(s)  
nsrindexasm: Pursuing index pieces of  
D:\win32app\nsr\index\mars.digital.com\db from  
mars.digital.com.  
\\.\Tape0: mounted dlt7000 tape mars.006  
The bootstrap entry in the on-line index for  
mars.digital.com has been recovered.  
The complete index is now being reconstructed from the  
various partial indexes which were saved during the normal  
save for this server.  
If your resource files were lost, they are now recovered  
in the 'res.R' directory. Copy or move them to the 'res'  
directory, after the index has been reconstructed and you  
have shut down the service. Then restart the service.  
Otherwise, just restart the service after the index has  
been reconstructed.  
D:\win32app\nsr\bin>Recovering files into their original  
locations.  
nsrindexasm -r D:\win32app\nsr\index\mars.digital.com\db\  
merging with existing mars.digital.com index  
mars.digital.com: 10712 records recovered, 0 discarded.  
nsrindexasm -r D:\win32app\nsr\index\mars.digital.com\db\  
merging with existing mars.digital.com index  
mars.digital.com: 64 records recovered, 0 discarded.  
nsrindexasm -r D:\win32app\nsr\index\mars.digital.com\db\  

```

Chapter 2: Disaster Recovery for Windows NT

```
merging with existing mars.digital.com index
mars.digital.com: 290 records recovered, 0 discarded.
Received 3 matching file(s) from NSR server
'mars.digital.com'
Recover completion time: Wed Jan 28 16:22:19 1998
The index for 'mars.digital.com' is now fully recovered.
The NetWorker server indexes and configuration files
should be fully recovered.
```

Recovery from Clone Volumes

For recovery from clone volumes, use the **mmrecov** command, as described in “Using the mmrecov Command” on page 40.

Select the bootstrap save set ID that includes the information associated with the cloned save set. The most recent bootstrap is the last save set listed in the bootstrap output.

In the following example, the *ssid* of the most recent bootstrap is “17851237.” The clone of the bootstrap save set resides on *mars_c.3*. The value for the file location is “6,” and the value for the record location is “0.”

```
Jun 17 22:21 1996 mars's NetWorker bootstrap information Page 1
date      time      level  ssid      file  record  volume
6/14/96   23:46:13 full   17826163  48    0        mars.1
6/14/96   23:46:13 full   17826163  12    0        mars_c.1
6/15/96   22:45:15 9      17836325  87    0        mars.2
6/15/96   22:45:15 9      17836325  24    0        mars_c.2
6/17/96   22:20:25 9      17851237  52    0        mars.3
6/17/96   22:20:25 9      17851237 6    0        mars_c.3
```

After **mmrecov** recovers the bootstrap save set, it continues recovering the remainder of the server’s client index to complete the recovery. The cloned bootstrap contains information about the original and cloned volumes.



Important: To most easily recover data from clone volumes, make sure that all the required clone volumes are mounted in attached devices at the time you run **mmrecov**. If some of the clone volumes are not online, **mmrecov** attempts to recover the server's client index from the original volume, not the clone volume.

Based on the preceding example of bootstrap output, the *mars_c.1* and *mars_c.3* volumes both need to be online. If the *mars_c.3* volume is the only one online, **mmrecov** also requests *mars.1*.

How to Rename the Configuration Files Directory

The information in this section only applies to NetWorker servers.

Unlike the `\nsr\index` directory, the `\nsr\res` directory that contains the configuration files cannot be reliably overwritten while NetWorker is running. Therefore, **mmrecov** recovers the `\nsr\res` directory as `\nsr\res.R`. To complete the recovery of the NetWorker configuration files, shut down NetWorker, rename the recovered `\nsr\res.R` directory to `\nsr\res`, and then restart NetWorker.

When the **mmrecov** program is complete, it displays this message:

```
The NetWorker server indexes and configuration files should  
be fully recovered.
```

To complete the recovery of the NetWorker configuration files, follow these steps:

1. Stop the NetWorker Backup and Recover Server service by using the Windows NT Service Control Panel.
2. Rename the existing `\nsr\res` directory to `\nsr\Res.orig`.
3. Rename the recovered `\res.R` directory to `\nsr\res`.
4. Restart the NetWorker Backup and Recover Server service by using the Windows NT Service Control Panel.
5. After you verify that the NetWorker configurations are correct, you can remove the *res.orig* directory.

How to Complete the Recovery of the NetWorker Server Data

The information in this section only applies to NetWorker servers.

After you recover the server's indexes and configuration files, you can recover the remainder of the server data that includes the Registry and client indexes by using the NetWorker User program.

To recover the remainder of the NetWorker data, follow these steps:

1. Log on as Administrator.
2. Open the NetWorker User program.
3. Click the Recover speedbar button to open the Recover window. NetWorker displays the system's directory structure in the Recover window.
4. Select and mark the NetWorker directory for recovery (the default location is `\win32app\nsr`).
5. Deselect the following directories and files before you recover the data:
 - `\nsr\index\server-name` file – recovered when you ran the **mmrecov** command.
 - `\nsr\res` and the `\nsr\mm` directories – recovered when you ran the **mmrecov** command. If you recover the `/nsr/res` directory and you used the autochanger to perform the disaster recovery, you will lose any special configurations you created when you added and configured the autochanger for recovery
6. Click the Start speedbar button to begin the recovery.
7. Either restart your system once the recovery has been completed, or stop and restart both the NetWorker Remote Exec Service and the NetWorker Backup and Recover Server Service by using the Windows NT Service Control Panel.

After you recover the server data, inventory the autochanger so NetWorker knows which slots contain which volumes.

The NetWorker server should be restored to the status it had prior to the disk crash.

Recovery to a New Server

This section describes a situation in which your original NetWorker server is beyond repair, so you want to move NetWorker to a new server. This procedure assumes that you are not updating the operating system or the NetWorker software.

Recovery to a New Server



Important: Do not make major changes to the operating system or NetWorker software at the same time you move to a new server.

If you want to make changes to the operating system or the NetWorker software, we strongly suggest that you configure the new server exactly like the original, using the same version of the operating system and NetWorker software. After configuring the new server, make sure the system is operational, perform a couple of successful backups, and then update or upgrade the operating system or the NetWorker software, one at a time.

To move NetWorker to a new server, use the same steps for recovering the operating system and NetWorker software, including the indexes and configuration files. Follow the instructions in these sections:

- “Operating System Recovery” on page 34
- “How to Prepare for Recovering NetWorker Software” on page 38
- “How to Recover NetWorker Indexes and Configuration Files” on page 39
- “How to Rename the Configuration Files Directory” on page 44
- “How to Complete the Recovery of the NetWorker Server Data” on page 45

However, you should be aware of the following requirements for configuring the software:

- Use the same *hostname* for the new NetWorker server. You must use the same hostname because the server indexes were created under the original NetWorker server name.
- Make sure the original server name is listed as an alias for the server in the Create Client dialog box of the NetWorker Administrator program.
- If the new server has a different TCP/IP address, it will be assigned a new host ID by NetWorker, as a result, you need to reregister the NetWorker software.

After you move the NetWorker server to another system, you must recover the resource database (*nsr.res* file) to ensure that you carry over the same resource and attribute settings to the new NetWorker server.

If the new server has a different host ID, you have 15 days to reregister the software with DIGITAL. Refer to the “Enabling and Registering NetWorker” section of the *Quick Start Guide*.

DIGITAL will send you a DIGITAL NetWorker *Host Transfer Affidavit*, which you must complete and return. After DIGITAL receives the signed affidavit, DIGITAL sends you a new authorization code to enter into the Auth code field of the Registration window.

After successfully moving your server, check the following:

- Verify that the server and all the clients are included in a scheduled backup.
- Schedule a full backup, or use the **savegrp -O** command to back up the server and all the clients as soon as possible. (Manual backups do not back up the server or client indexes.)
- Use the Recover window in the NetWorker User program to make sure all the client indexes are browsable and, therefore, “recoverable.”

DIGITAL Alpha NT Considerations

If you intend to perform a disaster recovery on a DIGITAL Alpha NT system, before following the steps described in this guide, consult the DIGITAL documentation for information. Follow the procedures that describe how to properly setup Windows NT to ensure a successful recovery. Use the same procedures for operating NetWorker on an Intel or DIGITAL Alpha NT system.

Microsoft Cluster Server Support

This section explains the current implementation of NetWorker Power Edition support for the Microsoft Cluster Server (MSCS) and describes how to back up and recover the data and *cluster database* for a Microsoft Cluster Server.

The implementation of MSCS that was released in Windows NT 4.0 Enterprise Edition is a failover model for a two-server cluster. Each system has private disks; the systems also share some disks. Failover for a NetWorker server is not currently available.

Recovery for Microsoft Cluster Servers include the following choices:

- Lost cluster data – the cluster is still running, but shared data, such as files applications, or documents has been lost. “How to Recover Cluster Data” on page 48.
- Damaged cluster program (database) – the cluster program or database has been damaged and you want to recover the database from a previous point in time. See “How to Recover the Cluster Database” on page 49.

- Loss of one or both of the cluster nodes – At least one of the servers in the cluster has suffered a disk crash. See “How to Recover a Cluster Server” on page 51.

Backing Up Cluster Data

The first phase of NetWorker Power Edition support for MSCS provides backup and recovery of the data on the systems in a cluster as though the systems were independent (two separate systems).

To prepare for regular backups, install the NetWorker client software on both systems in the cluster. Use only the system’s private disks for the installation. Configure the NetWorker client running on each system to back up the private disk on that system, as well as the shared storage owned by that system.

To back up either a private or shared disk, configure them either by driver letter or by using Save Set ALL. Each system in the cluster must be configured separately; you can specify Save Set ALL for both system. For example, when Save Set ALL is specified for *node_A*, all private disks of *node_A* as well as all shared disks owned by *node_A* are backed up.

To provide NetWorker server support to the cluster, install the NetWorker server only on a private disk of any of the systems in the cluster (for example, *node_A*). Any NetWorker clients that want to connect to the NetWorker server in the cluster should use the hostname of the node where the NetWorker server is installed (for example, *node_A*). You can also back up all systems in the cluster to a NetWorker server that does not belong to the cluster.

How to Recover Cluster Data

Recovering data backed up from private disks on a cluster node is similar to recovering data on a system that is not part of a cluster. Follow the regular recovery instructions described in this chapter.

To recover data from a shared disk, determine which node owned the shared disk when the most recent backup of the shared disk occurred. Ownership of shared disks can change as a result of some failure in the node or for some administrative purposes. Therefore, it is possible that a particular shared disk that is backed up one time as the storage of *node_A* might later be backed up as the shared disk of *node_B*.

Note: Looking at *CLUSDB.LOG* (cluster database activity log) would easily reveal what happened and when. Unfortunately, this file cannot be accessed for viewing when the cluster is up and running. Also, this database has a special format, so it can only be viewed with a special viewing tool, and no such tool is available at this time. Therefore, you can only check dates in the backed-up files before recovering them.

If the most recent backup of the shared disk was made from the node that now owns the shared disk, follow the regular recovery instructions.

If the node that currently owns a shared disk is not the one used during the most recent backup, you can recover the data of the shared disk in one of two ways:

- Use the directed recovery process.
- Move the resource group that contains this shared disk to the appropriate node before you recover the data.

How to Recover the Cluster Database

The cluster database is maintained synchronously on both systems; as a result, backing up or recovering the cluster database in a consistent state is an issue. NetWorker backs up the cluster database like any other Registry file.

To recover the cluster database, do the following:

1. Use the Services Control Panel to stop the cluster server on *node_B*, and set the Startup parameter of the Cluster Server service to Manual.
2. Uninstall the cluster server from *node_B*. This is necessary to enable access to the shared disk, which is assigned as the *quorum* resource, so that the quorum log stored on this disk can be deleted for a successful recovery of the cluster database.
3. Shut down *node_B*.
4. Set the Startup parameter of Cluster Server service to Manual on *node_A*.
5. Shut down *node_A*.
6. Start *node_B*.
7. Move the *quolog.log* file and **.tmp* files from the MSCS directory on the shared disk, which has been assigned as the quorum resource, to a safe location (such as a private disk). These moved files can be deleted once a successful recovery of the cluster database is complete.

You must remove these files in the MSCS directory from the shared disk, because the cluster server maintains some recovery information in the *quolog.log* file. If you do not remove this file, the cluster database recovery might not have any effect, since the cluster database is updated with the latest information present in *quolog.log* (by the cluster server). Removing the other (**.tmp*) files is only for cleanup purposes.

8. Shut down *node_B*.
9. Start *node_A*.

10. Move the *CLUSDB* and *CLUSDB.LOG* files from the cluster directory in *node_A* (the default location is *c:\winnt\cluster*) to a safe location. These moved files can be deleted once a successful recovery of the cluster database is complete.

You must move *CLUSDB.LOG* out of the cluster directory to remove any recovery information on activities in the cluster database maintained by the cluster server. If you do not remove this file, the cluster database recovery might not have any effect, since the cluster database is updated with the latest information present in *CLUSDB.LOG* (by the cluster server).

11. Use NetWorker to recover *CLUSDB* from the Registry filesystem, and move the file to the cluster directory.



Important: NetWorker restores this file to the *config* location in the system directory. You must move the recovered *CLUSDB* file from this *config* directory (for example, *C:\WINNT\system32\config*) to the cluster directory (for example, *C:\WINNT\cluster*).

NetWorker does not restore this file to the cluster directory because, if the cluster service is not started during system boot, the Cluster entry is not added as one of the entries in the Registry. Consequently, the NetWorker method of locating each major Registry file does not return a valid value for the *CLUSDB* Registry file. For this reason, the *config* directory under the system directory is used as the default location (for example, *C:\WINNT\system32\config*) for recovering the cluster database.

12. Restart *node_A*.
13. Start the Cluster Server service, either using the Services window or the Cluster Administrator program on *node_A*.
14. Set the Startup parameter of the Cluster Server service to Automatic so that the cluster server starts automatically when *node_A* boots the next time.
15. Evict (remove) *node_B* from the cluster if it is part of the cluster. You can use the Cluster Administrator GUI to evict *node_B*.

The cluster server software cannot be installed in *node_B* to make it join the cluster if the cluster server thinks that *node_B* is still a member.

16. Install the cluster in *node_B*, and make *node_B* join the cluster during installation.

How to Recover a Cluster Server

This section provides instructions for performing a disaster recovery for one system in a server cluster or for both systems in a server cluster. Three possible scenarios are provided for recovering a cluster server from a disaster.



Important: As a precaution and to ensure proper termination, never turn off the power to either of the systems in the cluster while following these instructions.

In this scenario there are two systems in the cluster: *node_A* and *node_B*. Only *node_A* needs to be recovered from a disaster. *Node_B* remains undamaged and fully operational.

Follow these instructions to perform a disaster recovery for only one system in the cluster:

1. Shut down both systems: *node_A* and *node_B*.
2. Perform a disaster recovery on the appropriate machine in the cluster, in this case *node_A*. Refer to the instructions in this chapter that best apply to recovering the system from a disaster.
3. Shut down *node_A*.
4. Restart *node_B* (the system that did not require disaster recovery), restart the cluster server software if it is not already running.
5. Restart the system, *node_A*, for which you just performed a disaster recovery, and restart the cluster server software.

In the second scenario both systems – *node_A* and *node_B* – need to be recovered from a disaster. These instructions assume that all cluster data, including binaries, Registry entries, and configurations (related to the cluster) have been safely backed up.

Follow these instructions to perform a disaster recovery for both nodes in the cluster:

1. Perform a disaster recovery on both *node_A* and *node_B*.
This includes recovering files to the shared disk where the quorum resource is stored. Refer to the instructions in this chapter that best apply to recovering the systems from a disaster.
2. Follow the instructions in “How to Recover the Cluster Database” on page 49 if you need to recover the cluster database.

If you need to perform a disaster recovery for both systems in the cluster but you question the integrity of the backups for the cluster-related data (other than the cluster database), follow these instructions:

1. Perform a disaster recovery for both systems.
2. Uninstall the cluster server software from both systems.
3. Shut down both systems.
4. Start *node_A*, and reinstall the cluster server software.
5. Set the Startup parameter of Cluster Server service to Manual on *node_A*.
6. Shut down *node_A*.
7. Move the *quolog.log* and **.tmp* files from the MSCS directory on the shared disk, which has been assigned as the quorum resource, to a safe location (such as a private disk). These moved files can be deleted once a successful recovery of the cluster database is complete.
8. Move the *CLUSDB* and *CLUSDB.LOG* files from the cluster directory on *node_A* (the default location of which is *c:\winnt\cluster*) to a safe location. These moved files can be deleted once a successful recovery of the cluster database is complete.
9. Use NetWorker to recover *CLUSDB* from the Registry filesystem, and move the file to the cluster directory.
10. Start the Cluster Server service, either using the Services window or the Cluster Administrator program on *node_A*.
11. Set the Startup parameter of the Cluster Server service to Automatic so that the cluster server starts automatically when *node_A* boots the next time.
12. Evict (remove) *node_B* from the cluster if it is part of the cluster. You can use the Cluster Administrator GUI to evict *node_B*.
13. Restart *node_B*.
14. Install the cluster in *node_B*, and make *node_B* join the cluster during installation.

See “How to Recover the Cluster Database” on page 49 if you want more instructions for restoring a cluster database.

Chapter 3: Disaster Recovery for UNIX

Use the information in this chapter to determine which disaster recovery procedures you should follow for NetWorker for UNIX servers and clients. However, it is important that you read and follow the procedures in Chapter 1 before you ever need to recover from a disaster. Chapter 1 explains how to prepare for recovering from a disaster and defines basic terms, procedures, and concepts used throughout this guide.

This chapter includes procedures for recovering from the following kinds of disasters:

- Loss of a drive or partition that contains critical data other than the operating system or NetWorker software
- Loss of the operating system
- Loss of a drive or partition that contains NetWorker software, which typically includes the NetWorker indexes and configuration files
- Loss of an entire NetWorker server to the extent that you need to recover to a new system

It is difficult to provide step-by-step instructions for performing a disaster recovery for a specific situation, because every situation is unique. The examples in this chapter are designed to give you *general principles* to recover from a disaster and to help you understand the procedures.

Requirements

While performing any of the disaster recovery procedures included in this chapter, keep in mind the requirements listed in this section. Fulfill the requirements pertinent to the disaster recovery procedure you are following.

Requirements

Requirements for Replacing the Hardware

If hardware becomes damaged or destroyed, use the following selections to install and configure your new system hardware correctly:

- Ensure that the replacement disk is as large or larger than the original disk.
- When replacing the hardware, try to use the same controller, driver, and SCSI ID used prior to the disaster.
- Re-create the same size or larger disk partitions on the new disk/system.
- Format the disk partitions using the same formats used by the original disk.

Requirements for Reinstalling the Operating System

If the operating system is damaged or destroyed, adhere to the following list when you reinstall UNIX:

- Reinstall the same version of UNIX.
- Use the same computer name, TCP/IP host name, and DNS domain name.
- Reinstall any operating system patches that existed before the disaster.
- Reinstall the device and SCSI drivers.
- Make sure all network protocols are working properly.
- After reinstalling UNIX, reboot your system, and log on as root. Make sure no error messages occur when you start up the system and that all the devices are recognized by the operating system.

Requirements for Reinstalling NetWorker

Fulfill the following requirements to ensure successful reinstallation of NetWorker. Refer to the *NetWorker Quick Start Guide* for installation instructions.

- Reinstall the same version of the NetWorker software.
- Reinstall NetWorker where it originally resided.
- Reinstall any patches that were installed prior to the disaster.
- For NetWorker servers, you will have to run additional procedures to retrieve the NetWorker server's indexes and configuration files. See "How to Recover NetWorker Indexes and Configuration Files" on page 61 for information.
- For NetWorker clients or storage nodes see "How to Recover NetWorker Clients and Storage Nodes" on page 60.

Critical Data Recovery

The following example assumes the disk containing the operating system and NetWorker software is still operational, but another disk containing critical data has been lost. The example applies to both UNIX NetWorker servers and clients.

If the disk is damaged beyond repair, replace it with a new disk the same size or larger than the original disk. You need a disk large enough to hold all the data you plan to recover.

How to Recover Critical Data

To recover the critical data, follow these steps:

1. Install the replacement disk. Make sure the operating system and kernel recognize the new disk.
2. Use the saved disk partition information to re-create the disk partitions with the same structure as the original disk. See “Disk Information” on page 15.

If you did not save the disk information, it should still be available because it is located on the primary disk, which in this case, is operational. Look at */etc/filesystems* for an IBM AIX system, */etc/vfstab* for a Solaris system, */etc/fstab* for a SunOS system, and use SAM for an HP-UX system to find the original disk partition information. However, you must guess how big each partition should be.

3. Use the output from the **disk information** command to make a filesystem for each raw partition you plan to recover, then mount the block partition. (NetWorker does not initialize or create filesystems; it recovers data into existing filesystems.)
4. Use the appropriate UNIX command to format the replacement disk. For SunOS and Solaris systems, use **newfs** or **mkfs**. For AIX systems, use SMIT. For HP-UX systems, use **mkfs**.



Important: Make sure the disk is no longer needed, because you will completely destroy the disk contents when you use SMIT, **newfs**, or **mkfs**.

Run **newfs** on a SunOS system:

```
# newfs /dev/rsd1g
...
```

Operating System Recovery

```
# mount /dev/sdlg /export
# newfs /dev/rsdlh
# mount /dev/sdlh /home
```

Run **newfs** on a Solaris system:

```
# newfs /dev/rdisk/c0t1d0s5
# mount /dev/dsk/c0t1d0s5
# newfs /dev/rdisk/c0t1d0s7
# mount /dev/dsk/c0t1d0s7
```

Use SMIT on an AIX system:

```
# smit crfs
```

SMIT displays a window where you answer questions pertaining to creating and mounting filesystems.

5. After creating and mounting all the filesystems on the replacement disk, use Save Set Recover feature in the **nwadmin** program or the normal recovery procedure in the **nwrecover** program to recover the files.

For an explanation about the best recovery method for your lost data, see the *NetWorker Administrator's Guide*.

Operating System Recovery

This example assumes a disk with the operating systems has been damaged or completely destroyed. You need to replace the damaged disk and reinstall the operating system. If the disk was not completely destroyed and either the operating system or NetWorker is still operational, use only the steps in this section that apply to your situation. Instructions in this section apply to NetWorker servers and clients, unless otherwise specified.



Important: When you recover the operating system, you must do so in single-user mode from the system console, not from the X window system.

How to Prepare for Recovering the Operating System

To prepare for recovering the operating system for either a server or client, follow these instructions:

1. Replace the damaged disk if necessary. Make sure the replacement disk is as large or larger than the original disk.

2. Use the saved disk partition information to re-create the disk partitions with the same structure as the original. See “Disk Information” on page 15.
3. Use the output from the **disk information** command to make a filesystem for each raw partition that you plan to recover, then mount the block partition. (NetWorker does not initialize or create filesystems; it recovers data into existing filesystems.)
4. Use the appropriate UNIX command to format the replacement disk. For SunOS and Solaris systems, use **newfs** or **mkfs**. For AIX systems, use SMIT. For HP-UX systems, use **mkfs**.
5. Reinstall the operating system in the same location where it originally resided, using the original software and accompanying documentation. Use the same system name, TCP/IP hostname, and DNS Domain name used prior to losing the operating system.

You can choose to fully configure the operating system now, or you can install the minimum number of files and make the minimum number of configurations required to create an operational networked system. See “Restoring the Operating System” on page 18 for more information.

6. Install and configure the SCSI controller and tape device drivers.
7. Reinstall the NetWorker software, using the original software and accompanying documentation. On a NetWorker client, you only need access to the NetWorker binaries. You can run NetWorker from the *nsr_extract* directory or NFS-mount the binaries from another system running NetWorker. Refer to the *NetWorker Quick Start Guide* for installation instructions. Reinstall any NetWorker patches you had installed prior to the disaster.

You might have several different releases of NetWorker software; reinstall the same release that was running prior to the disaster or a later release. The release must be equal to or later than the release used for the backups.

NetWorker servers only: When you reinstall the NetWorker server software, NetWorker automatically rediscovers indexes and configuration files if they are not corrupted.

NetWorker clients only: The client system is now ready to recover its data from the NetWorker server.

You can also use the following method to access the NetWorker binaries for recovery. If you have another system running NetWorker that is like the system being recovered on the network, you can NFS-mount the NetWorker binaries on the damaged system.

NetWorker Software Recovery

For example:

```
# mount venus:/usr/etc /mnt
# /mnt/recover -s server -q
recover> add /
recover> force
recover> recover
```

8. Install and configure the SCSI controller and tape device drivers.
9. Reboot the system, and log on as root.

How to Recover the Operating System

First create and mount all the filesystems on the replacement disk. Then to recover the UNIX operating system, use the Save Set recover feature in the **nwadmin** program or the normal recovery procedure in the **nwrecover** program to recover the necessary data.

NetWorker Software Recovery

The following example for recovering the NetWorker binaries, assumes a disk containing the NetWorker software has been damaged or completely destroyed. This example also assumes that the UNIX operating system is installed and operating properly.

The set of instructions you need to follow in this section depend upon which system you lost (server, client, or storage node) and the extent of the damage. Refer to the following list of disaster recovery scenarios to determine which set of instructions apply to your situation.

- If you are recovering NetWorker clients and storage nodes, you need to follow the instructions in these sections:
 - “How to Prepare for Recovering NetWorker Software” on page 59
 - “How to Recover NetWorker Clients and Storage Nodes” on page 60
- If you are recovering a NetWorker server that lost its indexes and configuration files, you need to follow the instructions in these sections:
 - “How to Prepare for Recovering NetWorker Software” on page 59
 - “How to Recover NetWorker Indexes and Configuration Files” on page 61
 - “How to Rename the Configuration Files Directory” on page 66
 - “How to Complete the Recovery of the NetWorker Server Data” on page 67

- If you are recovering a NetWorker server from clone volumes, you need to follow the instructions in these sections:
 - “How to Prepare for Recovering NetWorker Software” on page 59
 - “Recovery from Clone Volumes” on page 65
 - “How to Rename the Configuration Files Directory” on page 66
 - “How to Complete the Recovery of the NetWorker Server Data” on page 67
- If you are recovering NetWorker to a new server, you need to follow the instructions in this section:
 - “Recovery to a New Server” on page 68

How to Prepare for Recovering NetWorker Software

Before you can restore NetWorker configuration files and/or indexes, you must reinstall the NetWorker software from the original media on the damaged system.

To reinstall the NetWorker software, follow these instructions:

1. Replace the damaged disk if necessary. Make sure the replacement disk is as large or larger than the original disk.
2. Use the saved disk partition information to re-create the disk partitions with the same structure as the original disk. See “Disk Information” on page 15.
3. Use the output from the disk information command to make a filesystem for each raw partition that you plan to recover, then mount the block partition. (NetWorker does not initialize or create filesystems; it recovers data into existing filesystems.)
4. Use the appropriate UNIX command to format the replacement disk. For SunOS and Solaris systems, use **newfs** or **mkfs**. For AIX systems, use SMIT. For HP-UX systems, use **mkfs**.
5. Reinstall the NetWorker software, using the original software and accompanying documentation. On a NetWorker client, you only need access to the NetWorker binaries. You can run NetWorker from the *nsr_extract* directory or NFS-mount the binaries from another system running NetWorker. Refer to the appropriate *NetWorker Quick Start Guide* for detailed instructions. Reinstall any NetWorker patches you had installed prior to the disaster.

NetWorker Software Recovery

NetWorker servers only: You do not need to reload the license enablers if the `/nsr/res` directory (configuration files) still exists. If the `/nsr/res` directory was destroyed, the license enablers are recovered when you recover the configuration files.

6. If you had a link to another disk that contains the NetWorker indexes and configuration files (`/nsr`) or any other NetWorker directories located on another disk, re-create it now. For example, for AIX systems, `/nsr` is a link to `/usr/nsr`.

NetWorker servers only: If you back up to an autochanger and want to use it during the remainder of the disaster recovery, add and configure the autochanger with the `jbconfig` command after installing NetWorker. See “Recovery with Autochangers” on page 21 for more information.

You can also use the following method to access the NetWorker binaries for recovery. If you have another system running NetWorker that is like the system being recovered on the network, you can NFS-mount the NetWorker binaries to the damaged system.

For example:

```
# mount venus:/usr/etc /mnt
# /mnt/recover -s server -q
recover> add /
recover> force
recover> recover
```

If this system is a server, continue with the disaster recovery by restoring the NetWorker indexes and configuration files. See “How to Recover NetWorker Indexes and Configuration Files” on page 61 for instructions.

If this system is a NetWorker client or storage node, see “How to Recover NetWorker Clients and Storage Nodes” for instructions.

How to Recover NetWorker Clients and Storage Nodes

To recover clients and storage nodes, you simply need to reinstall the NetWorker client and storage node software, and then recover their configuration files, using the `nwrecover` program.

The NetWorker clients and storage nodes, similar to NetWorker servers, each have a `\nsr` directory that contains special configurations created during the initial installation. During the disaster recovery procedure, you will recover the `\nsr` directory, which restores the clients and storage nodes to their status prior to the disaster.

To recover a NetWorker client or storage node, follow these steps:

1. Log on as root.
2. Start the **nwrecover** program.
3. Click the Recover speedbar button to open the Recover window. NetWorker displays the system's directory structure in the Recover window.
4. Select and mark the NetWorker directory for recovery.
5. Click the Start speedbar button to begin the recovery.
6. Restart **nsrexecd**.

The NetWorker client or storage node should be restored to the status it had prior to the disk crash.

How to Recover NetWorker Indexes and Configuration Files

These steps only apply to NetWorker servers; because only servers store and maintain the indexes and configuration files. Use the **mmrecov** command to recover the NetWorker indexes and configuration files that reside in the */nsr* directory.

If the operating system and the NetWorker software were also destroyed, you must reinstall them prior to recovering the */nsr* directory contents. See “Operating System Recovery” on page 56 and “NetWorker Software Recovery” on page 58.

When you use the **mmrecov** command to recover the */nsr* directory, you recover the contents of three important directories:

- */nsr/mm* (media manager) directory – contains the NetWorker media index that tracks all the NetWorker backup volumes and their save sets.
- */nsr/index/server-name* directory – contains the server indexes, which has a list of all the server files that were backed up prior to the disaster. The server index includes information about the client indexes, for example, where they are located and how to recover them. Later, after you complete the recovery of the server index, you can use the **nwrecover** program to recover the client indexes.
- */nsr/res* directory – contains special NetWorker configuration files. The *nsr.res* file includes the list of clients that belong to the server, customized client configurations or selections, and device and registration information. The *nsrjb.res* file includes the location of the backup volumes in the jukebox and label template information. Unlike the indexes, the

NetWorker Software Recovery

contents of this directory cannot be reliably overwritten while NetWorker is running. Therefore, **mmrecov** recovers the `/nsr/res` directory as `/nsr/res.R`, which you rename later.

Using the **mmrecov** Command

Use the **mmrecov** command to recover the NetWorker server indexes and configuration files in the `/nsr` directory. Information in this section only applies to NetWorker servers.

The **mmrecov** command prompts you for the bootstrap save set identification number (ssid or save set ID). If you followed the recommended procedures to prepare for loss of critical data, you have a copy of the bootstrap file (either hardcopy or an electronic file) with the name of the needed backup media you need and the bootstrap ssid. (Never run the **mmrecov** command from root (`/`); you can use any other directory.)

In the following example, ssid “17851237” is the most recent bootstrap backup:

```
Jun 17 22:21 1997 mars's NetWorker bootstrap information
date      time      level  ssid      file  record  volume
6/14/92   23:46:13  full   17826163  48    0        mars.1
6/15/92   22:45:15  9      17836325  87    0        mars.2
6/16/92   22:50:34  9      17846505  134   0        mars.2
6/17/92   22:20:25  9      17851237  52    0        mars.3
```

If you do not have this information, you can still recover the indexes by finding the ssid using the **scanner -B** command. See “Bootstrap Save Set ID” on page 14.

With the operating system and NetWorker software in place, recover the indexes and configuration files from the backup media:

1. Find the bootstrap information, which you need for the next two steps.
2. Mount the backup media that contains the most recent backup named bootstrap in a storage device.
3. Use the **mmrecov** command to extract the contents of the bootstrap backup. (Never run the **mmrecov** command from root (`/`); you can use any other directory.) For example:

```
# mmrecov
mmrecov: Using mars.digital.com as server
NOTICE: mmrecov is used to recover the NetWorker server's
on-line file and media indexes from media (backup tapes or
```

Chapter 3: Disaster Recovery for UNIX

disks) when either of the server's on-line file or media index has been lost or damaged.

Note that this command will **OVERWRITE** the server's existing on-line file and media indexes. `mmrecov` is not used to recover NetWorker clients' on-line indexes; normal recover procedures may be used for this purpose. See the `mmrecov(8)` and `nsr_crash(8)` man pages for more details.

Enter the latest bootstrap save set id []: **17851237**

Enter starting file number (if known) [0]: **52**

Enter starting record number (if known) [0]: **0**

Please insert the volume on which save set id 17851237 started into `/disk1/file.tape`. When you have done this, press **<RETURN>**:

Scanning `/disk1/file.tape` for save set 17851237; this may take a while...

scanner: scanning file disk file.tape on `/disk1/file.tape`

scanner: ssid 17851237: scan complete

scanner: ssid 17851237: 28 KB, 11 file(s)

`/nsr/res/nsr.res`

`/nsr/res/nsr.res`: file exists, overwriting

`/nsr/res/nsrjb.res`

`/nsr/res/nsrjb.res`: file exists, overwriting

`/nsr/res/nsrla.res`

`/nsr/res/nsrla.res`: file exists, overwriting `/nsr/res/`

`/nsr/mm/`

`/nsr/index/mars.digital.com/`

`/nsr/index/`

`/nsr/`

`/`

`nsrmmdbasm -r /nsr/mm/mmvolume/`

`nsrindexasm -r /nsr/index/mars.digital.com/db/`

`/disk1/file.tape`: mount operation in progress

`mars.digital.com`: 7 records recovered, 0 discarded.

`/disk1/file.tape`: mounted file disk file.tape

NetWorker Software Recovery

The bootstrap entry in the on-line index for mars.digital.com has been recovered. The complete index is now being reconstructed from the various partial indexes which were saved during the normal save for this server.

If your resource files were lost, they are now recovered in the 'res.R' directory. Copy or move them to the 'res' directory, after the index has been reconstructed and you have shut down the daemons. Then restart the daemons.

Otherwise, just restart the daemons after the index has been reconstructed.

```
nsrindexasm: Pursuing index pieces of
/nsr/index/mars.digital.com/db from mars.digital.com.
```

Recovering files into their original locations.

```
nsrindexasm -r ./mars.digital.com/db/
```

merging with existing mars.digital.com index

```
mars.digital.com: 753 records recovered, 0 discarded.
```

```
Received 1 matching file(s) from NSR server
'mars.digital.com'
```

```
Recover completion time: Wed Jan 28 08:37:38 1998
```

```
The index for 'mars.digital.com' is now fully recovered.
```

```
#
```

You can use NetWorker commands such as **nsrwatch** or **nwadmin** to watch the progress of the server during the recovery of the indexes and configuration files. Open a new window (shell tool) to monitor the recovery so that the **mmrecov** output is not displayed on top of the **nsrwatch** output.

```
mars# nsrwatch
```

```
Server: mars.digital.com          Wed Jan 28 08:53:54
1998
```

```
Up since: Wed Jan 28 08:35:15 1998 Version: NetWorker
5.1.Build.63 Eval
```

```
Saves: 0 session(s) Recovers: 1 session(s), 131 KB total
```

```
Device          type      volume
```

```
Disk1/file.tape  file     file.tape  reading, done
```

```
Sessions:
```

```
Messages:
```



```
Wed 08:35:11 server notice: started
Wed 08:35:22 index notice: completed checking 1
client(s)
Wed 08:36:44 /disk1/file.tape mount operation in
progress
Wed 08:36:48 /disk1/file.tape mounted file disk
file.tape
Wed 08:37:36 /disk1/file.tape mounted file disk
file.tape
Wed 08:37:36
mars.digital.com:/nsr/index/mars.digital.com (1/28/98)
starting read from file.tape of 131 KB
Wed 08:37:37
mars.digital.com:/nsr/index/mars.digital.com (1/28/98)
done
reading 1
31 KB
Pending:
```

Recovery from Clone Volumes

For recovery from clone volumes, use the **mmrecov** command, as described in “Using the mmrecov Command” on page 62.

Select the bootstrap save set ID that includes the information associated with the cloned save set. The most recent bootstrap is the last save set listed in the bootstrap output.

In the following example, the *ssid* of the most recent bootstrap is “17851237.” The clone of the bootstrap save set resides on *mars_c.3*. The value for the file location is “6,” and the value for the record location is “0.”

```
Jun 17 22:21 1996 mars's NetWorker bootstrap information Page 1
date      time      level  ssid      file  record  volume
6/14/96   23:46:13 full   17826163  48    0       mars.1
6/14/96   23:46:13 full   17826163  12    0       mars_c.1
6/15/96   22:45:15 9      17836325  87    0       mars.2
6/15/96   22:45:15 9      91783632524  0    0       mars_c.2
6/17/96   22:20:25 9      17851237  52    0       mars.3
6/17/96   22:20:25 9      17851237  6    0       mars_c.3
```

NetWorker Software Recovery

After **mmrecov** recovers the bootstrap save set, it continues recovering the remainder of the server's client index to complete the recovery. The cloned bootstrap contains information about the original and cloned volumes.



Important: To most easily recover data from clone volumes, make sure that all the required clone volumes are mounted in attached devices at the time you run **mmrecov**. If some of the clone volumes are not online, **mmrecov** attempts to recover the server's client index from the original volume, not the clone volume.

Based on the preceding example of bootstrap output, the *mars_c.1* and *mars_c.3* volumes both need to be online. If the *mars_c.3* volume is the only one online, **mmrecov** also requests *mars.1*.

How to Rename the Configuration Files Directory

The information in this section only applies to NetWorker servers.

Unlike the */nsr/index* directory, the */nsr/res* directory that contains the configuration files cannot be reliably overwritten while NetWorker is running. Therefore, **mmrecov** recovers the */nsr/res* directory as */nsr/res.R*. To complete the recovery of the configuration files, shut down NetWorker, rename the recovered *\nsr\res.R* directory to *\nsr\res*, and then restart NetWorker.

When the **mmrecov** program is complete, it displays this message:

```
The index for 'server_name' is now fully recovered.
```

To complete the recovery of the NetWorker configuration files, follow these steps:

1. Shut down the NetWorker server using the **nsr_shutdown** command:

```
# nsr_shutdown
```

2. Save the original */res* directory as */res.orig*, and rename the recovered file (*res.R*) to *res*.

```
# mv res res.orig
```

```
# mv res.R res
```

3. Restart NetWorker. When it restarts, the server uses the recovered configuration data in the recovered */res* directory.

```
# nsrd
```

```
# nsrexecd
```

4. After you verify the NetWorker configurations are correct, you can remove the *res.orig* directory.

```
# rm -r /nsr/res.orig
```

How to Complete the Recovery of the NetWorker Server Data

The information in this section only applies to NetWorker servers.

After you recover the server's indexes and configuration files, you can recover the remainder of the server data that includes the client indexes by using the **nwrecover** program.



Important: If you recover the root directory (*/*), delete */bootrec* for IBM AIX systems, */*boot* for Solaris systems, and */boot* for SunOS systems from the save set recover list, not the filesystem. If you recover these files, you will not be able to reboot your system. If you recover */boot* on a SunOS system, for example, you must use the **installboot** command to boot your system. You must always reboot a system after recovering a primary disk. For Solaris, you must also unmark the */dev* and */devices* directories from the save set recover list.

To recover the remainder of the NetWorker data, follow these steps:

1. Log on as root.
2. Open the **nwrecover** program.
3. Click the Recover speedbar button to open the Recover window. NetWorker displays the system's directory structure.
4. Select and mark the NetWorker directory for recovery.
5. Deselect the following directories and files before you recover the remainder of the server data:
 - */nsr/index/server-name* file – recovered when you ran the **mmrecov** command.
 - */nsr/res* and the */nsr/mm* directories – recovered when you ran the **mmrecov** command. If you recover the */nsr/res* directory and you used the autochanger to perform the disaster recovery, you will lose any special configurations you created when you added and configured the autochanger for recovery.
6. Click the Start speedbar button to begin the recovery.
7. Restart **nsrd** and **nsrexecd**.

Recovery to a New Server



Important: You cannot boot from recovered versions of */etc/init* or */bin/sh*. Preserve the original *init* file and *sh* file by moving them to an alternate location before you recover the root filesystem (*/*). After you recover */*, overwrite the recovered versions of the *init* file and the *sh* file with the originals. It is also a good practice to preserve the original kernel (*/hp-ux* for HP-UX 9.0x, */stand/vmunix* for HP-UX 10.x, */vmunix* for SunOS, or */kernel/unix* for Solaris) by copying it to an alternate location when you recover the root filesystem.

After you recover the server data, inventory the autochanger so NetWorker knows which slots contain which volumes.

The NetWorker server should be restored to the status it had prior to the disk crash.

Recovery to a New Server

This section describes the case where your original NetWorker server is beyond repair, so you want to move NetWorker to a new server. This procedure assumes that you are not updating the operating system or the NetWorker software.



Important: Do not make major changes to the operating system or NetWorker software at the same time you move to a new server.

If you want to make changes to the operating system or the NetWorker software, we strongly suggest that you configure the new server exactly like the original, using the same version of the operating system and NetWorker software. After configuring the new server, make sure the system is operational, perform a couple of successful backups, and then update or upgrade the operating system or the NetWorker software, one at a time.

To move NetWorker to a new server, use the same steps for recovering the operating system and NetWorker software, including the indexes and configuration files. Follow the instructions in these sections:

- “Operating System Recovery” on page 56
- “How to Prepare for Recovering NetWorker Software” on page 59
- “How to Recover NetWorker Indexes and Configuration Files” on page 61

- “How to Rename the Configuration Files Directory” on page 66
- “How to Complete the Recovery of the NetWorker Server Data” on page 67

However, you should be aware of the following requirements for configuring and registering the software:

- Use the same *hostname* for the new NetWorker server. You must use the same hostname because the server indexes were created under the original NetWorker server name.
- Make sure the original server name is listed as an alias for the server in the Client window of the **nwadmin** program.
- If the new server has a different host ID, you need to reregister the NetWorker software.

After you move the NetWorker server to another system, you must recover the resource database (*nsr.res* file) to ensure that you carry over the same resource and attribute settings to the new NetWorker server.

If the new server has a different host ID, you have 15 days to reregister the software with DIGITAL. Refer to the “Enabling and Registering NetWorker” section of the *Quick Start Guide*.

DIGITAL will send you a DIGITAL NetWorker *Host Transfer Affidavit*, which you must complete and return. Once DIGITAL receives the signed affidavit, DIGITAL sends you a new authorization code to enter into the Auth Code field of the Registration window.

After you successfully move your server, check the following:

- Verify that the server and all the clients are included in a scheduled backup.
- Schedule a full backup or use the **savegrp -O** command to back up the server and all the clients as soon as possible. (Manual backups do not back up the server or client indexes.)
- Use the **nwrecover** program’s window Recover window to make sure all the client indexes are browsable and, therefore, recoverable.

Chapter 4: Disaster Recovery for NetWare

Use the information in this chapter to determine which disaster recovery procedures you should follow for NetWorker for NetWare servers and clients. However, it is important that you read and follow the procedures in Chapter 1 before you ever need to recover from a disaster. Chapter 1 explains how to prepare for recovering from a disaster and defines basic terms, procedures, and concepts used throughout this guide.

Hopefully, you will never need to use these procedures. However, if you back up data regularly and implement a plan to recover from a disaster, you will be well prepared in case of an emergency.

This chapter includes procedures for recovering from the following kinds of disasters:

- Loss of a non-SYS volume (containing critical data)
- Loss of a full server
- Loss of the SYS volume containing the operating system and NetWorker software
- Loss of the NetWorker indexes and configuration files
- Loss of a non-replicated NDS partition
- Loss of the NDS tree in a network wide disaster
- Loss of an entire NetWorker server that you need to recover to a new system

It is difficult to provide step-by-step instructions for performing a disaster recovery for a specific situation, because every situation is unique. The examples in this chapter are designed to give you general principles to recover from a disaster and to help you understand the procedures.

NetWare Terminology for Backup and Restore

The following terms only apply to NetWare and are used throughout this chapter:

New Disaster Recovery Assistance in NetWare 4.11/IntranetWare

- Novell Directory Services (NDS) – global distributed information database for managing network resources and services.
- NetWare Loadable Module (NLM) – NetWare executables that extend the functionality of the network operating system.
- Storage Management Services (SMS) – an operating system interface that provides functionality specific to storage management products.
- Target Service Agents (TSA) – software modules capable of accessing target data, such as a filesystem or NDS. TSAs are part of the SMS open architecture.

New Disaster Recovery Assistance in NetWare 4.11/IntranetWare

NetWare 4.11/IntranetWare has improvements that provide more effective backup and restore capabilities for Novell Directory Services (NDS). The TSAs included in this release are enhanced to simplify backup and restore. These TSAs are available for NetWare 4.10 by adding *SMSUP6*.

The TSA filesystem for IntranetWare is named *TSA410.NLM*. This is the same filename as the TSA that shipped with NetWare 4.10, but the new version dated 7-23-96 or later includes the enhancements.

TSA410.NLM provides a new resource called “Server Specific Info,” which appears in the Browse window. Selecting “Server Specific Info” includes five files containing critical server information that NetWorker can back up and use for recovery:

- *SERVDATA.NDS* – contains server-specific NDS information. The *INSTALL* utility uses this file to recover from a SYS volume failure. *SERVDATA.NDS* preserves trustee assignments and other NetWare information. This file enables recovery from a SYS volume failure in a multiple-server environment where replicas exist on other servers.
- *DSMISC.LOG* – is a text file containing a list of replicas, including the replica types, stored on the backup server at the time of backup. This text file also includes a list of the other servers that were in the failed server’s replica ring. *DSMISC.LOG* provides helpful information needed to prepare NDS for recovery and restoration of the failed server. (NetWare 4.10 servers do not have this file.)
- *VOLSINFO.TXT* – is a text file containing necessary information about the server’s volumes, including name space, compression, and data migration information, at the time of backup. This file provides helpful information for preparing volumes correctly during a restore.
- *STARTUP.NCF* – is the NetWare server boot file that loads the NetWare server’s disk driver, name spaces and some SET parameters.

- *AUTOEXEC.NCF* – is the NetWare server executable batch file, located in the NetWare partition of the server's disk, used to load modules and set the NetWare operating system configuration.

The new *TSANDS.NLM*, dated 3-31-97 or later, backs up and restores all extensions to the NDS schema. Therefore, the NDS backup contains the definitions of all the classes of objects you added to the NDS database. The new *TSANDS.NLM* also now enables selective backup and restoration of portions of the NDS tree.

For more information about the changes in NetWare 4.11/IntranetWare, refer to "Backing Up and Restoring Novell Directory Services in NetWare 4.11" in *Novell Application Notes* dated October, 1996. The Application Notes are available through the Novell web site. Retrieve the *SMSUP6.EXE* update from www.support.novell.com/search/patlst.htm and look for the self-extracting *DSBCK411.EXE* file in the `\DOCS\411` directory.

Disaster Recovery Preparation

Preparing for a disaster includes storing needed items in a safe place, preferably off-site. Storing copies of the following items will assist you in performing a smooth disaster recovery. Depending upon the degree of loss or damage, you might not need to use all of these items.

- MS-DOS Installation software
- Small Computer System Interface (SCSI) Controller software
- Network Interface Card (NIC) software
- Novell operating system installation software
- Novell license software
- *AUTOEXEC.BAT* file
- *CONFIG.SYS* file
- NetWorker for NetWare software
- Bootstrap printout
- Server Specific Info files including *AUTOEXEC.NCF* and *STARTUP.NCF* (see "New Disaster Recovery Assistance in NetWare 4.11/IntranetWare" on page 72)
- Disk partition size and format information

Before performing an NDS backup or recover, read the *Novell Application Notes* section "Backing Up and Restoring Novell Directory Services in NetWare 4.11," dated October, 1996. This document explains concepts that you need to understand before working with NDS backups and recovers.

NetWorker Indexes and Configuration Files Recovery

In networks with multiple servers, NDS automatically creates replicas (copies) of the NDS database or portions of it (partitions) and stores them on other servers. This process provides a readily available backup if NDS or a partition is damaged. Do **not** circumvent this replication process.

Whenever possible, use an active replica to restore what was lost from the NDS tree. If this is not feasible, you must restore from an Storage management Services (SMS) backup:

1. Restore NDS information first.
2. Restore filesystem data and trustee rights second.

These steps must be performed in the order indicated above. Because NDS backup and restore is based on object names, the objects must exist in the tree before you can restore the filesystem data and trustee assignments for those objects. NDS should be functional (time and partitions synchronizing normally) before you proceed with a restoration.

NetWorker Indexes and Configuration Files Recovery

This section provides information for NetWorker for NetWare servers installed on NetWare 4.10, and IntranetWare 4.11 servers. The `\nsr` directory containing the NetWorker server indexes, media database, and configuration files does not reside on NetWorker clients. You use the Recover from a Disaster command in the NetWorker Utilities (*NETUTIL.NLM*) program to recover the server indexes and configuration files that reside in the `\nsr` directory.

If the operating system and the NetWorker software are also destroyed, you must reinstall them prior to recovering the `\nsr` directory contents. See “SYS Volume Recovery on a Single Server Network” on page 78 for instructions.

When you use the Recover from a Disaster command, you recover the contents of three important directories:

- `\nsr` directory – contains special NetWorker configuration files. The *nsr.res* file includes the list of clients that belong to the server, customized client configurations or selections, and device and registration information. The *nsrjb.res* file includes the location of the backup volumes in the autochanger and label template information.
- `\nsr\index\<server_name>` directory – contains the server indexes (*legatodb*), which list all the server files backed up prior to the disaster. After you recover the server index, use NetWorker to recover the client indexes.
- `\nsr\mm` directory – contains the NetWorker media index (*legatomm*) that tracks all the NetWorker backup volumes.



Important: Do not try to recover from a disaster by manually recovering the *legatomm* file for the NetWorker server. Use the Recover from a Disaster command in the NetWorker Utilities program instead.

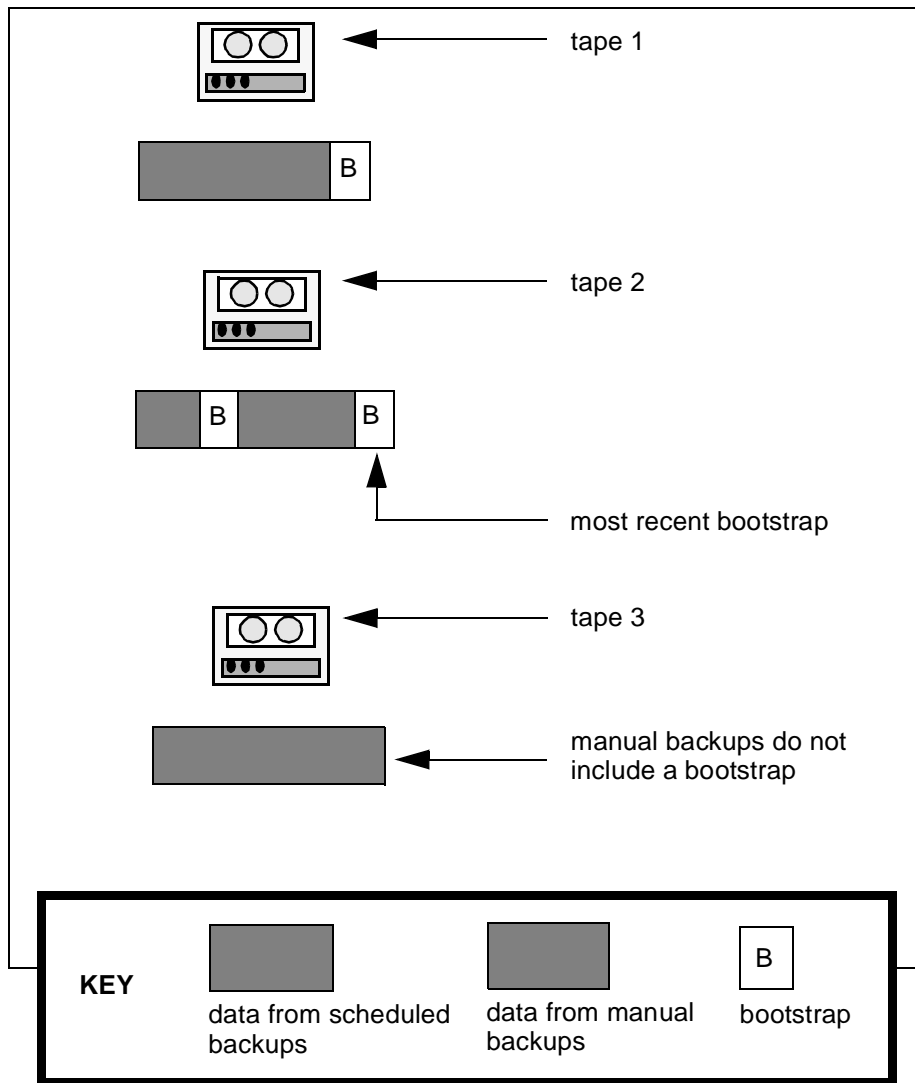
Recover from a Disaster Command

When you use the Recover from a Disaster command in the NetWorker Utilities program, NetWorker attempts to find the most current *bootstrap* information from the latest backup volume. Every time NetWorker performs a *scheduled* backup, it saves the media database, the server's client file index, and configuration files to a bootstrap save set on the backup volume. The bootstrap save set is not backed up during a manual backup.

If NetWorker cannot find the bootstrap, you must provide the next most recent backup volume.

Figure 11 on page 76 depicts what occurs when you use the Recover from a Disaster command.

Figure 11. Recover from a Disaster Command Illustrated



After NetWorker uses the bootstrap on *tape 2* to recover the NetWorker indexes, you can use the Recover command to rebuild your filesystems. You can only recover the data from *tape 1* and *tape 2*, because NetWorker now only “knows” about everything up until the last bootstrap.

If you want the data backed up on *tape 3* after the bootstrap on *tape 2*, you can recover the data using the NetWorker Utilities Recover Volume command.

Non-SYS Volume Recovery

This procedure assumes the volume containing the operating system and NetWorker software is still operational, but another non-SYS volume containing data has been lost due to a disk crash. All that is required is a restoration of filesystem data and trustee rights.

Because the disk is damaged, you need to replace it with a new disk of the same type. You need a disk large enough to hold all the data to be recovered. It should be at least as large, if not larger, than the destroyed disk.



Important: Do not delete the volume object for the failed volume from the NDS tree because you do not want to eliminate any references other objects might have to the volume.

Recovering a Non-SYS Volume

To recover a non-SYS volume, follow these steps:

1. Shut down the NetWare server and replace the damaged hard disk.
2. Re-create any non-NetWare partitions on the new disk. Use your printed copy of the system's disk information to reconstruct the partitions.
3. Restart the server, and then use the INSTALL utility to re-create the NetWare partition and redefine the volume.
4. After partitioning the replacement disk, use the Recover window to recover the filesystems and trustee rights. You can mark multiple volumes for recovery.

Full Server Recovery on a Single Server Network

This procedure assumes that you have lost everything on the server. It is strongly recommended that you configure the server exactly like it was before the disaster, using the same version of the operating system and NetWorker software. After configuring the server, make sure the system is operational by performing a couple of successful backups.

To perform a full server recovery, follow these steps:

1. Shut down the NetWare server and replace the damaged hard disk. Make sure the disk is as large as, or larger than, the original disk.
2. Partition and format the disk.
3. Reinstall DOS, including *AUTOEXEC.BAT* and *CONFIG.SYS* files.

SYS Volume Recovery on a Single Server Network

4. Reinstall NetWare and NDS with the INSTALL utility, re-create the NetWare volumes, and install the device drivers.

When reinstalling NDS, install it using the same name as the original tree. Use the same server name, container for the Administrator, and password used prior to the disk crash. The Administrator object must reside at the same level, underneath the same container, as it did in the original tree.

5. Continue with Step 2 of “SYS Volume Recovery on a Single Server Network” in the next section.

SYS Volume Recovery on a Single Server Network

This procedure assumes the SYS volume with the NetWare operating system and NetWorker software has been damaged on a single-server network. If the disk was not completely destroyed and the operating system or NetWorker is still operational, use only those steps that apply to your situation.

On a single-server network, there is no replication of the NDS tree. Consequently, you must use NetWorker to recover the filesystem and NDS.

To recover the SYS volume on a single-server network, follow these steps:

1. Shut down the NetWare server and replace the damaged hard disk. Make sure the disk is as large as, or larger than, the original disk.

If the server had volumes other than SYS that were not affected by the failure, run NDS Manager or DSREPAIR to remove invalid trustee rights from the filesystems on those volumes.

2. Make sure the server can access the backup device.
3. Reinstall NetWorker from the original distribution media, using the instructions in the *NetWorker Quick Start Guide*.
4. Load the necessary SMS TSAs and NLMS for NetWorker. At the server console, enter the following commands:

```
LOAD TSANDS
```

```
LOAD TSA410
```

```
NETWORKR
```

A login window displays.

5. Enter the typeful fully distinguished name of the backup administrator (for example, “.cn=Admin.O= ‘top level container’”) into the User field and the appropriate NetWare password into the Password field and press [Enter].



Important: Disable Scheduled Backups and do not use NetWorker to perform backups or restores while running the NetWorker Utilities program because you do not want to confuse the state of the NetWorker indexes.

6. Switch to the NetWare system console, and type the following command.

```
load netutil
```

The NetWorker Utilities dialog box displays.

7. Select the Recover from a Disaster command in the NetWorker Utilities menu, and press [Enter].

An informational warning message displays. Press [Enter].

Another login window displays.

8. Enter the typeful fully distinguished name of the backup administrator (for example, “.cn=Admin.O= ‘top level container’”) into the User field and the appropriate NetWare password into the Password field and press [Enter].

A Device Selection window displays.

9. Select the device you intend to use; press [Enter].

10. Load the most recent backup volume into the tape device and then press [Enter] when you see the following message.

```
Put the volume for disaster recovery in device xxxx and  
press Enter.
```

Refer to your printed bootstrap records to determine the required backup volume. If you do not have these records, use the **scanner -b** command to locate the most recent backup volume. Refer to your *Administrator's Guide* for detailed information about the **scanner** command.

- If you are using a single tape device, manually insert the volume.
- If you are using an autochanger, use the autochanger controls to manually select the slot containing the most recent backup volume.

NetWorker displays a message when it successfully recovers the client file index and media database to the server. (This operation might take some time to complete, depending on the amount of data on the backup volumes and the speed of the device.) NetWorker can now use these to identify and recover data.

SYS Volume Recovery on a Single Server Network

11. Press [Enter], exit NetWorker Utilities, then exit and restart NetWorker. This process restores NetWorker to its last backed up configuration – passwords, administrator privileges, backup groups, and schedules.
12. Verify that your NetWorker configuration and resources are restored. If they are not restored, repeat the Recover from a Disaster command or try an older volume.
13. Mount the most recent volume; press the [F3]-Operations key, select Mount, select the required volume, and press [Enter].

Notice that the volume is now marked (R) write-protected. The Recover from a Disaster command does this to protect the volume.
14. Press [F3]-Operation and select Recover to display the Client List window.
15. Select the client with the NetWare server name and press [Enter].

Another login window displays.
16. Enter the typeful fully distinguished name of the backup administrator (for example, “.cn=Admin.O= ‘top level container’”) into the User attribute and the appropriate NetWare password into the Password attribute and press [Enter].

The Browser window displays.
17. Select Schema and mark it for recover to recover all extensions to the NDS schema at the time of the backup.
18. Press the [F2]-File key, select Start Recover, and press [Enter].
19. When the recover completes, select .[Root] in the Browser window to recover the NDS object data.
20. Press the [F2]-File key, select Start Recover, and press [Enter].

You might see the Naming Conflict dialog box and a Conflict Resolution dialog box. Follow the directions in the box to perform the required action.
21. Continue using NetWorker to recover the remaining data, including the client indexes. In the Browser window, mark “/” for recovery, then unmark all still-operational volumes, *legatomm*, the server’s *legatodb*, *nsr.res*, *nsrjb.res*, Schema, and .[Root].

Make sure you recover each client index by selecting the client folder from the indexes directory. Each client has a *legatodb* file, which is located in `\nsr\index\client-name`.

If you run out of memory while recovering multiple files, try recovering one filesystem or disk volume per recovery session.

22. From the [F2]-File menu in the Browser window, display the NetWorker Recover Options dialog box. Select the Don't overwrite data; recover trustees, etc. command.
23. In the Browser window, mark all non-SYS volumes and recover them.
24. Verify the recovered data. From a workstation, use the RIGHTS /T /S and NDIR commands to check the data, trustee assignments, file ownership, and other related information.
25. Use the Cross-check index command in the NetWorker Administrator program's Indexes dialog box to compare the index records to the records in the media index.

SYS Volume Recovery on a Multiple-Server Network

This section assumes you lost a SYS volume on a NetWorker for NetWare 4.10/4.11 or IntranetWare server in a multiple server environment with a replicated NDS partition.

This section contains disaster recovery information for the following conditions:

- A replicated NDS partition has been damaged or destroyed.
- There is another NetWorker server on the network.

If the NetWare server did not contain an NDS partition (replicated or not), you only need to rebuild the NetWare operating system and the server's filesystems.



Important: For NetWare 4.11/IntranetWare servers, do not delete the server or volume objects for the failed volume from the NDS tree because you do not want to eliminate any references other objects might have to the volume. If for some reason you must delete objects on a NetWare 4.11/IntranetWare server, use the NetWare 4.10 procedure for recovering from a disaster.

SYS Volume Recovery on a NetWare 4.10 Server

To recover a SYS volume on a NetWare 4.10 server, follow these steps:

1. Use NWAdmin or NETADMIN to delete the volume object(s) associated with the failed server.
2. Use NDS Manager or PARTMGR to delete the server object for the failed server. You cannot use NETADMIN to delete a server object.

SYS Volume Recovery on a Multiple-Server Network

Partition Manager will display a warning message; type yes to confirm the deletion.

3. Use NDS Manager or DSREPAIR to check the replica synchronization.
If you see error messages, wait a few minutes and try again.

4. From your NetWorker server, perform a directed recover to restore the failed server's *Server Specific Info* (SSI) files from a tape backup to a functioning NetWorker client.

The server-specific information files (*SERVDATA.NDS*, *VOLSINFO.TXT*, *STARTUP.NCF* and *AUTOEXEC.NCF*) are restored to a subdirectory under *SYS:\SYSTEM* on the server you selected. This subdirectory is given a DOS 8.3 name derived from the source server name.

5. If the failed server held a master replica(s), use NDS Manager or DSREPAIR to designate a new master replica(s) on a different server in the replica ring. Figure 12 shows designating new master replicas and removing a failed server from the replica ring.
6. Use NDS Manager or DSREPAIR to perform an unattended full repair to check replica synchronization. If necessary, use NDS Manager or DSREPAIR on the server(s) containing master replicas to remove the failed server from the replica ring.
7. Shut down the failed server and replace the damaged hard disk or server hardware. The new disk must be as large, or larger than, the original disk.
8. Format the DOS partitions and reinstall DOS.



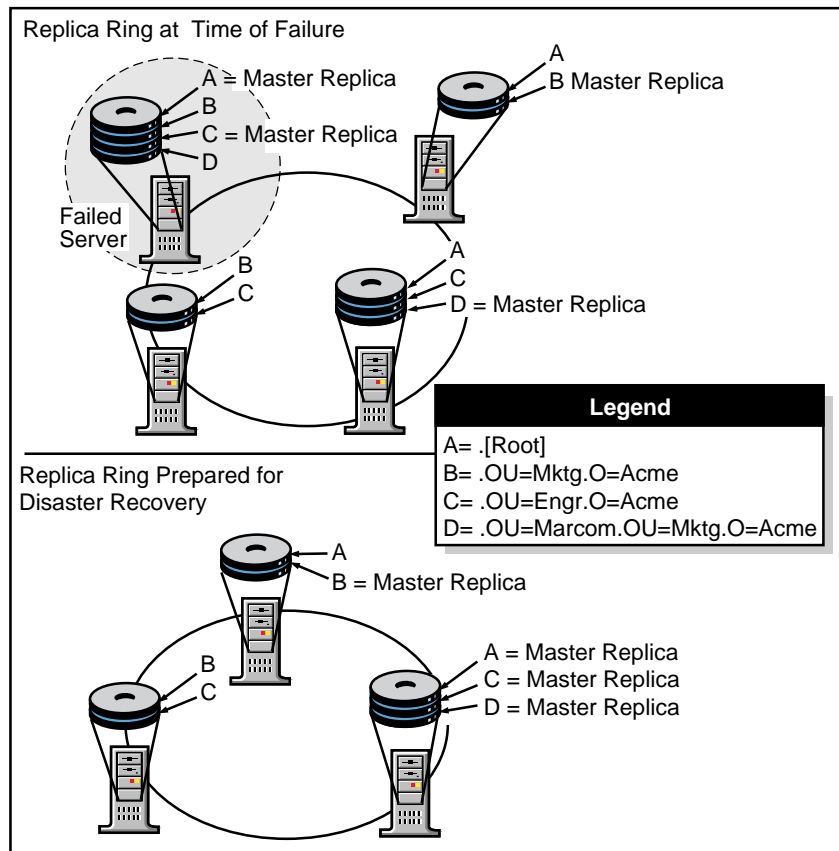
Important: Use the DOS Time command to ensure that your computer is set to the correct time to avoid time synchronization errors.

9. Reinstall NetWare 4.10 and NDS on the repaired or replaced server. Run *INSTALL*, select Custom Install, and follow the directions on the screen. Use the *STARTUP.NCF* and *AUTOEXEC.NCF* files recovered with SSI to answer the questions displayed on the screen.
 - Enter the same server name and internal IPX number that the server had prior to the failure.
 - When prompted, insert the NetWare License diskette for the server into the diskette drive.
 - When prompted for the name of the NDS tree, select the name of the tree that the server resided in before the failure.

- Select the time zone and configure the time.
- Log in and specify the context for the server and its objects. Use the same context used before the failure.
- Edit the *STARTUP.NCF* and *AUTOEXEC.NCF* files to match the versions recovered with SSI.

Installation continues; when complete, the server will contain all the files necessary to perform an SMS remote filesystem restore.

Figure 12. Repairing Replica Rings



10. Load the required name space modules for each restored volume. Use the *VOLSINFO.TXT* file to determine which name spaces need to be loaded (*MAC.NAM*, *OS2.NAM*, etc.).

SYS Volume Recovery on a Multiple-Server Network

11. Load the filesystem TSA by typing the following command at the prompt:

```
LOAD TSA410
```

12. Recover the filesystem for each volume affected by the failure. Do not recover the Schema and .[Root]; they are restored from a replica. You also do not need to recover Server Specific Info again. When prompted, suppress further prompting and overwrite files.

When prompted to log in, use the typeful fully distinguished name of the backup user.

13. If the failed server had non-SYS volumes that were not affected by the failure, from the [F2]-File menu in the Browser window, display the NetWorker Recover Options dialog box. Select the Don't overwrite data; restore trustees, etc. command, then recover the volumes that were not affected by the failure.
14. Shut down and restart the repaired or replaced server.
15. If necessary, use NDS Manager or DSREPAIR to re-establish replicas on the repaired or replaced server.
16. Type the following commands at the system prompt of the repaired or replaced server:

```
LOAD TSA410
```

```
LOAD TSANDS
```

17. From the Recover Browser window, recover the server object, volume objects, and any objects that formerly referenced the recovered volume or server objects. Expand the .[Root] resource, mark the required objects, and then select Recover. When prompted, suppress further prompting and overwrite files.
18. Use NDS Manager or the Schedule immediate synchronization function of DSREPAIR to synchronize the replica on all servers.
19. Verify the recovered data. From a workstation, use NWAdmin or the RIGHTS /T /S and NDIR commands to check the data, trustee assignments, file ownership, and other related information.

SYS Volume Recovery on a NetWare 4.11 or IntranetWare Server

To recover a SYS volume on a NetWare 4.11/IntranetWare server, follow these steps:

1. From your NetWorker server, perform a directed recover to restore the failed server's *Server Specific Info* (SSI) files from a tape backup to a functioning NetWorker for NetWare client.

The server-specific information files (*SERVDATA.NDS*, *DSMISC.LOG*, *VOLSINFO.TXT*, *STARTUP.NCF*, and *AUTOEXEC.NCF*) are restored to a subdirectory under *SYS:\SYSTEM* on the client you have selected. This subdirectory is given a DOS 8.3 name derived from the source server name.



Important: For NetWare 4.11/IntranetWare servers, do not delete the server or volume objects for the failed server from the NDS tree because you do not want to eliminate any references other objects might have to the server. If for some reason objects were deleted from the NDS tree, use the NetWare 4.10 procedure for recovering from a disaster.

2. If the failed server held a master replica(s), use NDS Manager or DSREPAIR to designate a new master replica(s) on a different server in the replica ring. Refer to *DSMISC.LOG* to determine which replicas were stored on the failed server. Figure 12 in the previous section shows designating new master replicas and removing a failed server from the replica ring.
3. If the failed server also contained any non-master replicas, use NDS Manager or DSREPAIR on the server(s) containing master replicas to remove the failed server from the replica ring.

You will see a NetWare warning message. Continue with the recovery procedure; reference "Backing Up and Restoring Novell Directory Services in NetWare 4.11" in *Novell Application Notes*, October 1996.

4. Use DSREPAIR to perform an unattended full repair to ensure the health of the ring.

Refer to *DSMISC.LOG* to determine which replicas were stored on the failed server. If *DSMISC.LOG* shows that no other server has exactly the same replicas as the failed server, run DSREPAIR on any server(s) containing replicas of partitions on the failed server.

SYS Volume Recovery on a Multiple-Server Network

5. Shut down the failed server and replace the damaged hard disk or server hardware. The new disk must be as large, or larger than, the original disk
6. Format the DOS partitions and reinstall DOS.



Important: Use the DOS Time command to ensure that your computer is set to the correct time to avoid time synchronization errors.

7. Reinstall NetWare 4.11 or IntranetWare and NDS on the repaired or replaced server. Run INSTALL, select Custom Install, and follow the directions on the screen.
 - When prompted, enter the same server name and internal IPX number that the server had prior to the failure. Use the *STARTUP.NCF* and *AUTOEXEC.NCF* files included with the server-specific information for needed information.
 - After INSTALL copies the preliminary files, the Choose a directory tree dialog box displays. Press <F5> to restore NDS (option listed at the bottom right of the screen).
 - A new window displays two options: A: (the default) or Press <F3> to specify a different path. If the *Server Specific Info* files are contained on diskette, insert the diskette into drive A and press [Enter]. Otherwise, press <F3> and enter the path to the *Server Specific Info* files restored in step 1.
 - A Remote Server Authentication login dialog box is displayed. Log in, and, when prompted, enter the Directory tree name. Press [Enter], and both the files and NDS are copied to the new server. *DSMISC.LOG*, *VOLSINFO.TXT*, and *AUTOEXEC.NCF* are copied to the *SYS:SYSTEM* directory. *STARTUP.NCF* is copied to the *C:\NWSERVER* directory.
 - The NDS restoration uses the information from *SERVDATA.NDS* (*TSANDS.NLM* is not needed). NDS is now fully functional on the server, though the partitions and replicas must still be reestablished.
 - When prompted, insert the NetWare License diskette for the server into the diskette drive.

- Edit the *STARTUP.NCF* and *AUTOEXEC.NCF* files.
If either the *STARTUP.NCF* or the *AUTOEXEC.NCF* files have changed because they were backed up with the server-specific information, both the original and the new files are displayed for you to compare and make edits as necessary. If the current files are the same as the original files, only the current files are displayed.
The server now contains all the files necessary to perform an SMS remote filesystem restore.
- 8. You can choose one of two ways to finish INSTALL.
 - It is recommended you press <Enter> to Continue, which skips copying the remaining system and public files and exits the INSTALL utility. This saves you time, because you restore the entire filesystem from a backup.
 - Or you can press <F3> to Continue installation and wait while INSTALL copies the remaining system and public files. Then exit INSTALL.
- 9. Load the required name space modules for each restored volume. Use the *VOLSINFO.TXT* file to determine which name spaces need to be loaded (*MAC.NAM*, *OS2.NAM*, etc.).
- 10. Load the filesystem TSA by typing the following command at the prompt of the repaired or replaced server:
LOAD TSA410
- 11. Recover the filesystem for each volume affected by the failure. Do not recover the Schema and *.[Root]*; they are restored from a replica. You also do not need to recover *Server Specific Info* again. When prompted, suppress further prompting and overwrite files.

If the failed server had non-SYS volumes that were not affected by the failure, no further action is needed because the *SERVDATA.NDS* file preserves the trustee assignments on these other volumes.
- 12. Shut down and restart the repaired or replaced server.
- 13. Use NDS Manager or DSREPAIR to re-establish replicas on the failed server. Use *DSMISC.LOG* to view a copy of the replica list that resided on the server at the time of backup.
- 14. Verify the recovered data. From a workstation, use NWAdmin or the RIGHTS /T /S and NDIR commands to check the data, trustee assignments, file ownership, and other related information.

Nonreplicated Partition Recovery

Nonreplicated Partition Recovery

Do not attempt to recover a non-replicated partition by yourself; this procedure requires a great deal of specific technical expertise.

Instead, contact Novell Technical Support and ask for assistance to rebuild the links to the missing partitions and to recover the server objects.

Network-wide Disaster Recovery

This section applies to NetWorker for NetWare servers installed on NetWare 4.10 and NetWare 4.11/IntranetWare servers.

The instructions in this section help you recover from a disaster where all the servers were destroyed. You need to replace the systems, completely restore the operating systems, NDS, and filesystem data. Prior planning makes the recovery from such a comprehensive disaster go much more smoothly. If you followed the instructions in Chapter 1 of the *Disaster Recovery Guide* about documenting NDS topology including, location of server objects, partitions, partition sizes, replicas, and Bindery context settings, refer to this information now.

To restore the destroyed NetWare file servers and network, follow these steps:

1. Replace the damaged servers and necessary hardware.
2. Reconstruct the first server by partitioning and formatting DOS and non-DOS partitions and reinstalling DOS. Re-create the partitions exactly as they were before the disaster.
3. Reinstall NetWare with the INSTALL utility, re-create the NetWare volumes, and install the device drivers. Place the servers on the network in the same containers they were located in prior to the disaster.
4. Install NDS using the same name as the original tree. Use the same server name, container for the Administrator, and password used prior to the disk crash. The Administrator object must reside at the same level, underneath the same container, as it did at the time of the last backup.



Important: This server automatically becomes the master of the NDS Root partition. During installation, make sure you re-create the Organization object using the same name. If the Organization object does not have the same name, you end up with a sub-tree that contains new empty containers.

Chapter 4: Disaster Recovery for NetWare

5. Re-create the other servers on the network so all servers and volumes are operational. Make sure all the servers are communicating properly and time synchronization is working.
6. Reinstall NetWorker on the designated servers from the original distribution media. Use the instructions in the *Quick Start Guide*.
7. Load the necessary SMS TSAs and NLM files for NetWorker.
8. Restore the NetWorker server indexes and configuration files to the NetWorker server. See “NetWorker Indexes and Configuration Files Recovery” on page 74.
9. Recover NDS. If you have multiple NDS trees, you need to recover NDS for each tree by selecting a NetWorker client residing in each tree. The latest *TSANDS.NLM* (dated 3-31-97 or later) must be loaded on each of these clients.
10. Use NetWorker to recover the filesystems on each server. NetWorker recovers the trustees assignments at the same time.
11. Reestablish NDS partitions, and distribute replicas to the other servers. The NDS tree(s) should exist as it did prior to the disaster.
12. Run DSREPAIR on each server with a master replica to verify the integrity of the NDS database(s).

You need to reregister your NetWorker for NetWare server if its host ID has changed. For more information, see the instructions in the following section.

We suggest you verify the recovered data. From a workstation, use NWAdmin or the RIGHTS /T /S and NDIR commands to check the data, trustee assignments, file ownership, and other related information.

Recovery to a New Server

The instructions in this section apply to NetWorker for NetWare servers installed on NetWare 4.10 and NetWare 4.11/IntranetWare servers. In this example, the original NetWorker server is beyond repair, so you need to move the operating system, NetWorker software, and data to a new server.



Important: If you want to make changes to the operating system or the NetWorker software, it is strongly recommended that you configure the new server exactly like the original, using the same version of the operating system and NetWorker software. Use the same *server-name* for the new server. After configuring the new server, make sure the system is operational and perform a couple of successful backups. Then, if necessary, update or upgrade the operating system or the NetWorker software, one at a time.

Moving NetWorker to a New Server with No Changes

If you move the NetWorker server to a system that uses the same hostname and NetWare license, use the appropriate instructions in this chapter to reinstall the operating system, NetWorker software, and the server indexes and configuration files.

Moving NetWorker to a New Server with Changes

To move NetWorker to another server that has a different NetWare license or a different server name, follow these steps:

1. Reinstall the operating system and NetWorker software by using the appropriate instructions in this chapter.
2. Create an additional “active SPX” client with the original server name, using the Client dialog box.
3. Mount the latest backup volume in the backup device.
4. Use the Recover Volume command in the NetWorker Utilities program to recover the server indexes from the latest backup volume.

NetWorker copies the data from the volume into the client directory with the original server name.

5. Select the Recover command to open the Recover window.
6. Recover only the client indexes (*legatodb*) at this time. Do **not** recover the original server indexes or the *nsr.res* file.

7. Add and configure the clients for the indexes you just recovered. Be sure the client names you enter match the names of the client indexes.

You should now have a fully functional NetWorker server, including all the clients and indexes that existed on the original server.

If you want to keep the client you created with the original server name, you must install the client software on the old server (if you managed to salvage it) and add and configure the system as you would any other client. You can also assign the original server name to the new system and add it as a NetWorker client.

DIGITAL suggests that you do not recover the media index (*legatomm*) at this time. Instead, save the original backup volumes, and use the Recover Volume command to recover data from a specific volume.

Reregistering NetWorker

You must also reregister the NetWorker software if the NetWare license or server name has changed. You have 15 days to register the new server with DIGITAL. Follow the instructions in the *Quick Start Guide*, for enabling and registering your NetWorker software.

DIGITAL sends you a DIGITAL NetWorker *Host Transfer Affidavit* for you to complete and return to DIGITAL. After DIGITAL receives the signed affidavit, you will receive a new authorization code to enter into the Auth code attribute of the Registration dialog box.

After successfully moving your server, complete these tasks:

- Verify that the server and all the clients are included in a scheduled backup.
- Schedule and run a full backup as quickly as possible for the server and all the clients. (Manual backups do not back up the server or client indexes.)
- Use the Recover window to make sure all the client indexes are browsable and, therefore, “recoverable.”

Appendix A: Win95 Client Recovery

This chapter provides any special instructions necessary to perform a disaster recovery on NetWorker clients.

To recover a Win95 client, follow these steps:

1. Do a full backup of your Win95 system.
2. Close down all applications.
3. Save the Win95 Registry to a floppy disk and to your hard drive:
 - a. Open a DOS window and start Regedit.
 - b. In the Registry Menu, give a filename, select export range all, and save to floppy and hard disk.
4. Make a Win95 boot disk and copy the following files to this boot disk:
 - *config.sys* (loading *himem.sys* and CD drive)
 - *autoexec.bat* (loading CD drive)
 - *himem.sys* and *format.exe*
 - Files needed for your CD drive and NIC card
5. Print out your TCP/IP and NIC information.
6. To restore the system, install your new hard drive and follow these steps:
 - a. Partition the new drive and format it (with /s option) using the *format.exe* program on the bootable disk you created.
 - b. Copy the *config.sys*, *autoexec.bat*, *himem.sys*, and CD drivers to your C: drive.
 - c. Reboot the system.
 - d. Change to the CD and install Win95 (using */setup*).
 - e. Set up TCP/IP, using the information you printed out in Step 8.
 - f. Install NetWorker.

Appendix A: Win95 Client Recovery

- g. Start NetWorker on the Win95 system and perform a recover:
 - Mark all files to be recovered.
 - Select overwrite/suppress.
 - Shut down the system after the recovery ends.
 - Restart the system.
7. Open a DOS window and start Regedit.
8. Import the Registry from the floppy.
9. Shut down Win95 and start it up again.

Your Win95 system should now be successfully recovered.

Glossary

This glossary contains terms and definitions found in this guide. Most of the terms are specific to NetWorker products.

Administrators group	Members of this Windows NT user group have all the rights and capabilities of users in other groups, plus the capability to create and manage all the users and groups in the domain. Only members of the Administrators group can modify Windows NT OS files, maintain the built-in groups, and grant additional rights to groups.
annotation	A comment that you associate with an archive save set, to help identify that data later on. Annotations are stored in the media index for ease of searching and are limited to 1024 characters.
Application Specific Module (ASM)	A program that, when used in a directive, specifies the way that a set of files or directories is to be backed up and recovered.
archive	The process by which NetWorker backs up directories or files to an archive volume and then optionally deletes them to free disk space.
archive clone pool	A volume pool composed exclusively of archive clone save sets.
archive pool	A volume pool composed exclusively of archive save sets.
archive volume	A tape or other storage medium used for NetWorker archives, as opposed to a backup volume.

Glossary

ASM	<i>See Application Specific Module</i>
autochanger	A mechanism that uses a robotic arm to move media among various components in a device, including slots, media drives, media access ports, and transports. Autochangers automate media loading and mounting functions during backups and recovers.
browse policy	The policy that determines how long entries for your files remain in the online file index.
Backup Operators group	Members of this Windows NT group have the capability to log on to a domain from a workstation or a server, back it up, and restore the data. Backup Operators can also shut down servers or workstations.
backup volume	Backup media, such as magnetic tape or optical disk.
bootstrap	Information that includes the server index, media index, and configuration files needed for recovering NetWorker after a disk crash.
client	A machine that accesses the NetWorker server to back up or recover files. Clients can be workstations, PCs, or file servers.
clone	The process by which NetWorker makes an exact copy of saved data (save sets). NetWorker can clone individual save sets or the entire contents of a backup volume.
clone volume	A duplicated volume. NetWorker can track four types of volumes: backup, archive, backup clone, and archive clone. Save sets of different types can not be intermixed on one volume.
cluster data	Data shared by cluster servers that resides on a public disk.
cluster database	Database that resides on a public disk that is shared by cluster servers.

cluster server	Server that belongs to a cluster. Cluster servers typically provide services that include sharing data and providing failover services to other cluster servers in the group. Cluster servers must have both shared and public disks.
command line	The shell prompt, where you enter commands.
compressasm	A NetWorker directive used for compressing and decompressing files.
device	The backup device (tape drive, optical drive, or autochanger) connected to the NetWorker server; it is used for backing up and recovering client files.
directive	An instruction directing NetWorker to take special actions on a given set of files.
enabler codes	Special codes provided by DIGITAL that enable you to run your NetWorker software product.
file index	A database of information maintained by NetWorker that tracks every file or filesystem backed up.
fileserver	A machine with disks that provides services to other machines on the network.
filesystem	1. A file tree which is on a specific disk partition or other mount point. 2. The entire set of all files. 3. A method of storing files.
full (f)	A backup level in which all files are backed up, regardless of when they last changed.
grooming	The process of removing files after a successful archive.
group	A client or group of clients that starts backing up their files at a designated time.

Glossary

heterogeneous	A type of network with systems of different platforms that interact meaningfully across the network.
incremental (i)	A backup level in which only files that have changed since the last backup are backed up.
interoperability	The ability of software and hardware on multiple machines from multiple vendors to communicate meaningfully.
carousel	A tray or tape cartridge that holds multiple backup volumes.
level [1-9]	A backup level that backs up files that have changed since the last backup of any lower level.
machine	Any computer, including file servers or compute servers, diskfull workstations, or diskless workstations.
media	Magnetic tape or optical disks used to back up files.
media database	A database of information maintained by NetWorker that tracks every backup volume.
media manager	The NetWorker component that tracks save sets to backup volumes.
NetWare Loadable Module (NLM)	NetWare executables that extend the functionality of the network operating system.
NetWorker client	A machine that can access the backup and recover services from a NetWorker server.
NetWorker server	The machine on a network running the NetWorker software, containing the online indexes, and providing backup and recover services to the clients on the same network.
Microsoft Cluster Server (MSCS)	Cluster server software that provides services for sharing data and failover operations to other servers in a cluster.

notice	A response to a NetWorker event.
Novell Directory Services (NDS)	Global distributed information database for managing network resources and services.
nsrhost	The logical <i>hostname</i> of the machine that is the NetWorker server.
online indexes	The databases located on the server that contain all the information pertaining to the client backups and backup volumes.
operator	The person who monitors the server status, loads backup volumes into the server devices, and otherwise executes day-to-day tasks using NetWorker.
override	A backup level that takes place instead of the scheduled one.
pathname	Instructions for accessing a file. An <i>absolute pathname</i> tells you how to find a file beginning at the root directory and working down the directory tree. A <i>relative pathname</i> tells you how to find the file starting where you are now.
preconfigured	Existing selections or configurations for different NetWorker features.
private disk	Local disk not shared by the other servers in a cluster.
public disk	<i>See shared disk</i>
recover	The NetWorker command used to browse the server index and recover files from a backup volume to a client's disk.
quorum database	A database that stores transactions that occur on a cluster server. The quorum database can be located on a shared or public disk.

Glossary

recycle	A volume whose data has passed both its browse and retention policies and is available for relabeling.
Registry	A database of configuration information central to Windows NT operations. The overall effect centralizes all Windows NT settings and provides security and control over system, security, and user account settings.
retention policy	A policy that determines how long entries are retained in the media index and, thus, are recoverable.
retrieval	The process of locating and copying back files and directories that NetWorker has archived.
save	The NetWorker command that backs up client files to backup volumes and makes data entries in the online index.
save set	A set of files or a filesystem backed up to backup media using NetWorker.
save set identification (save set ID or ssid)	An internal identification number assigned to a save set by NetWorker.
scanner	A NetWorker command used to read a backup volume when the online indexes are no longer available.
server	A machine on a network running the NetWorker software, that contains the online indexes and provides backup and recover services to the clients on a network.
shared disk	Hard disk shared by the servers in a cluster. The shared disk typically stores the quorum database.
shell prompt	A cue for input in a shell window where you enter a command.
skip (s)	A backup level in which files are skipped and not backed up.

stand-alone device	A backup device that contains a single drive for backing up data. Stand-alone devices cannot store or automatically load backup volumes.
Storage Management Services (SMS)	An operating system interface that provides functionality specific to storage management products.
system administrator	A person typically responsible for installing, configuring, and maintaining NetWorker.
Target Service Agents (TSA)	Software modules capable of accessing target data, such as a filesystem or NDS. TSAs are part of the SMS open architecture.
user	People who use NetWorker from their workstations to back up and recover files.
volume	Backup media, such as magnetic tape or optical disk.
volume ID	The internal identification assigned to a backup volume by NetWorker.
volume name	The name you assign to a backup volume when it is labeled.
volume pool	A feature that enables you to sort backup data to selected volumes. A volume pool contains a collection of backup volumes to which specific data has been backed up.

Index

A

- autochangers
 - mmrecov command, using with 22
 - Recover from a Disaster command, using with 22
 - recovering with
 - NetWare 24
 - UNIX 22
 - Windows NT 22
 - reenabling for disaster recovery 22

B

- backing up
 - cluster data 48
 - repair disk data 30
- backup device, verifying operation 21
- Backup Utility, Windows NT 21
- bootstrap 12-14

C

- choices for disaster recovery 18
- client indexes
 - recovering
 - NetWare 80
 - UNIX 61, 67
 - Windows NT 40
- client_name.txt report, Windows NT 29
- clients, recovering
 - UNIX 60
 - Windows NT 38
- CLUSDB file 52
- CLUSDB.LOG file 48
- cluster data
 - backing up 48
 - recovering 48
- cluster database, recovering 49

- command
 - dinfo 16
 - mmrecov
 - UNIX 62
 - Windows NT 40
 - NDIR 81, 84, 87
 - nsr_shutdown 66
 - nsrjb -I 23
 - nsrjb -u 23
 - nsrjb -vHE 23
 - nsrwatch 64
 - nwadmin 64
 - prvtoc 17
 - Recover from a Disaster 24, 75
 - RIGHTS 81, 84, 87
 - savegrp 13
 - saveindex 13
 - scanner 14, 15, 62
 - smit 56
 - tar 21
- command line recovery, repair disk data 33
- complete install of operating system 20
- completing the disaster recovery
 - UNIX 67
 - Windows NT 45
- configuration files
 - NetWare 80
 - recovering, defined 10
 - UNIX 66
 - Windows NT 44
- configuration files directory
 - NetWare 74
 - UNIX 61
 - Windows NT 40
- creating partitions 16
- critical data
 - lost 9
 - recovering

Index

- UNIX 55
 - Windows NT 34
- D**
- damaged NetWorker software 10
 - destroyed server 11
 - Diagnostic utility, Windows NT 29
 - DIGITAL Alpha NT, disaster recovery 47
 - directed recover, Windows NT 32
 - directories
 - configuration files
 - NetWare 74
 - UNIX 61
 - Windows NT 40
 - media index
 - NetWare 74
 - UNIX 61
 - Windows NT 39
 - REPAIRDISK 30
 - server index
 - NetWare 74
 - UNIX 61
 - Windows NT 39
 - disaster recovery
 - choices 18
 - preparing for 11
 - requirements 11
 - types 9
 - disk
 - saving information 15
 - size of replacement
 - NetWare 77
 - UNIX 54
 - Windows NT 28
 - dkinfo command 16
 - DSREPAIR program 18
- E**
- eliminating from backup, REPAIRDISK directory 31
- F**
- files
 - client_name.txt, Windows NT 29
 - CLUSDB 52
 - CLUSDB.LOG 48
 - quolog.log 52
 - finding NetWorker bootstrap 14
- H**
- hardware, replacing
 - NetWare 73
 - UNIX 54
 - Windows NT 28
- I**
- ID number for save set 14
 - index directory
 - NetWare 74
 - UNIX 61
 - Windows NT 39
 - installing the operating system 20
- L**
- log file, CLUSDB.LOG 48
- M**
- media index directory
 - NetWare 74
 - UNIX 61
 - Windows NT 39
 - Microsoft Cluster Server 47
 - Microsoft Diagnostic utility, Windows NT 29
 - Microsoft Repair Disk utility 29
 - mmrecov command
 - UNIX 62
 - Windows NT 40

-
- multiple server network, NetWare
 - recovering non-replicated partition 88
 - recovering replicated partition 81

 - N**
 - NDIR command 81, 84, 87
 - NETADMIN program 18
 - NetWare
 - bootstrap 13
 - configuration files
 - directory 74
 - restoring 80
 - media index directory 74
 - network-wide disaster, recovering 88
 - prepare for recovery
 - NetWorker 73
 - operating system 73
 - Recover from a Disaster command 75
 - recovering 90
 - configuration files 74
 - non-replicated partition 88
 - server indexes 74
 - to new server 90
 - with autochangers 24
 - with stand-alone drives 26
 - reinstalling NetWorker requirements 73
 - reregistering new server 91
 - saving disk information 18
 - server index directory 74
 - NetWorker
 - bootstrap, finding 14
 - damaged software 10
 - NetWare
 - preparing for recovery 73
 - Utilities program 79
 - UNIX
 - preparing for recovery 59
 - recovering 58
 - requirements for reinstalling 54
 - Windows NT
 - preparing for recovery 38
 - recovering 37
 - NetWorker server
 - reenabling for disaster recovery 22
 - reregistering
 - NetWare 91
 - UNIX 69
 - Windows NT 46
 - network-wide disaster, NetWare 88
 - new servers, recovering to
 - NetWare 90
 - UNIX 68
 - Windows NT 45
 - non-replicated partition, recovering 88
 - nsr_shutdown command 66
 - nsrjb -I command 23
 - nsrjb -u command 23
 - nsrjb -vHE command 23
 - nsrwatch command 64
 - nwadmin command 64
 - NWAdmin program 18

 - O**
 - operating system
 - NetWare
 - preparing for recovery 73
 - requirements for reinstalling 73
 - restoring 18-20
 - UNIX
 - preparing for recovery 56
 - requirements for reinstalling 54
 - Windows NT
 - corrupted files and partitions 29
 - prepare for recovering 35
 - requirements for reinstalling 28

 - P**
 - partial install of operating system 20
 - partitions, creating 16
 - preparing for a disaster 11
 - preparing for recovery
 - NetWorker

Index

- NetWare 73
 - UNIX 59
 - Windows NT 38
 - operating system
 - NetWare 73
 - UNIX 56
 - Windows NT 35
 - programs
 - DSREPAIR 18
 - NETADMIN 18
 - NetWorker Utilities 79
 - NWAdmin 18
 - SBackup 21
 - prtvoc command 17
 - Q**
 - quolog.log file 52
 - quorum resource 49–52
 - R**
 - Recover from a Disaster command 75
 - recover, directed, Windows NT 32
 - recovering
 - DIGITAL Alpha NT 47
 - NetWare
 - client indexes 80
 - configuration files 74
 - network-wide disaster 88
 - non-replicated partition 88
 - replicated partition 81
 - server indexes 74
 - to new server 90
 - with stand-alone drives 26
 - NetWorker
 - UNIX 58
 - Windows NT 37
 - UNIX
 - client indexes 61, 67
 - clients 60
 - configuration files 61
 - critical data 55
 - server indexes 61
 - storage nodes 60
 - to new server 68
 - with autochangers 22
 - with stand-alone drives 25
 - Windows NT
 - client indexes 40
 - clients 38
 - cluster data 48
 - cluster database 49
 - cluster server 51
 - configuration files 39
 - critical data 34
 - operating system 36
 - REPAIRDISK directory data 32
 - server indexes 39
 - storage nodes 38
 - to new server 45
 - using Setup disks 29
 - with autochangers 22
 - with Emergency Repair Disk 33
 - with stand-alone drives 25
 - with autochangers 24
 - defined 21
 - mmrecov 22
 - using the Recover from a Disaster command 22
- recovery requirements
 - NetWare 73
 - UNIX 53
 - Windows NT 27
 - reenabling
 - autochangers 22
 - NetWorker servers 22
 - reinstalling operating system, choices 19
 - renaming configuration files
 - UNIX 66
 - Windows NT 44
 - repair disk data
 - backing up 30
 - recovering from the command line 33
 - Repair Disk utility 29
 - REPAIRDISK directory

-
- defined 30
 - eliminating backups 31
 - recovering 32
 - REPAIRDISK directory data
 - recovering 32
 - replacement disk, size
 - NetWare 77
 - UNIX 54
 - Windows NT 28
 - replicated partition, recovering 81
 - report, client_name.txt, Windows NT 29
 - requirements, disaster recovery 11
 - NetWare 73
 - UNIX 53, 54
 - Windows NT 28
 - reregistering the new server
 - NetWare 91
 - UNIX 69
 - Windows NT 46
 - resource, quorum, Windows NT 49, 51
 - restoring the operating system 18
 - RIGHTS command 81, 84, 87
 - running mmrecov command
 - UNIX 62
 - Windows NT 40
- S**
- save set ID 14
 - savegrp command 13
 - saving
 - bootstrap 13
 - disk information 15
 - SBackup program 21
 - scanner command 14, 15, 62
 - secondary disk, recovering damaged 9
 - server
 - clusters, recovering 51
 - destroyed 11
 - index directory
 - NetWare 74
 - UNIX 61
 - Windows NT 39
 - server indexes, recovering
 - defined 10
 - NetWare 74
 - UNIX 61
 - Windows NT 39
 - Setup disks for Windows NT 29
 - smit command 56
 - stand-alone drives, recovering with 25
 - storage nodes, recovering
 - UNIX 60
 - Windows NT 38
- T**
- tar command 21
 - types of disasters 9
- U**
- UNIX
 - completing the disaster recovery 67
 - configuration files directory 61
 - finding bootstrap 14
 - media index directory 61
 - prepare for recovery
 - NetWorker 59
 - operating system 56
 - recovering
 - clients 60
 - configuration files 61
 - critical data 55
 - NetWorker 58
 - server indexes 61
 - storage nodes 60
 - to new server 68
 - with autochangers 22
 - with stand-alone drives 25
 - reinstalling
 - NetWorker requirements 54
 - reinstalling, requirements 53
 - renaming configuration files 66
 - replacing hardware, requirements 54
 - reregistering new server 69

Index

running mmrecov command 62
saving bootstrap 13
server index directory 61
utility, Microsoft Diagnostic 29

W

Windows NT

backing up cluster data 48
Backup Utility 21
client_name.txt 29
completing the disaster recovery 45
configuration files directory 40
Diagnostic utility 29
eliminating REPAIRDISK directory
 backups 31
finding bootstrap 14
media index directory 39
Microsoft Cluster Server support 47
prepare for recovery
 NetWorker 38
 operating system 35
quorum resource 49, 51
recovering
 clients 38
 cluster data 48
 cluster database 49
 cluster server 51
 configuration files 39
 critical data 34
 NetWorker 37
 operating system 36
 REPAIRDISK directory data 32
 server indexes 39
 storage nodes 38
 to new server 45
 with autochangers 22
 with Emergency Repair Disk 33
 with stand-alone drives 25
recovery requirements 27
reinstalling operating system 34
renaming configuration files 44
Repair Disk utility 29

REPAIRDISK directory 30
replacing hardware requirements 28
reregistering new server 46
running mmrecov command 40
saving
 bootstrap 13
 disk information 16
server index directory 39
Setup disks, used for recovery 29