

# VERITAS NetBackup™ 3.4.1

---

## Release Notes

January 2001  
30-000075-399

  
VERITAS

---

## Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

## Copyright

Copyright © 1993-2000 VERITAS Software Corporation. All rights reserved. VERITAS is a registered trademark of VERITAS Software Corporation in the US and other countries. The VERITAS logo, VERITAS NetBackup, and VERITAS NetBackup BusinessServer are trademarks of VERITAS Software Corporation. All other trademarks or registered trademarks are the property of their respective owners.

Portions of this software are derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm. Copyright 1991-92, RSA Data Security, Inc. Created 1991. All rights reserved.

Printed in the USA, January 2001.

VERITAS Software Corporation  
1600 Plymouth St.  
Mountain View, CA 94043  
Phone 650-335-8000  
Fax 650-335-8050  
[www.veritas.com](http://www.veritas.com)



# Contents

---

<b>Preface</b> .....	<b>ix</b>
Organization .....	ix
Related Documents .....	x
Online Documentation .....	x
On Windows NT/2000 .....	x
On UNIX .....	xi
On the Support Web Site .....	xi
Conventions .....	xii
Type Style .....	xii
Notes and Cautions .....	xii
Key Combinations .....	xii
Command Usage .....	xii
Getting Help .....	xiii
 <b>Chapter 1. New Features In NetBackup 3.4.1</b> .....	<b>1</b>
General NetBackup .....	1
Linux .....	2
Windows NT/2000 .....	2
Alternative Backup .....	2
Database Agents .....	2
Media Manager .....	2
 <b>Chapter 2. NetBackup 3.4.1 Supported Platforms and Peripherals</b> .....	<b>5</b>
Server and Client Platform Support .....	5



---

NetBackup DataCenter Supported Platforms .....	6
NetBackup BusinessServer Supported Platforms .....	7
Database Agent Platform Support .....	9
Support for Files Greater than Two Gigabytes .....	9
Binary Sizes .....	10
Supported Peripherals .....	11
Supported Peripherals by Vendor .....	11
Robot Type Support By Platform .....	12
NetBackup DataCenter 3.4.1 - Robot Support by Platform .....	13
NetBackup BusinessServer 3.4.1 - Robot Support by Platform .....	14
<b>Chapter 3. NetBackup 3.4.1 Operational Notes .....</b>	<b>15</b>
Installation .....	15
General Notes .....	17
NetBackup .....	18
Media Manager .....	21
Using NetBackup With VERITAS Storage Migrator (VSM) .....	26
NetBackup-Java Interfaces .....	26
General Items Applicable to All NetBackup-Java Applications .....	26
Activity Monitor Application .....	31
Backup Policy Management Application .....	31
NetBackup System Configuration Application .....	32
Media and Device Management Application .....	32
Reports Application .....	32
Backup, Archive, and Restore Application .....	32
Storage Migrator File System Analyzer (FSA) Application .....	32
Installing NetBackup 3.4.1 for Oracle on Red Hat Linux 6.2 .....	33
Using the STK SN6000 .....	34
Should SN6000 Drives Be Configured as Shared Drives? .....	34
Hosts Connected To a Single Port .....	34



---

Hosts Connected To Different Ports .....	34
<b>Chapter 4. Problems Fixed Since NetBackup 3.4 .....</b>	<b>37</b>
General NetBackup .....	37
PC Clients .....	37
UNIX Clients .....	37
Alternative Backup .....	37
DataBase Agents .....	38
Media Manager .....	38
<b>Chapter 5. NetBackup 3.4.1 Known Problems and Limitations .....</b>	<b>41</b>
Installation .....	41
General Notes .....	42
Media Manager .....	50
PC Clients .....	53
UNIX Clients .....	54
DataBase Agents (extensions) .....	56
NetBackup-Java Interfaces .....	57
General Items Applicable to All Applications .....	57
Backup Policy Management Application .....	59
NetBackup Catalog Backup Application .....	60
NetBackup System Configuration Application .....	60
Activity Monitor Application .....	61
Device Monitor Application .....	61
Media and Device Management Application .....	61
Reports Application .....	62
Backup, Archive, and Restore Application .....	63
NetBackup-Java Display Console Known Problems .....	63
Java Problems Seen in NetBackup-Java .....	64
Known Problems with Display of Online Help .....	66
Errors When NetBackup Daemons Are Not Running .....	67



---

Documentation Errata .....	69
----------------------------	----

<b>Appendix A. Using NetBackup with Microsoft Cluster Server .....</b>	<b>71</b>
--	-----------

How NetBackup Protects Data in a Cluster .....	71
Configurations for NetBackup and Clusters .....	72
Cluster with Tape Devices on a Shared SCSI Bus .....	73
Configuring a Shared SCSI Bus for Tape Devices .....	73
Cluster with Locally-attached Storage Devices .....	76
Clusters Sharing Devices on a Fibre Channel SAN .....	77
Installing a NetBackup Failover Server on a Cluster .....	78
Uninstalling a NetBackup Failover Server from a Cluster .....	83
Operational Notes for NetBackup Failover Servers .....	84
Installing Separate NetBackup Media Servers on a Cluster .....	85
Uninstalling Separate NetBackup Media Servers from a Cluster .....	86
Installing NetBackup Client on a Cluster .....	87
Uninstalling a NetBackup Client from a Cluster .....	87
Backing Up Clusters .....	87
Backing Up Local Disks in a Cluster .....	88
Backing Up Disks on the Shared SCSI Bus .....	88
Backing Up Database Files in a Cluster .....	89
Restoring Data to Clusters .....	89
Restoring the Cluster Quorum for Windows 2000 Systems .....	91
Restoring Cluster Quorum to Windows 2000 Node With Directory Services ....	92
Preparing for Disaster Recovery of A Cluster .....	93
Disaster Recovery of A Cluster .....	93
Recovering the Entire Cluster .....	94
Recovering All Shared Disks .....	94
Recovering NetBackup on a Shared Disk .....	95
Using NetBackup for SQL Server with Microsoft Cluster Server .....	95
NetBackup Server Configuration Parameters .....	96



---

NetBackup Client Configuration Parameters .....	97
Set Client Environment Variable .....	97
Performing an SQL Server Backup .....	98
Performing a SQL Server Restore .....	98
<b>Appendix B. Intel Hosts Running Red Hat Linux 6.2/7.0 .....</b>	<b>101</b>
Before You Start .....	101
Configuring Robotic Controls .....	102
Configuring SCSI Robotic Controls .....	102
Examples of SCSI Robotic Control Device Files .....	103
Configuring Tape Drives .....	103
Adding Standard Tape Drives .....	103
Examples of SCSI Tape Device Files .....	103
Verifying The Device Configuration .....	104
Frequently Asked Questions .....	104







# Preface

---

These release notes apply to VERITAS NetBackup 3.4.1 and are intended for the system administrator and other users. NetBackup 3.4.1 supplements NetBackup 3.4 and provides software for *only* the following:

- ◆ Linux Red Hat 6.2 and 7.0 NetBackup BusinessServer servers or clients (in this document, references to UNIX also apply to Linux, unless otherwise stated).
- ◆ Windows NT/2000 server and client (includes Windows 2000 Logo certification and other enhancements mentioned for Windows NT/2000 in Chapter 1).
- ◆ NetBackup for Oracle on Linux.
- ◆ NetBackup for NDMP on UNIX (enhanced to include support for NetBackup BusinessServer on Linux).
- ◆ NetBackup Advanced Reporter on HP-UX.
- ◆ All clients except Macintosh and OS/2. The NetBackup-Java Windows Display Console is also not included. The software for Macintosh, OS/2, and the Windows Display Console is unchanged from 3.4 and you can use the 3.4 server CD-ROM to install it.

Install 3.4.1 only if you require the above software. Otherwise, install 3.4. NetBackup 3.4 and 3.4.1 are completely interoperable and can be viewed as being at the same release level (for example, NetBackup 3.4 servers support 3.4.1 clients).

Software is not changed for Solaris and other platforms not listed above. See the *NetBackup 3.4 Release Notes* for information concerning other supported platforms.

## Organization

- ◆ Chapter 1 explains when this release of NetBackup is required and the important new features that it includes.
- ◆ Chapter 2 lists the platforms and peripherals supported by this release.
- ◆ Chapter 3 contains important operating information not documented elsewhere.
- ◆ Chapter 4 describes notable problems resolved by this release of NetBackup.



- ◆ Chapter 5 describes problems and limitations that you may encounter when using this release of NetBackup.
- ◆ Appendix A describes using NetBackup with Microsoft Cluster Server. This appendix includes descriptions of the NetBackup master server failover capability that was added at 3.4.1 and supercedes appendix J in the *NetBackup DataCenter System Administrator's Guide - Windows NT/2000*.
- ◆ Appendix B describes requirements for configuring devices on Red Hat Linux 6.2 and 7.0 NetBackup servers.

## Related Documents

- ◆ *NetBackup 3.4.1 Installation Guide - Windows NT/2000*  
Explains how to get NetBackup 3.4.1 software installed and running on Windows NT/2000.
- ◆ *NetBackup BusinessServer 3.4.1 Installation Guide - Red Hat Linux 6.2/7.0*  
Explains how to get NetBackup 3.4.1 software installed and running on UNIX.

With the exception of these release notes and the above, all 3.4 manuals also apply to 3.4.1. For a complete list of technical documents related to NetBackup, see the Related Documents appendix in the *NetBackup 3.4 Release Notes*.

## Online Documentation

### On Windows NT/2000

The released software contains on-line PDF and ASCII versions of these release notes and a readme file for the client. If you choose to install the documentation during setup, NetBackup installs these documents in the following locations on your disk:

- ◆ *install\_path\Help\*  
Adobe Acrobat Portable Document Format (PDF) copies of all related documents, including these release notes.
- ◆ *install\_path\NetBackup\Readme.txt*  
The *Readme.txt* file (ASCII format) may be slightly more up-to-date than the printed and pdf copies of the release notes.
- ◆ *install\_path\NetBackup\ReadmeCl.txt*  
The client readme file (ASCII format).

## On UNIX

During NetBackup installation, a text copy of the *NetBackup Media Manager Device Configuration Guide* is installed in

`/usr/opensv/volmgr/MediaMgr_DeviceConfig_Guide.txt`

You can copy example code from the device configuration guide if you need to reconfigure the kernel to provide specific tape or optical peripheral support.

The product CD-ROM also contains PDF copies of these release notes and other documents.

---

**Note** You will need Adobe Acrobat Reader to view the PDF documents. The latest version of Acrobat Reader is available on the Adobe web site:  
<http://www.adobe.com>.  
VERITAS assumes no responsibility for the correct installation or use of the reader.

---

## On the Support Web Site

Copies of the documentation are also available on the VERITAS support web site:

1. Go to the VERITAS support web page  
[www.support.veritas.com/](http://www.support.veritas.com/)
2. In the VERITAS Support Product List, choose NetBackup Products.
3. A page appears with a list of the NetBackup products. Choose NetBackup BusinessServer or NetBackup DataCenter.
4. The documents page appears. Choose the document you want.



# Conventions

The following explains typographical and other conventions used in this guide.

## Type Style

Table 1. Typographic Conventions

Typeface	Usage
<b>Bold fixed width</b>	Input. For example, type <b>cd</b> to change directories.
Fixed width	Paths, commands, filenames, or output. For example: The default installation directory is <code>/opt/VRTSxx</code> .
<i>Italics</i>	Book titles, new terms, or used for emphasis. For example: <i>Do not</i> ignore cautions.
<i>Sans serif</i> (italics)	Placeholder text or variables. For example: Replace <i>filename</i> with the name of your file.
Sans serif (no italics)	Graphical user interface (GUI) objects, such as fields, menu choices, etc. For example: Enter your password in the Password field.

## Notes and Cautions

---

**Note** This is a Note and is used to call attention to information that makes it easier to use the product or helps you to avoid problems.

---

---

**Caution** This is a Caution and is used to warn you about situations that can cause data loss.

---

## Key Combinations

Some keyboard command sequences use two or more keys at the same time. For example, you may have to hold down the **Ctrl** key while you press another key. When this type of command is referenced, the keys are connected by plus signs. For example:

Press **Ctrl+t**

## Command Usage

The following conventions are frequently used in the synopsis of command usage.

brackets [ ]

The enclosed command line component is optional.

Vertical bar or pipe (|)



Separates optional arguments from which the user can choose. For example, when a command has the following format:

command *arg1* | *arg2*

the user can use either the *arg1* or *arg2* variable.

## Getting Help

For updated information about this product, including system requirements, supported platforms, supported peripherals, and a list of current patches available from Technical Support, visit our web site:

<http://www.veritas.com/>

VERITAS Customer Support can also be reached by email at:

[support@veritas.com](mailto:support@veritas.com)





# New Features In NetBackup 3.4.1

1

## General NetBackup

1. NetBackup 3.4.1 supplements NetBackup 3.4 and provides software for *only* the following:
  - ◆ Linux Red Hat 6.2 and 7.0 NetBackup BusinessServer servers or clients.
  - ◆ Windows NT/2000 NetBackup server and client (includes Windows 2000 Logo certification and other Windows NT/2000 enhancements mentioned in this chapter).
  - ◆ NetBackup for Oracle on Linux (for installation instructions, see “Installing NetBackup 3.4.1 for Oracle on Red Hat Linux 6.2” on page 33).
  - ◆ NetBackup for NDMP on UNIX (enhanced to include support for NetBackup BusinessServer on Linux).
  - ◆ NetBackup Advanced Reporter on HP-UX. This is a port to HP-UX 11.0 of Advanced Reporter 3.2.1, which ships with NetBackup 3.4.
  - ◆ All clients except Macintosh and OS/2. The NetBackup-Java Windows Display Console is also not included. The software for Macintosh, OS/2, and the Windows Display Console is unchanged from 3.4 and you can use the 3.4 server CD-ROM to install it.

Install 3.4.1 only if you require the above software. Otherwise, install 3.4 and its latest jumbo patch. NetBackup 3.4 and 3.4.1 are completely interoperable and can be viewed as being at the same release level (for example, NetBackup 3.4 servers support 3.4.1 clients).

Software is not changed for Solaris and other platforms not listed above.

2. The 3.4 manuals still apply to 3.4.1, except for the release notes and the installation instructions.

For the release notes see:

- ◆ *NetBackup 3.4.1 Release Notes*

For 3.4.1 installation instructions, see:

- ◆ *NetBackup BusinessServer 3.4.1 Installation Guide - Red Hat Linux 6.2/7.0*



- ◆ *NetBackup 3.4.1 Installation Guide - Windows NT/2000*

PDF copies of the above manuals are included on the 3.4.1 CD-ROM.

---

**Note** The installation for Microsoft Windows clients has changed for 3.4.1 and is different than documented in the NetBackup Installation Guide for PC Clients. See the NetBackup 3.4.1 Installation Guide - Windows NT/2000 for the latest instructions.

---

## Linux

NetBackup 3.4.1 supports Red Hat Linux version 6.2 and 7.0 on NetBackup BusinessServer servers (not DataCenter). For information on configuring devices on these platforms, see Appendix B in these release notes.

## Windows NT/2000

1. NetBackup 3.4.1 for Windows NT/2000 meets Windows 2000 Logo certification requirements.
2. NetBackup failover Master server in a Microsoft Cluster Server (MSCS) environment is supported. For information on configuring this capability, see “Using NetBackup with Microsoft Cluster Server” on page 71 of these release notes.

## Alternative Backup

NetBackup for NDMP has been enhanced to support NetBackup BusinessServer servers running Linux Red Hat 6.2 or 7.0. The *NetBackup 3.4 for NDMP System Administrator's Guide* still applies.

## Database Agents

NetBackup for Oracle is now supported on Linux.

## Media Manager

1. The handling of default media type for robot inventory update has changed.  
On servers running 3.4.1, if you are specifying **Media Type** in **Update Options** before updating the Media Manager volume configuration for a robot (On the **Actions** menu, click **Inventory Robot**) and select **DEFAULT** as the media type:  
And the following is true:
  - ◆ The robot is not an ACS, LMF, RSM, TLH, or TLM robot type.



- ◆ You are not using barcode rules.

Then, the results are as follows:

If *all* of the drives in the robot (configured on this robot host) are:

- ◆ The same type, Media Manager uses the media type for the drives.
- ◆ *Not* the same type, Media Manager uses the default media type for the robot.

Previously, Media Manager used the default media type for the robot, regardless of the drive types.

**2.** The STK SN6000 (Storagenet 6000 Storage Domain Manager) is supported.

This feature requires installation of the Multihosted Drives (SSO) license key. StorageTek (STK) introduced the SN6000 as a method for providing tape drive virtualization. Logical tape drives are presented to standard host operating system interfaces (tape drivers), while robotic control is accomplished through the Automated Cartridge System (ACS).

For more information on the SN6000, see “Using the STK SN6000” on page 34.





# NetBackup 3.4.1 Supported Platforms and Peripherals

## 2

This chapter provides information on the platforms and peripherals that NetBackup 3.4.1 supports.

---

**Note** NetBackup 3.4 and 3.4.1 are completely interoperable and can be viewed as being at the same release level. For example, NetBackup 3.4 servers support 3.4.1 clients.

---

## Server and Client Platform Support

The tables in this section describe hardware and operating system combinations that this release of NetBackup BusinessServer and NetBackup DataCenter support.

- ◆ The Server OS Version column describes the operating system level required to run on a NetBackup master or media server.
- ◆ The Client OS Version column describes the operating system level required to support a NetBackup client. Predecessors and successors to the supported operating system levels may function without difficulty, as long as the release provides binary compatibility with the supported level.

### Notes on the tables:

- ◆ The supported platform tables list all platforms supported by NetBackup (both 3.4 and 3.4.1). However, NetBackup 3.4.1 includes server software for only the OS versions that are shaded. All client software is included with 3.4.1, except for Macintosh and OS2.
- ◆ The following NetBackup client support is available through special order:
  - ◆ Compaq running OpenVMS VAX V7.2-1
  - ◆ Compaq running OpenVMS Alpha for VAX V7.2-1
  - ◆ HP3000 running MPE/iX C55.08 (this support includes TurboStore API)
- ◆ The platform information in the tables was current at the time of printing. Check <http://support.veritas.com/> for the latest platform compatibility information.



## NetBackup DataCenter Supported Platforms

Hardware Type	Operating System	Server OS Version	Client OS Version	Notes
Auspex	NetOS	1.9M1Z3 1.9M1Z4	1.9M1Z3 1.9M1Z4	
Compaq Alpha	Digital UNIX	4.0D	4.0D	
Compaq Alpha	Tru64 UNIX	4.0F, 5.0, 5.0a	4.0F, 5.0, 5.0a	
Compaq Alpha	Windows	NT 4.0, Windows 2000	NT 4.0, Windows 2000	
Cray	UNICOS	----	10.0.x	
Data General (Intel)	DG/UX	----	R4.20MU02	a
HP9000-700	HP-UX	10.20, 11.0	10.20, 11.0	
HP9000-800	HP-UX	10.20, 11.0	10.20, 11.0	
IBM RS6000	AIX	4.2.1, 4.3, 4.3.1, 4.3.2, 4.3.3	4.2.1, 4.3, 4.3.1, 4.3.2, 4.3.3	
Intel 386, 486, Pentium	Novell NetWare	----	3.12, 3.2, 4.10, 4.11, 4.2, 5.x	b
Intel 386, 486, Pentium	OS/2	----	Warp 3, 4	b
Intel 486, Pentium	Windows	----	Windows 95, 98, ME	
Intel 486, PentiumX	Windows	NT 4.0, Windows 2000	NT 4.0, 2000	c
Intel x86	SCO	----	OpenServer 5.0.5	
Intel 386	FreeBSD	----	3.3, 4.0	
Intel x86	Linux	----	Red Hat 5.2, 6.0, 6.1, 6.2, and 7.0. Caldera OpenLinux 2.2 SuSe 6.1 TurboLinux 3.6 Debian GNU/Linux 2.1	d
Intel x86	SCO	----	UnixWare 7.0.1, 7.1	
Intel x86	Solaris	----	2.6, 7, 8	
Macintosh (680x0 or PowerPC)	MacOS	----	7.5.5 to 9.x	



Hardware Type	Operating System	Server OS Version	Client OS Version	Notes
Macintosh (PowerPC)	MacOS X Server	----	1.0, 1.2	
NCR	UNIX SVR4MP-RAS	3.02	3.02	
Pyramid	ReliantUNIX	5.43 C20, C30	5.43 C20, C30	
Sequent	DYNIX/ptx	4.4.2, 4.4.4, 4.5	4.4.2, 4.4.4, 4.5	e
SGI	IRIX	6.5 to 6.5.5	6.5 to 6.5.5	
SPARC/UltraSPARC	Solaris	2.6, 7, 8	2.6, 7, 8	

a. Only on Intel processor-based AViiON servers.

b. Does not support NetBackup Encryption.

c. Requires Windows NT 4.0 Service Pack 4 or later.

d. Requires Motif version 2.1 in order to use the user interface, xbp.

Motif is available from [www.opengroup.org](http://www.opengroup.org). Red Hat 7 requires bug fix for glibc and the ncurses4 compatibility library be installed.

e. Requires level 2.4.0 or later TCP to be installed.

## NetBackup BusinessServer Supported Platforms

Hardware Type	Operating System	Server OS Version	Client OS Version	Notes
Compaq Alpha	Digital UNIX	----	4.0D	
Compaq Alpha	Tru64	----	4.0F, 5.0, 5.0a	
Compaq Alpha	Windows	----	NT 4.0	
Data General (Intel)	DG/UX	----	R4.20MU02	a
HP9000-700	HP-UX	11.0	11.0	
HP9000-800	HP-UX	11.0	11.0	
IBM RS6000	AIX	----	4.2.1, 4.3, 4.3.1, 4.3.2, 4.3.3	
Intel 386, 486, Pentium	Novell NetWare	----	3.12, 3.2, 4.10, 4.11, 4.2, 5.x	b
Intel 386, 486, Pentium	OS/2	----	Warp 3, 4	b



Hardware Type	Operating System	Server OS Version	Client OS Version	Notes
Intel 486, Pentium	Windows	----	Windows 95, 98, ME	
Intel 486, Pentium	Windows	NT 4.0, Windows 2000	NT 4.0, 2000	c
Intel x86	SCO	----	OpenServer 5.0.5	
Intel 386	FreeBSD	----	3.3, 4.0	
Intel x86	Linux	Red Hat 6.2, 7.0	Red Hat 5.2, 6.0, 6.1, 6.2, and 7.0 Caldera OpenLinux 2.2 SuSe 6.1 TurboLinux 3.6 Debian GNU/Linux 2.1	d, b
Intel x86	SCO	----	UnixWare 7.0.1, 7.1	
Macintosh (680x0 or PowerPC)	MacOS	----	7.5.5 to 9.x	
Macintosh (PowerPC)	MacOS X Server	----	1.0, 1.2	
NCR	UNIX SVR4MP-RAS	----	3.02	
Pyramid	ReliantUNIX	----	5.43 C20, C30	
Sequent	DYNIX/ptx	----	4.4.2, 4.4.4, 4.5	e
SGI	IRIX	----	6.5 to 6.5.5	
SPARC/UltraSPARC	Solaris	2.6, 7, 8	2.6, 7, 8	

a. Only on Intel processor-based AViiON servers.

b. Does not support NetBackup Encryption.

c. Requires Windows NT 4.0 Service Pack 4 or later.

d. Requires Motif version 2.1 in order to use the user interface, xbp.  
Motif is available from [www.opengroup.org](http://www.opengroup.org).

e. Requires level 2.4.0 or later TCP to be installed.



## Database Agent Platform Support

The NetBackup 3.4.1 CD-ROM includes software for NetBackup for Oracle on Linux (the other NetBackup database agents are on the NetBackup 3.4 CD-ROM). To run NetBackup for Oracle on Linux, your system must have the following installed:

- ◆ Red Hat Linux 6.2.
- ◆ The 8.1.6.2 Oracle patchset This Oracle patchset is scheduled to be released by Oracle in the near future. For current status on this patchset, contact Oracle.

## Support for Files Greater than Two Gigabytes

The current version of NetBackup supports file sizes greater than two gigabytes on the following client systems.

- ◆ Compaq Alpha
- ◆ FreeBSD
- ◆ HP-UX
- ◆ IBM AIX
- ◆ Mac OS X Server (as NetBackup client)
- ◆ Novell NetWare
- ◆ IBM DYNIX
- ◆ SGI IRIX
- ◆ Sun Solaris
- ◆ Windows NT/2000



## Binary Sizes

The following table shows the approximate binary size of the NetBackup and Media Manager software for each platform and operating system supported by NetBackup.

**Note** In the following table, the shaded values indicate the server software included on the NetBackup 3.4.1 CD-ROM. All client software is included with 3.4.1, except for Macintosh and OS2.

Table 2. Binary Sizes

Hardware Type	Operating System	NetBackup Server	Media Manager	NetBackup Client
Auspex	Auspex	73 MB	38 MB	8001 KB
Compaq Alpha	OSF/1, Digital UNIX	96 MB	45 MB	7305 KB
Compaq Alpha	Tru64 UNIX	96 MB	45 MB	7305 KB
Cray J90	UNICOS	--	--	32 MB
Data General	DG/UX	--	--	4777 KB
Compaq Alpha	Windows NT	79.5 MB	11 MB	4160 KB
HP9000-700	HP-UX 10.20, 11.0	137 MB	28 MB	8323 KB (a)
HP9000-800	HP-UX 10.20, 11.0	141 MB	31 MB	9067 KB (a)
IBM RS6000	AIX	91 MB	39 MB	8648 KB
Intel 386	FreeBSD	--	--	3707 KB
Intel 386, 486, Pentium	OS/2	--	--	12.7 KB
Intel 486, Pentium	Windows 95, 98, ME	--	--	2.7 KB
Intel Pentium	Windows NT/2000	70 MB	9 MB	12.7 KB
Intel x86	Linux	110 MB	14 MB	4429 KB (b)
Intel x86	SCO UnixWare	--	--	5858 KB (c)
Intel x86	SCO OpenServer	--	--	4778 KB (c)
Intel x86	Solaris	--	--	7036 KB
Intel 386, 486, Pentium	Novell NetWare	--	--	NLM, 1.2 KB GUI, 756 KB
Macintosh (680x0 or PowerPC)	MacOS	--	--	5083 KB
Macintosh OS X Server	MacOS	--	--	5500 KB





Table 2. Binary Sizes (continued)

Hardware Type	Operating System	NetBackup Server	Media Manager	NetBackup Client
NCR	UNIX SVR4MP-RAS	64 MB	27 MB	5821 KB
Pyramid	ReliantUNIX	77 MB	28 MB	7132 KB
SGI	IRIX	90 MB	39 MB	8691 KB
Sequent	DYNIX ptx	78 MB	35 MB	7389 KB
SPARC/UltraSPARC	Solaris 2.6, 7, 8	150 MB	34 MB	15MB (d)

a. A total of 17228 KB installed on the server with the NetBackup-Java interface.

b. Applies to all the supported versions of Linux.

c. A total of 10474 KB installed on the server.

## Supported Peripherals

### Supported Peripherals by Vendor

For information on supported peripherals:

1. Go to the VERITAS support web page  
[www.support.veritas.com/](http://www.support.veritas.com/)
2. In the VERITAS Support Product List, choose **NetBackup Products**.
3. A page appears with a list of the NetBackup products. Choose **NetBackup BusinessServer** or **NetBackup DataCenter**.
4. The home page for the product appears. Look under **Support Options** and choose **Compatibility Lists**.
5. The compatibility matrix options page appears. Choose **Device Support Matrix**.
6. A page appears where you can choose the version for which you want device information (for example, **NetBackup BusinessServer Version 3.4**). Choose the desired version and on the next page that appears, pick one of the following:
  - ◆ The name of the hardware vendor
  - ◆ View All Supported Drives
  - ◆ View All Supported Libraries
  - ◆ View All Supported Robot Types.



## Robot Type Support By Platform

The following tables show the robot types that NetBackup and Media Manager support on each platform. The robot type classifies the devices and peripherals either by their physical characteristics, by their media type, or by the communication methods used by their underlying robotics. See the Media Manager system administrator's guide for more information about these robot types.

- ◆ ACS - Automated Cartridge System
- ◆ LMF - Library Management Facility
- ◆ ODL - Optical Disk Library
- ◆ RSM - Removable Storage Manager
- ◆ TL4 - Tape Library 4MM
- ◆ TL8 - Tape Library 8MM
- ◆ TLD - Tape Library DLT
- ◆ TLH - Tape Library Half-inch
- ◆ TLM - Tape Library Multimedia
- ◆ TS8 - Tape Stacker 8MM
- ◆ TSD - Tape Stacker DLT
- ◆ TSH - Tape Stacker Half-inch

---

**Note** The following tables list only 3.4.1 supported robots. For the list of robots supported by 3.4, see the *NetBackup 3.4 Release Notes*.

---

**NetBackup DataCenter 3.4.1 - Robot Support by Platform**

<b>Robot Type <sup>1</sup></b>	<b>Windows NT/2000</b>
ACS <sup>2</sup>	Yes
LMF	No
ODL	No
RSM	Yes <sup>4</sup>
TL4 <sup>4</sup>	Yes
TL8	Yes
TLD	Yes
TLH	Yes <sup>5</sup>
TLM	No
TS8	Yes
TSD	Yes
TSH	No

1. Use the acronym when you define the robot to NetBackup and Media Manager.
2. Contact your drive and operating system vendors to ensure that the standard tape drive support is available.
3. Supported only with Hewlett-Packard and Sony drives.
4. Supported only on Windows 2000.
5. IBM ATL package version level tested on Windows NT 4.0 is 4.0.5.0. Robotic control is not supported on Windows 2000 or Alpha-based Windows NT.



**NetBackup BusinessServer 3.4.1 - Robot Support by Platform**

<b>Robot Type <sup>1</sup></b>	<b>Windows NT/2000</b>	<b>Red Hat Linux 6.2/7.0</b>
RSM	Yes <sup>3</sup>	No
TL4 <sup>2</sup>	Yes	No
TL8	Yes	No
TLD	Yes	Yes <sup>4</sup>
TS8	Yes	No
TSD	Yes	Yes <sup>4</sup>

1. Use the acronym in this column when you define the robot to NetBackup and Media Manager.
2. Supported only with Hewlett-Packard and Sony drives.
3. Supported only on Windows 2000.
4. Linux NetBackup servers support only DLT type drives.



## NetBackup 3.4.1 Operational Notes

3

The following notes apply specifically to NetBackup 3.4.1 and explain important aspects of NetBackup operations that may not be documented elsewhere. Many of these notes also apply to 3.4. However, for a complete listing of NetBackup 3.4 operational notes see the *NetBackup 3.4 Release Notes*.

---

**Note** References to UNIX also apply to Linux, unless otherwise stated.

---

### Installation

1. It is not possible to revert to NetBackup BusinessServer after you install and begin using NetBackup DataCenter.

In addition, VERITAS does not support the installation of NetBackup BusinessServer software on a system that already has NetBackup DataCenter software installed.

2. To upgrade from 3.4.1 BusinessServer to 3.4.1 DataCenter:

On Windows NT/2000, enter the new license key. This is the only step required. All required software components are already installed. (NetBackup for Linux server does not support DataCenter)

3. For Microsoft Windows clients, before upgrading the operating system, first uninstall NetBackup to ensure that platform-specific registry entries are clean. Then upgrade the operating system and reinstall NetBackup.
4. Before doing an upgrade installation, exit all NetBackup applications and stop all daemons (UNIX) and services (Windows NT/2000).
5. When uninstalling NetBackup on Windows 2000 systems, the use of the **Remove** button in the Add/Remove Programs applet can take several minutes. To avoid this wait, it is recommended that you click the **Change** button, and select **Remove** from the screens that follow.
6. Client software for HP-UX 10.20 must be installed from the 3.4 GA CD-ROM.
7. NetBackup 3.4.1 supports the Windows Millennium Edition as a NetBackup client. To install or configure a Windows ME client, follow the Windows 98 installation instructions.



8. After installing NetBackup for Encryption or NetBackup for NDMP, restart `bpdbm` on the master server. If you install NetBackup Oracle Advanced BLI Agent, restart `bpdbm` on the master server after you change the NetBackup configuration to allow block incremental backups.

For instructions on configuring NetBackup to allow block incremental backups, see the *NetBackup for Oracle Advanced BLI Agent System Administrator's Guide*. For instructions on restarting `bpdbm`, see the section on Managing NetBackup daemons/services in the "Managing NetBackup" chapter of the NetBackup system administrator's guide.

9. When installing or deinstalling NetBackup for NDMP on a Windows NT/2000 media server (Intel or Alpha), you **MUST** stop the NetBackup Device Manager Service.
10. There are times when a Windows NT 4.0 system will require two system reboots. The first reboot may occur at the beginning of the install process. This reboot updates the Microsoft installer and associated DLLs. The second reboot may occur after you have added your license key and then selected either Master Server, Media Server, or Administrative Client.
11. Windows NT 4.0 service pack 4 or later is required on supported Windows NT NetBackup servers for this release. This brings the system DLLs to a level supporting the wizards.
12. You cannot install NetBackup Encryption on NetBackup 3.4.1 BusinessServer for Linux.
13. If you install the 56-bit NetBackup Encryption product, the 56-bit DES libraries may not install properly.

To work around this problem, issue the command below from the master server after installing the 56-bit DES Encryption product as explained in chapter 2 of the *NetBackup Encryption System Administrator's Guide*:

- ◆ On a Windows NT NetBackup Master Server, execute the following (all on one line):

```
install_path\bin\bpinst -CRYPT -crypt_strength des_56  
-client_libraries install_path\lib\client server
```

Where *server* is the name of the master server.

- ◆ On a UNIX (non-Linux) NetBackup master server, execute the following (all on one line):

```
/usr/opensv/netbackup/bin/bpinst -CRYPT -crypt_strength  
des_56 -client_libraries /usr/opensv/lib/client server
```

When you push the encryption libraries to the clients as explained in chapter 3 of the *NetBackup Encryption System Administrator's Guide*, include "-crypt\_strength des\_56" on the bpinst command to ensure that the 56-bit DES libraries are also pushed:

- ◆ On a Windows NT NetBackup master server, execute the following (all on one line):

```
install_path\bin\bpinst -CRYPT -crypt_strength des_56
-client_libraries install_path\lib\client client
```

Where *client* is one or more client names.

- ◆ On a UNIX (non-Linux) NetBackup master server, execute the following (all on one line):

```
/usr/opensv/netbackup/bin/bpinst -CRYPT -crypt_strength
des_56 -client_libraries /usr/opensv/lib/client client
```

14. To install NetBackup Advanced Reporter or other NetBackup add-on products, run the `install` script located at the base directory on the CD-ROM. The `install` script displays a menu from which you can choose the option to install NetBackup Add-On Product Software. Follow the prompts to complete the installation.

## General Notes

### 1. Back-level support

- ◆ 3.4.1 is completely interoperable with 3.4 (when the latest 3.4 jumbo patch is installed) and in the following is considered the same level. For example, NetBackup 3.4 servers support 3.4.1 clients.
- ◆ Within a NetBackup server-client group, all master and media servers must be running a version of NetBackup equal to or higher than each of the clients. The master and each media server must be running the same version of NetBackup. The clients can run one revision lower than the servers.
- ◆ Within a Global Data Manager (GDM) configuration, the Global Data Manager server must be running a version of NetBackup equal to or higher than each of the masters in its domain (for example, Global Data Manager 3.4 supports only NetBackup 3.4.1, 3.4, 3.3, or 3.2 servers).

The NetBackup server or client that you specify in the NetBackup-Java login dialog must be running the same version of NetBackup as the host where you started the NetBackup-Java application (the only exception is with 3.4.1 and 3.4, which are version compatible).



For example, on UNIX, if you attempt to login to the NetBackup-Java application server running on a NetBackup 3.2 host through NetBackup-Java applications running on a 3.4 host you get the following error message and cannot continue. You can either change the name of the host in the dialog or choose to exit the application.

```
NetBackup-Java: bpjava-msvc is not compatible with this
application version. You may try login to a
different NetBackup host or exit the application. The
remote NetBackup host will have to be configured with
the same version of NetBackup as the host you started
the application on.
```

Conversely, on UNIX, if you attempt to login to the NetBackup-Java application server running on a NetBackup 3.4 host through NetBackup-Java applications running on a 3.2 host you get the following error message and cannot continue. You can either change the name of the host on the dialog or choose to exit the application.

```
bpjava-msvc: the client is not compatible with this server
version (3.4)
```

2. The Motif administrator interfaces are not supported on NetBackup Business Server for UNIX and are not included with the software.

The `xnb`, `xbpadm`, `xvadm`, `xdevadm`, and `xbpmon` applications are not included with NetBackup Business Server for UNIX. The NetBackup-Java interface (`jnbSA`) is the primary administrator interface for UNIX platforms.

3. Local translations to other languages are not included in this package.
4. Man pages are not installed on UNIX clients.

NetBackup man pages are installed only on the UNIX NetBackup server.

If you want to provide man pages for the commands on UNIX client workstations, you will find troff source for them in the directory `/usr/opensv/netbackup/bin/goodies/man`.

5. Some command line interfaces are undocumented.

Some administrative command line interfaces to NetBackup and Media Manager are not documented and not supported.

## NetBackup

1. Decoding a time stamp.

Occasionally, it is desired to convert the time stamp used by NetBackup for its backup IDs into a human-readable format. Backup IDs take the form of *client\_name\_timestamp*; for example, `danr_0818775918`.



To convert 818775918 to a readable format, run the following command:

On Windows NT, execute:

```
install_path\NetBackup\bin\bpdbm -ctime timestamp
```

For example:

```
C:\Program Files\Veritas\NetBackup\bin\bpdbm -ctime 868775918
868775918 = Sun Jul 13 01:38:38 1997
```

On UNIX, execute:

```
/usr/opensv/netbackup/bin/bpdbm -ctime timestamp
```

For example:

```
# /usr/opensv/netbackup/bin/bpdbm -ctime 818775918
818775918 = Tue Dec 12 07:45:18 1995
```

## 2. Intentionally destroying NetBackup catalogs.

In a demonstration or “proof-of-concept” environment, it is sometimes desirable to destroy any image catalogs and tape files before taking the system into full production mode.

To delete all backup and archive image catalogs, as well as the information about the secondary storage being used for those images:

- a. Log on to the NetBackup server as the root user (on UNIX) or administrator (on Windows NT/2000).
- b. For each media in the NetBackup media listing (use the NetBackup Report interface), enter the following command (one line):

On Windows NT/2000:

```
install_path\NetBackup\bin\admincmd\bpxexpdate -d 0 -ev media_id [-host hname]
```

On UNIX:

```
/usr/opensv/netbackup/bin/admincmd/bpxexpdate -d 0 -ev media id [-host hname]
```

Where *media id* is the media ID to be deleted and *hname* is the name of the host on which the media resides. You must specify this hostname only if your configuration uses multiple volume database hosts.

Manual expiration of media with `bpxexpdate` causes the media to be removed from the NetBackup catalog and to be deassigned in the volume database, regardless of the media’s prior state (FROZEN, SUSPENDED, and so on).



3. On UNIX, the ATRIA ClearCase application does not work correctly with backup products.

The ATRIA ClearCase application does not operate correctly with any backup product, including NetBackup. The ATRIA release notes suggest stopping the ClearCase application before starting a backup. One way to accomplish this with NetBackup is to modify the `bpstart_notify` script to stop ClearCase before the backup and to modify the `bpend_notify` script to restart it when the backup is complete.

4. On UNIX, if you back up files with both NetBackup and `dump .ffs`, a `dump .ffs` incremental dump sees all files that NetBackup has accessed as candidates for an incremental dump.

The `dump .ffs` utility looks at the file's "inode-change" time when performing incremental dumps.

If NetBackup has backed up files in the same partition, the file's inode-change time is modified when NetBackup resets access time for any file that is opened and read. Therefore, a `dump .ffs` incremental dump will see all files that NetBackup has accessed as candidates for an incremental dump.

There is no method by which NetBackup can reset the inode-change time. See the description of the `(USE_CTIME_FOR_INCREMENTALS)` option for a client `bp.conf` file in the NetBackup system administrator's guide for UNIX.

5. On some UNIX platforms with NetBackup configurations it can be necessary to increase the system's message queue resources to avoid `bpsched` hangs.

Example:

Make the following changes to the `/etc/system` file:

```
set msgsys:msginfo_msgmap=500
set msgsys:msginfo_msgmnb=65536
set msgsys:msginfo_msgssz=16
set msgsys:msginfo_msgseg=8192
set msgsys:msginfo_msgtql=500
```

Reboot the system.

6. On a UNIX NetBackup server, if the backup of the NetBackup database fails with an EXIT STATUS of 124 and the database is on a RAID partition, check the `bpbkar` activity log for a message such as the following.

```
08:54:35 [27862] <8> bpbkar: WRN - Could not reset access time of
/var/openv/netbackup/db/.snapshot/nightly.0/images/troi/INDEXLEVEL
```

Perform the following workaround to avoid this problem. Change the NetBackup catalog backup configuration so catalog backups include all the files and directories in the `/usr/openv/netbackup/db` directory. If you have questions about what should be done, contact VERITAS customer support.

## 7. Windows 2000 and user-directed operations

If users other than the administrator will be using the client-user interface on a Windows 2000 system to perform backups and restores, write permission to the *install\_path*\NetBackup\Logs folder should be given to those users. On Windows 2000 systems the Program Files folder, by default, is not writable by users other than the administrator. NetBackup writes log files and progress files to the Program Files\Veritas\NetBackup\Logs folder by default. Users without write permission to the Logs folder receive an error message when attempting a backup or restore and the operation is aborted.

8. The NetBackup Administration Client for Windows NT is a version of NetBackup for Windows NT that can be used to remotely administer one or more UNIX or Windows NT NetBackup servers. It comes with all of the standard NetBackup Server for Windows NT interfaces and can be used to create backup policies (classes), manage volumes, view status, monitor tape drives, and so on, on a remote NetBackup server. It cannot be used as a NetBackup master or media server itself; it is just used for remote administration of other NetBackup servers, UNIX or Windows NT.

Although the Administration Client cannot be used as a master or media server, in order for it to remotely administer a NetBackup server, it must be added to the server list on that server in the same way that other NetBackup servers are added to the server list to give them access to that server.

The documentation set does not, in most cases, specifically refer to the NetBackup Administration Client since, for all practical purposes, using the NetBackup Server for Windows NT interfaces on the Administration Client is identical to using them locally on the server that is being administered. Of course, the master server or device host shown in the interface will be the server name that is being administered instead of the local server name.

9. For Windows 2000 clients if you do not use the *All\_local\_drives* directive in the files list, you must specify *System\_state:\* in the file list to ensure that the Windows 2000 system state is backed up.
10. A new status code, 134 indicates that all drives in the storage unit are in use. The scheduler then tries another storage unit and if one is not available requeues the job and retries it later. No corrective actions are necessary because scheduler handles the problem automatically.

## Media Manager

1. SCSI robotic peripherals must not be in sequential mode for use with Media Manager.

Media Manager robotic software expects SCSI robotic peripherals to be in random mode (SCSI control of the robot) rather than sequential mode. The robotic control processes cannot control robotic devices that are in sequential (stacker) mode.



2. Single-ended to differential SCSI converters are not supported.

We do not recommend or support the use of single-ended to differential SCSI converters on Media Manager controlled devices. You may encounter problems if you use these converters.

3. Drives and robots connected through fibre channel cause increased complexity in the Media Manager configuration. On some operating systems, the use of fibre-to-SCSI bridges may result in inconsistencies in the device path upon a server reboot. After rebooting the server, therefore, always verify the device configuration.
4. Authentication and authorization in Media Manager can affect systems where NetBackup authentication/authorization has been enabled. For more information, see the "vmd Security" topic in the system administrator's guide for Media Manager.
5. It is recommended that `vmd` be running at all times.

Device configuration changes, even those made local to a server, can require `vmd` (Media Manager volume daemon and NetBackup Volume Manager service) to be running. It is recommended that `vmd` be running at all times, including when changes are made to the Media Manager device configuration.

6. NetBackup BusinessServer supports only one robot per server and these robots can have a maximum of two drives and 30 slots.
7. Nonroot access to NetBackup devices and media on UNIX.

On UNIX, NetBackup media is "protected" from nonroot user access (both read and write) because the special files identifying the tape or optical drives allow only root usage when the Media Manager `ltid` process is executing. For example:

```
ls -al /dev/rmt/6_8mm8500cb /dev/rmt/6_8mm8500ncb
crw-----  1 bin bin 5 0x110603 Apr 27 09:06 /dev/rmt/6_8mm8500cb
crw-----  1 root bin 5 0x190603 May 18 05:51 /dev/rmt/6_8mm8500ncb
```

Other special files that reference the same device may exist. These files frequently define different densities at which the device is capable of writing. For example:

```
ls -al /dev/rmt/6_8mm8200
crw-rw-rw-  1 bin bin 5 0x000602 Apr 27 09:06 /dev/rmt/6_8mm8200
```

To protect NetBackup media from nonroot access, you must manually change the permissions on all of these special files to 600.

See the NetBackup system administrator's guide for more information on allowing nonroot administration.

8. UNIX Nonroot permissions for mounting and unmounting media.

For UNIX, the commands for mounting and unmounting media (`tpreq` and `tpunmount`) are released with permission modes set to 500 (`-r-x-----`). If you want to allow any user in the system to mount tapes, the mode can be changed to 555 (`-r-xr-xr-x`). If you want to allow a specific group of users to mount tapes, perform commands similar to the following:

```
cd /usr/opensv/volmgr/bin
chgrp tapeusers tpreq tpunmount
chmod 550 tpreq tpunmount
```

9. When using `xvmaadm` or `vmadm`, Robot host is NONE for Storage Tek Automated Cartridge System (ACS) media and ACS entries in robot inventory pick lists.

In releases previous to 3.0, the robot host field for ACS media (volume) entries was not consistently handled. The robot host for ACS media is set to the value NONE to ensure that:

- ◆ all compatible media in an ACS robot can be placed in the same volume group,
- ◆ ACS robot inventory requests are sent to the host where the ACS robot is configured under Media Manager.

When selecting an ACS robot for an inventory operation through the NetBackup administrator's interface, you will be prompted to enter the host. You should enter the host where the ACS robot is configured in Media Manager.

---

**Note** Do not enter the ACSLS host unless the ACS robot is also configured on that same host.

---

## 10. Automatic device discovery and configuration

- ◆ Auto discovery and configuration is currently available on Windows NT/2000 and Red Hat Linux 6.2/7.0.
- ◆ After adding or removing devices from a SCSI bus, the OS must be made aware of the new configuration before NetBackup auto discovery can be used. Often, this requires a reboot of the system.
- ◆ Auto discovery depends on the existence of a way to issue SCSI pass-thru commands to the devices.
  - ◆ On Windows NT/2000, a tape driver must exist for each tape device.
  - ◆ On Linux, device files must exist following the naming conventions described in the Media Manager Device Configuration Guide.
- ◆ Auto configuration depends on device serialization. For devices to be fully auto configured, the following two statements must be true for your system:
  - ◆ Each robot and drive reports a unique serial number.



- ◆ Each robot reports the serial number of each of the drives contained within the robot.

All information required for full auto configuration may not be available on some systems. In this case, auto configuration will do as much as possible with the limited device information. The user must manually configure the remaining devices.

Since device serialization is a relatively new capability for some devices, you may need to ask your hardware vendor for newer firmware that returns serial numbers. Even with the proper firmware, some devices require the vendor to perform another action to enable serialization for the device.

- ◆ On a system running Windows 2000, robots configured for use by Microsoft RSM are not discovered.
  - ◆ Not all robot types are discovered:
    - ◆ On Linux, only TLD and TSD robot types are discovered.
    - ◆ On Windows NT/2000, ACS, TLH, and RSM robots are not discovered.
  - ◆ If tape drives are in use, they cannot be discovered.
  - ◆ Optical disks are not discovered.
11. Shared Storage Option can be used in NetBackup DataCenter with standalone drives and the following robot types: ACS, TL8, TLD, and TLH. This supersedes information in the robot overview section of the Media Manager System Administrator's Guide appendixes.
  12. TapeAlert is supported on Windows NT. For more information on TapeAlert, see the Reference Topics appendix in the Media Manager system administrator's guide.
  13. On NetBackup BusinessServer for Linux, NetBackup 3.4.1 does not support version 3.x.x or later of the Linux sg driver. Specifically, NetBackup 3.4.1 was tested with sg versions 2.1.36 through 2.1.39.
  14. Using TLH robotic control, if the TLH drive map has not been frozen, tapes may be mounted in the wrong drives if the IBM Library Manager makes a device unavailable. In this situation, the Media Manager device daemon (NetBackup Device Manager service) should be stopped until the drive can be made available again, or instead, the device configuration must be corrected to account for the modified robot drive numbers. For information on TLH drive addressing, see step 3 under "Media Manager" on page 38.
  15. The NetBackup Tape Device Driver Installer is included on the NetBackup 3.4.1 NT/Windows2000 CD-ROM. This program installs VERITAS tape drive drivers for Microsoft Windows NT and Windows 2000. The file name is `NetBackupTapeDeviceDriverInstall_233895.exe`.

Double-clicking on the file displays a wizard that guides you through the installation of the VERITAS device drivers. The wizard offers the following choices for the devices to be used with VERITAS drivers:

- ◆ Choice 1 - Use VERITAS tape drivers for all tape devices. The VERITAS Device Driver Installer identifies existing tape devices and loads an appropriate VERITAS driver, replacing any non-VERITAS drivers currently bound to the device. This is the recommended selection setting.
- ◆ Choice 2 - Use VERITAS tape drivers for tape devices that do not already have drivers loaded. VERITAS tape drivers are installed for devices that are not supported by existing Microsoft or OEM drivers. VERITAS tape drivers are set to load prior to Plug and Play drivers. VERITAS tape drivers may detect additional supported hardware and will replace the current drivers.
- ◆ Choice 3 - Remove VERITAS Tape Drivers. All existing VERITAS tape device drivers are uninstalled. Windows 2000 Plug and Play Manager should detect the devices after a reboot and offer to reinstall tape device drivers of your choice. Windows NT tape drivers require manual reinstallation through the Control Panel > Tape Devices.

---

**Note** VERITAS tape class drivers are not compatible with the Windows 2000 Removable Storage service.

---

You can also get the NetBackupTapeDeviceDriverInstall\_233895.exe file from the VERITAS support website.

`ftp.support.veritas.com/Pub/Support/Products`

The NetBackup Tape Device Driver Install program includes the following Windows NT/2000 drivers:

VERITAS 04mmdat.sys  
VERITAS 0archqic.sys  
VERITAS 0dlttape.sys  
VERITAS 0exabyte2.sys  
VERITAS 0tandqic.sys  
VERITAS dlttape.sys  
VERITAS halfinch.sys  
VERITAS sonysdx.sys  
VERITAS trscsi.sys



## Using NetBackup With VERITAS Storage Migrator (VSM)

---

**Note** NetBackup BusinessServer does not support VERITAS Storage Migrator (VSM).

---

1. If you have VERITAS Storage Migrator installed on a NetBackup client system and you are upgrading to NetBackup 3.4.1 on that client, you must upgrade to release 3.4.1 of VERITAS Storage Migrator for UNIX at the same time you upgrade to NetBackup 3.4.1.

If you have VERITAS Storage Migrator Enterprise Extension installed on a NetBackup client system and you are upgrading to NetBackup 3.4.1 on that client, you must upgrade to release 3.4.1 of VERITAS Storage Migrator Remote for UNIX at the same time you upgrade to NetBackup 3.4.1.

Running HSM 3.1.x with NetBackup 3.4.1 on the same client is an unsupported configuration.

2. Archiving migrated files.

Do not archive files that have been migrated by the client component of VERITAS Storage Migrator on UNIX clients where VERITAS Storage Migrator is installed. Backing up migrated files will not cause problems.

A file migrated from a client workstation, through one of these products, exists on the workstation as a link file. Should the user subsequently archive this file using NetBackup, the link (not the data) is backed up. Then the link is deleted, causing the data associated with the file to become an “orphan” on the migration server.

If the link file is restored on the client after the administrator on the migration server deletes orphan files, the data associated with the link is irretrievable.

3. Do not place the NetBackup databases on a filesystem that is managed by VERITAS Storage Migrator.

## NetBackup-Java Interfaces

### General Items Applicable to All NetBackup-Java Applications

1. NetBackup-Java GUI application software is installed and configured only on the Solaris, Red Hat Linux 6.2/7.0, HP-UX, and Windows NT/2000, 95, and 98 platforms that NetBackup supports. NetBackup client capabilities are installed and configured on Solaris Intel 2.6, 7, or 8 and Red Hat Linux 6.2/7.0.
2. On GDM, the Activity Monitor and Device Monitor applications support activity and device monitoring of Backup Exec machines running VERITAS Backup Exec version 7.3 and higher.





3. A Solaris Intel NetBackup client cannot be used as a display console for NetBackup-Java administrative applications. Only the `jbpSA` application is supported on this platform and is started with the `jbpSA` command.
4. NetBackup-Java uses a reserved port for communication with the authentication service (`bpjava-msvc`) of its application server program.
5. Dialog modality in Java was changed in version 1.1.6 to use "full application modality" (see Sun's Java bug report 4058370). The reason for the change was to provide consistent behavior across Java environments (the behavior had varied between CDE and other windowing environments). What this means for NetBackup-Java is that if a modal dialog (one which blocks input to other windows) is open, input is blocked for all other NetBackup-Java windows, not just the dialog's parent window. For example: assume you are using the Storage Unit Management application and the "Change Storage Unit" dialog is open. In this instance, if you select the main NetBackup-Java "launch" window and try to start another application it will not respond. You must finish entering your choices into the "Change Storage Unit" dialog (or cancel the operation) before you can interact with another NetBackup-Java application.
6. Remote display to a different platform type from the one where the application was started is not supported. For example, if you are executing `jnbSA` on an HP 11.0 machine, you cannot use the `DISPLAY` environment variable to display back to a Solaris 2.6 machine.
7. If you are not set up properly to display to a remote machine from where you are executing `jnbSA`, you will see one of the following happen: nothing (it is probably displaying on the machine where `jnbSA` is executing), the command fails with no error message (that is, the OS command prompt is received) or the following error message is placed in the log file (the log file name is displayed to the window in which you executed the `jnbSA` command).

```
java.lang.InternalError: Can't connect to X11 window server using
"host_name" as the value of the DISPLAY variable.
```

Prior to starting `jnbSA`, be sure to execute the `xhost` command on the machine where you intend to see the user interface and set the `DISPLAY` environment variable on the machine executing `jnbSA` prior to starting `jnbSA`. Reference the man page for the `xhost` command for additional capabilities.

8. Due to problems in the HP-UX JRE used by NetBackup-Java, you probably can not display to a remote X server when starting up the NetBackup-Java applications on an HP-UX 11.0 system. It hangs with no GUI displayed and no error message. Your alternatives are:
  - ◆ Execute NetBackup-Java on another Solaris or HP machine that has a graphics console and login (through the NetBackup-Java login dialog) to the target HP machine you wish to administer. This is the most straightforward and



recommended method of doing remote administration through the NetBackup-Java applications of a NetBackup server that does not have a graphics console or when the console is not accessible.

- ◆ Use the Java Windows Display console from a Windows NT/2000/98/95 computer.
  - ◆ Use the Windows NT Administration client installed on a Windows NT/2000 computer.
9. For Linux, NetBackup-Java supports only Red Hat version 6.2/7.0 on an Intel Pentium that has 256 MB of RAM with 128MB available for the application. Other platforms, such as Sparc, Alpha, or PowerPC are not supported, nor are SMP OS/HW architectures.

The following window manager environments are supported.

- ◆ GNOME/Enlightment
  - ◆ KDE/KWM
10. Only the CDE and Motif window managers are supported on Solaris and HP-UX.
- VERITAS supports only the CDE and Motif window managers when using NetBackup-Java. There are a number of user interface anomalies using the various window managers available on UNIX platforms. Many of these problems are documented as Java bugs. Most of these problems are due to unusual or non-standard window manager configurations and will occur randomly and infrequently. In the most common cases of misplaced or shifted components within a dialog, simply resizing the dialog will repaint the display and cause the interface to be displayed correctly. Although CDE, MWM and OLWM have the most reported bugs, this is largely due to their popularity; do not use a `fvwm` or `twm` instead. The recommended window manager is CDE, with which we have seen the best overall performance.
11. Window managers configured for auto focus are not supported. Auto focus means that windows are activated (get the focus) when you position the mouse cursor over them. The following explains how to correctly set up a CDE environment.
- In the CDE environment, use the Style Manager -- Window dialog to change the window behavior to Click In Window To Make Active. NetBackup-Java will not run properly if the Style Manager has the following selected: Point in Window To Make Active.
12. To better facilitate getting support information for problems you may experience with NetBackup-Java when running on Solaris or HP-UX, the application startup script, `jnbSA`, writes a log file by default to `/usr/opensv/java/logs`. There will be one log file for every instance of the application. Normally, these log files are not large (less than two KB). However, periodic pruning of the files in this directory is recommended.

For more detail, refer to the “Gathering Information for NetBackup-Java” section in the *NetBackup Troubleshooting Guide - UNIX*.

13. You can access online help for the NetBackup-Java applications in a browser outside of the applications by opening one of the following document files.

For NetBackup DataCenter

file:/usr/opensv/java/vrts/nbu/helpDC/en/MainHelp.html - admin applications

file:/usr/opensv/java/vrts/nbu/helpDC/en/help.html - jbp

14. On Solaris the X11 shared library (libX11.so.4) is required for NetBackup-Java. It resides in /usr/openwin/lib if the OpenWindows package is installed. The application startup scripts, jnbSA and jbpSA, check for the existence of /usr/openwin/lib (as the default location for this library) prior to setting the LD\_LIBRARY\_PATH environment variable. If it doesn't exist the following error message appears.

Directory /usr/openwin/lib does not exist. It is the default location for libX11.so.4 which is required by NetBackup-Java. Please create the /usr/openwin/lib directory and a symbolic link for it or modify this script to properly set the LD\_LIBRARY\_PATH environment variable.

15. Long waits for application response and/or incomplete data may be returned in the applications as a result of invalid NetBackup configurations or inadequate file-system space in /usr/opensv/netbackup/logs.
16. NetBackup-Java doesn't support remote display back to a Windows NT/2000/95/98 machine using any X terminal emulator software. Instead, use the NetBackup Windows Display Console..
17. NetBackup-Java does not support monochrome terminals.
18. When using the NetBackup-Java applications on a Solaris X86 machine with a two-button mouse, right button popup menus can only be popped up using the right button with the Ctrl (control) key as follows:
  - a. Press Ctrl key and hold.
  - b. Press the second mouse button. A menu appears.
  - c. Release the Ctrl key.
  - d. Select an item from the menu in either of the following ways:
    - ◆ Drag the cursor to the item and release the second mouse button
    - ◆ or
    - ◆ Release the second mouse button and then select the menu item with the first mouse button.



- 19.** To allow administration through the NetBackup-Java application executing on a machine outside a firewall, the firewall must permit access to port 13722 and ports in the range defined by the Server Port Window setting on the NetBackup server or client (default is 1024-5000).
- ◆ The NetBackup-Java interface application and its application server always use port 13722 for its initial communication.
  - ◆ The highest available port in the Server Port Window range is always used internally by NetBackup Java on the server or client.
  - ◆ Subsequent communication (for example, a command to start Backup Policy Management) requires a unique port for each user. The NetBackup-Java application server selects the port from the range specified by the Server Port Window setting (default is 1024-5000). Selection can be random or can be the first port available, counting down from top of the range, depending on the Random Ports setting on the NetBackup server or client. Once a connection is established for a user, the same port is used for all further commands and responses for that user.

Therefore, three ports are the minimum required for one instance of a NetBackup-Java application (`jnbSA` or `jbpSA` command) to access a NetBackup server or client inside the firewall. For example, if Server Port Window is at the default and Random Ports is set to No, the three ports would be 13722, 5000, and 4999 (assuming 4999 is the first port available below 5000).

For more on the Server Port Window and Random Ports settings, see the NetBackup system administrator's guide. For information on NetBackup port usagem, see the *NetBackup Global Data Manager System Administrator's Guide* (this guide is available on the NetBackup 3.4.1 CD-ROM).

- 20.** Evaluation software expiration and the NetBackup-Java interface application.

Attempts to use the NetBackup-Java GUI application after an evaluation copy of NetBackup has expired result in the following error message being displayed in an error dialog and all the NetBackup-Java applications except Backup, Archive, and Restore disabled.

Administrator applications are not accessible due to the following error: Unable to get the attribute table

- 21.** The NetBackup-Java Windows Display Console is available to facilitate administration and user backup and restore operations on all supported UNIX platforms at locations where use of a Solaris or HP-UX NetBackup machine for displaying the GUI is not possible. This is done through the NetBackup-Java application server.

The display console requires no other NetBackup software to be running on the Windows machine you wish to install on and has been tested through PPP and dialup-modem type capabilities on Windows 95, thus easily facilitating truly remote administration from a home office for emergency situations.

22. For reasonable performance of the NetBackup-Java interfaces on UNIX (`jnbSA` and `jbpSA`), VERITAS recommends using a 256 MB machine that has 128 MB RAM available to the application.
23. Windows 2000 NetBackup host access from NetBackup-Java interface as nonadministrator must have write permission to the *install\_path*\NetBackup\Logs folder.

If users other than the administrator use the NetBackup-Java interface to log into a Windows 2000 NetBackup host, those users must have write permission to the *install\_path*\NetBackup\Logs folder. On Windows 2000 systems, the Program Files folder, by default, is not writable by users other than the administrator. NetBackup-Java writes various types of files (some temporary) to the Program Files\Veritas\NetBackup\Logs folder under the user's validations. Users without write permission to the Logs folder receive an error message when attempting the NetBackup-Java interface login to the Windows 2000 NetBackup host.

## Activity Monitor Application

1. The initial startup time of the Activity Monitor application in non-GDM mode is dependent on the number of jobs available for display on the server.

It is possible for Activity Monitor to hang without an indication that it ran out of memory to process all the job data. Increasing the value of the `-mx` argument on the `jre` command in the `jnbSA` script consistent with the amount of memory on the machine where `jnbSA` is executed may avoid this problem and will likely decrease the startup time of the application. Refer to the NetBackup-Java Performance Improvement Hints section of the *NetBackup System Administrator's Guide - UNIX* for more detail.

2. To allow remote job monitoring in the Activity Monitor, the NetBackup master server being monitored must include the monitoring host in the server list.
3. If using auto refresh in the Activity Monitor, the result of `kill` job operations may not become evident until a future refresh cycle in the application completes.

## Backup Policy Management Application

Sort operations are intentionally disabled for the Files list. Ordering is very important due to the file directives that NetBackup features use.



## NetBackup System Configuration Application

Multiple selections of the Impact Report button will result in multiple executions.

## Media and Device Management Application

It is recommended that you move only one volume or volume group at a time.

## Reports Application

The Media Contents report in the Reports application requires a specific media ID and does not work with value All.

## Backup, Archive, and Restore Application

1. On the Task Progress tab, the Status column of the Tasks Performed list may be empty or all jobs listed with status of In Progress. When option `DISALLOW_SERVER_FILE_WRITES` is set in the `bp.conf` file this status column is blank. You can check the status of the task by selecting it to display the progress log file in the bottom area of the Task Progress section.
2. Modify dates in the Restore section could be December 31, 1969 for some directories. When restoring files, you may see a fabricated modify date of December 31, 1969 for directories that were not fully backed up. These entries appear in the directory listing for ease of navigation to directories and files that have been backed up.
3. If you are searching for files and directories to restore that were backed up within a specific date, it is best to select a range of dates that includes only the files and directories you want to restore. If you select a large range of dates, all media used during that date range is displayed in the list, even if the selected files and directories were not backed up using all the media shown.
4. The NetBackup-Java Backup, Archive and Restore (jbpsA) application cannot be used to back up, archive or restore files directly on NetBackup Windows clients. Restoring of files to NetBackup Windows clients with the NetBackup-Java GUI can only be done by using the alternate client or server directed restore capabilities when logged into the NetBackup-Java application server running on a non-Windows NetBackup client.

## Storage Migrator File System Analyzer (FSA) Application

The FSA application requires administrative access to file systems you want to analyze. On both NetBackup-Java capable UNIX and Windows platforms, launching of the FSA is available from the NetBackup-Java interface **File** menu. It is available regardless of the user name specified on the NetBackup-Java login dialog. However, if you are nonroot (or Administrator on Windows), you must use the FSA's File menu Change Server option to log in to the relevant host as root (or Administrator). Running the FSA as nonroot (or nonAdministrator) can result in partial scans of the file systems.

## Installing NetBackup 3.4.1 for Oracle on Red Hat Linux 6.2

---

**Note** The 8.1.6.2 Oracle patchset is required. This patchset is scheduled to be released by Oracle in the near future. For the current status on this patch contact Oracle.

---

Refer to page 27 in the NetBackup 3.4 for Oracle on UNIX System Administrator's Guide and substitute the following for Step 3 of the installation instructions.

3. Set up automatic or manual linking.

- ◆ *To set up automatic linking:*

Run the `oracle_link` script located in:

*install\_path/netbackup/bin/*

This script determines the Oracle version level and then links Oracle to NetBackup accordingly. All output from this script is captured in a `/tmp/make_trace.pid` file. To change the trace file location, change the `MAKE_TRACE` variable in the `oracle_link` script.

- ◆ *To set up manual linking:*

First, make a copy of the existing Oracle executable:

```
cd ${ORACLE_HOME}/bin
cp oracle oracle.orig
```

Then, perform the following:

- a. Create a symbolic link from Oracle to the NetBackup API library:

```
cd ${ORACLE_HOME}/lib
ls -l libobk.so
```

If `libobk.so` exists:

```
mv libobk.so libobk.so.orig
ln -s /usr/opensv/netbackup/bin/libobk.so libobk.so
```

- b. Make a new Oracle executable:

```
cd ${ORACLE_HOME}/rdbms/lib
make -f ins_rdbms.mk ioracle LLIBOBK="${ORACLE_HOME}/lib/libobk.so"
```

---

**Note** The quotation marks must be included, as shown above, when executing the `make` command.

---



## Using the STK SN6000

Some SN6000 configurations may involve a different number of *logical* drives compared to the number of *physical* drives (or equivalent resources) available for satisfying requests for drives. Also, the relationship between the number of logical drives and physical drives may change if hardware failures occur.

NetBackup scheduling, drive allocation, and drive assignment algorithms can determine only *logical* drive availability, and will attempt to fully utilize all configured and available logical drives. If the number of logical drives being utilized exceeds the number of physical drives available, a NetBackup job may be started when insufficient drive resources are available to satisfy the job. The NetBackup job will encounter a resource issue when the scheduler initiates a job resulting in an ACS tape mount request. The mount request will then be re-queued within the ACS roboticdaemon process.

### Should SN6000 Drives Be Configured as Shared Drives?

The answer depends on how you connect hosts to SN6000 ports. Each SN6000 port presents a distinct set of logical drives. Drives accessed from different ports have different ACS drive addresses (ACS, LSM, Panel, and Drive numbers) for each drive, as well as different serial numbers.

#### Hosts Connected To a Single Port

If multiple hosts are connected to a single port, the logical drives accessible through that port are shared among the hosts connected to that port. The drive address and serial number is the same for each host on that port. In this type of configuration, the drives should be configured as *shared drives* in the NetBackup device configuration.

You must enter the Multihosted Drives license key on each media server where ACS drives in the SN6000 are configured.

#### Hosts Connected To Different Ports

If each host is connected to a different port, each host will have its own set of logical drives and the drives should *not be* configured as shared drives in the NetBackup device configuration.

With this type of configuration, the SN6000 hardware is providing drive sharing and the NetBackup scheduler and robotic drive selection components cannot avoid oversubscribing the drives. Tuning of the media mount timeout and backup class windows may be needed to avoid backup, restore, or duplication delays, and media mount timeouts.

You must enter the Multihosted Drives license key on each media server where ACS drives in the SN6000 are configured.



**NetBackup Tuning When Using Different Ports**

Since there is a fixed limit for the number of drives that can be in use at any one time in this type of configuration, you should configure backup windows so the different NetBackup storage units tied to the same physical drives are active only at non-overlapping times. Also, raise or set the media mount timeout to infinite to prevent job failures when the job cannot get a physical drive due to all the drives being busy.





# Problems Fixed Since NetBackup 3.4

---

4

This chapter describes general problems fixed since NetBackup 3.4 that are not documented in the *NetBackup 3.4 Release Notes*. Some problems may pertain to software that is only on the 3.4 CD-ROM.

## General NetBackup

On all NetBackup servers, host name comparison checks could occur if the hosts being compared had a different number of IP addresses. This caused problems such as not adding a device host because the host name comparison with an existing device host produced a false match. This applied to all NetBackup servers.

## PC Clients

For Windows NT Alpha/Intel, Windows 95/98 NetBackup clients, the following interface problems were fixed:

- ◆ Problems with the include/exclude list property pages in the configuration property sheet.
- ◆ Problem displaying sizes of files larger than 2 GB when navigating through the Network node in the backup window tree.

## UNIX Clients

For NetBackup Solaris clients, in the bpbbrm log on the NetBackup server when either bpbkar or tar was initiated, the following error message was encountered:

```
ld.so.1: fatal: relocation error: file
/opt/lotus/notes/latest/sunspa/libnotes.so: symbol verifyAtomics:
referenced symbol not found
```

## Alternative Backup

For Linux NetBackup servers:

- ◆ Different NDMP server platforms reported media errors in different ways.



NetBackup did not handle a NDMP\_NOTIFY\_PAUSED with a reason code of NDMP\_MOVER\_PAUSE\_MEDIA\_ERROR.

- ◆ If a configured NDMP host was not available when NetBackup started, the `tlcdc` and/or `tl8cd` process would crash.
- ◆ Corrected end case problems processing EOM (end-of-media) when writing to NDMP media.

In certain cases, such as writing the tar header/trailer during a NDMP backup, if EOM was encountered it would erroneously be interpreted as a media error.

## DataBase Agents

For Windows NT Alpha/Intel NetBackup clients, we removed NetBackup for SQL Server limitations on Database names containing special characters such as spaces, front and backslashes, and periods.

There still are known issues outside of the SQL Server extension related to usage of the front square bracket and the ampersand.

## Media Manager

1. The `avrd` process consumed much more CPU time than expected in some SAN media server configurations. Under heavy mount/dismount activity, if there were no locally attached drives configured on a media server, and if the media server was not serving as the scan host for any multihosted drives, the `avrd` process used excess CPU time.
2. Robotic inventory filters for TLH robots did not work on Windows NT/2000. Volumes in the desired IBM volume categories did not get returned on the inventory request when the volume category in the `vm.conf INVENTORY_FILTER` entry was provided in hexadecimal format.
3. TLH (Tape Library Half-inch) robotic drive addressing may change and thereby become incorrect if hardware errors or library reconfiguration occurs while TLH robotic control is active. TLH robotic drive addressing is based on a drive list returned from an IBM Library Device Driver interface. If this drive list changes without being accompanied by a change in the device configuration, mount requests may lead to media being mounted on the wrong drives, or drives may be configured DOWN.

The TLH robotic test utility, `tlhtest`, contains three new subcommands:

`drmapfreeze` - Freeze drive address mapping

`drmapshow` - Show drive address mapping

`drmapclear` - Clear drive address mapping

In order to take advantage of more a more resilient drive addressing method, the drive mapping must be frozen. Using `robtest` or `tlhtest` directly, execute the `drstat` subcommand and verify that the drives being returned in the drive list are consistent with the device configuration. If they are correct, run the `drmapfreeze` `tlhtest` subcommand. This will *freeze* the mapping between the robot drive number and the IBM device name and number. The current mapping can be displayed with the `drmapshow` subcommand. `tlhtest` and `tlhcd` (the TLH robotic control daemon) will then use the frozen drive map (a database) during a mount request to dynamically convert the robot drive number to the correct IBM device number.

Once a drive map has been frozen, it remains active until it is cleared with the `tlhtest drmapclear` subcommand, or refrozen with the `tlhtest drmapfreeze` subcommand. Use the `tlhtest drstat` command, as always, to obtain the robot drive numbers that are used in the device configuration.





# NetBackup 3.4.1 Known Problems and Limitations

5

The following list explains the known problems and limitations in NetBackup 3.4.1 and includes workarounds where known. Many of these items also apply to 3.4. However, for a complete listing of NetBackup 3.4 problems and limitations, see the *NetBackup 3.4 Release Notes*.

---

**Note** References to UNIX also apply to Linux, unless otherwise stated.

---

## Installation

1. When Microsoft Outlook is left running during Windows NT/2000 NetBackup installation, some programs generated by InstallShield are affected. The setup program for NetBackup Server for Windows NT/2000 initialization, for example, will proceed very slowly and can appear to be hung. The recommended solution from InstallShield is to close Outlook before running setup. See InstallShield Knowledge Base article Q102626 for further information about this problem.
2. The following errors can occur during Windows NetBackup server and client installation.
  - ◆ During NetBackup installation (server or client), a dialog box may appear with an "unspecified error" message from Windows Installer. If this message appears, click OK and proceed with the install, which should complete successfully. After completing the installation and configuration, perform a test backup to ensure that NetBackup is working correctly.
  - ◆ During NetBackup server installation, the Windows installer may fail and display an Internal error 2755,995. If this occurs, execute `instmsiw.exe` in the x86 directory on the CD-ROM. Ignore any errors it produces. Then, reboot the computer and re-run the installation.
3. During installation of the server on Windows NT/2000, there can be a long delay during "upgrading databases" without the progress bar being updated. Installation should complete successfully.



4. When installing Microsoft Windows clients (both local and remote installs) the client name is written in all lower case to the registry. If the classes on the server do not specify the client names in all lower case, backups fail because the names do not match.
5. A remote install of any Database Agent from the VERITAS NetBackup 3.4 Database Agents CD-ROM onto a Linux 3.4.1 server is not supported. The 3.4 Database Agents must be installed locally on each of the Linux server's clients.
6. For Microsoft Windows clients, if you perform a remote install to a computer in another domain, you may encounter errors stating that the system cannot find the file specified. If you encounter this problem, do the following:
  - a. Ensure both the source and target system are members of the same domain.
  - b. Retry the installation and when prompted, enter the user name, password, and domain of a user with administrative rights on the target system.

## General Notes

1. The Red Hat conversion script `/usr/sbin/inetdconvert` does not format the `xinet.d` files for `bpcd`, `bpjava-msvc`, and `vopied` correctly.

The conversion script `inetdconvert` provided by Red Hat adds a `server_args` line with the service name for the NetBackup services `bpcd`, `bpjava-msvc`, and `vopied`. To fix this, edit the files `bpcd`, `bpjava-msvc`, and `vopied` in `/etc/xinetd.d` and take out the service name as an argument. For example, the file for `bpjava-msvc` has a line:

```
server_args                = bpjava-msvc -transient
```

it should be:

```
server_args                = -transient
```

The `server_args` line in the files `bpcd`, and `vopied` can be removed since no arguments are passed to these services."

2. The Java GUI segfaults on Red Hat Linux 7 when it is started.

This is a known Red Hat Linux 7 bug. You must install at least the `glibc(RHBA-2000:079-04)` bug fix from Red Hat (<http://www.redhat.com>).
3. The NetBackup menu interface gets an error loading shared libraries on Red Hat 7.

You must install the `ncurses4` package from Red Hat (`ncurses.4-5.0-2`). If you do not you will see the following error when trying to start the NetBackup menu interface:

```
error while loading shared libraries: libncurses.so.4:
cannot open shared object file: No such file or directory
```



4. On linux, the NetBackup menu interface (bpadm) the output for reports is not correctly aligned.

We have seen this problem when logging into Red Hat Linux from another Unix OS (for example, Solaris, HP/UX, AIX) with the `TERM` variable set to `xterm`. If you set the `TERM` variable to `vt100` or `dtterm` the columns are correctly aligned. We have not seen this symptom if the system you are logging in from is another Linux system.

5. The UNIX NetBackup X user interface (xbp) for Red Hat Linux is linked dynamically. This means that in order to use xbp you must have Motif version 2.1 installed. OpenMotif is available at <http://www.opengroup.org/openmotif>.
6. On Windows NT/2000, if server and client are in different time zones you may see problems doing restores or listing images.

Backups are done and timestamped as the server sees them. There is no accommodation for client requests specifying a TZ or time offset.

7. Manually initiating a backup of the NetBackup catalog can fail if backups are in progress.

Backing up the NetBackup catalog can fail if it is manually initiated and backups are in progress. The workaround for this is to initiate these backups when no other NetBackup activity is occurring, or to schedule the backup of the catalog to occur automatically.

8. Jobs are not deleted from the jobs list immediately after a master server crash and reboot.

If the master server crashes and reboots, the Activity Monitor incorrectly assumes that jobs running at the time of the crash are still active and queued. It does delete them, however, when it starts the first backup after the reboot.

9. The Activity Monitor does not allow you to kill a queued restore. A restore is in the queued state from the time it is first received until NetBackup has figured out what files are needed from each of the images.

Other limitations with monitoring restores include:

- ◆ Some columns on the job monitor are empty for restore jobs.
- ◆ Unable to view detailed job monitor for restores.

10. Files Written count (Current, Previous) in Activity Monitor does not include extra directory entries used for restore file browsing.

When viewing the Files Written count for a job in the Activity Monitor, the value for Current Files Written does not include the extra directory entries (which are used during restore file browsing). The value displayed for Previous Files Written does include those extra directory entries, and are slightly larger.



**11. Daylight Savings Time causes minor problems for NetBackup.**

When Daylight Savings Time changes take effect, anomalies can occur in the scheduling of some client backups and the displaying of some report screens. This is due to the method NetBackup uses in calculating the beginning of a backup window and comparing it to (potentially) completed backups.

In the Spring, when Daylight Savings Time takes effect, you see misordered reports (for example, All Log Entries, Backup Status). This is due to the discrepancy between Greenwich Mean Time (which UNIX uses) and your system's "local time." After the time changes (for the day of the time change only), you see entries logged between midnight and 2 am displayed after entries logged between 3 am and midnight. You also must adjust the starting time of the display to 11 p.m. of the previous day to see all entries made for that day.

If a backup occurs within one hour of the backup window's opening and the backup window spans the time change, the backup may be re-executed (in the fall) or seen as already having occurred (in the spring). This is due to the fact that once a backup has completed it is given an absolute time, while the opening of the backup window is calculated in a relative fashion.

Until this algorithm is corrected, you should carefully check backups that are scheduled to occur when the time changes to assure that your data is adequately protected.

**12. Class and schedule names cannot include commas.**

Do not create class or schedule names that include the comma (,) character; for example: *full, many*.

Only the UNIX NetBackup `bpadm` utility permits this syntax.

**13. On UNIX, restores of NFS mounted files fail when attempting to perform a server directed restore. The progress log may show the following types of messages.**

```
Could not make directory /net/machine/abc: The file access
permissions do not allow specified action
```

```
Couldn't change access and modification time of
/net/machine/abc: Not owner
```

```
Couldn't change access and modification time of
/net/machine/abc: Operation not permitted
```

```
Could not create file /net/machine/abc/123: Permission denied
```

```
Could not create file /net/machine/abc/123: A file or directory
in the path name does not exist
```

To work around this situation, the owner must restore the NFS files on the client machine.

- 14.** The multiple data streams feature when used in autodiscover mode can cause a delay in the scheduling of jobs if many classes and clients use it. This problem occurs because the scheduler must contact the client to discover the current backup requirements. To reduce the impact of this behavior, there is a parameter called `preprocess interval` that you can set with the `bpconfig` utility. To start this utility on UNIX, execute `netbackup/bin/admincmd/bpconfig`. To start this utility on Windows NT/2000, execute `NetBackup\bin\admincmd\bpconfig`. On UNIX, you can also set it through `bpadm`. Using the `bpconfig` utility use the `-prep` option to set the number of hours for the `preprocess interval`. In `bpadm`, `preprocess interval` is found in the global parameters. This value of `preprocess interval` limits the number of times that the client is contacted by allowing autodiscover to occur only this often. The default value for this is four hours. If the time spent preprocessing is excessive due to a large number of clients, the period can be increased. If there are schedules with a frequency of less than four hours, the `preprocess interval` can be reduced. (if the `preprocess interval` is set to 0, the default of four hours is used).

- 15.** Compaq Alpha systems with the OSF/1 operating system can crash when backing up a symbolic link that has Extended File Attributes. The console may display the following type of message.

```
panic (cpu 1): ufs_getproplist: pl_descp->pl_magic
```

The crash is due to an operating system bug. The use of the `/bin/tar` command to archive the symbolic link also causes the system to crash. This problem has been seen on Digital Alpha machines running the OSF/1 version 3.2 214 operating system.

To work around this problem, add an entry for the symbolic link to the exclude list for the client or remove the symbolic link.

- 16.** On a Windows NT/2000 NetBackup master server, no automatic update of server lists is performed on clients when a media server is added. (This applies only to NetBackup DataCenter. NetBackup BusinessServer does not support media servers.)

The NetBackup clients' server lists are not automatically updated when a media server is added on the Windows NT/2000 NetBackup master server. The clients' server lists must be manually updated. On UNIX clients, a new `SERVER=media_server_name` entry should be added to the `bp.conf` file. Other clients must have the media server name added to the server list through the client user interface.

- 17.** There are no automatic update of the server lists on the master and media server when a remote media server is added. (This applies only to NetBackup DataCenter. BusinessServer does not support remote media servers.)

The server lists on the NetBackup master and media server are not updated when a media server is added on the Windows NT/2000 NetBackup master server. The server's server lists must be updated manually using the NetBackup Configuration interface. On UNIX media servers, a new `SERVER=media_server_name` entry should



be added to the `bp.conf` file. The Windows NT/2000 master server and any Windows NT/2000 media servers must have the new media server name added to the server list through the client user interface.

- 18.** Block-level Incrementals using VxFS (applies only to NetBackup DataCenter) requires the use of VERITAS File System version 3 and cannot be used to backup raw partitions.

- 19.** The limit to the amount of data that can be backed up in a single stream is one terabyte.

The last file backed up must start within one terabyte. For larger backups, use multiple data streams.

- 20.** On UNIX, `bprd` or `bpdbm` fails to obtain its required port.

If `bprd` is terminated using the `kill` command it may be unable to bind to its assigned port when next initiated. If the problem persists longer than ten minutes, you may need to reboot the server in order to clear the problem.

If `bpdbm` is terminated using the `kill` command rather than the `/usr/opensv/netbackup/bin/bpdbm -terminate` command, it may be unable to bind to its assigned port when next initiated. If the problem persists longer than ten minutes, you may need to reboot the server in order to clear the problem.

This problem may be identified by lines in the process activity log similar to the following:

```
<16> getsockbound: bind() failed, Address already in use (114)
<32> listen_loop: cannot get bound socket. errno = 114
<4> terminate: termination begun...error code = 146
```

Similar entries are found in the error logs.

- 21.** On DEC Alpha, there is a problem with arrow key usage in the UNIX interface program `bp`.

The program terminates with a core file when arrow keys are used on scrollable displays for `bp`. This problem occurs on DEC Alpha. If you want to scroll scrollable displays, use the letter keys.

- 22.** On Windows NT/2000 NetBackup servers, backups can fail with `media write error` if maximum transfer size is less than 64 Kbytes.

Backup with NetBackup can fail with `media write error` if the maximum transfer size of the tape device is less than 64K (65536) bytes. The maximum transfer size of a tape device is determined by the limits imposed by the tape device, the SCSI bus, the tape device driver, the SCSI bus driver, and the operating system.

NetBackup checks the maximum transfer size for a tape device before performing the actual tape writes. If the maximum transfer size is less than the block size NetBackup uses (typically 64 Kbytes), the backup fails with a `media write error` to prevent writing data to tape that it cannot recover. When the backup fails an entry similar to the following appears in the NetBackup Problems report.

```
io_open: The tape device at index X has a maximum block size
of 61440 bytes, a buffer size of 65536 cannot be used
```

This can be worked around by changing the block size NetBackup uses to the maximum block size for the device or less. The NetBackup block size can be changed by creating a text file named

```
install_dir\NetBackup\db\config\SIZE_DATA_BUFFERS
```

The contents of this file should be the text value of the block size in bytes. The block size **MUST** be a multiple of 1 Kbyte (1024) bytes. For the example error message above, the text we would put into the file would be 61440.

- 23.** On Windows NT/2000, client configuration conflicts are possible when using the NetBackup Configuration application.

If a user is updating the NetBackup client configuration through the Configuration dialog box in the client Browser at the same time the client configuration is being updated by the NetBackup Configuration application on the NetBackup server, only one set of updates are saved. This is the last set written.

- 24.** When starting the Windows NT/2000 NetBackup Reports application, it takes extra time if a media server is down (NetBackup Volume Manager service (vmd) is not running). The application is gathering the list of Volume Pools, and it times out for each unavailable Media Server.
- 25.** Large sparse files may not backup or restore properly if Windows 2000 cannot reserve memory in proportion to the file size (approximately 1MB per 1GB of file space). This means that backup/restore of these items is currently not possible. An appropriate error message is logged which will indicate that the system had insufficient resources to perform the operation.
- 26.** The HP-UX VxFS snapshot mechanism requires a dedicated cache partition for each snapshot. If two backups start simultaneously, both trying to mount the same cache partition, a number of conditions can occur if the following VxFS patches are not installed:
  - vxfs 3.3.2 patch 2
  - vxfs 3.3.3 patch 1



If FlashBackup detects that the intended cache partition is already mounted in `/etc/mnttab`, it fails with an error code 20. However, if the backups occur simultaneously, both attempting to mount the cache partition at the same time, both mount commands may work, causing invalid backups and a hung `umount` command.

The solution is to:

- a.** Change your configuration to use a dedicated cache partition for each backup. For multiple data streams, each stream must have its own dedicated cache partition.
  - b.** Install the VxFS patches as listed above.
- 27.** If you use the NetBackup BusinessServer Windows NT/2000 interface on to connect to a DataCenter server, you can add or change only storage unit types that are supported by NetBackup BusinessServer.
- 28.** There may be a delay in detecting of loss of connection from a NetBackup Windows NT master server to a media server

In certain situations, there can be a delay on a NetBackup Windows NT master server before it detects that the connection to a media server has been aborted. For example, if a media server goes down while running a backup, there may be a delay on the master server before it detects that the media server is no longer available.

While at first it may appear that there is a problem with the NetBackup Windows NT master server, this delay is actually a result of a certain TCP/IP configuration parameter on Microsoft Windows NT called `KeepAliveTime` that is set to 7,200,000 (two hours, in milliseconds) by default. More information about the `KeepAliveTime` and other associated TCP/IP configuration parameters on Microsoft Windows NT may be found in the following Microsoft Knowledge Base articles: Q140325 and Q120642.

The effect of this delay is that NetBackup jobs running on that media server appear to be active for a period of time after the connection to the media server has gone down. In some cases this can result in an undesirable delay before the current backup job fails and is subjected to the normal NetBackup retry logic for execution on a different media server, if one is available.

This delay is especially noticeable when the media server in question is a NetBackup failover media server running in a Microsoft Cluster Server (MSCS) environment. NetBackup relies upon the retry logic of the NetBackup master server to restart NetBackup jobs that were running on the NetBackup failover media server when a failover occurs.

It may be advantageous to modify the `KeepAliveTime` configuration parameter on the NetBackup NT master server for the reasons described above. However, this must be done using extreme caution because the parameter is a system wide parameter that affects all TCP/IP communications for that system.

Also, with the added support in 3.4.1 of a NetBackup failover master server running in an MSCS environment, it may for the same reasons be advantageous to modify this parameter on Windows NT/2000 media servers that use the failover master server.

29. If you configure NetBackup for NDMP on NetBackup BusinessServer, the robotic control must be on the master server, not the NDMP host.
30. On Windows NT/2000, the `bpdwn` command has a peculiar behavior when using the `-s` or `-r` options. If you do not have an IBM Automated Tape Library configured, you get a popup error dialog saying that the dynamic link library `libibm.dll` could not be found. This is harmless. Click the OK button and the `bpdwn` function will complete. The `bpdwn` function reports that one or more robot daemons could not be shut down, but that means only that the function to shut down the IBM Automated Tape Library failed because you do not have one configured.

If the popup dialog is annoying, you can stop this from happening by deleting (or renaming) the `tlhcd.exe` file from VERITAS *install\_dir*\volmgr\bin directory.

31. The `-tpath` option on the `bpbbackupdb` command does not work on Windows NT/2000 servers. There is no work-around, do not use the `-tpath` option.
32. On Windows NT/2000, adding clients to the client database through the Client Attributes tab on the Master Server Properties property sheet in the Configure NetBackup application will cause restores of selected files for those clients to fail with the message `ERROR: invalid request`. We recommend using the Configure NetBackup application to delete all clients entered in the client database. Additionally the Add button has been disabled to prevent adding clients to the client database until this problem is fixed.
33. Due to a problem in Windows ME Explorer, files created by copy operations in Explorer are not marked with the archive bit. Rather, the status of the archive bit for the destination is the same as in the source file. This means that using default NetBackup parameters for incremental backups, these newly created files will not be backed up. This problem does not occur in any other supported Windows(tm) operating system.

There are two ways to work around this:

- ◆ Use the `copy` command in a DOS window to perform copies.
- ◆ Clear the Perform incrementals based on archive bit checkbox on the Windows Client tab of the Client Properties dialog box (see the Configure NetBackup menu item in Netbackup Administration). This will also have side effects as timestamps from copied files retain the source file timestamp.



## Media Manager

1. On Windows NT NetBackup servers, the Windows NT SCSI configuration information may change after the system's SCSI configuration changes when adding, removing, or reconfiguring SCSI adapters or SCSI tape devices. Windows NT configures the SCSI devices when the system is rebooted. If the configuration was changed, the logical names of the devices can change. For example, if a system had one SCSI tape drive, Tape0, and another tape drive is added to the system, the system now has two tape devices, Tape0 and Tape1. There is no guarantee that the tape drive that was Tape0 before the new tape drive was attached is still Tape0. It may be Tape1 after the reboot.

See the device configuration wizard.

---

**Caution** Because of the dynamic configuration of the logical names for SCSI devices after a system reconfiguration and boot, the Media Manager device configuration may need to be updated when the SCSI configuration changes. For information on configuring devices, see the system administrator's guide for Media Manager.

---

2. On Windows NT/2000, hardware compression is not supported on the Colorado (HP) T4000 tape drive.
3. On UNIX, ejecting tapes through the inport of the ATL P3000 or Sun StorEdge L11000 robotic library can lead to the error `unable to sense robotic device` (applies only to NetBackup DataCenter).

The workaround is to wait until the robot has finished reinitializing (checking its media port for media) after the inport/export door has been closed, before responding in the GUI interface that the tapes have been removed. During testing, the library initialization period for an empty inport lasted for 2 minutes, 10 seconds.

4. On UNIX, when configuring robotic volumes with a media management New Volumes/Add Volumes interface, volumes are added to the Media Manager volume database, even if an error is reported because one or more volumes were not currently in their specified slots, or if the barcodes on added volumes could not be verified (for some robot types).

The workaround is to use robotic inventory for managing volumes. With robotic inventory, only the volumes actually contained in the robot are configured, and knowledge of slot information is not required.

5. In environments where network traffic or machine load is high, restarting the Media Management Device daemon (on UNIX) or Device Manager service (on Windows NT/2000) can result in individual robotic daemons not being active. This situation occurs when the daemon/service start occurs too soon after the shutdown, such that



the full shutdown of all daemons/services does not complete before the daemons/services are started. This in turn leads to a newly-started daemon/service being terminated by a delayed stop signal.

How do you know if this situation occurs? In the Volume Configuration wizard, at the robot inventory stage, the inventory fails with a message similar to `cannot connect to tldcd on host lettuce`. If you see this message, we recommend that you stop the Media Management Device daemon (on UNIX) or Device Manager service (on Windows NT/2000), wait at least 20 to 30 seconds, and then restart it.

Ideally, you should verify that all device processes have terminated before starting the Media Management Device daemon (UNIX) or Device Manager service (Windows NT/2000).

On UNIX, you can do this by executing the `vmops` command located in the `volmgr/bin/` directory and verifying that neither `ltid` nor any robotic daemons are running. On Windows NT/2000, you can do this by using the Activity Monitor to verify that neither `ltid` nor any robotic daemons are running.

---

**Note** The next two limitations apply only to NetBackup DataCenter because they are for features not available on NetBackup BusinessServer.

---

**6.** Some robotic daemons not supported on Windows NT/2000.

At this release, Windows NT/2000 NetBackup servers do not support ODL, TLM, and TSH robotic daemons.

**7.** Optical disk media support is limited for NetBackup on Windows NT/2000.

The Windows NT/2000 NetBackup server currently cannot:

- ◆ Add optical media
- ◆ Label optical media

In addition, moves do not recognize optical partners, so if both partners are selected the move may fail.

**8.** The following are known problems and limitations with RSM support on Windows NT/2000:

- ◆ NetBackup cannot immediately use media. RSM media must be manually moved from a robot's physical media list to the NetBackup media pool that corresponds with this device in NetBackup. This must be done BEFORE NetBackup can use the media (that is, inventory).

For example, when you configure the robot and its drives using the "Media and Device Management" GUI, a NetBackup media pool is created for that robot number with a pool for each supported media type for that drive type. The user



must use the "Computer Management" application, located in Administrative Tools, to drag and drop the media from the robot's media list to the newly created media pool which corresponds to their media type.

- ◆ At times RSM has problems writing Free Media Labels to a tape. This is because the On Media Identifier Label (OMID) does not match up with what RSM has recorded in its database. The user should eject such media(s), delete all references to it from RSM and then reinsert into the robot. At this point RSM considers it new media(s), updates its database and allows writing a Free Media Label on the media.
  - ◆ Occasional mount timeouts from RSM robots. If RSM has problems trying to mount assigned media, it probably is because (a) the media label is not unique within the library, (b) it is not in the correct NetBackup media pool, (c) RSM had problems writing a Free Media Label (as stated in the previous limitation above), therefore leaving media in an indeterminate state.
  - ◆ Physically DOWN drives may not be DOWN in the Device Monitor. The NetBackup Device Daemons do not scan RSM devices for physical status. Therefore, physical device status changes may have to be manually updated in Device Monitor.
9. The following are implementation strategies and considerations for RSM robots.
- ◆ The "Perform full inventory on mount failure property" on the General Properties tab of the RSM applet could be turned off as it slows down robotic operations.
  - ◆ NetBackup Media Manager NEVER deletes, frees or deallocates media in the RSM NTMS database. This must be done manually in the RSM applet by the user since it may result in the loss of data.
  - ◆ NetBackup Media Manager does not support cleaning functions for any RSM robots. These functions must be done using the RSM interface in the Computer Management application.
  - ◆ NetBackup Media Manager does not support RSM-enabled standalone drives. Standalone drives to be used with NetBackup must be disabled in RSM.
  - ◆ When media is removed from RSM and recreated, or moved among devices, it is a good practice to update the volume's unique identifier in NetBackup Media Manager by running the command:

```
vmquery -vuguid Media_Id
```

---

**Caution** If the network card in an RSM server is replaced, RSM creates all new unique identifiers for ALL RSM objects including robots, drives and volumes. This means that all of your devices must be reconfigured in NetBackup and all volumes must have their unique identifiers updated with the above command.

---

10. Drive Cleaning is not supported for SSO drives. This is due to a problems with tracking the hours of drive usage among hosts.
11. Robot inventory may add media with a media type that is not compatible with with the drive type (applies only to NetBackup DataCenter).

This limitation only applies to TLD or TL8 robots that have no drives configured on the robot control host or are using a multimedia robot (for example, DLT7000 and DLT8000 in the same library).

Example 1: If your TLD robot has DLT2 drives on a host that is not the robot control host and the robot control host has no configured drives in that robot then you must specify DLT2 as the media type on the inventory robot update.

Example 2: If you are using a multimedia robot, you must use barcode rules (see “Managing the Controls of the Robot” in the Media Manager System Administrator’s Guide).

If media are configured with the wrong media type, the media will be unmountable, possibly causing backups to fail.

12. When using NetBackup Media and Device Management on Windows NT/2000, a robot may be selected for robotic inventory when listed with the wrong robot control host, leading to a robotic inventory that fails because it tried connecting to a robotic control daemon/process on the wrong host.

## PC Clients

1. The following are IBM Directory and Security Server Environment Considerations.

NetBackup in general, and the NetBackup Client for OS/2 in particular are not Distributed Computing Environment (DCE) compliant applications. This means that they are not built to call the DCE services for authentication and naming.

Instead, NetBackup OS/2 relies on IBM’s backward compatibility of the IBM LAN Server APIs to perform authentication etc. IBM DSS for OS/2 modifies the behavior of many of the IBM LAN Server APIs, especially for user account information and access privilege. Consequently, NetBackup OS/2 in an IBM DSS environment may have difficulty accessing, reading, writing, and using Access Control Lists.

2. Alternate path restores for Novell NetWare clients must be done from the Novell server that is the NetBackup client.

This limitation exists because the user interface on a NetBackup server cannot resolve the namespaces on Novell servers.

3. Files with the following characteristics are not scanned for viruses:

- ◆ Fully qualified filenames longer than 255 characters
- ◆ Open files that are locked



- ◆ There is no support for cleaning a virus found in a compressed file, although it is reported as detected during a scan.
- 4. Email notifications of backup status is not sent to Windows NT client users.
- 5. Automatic client installation and update when the client is added to a class is not supported at this release on the Windows NT NetBackup server.
- 6. When changing the debug logging levels, some of the changes take effect right away while other require the `BPCD.NLM` to be unloaded and then reloaded. A change to the level debug value takes effect right away while a change to the tcp debug value does not take effect until the `BPCD.NLM` is unloaded and then reloaded.

This only pertains to NetWare file servers that are NetBackup clients.

- 7. When using `bpstart_notify` and `bpend_notify` scripts on Windows NT or Windows 95/98 clients, the script should not require user interaction to complete. The backup waits for the notify script to complete and eventually times out. The backup fails with a status code 24, `socket write failed`.
- 8. On Windows 95 clients, the default main toolbar in the NetBackup client interface may display improperly if the client has a `comctl32.dll` that is at a revision less than 4.7. To avoid this problem, select **View->Toolbar Options->Large Buttons** from the main menu to use the large toolbar buttons.
- 9. Alternate client restores using the AFS client type are not supported by the Backup, Archive, and Restore interface for the Windows NT/2000 client and server (this applies only to NetBackup DataCenter. NetBackup BusinessServer does not support AFS clients).

## UNIX Clients

- 1. On UNIX, alternate client restores can set the UIDs or GIDs incorrectly when the UIDs or GIDs are too long.

The tar header has a fixed amount of space for the UID and GID. If the UID or GID exceed the space provided when converted to octal characters, then overflows can result in the tar header containing the wrong value. During restores to the same client this is not a problem because the `uname` and `gname` are used to look up the UID and GID and NetBackup uses what is returned by `getpwnam()` and `getgrnam()`. However, for an alternate client restore, the two machines can have different `/etc/passwd` and `/etc/group` files. If these files are different, the `getpwnam()` or `getgrnam()` can fail and NetBackup will set the UID or GID to the decoded values. When the decoded values do not fit in the tar header, the excess leading octal digits are lost and the files are restored with an incorrect UID or GID. UIDs and GIDs between 0 and 16777215 are supported in this release without overflows. Previous releases were limited to values up to 262143.

A possible solution is to share `/etc/passwd` and `/etc/group` files between the machines you plan to cross restore on (or use NIS).

2. Archive backups from any NetBackup 3.3 Unix client to a 3.4.1 NetBackup Server on NT 4.0/Windows 2000 fails with the following error message:

```
(3) valid archive image procured, but no files deleted due to non-fatal
problems.
```

A valid backup image has been created so the files can safely be deleted manually. Updating the Unix client to NetBackup 3.4.1 will correct the problem.

3. On UNIX, when initiating a user interface (`bp` or `xbp`) on SCO OpenServer Release 5.0.5 it can fail with the following error:

```
Exit status = client cannot read the mount table
```

The NetBackup executable `bpbkar` can fail when attempting a backup on SCO OpenServer Release 5.0.5 with the following error:

```
FTL - Cannot statfs <filesystem name>
Errno = 2: No such file or directory
INF - EXIT STATUS 60: client cannot read the mount table
```

The reason for this problem is that on SCO OpenServer the `mt_filsys` field of the `mnttab` structure is defined as an array of 32 characters (see config file `/usr/include/mnttab.h`) including ending null. If a mounted filesystems path exceeds this size it is truncated and the `statfs` command fails.

Until this is fixed by SCO the workaround is to not mount filesystems with a path greater than 31 characters.

4. The UNIX user-interface application `xbp` cannot correctly perform OK requests on two or more instances of the `xbp_confirm` dialog, if those dialogs are displayed simultaneously.

The `xbp_confirm` dialog is used when requesting user-directed backups, archives, or restores. One `xbp_confirm` dialog can proceed with a click on its OK button, the other(s) cause `xbp` to wait indefinitely with the cursor shown as a wristwatch. The `xbp` process can be cleaned up with a `kill` command from a shell prompt. There is no limitation against sequentially displayed instances of the `xbp_confirm` dialog, i.e., once you OK or Cancel an `xbp_confirm` dialog, you can proceed to use `xbp` in other ways possibly including additional backup or archive or restore requests. The problem occurs only if you bring up additional `xbp_confirm` dialogs before using OK or Cancel to complete usage of the previous instance. In a future release, `xbp` will be modified to either allow multiple simultaneous `xbp_confirm` dialogs, or to prevent this usage with a specific warning message.



## DataBase Agents (extensions)

1. NetBackup supports only two node clusters for SQL Server and Microsoft Exchange.
2. Do not perform backup and restore operations with NetBackup for Microsoft SQL Server on `tempdb`. Microsoft SQL Server supports temporary database backups but does not support temporary database restores.
3. The NCR Teradata database agent does not handle object names that contain any of the following special characters: space, caret, period, backslash, and front slash.
4. It is not possible to recover Domino databases with transaction logging enabled on AIX 4.3.

When transaction logging is enabled on AIX 4.3, a problem has been encountered when attempting to recover Lotus databases. Because of this issue, the integrity of a Lotus database cannot be insured when recovering the database with transaction logging enabled. For this reason, it is recommended to disable transaction logging when running on AIX 4.3 until this issue has been resolved.

5. The About boxes for NetBackup for Microsoft SQL Server and NetBackup for NCR Teradata should specify that the copyright is 1993-2000 inclusive.
6. Observe the following special considerations before using NetBackup's Open Transaction Manager (OTM) to back up and restore databases. This information is an excerpt from VERITAS TechNote 233219. Also see VERITAS TechNote 233254.

The Open Transaction Manager (OTM) capability in NetBackup is designed to provide a Point-In-Time backup of data. With active files and directories, OTM has been an extremely useful option for NetBackup to backup active data. This TechNote summary is intended to clarify OTM usage with databases.

Many of the popular databases vendors provide a formal Application Program Interface (API) specifically designed for use with backup products. VERITAS software works closely with some of these database vendors to ensure that these interfaces are stable, efficient, and reliable when used in conjunction with NetBackup and its database extension features. Many of these APIs were jointly developed to ensure your data is protected and can be restored when needed. Oracle, Microsoft (SQL Server, Exchange), IBM (Lotus Notes, DB2), NCR (Teradata), Sybase and Informix are examples of database vendors that provide an API for use with backup products. VERITAS Software strongly recommends that NetBackup's database extension features be used when a backup API is available and backing up a database in a hot mode is required. Hot backups are done on active databases and only by using these formal APIs will the confidence of a backup and the ability to perform a successful restore be achieved. VERITAS recommends that OTM not be used for hot backups of these databases. Cold or inactive backups of these databases may be possible with OTM, but success will vary with each database vendor. Customers should contact the specific database vendor to identify the recommended method for database backup where data reliability is ensured as database programs recover from a Point-In-Time

restore differently. If the data being backed up and restored does not conform to the specification designed into the database product being used, the integrity of the database, as a whole can be in question.

There are several databases that do not have a backup/restore API. Some customers have explored using OTM to backup these databases. The safest method is to back up these databases when they are inactive (cold). In specific cases where VERITAS Software does not provide a database extension product for a specific database, VERITAS recommends shutting down the database and performing a file system level or cold backup.

If the databases cannot be backed up cold and the only option is hot, the OTM feature documentation identifies the criteria for creating a Point-In-Time snapshot is file system inactivity for five seconds. If the file system does not achieve a quiescent state, it will not execute the OTM snapshot. NetBackup will not fail the backup when a quiescent state is not achieved. It will continue the backup as if NetBackup OTM was not being used. The result is that NetBackup will skip open or active or locked files. The backup job will end with an exit status code 1. Exit Status code 1 indicates the backup job completed but not all files were successfully backed up.

If the decision is made to use the NetBackup OTM feature to back up database environments, VERITAS strongly recommends that you first back up the data and validate that the backup exited with a Status 0. Then the database should be restored and the integrity of the data and the functionality of the database confirmed. Using OTM to back up active database without using formal APIs has risk. Customers should contact the database supplier to ensure support of database backups using Point-In-Time technology. Also, significant back up and restore testing should be performed to assure database availability and reliability.

## NetBackup-Java Interfaces

### General Items Applicable to All Applications

1. All applications have been seen to hang when trying to display online help from within one of them. If this occurs, the only recourse is to terminate the application and restart it. See “Known Problems with Display of Online Help” later in this chapter for more information.
2. You can sort a table based on the data in a single column by clicking on the column header. The sort order alternates between ascending and descending order with each click. A known limitation in this release of NetBackup-Java is that the sort is based on a text comparison, and therefore sorts of columns with numeric values are not always sorted in correct numeric order. Columns that do sort correctly are: Job ID column of Activity Monitor, JBP numeric columns, Backup Policy Management main window: Jobs/Class and Priority columns, Backup Policy Management schedule window: Retention level and Media Multiplexing columns.



3. On rare occasions we have seen repaint problems. For example, you select a menu title, but the menu fails to paint unless you move another window in front of the NetBackup-Java window, then make the NetBackup-Java window visible again. Or you select a row in the table, but it fails to be highlighted until you force a repaint by either minimizing/maximizing the NetBackup-Java window, or covering/uncovering the NetBackup-Java window. Once it gets into this repaint predicament, nothing clears the problem except exiting the program. You must stop NetBackup-Java, then restart it.
4. Quite frequently, buttons, check boxes, and List widgets (list of items with scroll bar) fail to respond to the first mouse-release/click. The result is that the widget behaves as if a mouse-drag operation is occurring. The result with a button is that the button does not respond to the click, just changes in appearance. The result in a check box is that the selection state fails to toggle, instead the check box changes in appearance -- gets a more pronounced beveled border. The result in a List is that it doesn't respond to the selection. Instead, if you drag the mouse the list begins to scroll and the selection changes.
5. In some cases, you can close an application window from the window's menu even while child dialogs are visible.
6. If a non-modal dialog is visible and behind the parent frame and subsequently a modal dialog is made visible, Java moves the original non-modal dialog in front of the parent frame, but behind the newest dialog (a modal dialog requires a response and blocks input to all other dialogs for the application until the response is received). When the modal dialog is hidden, the non-modal dialog is moved back to its original position behind the parent frame.
7. If you enter text into a dialog's text field while either NetBackup-Java is busy performing other operations, or while your system is busy, the characters you enter may be transposed in order when displayed in the text field. For example, if you have started the Backup Policy Management Install Client Software operation and it is currently busy installing software, if you then try to perform other operations in Backup Policy Management which require entering text, the characters you enter into the text field may be displayed in the field out of order. You may also notice that response time is slow.
8. Hangs in NetBackup-Java have been encountered when looking up a host name. The hang is most likely to occur when you are asked to specify a host name. For example, assume you select the Append Host or Change Host feature of a NetBackup-Java application and specify a host name. When you select OK to commit the selection, the operation does not finish and the application no longer responds to user input. The problem is caused by the `java.net.InetAddress` class and occurs when a call to `InetAddress.getByName()` to look up a host name does not return. The problem may be related to Sun Java bug reports 4232651 and 4147517.



9. Some hang conditions that have been observed in the Java applications, are documented problems in Java (see “Java Problems Seen in NetBackup-Java”). To be certain it is not a “new” hang condition, please follow the instructions outlined in the “Gathering Information for NetBackup-Java” section of the *NetBackup Troubleshooting Guide - UNIX*.
10. The Storage Migrator File System Analyzer tool can not be launched from the NetBackup-Java GUI on HP-UX. Upon trying, there is no error message and no GUI application will appear. Your alternative is to execute the File System Analyzer startup script directly. The command is `/usr/opensv/java/FSA`.
11. The settings that are available through the NetBackup - Configure windows on Windows NT/2000 (for example, setting up OTM) are not available in the NetBackup-Java interface. You must use the NetBackup interface on the Windows NT/2000 server.
12. The NetBackup-Java interface includes functions not supported by NetBackup 3.4.1 on Linux. For example, all robot selections available on UNIX, also appear in NetBackup-Java on Linux.
13. The NetBackup-Java interface works best in 24-bit color. Using fewer colors can cause a flashing effect seen when the color pallet does not contain enough colors.
14. If you display NetBackup-Java on a Solaris Ultra that has a standard VGA card, the NetBackup-Java launch screen may have a gray rather than the normal tan background color and Java may report an error message about the "LightGray" color. You may also see reduced resolution graphics for large images on other screens. Closing other applications that use graphics, such as NetScape, can improve the appearance of NetBackup-Java.

Adding a 3-D graphics (24 bit TrueColor) card such as those listed below, to the workstation will eliminate these problems.

- ◆ Creator3D
- ◆ Elite3D m3
- ◆ Elite3D m6

## Backup Policy Management Application

1. Sort order in the table is not maintained after deleting one or more rows. After a delete operation the table reverts to its original, unsorted order.
2. Sort order in table is not maintained after changing tree nodes: If you click on a table header to sort the list, then select another tree node, the table reverts to displaying data in unsorted order.
3. Remote client software install limitations:



- ◆ It does not support software install for non-UNIX clients and a small subset of UNIX clients are also not supported. An attempt to install on a UNIX client for which remote install is not supported, results in an `Unknown hardware type: hardware type` message.
  - ◆ It is enabled only when a master server node is selected, and only if the master server is the server the user logged into when starting NetBackup-Java.
4. On rare occasions, we have seen hangs in the Backup Policy Configuration wizard during startup or when specifying a client to add to the client list. The sequence of events leading up to the hang are as follows:
- a. On the Client list wizard page, select the **Add or Change** button.
  - b. A dialog for adding or changing the client appears.
  - c. Enter a host name in the Client name: field.
  - d. Select the **Add or OK** button.

Under normal circumstances this sequence causes the host name to be added to the client list. Under rare circumstances, after selecting **Add or OK**, the operation does not finish and NetBackup-Java no longer responds to user input. This hang is caused by a problem in the Java virtual machine. Occasionally, calls to `java.net.InetAddress.getByName()` to look up a host name do not return and do not time out. The problem is more likely to occur if the host name does not exist on the network. All that can be done if this hang occurs is to kill NetBackup-Java and restart the application.

This hang has also been seen during startup of the Backup Policy Configuration wizard. The symptom in that case is that the wait cursor becomes visible after selecting the **Create a Backup Policy** button in the NetBackup Assistant, but the Backup Policy Configuration wizard never appears and NetBackup-Java no longer responds to user input.

## NetBackup Catalog Backup Application

No checking is done to determine if the format of the pathname is valid. Embedded spaces in pathnames cause problems and Windows NT style pathnames are not supported.

## NetBackup System Configuration Application

1. No checking is done to determine if the format of the email address is valid.
2. Blank text fields in the Global Attributes tab are allowed and treated as no change with the exception of the email address field.

## Activity Monitor Application

When using Global Data Manager across multiple DNS domains, attempts to use the Activity Monitor to delete or kill jobs from a server in a DNS domain different from that of the machine where you are running NetBackup-Java, can fail with status code 20 (invalid command parameter). This failure occurs because Activity Monitor uses the host's name as it is in the job's record and this is usually the host's unqualified name.

The workaround is to add unqualified names of servers that will be monitored to the `hosts` file of the server where you are running NetBackup-Java (`/etc/hosts` on UNIX and `%SystemRoot%\system32\drivers\etc\hosts` on Windows NT/2000). If there are servers in different domains but with the same unqualified name, you can have an entry for only one of them (for example, if there are two hosts named `shark`, you can have only one `shark` entry in the `hosts` file).

If DNS is not properly configured, an attempt to delete a job could result in NetBackup-Java becoming hung. In such cases, the above bypass will not be effective and the DNS configuration must be corrected in order for delete to function properly.

## Device Monitor Application

1. If the `bprd` daemon is down, the Global Data Manager permits connections to device hosts with configurations that disallow connections from the Master of Masters host.
2. If a device host does not have a valid configured device, then the Media Manager device daemon (`ltid`) starts and shuts down after a brief initialization phase. Therefore, attempts to start the daemon through the Start/Stop Media Manager Device Daemon dialog results in a report that the daemon was started successfully, but a short time later the application displays the error message that the daemon is inactive. The appropriate response is to configure a device and then start the Media Manager device daemon (`ltid`).

## Media and Device Management Application

1. When connecting to (or refreshing) a media manager, the cursor can remain in the hourglass state for several seconds after the "Loading data from ..." popup dialog has disappeared. If the media manager has a significant number of volumes or device hosts, the delay is due to data being added to unseen portions of the tree and table panes.
2. If the `bprd` daemon is down, the Global Data Manager permits connections to media managers with configurations that disallow connections from the Master of Masters host.
3. Unexpected results can occur when entering non-numeric values into numeric-only textfield controls. It is recommended that you use the arrow buttons to the right of the control to increment or decrement the numeric value. Numeric textfield controls appear on the following dialogs in Media and Device Management: Add New



Volume, Move Volumes, Change Volumes, Add New Robot, Change Robot, Add New Drive, Change Drive, ACS Drive ID, Add New Barcode Rule, and Change Barcode Rule.

4. Administration of optical devices and optical media is not supported in this release. While some of the pick lists contain optical entries (e.g., drive type, media type, and robot picklists), you could receive an error message when trying to use them. Use `vmadm` to add new optical volumes and `tpconfig` for adding new optical drives and robots.
5. When changing or viewing the attributes for a Windows NT controlled robot through the Change Robot dialog, the port, lun, target and bus fields show a value of zero if the robot's device host (the host on which the robot was defined) is running a NetBackup version earlier than 3.2. Use `tpconfig` to retrieve the correct SCSI values.
6. If a device host does not have a valid configured device, then the Media Manager device daemon (`ltid`) starts and shuts down after a brief initialization phase. Therefore, attempts to start the daemon through the Start/Stop Media Manager Device Daemon dialog will report that the daemon was started successfully, but a short time later the application displays an error message indicating that the daemon is inactive. The appropriate response is to configure a device and then start the Media Manager device daemon (`ltid`).
7. The media inject and eject functionality is incomplete. Only single volumes can be injected or ejected. Multiple tape eject/inject is not supported in this release of the NetBackup-Java Media and Device Management application.

## Reports Application

1. Trying to execute reports in more than one copy of the Reports application can cause a hang of all the NetBackup-Java applications that have been initiated from the same launch screen. This occurs most often when executing reports in the different instances of the application for the All Recognized Master Servers node on a Global Data Manager server (master of masters).
2. The View Media Contents report is not functional if you have the All Recognized Master Servers node selected when executing on a Global Data Manager server (master of masters).
3. After specifying non-default report criteria via the Reports Settings dialog, use the dialog's Run button to start the report instead of the Run button on the toolbar. The criteria associated with the toolbar button is not kept in sync with that in the dialog.
4. When running the Media Contents report, explicitly specify a host in the Server picklist field on the Report Settings dialog. If the Server parameter is set to All, then the report cannot find the specified media ID in the Media Manager volume database.

5. The Media Contents report requires the mount of media and is likely to take a long time for any data to be returned to the application. In this context the interrupt button on the load in progress dialog window is ineffective.

## Backup, Archive, and Restore Application

Depending on the task submitted, you may not see the type of task (Backup, Restore, Archive) listed in this column on the display in the Progress tab.

## NetBackup-Java Display Console Known Problems

Following are known problems in NetBackup-Java specific to running the applications on a Windows NT/2000, 98, or 95 system (that is, using the NetBackup - Java Display Console for Microsoft Windows).

1. Other installed instances of the Java Development Kit (JDK) or Java Runtime Environment (JRE) can interfere with the correct execution of NetBackup-Java. This is caused by a known Sun Java problem (4071807).

The Java Runtime Environment program normally should look in the directory where it is installed to find the `javai.dll` runtime library. NetBackup installs a version of JRE 1.1 in the `install_path\Java\jre` directory and expects the Java Runtime Environment program to load `javai.dll` from this same directory. However, if there is a JavaHome key from another JRE installation defined in the Windows registry, it will load `javai.dll` from the JavaHome bin directory instead.

The versions of JDK or JRE that cause conflicts are any of the Java 1.1 versions. For example, JDK or JRE 1.1.7B. If you have a 1.1.x version of the JDK or JRE on your system, either:

- ◆ Uninstall the conflicting versions of the JDK or JRE (recommended solution).
- or
- ◆ Use the Windows `regedit` program to delete or rename the JavaHome registry keys for the conflicting installations. The registry keys are located in:

HKEY\_LOCAL\_MACHINE

Software

JavaSoft

Java Development Kit

1.1 (JavaHome is in here)

Java Runtime Environment

1.1 (JavaHome is in here)



2. On Windows NT/2000, the background color is not consistent in all the dialog windows of NetBackup-Java. This is a known Sun Java problem (4102565) and is out of our control.
3. On the Windows platforms, you may see transparent backgrounds in some of the NetBackup-Java application dialog windows.
4. On the Windows platforms, on occasion we have seen failures right after initialization. When this occurs, a Dr. Watson window appears with a message indicating that `jrew.exe` had a divide-by-zero exception followed by a program address (various addresses have occurred). This is a timing problem and Java bug 4223311 corresponds to our analysis of the problem.
5. On Windows NT/2000, secondary dialog windows are sometimes placed off screen. This most often occurs if the main application window is positioned close to the top of the screen. In this case the dialog's title bar may be off screen and you cannot reposition the dialog window.

## Java Problems Seen in NetBackup-Java

1. Some UI anomalies seen in this version of the Java Runtime Environment:
  - ◆ Buttons don't always respond to the first mouse click. Instead they change in appearance to indicate "mouse-over" action. It may take several clicks to respond depending on system activity.
  - ◆ List components sometimes continue to scroll as if a mouse-drag operation is in progress, even though the mouse button has been released. Symptoms: after selecting an item in the list and releasing the mouse button, if you move the mouse below or above the list or to either side, the list scrolls in the direction the mouse is being moved, and the list selection changes.
  - ◆ Check boxes occasionally do not toggle their state properly when the mouse is clicked over the check box. Instead, the check box changes in appearance to indicate a mouse-drag operation. It may take several clicks to respond depending on system activity.
  - ◆ Menus sometimes stay permanently opened as a result of rapid and frequent mouse or window activity. The menu still remains visible even if the window is closed and re-opened. (Sun bug report 4178589)
2. Closing an application's main window via a window manager's title bar menu Close selection while the application has a dialog visible, makes a subsequent invocation of the application from the same launch screen unusable. This is a bug we have documented to Sun. We have worked around most cases in which this can occur.
3. We have seen a number of hangs caused by race conditions when opening/closing modal dialogs (a modal dialog requires a response and blocks input to all other dialogs for the application until the response is received). Refer to Sun bug reports

4122683 and 4161680 as examples. These hangs occur when one modal dialog is opened very soon after another has been closed. In NetBackup-Java the risk of encountering this problem is much higher when switching from one NetBackup-Java application to another, especially if the switch occurs at about the time a NetBackup-Java 'application' is asynchronously popping up a warning message, for example when it displays a "Loading data..." message. For this reason, we recommend you do not switch from one NetBackup-Java application to another when the first application has an open dialog.

4. When the wait cursor is set for a window, the window's text fields still have the normal text cursor (Sun bug report 4040417).
5. We have seen a number of paint and repaint problems that appear to be caused by the Java JFC Swing classes. These problems are more likely to occur when using an X emulator to run the Java application remotely. One often seen symptom is:
  - ◆ After a dialog is dismissed, a small portion of the window it was covering may be corrupted. If this happens, minimizing/maximizing the window forces a complete repaint of the window.
6. The application may "hang". See Sun bug reports 4089377 and 4041699. The first symptom that the application is "hung" is that when you change from window to window, the portion of a window that was previously covered by another window remains unpainted, and the application does not respond to user input.

The most frequently occurring "hang" we have seen is similar to Sun bug report 4089377. This problem can happen when rapidly selecting tree and list items, or performing operations that cause the display of multiple dialogs in quick succession.

Sun bug report 4041699 describes hangs caused by internal class synchronization that we have seen.

Sun bug reports 4089377, 4091873, and 4041759 describe hangs we have seen during Java class loading and "finalization". The typical symptom is that the logon screen does not appear, or that logon completes but NetBackup-Java stops responding shortly thereafter.

Note that there may be some short periods of time where the NetBackup applications appear to be "hung" momentarily while they are accessing the NetBackup-Java application server. But if a "hang" persists for a considerable period of time, suspect a true application hang or deadlock.

7. We have seen a number of SIGSEGV 11 segmentation violations followed by abort of the Java virtual machine (VM). These problems have been reported to Sun (no bug report numbers available). There are references to various SIGSEGV 11 segmentation violations at the Sun bug tracking web site. For an example, see Sun bug report 4097528. (Note that not all SIGSEGV problems stem from the same cause).

When these types of errors occur, the application fails. The following error message appears in the xterm window where you started the application.



Abort - core dumped

One particularly noteworthy scenario when NetBackup-Java will not initiate due to insufficient memory - failing with Abort - core dumped message.

To get more detail, follow the procedure for NetBackup Java as outlined in Chapter 1 of the *NetBackup Troubleshooting Guide - UNIX*.

8. We have seen a few bus errors followed by the abort of the Java VM (problem reported to Sun, no bug report number available):

When these types of errors occur, the application can fail. The following error message appears in the xterm window where you started the application.

Killed

To get more detail, follow the procedure for NetBackup-Java as outlined in Chapter 1 of the *NetBackup Troubleshooting Guide - UNIX*.

9. On occasion we have seen the CDE and Motif window managers hang while using the NetBackup-Java applications. If this occurs, the only recourse is to telnet into the system, execute the `/usr/opensv/netbackup/bpps` command and kill all jre processes listed.

## Known Problems with Display of Online Help

Following is a list of known problems in the HotJava HTML Component of Java that may adversely affect the display of online help. If this becomes too frequent, you could use a Web browser to view NetBackup-Java online help. You can view online help outside of the applications by opening the following locations in a Web browser for NetBackup-Java administrator applications and jbpSA, respectively.

For NetBackup BusinessServer

`file:/usr/opensv/java/vrts/nbu/help/en/MainHelp.html` - NetBackup-Java admin

`file:/usr/opensv/java/vrts/nbu/help/en/help.html` - jbpSA

For NetBackup DataCenter

`file:/usr/opensv/java/vrts/nbu/helpDC/en/MainHelp.html` - NetBackup-Java admin

`file:/usr/opensv/java/vrts/nbu/helpDC/en/help.html` - jbpSA

Alternatively, you can make a configuration change that forces the NetBackup-Java applications to use a Web browser for viewing online help. Refer to the documentation for the `browser_path` option in the following two files.

`/usr/opensv/java/JBPSimple.properties` - used by jbpSA only, i.e., jbpSA command

`/usr/opensv/java/Launch.properties` - used by the admin apps, i.e., jnbSA command



1. Sometimes the Java runtime environment hangs when a help file is displayed in the help browser. The only solution is to restart NetBackup-Java.
2. Forward and backward navigation using the toolbar buttons doesn't always work properly due to problems in the HotJava HTML Component. Incorrect navigation occurs when the displayed URL includes a fragment identifier after the # sign. For example, suppose you select hot links in the help Table of Contents to go to pages with URLs similar to the following:

```
deviceBody.fm2.html#10345
```

```
deviceBody.fm2.html#10356
```

```
deviceBody.fm2.html#10457
```

When you select the hot links, the help browser navigates first to the head of `deviceBody.fm2.html`, then to the labeled fragment, `#10345` for example. But when you try to navigate backwards using the back button, it goes to the head of the page (`deviceBody.fm2.html` in this example) but doesn't scroll to the labeled fragment.

In our experience, navigation works using the hot links, but navigation using the forward and backward buttons is problematic when the URL points to a fragment within the page.

3. The Home button doesn't always work. The help browser calls the HotJava HTML Component's `setDocumentURL()` method when the button is pressed, but sometimes the HTML component does not display the requested URL.
4. The help browser has a status bar at the bottom of the window. The only item displayed in the status bar as a page is selected is the URL. The help browser was designed to listen for change in status and error messages from the HotJava HTML Component, but neither of these properties is reported by the HTML component.
5. Placing the mouse pointer over a hot link does not result in displaying the link's URL as one might expect in a browser. The help browser listens for the HotJava HTML Component's `indicatedElement` property, which is supposed to change when the mouse is over a hyper-text link. Unfortunately the property change is fired erratically and the method for accessing the property almost always returns null.
6. The HTML document's title is displayed in the title bar of the help browser only the first time a help browser window is opened. This is because the `getDocumentTitle()` method of the HotJava HTML Component works only for the first instance of the HTML component. When the component is created multiple times for multiple help browser windows, calls to `getDocumentTitle()` from any instance of the HTML component other than the first instance return null.

## Errors When NetBackup Daemons Are Not Running

The following error messages can appear in an attention dialog, depending on whether:

- ◆ The server is configured as a Global Data Manager



- ◆ The specific daemons that are not running on the relevant machine(s)
- ◆ The application you start

**Messages:**

- ◆ Could not get retention level information: Unable to get retention levels definitions. error= 25 (cannot connect on socket)
- ◆ Unable to connect to host (name), it failed to respond
- ◆ The Media Manager device daemon (ltid) is not active on host (name)
- ◆ Cannot connect on socket
- ◆ Cannot connect to vmd (70)
- ◆ Connection requested by invalid server
- ◆ Error accessing server (name) - cannot connect on socket

If you acknowledge these initial messages and continue to use the application, a warning message dialog appears containing one of a variety of error messages. Also, these types of errors can appear if the daemons are stopped while the NetBackup-Java applications are running. Examples include:

- ◆ Error accessing server (name) - cannot connect on socket
- ◆ Unable to connect to host (name), it failed to respond
- ◆ The Media Manager device daemon (ltid) is not active on host (name)
- ◆ A command execution error occurred. The application will not be fully functional.
- ◆ An error occurred while reading configuration information. Select 'Refresh' to reload class data
- ◆ Unable to retrieve complete data
- ◆ Connection requested by invalid server
- ◆ Unable to load information about NetBackup storage units
- ◆ Unable to load information about NetBackup volume pools
- ◆ An error occurred while changing class, status:25 cannot connect on socket
- ◆ Could not get retention level information: Unable to get retention levels definition. error=25 (cannot connect on socket)
- ◆ Could not get Class\_att\_defs information: Unable to get the attributes table
- ◆ Warning - netbackup database backup is currently disabled
- ◆ Cannot connect on socket
- ◆ Unable to retrieve complete information for host(s)

- ◆ JSAT21: insert failed - cannot connect to vmd (70)
- ◆ Cannot retrieve data from Media Manager server: cannot connect to vmd (70)
- ◆ Cannot connect to vmd (70)

In many cases, with the Device Monitor and the Media and Device Management applications, the last part of the error message will be `cannot connect to vmd (70)`. For the other NetBackup-Java applications, a commonly occurring message is `cannot connect on socket`. Also, in some of the applications, data doesn't appear (for example, file and directory listings on the restore tab of jbpSA).

## Documentation Errata

In the following Media Manager guides:

- ◆ *NetBackup DataCenter Media Manager System Administrator's Guide - Windows NT/2000*
- ◆ *NetBackup BusinessServer Media Manager System Administrator's Guide - Windows NT/2000*

Step 4, of the Attaching New Devices section, in chapter 2 has the following note:

---

**Note** You can use the NetBackup tape driver installation utility to install tape drivers. This utility is available from the Windows Start programs menu (VERITAS NetBackup - NetBackup Tape Installer).

---

Ignore the above note. The NetBackup tape driver installation utility is not available on the Start menu. However, it is included on the NetBackup 3.4.1 CD-ROM. The file name is `NetBackupTapeDeviceDriverInstall_233895.exe`. Also see the operational note on the NetBackup Tape Device Driver Installer under "Media Manager" on page 21.





# Using NetBackup with Microsoft Cluster Server

---

A

Server clusters provide high availability of applications and data to users. In a server cluster, two or more servers (called *nodes*) are linked in a network, and run cluster software that allows each node access to the shared SCSI bus to which any number of disks can connect. If a node becomes unavailable, cluster resources migrate to an available node (this is called *failover*). The disks on the shared SCSI bus and the virtual server are kept available. During failover, users experience only a short interruption in service.

NetBackup protects data on the disks that attach to the shared SCSI bus, as well as data on the node's local disks. NetBackup can also protect Microsoft SQL Server and Exchange Server databases that are configured as virtual server applications; that is, they contain an IP address resource, a Network Name resource, and are displayed on the network with a unique server name (the virtual server name).

## How NetBackup Protects Data in a Cluster

There are several ways to use NetBackup for protecting the data in a Microsoft Cluster Server (MSCS) environment. One way is to back up the data across the network to a separate NetBackup server by installing a NetBackup client. This is the easiest method to set up and maintain since the NetBackup-specific configuration tasks for tape devices, media, and so on, are kept separate from the set up and maintenance of the cluster itself. For more information, see “Installing NetBackup Client on a Cluster” on page 87.

Another approach is to install a NetBackup media server. This allows you to back up the data to tape devices that attach directly to one or both of the MSCS nodes without going across the network.

A NetBackup media server can be installed on the cluster either as a single media server running as a MSCS virtual server application, or it can be installed as two separate media servers, each running on a node of the cluster independently of the other. Of course, installing separate media servers on each node of the cluster does not provide failover protection of the NetBackup media server itself, but there can be other advantages to this approach. For more information, see “Installing Separate NetBackup Media Servers on a Cluster” on page 85.

Installing a single NetBackup media server on the cluster as a virtual server application allows the media server to failover from one of the MSCS nodes to the other as described previously. This is called a NetBackup failover media server.



When you install a NetBackup failover media server, you assign NetBackup a network name resource (the virtual server name), an IP address resource, and a disk resource. Note that the network name and IP address must be unique and set up in your name resolution configuration prior to setting up a NetBackup failover server.

The virtual server name is used in the NetBackup storage unit and added to the server list of any NetBackup clients to be backed up to this media server. When a failover occurs, backup jobs that were running are rescheduled by using the normal NetBackup retry logic for a failed backup. The NetBackup services are restarted on the other node and backup processing resumes. For more information, see “Installing a NetBackup Failover Server on a Cluster” on page 78.

Yet another approach is to install a NetBackup master server on the cluster as a virtual server application. This is called a NetBackup failover master server and as the name implies, allows the duties of the master server to failover from one of the MSCS nodes to the other if a failure occurs on the active node. This provides high availability of the NetBackup master server itself.

As with a NetBackup failover media server, when you install a NetBackup failover master server, you assign it a network name resource (the virtual server name), an IP address resource, and a disk resource. Note that the network name and IP address must be unique and set up in your name resolution configuration prior to setting up a NetBackup failover server.

This virtual server name is used as the name of the master server for all media servers and clients using this master server. As above, when a failover occurs, backup jobs that were running are rescheduled using the normal NetBackup retry logic for a failed backup. The NetBackup services are restarted for the failover node and processing resumes. For more information, see “Installing a NetBackup Failover Server on a Cluster” on page 78.

Both types of NetBackup failover servers, master and media, operate in an active/passive failover configuration. The active node and the passive (or failover node) must be the same type of server, master or media. Mixing the two server types in the same failover server configuration is not supported. For example, a master server on one node cannot failover to a media server on the other node.

Specific details of how NetBackup runs in a cluster vary depending on the configuration you use in the cluster. For information about the supported configurations and their specific requirements, see the next topic, “Configurations for NetBackup and Clusters.”

## Configurations for NetBackup and Clusters

Several cluster configurations are supported by NetBackup; including the following:

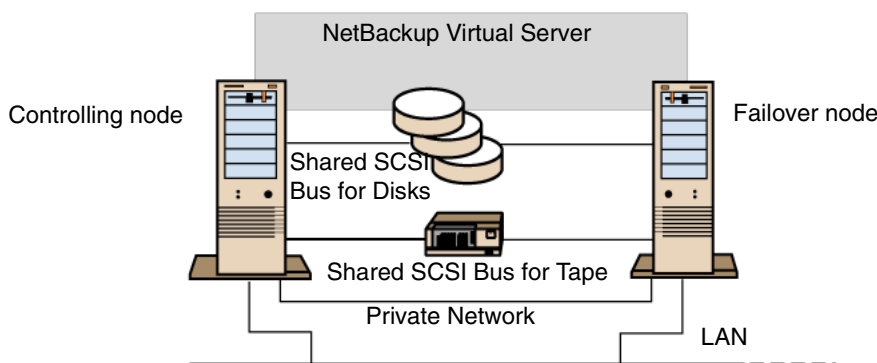
- ◆ “Cluster with Tape Devices on a Shared SCSI Bus”
- ◆ “Cluster with Locally-attached Storage Devices”
- ◆ “Clusters Sharing Devices on a Fibre Channel SAN”

Combinations of these configurations can also be used.

## Cluster with Tape Devices on a Shared SCSI Bus

In this configuration, a NetBackup failover server (master or media) is installed on the cluster. Only one of the NetBackup servers installed on each node of the cluster is active at any point in time. Each node in the cluster has access to the tape devices through a shared SCSI bus that is separate from any shared SCSI bus for disks. Access to the tape devices is controlled by the fact that only one node of the NetBackup failover server can be active at any point in time.

Figure 1. Example of a Cluster with NetBackup and tape devices on a shared SCSI bus



As explained later in this appendix, the devices are configured on each of the failover server nodes independently from the other node. This allows different SCSI bus numbers, and so on, on each of the nodes to refer to the same device. Remember, however, that any NetBackup storage units you create for the failover server must be configured with the actual number of devices. For example, do not make the erroneous assumption that the number of drives should be increased since there are multiple connections to the same tape device.

In certain situations, it is possible for a SCSI bus reset to be issued for the SCSI bus where the shared tape devices attach. Therefore, do not connect tape devices and shared disk drives to the same SCSI bus; connect each to separate SCSI buses.

## Configuring a Shared SCSI Bus for Tape Devices

Before configuring a shared SCSI bus for tape devices, read the following carefully.

To configure tape devices on a shared SCSI bus, you must have:

- ◆ SCSI cables.
- ◆ SCSI terminators.



- ◆ A SCSI adapter in each cluster server to provide a shared external bus between the nodes
- ◆ At least one tape device on the shared bus.

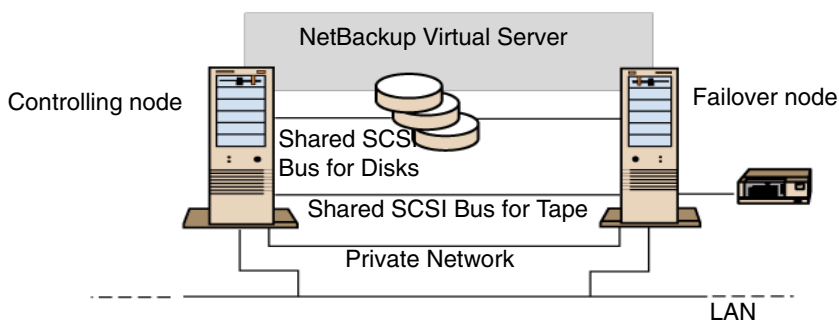
The tape devices must connect to a bus that uses the same method of transmission as the device (single-ended or differential). Only one transmission method can be used on a single SCSI bus.

Terminate the SCSI bus at both ends so commands and data can be transmitted to and from all devices on the bus. Each SCSI bus must have two terminators and they must be at each end of the segment.

If a tape device is in the middle of the bus as shown in Figure 1, remove any internal termination in that device.

If the tape device is at the end of the bus as shown in Figure 2 and the tape device has internal termination, you can use the device's internal termination to terminate the bus.

Figure 2. Example of a shared bus with tape devices at the end of the bus



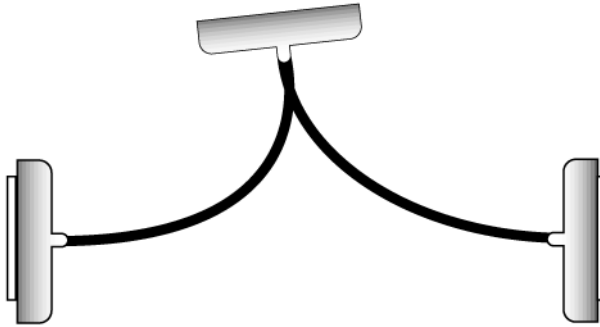
- ◆ SCSI adapters - this method is not recommended because if the server is disconnected from the shared bus, or if there is a power supply failure, the bus may not be properly terminated and be inoperable.
- ◆ Pass-through (or feed-through) SCSI terminators - these can be used with SCSI adapters and with some tape devices. If the tape device is at the end of the bus, you can attach a pass-through SCSI terminator to terminate the bus. The internal terminators in the tape device must be disabled. This is a recommended method.

**Tip** To ensure termination if a power supply failure occurs, turn off the on-board terminators on the SCSI controller (using the method that the host adapter manufacturer recommends) and physically terminate the controller with a terminator.



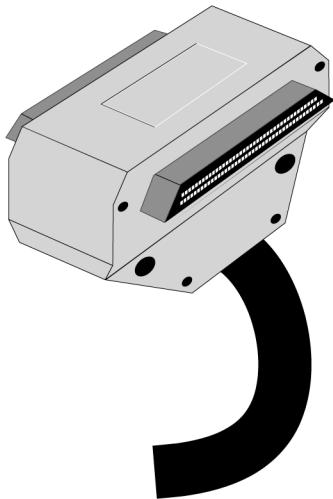
- ◆ Y cables - these can be used with some tape devices. If the tape device is at the end of the bus, you can attach a terminator to one branch of the Y cable to terminate the bus. The internal terminators in the tape device must be disabled. This is a recommended method.

Figure 3. Example of a Y cable



- ◆ Trilink connectors - these can be used with some tape devices. If the tape device is at the end of the bus, you can attach a terminator to one of the trilink connectors to terminate the bus. The internal terminators in the tape device must be disabled. This is a recommended method.

Figure 4. Example of a Trilink connector



Besides terminating the bus, Y-cables and trilink connectors also let you isolate the devices from the shared bus without affecting the bus termination. You can maintain or remove that device without affecting the other devices on the shared SCSI bus.

▼ **To configure a shared SCSI bus for tape devices:**

1. Install the SCSI controllers for the shared SCSI bus.

Ensure that the SCSI controllers for the shared SCSI bus are using different SCSI IDs. For example, on the controlling node, set the SCSI controller ID to 6 and on the failover node set the SCSI controller ID to 7.

2. Prepare the SCSI controllers for the shared SCSI bus. For details, see the documentation provided by your SCSI host adapter manufacturer.

---

**Note** Do not have power on both nodes while configuring the systems. Or, if both nodes have power on, do not connect the shared SCSI buses to both nodes.

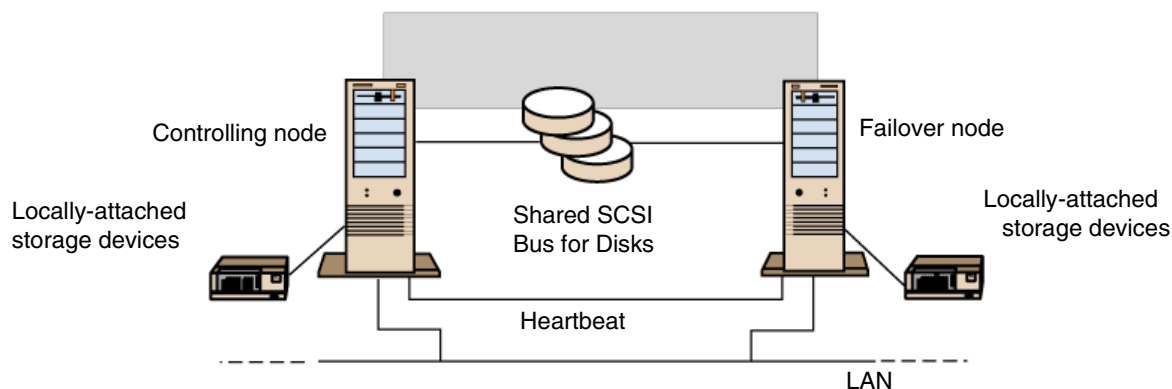
---

3. Connect the shared SCSI tape devices to the cable, connect the cable to both nodes, then terminate the bus segment using one of the methods discussed in the previous section.

## Cluster with Locally-attached Storage Devices

In this configuration, a separate NetBackup media server is installed on each node, storage devices are locally attached to each node, and no failover protection is available for the NetBackup media servers.

Figure 5. Cluster with NetBackup and Locally-attached Storage Devices

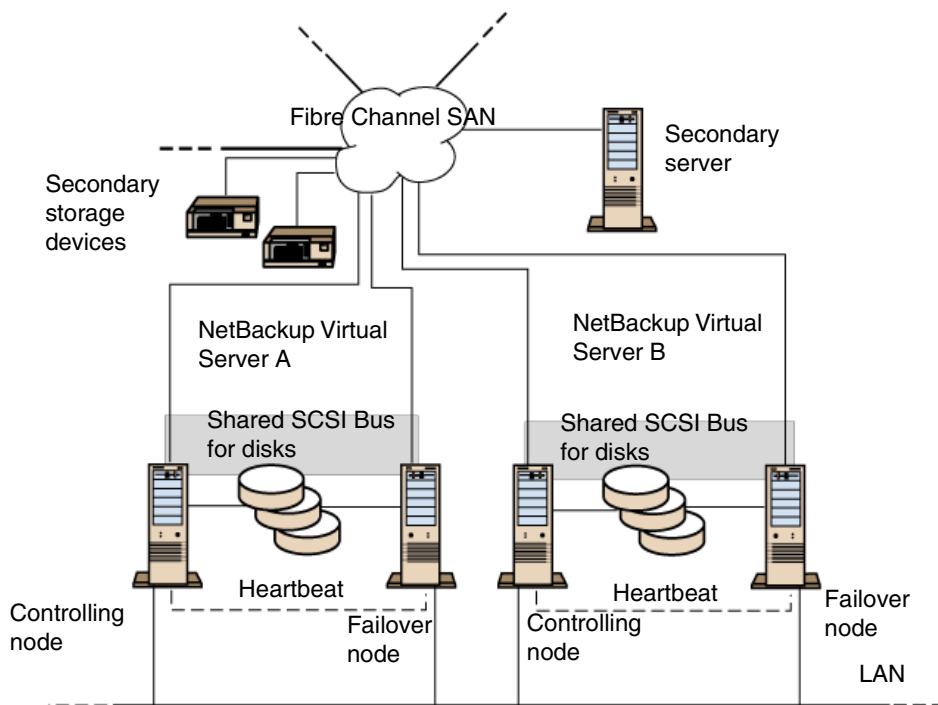


You may want to set the NetBackup alternate restore failover machine configuration parameter as described later to allow restores on either node if the other node is unavailable at the time of the restore request. Remember, however, that a locally attached device is available only when the node to which it attaches is online.

## Clusters Sharing Devices on a Fibre Channel SAN

In this configuration, one or more clusters attach to a fibre channel storage area network (SAN), with a NetBackup failover server (master or media) installed on the cluster. Tape devices are shared through the SAN and are set up for NetBackup use by using the multihomed drive wizard in the Media and Device Management utility or the Device Configuration wizard in the NetBackup Assistant.

Figure 6. Clusters on a Fibre Channel with NetBackup



This configuration offers the normal advantages of a SAN backup environment such as performing backups locally to tape devices through the fibre connections, instead of across the network to a separate NetBackup server.



## Installing a NetBackup Failover Server on a Cluster

---

**Note** Only Microsoft Cluster Server (MSCS) is supported in NetBackup 3.4.1. We do not currently support VCS (VERITAS Cluster Server). NetBackup Failover Server supports only *one* active node in a two or more node cluster. Database agents are not supported in a NetBackup Failover Server cluster configuration greater than two nodes.

---

The Microsoft Cluster Administrator must be installed on all NetBackup servers (including NetBackup Administration Clients) that you will use to remotely administer the NetBackup failover server (master or media). You must also have administrator rights to the server cluster.

For more information about protecting local and shared data on the cluster, see “Backing Up Clusters” on page 87.

---

**Note** These instructions assume that this is a new installation of a NetBackup failover server. If you have an existing NetBackup master or media server to convert to a failover server, there are additional steps that are outside the scope of this document. Essentially, the process is similar to setting up a new NetBackup server to replace the old one and migrating relevant data to the new server. Because of the complexity of this process, we recommend that you contact NetBackup consulting for assistance in the conversion.

---

### ▼ To install a NetBackup failover server on a cluster:

1. Use the normal 3.4.1 NetBackup server installation to install a NetBackup master or media server on each of the nodes in the cluster.

Choose a destination directory for the installation that resides on a local disk when installing on each node of the cluster. Do not choose a disk that is shared (that is, a disk that fails over from one node to the other). Also, as stated earlier in this appendix, each node must have the same type of NetBackup server installed on it. Mixing a NetBackup master server with a NetBackup media server in a cluster failover configuration is not allowed.

Use the server node name as the name of server during the install (the NetBackup MSCS Setup wizard described later will change the name of the server). If installing a NetBackup failover media server, ensure that both the media server nodes reference the same NetBackup master server name during the install.

Do not start the NetBackup services or configure any devices, storage units, and so on, at this time. Also, do not run the Getting Started wizard at this time.

**Note** When using the NetBackup MSCS Setup wizard to install the NetBackup failover server (master or media) in the following steps, each node in the cluster must be online. Otherwise, the wizard fails.

---

2. From either node, run the NetBackup MSCS Setup wizard by executing the `NBCluster.exe` program located in the *install\_path*\NetBackup\bin directory. This wizard guides you step-by-step through the rest of the installation.
  3. In the NetBackup MSCS Setup wizard, enter the name of the Microsoft Cluster Server where the NetBackup failover server (master or media) is to be set up and click **Next**.
- 

**Note** NetBackup also supports three or four node MSCS cluster configurations. If you have more than two nodes in your MSCS cluster, the wizard shows an extra screen at this point that asks you to identify the nodes to be used for the NetBackup failover server.

---

4. Enter the name of the MSCS group to create for the NetBackup failover server. The default name is *NetBackup Group* for a NetBackup failover media server and *NetBackup Master Server Group* for a NetBackup failover master server. From the drop-down list, select the shared disk that you want NetBackup to use for the portion of its data that must be shared between the MSCS nodes. Enter the path to a directory on that shared disk and click **Next**. Note this path as you will use it to update the NetBackup Catalog Backup file list below.
- 

**Note** The NetBackup MSCS Setup wizard moves the shared disk resource specified in this step to the new NetBackup MSCS group, along with any other MSCS resources that have the shared disk resource listed as a dependency. If this shared disk resource is currently used for other MSCS groups in the cluster (that is, already listed as a dependency for other resources in MSCS), you should take additional manual steps after running the wizard to ensure that everything is configured correctly. For simplicity, you can dedicate a shared disk for exclusive use by the NetBackup MSCS group.

---

5. Enter the following information, and then click **Next**.



Table 3. Failover Server Network Information

Field	Description
MSCS virtual server name	Type the virtual server name of the NetBackup failover server. <i>Remember that the NetBackup failover server requires its own unique name.</i>  For a NetBackup failover media server, this is the server name used in the NetBackup storage unit and added to the server list of any NetBackup clients that are backed up to this NetBackup failover media server.  For a NetBackup failover master server, this is the server name used anywhere that the name of the NetBackup master server is normally used (for example, when browsing for restores in the user interface or in the Change Server dialog box of the administration interface).
IP Address	Type the IP address of the NetBackup failover server. <i>Remember that the name and IP address of the NetBackup failover server must be unique.</i>
Subnet Mask	The Subnet Mask field displays the default subnet mask. If necessary, edit the subnet mask.
MSCS network	Select the MSCS network to use for the NetBackup failover server from the dropdown list.

- Review the attributes for the NetBackup failover server on the NetBackup MSCS Setup Summary screen. Note that clicking **Next** applies the changes you made to NetBackup and MSCS in order to set up the NetBackup failover server. If you cancel and exit the wizard at this point, no changes will have been committed.

---

**Note** If you run the NetBackup administration interfaces locally on a node of the NetBackup failover server, you must run them on the active node of the NetBackup failover server. If you run them on the inactive (or failover) node, you may see connection errors when connecting to the failover server.

If you attempt to execute one of the NetBackup administration interfaces on a node of the cluster and you get the connection failure described above, try running the interfaces on the other node. If the failure still occurs, another problem is present, such as the NetBackup services resources being offline.

---

- After the NetBackup MSCS Setup wizard is complete, if you have devices to configure for this server go to the next step. Otherwise, skip to step 15.
- You now must configure the devices that connect to each node of the NetBackup failover server. The following are guidelines for avoiding problems as you configure the devices for this server:

- ◆ If there are devices attached to one node but not to the other node, they are available only when the node where they attach is online. For a NetBackup failover server, it is usually best to attach all of the devices to each node, using shared SCSI connections as necessary to share the devices.
  - ◆ Ensure that the robot numbers you define for robots used by the failover server are consistent on all servers that use that robot. If the robot number defined for the robot on one node does not match the number defined on the other node for the same robot, problems will occur when failing over from one node to the other.
  - ◆ Ensure that the volume database host you define for robots in the cluster is consistent on all servers that use the robots. Otherwise problems will occur during failover.
  - ◆ To keep the configuration as straightforward as possible, use the NetBackup master server as the volume database host for robots in the cluster and as the standalone volume database host for standalone tape devices in the cluster.
  - ◆ For tape devices that are in a robotic library, ensure the robot drive number field is set correctly according to the drive numbering scheme implemented by the manufacturer of the robotic library. Note that the first drive in the robot is always considered robot drive number 1 for NetBackup; if the manufacturer's drive numbering scheme starts with a different number such as 0, adjust it accordingly.
  - ◆ To avoid confusion, always point to the same Media Manager host when configuring devices or adding volumes for the NetBackup failover server. It is usually best to use the NetBackup master server as the Media Manager host in this environment.
  - ◆ Use the virtual server name of the NetBackup failover server in the **Device host** field when adding devices or including a new device host in the Media and Device Management utility.
9. To accommodate disparate SCSI connections on each node of the cluster, configure the devices for each node separately. Do this by first configuring the devices on one node and then moving the NetBackup MSCS group to the other node and configuring the devices for that node.
10. To configure the devices that connect to any one of the nodes in the cluster, first run the Microsoft Cluster Administrator and note which node currently has control of the NetBackup MSCS group, then determine which devices attach to that node.

You can also use the Device Configuration wizard to configure the devices and storage units for the failover server. Run the wizard once, then use the **Move Group** command mentioned below to move control of the NetBackup MSCS group to the other node and run the wizard again. Each time, be sure to use the virtual server name as the device host to be scanned for automatic discovery of devices.



11. Start the Media and Device Management utility and add the virtual server name of the NetBackup failover server as a new device host. Configure the devices that attach to the node that currently has control of the NetBackup MSCS group as noted in the previous step. Remember the guidelines given earlier for configuring devices in a failover server configuration.
12. Using the Move Group command in the Microsoft Cluster Administrator, move control of the NetBackup MSCS group to the other node in the cluster.
13. Refresh the view in the Media and Device Management utility. Note that devices for the NetBackup failover server are no longer displayed. The Media and Device Management utility shows the devices that are configured for the node that controls the NetBackup MSCS group. By using the Move Group command in the Microsoft Cluster Administrator to move control of the NetBackup MSCS group from one node to the other, you can examine the device configuration for each node.
14. After determining which devices attach to the node that has control of the NetBackup MSCS group, configure those devices by using the Media and Device Management utility. Again, remember the guidelines given earlier for configuring devices in a failover server configuration.

---

**Note** The same basic procedure will be used in the future to add new devices to the cluster. First, configure them on one node, then move the NetBackup group to the other node and configure the devices for that node.

---

15. At this time, you might have to create NetBackup storage units for backups. If you used the Device Configuration wizard to configure the devices (if any) in the cluster, the wizard created the storage units. If you did not use the wizard or if you want to create disk storage units (for example, for testing purposes), use the Storage Unit Management utility to create the storage units. Always use the virtual server name of the NetBackup failover server in the host field when creating storage units that reside on the cluster.
16. Verify the entries in the NetBackup Catalog Backup file list for the failover servers. For each of the cluster nodes, the list must contain the following three entries:

*nodename:install\_path*\NetBackup\db

*nodename:install\_path*\Volmgr\database

*nodename:install\_path*\NetBackup\var

Where *nodename* is the physical node name of that node and *install\_path* is the path to the installation on the local disk drive of that node for NetBackup.

For the NetBackup failover server, the list must also contain the following two entries:

*virtual\_server\_name:shared\_disk\_path*\NetBackup\db

*virtual\_server\_name:shared\_disk\_path*\Volmgr\database



Where *virtual\_server\_name* is the virtual server name of the NetBackup failover server and *shared\_disk\_path* is the path to the NetBackup files on the shared disk from step 4.

17. You are now ready to continue configuring backup policies and so on for NetBackup in order to protect data in the cluster or for other clients in your network.

Remember to use the virtual server name of the NetBackup failover server whenever the name of that Netbackup server is required. For example:

- ◆ In the server list on a client
- ◆ The server to use to when browsing for restores
- ◆ The name of the server for any storage units defined on that virtual server

## Uninstalling a NetBackup Failover Server from a Cluster

### ▼ To Uninstall a NetBackup Failover Server from a cluster:

1. On the controlling node, click Start, point to Settings, and then click Control Panel.
2. Double-click Add/Remove Programs. Then, in the list of currently installed programs, select VERITAS NetBackup and click Change/Remove.

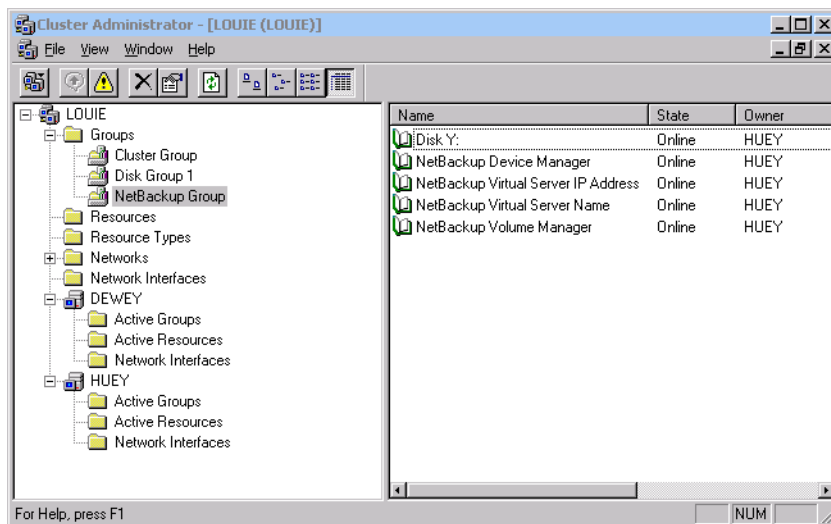
For additional information on Add/Remove Programs, see your Microsoft documentation.

3. Click Yes when prompted to uninstall NetBackup.
4. Move the NetBackup resource group to another node of the NetBackup failover server, if has not already been automatically moved by MSCS. To view a list of the nodes, examine the Possible owners: field of the properties of one of the resouces in the NetBackup group.
5. To completely uninstall NetBackup from the cluster, repeat step 1 through step 4 for each node of the NetBackup failover server and then continue to the next step.
6. After NetBackup has been uninstalled from each node of the NetBackup failover server, delete the NetBackup directory on the shared resource disk and all its contents. Then move any resource disks from the NetBackup MSCS group to another group and delete the NetBackup MSCS group.

In the following example, you would move Disk Y to Disk Group 1, and then delete the NetBackup Group, highlighted under Groups in LOUIE.



Figure 7. Example of NetBackup MSCS group



## Operational Notes for NetBackup Failover Servers

- ◆ You must perform certain configuration operations separately for each node in the failover server. One notable item in this category is the NetBackup server list, which must be set up correctly on each node of the NetBackup failover server. Another is the device configuration on each node.

We recommend that any configuration change be verified for each node in the cluster by using the MSCS Move Group command to check each node for the correct setting. Note that backup policies, storage units, and the NetBackup catalog backup configuration do not need to be configured separately for each node.

- ◆ The Standalone Volume Database Host setting must be changed to the appropriate NetBackup server setting (usually the NetBackup master server). The NetBackup Cluster wizard does not change this setting, so you must verify the setting is correct if you are using one or more standalone tape drives.
- ◆ If there are no tape devices configured on the controlling node of the NetBackup failover server, the NetBackup Device Manager service resource takes itself offline since it is not needed. If you do not intend to configure tape devices for the NetBackup failover server, you may want to delete the NetBackup Device Manager service resource from the NetBackup group. This avoids always viewing the group as being in a warning or failed state, since the Device Manager resource will always be offline and is not needed when no tape devices are configured.

- ◆ For three or four node MSCS clusters, the MSCS Move Group command lists all of the nodes in the cluster, not just the ones used for the NetBackup failover server. Attempting to move the NetBackup failover server group to an invalid node will fail. You must pick a node that is valid for the NetBackup failover server to use.
- ◆ When a failover occurs for a NetBackup failover server (master or media), any backups or restores that are currently using that server will fail and show up as failed jobs in the Activity Monitor or NetBackup reports. Regularly scheduled backup jobs are retried according to the normal retry logic, assuming that the schedule window and so on permit the retry of the job. After the failover occurs, the user must restart restores, user directed backups, and manual backups.
- ◆ After a failover occurs on a NetBackup failover server (master or media), it can take a while for the tape devices and media servers to be reset to a point where they can be used again by NetBackup. For example, a tape may have to be rewound before being available. Until the device is again ready for use by NetBackup, you may see errors such as 213 (no storage units available for use) or 219 (the required storage unit is unavailable).
- ◆ If you have one of the NetBackup administration interfaces currently connected to a NetBackup failover server, it may be necessary to refresh or restart the interface after a failover occurs. This is due to the interface maintaining its own cache of data that needs to be refreshed.

## Installing Separate NetBackup Media Servers on a Cluster

Instead of installing a NetBackup failover media server on a cluster, you can install a separate NetBackup media server on each node of the cluster. There is no cluster failover protection of the NetBackup media server when it is installed as two separate media servers. This configuration is set up in nearly the same way as two standalone media servers. However, there are additional items to consider when installing on a cluster:

For more information about protecting local and shared data on the cluster, see “Backing Up Clusters” on page 87.

- ◆ To avoid possible confusion and connection errors, set the **Required network interface** parameter for each media server to the node name of the cluster node where the NetBackup media server is installed (as opposed to a NetBackup failover media server, for which the NetBackup MSCS Setup wizard sets it to the NetBackup virtual server name). Also, see “Required network interface” in the *NetBackup DataCenter System Administrator’s Guide*.
- ◆ Use the cluster node name as the server name of the NetBackup media server in storage units, client server lists, NetBackup reports, and so on.
- ◆ Ensure that both media server names are in the server lists of the NetBackup master server and the NetBackup clients that can be backed up by these media servers.



- ◆ Create separate storage units for each node on which you have installed a NetBackup media server.
- ◆ Add entries in the NetBackup Catalog Backup file list for each media server. Create two entries for each media server by using the node name as the server name and the *install\_path\NetBackup\db* and *install\_path\Volmgr\database* paths to protect the catalog information on the media server.
- ◆ Consider using the NetBackup property **Alternate restore failover machines** to set up each of the media servers as a failover restore server for the other (note that this setting is available only for NetBackup DataCenter). Use the cluster node names as the server names. By using **Alternate restore failover machines**, you can help ensure that backup images written by one node of the cluster can be restored by the other node if the node that wrote the backup image is unavailable when a restore is initiated. It is especially useful if the tape devices used by each node are in the same robotic tape library.
- ◆ Any devices that connect to one of the NetBackup media server nodes in the cluster are not accessible if that node is not running. If one of the media server nodes is the robotic control host of a robotic tape library where tape devices used by both nodes are located, no tapes can be loaded or unloaded for those tape devices when the robotic control host node of the cluster is unavailable.
- ◆ It is not possible to share a robotic tape library connection between the cluster nodes in this configuration.
- ◆ If there are tape devices that must be shared between the cluster nodes, use an alternate method such as the multihosted drive wizard in the Media and Device Management utility to share the devices between the nodes. If you must share the tape devices between the cluster nodes, consider using a NetBackup failover media server.

## Uninstalling Separate NetBackup Media Servers from a Cluster

When using separate NetBackup media servers in a cluster, deinstallation consists of uninstalling NetBackup software from each node. No additional steps are necessary.

### ▼ To Uninstall separate NetBackup media servers from a cluster:

1. On each node, click Start, point to Settings, and then click Control Panel.
2. Double-click Add/Remove Programs, and then in the list of currently installed programs, select VERITAS NetBackup and click Change/Remove.

For additional information on Add/Remove Programs, see your Microsoft documentation.

3. Click Yes when prompted to uninstall NetBackup.

## Installing NetBackup Client on a Cluster

If you are backing up the data across the network to a separate NetBackup server, you can install the NetBackup client on the cluster. In this case, you must install the NetBackup client on each node of the cluster. You set up this configuration in nearly the same way as two standalone clients. However, if you have problems with name resolution when trying to back up data on the cluster (either local data or shared data), consider setting the **Required network interface** parameter for each client to the node name of the cluster node where the NetBackup client is installed.

For more information about protecting local and shared data on the cluster, see “Backing Up Clusters” on page 87.

## Uninstalling a NetBackup Client from a Cluster

When using NetBackup clients in a cluster, deinstallation consists of uninstalling NetBackup software from each node. No additional steps are necessary.

### ▼ To Uninstall a NetBackup client from a cluster:

1. On each node, click **Start**, point to **Settings**, and then click **Control Panel**.
2. Double-click **Add/Remove Programs**, and then in the list of currently installed programs, select **VERITAS NetBackup** and click **Change/Remove**.

For additional information on **Add/Remove Programs**, refer to your Microsoft documentation.

3. Click **Yes** when prompted to uninstall NetBackup.

## Backing Up Clusters

Back up the following to protect all data in the cluster, including file systems, databases, and the cluster quorum (Windows 2000 only):

- ◆ Local disks and System State on each node. The cluster quorum, which contains recovery information for the cluster and information about changes to the cluster configuration, is included in the System State backup (Windows 2000 only). See “Backing Up Local Disks in a Cluster” on page 88.
- ◆ All disks that attach to the shared SCSI bus. See “Backing Up Disks on the Shared SCSI Bus” on page 88.
- ◆ Virtual servers, which may contain data or contain applications such as Microsoft SQL Server or Exchange Server. Use NetBackup database agents to back up databases. See “Backing Up Database Files in a Cluster” on page 89.



- ◆ User backups that are run on either node of the cluster generally run as a backup of the node, not the NetBackup virtual server. Because of this, it is usually easier and less confusing to use scheduled backups rather than user backups to protect the data in the cluster.

## Backing Up Local Disks in a Cluster

To protect the data on the node's local disks, configure a NetBackup backup policy (also known as a NetBackup class) that includes the cluster node names in the client list for the class. The following are guidelines for configuring the class:

- ◆ If NetBackup is installed on the cluster as a NetBackup failover media server, select as the class storage unit, the storage unit created for the failover media server.
- ◆ If NetBackup is installed on the cluster as separate NetBackup media servers, configure two classes, each having one of the cluster node names listed as a client. For each class, select the storage unit created for the NetBackup media server that is installed on that cluster node.
- ◆ Use the specific drive letters (C : \, D : \, and so on) of the local disks as the file list for the class. If you use ALL\_LOCAL\_DRIVES as the file list for the class, the shared disks are included in the backup of the cluster node that currently has control of the shared disks, and this is probably not the desired result.
- ◆ For Windows 2000 clusters, always include `System_State:\` in the file list to back up the System State, including the cluster quorum information, for each cluster node.

## Backing Up Disks on the Shared SCSI Bus

To protect the data on the disks that attach to the shared SCSI bus, configure a NetBackup backup policy (also known as a NetBackup class) that includes the virtual server name of the cluster in the client list for the class. The following are guidelines for configuring the class:

- ◆ If NetBackup is installed on the cluster as a NetBackup failover media server, select as the class storage unit, the storage unit created for the failover media server.
- ◆ If NetBackup is installed on the cluster as separate NetBackup media servers, you can select either a storage unit that was created for one of the media servers as the class storage unit or select **Any Available** as the storage unit.
- ◆ If a storage unit that does not have local, direct access to the shared disk drives is used for the backup, the data is backed up across the network. This occurs even if the storage unit selected for the backup refers to a NetBackup media server running on a node of the cluster that does not currently have control of the shared disk drives.

- ◆ Use the specific drive letters (J: \, K: \, and so on) of the shared disks as the file list for the class. If you use `ALL_LOCAL_DRIVES` as the file list for the class, the local disks of the cluster node that currently has control of the shared disks are included in the backup, and this is probably not the desired result.
- ◆ For Windows 2000 clusters, the System State information is included in the backup of the node's local disks, so it is not necessary to include `System_State: \` in the file list for this class.

---

**Note** At the time the backup is initiated, if the cluster resource that defines the virtual server name of the cluster is controlled by one node of the cluster, while the cluster resource that defines the shared disks is controlled by another node of the cluster, the backup will fail. To prevent this condition, ensure that the virtual server name and the shared disks are configured using the Microsoft Cluster Administrator to failover together so that the same node always controls them.

---

## Backing Up Database Files in a Cluster

Applications such as Microsoft SQL Server or Exchange Server are installed on a cluster as virtual servers. To protect the data for these virtual servers, install the appropriate NetBackup database extension on each node of the cluster (this assumes you have installed the NetBackup client or media server as explained previously). Then, see the NetBackup documentation for the specific database extension in order to create a NetBackup class and schedule for that database extension.

When configuring a class to protect the data for the application/database in the cluster, always use the virtual server name of the application/database as the client name for the NetBackup class.

## Restoring Data to Clusters

For all file restore operations, use the procedures on performing restores in the *NetBackup User's Guide – Microsoft Windows*.

When restoring files to the shared disk drives, restore those files to the virtual server name.

When restoring individual database files, such as Microsoft SQL Server or Exchange Server, restore those files to the virtual server name of a specific installation of the SQL or Exchange database.

---

**Note** Because of the multiple virtual names that refer to the same computer in a cluster environment, it is possible for files to be backed up in the context of more than one client name. Careful planning of backup policies and schedules should avoid this



problem. However, still remember that when restoring to a cluster, it may be necessary to browse more than one client name and run more than one restore to restore all of the files that you need.

---

If you are using the Backup, Archive, and Restore interface on a NetBackup client that is installed on a cluster, additional configuration steps may be necessary to restore files that were backed up using the MSCS virtual server name. Since the Backup, Archive, and Restore interface on the client operates in the context of that client's name, you must perform an alternate-client restore to restore the files on the shared disk that were backed up using the virtual server name. NetBackup allows this alternate-client restore operation only if the necessary configuration is performed on the NetBackup master server. This configuration consists of creating the `install_path\NetBackup\db\altnames` directory on the master server and adding files as explained in "Managing Client Restores" in the *NetBackup DataCenter System Administrator's Guide*.

For example, assume the cluster virtual server name is TOE and the cluster node names are TIC and TAC. Files on the shared disk must be backed up by a NetBackup class that includes TOE in the client list. Using a server-directed restore is easy, both the source client and the destination client are set to TOE and the files on the shared disk are restored. The server-directed restore does not have to know which node is in control of the shared disk at the time of the restore.

To restore from the client, determine which node (TIC or TAC) has control of the shared disk. Then, start the Backup, Archive, and Restore interface on that node and select the virtual server name (TOE) as the source client on the Specify NetBackup Machines screen. Then, browse the backed-up files by using the MSCS virtual server name (TOE) from the shared disk and restore them as needed.

To allow this operation to occur, create the necessary entries in the `altnames` directory on the master server as described previously. In this example, files named TIC and TAC (one for each node) are created in the `install_path\NetBackup\db\altnames` directory on the master server. Each file contains the virtual server name TOE on one line in the file. For more details, see "Managing Client Restores" in the *NetBackup DataCenter System Administrator's Guide*.

There may be other situations that require the appropriate `altnames` directory entries to be created on the master server. If while attempting to restore files from the client, the operation fails with the error 131 `client is not validated to use this server` message, you must set up the `altnames` directory to allow the operation to succeed. One example is when the required interface parameter is set to a valid network name for the client but it does not match the NetBackup client name parameter for that client. Note that this may often be true for NetBackup clients in a cluster. Of course, as stated above, using a server-directed restore is always an option and avoids the need to set up the `altnames` directory.



## Restoring the Cluster Quorum for Windows 2000 Systems

The cluster quorum is backed up as part of System State for each node.

To restore the cluster quorum, other nodes in the cluster must be offline. If you cannot take the other nodes in the cluster offline before restoring the cluster quorum, you can create the following registry entry to force the restore of the cluster quorum even if the other nodes are still online:

```
HKEY_LOCAL_MACHINE\Software\VERITAS\NetBackup\CurrentVersion\Config\
Cluster_Database_Force_Restore
```

(note that the actual entry must be on a single line)

If required, create this registry value as data type REG\_SZ with a value of YES. When this value is set, the cluster service is stopped for any nodes that are online.

Restoring the quorum to a node that is running Active Directory or to a node that is currently a domain controller, requires additional steps not listed here. If Active Directory is running on the target server or the target server is currently a domain controller, see “Restoring Cluster Quorum to Windows 2000 Node With Directory Services” on page 92.

### ▼ To restore the cluster quorum:

1. From the NetBackup Backup, Archive, and Restore interface, select the backup image (or range of images) that contains the backup of the System State for this node of the cluster. Then, select the node of the tree labeled *System\_State* as the directory to be restored. For details, see the section on performing restores in the *NetBackup User's Guide – Microsoft Windows*.
2. If the disk where cluster quorum previously resided has been changed, you may have to set the registry entry described above to force the restore to continue. The disk could have been replaced with a new one, or the disk configuration could have been changed so that the cluster quorum now resides on a different disk. This allows the drive letter of the disk that the cluster quorum was on to remain the same, even if the configuration has changed and the disk signatures contained in the restore media do not match the disk signatures contained in the cluster quorum.
3. Continue the restore operation as explained in the section on performing restores in the *NetBackup User's Guide – Microsoft Windows*.
4. When the restore operation is complete, either reboot the cluster node or use the Microsoft Cluster Administrator to restart the cluster service on any nodes where it was stopped, whichever is appropriate.



## Restoring Cluster Quorum to Windows 2000 Node With Directory Services

To restore the quorum to a node that is running Active Directory or to a node that is currently a domain controller, the node must be in Directory Services Restore Mode. The cluster services cannot run in this mode, so the cluster quorum must be restored separately, after System State is restored and the node has been rebooted.

▼ **To restore the cluster quorum to a node running Active Directory or that is currently a domain controller:**

1. From the NetBackup Backup, Archive, and Restore interface, select the backup image (or range of images) that contains the backup of the System State for this node of the cluster. Then, select the node of the tree labeled *System\_State* as the directory to be restored. For details, see the section on performing restores in the *NetBackup User's Guide – Microsoft Windows*.
2. Exclude the cluster quorum from being restored with System State at this time by expanding the *System\_State* node and deselecting the *Cluster\_Database* node of the tree that is found under the *System\_State* node.
3. Continue the restore operation by following the steps on performing restores in the *NetBackup User's Guide – Microsoft Windows*.
4. When the restore operation is complete, reboot the cluster node in safe (repair) mode (restart the computer and press F8 when prompted to select an operating system) and then select Directory Services Restore Mode.
5. Start the NetBackup service(s).
6. Using the NetBackup Backup, Archive, and Restore interface as described earlier, select only the *Cluster\_Database* node under the *System\_State* node to be restored. For details, see the section on performing restores in the *NetBackup User's Guide – Microsoft Windows*.
7. If the disk where the cluster quorum previously resided has been changed, you may have to set the registry entry described above to force the restore to continue. The disk could have been replaced with a new one, or the disk configuration could have been changed so that the cluster quorum now resides on a different disk. This allows the drive letter of the disk that the cluster quorum was on to remain the same, even if the configuration has changed and the disk signatures contained in the restore media do not match the disk signatures contained in the cluster quorum.
8. Continue the restore operation by following the steps in the section on performing restores in the *NetBackup User's Guide – Microsoft Windows*.
9. When the restore has completed, reboot the target node.
10. When the restore operation is complete, use the Microsoft Cluster Administrator to restart the cluster service on any nodes on which it was stopped.

## Preparing for Disaster Recovery of A Cluster

If a disaster occurs, the following information is required to successfully recover the cluster:

### General Cluster Information

- ◆ Cluster name
- ◆ Cluster IP address and subnet mask
- ◆ Cluster node names
- ◆ Node IP addresses
- ◆ Local and shared drive letters and partition scheme

### Cluster Groups

- ◆ Group name
- ◆ Preferred nodes
- ◆ Failover/failback policies

### Cluster Resources

- ◆ Resource name
- ◆ Resource type
- ◆ Group membership
- ◆ Possible owners
- ◆ Resource dependencies
- ◆ Restart and Looks Alive/Is Alive properties
- ◆ Resource-related parameters
- ◆ Application-specific configuration (that is, SQL Database Character Set)

## Disaster Recovery of A Cluster

Several scenarios are discussed in this section:

- ◆ To recover the entire cluster, see the next topic “Recovering the Entire Cluster.”
- ◆ To recover all shared disks, see “Recovering All Shared Disks” on page 94.
- ◆ To recover the shared disk that the NetBackup application resides on, see “Recovering NetBackup on a Shared Disk” on page 95.



## Recovering the Entire Cluster

▼ To recover the nodes to their pre-disaster state:

1. On the first node you want to recover, reinstall Windows NT 4 or Windows 2000, including the last service pack applied before the failure.

---

**Caution** After booting the nodes in a cluster, ensure that the drive letters match the original cluster configuration. If the original configuration does not match, you can use the Disk Administrator to control to some extent, the hard drive numbering scheme that Windows NT/2000 devices.

---

2. On the second node you want to recover, reinstall Windows NT 4 or Windows 2000, including the last service pack applied before the failure. Also, see the previous caution.
3. Reinstall the cluster services and bring the cluster online.
4. Reinstall the same NetBackup for Windows NT/2000 software on the cluster that was installed before the failure. For details, see the earlier sections of this appendix that describe installing a NetBackup client or media server on a cluster, whichever applies.
5. If a NetBackup failover server was installed on the cluster or separate NetBackup media servers were installed on the nodes of the cluster as described earlier in this appendix, use the NetBackup `bprecover` command to restore the NetBackup catalog information before continuing. See the *NetBackup Troubleshooting Guide - Windows NT Server* for more information on recovering the NetBackup catalog database.
6. Restore the data files through the virtual server.
7. If you must restore a database to the shared drives, see the NetBackup guide for your database extension (*NetBackup for Microsoft Exchange Server System Administrator's Guide*, for example) to continue the restore.

## Recovering All Shared Disks

▼ To recover all shared disks:

1. Uninstall the cluster software from both nodes.
2. Replace and repartition the shared disks.
3. Reinstall the cluster software.
4. Reinstall the same NetBackup for Windows NT/2000 software on the cluster that was installed before the failure. For details, see the earlier sections of this appendix that describe installing a NetBackup client or media server on a cluster, whichever applies.

5. If a NetBackup failover server was installed on the cluster as described earlier in this appendix, use the NetBackup `bprecover` command to restore the NetBackup catalog information on the shared disk before continuing. See the *NetBackup Troubleshooting Guide - Windows NT Server* for more information on recovering the NetBackup catalog database.
6. Use NetBackup to restore any data on the shared disks. For details, see section on performing restores in the *NetBackup User's Guide – Microsoft Windows*.

## Recovering NetBackup on a Shared Disk

If a NetBackup failover server was installed on the cluster as described earlier in this appendix and you must recover the shared disk that was used for the NetBackup failover server, use the NetBackup `bprecover` command to restore the NetBackup catalog information on the shared disk. See the *NetBackup Troubleshooting Guide - Windows NT Server* for more information on recovering the NetBackup catalog database.

## Using NetBackup for SQL Server with Microsoft Cluster Server

---

**Note** This information is for a *two* node configuration. NetBackup supports only two node clusters for SQL Server and Microsoft Exchange.

---

This section describes how to use NetBackup for Microsoft SQL Server to back up and restore a virtual SQL Server 7 and SQL Server 2000 installation that has been configured with Microsoft Cluster Server. The procedures described are applicable if SQL Server exists in its own cluster or if it shares a cluster with a virtual NetBackup Media Server. If SQL Server shares a cluster with a virtual NetBackup media or master server, then SQL Server and the NetBackup server may be placed in the same group; but they must have different IP and network names.

You can use NetBackup for SQL Server to back up both active-passive and active-active SQL Server installations.

---

**Note** The SQL Server active-active configuration is not supported for NetBackup 3.4. You must upgrade to 3.4.1 to use an SQL Server active-active configuration.

---

In the following sections, example names are used. For example, let VIRTUALSERVER be the name of the virtual SQL Server instance in an active-passive configuration. Also, let NODEA and NODEB be the names of the physical nodes in the cluster. Let NODE0 be the name of the master server.



For an active-active configuration, there would be two or more SQL Server instances, say, VIRTUALSERVER1 and VIRTUALSERVER2. To configure for active-active, use the following instructions first to configure VIRTUALSERVER1 and then to configure VIRTUALSERVER2. Continue with the same procedure for any additional virtual SQL Server instances.

## NetBackup Server Configuration Parameters

Perform the following configuration steps after the virtual installation of SQL Server (VIRTUALSERVER) has been created and (if applicable) the virtual installation of NetBackup media server has been created, as well. The following actions must be performed on the master server (or on an administrative client acting for the master server).

1. Using the NetBackup Configuration Interface, create a MS-SQL-Server class (for example, VIRTSQLCLASS), to specify the storage attributes of the backup. Set up the following attributes:
  - a. Class-storage unit: Specify a storage unit belonging to the storage group intended for backup. If you are using a virtual media server, then specify a storage unit belonging to the virtual media server.
  - b. Create a backup policy schedule for VIRTSQLCLASS.
  - c. Add the virtual SQL Server name (VIRTUALSERVER) to the client list.
2. To incorporate SQL Server backup scheduling, create an automatic schedule in the VIRTSQLCLASS. Create the automatic schedule as follows:
  - a. Add an automatic backup schedule to VIRTSQLCLASS.
  - b. Add one or more script names (batch files) to the file list.
3. Create a standard backup class (say, STDCLASS). Add both physical nodes (NODEA and NODEB) to the client list of STDCLASS.
4. Establish the permissions settings as follows for alternate client restore: On the master server, either:
  - ◆ Create a file called *install\_path*\NetBackup\db\altnames\No.Restrictions
  - or
  - ◆ Create each of the files, *install\_path*\NetBackup\db\altnames\NODEA, *install\_path*\NetBackup\db\altnames\NODEB.

---

**Note** Creating the No.Restrictions file allows all clients to perform alternate client restores. This parameter may need to be added and removed according to site policies.

---

## NetBackup Client Configuration Parameters

Install NetBackup for SQL Server on each physical node. Perform the following steps on both NetBackup clients, NODEA and NODEB:

1. Check to make sure that the Master Server NODE0 is in the server list for this NetBackup client. If it is not, then add it using the NetBackup client-user interface.
2. Create a user ODBC data source name (for example, VIRTUALDSN) for the virtual SQL Server. Specify the server as VIRTUALSERVER. Be sure to add a description.
3. Open the NetBackup for SQL Server interface, from the DBMS options dialog box, select VIRTUALDSN as the current DSN.
4. Select NODE0 as the current NetBackup server from the Client options dialog box of the NetBackup for SQL Server interface.
5. Close the NetBackup for SQL Server interface.

---

**Note** Perform these steps on both physical nodes.

---

## Set Client Environment Variable

---

**Note** The requirement noted in this section is applicable only if you are working with SQL Server 7.0 and NetBackup 3.4, and if patch J0850559 (or greater) has not been installed. You do not need to create an environment variable if you using NetBackup 3.4.1. Note if you do apply patch J0850559 contact VERITAS Technical support for additional information about the impact of this patch on your cluster environment.

---

Set `_VIRTUAL_SERVER_NAME_` as a system environment variable on both physical nodes (NODEA and NODEB). Set the value of this variable to the name of the virtual SQL Server, VIRTUALSERVER.

To set this environmental variable, right click on the Windows **My Computer** icon, select properties, and, then, select environment. In the edit box labeled **variable name**, enter `_VIRTUAL_SERVER_NAME_`. In the edit box labeled **value name**, enter the virtual SQL Server name (for example, VIRTUALSERVER). Be sure that this variable is added as a system variable and not a user variable.

---

**Note** It is critical to use the correct spelling of the variable name,

---

`_VIRTUAL_SERVER_NAME_`

After setting this environment variable on NODEA, do the same on NODEB.



## Performing an SQL Server Backup

Although NetBackup for SQL Server supports browsing for databases and images on either of the physical nodes, a user backup or restore will not be successful unless it is launched from the platform host that is active. After NetBackup has been configured as described in the previous sections, backing up a SQL Server database from a virtual instance is similar to backing up a database from a non-virtual one.

1. Open the NetBackup for SQL Server interface on the active platform node.
2. Open the backup databases dialog box.
3. Select one or more databases.
4. In the NetBackup Class edit box, enter the name of the MS-SQL Server policy class (VIRTSQLCLASS) that was created for specifying storage attributes for the virtual SQL Server backup.
5. Click OK.
6. Select the "Save for later execution" radio button, to save the script to the NetBackup\dbext\mssql folder.
7. Open the script for editing from the batch files window and insert the <keyword value> pair:

```
ALTCLIENT VIRTUALSERVER
```

```
One line prior to OPERATION ENDOPER
```

8. Launch the script by selecting it in the batch files window and clicking on OK.

---

**Note** After you have applied the latest patches to NetBackup the NetBackup for SQL Server script generator, automatically inserts the alternate client name into the backup and restore scripts for you.

---

## Performing a SQL Server Restore

1. Open the NetBackup for SQL Server interface on the active platform node.
2. Select the restore databases, differentials, and transaction logs from the **Actions** menu.
3. When asked, "Would you like to change the database instance?" Choose yes, and the Backup History dialog box will appear.
4. From the Backup History dialog box, enter the Virtual Server name (VIRTUALSERVER) as the host computer.
5. Also from the Backup History dialog box, enter the Virtual Server, choose <default> as the instance name.
6. Click OK, on the Backup History dialog box; and the Restore dialog box will appear.



7. Select a backup image or staged image list, from the backup history window.

---

**Note** Perform step 8 if you are running NetBackup 3.4.1 or if you are working with 3.4 and patch J0850559 (or greater has been applied). Otherwise, perform step 9, step 10, and step 11. Note if you do apply patch J0850559 contact VERITAS Technical support for additional information about the impact of this patch on your cluster environment.

---

8. Click OK.
9. Select the **Save for later execution** radio button, to save the script to the NetBackup\dbext\mssql folder.
10. Open the script for editing from the batch files window. Insert the *keyword value* pair:  
ALTCLIENT *VIRTUALSERVER*  
one line prior to OPERATION ENDOPER.
11. Launch the script by selecting it in the batch files window and clicking OK.





# Intel Hosts Running Red Hat Linux 6.2/7.0

# B

This chapter explains how to configure devices for use with Media Manager on a Intel host platform running Red Hat Linux. You can configure robots and drives for Media Manager using one of the available Media Manager administrative interfaces.

The main topics included in this chapter are

- ◆ Before You Start
- ◆ Configuring Robotic Controls
- ◆ Configuring Tape Drives
- ◆ Verifying The Device Configuration
- ◆ Frequently Asked Questions

## Before You Start

Observe the following points when performing the tasks described in this chapter:

- ◆ Verify that the st (tape) device driver is installed or loaded in the kernel. This driver allows the use of SCSI tape drives.
- ◆ If you are going to use robotic devices, verify that the sg device driver is installed or loaded in the kernel.
- ◆ Use the following command to display and verify that these modules are loaded in the kernel: `/sbin/lsmmod`. Example output from this command follows:

Module	Size	Used by
sg	14844	0
st	24556	0

The standard Red Hat Linux 6.2 distribution has these modules available for loading. When running Red Hat Linux, these modules are dynamically loaded as needed.

- ◆ To load these modules if they are not in the kernel, use the following commands:

```
/sbin/insmod st  
/sbin/insmod sg
```



- ◆ To install the st and sg modules in the kernel, use the standard system utilities to modify the configuration file in `/usr/src/linux` and then rebuild the kernel. If the `Linux` directory is not there, install the kernel source code.
- ◆ Media Manager device discovery is run during the NetBackup install and the start up processes. Device discovery
  - ◆ Runs the binary `/usr/opensv/volmgr/bin/make_scsi_dev` which creates the directories `/dev/sg` and `/dev/st`.
  - ◆ Obtains the device file output generated by the sg and st drivers.
  - ◆ Creates device files of the format required for Media Manager and places them in these directories. See “Configuring SCSI Robotic Controls” on page 102 and “Adding Standard Tape Drives” on page 103.

## Configuring Robotic Controls

To use robotics, the following drivers must be configured in the kernel or loaded as modules:

- ◆ Standard SCSI driver.
- ◆ SCSI-adaptor driver.
- ◆ Linux SCSI generic (sg) driver.

See the NetBackup release notes for a list of the vendor models associated with the following supported Media Manager robot types: TLD - Tape Library DLT and TSD - Tape Stacker DLT.

## Configuring SCSI Robotic Controls

Media Manager device discovery creates device files in the `/dev/sg` directory. The names of these files in this directory have the following format:

`hHOSTcCHANNELtTARGETlLUN`

Where:

*HOST* is the host bus adaptor.

*CHANNEL* is channel.

*TARGET* is the target ID.

*LUN* is the logical unit number.

Use the files in the `/dev/sg` directory for the robotic path when using Media Manager to configure robots.

## Examples of SCSI Robotic Control Device Files

```
h10c0t110
h10c0t210
h10c0t310
h25c0t010
h25c0t110
```

## Configuring Tape Drives

To use SCSI tape drives, the following drivers must be configured in the kernel or loaded as modules:

- ◆ Standard SCSI driver.
- ◆ SCSI-adaptor driver.
- ◆ SCSI tape (st) driver.

## Adding Standard Tape Drives

Media Manager device discovery creates device files in the `/dev/st` directory. The names of the no rewind device files in this directory have the following format:

```
nhHOSTcCHANNELtTARGETlLUN
```

Where:

*n* is the no rewind on close device file.

*HOST* is the host bus adaptor.

*CHANNEL* is channel.

*TARGET* is the target ID.

*LUN* is the logical unit number.

When adding tape drives to a Media Manager configuration, you need to specify a no rewind on close device path. Use the files in the `/dev/st` directory when configuring tape drives.

## Examples of SCSI Tape Device Files

```
nh10c0t210
nh10c0t310
```



## Verifying The Device Configuration

The file `/proc/scsi/scsi` shows all devices recognized by the SCSI driver. To verify that the operating system can see the devices, run the following command from a terminal window to view this file:

```
cat /proc/scsi/scsi
```

The output displayed should be similar to the following example:

Attached devices:

```
Host: scsi0 Channel: 00 Id: 01 Lun: 00
  Vendor: HP          Model: C7200-8000          Rev: 1040
  Type:   Medium Changer                      ANSI SCSI revision: 03
Host: scsi0 Channel: 00 Id: 02 Lun: 00
  Vendor: QUANTUM     Model: DLT8000             Rev: 010F
  Type:   Sequential-Access                    ANSI SCSI revision: 02
Host: scsi0 Channel: 00 Id: 03 Lun: 00
  Vendor: QUANTUM     Model: DLT8000             Rev: 010F
  Type:   Sequential-Access                    ANSI SCSI revision: 02
```

If the operating system can see your SCSI devices, Media Manager device discovery will also see the devices.

## Frequently Asked Questions

### Question

What types of SCSI controllers are supported?

### Answer

At this release of NetBackup, we are not limiting support to specific SCSI controllers. However, testing was done with DLT tape drives using TLD and TSD robotic control and SCSI controllers supported by the Adaptec aic7xxx driver. Testing has not been done with other SCSI controllers and other drivers.

### Question

How can I tell what SCSI devices are attached to my system?

**Answer**

At a command prompt enter the following:

```
cat /proc/scsi/scsi
```

**Question**

How can I tell what drivers are loaded on my system?

**Answer**

At a command prompt enter the following:

```
/sbin/lsmmod
```

**Question**

What device names does NetBackup use to control media changers (robots) and tape drives?

**Answer**

NetBackup runs the binary `/usr/opensv/volmgr/bin/make_scsi_dev` which creates the directories `/dev/sg` and `/dev/st`. This binary then creates symbolic links in these directories to the actual device file created by the `sg` or `st` driver. The names in `/dev/sg` are used to control media changers and the names in `/dev/st` are used to control tape devices.

**Question**

How can I prevent the `sg` and `st` drivers from being unloaded from kernel memory?

**Answer**

These drivers are released in Red Hat as loadable modules. If you see problems which leave NetBackup Media Manager processes hanging because the drivers are unloaded, VERITAS suggests you install these modules in the kernel by building a custom kernel.

Building a custom kernel is documented in the Red Hat Linux Reference Guide. When building a custom kernel, include the following:

- ◆ SCSI Support
  - SCSI tape support.
  - SCSI generic support.
  - Probe all LUNS on each SCSI device.
- ◆ SCSI low-level drivers
  - Include the drivers for your SCSI adaptor.



**Question**

Are there any utilities to test SCSI devices?

**Answer**

You can manipulate tape devices with the system `mt` command. The man page for `MT(1)` explains how to do this.

Robots can be tested using the `robtest` utility in `/usr/opensv/volmgr/bin`.

There is also a set of SCSI utilities available from the Linux SCSI Generic (`sg`) driver home page:

`http://gear.torque.net/sg`