Symantec NetBackup™ Backup Planning and Performance Tuning Guide

UNIX, Windows, and Linux

Release 7.0 through 7.1

Symantec

Symantec NetBackup™ Backup Planning and Performance Tuning Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation versions 7.0 through 7.1

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Section 1

Backup planning and configuration guidelines

Chapter 1

NetBackup capacity planning

This chapter includes the following topics:

Purpose of this guide

This guide covers NetBackup releases 7.0, 7.0.1, and 7.1.

Symantec NetBackup is a high-performance data protection application. Its architecture is designed for large and complex distributed computing environments. NetBackup provides scalable storage servers (master and media servers) that can be configured for network backup, recovery, archiving, and file migration services.

This manual is for administrators who want to analyze, evaluate, and tune NetBackup performance. This manual is intended to provide guidance on questions such as the following: How big should the NetBackup master server be? How can the server be tuned for maximum performance? How many CPUs and disk or tape drives are needed? How to configure backups to run as fast as possible? How to improve recovery times? What tools can characterize or measure how NetBackup handles data?

Note: Most critical factors in performance are based in hardware rather than software. Compared to software, hardware and its configuration have roughly four times greater effect on performance. Although this guide provides some hardware configuration assistance, it is assumed for the most part that your devices are correctly configured.

For additional planning or performance-related information, refer to the following documents:

- Virtualization:
  http://www.symantec.com/docs/TECH127089
- Deduplication:
  http://www.symantec.com/docs/TECH77575
- Storage Lifecycle Policies:
  http://www.symantec.com/docs/TECH153154
- Media server encryption option (MSEO):
  http://www.symantec.com/docs/TECH73132

Disclaimer

It is assumed you are familiar with NetBackup and your applications, operating systems, and hardware. The information in this manual is advisory only, presented in the form of guidelines. Changes to an installation that are undertaken as a result of the information in this guide should be verified in advance for appropriateness and accuracy. Some of the information that is contained herein may apply only to certain hardware or operating system architectures.

Note: The information in this manual is subject to change.

About backup requirements and bottlenecks

To estimate your backup requirements, the first step is to understand your environment. Many performance issues can be traced to hardware or environmental issues. An understanding of the entire backup data path is important to determine the maximum performance you can expect from your installation.

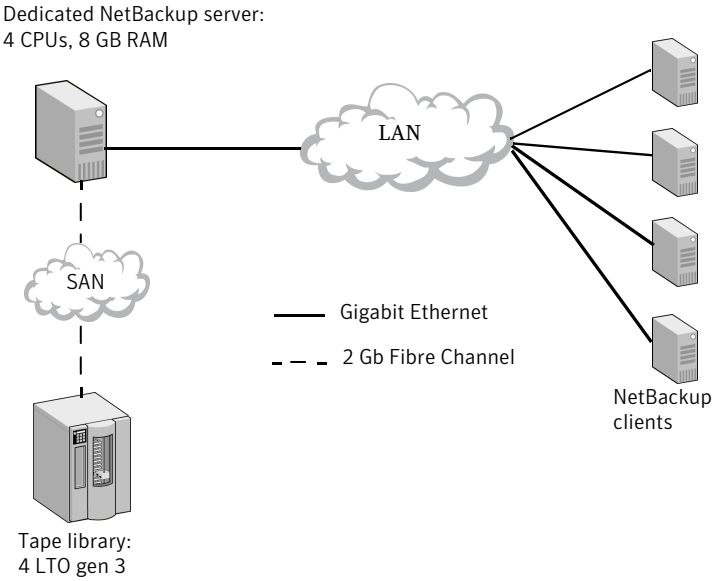
Every backup environment has a bottleneck. It may be a fast bottleneck, but it determines the maximum performance obtainable with your system.

Consider the following example environment, where backups run slowly (in other words, they do not complete in the scheduled backup window). Total throughput is 80 MB per second.

What makes the backups run slowly? How can NetBackup or the environment be configured to increase backup performance in this situation?

Figure 1-1 shows this environment.

Figure 1-1 Dedicated NetBackup environment



The explanation is the following: the four LTO gen 3 tape drives have a combined throughput of 320 MB (megabytes) per second. And the 2 Gbit SAN connection from the server to the tape drives has a theoretical throughput of 200 MB per second. The LAN, however, has a theoretical throughput of 125 MB per second (1 gigabit per second). In practice, 1-gigabit throughput is unlikely to exceed 70% utilization. Therefore, the best delivered data rate is about 90 MB per second to the NetBackup server.

The throughput may be even lower when you consider the following:

- TCP/IP packet headers
- TCP-window size constraints
- Router hops (packet latency for ACK packets delays the sending of the next data packet)
- Host CPU utilization

- File system overhead
- Other LAN users' activity
- Database management daemons and services

Since the LAN is the slowest element in the configuration, it is the first place to look to increase backup performance.

How to analyze your backup requirements

Many factors can influence your backup strategy. You should analyze these factors and then make backup decisions according to your site's priorities.

When you plan your installation's NetBackup capacity, ask yourself the following questions:

Table 1-1 Questions to ask when planning NetBackup capacity

Questions	Actions and related considerations
Which systems need to be backed up?	Identify all systems that need to be backed up. List each system separately so that you can identify any that require more resources to back up. Document which computers have disk drives or tape drives or libraries attached and write down the model type of each drive or library. Identify any applications on these computers that need to be backed up, such as Oracle, DB2, or MS-Exchange. In addition, record each host name, operating system and version, database type and version, network technology (for example, 1000BaseT), and location.
How much data is to be backed up?	Calculate how much data you need to back up. Include the total disk space on each individual system, including that for databases. Remember to add the space on mirrored disks only once. By calculating the total size for all disks, you can design a system that takes future growth into account. Try to estimate how much data you will need to back up in six months to a few years from now. Consider the following: ■ Do you plan to back up databases or raw partitions? To back up databases, identify the database engines, their version numbers, and the method to back them up. NetBackup can back up several database engines and raw file systems, and databases can be backed up while they are online or offline. To back up a database that is online, you need a NetBackup database agent for your particular database engine. With a Snapshot Client backup of databases using raw partitions, you back up as much data as the total size of your raw partition. Also, remember to add the size of your database backups to your final calculations when figuring out how much data you need to back up. ■ Do you plan to back up special application servers such as MS-Exchange or Lotus Notes? To back up application servers, identify their types and application release numbers. As previously mentioned, you may need a special NetBackup agent to back up your particular servers.

Table 1-1 Questions to ask when planning NetBackup capacity *(continued)*

Questions	Actions and related considerations
What types of backups are needed and how often should they take place?	The frequency of your backups has a direct impact on your: ■ Disk or tape requirements ■ Data transfer rate considerations ■ Restore opportunities. To properly size your backup system, you must decide on the type and frequency of your backups. Will you perform daily incremental and weekly full backups? Monthly or bi-weekly full backups?
How much time is available to run each backup?	What is the window of time that is available to complete each backup? The length of a window dictates several aspects of your backup strategy. For example, you may want a larger window of time to back up multiple, high-capacity servers. Or you may consider the use of advanced NetBackup features such as synthetic backups, a local snapshot method, or FlashBackup.
How long should backups be retained?	An important factor while designing your backup strategy is to consider your policy for backup expiration. The amount of time a backup is kept is also known as the "retention period." A fairly common policy is to expire your incremental backups after one month and your full backups after six months. With this policy, you can restore any daily file change from the previous month and restore data from full backups for the previous six months. The length of the retention period depends on your own unique requirements and business needs, and perhaps regulatory requirements. However, the length of your retention period is directly proportional to the number of tapes you need and the size of your NetBackup image database. Your NetBackup image database keeps track of all the information on all your disk drives and tapes. The image database size is tightly tied in to your retention period and the frequency of your backups.
If backups are sent off site, how long must they remain off site?	If you plan to send tapes off-site as a disaster recovery option, identify which tapes to send off site and how long they remain off site. You might decide to duplicate all your full backups, or only a select few. You might also decide to duplicate certain systems and exclude others. As tapes are sent off site, you must buy new tapes to replace them until they are recycled back from off site storage. If you forget this detail, you may run out of tapes when you most need them.
What is your network technology?	If you plan to back up any system over a network, note the network types. The next section explains how to calculate the amount of data you can transfer over those networks in a given time. See "Designing your backup system" on page 20. Based on the amount of data that you want to back up and the frequency of those backups, consider installing a private network for backups.
What systems do you expect to add in the next six months?	Plan for future growth when designing your backup system. Analyze the potential growth of your system to ensure that your current backup solution can accommodate future requirements. Remember to add any resulting growth factor that you incur to your total backup solution.

Table 1-1 Questions to ask when planning NetBackup capacity *(continued)*

Questions	Actions and related considerations
Will user-directed backups or restores be allowed?	Allow users to do their own backups and restores, to reduce the time it takes to initiate certain operations. However, user-directed operations can also result in higher support costs and the loss of some flexibility. User-directed operations can monopolize media and tape drives when you most need them. They can also generate more support calls and training issues while the users become familiar with the new backup system. Decide whether user access to some of your backup systems' functions is worth the potential cost.
What data types are involved?	What are the types of data: text, graphics, database? How compressible is the data? How many files are involved? Will the data be encrypted? (Note that encrypted backups may run slower.) See "Encryption and NetBackup performance" on page 168.
Where is the data located?	Is the data local or remote? What are the characteristics of the storage subsystem? What is the exact data path? How busy is the storage subsystem?
How to test the backup system?	Because hardware and software infrastructure change over time, create an independent test-backup environment to ensure your production environment will work with the changed components.

Designing your backup system

The planning and configuration examples that follow are based on standard and ideal calculations. Your numbers can differ based on your particular environment, data, and compression rates.

After an analysis of your backup requirements, you can begin designing your backup system. The table below summarizes the steps to completing a design for your backup system.

Table 1-2 Steps to design your backup system

Step	Action	Description
Step 1	Calculate the required data transfer rate for your backups.	Calculate the rate of transfer your system must achieve to complete a backup of all your data in the time available. See "How to calculate the required data transfer rate for your backups" on page 22.

Table 1-2 Steps to design your backup system *(continued)*

Step	Action	Description
Step 2	Calculate how long it takes to back up to tape or disk	Determine what kind of tape or disk technology meets your needs. See "How to calculate the time required to back up to tape" on page 23. See "About how to calculate how long it will take to back up to conventional disk storage" on page 26. See "About how to calculate how long it will take to back up to deduplicating disk storage" on page 26.
Step 3	Calculate the required number of tape drives	Determine how many tape drives are needed. See "How to calculate the required number of tape drives" on page 26.
Step 4	Calculate the required data transfer rate for your network(s)	For backups over a network, you must move data from your client(s) to your media server(s) fast enough to finish backups within your backup window. See "How to calculate the required data transfer rate for your network(s)" on page 28.
Step 5	Calculate the size of your NetBackup image database	Determine how much disk space is needed to store your NetBackup image database. See "How to calculate the size of your NetBackup image database" on page 32.
Step 6	Calculate the size of the NetBackup relational database (NBDB)	Determine the space required for NBDB. See "How to calculate the size of the NetBackup relational database (NBDB)" on page 35.
Step 7	Calculate media needed for full and incremental backups	Determine how many tapes are needed to store and retrieve your backups. See "How to calculate the media needed for full and incremental backups" on page 36.
Step 8	Calculate the size of the tape library needed to store your backups	Determine how many robotic library tape slots are needed to store all your backups. See "How to calculate the size of the tape library needed to store your backups" on page 38.
Step 9	Design your master server	Use the previous calculations to design and configure a master server. See "How to design and configure your master server" on page 39.

Table 1-2 Steps to design your backup system *(continued)*

Step	Action	Description
Step 10	Estimate the number of master servers needed	The following topic lists some considerations for estimating the number of master servers. See "How to estimate the number of master servers needed" on page 40.
Step 12	Estimate the number of media servers needed	The following topic contains guidelines for estimating how many media servers are needed. See "How to estimate the number of media servers needed" on page 42.
Step 13	Design your OpsCenter server	The following topic contains links to OpsCenter information. See "About how to design your OpsCenter server" on page 43.
Step 14	Review a summary of these steps	The following is a condensed overview. See "How to design your backup system: Summary" on page 43.

How to calculate the required data transfer rate for your backups

This section helps you calculate the rate of transfer your system must achieve to complete a backup of all your data in the allowed time window. Use the following formula to calculate your ideal data transfer rate for full and incremental backups:

Ideal data transfer rate = (amount of data to back up) / (backup window)

On average, the daily change in data for many systems is between 10 and 20 percent. Calculate a change of 20% in the (amount of data to back up). Then divide it by the (backup window) for the backup rate for incremental backups.

If you run cumulative-incremental backups, account for data that undergoes changes. For example: if the same 20% of the data changes daily, your cumulative-incremental backup is smaller than if a different 20% changes every day.

The following is an example of how to calculate your ideal data transfer rate during the week.

This example makes the following assumptions:

- Amount of data to back up during a full backup = 500 gigabytes
- Amount of data to back up during an incremental backup = 20% of a full backup
  Daily backup window = 8 hours

Solution 1:

Full backup = 500 gigabytes

Ideal data transfer rate = 500 gigabytes per 8 hours = 62.5 gigabytes per hour

Solution 2:

Incremental backup = 100 gigabytes

Ideal data transfer rate = 100 gigabytes per 8 hours = 12.5 gigabytes per hour

For your ideal weekend transfer rate, divide the amount of data that must be backed up by the length of the weekend backup window.

How to calculate the time required to back up to tape

When you know your ideal data transfer rates for backups, you can figure out what kind of tape drive technology meets your needs. With the length of your backup windows and the amount of data to back up, you can calculate the number of required tape drives.

Table 1-3 lists the transfer rates for several tape drive technologies.

Table 1-3 Tape drive data transfer rates

Drive	Megabytes per second	Gigabytes per hour, no compression	Gigabytes per hour, at 60% utilization	Gigabytes per hour, at 2:1 compression and 60% utilization
AIT-5	24	86.4	51.84	103.68
DLT-S4/S4A	60	216	129.6	259.2
DLT-V4	10	36	21.6	43.2
LTO-3	80	288	172.8	345.6
LTO-4	120	432	259.2	518.4
LTO-5	140	504	302.4	604.8
SAIT-1	30	108	64.8	129.6
SAIT-2	45	162	97.2	194.4
SDLT 600/600A	36	129.6	77.76	155.52
TS1120 (3592E05)	100	360	216	432
TS1130 (3592E06)	160	576	345.6	691.2

Table 1-3 Tape drive data transfer rates *(continued)*

Drive	Megabytes per second	Gigabytes per hour, no compression	Gigabytes per hour, at 60% utilization	Gigabytes per hour, at 2:1 compression and 60% utilization
T10000A (STK, Sun, Oracle)	120	432	259.2	518.4
T10000B (STK, Sun, Oracle)	120	432	259.2	518.4

The values in the table are those published by individual manufacturers and observed in real-life situations. These values are not definitive, but should be useful for planning your requirements.

Keep in mind that device manufacturers list optimum rates for their devices. In the table, the column labeled **Gigabytes per hour, no compression** lists these optimum rates. In reality, it is rare to achieve those rates when a system has to deal with the following: the overhead of the operating system, CPU loads, bus architecture, data types, and other hardware and software issues. The 60% utilization columns in the table are conservative estimates, meant to approximate average, real-world performance.

When you design your backup system, consider the nature of both your data and your environment. A backup image that contains many small files may take longer to write to tape than one that contains a few large files. To be on the conservative side, use the 60% values from the table when making your estimates.

Note: Unlike tape drives, disk devices (including VTLs) do not have a minimum streaming speed. It may therefore be a good strategy to stage slower backups to disk before duplicating them to tape: the duplication of the backup image from disk runs faster than the original slow backup.

To calculate the length of your backups using a particular tape drive, use this formula:

Actual data transfer rate = (Amount of data to back up)/((Number of drives) * (Tape drive transfer rate))

The following is an example of how to calculate the time required to back up to tape.

This example makes the following assumptions:

- Amount of data to back up during a full backup = 1000 gigabytes (1 terabyte)

- Daily backup window = 8 hours
- Ideal transfer rate (data/(backup window)) =1000 gigabytes per 8 hours = 125 gigabytes per hour

Solution 1:

Tape drive = 1 drive, LTO-2

Tape drive transfer rate = 64.8 gigabytes per hour at 60% utilization with no compression, or 129.6 gigabytes per hour at 60% utilization with 2:1 compression

Actual data transfer rate, no compression = 1000 gigabytes/((1 drive) * (64.8 gigabytes per hour)) = 15.43 hours

Actual data transfer rate, 2:1 compression = 1000 gigabytes/((1 drive) * (129.6 gigabytes per hour)) = 7.72 hours

At 64.8 gigabytes per hour, an LTO-2 tape drive takes approximately 15.43 hours to perform a 1000-gigabyte backup. Under normal circumstances, the LTO-2 tape drive with no compression cannot perform the backup in eight hours. But, at 129.6 gigabytes per hour (with 2:1 compression), an LTO-2 tape drive takes 7.72 hours to perform a 1000-gigabyte backup.

In this example, you need to use compression or a faster tape drive, or add another LTO-2 tape drive.

Solution 2:

Tape drive = 1 drive, LTO-3

Tape drive transfer rate = 172.8 gigabytes per hour at 60% utilization with no compression, or 345.6 gigabytes per hour at 60% utilization with 2:1 compression

Actual data transfer rate, no compression = 1000 gigabytes/((1 drive) * (172.8 gigabytes per hour)) = 5.79 hours

Actual data transfer rate, 2:1 compression = 1000 gigabytes/((1 drive) * (345.6 gigabytes per hour)) = 2.89 hours

With a data transfer rate of either 172.8 or 345.6 gigabytes per hour, a single LTO-3 tape drive easily performs the 1000-gigabyte backup in less than 8 hours.

Depending on the factors that can influence the transfer rates of your tape drives, you can obtain higher or lower transfer rates. These example solutions are approximations of what you can expect.

Note also that a backup of encrypted data may take more time.

See "Encryption and NetBackup performance" on page 168.

Faster tape drives are not always better

The fastest tape technology may not be the most appropriate for your site. Consider the following. The figures in Table 1-3 are the maximum speeds that the tape drives can achieve. But tape drives also have a minimum speed below which they start to operate inefficiently. This figure is known as the "minimum streaming speed" and is usually around 40% of the native (no compression) speed of the device. If the drive receives data at less than minimum streaming speed, it operates in a stop-and-start mode ("shoe shining"). In this mode the drive empties the data buffers faster than they can be filled and has to stop while the buffers fill up again. When the buffers are full the drive must start up and reposition the tape before it writes the next data block. This stop-and-start behavior damages both the tape and the drive and also results in a further slowing down of the backup. For this reason, the fastest tape technology may not always be the most appropriate one to use.

Also note that the use of data compression raises the minimum streaming speed. The more hardware compression that is used as the data is written to the tape, the slower the streaming speed to tape. For example, if the data is written at 2:1 compression, the data must stream to the drive at 80% of the drive's native speed (not 40%) to exceed the minimum streaming speed.

About how to calculate how long it will take to back up to conventional disk storage

Disk performance is more difficult to predict; no hard and fast rules exist on disk performance. Backup speed depends on the type of disk and on the disk layout. In general, the speed of the backup will depend on the speed of the disks and disk controllers that the backup is being written to.

About how to calculate how long it will take to back up to deduplicating disk storage

Backup speed for conventional disk storage may not be the same as for deduplicating storage. The following document contains guidelines on the type of deduplication to use and provides examples for sizing your deduplication requirements:

NetBackup Deduplication: Additional Usage Information

http://www.symantec.com/docs/TECH77575

How to calculate the required number of tape drives

Here is the formula:

Number of drives = (amount of data to back up) /((backup window) * (tape drive transfer rate))

The following is an example of how to calculate the required number of tape drives.

This example makes the following assumptions:

- Amount of data to back up = 1000 gigabytes (1 terabyte)
- Backup window = 8 hours

Solution 1:

Tape drive type = LTO-2

Tape drive transfer rate = 64.8 gigabytes per hour at 60% utilization with no compression, or 129.6 gigabytes per hour at 60% utilization with 2:1 compression

Number of drives, no compression = 1000 gigabytes/ ((8 hours) * (64.8 gigabytes per hour)) = 1.93 = 2 drives

Number of drives, 2:1 compression = 1000 gigabytes/ ((8 hours) * (129.6 gigabytes per hour)) = .96 = 1 drive

Solution 2:

Tape drive type = LTO-3

Tape drive transfer rate = 172.8 gigabytes per hour at 60% utilization with no compression, or 345.6 gigabytes per hour at 60% utilization with 2:1 compression

Number of drives, no compression = 1000 gigabytes/ ((8 hours) * (172.8 gigabytes per hour)) = .72 = 1 drive

Number of drives, 2:1 compression = 1000 gigabytes/ ((8 hours) * (345.6 gigabytes per hour)) = .36 = 1 drive

You can calculate the number of drives that are needed to perform a backup. It is difficult, however, to spread the data streams evenly across all drives. To spread your data, experiment with various backup schedules, NetBackup policies, and your hardware configuration.

See "Tuning suggestions for the NetBackup data transfer path" on page 110.

To calculate how many tape devices you need, you must calculate how many tape devices you can attach to a drive controller.

To calculate the maximum number of drives that you can attach to a controller, you need the manufacturers' maximum transfer rates for drives and controllers. Failure to use maximum transfer rates for your calculations can result in saturated controllers and unpredictable results.

Note: Knowing the throughput of individual tape drives does not guarantee that these rates can be met. Ensure that the drive controllers have sufficient bandwidth. Do not attach more drives to a controller than the controller bandwidth can support.

Table 1-4 displays the transfer rates for several drive controllers.

Table 1-4 Drive controller data transfer rates

Drive Controller	Theoretical megabytes per second	Theoretical gigabytes per hour
ATA-5 (ATA/ATAPI-5)	66	237.6
Wide Ultra 2 SCSI	80	288
iSCSI	100	360
1 gigabit Fibre Channel	100	360
SATA/150	150	540
Ultra-3 SCSI	160	576
2 gigabit Fibre Channel	200	720
SATA/300	300	1080
Ultra320 SCSI	320	1152
4 gigabit Fibre Channel	400	1440

In practice, your transfer rates might be slower because of the inherent overhead of several variables. Variables include your file system layout, system CPU load, and memory usage.

How to calculate the required data transfer rate for your network(s)

For backups over a network, you must move data from your client(s) to your media server(s) fast enough to finish backups within your backup window. Table 1-5 shows the typical transfer rates of some common network technologies. To calculate the required data transfer rate, use this formula:

Required network data transfer rate = (amount of data to back up) / (backup window)

Table 1-5 Network data transfer rates

Network Technology	Theoretical gigabytes per hour	Typical gigabytes per hour
100BaseT (switched)	36	25
1000BaseT (switched)	360	250
10000BaseT (switched)	3600	2500

Additional information is available on the importance of matching network bandwidth to your tape drives.

See "Network and SCSI/FC bus bandwidth" on page 67.

The following is an example of how to calculate the required data transfer rate for your network(s).

This example makes the following assumptions:

- Amount of data to back up = 500 gigabytes
- Backup window = 8 hours
- Required network transfer rate = 500 gigabytes/8hr = 62.5 gigabytes per hour

Solution 1: Network Technology = 100BaseT (switched)

Typical transfer rate = 25 gigabytes per hour

A single 100BaseT network has a transfer rate of 25 gigabytes per hour. This network cannot handle your required data transfer rate of 62.5 gigabytes per hour.

In this case, you would have to explore other options, such as the following:

- Backing up your data over a faster network (1000BaseT)
- Backing up large servers to dedicated tape drives (SAN media servers)
- Backing up over SAN connections by means of SAN Client
- Performing off-host backups using Snapshot Client to present a snapshot directly to a media server
- Performing your backups during a longer time window
- Performing your backups over faster dedicated networks

Solution 2: Network Technology = 1000BaseT (switched)

Typical transfer rate = 250 gigabytes per hour

Based on Table 1-5, a single 1000BaseT network has a transfer rate of 250 gigabytes per hour. This network technology can handle your backups with room to spare.

Calculate the data transfer rates for your networks to help you identify your potential bottlenecks. Several solutions for dealing with multiple networks and bottlenecks are available.

See "Tuning suggestions for the NetBackup data transfer path" on page 110.

Recommendation for sizing the catalog

A little background information is in order. The term catalog refers to all of the following components:

- The image database, which contains information about what has been backed up. It is by far the largest part of the catalog (more than 90%).
- NetBackup data in relational databases.
- NetBackup configuration files.

See "About the NetBackup catalog" on page 55.

The size of the NetBackup catalog depends on the number of files in the backups and the number of copies of the backups that are retained. As a result, the catalog has the potential to grow quite large. You should consider two additional factors, however, when estimating the ultimate size of the catalog: can it be backed up in an acceptable time window, and can the general housekeeping activities complete within their execution windows. The time that is required to complete a catalog backup depends on the amount of space it occupies. The time that is required for the housekeeping activities depends on the number of entries it contains. Note that NetBackup's catalog archiving feature can be used to move older catalog data to other disk or tape storage. Archiving can reduce the size of the catalog on disk and thus reduce the backup time. Archiving, however, does not decrease the amount of time that is required for housekeeping activities.

Symantec recommends that you plan your environment to meet the following criteria for the catalog:

- The amount of data that is held in the online catalog should not exceed 750 GB. Archiving can be used to keep the online portion of the catalog below this value.
- The total number of catalog entries should not exceed 2,000,000. This number equals the total of all retained copies of all backups from all clients held both online and in the catalog archive.

Table 1-6 Guidelines for catalog size (these guidelines are not hard limits)

Catalog guideline	Notes on the guidelines	Potential consequences of exceeding the guidelines

Online catalog should not contain more than 750 GB of data	Use archiving to keep the online portion of the catalog below 750 GB.
	The reasons for the 750 GB guideline relate to catalog backup and recovery times:
	■ A catalog backup is not a simple flat-file backup:
	  ■ A catalog backup is based on a synchronization check point and requires extra time to process the work list.
	  ■ Catalog backup uses locking to allow other NetBackup jobs to be active concurrently (extra processing time is required).
	■ No snapshot mechanism exists for catalog backup.
	■ Catalog backups typically run at around 30 MB/second. It takes about 7 hours to back up 750 GB. (Restore rates are faster because of less processing overhead).
		The potential results of exceeding 750 GB are the following:
		■ The time that is required to back up the catalog could become excessive.
		■ Using incremental backups can reduce backup time but increase recovery time.
		■ Consider creating a service level agreement (SLA) for recovery. Replication can help in most cases but a catalog backup is still required for insurance or fall-back purposes.

The total number of catalog entries should not exceed 2,000,000	Reasons for the 2,000,000-entry guideline:
	■ Cleanup jobs run every 12 hours.
	  ■ Cleanup jobs check the information in each image metadata file.
	  ■ Processing 30 to 50 records a second, cleanup jobs need between 5 and 9 hours to complete the run if the catalog contains 1,000,000 entries (longer if 2,000,000).
	  ■ If the jobs fail to complete in 12 hours, the next run of each job is cancelled and the run interval extends to 24 hours. A cleanup job frequency of once in 24 hour usually has a negligible effect on overall operation.
	■ The image cleanup does the following:
	  ■ Removes expired images from the catalog.
	  ■ Reclaims the disk space on disk storage devices.
	  ■ Prunes TIR information, and optionally compresses catalog files.
	■ The media cleanup deassigns empty tapes and returns them to the scratch pool.
		The potential results of too many catalog entries are the following:
		■ If the image count grows to such an extent that the cleanup job takes more than 24 hours to complete, the next cleanup job is skipped.
		■ If the next cleanup job is skipped, the recycling of expired media is delayed. As a result, more scratch media are required.
		Note: In general, it is safe to miss a few cleanup jobs; image counts of two to three million may not cause serious problems.

Note that the actual limits of acceptable catalog performance are influenced by the speed of the storage and the power of the server. Your performance may vary significantly from the guideline figures provided in this section.

Note: If you expect your catalog to exceed these limits, consider deploying multiple NetBackup domains in your environment.

The following Symantec document describes best practices for the catalog layout:

http://www.symantec.com/docs/TECH144969

More information on catalog archiving is available in the *NetBackup Administrator's Guide, Volume I*.

How to calculate the size of your NetBackup image database

An important factor when designing your backup system is to calculate how much disk space is needed to store your NetBackup image database. Your image database keeps track of all the files that have been backed up.

The image database size depends on the following variables, for both full and incremental backups:

- The number of files being backed up
- The frequency and the retention period of the backups

You can use either of two methods to calculate the size of the NetBackup image database. In both cases, since data volumes grow over time, you should factor in expected growth when calculating total disk space used.

NetBackup automatically compresses the image database to reduce the amount of disk space required. When a restore is requested, NetBackup automatically decompresses the image database, only for the time period needed to accomplish the restore. You can also use archiving to reduce the space requirements for the image database. More information is available on catalog compression and archiving.

See the *NetBackup Administrator's Guide, Volume I*.

Note: If you select NetBackup's True Image Restore option, your image database becomes larger than an image database without this option selected. True Image Restore collects the information that is required to restore directories to their contents at the time of any selected full or incremental backup. The additional information that NetBackup collects for incremental backups is the same as the information that is collected for full backups. As a result, incremental backups take much more disk space when you collect True Image Restore information.

First method: You can use this method to calculate image database size precisely. It requires certain details: the number of files that are held online and the number of backups (full and incremental) that are retained at any time.

To calculate the size in gigabytes for a particular backup, use the following formula:

image database size = (132 * number of files in all backups)/ 1GB

To use this method, you must determine the approximate number of copies of each file that is held in backups and the typical file size. The number of copies can usually be estimated as follows:

Number of copies of each file that is held in backups = number of full backups + 10% of the number of incremental backups held

The following is an example of how to calculate the size of your NetBackup image database with the first method.

This example makes the following assumptions:

- Number of full backups per month: 4
- Retention period for full backups: 6 months
- Total number of full backups retained: 24
- Number of incremental backups per month: 25
- Total number of files that are held online (total number of files in a full backup): 17,500,000

Solution:

Number of copies of each file retained:

24 + (25 * 10%) = 26.5

NetBackup image database size for each file retained:

(132 * 26.5 copies) = 3498 bytes

Total image database space required:

(3498 * 17,500,000 files) /1 GB = 61.2 GB

Second method: Multiply by a small percentage (such as 2%) the total amount of data in the production environment (not the total size of all backups). Note that 2% is an example; this section helps you calculate a percentage that is appropriate for your environment.

Note: You can calculate image database size by means of a small percentage only for environments in which it is easy to determine the following: the typical file size, typical retention policies, and typical incremental change rates. In some cases, the image database size that is obtained using this method may vary significantly from the eventual size.

To use this method, you must determine the approximate number of copies of each file that are held in backups and the typical file size. The number of copies can usually be estimated as follows:

Number of copies of each file that is held in backups = number of full backups + 10% of the number of incremental backups held

The multiplying percentage can be calculated as follows:

Multiplying percentage = (132 * number of files that are held in backups / average file size) * 100%

Then, the size of the image database can be estimated as:

Size of the image database = total disk space used * multiplying percentage

The following is an example of how to calculate the size of your NetBackup image database with the second method.

This example makes the following assumptions:

- Number of full backups per month: 4
- Retention period for full backups: 6 months
- Total number of full backups retained: 24
- Number of incremental backups per month: 25
- Average file size: 70 KB
- Total disk space that is used on all servers in the domain: 1.4 TB

Solution:

Number of copies of each file retained:

24 + (25 * 10%) = 26.5

NetBackup image database size for each file retained:

(132 * 26.5 copies) = 3498 bytes

Multiplying percentage:

(3498/70000) * 100% = 5%

Total image database space required:

(1,400 GB * 4.5%) = 63 GB

How to calculate the size of the NetBackup relational database (NBDB)

By default, the NBDB database resides on the NetBackup master server. Other configurations are possible.

See "About merging, splitting, or moving servers" on page 61.

Note: This space must be included when determining size requirements for a master server or media server, depending on where the NBDB database is installed.

The NBDB database is part of the NetBackup catalog. More information is available on the components of the catalog.

See "About the NetBackup catalog" on page 55.

Space for the NBDB database is required in the following two locations:

UNIX

```
/usr/openv/db/data
/usr/openv/db/staging
```

Windows

```
install_path\NetBackupDB\data
install_path\NetBackupDB\staging
```

To calculate the required space for the NBDB in each of the two directories, use this formula

160 MB + (2 KB * number of volumes that are configured for EMM) + (number of images in disk storage other than BasicDisk * 5 KB) + (number of disk volumes * number of media severs * 5 KB)

where EMM is the Enterprise Media Manager, and volumes are NetBackup (EMM) media volumes. Note that 160 MB is the default amount of space that is needed for the NBDB database. It includes pre-allocated space for configuration information for devices and storage units.

Note: During NetBackup installation, the install script looks for 160 MB of free space in the `/data` directory. If the directory has insufficient space, the installation fails. The space in `/staging` is only required when a catalog backup runs.

The NBDB transaction log occupies a portion of the space in the /data directory that NBDB requires. This transaction log is only truncated (not removed) when a catalog backup is performed. The log continues to grow indefinitely if a catalog backup is not made at regular intervals.

The following is an example of how to calculate the space needed for the NBDB database.

Assuming there are 1000 EMM volumes to back up, the total space that is needed for the NBDB database in `/usr/openv/db/data` is:

160 MB + (2 KB * 1000 volumes) + (5 KB * 1000 AdvancedDisk images) + (5 KB * 10 AdvancedDisk volumes * 4 media servers) = 167.2 MB

The same amount of space is required in `/usr/openv/db/staging`. The amount of space that is required may grow over time as the NBDB database increases in size.

Note: The 160 MB of space is pre-allocated.

Additional details are available on the files and database information that are included in the NBDB database. See the *NetBackup Administrator's Guide*.

How to calculate the media needed for full and incremental backups

Calculate how many tapes are needed to store and retrieve your backups.

The number of tapes depends on the following:

- The amount of data that you back up
- The frequency of your backups
- The planned retention periods
- The capacity of the media that is used to store your backups.

If you expect your site's workload to increase over time, you can ease the pain of future upgrades by planning for expansion. Design your initial backup architecture so it can evolve to support more clients and servers. Invest in the faster, higher-capacity components that can serve your needs beyond the present.

You can use the following formula to calculate your tape needs:

Number of tapes = (Amount of data to back up) / (Tape capacity)

To calculate how many tapes are needed based on all your requirements, the previous formula can be expanded to the following:

Number of tapes = ((Amount of data to back up) * (Frequency of backups) * (Retention period)) / (Tape capacity)

Table 1-7 lists some common tape capacities.

Table 1-7 Tape capacities

Cartridge type	Cartridge size in gigabytes, no compression	Cartridge size in gigabytes, 2:1 compression
AIT-5	400	800
DLT-S4/S4A	800	1600
DLT-V4	80	160
LTO-3	400	800
LTO-4	800	1600
LTO-5	1500	3000
SAIT-1	500	1000
SAIT-2	800	1600
SDLT 600/600A	300	600
TS1120 (3592E05)	500	1000
TS1130 (3592E06)	640	1280
T10000A (STK, Sun, Oracle)	500	1000
T10000B (STK, Sun, Oracle)	1000	2000

The following is an example of how to calculate the number of tapes needed for your backups.

This example depends on the following preliminary calculations:

- Size of full backups = 500 gigabytes * 4 (per month) * 6 months = 12 terabytes
- Size of incremental backups = (20% of 500 gigabytes) * 30 * 1 month = 3 terabytes
- Total data tracked = 12 terabytes + 3 terabytes = 15 terabytes

Solution:

Tape drive type = LTO-3

Tape capacity without compression = 400 gigabytes

Tape capacity with compression = 800 gigabytes

Without compression:

Tapes that are needed for full backups = 12 terabytes/400 gigabytes = 30

Tapes that are needed for incremental backups = 3 terabytes/400 gigabytes = 7.5 ~= 8

Total tapes needed = 30 + 8 = 38 tapes

With 2:1 compression:

Tapes that are needed for full backups = 12 terabytes/800 gigabytes = 15

Tapes that are needed for incremental backups = 3 terabytes/800 gigabytes = 3.75 ~= 4

Total tapes needed = 15 + 4 = 19 tapes

How to calculate the size of the tape library needed to store your backups

To calculate how many robotic library tape slots are needed to store all your backups, do the following: take the number of backup tapes that was calculated in a previous section and add tapes for catalog backup and for cleaning.

See "How to calculate the media needed for full and incremental backups" on page 36.

The formula is the following:

Tape slots needed = (the number of tapes that are needed for backups) + (the number of tapes that are needed for a full backup) + (the number of tapes that are needed for catalog backups) + (the number of cleaning tapes)

This formula may be on the conservative side. Above all, you need an ample stock of scratch tapes: backup retention periods generally cause the oldest backup to expire after the latest backup.

Note: The number of tapes for catalog backup = the number of full and incremental catalog backups that are retained.

Additional tapes may be needed for the following:

- If you plan to duplicate tapes or to reserve some media for special (non-backup) use, add those tapes to the formula.

- Add the tapes that are needed for future data growth. Make sure your system has a viable upgrade path as new tape drives become available.

How to design and configure your master server

To design and configure a master server, do the following:

- Perform an analysis of your initial backup requirements.
  See "How to analyze your backup requirements" on page 18.
- In the following topic, perform the calculations in the steps leading up to Design your master server:
  See "Designing your backup system" on page 20.

You can design a master server when the following design constraints are known:

- Amount of data to back up
- Size of the NetBackup catalog
- Number of tape drives needed
- Number of disk drives needed
- Number of networks needed

When you have the design constraints, use the following procedure as an outline to configure your master server.

To configure the master server

1. Acquire a dedicated server.
2. Add tape drives and controllers, for saving your backups.
3. Add disk drives and controllers, for saving your backups, and for OS and NetBackup catalog.
4. Add network cards.
5. Add memory.
6. Add CPUs.

Note: In some cases, it may not be practical to design a server to back up all of your systems. You might have one or more large servers that cannot be backed up over a network within your backup window. In such cases, back up those servers by means of their own locally-attached drives or drives that use the Shared Storage Option. Although this section discusses how to design a master server, you can use this information to add the drives and components to your other servers.

Modern servers work well with NetBackup. All modern servers now have multiple CPUs with multiple cores. NetBackup uses a percentage of the available CPU cycles and RAM, based on the required processes.

Be sure to follow your hardware vendors' recommendations for CPUs and RAM. For example, the new DDR3 RAM has to be installed in groups of 6GB.

When designing your master server, begin with a dedicated server for optimum performance. In addition, consult with your server's hardware manufacturer to ensure that the server can handle your other components. In most cases, servers have specific restrictions on the number and mixture of hardware components that can be supported concurrently. If you overlook this last detail, it can cripple the best of plans.

How to estimate the number of master servers needed

To determine how many master servers are required, consider the following:

- The master server must be able to periodically communicate with all its media servers. If you have too many media servers, the master server may be overloaded.
- Consider business-related requirements. For example, if an installation has different applications that require different backup windows, a single master may have to run backups continually. As a result, resources for catalog cleaning, catalog backup, or other maintenance activity may be insufficient.
- As a rule, the number of clients (separate physical hosts) per master server is not a critical factor for NetBackup. The backup processing that clients perform has little or no effect on the NetBackup server. Exceptions do exist. For example, if all clients have database extensions, or all clients run ALL_LOCAL_DRIVES backups at the same time, server performance may be affected.
- Plan your configuration so that it contains no single point of failure. Provide sufficient redundancy to ensure high availability of the backup process. More tape drives or media may reduce the number of media servers that are needed per master server.
- Do not plan to run more than about 20,000 backup jobs per 12-hour period on a single master server.
  See the "Limits to scalability" item later in this topic.
- Consider limiting the number of media servers that are handled by a master to the lower end of the estimates in the following table.
  A well-managed NetBackup environment may be able to handle more media servers than the numbers that are listed in this table. Your backup operations, however, may be more efficient and manageable with fewer, larger media servers. The variation in the number of media servers per master server for

each scenario in the table depends on the following: number of jobs submitted, multiplexing, multiple data streams, and network capacity.

Table 1-8 Estimates of processors and memory for a master server

Number of processors	Minimum RAM	Maximum number of jobs per day	Maximum number of media servers per master server
2	4 GB	2000	20
4	8 GB	5000	50
8	16 GB	10000	100

These estimates are based on the number of media servers and the number of jobs the master server must support. This table is for guidance only; it is based on test data and customer experiences. The amount of RAM and number of processors may need to be increased based on other site-specific factors.

In this table, a processor is defined as a state-of-the-art CPU. An example is a 3-GHz processor for an x86 system, or the equivalent on a RISC platform such as Sun SPARC.

When making an estimate, consider the following:

- Type of processor
  For a NetBackup master server, Symantec recommends using multiple discrete processors instead of a single multi-core processor. The individual cores in a multi-core processor lack the resources to support some of the CPU-intensive processes that run on a master server. Two physical dual-core processors (for a total of four processors) are better than a single quad-core processor.
- Definition of a job
  For the purposes of Table 1-8, a job is defined as an individual backup stream. Database and application backup policies, and the policies that use the ALL_LOCAL_DRIVES directive, usually launch multiple backup streams (thus multiple jobs) at the same time.
- Limits to scalability
  Regardless of the size of the master server, the theoretical maximum rate at which backup jobs can launch is about one job per second. Therefore, a domain cannot run much more than 43,000 backup jobs in a 12 hour period.

Note: Real world limitations make it unlikely that this theoretical figure can be achieved.

Background: A NetBackup domain is defined as a number of NetBackup media servers and client computers under the control of a single NetBackup master server. A NetBackup domain may span multiple sites and datacenters . A single site or datacenter may consist of more than one NetBackup domain. Within a NetBackup domain, each backup job receives an identifier that includes a unique 10-digit UTC timestamp. As each timestamp must be unique, only one backup job can be launched per second, regardless of the resources available. As a result, a single NetBackup domain can launch a maximum of 86,400 backup jobs per day. In most situations, constraints within the hardware resources and infrastructure are likely to prevent the server from reaching the 86,400 limit. If a domain does not allow sufficient jobs, an environment can be configured to support multiple NetBackup domains.

How to estimate the number of media servers needed

You can use a media server to back up other systems and reduce or balance the load on your master server. With NetBackup, disk storage control and the robotic control of a library can be on either the master server or the media server.

The following are guidelines for estimating the number of media servers needed:

- I/O performance is generally more important than CPU performance.
- Consider CPU, I/O, and memory expandability when choosing a server.
- Consider how many CPUs are needed. Refer to the following topic:
  Here are some general guidelines for making a CPU estimate:
  Experiments (with Sun Microsystems) indicate that a useful, conservative estimate is the following: 5MHz of CPU capacity for each 1MB per second of data movement in and out of the NetBackup media server. Keep in mind that the operating system and other applications also use the CPU. This estimate is for the power available to NetBackup itself.
  Example:

  A system that backs up clients to tape at 10 MB per second needs 100 MHz of CPU power, as follows:

  - 50MHz to move data from the network to the NetBackup server.
  - 50MHz to move data from the NetBackup server to tape.
- Consider how much memory is needed. Refer to the following topic:
  At least 512 megabytes of RAM is recommended if the server is running a Java GUI. NetBackup uses shared memory for local backups. NetBackup buffer usage affects how much memory is needed.
  Keep in mind that non-NetBackup processes need memory in addition to what NetBackup needs.

A media server moves data from disk (on relevant clients) to storage (usually disk or tape). The server must be carefully sized to maximize throughput. Maximum throughput is attained when the server keeps its tape devices streaming.
More information is available on tape streaming.
See "NetBackup storage device performance in the data transfer path" on page 157.

Additional factors to consider for media server sizing include the following:

- Disk storage access time
- Adapter (for example, SCSI) speed
- Bus (for example, PCI) speed
- Tape or disk device speed
- Network interface (for example, 100BaseT) speed
- Amount of system RAM
- Other applications, if the host is non-dedicated
- Your platform must be able to drive all network interfaces and keep all tape devices streaming.

About how to design your OpsCenter server

Symantec OpsCenter is a Web-based software application that provides detailed information on your data protection environment. It can track the effectiveness of data backup and archive operations by generating comprehensive reports. OpsCenter combines the features of NetBackup Operations Manager (NOM) and Veritas Backup Reporter (VBR).

For assistance in planning and designing an OpsCenter installation, refer to the following documents:

- *Symantec OpsCenter Administrator's Guide*
- *NetBackup 7.0 Additional Operational Notes*: http://www.symantec.com/docs/TECH76770

How to design your backup system: Summary

Design a solution that can do a full backup and incremental backups of your largest system within your time window. The remainder of the backups can happen over successive days.

Eventually, your site may outgrow its initial backup solution. By following the guidelines in the following topic, you can add more capacity at a future date without having to redesign your strategy.

See "Designing your backup system" on page 20.

With proper design, you can create a backup strategy that can grow with your environment.

The number and location of the backup devices are dependent on factors such as the following:

- The amount of data on the target systems
- The available backup and restore windows
- The available network bandwidth
- The speed of the backup devices

If one drive causes backup-window time conflicts, another can be added, providing an aggregate rate of two drives. The trade-off is that the second drive imposes extra CPU, memory, and I/O loads on the media server.

If backups do not complete in the allocated window, increase your backup window or decrease the frequency of your full and incremental backups.

Another approach is to reconfigure your site to speed up overall backup performance. Before you make any such change, you should understand what determines your current backup performance. List or diagram your site network and systems configuration. Note the maximum data transfer rates for all the components of your backup configuration and compare these against the required rate for your backup window. This approach helps you identify the slowest components and, consequently, the cause of your bottlenecks. Some likely areas for bottlenecks include the networks, tape drives, client OS load, and file system fragmentation.

Questionnaire for NetBackup capacity planning

Use this questionnaire to describe the characteristics of your systems and how they are to be used. This data can help determine your NetBackup client configurations and backup requirements.

Table 1-9 contains the questionnaire.

Table 1-9 Backup questionnaire

Question	Explanation
System name	Any unique name to identify the computer. Hostname or any unique name for each system.
Vendor	The hardware vendor who made the system (for example, Sun, HP, IBM, generic PC)
Model	For example: Sun T5220, HP DL580, Dell PowerEdge 6850
OS version	For example: Solaris 10, HP-UX 11i, Windows 2003 DataCenter
Building / location	Identify physical location by room, building, or campus.
Total storage	Total available internal and external storage capacity.
Used storage	Total used internal and external storage capacity. If the amount of data to be backed up is substantially different from the amount of storage capacity used, please note that fact.
Type of external array	For example: Hitachi, EMC, EMC CLARiiON, STK.
Network connection	For example, 100MB, gigabit, T1. You should know whether the LAN is a switched network.
Database (DB)	For example, Oracle 8.1.6, SQL Server 7.
Hot backup required?	A hot backup requires the optional database agent if backing up a database.
Approximate number of files on server, and average file size	The file counts and average file size can have a significant effect on backup throughput.
Key application	For example: Exchange server, accounting system, software developer's code repository, NetBackup critical policies.
Backup window	For example: incremental backups run M-F from 11PM to 6AM. Fulls are all day Sunday. This information helps locate potential bottlenecks and how to configure a solution.
Recovery requirements (RPO, RTO)	Identify the following for your organization: ■ The recovery point objective (RPO). RPO is the point-in-time to which data must be recovered after a disaster or disruption. ■ The recovery time objective (RTO). RTO is the amount of time it should take to restore your organization's business processes after a disaster or disruption.

Table 1-9 Backup questionnaire *(continued)*

Question	Explanation
Retention policy	For example: incremental backups for 2 weeks, full backups for 13 weeks. This information helps determine how to size the number of slots that are needed in a library.
Existing backup media	Type of media currently used for backups.
Comments?	Any special situations to be aware of? Any significant patches on the operating system? Will the backups be over a WAN? Do the backups need to go through a firewall?

Chapter 2

Master server configuration guidelines

This chapter includes the following topics:

- Legacy error log fields

Factors that limit job scheduling

When many requests are submitted to NetBackup simultaneously, NetBackup increases its use of memory. The number of requests may eventually affect the overall performance of the system. This type of performance degradation is associated with the way a given operating system handles memory requests. It may affect the functioning of all applications that currently run on the system, not limited to NetBackup.

Note: In the UNIX (Java) Administration Console, the Activity Monitor may not update if there are thousands of jobs to view. In this case, you may need to change the memory setting by means of the NetBackup Java command jnbSA with the -mx option. See the "INITIAL_MEMORY, MAX_MEMORY" subsection in the *NetBackup Administrator's Guide for UNIX and Linux, Volume I*. Note that this situation does not affect NetBackup's ability to continue running jobs.

See "NetBackup job delays" on page 48.

Stagger the submission of jobs for better load distribution

When the backup window opens, Symantec recommends scheduling jobs to start in small groups periodically, rather than starting all jobs at the same time. If the submission of jobs is staggered, the NetBackup resource broker (nbrb) can allocate job resources more quickly.

The best job scheduling depends on many factors. Experimentation may be necessary.

See "NetBackup job delays" on page 48.

NetBackup job delays

NetBackup jobs may be delayed for a variety of reasons. Table 2-1 describes the kinds of delays that may occur and in some cases suggests possible remedies.

Table 2-1 NetBackup job delays

Type of job delay	Explanation and remedy (if any)
Delays in starting jobs	The NetBackup Policy Execution Manager (nbpem) may not begin a backup at exactly the time a backup policy's schedule window opens. This delay can happen when you define a schedule or modify an existing schedule with a window start time close to the current time. For instance, suppose you create a schedule at 5:50 PM, and specify that backups should start at 6:00 PM. You complete the policy definition at 5:55 PM. At 6:00 PM, you expect to see a backup job for the policy start, but it does not. Instead, the job takes another several minutes to start. The explanation is the following: NetBackup receives and queues policy change events as they happen, but processes them periodically as configured in the Policy Update Interval setting. (The Policy Update Interval is set under **Host Properties > Master Server > Properties > Global Settings**. The default is 10 minutes.) The backup does not start until the first time NetBackup processes policy changes after the policy definition is completed at 5:55 PM. NetBackup may not process the changes until 6:05 PM. For each policy change, NetBackup determines what needs to be done and updates its work list accordingly.

Delays in running queued jobs	If jobs are queued and only one job runs at a time, use the **State Details** column in the Activity Monitor to see the reason for the job being queued.
	
	If jobs are queued and only one job runs at a time, set one or more of the following to allow jobs to run simultaneously:
	
	■ **Host Properties > Master Server > Properties > Global Attributes > Maximum jobs per client** (should be greater than 1).
	■ Policy attribute **Limit jobs per policy** (should be greater than 1).
	■ Schedule attribute **Media multiplexing** (should be greater than 1).
	■ Check the following storage unit properties:
	  ■ Is the storage unit enabled to use multiple drives (**Maximum concurrent write drives**)? If you want to increase this value, remember to set it to fewer than the number of drives available to this storage unit. Otherwise, restores and other non-backup activities cannot run while backups to the storage unit are running.
	  ■ Is the storage unit enabled for multiplexing (**Maximum streams per drive**)? You can write a maximum of 32 jobs to one tape at the same time.
	
	For example, you can run multiple jobs to a single storage unit if you have multiple drives. (Maximum concurrent write drives set to greater than 1.) Or, you can set up multiplexing to a single drive if Maximum streams per drive is set to greater than 1. If both Maximum concurrent write drives and Maximum streams per drive are greater than 1: you can run multiple streams to multiple drives, assuming Maximum jobs per client is set high enough.

Table 2-1 NetBackup job delays *(continued)*

Type of job delay	Explanation and remedy (if any)
Delays in jobs becoming active	Shared disk jobs are generally slower to become active than tape jobs, because shared disk jobs must wait for a disk volume to be mounted. Tape jobs become active as soon as the resources are allocated. NetBackup makes the jobs active as follows: ■ Tape jobs The NetBackup Job Manager (nbjm) requests resources from the NetBackup Resource Broker (nbrb) for the job. nbrb allocates the resources and gives the resources to nbjm. nbjm makes the job active. nbjm starts bpbrm which in turn starts bptm; bptm mounts the tape medium in the drive. ■ Shared disk jobs The NetBackup Job Manager (nbjm) requests job resources from nbrb. nbrb allocates the resources and initiates the shared disk mount. When the mount completes, nbrb gives the resources to nbjm. nbjm makes the job active.
Job delays caused by unavailable media	The job fails if no other storage units are usable, in any of the following circumstances: ■ If the media in a storage unit are not configured or are unusable (such as expired) ■ The maximum mounts setting was exceeded ■ The wrong pool was selected If media are unavailable, consider the following: ■ Add new media ■ Or change the media configuration to make media available (such as changing the volume pool or the maximum mounts). If the media in a storage unit are usable but are busy, the job is queued. In the NetBackup Activity Monitor, the "State Details" column indicates why the job is queued, such as "media are in use." (The same information is available in the Job Details display. Right-click on the job and select "Details.") If the media are in use, the media eventually stop being used and the job runs.

Table 2-1 NetBackup job delays *(continued)*

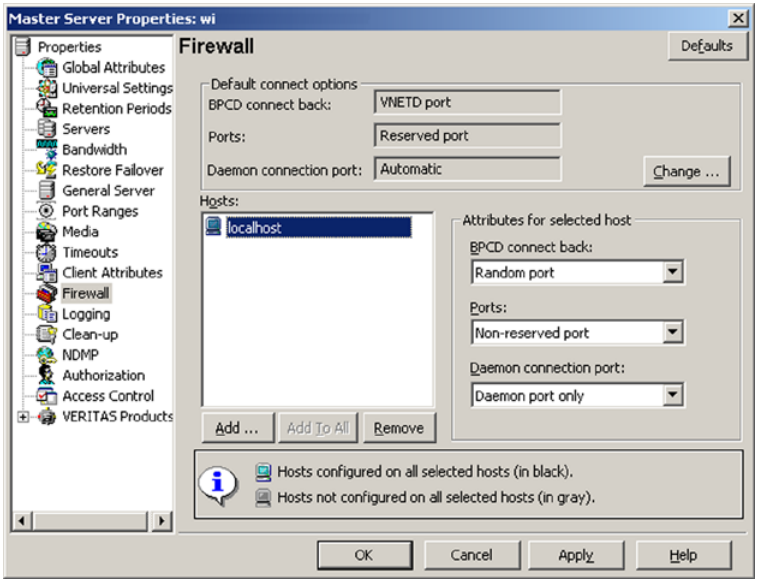
Type of job delay	Explanation and remedy (if any)
Job delays after removing a media server	A job may be queued by the NetBackup Job Manager (nbjm) if the media server is not available. The job is not queued because of communication timeouts, but because EMM knows the media server is down and the NetBackup Resource Broker (nbrb) queues the request to be retried later. If no other media servers are available, EMM queues the job under the following circumstances: ■ If a media server is configured in EMM but the server has been physically removed, turned off, or disconnected from the network ■ If the network is down The Activity Monitor should display the reason for the job queuing, such as "media server is offline." Once the media server is online again in EMM, the job starts. In the meantime, if other media servers are available, the job runs on another media server. If a media server is not configured in EMM, regardless of the physical state of the media server, EMM does not select that media server for use. If no other media servers are available, the job fails. To permanently remove a media server from the system, consult the "Decommissioning a media server" section in the *NetBackup Administrator's Guide, Volume II.*

Adjusting the server's network connection options

When many jobs run simultaneously, the CPU utilization of the master server may become very high. To reduce utilization and improve performance, adjust the network connection options for the local computer.

To adjust the network connection options for the local computer

1 In the NetBackup Administration Console, use the **Host Properties > Master Server > Master Server Properties > Firewall** dialog box.



2 Or add the following bp.conf entry to the UNIX master server:

```
CONNECT_OPTIONS = localhost 1 0 2
```

This entry only affects connections to NetBackup 7.0 and earlier. For an explanation of the CONNECT_OPTIONS values, refer to the *NetBackup Administrator's Guide for UNIX and Linux, Volume II*.

For connections to NetBackup 7.0.1 and later, use the veritas_pbx port. For information, refer to the Port security chapter of the *NetBackup Security and Encryption Guide*.

The *NetBackup Troubleshooting Guide* provides information on network connectivity issues.

About using OpsCenter to monitor jobs

Symantec OpsCenter can monitor the performance of NetBackup jobs. It can also manage and monitor dozens of NetBackup installations in multiple locations.

For more information on using OpsCenter to monitor jobs, refer to the *Symantec OpsCenter Administrator's Guide*.

Selection of storage units: performance considerations

Many different NetBackup mechanisms write backup images to storage devices, such as: backup policies, storage lifecycle policies, staging storage units, Vault duplication, and ad hoc (manual) duplication. When writing a backup image to storage, you can tell NetBackup how to select a storage unit or let NetBackup choose the storage unit.

Table 2-2 discusses the pros and cons of specifying a storage unit group versus allowing NetBackup to choose from a group (Any Available).

Note: The more narrowly defined the storage unit designation is, the faster NetBackup can assign a storage unit and the sooner the job starts.

Table 2-2 Performance considerations of Any Available vs. a specific storage unit group

Any Available	Storage unit groups
As a rule, the Any Available method should only be used in small, simple environments. For most backup operations, the default is to let NetBackup choose the storage unit (a storage destination of Any Available). Any Available may work well in small configurations that include relatively few storage units and media servers. However, Any Available is NOT recommended for the following: ■ Configurations with many storage units and media servers. Any Available is not recommended. ■ Configurations with disk technologies (such as AdvancedDisk, PureDisk, OpenStorage). With these newer disk technologies, Any Available causes NetBackup to analyze all options to choose the best one available. Any Available is not recommended. In general, if the configuration includes many storage units, many volumes within many disk pools, and many media servers, note: the deep analysis that Any Available requires can delay job initiation when many jobs (backup or duplication) are requested during busy periods of the day. Instead, specify a particular storage unit, or narrow NetBackup's search by means of storage unit groups (depending on how storage units and groups are defined). For more details on Any Available, see the *NetBackup Administrator's Guide, Volume I.* In addition, note the following about Any Available: ■ For Any Available, NetBackup operates in prioritized mode, as described in the next section. NetBackup selects the first available storage unit in the order in which they were originally defined. ■ Do not specify Any Available for multiple copies (Inline Copy) from a backup or from any method of duplication. The methods of duplication include Vault, staging disk storage units, lifecycle policies, or manual duplication through the Administration Console or command line. Instead, specify a particular storage unit.	A storage unit group is the preferred method for most large environments. It contains a specific list of storage units for NetBackup to choose from. Only these storage units are candidates for the job. You can configure a storage unit group to choose a storage unit in any of the following ways: ■ Prioritized Choose the first storage unit in the list that is not busy, down, or out of media. ■ Failover Choose the first storage unit in the list that is not down or out of media. ■ Round robin Choose the storage unit that is the least recently selected. ■ Media server load balancing NetBackup avoids sending jobs to busy media servers. This option is not available for the storage unit groups that contain a BasicDisk storage unit. You can use the New or Change Storage Unit Group dialog in the NetBackup Administration Console. NetBackup gives preference to a storage unit that a local media server can access. For more information, see the NetBackup online Help for storage unit groups, and the *NetBackup Administrator's Guide, Volume I.* **Note:** Regarding storage unit groups: the more narrowly defined your storage units and storage unit groups, the sooner NetBackup can select a resource to start a job. In complex environments with large numbers of jobs required, the following are good choices: ■ Fewer storage units per storage unit group. ■ Fewer media servers per storage unit. In the storage unit, avoid Any Available media server when drives are shared among multiple media servers. ■ Fewer disk volumes in a disk pool. ■ Fewer concurrent jobs. For example, less multiplexing, or fewer tape drives in each storage unit.

See "NetBackup job delays" on page 48.

About disk staging and NetBackup performance

Disk staging can increase backup speed. For more information, refer to the *NetBackup Administrator's Guide, Volume I.*

With disk staging, images can be created on disk initially, then copied later to another media type (as determined in the disk staging schedule). The media type for the final destination is typically tape, but can be disk. This two-stage process leverages the advantages of disk-based backups in the near term, while preserving the advantages of tape-based backups for long term.

You should consider disk staging in the following case:

- When the read speed of the source system is slow, and
- When the size of the backup is small. As a result, the time to mount, position, and dismount a tape is much longer than the time to back up.

About file system capacity and NetBackup performance

Ample file system space must exist for NetBackup to record its logging or catalog entries on each master server, media server, and client. If logging or catalog entries exhaust available file system space, NetBackup ceases to function.

Symantec recommends the following:

- You should be able to increase the size of the file system through volume management.
- The disk that contains the NetBackup master catalog should be protected with mirroring or RAID hardware or software technology.

About the NetBackup catalog

The NetBackup catalog resides on the disk of the NetBackup master server.

The catalog consists of the following parts:

Image database	The image database contains information about what has been backed up. It is by far the largest part of the catalog.

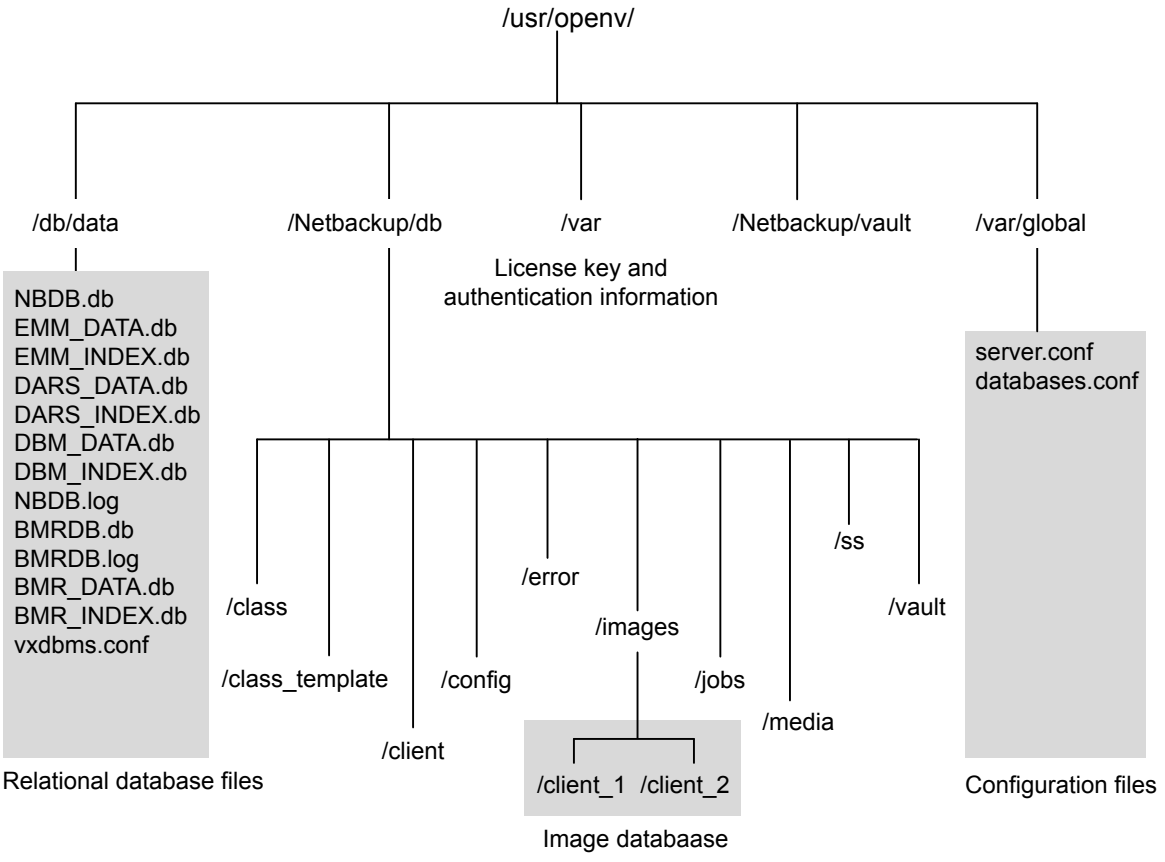
NetBackup data in relational databases	This data includes the media and volume data describing media usage and volume information that is used during the backups.
NetBackup configuration files	Policy, schedule, and other flat files that are used by NetBackup.

For more information on the catalog, refer to "Catalog Maintenance and Performance Optimization" in the *NetBackup Administrator's Guide Volume 1*.

The NetBackup catalogs on the master server tend to grow large over time and eventually fail to fit on a single tape.

Figure 2-1 shows the layout of the first few directory levels of the NetBackup catalogs on the master server.

Figure 2-1 Directory layout on the master server (UNIX)



Guidelines for managing the catalog

Consider the following:

- Back up the catalog
  Catalog backup can be performed while regular backup activity takes place. It is policy-based and can span more than one tape. It also allows for incremental backups, which can significantly reduce catalog backup times for large catalogs.

  Note: Symantec recommends schedule-based, incremental catalog backups with periodic full backups.

- Store the catalog on a separate file system (UNIX systems only)
  The NetBackup catalog can grow quickly depending on backup frequency, retention periods, and the number of files being backed up. With the NetBackup catalog data on its own file system, catalog growth does not affect other disk resources, root file systems, or the operating system.
  Information is available on how to move the catalog (UNIX systems only).
  See "Image database compression" on page 60.
  See "How to calculate the size of your NetBackup image database" on page 32.
- Change the location of the NetBackup relational database files
  The location of the NetBackup relational database files can be changed or split into multiple directories, for better performance. For example, by placing the transaction log file (NBDB.log) on a physically separate drive, you gain the following: better protection against disk failure, and increased efficiency in writing to the log file.
  Refer to the procedure in the "NetBackup relational database" appendix of the *NetBackup Administrator's Guide, Volume I*.
- Set a delay to compress the catalog
  The default value for this parameter is 0, which means that NetBackup does not compress the catalog. As your catalog increases in size, you may want to use a value between 10 and 30 days for this parameter. When you restore old backups, NetBackup automatically uncompresses the files as needed, with minimal performance impact.
  See "Image database compression" on page 60.
- Adjust the batch size for sending metadata to the catalog
  This setting affects overall backup performance, not the performance of catalog backups.
  See "Adjusting the batch size for sending metadata to the NetBackup catalog" on page 58.
- Best practices for the catalog layout are available in the following Symantec document:
  http://www.symantec.com/docs/TECH144969

Adjusting the batch size for sending metadata to the NetBackup catalog

You can change the batch size that is used to send metadata to the NetBackup catalog during backups. Note also that NetBackup 7.1 added a setting to change the batch size for sending metadata to the catalog specifically for catalog backups.

A change to the batch size can help in the following cases:

- If backups fail because a query to add files to the catalog takes more than 10 minutes to complete.
  In this case, the backup job fails, and the bpbrm log contains a message that indicates a failed attempt to add files to the catalog. Note that the bpdbm log does not contain a similar message.
- To improve backup performance when the folders to back up contain a large number of files or subfolders.

To adjust the batch size for sending metadata to the catalog (NetBackup 7.x)

1. Create the following file:

   For FlashBackup-Windows policies (including NetBackup for VMware and Hyper-V):

   /usr/openv/netbackup/FBU_MAX_FILES_PER_ADD

   For all other policy types (including FlashBackup for UNIX):

   /usr/openv/netbackup/MAX_FILES_PER_ADD

2. In the file, enter a value for the number of metadata entries to be sent to the catalog in each batch. The allowed values are from 1 to 100,000.

   The default for FlashBackup-Windows is 95,000 entries per batch (FBU_MAX_FILES_PER_ADD). For all other policy types, the default is 5,000 entries per batch (MAX_FILES_PER_ADD).

   For FBU_MAX_FILES_PER_ADD, experiment with a number that is lower than the 95,000 default. A lower number may avoid a timeout that is caused by a packet that is too large.

   For MAX_FILES_PER_ADD, try a number that is larger than the 5,000 default. A larger number may improve backup performance, particularly when the connections between media servers and the master server are slow.

   The setting you enter affects only the backups that are initiated after you make this change.

   Note that the MAX_FILES_PER_ADD file also sets that batch size for catalog backups (policy type NBU-Catalog). In NetBackup 7.1 and later, you can use the CAT_BU_MAX_FILES_PER_ADD file to change the batch size for catalog backups independently of all other policy types. (See the next procedure.)

To adjust the batch size for sending metadata to the catalog for NBU-Catalog backups (NetBackup 7.1 and later)

1. Create the following file:

   /usr/openv/netbackup/CAT_BU_MAX_FILES_PER_ADD

2. In the file, enter a value for the number of metadata entries to be sent to the catalog in each batch, for catalog backups. The allowed values are from 1 to 100,000.

   The default is the maximum (100,000 entries per batch). Experiment with a lower value.

   Note that the setting in this file applies only to backups of the catalog, for NetBackup 7.1 and later. For other policy types, use the FBU_MAX_FILES_PER_ADD and MAX_FILES_PER_ADD files as explained in the previous procedure.

Catalog archiving

If catalog backups run too long, consider the use of catalog archiving.

Catalog archiving reduces the size of online catalog data by relocating the large catalog .f files to secondary storage. NetBackup administration continues to require regularly scheduled catalog backups, but without the large amount of catalog data, the backups are faster.

For more information on archiving the catalog, refer to the *NetBackup Administrator's Guide, Volume I*.

Image database compression

When the image database portion of the catalog becomes too large for the available disk space, you can do either of the following:

- Compress the image database
- Move the image database

For details, refer to "Moving the image catalog" and "About image catalog compression" in the *NetBackup Administrator's Guide, Volume I*.

See "About the NetBackup catalog" on page 55.

Note that NetBackup compresses the image database after each backup session, regardless of whether any backups were successful. The compression happens right before the execution of the session_notify script and the backup of the image database. The actual backup session is extended until compression is complete.

About merging, splitting, or moving servers

The master server schedules and maintains backup information for a given set of systems. The Enterprise Media Manager (EMM) and its database maintain centralized device and media-related information for all servers that are part of the configuration. By default, the EMM server and the NetBackup Relational Database (NBDB) that contains the EMM data are located on the master server.

To further centralize backup management, it is possible to have two master servers or EMM servers merged into one server. On the other hand, it is possible to split an existing server into two separate servers, for better load management. Another possibility is to have a media server converted to a master server or a master server to a media server.

Note: The procedures to merge, split, or convert servers are complex and may only be appropriate as a last resort. They require a detailed knowledge of NetBackup database interactions. Such procedures require the assistance of a Symantec consulting partner.

Performance guidelines for NetBackup policies

The following policy items may have performance implications.

Table 2-3

Policy items	Guidelines
Include and exclude lists	Consider the following: ■ Do not use excessive wild cards in file lists. When wildcards are used, NetBackup compares every file name against the wild cards. This decreases NetBackup performance. Instead of placing `/tmp/*` (UNIX) or `C:\Temp\*` (Windows) in an include or exclude list, use `/tmp/` or `C:\Temp`. ■ Use exclude lists to exclude large unwanted files. Reduce the size of your backups by using exclude lists for the files your installation does not need to preserve. For instance, you may decide to exclude temporary files. Use absolute paths for your exclude list entries, so that valuable files are not inadvertently excluded. Before adding files to the exclude list, confirm with the affected users that their files can be safely excluded. Should disaster (or user error) strike, not being able to recover files costs much more than backing up extra data. When a policy specifies that all local drives be backed up (ALL_LOCAL_DRIVES), nbpem initiates a parent job (nbgenjob). nbgenjob connects to the client and runs `bpmount -I` to get a list of mount points. Then nbpem initiates a job with its own unique job identification number for each mount point. Next the client `bpbkar` starts a stream for each job. Only then does Netbackup read the exclude list. When the entire job is excluded, `bpbkar` exits with status 0, stating that it sent 0 of 0 files to back up. The resulting image files are treated the same as the images from any other successful backup. The images expire in the normal fashion when the expiration date in the image header files specifies they are to expire. ■ Use exclude lists to exclude files from regular backups if the files are already backed up by a NetBackup database agent backup.
Critical policies	For catalog backups, identify the policies that are crucial to recovering your site in the event of a disaster. For more information on catalog backup and critical policies, refer to the *NetBackup Administrator's Guide, Volume I*. See "Guidelines for managing the catalog" on page 57.
Schedule frequency	Minimize how often you back up the files that have not changed, and minimize your consumption of bandwidth, media, and other resources. To do so, limit full backups to monthly or quarterly, followed by weekly cumulative incremental backups and daily incremental backups.

How to optimize the performance of vxlogview

The vxlogview command is used for viewing logs created by unified logging (VxUL). The vxlogview command displays log messages faster when you use the -I option to specify a log file ID.

For example:

```
vxlogview -I nbrb -n 0
```

In this example, `-I nbrb` specifies the file ID for the NetBackup Resource Broker process (originator ID 118). vxlogview searches only the log files that were created by nbrb. That is, it searches only the files that contain 118 as the originator ID in the log file name. By limiting the log files that it has to search, vxlogview can return a result faster.

Note: The `-I` option works only for NetBackup processes that create unified log files with an originator ID in the file name. Such processes are referred to as services. The following is an example of such a log file name:

UNIX:

```
/usr/openv/logs/51216-118-2201360136-041029-0000000000.log
```

Windows:

```
install_path\logs\51216-118-2201360136-041029-0000000000.log
```

where `-118-` is the originator ID of nbrb.

As a rule, a NetBackup process is a service if it appears in the Activity Monitor of the NetBackup Administration Console, under the Daemons tab (UNIX) or Services tab (Windows).

Important note: If the process named on the `vxlogview -I` option is not a service (does not write log files with an originator ID in the file name), vxlogview returns "No log files found." In that case, use the -o option instead of -I. For example:

```
vxlogview -o mds -n 0
```

In this example, vxlogview searches all unified log files for messages logged by mds (the EMM Media and Device Selection component).

More vxlogview examples are available in the *NetBackup Troubleshooting Guide*.

Legacy error log fields

This section describes the fields in the legacy log files that are written to the following locations:

UNIX

```
/usr/openv/netbackup/db/error
```

Windows

```
install_path\NetBackup\db\error
```

On UNIX, there is a link to the most current file in the error directory. The link is called `daily_messages.log`.

The information in these logs provides the basis for the NetBackup ALL LOG ENTRIES report. For more information on legacy logging and unified logging (VxUL), refer to the *NetBackup Troubleshooting Guide*.

Here is a sample message from an error log:

```
1021419793 1 2 4 nabob 0 0 0 *NULL* bpjobd TERMINATED bpjobd
```

Table 2-4 defines the various fields in this message (the fields are delimited by blanks).

Table 2-4 Meaning of daily_messages log fields

Field	Definition	Value
1	Time this event occurred (ctime)	1021419793 (= number of seconds since 1970)
2	Error database entry version	1
3	Type of message	2
4	Severity of error: 1: Unknown 2: Debug 4: Informational 8: Warning 16: Error 32: Critical	4
5	Server on which error was reported	nabob
6	Job ID (included if pertinent to the log entry)	0
7	(optional entry)	0
8	(optional entry)	0
9	Client on which error occurred, if applicable. Otherwise *NULL*	*NULL*
10	Process which generated the error message	bpjobd

Table 2-4 Meaning of daily_messages log fields *(continued)*

Field	Definition	Value
11	Text of error message	TERMINATED bpjobd

Table 2-5 lists the values for the message type, which is the third field in the log message.

Table 2-5 Message types

Type Value	Definition of this message type
1	Unknown
2	General
4	Backup
8	Archive
16	Retrieve
32	Security
64	Backup status
128	Media device

Chapter 3

Media server configuration guidelines

This chapter includes the following topics:

Network and SCSI/FC bus bandwidth

Configure the number of tape drives that the Fibre Channel connection can support. Keep in mind the amount of data that is pushed to the media server from the clients. Tape drive wear and tear are much reduced and efficiency is increased if the data stream matches the tape drive capacity and is sustained.

Note: Make sure that both your inbound network connection and your SCSI/FC bus have enough bandwidth to feed all of your tape drives.

Example:

iSCSI (360 GB/hour)

Two LTO gen 3 drives, each rated at approximately 300 GB/hour (2:1 compression)

In this example, the tape drives require more speed than provided by the iSCSI bus. In this configuration, only one tape drive streams. Add a second iSCSI bus, or move to a connection that is fast enough to efficiently feed data to the tape drives.

Further information is available on network bandwidth:

See "How to calculate the required data transfer rate for your network(s)" on page 28.

See "Tuning suggestions for the NetBackup data transfer path" on page 110.

NetBackup media not available

Some backup failures can occur because there is no media available. In that case, execute the following script and run the NetBackup Media List report to check the status of media:

UNIX

```
/usr/openv/netbackup/bin/goodies/available_media
```

Windows

```
install_path\NetBackup\bin\goodies\available_media
```

The NetBackup Media List report may show that some media is frozen and therefore cannot be used for backups.

I/O errors that recur can cause NetBackup to freeze media. The *NetBackup Troubleshooting Guide* describes how to deal with this issue. For example, see under NetBackup error code 96.

You can also configure the NetBackup error threshold value.

About the threshold for media errors

Each time a read, write, or position error occurs, NetBackup records the time, media ID, type of error, and drive index in the EMM database. Then NetBackup scans to see whether that media has had "m" of the same errors within the past "n" hours. The variable "m" is a tunable parameter known as the media_error_threshold. The default value of media_error_threshold is 2 errors. The variable "n" is the time_window parameter (default 12 hours).

If a tape volume has more than media_error_threshold errors, NetBackup takes the appropriate action.

Table 3-1 If number of tape volume errors exceeds media_error_threshold

Situation	NetBackup action
If the volume has not been previously assigned for backups	NetBackup does the following: ■ Sets the volume status to FROZEN ■ Selects a different volume ■ Logs an error
If the volume is in the NetBackup media catalog and was previously selected for backups	NetBackup does the following: ■ Sets the volume to SUSPENDED ■ Aborts the current backup ■ Logs an error

Adjusting the media_error_threshold

You can adjust the NetBackup media error threshold as follows.

To adjust the NetBackup media error thresholds

◆ Use the `nbemmcmd` command on the media server:

UNIX

```
/usr/openv/netbackup/bin/admincmd/nbemmcmd -changesetting
-time_window unsigned integer -machinename string
-media_error_threshold unsigned integer -drive_error_threshold
unsigned integer
```

Windows

```
install_path\NetBackup\bin\admincmd\nbemmcmd.exe -changesetting
-time_window unsigned integer -machinename string
-media_error_threshold unsigned integer -drive_error_threshold
unsigned integer
```

For example, if the `-drive_error_threshold` is set to the default value of 2, the drive is downed after 3 errors in 12 hours. If the `-drive_error_threshold` is set to 6, it takes 7 errors in the same 12 hour period before the drive is downed.

NetBackup freezes a tape volume or downs a drive for which these values are exceeded. For more detail on the `nbemmcmd` command, refer to the man page or to the *NetBackup Commands Guide*.

About tape I/O error handling

Note: This topic has nothing to do with the number of times NetBackup retries a backup or restore that fails. That situation is controlled by the global configuration parameter "Backup Tries" for backups and the bp.conf entry RESTORE_RETRIES for restores.

The algorithm described here determines whether I/O errors on tape should cause media to be frozen or drives to be downed.

When a read/write/position error occurs on tape, the error returned by the operating system does not identify whether the tape or drive caused the error. To prevent the failure of all backups in a given time frame, bptm tries to identify a bad tape volume or drive based on past history.

To do so, bptm uses the following logic:

- Each time an I/O error occurs on a read/write/position, bptm logs the error in the following file.
  UNIX

  ```
  /usr/openv/netbackup/db/media/errors
  ```

  Windows

  ```
  install_path\NetBackup\db\media\errors
  ```

  The error message includes the time of the error, media ID, drive index, and type of error. Examples of the entries in this file are the following:

  ```
  07/21/96 04:15:17 A00167 4 WRITE_ERROR
  07/26/96 12:37:47 A00168 4 READ_ERROR
  ```

- Each time an entry is made, the past entries are scanned. The scan determines whether the same media ID or drive has had this type of error in the past "n" hours. "n" is known as the time_window. The default time window is 12 hours. During the history search for the time_window entries, EMM notes the past errors that match the media ID, the drive, or both. The purpose is to determine the cause of the error. For example: if a media ID gets write errors on more than one drive, the tape volume may be bad and NetBackup freezes the volume. If more than one media ID gets a particular error on the same drive, the drive goes to a "down" state. If only past errors are found on the same drive with the same media ID, EMM assumes that the volume is bad and freezes it.
- The freeze or down operation is not performed on the first error.

Note two other parameters: media_error_threshold and drive_error_threshold. For both of these parameters the default is 2. For a freeze or down to happen, more than the threshold number of errors must occur. By default, at least three errors must occur in the time window for the same drive or media ID.

If either media_error_threshold or drive_error_threshold is 0, a freeze or down occurs the first time an I/O error occurs. media_error_threshold is looked at first, so if both values are 0, a freeze overrides a down. Symantec does not recommend that these values be set to 0.

A change to the default values is not recommended without good reason. One obvious change would be to put very large numbers in the threshold files. Large numbers in that file would disable the mechanism, such that to "freeze" a tape or "down" a drive should never occur.

Freezing and downing is primarily intended to benefit backups. If read errors occur on a restore, a freeze of media has little effect. NetBackup still accesses the tape to perform the restore. In the restore case, downing a bad drive may help.

For further tuning information on tape backup, see the following topics:

See "About the threshold for media errors" on page 68.

See "How to calculate the time required to back up to tape" on page 23.

See "How to calculate the required number of tape drives" on page 26.

See "How to calculate the media needed for full and incremental backups" on page 36.

See "How to calculate the size of the tape library needed to store your backups" on page 38.

Reloading the st driver without restarting Solaris

The devfsadmd daemon enhances device management in Solaris. This daemon can dynamically reconfigure devices during the boot process and in response to kernel event notification.

The devfsadm that is located in `/usr/sbin` is the command form of devfsadmd. devfsadm replaces drvconfig (for management of physical device tree `/devices`) and devlinks (for management of logical devices in `/dev`). devfsadm also replaces the commands for specific device class types, such as `/usr/sbin/tapes`.

Without restarting the server, you can recreate tape devices for NetBackup after changing the `/kernel/drv/st.conf` file. Do the following.

To reload the st driver without restarting

1. Turn off the NetBackup and Media Manager daemons.
2. Obtain the module ID for the st driver in kernel:

   ```
   /usr/sbin/modinfo | grep SCSI
   ```

   The module ID is the first field in the line that corresponds to the SCSI tape driver.
3. Unload the st driver from the kernel:

   ```
   /usr/sbin/modunload -I "module id"
   ```

4. Run one (not all) of the following commands:

   ```
   /usr/sbin/devfsadm -I st

   /usr/sbin/devfsadm -c tape

   /usr/sbin/devfsadm -C -c tape
   ```

   Use the last command to enforce cleanup if dangling logical links are present in `/dev`.

   The devfsadm command recreates the device nodes in `/devices` and the device links in `/dev` for tape devices.
5. Reload the st driver:

   ```
   /usr/sbin/modload st
   ```

6. Restart the NetBackup and Media Manager daemons.

About NetBackup Media Manager drive selection

When NetBackup EMM determines which storage unit to use, it attempts to select a drive that matches the storage unit selection criteria. The criteria, for example, may be media server, robot number, robot type, or density.

Note the following:

- EMM prefers loaded drives over unloaded drives (a loaded drive removes the overhead of loading a media in a drive).
- If no loaded drives are available, EMM attempts to select the best usable drive that is suited for the job.

- In general, EMM prefers non-shared drives over shared drives, and it attempts to select the least recently used drive.

Chapter 4

Media configuration guidelines

This chapter includes the following topics:

About dedicated versus shared backup environments

Your backup environment can be dedicated or shared.

Note the following:

- Dedicated SANs are secure but expensive.
- Shared environments cost less, but require more work to make them secure.
- A SAN installation with a database may require the performance of a RAID 1 array. An installation backing up a file structure may satisfy its needs with RAID 5 or NAS.

Suggestions for NetBackup media pools

The following are good practices for media pools (formerly known as volume pools):

- Configure a scratch pool for management of scratch tapes. If a scratch pool exists, EMM can move volumes from that pool to other pools that do not have volumes available.
- Use the available_media script in the goodies directory. You can put the available_media report into a script. The script redirects the report output to a file and emails the file to the administrators daily or weekly. The script helps track the tapes that are full, frozen, suspended, and so on. By means of a script, you can also filter the output of the available_media report to generate custom reports.

  To monitor media, you can also use the Symantec OpsCenter. For instance, OpsCenter can issue an alert based on the number of media available or the percent of media that are frozen or suspended.
- Use the none pool for cleaning tapes.
- Do not create more pools than you need. In most cases, you need only 6 to 8 pools. The pools include a global scratch pool, catalog backup pool, and the default pools that are created by the installation. The existence of too many pools causes the library capacity to become fragmented across the pools. Consequently, the library becomes filled with many tapes that are partially full.

Disk versus tape: performance considerations

Disk is now a common backup medium. Backup data on disk generally provides faster restores.

Tuning disk-based storage for performance is similar to tuning tape-based storage. The optimal buffer settings for a site can vary according to its configuration. It takes thorough testing to determine these settings.

Disk-based storage can be useful if you have a lot of incremental backups and the percentage of data change is small. If the volume of data in incremental copies is insufficient to ensure efficient writing to tape, consider disk storage. After writing the data to disk, you can use staging or storage lifecycle policies to copy batches of the images to tape. This arrangement can produce faster backups and prevent wear and tear on your tape drives.

Consider the following factors when backing up a dataset to disk or tape:

- Short or long retention period

  Disk is well suited for short retention periods; tape is better suited for longer retention periods.
- Intermediate (staging) or long-term storage

  Disk is suited for staging; tape for long-term storage.

- Incremental or full backup
  Disk is better suited to low volume incremental backups.
- Synthetic backups
  Synthetic full backups are faster when incremental backups are stored on disk.
- Data recovery time
  Restore from disk is usually faster than from tape.
- Multi-streamed restore
  Must a restore of the data be multi-streamed from tape? If so, do not stage the multi-streamed backup to disk before writing it to tape.
- Speed of the backups
  If client backups are too slow to keep the tape in motion, send the backups to disk. Later, staging or lifecycle policies can move the backup images to tape.
- Size of the backups
  If the backups are too small to keep the tape in motion, send the backups to disk. Small backups may include incrementals and frequent backups of small database log files. Staging or lifecycle policies can later move the backup images to tape.

The following are some benefits of backing up to disk rather than tape:

- No need to multiplex
  Backups to disk do not need to be multiplexed. Multiplexing is important with tape because it creates a steady flow of data which keeps the tape in motion efficiently (tape streaming). However, multiplexing to tape slows down a subsequent restore.
  More information is available on tape streaming.
  See "NetBackup storage device performance in the data transfer path" on page 157.
- Instant access to data
  Most tape drives have a "time to data" of close to two minutes. Time is required to move the tape from its slot, load it into the drive, and seek to an appropriate place on the tape. Disk has an effective time to data of 0 seconds. Restoring a large file system from 30 different tapes can add almost two hours to the restore: a two-minute delay per tape for load and seek, and a possible two-minute delay per tape for rewind and unload.
- Fewer full backups
  With tape-based systems, full backups must be done regularly because of the "time to data" issue. If full backups are not done regularly, a restore may require too many tapes from incremental backups. As a result, the time to restore increases, as does the chance that a single tape may cause the restore to fail.

Information on NetBackup deduplication

The following tech note supplements the NetBackup Deduplication Guide. It contains information that was not available when NetBackup 7.0.1 was released. Some of the sections in the tech note may be updates of sections in the NetBackup Deduplication Guide.

The tech note is titled *NetBackup Deduplication: Additional Usage Information*:

http://www.symantec.com/docs/TECH77575

Chapter 5

Best practices

This chapter includes the following topics:

Best practices: NetBackup SAN Client

The NetBackup SAN Client feature is designed for a computer that has the following characteristics:

- Contains critical data that requires high bandwidth for backups
- Is not a candidate for converting to a media server

A SAN Client performs a fast backup over a Fibre Channel SAN to a media server. Media servers that have been enabled for SAN Client backups are called Fibre Transport Media Servers.

Note: The FlashBackup option should not be used with SAN Clients. Restores of FlashBackup backups use the LAN path rather than the SAN path from media server to the client. The LAN may not be fast enough to handle a full volume (raw partition) restore of a FlashBackup backup.

A Symantec technote contains information on SAN Client performance parameters and best practices:

http://www.symantec.com/docs/TECH54778

The main point of the technote is the following: that effective use of a SAN Client depends on the proper configuration of the correct hardware. (Refer to the technote for in-depth details.)

In brief, the technote contains the following information:

- A list of the HBAs that NetBackup supports.
  Further information is available on supported hardware.
  See the NetBackup 7.x hardware compatibility list:
  http://www.symantec.com/docs/TECH76495
- Tips on how to deploy a Fibre Channel SAN between the SAN Client and the Fibre Transport Media Server.
- A list of supported operating systems and HBAs for the Fibre Transport Media Server. Also a list of tuning parameters that affect the media server performance.
- A similar list of supported operating systems and tuning parameters for the SAN Client.
- A description of recommended architectures as a set of best practices

  The document describes the following best practices:

  - To make best use of high-speed disk storage, or to manage a pool of SAN Clients for maximum backup speed: dedicate Fibre Transport Media Servers for SAN Client backup only. Do not share media servers for LAN-based backups.
  - For a more cost-effective use of media servers, Fibre Transport Media Servers can be shared for both SAN Client and LAN-based backups.
  - Use multiple data streams for higher data transfer speed from the SAN Client to the Fibre Transport Media Server. Multiple data streams can be combined with multiple HBA ports on the Fibre Transport Media Server. The maximum number of simultaneous connections to the Fibre Transport Media Server is 32.

Further information is available on SAN Client.

See the *NetBackup SAN Client and Fibre Transport Troubleshooting Guide*:

http://www.symantec.com/docs/TECH51454

See the following for related information on network data transfer rates:

See "How to calculate the required data transfer rate for your backups" on page 22.

Best practices: NetBackup AdvancedDisk

With AdvancedDisk, NetBackup can fully use file systems native to the host operating system of the media server. NetBackup assumes full ownership of the file systems and also uses the storage server capabilities of the host operating system.

AdvancedDisk does not require any specialized hardware. AdvancedDisk disk types are managed as disk pools within NetBackup.

The following Symantec tech note provides performance considerations and best practices for AdvancedDisk:

http://www.symantec.com/docs/TECH158427

Best practices: New tape drive technologies for NetBackup

Symantec provides a white paper on best practices for migrating your NetBackup installation to new tape technologies:

NetBackup best practices guide on migrating to or integrating new tape drive technologies in existing libraries

http://www.symantec.com/docs/TECH45857

Recent tape drives offer noticeably higher capacity than the previous generation of tape drives that are targeted at the open-systems market. Administrators may want to take advantage of these higher-capacity, higher performance tape drives, but are concerned about how to integrate these into an existing tape library. The white paper discusses different methods for doing so and the pros and cons of each.

Best practices: NetBackup tape drive cleaning

You can use the following tape drive cleaning methods in a NetBackup installation:

- Frequency-based cleaning

- TapeAlert (on-demand cleaning)
- Robotic cleaning

Refer to the *NetBackup Administrator's Guide, Volume II*, for details on how to use these methods. Following are brief summaries of each method.

Table 5-1 describes the three tape drive cleaning methods.

Table 5-1 Tape drive cleaning methods

Tape drive cleaning method	Description
Frequency-based cleaning	NetBackup does frequency-based cleaning by tracking the number of hours a drive has been in use. When this time reaches a configurable parameter, NetBackup creates a job that mounts and exercises a cleaning tape. This practice cleans the drive in a preventive fashion. The advantage of this method is that typically no drives are unavailable awaiting cleaning. No limitation exists as to the platform type or robot type. On the downside, cleaning is done more often than necessary. Frequency-based cleaning adds system wear and takes time that can be used to write to the drive. This method is also hard to tune. When new tapes are used, drive cleaning is needed less frequently; the need for cleaning increases as the tape inventory ages. This increases the amount of tuning administration that is needed and, consequently, the margin of error.
TapeAlert (reactive cleaning, or on-demand cleaning)	TapeAlert (on-demand cleaning) allows reactive cleaning for most drive types. TapeAlert allows a tape drive to notify EMM when it needs to be cleaned. EMM then performs the cleaning. You must have a cleaning tape configured in at least one library slot to use this feature. TapeAlert is the recommended cleaning solution if it can be implemented. Certain drives at some firmware levels do not support this type of reactive cleaning. If reactive cleaning is not supported, frequency-based cleaning may be substituted. This solution is not vendor or platform specific. Symantec has not tested the specific firmware levels. The vendor should be able to confirm whether the TapeAlert feature is supported. See "How NetBackup TapeAlert works" on page 83. See "Disabling TapeAlert" on page 84.

Table 5-1 Tape drive cleaning methods *(continued)*

Tape drive cleaning method	Description
Robotic cleaning	Robotic cleaning is not proactive, and is not subject to the limitations of the other drive cleaning methods. Unnecessary cleanings are eliminated, and frequency tuning is not an issue. The drive can spend more time moving data, rather than in maintenance operations. NetBackup EMM does not support library-based cleaning for most robots, because robotic library and operating systems vendors implement this type of cleaning in different ways.

How NetBackup TapeAlert works

To understand drive-cleaning TapeAlerts, it is important to understand the TapeAlert interface to a drive. The TapeAlert interface to a tape drive is by means of the SCSI bus. The interface is based on a Log Sense page, which contains 64 alert flags. The conditions that cause a flag to be set and cleared are device-specific and device-vendor specific.

The configuration of the Log Sense page is by means of a Mode Select page. The Mode Sense/Select configuration of the TapeAlert interface is compatible with the SMART diagnostic standard for disk drives.

NetBackup reads the TapeAlert Log Sense page at the beginning and end of a write or read job. TapeAlert flags 20 to 25 are used for cleaning management, although some drive vendors' implementations vary. NetBackup uses TapeAlert flag 20 (Clean Now) and TapeAlert flag 21 (Clean Periodic) to determine when to clean a drive.

When NetBackup selects a drive for a backup, `bptm` reviews the Log Sense page for status. If one of the clean flags is set, the drive is cleaned before the job starts. If a backup is in progress and a clean flag is set, the flag is not read until a tape is dismounted from the drive.

If a job spans media and, during the first tape, one of the clean flags is set, the following occurs: the cleaning light comes on and the drive is cleaned before the second piece of media is mounted in the drive.

The implication is that the present job concludes its ongoing write despite a TapeAlert Clean Now or Clean Periodic message. That is, the TapeAlert does not require the loss of what has been written to tape so far. This is true regardless of the number of NetBackup jobs that are involved in writing out the rest of the media.

If a large number of media become FROZEN as a result of having implemented TapeAlert, other media or tape drive issues are likely to exist.

Disabling TapeAlert

Use the following procedure.

To disable TapeAlert in NetBackup

- Create a touch file called NO_TAPEALERT, as follows:

  UNIX:

  ```
  /usr/openv/volmgr/database/NO_TAPEALERT
  ```

  Windows:

  ```
  install_path\volmgr\database\NO_TAPEALERT
  ```

Best practices: NetBackup data recovery methods

Recovering from data loss involves both planning and technology to support your recovery objectives and time frames. You should document your methods and procedures and test them regularly to ensure that your installation can recover from a disaster.

Table 5-2 describes how you can use NetBackup and other tools to recover from various mishaps.

Table 5-2 Methods and procedures for data recovery

Operational risk	Recovery possible?	Recovery methods and procedures
File deleted before backup	No	None
File deleted after backup	Yes	Standard NetBackup restore procedures
Backup client failure	Yes	Data recovery using NetBackup
Media failure	Yes	Backup image duplication: create multiple backup copies
Media server failure	Yes	Recovery is usually automatic, by pre-configuring storage unit groups (for backup) and FAILOVER_RESTORE_MEDIA_SERVER (for restore from tape).

Table 5-2 Methods and procedures for data recovery *(continued)*

Operational risk	Recovery possible?	Recovery methods and procedures
Master server failure	Yes	Deploy the master server in a cluster, for automatic failover
Loss of backup database	Yes	NetBackup database recovery
No NetBackup software	Yes	If multiplexing was not used, recovery of media without NetBackup, using GNU tar
Complete site disaster	Yes	Vaulting and off site media storage

Additional material may be found in the following books:

The Resilient Enterprise, Recovering Information Services from Disasters, by Symantec and industry authors. Published by Symantec Software Corporation.

Blueprints for High Availability, Designing Resilient Distributed Systems, by Evan Marcus and Hal Stern. Published by John Wiley and Sons.

Implementing Backup and Recovery: The Readiness Guide for the Enterprise, by David B. Little and David A. Chapa. Published by Wiley Technology Publishing.

Best practices: Suggestions for disaster recovery planning

You should have a well-documented and tested plan to recover from a logical error, an operator error, or a site disaster.

See the following documents for more information on disaster recovery:

A Guide to Site Disaster Recovery Options

http://www.symantec.com/docs/TECH66060

NetBackup Troubleshooting Guide

NetBackup Administrator's Guide, Volumes I & II

NetBackup in Highly Available Environments Administrator's Guide

NetBackup Clustered Master Server Administrator's Guide

For recovery planning, use the following preparatory measures:

- Always use a scheduled catalog backup
  Refer to "Catalog Recovery from an Online Backup" in the *NetBackup Troubleshooting Guide*.

- Review the disaster recovery plan often
  Review your site-specific recovery procedures and verify that they are accurate and up-to-date. Also, verify that the more complex systems, such as the NetBackup master and media servers, have procedures for rebuilding the computers with the latest software.
- Perform test recoveries on a regular basis
  Implement a plan to perform restores of various systems to alternate locations. This plan should include selecting random production backups and restoring the data to a non-production system. A checksum can then be performed on one or many of the restored files and compared to the actual production data. Be sure to include off-site storage as part of this testing. The end-user or application administrator can also help determine the integrity of the restored data.
- Use and protect the NetBackup catalog

  Do the following:

  - Back up the NetBackup catalog to two tapes.
    The catalog contains information vital for NetBackup recovery. Its loss can result in hours or days of recovery time using manual processes. The cost of a single tape is a small price to pay for the added insurance of rapid recovery in the event of an emergency.
  - Back up the catalog after each backup.
    If a catalog backup is used, an incremental catalog backup can be done after each backup session. Busy backup environments should also use a scheduled catalog backup, because their backup sessions end infrequently.
    In the event of a catastrophic failure, the recovery of images is slow if some images are not available. If a manual backup occurs shortly before the master server or the drive that contains the backed-up files crashes, note: the manual backup must be imported to recover the most recent version of the files.
  - Record the IDs of catalog backup tapes.
    Record the catalog tapes in the site run book or another public location to ensure rapid identification in the event of an emergency. If the catalog tapes are not identified, time may be lost by scanning every tape in a library to find them.
    The utility `vmphyinv` can be used to mount all tapes in a robotic library and identify the catalog tape(s).
  - Designate label prefixes for catalog backups.

Make it easy to identify the NetBackup catalog data in times of emergency. Label the catalog tapes with a unique prefix such as "DB" on the tape bar code, so your operators can find the catalog tapes without delay.

- Place NetBackup catalogs in specific robot slots.
  Place a catalog backup tape in the first or last slot of a robot to identify the tape in an emergency. This practice also allows for easy tape movement if manual tape handling is necessary.
- Put the NetBackup catalog on different online storage than the data being backed up.
  Your catalogs should not reside on the same disks as production data. If a disk drive loses production data, it can also lose any catalog data that resides on it, resulting in increased downtime.
- Regularly confirm the integrity of the NetBackup catalog.
  On a regular basis, such as quarterly or after major operations or personnel changes, walk through the process of recovering a catalog from tape. This essential part of NetBackup administration can save hours in the event of a catastrophe.

Best practices: NetBackup naming conventions

Use a consistent name convention on all NetBackup master servers. Use lower case for all names. Case-related issues can occur when the installation comprises UNIX and Windows master and media servers.

Table 5-3

Object to name	Guidelines for naming
Policy	One good naming convention for policies is platform_datatype_server(s). Example 1: w2k_filesystems_trundle This policy name designates a policy for a single Windows server doing file system backups. Example 2: w2k_sql_servers This policy name designates a policy for backing up a set of Windows 2000 SQL servers. Several servers may be backed up by this policy. Servers that are candidates for being included in a single policy are those running the same operating system and with the same backup requirements. Grouping servers within a single policy reduces the number of policies and eases the management of NetBackup.

Table 5-3 *(continued)*

Object to name	Guidelines for naming
Schedule	Create a generic scheme for schedule names. One recommended set of schedule names is daily, weekly, and monthly. Another recommended set of names is incremental, cumulative, and full. This convention keeps the management of NetBackup at a minimum. It also helps with the implementation of Vault, if your site uses Vault.
Storage unit and storage group	A good naming convention for storage units is to name the storage unit after the media server and the type of data being backed up. Two examples: `mercury_filesystems and mercury_databases` where "mercury" is the name of the media server, and "filesystems" and "databases" identify the type of data being backed up.

Best practices: NetBackup duplication

Note the following about NetBackup image duplication:

- When duplicating an image, specify a volume pool that is different from the volume pool of the original image. (Use the Setup Duplication Variables dialog of the NetBackup Administration Console.)
- If multiple duplication jobs are active simultaneously (such as duplication jobs for Vault), specify a different storage unit or volume pool for each job. Using different destinations may prevent media swapping among the duplication jobs.
- NetBackup provides the bpduplicate command to run and script duplication jobs. Symantec, however, recommends using either Storage Lifecycle Policies or the Vault option when implementing duplication as part of a backup strategy.
  See the following document for more information:
  Best practices for using Storage Lifecycle Policies and Auto Image Replication in NetBackup 7.1
  http://www.symantec.com/docs/TECH153154

Information on related topics is available.

Section 2

Performance tuning

Chapter 6

Measuring performance

This chapter includes the following topics:

Measuring NetBackup performance: overview

The final measure of NetBackup performance is the following:

- The length of time that is required for backup operations to complete (usually known as the backup window).
- The length of time that is required for a critical restore operation to complete.

However, to measure and improve performance calls for performance metrics more reliable and reproducible than wall clock time. This chapter discusses these metrics in more detail.

After establishing accurate metrics as described here, you can measure the current performance of NetBackup and your system components to compile a baseline performance benchmark. With a baseline, you can apply changes in a controlled

way. By measuring performance after each change, you can accurately measure the effect of each change on NetBackup performance.

How to control system variables for consistent testing conditions

For reliable performance evaluation, eliminate as many unpredictable variables as possible to create a consistent backup environment. Only a consistent environment can produce reliable and reproducible performance measurements. This topic explains some of the variables to consider as they relate to the NetBackup server, the network, the NetBackup client, or the data itself.

Table 6-1 System variables to control for testing

Variables	Considerations for controlling
Server variables	Eliminate all other NetBackup activity from your environment when you measure the performance of a particular NetBackup operation. One area to consider is the automatic scheduling of backup jobs by the NetBackup scheduler. When policies are created, they are usually set up to allow the NetBackup scheduler to initiate the backups. The NetBackup scheduler initiates backups according to the following: traditional NetBackup frequency-based scheduling, or on certain days of the week, month, or other time interval. This process is called calendar-based scheduling. As part of the backup policy, the **Start Window** indicates when the NetBackup scheduler can start backups using either frequency-based or calendar-based scheduling. When you perform backups to test performance, this scheduling might interfere. The NetBackup scheduler may initiate backups unexpectedly, especially if the operations you intend to measure run for an extended period of time. See "Running a performance test without interference from other jobs" on page 94.
Network variables	Network performance is key to optimum performance with NetBackup. Ideally, you should use a separate network for testing, to prevent unrelated network activity from skewing the results. In many cases, a separate network is not available. If not, ensure that non-NetBackup activity is kept to a minimum during the test. If possible, schedule the test when backups are not active. Even occasional bursts of network activity may be enough to skew the test results. If you share the network with production backups occurring for other systems, you must account for this activity during the test. Another network variable is host name resolution. NetBackup depends heavily upon a timely resolution of host names to operate correctly. If you have any delays in host name resolution, try to eliminate that delay. An example of such a delay is a reverse name lookup to identify a server name from an incoming connection from an IP address. You can use the `HOSTS` (Windows) or `/etc/hosts` (UNIX) file for host name resolution on systems in your test environment.

Table 6-1 System variables to control for testing *(continued)*

Variables	Considerations for controlling
Client variables	Make sure the client system is relatively quiescent during performance testing. A lot of activity, especially disk-intensive activity such as Windows virus scanning, can limit the data transfer rate and skew the test results. Do not allow another NetBackup server, such as a production server, to access the client during the test. NetBackup may attempt to back up the same client to two different servers at the same time. The results of a performance test that is in progress can be severely affected. Different file systems have different performance characteristics. It may not be valid to compare data throughput on UNIX VxFS or Windows FAT file systems to UNIX NFS or Windows NTFS systems. For such a comparison, factor the difference between the file systems into your performance tests and into any conclusions.

Table 6-1 System variables to control for testing *(continued)*

Variables	Considerations for controlling
Data variables	Monitoring the data you back up improves the repeatability of performance testing. If possible, move the data you use for testing to its own drive or logical partition (not a mirrored drive). Defragment the drive before you begin performance testing. For testing restores, start with an empty disk drive or a recently defragmented disk drive with ample empty space. For testing backups to tape, always start each test with an empty piece of media, as follows: ■ Expire existing images for that piece of media through the Catalog node of the NetBackup Administration Console, or run the `bpexpdate` command. ■ Another approach is to use the `bpmedia` command to freeze any media containing existing backup images so that NetBackup selects a new piece of media for the backup operation. This step reduce the impact of tape positioning on the performance test and yields more consistent results between tests. It also reduces mounting and unmounting of media that has NetBackup catalog images and that cannot be used for normal backups. When you test restores from tape, always restore from the same backup image on the tape to achieve consistent results between tests. A large set of data generates a more reliable, reproducible test than a small set of data. A performance test with a small data set would probably be skewed by startup and shutdown overhead within the NetBackup operation. These variables are difficult to keep consistent between test runs and are therefore likely to produce inconsistent test results. A large set of data minimizes the effect of startup and shutdown times. Design the dataset to represent the makeup of the data in the intended production environment. If the data set in the production environment contains many small files on file servers, the data set for the tests should also contain many small files. A representative data set can more accurately predict the NetBackup performance that can be expected in a production environment. The type of data can help reveal bottlenecks in the system. Files that contain non-compressible (random) data cause the tape drive to run at its lower rated speed. As long as the other components of the data transfer path can keep up, you can identify the tape drive as the bottleneck. On the other hand, files containing highly-compressible data can be processed at higher rates by the tape drive when hardware compression is enabled. The result may be a higher overall throughput and may expose the network as the bottleneck. Many values in NetBackup provide data amounts in kilobytes and rates in kilobytes per second. For greater accuracy, divide by 1024 rather than rounding off to 1000 when you convert from kilobytes to megabytes or kilobytes per second to megabytes per second.

Running a performance test without interference from other jobs

Use the following procedure to run a test. This procedure helps prevent the NetBackup scheduler from running other backups during the test.

To run a test

1. Create a policy specifically for performance testing.
2. Leave the schedule's **Start Window** field blank.

   This policy prevents the NetBackup scheduler from initiating any backups automatically for that policy.
3. To prevent the NetBackup scheduler from running backup jobs unrelated to the performance test, consider setting all other backup policies to inactive.

   You can use the **Deactivate** command from the NetBackup Administration Console. You must reactivate the policies after the test, when you want to start running backups again.
4. Before you start the performance test, check the Activity Monitor to make sure no NetBackup jobs are in progress.
5. To gather more logging information, set the legacy and unified logging levels higher and create the appropriate legacy logging directories.

   By default, NetBackup logging is set to a minimum level. Note that higher log levels may reduce performance, depending on the tests and the log levels.

   For details on how to use NetBackup logging, refer to the logging chapter of the *NetBackup Troubleshooting Guide*. Keep in mind that higher logging levels consume more disk space.
6. From the policy you created for testing, run a backup on demand.

   Click **Actions > Manual Backup** in the NetBackup Administration Console.

   Or, you can use a user-directed backup to run the performance test. However, the **Manual Backup** option is preferred. With a manual backup, the policy contains the entire definition of the backup job. The policy includes the clients and files that are part of the performance test. If you run the backup manually from the policy, you can be certain which policy is used for the backup. This approach makes it easier to change and test individual backup settings, from the policy dialog.
7. During the performance test, check for non-NetBackup activity on the server and try to reduce or eliminate it.
8. Check the NetBackup Activity Monitor after the performance test for any unexpected activity that may have occurred during the test, such as a restore job.

About evaluating NetBackup performance

You can obtain statistics on NetBackup data throughput from these tools:

- The NetBackup Activity Monitor
- The NetBackup All Log Entries report

Select the reporting tool according to the type of NetBackup operation you want to measure:

- Non-multiplexed backup
- Multiplexed backup
- Restore

Table 6-2 Where to obtain NetBackup performance statistics

Operation to report on	In Activity Monitor	In All Log Entries report
Non-multiplexed backup	Yes	Yes
Multiplexed backup	No (see next column)	Yes Obtain the overall statistics from the All Log Entries report. Wait until all the individual backup operations which are part of the multiplexed backup are complete. In this case, the statistics available in the Activity Monitor for each of the individual backup operations are relative only to that operation. The statistics do not reflect the total data throughput to the tape drive.
Restore	Yes	Yes

The statistics from these two tools may differ, because of differences in rounding techniques in the Activity Monitor versus the All Logs report. For a given type of operation, choose one of the tools and consistently record your statistics only from that tool. In both the Activity Monitor and the All Logs report, the data-streaming speed is reported in kilobytes per second. If a backup or restore is repeated, the reported speed can vary between repetitions depending on many factors. Factors include the availability of system resources and system utilization. The reported speed can be used to assess the performance of the data-streaming process.

The statistics from the NetBackup error logs show the actual amount of time reading and writing data to and from tape. The statistics do not include the time for mounting and positioning the tape. You should cross-reference the information from the error logs with data from the bpbkar log on the NetBackup client. (The bpbkar log shows the end-to-end elapsed time of the entire process.) Such cross references can indicate how much time was spent on operations unrelated to reading and writing tape.

Evaluating NetBackup performance through the Activity Monitor

To evaluate performance through the NetBackup Activity Monitor

1. Run the backup or restore job.
2. Open the NetBackup Activity Monitor.
3. Verify that the backup or restore completed successfully.

   The Status column should contain a zero (0).
4. View the log details for the job by selecting the **Actions > Details** menu option, or by double-clicking on the entry for the job.
5. Select the **Detailed Status** tab.
6. Obtain the NetBackup performance statistics from the following fields in the Activity Monitor:

Start Time/End Time	These fields show the time window during which the backup or restore job took place.
Elapsed Time	This field shows the total elapsed time from when the job was initiated to job completion. It can be used as an indication of total wall clock time for the operation.
KB per Second	The data throughput rate.
Kilobytes	Compare this value to the amount of data. Although it should be comparable, the NetBackup data amount is slightly higher because of administrative information (metadata) that is saved for the backed up data.

For example, if you display properties for a directory that contains 500 files, each 1 megabyte in size, the directory shows a size of 500 megabytes. (500 megabytes is 524,288,000 bytes, or 512,000 kilobytes.) The NetBackup report may show 513,255 kilobytes written, reporting 1255 kilobytes more than the file size of the directory. This report is true for a flat directory. Subdirectory structures may diverge due to the way the operating system tracks used and available space on the disk.

Note that the operating system may report how much space was allocated for the files in question, not only how much data is present. If the allocation block size is 1 kilobyte, 1000 1-byte files report a total size of 1 megabyte, although 1 kilobyte of data is all that exists. The greater the number of files, the larger this discrepancy may become.

Evaluating NetBackup performance through the All Log Entries report

To evaluate performance through the All Log Entries report

1. Run the backup or restore job.
2. Run the All Log Entries report from the NetBackup reports node in the NetBackup Administrative Console. Be sure that the Date/Time Range that you select covers the time period during which the job was run.
3. Verify that the job completed successfully by searching for entries such as the following:

   For a backup: "the requested operation was successfully completed"

   For a restore: "successfully read (restore) backup id..."
4. Obtain the NetBackup performance statistics from the messages in the report.

Table of NetBackup All Log Entries report

Table 6-3 describes messages from the All Log Entries report.

The messages vary according to the locale setting of the master server.

Table 6-3 Messages in All Log Entries report

Entry	Statistic
`started backup job for client <name>, policy <name>, schedule <name> on storage unit <name>`	The **Date** and **Time** fields for this entry show the time at which the backup job started.
`successfully wrote backup id <name>, copy <number>, <number> Kbytes`	For a multiplexed backup, this entry shows the size of the individual backup job. The **Date** and **Time** fields indicate when the job finished writing to the storage device. The overall statistics for the multiplexed backup group, which include the data throughput rate to the storage device, are found in a subsequent entry.
`successfully wrote <number> of <number> multiplexed backups, total Kbytes <number> at Kbytes/sec`	For multiplexed backups, this entry shows the overall statistics for the multiplexed backup group including the data throughput rate.

Table 6-3 Messages in All Log Entries report *(continued)*

Entry	Statistic
`successfully wrote backup id <name>, copy <number>, fragment <number>, <number> Kbytes at <number> Kbytes/sec`	For non-multiplexed backups, this entry combines the information in the previous two entries for multiplexed backups. The single entry shows the following: ■ The size of the backup job ■ The data throughput rate ■ When the job finished writing to the storage device (in the **Date** and **Time** fields).
`the requested operation was successfully completed`	The **Date** and **Time** fields for this entry show the time at which the backup job completed. This value is later than the "successfully wrote" entry (in a previous message): it includes extra processing time at the end of the job for tasks such as NetBackup image validation.
`begin reading backup id <name>, (restore), copy <number>, fragment <number> from media id <name> on drive index <number>`	The **Date** and **Time** fields for this entry show when the restore job started reading from the storage device. (Note that the latter part of the entry is not shown for restores from disk, because it does not apply.)
`successfully restored from backup id <name>, copy <number>, <number> Kbytes`	For a multiplexed restore, this entry shows the size of the individual restore job. (As a rule, all restores from tape are multiplexed restores, because non-multiplexed restores require additional action from the user.) The **Date** and **Time** fields indicate when the job finished reading from the storage device. The overall statistics for the multiplexed restore group, including the data throughput rate, are found in a subsequent entry below.
`successfully restored <number> of <number> requests <name>, read total of <number> Kbytes at <number> Kbytes/sec`	For multiplexed restores, this entry shows the overall statistics for the multiplexed restore group, including the data throughput rate.
`successfully read (restore) backup id media <number>, copy <number>, fragment <number>, <number> Kbytes at <number> Kbytes/sec`	For non-multiplexed restores, this entry combines the information from the previous two entries for multiplexed restores. The single entry shows the following: ■ The size of the restore job ■ The data throughput rate ■ When the job finished reading from the storage device (in the **Date** and **Time** fields) As a rule, only restores from disk are treated as non-multiplexed restores.

Additional information on the NetBackup All Log Entries report

For other NetBackup operations, the NetBackup All Log Entries report has entries that are similar to those in the following table:

See Table 6-3 on page 98.

For example, it has entries for image duplication operations that create additional copies of a backup image. The entries may be useful for analyzing the performance of NetBackup.

The `bptm` debug log file for tape backups (or `bpdm` log file for disk backups) contains the entries that are in the All Log Entries report. The log also has additional detail about the operation that may be useful. One example is the message on intermediate data throughput rate for multiplexed backups:

```
... intermediate after number successful, number Kbytes at
number Kbytes/sec
```

This message is generated whenever an individual backup job completes that is part of a multiplexed backup group. For example, the debug log file for a multiplexed backup group (that consists of three individual backup jobs) may include the following: two intermediate status lines, then the final (overall) throughput rate.

For a backup operation, the `bpbkar` debug log file also contains additional detail about the operation that may be useful.

Note that writing the debug log files during the NetBackup operation introduces overhead that may not be present in a production environment. Factor that additional overhead into your calculations.

The information in the All Logs report is also found in the following locations:

UNIX

```
/usr/openv/netbackup/db/error
```

Windows

```
install_path\NetBackup\db\error
```

See the *NetBackup Troubleshooting Guide* to learn how to set up NetBackup to write these debug log files.

Evaluating UNIX system components

In addition to your evaluation of NetBackup's performance, you should also verify that common system resources are in adequate supply.

Monitoring CPU load (UNIX)

To monitor UNIX CPU load

1. Use the `vmstat` utility to monitor memory use.
2. Add up the "us" and "sy" CPU columns to get the total CPU load on the system.

   Refer to the `vmstat` man page for details.

   The `vmstat` scan rate indicates the amount of swapping activity taking place.

Note: The `sar` command also provides insight into UNIX memory usage.

About measuring performance independent of tape or disk output

You can measure the disk (read) component of NetBackup's speed independent of the network components and tape components.

The following techniques are available:

- bpbkar
  This technique is easier.
- SKIP_DISK_WRITES touch file
  This technique may be helpful in more limited circumstances.

Note: In these procedures, the master server is the client.

Measuring disk performance with bpbkar

Use this procedure.

To measure disk I/O using bpbkar

1. Turn on the legacy bpbkar log by ensuring that the bpbkar directory exists.

   UNIX

   `/usr/openv/netbackup/logs/bpbkar`

   Windows

   `install_path``\NetBackup\logs\bpbkar`

2. Set logging level to 1.

3 Enter the following:

UNIX

```
/usr/openv/netbackup/bin/bpbkar -nocont -dt 0 -nofileinfo
  -nokeepalives file system > /dev/null
```

Where *file system* is the path being backed up.

Windows

```
install_path\NetBackup\bin\bpbkar32 -nocont X:\ > NUL
```

Where *X*:\ is the path being backed up.

4 Check how long it took NetBackup to move the data from the client disk:

UNIX: The start time is the first PrintFile entry in the bpbkar log. The end time is the entry "Client completed sending data for backup." The amount of data is given in the entry "Total Size."

Windows: Check the bpbkar log for the entry "Elapsed time."

Measuring disk performance with the SKIP_DISK_WRITES touch file

The SKIP_DISK_WRITES procedure can be used on UNIX or Windows.

The SKIP_DISK_WRITES procedure is a useful follow-on to the bpbkar procedure. The bpbkar procedure may show that the disk read performance is not the bottleneck. If it is not the bottleneck, the bottleneck is in the data transfer between the client bpbkar process and the server bpdm process. The following SKIP_DISK_WRITES procedure may be helpful.

If the SKIP_DISK_WRITES procedure shows poor performance, the problem may involve the network, or shared memory (such as not enough buffers, or buffers that are too small). You can change shared memory settings.

You can change shared memory settings.

See "About shared memory (number and size of data buffers)" on page 123.

Caution: The following procedure can lead to data loss. The SKIP_DISK_WRITES touch file disables the writing of all backup data to disk for all policies on this server. Disable active production policies for the duration of this test and remove the touch file when this test is complete.

To measure disk I/O using the SKIP_DISK_WRITES touch file

1. Create a new disk storage unit, with /tmp or some other directory as the image directory path.
2. Create a policy that uses the new disk storage unit.
3. Deactivate any active production policies for the duration of this test.
4. Enter the following:

   UNIX:

   ```
   /usr/openv/netbackup/db/config/SKIP_DISK_WRITES
   ```

   Windows:

   ```
   install_path\Netbackup\db\config\SKIP_DISK_WRITES
   ```

   This file disables all data-write operations for disk backups but retains the creation of disk fragments and associated metadata.
5. Run a backup from this policy.

   NetBackup creates a file in the storage unit directory as if this backup is a real backup to disk. The image file is 0 bytes long.
6. To remove the zero-length file and clear the NetBackup catalog of a backup that cannot be restored, run this command:

   UNIX:

   ```
   /usr/openv/netbackup/bin/admincmd/bpexpdate -backupid backupid -d 0
   ```

   Windows:

   ```
   install_path\Netbackup\bin\admincmd\bpexpdate -backupid backupid -d 0
   ```

   where backupid is the name of the file that resides in the storage unit directory.
7. Remove the SKIP_DISK_WRITES file.
8. Re-activate any policies that were deactivated for this procedure.

Evaluating Windows system components

In addition to your evaluation of NetBackup's performance, you should also verify that common system resources are in adequate supply. For high level information, you can use the Windows Task Manager. For more detailed information, use the Windows Performance Monitor utility.

For further information on the Performance Monitor, refer to your Microsoft documentation.

About the Windows Performance Manager

The Performance Monitor organizes information by object, counter, and instance.

An object is a system resource category, such as a processor or physical disk. Properties of an object are counters. Counters for the **Processor** object include **%Processor Time**, which is the default counter, and **Interrupts/sec**. Duplicate counters are handled by instances. For example, to monitor the **%Processor Time** of a specific CPU on a multiple CPU system, the **Processor** object is selected. Then the **%Processor Time** counter for that object is selected, followed by the specific CPU instance for the counter.

In the Performance Monitor, you can view data in real-time format or collect the data in a log for future analysis. Specific components to evaluate include CPU load, memory use, and disk load.

Note: You should use a remote host for monitoring of the test host, to reduce load that might otherwise skew results.

Monitoring Windows CPU load

Use the following procedure to determine if the system has enough power to accomplish the requested tasks.

To monitor Windows CPU load

1. Start the Windows Performance Manager.

   For instructions, refer to your Microsoft documentation.

2. To determine how hard the CPU is working, monitor the **% Processor Time** counter for the **Processor** object.

   For **% Processor Time**, values of 0 to 80 percent are generally safe. Values from 80 percent to 90 percent indicate that the system is heavily loaded. Consistent values over 90 percent indicate that the CPU is a bottleneck.

   Spikes close to 100 percent are normal and do not necessarily indicate a bottleneck. However, if sustained loads close to 100 percent are observed, consider tuning the system to decrease process load, or upgrade to a faster processor.

3. To determine how many processes are actively waiting for the processor, monitor the **Process Queue Length** counter for the **System** object.

   Sustained **Processor Queue Lengths** greater than 2 indicate too many threads are waiting to be executed. To correctly monitor the **Processor Queue Length** counter, the Performance Monitor must track a thread-related counter. If you consistently see a queue length of 0, verify that a non-zero value can be displayed.

   The default scale for the **Processor Queue Length** may not be equal to 1. Be sure to read the data correctly. For example, if the default scale is 10x, then a reading of 40 means that only 4 processes are waiting.

Monitoring Windows memory use

Memory is a critical resource for increasing the performance of backup operations.

To monitor Windows memory use

1 Start the Windows Performance Manager.

For instructions, refer to your Microsoft documentation.

2 To examine memory usage, view information on the following:

Committed Bytes	Committed Bytes displays the size of virtual memory that has been committed, as opposed to reserved. Committed memory must have disk storage available or must not require the disk storage because the main memory is large enough. If the number of Committed Bytes approaches or exceeds the amount of physical memory, you may encounter issues with page swapping.
Page Faults/sec	Page Faults/sec is a count of the page faults in the processor. A page fault occurs when a process refers to a virtual memory page that is not in its Working Set in main memory. A high Page Fault rate may indicate insufficient memory.

Monitoring Windows disk load

To use disk performance counters to monitor the disk performance in Performance Monitor, you may need to enable the counters. Windows may not have enabled the disk performance counters by default for your system.

To get more information about disk performance counters

- Enter the following:

```
diskperf -help
```

To enable the counters and allow disk monitoring

1 Enter the following:

```
diskperf -y
```

2 Reboot the system.

To disable the counters and cancel disk monitoring

1 Enter the following:

```
diskperf -n
```

2 Reboot the system.

To monitor disk performance

1 Use the **%Disk Time** counter for the **PhysicalDisk** object.

Track the percentage of elapsed time that the selected disk drive is servicing read or write requests.

2 Monitor the **Avg. Disk Queue Length** counter and watch for values greater than 1 that last for more than one second.

Values greater than 1 for more than a second indicate that multiple processes are waiting for the disk to service their requests.

See "Measuring disk performance with the SKIP_DISK_WRITES touch file" on page 102.

Increasing disk performance

You can use the following techniques to increase disk performance:

- Refer to the following topic on measuring disk performance.
  See "Measuring disk performance with the SKIP_DISK_WRITES touch file" on page 102.
- Check the fragmentation level of the data.
  A highly fragmented disk limits throughput levels. Use a disk maintenance utility to defragment the disk.
- Consider adding additional disks to the system to increase performance.
  If multiple processes attempt to log data simultaneously, divide the data among multiple physical disks.
- Determine if the data transfer involves a compressed disk.
  Windows drive compression adds overhead to disk read or write operations, with adverse effects on NetBackup performance. Use Windows compression only if it is needed to avoid a disk full condition.
- Consider converting to a system with a Redundant Array of Independent Disks (RAID).
  Though more expensive, RAID devices offer greater throughput and (depending on the RAID level) improved reliability.

- Determine what type of controller technology drives the disk.
  A different system might yield better results.
  See Table 1-4 on page 28.

Chapter 7

Tuning the NetBackup data transfer path

This chapter includes the following topics:

About the NetBackup data transfer path

The overall performance of NetBackup is limited by the slowest component in the backup system. For example, a fast tape drive that is combined with an overloaded server yields poor performance. A fast tape drive on a slow network also yields poor performance.

The backup system is referred to as the data transfer path. The path usually starts at the data on the disk and ends with a backup copy on tape or disk.

This chapter subdivides the standard NetBackup data transfer path into four components: the NetBackup client, the network, the NetBackup server, and the storage device.

This chapter discusses NetBackup performance evaluation and improvement from a testing perspective. It describes ways to isolate performance variables to learn

the effect of each variable on overall system performance. It also describes how to optimize NetBackup performance with regard to those variables. It may not be possible to optimize every variable on your production system.

Note: The requirements for database backups may not be the same as for file system backups. This information in this chapter applies to file system backups unless otherwise noted.

About tuning the data transfer path

This chapter contains information on ways to optimize NetBackup. This chapter is not intended to provide tuning advice for particular systems. For help fine-tuning your NetBackup installation, please contact Symantec Consulting Services.

Before trying particular tuning steps, consider the following:

- Ensure that your system meets NetBackup's recommended minimum requirements
  Refer to the *NetBackup Installation Guide* and *NetBackup Release Notes* for information about these requirements.
- Ensure that you have the most recent NetBackup software patch installed
- Know your hardware
  Many performance issues can be traced to hardware or other environmental issues. You must understand the entire data transfer path to determine the maximum obtainable performance in your environment. Poor performance is often the result of poor planning, which results from unrealistic expectations of components of the transfer path.

Tuning suggestions for the NetBackup data transfer path

In every backup system there is room for improvement. To obtain the best performance from a backup infrastructure is not complex, but it requires careful review of the many factors that can affect processing. The first step is to gain an accurate assessment of each hardware, software, and networking component in the backup data path. Many performance problems are resolved before attempting to change NetBackup parameters.

NetBackup software offers plenty of resources to help isolate performance problems and assess the impact of configuration changes. However, it is essential

to thoroughly test both backup and restore processes after making any changes to the NetBackup configuration parameters.

This topic provides practical ideas to improve your backup system performance and avoid bottlenecks.

You can find background details in the following NetBackup manuals:

NetBackup Administrator's Guide, Volumes I & II

NetBackup Troubleshooting Guide

Table 7-1 Tuning suggestions for the NetBackup data path

Tuning suggestions	Description
Use multiplexing	Multiplexing writes multiple data streams from several clients to a single tape drive or several tape drives. Multiplexing can improve the backup performance of slow clients, multiple slow networks, and many small backups (such as incremental backups). Multiplexing reduces the time each job waits for a device to become available. It thereby makes the best use of the transfer rate of your storage devices. See "Fragment size: restore of a multiplexed image" on page 151. Refer also to the *NetBackup Administrator's Guide, Volume II*, for more information about using multiplexing.
Stripe a disk volume across drives.	A striped set of disks can pull data from all drives concurrently, to allow faster data transfers between disk drives and tape drives.
Maximize the use of your backup windows	You can configure all your incremental backups to happen at the same time every day. You can also stagger the execution of your full backups across multiple days. Large systems can be backed up over the weekend while smaller systems are spread over the week. You can start full backups earlier than the incremental backups. They might finish before the incremental backups and return all or most of your backup window to finish the incremental backups.
Convert large clients to SAN Clients or SAN Media Servers	A SAN Client is a client that is backed up over a SAN connection to a media server rather than over a LAN. SAN Client technology is for large databases and application servers where large data files are rapidly read from disk and streamed across the SAN. SAN Client is not suitable for file servers where the disk read speed is relatively slow. See "Best practices: NetBackup SAN Client" on page 79.
Use dedicated private networks to decrease backup times and network traffic	Dedicate one or more networks to backups, to reduce backup time and reduce or eliminate network traffic on your enterprise networks. In addition, you can convert to faster technologies and back up your systems at any time without affecting the enterprise network's performance. This approach assumes that users do not mind the system loads while backups take place.

Table 7-1 Tuning suggestions for the NetBackup data path *(continued)*

Tuning suggestions	Description
Avoid a concentration of servers on one network	If many large servers back up over the same network, convert some of them to media servers or attach them to private backup networks. Either approach decreases backup times and reduces network traffic for your other backups.
Use dedicated backup servers to perform your backups	For a backup server, use a dedicated system for backups only. Using a server that also runs several applications unrelated to backups can severely affect your performance and maintenance windows.
Consider the requirements of backing up your catalog	Remember that the NetBackup catalog needs to be backed up. To facilitate NetBackup catalog recovery, the master server should have access to a dedicated tape drive, either stand-alone or within a robotic library.
Level the backup load	You can use multiple drives to reduce backup times. To spread the load across multiple drives, you may need to reconfigure the streams or the NetBackup policies.
Consider bandwidth limiting	Bandwidth limiting lets you restrict the network bandwidth that is consumed by one or more NetBackup clients on a network. The bandwidth setting appears under **Host Properties > Master Servers, Properties**. The actual limiting occurs on the client side of the backup connection. This feature only restricts bandwidth during backups. Restores are unaffected. When a backup starts, NetBackup reads the bandwidth limit configuration and then determines the appropriate bandwidth value and passes it to the client. As the number of active backups increases or decreases on a subnet, NetBackup dynamically adjusts the bandwidth limiting on that subnet. If additional backups are started, the NetBackup server instructs the other NetBackup clients that run on that subnet to decrease their bandwidth setting. Similarly, bandwidth per client is increased if the number of clients decreases. Changes to the bandwidth value occur on a periodic basis rather than as backups stop and start. This characteristic can reduce the number of bandwidth value changes.

Table 7-1 Tuning suggestions for the NetBackup data path *(continued)*

Tuning suggestions	Description
Try load balancing	NetBackup provides ways to balance loads between servers, clients, policies, and devices. Note that these settings may interact with each other: compensating for one issue can cause another. The best approach is to use the defaults unless you anticipate or encounter an issue. Try one or more of the following: ■ Adjust the backup load on the server. Change the **Limit jobs per policy** attribute for one or more of the policies that the server backs up. For example, you can decrease **Limit jobs per policy** to reduce the load on a server on a specific subnetwork. Reconfigure policies or schedules to use storage units on other servers. Use bandwidth limiting on one or more clients. ■ Adjust the backup load on the server during specific time periods only. Reconfigure schedules to use storage units on the servers that can handle the load (if you use media servers). ■ Adjust the backup load on the clients. Change the **Maximum jobs per client** global attribute. An increase to **Maximum jobs per client** can increase the number of concurrent jobs that any one client can process and therefore increase the load. ■ Reduce the time to back up clients. Increase the number of jobs that clients can perform concurrently, or use multiplexing. Increase the number of jobs that the server can perform concurrently for the policies that back up the clients. ■ Give preference to a policy. Increase the **Limit jobs per policy** attribute value for the preferred policy relative to other policies. Alternatively, increase the priority for the policy. ■ Adjust the load between fast and slow networks. Increase the values of **Limit jobs per policy** and **Maximum jobs per client** for the policies and clients on a faster network. Decrease these values for slower networks. Another solution is to use bandwidth limiting. ■ Limit the backup load that one or more clients produce. Use bandwidth limiting to reduce the bandwidth that the clients use. ■ Maximize the use of devices Use multiplexing. Also, allow as many concurrent jobs per storage unit, policy, and client as possible without causing server, client, or network performance issues. ■ Prevent backups from monopolizing devices. Limit the number of devices that NetBackup can use concurrently for each policy or limit the number of drives per storage unit. Another approach is to exclude some of your devices from Media Manager control.

See "NetBackup client performance in the data transfer path" on page 114.

See "NetBackup network performance in the data transfer path" on page 115.

See "NetBackup server performance in the data transfer path" on page 122.

See "NetBackup storage device performance in the data transfer path" on page 157.

NetBackup client performance in the data transfer path

Many factors can affect the NetBackup client component of the NetBackup data transfer path. Consider the following to identify possible changes that may improve NetBackup performance:

Table 7-2 Factors that affect the client component of the NetBackup data transfer path

Factors	Notes
Disk fragmentation	Fragmentation severely affects the data transfer rate from the disk. Fragmentation can be repaired using disk management utility software.
Number of disks	Add disks to the system to increase performance. If multiple processes attempt to log data simultaneously, divide the data among multiple physical disks.
Disk arrays	Convert to a system that is based on a Redundant Array of Inexpensive Disks (RAID). RAID devices generally offer greater throughput and (depending on the RAID level) improved reliability.
SAN client	For critical data that requires high bandwidth for backups, consider the SAN client feature. Refer to the following documents for more information: ■ NetBackup Shared Storage Guide ■ "SAN Client Deployment, Best Practices and Performance Metrics" tech note. http://www.symantec.com/docs/TECH54778
Type of controller technology that drives the disk	A different system could yield better results.
Virus scanning	Virus scanning can severely affect the performance of the NetBackup client, especially for systems such as large Windows file servers. Consider disabling virus scans during backup or restore.

Table 7-2 Factors that affect the client component of the NetBackup data transfer path *(continued)*

Factors	Notes
NetBackup notify scripts	The `bpstart_notify.bat` and `bpend_notify.bat` scripts are very useful in certain situations, such as shutting down a running application to back up its data. However, these scripts must be written with care to avoid any unnecessary lengthy delays at the start or end of the backup. If the scripts do not perform tasks essential to the backup, remove them.
NetBackup software location	If the data being backed up is on the same physical disk as the NetBackup installation, note: performance may be adversely affected, especially if NetBackup debug log files are generated. If logs are used, the extent of the degradation is greatly influenced by the logs' verbose setting. If possible, install NetBackup on a separate physical disk to avoid disk drive contention.
Snapshots (hardware or software)	If snapshots are taken before the backup of data, the time that is needed to take the snapshot can affect the performance.
NetBackup Client Job Tracker	If the Job Tracker is running on the client, NetBackup estimates the data to be backed up before the backup. Gathering this estimate affects the startup time and the data throughput rate, because no data is written to the NetBackup server during this estimation. **Note:** The Job Tracker is disabled by default. If it is launched, it runs until the user logs out. Avoid running the NetBackup Client Job Tracker if the data-gathering process takes too long.
Determine the theoretical performance of the NetBackup client software	Use the NetBackup client command `bpbkar` (UNIX) or `bpbkar32` (Windows) to determine how fast the NetBackup client can read the data to be backed up. You may be able to eliminate data read speed as a performance bottleneck. See "About measuring performance independent of tape or disk output" on page 101.

NetBackup network performance in the data transfer path

To improve the overall performance of NetBackup, consider the following network components and factors.

Network interface settings

Make sure your network connections are properly installed and configured.

Note the following:

- Network interface cards (NICs) for NetBackup servers and clients must be set to full-duplex. Do not use Auto-sense or Auto-negotiate.
- Both ends of each network cable (the NIC card and the switch) must be set identically as to speed and mode. (Both NIC and switch must be at full duplex.) Otherwise, link down, excessive or late collisions, and errors result.
- If auto-negotiate is used, make sure that both ends of the connection are set at the same mode and speed. The higher the speed, the better.
- In addition to NICs and switches, all routers must be set to full duplex.
- Using AUTOSENSE may cause network problems and performance issues.
- Consult the operating system documentation for instructions on how to determine and change the NIC settings.

Network load

To evaluate remote backup performance, consider the following:

- The amount of network traffic
- The amount of time that network traffic is high

Small bursts of high network traffic for short durations can decrease data throughput rate. However, if the network traffic remains high, the network is probably the bottleneck. Try to schedule backups when network traffic is low. If your network is loaded, you may want to implement a secondary network which is dedicated to backup and restore traffic.

Note also: to check the network, use FTP to transfer a large file (50 megabytes or more) from the media server to the client and back again. Time each operation. If moving the file in either direction takes significantly longer than the other, the network has a problem.

Setting the network buffer size for the NetBackup media server

The NetBackup media server has a tunable parameter that you can use to adjust the size of the network buffer space. The operating system uses this buffer space for the connection between the bptm child process and the client process. This buffer space caches either received data from the network (a backup) or written data to the network (a restore). The parameter sets the value for NetBackup to use for the network buffer space, but the operating system may not allow the change.

The NetBackup media server can be configured to request that the operating system use a non-default size for the network buffer space. If the NET_BUFFER_SZ touch file exists, bptm requests that the operating system adjust the size. The

operating system may or may not allow the change, depending on the operating system revision and the current TCP tuning.

The following examples are from bptm logs on various platforms. These examples show how bptm records the size that was used and any previous size requested by NetBackup.

For example:

Solaris 10

```
setting receive network buffer to 65536 bytes
receive network buffer is 64240 bytes
```

AIX 5.3

```
receive network buffer is 134752 bytes
```

HP-UX 11.00

```
setting receive network buffer to 131072 bytes
receive network buffer is 65535 bytes
```

Windows

The default value for this parameter is derived from the NetBackup data buffer size using the following formula:

For backup jobs: (*<data_buffer_size>* * 4) + 1024

For restore jobs: (*<data_buffer_size>* * 2) + 1024

For tape:

Because the default value for the NetBackup data buffer size is 65536 bytes, the formula results in the following: a default NetBackup network buffer size of 263168 bytes for backups and 132096 bytes for restores.

For disk:

Because the default value for the NetBackup data buffer size is 262144 bytes, the formula results in the following: a default NetBackup network buffer size of 1049600 bytes for backups and 525312 bytes for restores.

To set the network buffer size

1 Create the following files:

UNIX

```
/usr/openv/netbackup/NET_BUFFER_SZ
/usr/openv/netbackup/NET_BUFFER_SZ_REST
```

Windows

```
install_path\NetBackup\NET_BUFFER_SZ
install_path\NetBackup\NET_BUFFER_SZ_REST
```

2 Note the following about the buffer files:

These files contain a single integer that specifies the network buffer size in bytes. For example, to use a network buffer size of 64 kilobytes, the file would contain 65536. If the files contain the integer 0 (zero), the default value for the network buffer size is used.

If the NET_BUFFER_SZ file exists, and the NET_BUFFER_SZ_REST file does not exist, NET_BUFFER_SZ specifies the network buffer size for backup and restores.

If the NET_BUFFER_SZ_REST file exists, its contents specify the network buffer size for restores.

If both files exist, the NET_BUFFER_SZ file specifies the network buffer size for backups. The NET_BUFFER_SZ_REST file specifies the network buffer size for restores.

Because local backup or restore jobs on the media server do not send data over the network, this parameter has no effect on those operations. This parameter is used only by the NetBackup media server processes that read from or write to the network, specifically, the `bptm` or `bpdm` processes. No other NetBackup process uses this parameter.

Network buffer size in relation to other parameters

The network buffer size parameter is the counterpart on the media server to the communications buffer size parameter on the client. The network buffer sizes need not be the same on all of your NetBackup systems for NetBackup to function properly. However, if the media server's network buffer size is the same as the client's communications buffer size, network throughput may improve.

Similarly, the network buffer size does not have a direct relationship to the NetBackup data buffer size.

See "About shared memory (number and size of data buffers)" on page 123.

The two buffers are separately tunable parameters. However, setting the network buffer size to a substantially larger value than the data buffer has achieved the best performance in many NetBackup installations.

Increasing the network buffer size on AIX for synthetic full backups

If synthetic full backups on AIX are running slowly, increase the `NET_BUFFER_SZ` network buffer to 262144 (256KB).

To increase the network buffer size on AIX

1. Create the following file:

   ```
   /usr/openv/netbackup/NET_BUFFER_SZ
   ```

2. To change the default setting from 32032 to 262144, enter the number 262144 in the file.

   This file is unformatted, and should contain only the size in bytes:

   ```
   $ cat /usr/openv/netbackup/NET_BUFFER_SZ
   262144
   $
   ```

   A change in this value can affect backup and restore operations on the media servers. Test backups and restores to ensure that the change you make does not negatively affect performance.

Setting the NetBackup client communications buffer size

The NetBackup client has a tunable parameter to adjust the size of the network communications buffer. This buffer writes data to the network for backups.

This client parameter is the counterpart to the network buffer size parameter on the media server. The network buffer sizes are not required to be the same on all of your NetBackup systems for NetBackup to function properly. However, if the media server's network buffer size is the same as the client's communications buffer size, you may achieve better performance.

To set the communications buffer size parameter on UNIX clients

- Create the `/usr/openv/netbackup/NET_BUFFER_SZ` file.

  As with the media server, the file should contain a single integer that specifies the communications buffer size. Generally, performance is better when the value in the NET_BUFFER_SZ file on the client matches the value in the NET_BUFFER_SZ file on the media server.

  The NET_BUFFER_SZ_REST file is not used on the client. The value in the NET_BUFFER_SZ file is used for both backups and restores.

To set the communications buffer size parameter on Windows clients

1. From **Host Properties** in the NetBackup Administration Console, do the following: expand **Clients** and open the **Client Properties > Windows Client > Client Settings** dialog for the client on which the parameter is to be changed.
2. Enter the new value in the **Communications buffer** field.

   This parameter is specified in number of kilobytes. The default value is 32. An extra kilobyte is added internally for backup operations. Therefore, the default network buffer size for backups is 33792 bytes. In some NetBackup installations, this default value is too small. A value of 128 improves performance in these installations.

   Because local backup jobs on the media server do not send data over the network, this parameter has no effect on these local operations. Only the NetBackup `bpbkar32` process uses this parameter. It is not used by any other NetBackup processes on a master server, media server, or client.
3. If you modify the NetBackup buffer settings, test the performance of restores with the new settings.

About the NOSHM file

Each time a backup runs, NetBackup checks for the existence of the NOSHM file. No services need to be stopped and started for it to take effect. You might use NOSHM, for example, when the NetBackup server hosts another application that uses a large amount of shared memory, such as Oracle.

NOSHM is also useful for testing: both as a workaround while solving a shared memory issue, and to verify that an issue is caused by shared memory.

Note: NOSHM only affects backups when it is applied to a system with a directly-attached storage unit.

NOSHM forces a local backup to run as though it were a remote backup. A local backup is a backup of a client that has a directly-attached storage unit. An example is a client that happens to be a master server or media server. A remote backup passes the data across a network connection from the client to a master server's or media server's storage unit.

A local backup normally has one or more `bpbkar` processes that read from the disk and write into shared memory. A local backup also has a `bptm` process that reads from shared memory and writes to the tape. A remote backup has one or more `bptm` (child) processes that read from a socket connection to bpbkar and write into shared memory. A remote backup also has a `bptm` (parent) process that reads from shared memory and writes to the tape. NOSHM forces the remote backup model even when the client and the media server are the same system.

For a local backup without NOSHM, shared memory is used between `bptm` and `bpbkar`. Whether the backup is remote or local, and whether NOSHM exists or not, shared memory is always used between `bptm` (parent) and `bptm` (child).

Note: NOSHM does not affect the shared memory that `bptm` uses to buffer data that is written to tape. `bptm` uses shared memory for any backup, local or otherwise.

Using socket communications (the NOSHM file)

When a master server or media server backs itself up, NetBackup uses shared memory to speed up the backup. In this case, NetBackup uses shared memory rather than socket communications to transport the data between processes. However, it may not be possible or desirable to use shared memory during a backup. In that case, you can use socket communications rather than shared memory to interchange the backup data.

To use socket communications

- Touch the following file:

  UNIX

  `/usr/openv/netbackup/NOSHM`

  Windows

  `install_path``\NetBackup\NOSHM`

  To touch a file means to change the file's modification and access times. The file name should not contain any extension.

Using multiple interfaces for NetBackup traffic

Distributing NetBackup traffic over several network interfaces can improve performance. Configure a unique hostname for the server for each network interface and set up bp.conf entries for the hostnames.

For example, suppose the server is configured with three network interfaces. Each of the network interfaces connects to one or more NetBackup clients. The following procedure allows NetBackup to use all three network interfaces.

To configure three network interfaces

1. In the server's bp.conf file, add one entry for each network interface:

```
SERVER=server-neta
SERVER=server-netb
SERVER=server-netc
```

2. In each client's bp.conf file, make the following entries:

```
SERVER=server-neta
SERVER=server-netb
SERVER=server-netc
```

   A client can have an entry for a server that is not currently on the same network.

   For more information on how to set network interfaces, refer to the *NetBackup Administrator's Guide, Volume I*.

NetBackup server performance in the data transfer path

To improve NetBackup server performance, consider the following factors regarding the data transfer path:

- See "About shared memory (number and size of data buffers)" on page 123.
- See "Changing parent and child delay values for NetBackup" on page 133.
- See "About NetBackup wait and delay counters" on page 134.
- See "Effect of fragment size on NetBackup restores" on page 149.
- See "Other NetBackup restore performance issues" on page 153.

About shared memory (number and size of data buffers)

The NetBackup media server uses shared memory to buffer data between the network and the tape drive or disk drive. (Or it buffers data between the disk and tape if the NetBackup media server and client are the same system.) The number and size of these shared data buffers can be configured on the NetBackup media server.

The number and size of the tape and disk buffers may be changed so that NetBackup optimizes its use of shared memory. A different buffer size may result in better throughput for high-performance tape drives. These changes may also improve throughput for other types of drives.

Buffer settings are for media servers only and should not be used on a pure master server or client.

Note: Restores use the same buffer size that was used to back up the images being restored.

Default number of shared data buffers

Table 7-3 shows the default number of shared data buffers for various NetBackup operations.

Table 7-3 Default number of shared data buffers

NetBackup operation	Number of shared data buffers UNIX	Number of shared data buffers Windows
Non-multiplexed backup	30	30
Multiplexed backup	12	12
Restore that uses non-multiplexed protocol	30	30
Restore that uses multiplexed protocol	12	12
Verify	30	30
Import	30	30
Duplicate	30	30
NDMP backup	30	30

Default size of shared data buffers

The default size of shared data buffers for various NetBackup operations is shown in Table 7-4.

Table 7-4 Default size of shared data buffers

NetBackup operation	Size of shared data buffers UNIX	Size of shared data buffers Windows
Non-multiplexed backup	64K (tape), 256K (disk)	64K (tape), 256K (disk)
Multiplexed backup	64K (tape), 256K (disk)	64K (tape), 256K (disk)
Restore, verify, or import	same size as used for the backup	same size as used for the backup
Duplicate	read side: same size as used for the backup write side: 64K (tape), 256K (disk)	read side: same size as used for the backup write side: 64K (tape), 256K (disk)
NDMP backup	64K (tape), 256K (disk)	64K (tape), 256K (disk)

On Windows, a single tape I/O operation is performed for each shared data buffer. Therefore, this size must not exceed the maximum block size for the tape device or operating system. For Windows systems, the maximum block size is generally 64K, although in some cases customers use a larger value successfully. For this reason, the terms "tape block size" and "shared data buffer size" are synonymous in this context.

Amount of shared memory required by NetBackup

You can use this formula to calculate the amount of shared memory that NetBackup requires:

Shared memory required = (number_data_buffers * size_data_buffers) * number_tape_drives * max_multiplexing_setting

For example, assume that the number of shared data buffers is 16, and the size of the shared data buffers is 64 kilobytes. Also assume two tape drives, and a maximum multiplexing setting of four. Following the formula, NetBackup requires 8 MB of shared memory:

```
(16 * 65536) * 2 * 4 = 8 MB
```

Be careful when changing these settings.

See "Testing changes made to shared memory" on page 132.

How to change the number of shared data buffers

You can change the number of shared data buffers by creating the following file(s) on the media server. In the files, enter an integer number of shared data buffers.

See "Notes on number data buffers files" on page 126.

- UNIX
  For tape:

  ```
  /usr/openv/netbackup/db/config/NUMBER_DATA_BUFFERS
  /usr/openv/netbackup/db/config/NUMBER_DATA_BUFFERS_RESTORE
  ```

  The value specified by `NUMBER_DATA_BUFFERS` determines the number of shared memory buffers for all types of backups if none of the following `NUMBER_DATA_BUFFERS_xxxx` files exists.
  For disk:

  ```
  /usr/openv/netbackup/db/config/NUMBER_DATA_BUFFERS_DISK
  ```

  For multiple copies (Inline Copy):

  ```
  /usr/openv/netbackup/db/config/NUMBER_DATA_BUFFERS_MULTCOPY
  ```

  For the FT media server:

  ```
  /usr/openv/netbackup/db/config/NUMBER_DATA_BUFFERS_FT
  ```

- Windows
  For tape:

  ```
  install_path\NetBackup\db\config\NUMBER_DATA_BUFFERS
  install_path\NetBackup\db\config\NUMBER_DATA_BUFFERS_RESTORE
  ```

  The value specified by `NUMBER_DATA_BUFFERS` determines the number of shared memory buffers for all types of backups if none of the following `NUMBER_DATA_BUFFERS_xxxx` files exists.
  For disk:

  ```
  install_path\NetBackup\db\config\NUMBER_DATA_BUFFERS_DISK
  ```

  For multiple copies (Inline Copy):

  ```
  install_path\NetBackup\db\config\NUMBER_DATA_BUFFERS_MULTCOPY
  ```

  For the FT media server:

Note: The FT media server is not yet supported on Windows.

See "Testing changes made to shared memory" on page 132.

Notes on number data buffers files

Note the following points:

- The various number data buffers files must contain a single integer that specifies the number of shared data buffers NetBackup uses.
- If the NUMBER_DATA_BUFFERS file exists, its contents determine the number of shared data buffers to be used for multiplexed and non-multiplexed backups.
- The following NUMBER_DATA_BUFFERS files allow buffer settings for particular types of backups:
  - NUMBER_DATA_BUFFERS_DISK
  - NUMBER_DATA_BUFFERS_MULTCOPY
  - NUMBER_DATA_BUFFERS_FT

  The values specified in these files override either the NetBackup default number or the value that is specified in NUMBER_DATA_BUFFERS.
  For example, NUMBER_DATA_BUFFERS_DISK allows for a different value when you back up to disk instead of tape. If NUMBER_DATA_BUFFERS exists but NUMBER_DATA_BUFFERS_DISK does not, NUMBER_DATA_BUFFERS applies to tape and disk backups. If both files exist, NUMBER_DATA_BUFFERS applies to tape backups and NUMBER_DATA_BUFFERS_DISK applies to disk backups. If only NUMBER_DATA_BUFFERS_DISK is present, it applies to disk backups only.
- The NUMBER_DATA_BUFFERS file also applies to remote NDMP backups, but does not apply to local NDMP backups or to NDMP three-way backups.
  See "Note on shared memory and NetBackup for NDMP" on page 130.
- The NUMBER_DATA_BUFFERS_RESTORE file is only used for restore from tape, not from disk. If the NUMBER_DATA_BUFFERS_RESTORE file exists, its contents determine the number of shared data buffers for multiplexed restores from tape.
- The NetBackup daemons do not have to be restarted for the new buffer values to be used. Each time a new job starts, bptm checks the configuration file and adjusts its behavior.
- For a recommendation for setting NUMBER_DATA_BUFFERS_FT, refer to the following topic:
  See "Recommended number of data buffers for SAN Client and FT media server" on page 132.

How to change the size of shared data buffers

You can change the size of shared data buffers by creating the following file(s) on the media server. In the files, enter an integer size in bytes for the shared data buffer. The integer should be a multiple of 1024 (a multiple of 32 kilobytes is recommended).

See "Notes on size data buffer files" on page 128.

- UNIX
  For tape:

  ```
  /usr/openv/netbackup/db/config/SIZE_DATA_BUFFERS
  ```

  The value specified by SIZE_DATA_BUFFERS determines the shared memory buffer size for all types of backups if none of the following SIZE_DATA_BUFFERS_xxxx files exists.
  For tape (NDMP storage units):

  ```
  /usr/openv/netbackup/db/config/SIZE_DATA_BUFFERS_NDMP
  ```

  For disk:

  ```
  /usr/openv/netbackup/db/config/SIZE_DATA_BUFFERS_DISK
  ```

  The `SIZE_DATA_BUFFERS_DISK` file also affects NDMP to disk backups.
  For multiple copies (Inline Copy):

  ```
  /usr/openv/netbackup/db/config/SIZE_DATA_BUFFERS_MULTCOPY
  ```

  For the FT media server:

  ```
  /usr/openv/netbackup/db/config/SIZE_DATA_BUFFERS_FT
  ```

- Windows
  For tape:

  ```
  install_path\NetBackup\db\config\SIZE_DATA_BUFFERS
  ```

  The value specified by SIZE_DATA_BUFFERS determines the shared memory buffer size for all types of backups if none of the following SIZE_DATA_BUFFERS_xxxx files exists.
  For tape (NDMP storage units):

  ```
  install_path\NetBackup\db\config\SIZE_DATA_BUFFERS_NDMP
  ```

  For disk:

  ```
  install_path\NetBackup\db\config\SIZE_DATA_BUFFERS_DISK
  ```

The SIZE_DATA_BUFFERS_DISK file also affects NDMP to disk backups.
For multiple copies (Inline Copy):

install_path\NetBackup\db\config\SIZE_DATA_BUFFERS_MULTCOPY

For the FT media server:
Note: The FT media server is not yet supported on Windows.

See "Testing changes made to shared memory" on page 132.

Notes on size data buffer files

Note the following points:

- The various size data buffers files contain a single integer that specifies the size of each shared data buffer in bytes. The integer should be a multiple of 1024 (a multiple of 32 kilobytes is recommended).
  See "Size values for shared data buffers" on page 129.
- If the SIZE_DATA_BUFFERS file exists, its contents determine the size of shared data buffers to be used for multiplexed and non-multiplexed backups.
- The other SIZE_DATA_BUFFERS files (SIZE_DATA_BUFFERS_DISK, SIZE_DATA_BUFFERS_MULTCOPY, SIZE_DATA_BUFFERS_FT) allow buffer settings for particular types of backups. The values specified in these files override either the NetBackup default size or the value that is specified in SIZE_DATA_BUFFERS.
  For example, SIZE_DATA_BUFFERS_DISK allows for a different value when you back up to disk instead of tape. If SIZE_DATA_BUFFERS exists but SIZE_DATA_BUFFERS_DISK does not, SIZE_DATA_BUFFERS applies to all backups. If both files exist, SIZE_DATA_BUFFERS applies to tape backups and SIZE_DATA_BUFFERS_DISK applies to disk backups. If only SIZE_DATA_BUFFERS_DISK is present, it applies to disk backups only.
- The SIZE_DATA_BUFFERS_DISK file also affects NDMP to disk backups.
- Perform backup and restore testing if the shared data buffer size is changed. If NetBackup media servers are not running the same operating system, test restores on each media server that may be involved in a restore operation. If a UNIX media server writes a backup to tape with a shared data buffer of 256 kilobytes, a Windows media server may not be able to read that tape.

Warning: Test restore as well as backup operations, to avoid the potential for data loss.

See "Testing changes made to shared memory" on page 132.

Size values for shared data buffers

Table 7-5 lists appropriate values for the various SIZE_DATA_BUFFERS files. The integer represents the size of one tape or disk buffer in bytes. For example, to use a shared data buffer size of 64 kilobytes, the file would contain the integer 65536.

These values are multiples of 1024. If you enter a value that is not a multiple of 1024, NetBackup rounds it down to the nearest multiple of 1024. For example, if you enter a value of 262656, NetBackup uses the value of 262144.

The NetBackup daemons do not have to be restarted for the parameter values to be used. Each time a new job starts, bptm checks the configuration file and adjusts its behavior.

Analyze the buffer usage by checking the bptm debug log before and after altering the size of buffer parameters. Note that the bptm log applies to both tape and disk backups.

Table 7-5 Byte values for SIZE_DATA_BUFFERS_xxxx files

Kilobytes per data buffer	SIZE_DATA_BUFFER value in bytes
32	32768
64	65536
96	98304
128	131072
160	163840
192	196608
224	229376
256	262144

Important: the data buffer size equals the tape I/O size. Therefore the SIZE_DATA_BUFFERS value must not exceed the maximum tape I/O size that the tape drive or operating system supports. This value is usually 256 or 128 kilobytes. Check your operating system and hardware documentation for the maximum values. Take into consideration the total system resources and the entire network. The Maximum Transmission Unit (MTU) for the LAN network may also have to be changed. NetBackup expects the value for NET_BUFFER_SZ and SIZE_DATA_BUFFERS to be in bytes. For 32K, use 32768 (32 x 1024).

Note: Some Windows tape devices cannot write with block sizes higher than 65536 (64 kilobytes). Some Windows media servers cannot read backups on a UNIX media server with SIZE_DATA_BUFFERS set to more than 65536. The Windows media server would not be able to import or restore images from media that were written with SIZE_DATA_BUFFERS greater than 65536.

Note: The size of the shared data buffers for a restore is determined by the size of the shared data buffers in use at the time the backup was written. Restores do not use the `SIZE_DATA_BUFFERS` files.

Note on shared memory and NetBackup for NDMP

The following tables describe how NetBackup for NDMP uses shared memory.

Table 7-6 shows the effect of NUMBER_DATA_BUFFERS according to the type of NDMP backup.

Table 7-6 NetBackup for NDMP and number of data buffers

Type of NDMP backup	Use of shared memory
Local NDMP backup or three-way backup	NetBackup does not use shared memory (no data buffers). `NUMBER_DATA_BUFFERS` has no effect.
Remote NDMP backup	NetBackup uses shared memory. You can use `NUMBER_DATA_BUFFERS` to change the number of memory buffers.

Table 7-7 shows the effect of SIZE_DATA_BUFFERS_NDMP according to the type of NDMP backup.

Table 7-7 NetBackup for NDMP and size of data buffers

Type of NDMP backup	Use of shared memory
Local NDMP backup or three-way backup	NetBackup does not use shared memory (no data buffers). You can use `SIZE_DATA_BUFFERS_NDMP` to change the size of the records that are written to tape. Use `SIZE_DATA_BUFFERS_DISK` to change record size for NDMP disk backup.

Table 7-7 NetBackup for NDMP and size of data buffers *(continued)*

Type of NDMP backup	Use of shared memory
Remote NDMP backup	NetBackup uses shared memory. You can use `SIZE_DATA_BUFFERS_NDMP` to change the size of the memory buffers and the size of the records that are written to tape. Use `SIZE_DATA_BUFFERS_DISK` to change buffer size and record size for NDMP disk backup.

The following is a brief description of NDMP three-way backup and remote NDMP backup:

- In an NDMP three-way backup, the backup is written to an NDMP storage unit on a different NAS filer.
- In remote NDMP backup, the backup is written to a NetBackup Media Manager-type storage device.

More information is available on these backup types.

See the *NetBackup for NDMP Administrator's Guide*.

Recommended shared memory settings

The `SIZE_DATA_BUFFERS` setting for backup to tape is typically increased to 256 KB and `NUMBER_DATA_BUFFERS` is increased to 16. To configure NetBackup to use 16 x 256 KB data buffers, specify 262144 (256 x 1024) in `SIZE_DATA_BUFFERS` and 16 in `NUMBER_DATA_BUFFERS`.

Note that an increase in the size and number of the data buffers uses up more shared memory, which is a limited system resource. The total amount of shared memory that is used for each tape drive is:

(number_data_buffers * size_data_buffers) * number_tape_drives * max_multiplexing_setting

For two tape drives, each with a multiplexing setting of 4 and with 16 buffers of 256KB, the total shared memory usage would be:

(16 * 262144) * 2 * 4 = 32768 KB (32 MB)

If large amounts of memory are to be allocated, the kernel may require additional tuning to provide enough shared memory for NetBackup.

See "About kernel parameters on Solaris 10" on page 191.

Note: Note that AIX media servers do not need to tune shared memory because AIX uses dynamic memory allocation.

Make changes carefully, monitoring for performance changes with each modification. For example, an increase in the tape buffer size can cause some backups to run slower. Also, there have been cases with restore issues. After any changes, be sure to include restores as part of your validation testing.

Recommended number of data buffers for SAN Client and FT media server

For SAN Client Fibre Transport, the effective total number of data buffers is approximately twice the number of buffers specified for non-multiplexed backups. The reason is that the specified number of buffers are present on both the SAN Client and on the FT media server.

Note: It usually does not improve performance to increase memory buffers to a number that is significantly more than the SAN Client Fibre Transport default (16). Such an increase usually causes the majority of the buffers on either the client or server side to be empty.

Testing changes made to shared memory

After making any changes, it is vitally important to verify that the following tests complete successfully.

To test changes made to shared memory

1. Run a backup.
2. Restore the data from the backup.

3 Restore data from a backup that was created before the changes to the SIZE_DATA_BUFFERS_xxxx and NUMBER_DATA_BUFFERS_xxxx files.

4 Before and after altering the size or number of data buffers, examine the buffer usage information in the bptm debug log file.

The values in the log should match your buffer settings. The relevant bptm log entries are similar to the following:

```
12:02:55 [28551] <2> io_init: using 65536 data buffer size
12:02:55 [28551] <2> io_init: CINDEX 0, sched bytes for
monitoring = 200
12:02:55 [28551] <2> io_init: using 8 data buffers
```

or

```
15:26:01 [21544] <2> mpx_setup_restore_shm: using 12 data
buffers, buffer size is 65536
```

When you change these settings, take into consideration the total system resources and the entire network. The Maximum Transmission Unit (MTU) for the local area network (LAN) may also have to be changed.

Changing parent and child delay values for NetBackup

You can modify the parent and child delay values for a process.

To change the parent and child delay values

1 Create the following files:

UNIX

```
/usr/openv/netbackup/db/config/PARENT_DELAY
/usr/openv/netbackup/db/config/CHILD_DELAY
```

Windows

```
install_path\NetBackup\db\config\PARENT_DELAY
install_path\NetBackup\db\config\CHILD_DELAY
```

These files contain a single integer that specifies the value in milliseconds for the delay corresponding to the name of the file.

2 For example, for a parent delay of 50 milliseconds, enter 50 in the PARENT_DELAY file.

See "About NetBackup wait and delay counters" on page 134.

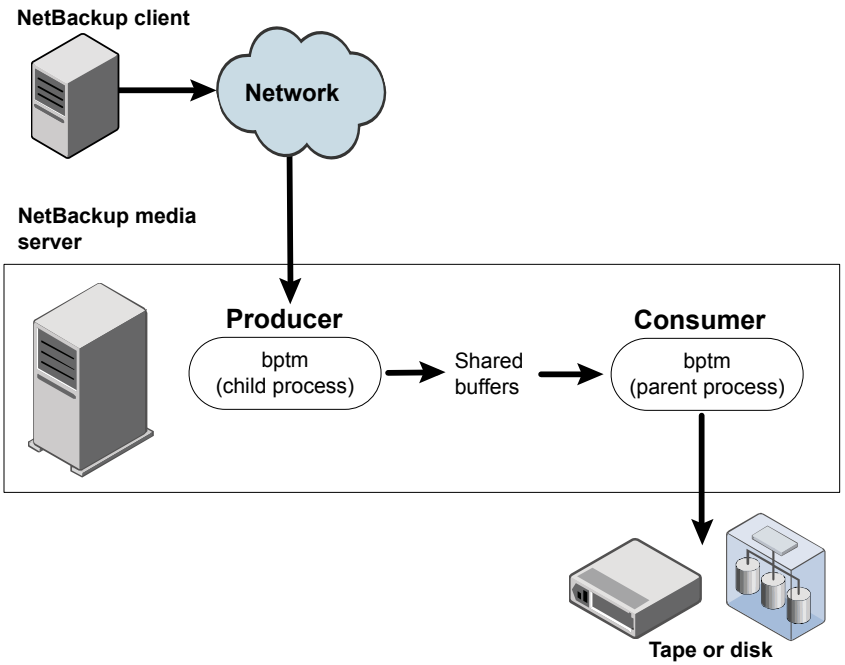
About NetBackup wait and delay counters

During a backup or restore operation, the NetBackup media server uses a set of shared data buffers to do the following: isolate the process of communicating with the storage device (tape or disk) from the process of interacting with the client disk or network. Through the use of wait and delay counters, you can determine which process on the NetBackup media server has to wait more often: the data producer or the data consumer.

Achieving a good balance between the data producer and the data consumer processes is an important factor in achieving optimal performance from the NetBackup server component of the NetBackup data transfer path.

Figure 7-1 shows the producer-consumer relationship.

Figure 7-1 Producer-consumer relationship during a remote client backup



About the communication between NetBackup client and media server

The communication process between the NetBackup client and the media server varies depending on the following:

- Whether the operation is a backup or restore

- Whether the operation involves a local client or a remote client

Table 7-8 NetBackup communication during backup and restore

Type of client (local or remote)	Communication process during backup and restore
Local client	When the NetBackup media server and the NetBackup client are part of the same system, the NetBackup client is referred to as a local client. ■ Backup of local client For a local client, the `bpbkar` (UNIX) or `bpbkar32` (Windows) process reads data from the disk during backup and places it in shared buffers. The `bptm` process reads the data from the shared buffer and writes it to tape or disk. ■ Restore of local client During a restore of a local client, the `bptm` process reads data from the tape or disk and places it in the shared buffers. The tar (UNIX) or tar32 (Windows) process reads the data from the shared buffers and writes it to disk. **Note:** Other processes may be used instead of bpbkar and bptm, depending on the data to be backed up or restored. See "Processes used in NetBackup client-server communication" on page 135.
Remote client	When the NetBackup media server and the NetBackup client are part of two different systems, the NetBackup client is referred to as a remote client. ■ Backup of remote client The `bpbkar` (UNIX) or `bpbkar32` (Windows) process on the remote client reads data from the disk and writes it to the network. Then a child `bptm` process on the media server receives data from the network and places it in the shared buffers. The parent `bptm` process on the media server reads the data from the shared buffers and writes it to tape or disk. ■ Restore of remote client During the restore of the remote client, the parent `bptm` process reads data from the tape or disk and places it into the shared buffers. The child `bptm` process reads the data from the shared buffers and writes it to the network. The tar (UNIX) or tar32 (Windows) process on the remote client receives the data from the network and writes it to disk. **Note:** Other processes may be used instead of bpbkar and bptm, depending on the data to be backed up or restored. See "Processes used in NetBackup client-server communication" on page 135.

Processes used in NetBackup client-server communication

The logs described in this topic record details about the NetBackup client-server communication. You can use these logs to adjust NetBackup client-server communication by means of wait and delay counters, as described in related topics.

Table 7-9 Logs used in NetBackup client-server communication

Log directory	Type of backup
UNIX log: /usr/openv/netbackup/logs/bpbkar Windows log: *install_path*\Veritas\NetBackup\logs\bpbkar	Standard, MS-Windows, FlashBackup, FlashBackup-Windows, Enterprise Vault, Lotus Notes, Domino, Sharepoint, DB2 snapshot backups, Oracle RMAN PROXY/snapshot backups, Oracle Block Incremental Backups without RMAN, MS-SQL-Server snapshot backups
UNIX log: /usr/openv/netbackup/logs/bpdb2 Windows log: *install_path*\Veritas\NetBackup\logs\bpdb2	DB2 stream-based backups. The bpdb2 directory must be writable by the DB2 user (not just by the root user).
UNIX log: /usr/openv/netbackup/logs/dbclient Windows log: *install_path*\Veritas\NetBackup\logs\dbclient	Oracle RMAN stream-based backups. The dbclient directory must be writable by the Oracle user (not just by the root user).
Windows log: *install_path*\Veritas\NetBackup\logs\dbclient	MS-SQL-Server stream-based backups. (Not supported on UNIX or Linux.)
UNIX log: /usr/openv/netbackup/logs/exten_client Windows log: *install_path*\Veritas\NetBackup\logs\exten_client	DataStore/XBSA stream-based backups. The exten_client directory must be writable by the application that is performing the backup/restore operation.
UNIX log: /usr/openv/netbackup/logs/infxbsa	Informix stream-based backups. The infxbsa directory must be writable by the Informix user. (Not supported on UNIX or Linux.)
UNIX log: /usr/openv/netbackup/logs/sybackup Windows log: *install_path*\Veritas\NetBackup\logs\sybackup	Sybase stream-based backups. The sybackup directory must be writable by the application that is performing the backup/restore operation.

Roles of processes during backup and restore

When a process attempts to use a shared data buffer, it first verifies that the next buffer is ready. A data producer needs an empty buffer, while a data consumer needs a full buffer.

The following table uses log directory names to represent the NetBackup processes.

Table 7-10 Roles of data producer and consumer

Operation	Data producer (Log directory name)	Data consumer (Log directory name)
Local Backup	bpbkar, bpdb2, dbclient, exten_client, infxbsa, sybackup.	bptm
Remote Backup	bptm (child)	bptm (parent)
Local Restore	bptm	tar (UNIX) or tar32 (Windows), bpdb2, dbclient, exten_client, infxbsa, sybackup.
Remote Restore	bptm (parent)	bptm (child)

If the data consumer lacks a full buffer, it increments the wait and delay counters to indicate that it had to wait for a full buffer. After a delay, the data consumer checks again for a full buffer. If a full buffer is still not available, the data consumer increments the delay counter to indicate that it had to delay again while waiting for a full buffer. The data consumer repeats the delay and full buffer check steps until a full buffer is available.

This sequence is summarized in the following algorithm:

```
while (Buffer_Is_Not_Full) {
++Wait_Counter;
      while (Buffer_Is_Not_Full) {
   ++Delay_Counter;
      delay (DELAY_DURATION);
        }
    }
```

If the data producer lacks an empty buffer, it increments the wait and delay counter to indicate that it had to wait for an empty buffer. After a delay, the data producer checks again for an empty buffer. If an empty buffer is still not available, the data producer increments the delay counter to indicate that it had to delay again while waiting for an empty buffer. The data producer repeats the delay and empty buffer check steps until an empty buffer is available.

The algorithm for a data producer has a similar structure:

```
while (Buffer_Is_Not_Empty) {
     ++Wait_Counter;
    while (Buffer_Is_Not_Empty) {
```

```
    ++Delay_Counter;
       delay (DELAY_DURATION);
    }
}
```

Analysis of the wait and delay counter values indicates which process, producer or consumer, has had to wait most often and for how long.

Four wait and delay counter relationships exist, as follows:

Table 7-11 Relationships between wait and delay counters

Relationship	Description
Data Producer >> Data Consumer	The data producer has substantially larger wait and delay counter values than the data consumer. The data consumer is unable to process the received data fast enough to keep the data producer busy. Investigate a means to improve the performance of the data consumer. For a backup, check if the data buffer size is appropriate for the tape or disk drive being used. If the data consumer still has a substantially large value in this case, try increasing the number of shared data buffers to improve performance.
Data Producer = Data Consumer (large value)	The data producer and the data consumer have very similar wait and delay counter values, but those values are relatively large. This situation may indicate that the data producer and data consumer regularly attempt to use the same shared data buffer. Try increasing the number of shared data buffers to improve performance. See "Finding wait and delay counter values" on page 139.
Data Producer = Data Consumer (small value)	The data producer and the data consumer have very similar wait and delay counter values, but those values are relatively small. This situation indicates that there is a good balance between the data producer and data consumer. It should yield good performance from the NetBackup server component of the NetBackup data transfer path.

Table 7-11 Relationships between wait and delay counters *(continued)*

Relationship	Description
Data Producer << Data Consumer	The data producer has substantially smaller wait and delay counter values than the data consumer. The data producer is unable to deliver data fast enough to keep the data consumer busy. Investigate ways to improve the performance of the data producer. For a restore operation, check if the data buffer size is appropriate for the tape or disk drive. If the data producer still has a relatively large value in this case, try increasing the number of shared data buffers to improve performance. See "How to change the number of shared data buffers" on page 125.

Of primary concern is the relationship and the size of the values. Information on determining substantial versus trivial values appears on the following pages. The relationship of these values only provides a starting point in the analysis. Additional investigative work may be needed to positively identify the cause of a bottleneck within the NetBackup data transfer path.

Finding wait and delay counter values

Wait and delay counter values can be found by creating debug log files on the NetBackup media server.

Note: The debug log files introduce additional overhead and have a small effect on the overall performance of NetBackup. This effect is more noticeable for a high verbose level setting. Normally, you should not need to run with debug logging enabled on a production system.

To find the wait and delay counter values for a local client backup

1. Activate debug logging by creating the appropriate log directories on the media server:

   UNIX

   For example:

   ```
   /usr/openv/netbackup/logs/bpbkar
   /usr/openv/netbackup/logs/bptm
   ```

   Windows

   ```
   install_path\NetBackup\logs\bpbkar
   install_path\NetBackup\logs\bptm
   ```

   The following topic lists log directories for processes that may be used in place of bpbkar, for database extensions:

   See "Processes used in NetBackup client-server communication" on page 135.

2. Execute your backup.

3. Consult the log for the data producer process.

   The line should be similar to the following, with a timestamp corresponding to the completion time of the backup:

   Example from the bpbkar log:

   ```
   ... waited 224 times for empty buffer, delayed 254 times
   ```

   In this example the wait counter value is 224 and the delay counter value is 254.

4. Look at the log for the data consumer process.

   The line should be similar to the following, with a timestamp corresponding to the completion time of the backup:

   ```
   ... waited for full buffer 1 times, delayed 22 times
   ```

   In this example, the wait counter value is 1 and the delay counter value is 22.

To find the wait and delay counter values for a remote client backup

1. Activate debug logging by creating this directory on the media server:

   UNIX

   ```
   /usr/openv/netbackup/logs/bptm
   ```

   Windows

   ```
   install_path\NetBackup\logs\bptm
   ```

2. Execute your backup.
3. Look at the log for the bptm process in:

   UNIX

   ```
   /usr/openv/netbackup/logs/bptm
   ```

   Windows

   ```
   install_path\NetBackup\Logs\bptm
   ```

   Delays that are associated with the data producer (bptm child) appear as follows:

   ```
   ... waited for empty buffer 22 times, delayed 151 times, ...
   ```

   In this example, the wait counter value is 22 and the delay counter value is 151.

   Delays that are associated with the data consumer (bptm parent) appear as:

   ```
   ... waited for full buffer 12 times, delayed 69 times
   ```

   In this example the wait counter value is 12, and the delay counter value is 69.

To find the wait and delay counter values for a local client restore

1. Activate logging by creating the two directories on the NetBackup media server:

   UNIX

   ```
   /usr/openv/netbackup/logs/bptm
   /usr/openv/netbackup/logs/tar
   ```

   Windows

   ```
   install_path\NetBackup\logs\bptm
   install_path\NetBackup\logs\tar
   ```

   The following topic lists log directories for processes that may be used in place of tar, for database extensions:

   See "Processes used in NetBackup client-server communication" on page 135.

2. Execute your restore.

3. Look at the log for the data consumer (tar or tar32) in the tar log directory.

   The line should be similar to the following, with a timestamp corresponding to the completion time of the restore:

   ```
   ... waited for full buffer 27 times, delayed 79 times
   ```

   In this example, the wait counter value is 27, and the delay counter value is 79.

4. Look at the log for the data producer (`bptm`) in the bptm log directory.

   The line should be similar to the following, with a timestamp corresponding to the completion time of the restore:

   ```
   ... waited for empty buffer 1 times, delayed 68 times
   ```

   In this example, the wait counter value is 1 and the delay counter value is 68.

To find the wait and delay counter values for a remote client restore

1. Activate debug logging by creating the following directory on the media server:

   UNIX

   ```
   /usr/openv/netbackup/logs/bptm
   ```

   Windows

   ```
   install_path\NetBackup\logs\bptm
   ```

2. Execute your restore.
3. Look at the log for bptm in the bptm log directory.

   Delays that are associated with the data consumer (`bptm` child) appear as follows:

   ```
   ... waited for full buffer 36 times, delayed 139 times
   ```

   In this example, the wait counter value is 36 and the delay counter value is 139.

   Delays that are associated with the data producer (`bptm` parent) appear as follows:

   ```
   ... waited for empty buffer 95 times, delayed 513 times
   ```

   In this example the wait counter value is 95 and the delay counter value is 513.

Note on log file creation

When you run multiple tests, you can rename the current log file. Renaming the file causes NetBackup to create a new log file, which prevents you from erroneously reading the wrong set of values.

Deleting the debug log file does not stop NetBackup from generating the debug logs. You must delete the entire directory. For example, to stop bptm from logging, you must delete the bptm subdirectory. NetBackup automatically generates debug logs at the specified verbose setting whenever the directory is detected.

Use care when manipulating the bptm log files if the backup or restore is part of a multiplex (MPX) group that includes unrelated operations. In those instances, the bptm parent process opens the log file once at startup and receives a file descriptor from the operating system. The parent process and child processes write to that file descriptor until all current (and future) jobs that join the MPX

group have completed. Unexpected consequences may result if the log file is renamed or deleted while the MPX group is still active.

If the log file is renamed, the file descriptor remains open against the renamed file. And if the next test job joins the same MPX group the new log entries appear in the renamed log file. If the log file is deleted, the file is no longer visible in the directory but the file descriptor remains open. If the next test job joins the same MPX group, the new log entries are written to the open file. Note that the user can no longer access the open file.

This behavior also applies to the MPX groups that have been running for multiple days. If the test job joins an MPX group that became active two days ago, the log entries are in the log from two days ago. If the bptm log directory did not exist two days ago, the bptm processes handling the backup do not generate any log entries.

If the bptm log directory did not exist two days ago, do one of the following:

- Wait for the MPX group to complete before starting the test job.
- Change either the storage unit, volume pool, or retention for the backup. The job is assigned to a drive and to media that is not already in use, and a new bptm parent process is started.

About tunable parameters reported in the bptm log

You can use the bptm debug log file to verify that the following tunable parameters have successfully been set to the desired values. You can use these parameters and the wait and delay counter values to analyze issues.

These additional values include the following:

Data buffer size	The size of each shared data buffer can be found on a line similar to: ... io_init: using 65536 data buffer size
Number of data buffers	The number of shared data buffers may be found on a line similar to: ... io_init: using 16 data buffers
Parent/child delay values	For the duration of the parent and child delays, the values in use can be found on a line similar to: ... io_init: child delay = 10, parent delay = 15 (milliseconds)

NetBackup media server network buffer size	The Network buffer size values on the media server appear in the debug log files in lines similar to the following. The first line indicates that the NET_BUFFER_SZ touch file exists. It also indicates that bptm has tried to change the network buffer space from the operating system default. (This first line may not be present.) The second line is always present and reflects the value that the operating system uses for the current backup or restore. If the two values differ, the operating system did not allow the change to be made. You should delete the NET_BUFFER_SZ file.
	
	The bptm child process reads from the receive network buffer during a remote backup.
	
	`...setting receive network buffer to 263168 bytes`
	`…receive network buffer is 49640 bytes`
	
	The bptm child process writes to the network buffer during a remote restore:
	
	`...setting send network buffer to 131072 bytes`
	`…send network buffer is 131072 bytes`
	
	See "Setting the network buffer size for the NetBackup media server" on page 116.

Example of using wait and delay counter values

Suppose you wanted to analyze a local backup that has a 30-minute data transfer that is baselined at 5 MB per second. The backup involves a total data transfer of 9,000 MB. Because a local backup is involved, bptm is the data consumer. The data producer depends on the type of data that is backed up.

See "Processes used in NetBackup client-server communication" on page 135.

See "Roles of processes during backup and restore" on page 136.

Find the wait and delay values for the appropriate data producer process and for the consumer process (bptm) from the following:

See "Finding wait and delay counter values" on page 139.

For this example, suppose those values are the following:

Table 7-12 Examples for wait and delay

Process	Wait	Delay
bpbkar (UNIX) bpbkar32 (Windows)	29364	58033
bptm	95	105

These values reveal that `bpbkar` (or `bpbkar32`) is forced to wait by a `bptm` process that cannot move data out of the shared buffer fast enough.

Next, you can determine time lost due to delays by multiplying the delay counter value by the parent or child delay value, whichever applies.

In this example, the `bpbkar` (or `bpbkar32`) process uses the child delay value, while the `bptm` process uses the parent delay value. (The defaults for these values are 10 milliseconds for child delay and 15 milliseconds for parent delay.)

You can use the following equations to determine the amount of time lost due to these delays:

Table 7-13 Example delays

Process	Delay
bpbkar (UNIX) bpbkar32 (Windows)	58033 delays x 0.010 seconds = 580.33 seconds = 9 minutes 40 seconds
bptm	105 x 0.015 seconds = 1.6 seconds

Use these equations to determine if the delay for `bpbkar` (or `bpbkar32`) is significant. In this example, if this delay is removed, the resulting transfer time is:

30 minutes original transfer time - 9 minutes 40 seconds = 20 minutes 20 seconds (1220 seconds)

A transfer time of 1220 seconds results in the following throughput value:

9000 MB / 1220 seconds = 7.38 MB per second

7.38 MB per second is a significant increase over 5 MB per second. With this increase, you should investigate how the tape or disk performance can be improved.

You should interpret the number of delays within the context of how much data was moved. As the amount of moved data increases, the significance threshold for counter values increases as well.

Again, for a total of 9,000 MB of data being transferred, assume a 64-KB buffer.

You can determine the total number of buffers to be transferred using the following equation:

Number of kilobytes	9,000 x 1024 = 9,216,000 KB
Number of buffers	9,216,000 / 64 = 144,000

You can now express the wait counter value as a percentage of the total number of buffers:

bpbkar (UNIX), or bpbkar32 (Windows)	29364 / 144,000 = 20.39%
bptm	95 / 144,000 = 0.07%

In the 20 percent of cases where `bpbkar` (or `bpbkar32`) needed an empty shared data buffer, `bptm` has not yet emptied the shared data buffer. A value of this size indicates a serious issue. You should investigate as to why the data consumer (`bptm`) cannot keep up.

In contrast, the delays that `bptm` encounters are insignificant for the amount of data transferred.

You can also view the delay and wait counters as a ratio:

bpbkar (UNIX)	= 58033 delays / 29364 waits
bpbkar32 (Windows)	= 1.98

In this example, on average `bpbkar` (or `bpbkar32`) had to delay twice for each wait condition that was encountered. If this ratio is large, increase the parent or child delay to avoid checking for a shared data buffer in the correct state too often.

See "Changing parent and child delay values for NetBackup" on page 133.

Conversely, if this ratio is close to 1, reduce the applicable delay value to check more often, which may increase your data throughput performance. Keep in mind that the parent and child delay values are rarely changed in most NetBackup installations.

The preceding information explains how to determine if the values for wait and delay counters are substantial enough for concern.

Note: The wait and delay counters are related to the size of the data transfer. A value of 1,000 may be extreme when only 1 megabyte of data is moved. The same value may indicate a well-tuned system when gigabytes of data are moved. The final analysis must determine how these counters affect performance.

Issues uncovered by wait and delay counter values

You can correct issues by checking the following:

- bptm-read waits
  The `bptm` debug log contains messages such as the following:

  ```
  ...waited for full buffer 1681 times, delayed 12296 times
  ```

  The first number is the number of times bptm waited for a full buffer: in other words, how many times the bptm write operations waited for data from the source. If the wait counter indicates a performance issue, a change in the number of buffers does not help.
  See "Finding wait and delay counter values" on page 139.
  Multiplexing may help.

- bptm-write waits
  The bptm debug log contains messages such as the following:

  ```
  ...waited for empty buffer 1883 times, delayed 14645 times
  ```

  The first number is the number of times bptm waited for an empty buffer: the number of times bptm encountered data from the source faster than the data can be written to tape or disk. If the wait counter indicates a performance issue, reduce the multiplexing factor.
  See "Finding wait and delay counter values" on page 139.
  More buffers may help.

- bptm delays
  The bptm debug log contains messages such as the following:

  ```
  ...waited for empty buffer 1883 times, delayed 14645 times
  ```

  The second number is the number of times bptm waited for an available buffer. If the delay counter indicates a performance issue, investigate. Each delay interval is 30 microseconds.

Estimating the impact of Inline copy on backup performance

Inline Copy (multiple copies) takes one stream of data that the bptm buffers receive and writes the data to two or more destinations sequentially. The time to write

to multiple devices is the same as the time required to write to one device multiplied by the number of devices. The overall write speed, therefore, is the write speed of a single device divided by the number of devices.

The write speed of a backup device is usually faster than the read speed of the source data. Therefore, switching to Inline Copy may not necessarily slow down the backup. The important figure is the write speed of the backup device: the native speed of the device multiplied by the compression ratio of the device hardware compression. For tape backups this compression ratio can be approximated by looking at how much data is held on a single tape (as reported by NetBackup). Compare that amount of data with the uncompressed capacity of a cartridge.

For example:

An LTO gen 3 cartridge has an uncompressed capacity of 400 GB. An LTO gen 3 drive has a native write capacity of 80 MB per second. If a full cartridge contains 600 GB, the compression ratio is 600/400 or 1.5:1. Thus, the write speed of the drive is 1.5 * 80 = 120 MB per second.

If Inline copy to two LTO gen 3 drives is used, the overall write speed is 120/2 = 60 MB per second.

If the backup normally runs at 45 MB per second (the read speed of the source data is 45 MB per second), Inline copy does not affect the backup speed. If the backup normally runs at 90 MB per second, Inline Copy reduces the speed of the backup to 60 MB per second. The performance limit is moved from the read operation to the write operation.

Effect of fragment size on NetBackup restores

Fragment size can affect NetBackup restores for non-multiplexed and multiplexed images.

The fragment size affects where tape markers are placed and how many tape markers are used. (The default fragment size is 1 terabyte for tape storage units and 512 GB for disk.) As a rule, a larger fragment size results in faster backups, but may result in slower restores when recovering a small number of individual files.

The "Reduce fragment size to" setting on the Storage Unit dialog limits the largest fragment size of the image. By limiting the size of the fragment, the size of the largest read during restore is minimized, reducing restore time. The fragment size is especially important when restoring a small number of individual files rather than entire directories or file systems.

For many sites, a fragment size of approximately 10 GB results in good performance for backup and restore.

For a fragment size, consider the following:

- Larger fragment sizes usually favor backup performance, especially when backing up large amounts of data. Smaller fragments can slow down large backups. Each time a new fragment is created, the backup stream is interrupted.
- Larger fragment sizes do not hinder performance when restoring large amounts of data. But when restoring a few individual files, larger fragments may slow down the restore.
- Larger fragment sizes do not hinder performance when restoring from non-multiplexed backups. For multiplexed backups, larger fragments may slow down the restore. In multiplexed backups, blocks from several images can be mixed together within a single fragment. During restore, NetBackup positions to the nearest fragment and starts reading the data from there, until it comes to the desired file. Splitting multiplexed backups into smaller fragments can improve restore performance.
- During restores, newer, faster devices can handle large fragments well. Slower devices, especially if they do not use fast locate block positioning, restore individual files faster if fragment size is smaller. (In some cases, SCSI fast tape positioning can improve restore performance.)

Unless you have particular reasons for creating smaller fragments, larger fragment sizes are likely to yield better overall performance. For example, reasons for creating smaller fragments are the following: restoring a few individual files, restoring from multiplexed backups, or restoring from older equipment.

Fragment size: restore of a non-multiplexed image

bptm positions to the media fragment and the actual tape block that contains the first file to be restored. If fast-locate is available, bptm uses that for the positioning. If fast-locate is not available, bptm uses MTFSF/MTFSR (forward space filemark/forward space record) to do the positioning.

The first file is then restored.

After that, for every subsequent file to be restored, bptm determines where that file is, relative to the current position. It may be faster for bptm to position to that spot rather than to read all the data in between (if fast locate is available). In that case, bptm uses positioning to reach the next file instead of reading all the data in between.

If fast-locate is not available, bptm can read the data as quickly as it can position with MTFSR (forward space record).

Therefore, fragment sizes for non-multiplexed restores matter if fast-locate is NOT available. With smaller fragments, a restore reads less extraneous data. You

can set the maximum fragment size for the storage unit on the Storage Unit dialog in the NetBackup Administration Console (**Reduce fragment size to**).

Fragment size: restore of a multiplexed image

bptm positions to the media fragment that contains the first file to be restored. If fast-locate is available, bptm uses that for the positioning. If fast_locate is not available, bptm uses MTFSF (forward space file mark) for the positioning. The restore cannot use "fine-tune" positioning to reach the block that contains the first file, because of the randomness of how multiplexed images are written. The restore starts to read, throwing away all the data (for this client and other clients). It continues throwing away data until it reaches the block that contains the first file.

The first file is then restored.

From that point, the logic is the same as for non-multiplexed restores, with one exception. If the current position and the next file position are in the same fragment, the restore cannot use positioning. It cannot use positioning for the same reason that it cannot use "fine-tune" positioning to get to the first file.

If the next file position is in a subsequent fragment (or on a different media), the restore uses positioning to reach that fragment. The restore does not read all the data in between.

Thus, smaller multiplexed fragments can be advantageous. The optimal fragment size depends on the site's data and situation. For multi-gigabyte images, it may be best to keep fragments to 1 gigabyte or less. The storage unit attribute that limits fragment size is based on the total amount of data in the fragment. It is not based on the total amount of data for any one client.

When multiplexed images are written, each time a client backup stream starts or ends, the result is a new fragment. A new fragment is also created when a checkpoint occurs for a backup that has checkpoint restart enabled. So not all fragments are of the maximum fragment size. End-of-media (EOM) also causes new fragment(s).

Some examples may help illustrate when smaller fragments do and do not help restores.

Example 1:

Assume you want to back up four streams to a multiplexed tape. Each stream is a single, 1 GB file. A default maximum fragment size of 1 TB has been specified. The resultant backup image logically looks like the following. ‘TM’ denotes a tape mark or file mark, which indicates the start of a fragment.

TM <4 gigabytes data> TM

To restore one of the 1 GB files, the restore positions to the TM. It then has to read all 4 GB to get the 1 GB file.

If you set the maximum fragment size to 1 GB:

TM <1 GB data> TM <1 GB data> TM <1 GB data> TM <1 GB data> TM

this size does not help: the restore still has to read all four fragments to pull out the 1 GB of the file being restored.

Example 2:

This example is the same as Example 1, but assume that four streams back up 1 GB of /home or C:\. With the maximum fragment size (**Reduce fragment size**) set to a default of 1 TB (assuming that all streams are relatively the same performance), you again end up with:

TM <4 GBs data> TM

Restoring the following

```
/home/file1
```

or

```
C:\file1
/home/file2
```

or

```
C:\file2
```

from one of the streams, NetBackup must read as much of the 4 GB as necessary to restore all the data. But, if you set **Reduce fragment size** to 1 GB, the image looks like the following:

TM <1 GB data> TM <1 GB data> TM <1 GB data> TM <1 GB data> TM

In this case, home/file1 or C:\file1 starts in the second fragment. bptm positions to the second fragment to start the restore of home/file1 or C:\file1. (1 GB of reading is saved so far.) After /home/file1 is done, if /home/file2 or C:\file2 is in the third or forth fragment, the restore can position to the beginning of that fragment before it starts reading.

These examples illustrate that whether fragmentation benefits a restore depends on the following: what the data is, what is being restored, and where in the image the data is. In Example 2, reducing the fragment size from 1 GB to half a GB (512 MB) increases the chance the restore can locate by skipping instead of reading, when restoring small amounts of an image.

Fragmentation and checkpoint restart

If the policy's Checkpoint Restart feature is enabled, NetBackup creates a new fragment at each checkpoint. It creates the fragment according to the **Take checkpoints every** setting. For more information on Checkpoint Restart, refer to the *NetBackup Administrator's Guide, Volume I*.

Other NetBackup restore performance issues

Restore performance issues related to fragment size are described in the following topic:

See "Effect of fragment size on NetBackup restores" on page 149.

Table 7-14 describes additional restore performance items.

Table 7-14 Issues that affect NetBackup restore performance

Restores issues	Comments
NetBackup catalog performance	The disk subsystem where the NetBackup catalog resides has a large impact on the overall performance of NetBackup. To improve restore performance, configure this subsystem for fast reads. NetBackup binary catalog format provides scalable and fast catalog access.
NUMBER_DATA_BUFFERS_RESTORE setting	This parameter can help keep other NetBackup processes busy while a multiplexed tape is positioned during a restore. An increase in this value causes NetBackup buffers to occupy more physical RAM. This parameter only applies to multiplexed restores. See "About shared memory (number and size of data buffers)" on page 123.
Index performance issues	Refer to "Indexing the Catalog for Faster Access to Backups" in the *NetBackup Administrator's Guide, Volume I*.
Search performance for many small backups	You can improve search performance when you have many small backup images. See "Improving search performance for many small backups" on page 156.

Table 7-14 Issues that affect NetBackup restore performance *(continued)*

Restores issues	Comments

Restore performance in a mixed environment	If you encounter restore performance issues in a mixed environment (UNIX and Windows), consider reducing the tcp wait interval parameter: `tcp_deferred_ack_interval`. Root privileges are required to change this parameter.
	
	The current value of `tcp_deferred_ack_interval` can be obtained by executing the following command (this example is for Solaris):
	
	`/usr/sbin/ndd -get /dev/tcp tcp_deferred_ack_interval`
	
	The value of `tcp_deferred_ack_interval` can be changed by executing the command:
	
	`/usr/sbin/ndd -set /dev/tcp tcp_deferred_ack_interval value`
	
	where *value* is the number which provides the best performance for the system. This approach may have to be tried and tested: it may vary from system to system. A suggested starting value is 20. In any case, the value must not exceed 500ms, otherwise it may break TCP/IP.
	
	With the optimum value for the system, you can set the value permanently in a script under the following directory:
	
	`/etc/rc2.d`
	
	Now it is executed when the system starts.

Multiplexing set too high	If multiplexing is too high, needless tape searching may occur. The ideal setting is the minimum needed to stream the drives.

Table 7-14 Issues that affect NetBackup restore performance *(continued)*

Restores issues	Comments
Restores from multiplexed database backups	NetBackup can run several restores at the same time from a single multiplexed tape, by means of the MPX_RESTORE_DELAY option. This option specifies how long in seconds the server waits for additional restore requests of files or raw partitions that are in a set of multiplexed images on the same tape. The restore requests received within this period are executed simultaneously. By default, the delay is 30 seconds. This option may be useful if multiple stripes from a large database backup are multiplexed together on the same tape. If the MPX_RESTORE_DELAY option is changed, you do not need to stop and restart the NetBackup processes for the change to take effect. When the request daemon on the master server (bprd) receives the first stream of a multiplexed restore request, it triggers the MPX_RESTORE_DELAY timer. The timer starts counting the configured amount of time. bprd watches and waits for related multiplexed jobs from the same client before it starts the overall job. If another associated stream is received within the timeout period, it is added to the total job: the timer is reset to the MPX_RESTORE_DELAY period. When the timeout has been reached without bprd receiving an additional stream, the timeout window closes. All associated restore requests are sent to bptm. A tape is mounted. If any associated restore requests arrive, they are queued until the tape that is now "In Use" is returned to an idle state. If MPX_RESTORE_DELAY is not high enough, NetBackup may need to mount and read the tape multiple times to collect all header information for the restore. Ideally, NetBackup would read a multiplexed tape and collect all the required header information with a single pass of the tape. A single pass minimizes the restore time. See "Example of restore from multiplexed database backup (Oracle)" on page 156.

Improving search performance for many small backups

To improve search performance

1 Run the following command as root on the master server:

UNIX

```
/usr/openv/netbackup/bin/admincmd/bpimage -create_image_list
-client client_name
```

Windows

```
install_directory\bin\admincmd\bpimage -create_image_list
-client client_name
```

where *client_name* is the name of the client that has many small backups.

In the following directory:

UNIX

```
/usr/openv/netbackup/db/images/client_name
```

Windows

```
install_path\NetBackup\db\images\client_name
```

the bpimage command creates the following files:

IMAGE_LIST	List of images for this client
IMAGE_INFO	Information about the images for this client
IMAGE_FILES	The file information for small images

2 Do not edit these files. They contain offsets and byte counts that are used to find and read the image information.

These files increase the size of the client directory.

Example of restore from multiplexed database backup (Oracle)

Suppose that MPX_RESTORE_DELAY is not set in the bp.conf file, so its value is the default of 30 seconds. Suppose also that you initiate a restore from an Oracle RMAN backup that was backed up using 4 channels or 4 streams. You also use the same number of channels to restore.

RMAN passes NetBackup a specific data request, telling NetBackup what information it needs to start and complete the restore. The first request is received

by NetBackup in 29 seconds, which causes the MPX_RESTORE_DELAY timer to be reset. The next request is received by NetBackup in 22 seconds; again the timer is reset. The third request is received 25 seconds later, resetting the timer a third time. But the fourth request is received 31 seconds after the third. Since the fourth request was not received within the restore delay interval, NetBackup starts three of the four restores. Instead of reading from the tape once, NetBackup queues the fourth restore request until the previous three requests are completed. Note that all of the multiplexed images are on the same tape. NetBackup mounts, rewinds, and reads the entire tape again to collect the multiplexed images for the fourth restore request.

In addition to NetBackup's reading the tape twice, RMAN waits to receive all the necessary header information before it begins the restore.

If MPX_RESTORE_DELAY is longer than 30 seconds, NetBackup can receive all four restore requests within the restore delay windows. It collects all the necessary header information with one pass of the tape. Oracle can start the restore after this one tape pass, for better restore performance.

Set the MPX_RESTORE_DELAY with caution, because it can decrease performance if set too high. Suppose that the MPX_RESTORE_DELAY is set to 1800 seconds. When the final associated restore request arrives, NetBackup resets the request delay timer as it did with the previous requests. NetBackup must wait for the entire 1800-second interval before it can start the restore.

Therefore, try to set the value of MPX_RESTORE_DELAY so it is neither too high or too low.

NetBackup storage device performance in the data transfer path

This section looks at storage device functionality in the NetBackup data transfer path. Changes in these areas may improve NetBackup performance.

Tape drive wear and tear is much less, and efficiency is greater, if the data stream matches the tape drive capacity and is sustained. Most tape drives have slower throughput than disk drives. Match the number of drives and the throughput per drive to the speed of the SCSI/FC connection, and follow the hardware vendors' recommendations.

The following factors affect tape drives:

- Media positioning

  When a backup or restore is performed, the storage device must position the tape so that the data is over the read and write head. The positioning can take a significant amount of time. When you conduct performance analysis with

media that contains multiple images, allow for the time lag that occurs before the data transfer starts.

- SCSI bus assignment
  Connect the tape drives to different SCSI buses. For example: If you have 8 tape drives, use a minimum of 4 SCSI cards and connect no more than 2 drives to each card.
- Tape streaming
  If a tape device is used at its most efficient speed, it is "streaming" the data onto the tape. If a tape device is streaming, the media rarely has to stop and restart. Instead, the media constantly spins within the tape drive. If the tape device is not used at its most efficient speed, it may continually start and stop the media from spinning. This behavior is the opposite of tape streaming and usually results in a poor data throughput.
- Data compression
  Most tape devices support some form of data compression within the tape device itself. Compressible data (such as text files) yields a higher data throughput rate than non-compressible data, if the tape device supports hardware data compression.
  Tape devices typically come with two performance rates: maximum throughput and nominal throughput. Maximum throughput is based on how fast compressible data can be written to the tape drive when hardware compression is enabled in the drive. Nominal throughput refers to rates achievable with non-compressible data.

Note: NetBackup cannot set tape drive data compression. Follow the instructions that are provided with your OS and tape drive.

In general, tape drive data compression is preferable to client (software) compression. Client compression may be desirable for reducing the amount of data that is transmitted across the network for a remote client backup.
See "Compression and NetBackup performance" on page 170.

Chapter 8

Tuning other NetBackup components

This chapter includes the following topics:

When to use multiplexing and multiple data streams

Multiple data streams can reduce the time for large backups. The reduction is achieved by first splitting the data to be backed up into multiple streams. Then you use multiplexing, multiple drives, or a combination of the two for processing the streams concurrently. In addition, you can configure the backup so each physical device on the client is backed up by a separate data stream. Each data stream runs concurrently with streams from other devices, to reduce backup times.

Note: For best performance, use only one data stream to back up each physical device on the client. Multiple concurrent streams from a single physical device can adversely affect the time to back up the device: the drive heads must move back and forth between tracks that contain the files for the respective streams.

Multiplexing is not recommended for database backups, when restore speed is of paramount interest or when your tape drives are slow.

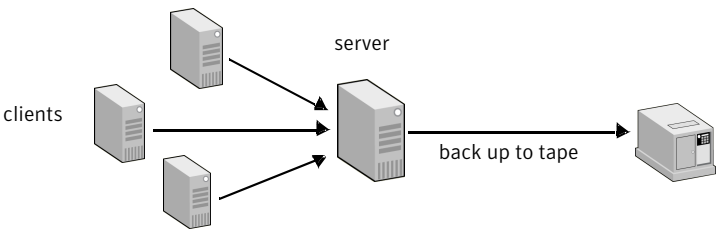
Backing up across a network, unless the network bandwidth is very broad, can nullify the ability to stream. Typically, a single client can send enough data to saturate a single 100BaseT network connection. A gigabit network has the capacity to support network streaming for some clients. Multiple streams use more of the client's resources than a single stream. Symantec recommends testing to make sure of the following: that the client can handle the multiple data streams, and that the high rate of data transfer does not affect users.

Multiplexing and multiple data streams can be powerful tools to ensure that all tape drives are streaming. With NetBackup, both can be used at the same time. Be careful to distinguish between the two concepts, as follows.

Multiplexing writes multiple data streams to a single tape drive.

Figure 8-1 shows multiplexing.

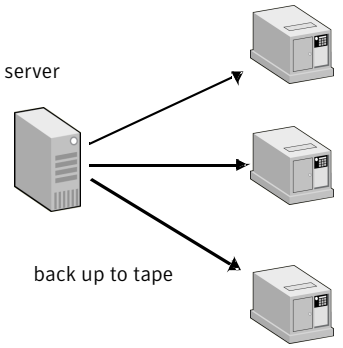
Figure 8-1 Multiplexing diagram



The multiple data streams feature writes multiple data streams, each to its own tape drive, unless multiplexing is used.

Figure 8-2 shows multiple data streams.

Figure 8-2 Multiple data streams diagram



Consider the following about multiplexing:

- Experiment with different multiplexing factors to find the one that is minimally sufficient for streaming.
  Find a setting at which the writes are enough to fill the maximum bandwidth of your drive: that setting is the optimal multiplexing factor. If you get 5 MB per second from each of the read streams, use a multiplexing factor of two to get the maximum throughput to a DLT7000. (That is, 10 MB per second.)
- Use a higher multiplexing factor for incremental backups.
- Use a lower multiplexing factor for local backups.
- Expect the duplication of a multiplexed tape to take longer if it is demultiplexed (unless "Preserve Multiplexing" is specified on the duplication). Without "Preserve Multiplexing," the duplication may take longer because multiple read passes of the source tape must be made. Using "Preserve Multiplexing," however, may affect the restore time (see next bullet).
- When you duplicate a multiplexed backup, demultiplex it.
  By demultiplexing the backups when they are duplicated, the time for recovery is significantly reduced.

Consider the following about multiple data streams:

- Do not use multiple data streams on single mount points.
  The multiple data streams feature takes advantage of the ability to stream data from several devices at the same time. Streaming from several devices permits backups to take advantage of Read Ahead on a spindle or set of spindles

in RAID environments. The use of multiple data streams from a single mount point encourages head thrashing and may result in degraded performance. Only conduct multistreamed backups against single mount points if they are mirrored (RAID 0). However, degraded performance is a likely result.

Effects of multiplexing and multistreaming on backup and restore

Note the following:

- Multiplexing
  To use multiplexing effectively, you must understand the implications of multiplexing on restore times. Multiplexing may decrease backup time for large numbers of clients over slow networks, but it does so at the cost of recovery time. Restores from multiplexed tapes must pass over all non-applicable data. This action increases restore times. When recovery is required, demultiplexing causes delays in the restore: NetBackup must search the tape to accomplish the restore.
  Restores should be tested to determine the impact of multiplexing on restore performance. Also, a smaller maximum fragment size when multiplexing may help restore performance.
  See "Effect of fragment size on NetBackup restores" on page 149.
  When you initially set up a new environment, keep the multiplexing factor low. A multiplexing factor of four or less does not highly affect the speed of restores, depending on the type of drive or system. If the backups do not finish within their assigned window, multiplexing can be increased to meet the window. However, a higher multiplexing factor provides diminishing returns as the number of multiplexing clients increases. The optimum multiplexing factor is the number of clients that are needed to keep the buffers full for a single tape drive.
  Set the multiplexing factor to four and do not multistream. Run benchmarks in this environment. Then you can begin to change the values until both the backup and restore window parameters are met.
- Multiple data streams
  The NEW_STREAM directive is useful for fine-tuning streams so that no disk subsystem is under-utilized or over-utilized.

How to improve NetBackup resource allocation

The following adjustments can be made to improve NetBackup resource allocation.

See "Improving the assignment of resources to NetBackup queued jobs" on page 163.

See "Sharing reservations in NetBackup" on page 165.

See "Disabling the sharing of NetBackup reservations" on page 166.

See "Adjusting the resource monitoring interval" on page 167.

See "Disabling on-demand unloads" on page 168.

Improving the assignment of resources to NetBackup queued jobs

In certain situations, nbrb may take too long to process jobs that are waiting for drives. This delay may occur when many jobs are queued for resources and the jobs are completing faster than nbrb can re-use the released resources for new jobs.

The following configuration file contains parameters that may improve nbrb performance in this situation.

UNIX:

/usr/openv/var/global/nbrb.conf

Windows:

install_path\Veritas\NetBackup\var\global\nbrb.conf

The following parameters can be configured:

- SECONDS_FOR_EVAL_LOOP_RELEASE
- RESPECT_REQUEST_PRIORITY
- DO_INTERMITTENT_UNLOADS
- BREAK_EVAL_ON_DEMAND

Example format for these parameters in nbrb.conf:

```
SECONDS_FOR_EVAL_LOOP_RELEASE = 180
RESPECT_REQUEST_PRIORITY = 0
DO_INTERMITTENT_UNLOADS = 1
```

The following table describes the nbrb.conf parameters.

Table 8-1 NetBackup nbrb.conf parameters

Parameter	Description
SECONDS_FOR_EVAL_LOOP_RELEASE	The default value is 180. If the value is 0, nbrb reverts to normal default behavior, evaluating all queued job requests before releasing any drives that have been released by completing jobs. When set to a nonzero value, SECONDS_FOR_EVAL_LOOP_RELEASE sets the time interval after which nbrb breaks into its evaluation cycle. After the specified interval, nbrb releases drives that have been given up by completed jobs, making them available for use by other jobs.
RESPECT_REQUEST_PRIORITY	The default value is 0. This option only has effect if SECONDS_FOR_EVAL_LOOP_RELEASE is set to a nonzero value. If RESPECT_REQUEST_PRIORITY is set to 1, nbrb restarts its evaluation queue at the top of the prioritized job queue after resources have been released when the SECONDS_FOR_EVAL_LOOP_RELEASE interval has passed. If RESPECT_REQUEST_PRIORITY is set to 0: NBRB continues evaluating jobs in the prioritized job queue at the point where the evaluation cycle was interrupted for drive releases due to SECONDS_FOR_EVAL_LOOP_RELEASE interval. As a result, a job is likely to reuse a drive more quickly after the drive has been released. Some lower priority jobs however may get drives before higher priority jobs do.

Table 8-1 NetBackup nbrb.conf parameters *(continued)*

Parameter	Description
DO_INTERMITTENT_UNLOADS	The default value is 1. This option only has effect if SECONDS_FOR_EVAL_LOOP_RELEASE is set to a nonzero value. If DO_INTERMITTENT_UNLOADS is set to 1: when resources are released after the SECONDS_FOR_EVAL_LOOP_RELEASE interval, nbrb initiates unloads of drives that have exceeded the media unload delay. Drives become available more quickly to jobs that require different media servers or different media than the job that last used the drive. However, the loaded media/drive pair may not be available for jobs further down in the prioritized evaluation queue that could use the drive/media without unload.
BREAK_EVAL_ON_DEMAND	The default value is 1. When a high priority request appears (a tape span request, or a request for a synthetic or duplication job), the evaluation cycle is immediately interrupted. nbrb releases drives, and it unloads drives if required. Then the evaluation cycle begins again. If the value is set to 0, high priority interrupts are not allowed and the evaluation cycle continues for the time interval specified by SECONDS_FOR_EVAL_LOOP_RELEASE.

Note the following:

- If nbrb.conf does not exist or parameters are not set in the file, the parameters assume their default values as described in the table.
- The addition or modification of the nbrb.conf file does not require stopping and restarting NetBackup processes. The processes read nbrb.conf at the start of every evaluation cycle, and changes of any type are implemented at that time.

Sharing reservations in NetBackup

To improve performance, NetBackup allows shared reservations. NetBackup shares reservations by default. With shared reservations, multiple jobs can reserve

the same media, though only one job can use it at a time. In other words, the second job does not have to wait for the first job to terminate. The second job can access the media as soon as the first job is done with it.

To enable the sharing of reservations

- Create the following file:

  On UNIX

  ```
  /usr/openv/netbackup/db/config/RB_USE_SHARED_RESERVATIONS
  ```

  On Windows

  ```
  install_path\Veritas\NetBackup\db\config\RB_USE_SHARED_RESERVATIONS
  ```

Disabling the sharing of NetBackup reservations

In NetBackup, shared reservations are enabled by default.

See "Sharing reservations in NetBackup" on page 165.

In most cases, sharing reservations results in better performance.

However, it may be helpful to disable sharing reservations in the following case:

- Many duplication jobs are running (using a storage lifecycle policy, or Vault, or bpduplicate), and
- Many read media are shared between different duplication jobs

In this case, without shared reservations, one job runs and other jobs requiring the same media are queued because they cannot get a reservation. With shared reservations, the jobs can start simultaneously. However, with a limited set of resources (media/drive pair or disk drives), resources may bounce or "ping-pong" between different jobs as each job requests the resource.

For example, assume the following:

Two duplication jobs, job 1 and job 2, are duplicating backup images. Job 1 is duplicating images 1 through 5, and job 2 is duplicating images 6 through 9. The images are on the following media:

Table 8-2 Media required by jobs 1 and 2

Media used by job 1	Media used by job 2
Image 1 is on media A1	Image 6 is on media A2
Image 2 is on media A2	Image 7 is on media A2
Image 3 is on media A2	Image 8 is on media A2
Image 4 is on media A2	Image 9 is on media A3
Image 5 is on media A3	

In this example, both jobs require access to media A2. Without shared reservations, if job 1 gets the reservation first, job 2 cannot start, because it needs to reserve media A2. A2 is already reserved by job 1. With shared reservations, both jobs can start at the same time.

Assume, however, that only a few drives are available for writing. Also assume that job 1 begins first and starts duplicating image 1. Then job 2 starts using media A2 to duplicate image 6. Media A2 in effect bounces between the two jobs: sometimes it is used by job 1 and sometimes by job 2. As a result, the overall performance of both jobs may degrade.

You can use the following procedure to disable the sharing of reservations.

To disable the sharing of reservations

- Create the following file:

  On UNIX

  ```
  /usr/openv/netbackup/db/config/RB_DO_NOT_USE_SHARED_RESERVATIONS
  ```

  On Windows

  ```
  install_path\Veritas\NetBackup\db\config\RB_DO_NOT_USE_SHARED
  _RESERVATIONS
  ```

Adjusting the resource monitoring interval

For resource monitoring, the NetBackup nbrb process periodically runs bptm -rptdrv on each media server by means of the master server. By default, bptm -rptdrv is run every 10 minutes. bptm -rptdrv serves two functions:

- Determines master-media connectivity
- Determines if any allocations are pending or if bptm is hung

In certain cases, it may be advantageous to monitor these resources less often. If you have many media servers, bptm -rptdrv can take CPU cycles from nbrb and nbjm. Also, starting bptm -rptdrv on the media server and reporting on the data requires network bandwidth. bptm -rptdrv also causes a lot of activity on the EMM server.

To adjust the resource monitoring interval

- In the bp.conf file on the NetBackup master server, set the following option:

  ```
  RESOURCE_MONITOR_INTERVAL = number_of_seconds
  ```

  The allowed values are from 600 to 3600 seconds (10 minutes to 1 hour).

Disabling on-demand unloads

The NetBackup EMM service may ask the resource broker (nbrb) to unload drives even though the media unload delay has not expired. This request is called an on-demand unload. If allocating resources for a request is not possible without unloading the drive, EMM may ask nbrb to unload the drive.

It may be helpful to disable on-demand unloads when a series of small related backup jobs are scheduled (such as multiple NetBackup database agent jobs).

To disable on-demand unloads

- Create the following file:

  On UNIX

  ```
  /usr/openv/netbackup/db/config/RB_DISABLE_REAL_UNLOADS_ON_DEMAND
  ```

  On Windows

  ```
  install_path\Veritas\NetBackup\db\config\RB_DISABLE_REAL_UNLOADS_ON
  _DEMAND
  ```

Encryption and NetBackup performance

During the backup, encryption can be performed in any of the following ways, depending on your backup environment:

- The NetBackup client performs the encryption.
- The NetBackup media server performs the encryption.
- The tape drive performs the encryption, together with the NetBackup Key Management Service. The tape drive must have built-in encryption capability.

Table 8-3 describes the performance effect of each technology.

Table 8-3 Encryption options and NetBackup performance

Encryption option	Performance considerations
Client encryption (the **Encryption** option on the NetBackup policy attributes tab)	Data encryption (and compression) can be performed by the NetBackup client. (Use the encryption and compression options on the policy Attributes tab.) If the client has sufficient CPU resources to perform the encryption (plus the rest of its backup processing), client encryption can be an effective option. Note that when NetBackup client encryption is used, backups may run slower. How much slower depends on the throttle point in your backup path. If the network is the issue, encryption should not hinder performance. If the network is not the issue, then encryption may slow down the backup. If you multi-stream encrypted backups on a client with multiple CPUs, try to define one fewer stream than the number of CPUs. For example, if the client has four CPUs, define three or fewer streams for the backup. This approach can minimize CPU contention. See "Effect of encryption plus compression on NetBackup performance" on page 172.
Media Server Encryption Option (MSEO)	Data encryption (and compression) can be performed on the NetBackup media server, by means of the Media Server Encryption Option (MSEO). Note the following: ■ In most cases, to avoid the need for additional tapes, you should compress the data before encrypting it. MSEO can both compress the data and encrypt it. ■ MSEO compression increases the amount of data that the media server must process in order to keep the tape drive streaming. ■ MSEO is usually most effective when only a limited amount of the backup data needs encryption. ■ The greater the amount of data to be encrypted, the greater the CPU load that is placed on the media server. If MSEO also compresses the data before encrypting it, the CPU demands are even greater. For example, to compress and encrypt 100 MB/second of data with a Solaris media server requires roughly an additional 8.7 GHz of CPU processing for MSEO. For more information on MSEO performance, see "A guide to best practices when using the NetBackup Media Server Encryption Option:" http://www.symantec.com/docs/TECH73132
Tape drive encryption, with the NetBackup Key Management Service (KMS)	Encryption that is performed by the tape drive has little or no effect on the backup performance. Use of this option requires the NetBackup Key Management Service (KMS). Note: In NetBackup 7.1, the number of key groups in KMS increased to 100.

Compression and NetBackup performance

NetBackup supports two types of compression:

- Client compression (configured in the NetBackup policy)
- Tape drive compression (handled by the device hardware)

Consider the following when choosing the type of compression:

- The decision to use data compression should be based on the compressibility of the data itself.

  Note the following levels of compressibility, in descending order:

  - Plain text
    Usually the most compressible type of data.
  - Executable code
    May compress somewhat, but not as much as plain text.
  - Already compressed data
    Often, no further compression is possible.
  - Encrypted data
    May expand in size if compression is applied.
    See "Effect of encryption plus compression on NetBackup performance" on page 172.
- Tape drive compression is almost always preferable to client compression. Compression is CPU intensive, and tape drives have built-in hardware to perform compression.
- Avoid using both tape compression and client compression
  Compressing data that is already compressed can increase the amount of backed up data.
- Only in rare cases is it beneficial to use client (software) compression

  Those cases usually include the following characteristics:

  - The client data is highly compressible.
  - The client has abundant CPU resources.
  - You need to minimize the data that is sent across the network between the client and server.

  In other cases, however, NetBackup client compression should be turned off, and the hardware should handle the compression.
- Client compression reduces the amount of data that is sent over the network, but increases CPU usage on the client.

- On UNIX, the NetBackup client configuration setting MEGABYTES_OF_MEMORY may help client performance.
  This option sets the amount of memory available for compression.
  Do not compress files that are already compressed. If the data is compressed twice, refer to the NetBackup configuration option COMPRESS_SUFFIX. You can use this option to exclude files with certain suffixes from compression.
  Edit this setting through bpsetconfig.
  See the *NetBackup Administrator's Guide, Volume II*.

How to enable NetBackup compression

Table 8-4 Tips on how to enable NetBackup compression

Type of compression	How to enable
Client compression	Select the compression option in the NetBackup Policy Attributes window.
Tape drive compression	Enabling tape drive compression depends on your operating system and the type of tape drive. Check with the operating system and drive vendors, or read their documentation to find out how to enable tape compression. Tips: With UNIX device addressing, these options are frequently part of the device name. A single tape drive has multiple names, each with a different functionality built into the name. (Multiple names are accomplished with major and minor device numbers.) On Solaris, if you address /dev/rmt/2cbn, you get drive 2 hardware-compressed with no-rewind option. If you address /dev/rmt/2n, its function should be uncompressed with the no-rewind option. The choice of device names determines device behavior. If the media server is UNIX, there is no compression when the backup is to a disk storage unit. The compression options in this case are limited to client compression. If the media server with the disk storage unit is Windows, and the directory that is used by the disk storage unit is compressed, note: compression is used on the disk write as for any file writes to that directory by any application.

Effect of encryption plus compression on NetBackup performance

If a policy is enabled for both encryption and compression, the client first compresses the backup data and then encrypts it. When data is encrypted, it becomes randomized, and is no longer compressible. Therefore, data compression must be performed before any data encryption.

Information on NetBackup Java performance improvements

For performance improvements, refer to the following sections in the *NetBackup Administrator's Guide for UNIX and Linux, Volume I:*

- "Configuring the NetBackup-Java Administration Console,"
- "NetBackup-Java Performance Improvement Hints"

The *NetBackup Release Notes* may also contain information about NetBackup Java performance.

Information on NetBackup Vault

Information on tuning NetBackup Vault is available.

Refer to the "Best Practices" chapter of the *NetBackup Vault Administrator's Guide*.

Fast recovery with Bare Metal Restore

Veritas Bare Metal Restore (BMR) provides a simplified, automated method by which to recover an entire system (including the operating system and applications). BMR automates the restore process to ensure rapid, error-free recovery. This process requires one Bare Metal Restore command and then a system boot. BMR guarantees integrity and consistency and is supported for both UNIX and Windows systems.

Note: BMR requires the True image restore option. This option has implications for the size of the NetBackup catalog.

See "How to calculate the size of your NetBackup image database" on page 32.

How to improve performance when backing up many small files

NetBackup may take longer to back up many small files than a single large file.

Table 8-5 How to improve performance when backing up many small files

Try the following	Notes
Use the FlashBackup (or FlashBackup-Windows) policy type.	FlashBackup is a feature of NetBackup Snapshot Client. FlashBackup is described in the *NetBackup Snapshot Client Administrator's Guide*. See "How to improve FlashBackup performance" on page 174.
Windows: turn off virus scans.	Turning off scans may double performance.
Snap a mirror (such as with the FlashSnap method in Snapshot Client) and back that up as a raw partition.	Unlike FlashBackup, this type of backup does not allow individual file restore.
Turn off or reduce logging.	The NetBackup logging facility has the potential to affect the performance of backup and recovery processing. Logging is usually enabled temporarily, to troubleshoot a NetBackup problem. The amount of logging and its verbosity level can affect performance.
Make sure the NetBackup buffer is the same size on the servers and clients.	See "Setting the network buffer size for the NetBackup media server" on page 116. See "Setting the NetBackup client communications buffer size" on page 119.
Adjust the batch size for sending metadata to the catalog	See "Adjusting the batch size for sending metadata to the NetBackup catalog" on page 58.
Upgrade NIC drivers as new releases appear.	

Run a `bpbkar` throughput test	Run the following `bpbkar` throughput test on the client with Windows.
	`C:\Veritas\Netbackup\bin\bpbkar32 -nocont > NUL 2>`
	For example:
	`C:\Veritas\Netbackup\bin\bpbkar32 -nocont c:\ > NUL 2> temp.f`

Optimize TCP/IP throughput	When initially configuring the Windows server, optimize TCP/IP throughput as opposed to shared file access.

Table 8-5 How to improve performance when backing up many small files *(continued)*

Try the following	Notes
Boost background performance on Windows versus foreground performance.	
Turn off NetBackup Client Job Tracker if the client is a system server.	See "NetBackup client performance in the data transfer path" on page 114.
Install appropriate patches	Regularly review the patch announcements for every server OS. Install patches that affect TCP/IP functions, such as correcting out-of-sequence delivery of packets.

How to improve FlashBackup performance

You can adjust NetBackup FlashBackup performance in the following ways.

Table 8-6 Tips for improving FlashBackup performance

Tips	Notes
Assign the snapshot cache device to a separate hard drive	If using the FlashBackup feature with a copy-on-write method such as nbu_snap, assign the snapshot cache device to a separate hard drive. A separate hard drive reduces disk contention and the potential for head thrashing. Refer to the *NetBackup Snapshot Client Administrator's Guide* for more information on FlashBackup configuration.

Table 8-6 Tips for improving FlashBackup performance *(continued)*

Tips	Notes
Adjust the FlashBackup read buffer	If the storage unit write speed is fast, reading the client disk may become a bottleneck during a FlashBackup raw partition backup. By default, FlashBackup (on UNIX) reads the raw partition using fixed 128 KB buffers for full backups and 32 KB buffers for incrementals. FlashBackup-Windows, by default, reads the raw partition using fixed 32 KB buffers for full backups and for incrementals. In most cases, the default read buffer size allows FlashBackup to stay ahead of the storage unit write speed. To minimize the number of I/O waits when reading client data, you can tune the FlashBackup read buffer size. Tuning this buffer allows NetBackup to read continuous device blocks up to 1 MB per I/O wait, depending on the disk driver. The read buffer size can be adjusted separately for full backup and for incremental backup. In general, a larger buffer yields faster raw partition backup (but see the following note). In the case of VxVM striped volumes, the read buffer can be configured as a multiple of the striping block size: data can be read in parallel from the disks, speeding up raw partition backup. **Note:** Resizing the read buffer for incremental backups can result in a faster backup in some cases, and a slower backup in others. Experimentation may be necessary to achieve the best setting. The result of the resizing depends on the following factors: ■ The location of the data to be read ■ The size of the data to be read relative to the size of the read buffer ■ The read characteristics of the storage device and the I/O stack. See "Adjusting the read buffer for FlashBackup and FlashBackup-Windows" on page 175.
Adjust the batch size for sending metadata to the catalog	See "Adjusting the batch size for sending metadata to the NetBackup catalog" on page 58.

Adjusting the read buffer for FlashBackup and FlashBackup-Windows

Use the following procedures to adjust the read buffer for NetBackup FlashBackup and FlashBackup-Windows raw partition backups.

To adjust the FlashBackup read buffer for UNIX and Linux clients

1 Create the following touch file on each client:

```
/usr/openv/netbackup/FBU_READBLKS
```

2 Enter the values in the `FBU_READBLKS` file, as follows.

On the first line of the file: enter an integer value for the read buffer size in blocks for full backups and/or for incremental backups. The defaults are 256 blocks (131072 bytes, or 128 KB) during full backups and 64 blocks (32768 bytes, or 32 KB) for incremental backups. The block size is equal to (KB size * 2), or (Number of bytes/512).

To change both values, separate them with a space.

For example:

```
512 128
```

This entry sets the full backup read buffer to 256 KB and the incremental read buffer to 64 KB.

You can use the second line of the file to set the tape record write size, also in blocks. The default is the same size as the read buffer. The first entry on the second line sets the full backup write buffer size. The second value sets the incremental backup write buffer size. To set read buffer size and tape record write size to the same values, the file would read altogether as:

```
512 128
512 128
```

To adjust the FlashBackup-Windows read buffer for Windows clients

1 Click **Host Properties > Clients**, right-click on the client and select **Properties**.

Click **Windows Client > Client Settings**.

2 For **Raw partition read buffer size**, specify the size of the read buffer.

A read buffer size larger than the 32 KB default may increase backup speed. Results vary from one system to another; experimentation may be required. A setting of 1024 may be a good starting point.

Note the following:

- This setting applies to raw partition backups as well as to FlashBackup-Windows policies (including NetBackup for VMware).
- This setting applies to full backups and to incremental backups.

Adjust the allocation size of the snapshot mount point volume for NetBackup for VMware

For VCB backups: To increase the speed of full virtual machine backups, try increasing the file system allocation size of the volume that is used as the snapshot mount point on the VMware backup proxy server. A larger allocation size, for instance 64 KB, may result in faster backups. Results can vary from one system to another; experimentation may be required.

Note: NetBackup 7.x uses VMware vStorage APIs (instead of VCB) to back up most VMware environments. VCB is required only for the following VMware environments: ESX servers older than 3.5 if no VirtualCenter server is present, or for VirtualCenter servers older than 2.5.

For a different tuning suggestion for NetBackup for VMware, see the following:

See "Adjusting the read buffer for FlashBackup and FlashBackup-Windows" on page 175.

The following documents contain information on NetBackup for VMware:

- For information on the snapshot mount point and the VMware backup proxy server when using VCB, see the *NetBackup for VMware Administrator's Guide* for 7.1.
- For up-to-date information on NetBackup support in virtual environments, see the following:
  http://www.symantec.com/docs/TECH127089

Symantec OpsCenter

For assistance in tuning OpsCenter for better performance, refer to the *Symantec OpsCenter Administrator's Guide*.

Chapter 9

Tuning disk I/O performance

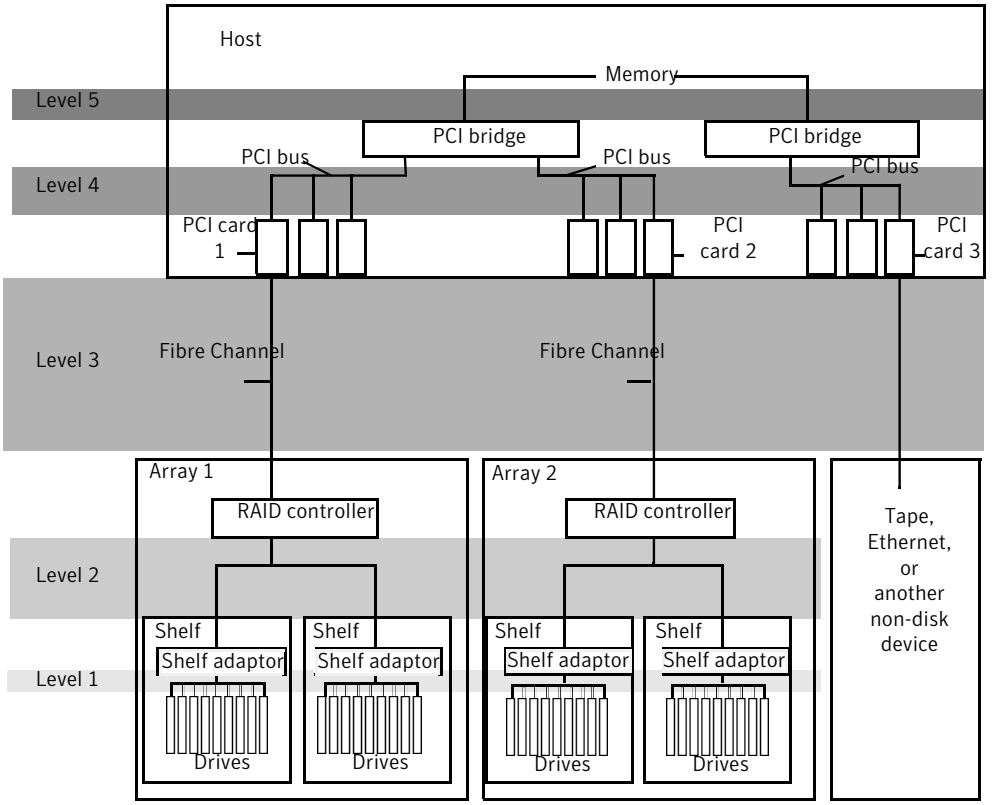
This chapter includes the following topics:

About NetBackup performance and the hardware hierarchy

The critical factors in NetBackup performance are not software-based. The critical factors are hardware selection and configuration. Hardware has roughly four times the weight that software has in determining performance.

Figure 9-1 shows the key hardware elements that affect performance, and the interconnections (levels) between them. The figure shows two disk arrays and a single non-disk device (tape, Ethernet connections, and so forth).

Figure 9-1 Performance hierarchy diagram

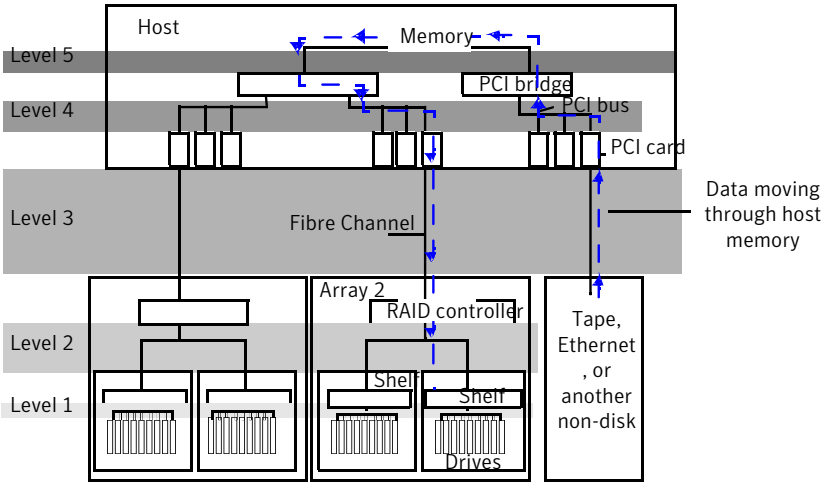


Performance hierarchy levels are described in later sections of this chapter.

In general, all data that goes to or comes from disk must pass through host memory.

Figure 9-2 includes a dashed line that shows the path that the data takes through a media server.

Figure 9-2 Data stream in NetBackup media server to arrays



The data moves up through the ethernet PCI card at the far right. The card sends the data across the PCI bus and through the PCI bridge into host memory. NetBackup then writes this data to the appropriate location. In a disk example, the data passes through one or more PCI bridges. It then passes over one or more PCI buses, through one or more PCI cards, across one or more Fibre Channels, and so on.

Sending data through more than one PCI card increases bandwidth by breaking up the data into large chunks. It also sends a group of chunks at the same time to multiple destinations. For example, a write of 1 MB can be split into 2 chunks that go to 2 different arrays at the same time. If the path to each array is *x* bandwidth, the aggregate bandwidth is approximately 2*x*.

Each level in the Performance Hierarchy diagram represents the transitions over which data flows. These transitions have bandwidth limits.

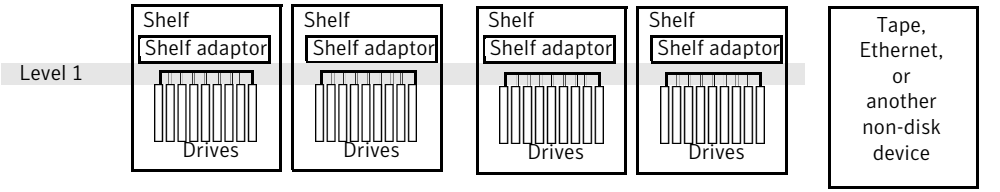
Between each level there are elements that can affect performance as well.

About performance hierarchy level 1

Level 1 is the interconnection within a typical disk array. Level 1 attaches individual disk drives to the adaptor on each disk shelf. A shelf is a physical entity placed into a rack. Shelves usually contain around 15 disk drives. If you use Fibre Channel drives, the level 1 interconnection is 1 or 2 Fibre Channel arbitrated loops (FC-AL). When Serial ATA (SATA) drives are used, the level 1 interconnect is the SATA interface.

Figure 9-3 shows the performance hierarchy level 1.

Figure 9-3 Performance hierarchy level 1



Level 1 bandwidth potential is determined by the technology used.

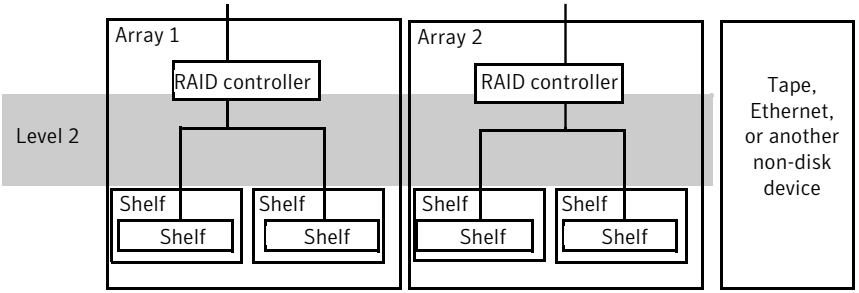
For FC-AL, the arbitrated loop can be either 1 gigabit or 2-gigabit Fibre Channel. An arbitrated loop is a shared-access topology, which means that only 2 entities on the loop can communicate at one time. For example, one disk drive and the shelf adaptor can communicate. So even though a single disk drive might be capable of 2-gigabit bursts of data transfers, the bandwidth does not aggregate. That is, multiple drives cannot communicate with the shelf adaptor at the same time, resulting in multiples of the individual drive bandwidth.

About performance hierarchy level 2

Level 2 is the interconnection external to the disk shelf. It attaches one or more shelves to the array RAID controller. This interconnection is usually FC-AL, even if the drives in the shelf are something other than Fibre Channel (SATA, for example). This shared-access topology allows only one pair of endpoints to communicate at any given time.

Figure 9-4 shows the performance hierarchy level 2.

Figure 9-4 Performance hierarchy level 2



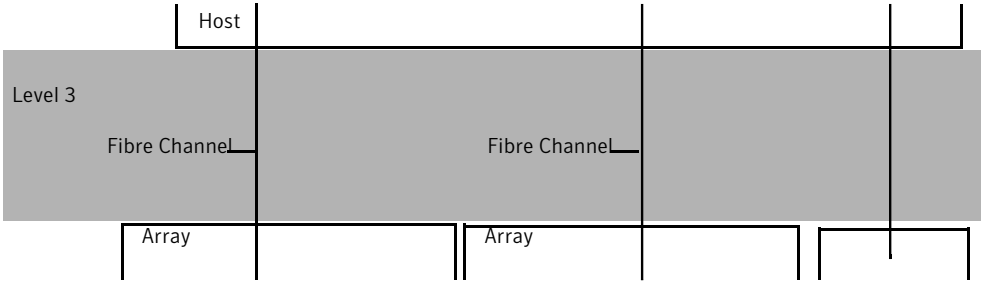
Larger disk arrays have more than one internal FC-AL. Shelves may even support 2 FC-AL, so that two paths exist between the RAID controller and every shelf, which provides for redundancy and load balancing.

About performance hierarchy level 3

Level 3 is the interconnection external to the disk array and host.

Figure 9-5 shows the performance hierarchy level 3.

Figure 9-5 Performance hierarchy level 3



This diagram shows a single point-to-point connection between an array and the host. A real-world scenario typically includes a SAN fabric (with one or more Fibre Channel switches). The logical result is the same, in that either is a data path between the array and the host.

When these paths are not arbitrated loops (for example, if they are fabric Fibre Channel), they do not have the shared-access topology limitations. That is, two arrays may be connected to a Fibre Channel switch and the host may have a single Fibre Channel connection to the switch. The arrays can then communicate at the same time (the switch coordinates with the host Fibre Channel connection). However, this arrangement does not aggregate bandwidth, since the host is still limited to a single Fibre Channel connection.

Fibre Channel is generally 1 or 2 gigabit (both arbitrated loop and fabric topology). Faster speeds are available. A general rule-of-thumb when considering protocol overhead is to divide the gigabit rate by 10 to get an approximate megabyte-per-second bandwidth. So, 1-gigabit Fibre Channel can theoretically achieve approximately 100 MB per second. 2-gigabit Fibre Channel can theoretically achieve approximately 200 MB per second.

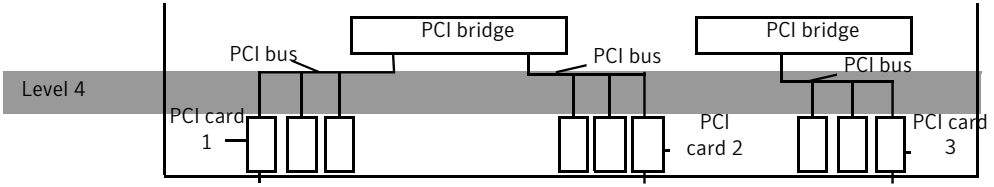
Fibre Channel is also similar to traditional LANs, in that a given interface can support multiple connection rates. That is, a 2-gigabit Fibre Channel port can also connect to devices that only support 1 gigabit.

About performance hierarchy level 4

Level 4 is the interconnection within a host for the attachment of PCI cards.

Figure 9-6 shows the performance hierarchy level 4.

Figure 9-6 Performance hierarchy level 4



A typical host supports 2 or more PCI buses, with each bus supporting 1 or more PCI cards. A bus has a topology similar to FC-AL: only 2 endpoints can communicate at the same time. That is, if 4 cards are in a PCI bus, only one of them can communicate with the host at a given instant. Multiple PCI buses are implemented to allow multiple data paths to communicate at the same time, for aggregate bandwidth gains.

PCI buses have 2 key factors involved in bandwidth potential: the width of the bus - 32 bits or 64 bits, and the clock or cycle time of the bus (in MHZ).

As a rule of thumb, a 32-bit bus can transfer 4 bytes per clock and a 64-bit bus can transfer 8 bytes per clock. Most modern PCI buses support both 64-bit and 32-bit cards.

PCI buses are available in the following clock rates:

- 33 MHz
- 66 MHz
- 100 MHz (sometimes referred to as PCI-X)
- 133 MHz (sometimes referred to as PCI-X)

PCI cards also come in different clock rate capabilities.

Backward compatibility is very common; for example, a bus that is rated at 100 MHz supports 100, 66, and 33 MHz cards.

Likewise, a 64-bit bus supports both 32-bit and 64-bit cards.

PCI buses can also be mixed. For example, a 100-MHz 64-bit bus can support any mix of clock and width that are at or below those values.

Note: In a shared-access topology, a slow card can retard the performance of other fast cards on the same bus: the bus adjusts to the right clock and width for each transfer. One moment it can do a 100 MHz 64 bit transfer to card #2. At another moment it can do a 33 MHz 32 bit to card #3. Since the transfer to card #3 is much slower, it takes longer to complete. The time that is lost may otherwise have been used for moving data faster with card #2. A PCI bus is unidirectional: when it conducts a transfer in one direction, it cannot move data in the other direction, even from another card.

Real-world bandwidth is generally around 80% of the theoretical maximum (clock * width). Following are rough estimates for bandwidths that can be expected:

64 bit/ 33 MHz = approximately 200 MB per second

64 bit/ 66 MHz = approximately 400 MB per second

64 bit/100 MHz = approximately 600 MB per second

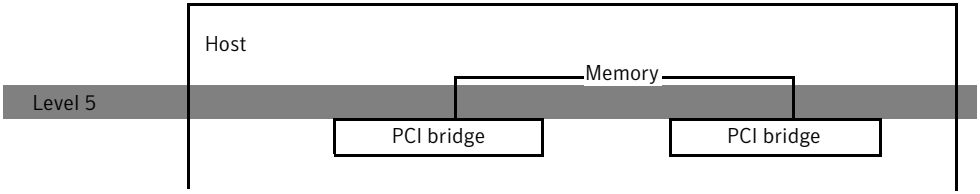
64 bit/133 MHz = approximately 800 MB per second

About performance hierarchy level 5

Level 5 is the interconnection within a host, between PCI bridge(s) and memory. This bandwidth is rarely a limiting factor in performance.

Figure 9-7 shows the Performance hierarchy level 5.

Figure 9-7 Performance hierarchy level 5



Notes on performance hierarchies

The hardware components between interconnection levels can also affect bandwidth, as follows:

- A drive has sequential access bandwidth and average latency times for seek and rotational delays.
  Drives perform optimally when doing sequential I/O to disk. Non-sequential I/O forces movement of the disk head (that is, seek and rotational latency). This movement is a huge overhead compared to the amount of data transferred. The more non-sequential I/O done, the slower it becomes.

Simultaneously reading or writing more than one stream results in a mix of short bursts of sequential I/O with seek and rotational latency in between. This situation significantly degrades overall throughput. Different drive types have different seek and rotational latency specifications. Therefore, the type of drive has a large effect on the amount of degradation.
From best to worst, such drives are Fibre Channel, SCSI, and SATA, with SATA drives usually twice the latency of Fibre Channel. However, SATA drives have about 80% of the sequential performance of Fibre Channel drives.

- A RAID controller has cache memory of varying sizes. The controller also does the parity calculations for RAID-5. Better controllers have this calculation (called "XOR") in hardware, which makes it faster. If there is no hardware-assisted calculation, the controller processor must perform it, and controller processors are not usually high performance.
- A PCI card can be limited either by the speed of the port(s) or the clock rate to the PCI bus.
- A PCI bridge is usually not an issue because it is sized to handle whatever PCI buses are attached to it.

Memory can be a limit if there is intensive non-I/O activity in the system.

Note that no CPUs exist for the host processor(s) in the Performance hierarchy diagram.

See Figure 9-1 on page 180.

While CPU performance contributes to all performance, it is not the bottleneck in most modern systems for I/O intensive workloads: very little work is done at that level. The CPU must execute a read operation and a write operation, but those operations do not take up much bandwidth. An exception is when older gigabit ethernet card(s) are involved, because the CPU has to do more of the overhead of network transfers.

Hardware examples for better NetBackup performance

These examples are not intended as recommendations for your site. The examples illustrate various hardware factors that can affect NetBackup performance.

Example 1

A general hardware configuration can have dual 2-gigabit Fibre Channel ports on a single PCI card.

In such a case, the following is true:

- Potential bandwidth is approximately 400 MB per second.
- For maximum performance, the card must be plugged into at least a 66 MHz PCI slot.
- No other cards on that bus should need to transfer data at the same time. That single card saturates the PCI bus.
- Do not expect 2 cards (4 ports total) on the same bus to aggregate to 800 MB per second, unless the bus and cards are 133 MHz.

Example 2

The next example shows a pyramid of bandwidth potentials with aggregation capabilities at some points.

Suppose you have the following hardware:

- 1x 66 MHz quad 1-gigabit ethernet
- 4x 66 MHz 2-gigabit Fibre Channel
- 4x disk array with 1-gigabit Fibre Channel port
- 1x Sun V880 server (2x 33 MHz PCI buses and 1x 66 MHz PCI bus)

In this case, the following is one way to assemble the hardware so that no constraints limit throughput:

- The quad 1-gigabit ethernet card can do approximately 400 MB per second throughput at 66 MHz.
- It requires at least a 66 MHz bus. A 33 MHz bus would limit throughput to approximately 200 MB per second.
- It completely saturates the 66 MHz bus. Do not put any other cards on that bus that need significant I/O at the same time.

Since the disk arrays have only 1-gigabit Fibre Channel ports, the Fibre Channel cards degrade to 1 gigabit each.

Note the following:

- Each card can therefore move approximately 100 MB per second. With four cards, the total is approximately 400 MB per second.
- However, you do not have a single PCI bus that can support 400 MB per second. The 66-MHz bus is already taken by an ethernet card.
- Two 33-MHz buses can each support approximately 200 MB per second. Therefore, you can put 2 of the Fibre Channel cards on each of the 2 buses.

This configuration can move approximately 400 MB per second for backup or restore. Real-world results of a configuration like this show approximately 350 MB per second.

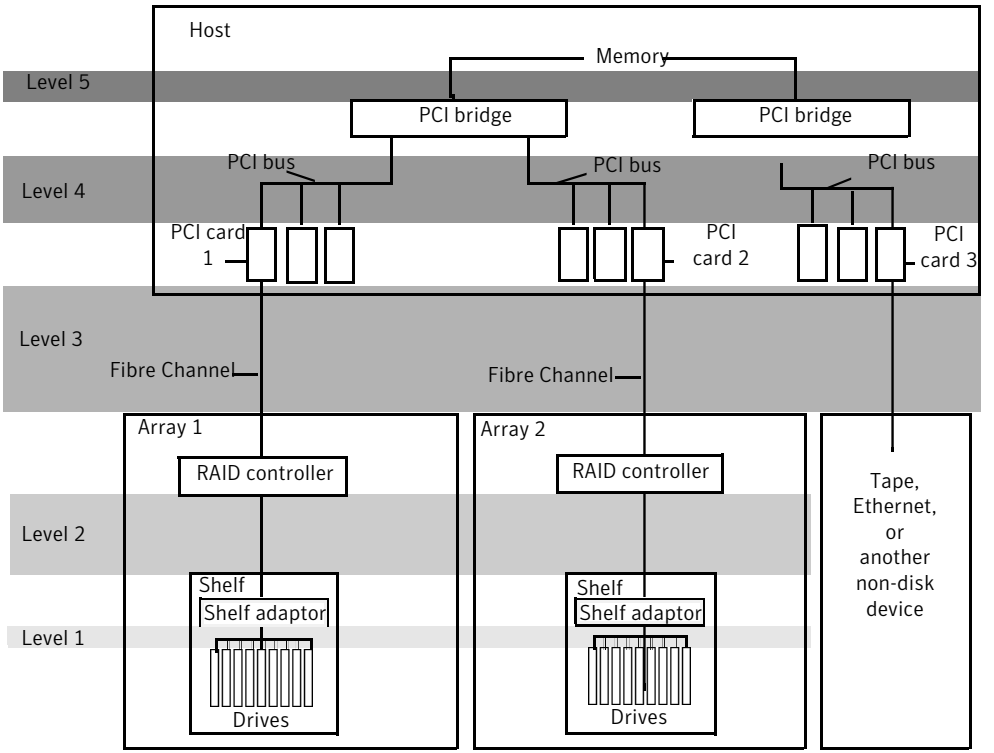
How to scale I/O operations for better NetBackup performance

The size of individual I/O operations should be scaled such that the overhead is relatively low compared to the amount of data moved. For NetBackup, that means the I/O size for a bulk transfer operation (such as a backup) should be relatively large.

The optimum size of I/O operations is dependent on many factors and varies greatly depending on the hardware setup.

Figure 9-8 is a variation on the performance hierarchy diagram.

Figure 9-8 Example hierarchy with single shelf per array



Note the following:

- Each array has a single shelf.
- Each shelf in the disk array has 9 drives because it uses a RAID 5 group of 8 + 1. That is, 8 data disks + 1 parity disk.

The RAID controller in the array uses a stripe unit size when performing I/O to these drives. Suppose that you know the stripe unit size to be 64KB. This stripe unit size means that when writing a full stripe (8 + 1), it writes 64 KB to each drive.

The amount of non-parity data is 8 * 64 KB, or 512 KB. So, internal to the array, the optimal I/O size is 512 KB. This size means that crossing Level 3 to the host PCI card should perform I/O at 512 KB.

- The diagram shows two separate RAID arrays on two separate PCI buses. You want both to perform I/O transfers at the same time.

  If each is optimal at 512 KB, the two arrays together are optimal at 1 MB.

  You can implement software RAID-0 to make the two independent arrays look like one logical device. RAID-0 is a plain stripe with no parity. Parity protects against drive failure, and this configuration already has RAID-5 parity to protect the drives inside the array.

  The software RAID-0 is configured for a stripe unit size of 512 KB (the I/O size of each unit). It is also configured for a stripe width of 2 (1 for each of the arrays).

  1 MB is the optimum I/O size for the volume (the RAID-0 entity on the host). A size of 1MB is used throughout the rest of the I/O stack.

- If possible, configure an I/O size of 1 MB for the file system that is mounted over the volume.

  The application that performs I/O to the file system also uses an I/O size of 1 MB.

  In NetBackup, I/O sizes are set in the configuration touch file:

  ```
  .../db/config/SIZE_DATA_BUFFERS_DISK.
  ```

  See "How to change the size of shared data buffers" on page 127.

Chapter 10

OS-related tuning factors for UNIX and Linux

This chapter includes the following topics:

About kernel parameters on Solaris 10

In Solaris 10, all System V IPC facilities are either automatically configured or can be controlled by resource controls. Facilities that can be shared are memory, message queues, and semaphores. These facilities can affect NetBackup performance.

Note: A change to these facilities may affect other applications that use the same facilities. Sizeable changes may result in performance trade-offs. Usually, the best approach is to make small changes and monitor the results.

For information on tuning these system resources, see Chapter 6, "Resource Controls (Overview)," in the Sun *System Administration Guide: Solaris Containers-Resource Management and Solaris Zones*.

For further assistance with Solaris parameters, refer to the *Solaris Tunable Parameters Reference Manual*, available at:

http://docs.sun.com/app/docs/doc/819-2724?q=Solaris+Tunable+Parameters

The following sections of the *Solaris Tunable Parameters Reference Manual* may be of particular interest:

- What's New in Solaris System Tuning in the Solaris 10 Release?
- System V Message Queues
- System V Semaphores
- System V Shared Memory

Recommendations on particular Solaris 10 parameters

For better NetBackup performance, Symantec recommends the following for Solaris 10.

Table 10-1 Recommendations for Solaris 10

Recommendation for Solaris 10	Description
Change the shmmax setting	Use the following setting: set shmsys:shminfo_shmmax=one half of system memory
Disable tcp_fusion	Symantec recommends that tcp_fusion be disabled. With tcp_fusion enabled, NetBackup performance may be degraded and processes such as bptm may pause intermittently. See "Disabling tcp_fusion" on page 192.

Note parameters obsolete in Solaris 10	The following parameters are obsolete in Solaris 10. These parameters can be included in the Solaris `/etc/system` file and are used to initialize the default resource control values. But Sun does not recommend their use in Solaris 10.
	`semsys:seminfo_semmns`
	`semsys:seminfo_semvmx`
	`semsys:seminfo_semmnu`
	`semsys:seminfo_semaem`
	`semsys:seminfo_semume`

Disabling tcp_fusion

For better NetBackup performance, use one of the following methods to disable tcp_fusion.

The first procedure does not require a system restart. Note however that tcp_fusion is re-enabled at the next restart. You must follow these steps each time the system is restarted.

The second procedure is simpler but requires the system to be restarted.

Caution: System operation could be disrupted if you do not follow the procedure carefully.

To use the modular debugger (mdb)

1 When no backup or restore jobs are active, run the following command:

```
echo 'do_tcp_fusion/W 0' | mdb -kw
```

2 The NetBackup processes must be restarted. Enter the following:

```
cd /usr/openv/netbackup/bin/goodies
./netbackup stop
./netbackup start
```

To use the /etc/system file

1 Add the following line in the /etc/system file.

```
set ip:do_tcp_fusion = 0
```

2 Restart the system to have the change take effect.

Message queue and shared memory parameters on HP-UX

The kernel parameters that deal with message queues and shared memory can be mapped to work on an HP-UX system. These parameters can affect NetBackup performance.

Table 10-2 is a list of HP kernel tuning parameter settings.

Table 10-2 Kernel tuning parameters for HP-UX

Name	Minimum Value
mesg	1
msgmap	514

Table 10-2 Kernel tuning parameters for HP-UX *(continued)*

Name	Minimum Value
msgmax	8192
msgmnb	65536
msgssz	8
msgseg	8192
msgtql	512
msgmni	256
sema	1
semmap	semmni+2
semmni	300
semmns	300
semmnu	300
semume	64
semvmx	32767
shmem	1
shmmni	300
shmseg	120
shmmax	Calculate shmmax using the formula that is provided under the following: See "Recommended shared memory settings" on page 131. Also note the following: shmmax = NetBackup shared memory allocation = (SIZE_DATA_BUFFERS * NUMBER_DATA_BUFFERS) * number of drives * MPX per drive

Changing the HP-UX kernel parameters

To change the HP kernel parameters, you can use the System Administration Manager (SAM).

To change the HP-UX kernel parameters

1. From SAM, select **Kernel Configuration > Configurable Parameters**.
2. Find the parameter to change and select **Actions > Modify Configurable Parameter**.
3. Key in the new value.

   Repeat these steps for all the parameters you want to change.
4. When all the values have been changed, select **Actions > Process New Kernel**.

   A warning states that a restart is required to move the values into place.
5. After the restart, the `sysdef` command can be used to confirm that the correct value is in place.

Caution: Any changes to the kernel require a restart, to move the new kernel into place. Do not make changes to the parameters unless a system restart can be performed. Otherwise, the changes are not saved.

Changing the Linux kernel parameters

To modify the Linux kernel tunable parameters, use sysctl. sysctl is used to view, set, and automate kernel settings in the `/proc/sys` directory. Most of the parameters can be changed online. To make your changes permanent, edit `/etc/sysctl.conf`. The kernel must support the procfs file system statically compiled or dynamically loaded as a module.

The default buffer size for tapes is 32K on Linux.

To change the default buffer size for tapes

1. Do one of the following:
   - Rebuild the kernel (make changes to `st_options.h`)
   - Or add a resize parameter to the startup of Linux.
     An example for a `grub.conf` entry is the following:

```
title Red Hat Linux (2.4.18-24.7.x)
root (hd0,0)
kernel /vmlinuz-2.4.18-24.7.x ro root=/dev/hda2
```

```
st=buffer_kbs:256,max_buffers:8
initrd /initrd-2.4.18-24.7.x.img
```

2 For further information on setting restart options for st, see the following: `/usr/src/linux*/drivers/scsi/README.st`, subsection BOOT TIME.

Chapter 11

OS-related tuning factors for Windows

This chapter includes the following topics:

About tuning Windows for NetBackup

Windows includes tuning parameters that can affect NetBackup performance. Some default values are not suitable for high I/O loads.

I/O paths are an important concern for backup efficiency: you need to optimize how the data is moved to avoid straining the infrastructure and to keep the backup windows to a minimum. Also important is an efficient means of restoring the data, thus the need for fast I/O from tape and disk.

The following sites provide additional information on tuning Windows systems. This information can be helpful in tuning NetBackup.

Performance Tuning Guidelines for Windows Server 2003

Performance Tuning Guidelines for Windows Server 2008 R2

Windows I/O paths

For NetBackup, you should design the I/O paths for maximum throughput on the server's backplane. Typically, data I/O enters through the network interfaces to the CPU and continues to the tape drives or disks.

Use multiple network interfaces for incoming traffic. To that end, you do not have to configure the network switch to allow IEEE802.3ad link aggregations. Allow the switch to distribute incoming packets to fully use the bandwidth.

As a rule, host-based teaming only supports failover and outbound-traffic load balancing. For NetBackup, load balancing of outbound traffic is seldom useful, except for the following cases: to vault the data between media servers, or for network-based disk pool appliances such as PureDisk, NetApp, or Data Domain.

Regarding an HBA for SAN connectivity, the I/O for disk and tape should be split. Tape I/O is synchronous and can degrade the disk I/O severely. Also, use several HBA ports to distribute traffic to the tape drives. For example, a 4GBit HBA port can serve up to four LTO3 drives. But in practice a maximum of two drives per port work better, because of I/O interrupt handling and other hardware and kernel

constraints. If possible, distribute several single port HBAs over the available I/O slots in the server. This configuration typically improves the balancing of the I/O on the backplane, CPU, and memory.

Use persistent bindings for HBAs

To avoid problems in the Windows kernel, configure each HBA with persistent bindings. If a path disappears and then becomes active again, or if the server is restarted, the kernel may allocate a new internal path name. As a result, the path NetBackup uses becomes non-functional. The message `MISSING PATH` appears in the NetBackup Device Monitor.

HBA vendors have their own tools for configuring the settings on the HBA. Refer to your vendor's documentation when configuring persistent bindings.

Recommendations for Windows software

Table 11-1 lists recommendations for Windows software that may improve NetBackup performance.

Table 11-1 Software recommendations for better NetBackup performance

Recommendation	Notes
Update Windows 2003 to version R2 with all applicable updates.	
Install additional software for SAN connectivity when disk or tape drives are SAN attached.	The software should be the latest recommended versions from the respective vendors.

Table 11-1 Software recommendations for better NetBackup performance *(continued)*

Recommendation	Notes
Disable or reconfigure Windows antivirus software when NetBackup is running.	Antivirus applications scan all files that are backed up by NetBackup, and thus load down the client's CPU. The result can be slower backups. Consider disabling Windows antivirus software. As an alternative, leave antivirus scanning enabled and work around it: ■ In the Backup, Archive, and Restore interface, on the **NetBackup Client Properties** dialog, General tab: Clear the check box for **Perform incrementals based on archive bit**. ■ Configure antivirus software to exclude NetBackup processes and directories. The following Symantec tech notes explain how to exclude NetBackup directories and processes for antivirus software: http://www.symantec.com/docs/TECH152328 http://www.symantec.com/docs/TECH56658

Disabling the Windows Removable Storage service

Many services are started automatically on Windows servers. Some can safely be left started, but the Removable Storage service should always be disabled. This service interferes with NetBackup's device management. (See the procedure in this topic.)

After the Removable Storage service is disabled, DCOM errors may be logged in the system event viewer log. The following tech note describes a work-around for these errors:

http://www.symantec.com/docs/TECH16248

Note also: When backing up the NetBackup servers, the bpbkar process logs an error because the Removable Storage service is not running. To fix this problem, exclude the `<system_drive>:\WINDOWS\system32\ntmsdata` directory from the backups. The following tech note describes how to exclude the directory:

http://www.symantec.com/docs/TECH19862

To disable the Removable Storage service

1. Click **Start > Administrative Tools > Services**.
2. Double click the **Removable Storage** service to open the properties.
3. If the service is running, click **Stop** to stop the service.
4. Change the **Startup type** to **Disabled**, then click **OK**.

Disabling Windows device driver verification

Use the latest supported combination of device drivers and firmware for network adapters and HBAs. Note that most disk drives come with the default settings that are more or less optimum.

By default, Windows 2003 and 2008 randomly test device drivers. You can improve performance by disabling that test feature. Otherwise, the kernel spends unnecessary time repeatedly testing drivers.

Use the following registry parameter to disable device driver testing. The registry parameter applies to Windows 2003 and 2008. As of this writing, it is not clear whether disabling this feature is needed for Windows 2008 R2.

Table 11-2 Parameter to disable device driver testing: Windows 2003 and 2008

Windows registry parameter (DWORD)	Recommended value
HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management\DontVerifyRandomDrivers	1

To disable the Windows device driver verification

1. On the Windows server, click **Start > Run** and enter `regedit`.
2. To be on the safe side, make a backup of the current registry (**File > Export**).
3. Go to **HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management** and create a DWORD called `DontVerifyRandomDrivers`.
4. Right-click on the new DWORD, select **Modify**, and enter 1 as the value.
5. Click **OK**.
6. Exit the registry editor, then turn off and restart the system.

Disabling the Test Unit Ready request

For tape libraries on a SAN with the tape drives that are shared among several media servers: disable the Test Unit Ready (TUR) functionality for the tape device drivers. For instructions, refer to the following Microsoft article:

Windows Server 2003 cannot perform backup jobs to tape devices on a storage area network

http://support.microsoft.com/kb/842411

The TUR requests affect NetBackup when it uses the Shared Storage Option (SSO) for tape drives. With SSO and TUR, any Windows media server may send SCSI commands to the drives to check whether they are ready. In SSO configurations, another host may need a tape drive: any SCSI commands that are sent from another server would interfere. As a result, backup and restore operations experience problems such as slow performance or even failures.

Adjust the size of the Windows virtual memory swap file

It is important to properly size the Windows virtual memory swap file before you install NetBackup. A general recommendation is to have a swap file at least twice the size of physical memory. The swap file must be preset to that size, not automatically extended.

When a swap file is extended automatically, the I/O operation in memory is denied and NetBackup reports a job failure (usually status 81). This failure in effect aborts the backup job on the media server. On Windows, this problem can be avoided only by pre-sizing the swap file.

Tuning the Windows file system cache

By default, Windows 2003 is optimized for file services. Windows prioritizes the file system cache in memory. For media servers sending data directly to tape, to a NAS device, or to other OpenStorage devices, note: it may be better to optimize the kernel by means of the parameters in Table 11-3.

Note: Media servers that have a Basic or Enterprise type of disk storage unit may be better off with the default setting.

The following registry variables can be used to tune file system cache.

Table 11-3 Registry parameters for tuning the Windows file system cache

Windows registry parameter (DWORD)	Recommended value	Notes
HKLM\System\CurrentControlSet\Services\LanmanServer\Parameters\Size	3	The default is 3, which maximizes throughput for both file sharing as well as network applications.
HKLM\System\CurrentControlSet\Control\Session Manager\Memory Management\LargeSystemCache	0	The LargeSystemCache variable should be set to 0 to minimize the file system cache and thus allow more memory for network applications. On servers with a lot of memory, such as 8GB or more, both of these settings may be left unchanged.

For instructions on how to change registry values, see the following topic (substitute the appropriate registry path, parameter names, and values):

See "Disabling Windows device driver verification" on page 201.

Disabling last accessed time stamping

The NTFS file system records the last accessed time for each file and directory. Recording last accessed time creates additional I/O operations. Because the catalog database consists of many thousands if not millions of files, requiring the kernel to update each file access adds overhead.

Some audit policies do not require last accessed information. Note that the NetBackup master server can benefit from disabling it.

Table 11-4 Parameter to disable last-accessed time stamping

Windows registry parameter (DWORD)	Recommended value
HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NTFSDisableLastAccessUpdate	1 (Disables last access time stamping.)

For instructions on how to change registry values, see the following topic (substitute the appropriate registry path, parameter names, and values):

See "Disabling Windows device driver verification" on page 201.

Disabling Windows 8.3 file names

The NTFS file system keeps a short name for every file, to maintain compatibility with older operating systems. This setting is not required for a NetBackup master server. By disabling it, you decrease the number of I/O operations per file creation.

Note: If 8.3 file names are disabled, verify that no 16-bit applications run on the master server.

Table 11-5 Parameter to disable 8.3 format file names

Windows registry parameter (DWORD)	Recommended value
HKLM\SYSTEM\CurrentControlSet\Control\FileSystem\NTFSDisable8dot3NameCreation	1

For instructions on how to change registry values, see the following topic (substitute the appropriate registry path, parameter names, and values):

See "Disabling Windows device driver verification" on page 201.

Adjusting the TCP KeepAliveTime parameter

Several TCP parameters can be tuned to better accommodate typical NetBackup I/O. The I/O pattern for a Windows server is normally not a sustained data-transfer, but rather short bursts of I/O.

In certain situations, a delay may occur on a NetBackup master server before it detects that the connection to a media server has been aborted. For example, if a media server goes down during a backup, a delay may occur on the master server before it detects that the media server is no longer available. While at first there may appear to be a problem with the NetBackup master server, this delay results from a TCP/IP configuration parameter called `KeepAliveTime`. By default this parameter is set to 7,200,000 milliseconds (two hours). Decrease the value to 900,000 milliseconds (15 minutes).

The delay causes NetBackup jobs on the media server to appear to be active after the connection to the media server has gone down. The result is an undesirable

delay before the current backup job fails and before the NetBackup retry logic starts.

A shorter timeout delay may also be needed if the I/O path includes a firewall. Firewalls are often encountered in secure networks, or when backing up the servers that are located in a DMZ or untrusted network. Firewalls typically drop the session if no traffic occurs for a set time. NetBackup does not respond well and the jobs fail. These problems usually happen during incremental backups, when the client may take a long time to send data to the media server. To solve this problem, set KeepAliveTime to a value lower than the firewall's timeout.

Table 11-6 Parameter for KeepAliveTime

Windows registry parameter (DWORD)	Recommended value
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime	0xDBBA0 (= 900,000 milliseconds, or 15 minutes)

To reduce the TCP keepalive time delay

1. On the Windows server, click **Start > Run** and enter `regedit`.
2. To be on the safe side, make a backup of the current registry (**File > Export**).
3. Go to **HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters** and create a DWORD called `KeepAliveTime`.
4. Right-click on the new DWORD, select **Modify**, and enter 1 as the value.
5. Click **OK**.
6. Exit the registry editor, then turn off and restart the system.

Adjusting TCPWindowSize and Window Scaling

The TCPWindowSize parameter determines the largest possible TCP receive window. In Windows 2003, the TCPWindowSize parameter for gigabit network interfaces should be set to its maximum value of 65535.

Note: In Windows 2008 and 2008 R2, this parameter is obsolete and is disregarded by the kernel.

Table 11-7 Windows 2003: Parameter to adjust TCPWindowSize

Windows 2003 registry parameter (DWORD)	Recommended value (decimal)
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpWindowSize	65535

The TCPWindowSize variable can be increased to a value of 1GB. Once this variable is set and the system is restarted, the TCP/IP stack supports large windows.

For Windows 2003, it may also help to allow TCP window scaling, to allow a TCP receive window larger than 64KB. Adjusting TCP window scaling may not be necessary: use trial and error to determine whether the following parameter improves the I/O throughput.

Table 11-8 Windows 2003: Parameter to adjust TCP window scaling

Windows 2003 registry parameter (DWORD)	Recommended value
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\Tcp1323Opts	1

Note: Like TCPWindowSize, Tcp1323Opts is deprecated in Windows 2008 and 2008 R2.

For instructions on how to change registry values, see the following topic (substitute the appropriate registry path, parameter name, and value):

See "Disabling Windows device driver verification" on page 201.

Increase the value of the MaxHashTableSize parameter

It may be useful to set the `MaxHashTableSize` variable to a higher value. A higher value may be helpful on media servers with many concurrent connections, such as for high multiplexing and many concurrent sessions to disk. The default is 128 * CPUs^2. The maximum value is 65535 (DWORD).

Note: Windows 2008 and 2008 R2: this parameter is obsolete and is disregarded by the kernel.

Table 11-9 Windows 2003: MaxHashTableSize parameter

Windows 2003 registry parameter (DWORD)	Recommended value (decimal)
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\MaxHashTableSize	65535

For instructions on how to change registry values, see the following topic (substitute the appropriate registry path, parameter name, and value):

See "Disabling Windows device driver verification" on page 201.

Change the value of the NumTcbTablePartitions parameter

By default this variable is calculated as the number of CPUs[2]. This setting may not be good for servers with 8 or more CPUs. For most large servers it is better to use a value equal to four times the number of CPUs.

Note: Windows 2008 and 2008 R2: this parameter is obsolete and is disregarded by the kernel.

Table 11-10 Windows 2003: NumTcbTablePartitions parameter

Windows 2003 registry parameter (DWORD)	Recommended value (decimal)
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\NumTcbTablePartitions	16

For instructions on how to change registry values, see the following topic (substitute the appropriate registry path, parameter name, and value):

See "Disabling Windows device driver verification" on page 201.

Increasing the MaxUserPort parameter

The default number of ports per IP address is only 5000. For a large NetBackup domain, 5000 may not be sufficient for all required connections between the master server, media servers, and clients. As a rule, an increase in this value is only useful on master and media servers. It may be useful on the client as well, if for example the client serves as a web server or database server.

Windows 2003 supports up to 65534 concurrent ports per IP address. The MaxUserPort parameter does not exist by default, and must be created manually.

The first 1024 ports are reserved, thus it makes little sense to set it to maximum value. If a host has more than 60000 concurrent connections, other problems may exist. Examples are CPU and disk bottlenecks. A value of 60000 however would provide ample room.

Table 11-11 Windows 2003: MaxUserPort parameter

Windows 2003 registry parameter (DWORD)	Recommended value (decimal)
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\MaxUserPort	60000

For instructions on how to change registry values, see the following topic (substitute the appropriate registry path, parameter name, and value):

See "Disabling Windows device driver verification" on page 201.

The procedure for increasing the available ports is different in Windows 2008 and 2008 R2. Use the `netsh` command to configure a start port and the range. By default, the start port is 49152 and the end port is 65535, which provides 16383 usable dynamic ports. If the NetBackup environment is very large, you may have to increase the range. Enter the following commands to allow 60000 connections:

```
netsh int ipv4 set dynamicport tcp start=10000 num=50000

netsh int ipv4 set dynamicport udp start=10000 num=50000

netsh int ipv6 set dynamicport tcp start=10000 num=50000

netsh int ipv6 set dynamicport udp start=10000 num=50000
```

The UDP ports are set to have the same range as TCP, but NetBackup does not use UDP ports.

Increasing the number of kernel threads

By default, Windows does not optimize the kernel for large numbers of concurrent threads. When the OS is started the kernel allocates structures for the kernel worker threads that carry out the work that the running processes require. Examples are device driver I/O, the kernel itself, and other internal components.

NetBackup puts a very high load on the master servers and media servers: it starts many processes on the servers for each active job. A master server in a domain of approximately 300 clients may require all the kernel threads that Windows creates by default.

In some cases, you can distribute the backup jobs over a longer period of time, to live within the default number of threads. But that may not be feasible. As an

alternative, you can increase the kernel threads to their maximum number, so that the kernel can serve as many processes as possible.

Use the following Windows parameters:

- DefaultNumberofWorkerThreads
- AdditionalDelayedWorkerThreads
- AdditionalCriticalWorkerThreads

Table 11-12 describes these parameters.

All three variables use DWORD as their type. The AdditionalDelayedWorkerThreads and AdditionalCriticalWorkerThreads variables should already exist.

Table 11-12 Kernel thread parameters (DWORD)

Windows registry parameter (DWORD)	Recommended value (decimal)	Description
HKLM\SYSTEM\CurrentControlSet\Services\RpcXdr\Parameters\DefaultNumberofWorkerThreads	64	Controls the number of threads that are allocated for each work queue in the kernel. The `RpcXdr\Parameters\DefaultNumberofWorkerThreads` path and variable may have to be created. **Note:** Allocating too many threads may use more system resources than what is optimal.
HKLM\SYSTEM\CurrentControlSet\Control\ Session Manager\Executive\AdditionalDelayedWorkerThreads	16	For the work that is not real-time or time-critical. Memory pages for these threads may be swapped out from CPU cache and memory while in queue.
HKLM\SYSTEM\CurrentControlSet\Control\ Session Manager\Executive\AdditionalCriticalWorkerThreads	16	For the time-critical processes that have high priority and for which the memory pages must stay in CPU cache or memory.

For instructions on how to change registry values, see the following topic (substitute the appropriate registry path, parameter name, and value):

See "Disabling Windows device driver verification" on page 201.

Configuring CPU affinity

On media servers with many CPUs, note: you can improve I/O throughput by assigning certain CPUs to network I/O and other CPUs to tape I/O or disk I/O. Such an assignment is called CPU (or processor) affinity.

With CPU affinity, the OS thread scheduler avoids unnecessary context switches. Instead, the various I/O threads sit on their respective CPUs. Context switching and memory page faults are very expensive in high I/O load applications such as NetBackup.

The CPU affinity can be configured by means of the Interrupt-Affinity Filter Tool (intfiltr.exe) in the Windows 2003 Resource Kit Tools.

Caution: Use great care with this tool!

Note the following:

- Use the intfiltr.exe tool from the physical console.
- The intfiltr.exe tool allows selecting the various devices present in the system. Select a network device and add it to the interrupt filter.
- You may have to select “Don’t Restart Device when Making Changes” before adding it to the filter, to avoid service interruption or a system crash.
- Once the device is present in the filter, the CPU masking can be set by clicking on the “Set Mask” button in the “Interrupt Affinity Mask box.”

Note: Some devices may not work with the affinity setting. A restart may be necessary. If the device does not work after a restart, remove the filter. In that case, no CPU affinity can be used for that device.

In Windows 2008, the intfiltr.exe tool has been replaced by the Interrupt-Affinity Policy (IntPolicy) tool. The following Microsoft document contains more information:

Interrupt-Affinity Policy Tool

http://msdn.microsoft.com/en-us/windows/hardware/gg463378

Windows 2008 R2 provides better control of resources with the NUMA (non-uniform memory access) architecture. Applications that demand high performance are written so that the threads are distributed to several cores or maintained on a CPU. In general, the principle of locality generates fewer context switches on the CPUs.

About Windows data buffer size

The size limit for data buffers on Windows is 1024 KB. This size is calculated as a multiple of operating system pages (one page = 4 KB). Therefore, the maximum is 256 OS pages, from 0 to 255 (the hex value 0xFF). A larger setting defaults to 64 KB, which is the default size for the scatter-gather list.

The maximum usable block size is dependent on the host bus adapter (HBA) miniport driver, not on the tape driver or the OS. For example, the readme for the QLogic QLA2200 card contains the following:

```
* MaximumSGList
```

Windows includes enhanced scatter-gather list support for very large SCSI I/O transfers. Windows supports up to 256 scatter-gather segments of 4096 bytes each, for transfers up to 1048576 bytes.

Note: The OEMSETUP.INF file has been updated to automatically update the registry to support 65 scatter-gather segments. Normally, no additional changes are necessary: this setting typically results in the best overall performance.

SGList (scatter-gather list) registry value

The SGList registry parameter sets the number of pages that can be either scattered or gathered (that is, read or written) in one DMA transfer. For the QLA2200, you set the parameter MaximumSGList to 0xFF (or to 0x40 for 256Kb) and can then set 256Kb buffer sizes for NetBackup. Use extreme caution when you modify this registry value. You should always contact the vendor of the SCSI or Fibre channel card first to ascertain the maximum value that a particular card supports.

The same should be possible for other HBAs, especially Fibre channel cards.

The default for JNI Fibre cards that use driver version 1.16 is 0x80 (512 KB or 128 pages). The default for the Emulex LP8000 is 0x81 (513 KB or 129 pages).

For this approach to work, the HBA has to install its own SCSI miniport driver. If it does not, transfers are limited to 64 KB, for legacy cards such as old SCSI cards.

The built-in limit on Windows is 1024 KB, unless you use the default Microsoft miniport driver for legacy cards. The limitations are all to do with the HBA drivers and the limits of the physical devices that are attached to them.

For example, Quantum DLT7000 drives work best with 128-KB buffers and StorageTek 9840 drives with 256-KB buffers. If these values are increased too far, damage can result. The HBA or the tape drives or any devices in between (such as fibre bridges and switches) can be damaged.

Adjusting Windows data buffer size

You can adjust the data buffer size on Windows as follows.

To change the Windows data buffer size

1. Click **Start > Run** and open the REGEDT32 program.
2. Select **HKEY_LOCAL_MACHINE** and follow the tree structure down to the HBA driver as follows:

   HKEY_LOCAL_MACHINE > SYSTEM > CurrentControlSet > Services > *HBA_driver* **> Parameters > Device**

   For QLogic, the *HBA_driver* is Ql2200.
3. Adjust the SGList parameter.

   Do the following:

   - Double click MaximumSGList:REG_DWORD:0x21
   - Enter a value from 16 to 255 (0x10 hex to 0xFF).
     A value of 255 (0xFF) enables the maximum 1-MB transfer size. A value higher than 255 reverts to the default of 64-KB transfers. The default value is 33 (0x21).
     More information is available on this parameter.
     See "SGList (scatter-gather list) registry value" on page 211.
4. Click **OK**.
5. Exit the registry editor, then turn off and restart the system.

Requirements for NetBackup configuration files on Windows

Note the following requirements for NetBackup's configuration files on Windows:

- If you create a configuration file on Windows for NetBackup, the file name must match the file name that NetBackup expects.
  Make sure that the file name does not have an extension, such as .txt. (On UNIX systems, such files are called touch files.)
  If you create a NOexpire file to prevent the expiration of backups, the file does not work if the file's name is NOexpire.txt.
- The configuration file must use a supported type of encoding, such as ANSI. Unicode encoding is not supported. If the file is in Unicode, it does not work.

To check the encoding type, open the file using a tool that displays the current encoding, such as Notepad. Select **File > Save As** and check the options in the **Encoding** field. ANSI encoding works properly.

Appendix A

Additional resources

This appendix includes the following topics:

- Additional tuning resources on NetBackup

Additional tuning resources on NetBackup

Table A-1 lists additional sources of information for tuning NetBackup.

Table A-1 Additional tuning resources on NetBackup

Type of resource	Sources of information
Vision online	For information on NetBackup tuning from Vision online, click the following and search on "vision": http://www.symantec.com/stn/vision/index.jsp
Performance monitoring utilities	The following article discusses how and why to design a scalable data installation. "High-Availability SANs," Richard Lyford, FC Focus Magazine, April 30, 2002.
Freeware tools for bottleneck detection	Information is available from the following sources: ■ Bonnie, for measuring the performance of UNIX file system operations. http://www.textuality.com/bonnie ■ Bonnie++, extends the capabilities of Bonnie. http://www.coker.com.au/bonnie++/readme.html ■ Tiobench, for testing I/O performance with multiple running threads. http://sourceforge.net/projects/tiobench/

Table A-1 Additional tuning resources on NetBackup *(continued)*

Type of resource	Sources of information
Mailing list resources	Information is available from the following sources: ■ Veritas NetBackup news groups. http://forums.veritas.com Search on the keyword "NetBackup" to find threads relevant to NetBackup. ■ The email list Veritas-bu discusses backup-related products such as NetBackup. Archives for Veritas-bu are located at: http://mailman.eng.auburn.edu/mailman/listinfo/veritas-bu

Index

Symbols

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

T

U

V

W