Symantec NetBackup™ for Microsoft Exchange Server Administrator's Guide

for Windows

Release 7.5

✔Symantec.

Symantec NetBackup™ for Microsoft Exchange Server Administrator's 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 version: 7.5

Legal Notice

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, DVDs, 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

Chapter 7   Protecting Exchange Server data with VMware backups 193

Chapter 8   Recovering an Exchange database to a repaired or an alternate Exchange server 203

Chapter **1**

Introducing NetBackup for Exchange

This chapter includes the following topics:

- About NetBackup for Exchange
- Features of NetBackup for Exchange
- NetBackup for Exchange terminology
- About Exchange backup operations
- About Exchange restore operations
- About Exchange backups and Granular Recovery Technology (GRT)
- About snapshot backups with Exchange Server
- About Exchange Instant Recovery methods
- About Exchange backups and restores in a VMware environment
- NetBackup documentation

About NetBackup for Exchange

NetBackup for Microsoft Exchange Server extends the capabilities of NetBackup to include online backups and restores of Exchange databases when Exchange Server is installed. This capability is provided as an add-on or extension to the NetBackup for Windows client software. Because this product is tightly integrated with the Backup, Archive, and Restore interface, this topic only gives an overview of NetBackup functionality. In general, backup and restore operations for Exchange files are identical to other NetBackup file operations.

Features of NetBackup for Exchange

Table 1-1 describes the features of the NetBackup for Exchange Server agent.

Table 1-1   NetBackup for Exchange Server features

Feature	Description
Tight NetBackup integration	Tight integration with NetBackup allows for the following:
	■ An administrator already familiar with NetBackup procedures and software can easily configure and use NetBackup to perform Exchange Server backup and restore operations.
	■ Features and strengths of the NetBackup product suite are available to the Exchange Server backup user. These features include software data compression and encryption, scheduled and user-directed operations, backups of multiple data streams, and in-line tape copy.
	See the *NetBackup Administrator's Guide, Volume I.*
Central administration	Administrators can define, back up, and restore Exchange Servers and other NetBackup client computers from a central location.
Media management	Exchange Server backups can be saved directly to a wide variety of storage devices that the NetBackup master server supports.
Minimal backup time	An administrator has the choice of to perform full or incremental backups. A full backup may take considerable time, so it may be performed infrequently. In the interim, any updates that occurred since the full backup can be quickly and incrementally backed up through a transaction log backup. In the event of a failure, the full backups and incremental backups would be restored.
	During recovery, the Exchange Server updates the databases and applies each of the logged transactions to the database. After the Exchange Server recovery completes, the system is brought back to the state as it existed when the last incremental backup was performed.
Exchange Server Backup methods	NetBackup supports all Exchange Server backup methods: full backups, cumulative incremental backups, and differential incremental backups. User backups function as copy backups.
Online backups	Exchange Server data and transaction logs can be backed up without taking the Exchange Server offline. Exchange services and data remain available during the Exchange Server backup.
Automated backups	Administrators can set up schedules for automatic, unattended backups for local or remote clients across the network. These backups can be full or incremental and are managed entirely by the NetBackup server from a central location. The administrator can also manually back up the clients.
Restore operations	An administrator using the Backup, Archive, and Restore interface can browse backups and select the ones to be restored.

Table 1-1	NetBackup for Exchange Server features *(continued)*
Feature	**Description**
Support for VMware backups that protect Exchange	Users can create consistent full backups of virtual machines running Exchange Server. You can restore Exchange storage groups or databases and individual database objects from a VMware image.
Exchange 2010 standalone server and DAG support	NetBackup for Exchange supports backups of Exchange 2010 standalone servers and Exchange 2010 Database Availability Groups (DAGs). VSS is the only backup Microsoft supports of Exchange 2010 backups. For a DAG, NetBackup supports backups of the active and the passive VSS writer of a Database Availability Group (DAG). When NetBackup backs up the data that is replicated the benefit is that I/O impact is reduced on the active Exchange server. NetBackup accesses the replicated data and leaves the active (or live) Exchange server alone. You can also configure a list of preferred servers you want to use to perform backups.
Exchange 2007 and earlier backup and restore features	NetBackup can back up and restore storage groups and databases within the storage group. The capabilities of this feature are as follows: ■ Scheduled backups of individual storage groups and databases ■ User-directed backups of individual storage groups and databases ■ Restores of individual storage groups and databases. These restores can be performed with the Backup, Archive, and Restore interface (on the server or on the client). Or you can use the Remote Administration Console for Windows or UNIX.
Exchange 2007 and later enhancements to consistency checks of snapshot backups	For snapshot backups, NetBackup uses the Microsoft consistency check API to check the consistency of databases and transaction logs and to provide additional details. This speeds up a snapshot backup, because it allows the backup to proceed in parallel with the consistency check. For an Exchange 2010 DAG, you can disable the consistency check or ignore the check and continue with the backup.
Snapshot backups and restores	NetBackup for Exchange can perform backups and restores of Exchange objects with snapshot methodology. With a separate Snapshot Client license, you can perform off-host backups, Instant Recovery backups, and backups with a hardware provider. See "About snapshot backups with Exchange Server" on page 20.
Restores of individual items using Granular Recovery Technology (GRT)	When a backup uses GRT, users can restore individual mailbox and public folder items directly from any full database backup. See "About Exchange backups and Granular Recovery Technology (GRT)" on page 19.
Redirected restores of mailbox objects	You can restore mailboxes, mailbox folders, mailbox messages, public folders, and public folder items to a new location.
Redirected restores of databases or storage groups	Exchange 2007 and later backups can be restored to another database or another storage group on the local server or on a different server. Exchange 2003 snapshot backups can be restored to an identical storage group on a different server.

Table 1-1	NetBackup for Exchange Server features *(continued)*
Feature	**Description**
Redirection to the recovery database (RDB) or recovery storage group (RSG)	Exchange 2007 and later backups can be redirected to the recovery database or RSG. Streaming backups of Exchange 2003 can be redirected to the RSG.
Compression of backups	Compression increases backup performance over the network and reduces the size of the backup image that is stored on the disk or tape. NetBackup does not support GRT for any backups that use compression.
Encryption	When the Encryption attribute is enabled, the server encrypts the backup for the clients that are listed in the policy. NetBackup does not support GRT for any backups that use encryption.
Cluster support	The NetBackup for Exchange Server agent supports Microsoft Cluster Server (MSCS) environment and Veritas Cluster Server (VCS). See the *NetBackup Enterprise Server 7.5 Cluster Compatibility* list. This list contains information on the versions of Exchange Server that are supported with the cluster environments.
LCR/CCR support	NetBackup for Exchange with Snapshot Client supports backups of the passive VSS writer of an Exchange 2007 LCR and CCR configuration. NetBackup can back up the data that is replicated by interfacing with the replica (or passive) Exchange server. The benefit of such a backup is to reduce I/O impact on the active Exchange server. NetBackup accesses the replicated data and leaves the active (or live) Exchange server alone. This type of backup is especially beneficial for a backup of a CCR node because the active node is completely left out of the backup. VSS is the only backup Microsoft supports of this replicated data.
MAPI public folder backup and restore	With Exchange 2007 or earlier, users can perform MAPI backups and restores of individual public folder items, as follows: ■ Scheduled backups of individual folders ■ User-directed backups of individual folders ■ Restores of individual folders or documents. You can perform this type of restore can with the Backup, Archive, and Restore interface (on the server or on the client). Or you can use the Remote Administration Console.
MAPI mailbox backup and restore	With Exchange 2007 or earlier, users can perform MAPI backups and restores of individual mailboxes and folders, as follows: ■ Scheduled backups of individual mailboxes and folders ■ User-directed backups of individual mailboxes and folders ■ Restores of individual mailboxes, folders, or messages. You can perform this type of restore with the Backup, Archive, and Restore interface (on the server or on the client). Or you can use the Remote Administration Console.

Table 1-1	NetBackup for Exchange Server features *(continued)*

Feature	Description
Single Instance Storage (SIS) of mailbox message attachments	This feature applies only to Exchange 2007 or 2003 MAPI mailbox backups. Users can enable Single Instance Storage for message attachments so that NetBackup writes only one copy of an attachment to the backup.

NetBackup for Exchange terminology

Table 1-2	NetBackup for Exchange terminology

Term	Definition or description
Exchange Server, Exchange	In the *NetBackup for Microsoft Exchange Server* documentation, "Microsoft Exchange Server" is referred to as "Exchange Server" or "Exchange".
Granular Recovery Technology (GRT)	Allows a user to restore individual mailbox and public folder items from full database backups.
MAPI mailbox or MAPI public folder backups and restores	Refers to any mailbox and public folder operations that are performed with MAPI. This type of backup and restore is only available with Exchange 2007 and earlier.
Microsoft consistency check API	Refers to the Microsoft CHKSGFILS API or interface.
NetBackup File System daemon (NBFSD)	The NetBackup File System daemon on the NetBackup media server is a process that allows NetBackup clients to mount, browse, and read tar images. This process is used with a client for Granular Recovery Technology (GRT) operations. These operations include backups, browsing for backup images, restores, and duplication.
NetBackup for Microsoft Exchange Server	In the *NetBackup for Microsoft Exchange Server* documentation, "NetBackup for Microsoft Exchange Server " is referred to as "NetBackup for Exchange Server" or "NetBackup for Exchange".
Snapshot	Refers to backups and restores performed with snapshot technology. In the NetBackup for Exchange Server documentation, "VSS" is synonymous with "snapshot".
Streaming backups and restores	Refers to Exchange database backups and restores that use the Microsoft Exchange Backup and Restore API and not snapshot technology or the VSS provider.
VSS	Refers to the software provider used to perform snapshot backups and restores. In the NetBackup for Exchange Server documentation, "snapshot" is synonymous with "VSS".

About Exchange backup operations

NetBackup provides the following methods to perform backups:

- Automatic
- Manual
- User-directed

For more information on these backup methods and other administrator-directed activities, see the *NetBackup Administrator's Guide, Volume I*.

With automatic backups, the NetBackup administrator can schedule the full backups and the incremental backups that occur automatically and unattended. (Incremental backups can be differential incremental backups or cumulative incremental backups.) Automatic backups meet most backup requirements.

You cannot perform an automatic copy backup. To perform a copy backup, run a user-directed backup.

With manual backups, the administrator can perform immediate backups of the files that are associated with any policy, client, or schedule.

The manual backup option can be useful for the following situations:

- Testing a configuration
- When workstations miss their regular backups
- Before installing new software (to preserve the old configuration)
- Preserving records before a special event such as when companies split or merge

With the Backup, Archive, and Restore interface, the user can perform backups of Exchange Server, mailboxes, and public folders. A user-directed backup produces a copy backup for Exchange, which is a full backup that does not truncate the transaction logs.

About Exchange restore operations

With the Backup, Archive, and Restore interface, the administrator can browse for Exchange Server backups and select the ones to restore. The following types restores are available:

- Server-directed
- Redirected restores to a different client
- Redirected restores to a different target or database location

With a server-directed restore, an administrator can browse Exchange Server databases and select the ones you want to restore. NetBackup lets you select the NetBackup server from which files are restored, view the backup history, and select items to restore. You can select a specific client or other clients that were backed up by the selected NetBackup server.

When you redirect to a different client, you can restore to an Exchange client other than the one that was originally backed up. You can redirect the Exchange databases, directories, or mailbox objects. The administrator can direct restores to any NetBackup for Exchange client (regardless of which client performed the backup). To redirect a restore, the administrator can use the NetBackup Administration Console on the master server or the Remote Administration Console.

See the *NetBackup Administrator's Guide* for the configuration that is needed for this type of redirected restore.

A redirected restore to a different target or database location allows a user to restore mailbox or public folder objects to a target or a database location different from the location from which the objects were backed up. Depending on the Exchange version and type of backup, database objects can be redirected to the following:

■ The Exchange recovery database (RDB)

■ The Exchange recovery storage group (RSG)

■ Another database

■ Another storage group

About Exchange backups and Granular Recovery Technology (GRT)

When a backup uses Granular Recovery Technology (GRT), users can restore individual items directly from any full database backup. This type of backup can serve both kinds of recovery situations. From the same backup image you can restore entire storage groups or databases. Or you can select individual folders or messages within a mailbox or public folder. This backup can replace the existing MAPI mailbox backup.

You can restore individual items using GRT from the following types of backups:

■ Full or user-directed backups
Incremental backups are not yet supported.

■ Local snapshot backups

- Off-host snapshot backups
- Instant recovery backups, when the schedule copies the snapshot to a storage unit
- Replica snapshot backups
  This type of backup applies to LCR or to CCR environments with Exchange 2007 or a Database Availability Group (DAG) with Exchange 2010.
- Streaming backups (Exchange 2007 and earlier)

About snapshot backups with Exchange Server

NetBackup for Exchange Server includes support for snapshot backups. NetBackup for Exchange Server can back up and restore Exchange objects by taking snapshots of the component files. Data is captured at a particular instant. The resulting snapshot can be backed up without affecting the availability of the database. These snapshots are backed up to tape or to the storage unit.

A separate Snapshot Client license provides additional features for snapshot backups. You can configure the snapshot image for Instant Recovery and you can configure an alternate client to perform the snapshot backup.

NetBackup for Exchange supports the Microsoft Volume Shadow Copy Service (VSS) for creating a snapshot image. The actual VSS provider that is used is dependent on your hardware environment and software environment. A list of the VSS providers available for use with NetBackup for Exchange Server is available.

See the *NetBackup Snapshot Client (Advanced Client) OS, Arrays, and Database Agent Compatibility* list.

The following Snapshot Client features are available for use with NetBackup for Exchange Server:

Snapshot backup	A snapshot is a disk image of the client's data. NetBackup backs up the data from the snapshot volume, not directly from the client's original volume. Client operations and user access are allowed to continue without interruption during the backup.

Instant Recovery   NetBackup supports Instant Recovery backups with Exchange
2007 or later for non-clustered and non-replicated environments.
Instant Recovery requires a separate Snapshot Client license key.

This feature makes backups available for "instant recovery" from
disk. Instant Recovery combines snapshot technology with the
ability to do rapid disk-based restores. Optionally, the image is
retained on disk as well as backed up to storage.

To perform an Instant Recovery, one of the following methods is
used:

- Files are copied back from the snapped volume to the original
  volume
- The volume is rolled back

Off-host backup   NetBackup supports off-host backups of Exchange using an
alternate client. Off-host backups require a separate Snapshot
Client license key.

Off-host backups use a second, or alternate, client to perform the
backup on behalf of the primary client. Compared to local Snapshot
Client backups, this approach reduces the backup I/O burden on
the primary client.

NetBackup also supports off-host Instant Recovery backups for
Exchange 2007 and later.

See "Configuration and licensing requirements for Exchange snapshot backups
and restores" on page 28.

See "Limitations of Exchange snapshot operations" on page 103.

About Exchange Instant Recovery methods

If the snapshot is preserved with the Instant Recovery option, NetBackup restores
the database using rollback of the snapshot volume(s) when appropriate. Usually,
a rollback of the snapshot volume(s) that contain the Exchange files is the fastest
way. However, the whether or not a rollback is appropriate depends on several
things: the configuration of the Exchange database files, the contents of the
volumes, and configuration of the disk array. If a volume rollback cannot be
performed, the files that are required for restoration are copied from the snapshot
volume to the destination volume. Instant recovery of Exchange differs from
Instant Recovery of a file system. For Exchange, NetBackup decides which recovery
method to use. For file system restores, the user chooses the Instant Recovery
method.

NetBackup uses the following methods during an Exchange database restore to restore the physical files:

Volume rollback	The entire volume is rolled back, or resynchronized, by using the snapshot. This method overwrites the entire volume with the snapped volume.
File copy back	Individual files are copied back from the snapped volume to the current volume.

To determine if a volume can be rolled back, checks are made to insure that the same list of files exists in the following places:

- The snapshot volume is compared with the cataloged list of files to restore. These lists must match exactly. An example of a difference is a file that was included in the snapshot, but was not cataloged because it is not an Exchange file. The snapshot is not rolled back because that action overwrites the non-Exchange file. Exchange files also may exist on the snapshot but not in the catalog if the backup did not include all the databases on the volume.

- The snapshot volume is compared with the current volume. All files on the current volume must also exist in the snapshot. If there is a file that is not on the snapshot, a rollback is not performed because that action does not restore that file.

In both comparisons, NetBackup excludes certain files from consideration. For example, unneeded Exchange transaction logs, files Exchange re-generates, or any files that are artifacts of the NetBackup process. The `bppfi` log shows when such a file difference is found and excluded from consideration.

The copy-back restore method is used in the following situations:

- If the system provider is used and the snapshot selected for restore is not the most recent snapshot

- If there are other files on the volume that could be lost

- If all the files on the snapshot are not selected for restore

- If you select **Roll-Forward Recovery**. The copy-back method must be used for the volume that contains the log files. A roll-forward recovery needs the log files that were created since the backup. A rollback cannot be performed since it removes those log files. If the database file (`.edb`) is on a different volume, that volume is still evaluated with the other criteria to determine if it is eligible for rollback.

If multiple volumes are included in the restore set, each volume is evaluated separately to determine if it is eligible for rollback. (The restore set is based on the location of the Exchange database, transaction logs, and system files that are

part of the restore.) For example, perhaps the volume that contains the database files is eligible for rollback, but the volume that contains log files has extra, non-Exchange files. At the time of the restore, only the volume that contains the database files is rolled back. All the log files are copied back from the snapshot to the current volume.

See "Configuring a snapshot policy for Exchange Server" on page 106.

See "About configuration requirements for the Exchange Server when you use Instant Recovery" on page 116.

About Exchange backups and restores in a VMware environment

In NetBackup 7.5, application-aware VMware backups provide a single pass backup that protects Exchange Server. From one VMware backup the following restore options are available: restore of the .vmdk (disk level), SFR restore (file-level recovery), Exchange storage group or database restore, or Exchange granular-level restore (GRT). You can also choose whether or not to truncate logs.

NetBackup documentation

NetBackup documentation is part of the NetBackup media kit and can be found in a directory on the installation DVD for each release platform.

The documents are in Adobe® Portable Document Format (PDF), viewable with the Adobe Acrobat Reader. Download the reader from http://www.adobe.com.

Symantec Corporation assumes no responsibility for the installation and use of the reader.

For a complete list of NetBackup technical documents, see the Related Documents appendix in the *NetBackup Release Notes*.

The Symantec Corporation support Web site contains links to the most recent documentation plus a list of helpful how-to and product alert topics.

http://www.symantec.com/business/support/index?page=landing&key=15143

Installing NetBackup for Exchange

This chapter includes the following topics:

- Planning the installation of NetBackup for Exchange
- Verifying the operating system and platform compatibility for NetBackup for Exchange
- NetBackup server and client requirements for NetBackup for Exchange
- Exchange server software requirements for NetBackup for Exchange
- Requirements for Exchange in a cluster environment
- Configuration and licensing requirements for Exchange snapshot backups and restores
- Adding license keys for NetBackup for Exchange backups

Planning the installation of NetBackup for Exchange

Perform the following tasks before you use NetBackup for Exchange.

Table 2-1 Installation steps for NetBackup for Exchange

Step	Action	Description
Step 1	Verify the operating system and platform compatibility.	See "Verifying the operating system and platform compatibility for NetBackup for Exchange" on page 26.

	Table 2-1	Installation steps for NetBackup for Exchange *(continued)*
Step	**Action**	**Description**
Step 2	Verify the NetBackup server and client requirements for NetBackup for Exchange.	See "NetBackup server and client requirements for NetBackup for Exchange" on page 27.
Step 3	Verify the Exchange software requirements for NetBackup for Exchange.	See "Exchange server software requirements for NetBackup for Exchange" on page 28.
Step 4	For snapshot operations, verify the requirements for this type of backup.	See "Configuration and licensing requirements for Exchange snapshot backups and restores" on page 28.
Step 5	If you installed Exchange Server in a cluster, review the requirements for that environment.	See "Requirements for Exchange in a cluster environment" on page 28.
Step 6	Add the applicable license key(s) to the master server.	See "Adding license keys for NetBackup for Exchange backups" on page 30.

Verifying the operating system and platform compatibility for NetBackup for Exchange

Verify that the NetBackup for Exchange agent is supported on your operating system or platform.

To verify operating system and compatibility

1   Go to the Symantec Support Web page:

    http://www.symantec.com/business/support/index.jsp

2   Click on the link for **NetBackup Enterprise Server**.

3   In the list of documents, click on the following document:

    NetBackup Database Agent Compatibility List

4   For information on supported cluster environments for NetBackup for Exchange, see the following document:

    NetBackup Cluster Compatibility List

5   For information on support for Snapshot Client, see the following document:

    NetBackup Snapshot Client Compatibility List

6   For information on support for VMware, see the following document:

    Statement of Support for NetBackup in a Virtual Environment (Virtualization Technologies)

NetBackup server and client requirements for NetBackup for Exchange

Verify that the following requirements are met for the NetBackup server:

■ The NetBackup server software is installed and operational on the NetBackup server. The NetBackup server platform can be any that NetBackup supports. See the *NetBackup Installation Guide*.

■ Make sure that you configure any backup media that the storage unit uses.

The number of media volumes that are required depends on several things:

  ■ The devices used

  ■ The sizes of the databases that you want to back up

  ■ The amount of data that you want to archive

  ■ The size of your backups

  ■ The frequency of backups or archives

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

Verify that the following requirements are met for the NetBackup clients:

■ The NetBackup client software is installed as follows:

  ■ In a non-VMware environment, on the computer that has the databases you want to back up.
  Install the NetBackup client software on the computer that has the Exchange Server, any off-host clients, and all CAS servers that are used for mailbox databases. In an Exchange Server cluster, install the NetBackup client on each node in the cluster.
  The following PowerShell command can be used to change which CAS server is assigned to a database. Refer to Microsoft documentation for more information.

    ```
    Set-MailboxDatabase <Mailbox Database Name>
    -RpcClientAccessServer <ClientAccessServer or
    ClientAccessServerArrayID>
    ```

  ■ In a VMware environment, the NetBackup client software must be installed on the virtual machines that have Exchange running.

■ To use the new features that are included in NetBackup for Exchange in NetBackup 7.5 or later releases, you must upgrade your NetBackup for Exchange clients. The media server and NetBackup for Exchange clients must be at the same NetBackup version.

Exchange server software requirements for NetBackup for Exchange

Verify the following regarding the Exchange server software on the NetBackup server or client:

- Exchange server software must be installed and operational.

- For Exchange 2007, Symantec recommends that you do not install Microsoft Outlook on the same server on which Exchange is installed. This recommendation does not apply if you do not perform MAPI backups or perform restores with Granular Recovery Technology (GRT).

- Install the NetBackup client on the Exchange server, if the Exchange server is not locally installed on a NetBackup server.

- (Exchange 2007) This requirement applies if you want to perform MAPI operations or operations with Granular Recovery Technology (GRT). On the Exchange Server install the Microsoft Exchange Server MAPI Client and Collaboration Data Objects (CDO) package. On Windows 2008 and later, install version 6.05.8022.0 or higher. On Windows 2003 and later, install version 6.05.7888 or higher.
  These packages are available on the following Microsoft Web site:
  http://www.microsoft.com/downloads/

Requirements for Exchange in a cluster environment

If you plan to use NetBackup for Exchange to back up an Exchange 2007 server in a VCS 5.0 environment, verify the following:

- A patch is required to cluster Exchange 2007 in a VCS 5.0 environment. See the following TechNote for more information.
  http://www.symantec.com/docs/TECH51616

Configuration and licensing requirements for Exchange snapshot backups and restores

To perform snapshot backups of restores of Exchange Server, you must meet the following requirements:

- Confirm that the type of snapshot you want to configure is supported for your Exchange environment. See the following compatibility list:
  NetBackup Snapshot Client (Advanced Client) OS, Arrays, and Database Agent Compatibility

- Configure the NetBackup Snapshot Client and verify that you meet the configuration requirements for the snapshot method you want to use. See the *NetBackup Snapshot Client Administrator's Guide*.

- If you use Veritas Storage Foundation for Windows (SFW), verify that you have the minimum software level.

Windows 2008 and later, Windows 2008 R2 and later	SFW 5.1 SP2 or 6.0
Windows 2003 x64	SFW 5.0
Windows 2003 x86	SFW 4.3

- The following snapshot options or Exchange configurations require a separate Snapshot Client license:
  - Instant recovery
  - Off-host backups
  - Backups using a hardware provider
  - A CCR environment

  Additional installation requirements apply for Instant Recovery and off-host backups.

  See "Requirements for Exchange off-host backups" on page 29.

  See "Requirements for Exchange Instant Recovery backups" on page 30.

- If you want to restore individual items from database backups (granular recovery), additional installation requirements apply and other configuration is necessary.

  See "Configuring NetBackup for Exchange backups that use Granular Recovery Technology (GRT)" on page 62.

See "Limitations of Exchange snapshot operations" on page 103.

Requirements for Exchange off-host backups

Note the following requirements and operational notes for off-host backups:

- (Exchange 2007) Storage Foundation for Windows (SFW) 5.0 or later is required for off-host backups that use the SFW VSS provider. For Windows 2008 and later and Windows 2008 R2 and later, SFW 5.1 SP1 is required for local and off-host snapshot backups.

- (Exchange 2007) To successfully perform backups with the SFW VSS provider for SFW 5.0, apply the following hotfixes on the hosts where a snapshot backup occurs:

    - http://www.symantec.com/docs/TECH56286
      This hotfix is also included in the SFW/SFW-HA 5.0 MP1 release.

    - http://www.symantec.com/docsTECH54364

    Note: These hotfixes are included in SFW/SFW-HA 5.1 and are not required if you have that version.

- The Exchange Server does not need to be installed on the off-host client.

- (Exchange 2007 and later) For consistency checks of Exchange with the Microsoft consistency check API, Symantec recommends that you install the Exchange System Management Tools on the alternate client. Then restart the Exchange Server. If you choose not to install the Exchange System Management Tools on an Exchange 2010 alternate client, you must install the VC9 runtime DLLs. These DLLs can be downloaded from Microsoft x64 VC9 download page: http://www.microsoft.com/downloads/details.aspx?familyid=BD2A6171-E2D6-4230-B809-9A8D7548C1B6&displaylang=en
  More information is available about consistency checks in general and options for Exchange 2010 consistency checks:
  See "Consistency checks on Exchange snapshot backups" on page 105.
  See "About consistency checks options for an Exchange 2010 backup" on page 74.

- For Instant Recovery off-host backups, see the following requirements:
  See "Requirements for Exchange Instant Recovery backups" on page 30.

Requirements for Exchange Instant Recovery backups

With Windows 2008 and later and Windows 2008 R2 and later, Instant Recovery backups require Storage Foundations for Windows (SFW) 5.1 SP1 if you use the SFW VSS provider.

Adding license keys for NetBackup for Exchange backups

To use NetBackup for Exchange, add a valid license key for it on the master server. More information is available on how to add license keys.

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

In a NetBackup cluster, add the key on each node where the NetBackup server is installed.

To add a NetBackup for Exchange license key in the NetBackup Administration Console

1   On the master server, open the NetBackup Administration Console.

2   Choose **Help > License Keys**.

3   Click the **New** icon.

4   Type the license key and click **Add**.

Exchange Granular Recovery

This chapter includes the following topics:

- Configurations that are supported for Exchange Granular Recovery

- Requirements to perform backups and restores of Exchange with Granular Recovery Technology (GRT)

- About installing and configuring Network File System (NFS) for Exchange Granular Recovery

- About configuring Services for Network File System (NFS) on the Windows 2008 and Windows 2008 R2 NetBackup media server and NetBackup clients

- About configuring Services for Network File System (NFS) on the Windows 2003 R2 SP2 NetBackup media server and NetBackup clients

- Configuring a UNIX or Linux media server and Windows clients for backups and restores that use Granular Recovery Technology

- Configuring a different network port for NBFSD

Configurations that are supported for Exchange Granular Recovery

For information on the Exchange versions and Windows Server releases that are supported for Granular Recovery Technology (GRT) see the following:

NetBackup Database Agent Compatibility List

For information on the media server platforms that are supported for Granular Recovery Technology (GRT) see the following:

NetBackup Operating System Compatibility List

Requirements to perform backups and restores of Exchange with Granular Recovery Technology (GRT)

Table 3-1		Requirements to perform backups and restores of Exchange with Granular Recovery Technology (GRT)
Step	**Action**	**Description**
Step 1	Verify that you have a supported Exchange Server configuration and have a media server platform that supports GRT.	See the *NetBackup Database Agent Compatibility List.* See the *NetBackup Operating System Compatibility List.*
Step 2	Ensure that requirements are met for the Exchange server software.	See "Exchange server software requirements for NetBackup for Exchange" on page 28.
Step 3	On all Exchange granular clients, ensure that the computer has an available drive letter on which to mount the backup image.	To determine which clients to configure, refer to the following topic: See "About Exchange client and server privileges" on page 66.
Step 4	Enable or configure NFS for your environment. ■ Windows 2008 and Windows 2008 R2 media server and clients ■ Windows 2003 R2 SP2 media server and clients ■ UNIX/Linux media server and Windows clients	See "About configuring Services for Network File System (NFS) on the Windows 2008 and Windows 2008 R2 NetBackup media server and NetBackup clients" on page 35. See "About configuring Services for Network File System (NFS) on the Windows 2003 R2 SP2 NetBackup media server and NetBackup clients" on page 43. See "Configuring a UNIX or Linux media server and Windows clients for backups and restores that use Granular Recovery Technology" on page 50.
Step 5	Configure NetBackup.	Once you have met the requirements described in this procedure and configured NFS, continue with the configuration of NetBackup. See "Configuring NetBackup for Exchange backups that use Granular Recovery Technology (GRT)" on page 62.

About installing and configuring Network File System (NFS) for Exchange Granular Recovery

NetBackup Granular Recovery leverages Network File System, or NFS, to read individual objects from a database backup image. Specifically, the NetBackup client uses NFS to extract data from the backup image on the NetBackup media server. The NetBackup client uses "Client for NFS" to mount and access a mapped drive that is connected to the NetBackup media server. The NetBackup media server handles the I/O requests from the client through NBFSD.

NBFSD is the NetBackup File System (NBFS) service that runs on the media server. NBFSD makes a NetBackup backup image appear as a file system folder to the NetBackup client over a secure connection.

Network File System, or NFS, is a widely recognized, open standard for client and server file access over a network. It allows clients to access files on dissimilar servers through a shared TCP/IP network. NFS is typically bundled with the host operating system. NetBackup uses Granular Recovery Technology (GRT) and NFS to recover the individual objects that reside within a database backup image, such as:

- A user account from an Active Directory database backup

- Email messages or folders from an Exchange database backup

- A document from a SharePoint database backup

Multiple NetBackup agents that support GRT (for example, Exchange, SharePoint, and Active Directory) can use the same media server.

About configuring Services for Network File System (NFS) on the Windows 2008 and Windows 2008 R2 NetBackup media server and NetBackup clients

Note: For VMware backups and restores of Exchange 2007, the only systems that require configuration of NFS are the following: the systems that you use to browse for backups or the systems you use to perform restores. For Exchange 2010, you need only configure the systems that browse for backups and the CAS server. This configuration is not needed to capture the data during backups of the virtual machine.

Table 3-2   Configuring NFS in a Windows 2008 or Windows 2008 R2 environment

Step	Action	Description
Step 1	Stop and disable the Portmapper service.	Before you configure NFS on the media server or client(s), look for the ONC Portmapper service. If it exists, stop it and disable it. Otherwise, the configuration of NFS Services for Windows fails.
Step 2	Enable NFS.	Enable NFS on the following: ■ The NetBackup media server ■ The Exchange granular clients See "About Exchange client and server privileges" on page 66. ■ The CAS Server See "Enabling Services for Network File System (NFS) on Windows 2008 or Windows 2008 R2" on page 36.
Step 3	Disable Server for NFS.	You can disable the Server for NFS on the following: ■ The NetBackup media server ■ The Exchange granular clients See "About Exchange client and server privileges" on page 66. ■ The CAS Server See "Disabling the Server for NFS" on page 40.
Step 4	Disable Client for NFS.	You can disable the Client for NFS on the NetBackup media server. See "Disabling the Client for NFS on the media server" on page 41. If an Exchange granular client resides on the media server, do not disable the Client for NFS.

Enabling Services for Network File System (NFS) on Windows 2008 or Windows 2008 R2

To restore individual items from a backup that uses Granular Recovery Technology (GRT), you must enable Services for Network File System. When this configuration is completed on the media server and the Exchange granular clients, you can disable any unnecessary NFS services. More information is available on which clients require this configuration.

See "About Exchange client and server privileges" on page 66.

Exchange Granular Recovery | 37
About configuring Services for Network File System (NFS) on the Windows 2008 and Windows 2008 R2 NetBackup
media server and NetBackup clients

To enable Services for Network File System (NFS) on Windows 2008 or Windows 2008 R2

1   Open the Server Manager.

2   In the left pane, click **Roles** and, in the right pane, click **Add Roles**.
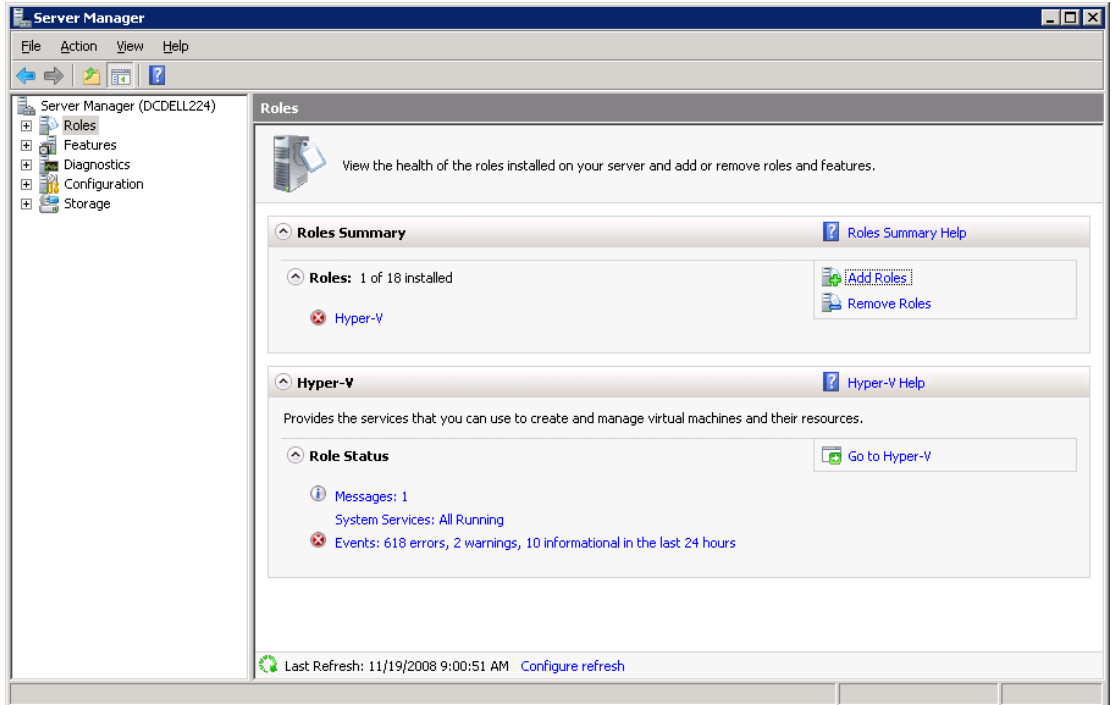
3   In the Add Roles Wizard, on the **Before You Begin** page, click **Next**.

4   On the **Select Server Roles** page, under **Roles**, check the **File Services** check box.
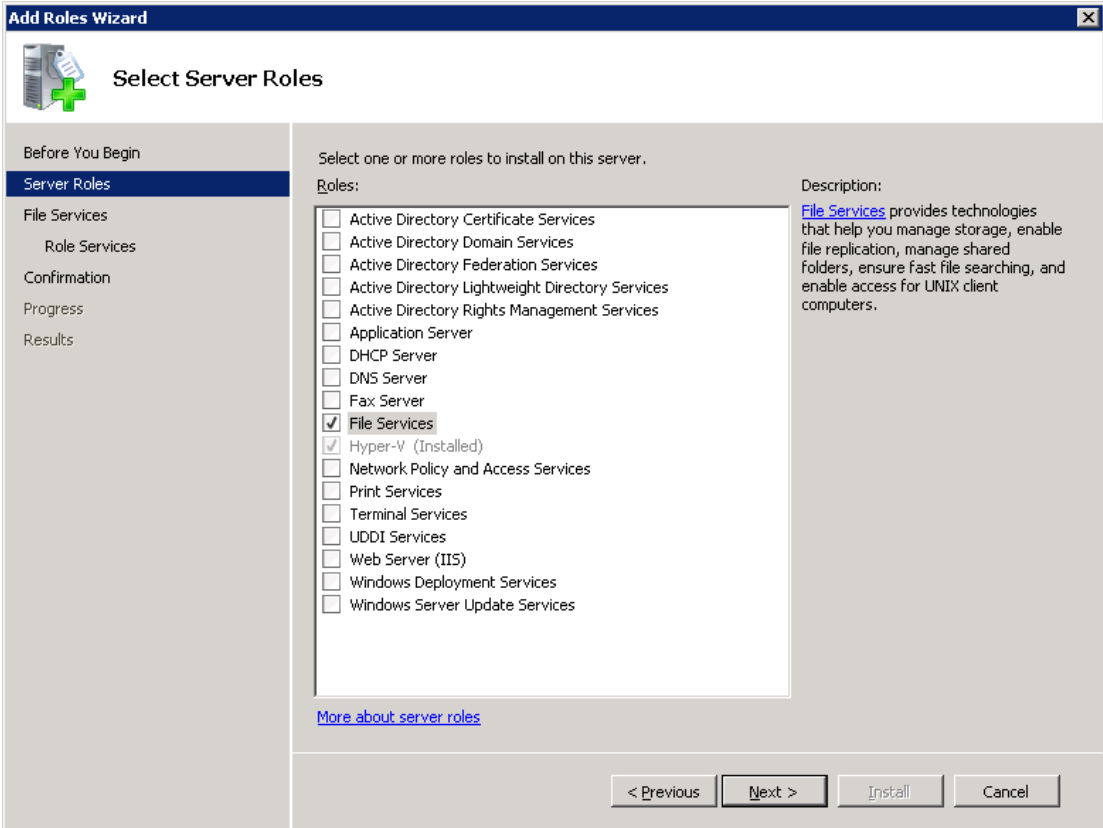
5   Click **Next**.

6   On the **Files Services** page, click **Next**.

7   On the **Select Role Services** page, uncheck **File Server**.

Exchange Granular Recovery | 39

**About configuring Services for Network File System (NFS) on the Windows 2008 and Windows 2008 R2 NetBackup
media server and NetBackup clients**

8   Check **Services for Network File System**.
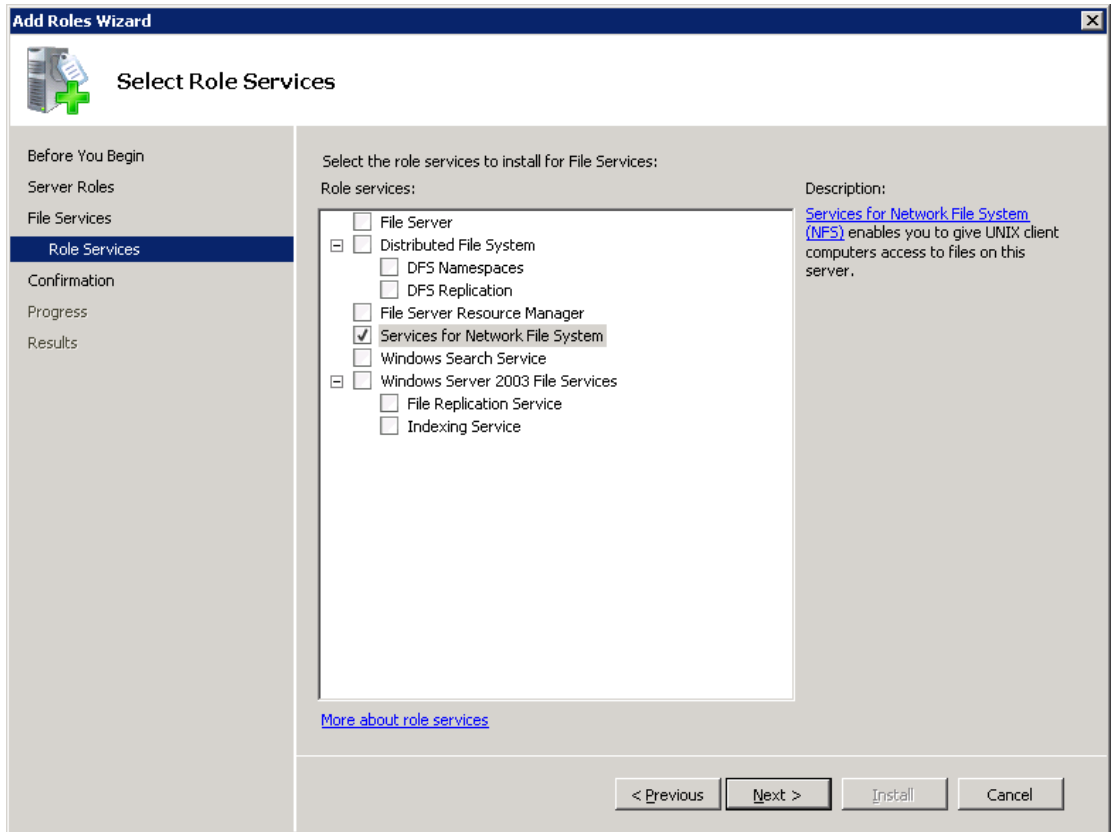
9   Click **Next** and complete the wizard.

10   On the media server, configure the portmap service to start automatically at
     server restart.

     Issue the following from the command prompt:

     `sc config portmap start= auto`

     This command should return the status `[SC] ChangeServiceConfig SUCCESS`.

11   For each host in your configuration, choose from one of the following:

     ■ If you have a single host that functions as both the media server and the
       Exchange granular client, you can disable the Server for NFS.

     ■ For a host that is only the NetBackup media server, you can disable the
       Server for NFS and the Client for NFS.

■ For a host that is only an Exchange granular client, you can disable the Server for NFS.

Disabling the Server for NFS

After you enable Services for Network File System (NFS) on the media server and on the Exchange granular clients, you can disable Server for NFS.

To disable the Server for NFS

1   Open the Server Manager.
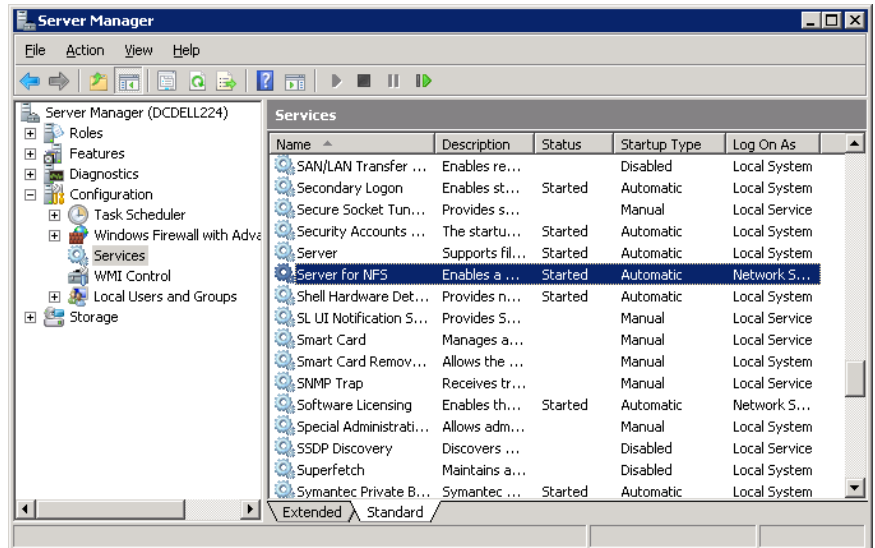
2   In the left pane, expand **Configuration**.

3   Click **Services**.

4   In the right pane, right-click on **Server for NFS** and click **Stop**.

5   In the right pane, right-click on **Server for NFS** and click **Properties**.

Exchange Granular Recovery | 41
About configuring Services for Network File System (NFS) on the Windows 2008 and Windows 2008 R2 NetBackup
media server and NetBackup clients

6   In the **Server for NFS Properties** dialog box, from the **Startup type** list, click
    Disabled.
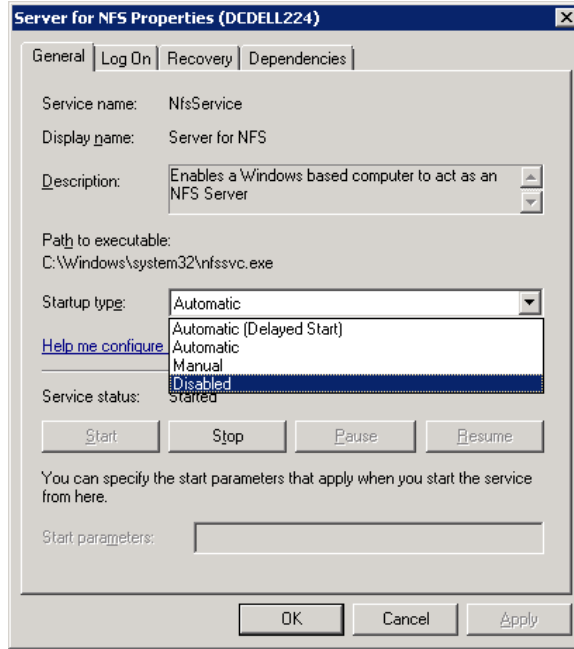
7   Click **OK**.

8   Repeat this procedure for the media server and for each Exchange granular
    client.

Disabling the Client for NFS on the media server

After you enable Services for Network File System (NFS) on a host that is only a
NetBackup media server, you can disable the Client for NFS.

To disable the Client for NFS on the NetBackup media server

1   Open the Server Manager.
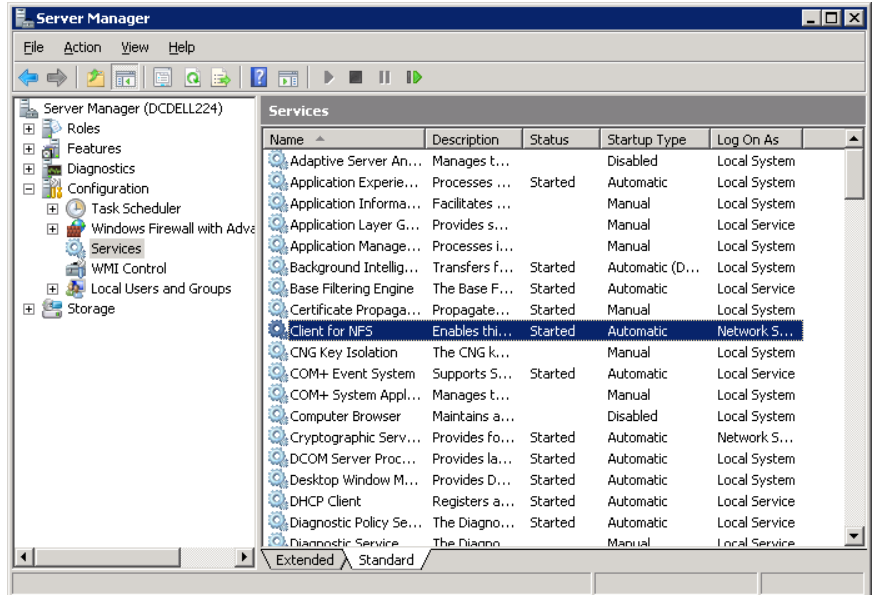
2   In the left pane, expand **Configuration**.

3   Click **Services**.

4   In the right pane, right-click on **Client for NFS** and click **Stop**.

5   In the right pane, right-click on **Client for NFS** and click **Properties**.

Exchange Granular Recovery | 43

About configuring Services for Network File System (NFS) on the Windows 2003 R2 SP2 NetBackup media server and
NetBackup clients

6   In the **Client for NFS Properties** dialog box, from the **Startup type** list, click
    Disabled.
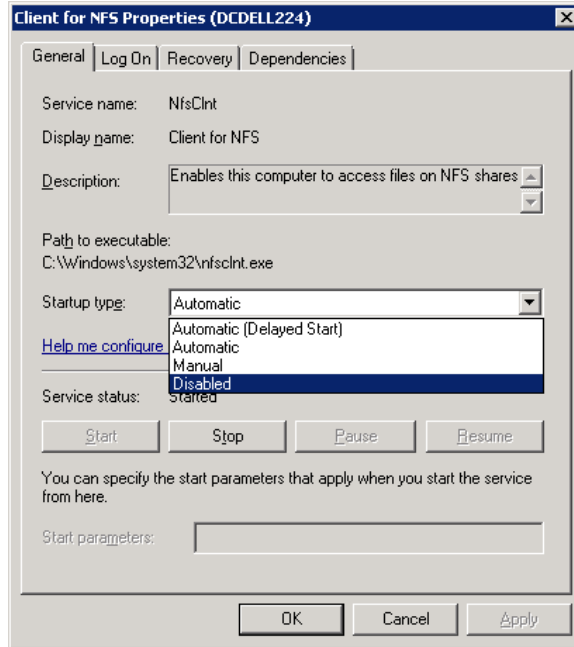
7   Click **OK**.

About configuring Services for Network File System (NFS) on the Windows 2003 R2 SP2 NetBackup media server and NetBackup clients

Note: NetBackup does not support Granular Recovery Technology (GRT) with
Windows Server 2003 R1 or earlier versions.

Note: For VMware backups and restores of Exchange 2007, the only systems that require configuration of NFS are the following: the systems that you use to browse for backups or the systems you use to perform restores. For Exchange 2010, you need only configure the systems that browse for backups and the CAS server. This configuration is not needed to capture the data during backups of the virtual machine.

Table 3-3

Step	Action	Description
Step 1	Install the necessary NFS components on the NetBackup media server.	See Table 3-4 on page 44.
		See "Installing Services for NFS on the Windows 2003 R2 SP2 media server" on page 44.
Step 2	Install the necessary NFS components on the Exchange granular clients.	See Table 3-4 on page 44.
		See "About Exchange client and server privileges" on page 66.
		See "Installing Services for NFS on Exchange granular clients with Windows 2003 R2 SP2" on page 48.
		Note: If an Exchange granular client resides on the media server, install all the components on the media server.
Step 3	Install the hotfix for Client for NFS on the Exchange granular clients.	The hotfix is available at the following location:
		http://support.microsoft.com/kb/947186

Table 3-4   NFS components required for Windows 2003 R2 SP2

NFS component	NetBackup client	NetBackup media server
Client for NFS	X	
Microsoft Services for NFS Administration	X	
RPC External Data Representation	X	X
RPC Port Mapper		X

Installing Services for NFS on the Windows 2003 R2 SP2 media server

This topic describes how to install Services for NFS on a Windows 2003 R2 SP2 media server.

To install Services for NFS on the Windows 2003 R2 SP2 media server

1   Click **Start** > **Control Panel** > **Add or Remove Programs**.

2   Click **Add/Remove Windows Components**.

3   Check **Other Network File and Print Services** and click **Details**.
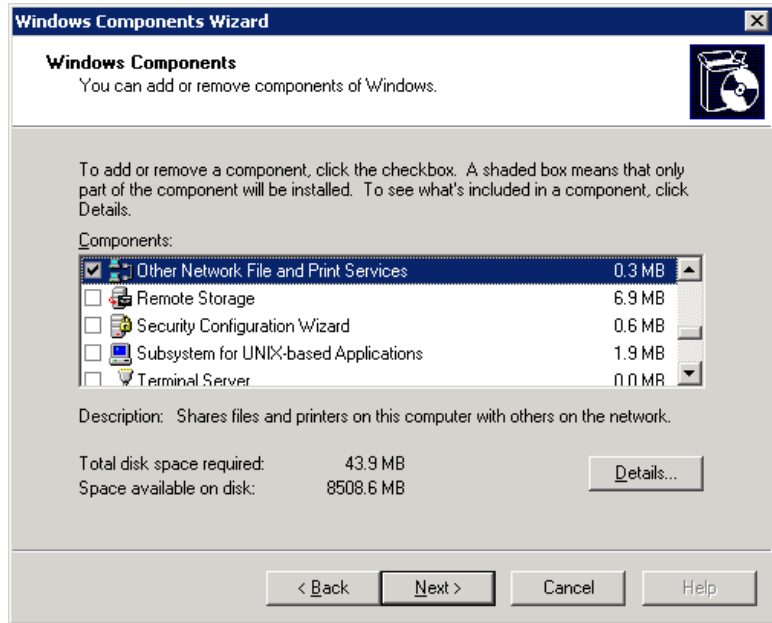
4   Check **Microsoft Service for NFS** and click **Details**.
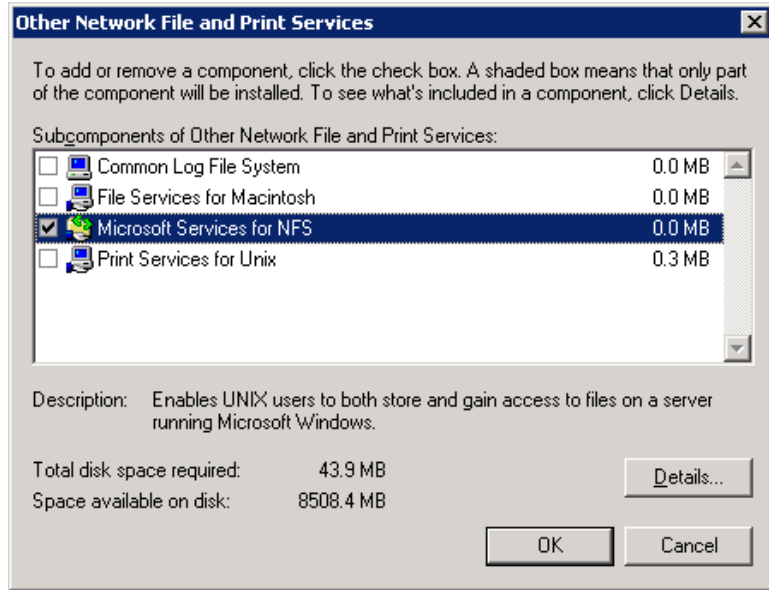
5   Install the components that apply to your configuration.

- If the host is only a NetBackup media server, check the following components:
  - RPC External Data Representation
  - RPC Port Mapper
- If you have a single host that functions as both the media server and the Exchange granular client, check the following components:
  - Client for NFS
  - Microsoft Services for NFS Administration
  - RPC External Data Representation
  - RPC Port Mapper

Exchange Granular Recovery | 47

About configuring Services for Network File System (NFS) on the Windows 2003 R2 SP2 NetBackup media server and NetBackup clients
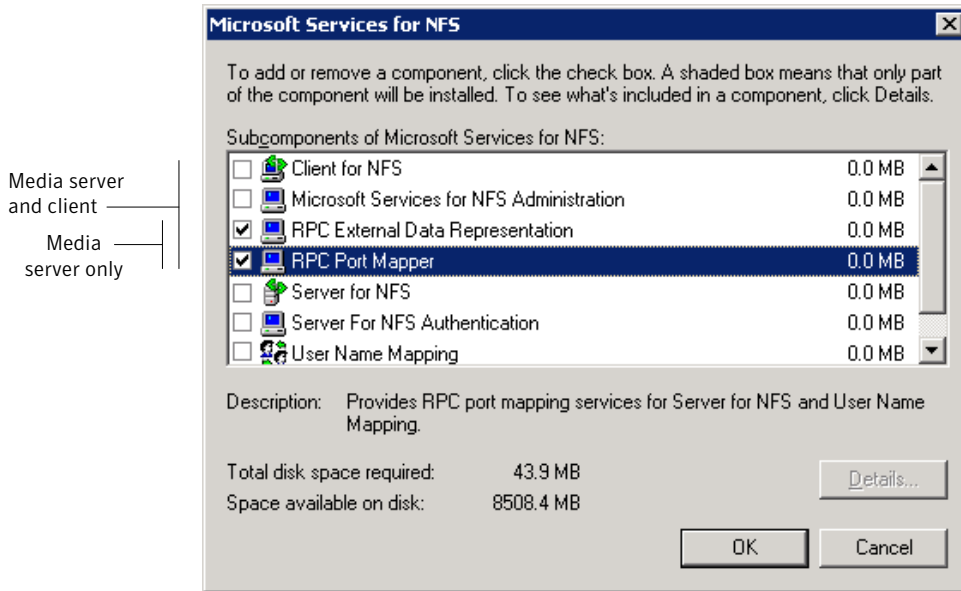
6   Click **OK**.

7   Click **OK**.

8   Click **Next** and complete the Windows Components Wizard.

9   After the installation is complete, open Services in the Control Panel.

10 Depending on configuration of the host, verify that Client for NFS is running or is stopped and disabled:

- ■   For a single host that has both the media server and the Exchange granular client, ensure Client for NFS is running.

- ■   For a host that is only a NetBackup media server, Client for NFS can be stopped and disabled.

11 Configure the portmap service to start automatically at server restart.

Issue the following from the command prompt:

```
sc config portmap start= auto
```

This command should return the status [SC] ChangeServiceConfig SUCCESS.

Installing Services for NFS on Exchange granular clients with Windows 2003 R2 SP2

This topic describes how to install NFS on the NetBackup clients with Windows 2003 R2 SP2. Only the clients that perform granular operations require NFS. If an Exchange granular client is also a media server, you must follow a different procedure.

See "Installing Services for NFS on the Windows 2003 R2 SP2 media server" on page 44.

More information is available on which clients require NFS.

See "About Exchange client and server privileges" on page 66.

To install Services for NFS on the NetBackup clients with Windows 2003 R2 SP2

1   Click **Start** > **Control Panel** > **Add or Remove Programs**.

2   Click **Add/Remove Windows Components**.

3   Check **Other Network File and Print Services** and click **Details**.

4   Check **Microsoft Service for NFS** and click **Details**.

Other Network File and Print Services   [X]

To add or remove a component, click the check box. A shaded box means that only part
of the component will be installed. To see what's included in a component, click Details.

Subcomponents of Other Network File and Print Services:

☐ 🖥 Common Log File System	0.0 MB
☐ 🖥 File Services for Macintosh	0.0 MB
☑ 🌐 Microsoft Services for NFS	0.0 MB
☐ 🖥 Print Services for Unix	0.3 MB

Description: Enables UNIX users to both store and gain access to files on a server
               running Microsoft Windows.

Total disk space required: 43.9 MB   [Details...]
Space available on disk: 8508.4 MB

                                              [OK]   [Cancel]

5   Check the following components:

- Client for NFS

- Microsoft Services for NFS Administration

- RPC External Data Representation
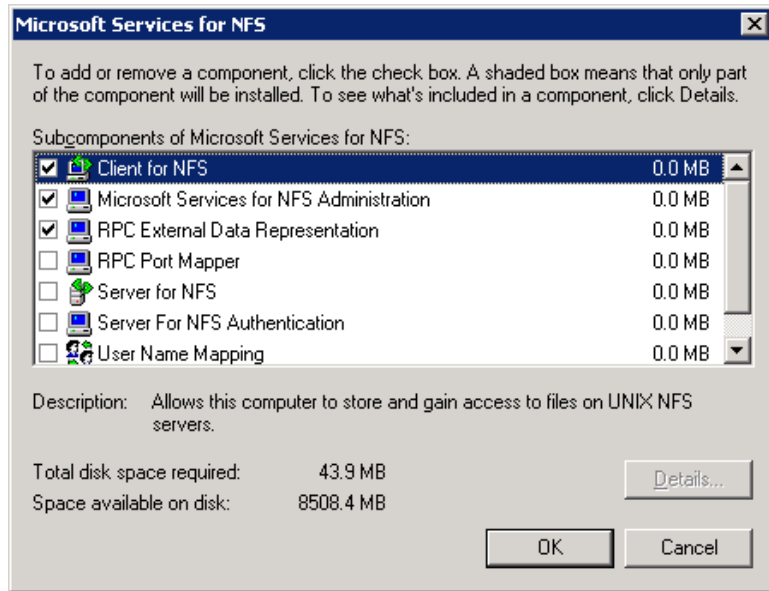
6   Click **OK**.

7   Click **OK**.

8   Click **Next** and complete the Windows Components Wizard.

9   After the installation is complete, open Services in the Control Panel.

10 Ensure the following that the Client for NFS service is running.

11 Repeat this procedure for each Exchange client that performs granular operations.

Configuring a UNIX or Linux media server and Windows clients for backups and restores that use Granular Recovery Technology

To perform backups and restores that use Granular Recovery Technology, perform the following configuration if you use a UNIX or Linux media server and Windows clients:

■ Confirm that your media server is installed on a platform that supports granular recovery.
See the *NetBackup X Operating System* compatibility list.

- No other configuration is required for the UNIX or Linux media server.

- Enable or install NFS on the Exchange granular clients.
  See "Enabling Services for Network File System (NFS) on Windows 2008 or Windows 2008 R2" on page 36.
  See "Installing Services for NFS on Exchange granular clients with Windows 2003 R2 SP2" on page 48.

- You can configure a different network port for NBFSD.
  See "Configuring a different network port for NBFSD" on page 51.

Configuring a different network port for NBFSD

NBFSD runs on port 7394. If another service uses the standard NBFSD port in your organization, you can configure the service on another port. The following procedures describe how to configure a NetBackup server to use a network port other than the default.

To configure a different network port for NBFSD (Windows server)

1 Log on as administrator on the computer where NetBackup server is installed.

2 Open Regedit.

3 Open the following key.:

HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Config

4 Create a new DWORD value named **FSE_PORT**.

5 Right-click on the new value and click **Modify**.

6 In the **Value data** box, provide a port number between 1 and 65535.

7 Click **OK**.

To configure a different network port for NBFSD (UNIX or Linux server)

1 Log on as root on the computer where NetBackup server is installed.

2 Open the bp.conf file.

3 Add the following entry, where *XXXX* is an integer and is a port number between 1 and 65535.

   FSE_PORT = *XXXX*

Configuring NetBackup for Exchange

This chapter includes the following topics:

- About configuring NetBackup for Exchange
- About user interface terminology
- About configuring the NetBackup Client Service for backups and restores that use Granular Recovery Technology (GRT) or MAPI
- Configuring NetBackup for Exchange backups that use Granular Recovery Technology (GRT)
- About Exchange client and server privileges
- Configuring host properties for Exchange clients
- Testing configuration settings for NetBackup for Exchange

About configuring NetBackup for Exchange

To successfully perform backups and restores of Exchange Server and Exchange mailboxes, complete the following steps.

For additional information on how to configure NetBackup in preparation of VMware backups that protect Exchange, refer to the following topic.

	Table 4-1	Configuring NetBackup for Exchange
Step	**Action**	**Description**
Step 1	Review the information for configuring the backup and restore operations that use Granular Recovery Technology (GRT).	GRT lets you restore individual mailbox messages, etc. from a database backup. GRT is an option limited to certain Exchange versions of Exchange Server and Windows Server. GRT is included in VMware backups that protect Exchange. See "Configuring NetBackup for Exchange backups that use Granular Recovery Technology (GRT)" on page 62.
Step 2	Configure the NetBackup Client Service.	Required if you want to do the following: ■ Restore individual mailboxes and public folder items with Granular Recovery Technology (GRT). ■ Perform MAPI backups of individual mailbox and public folder objects (Exchange 2007 and earlier). See "About configuring the NetBackup Client Service for backups and restores that use Granular Recovery Technology (GRT) or MAPI" on page 55.
Step 3	If applicable, configure the client and the server privileges.	See "About Exchange client and server privileges" on page 66.
Step 4	If applicable, configure the host properties for Exchange clients.	See "Configuring host properties for Exchange clients" on page 68.

	Table 4-1	Configuring NetBackup for Exchange *(continued)*
Step	**Action**	**Description**
Step 5	Follow the procedures for the type of backup you want to perform.	See "About configuring a backup policy for Exchange Server" on page 77. See "About configuring snapshot backups of Exchange Server" on page 101. See "About configuring Instant Recovery backups of Exchange Server (Exchange 2007 and later)" on page 113. See "Configuring a policy for backups of individual Exchange mailboxes or public folders (Exchange 2007 and earlier)" on page 126. See "Configuring a streaming NetBackup for Exchange policy (Exchange 2007 and earlier)" on page 123. See "About configuring VMware policies to protect Exchange Server" on page 198.
Step 7	Test your configuration settings.	See "Testing configuration settings for NetBackup for Exchange" on page 75.

About user interface terminology

You perform many configuration steps from the NetBackup Administration Console on the master server. The type of console available depends on your master server platform. NetBackup supports a Java interface for both Windows and UNIX master servers. In addition, NetBackup supports a Windows interface for Windows master servers.

The Java and Windows interfaces are nearly identical. If interface differences exist in the configuration procedures, the term "Windows" or "Java" appears in the procedure to differentiate between the two interfaces.

About configuring the NetBackup Client Service for backups and restores that use Granular Recovery Technology (GRT) or MAPI

To restore individual mailbox and public folder items from database backups, you must configure an account and mailbox for NetBackup to use. This configuration

is also required for Exchange 2007 and earlier if you perform MAPI backups of individual mailbox and public folder objects.

NetBackup must have access to Exchange mailboxes and public folders so it can do the following:

■ Enumerate mailboxes when defining a policy.

■ Restore mailbox and public folder objects from the backups that use Granular Recovery Technology (GRT).

■ Perform backups or restores of mailbox and public folder objects with MAPI (Exchange 2007 and earlier).

Note: For VMware backups and restores of Exchange 2007, the only systems that require configuration of NFS are the following: the systems that you use to browse for backups or the systems you use to perform restores. For Exchange 2010, you need only configure the systems that browse for backups and the CAS server. This configuration is not needed to capture the data during backups of the virtual machine.

Table 4-2   Steps to configure the NetBackup Client Service for backups and restores that use Granular Recovery Technology (GRT) or MAPI

Step	Action	Description
Step 1	Create an Exchange mailbox to associate with the NetBackup Client Service.	Symantec recommends that you create a uniquely named mailbox. Verify that this mailbox is not hidden.
Step 2	Configure the NetBackup service account as follows: ■ See the specific procedure for the Exchange version you have. ■ Ensure that the NetBackup service account has domain privileged rights.	See "Creating a privileged NetBackup user account for EWS access (Exchange 2010)" on page 57. See "Configuring the NetBackup service account (Exchange 2007)" on page 58. See "Configuring the NetBackup service account (Exchange 2003)" on page 59.
Step 3	Configure the log on account for the NetBackup Client Service.	Symantec recommends that the NetBackup Client Service uses the same account that runs Exchange Services. See "Configuring the log on account for the NetBackup Client Service for NetBackup for Exchange on Windows" on page 60.

Creating a privileged NetBackup user account for EWS access (Exchange 2010)

This procedure provides an example of how to create a privileged NetBackup user account for EWS access with Exchange 2010. In a cluster or replicated environment, create the NetBackup user account on the following Exchange clients: the clients that are backed up, the clients that are used to browse for backups, and the Exchange Client Access Server (CAS).

Note: For VMware backups and restores, you need only configure the systems that browse for backups and the CAS server. This configuration is not needed to capture the data during backups of the virtual machine.

To create a privileged NetBackup user account for EWS access (Exchange 2010)

1   In Active Directory Users and Computers, select the **Users** directory.

2   Right-click and select **New > User** and indicate a name for your new account.

3   Double-click on the account you created.

4   Select the **Member Of** tab.

5   Click **Add** and add these objects to the user:

   ■ Domain Users

   ■ Organization Management

   If permissions issues persist, try adding the Domain Admins group to this account.

6   Configure the NetBackup Client Service log on account.

   See "Configuring the log on account for the NetBackup Client Service for NetBackup for Exchange on Windows" on page 60.

7   If you receive an "Access is denied" error when you perform a restore, you may need to run the following commands:

```
New-ManagementRole -Name EWSImpersonationRole -Parent ApplicationImpersonation

New-ManagementRoleAssignment -Role EWSImpersonationRole -User Administrator
EWSImpersonationRoleAssignment
```

where *Administrator* is the alias of the Active Directory account you want to use.

See "About configuring NetBackup for Exchange" on page 53.

About NetBackup and Microsoft Exchange Web Services (Exchange 2010)

For Exchange 2010, NetBackup uses Microsoft Exchange Web Services (EWS) to support a backup that uses the Granular Recovery Technology (GRT). EWS provides support for the restore of individual mailboxes, mail messages, and public folders from an Exchange 2010 database backup.

To use EWS to restore individual items, the client throttling policy is disabled for the resource credentials you specify for the restore job. The client throttling policy is located on the Client Access Server and enforces connection bandwidth limits on the Exchange server.

NetBackup also creates an impersonation role and a role assignment for Exchange Impersonation. Exchange Impersonation role assignment associates the impersonation role with the NetBackup resource credentials you specify for the restore job.

NetBackup creates and assigns the following roles:

- SymantecEWSImpersonationRole

- SymantecEWSImpersonationRoleAssignment

See "About configuring NetBackup for Exchange" on page 53.

See "About configuring the NetBackup Client Service for backups and restores that use Granular Recovery Technology (GRT) or MAPI" on page 55.

See "About Exchange backups and transaction logs" on page 100.

Configuring the NetBackup service account (Exchange 2007)

If in a cluster or replicated environment, perform the steps in the following procedures on each Exchange node.

Note: For VMware backups and restores, you need only configure the systems that browse for backups or the systems that you use to perform restores. This configuration is not needed to capture the data during backups of the virtual machine.

To configure the NetBackup service account (Exchange 2007)

1   In Active Directory Users and Computers, select the **Users** directory.

2   Right-click on the Administrator account, click **Copy**, and create an account
    for NetBackup.

    Create a user account that has a mailbox with a unique name. A unique name
    is one that does not already exist within the Exchange Organization. This
    name cannot be contained as a set of characters in an existing name.

    For example: EXCH1 is entered as the unique mailbox name, and other mailbox
    names such as EXCH1BACKUP or BACKUPEXCH1 exist. The backup or restore
    of individual mailboxes or both fail.

3   After you create the account, double-click the account, click the **Members Of**
    tab, and add this account to the Domain Admins group.

4   Open the Exchange Management Console.

5   In the Exchange Management Console, right-click on **Organization
    Configuration** and click **Add Exchange Administrator**.

6   On the **Add Exchange Administrator page**, click **Browse** and select the user
    to which you want to delegate control.

7   Click the **Exchange Server Administrator** role.

8   Under **Select the server(s) to which this role has access**, click **Add**.

9   Select the servers to which you want to delegate control and click **OK**.

10 Click **Add**.

11 On the **Completion** page, verify that the delegation was successful and click
    Finish.

12 Configure the NetBackup Client Service log on account.

    See "Configuring the log on account for the NetBackup Client Service for
    NetBackup for Exchange on Windows" on page 60.

See "About configuring NetBackup for Exchange" on page 53.

Configuring the NetBackup service account (Exchange 2003)

If in a cluster environment, perform the steps in the following procedures on each
Exchange node.

To configure the NetBackup service account (Exchange 2003)

1   Use Active Directory Users and Computers to create a user account that has a mailbox with a unique name.

    A unique name is one that does not already exist within the Exchange Organization. This name cannot be contained as a set of characters in an existing name.

    For example: EXCH1 is entered as the unique mailbox name, and other mailbox names such as EXCH1BACKUP or BACKUPEXCH1 exist. The backup or restore of individual mailboxes or both fail.

2   After you create the account, double-click the account, click the **Members Of** tab, and add this account to the Domain Admins group.

3   Open Exchange System Manager.

4   Right-click the Exchange Organization and click **Delegate Control**.

5   Click **Next**.

6   On the Users or the Groups screen, click **Add**.

7   In the **Delegate Control** dialog box, provide the following information.

Group or User	Specify the name of the account that was created in step 1.
Role	Select Exchange Full Administrator.

8   Complete the Delegation wizard.

9   Configure the NetBackup Client Service log on account.

    See "Configuring the log on account for the NetBackup Client Service for NetBackup for Exchange on Windows" on page 60.

See "About configuring NetBackup for Exchange" on page 53.

Configuring the log on account for the NetBackup Client Service for NetBackup for Exchange on Windows

By default, the NetBackup Client Service uses "Local System" account to log on as. A different account is required for the following operations: MAPI mailbox and public folder items backups (Exchange 2007 and earlier) and any operations that use Granular Recovery Technology (GRT).

Change the service account to the Windows domain account that you previously created. To change this account, you must have administrator group privileges.

Note: For VMware backups and restores, the only systems that require configuration of the NetBackup Client Service are the following: the systems that you use to browse for backups or the systems you use to perform restores. For Exchange 2010, you need only to configure the systems that browse for backups and the CAS server.

See "Creating a privileged NetBackup user account for EWS access (Exchange 2010)" on page 57.

See "Configuring the NetBackup service account (Exchange 2007)" on page 58.

See "Configuring the NetBackup service account (Exchange 2003)" on page 59.

Note: In a cluster environment, perform the steps on each database node in the cluster. For Exchange 2010, perform the steps on each database node in the DAG and the CAS server. For an off-host backup, perform the steps on the alternate client.

To configure the log on account for the NetBackup Client Service

1   Open the Windows Services application.

2   Double-click on the **NetBackup Client Service** entry.

3   Click on the **Log On** tab.

4   If **Local System account** is not selected as the **Log on as** account, proceed with step 9.

5   Provide the name of the user account that you created for the NetBackup Client Service.

    See "Creating a privileged NetBackup user account for EWS access (Exchange 2010)" on page 57.

    See "Configuring the NetBackup service account (Exchange 2007)" on page 58.

    See "Configuring the NetBackup service account (Exchange 2003)" on page 59.

    The account must include the domain name, followed by the user account, *domain_name\account*. For example, **recovery\netbackup**.

6   Type the password.

7   Click **OK**.

8   Stop and start the NetBackup Client Service.

9   Close the Services control panel application.

Configuring NetBackup for Exchange backups that use Granular Recovery Technology (GRT)

Before you configure for granular recovery with NetBackup, ensure that you have met the requirements for using Granular Recovery Technology (GRT). These requirements include the configuration of NFS.

See "Requirements to perform backups and restores of Exchange with Granular Recovery Technology (GRT)" on page 34.

Table 4-3   Configuring NetBackup for Exchange backups that use Granular Recovery Technology (GRT)

Step	Action	Description
Step 1	Review the limitations and conditions.	See "About disk storage units and restores that use Granular Recovery Technology (GRT)" on page 63. See "Limitations and conditions for restores using Exchange Granular Recovery Technology (GRT)" on page 63.
Step 2	Create a user account for the NetBackup Client Service and configure the log on account for this service.	See "About configuring the NetBackup Client Service for backups and restores that use Granular Recovery Technology (GRT) or MAPI" on page 55.
Step 3	For non-VMware backups, select **Enable granular recovery** in the backup policy.	Granular recovery is automatically provided for VMware backups that protect Exchange. You do not need to enable it in the policy. See "About configuring snapshot backups of Exchange Server" on page 101. See "Configuring a streaming NetBackup for Exchange policy (Exchange 2007 and earlier)" on page 123.
Step 4	(Optional for non-VMware backups) Disable the cataloging when you duplicate any Exchange backups that use GRT.	See "Disabling the cataloging for duplications of Exchange backups using Granular Recovery Technology (GRT)" on page 64. You cannot use the Administration Console to duplicate VMware backups that protect Exchange. A command-line option is available. See "Duplicating a VMware backup that protects Exchange" on page 201.
Step 5	Configure a granular proxy server.	See "Configuring the granular restore proxy host" on page 73.

Table 4-3   Configuring NetBackup for Exchange backups that use Granular
                 Recovery Technology (GRT) *(continued)*

Step	Action	Description
Step 6	Configure the privileges for granular operations.	See "Configuring Exchange client and server privileges" on page 67.
Step 7	If applicable, configure the list of Exchange hosts.	See "Configuring the Exchange hosts for backups that use Granular Recovery Technology (GRT) " on page 65.

About disk storage units and restores that use Granular Recovery Technology (GRT)

Granular information is only cataloged for a backup image that is made to a disk storage unit. A backup that is made directly to tape does not contain granular information. You can duplicate the image to tape, but you cannot directly back up to tape. If you configure backups to a disk storage unit, no further configuration is required. You can only perform restores of individual items using Granular Recovery Technology (GRT) if the backup resides on a disk storage unit.

More information is available on the disk storage units that are supported with GRT.

See the *NetBackup Release Notes.*

Limitations and conditions for restores using Exchange Granular Recovery Technology (GRT)

The following limitations and conditions exist for jobs using Granular Recovery Technology (GRT):

■ The feature is limited to certain versions of Exchange Server and Windows Server.
See the *NetBackup Operating System Compatibility List.*
See the *NetBackup Database Agent Compatibility List.*

■ This feature only supports full and user-directed backups. NetBackup lets you create a complete policy for disaster recovery, with all the various types of schedules. However, you cannot restore individual items from an incremental backup.

■ Backups must be made to a disk storage unit, not to tape, and restores that use GRT must be made from a disk storage unit. You can manually duplicate the backup image to disk, but you cannot restore from the tape copy.

See "About disk storage units and restores that use Granular Recovery Technology (GRT)" on page 63.

■ Exchange Server provides a feature to retain deleted items for a period of time after you "permanently" delete them. Because the deleted items still exist, NetBackup includes them in the backup image. NetBackup displays these items when you browse the granular backup image and you can restore these items.

Disabling the cataloging for duplications of Exchange backups using Granular Recovery Technology (GRT)

Note: This option does not apply to duplicating Exchange VMware backups.

See "Duplicating a VMware backup that protects Exchange" on page 201.

Unlike a duplication of a backup that uses Granular Recovery Technology (GRT) from tape to disk, duplication of the same backup from disk to tape takes extra time. NetBackup requires this extra time to catalog the granular Exchange information. You can choose not to catalog the granular information so that the duplication is performed more quickly. However, then users are not able to browse for individual items on the image that was duplicated to tape if the disk copy expires.

During the duplication process, NetBackup writes log entries periodically to show the progress of the job.

To disable the cataloging of Exchange backups using Granular Recovery Technology

1 On the master server, open the NetBackup Administration Console.

2 In the left pane, expand **Host Properties**.

3 Click **Master Servers**.

4 In the right pane, right-click the master server click **Properties**.

5 Click **General Server**.

6 Uncheck **Enable message-level cataloging when duplicating Exchange images that use Granular Recovery Technology**.

7 Click **OK**.

Configuring the Exchange hosts for backups that use Granular Recovery Technology (GRT)

In NetBackup you can provide a list of the Exchange hosts so that a virtual client name can be used for the backup. You set the configuration parameters in the host properties for the master server.

For non-VMware backups, the following information applies:

- When you perform a backup with Granular Recovery Technology (GRT) in a DAG, cluster, or private network, NetBackup catalogs backup images under the client name in the policy. This name is the virtual name (DAG, cluster, or private network name).

- For an off-host backup with GRT, NetBackup catalogs under the primary client name.

- If you use a proxy server for backups using Granular Recovery Technology (GRT), also add the proxy server to the list.

- For restores to be successful in an Exchange 2010 DAG environment, you must add the CAS server to the list.

For VMware backups, the following information applies:

- When you perform a backup of a DAG, NetBackup catalogs backup images under the client name (the VM name) in the policy. You do not need to configure the list of hosts.
  When you perform a backup of a node that exists in a DAG, NetBackup catalogs the Exchange view of the backup images under the DAG name. This is different from the VM guest name.

- For a standalone server, the backup is cataloged under a different client name if you chose a **Primary VM identifier** other than **VM hostame**. You must add the NetBackup client name and the name that reflects the identifier that you chose in the policy.

To configure the Exchange hosts for backups that use Granular Recovery Technology (GRT)

1   On the master server, open the NetBackup Administration Console.

2   Select **NetBackup Management > Host Properties > Master Servers**.

3   In the right pane, double-click on the master server.

4   Select **Distributed Application Restore Mapping**.

5 Click **Add**.

6 Provide the name of the application host and the name of the component host, as follows:

Environment	Application host	Component host
DAG	Virtual name of DAG	Physical name of *Node 1*
	Virtual name of DAG	Physical name of *Node 2*
	Virtual name of DAG	Physical name of *Node 3*
	Virtual name of DAG	Physical name of CAS server
	Exchange host name	Off-host computer name
Cluster	Virtual cluster name	Physical name of *Node 1*
	Virtual cluster name	Physical name of *Node 2*
	Virtual cluster name	Physical name of *Node 3*
	Exchange host name	Off-host computer name
CCR	Virtual name of cluster	Physical name of *Node 1*
	Virtual name of cluster	Physical name of *Node 2*
Off-host	Exchange host name	Off-host computer name

About Exchange client and server privileges

When you perform a restore, sometimes the source client is different than the client that NetBackup uses for backup processing. These situations include the following:

■ When you use an Exchange granular proxy host
You can specify the granular proxy host in the NetBackup Administration Console, with the `bpduplicate` command, or with the `bplist` command. Note that NetBackup uses the proxy host when you duplicate a backup image.

■ Off-host backups

■ When you use a private network

- Backups of a clustered Exchange server

- Backups of an Exchange 2010 Database Availability Group

- When you select a destination client other than the source client to either browse the backup image or when you perform a restore

If one of these situations applies to your NetBackup configuration, the following requirements exist:

- The client(s) or the media server must have the same version of Windows as the client from which the backup is made.

- For Windows 2008 and Windows 2008 R2, the client(s) must have Services for Network File System enabled (under File Services). For Windows 2003 R2 SP2, the client(s) must have NFS installed.
  See "About installing and configuring Network File System (NFS) for Exchange Granular Recovery" on page 35.

- The proxy server must also meet the following additional requirements:

  - Has the same NetBackup version as the Exchange hosts

  - Uses the same NetBackup master server

- The client(s) or the media server must have privileges to perform granular operations.
  See "Configuring Exchange client and server privileges" on page 67.

Configuring Exchange client and server privileges

This configuration is required if you want to browse backups or perform restores and you have an environment where the source client is different than the client that NetBackup uses for backup processing. More information is available on when this configuration is necessary.

See "About Exchange client and server privileges" on page 66.

Alternatively, you can perform a server-directed restore. Further instructions are available on how to allow redirected restores in the *NetBackup Administrator's Guide, Volume I*.

To configure Exchange client and server privileges

1. On the master server, create the `altnames` directory, as follows:

   - In a non-clustered environment, create the following directory:
     install_path\NetBackup\db\altnames

   - In a clustered environment, create the following directory:

shared_drive_install_path\NetBackup\db\altnames

2   In the `altnames` directory, create a *peername* file.

peername refers to:

- The granular proxy host name
  See "Configuring the granular restore proxy host" on page 73.

- The off-host client name

- The private network host name

- The node names in the cluster
  Create a `peername` file for each node in the cluster.

- The physical Exchange servers in a DAG
  For a 2010 DAG, create one file for each physical Exchange server in the DAG.

- The destination client name, if it is different than the source client

For example, consider that you have a source client named `ClientA` and you want to use a proxy host named ProxyClient. On the master server, you create a file that is called `proxyclient`.

3   In the *peername* file, add the name of the source client.

The source client is the client that originally performed the backup. For clustered clients, use the virtual Exchange name. For a backup within a private network, use the private network host name. For a DAG, use the DAG name; this name should be the client name in the policy.

For example, in the `proxyclient`, include the name `clienta`.

Configuring host properties for Exchange clients

Note: These host properties do not apply to VMware backups that protect Exchange.

In the Exchange client host properties you configure settings for the Exchange clients you selected.

To configure Exchange client host properties

1   Open the NetBackup Administration Console or the Remote Administration Console.

2   In the left pane, expand **NetBackup Management > Host Properties > Clients**.

3   In the right pane, select the Exchange client(s) you want to configure.

> **Note:** For clustered or replicated environments, select each node. You must configure the same settings on each node. If you change the attributes for the virtual name of the client, only the active node or current node is updated.

4   Click **Actions > Properties**.

5   Expand **Windows Client** and click **Exchange**.
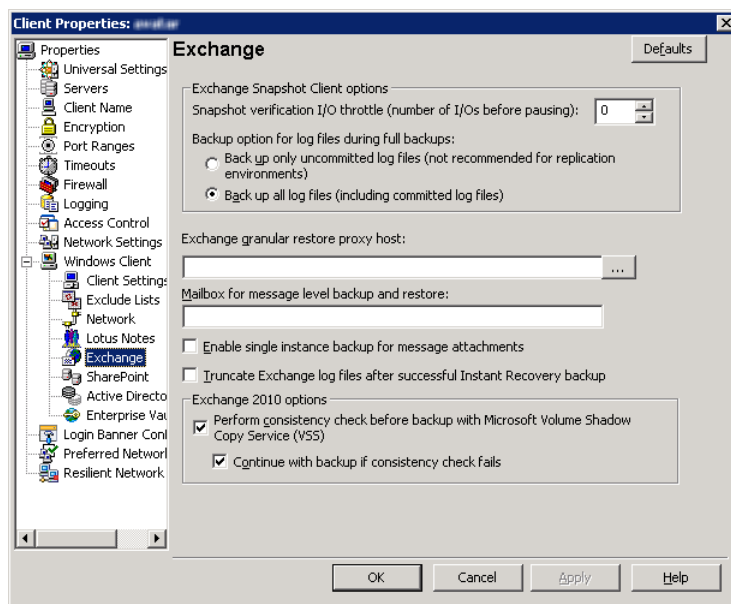
6   Enable the options you want.

See "Exchange properties" on page 69.

7   Click **OK**.

Exchange properties

The **Exchange** properties apply to the currently selected Windows clients. For clustered or replicated environments, configure the same settings for all nodes. If you change the attributes for the virtual server name, only the active node is updated.

Note: Except for **Exchange granular restore proxy host**, these host properties do not apply to VMware backups that protect Exchange.

The **Exchange** dialog box contains the following properties.

Table 4-4　　　　　Exchange dialog box properties

Property	Description
Snapshot verification I/O throttle	For snapshot backups, specify the number of I/Os to process for each 1-second pause. This option applies to Exchange 2003 SP2 and to Exchange 2007 if the Exchange Management Console is not installed on the alternate client. See "About configuring a pause in consistency checks for Exchange 2007 and earlier" on page 71.
Backup option for log files during full backups	Choose which logs to include with snapshot backups: ■ **Back up only uncommitted log files** Select this option to back up only the log files that are uncommitted. This option is not recommended for Exchange 2010 DAG or Exchange 2007 CCR environments. ■ **Back up all log files (including committed log files)** See "About backing up all or only uncommitted Exchange transaction log files with snapshot backups" on page 71. Note: As of NetBackup 7.0, the default option is now **Back up all log files (including committed log files)**. If you previously changed this setting for a client, your selection remains the same. For new installations of NetBackup, the default is **Back up all log files (including committed log files)**. For upgrade installations where you did not change this setting for a client, the default is changed to **Back up all log files (including committed log files)**
Truncate log after successful Instant Recovery backup	Enable this option to delete transaction logs after a successful Instant Recovery backup. By default, transaction logs are not deleted for a full Instant Recovery backup that is snapshot only. See "About truncating Exchange transaction logs with Instant Recovery backups" on page 72.
Exchange granular restore proxy host	You can specify a different Windows system to act as a proxy for the source client. Use a proxy if you do not want to affect the source client or if it is not available. This situation applies when you duplicate a GRT-enabled backup image from a disk storage unit to a tape storage unit or when you use the `bplist` command. See "Configuring the granular restore proxy host" on page 73. See "About Exchange client and server privileges" on page 66.

	Table 4-4	Exchange dialog box properties *(continued)*
Property		**Description**
Mailbox for message level backup and restore		As of NetBackup 7.0, this setting no longer needs to be configured.
Enable single instance backup for message attachments		Enable this option to back up the data that is stored on a Single Instance Store (SIS) volume. This feature only applies to Exchange Server 2007 and earlier versions.
		See "About configuring Exchange Single Instance Store backups (Exchange 2007 and earlier) " on page 74.
Perform consistency check before backup with Microsoft Volume Shadow Copy Service (VSS)		Disable this option if you do not want to perform a consistency check during an Exchange 2010 DAG backup. If you check **Continue with backup if consistency check fails**, NetBackup continues to perform the backup even if the consistency check fails.
		See "About consistency checks options for an Exchange 2010 backup" on page 74.

About configuring a pause in consistency checks for Exchange 2007 and earlier

Note: This option is only applicable to Exchange 2003 SP2 or later and for Exchange 2007 if the Exchange Management Console is not installed on the alternate client.

The value is used during snapshot validation by the Exchange command ESEUTIL /pXXX where XXX is the value of **Snapshot verification I/O throttle**. ESEUTIL defines the /p setting as a forced 1-second pause after every XXX I/Os to limit the I/O rate during database verification. See the Microsoft Exchange documentation regarding the ESEUTIL command for details.

For more information on how to configure client settings in the host properties, see the following topic:

See "Configuring host properties for Exchange clients" on page 68.

About backing up all or only uncommitted Exchange transaction log files with snapshot backups

The **Back up option for log files during full backups** determines how many log files are backed up during a full or user-directed snapshot backup. You can adjust this setting in the host properties for the Exchange client.

Note: In NetBackup 7.0, the default option is now **Back up all log files (including committed log files)**. If you previously changed this setting for a client, your selection remains the same. For new installations of NetBackup, the default is changed to **Back up all log files (including committed log files)**. For upgrade installations where you did not change this setting for a client, the default is changed to **Back up all log files (including committed log files)**

If you select **Back up only uncommitted log files** NetBackup only backs up and catalogs the transaction log files that were not committed to the Exchange database at the time that the snapshot was taken. Exchange requires these uncommitted log files during the recovery of the Exchange database to make the database consistent. If **Back up all log files (including committed log files)** is selected, all of the log files that exist on the snapshot volume are backed up and cataloged.

Back up only uncommitted log files is not recommended for replicated environments. See the following TechNote:

http://www.symantec.com/docs/TECH88101

When you back up only the uncommitted log files, the advantage is that less space is needed on the storage unit for the transaction logs. When you back up all of the log files, the advantage is that a consecutive set of log files is maintained. A previous full backup can use these log files for rolling forward. These options do not affect the ability to recover the current full or user-directed type backup. These options do affect the ability to roll forward from a previous full or user-directed type backup.

For example, consider if a full backup is performed, followed by two differential backups, followed by another full backup. If **Back up all log files** is specified, all of the log files exist in backup images. The first full backup, the log files from the two differential backups, and the log files from the second full backup can be restored. The existence of all the log files allows for a roll-forward recovery. If you select **Back up only uncommitted log files**, a gap exists in the sequence of transaction logs that are in the backup images. From the full backup, you can restore only as far as the time that is covered in the two differential backups.

For more information on how to configure the client host properties, see the following topic:

See "Configuring host properties for Exchange clients" on page 68.

About truncating Exchange transaction logs with Instant Recovery backups

By default, Exchange transaction logs are not truncated for a full Instant Recovery backup that does not back up to a storage unit. To truncate logs enable **Truncate**

log after successful Instant Recovery backup in the Exchange properties for the client. Consider carefully before you select this option. Ensure that you have an independent method to retain your snapshots for disaster recovery. Alternatively, you can perform a full Instant Recovery backup to a storage unit.

See "Truncating Exchange transaction logs by performing a backup to a storage unit" on page 73.

For more information on how to configure the client host properties, see the following topic:

See "Configuring host properties for Exchange clients" on page 68.

Truncating Exchange transaction logs by performing a backup to a storage unit

To truncate Exchange transaction logs by performing a backup to a storage unit

1   Create a new backup policy.

2   Create a full or a differential schedule type.

3   In the attributes for the schedule, select **Snapshots and copy snapshots to a storage unit**.

4   Select a storage unit for the policy.

5   Perform a snapshot backup with this policy.

Configuring the granular restore proxy host

When you browse for or restore individual items using Granular Recovery Technology (GRT), NetBackup uses the destination client to stage a virtual copy of the database that you want to restore. However, NetBackup uses the source client of the backup to stage the database in the following situations: when you duplicate a GRT-enabled backup image or when you use the `bplist` command. Alternatively, you can specify a different Windows system to act as a proxy for the client. Use a proxy if you do not want to affect the source client or if the source client is not available.

To specify a proxy, configure the **Exchange granular proxy host** in the Exchange properties for the client.

When you use the `bplist` command and the `bpduplicate` command, you can override the **Exchange granular proxy host** setting with the `-granular_proxy` option. More information is available on how to specify the granular host with these commands.

See "About using the command line to browse or restore Exchange granular backup images" on page 188.

NetBackup determines the granular restore proxy host in the following order:

- The host that is specified with the `-granular_proxy` option on the command line
- The granular restore proxy host that you specify in the host properties for the source client
- The source client

More information is available about how to configure the client host properties and about the requirements for the granular proxy server.

See "Configuring host properties for Exchange clients" on page 68.

See "About Exchange client and server privileges" on page 66.

About configuring Exchange Single Instance Store backups (Exchange 2007 and earlier)

Exchange Server 2007 and earlier uses the Single Instance Store (SIS) to maintain single-instance storage of mail messages. This capability in Exchange Server allows the database to keep one copy of a message sent to multiple users on the same server.

To back up the data that is stored on an SIS volume, select **Enable single instance backup for message attachments**. Enable this option in the Exchange properties for the NetBackup client where Exchange Server is installed.

See "Configuring host properties for Exchange clients" on page 68.

Note the following:

- This feature is only available for MAPI mailbox backups, not for snapshot backups or any backups that use Granular Recovery Technology (GRT).
- Only attachments larger than 100 KB are backed up as SIS objects. Attachments smaller than 100 KB are backed up with each individual message.

See "About configuring NetBackup for Exchange" on page 53.

About consistency checks options for an Exchange 2010 backup

By default, NetBackup is configured to run a consistency check on Exchange 2010 backups. The consistency check that runs on the snapshot determines if possible data corruption exists. For standalone servers, you must perform a consistency check. Consistency checks are optional for an Exchange 2010 Database Availability

Group (DAG). You can configure this option in the host properties for the Exchange client.

If **Perform consistency check before backup with Microsoft Volume Shadow Copy Service (VSS)** is selected, NetBackup backs up Exchange objects as follows:

- If you do not select **Continue with backup if consistency check fails**, a database backup fails if it contains database files or transaction log files that are corrupt. All other non-corrupt databases that you selected are backed up.

- When you select **Continue with backup if consistency check fails**, then all Exchange data is backed up regardless if corrupt files are detected.

For more information on how to configure client settings in the host properties, see the following topic:

See "Configuring host properties for Exchange clients" on page 68.

See "About snapshot backups with Exchange Server" on page 20.

Testing configuration settings for NetBackup for Exchange

After you configure the master server for NetBackup for Exchange, test the configuration settings. Perform a manual backup (or backups) with the automatic backup schedules you created. A description of status codes and other troubleshooting information is available.

See the *NetBackup Status Codes Reference Guide*.

See the *NetBackup Troubleshooting Guide*.

Note: A manual back creates a real backup. Exchange logs are truncated, if appropriate.

To test the configuration settings

1   Log onto the master server as administrator (Windows) or root (UNIX).

2   Start the NetBackup Administration Console.

3   In the left pane, click **Policies**.

4   Click the policy you want to test.

5 Select **Actions > Manual Backup**.

The **Schedules** pane contains the name of an automatic schedule (or schedules) configured for the policy that you want to test. The **Clients** pane contains the name of the client(s) listed in the policy that you want to test.

6 Follow the directions in the **Manual Backup** dialog box.

7 To check the status of the backup, click **Activity Monitor** in the NetBackup Administration Console.

For more information, see the *Troubleshooting* chapter.

Configuring Exchange backup policies (non-VMware)

This chapter includes the following topics:

- About configuring a backup policy for Exchange Server

- About configuring snapshot backups of Exchange Server

- About configuring Instant Recovery backups of Exchange Server (Exchange 2007 and later)

- Configuring a streaming NetBackup for Exchange policy (Exchange 2007 and earlier)

- Configuring a policy for backups of individual Exchange mailboxes or public folders (Exchange 2007 and earlier)

About configuring a backup policy for Exchange Server

Note: To configure a backup policy for full VMware backups that protect Exchange Server, you follow a different procedure. Incremental backups must be performed with an MS-Exchange-Server policy.

See "About protecting Exchange Server data with VMware backups" on page 193.

A backup policy for a database defines the backup criteria for a specific group of one or more clients.

These criteria include the following:

- Storage unit and media to use
- Policy attributes
  You can configure snapshot backups and backups that uses Granular Recovery Technology (GRT). For Exchange 2007 and earlier, you can also configure streaming database backups, MAPI mailbox backups, and public folder backups.
- Backup schedules
- Clients to be backed up
- Items (database objects) to be backed up

To back up a database environment, define at least one MS-Exchange-Server policy with the appropriate schedules. A configuration can have a single policy that includes all clients, or there can be many policies, some of which include only one client.

Most requirements for database policies are the same as for file system backups. In addition to the policy attributes for this database agent, other attributes are available that you should consider.

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

Table 5-1   Configuring a backup policy for Exchange Server

Step	Action	Description
Step 1	Refer to the policy recommendations for your Exchange version.	See "Policy recommendations for Exchange Server 2010" on page 79. See "Policy recommendations for Exchange Server 2007 and earlier database backups" on page 82. See "Policy recommendations for Exchange Server 2007 and earlier MAPI backups" on page 83.

Table 5-1   Configuring a backup policy for Exchange Server *(continued)*

Step	Action	Description
Step 2	Refer to the instructions for the type of backup you want to perform.	See "Configuring NetBackup for Exchange backups that use Granular Recovery Technology (GRT)" on page 62. See "About configuring snapshot backups of Exchange Server" on page 101. See "About configuring Instant Recovery backups of Exchange Server (Exchange 2007 and later)" on page 113. See "Configuring a streaming NetBackup for Exchange policy (Exchange 2007 and earlier)" on page 123. See "Configuring a policy for backups of individual Exchange mailboxes or public folders (Exchange 2007 and earlier)" on page 126.
Step 3	Configure the policy attributes.	See "About policy attributes for NetBackup for Exchange" on page 85.
Step 4	Configure the schedules for your policy.	See "Adding schedules to a NetBackup for Exchange policy" on page 86.
Step 4	Add clients to your policy.	See "Adding clients to a NetBackup for Exchange policy" on page 89.
Step 5	Add backup selections to your policy.	See "Adding backup selections to an Exchange policy" on page 90.

See "About configuring NetBackup for Exchange" on page 53.

Policy recommendations for Exchange Server 2010

Refer to the following recommendations when you create policies for an Exchange Server 2010 Database Availability Group (DAG):

■ Create a policy that backs up an entire DAG or one or more databases in a DAG. This policy supports full, incremental, and user-directed backups.
To perform a backup with Granular Recovery Technology (GRT) select the **Enable granular recovery** option. Then you can restore databases and individual mailbox and public folder items. You cannot restore individual mailbox and public folder items from any incremental backups.

- MAPI mailbox and public folder backups are not supported with Exchange 2010.
- The example policies include the basic policy settings for an Exchange backup. For more information on how to create policies, see the following:
  See "About configuring snapshot backups of Exchange Server" on page 101.

Table 5-2   Example policy that backs up all databases in an Exchange DAG

Policy item	Configuration
Policy type	**MS-Exchange-Server**
Backup selections	Microsoft Exchange Database Availability Groups:\
Auto backup frequency	Weekly Full Daily Incremental
Enable granular recovery	Optional. Enable this option if you want to restore individual mailbox and public folder objects from the database backup.
Other configuration	**Perform snapshot backups** must be enabled. You can include multiple clients on the **Clients** tab. The client names are the DAG names.

Table 5-3   Example policy that backs up a database for an Exchange DAG

Policy item	Configuration
Policy type	**MS-Exchange-Server**
Backup selections	Microsoft Exchange Database Availability Groups:*Mailbox Database* Microsoft Exchange Database Availability Groups:*forest or domain name*\Microsoft Information Store*Mailbox Database*
Auto backup frequency	Weekly Full Daily Incremental
Enable granular recovery	Optional. Enable this option if you want to restore individual mailbox and public folder objects from the database backup.
Other configuration	**Perform snapshot backups** must be enabled. You can only include one client on the **Clients** tab. A DAG is the client for the policy.

Refer to the following recommendations when you create policies for an Exchange 2010 standalone server:

■ Create a policy that backs up the Information Store or individual databases. To perform a backup with Granular Recovery Technology (GRT), select the **Enable granular recovery** option. This policy supports full, incremental, and user-directed backups.

From either policy you can restore databases and individual mailbox and public folder items. You cannot restore individual mailbox or public folder items from any incremental backups that use GRT.

■ MAPI mailbox and public folder backups are not supported with Exchange 2010.

■ For information on how to create snapshot backup policies, see the following: See "About configuring snapshot backups of Exchange Server" on page 101.

Table 5-4   Example policy that backs up all database in an Exchange 2010 standalone server

Policy item	Configuration
Policy type	**MS-Exchange-Server**
Backup selections	Microsoft Information Store:\
Auto backup frequency	Weekly Full Daily Incremental
Enable granular recovery	Optional. Enable this option if you want to restore individual mailbox and public folder objects from the database backup.
Other configuration	**Perform snapshot backups** must be enabled.

Table 5-5   Example policy that backs up a database in an Exchange 2010 standalone server

Policy item	Configuration
Policy type	**MS-Exchange-Server**
Backup selections	Microsoft Information Store:*Mailbox Database*
Auto backup frequency	Weekly Full Daily Incremental
Enable granular recovery	Yes
Other configuration	**Perform snapshot backups** must be enabled.

See "About configuring NetBackup for Exchange" on page 53.

Policy recommendations for Exchange Server 2007 and earlier database backups

Refer to the following recommendations when you create database backup policies for Exchange Server 2007 and earlier:

- Create a policy that backs up the Information Store, a storage group, or an individual database. This policy supports full, incremental, and user-directed backups.

  To perform the backup with Granular Recovery Technology (GRT) select the **Enable granular recovery** option. Then you can restore databases and individual mailbox and public folder items. You cannot restore these individual items from any incremental backups that use GRT.

- The example policies include the basic policy settings for an Exchange backup. For more information on how to create policies, see the following:

  See "About configuring snapshot backups of Exchange Server" on page 101.

  See "Configuring a streaming NetBackup for Exchange policy (Exchange 2007 and earlier)" on page 123.

Table 5-6   Example Exchange 2007 and earlier streaming backup or snapshot policy that backs up all the databases

Policy item	Configuration
Policy type	**MS-Exchange-Server**
Backup selections	Microsoft Information Store:\
Auto backup frequency	Weekly Full Daily Incremental
Enable granular recovery	Optional. Enable this option if you want to restore individual mailbox and public folder objects from the database backup.
Other configuration	For snapshot backups, select **Perform snapshot backups**.

Table 5-7   Example snapshot policy that backs up a storage group for an Exchange 2007 or earlier database

Policy item	Configuration
Policy type	**MS-Exchange-Server**
Backup selections	Microsoft Information Store:*Storage Group*

Table 5-7   Example snapshot policy that backs up a storage group for an
                   Exchange 2007 or earlier database *(continued)*

Policy item	Configuration
Auto backup frequency	Weekly Full Daily Incremental
Enable granular recovery	Optional. Enable this option if you want to restore individual mailbox and public folder objects from the database backup.
Other configuration	Select **Perform snapshot backups**.

Table 5-8   Example Exchange 2007 or earlier streaming backup policy that
                   backs up a storage group or a storage group database

Policy item	Configuration
Policy type	**MS-Exchange-Server**
Backup selections	Microsoft Information Store:*Storage Group* Microsoft Information Store:*Storage Group**Database*
Auto backup frequency	Weekly Full Daily Incremental
Enable granular recovery	Optional. Enable this option if you want to restore individual mailbox and public folder objects from the database backup.
Other configuration	Do not select **Perform snapshot backups**. To ensure that transaction logs are deleted regularly include all databases for a storage group in a full backup policy. Or specify the storage group (not individual databases) in the backup policy. See "About Exchange backups and transaction logs" on page 100.

See "About configuring NetBackup for Exchange" on page 53.

Policy recommendations for Exchange Server 2007 and earlier MAPI backups

Refer to the following recommendations when you create MAPI backup policies for Exchange Server 2007 and earlier:

- Create a policy that backs up mailbox objects. This policy supports full, incremental, and user-directed backups. (In Table 5-9.)

- Create a policy that backs up public folder objects. This policy supports full, incremental, and user-directed backups. (In Table 5-10.)

- The **Enable granular recovery** and **Perform snapshot backups** options are not applicable for MAPI backups.

- The example policies include the basic policy settings for an Exchange backup. For more information on how to create policies, see the following:
  See "Configuring a policy for backups of individual Exchange mailboxes or public folders (Exchange 2007 and earlier)" on page 126.

Table 5-9   NetBackup policy example for Exchange Server 2007 or earlier MAPI mailbox backup

Policy item	Configuration
Policy type	**MS-Exchange-Server**
Backup selections	Microsoft Exchange Mailboxes:\
Auto backup frequency	Weekly Full Daily Incremental
Enable granular recovery	Not applicable for MAPI backups.
Other configuration	A backup of all mailboxes may not complete within the backup windows. Consider adding smaller groups of mailboxes to multiple policies. **Perform snapshot backups** is not applicable for MAPI backups.

Table 5-10   NetBackup policy example for Exchange Server 2007 or earlier MAPI public folder backup

Policy item	Configuration
Policy type	**MS-Exchange-Server**
Backup selections	Microsoft Exchange Public Folders:\
Auto backup frequency	Weekly Full Daily Incremental
Enable granular recovery	Not applicable for MAPI backups.

Table 5-10 NetBackup policy example for Exchange Server 2007 or earlier MAPI
public folder backup *(continued)*

Policy item	Configuration
Other configuration	**Perform snapshot backups** is not applicable for MAPI backups.

See "About configuring NetBackup for Exchange" on page 53.

About policy attributes for NetBackup for Exchange

With a few exceptions, NetBackup manages a database backup like a file system
backup. Other policy attributes vary according to your specific backup strategy
and system configuration.

For more information on policy attributes, see the *NetBackup Administrator's
Guide, Volume I*.

Table 5-11 Policy attribute descriptions for NetBackup for Exchange policies

Attribute	Description
Policy type	Determines the types of clients that can be in the policy. In some cases the policy type determines the types of backups that NetBackup can perform on those clients. To use the Exchange database agent, you must define at least one policy of type that is MS-Exchange-Server.
Policy storage	In an Exchange 2010 DAG environment where the Exchange server is a both a client and a media server, policy storage is treated differently. If you want to back up to the local Exchange client that is also a media server, specify a storage unit group. NetBackup automatically selects the local storage unit from the storage unit group during the backup processing. If you specify a single storage unit, all backups use this storage unit.
Allow multiple data streams	Specifies that NetBackup can divide automatic backups for each client into multiple jobs. Each job backs up only a part of the list of backup selections. The jobs are in separate data streams and can occur concurrently. The number of available storage units, multiplex settings, and the maximum jobs parameters determine the total number of streams and how many can run concurrently. Not all directives in the backup selections list allow for multiple database streams.

For Exchange 2010, you can create multiple data streams at the database level. For Exchange 2007 and earlier, you can create multiple data streams at the storage group level. For MAPI mailbox and public folder backups, you can create multiple data streams at the mailbox or public folder level. |

Table 5-11	Policy attribute descriptions for NetBackup for Exchange policies *(continued)*

Attribute	Description
Enable granular recovery	Allows restores of individual items using Granular Recovery Technology (GRT). Users can only restore individual items from a full backup. (You can perform incremental backups using GRT, but the backup does not save granular information and you cannot restore individual items from an incremental backup.)
	You can restore individual items only if the backup image resides on a disk storage unit. If you want to retain a granular backup on tape, you must duplicate the image. If you want to restore from a granular backup that was duplicated to tape, you must import the image to a disk storage unit.
	See "About disk storage units and restores that use Granular Recovery Technology (GRT)" on page 63.
	Exchange Server GRT-enabled backups do not support encryption or compression.
Keyword phrase	A textual description of a backup. Useful for browsing backups and restores.
Perform snapshot backups	This option enables snapshot backups. For Exchange 2010 you must enable this option for all backup policies.
	See "About snapshot backups with Exchange Server" on page 20.
Microsoft Exchange Attributes	Indicates what database backup source you want to use for an Exchange 2010 Database Availability Group (DAG) or for an Exchange 2007 replication backup (LCR or CCR). For Exchange 2010, you can also indicate a preferred server list.
	See "Backup source for an Exchange 2010 DAG backup or an Exchange 2007 replication backup " on page 110.
	See "Configuring a preferred server list for an Exchange 2010 Database Availability Group (DAG)" on page 111.

Adding schedules to a NetBackup for Exchange policy

Each policy has its own set of schedules. These schedules control the initiation of automatic backups and also specify when user operations can be initiated.

To add a schedule to a NetBackup for Exchange policy

1   In the **Policy** dialog box, click the **Schedules** tab.

    To access the **Policy** dialog box, double-click the policy name in the **Policies** list in the NetBackup Administration Console.

2   Click **New**.

3   Specify a unique name for the schedule.

4   Select the **Type of backup**.

5   Specify the other properties for the schedule.

6   Click **OK**.

NetBackup for Exchange backup types

This topic describes the types of backups you can schedule for backups of Exchange Server.

Note: Incremental backups fail if database circular logging is configured for the Exchange Server. See Microsoft's *Exchange Server Administration Guide* for more information on how to configure circular logging.

Note: Incremental backups back up the Exchange transaction logs. Therefore, since Exchange 2007 and earlier maintains transaction logs at the storage group level, NetBackup performs incremental backups of storage groups, not individual databases within storage groups. NetBackup lets you configure incremental schedules for individual databases. The backup job still runs according to the configured incremental schedules, but the job logs warnings for attempted incremental backups of these objects.

Table 5-12   NetBackup for Exchange backup types

Type of backup	Description
Full backup	This schedule type backs up the Exchange Server database and associated transaction logs. Exchange truncates all committed transaction logs after NetBackup notifies it that the backup succeeded. In replicated environments, the truncation is scheduled and does not occur immediately.
	By default, transaction logs are not truncated for Instant Recovery backups. You can enable the truncation of logs for this type of backup or you can perform a backup to a storage unit.
	See "About truncating Exchange transaction logs with Instant Recovery backups" on page 72.
	See "Truncating Exchange transaction logs by performing a backup to a storage unit" on page 73.

Table 5-12   NetBackup for Exchange backup types *(continued)*

Type of backup	Description
Differential incremental backup	Includes the changes since the last full or differential incremental backup. After NetBackup notifies it that the backup succeeded, Exchange truncates all committed transaction logs. The truncation of the transaction logs sets the context for the next backup. For backups of databases, storage groups, or the entire Information Store, the backup only includes the transaction logs. This type of schedule is not supported for Exchange 2003 pre-SP1 snapshot backups. Individual items cannot be restored for this type of backup if **Enable granular recovery** is enabled. To perform a full restore the data that is needed is contained in multiple NetBackup images. One image for the full backup and another image for each differential incremental that was performed.
Cumulative incremental backup	Includes the changes since the last full backup or differential incremental backup. (However, most configurations do not mix cumulative and differential incremental backups between full backups.) Exchange does not truncate the logs when the backup is completes. When a series of cumulative incremental backups follows a full backup, transaction logs remain intact since the last full backup. For backups of databases, storage groups, or the entire Information Store, the backup only includes the transaction logs. For Exchange 2007 and earlier, you also can use this schedule type to back up changes to the mailboxes or the Public Folders. This type of schedule is not supported for Exchange 2003 pre-SP1 snapshot backups. Individual items cannot be restored for this type of backup if **Enable granular recovery** is enabled. Consider an Exchange Server data recovery scenario where the transaction logs are all intact. You only need to restore the database from the last full backup and the last cumulative incremental backup. During recovery, Exchange Server replays all the logs that are in the log folder.
User backup	A user backup is not automatically scheduled and is initiated on the target client computer. It is like a snapshot (or a copy backup) of the databases at a given point in time. This backup does not affect the content of ongoing full and incremental backups. Transaction logs are not truncated for Exchange 2003 SP1 and later snapshot backups, but are truncated for Exchange 2003 pre-SP1 snapshot backups . For streaming backups, you can configure user backups to truncate the logs. See "Performing user-directed full streaming backups (Exchange 2007 and earlier)" on page 136. You may want to consider creating a separate policy for user backup schedule types. Then you can easily separate user-directed and scheduled backups when you restore files. If you decide to create separate policies for user backup schedule types, the considerations are similar to those for automatic backups. A backup selections list is not needed because users select the files to restore.

About NetBackup for Exchange schedule properties

This topic describes the schedule properties that have a different meaning for database backups than for file system backups. Other schedule properties vary according to your specific backup strategy and system configuration. Additional information about other schedule properties is available.

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

Table 5-13   Description of schedule properties

Property	Description
Type of backup	Specifies the type of backup that this schedule controls. The selection list shows only the backup types that apply to the policy you want to configure. See "NetBackup for Exchange backup types" on page 87.
Schedule type	You can schedule a backup in one of the following ways: ■ **Frequency** This setting is used only for scheduled backups. It is not used for user-directed backups. **Frequency** specifies the period of time that can elapse until the next backup or archive operation begins on this schedule. For example, assume that the frequency is seven days and a successful backup occurs on Wednesday. The next full backup does not occur until the following Wednesday. Typically, incremental backups have a shorter frequency than full backups. ■ **Calendar** This setting is used only for scheduled backups. It is not used for user-directed backups. The **Calendar** option allows you to schedule backup operations that are based on specific dates, recurring week days, or recurring days of the month. More information is available on schedule types and instant recovery backups. See "Adding schedules for Exchange Instant Recovery" on page 120. See "Schedules settings in Exchange Instant Recovery policies" on page 121.
Retention	Specifies a retention period to keep backup copies of files before they are deleted. The retention level also denotes a schedules priority within the policy. A higher level has a higher priority. Set the time period to retain at least two full backups of your database. In this way, if one full backup is lost, you have another full backup to restore. For example, if your database is backed up once every Sunday morning, you should select a retention period of at least 2 weeks.

Adding clients to a NetBackup for Exchange policy

The clients list contains a list of the clients that are backed up during an automatic backup. A NetBackup client must be in at least one policy but can be in more than one.

For a NetBackup for Exchange policy, clients you want to add must have the following software installed:

■ Exchange Server

■ NetBackup client or server

To add clients to a NetBackup for Exchange policy

1 In the **Policy** dialog box, click the **Clients** tab.

   To access the **Policy** dialog box, double-click the policy name in the **Policies** list in the NetBackup Administration Console.

2 Click **New**.

3 Type the name of the client and press **Enter** (Windows) or click **Add** (Java).

   Note the following:

   ■ If Exchange is clustered or in a Database Availability Group (DAG), specify the virtual Exchange name that represents that cluster or DAG.
     You can also use a DAG node name as the client in the policy, but only local databases are protected and are cataloged under that node name. Any attempts to back up databases on other nodes fail.

   ■ If you want to perform a restore from a backup using Granular Recovery Technology (GRT), ensure that the clients meet the requirements for granular restore.
     See "Configuring Exchange client and server privileges" on page 67.

   ■ For off-host backups, the client name should be the name of the primary client.

4 (Windows) To add another client, repeat step 2 and step 3.

5 (Java) To add another client, repeat step 3.

6 If this client is the last client you want to add, click **OK**.

7 (Java) In the **Policy** dialog box, click **Close**.

Adding backup selections to an Exchange policy

The backup selections list defines the Exchange objects to back up and the grouping of Exchange objects for multiple data streams. Exchange objects are defined through directives. You can append an individual object name to a directive to specify a storage group, database, mailbox, or public folder. You can use wildcards to specify a group of such objects.

Note: In a backup policy, include directives from only one directive set. For example, do not add `Microsoft Exchange Database Availability Groups:\` (a DAG directive) and `Microsoft Information Store:\` (a standalone database directive) to the same policy. Also do not add `Microsoft Information Store:\` and `Microsoft Exchange Mailboxes:\` or `Microsoft Exchange Public Folders:\` to the same policy.

The following directives exist:

Table 5-14   NetBackup for Exchange Server directive sets and directives

Directive set	Directive(s)	Notes
MS_Exchange_Database	NEW_STREAM Microsoft Information Store:\	This directive set applies to Exchange 2010 standalone servers and to Exchange 2007 and earlier. See "Notes and limitations for creating a backup selections list for Exchange 2007 and earlier streaming database backups" on page 126. See "About excluding Exchange items from backups" on page 96.
MS_Exchange_ Database_ Availability_Groups	NEW_STREAM Microsoft Exchange Database Availability Groups:\	
MS_Exchange_Mailbox	NEW_STREAM Microsoft Exchange Mailboxes:\	Only supported for Exchange 2007 and earlier. See "Notes and limitations when you create a backup selections list for MAPI mailbox and public folder backups" on page 129. See "About excluding Exchange items from backups" on page 96.
MS_Exchange_Public_ Folders	NEW_STREAM Microsoft Exchange Public Folders:\	Only supported for Exchange 2007 and earlier. See "Notes and limitations when you create a backup selections list for MAPI mailbox and public folder backups" on page 129. See "About excluding Exchange items from backups" on page 96.

Refer to the following topics when you add backup selections:

■ See "Adding Exchange entries to a backup selections list by browsing (Windows only)" on page 92.

- See "Adding Exchange entries to the backup selections list manually" on page 92.

- See "Performing Exchange backups with multiple data streams" on page 93.

- See "About excluding Exchange items from backups" on page 96.

Adding Exchange entries to a backup selections list by browsing (Windows only)

On Windows systems, you can browse for Exchange objects and add them to the backup selections list. Alternatively, you can specify the objects manually..

To add Exchange entries to the backup selections list by browsing (Windows only)

1   In the **Policy** dialog box, click the **Backup Selections** tab.

2   Click **New**.

3   Click the **Remote Folder** icon.

4   Navigate to and click the Exchange object to back up and click **OK**.

5   If necessary, edit the entry.

- Append the object name to the new entry.

- If a mailbox specification without wildcards does not end with a backslash, add it.

- Add wildcard characters if you want to define groups of objects or use multiple data streams.
See "Performing Exchange backups with multiple data streams" on page 93.
See "Using wildcards in an Exchange backup selections list" on page 94.

6   Click **OK**.

Adding Exchange entries to the backup selections list manually

You can add database objects manually to the backup selections list, if you do not want to use the browse feature.

To manually add entries to the backup selections list

1   In the **Policy** dialog box, click the **Backup Selections** tab.

2   Click **New**.

3   (Windows) Click the **Directives** button.

4   Select the directive set.

5   Select the directive.

6 Click **OK**.

7 Edit the new entry if you want to define groups of objects or use multiple data streams.

8 Click **OK**.

Performing Exchange backups with multiple data streams

When you enable multiple data streams, backups are divided into multiple jobs. Each job backs up only a part of the backup selections list. To use multiple data streams, enable **Allow multiple data streams** on the **Attributes** tab for the policy.

You can choose to have NetBackup automatically determine where to begin new streams by adding an asterisk (*) after the directive. Or you can control where each stream begins by inserting the NEW_STREAM directive at a certain point or points in the backup selections list. If you use wildcard characters to define Exchange objects in the backup selections list, those objects are backed up in multiple streams.

When you back up multiple Exchange 2010 databases, NetBackup groups the backup jobs by the selected server. One snapshot is performed for all of the replicated databases on a given server. Another snapshot is performed for all the active databases on the server. Multistreaming then applies to the database backups that are performed on each snapshot.

For more information on the multiple data streams feature, see the following:

NetBackup Administrator's Guide, Volume I

Using multiple datastreams with Exchange Database Availability Groups (DAG)s

When you back up databases in a Database Availability Group (DAG), NetBackup selects the server to back up each database according to your data source and preferred server list settings. The backup jobs are grouped by server. From your backup selections list, all of the databases that have passive copies on a given server are grouped under one snapshot job. They are then backed up by one or more child backup jobs. All of the databases that have active copies on the server are grouped under another snapshot job, followed by one or more backup jobs.

Note: Use explicit NEW_STREAM directives in a DAG only when you are confident which servers will back up which databases.

The NEW_STREAM directive works as follows:

- When you do not enable multiple backup streams, all of the databases for a snapshot job are backed up in a single backup job.

- When you enable multiple backup streams and do not specify any `NEW_STREAM` directives, each database is backed up in its own backup job.

- When you enable multiple backup streams and do specify `NEW_STREAM` directives in your policy, then NetBackup tries to group the database backups into jobs according to the placement of the `NEW_STREAM` directives in the backup selection list. The result is affected by the grouping of database backups into snapshot jobs. NetBackup separates backup jobs after any database that is followed by a `NEW_STREAM` directive in the policy.

See "About excluding Exchange items from backups" on page 96.

See "About configuring NetBackup for Exchange" on page 53.

Using wildcards in an Exchange backup selections list

Wildcard characters can be used to define groups of databases, storage groups, mailboxes or public folders. This way multiple objects can be backed up without having to specify the objects individually in the backup selections list. Multiple data streams must also be enabled. If this feature is not enabled, the backup fails.

See "Performing Exchange backups with multiple data streams" on page 93.

Table 5-15   Supported wildcard characters

Wildcard character	Action
Asterisk (*)	Use as a substitute for zero or more characters. Specify the asterisk as the last character in the string. Example: To specify all objects that start with an `a` use `a*`.
Question mark (?)	Use as a substitute for one or more characters in a name. Example 1: The string `s?z` processes all objects that have `s` for a first character, any character for a second character, and `z` for a third character. Example 2: The string `Data??se` processes all objects that have `Data` as the first four characters, any characters for the fifth and sixth characters, and `se` as the seventh and either characters.

Table 5-15 Supported wildcard characters *(continued)*

Wildcard character	Action
Left & right brackets ([...])	Use to match any one character that is enclosed in square brackets. A minus (–) can be used to indicate a range of consecutive characters; for example, [0-9] is equivalent to [0123456789].

These wildcard characters are not supported for the `Microsoft Information Store:\` directive or for the `Microsoft Exchange Database Availability Groups:\` directive.

Note: The minus (-) loses this special meaning if it occurs last in the string.

Note: The right square bracket (]) does not terminate such a string when it is the first character within it. For example, `[] a-f]` matches either a right square bracket (]) or one of the ASCII letters a through f inclusive. Asterisk (*) and Question Mark (?) stand for themselves within such a string of characters. |

The following rules apply when wildcard characters are used in the backup selections list:

- Only one wildcard pattern per backup selections list entry is allowed.

- If a wildcard pattern is not honored it is treated literally.

- Wildcard patterns are honored only in the final segment of the path name.
  Correct
```
Microsoft Information Store:\*
Microsoft Information Store:\StorageGroup?
Microsoft Information Store:\Database*
Microsoft Information Store:\Data??se
Microsoft Information Store:\Storage Group*
Microsoft Information Store:\Storage?G?oup
Microsoft Exchange Mailboxes:\John Anderson [janderson]\Top of
Information Store\*
Microsoft Exchange Database Availability Groups:\*
Microsoft Exchange Database Availability Groups:\Database*
Microsoft Exchange Database Availability Groups:\Data??se
```
  Incorrect
```
Microsoft Information Store:\StorageGroup?\Mailbox Database
```

```
Microsoft Exchange Mailboxes:\John Anderson [janderson]\*\Inbox
```

- For an Exchange Mailboxes path: Any segment of the path can contain wildcard characters as long as the wildcard characters are the last characters in the segment. These segments include mailbox names, folders, or messages within the mailbox hierarchy.

  Correct
  ```
  Microsoft Exchange Mailboxes:\John Anderson [janderson]\Top of
  Information Store\*
  Microsoft Exchange Mailboxes:\John Anderson [janderson]\Top of
  Information Store\[a-h]
  ```
  Incorrect
  ```
  Microsoft Exchange Mailboxes:\[a-h]\Top of Information Store
  Microsoft Exchange Mailboxes:\John Anderson [janderson]\Top*\
  ```

- For Exchange public folders: Any segment of the path can contain wildcard characters as long as the wildcard characters are the last characters in the segment. These segments include workspace names or workspace folders.

  Correct
  ```
  Microsoft Exchange Public Folders:\Folder1\Subfolder?
  ```
  Incorrect
  ```
  Microsoft Exchange Public Folders:\Folder?\Subfolder1
  Microsoft Exchange Public Folders:\*\Subfolder1
  ```

See

About excluding Exchange items from backups

If you do not want to back up certain storage groups, databases, mailboxes, or public folders, you can create an exclude list. When NetBackup runs a NetBackup for Exchange backup policy, NetBackup ignores the items that appear in the exclude list.

For more information on how to create an exclude list by using the NetBackup Administration Console, see one of the following:

- See

- The *NetBackup Administrator's Guide, Volume I*.

NetBackup excludes certain files and directories by default. These default exclusions always appear in the Administration Console's exclude list. The default exclusions are as follows:

- `C:\Program Files\Veritas\NetBackup\bin\bprd.d\*.lock`

- `C:\Program Files\Veritas\NetBackup\bin\bpsched.d\*.lock`

- `C:\Program Files\Veritas\NetBackupDB\data\*`

- `C:\Program Files\Veritas\Volmgr\misc\*`

For Exchange 2010, you can exclude specific databases from a backup, both for the databases that exist in a DAG or on a standalone Exchange server. You can specify the exclude list entry under **All Policies** or under a specific policy or schedule.

For Exchange 2007 and earlier you must specify the storage group name in the exclude list. Entering a database is not valid because Exchange requires that VSS backups must contain the entire storage group (for log truncation purposes). The exclude list entry can be specified under **All Policies** or under a specific policy or schedule.

Table 5-16 provides examples of Exchange 2010 entries you can add to an exclude list.

Table 5-16 Example Exchange 2010 entries in an exclude list

This entry ...	excludes ...
`Microsoft Information Store:\Database2`	The database named *Database2*. You can use the same `Microsoft information Store:\` directive for both DAG and standalone databases. Note that `Microsoft Exchange Database Availability Groups:\Database 2` is an invalid exclude entry.

Table 5-17 provides examples of Exchange 2007 or earlier entries you can add to an exclude list.

Table 5-17 Example Exchange 2007 or earlier entries in an exclude list

This entry ...	excludes ...
`Microsoft Information Store:\Storage_Group1`	The storage group named *Storage_Group1*.

Table 5-18 provides examples of Exchange mailbox entries you can add to an exclude list.

Table 5-18 Example Exchange mailbox entries in an exclude list

This entry ...	excludes ...
`Microsoft Exchange Mailboxes:\J*`	All mailboxes with a name that starts with "J".

Table 5-18   Example Exchange mailbox entries in an exclude list *(continued)*

This entry …	excludes …

`Microsoft Exchange Mailboxes:\Joe Smith\`
 	
`Microsoft Exchange Mailboxes:\Joe Smith [JoeS]\`
	The mailbox "Joe Smith" or "Joe Smith [JoeS]" with a name that starts with "Joe Smith".

`Microsoft Exchange Mailboxes:\Joe Smith*\Top of Information Store\Deleted Items`	The Deleted Items folder for the mailbox "Joe Smith".
`Microsoft Exchange Mailboxes:\*\Top of Information Store\Inbox\SPAM*`	Any messages that begin with "SPAM" in the user's "Inbox".

Table 5-19 provides examples of public folder entries you can add to an exclude list.

Table 5-19   Example public folder entries in an exclude list

This entry …	excludes …
`Microsoft Exchange Public Folders:\Marketing`	The root public folder called "Marketing".
`Microsoft Exchange Public Folders:\Marketing\*.xls`	All `.xls` documents under the Public Folder called "Marketing".

Configuring exclude lists for Exchange clients
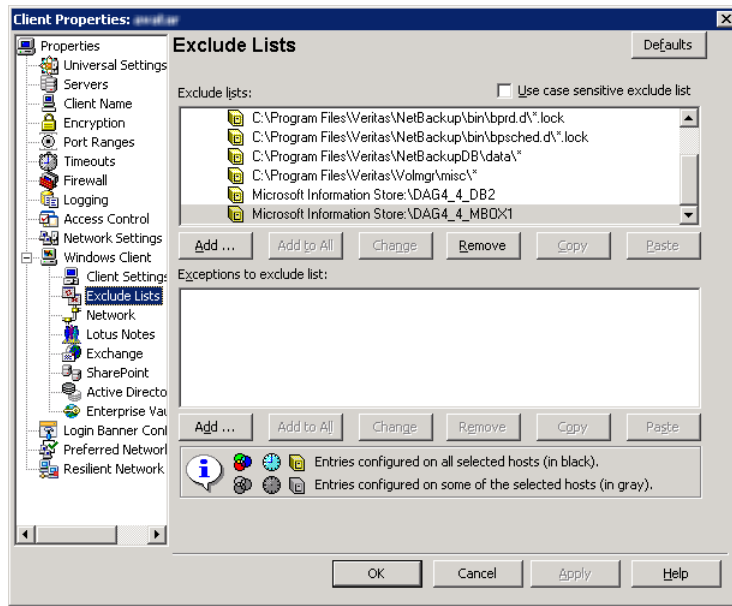
This topic describes how to exclude items from an Exchange backup.

For more information about this topic, see the following:

The following figure shows an exclude list with two databases:

Figure 5-1   Exclude list for two Exchange databases

Note: For DAG backups in clustered or replicated environments, select each node and perform the configuration procedure on each node. You must configure the same settings on each node. If you change the attributes for the virtual name of the client, NetBackup updates only the active node or current node.

To configure an Exchange client exclude list

1   Open the NetBackup Administration Console or the Remote Administration Console.

2   In the left pane, expand **NetBackup Administration > Host Properties > Clients**.

3   In the right pane, select the Exchange client(s) that you want to configure.

4   Click **Actions > Properties**.

5   Expand **Windows Client** and click **Exclude Lists**.

6   Click **Add**.

7   Specify objects to exclude in one of the following ways:

    ■ In the **Policy** field, select `<<All Policies>>` or type the name of a specific policy.

- ■ In the **Schedules** field, select `<<All Schedules>>` or type the name of a specific schedule.

- ■ In the **Files/Directories** field, type the name of a storage group, database in the following format:

    `Microsoft Information Store:\`*`name`*

    `Microsoft Exchange Mailboxes:\J*`

    For *name*, specify the name of a storage group or Exchange 2010 database, as follows:

    - ■ To exclude a specific storage group from an Exchange 2003 or Exchange 2007 backup, type the name of a specific storage group. Do not type the name of a database in this field. For log truncation purposes, Exchange requires that snapshot (VSS) backups contain the entire storage group.

    - ■ To exclude a specific database from an Exchange 2010 backup, type the name of a database to be excluded, even for DAG backups.

    When you specify a storage group or Exchange 2010 database to exclude, do not include any wildcard characters.

8 (Conditional) Repeat step 3 through step 7 for the other nodes in the environment.

Perform this step if the NetBackup environment is clustered or replicated.

If you specify the name of the virtual client, only the active node or current node is updated. For the changes to be effective throughout the cluster, repeat the configuration steps on each node.

See "About excluding Exchange items from backups" on page 96.

See "Using wildcards in an Exchange backup selections list" on page 94.

About Exchange backups and transaction logs

For performance and recoverability, the Exchange database uses transaction logs to accept, track, and maintain data. All transactions are first written to transaction logs and memory, and then committed to their respective databases. Transaction logs can be used to recover Information Store databases in the event that a failure corrupted the database. The Exchange 2010 Information Store can have multiple separate databases, each of which has its own set of transaction logs. For Exchange 2007 and earlier, the databases in each storage group share a common set of transaction logs.

Transactions are first written to the log file and then later written to the database. The effective database is a combination of the uncommitted transactions in the transaction log file and the actual database file. When the log file is filled with

transaction data, it is renamed and a new log file is created. When the log file is renamed, the other renamed log files are stored in the same subdirectory. The renamed log files are named in a sequential numbering order, in hexadecimal.

For Exchange 2007 and later the database transaction log for the Information Store is named E*XXYYYYYYYY*.log. *XX* is the database number or storage group number (in hex). *YYYYYYYY* is the log file number (in hex). The size of the transaction logs is 1 MB.

For Exchange 2003, the database transaction log for the Information Store is named E0*yXXXXX*.log. *Y* is a number from 0 to 3 representing the storage group. *XXXXX* is a five-digit hexadecimal number that is incremented each time an E0y.log file is renamed. For example, E010029E.log, E010029F.log, E010029A.log.The size of the transaction logs is 5 MB.

After every 1 MB or 5 MB of transaction log data is written, a new log is created. The log is created even though the transaction data may not be committed to the database. There may be several transaction logs that contain uncommitted data, therefore they cannot be purged.

Exchange 2010 transaction logs get committed to their database over time or when the services are brought down. Any transactions that existed in log files and not in the database file are committed to the database.

Exchange 2007 and earlier transactions in log files are committed to the respective database over time, or when the service shuts down normally. For example, consider when the Information Store service experiences a normal shutdown (service shuts down with no errors). Any transactions that existed in log files and not in the database file are committed to the database.

Do not manually purge log files. Instead, purge logs through the backup process. For backups of a replicated copy (LCR, CCR or DAG), the log truncation is scheduled. It starts with the active copy when Exchange has the resources to start truncation. It does not happen instantly after a backup as with non-replicated copies.

For information on how transaction logs are truncated, see the following topics:

See "NetBackup for Exchange backup types" on page 87.

See "Adding schedules for Exchange Instant Recovery" on page 120.

About configuring snapshot backups of Exchange Server

Use the following steps to configure snapshot backups of Exchange Server.

Table 5-20   Configuring a snapshot backup of Exchange Server

Step	Action	Description
Step 1	Review the configuration and the licensing requirements for snapshot backups.	See "Configuration and licensing requirements for Exchange snapshot backups and restores" on page 28.
Step 2	Additional configuration is required if you want to restore mailbox items from a database backup (using Granular Recovery Technology or GRT). Create a user account for the NetBackup Client Service and configure the log on account for this service.	See "About configuring the NetBackup Client Service for backups and restores that use Granular Recovery Technology (GRT) or MAPI" on page 55.
Step 3	If you want to perform off-host backups, review the installation requirements for that type of backup.	See "Requirements for Exchange off-host backups" on page 29.
Step 4	Review the general configuration requirements for snapshot operations.	See "Configuration requirements for snapshot backups of Exchange Server" on page 103. See "Limitations of Exchange snapshot operations" on page 103.
Step 5	Review the configuration requirements for Exchange Server.	See "Configuration recommendations for the Exchange Server when performing snapshot operations" on page 104.
Step 6	Choose which transaction logs to back up.	See "About backing up all or only uncommitted Exchange transaction log files with snapshot backups" on page 71.
Step 7	Configure consistency checks.	See "Consistency checks on Exchange snapshot backups" on page 105. See "About consistency checks options for an Exchange 2010 backup" on page 74. See "About configuring a pause in consistency checks for Exchange 2007 and earlier" on page 71.
Step 8	Configure an MS-Exchange-Server policy that has the applicable snapshot attributes selected.	See "Configuring a snapshot policy for Exchange Server" on page 106.
Step 9	Choose whether to back up the passive or the active copy. This applies to Exchange 2007 replication backups or Exchange 2010 backups of a Database Availability Group (DAG). For an Exchange 2010 DAG, you must also define a preferred server list.	See "Backup source for an Exchange 2010 DAG backup or an Exchange 2007 replication backup " on page 110. See "Configuring a preferred server list for an Exchange 2010 Database Availability Group (DAG)" on page 111.

	Table 5-20	Configuring a snapshot backup of Exchange Server *(continued)*
Step	**Action**	**Description**
Step 10	Configure the snapshot volume that you want to use during the backup process.	
Step 11	For Exchange 2007 and earlier, disable circular logging for all Exchange storage groups. For Exchange 2010, disable circular logging for all databases.	

Limitations of Exchange snapshot operations

The following limitations exist when you perform snapshot operations with NetBackup for Exchange:

■ Data movers are not supported with off-host backups. Only alternate clients are supported for off-host backups.

The following additional limitations exist for snapshot operations performed with Exchange 2007 and earlier:

■ Snapshot backups are supported only for the full Information Store, or storage groups. The entire Information Store or storage group must be selected for backup. (However, you can select individual databases for restore.)

■ Snapshot backups are not supported for individual Exchange mailboxes or public folders.

■ (Exchange 2003, pre-Service Pack 1) Differential and cumulative backups are not supported.

■ You cannot restore snapshot backups and streaming or MAPI backups in the same restore job.

■ An incremental backup must be of the same type (streaming or snapshot) as the last full backup.

See "About snapshot backups with Exchange Server" on page 20.

Configuration requirements for snapshot backups of Exchange Server

Observe the following configuration requirements before you perform snapshot backups:

■ The hardware and software for the appropriate snapshot method is installed and configured correctly.
See the *NetBackup Snapshot Client Administrator's Guide*.

See the Symantec Support Web site for details on the snapshot methods and platforms that are supported for your agent.

- NetBackup Snapshot Client is configured correctly.
  See the *NetBackup Snapshot Client Administrator's Guide* for details.
  A Snapshot Client license key is not required for any Exchange snapshot backups that use the Microsoft default provider or SFW.

- To perform off-host backups, perform any special configuration that is required.
  See the *NetBackup Snapshot Client Administrator's Guide* for information.

- Mount databases before you perform a backup.

- If you want to create a virtual storage unit for an Exchange 2007 CCR environment when the Exchange cluster is also configured as a SAN Media server, see the following:
  http://www.symantec.com/docs/TECH69539

Configuration recommendations for the Exchange Server when performing snapshot operations

Symantec recommends the following configuration when you perform snapshot backups:

- The volume(s) that contains the Exchange databases should be dedicated to Exchange only. Other types of databases (for example, SQL Server) should not reside on the volume(s). Only Exchange objects are included in a snapshot backup.

- Transaction logs or Exchange system files should not reside on the same volume as the Exchange database files (`edb` and `stm`).

- (Exchange 2003, pre-Service Pack 1) The Information Store must be configured with only one database per storage group.

- (Exchange 2003 SP1 or later, Exchange 2007) Restore all databases in a storage group at the same time. Also restore all the databases before the transaction logs are committed and the databases are mounted. Transaction logs are committed at a storage group level, rather than at a database level.

- For off-host backups using Storage Foundations for Windows (SFW), SFW deports and imports at the disk level. The volumes that you back up must constitute whole disks.

For Exchange 2003, the database files are the `.edb` and `.stm` files. For Exchange 2007 and later, the database file is the `.edb` file.

Consistency checks on Exchange snapshot backups

NetBackup is configured to run consistency checks for Exchange snapshot backups. Consistency checks are required for Exchange 2007 and earlier or for a standalone Exchange 2010 server. Consistency checks are not required for an Exchange 2010 Database Availability Group (DAG) because of the checks that are performed during replication.

The consistency check runs with the proper options against the files that exist on the snapshot. If any of the files fail the consistency check, the backup fails and the backup image is discarded. The Exchange VSS Writer is notified of the failure. When this kind of backup failure occurs, Exchange does not truncate log files. Failure of the consistency check may be an indication of either database corruption or a problem with the snapshot.

For Exchange 2003 NetBackup uses `ESEUTIL.EXE`. For Exchange 2007 and later local snapshot backups, NetBackup uses the Microsoft consistency check API. This API allows the user to view problems or information in the application event logs.

For off-host backups, the consistency checks are run on the off-host client rather than on the primary client. For Exchange 2007 and later, Symantec recommends that you install the Exchange System Management Tools on the alternate client. NetBackup performs the backup faster with this configuration. If the Exchange System Management Tools are not installed on the alternate client, the following occurs:

■ (Exchange 2010) If you choose not to install the Exchange System Management Tools, , the backup may fail. You must install the VC9 runtime DLLs on the alternate client. These DLLs can be downloaded from Microsoft x64 VC9 download page:

http://www.microsoft.com/downloads/details.aspx?familyid=BD2A6171-E2D6-4230-B809-9A8D7548C1B6&displaylang=en

■ `bpfis` logs a message. The message indicates that the DLL cannot be loaded and that `eseutil` is used for the consistency check.

■ NetBackup performs the consistency check during the snapshot import step.

More information is available about configuring consistency checks for Exchange 2010 and the pause option for Exchange 2003 SP2.

Configuring a snapshot policy for Exchange Server

To configure a snapshot policy with Instant Recovery, you follow a different procedure.

See

If you have existing streaming backup policies and you upgraded to Exchange 2010, you must update your backup policies. Exchange 2010 backup policies require that **Perform snapshot backups** is enabled. You may have to update the backup selections list with the correct directives.

With a snapshot policy you can optionally perform an off-host backup. Also refer to the following topics for policy recommendations:

See

See

To configure a snapshot policy for Exchange Server

1   Create a new policy or open the policy you want to configure.

2   In the **Policy** dialog box, click the **Attributes** tab.

3   In the **Policy type** list, click **MS-Exchange-Server**.

4   Select the **Policy storage**.

5   Click **Perform snapshot backups**.

6   In the **Snapshot Client** group, click **Options**.

7   In the **Snapshot Client Options** dialog box, from the **Snapshot method** list, click **VSS**.

8   Adjust the configuration parameters.

    See

9   (Optional) To perform off-host backups with Exchange 2007 or earlier or with an Exchange 2010 standalone server, do the following:

    ■ Click **Perform off-host backup**.

    ■ In the **Use** box, select **Alternate Client**.

    ■ In the **Machine** box, type the name of the alternate client.

    If you use the SFW VSS provider, review the additional installation requirements and configuration that exist.

    See
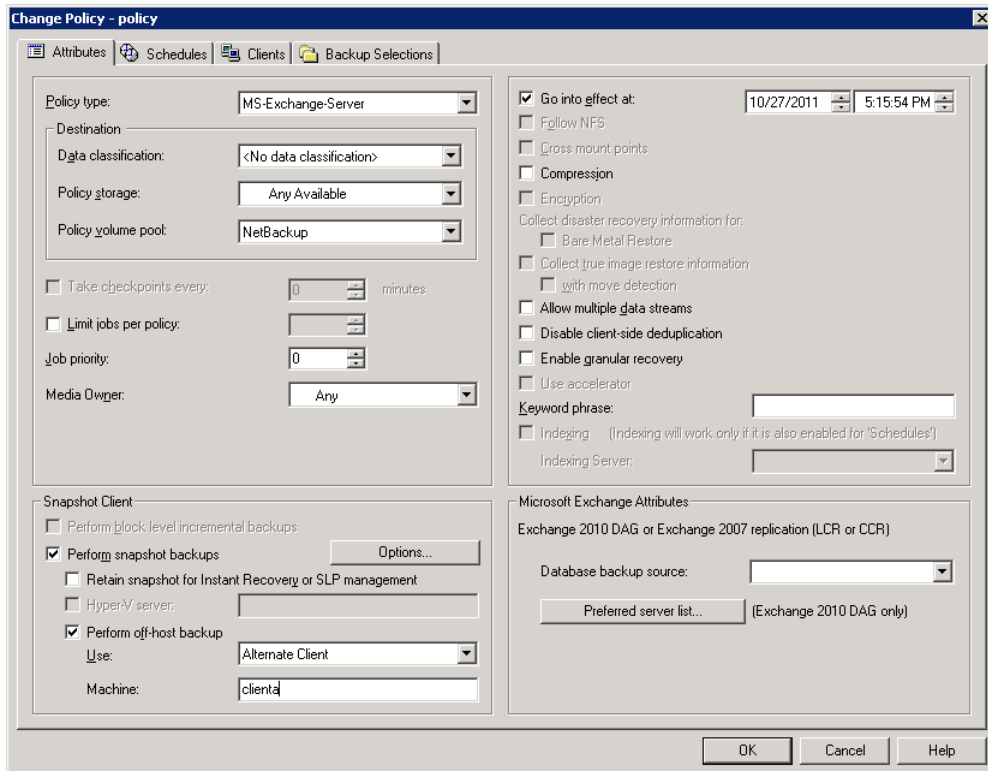
10 Optional: To divide backups into multiple jobs, click **Allow multiple data streams**.

11 To enable restores of individual items from database backups, click **Enable granular recovery**.
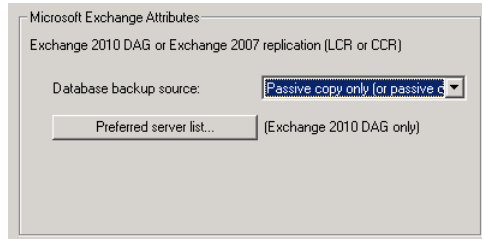
See "Configuring NetBackup for Exchange backups that use Granular Recovery Technology (GRT)" on page 62.

12 For an Exchange 2010 DAG or Exchange 2007 replication backup, in the
Microsoft Exchange Attributes group choose the **Database backup source**.

See "Backup source for an Exchange 2010 DAG backup or an Exchange 2007
replication backup " on page 110.

See "Configuring a preferred server list for an Exchange 2010 Database
Availability Group (DAG)" on page 111.

Note that the settings you choose for **Microsoft Exchange Attributes** only
apply for NetBackup 7.0 and later clients.

13 To configure schedules, click the **Schedules** tab.

See "Adding schedules to a NetBackup for Exchange policy" on page 86.

14 Use the **Clients** tab to specify clients to be backed up by this policy.

See "Adding clients to a NetBackup for Exchange policy" on page 89.

For a DAG policy, the client name is the name of the DAG and not the client
on which the backup is run. If you want to use a particular Exchange server,
add it to the preferred server list. For an Exchange 2010 DAG, you must
configure the preferred server list.

See "Configuring a preferred server list for an Exchange 2010 Database
Availability Group (DAG)" on page 111.

For off-host backups, the client name should be the name of the primary
client. The alternate client must be the client that shares the disk array. This
option may require additional configuration.

See to the *NetBackup Snapshot Client Administrator's Guide*.

15 Use the **Backup Selections** tab to enter the directives or browse for Exchange
objects.

See "Notes and limitations for creating a backup selections list for Exchange
2007 and earlier streaming database backups" on page 126.

Off-host backups with the SFW VSS provider have a requirement. You must
back up storage groups only on the same SFW disk group.

16 Click **OK** to close the dialog box.

17 For any backups that use Granular Recovery Technology (GRT), configure the list of Exchange hosts.

See "Configuring the Exchange hosts for backups that use Granular Recovery Technology (GRT) " on page 65.

See "About Exchange Instant Recovery methods" on page 21.

See "About configuration requirements for the Exchange Server when you use Instant Recovery" on page 116.

Snapshot options for Exchange Server

Table 5-21 lists the options that are available for snapshot backups.

Table 5-21   Snapshot options

Parameter	Value	Description
Provider Type	0-auto	The VSS Provider is automatically selected based on the providers available for the snapshot volumes.
	1-system	Only the default Microsoft VSS Provider is used.
	2-software	Currently, the only software VSS Provider that is supported is SFW. If this provider is not in control of one of the volumes that is required for the backup, the backup fails.
	3-hardware	The applicable hardware VSS Provider is used for the volumes. If a hardware provider is not available for one of the volumes that is required for the backup, the backup fails.
Snapshot Attribute	0-unspecified 1-differential 2-plex	The setting for this option depends on the configuration of the snapshot volume.
Maximum Snapshots (Instant Recovery only)		This option defines the number of snapshots that is retained for Instant Recovery. When this threshold is reached, a snapshot is automatically snapped back or deleted, depending on the VSS provider and its configuration before another snapshot backup is performed. Select a number that is appropriate for the number of volumes that you have available to become snapshot volumes for your backup. If you use the Microsoft VSS Provider, consider the amount of disk space available for the virtual snapshots that it creates.

See "About snapshot backups with Exchange Server" on page 20.

See "Limitations of Exchange snapshot operations" on page 103.

See "Configuration recommendations for the Exchange Server when performing snapshot operations" on page 104.

Backup source for an Exchange 2010 DAG backup or an Exchange 2007 replication backup

An Exchange 2010 DAG is an environment where each database is active on one server and has zero or more replicated passive copies on other Exchange servers. Exchange 2007 includes the mirroring (replicating) of Exchange databases and logs to a local server with replication enabled (LCR). Or databases and logs can be replicated to a passive node of a Microsoft Cluster with replication enabled (CCR).

The supported backup interface to the DAG or the replicated data is the VSS passive writer. NetBackup allows the user to select which VSS writer is backed up from the **Attributes** tab in the policy. The client backs up and catalogs as if it were a local snapshot backup.

See "Configuring a preferred server list for an Exchange 2010 Database Availability Group (DAG)" on page 111.

Note: The Instant Recovery and off-host options cannot be used with a replication or DAG backup.

The backup source for the DAG or replication backup can be defined as one of the following:

Passive copy only (or passive copy from preferred server list)	This option backs up the passive copy of a database if the database is all of the following: mounted, included in the backup selections list, and healthy. For an Exchange 2010 DAG, you must also configure a preferred server list. In that case, NetBackup backs up the passive copy on a server in the preferred server list, provided that the database meets the other criteria.

Active databases other than Public Folder databases are not backed up with this option. |
| **Active copy only** | This option backs up the active copy of a database. For Exchange 2010, the preferred server list is ignored. |

Passive copy and if not available the active copy	This option backs up the passive copy of a database that is all of the following: mounted, included in the backup selections list, and healthy. For an Exchange 2010 DAG, you can also configure a preferred server list. In that case, NetBackup backs up the passive copy on a server in the preferred server list, provided that the database meets the other criteria. If the passive copy is not available and healthy, NetBackup backs up the active copy.
	This option is the default.

See "About configuring NetBackup for Exchange" on page 53.

Configuring a preferred server list for an Exchange 2010 Database Availability Group (DAG)

You can create preferred server configurations for an Exchange 2010 Database Availability Groups (DAG). The preferred server list is a collection of one or more servers in the DAG that you select as preferred backup sources. Preferred server configurations take priority as backup sources in instances where database copies are replicated between multiple servers. The preferred server list is required for **Passive copy only**. It is ignored for **Active copy only** and is optional for **Passive copy and if not available the active copy**.

You can let NetBackup choose the best server from which to back up the replicated database copies or you can designate a preferred server list. Designating a preferred server list gives you more control over your backup jobs. For example, you can configure a list of preferred servers that are local to avoid having to back up replicated data over your WAN. You can arrange the servers in order of preference. Or you may have one node of a DAG that contains passive copies for all or most of your databases and that is also a fast media server. Add only this server to your preferred list to make the backup more efficient.

For each replicated database you select for backup, NetBackup picks a server as follows:

- The server is the one from which NetBackup most recently attempted to back up the database.

- The backup attempt on the server was successful.
  NetBackup tracks the success or failure of backup attempts to determine which Exchange node to perform a passive copy database backup from.
  See "Backup status for Exchange Database Availability Groups (DAGs) and the preferred server list" on page 112.

- The server is included in the preferred server list.

If this algorithm does not choose a server, the database is not backed up. A message appears in the progress log identifying each database that is skipped for this reason.

To configure a preferred server list

1   In the **Policy** dialog box, click the **Attributes** tab.

2   In the **Microsoft Exchange Attributes** group, from the **Database backup source** list, select **Passive copy only**.

    See "Backup source for an Exchange 2010 DAG backup or an Exchange 2007 replication backup " on page 110.

3   Click **Preferred server list**.

4   In the **Name** box, type the fully qualified domain name (FQDN) of the DAG node you want to add to the list.

5   Click **Add**.

6   Add any other DAG nodes.

7   Use the up and down buttons to indicate the order in which you want NetBackup to select the servers.

8   Click **OK**.

See "Backup status for Exchange Database Availability Groups (DAGs) and the preferred server list" on page 112.

Backup status for Exchange Database Availability Groups (DAGs) and the preferred server list

In an Exchange 2010 Database Availability Groups (DAG) environment, NetBackup tracks the success or failure of a backup attempt for each passive copy database backup. This information is stored in the Backup Status database on the NetBackup master server. This status is used in subsequent backup attempts for each database in a DAG. It helps determine from which Exchange node to perform a passive copy database backup.

NetBackup chooses a server from the preferred server list for a subsequent passive copy database backup attempt as follows:

If the last backup was successful and the last backup server exists in the preferred server list...	NetBackup uses that same server.
If the last backup was successful but the last backup server does not exist in the preferred server list...	NetBackup chooses a server from the list based on the order they appear.

If the last backup attempt failed...	NetBackup chooses a server from the list based on the order they appear. The last failed server is effectively pushed to the bottom of the list.
If no backup status exists for a database...	NetBackup chooses a server from the list based on the order they appear.
If no backup status exists for a database *and* if the preferred server list is not configured or if no servers in the preferred server list are relevant for an Exchange database...	NetBackup ranks the health of the passive copies of a database to determine the server.

To have NetBackup use a particular server for the subsequent passive copy database backup attempt, change the backup status for the database. Indicate that the last successful backup came from the desired server with the following command:

```
bpclient -client DAG_Name -update -exdb
database_name:server_name:0:0:0
```

See "Displaying and resetting the Backup Status for a Database Availability Group (DAG)" on page 218.

See "Configuring a preferred server list for an Exchange 2010 Database Availability Group (DAG)" on page 111.

See "About configuring NetBackup for Exchange" on page 53.

About configuring Instant Recovery backups of Exchange Server (Exchange 2007 and later)

Table 5-22   Configuring Instant Recovery backups of Exchange Server (Exchange 2007 and later)

Step	Action	Description
Step 1	For Exchange 2007 and earlier, disable circular logging for all Exchange storage groups. For Exchange 2010, disable circular logging for all databases.	

Table 5-22   Configuring Instant Recovery backups of Exchange Server (Exchange 2007 and later) *(continued)*

Step	Action	Description
Step 2	Review the configuration and the licensing requirements for snapshot backups.	See "Configuration and licensing requirements for Exchange snapshot backups and restores" on page 28.
Step 3	Review the installation requirements for Instant Recovery backups.	See "Requirements for Exchange Instant Recovery backups" on page 30.
Step 4	Review the general configuration requirements for snapshot operations.	See "Configuration requirements for snapshot backups of Exchange Server" on page 103. See "Limitations for Exchange Instant Recovery operations" on page 115. See "About Software Foundations for Windows (SFW) and Exchange Instant Recovery" on page 116. See "About Exchange Instant Recovery with the Microsoft VSS Provider" on page 117.
Step 5	Review the configuration requirements for Exchange Server for Instant Recovery operations.	See "About configuration requirements for the Exchange Server when you use Instant Recovery" on page 116.
Step 6	Choose which transaction logs to back up.	See "About backing up all or only uncommitted Exchange transaction log files with snapshot backups" on page 71.
Step 7	Configure a pause in consistency checks.	See "About configuring a pause in consistency checks for Exchange 2007 and earlier" on page 71.
Step 8	Review the backup policy recommendations for Instant Recovery backups.	See "Policy recommendations for Exchange Instant Recovery" on page 114.
Step 9	Configure an MS-Exchange-Server policy that has the Instant Recovery attribute selected and the Snapshot Client options that you want.	See "Configuring an Exchange snapshot policy with Instant Recovery" on page 117.
Step 10	Configure one snapshot volume for each backup image that you need to retain on disk.	

Policy recommendations for Exchange Instant Recovery

Create a policy with the following schedules when you use Instant Recovery:

- Create a snapshot policy with Instant Recovery enabled and with the option **Snapshots and copy snapshots to a storage unit** selected. (In Table 5-23 , see Schedules 1 and 2.)

- (Optional) For fast, temporary backups, create a separate policy with a **Full Backup** schedule. Enable **Retain snapshots for Instant Recovery or SLP management** and the Instant Recovery option **Snapshots only**. (In Table 5-23, see Schedule 3.)

Information is available on how transaction logs are truncated according to the backup type you select.

See "NetBackup for Exchange backup types" on page 87.

Table 5-23   Instant recovery policy examples for Exchange Server

Policy type	Auto backup frequency	Copy to storage unit	Description and other configuration
MS-Exchange-Server	Schedule 1:Weekly Full	Yes	This schedule provides for disaster recovery .
	Schedule 2: Daily Incremental or Differential	Yes	This schedule provides for disaster recovery . **Note:** Do not include cumulative and differential schedules in the same policy. **Note:** If you choose differential backups, you must choose **Snapshots and copy snapshots to a storage unit**.
	Schedule 3: Every 4 hours	No	This schedule provides fast, temporary backups because the snapshot is not copied to the storage unit. In the **Snapshot Client** group, click **Options** and set **Maximum Snapshots** to a small number.

See "About Exchange Instant Recovery methods" on page 21.

See "Limitations for Exchange Instant Recovery operations" on page 115.

See "About configuring Instant Recovery backups of Exchange Server (Exchange 2007 and later)" on page 113.

Limitations for Exchange Instant Recovery operations

The following limitations exist for Instant Recovery operations:

- Instant recovery is only supported for Exchange 2007 and later.

- NetBackup can only restore an Instant Recovery backup that was performed with NetBackup 6.5.2 or later.

■ Granular Recovery Technology (GRT) is only supported with Instant Recovery if you also configure a backup to a storage unit.

See "About Exchange Instant Recovery methods" on page 21.

See "Configuring a snapshot policy for Exchange Server" on page 106.

See "About configuration requirements for the Exchange Server when you use Instant Recovery" on page 116.

About Software Foundations for Windows (SFW) and Exchange Instant Recovery

When you use the SFW VSS provider to create your Exchange IR snapshots, use Veritas Enterprise Administrator (VEA) rather than VShadow or Vssadmin to view and manage your snapshots. SFW resnaps a volume after a rollback restore, but the Microsoft utilities are not aware of the new snapshot. They falsely report that the snapshot does not exist.

See "Limitations for Exchange Instant Recovery operations" on page 115.

See "About snapshot backups with Exchange Server" on page 20.

See "About configuration requirements for the Exchange Server when you use Instant Recovery" on page 116.

About configuration requirements for the Exchange Server when you use Instant Recovery

The following configuration is required for the Exchange Server when you use Instant Recovery:

■ The volume(s) that contains the Exchange databases should be dedicated to Exchange only. Other types of databases (for example, SQL Server) should not reside on the volume(s). Only Exchange objects are included in a snapshot backup.

■ To allow volume rollback to occur during a restore, a volume should contain the database files for only one database.

■ Transaction logs or Exchange system files should not reside on the same volume as the Exchange database file (.edb).

■ (Exchange 2007) Restore all databases in a storage group at the same time. Also restore the all the databases before the transaction logs are committed and the databases are mounted. Transaction logs are committed at a storage group level, rather than at a database level.

About Exchange Instant Recovery with the Microsoft VSS Provider

A special requirement exists when you want to use Instant Recovery with the Microsoft VSS Provider. Symantec recommends when you create a policy for an Exchange 2010 standalone server that you include only the databases that are on a common volume. For Exchange 2007, include only the storage groups whose databases are on a common volume.

If an IR policy backs up databases on multiple volumes and you restore a subset of those volumes, NetBackup deletes the other snapshots. Otherwise the backup image contains an incomplete snapshot set. A rollback with the Microsoft VSS Provider consumes the snapshot because it does not provide for re-snapping the volume.

If you use Instant Recovery with the Microsoft VSS Provider and you select any items that span multiple volumes, the following occurs:

- NetBackup creates a backup set with one snapshot for each volume.

- During restores, if any snapshots are rolled back, all of the snapshots in that set are deleted. (With the SFW VSS provider or the hardware system provider, the rolled back snapshots are re-snapped so that the snapshot set remains complete.)
  This situation is a limitation of the Microsoft VSS Provider. It typically occurs when you do a roll-forward restore of a database and log folders that are on separate volumes (Exchange 2010). Or when you do a roll-forward restore of a storage group whose database and log folders are on separate volumes (Exchange 2007). The database volume normally is rolled back but the log volume is copied back. This action preserves the logs that were created since the backup. NetBackup then deletes the log snapshot and removes the IR copy of the backup image from the catalog. If a storage unit copy of the backup exists, it remains.

Configuring an Exchange snapshot policy with Instant Recovery

This topic describes how to configure a snapshot policy with Instant Recovery. This topic only covers what is necessary to configure Instant Recovery snapshot backups of Exchange Server. Information on how to configure other policy information is described in other topics. (This information includes other policy attributes and how to create schedules, add clients, and add backup selections.)

If you have existing streaming backup policies and you upgraded to an Exchange 2010 standalone server, you must update your backup policies. Exchange 2010 backup policies require that **Perform snapshot backups** is enabled. You may have to update the backup selections list with the correct directives.

Optionally you can perform an off-host Instant Recovery backup.

To configure a snapshot policy with Instant Recovery for Exchange Server

1   Create a new policy.

2   Click the **Attributes** tab.

3   In the **Policy type** drop-down list, click **MS-Exchange-Server**

4   Select the **Policy storage**.

    See "Adding schedules for Exchange Instant Recovery" on page 120.

5   Click **Perform snapshot backups**.

6   Click **Retain snapshots for Instant Recovery or SLP management**.

NetBackup retains the snapshot on disk, so that Instant Recovery can be performed from the snapshot. A normal backup to storage is also performed when the backup schedule specifies **Snapshot and copy to storage unit**.

See "Adding schedules for Exchange Instant Recovery" on page 120.

See "Schedules settings in Exchange Instant Recovery policies" on page 121.
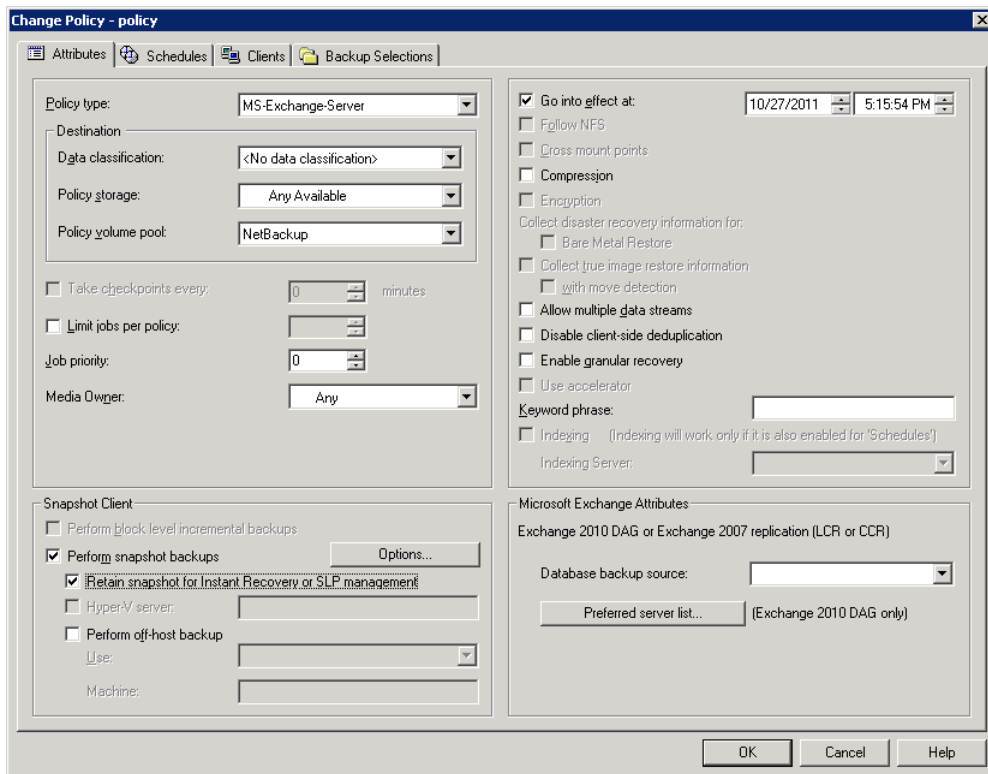
7   In the **Snapshot Client** group, click **Options**.

8   In the **Snapshot Client Options** dialog box, from the **Snapshot method** list click **VSS**.

9   Adjust the configuration parameters.

See "Snapshot options for Exchange Server" on page 109.

10 Optional: If you selected that you want to divide backups into multiple jobs and you selected **Snapshot and copy to storage unit**, click **Allow multiple data streams**.

See "Performing Exchange backups with multiple data streams" on page 93.

11 (Optional) To perform off-host Instant Recovery backups do the following:

- Click **Perform off-host backup**.

- In the **Use** box, select **Alternate Client**.

- In the **Machine** box, type the name of the alternate client.

If you use the SFW VSS provider, review the additional installation requirements and configuration that exist.

See "Requirements for Exchange off-host backups" on page 29.

12 Add other policy information as follows:

- Add clients to the policy.
  See "Adding clients to a NetBackup for Exchange policy" on page 89.

- Add backup selections to the policy.
  See "Notes and limitations for creating a backup selections list for Exchange 2007 and earlier streaming database backups" on page 126.
  See "Adding backup selections to an Exchange policy with Instant Recovery " on page 123.

13 After you add all the clients, schedules, and backup selections you need, click **OK**.

See "Policy recommendations for Exchange Instant Recovery" on page 114.

Adding schedules for Exchange Instant Recovery

Follow these instructions to configure schedules for an Instant Recovery policy.

To add schedules for Instant Recovery

1 In the **Policy** dialog box, click the **Schedules** tab.

2 Click **New**.

3 In the **Schedules** dialog box, create at least one **Full** type of schedule.

4 From the **Instant Recovery** group, select one of the following options.

Snapshots and copy snapshots to a storage unit	This option is required for the following: ■ Differential backups ■ Disaster recovery scenarios where both the primary and the snapshot volume have been damaged ■ Instant Recovery backups with **Enable granular recovery** enabled
Snapshots only	For fast, temporary backups.

5 Click **OK**.

6 To close the dialog box, click **OK**.

See "About configuring snapshot backups of Exchange Server" on page 101.

See "Configuring a snapshot policy for Exchange Server" on page 106.

See "Configuring an Exchange snapshot policy with Instant Recovery" on page 117.

Schedules settings in Exchange Instant Recovery policies

Note the following settings in the **Schedules** tab when you add a schedule for a policy with Instant Recovery.

Table 5-24   Settings for schedules in Instant Recovery policies

Setting	Options	Description
Type of Backup	Full or user	Snaps the volumes that contain the Exchange database, system, and log files.
	Differential or cumulative incremental	Snaps the volumes that contain the Exchange system and log files. Differential backups require that the transaction logs are backed up to a storage unit and kept on the Instant Recovery snapshot volume. (Select the **Snapshots and copy snapshots to a storage unit** option.) This configuration is required because all of the differential backups after the last full backup are required to fully restore a database. Since a differential backup truncates the transaction logs, there is no way to guarantee that all of the log files exist. Also, snapshot rotation might have snapped back or deleted one or more snapshot images. They must be backed up to a storage unit.

Table 5-24   Settings for schedules in Instant Recovery policies *(continued)*

Setting	Options	Description
Retention	One week - infinity	The retention level indicates the maximum time that the Instant Recovery snapshot is retained. For full backups, select a retention level that ensures a full backup is always available for restore. The snapshot can be deleted before that time if the snapshot volume is required for another backup attempt. See "About Exchange Instant Recovery volume rotation" on page 122.
Instant Recovery	Snapshots and copy snapshots to a storage unit	**Note:** The Instant Recovery options are available if you select **Retain snapshots for Instant Recovery or SLP management** (on the **Attributes** tab of the policy). NetBackup creates a disk snapshot and backs up the client's data to the storage unit that is specified for the policy. This option is required if you want to perform Instant Recovery backups with Granular Recovery Technology (GRT). Transaction logs are deleted when the backup (full or differential) to the storage unit has completed.
	Snapshots only	The image is not backed up to tape or to other storage. NetBackup creates a persistent snapshot only. Note that this persistent snapshot is not considered a replacement for traditional backup. Transaction logs are not deleted for this schedule option. To delete transaction logs, you must perform a backup to a storage unit. Alternatively, you can configure NetBackup to delete logs for any full Instant Recovery backups that are snapshot only. See "About truncating Exchange transaction logs with Instant Recovery backups" on page 72.

See "Snapshot options for Exchange Server" on page 109.

About Exchange Instant Recovery volume rotation

At the start of a backup, the Snapshot Client is queried to determine how many Instant Recovery snapshots currently exist for each volume. This information is required for the Exchange storage groups that are selected for backup. If the number of snapshots is currently at the configured maximum level of snapshots, a snapshot is resynced (or snapped backup or deleted). Then a snapshot is available for the upcoming backup attempt.

The algorithm to determine which snapshot volume is resynced considers whether the snapshot was taken as part of a full backup or an incremental backup. The

algorithm tries to maintain as many full backups as possible, even if newer incremental backups have to be resynced.

Adding backup selections to an Exchange policy with Instant Recovery

You can include each Exchange storage group in one backup policy. Or you can choose to include a storage group in more than one policy. In the latter case, ensure that enough snapshot volumes exist to satisfy the **Maximum Snapshots** value for each policy that contains the storage group.

When you configure an Exchange snapshot backup policy, the only valid directives are: `Microsoft Exchange Database Availability Groups:\` or `Microsoft Information Store:\` (a database or storage group can be appended) .

Note: To back up individual databases, you must select all the databases in the storage group.

Configuring a streaming NetBackup for Exchange policy (Exchange 2007 and earlier)

This topic describes how to cofigure a streaming backup policy for an Exchange database.

To configure a streaming NetBackup for Exchange policy (Exchange 2007 and earlier)

1   Review the notes and limitations for this type of backup.

2   Log on to the master server as administrator (Windows) or root (UNIX).

3   Start the NetBackup Administration Console.

4   If your site has more than one master server, choose the one on which you want to add the policy.

5   (Windows) In the left pane, right-click **Policies** and choose **New Policy**.

6   (Java interface) In the left pane, click **Policies**. In the **All Policies** pane, right-click the master server, and click **New Policy**.

7   In the **Add a New Policy** dialog box, in the **Policy name** box, type a unique name for the new policy.

8   Click **OK**.

9   In the **Add New Policy** dialog box, in the **Policy type** list, select **MS-Exchange-Server**.

    The database agent policy type does not appear in the drop-down list unless your master server has a license key for the database agent.

10 (Optional) To enable restores of individual items from database backups, click **Enable granular recovery**.

See "Configuring NetBackup for Exchange backups that use Granular Recovery Technology (GRT)" on page 62.
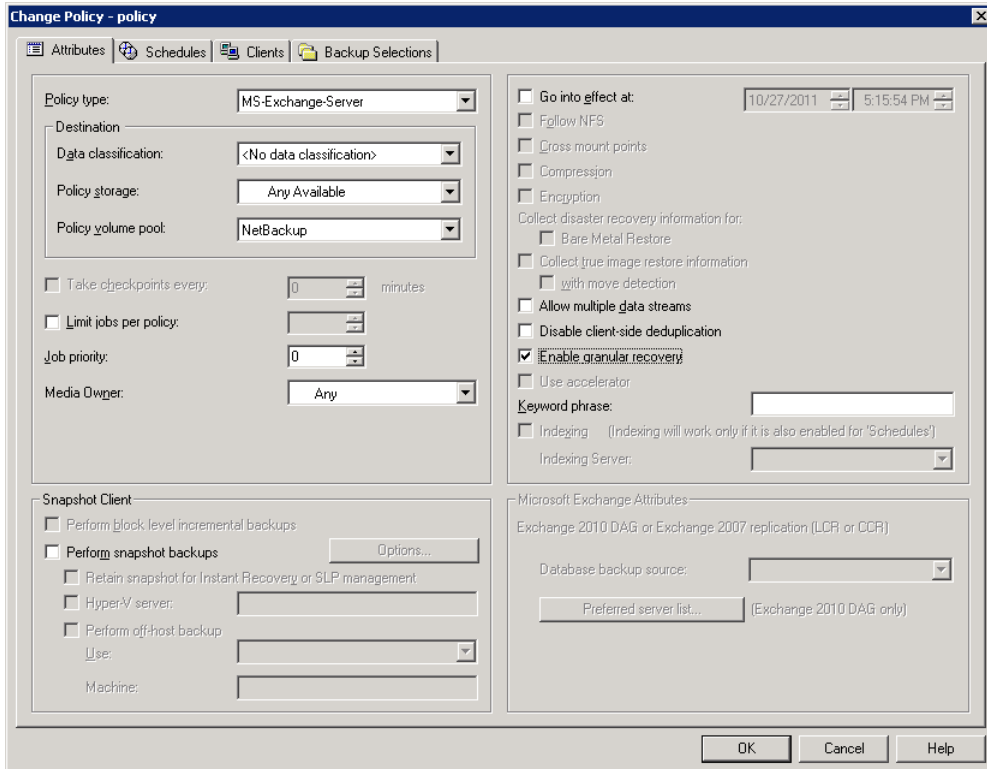
11 Complete the entries on the **Attributes** tab.

See "About policy attributes for NetBackup for Exchange" on page 85.

12 Add other policy information as follows:

■ Add schedules.
    See "Adding schedules to a NetBackup for Exchange policy" on page 86.

■ Add clients.
    See "Adding clients to a NetBackup for Exchange policy" on page 89.

■ Add database objects to the backup selections list.
    See "Adding backup selections to an Exchange policy" on page 90.

See "Notes and limitations for creating a backup selections list for Exchange 2007 and earlier streaming database backups" on page 126.

13 For any backups that use Granular Recovery Technology (GRT), configure the list of Exchange hosts.

See "Configuring the Exchange hosts for backups that use Granular Recovery Technology (GRT) " on page 65.

14 When you have added all the schedules, clients, and backup selections you need, click **OK**.

See "About configuring NetBackup for Exchange" on page 53.

Notes and limitations for creating a backup selections list for Exchange 2007 and earlier streaming database backups

Streaming backups include the `Microsoft Information Store:\` directive.

Review the following information before you create a backup selections list for the Exchange 2007 or earlier streaming database backups:

■ NetBackup for Exchange does not support incremental backups of individual databases within a storage group.

■ When individual databases in a storage group are backed up, the transaction logs for the entire storage group are also included in the backup.

   Transaction logs are not truncated (deleted) until a full backup is run on every database in the storage group. To ensure that transaction logs are truncated (deleted) regularly, include all databases for a storage group in a full backup policy. Or specify the storage group (not individual databases) in the backup policy.

See "About configuring NetBackup for Exchange" on page 53.

Configuring a policy for backups of individual Exchange mailboxes or public folders (Exchange 2007 and earlier)

A MAPI mailbox or public folder policy includes individual mailbox or public folder objects. This type of policy can only be configured for Exchange 2007 and earlier. Before you configure NetBackup for Exchange policy for these objects, review the configuration that is necessary for this type of backup.

See "About configuring the NetBackup Client Service for backups and restores that use Granular Recovery Technology (GRT) or MAPI" on page 55.

To configure a NetBackup for Exchange policy for MAPI mailbox or public folder backups

1   Log on to the master server as administrator.

2   Start the NetBackup Administration Console.

3   If your site has more than one master server, choose the one on which you want to add the policy.

4   (Windows) In the left pane, right-click **Policies** and choose **New Policy**.

5   (Java interface) In the left pane, click **Policies**. In the **All Policies** pane, right-click the master server, and click **New Policy**.

6   In the **Add a New Policy** dialog box, in the **Policy name** box, type a unique name for the new policy.

7   Click **OK**.

8 In the **Add New Policy** dialog box, in the **Policy type** list, select **MS-Exchange-Server**.

The database agent policy type does not appear in the drop-down list unless your master server has a license key for the database agent.
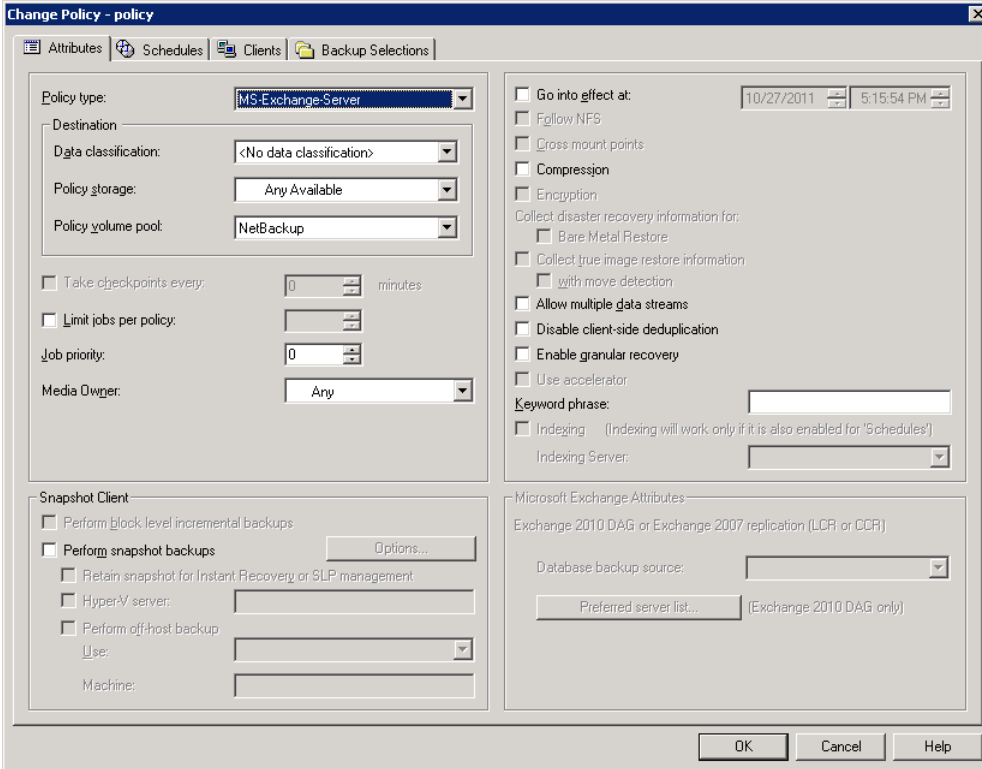
9 Complete the entries on the **Attributes** tab.

See "About policy attributes for NetBackup for Exchange" on page 85.

10 Add other policy information as follows:

- Add schedules.
  See "Adding schedules to a NetBackup for Exchange policy" on page 86.

- Add clients.
  See "Adding clients to a NetBackup for Exchange policy" on page 89.

- Add database objects to the backup selections list.
  See "Adding backup selections to an Exchange policy" on page 90.

See "Notes and limitations when you create a backup selections list for MAPI mailbox and public folder backups" on page 129.
See "Policy recommendations for Exchange Server 2007 and earlier MAPI backups" on page 83.

11 When you have added all the schedules, clients, and backup selections you need, click **OK**.

Notes and limitations when you create a backup selections list for MAPI mailbox and public folder backups

MAPI mailbox backups are performed with the `Microsoft Exchange Mailboxes:\` directive. MAPI public folder backups are performed with the `Microsoft Exchange Public Folders:\` directive.

Review the following information before you create a backup selections list for MAPI mailbox or public folder backups:

■ To perform backups of mailboxes, additional steps are required beyond policy configuration.
   See "About configuring the NetBackup Client Service for backups and restores that use Granular Recovery Technology (GRT) or MAPI" on page 55.

■ When you use mailbox or public folder directives, only backups of mailboxes or folders are allowed. You cannot specify the backup of an individual message or individual public document.

■ MAPI mailbox and public folder backups allow for mailbox or public folder recovery, but are not adequate for disaster recovery. Exchange database backups are required for disaster recovery.

■ The root path of an Exchange Mailbox object (Microsoft Exchange Mailboxes:\) is case sensitive.

See "About configuring NetBackup for Exchange" on page 53.

Performing backups and restores of Exchange Server, mailboxes, and public folders

This chapter includes the following topics:

- About backing up Exchange Server data
- About restoring Exchange database data
- About restoring individual Exchange mailbox and public folder items
- About restoring Backup Exec Exchange images with NetBackup
- About selecting a source client for an Exchange Server backup or restore operation
- About selecting a destination client for an Exchange Server restore operation

About backing up Exchange Server data

With NetBackup for Exchange you can perform snapshot and streaming database backups. You can also perform MAPI backups of individual mailboxes and public folders.

Table 6-1 Snapshot and streaming backups available for Exchange Server

Backup type	Exchange 2010	Exchange 2007 and earlier	Procedure
Snapshot	X	X	See "Performing user-directed snapshot backups of Exchange Server" on page 132.
Streaming		X	See "Performing user-directed streaming backups of Exchange Server (Exchange 2007 and earlier)" on page 135.
Individual mailboxes and public folders (MAPI)		X	See "Performing user-directed MAPI backups of individual mailboxes and public folders (Exchange 2007 and earlier)" on page 137.

Options for Exchange backups

Table 6-2 Backup options

Option	Description
NetBackup server	To change the NetBackup server that you want to perform the backup operation, select another server from the drop-down list.
Items marked to be backed up	Contains a list of objects to be backed up.
Keyword phrase to associate with the backup or archive	Specifies a keyword phrase, up to 128 characters in length, that NetBackup associates with the image created by this backup operation. You then can restore the image by specifying the keyword phrase in the Search Backups dialog box.
	All printable characters are permitted including space (" ") and period ("."). The default keyword phrase is the null (empty) string
Start Backup	Initiates the backup operation.

Performing user-directed snapshot backups of Exchange Server

To perform a user-directed snapshot backup, a policy must exist on the server that is configured for snapshot backups. This policy must also have a User schedule. Exchange 2010 users can back up a DAG, the Information Store, or a database. Exchange 2007 and earlier users can back up the Information Store or a storage group. Transaction logs are also backed up. However, transaction logs are not truncated for user-directed backups.


Note: For Exchange 2003 pre-SP1, a user-directed backup also truncates the transaction logs.

When **Enable granular recovery** is enabled in the backup policy, you can later restore individual mailbox and public folder items from the backup.

To perform a user-directed snapshot backup of Exchange Server objects

1   Mount any databases that you want to back up.

2   Open the Backup, Archive, and Restore interface.

    For a Database Availability Group (DAG), you must initiate the user backup operation from the node where the DAG virtual name is active (online).

3   Click **Actions > Specify Policy and Schedule**.

4   In the **Backup Policy and Schedule** box, type the name of the Snapshot Client policy.

5   Click **File > Select Files and Folders to Back Up**.

6   Select **File > Specify NetBackup Machines and Policy Type**.

7   In the **Specify NetBackup Machines and Policy Type** dialog box, provide the following information:

    ■ The server you want to perform the backup.

    ■ If you are in a cluster environment, specify the name of the virtual Exchange Server or the DAG virtual name.
    See "About selecting a source client for an Exchange Server backup or restore operation" on page 190.

8   In the **All Folders** pane, select the objects you want to back up.

    See Table 6-3 on page 134.

    Note the following:

    ■ For an Exchange 2010 Database Availability Group (DAG), you cannot select a specific server in the Backup, Archive, and Restore interface from which to perform the backup. If you want to use a specific server, specify it in the **Preferred server list**.
    See "Backup source for an Exchange 2010 DAG backup or an Exchange 2007 replication backup " on page 110.
    All databases in the DAG, regardless of what server they reside on, are displayed.

    ■ For Exchange 2007 or earlier backups of individual storage group databases, you must select all the databases in the storage group. If you do not select all the databases, the backup job fails.
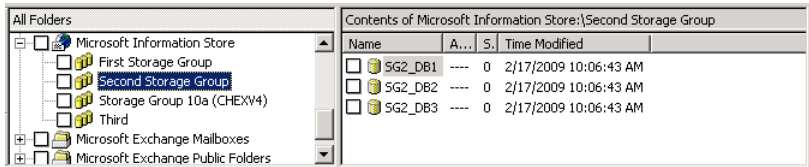
The following figure shows a backup of an Exchange 2010 DAG.
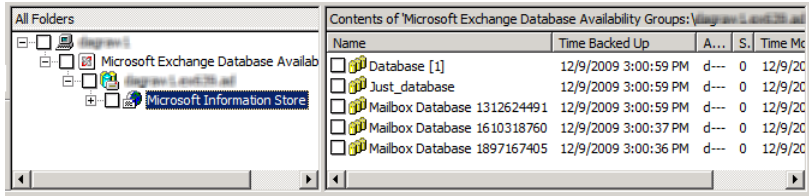
The following figure shows a backup of an Exchange 2010 standalone server.
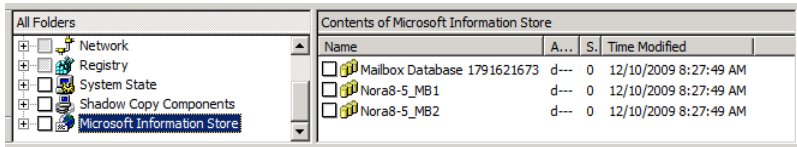
The following figure shows a backup of an Exchange 2007 storage group.

9   Click **Actions > Backup**.

10   In the **Backup Files** dialog box, click **Start Backup**.

11   To view the progress of the backup, click **Yes**.

   If you do not want to view the progress of the backup, click **No**.

Table 6-3   Selecting Exchange database objects for user-directed backups

Exchange version	Node	Objects to back up
Exchange 2010 DAG	**Microsoft Exchange Database Availability Groups**	DAG All databases in the DAG
Exchange 2010 standalone server	**Microsoft Information Store**	Microsoft Information Store All databases

Table 6-3   Selecting Exchange database objects for user-directed backups
(continued)

Exchange version	Node	Objects to back up
Exchange 2007 and 2003	**Microsoft Information Store**	Microsoft Information Store Storage groups All databases

See "About Exchange Instant Recovery methods" on page 21.

See "Configuring an Exchange snapshot policy with Instant Recovery" on page 117.

See "Configuration recommendations for the Exchange Server when performing snapshot operations" on page 104.

Performing user-directed streaming backups of Exchange Server (Exchange 2007 and earlier)

To perform a user-directed backup, the backup policy must have a User schedule. Users can back up the Information Store, storage groups, and individual databases. When **Enable granular recovery** is enabled in the backup policy, you can later restore individual mailbox items from the backup.

To perform a user-directed backup

1   Log onto the server as Administrator.

2   Ensure all databases that you want to back up are mounted and online.

3   Open the Backup, Archive, and Restore interface.

4   Click **File > Select Files and Folders to Back Up**.

5   Select **File > Specify NetBackup Machines and Policy Type**.

6   In the **Specify NetBackup Machines and Policy Type** dialog box, provide the following information:

■   The server you want to perform the backup.

■   If you are in a cluster environment, specify the name of the virtual Exchange Server or the DAG virtual name.
See "About selecting a source client for an Exchange Server backup or restore operation" on page 190.

7   In the **All Folders** pane, click the objects you want to back up, as follows:

■   Storage groups. Expand the Microsoft Information Store node and select the storage group to back up.

■ Individual databases. To back up an individual database within a specific storage group, expand the Microsoft Information Store. Then expand the storage group and select the database to back up.
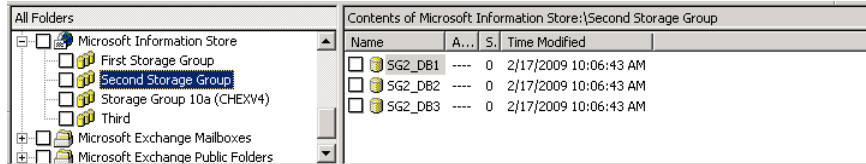
8 Click **Actions > Backup**.

9 Select the backup options you want.

See "Options for Exchange backups" on page 132.

10 Click **Start Backup**.

11 To view the progress of the backup, click **Yes**.

See "About backing up Exchange Server data" on page 131.

See "Performing user-directed full streaming backups (Exchange 2007 and earlier)" on page 136.

See "Configuring a policy for backups of individual Exchange mailboxes or public folders (Exchange 2007 and earlier)" on page 126.

See "Configuring a streaming NetBackup for Exchange policy (Exchange 2007 and earlier)" on page 123.

See "About restoring streaming backups of Exchange Server (Exchange 2007 and earlier)" on page 164.

Performing user-directed full streaming backups (Exchange 2007 and earlier)

In NetBackup, a user-directed backup of Exchange acts as a copy backup. Copy backups are the same as full backups, except copy backups do not truncate the Exchange log files. You can change the behavior of a user backup so that it normally acts as a full backup instead of a copy backup. As with regular full backups, the logs are truncated.

Note: This configuration is only available for streaming backups.

To perform a user-directed copy backup

1   Log onto the server as Administrator.

2   From the Backup, Archive, and Restore interface, perform a user-directed streaming backup.

    See "Performing user-directed streaming backups of Exchange Server (Exchange 2007 and earlier)" on page 135.

To configure user-directed backups to act as full backups

1   On the Exchange client, open Regedit.

2   Open the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Agents\Exchange
```

3   Create a new DWORD value named **Convert_USER_to_FULL**.

4   Right-click on the new value and click **Modify**.

5   In the **Value data** box, type **1**.

6   Click **OK**.

7   Repeat these steps for any other Exchange clients.

See "Configuring a policy for backups of individual Exchange mailboxes or public folders (Exchange 2007 and earlier)" on page 126.

See "Notes and limitations for creating a backup selections list for Exchange 2007 and earlier streaming database backups" on page 126.

See "Configuring a streaming NetBackup for Exchange policy (Exchange 2007 and earlier)" on page 123.

See "Performing user-directed streaming backups of Exchange Server (Exchange 2007 and earlier)" on page 135.

See "About restoring streaming backups of Exchange Server (Exchange 2007 and earlier)" on page 164.

See "About backing up Exchange Server data" on page 131.

Performing user-directed MAPI backups of individual mailboxes and public folders (Exchange 2007 and earlier)

Before you perform backups of individual Exchange mailboxes or public folders, special configuration is required.

See "About configuring the NetBackup Client Service for backups and restores that use Granular Recovery Technology (GRT) or MAPI" on page 55.

Note: The user account you use to log on must have the same Exchange privileges as the NetBackup Client service account.

To back up individual mailboxes, mailbox folders, or public folders, the backup policy must include the `Microsoft Exchange Mailboxes:\` or the `Microsoft Exchange Public Folders:\` directive. These directives are only available for Exchange 2007 and earlier.

Alternatively, you can perform a user-directed backup from a database backup policy that has **Enable granular recovery** enabled. You cannot back up individual mailboxes, mailbox folders, or public folders with a database backup policy. However, you can restore these items from the database backup.

See "Performing user-directed streaming backups of Exchange Server (Exchange 2007 and earlier)" on page 135.

See "Performing user-directed snapshot backups of Exchange Server" on page 132.

To perform a user-directed MAPI backup of individual mailboxes and public folders

1   Log onto the server as Administrator.

2   Open the Backup, Archive, and Restore interface on the Exchange Server.

3   Click **File > Select Files and Folders to Back Up**.

4   Select **File > Specify NetBackup Machines and Policy Type**.

5   In the **Specify NetBackup Machines and Policy Type** dialog box, provide the following information:

   ■   The server you want to perform the backup.

   ■   If you are in a cluster environment, specify the name of the virtual Exchange Server or the DAG virtual name.
       See "About selecting a source client for an Exchange Server backup or restore operation" on page 190.

6   In the **All Folders** pane, expand the node that contains the objects you want
    to back up and select those objects.

    See Table 6-4 on page 139.
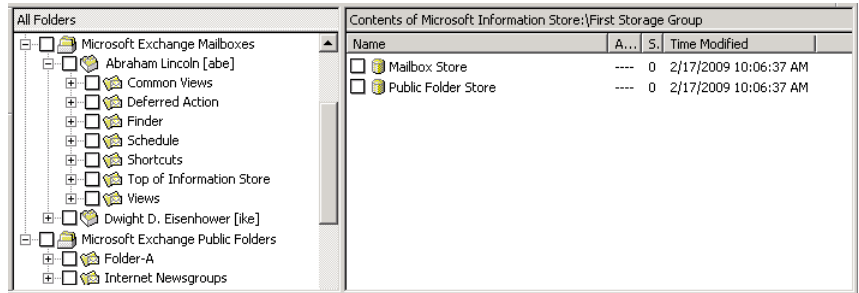
7   Click **Actions > Backup**.

8   Select the backup options you want.

    See "Options for Exchange backups" on page 132.

9   Click **Start Backup**.

10 To view the progress of the backup, click **Yes**.

    If you do not want to view the progress of the backup, click **No**.

Table 6-4   Selecting individual Exchange mailboxes and public folders for
            user-directed backups

Node	Select
Microsoft Exchange Mailboxes	Mailbox(es)
	Mailbox folder(s)
Microsoft Exchange Public Folders	Public folder(s)

See "About restoring streaming backups of Exchange Server (Exchange 2007 and
earlier)" on page 164.

See "Configuring a streaming NetBackup for Exchange policy (Exchange 2007
and earlier)" on page 123.

About restoring Exchange database data

Review the following information before you perform restores of Exchange Server:

- Restore all databases in a storage group at the same time and before the transaction logs are committed and the databases are mounted.

- When an administrator restores individual databases or transaction logs, the administrator should have a thorough working knowledge of Exchange Server databases, transaction logs, and utilities. If the correct files are not restored, the database(s) may fail to mount.

- Do not restore `Microsoft Exchange Mailboxes:\` or `Microsoft Exchange Public Folders:\` objects and `Microsoft Information Store:\` objects at the same time. Do not restore mailbox or public folder items from a GRT-enabled backup and a streaming backup at the same time. You must dismount databases before you restore them. But because they are dismounted, the attempt to restore mailbox objects fails. Or the restore of the Exchange mailbox items can finish before the restore of the Exchange databases starts. In this case the restore of the Exchange databases overwrites the restored mailbox objects.

- To restore full and incremental backups, you can restore backups in one of the following ways:

  - restore all the backups in a single operation
    The backup images must be of the same type. For example, you must restore snapshot and streaming images in separate restore jobs. You can, however, restore a full VMware backup and a differential snapshot in a single restore job.
    When you restore all the backups in a single operation, NetBackup performs a commit after the last incremental is restored.

  - restore the full backups and incremental backups individually
    When you restore the backups individually, deselect **Commit after last backup set is restored** for the full backup and all but the *last* incremental backup set. Select the following options when you restore the *last* incremental backup set: **Commit after last backup set is restored** and **Mount database after restore**.

- (Exchange 2007 and earlier streaming restores) Make sure the temporary location for log files is empty before you start a restore job. If a restore job fails, check the temporary location (including subdirectories) to make sure log files from a previous restore job are deleted.
  NetBackup copies logs to the Exchange working directory. It creates a subdirectory for each storage group being restored. After the database is restored, Exchange applies the log files from the temporary location to the database, and then it applies the current log files. After the recovery is complete, Exchange deletes the log files from the temporary location (including any subdirectories).

- A restore of Exchange Server files always overwrites existing files. (For example, if `Pub.edb` already exists on the target machine, it is replaced with the copy from the backup.)

- Review the information for existing transaction logs.
  See "About existing Exchange Server transaction logs" on page 141.

See "Restoring storage groups or storage group databases from a streaming backup" on page 166.

See "About restoring streaming backups of Exchange Server (Exchange 2007 and earlier)" on page 164.

See "About restoring individual Exchange mailbox and public folder items" on page 172.

See "Prerequisites and operational notes for restoring Exchange individual mailboxes, mailbox folders, public folders, or messages" on page 173.

About existing Exchange Server transaction logs

Depending upon the data recovery scenario you have, you must take existing transaction logs into consideration.

For example, do one of the following tasks:

- Roll-forward recovery (or replay all log files)
  After you restore the files and the service starts up, Exchange commits the transactions in the logs you restored. If contiguous logs exist on the server beyond the log with the highest number you restored, those transactions also are committed. If there is any gap in the numeric sequence of log names, no further transactions are committed beyond the gap.
  This scenario is useful when the transaction logs are intact but you require the database to be restored. When you keep existing transaction logs, Exchange Server can recover to the point of the failure. Otherwise, you must recover to the time of the last full backup or the last incremental backup.

- Point-in-time recovery (or replay only restored log files)
  Use this option if you only want to restore up to the point of the last backup. Any transaction logs that are created after the last backup are not involved in the recovery of the database(s). For snapshot restores, NetBackup renames current log files to `.delete`.

See "About Exchange backups and transaction logs" on page 100.

See "About truncating Exchange transaction logs with Instant Recovery backups" on page 72.

See "Truncating Exchange transaction logs by performing a backup to a storage unit" on page 73.

See "About Exchange backup operations" on page 18.

See "About Exchange Instant Recovery methods" on page 21.

About restoring Exchange snapshot backups

From a snapshot backup you can restore the Microsoft Information Store, Exchange 2010 databases, and Exchange 2007 and earlier storage groups and storage group databases. If you enabled Granular Recovery Technology (GRT) for the backup, you can also restore mailbox and public folder items from the backup.

See "About restoring individual Exchange mailbox and public folder items" on page 172.

Note the following when you restore snapshot backups:

- (Exchange 2007 and earlier) All databases in a storage group must be dismounted before you begin a restore operation. You can instruct NetBackup to dismount the databases before the restore begins.
  See "Exchange snapshot restore options" on page 143.

- All of the images you select for the restore must be from snapshot backups.

- Only Exchange 2007 allows snapshot restores to the recovery storage group (RSG).

- Exchange 2010 allows restores to the recovery database (RDB).
  See "Redirecting an Exchange 2010 Database Availability Group (DAG) snapshot backup to another database or to the recovery database (RDB)" on page 151.
  See "Redirecting an Exchange 2010 standalone server snapshot backup to another database or to the recovery database (RDB)" on page 155.

- (Exchange 2007 and later) For Instant Recovery restores:
  Select **Normal Backup** even if you want to perform volume rollback. NetBackup automatically rolls back volumes whenever it is appropriate

  One of the following occurs:

  - NetBackup snaps back (resyncs) the selected database volumes from the snapshot to the original volume.

  - NetBackup copies back the files of the selected databases from the snapped volume to the original volume

See "About snapshot backups with Exchange Server" on page 20.

See "Limitations of Exchange snapshot operations" on page 103.

See "Configuration requirements for snapshot backups of Exchange Server" on page 103.

Exchange snapshot restore options

The following restore options are available when you perform snapshot restores.

Table 6-5   Snapshot restore options

Option	Description
Roll-Forward Recovery (Replay all log files)	Retains the existing transaction logs. Exchange replays transaction logs that are part of the restore operation, followed by any transaction logs that currently exist. See "About existing Exchange Server transaction logs" on page 141.
Point-in-Time Recovery (Replay only restored log files)	Restores the database(s) or storage group(s) and replaces only the transaction logs that existed at the time of backup. A restore may require a full backup and one or more incremental backups. You can select all of the images and perform the restore in one job. Or you can restore each backup image separately. In the latter case, only enable **Point-in-Time Recovery** for the first job. Otherwise, each point-in-time recovery deletes the transaction logs from the preceding restore jobs. NetBackup renames all transaction log files that exist at the start of the recovery operation to E*XXYYYYYYYY*.log.delete or E0*yXXXXX*.log.delete. Current transaction logs are only renamed for the Exchange database or storage group that is restored. Then NetBackup copies logs from the backup image. You can manually delete any logs named E*.log.delete when the restore or recovery is successful. Otherwise, NetBackup deletes them on the next point-in-time recovery.
Temporary location for log files	Not applicable for snapshot restores.
Dismount database prior to restore	Dismounts the database(s) before the restore begins. For Exchange 2007 and earlier, this option dismounts all of the databases in the storage that you want to restore, even if a database is not selected for restore. By default this option is not selected. This option also sets the **Database can be overwritten by a restore** flag in Exchange 2007 and later. **Note:** Use this option with caution. Ensure that you selected the correct database to restore before you choose to dismount it with this option.

Table 6-5   Snapshot restore options *(continued)*

| Option	Description
Commit after last backup set is restored	This option should only be set on the last job of a multi-job restore. This option enables the restore operation to play through log files and roll back any uncompleted transactions. If this option is not selected, the database needs to be mounted manually after the restore.
	If **Commit after last backup set is restored** is selected when an intermediate backup is applied, you cannot restore further backups. You must restart the restore operation from the beginning.
Mount database after restore	**Mount database after restore** is automatically selected if **Commit after last backup set is restored** is selected. Otherwise, this option is disabled.
Redirect to Recovery Storage Group (RSG) (Only for Exchange 2007)	Check this option to restore to the recovery storage group (RSG, only applies to Exchange 2007 restores). You cannot restore Exchange 2003 VSS backups to the recovery storage group.
	See "Redirecting an Exchange 2007 snapshot backup to a storage group or the recovery storage group" on page 159.
	See "Redirecting an Exchange 2010 Database Availability Group (DAG) snapshot backup to another database or to the recovery database (RDB)" on page 151.
Start Restore	Initiates the restore operation.

Performing a snapshot restore of a Database Availability Group (DAG)

To perform a snapshot restore of a Database Availability Group (DAG)

1   Manually suspend replication. This step applies for any snapshot provider you use.

    http://technet.microsoft.com/en-us/library/dd298159.aspx

2   Dismount all Exchange databases that you want to restore.

    Or, when you perform the restore, click the **Dismount database prior to restore** option.

3   Open the Backup, Archive, and Restore interface.

4   Click **File > Select Files and Folders to Restore > from Normal Backup**.

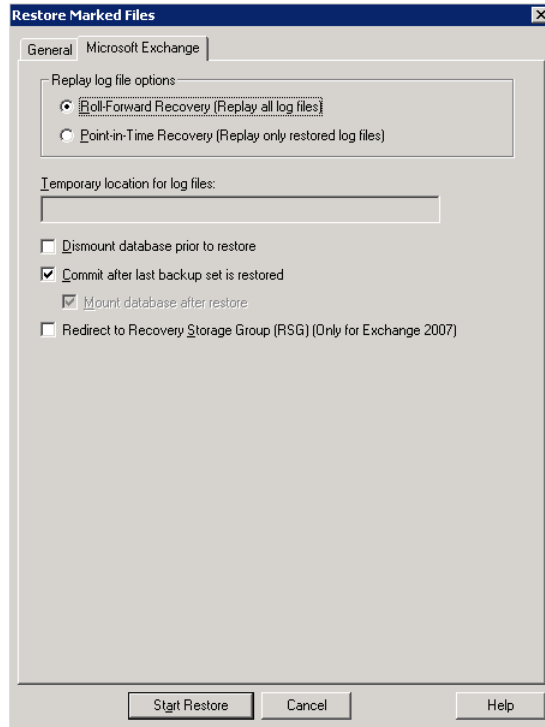5   Select **File > Specify NetBackup Machines and Policy Type**.

6 In the **Specify NetBackup Machines and Policy Type** dialog box, provide the following information:

■ The server that performed the restore.

■ For the source client, select the DAG virtual name.
See "About selecting a source client for an Exchange Server backup or restore operation" on page 190.

■ For the policy type, select **MS-Exchange-Server**.

7 From the **NetBackup History** pane, click the backup image that contains the objects you want to restore as follows:

■ The last full backup or user-directed backup

■ The last full backup and all subsequent differential backups

■ The last full backup and the last cumulative backup

8 In the **All Folders** pane, select the objects you want to restore, as follows:

■ The Database Availability Group.
Selecting this object restores all the databases.

■ Databases.
Expand the DAG. Then select the database(s) and log files you want to restore.
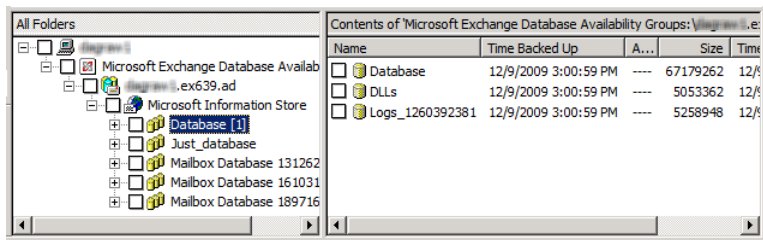
9 Click **Actions > Restore**.

10 Click the **Microsoft Exchange** tab.

See "Exchange snapshot restore options" on page 143.

11 Click **Start Restore**.

The restore is directed to the active Exchange database, regardless of which database was backed up. NetBackup automatically detects the Exchange server that currently contains the active Exchange database.

12 When the restore completes, resume replication.

13 If necessary, update the mailbox database copy.

http://technet.microsoft.com/en-us/library/dd351100.aspx

Performing a snapshot restore of an Exchange 2010 standalone server or an Exchange 2007 or earlier server

To perform a snapshot restore of an Exchange 2010 standalone server or an Exchange 2007 or earlier server

1   Dismount all Exchange databases that you want to restore.

   Or, when you perform the restore, click the **Dismount database prior to restore** option.

2   Open the Backup, Archive, and Restore interface.

3   Click **File > Select Files and Folders to Restore > from Normal Backup**.

4   Select **File > Specify NetBackup Machines and Policy Type**.

5   In the **Specify NetBackup Machines and Policy Type** dialog box, provide the following information:

   ■   The server that performed the restore.

   ■   If you have an Exchange 2007 cluster environment, for the source client select the virtual Exchange server name.
       See "About selecting a source client for an Exchange Server backup or restore operation" on page 190.

   ■   For the policy type, select **MS-Exchange-Server**.

6   From the **NetBackup History** pane, click the backup image that contains the objects you want to restore as follows:

   ■   The last full backup or user-directed backup

   ■   The last full backup and all subsequent differential backups

   ■   The last full backup and the last cumulative backup

7   In the **All Folders** pane, select the objects you want to restore, as follows:

   ■   The Microsoft Information Store.
       Click the checkbox next to the computer name or the **Microsoft Information Store**.

   ■   (Exchange 2007 and earlier) storage groups.
       Expand the **Microsoft Information Store** node and select the storage group to restore.

   ■   Exchange 2010 databases.
       Expand the **Microsoft Information Store** node. Then select the database(s) and log files you want to restore.

   ■   Exchange 2007 and earlier databases.

Expand the **Microsoft Information Store** node and the storage group. Then select the database(s) and log files you want to restore.

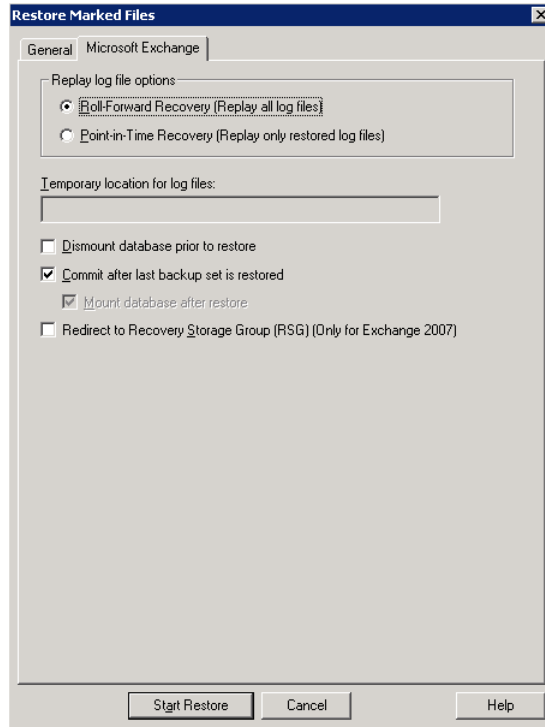The following figure shows a restore of Exchange 2010.
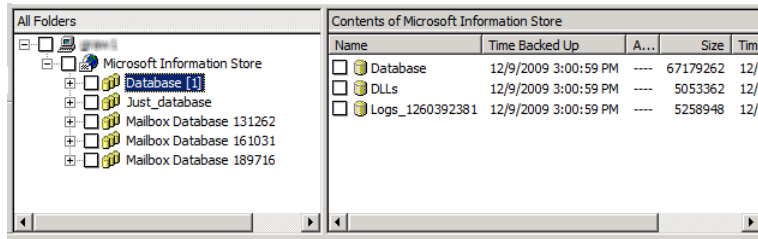
The following figure shows a restore of an Exchange 2007 storage group.
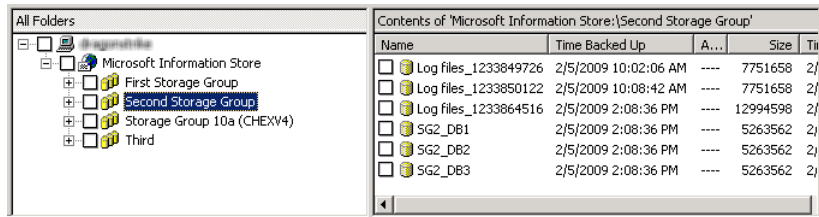
8   Click **Actions > Restore**.

9   Click the **Microsoft Exchange** tab.

10 Click **Start Restore**.

Recovering an Exchange 2007 Local Continuous Replication (LCR) environment

This topic describes how to recover a storage group with LCR enabled. Most of the following PowerShell commands are now available in the Exchange Management Console with Exchange 2007 SP1. You must manually suspend replication in a LCR environment. This applies to VSS and non VSS.

Refer to *Managing Local Continuous Replication* for more information:

http://technet.microsoft.com/en-us/library/aa998823.aspx

Follow these steps:

■   Issue the PowerShell command `Suspend-StorageGroupCopy` for a storage group before you restore that storage group.

- Perform a database restore.
  See "Performing a snapshot restore of an Exchange 2010 standalone server or an Exchange 2007 or earlier server" on page 147.

- You may need to re-seed the copy before you resume the copy.
  Do the following:

  - Remove the database files, all log files, and all checkpoint files from the copy location. (If you use it, the Exchange Management Console prompts you to perform this step.)

  - Issue the PowerShell command `Update-StorageGroupCopy`.
    See *How to Seed a Local Continuous Replication Copy* for more information:
    http://technet.microsoft.com/en-us/library/aa995973.aspx

- Issue the PowerShell command `Resume-StorageGroupCopy` to properly resume the copy.

See "Recovering an Exchange 2007 Clustered Continuous Replication (CCR) environment" on page 150.

See "Policy recommendations for Exchange Server 2007 and earlier database backups" on page 82.

See "Configuring the NetBackup service account (Exchange 2007)" on page 58.

See "Notes and limitations for creating a backup selections list for Exchange 2007 and earlier streaming database backups" on page 126.

Recovering an Exchange 2007 Clustered Continuous Replication (CCR) environment

This topic describes how to recover a storage group with CCR enabled. Most of the following PowerShell commands are now available in the Exchange Management Console with Exchange 2007 SP1. You must manually suspend replication in a LCR environment. This applies to VSS and non VSS.

Note: A restore can only be directed to the active node.

See *Managing Cluster Continuous Replication* for more information:

http://technet.microsoft.com/en-us/library/aa997676.aspx

Follow these steps:

- For Exchange 2007 pre-SP1, The NetBackup Client Service must be run as a privileged domain account on each node. Otherwise, NetBackup is not properly authorized to perform dismounts or restores.

- Issue the PowerShell command `Suspend-StorageGroupCopy` for a storage group before you restore that storage group.

- Perform a database restore.
  See "Performing a snapshot restore of an Exchange 2010 standalone server or an Exchange 2007 or earlier server" on page 147.

- You may need to re-seed the cluster copy before you resume the copy.

  Do the following:

  - Remove the database files, all log files, and all checkpoint files from the passive node. (If you use it, the Exchange Management Console, prompts you to perform this step.)

  - From the passive node, issue the PowerShell command `Update-StorageGroupCopy`.
    See *How to Seed a Cluster Continuous Replication Copy* for more information:
    http://technet.microsoft.com/en-us/library/bb124706.aspx

- Issue the PowerShell command `Resume-StorageGroupCopy` to properly resume the cluster copy.

See "Recovering an Exchange 2007 Local Continuous Replication (LCR) environment" on page 149.

See "Redirecting an Exchange 2007 snapshot backup to a storage group or the recovery storage group" on page 159.

See "Configuring the NetBackup service account (Exchange 2007)" on page 58.

See "Policy recommendations for Exchange Server 2007 and earlier database backups" on page 82.

Redirecting an Exchange 2010 Database Availability Group (DAG) snapshot backup to another database or to the recovery database (RDB)

To redirect an Exchange 2010 snapshot backup to another database or to the recovery database

1   Manually suspend replication. This step applies for any snapshot provider you use.

    http://technet.microsoft.com/en-us/library/dd298159.aspx

2   The database or the recovery database must already exist.

    To restore to the RDB, create the RDB on an Exchange server, if necessary. Leave the RDB dismounted.

3   Open the Backup, Archive, and Restore interface.

4   Click **File > Select Files and Folders to Restore > from Normal Backup**.

5   Click **File > Specify NetBackup Machines and Policy Type**.

6   In the **Specify NetBackup Machines and Policy Type** dialog box, provide the
      following information:

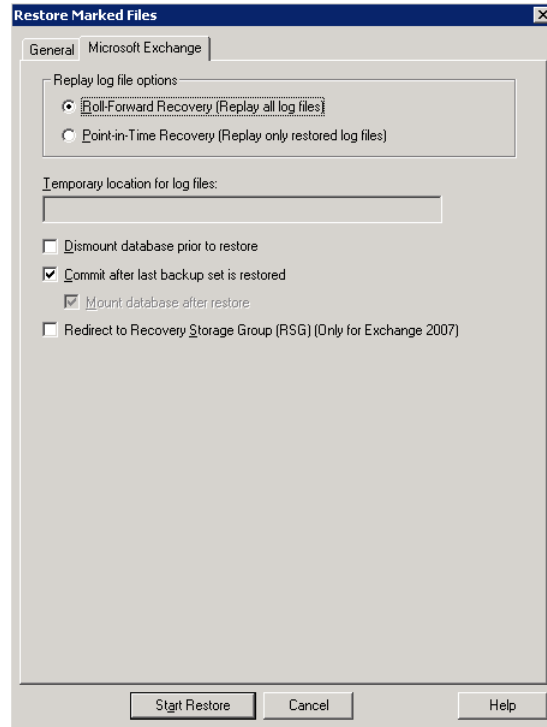|	
Server to use for backups and restores	Select the server that performed the restore.
Source client for restores	Select the virtual DAG name.
Destination clients for restores	To restore to another database in the same DAG, leave the destination client the same as the source client. NetBackup detects the active server to which to redirect the restore.
	To redirect the restore to a different DAG, indicate the DAG name where that database exists. NetBackup automatically detects the CAS server that is assigned to the database. To restore to the RDB, indicate the DAG name. If the RDB exists on a standalone server, indicate that server name as the destination client.
	If applicable, review the notes and limitations for redirecting to a different client.
	See "About selecting a destination client for an Exchange Server restore operation" on page 191.
Policy type for restores	Select **MS-Exchange-Server**.

7   From the **NetBackup History** pane, select one of the following:

      ■   The last full backup, or

      ■   The last full backup and all subsequent differential backups, or

      ■   The last full backup and the last cumulative backup

8   In the **All Folders** pane, expand **Microsoft Exchange Database Availability Groups > *Forest or domain name***.

9   Select the database you want to restore.

10   Click **Actions > Restore**.

11   Change the destination path to another database or to the RDB:

      ■   Click the **General** tab.

■ Select **Restore everything to a different location**.

■ In the **Destination** box, provide the name of the alternate database you want to restore to. Or provide the name of the RDB you previously created. Exchange 2010 does not automatically redirect a database to its RDB, if it exists.

Restore Marked Files

General | Microsoft Exchange |

Restore Destination Choices

○ Restore everything to its original location

● Restore everything to a different location (maintaining existing structure)

Destination:

`bs:\ _____ \Microsoft Information Store\AnotherDatabase\`   Browse...

○ Restore individual folders and files to different locations (double-click to modify)

`base Availability Groups:\ _____ \Microsoft Information Store\Database [1]\`

○ Create and restore to a new virtual hard disk file

Destination for virtual hard disk file:

Properties

Restore Options

☐ Restore without access-control attributes (Windows clients only)

○ Overwrite existing files

○ Restore the file using a temporary filename

○ Do not restore the file

☐ Override default job priority

Job priority   `90000`

(Higher number is greater priority)

Start Restore   Cancel   Help

12 Click the **Microsoft Exchange** tab.

See "Exchange snapshot restore options" on page 143.

13 Check **Commit after last backup set is restored**.

If you choose to restore backup images separately, you must check **Commit after last backup set is restored** only when you restore the *last* incremental backup set.

If you do not select **Commit after last backup set is restored**, manually mount the database after the restore is complete.

See "Manually mounting an Exchange database after a restore" on page 163.

14 Click **Start Restore**.

The restore is directed to the active Exchange database, regardless of which database was backed up. NetBackup automatically detects the Exchange server that currently contains the active Exchange database.

15 When the restore completes, resume replication.

16 If necessary, update the mailbox database copy.

   http://technet.microsoft.com/en-us/library/dd351100.aspx

See "Redirecting an Exchange 2010 standalone server snapshot backup to another database or to the recovery database (RDB)" on page 155.

See "Redirecting an Exchange 2007 snapshot backup to a storage group or the recovery storage group" on page 159.

See "About redirecting restores of Exchange 2003 snapshot backup images" on page 163.

Redirecting an Exchange 2010 standalone server snapshot backup to another database or to the recovery database (RDB)

This topic describes how to redirect a snapshot backup of an Exchange 2010 standalone server to another database or the recovery database (RDB).

To redirect an Exchange 2010 standalone server snapshot backup to the recovery database

1 The database or the recovery database must already exist.

   To restore to the RDB, create the RDB on an Exchange server, if necessary. Leave the RDB dismounted.

2 Open the Backup, Archive, and Restore interface.

3 Click **File > Select Files and Folders to Restore > from Normal Backup**.

4 Click **File > Specify NetBackup Machines and Policy Type**.

5   In the **Specify NetBackup Machines and Policy Type** dialog box, provide the
     following information:

Server to use for backups and restores	Select the server that performed the restore.
Destination clients for restores	To restore to the RDB on a different server, change the destination client to the Exchange server that hosts the RDB. This client must be the Exchange server that hosts the database to which you want to redirect the restore. Also review the notes and limitations for redirecting to a different client.
	See "About selecting a destination client for an Exchange Server restore operation" on page 191.
	To restore to the RDB or to a database on the local server, leave the destination client the same as the source client.
Policy type for restores	Select **MS-Exchange-Server**.

6   From the **NetBackup History** pane, select one of the following:

■   The last full backup, or

■   The last full backup and all subsequent differential backups, or

■   The last full backup and the last cumulative backup

7   In the **All Folders** pane, expand **Microsoft Information Store**.

8   Select the database you want to restore.

9   Click **Actions > Restore**.

10   In the **Restore Marked Files** dialog box, click the **General** tab.

11   Change the destination path to another database or to the RDB:

■   Select **Restore everything to a different location**.

■   In the **Destination** box, provide the name of the alternate database you
    want to restore to. Or provide the name of the RDB you previously created.
    Exchange 2010 does not automatically redirect a database to its RDB, if
    it exists.

12 Click the **Microsoft Exchange** tab.
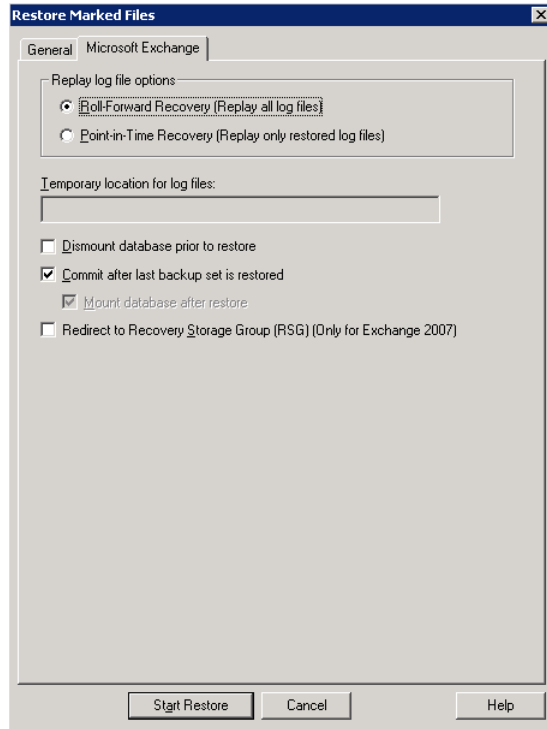
See "Exchange snapshot restore options" on page 143.

13 Check **Commit after last backup set is restored**.

If you choose to restore backup images separately, you must check **Commit after last backup set is restored** only when you restore the *last* incremental backup set.

If you do not select **Commit after last backup set is restored**, manually mount the database after the restore is complete.

See "Manually mounting an Exchange database after a restore" on page 163.

14 Click **Start Restore**.

See "Redirecting an Exchange 2010 Database Availability Group (DAG) snapshot backup to another database or to the recovery database (RDB)" on page 151.

See "Redirecting an Exchange 2007 snapshot backup to a storage group or the recovery storage group" on page 159.

See "About redirecting restores of Exchange 2003 snapshot backup images" on page 163.

Redirecting an Exchange 2007 snapshot backup to a storage group or the recovery storage group

This topic describes how to redirect an Exchange 2007 snapshot backup. You can redirect the restore to another storage group or to the recovery storage group (RSG).

For further instructions, refer to the following information on recovery storage groups on Microsoft's Technet site:

http://technet.microsoft.com/en-us/library/aa997260.aspx

To redirect an Exchange 2007 snapshot backup to a storage group or the recovery storage group

1   The RSG or storage group must already exist. Do the following:

   ■   To restore to the RSG, create the RSG and the databases you want to recover on an Exchange server, if necessary. Leave the RSG dismounted.

   ■   To restore to another storage group, create a storage group that has databases. Those databases must have the same names as those in the original storage group.

2   Open the Backup, Archive, and Restore interface.

3   Click **File > Select Files and Folders to Restore > from Normal Backup**.

4   Click **File > Specify NetBackup Machines and Policy Type**.

5   In the **Specify NetBackup Machines and Policy Type** dialog box, provide the following information:

Server to use for backups and restores	Select the server that performed the restore.
Destination clients for restores	If you want to restore to a different server, change the destination client to the Exchange server that hosts the RSG or the storage group. Also review the notes and limitations for redirecting to a different client.
	See "About selecting a destination client for an Exchange Server restore operation" on page 191.
	If you want to restore the RSG or a storage group to the local server, leave the destination client the same as the source client.
Policy type for restores	Select **MS-Exchange-Server**.

6   From the **NetBackup History** pane, select one of the following:

■   The last full backup, or

■   The last full backup and all subsequent differential backups, or

■   The last full backup and the last cumulative backup

7   In the **All Folders** pane, expand the Microsoft Information Store.

8   Select the storage group you want to restore.

9   Click **Actions > Restore**.

10 In the **Restore Marked Files** dialog box, click the **General** tab.

11 To redirect the storage group, do the following:

■   Select **Restore everything to a different location**.

■   Change the destination path.
    When you redirect a snapshot restore to the RSG, the ESE engine does not automatically redirect the storage group restore to its RSG, if it exists.
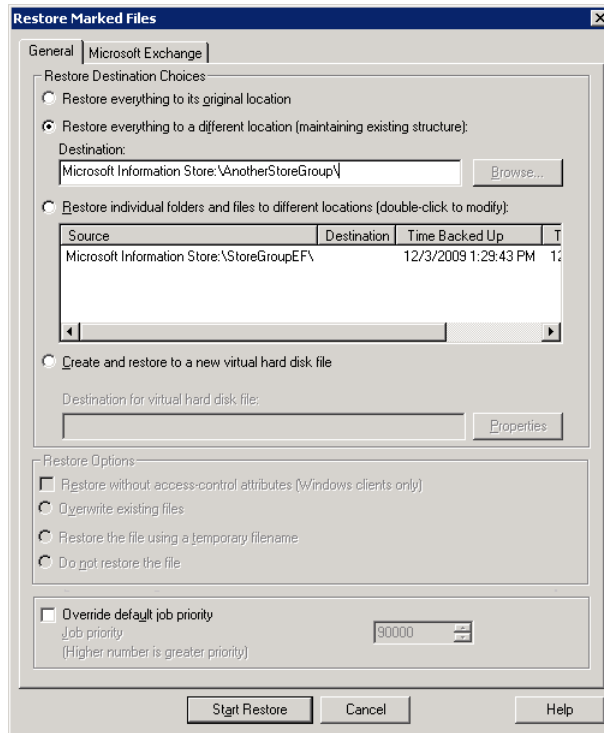
Restore Marked Files

General | Microsoft Exchange

Restore Destination Choices

○ Restore everything to its original location

● Restore everything to a different location (maintaining existing structure):

Destination:

Microsoft Information Store:\AnotherStoreGroup\   [Browse...]

○ Restore individual folders and files to different locations (double-click to modify):

Source	Destination	Time Backed Up	T
Microsoft Information Store:\StoreGroupEF\		12/3/2009 1:29:43 PM	12

○ Create and restore to a new virtual hard disk file

Destination for virtual hard disk file:

[   ]   [Properties]

Restore Options

☐ Restore without access-control attributes (Windows clients only)

○ Overwrite existing files

○ Restore the file using a temporary filename

○ Do not restore the file

☐ Override default job priority

Job priority   [90000]

(Higher number is greater priority)

[Start Restore]   [Cancel]   [Help]

12 Click the **Microsoft Exchange** tab.

See "Exchange snapshot restore options" on page 143.

13 Check **Commit after last backup set is restored**.

If you choose to restore backup images separately, you must check **Commit after last backup set is restored** only when you restore the *last* incremental backup set.

If you do not select **Commit after last backup set is restored**, manually mount the database after the restore is complete.

See "Manually mounting an Exchange database after a restore" on page 163.

14 If you want to restore to an RSG, check **Redirect to Recovery Storage Group (RSG) (Only for Exchange 2007)**.

15 Click **Start Restore**.

See "Recovering an Exchange 2007 Local Continuous Replication (LCR) environment" on page 149.

See "About redirecting restores of Exchange 2003 snapshot backup images" on page 163.

About redirecting restores of Exchange 2003 snapshot backup images

The following limitations and requirements exist to redirect restores of Exchange 2003 snapshot backups:

■ You cannot restore an Exchange 2003 snapshot backup to an RSG.

■ With this Exchange version, you cannot redirect to a different storage group on the local server.

■ If you want to redirect to a storage group on another server the storage group and the database must be identical. The path(s) of the storage group also must be identical to the original storage group.

See "Redirecting an Exchange 2007 or Exchange 2003 streaming backup to a recovery storage group" on page 168.

See "Configuring the NetBackup service account (Exchange 2003)" on page 59.

Manually mounting an Exchange database after a restore

If you did not click **Commit after last backup set is restored**, you need to mount the database manually after the restore is completed.

To mount a database manually after a restore

1   Mount all of the databases that were restored in the storage group.

2   If the mount fails, try a soft recovery (ignore mismatched database attachments) of the Exchange databases to bring the databases to a consistent state.

```
eseutil /r E0n /i
```

3   Mount the databases again.

See "Recovering an Exchange database" on page 204.

See "Restoring storage groups or storage group databases from a streaming backup" on page 166.

See "About backing up Exchange Server data" on page 131.

See "About restoring Exchange database data" on page 139.

About restoring streaming backups of Exchange Server (Exchange 2007 and earlier)

Streaming backups can only be performed with Exchange 2007 or earlier. NetBackup uses snapshot technology for all Exchange 2010 backups.

NetBackup can restore the following Exchange Server objects from streaming backups:

- Microsoft Information Store
- Storage groups
- Storage group databases

You can also redirect a restore to the recovery storage group (RSG).

See "Redirecting an Exchange 2010 Database Availability Group (DAG) snapshot backup to another database or to the recovery database (RDB)" on page 151.

See "Redirecting an Exchange 2007 snapshot backup to a storage group or the recovery storage group" on page 159.

See "Redirecting an Exchange 2007 or Exchange 2003 streaming backup to a recovery storage group" on page 168.

Restore options for streaming restores of Exchange databases

The **Roll-Forward Recovery** and **Point-in-Time Recovery** options correspond to the **Delete existing transaction logs prior to restore** option in NetBackup 6.5 and earlier. However, the default option has changed. In those previous releases, **Delete existing transaction logs prior to restore** was enabled by default, which corresponds to **Point-in-Time Recovery**. The new default option is **Roll-Forward Recovery**.

Different options are available when you perform a MAPI mailbox restore or a snapshot restore.

See "Restore options for restores of Exchange Server mailbox objects or public folder objects" on page 174.

See "Exchange snapshot restore options" on page 143.

Table 6-6   Restore options for streaming restores of Exchange databases

Option	Description
Roll-Forward Recovery (Replay all log files)	Retains the existing transaction logs. Exchange replays the transaction logs that are part of the restore, followed by any transaction logs that currently exist. See "About existing Exchange Server transaction logs" on page 141.

Table 6-6   Restore options for streaming restores of Exchange databases
(continued)

Option	Description
Point-in-Time Recovery (Replay only restored log files)	Restores the database and replaces only the transaction logs that existed at the time of backup.
Temporary location for log files	Enter a location where the associated log files are kept until the database is restored. The default location is `c:\temp`. If you choose to restore storage groups, NetBackup creates a subdirectory in `c:\temp` for each storage group. It keeps log files for each storage group in the corresponding subdirectory.
	If **Commit after last backup** set is restored is selected during the restore, Exchange applies to the database. Then it applies the current log files. After the restore is complete, Exchange deletes the log files from the temporary location (including any subdirectories).
	Note: Make sure the temporary location for log files is empty before you start a restore job. If a restore job fails, check the temporary location (including subdirectories) to make sure any previous log files from a previous restore job were deleted.
Dismount database prior to restore	Dismounts the database(s) before the restore begins. This option dismounts all of the databases in the storage groups that you want to restore, even if a database is not selected for restore. By default this option is not selected.
	This option also sets the **Database can be overwritten by a restore** flag in Exchange 2007.
	Note: Use this option with caution. Ensure that you selected the correct database to restore before you choose to dismount it with this option.
Commit after last backup set is restored	This option should only be set on the last job of a multi-job restore. This option enables the restore operation to play through log files and roll back any uncompleted transactions. If this option is not selected, the database needs to be mounted manually after the restore.
	If **Commit after last backup set is restored** is selected when an intermediate backup is applied, you cannot restore further backups. You must restart the restore operation from the beginning.
Mount database after restore	Mounts the database so that it is available to users.
Redirect to Recovery Storage Group (RSG) (Only for Exchange 2007)	This option is not applicable for streaming restores.
Start Restore	Initiates the restore operation.

Restoring storage groups or storage group databases from a streaming backup

This topic describes how to restore storage groups or databases.

Note: A restore of Exchange Server files always overwrites any existing files. For example, if `Pub.edb` already exists on the target computer, it is replaced with the copy from the backup.

To restore storage groups or storage group databases from a streaming backup

1   Log onto the server as Administrator.

2   Dismount all Exchange databases that need to be restored.

    Or, when you perform the restore, click the **Dismount database prior to restore** option.

3   Open the Backup, Archive, and Restore interface.

4   Click **File > Select Files and Folders to Restore > from Normal Backup**.

5   Click **File > Specify NetBackup Machines and Policy Type**.

6   In the **Specify NetBackup Machines and Policy Type** dialog box, provide the following information:

   ■   The server that performed the restore.

    ■   For the policy type, select **MS-Exchange-Server**.

7   From the NetBackup History pane, select one of the following:

    ■   The last full backup

    ■   The last full backup and all subsequent differential backups

    ■   The last full backup and the last cumulative backup

8   In the **All Folders** pane, select the objects you want to restore:

    ■   Storage groups.
        Expand **Microsoft Information Store** and click the storage group to restore.

    ■   Individual databases.
        To restore an individual database within a specific storage group, expand **Microsoft Information Store**, then the storage group, and click the database.

A full backup of an Exchange database includes the database transaction log files. When you restore a database, you must also restore the transaction log files.
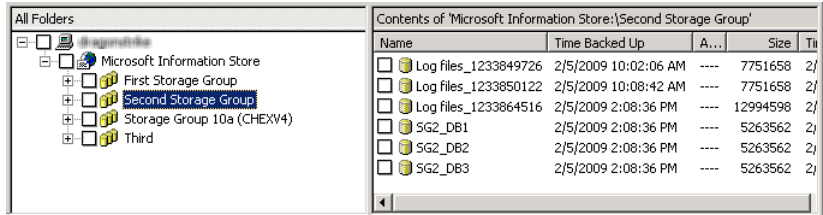

9   Click **Actions > Restore**.
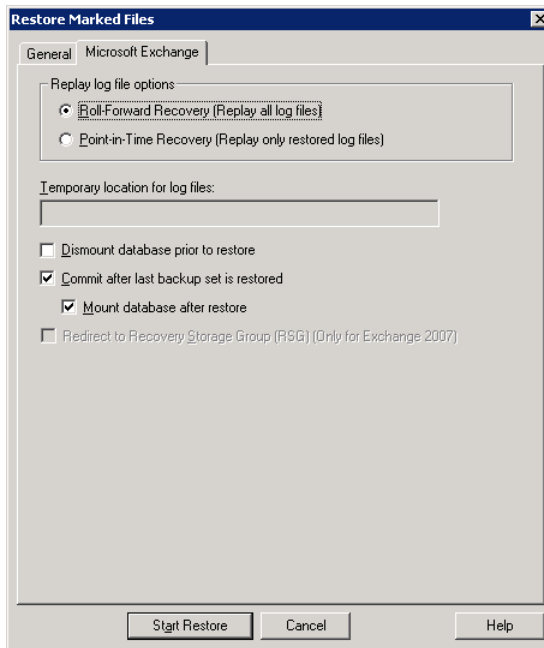
10   Select the restore options you want.

See "Restore options for streaming restores of Exchange databases" on page 164.

11 If you chose to restore the backups individually, uncheck **Commit after last backup set is restored** for the full and all but the last incremental backup.

When you restore the *last* incremental backup set, check **Commit after last backup set is restored** and **Mount database after restore**.

12 Click **Start Restore**.

13 If you restored storage groups and did not click **Mount database after restore** (after the restore), be sure to mount the storage group databases that were restored.

See "About restoring streaming backups of Exchange Server (Exchange 2007 and earlier)" on page 164.

See "Recovering an Exchange database" on page 204.

See "About configuring the NetBackup Client Service for backups and restores that use Granular Recovery Technology (GRT) or MAPI" on page 55.

See "Configuring a streaming NetBackup for Exchange policy (Exchange 2007 and earlier)" on page 123.

See "Policy recommendations for Exchange Server 2010" on page 79.

See "Policy recommendations for Exchange Server 2007 and earlier database backups" on page 82.

Redirecting an Exchange 2007 or Exchange 2003 streaming backup to a recovery storage group

NetBackup supports restores to the recovery storage group. With streaming backups, you do not need to redirect the restore as long as the RSG already exists and is added for the selected storage group and database(s). The restore automatically is restored to the recovery storage group.

For further instructions, refer to the following information on recovery storage groups on Microsoft's Technet site:

Exchange 2007   http://technet.microsoft.com/en-us/library/aa997260.aspx

Exchange 2003   http://technet.microsoft.com/en-us/library/aa998782.aspx

To redirect an Exchange 2007 or Exchange 2003 streaming backup to a recovery storage group

1 Log onto the server as Administrator.

2 Create the RSG on the target Exchange Server, if necessary.

3   (Exchange 2007) Dismount all Exchange databases you want to restore.

Or, when you perform the restore, click the **Dismount database prior to restore** option.

4   Confirm that the RSG databases are not mounted.

5   Open the Backup, Archive, and Restore interface.

6   Click **File > Select Files and Folders to Restore > from Normal Backup**.

7   Click **File > Specify NetBackup Machines and Policy Type**.

8   In the **Specify NetBackup Machines and Policy Type** dialog box, provide the following information:

Destination clients for restores	If you want to restore to a different server, change the destination client to the Exchange server that holds the RSG. Also review the notes and limitations for redirecting to a different client.
	See "About selecting a destination client for an Exchange Server restore operation" on page 191.
	If you want to restore to the local server, leave the destination client the same as the source client.
Policy type for restores	Select MS-Exchange-Server.

9   From the **NetBackup History** pane, select one of the following:

- The last full backup

- The last full backup and all subsequent differential backups

- The last full backup and the last cumulative backup

10 In the **All Folders** pane, click the objects you want to restore:

- A storage group
  Expand the Microsoft Information Store node and click the storage group to restore.

- Individual databases
  To restore an individual database within a specific storage group, expand the Microsoft Information Store, then the storage group, and click the database.

A full backup of an Exchange database includes the database transaction log files. When you restore a database, you must also restore the transaction log files.

11 Click **Actions > Restore**.
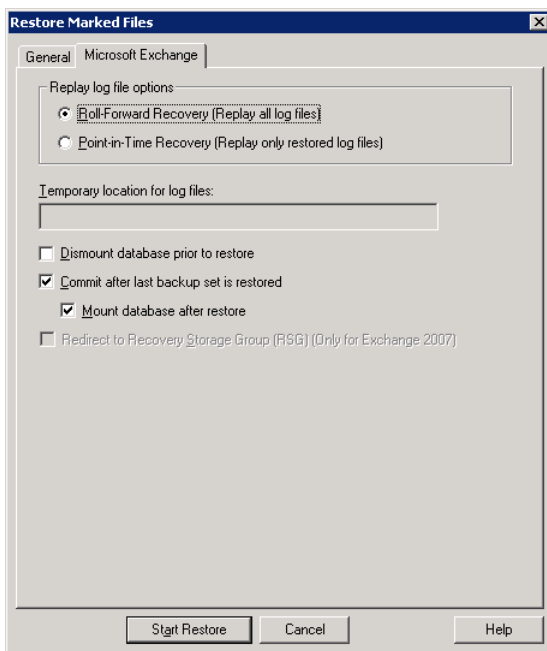
12 To restore the backups individually, click **Commit after last backup set is restored** and **Mount database after restore** when you restore the *last* incremental backup set.

13 Select the other restore options you want.

See "Restore options for streaming restores of Exchange databases" on page 164.

14 (Optional) If wanted, click the **General** tab and change the destination path to the RSG name.

The destination path does not need to be changed even though the RSG is a different name than the original storage group. The ESE engine automatically redirects the restore to the proper location.
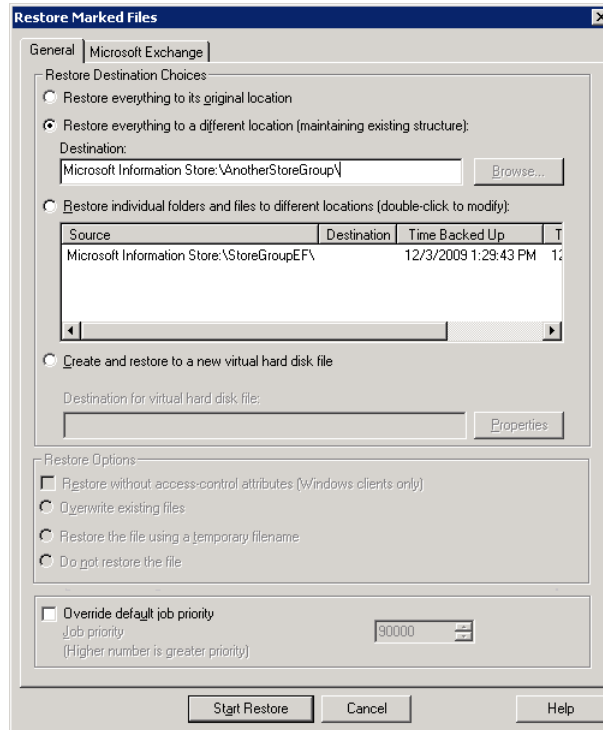
15 Click **Start Restore**.

16 If you chose to restore storage groups and you did not click **Mount database after restore** (after the restore), mount the storage group databases that were restored.

See "Policy recommendations for Exchange Server 2007 and earlier database backups" on page 82.

See "Configuring a streaming NetBackup for Exchange policy (Exchange 2007 and earlier)" on page 123.

See "About restoring streaming backups of Exchange Server (Exchange 2007 and earlier)" on page 164.

About restoring individual Exchange mailbox and public folder items

You can restore individual mailbox or public folder items (folders, messages, and documents) from the following types of backups:

■ MAPI mailbox backups. This backup type applies to Exchange 2007 and earlier.

■ MAPI public folder backups. This backup type applies to Exchange 2007 and earlier.

■ Streaming or snapshot backups with Granular Recovery Technology (GRT) enabled.

About special characters in Exchange mailbox folders and message subjects

NetBackup uses escape sequences for slashes and backslashes in mailbox folder names and message subjects because the objects are handled using file path syntax. The tilde (~) character is the escape character, so it also has to be escaped.

When you browse for items to restore, you see the escaped character sequences. Use Table 6-7 to convert the translated characters back to the characters that appear in the restored items.

Table 6-7   Translation of special characters in mailbox folders and message subjects

Character	Translation
~	~0
/	~1
\	~2

See "About restoring individual Exchange mailbox and public folder items" on page 172.

See "Prerequisites and operational notes for restoring Exchange individual mailboxes, mailbox folders, public folders, or messages" on page 173.

See "About restoring individual Exchange mailbox and public folder items" on page 172.

Prerequisites and operational notes for restoring Exchange individual mailboxes, mailbox folders, public folders, or messages

Review the following prerequisites before you restore individual mailboxes, mailbox folders, public folders, or messages:

■ The destination mailbox must exist to successfully restore a mailbox.

Review the following information before you restore individual mailboxes, mailbox folders, public folders, or messages:

■ When you restore mailbox messages or public folder documents, the option **Overwrite existing message(s)** overwrites the contents and properties of the original objects. Messages are overwritten regardless of their location. (For example, if the messages were moved to the "Deleted Items" folder.) If the original message no longer exists, a new message is generated with the same contents and properties. A new message is also generated if a new destination location is entered.

   If the option **Do not restore the message(s)** is selected, NetBackup skips the restore of any message that still exists, regardless of the current location. Note that if the original message(s) no longer exists, a restore of the message(s) generates a new copy every time it is restored. A restored copy of the message does not count as the original message in the existence check.

■ When a mailbox is restored, all folders and messages that are contained in the mailbox are restored. You can choose to restore specific folders or messages or both from the mailbox backup image.

■ When a folder is restored, all subfolders and messages that are contained in the folder are restored. You also can choose to restore specific subfolders or specific messages or both from the folder backup image.

■ NetBackup can back up the online archive mailbox for users. However, a restore from a backup using Granular Recovery Technology (GRT) by default restores the items to the user's mailbox and not the archive mailbox. Items are restored starting at the root of the mailbox hierarchy. Alternatively, you may want to redirect the restore to the path `Top of Information Store\Inbox\Archives\`.

See "About special characters in Exchange mailbox folders and message subjects" on page 172.

See "About restoring individual Exchange mailbox and public folder items" on page 172.

See "Restoring Exchange mailbox or public folder objects" on page 174.

Restore options for restores of Exchange Server mailbox objects or public folder objects

When you restore mailbox or public folder objects, NetBackup may encounter messages that already exist in the database. Select one of the options from Table 6-8 to indicate whether NetBackup should pass over or replace the pre-existing object.

Note: These options are ignored for a redirected restore.

Table 6-8   Restore options for restores of Exchange Server mailbox objects of public folder objects

Option	Description
Do not restore the message(s)	Does not restore mailbox messages if they already exist.
Overwrite the message	Replaces the existing message with the one from the backup.

Restoring Exchange mailbox or public folder objects

To restore a mailbox object to a different location, you follow a different procedure.

See "About redirecting a restore of Exchange mailbox or public folder objects to a different path" on page 178.

Note: Browse time for a backup that uses Granular Recovery Technology may take longer than for a non-granular backup image. The media server gathers granular information at this time and wait times may vary. Depending on the load on the media server, you may need to increase the **Client read timeout** value. This option is located in the Client host properties in the **Timeouts** tab.

Note: Do not restore mailbox or public folder backups and database backups in the same restore job. If the database restore starts first, NetBackup dismounts the database during the restore. Or it requires that the database be dismounted before the restore. Then the database being dismounted causes the mailbox or public folder object restore to fail. Or, the restore of the Exchange mailbox or public folder items finishes before the restore of the Exchange databases starts. Then the restore of the Exchange databases deletes the restored mailbox or public folder objects.

Note: Do not restore any backups that use Granular Recovery Technology with any backups that do not in the same restore job.

To restore mailbox or public folder objects

1   Log onto the server as Administrator.

2   Open the Backup, Archive, and Restore interface.

3   Click **File > Select Files and Folders to Restore > from Normal Backup**.

4   Click **File > Specify NetBackup Machines and Policy Type**.

5   In the **Specify NetBackup Machines and Policy Type** dialog box, select the server and the policy type.

6   From the **NetBackup History** pane, click the image(s) that contain the objects you want to restore.

    Symantec recommends that you select one backup image set at a time for individual item restore. While this recommendation is not a restriction, you may at times restore more copies of messages than you intend.

    You cannot restore individual items from a snapshot incremental backup that uses Granular Recovery Technology (GRT).

    Select one of the following:

    ■ The last full backup

    ■ The last full backup and all subsequent differential backups

    ■ The last full backup and the last cumulative backup

7   Expand one of the following:

    ■ **Microsoft Exchange Database Availability Groups >** *Forest or Domain* **> Microsoft Information Store >** *Mailbox Database*

    ■ **Microsoft Exchange Database Availability Groups >** *Forest or Domain* **> Microsoft Information Store >** *Public Store*

    ■ **Microsoft Information Store >** *Mailbox Database*

    ■ **Microsoft Information Store >** *Public Store*

    ■ **Microsoft Information Store >** *Storage Group > Mailbox Database*

    ■ **Microsoft Information Store >** *Storage Group > Public Store*

    ■ **Microsoft Exchange Mailboxes**

    ■ **Microsoft Exchange Public Folders**

8   In the **All Folders** pane, select objects you want to restore from the following:

- Mailboxes

- Mailbox folders

- Mailbox objects

- Public folders

- Documents in a public folder

You can ignore the `DLLs` folder.

The following figure shows a restore of a DAG using Granular Recovery Technology (GRT).
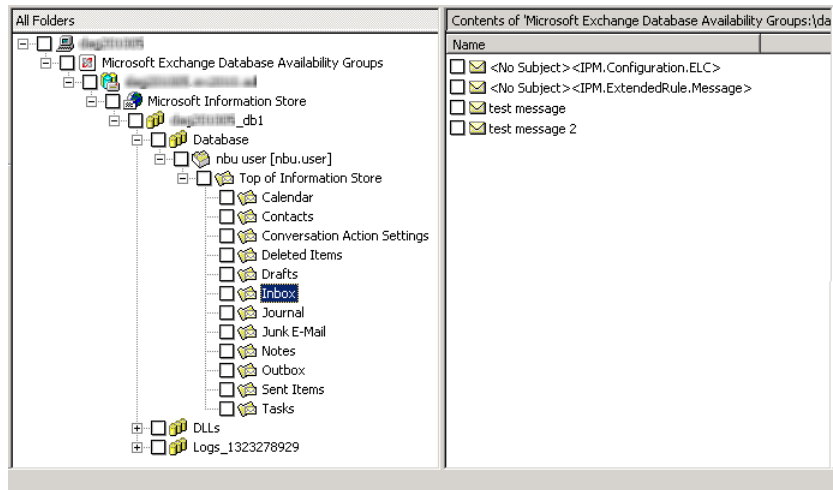
The following figure shows an Exchange 2007 restore using Granular Recovery Technology.
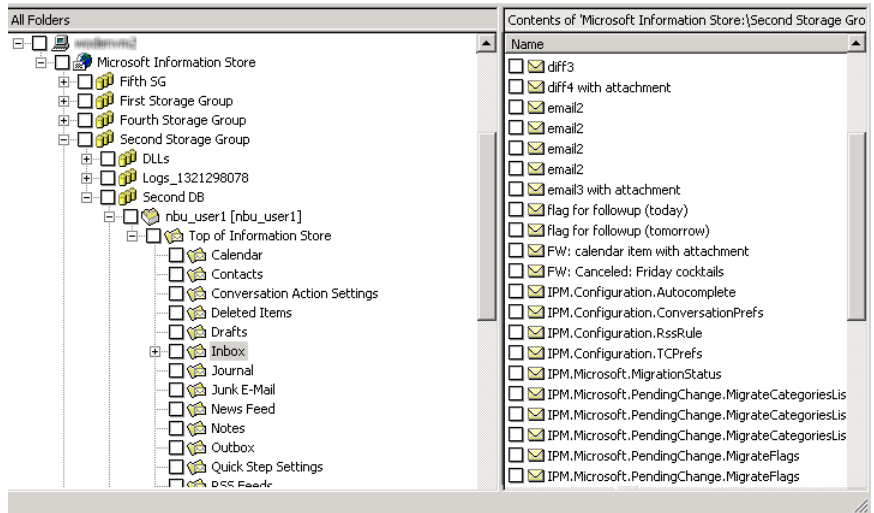
The following figure shows a MAPI mailbox restore.
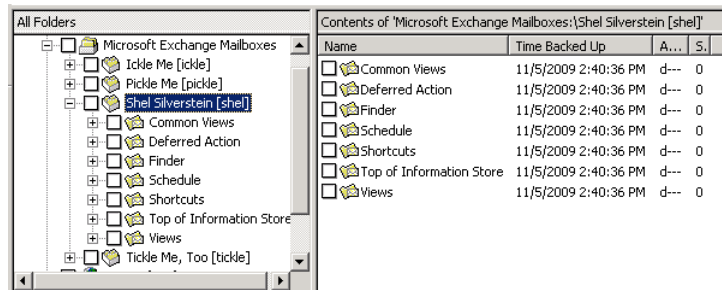
All objects appear as folders and messages. You can identify some non-message objects by the subject line. For example, if you create a Calendar event named Appointment1, that name appears in the subject line for that object.

However, some objects such as Forms and Views do not have a subject line (even though they can be named). They may not be so easily identified.

9 Click **Actions > Restore**.

10 On the **Microsoft Exchange** tab, choose whether or not to restore existing mailbox messages.

See "Restore options for restores of Exchange Server mailbox objects or public folder objects" on page 174.
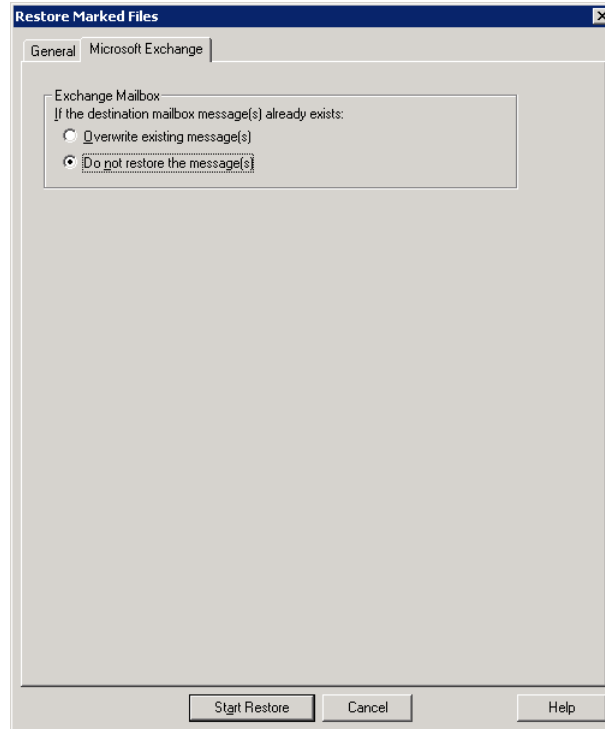
11 You can restore individual mailbox items to alternate mailboxes or mailbox folders.

See "About redirecting a restore of Exchange mailbox or public folder objects to a different path" on page 178.

12 Click **Start Restore**.

About redirecting a restore of Exchange mailbox or public folder objects to a different path

NetBackup can restore Exchange mailbox or public folder objects to different locations.

Refer to the following topics for more information and instructions:

- See "About requirements for redirecting the restore of an Exchange mailbox or public folder object to a different path" on page 179.
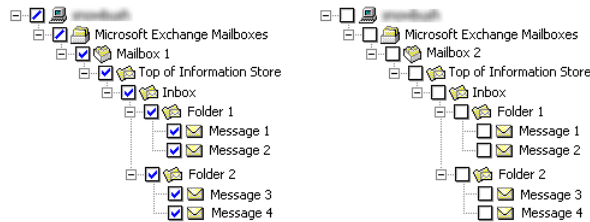
- See "Redirecting the restore of an Exchange mailbox, mailbox folder, or public folder" on page 181.

- See "Redirecting a restore of an Exchange mailbox or a public folder object to a different path" on page 184.

About requirements for redirecting the restore of an Exchange mailbox or public folder object to a different path

Review the following requirements for redirecting the restore of an Exchange mailbox or public folder to a different path:

- You must indicate an explicit path (or full path).

- In the destination path, the following segment of the path cannot be changed:

  `Microsoft Exchange Database Availability Groups:\`

  `Microsoft Information Store:\`

  `Microsoft Exchange Mailboxes:\`

  `Microsoft Exchange Public Folders:\`

  If you change this part of the path, NetBackup attempts to restore the objects as normal (non-Exchange) files.

- The destination mailbox or destination folder must have an associated user account.

- When you redirect a restore of public folders, the folder you indicate in the destination path does *not* have to exist.

- When you redirect mailbox backups, if you modify the name of the Exchange folders, NetBackup restores the selected object to that specified folder name. These Exchange folders include "Top of Information Store," "Views," "Finder", etc. You can see the new folder when you browse for backups and it is backed up on subsequent backups of that mailbox. However, you cannot use Outlook to view the folder and any subfolders and messages in that folder.

- (Exchange 2010) If you want to redirect the restore of a mailbox from a Database Availability Group (DAG) to a standalone Exchange server, you must include `Microsoft Exchange Database Availability Groups:\` and not `Microsoft Information Store\:` in the destination path.

  Correct

```
Microsoft Exchange Database Availability Groups:\Database Name\
John Q. Employee [johnq]\Top of Information Store\Calendar\
```

  Incorrect

```
Microsoft Information Store:\Database Name\John Q. Employee [johnq]\
Top of Information Store\Calendar\
```

- Additional requirements exist when you restore mailboxes from a granular backup. Assume that the source path is one of the following:

```
Microsoft Information Store:\My-Store-Group\My-database\John Q. Employee\
Top of Information Store\Inbox\Nancy's birthday

Microsoft Information Store:\My-database\John Q. Employee\Top of Information Store\
Inbox\Nancy's birthday
```

Note the following:

- "My-Store-Group" must be a valid storage group on the destination Exchange server. However, the target mailbox does not have to exist in the specified storage group.

- "My-database" must exist but is not used at restore time. The mailbox for John Q. Employee is located on the destination Exchange Server but it is independent of the database specification.

- Before you attempt the restore, the mailbox for "John Q. Employee" must exist on the destination server.

See "Prerequisites and operational notes for restoring Exchange individual mailboxes, mailbox folders, public folders, or messages" on page 173.

See "About redirecting a restore of Exchange mailbox or public folder objects to a different path" on page 178.

See "Examples of redirecting an Exchange mailbox restore" on page 180.

See "Redirecting the restore of an Exchange mailbox, mailbox folder, or public folder" on page 181.

Examples of redirecting an Exchange mailbox restore

Mailbox 1 consists of Top of Information Store, Inbox, and Folders 1 and 2, each containing some mail messages. Assume that you back up Mailbox 1. If you restore Mailbox 1 to the existing Mailbox 2, all of the Mailbox 1 contents are restored to Mailbox 2. Note that Mailbox 1 itself is not created under Mailbox 2.

See Figure 6-1.

Figure 6-1   Redirecting the restore of mailbox 1 to mailbox 2

Assume that you redirect the restore of `Mailbox 1\Top of Information Store\Folder 2` to `Mailbox 2`. The contents of `Mailbox 1\Top of Information Store\Folder 2`, `Message 3`, and `Message 4`, are placed in `Mailbox 2` in the same folder as they were in `Mailbox 1`.

See Figure 6-2.

Figure 6-2   Redirecting the restore of folder 2 to mailbox 2
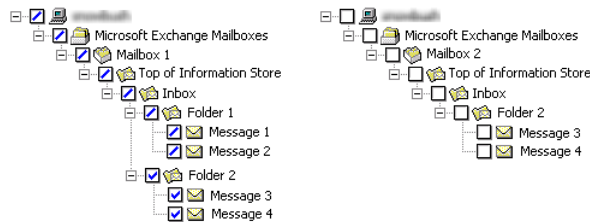
See "Redirecting the restore of an Exchange mailbox, mailbox folder, or public folder" on page 181.

See "About requirements for redirecting the restore of an Exchange mailbox or public folder object to a different path" on page 179.

See "About redirecting a restore of Exchange mailbox or public folder objects to a different path" on page 178.

Redirecting the restore of an Exchange mailbox, mailbox folder, or public folder

This topic describes how to redirect the restore of a mailbox, mailbox folder, or public folder to a different mailbox or public folder.

To redirect the restore of a mailbox, mailbox folder, or public folder

1   Log onto the server as Administrator.

2   Open the Backup, Archive, and Restore interface.

3　Click **File > Select Files and Folders to Restore > from Normal Backup**.

4　Click **File > Specify NetBackup Machines and Policy Type**.

5　In the **Specify NetBackup Machines and Policy Type** dialog box, select the server and the policy type.

6　From the **NetBackup History** pane, click the image(s) that contain the objects you want to restore. Select one of the following:

■　The last full backup

■　The last full backup and all subsequent differential backups

■　The last full backup and the last cumulative backup

You cannot restore individual items from an incremental backup that uses Granular Recovery Technology (GRT).

7　In the **All folders** or right pane, click the mailbox or public folder to restore.

8　Click **Actions > Restore**.

9 On the **Microsoft Exchange** tab, select the restore options you want.

See "Restore options for restores of Exchange Server mailbox objects or public folder objects" on page 174.
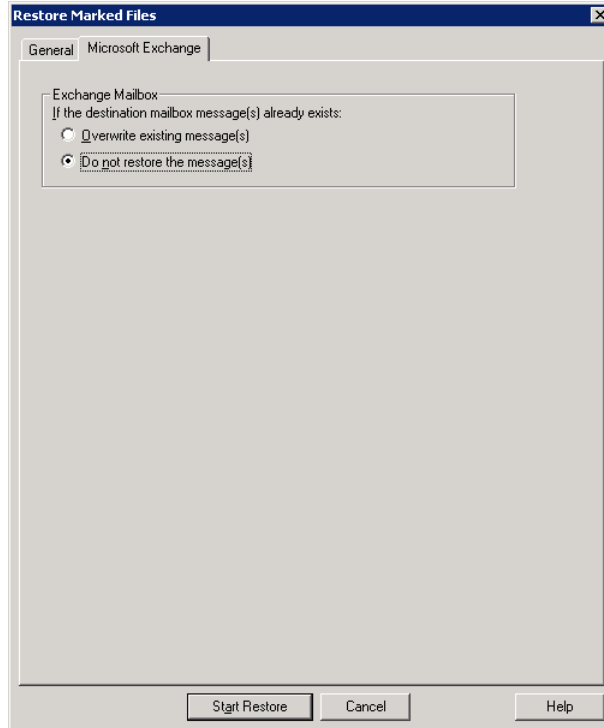
10 On the **General** tab, click **Restore everything to a different location**.

11 In the **Destination** box, indicate where you want to restore the object. You must indicate an explicit path (or full path).

- Change the mailbox name to another existing mailbox. For example, if you want to restore the contents of Mailbox 1 to Mailbox 2\Folder, specify one of the following in the **Destination** box:

```
Microsoft Exchange Database Availability Groups:\Forest or Domain\

                  Microsoft Information Store\Mailbox Database [Mailbox]\Mailbox 2\

Microsoft Information Store:\Mailbox Database\Mailbox 2\

Microsoft Information Store:\Storage Group\Mailbox Database\Mailbox 2\
```

```
Microsoft Information Store:\Storage Group\Mailbox Database\Mailbox 2\

Microsoft Exchange Mailboxes:\Mailbox 2\
```

■ When you restore public folders, change the public folder name to the folder to which you want to restore. This folder does not have to exist.

12 Click **Start Restore**.

Redirecting a restore of an Exchange mailbox or a public folder object to a different path

This topic describes how to restore a mailbox or a public folder object to a different path.

To restore a mailbox or a public folder object to a different path

1 Log onto the server as Administrator.

2 Click **File > Select Files and Folders to Restore > from Normal Backup**.

3 Click **File > Specify NetBackup Machines and Policy Type**.

4   In the **Specify NetBackup Machines and Policy Type** dialog box, select the server and the policy type.

5   From the **NetBackup History** pane, click the image(s) that contain the folder you want to restore.

Select one of the following:

■   The last full backup

■   The last full backup and all subsequent differential backups

■   The last full backup and the last cumulative backup

You cannot restore individual items from an incremental backup that uses Granular Recovery Technology (GRT).

6   In the **Contents of** or right pane, click the folders, messages, or documents to restore.

If you select items in the **All Folders** pane, you cannot redirect individual objects.

7   Click **Actions > Restore**.

8 On the **Microsoft Exchange** tab, select the restore options you want.

See "Restore options for restores of Exchange Server mailbox objects or public folder objects" on page 174.
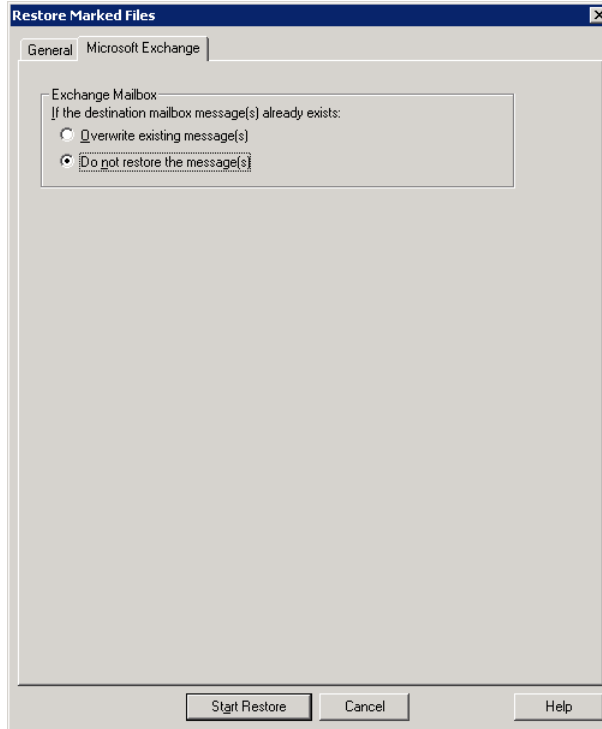
9 On the **General** tab, click **Restore individual folders and files to different locations** option.

Each row under **Restore individual folders and files to different locations** is associated with an individual folder, message, or document.

10 Double-click a row to modify the restore destination.

11 In the **New Destination** box, indicate the mailbox or folder where you want to restore the object(s).

To redirect a mailbox folder or message, the destination can be any existing mailbox or mailbox folder. To redirect a public folder or document, the destination can be a new or existing public folder. You must indicate an explicit path (or full path).

For example, consider that you want to restore the contents of `Inbox` in `Mailbox 1` to the folder `Other` in the same mailbox. Specify one of the following in the **Destination** box:

```
Microsoft Exchange Database Availability Groups:\Forest or Domain\
Microsoft Information Store\Mailbox Database [Mailbox]\Mailbox 1\Other

Microsoft Information Store:\Mailbox Database\Mailbox 1\Other

Microsoft Information Store:\Storage Group\Mailbox Database\Mailbox 1\
Top of Information Store\Other

Microsoft Exchange Mailboxes:\Mailbox 1\Top of Information Store\Other
```
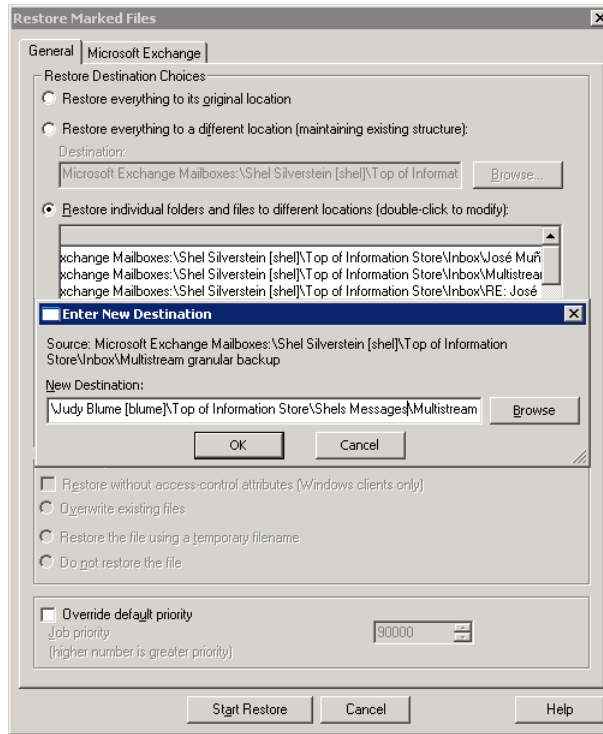
12 Click **OK**.

13 Click **Start Restore**.

See "About using the command line to browse or restore Exchange granular backup images" on page 188.

About using the command line to browse or restore Exchange granular backup images

Note the following information when you use the command line to browse or restore granular backup images:

■ When you perform a snapshot restore of mailboxes or mailbox folders, specify the file names as relative to the Microsoft Information Store or DAG and to the storage group or database.
Correct:

```
\Microsoft Database Availability Groups\My-database\John Q. Employee\
Top of Information Store\Inbox\Nancy's birthday
```

```
\Microsoft Information Store\My-database\John Q. Employee\Top of Information Store\
Inbox\Nancy's birthday
```

```
\Microsoft Information Store\My-Store-Group\My-database\John Q. Employee\
Top of Information Store\Inbox\Nancy's birthday
```

Incorrect:

```
\Microsoft Exchange Mailboxes\John Q. Employee\Top of Information Store\Inbox\
Nancy's birthday
```

- The "-granular_proxy" option is included with the `bpduplicate` command and the `bplist` command. Use the "-granular_proxy" option to specify a proxy host if one of the following situations apply:

  - You do not want to affect the source client

  - The source client is not available

  - You want to use a different proxy host than the one specified in the host properties for the source client

- If you specify a proxy host, it must have the same version of Windows as the client from which the backup is made. The proxy host also must have privileges to perform granular operations.
  See "About Exchange client and server privileges" on page 66.

The following example shows how you can specify a proxy host with the `bplist` command:

```
bplist -t 16 -k exchgranpolicy -R -s 06/09/2008 16:00:00
-granular_proxy ProxyServerA "\Microsoft Information Store\StorageGroup1\
DeptA\EmployeeA\Top of Information Store\Inbox\*"
```

More information is available on how to configure the proxy server in the client host properties.

See "Configuring the granular restore proxy host" on page 73.

About restoring Backup Exec Exchange images with NetBackup

Note that Backup Exec Tape Reader (BETR) support will be dropped after the NetBackup 7.x lifecycle. To restore Backup Exec backup images, follow the

instructions for restoring a NetBackup for Exchange image, except select **File > Select Files and Folders to Restore > from Backup Exec Backup**.

Verify that NetBackup supports the restore type of you want to perform. See the following Technote:

http://www.symantec.com/docs/TECH125836

About selecting a source client for an Exchange Server backup or restore operation

When you back up or restore from a standalone server or non-virtual environment, you do not need select or add a particular source client. However, to perform an Exchange backup or restore in a cluster or DAG environment, you select the virtual client name as the source client. NetBackup requires this configuration for backups of clusters to be successful.

Note: Note that you cannot use the Java client interface to select a virtual client or virtual DAG name for a backup operation. Instead, log on with the virtual client name or virtual DAG name.

To select a source client for an Exchange Server backup or restore operation

1   In the NetBackup Backup, Archive, and Restore interface, select **File > Specify NetBackup Machines and Policy Type**.

2   Select the source client as described in Table 6-9.

Table 6-9   Source client for an Exchange Server backup operation

To perform a backup or restore for	For Source client for restores (or virtual client for backups), select
An Exchange DAG	the DAG name. If necessary, add the virtual name to the list and then select it.
An Exchange 2007 cluster	the virtual Exchange Server name. If necessary, add the virtual name to the list and then select it.

About selecting a destination client for an Exchange Server restore operation

If you want to perform a restore to the original client that performed the backup, you do not need to change the destination client. However, it may not be possible to restore an Exchange database from a NetBackup client-only installation on a cluster. You may not be able to change the destination client value to match the virtual server name. In that case, use the Backup, Archive, and Restore interface on a NetBackup server. From the server you can change the destination client value to the virtual server name.

When you perform a restore of an Exchange backup, you can choose a different destination client to which you want to restore a backup. (This type of operation is called redirecting a restore to a different client.) Most of the Exchange objects that are backed up can be redirected to a different client. The Microsoft Exchange Information Store databases can be restored to a different Exchange server.

The following requirements must be met before you redirect the restore of databases, storage groups, or storage group databases:

■ You must have NetBackup server privileges or be logged into a server with the NetBackup Administration Console or the NetBackup Remote Administration Console.

■ The databases or the storage groups must exist on the target server.

■ (Exchange 2007 and earlier) The storage group databases must have the same names as those in the original storage group.

■ (Exchange 2007 and earlier streaming backups) The target server must have the same Organization and Administrative Group name as the source server.

The following additional limitations apply for Exchange 2003 when you redirect a snapshot restore to a different client:

■ The storage group log prefix on the target server must be the same as the prefix of the original storage group. (For example, E00.log.) You may need to create temporary storage groups so that the target storage group has the same log prefix as the original.

■ The target storage group and databases must have the same path as the original storage group and databases for the following: Exchange database, transaction logs, and system files.

To select a destination client for an Exchange Server restore operation

1   In the NetBackup Backup, Archive, and Restore interface, select **File > Specify NetBackup Machines and Policy Type**.

2   Select the destination client as described for the specific restore you want to perform:

Protecting Exchange Server data with VMware backups

This chapter includes the following topics:

- About protecting Exchange Server data with VMware backups

- About configuring NetBackup for VMware backups that protect Exchange Server

- Installing the Symantec VSS provider for vSphere

- About configuring VMware policies to protect Exchange Server

- About restoring Exchange data from a VMware backup

- Duplicating a VMware backup that protects Exchange

About protecting Exchange Server data with VMware backups

Through a VMware backup policy, NetBackup can create consistent full backups of an Exchange Server that resides on a virtual machine. To protect a supported application with a VMware policy, there is a new job or phase during the backup. An Application State Capture (ASC) job executes after the VMware discovery job and before the snapshot job(s). This ASC job contacts the NetBackup client on the guest virtual machine. The ASC job collects and catalogs application, the specific data that is needed for application recovery and granular recovery (GRT) functionality.

More information is available on the ASC job and its associated logs.

See "Limitations of using a VMware policy to protect Exchange Server" on page 195.

See "Troubleshooting VMware backups and restores of Exchange Server" on page 220.

About the Symantec VSS provider for vSphere

When the Symantec VSS provider is installed and NetBackup starts a virtual machine snapshot, VMware Tools calls the Symantec VSS provider to quiesce the VSS writers for a file-level consistent backup. If it is enabled in the policy, the Exchange VSS writer truncates the transaction logs when the VMware snapshot is complete.

Note: The Symantec VSS provider must be installed separately.

See "Installing the Symantec VSS provider for vSphere " on page 197.

Although the VSS provider in VMware Tools is suitable in many cases, it has the following deficiencies:

■ When you use the VMware 4.x VSS provider, you cannot truncate logs with the VMware backup. The VMware provider only supports copy backups.

The Symantec VSS provider is recommended instead of the VMware VSS provider in the following cases:

■ You want VMware backups to truncate the logs on Microsoft Exchange virtual machines.
   The Symantec VSS provider truncates logs for Microsoft Exchange, by means of full VSS backups.

■ The virtual machine you want to back up is a node in an Exchange 2010 DAG or an Exchange 2007 CCR. In this case, only the active copies of the database are cataloged and the log files for only those same databases are truncated.

■ You want to use an exclude file list for Exchange. See the following for details on how to configure an exclude file list for Exchange.
   See "About excluding Exchange items from backups" on page 96.

Support for VMware backups that protect Exchange Server

The following are supported with VMware backups that protect Exchange Server:

■ ESX Server 4.x or 5.0

■ Exchange Server 2010 (x64)

■ Exchange Server 2007 (x64)

■ NetBackup 7.5 server software

- NetBackup 7.5 client software is installed on the virtual machine

- Either Symantec VSS Provider or VMware VSS Provider is required. Without one of these providers, database recovery may require manual steps and granuar recovery is not supported.

  Symantec recommends the Symantec VSS provider for the virtual machines that host Exchange.

  See "Installing the Symantec VSS provider for vSphere " on page 197.

  Up-to-date support information on the Symantec VSS provider is available in the following tech note:

  Support for NetBackup 7.x in a virtual environment

- VMware backups are supported for stand-alone Exchange servers, DAGs, and CCR clusters.

- For Exchange 2010 DAG nodes or Exchange 2007 CCR nodes, only the active copies of the database are cataloged. The passive copies of the databases are not cataloged. Log files are not truncated for the passive copies as long as the Symantec VSS Provider is installed.

  For DAGs, NetBackup protects at the node level of a DAG. This behavior is different than for an agent backup, where protection is at the DAG level.

Limitations of using a VMware policy to protect Exchange Server

The following limitations exist when you configure a VMware policy to protect Exchange Server:

- VMware incremental backups of Exchange Server are not supported with this version of NetBackup.

- The Application State Capture (ASC) job fails and the databases are not protected if you do any of the following:

  - Disable the **Virtual Machine quiesce** option.

  - Select the **Exclude data disks** option.

Databases are cataloged and protected only if they exist in a configuration that is supported for VMware backups. As long as there are any databases that can be protected, the ASC job continues. If you select databases for backup that exist on supported and on unsupported disks, the ASC job produces a status 1 (partially successful). The ASC job detects these situations and the job details include the result of the backup operation.

Exchange Server databases are not cataloged and backed up if they exist on the following:

- Raw device mapping (RDMs). Make sure that the Exchange virtual machine does not use RDM as storage for databases and transaction logs.

- Virtual Machine Disk (vmdk) volumes that are marked as independent. Make sure that the Exchange databases and transaction logs are not stored on independent disks.

- Mount point volumes.

- Virtual hard disks (VHDs).
  If NetBackup detects any database objects on a VHD, the ASC job fails and no Exchange content is cataloged. This exclusion includes any objects that do not exist on the VHD.

- The ASC job detects an excluded Windows boot disk and treats it like an independent disk.
  The VMware backup cannot exclude for any reason the disk on which NetBackup is installed. For example, do not select the **Exclude boot disk** option if NetBackup is installed on the boot drive (typically C:).

See "Troubleshooting VMware backups and restores of Exchange Server" on page 220.

About configuring NetBackup for VMware backups that protect Exchange Server

Use the following steps to configure NetBackup for VMware backups that protect Exchange Server.

Table 7-1   Steps to configure VMware backups that protect Exchange Server

Step	Action	Description
Step 1	Install the Symantec VSS Provider.	See "Installing the Symantec VSS provider for vSphere " on page 197.
Step 2	Review the requirements for granular recovery.	See "Requirements to perform backups and restores of Exchange with Granular Recovery Technology (GRT)" on page 34. For Exchange 2010, configure NFS and the NetBackup Client Service on the CAS server and on any clients that are used for browsing. For Exchange 2007, configure NFS and the NetBackup Client Service on any clients that are used to browse or restore.

	Table 7-1	Steps to configure VMware backups that protect Exchange Server *(continued)*

Step	Action	Description
Step 3	Configure the client and the server privileges for granular operations.	See "About Exchange client and server privileges" on page 66.
Step 4	Configure a VMware policy that has the applicable attributes selected.	See "Configuring a VMware policy to back up Exchange Server" on page 199. See the *NetBackup for VMware Administrator's Guide*.
Step 5	For Exchange 2007, disable circular logging for all Exchange storage groups. For Exchange 2010, disable circular logging for all databases.	

Installing the Symantec VSS provider for vSphere

To use the Symantec VSS provider you must install it manually following installation of the NetBackup for Windows client. If the VMware VSS provider is installed, the installation program removes it and may require a restart of the computer.

To install the Symantec VSS provider

1   Browse to the following location:

    install_path\Veritas\NetBackup\bin\goodies\

2   Double-click on the Symantec VSS Provider for vSphere shortcut.

3   Follow the prompts.

4   When the utility has completed, restart the computer if prompted.

5   Following the restart, the utility resumes. Follow the prompts to complete the installation.

To uninstall the Symantec VSS provider

1   In the Control Panel, open **Add or Remove Programs** or **Programs and Features**.

2   Double-click on the Symantec VSS Provider for vSphere.

    The uninstall program does not automatically reinstall the VMware VSS provider.

About configuring VMware policies to protect Exchange Server

To back up an Exchange Server in a virtual machine, you configure a full backup using the **VMware** policy type. Log truncation is optional. Granular Recovery Technology (GRT) is automatically provided in the VMware backup.

Only the details specific to protecting Exchange Server are covered here. For complete details on how to create a VMware policy, see the instructions in the following document:

NetBackup for VMware Administrator's Guide

For NetBackup to successfully truncate logs after a backup, the following apply:

■ You must install the Symantec VSS provider.

■ The ASC job must detect that the Symantec VSS provider is installed.

■ The databases must be active, mounted, not in the exclude list, and protectable. See "Limitations of using a VMware policy to protect Exchange Server" on page 195.

Note the following when you configure a VMware policy for Exchange Server backups:

■ Dismounted databases are not protected.

■ You cannot configure an incremental backup of Exchange with a VMware policy. Instead, you must create an MS-Exchange-Server policy for Exchange incremental backups. If you attempt to back up Exchange with a VMware incremental policy, the Application State Capture (ASC) job fails. However, the VMware backup job is successful. Use caution if you use both a VMware policy for full backups and an Exchange policy for incremental backups. Ensure that the backups are scheduled to occur at distinct times.

■ Consistency checks of the Exchange databases are not performed with VMware backups.

■ The host properties for Exchange clients do not apply to VMware backups (for example, **Backup option for log files during full backups**).

■ Granular Recovery Technology (GRT) is always available in the VMware policy.

■ The backup history is not saved for VMware backups that protect Exchange Server. It does not apply with VMware backups because NetBackup protects only the databases whose active copy is on the virtual machine.

■ You may encounter problems if you select **VM Host Name** for the **Primary VM identifier**. When you browse for and select the virtual machine for the

VMware policy, the appropriate address or client name may not be returned. If this problem occurs, use **VMware display name** instead.

Configuring a VMware policy to back up Exchange Server

This topic describes how to configure a VMware policy to back up Exchange Server

To configure a VMware policy to back up Exchange Server

1   Create a new policy or open the policy you want to configure.

2   In the **Policy** dialog box, click the **Attributes** tab.

3   In the **Policy type** list, click **VMware**.

    For complete details on how to create a policy for Exchange Server backups in a VMware environment, see the instructions in the following document:

    NetBackup for VMware Administrator's Guide

4   On the **Clients** tab, you must add clients using a query, not manually.

    If you encounter problems using a query, try changing the **Primary VM identifier** from **VM hostname** to **VM display name**.

5   Click the **VMware** tab.

    For details on the options in this dialog box, see the following document:

    NetBackup for VMware Administrator's Guide

6   Select **Enable file recovery from VM backup**.

    This option must be enabled for application protection of Exchange Server.

7   Uncheck **Enable block-level incremental backup**.

    This option must be disabled for Exchange Server protection using a VMware backup.

8   Select **Enable Exchange Recovery**.

    This option enables recovery of the Exchange databases or mailbox messages from the virtual machine backups. If this option is disabled, you can recover the entire virtual machine from the backup, but you cannot recover the databases or mailbox messages individually.

9   (Optional) Select **Truncate logs**.

    For Exchange, this option truncates the transaction logs when the VMware snapshot of the virtual machine is complete. If you do not check **Truncate logs**, the logs are not truncated.

About restoring Exchange data from a VMware backup

The user restores Exchange data from a VMware backup in the same manner that you restore from a backup that is performed with the Exchange Agent. Though you use a VMware policy type to back up the data, you use the **MS-Exchange-Server** policy type for the restore. NetBackup displays the Exchange data in the VMware backup image that is available for restore.

Note the following when you restore Exchange from a VMware backup:

- You cannot browse or recover granular items (GRT) from GPT disks (GUID partition table).

- All the restore options are available, including the following:

  - A recovery storage group or recovery database

  - Another storage group or database
    The target server can be a virtual computer or physical computer.

  - An alternate server

When you perform a restore, it is important that you select the appropriate source or destination clients. Note the following:

- In some cases the Primary VM identifier in the VMware policy does not match the NetBackup client name that is configured for the VMware host. In this case, you must configure the client to perform a redirected restore.
  See "Configuring Exchange client and server privileges" on page 67.

- For restores of a cluster (including CCR and DAG), select the virtual Exchange server name for the source client. If the client name for the VMware backup used a fully qualified domain name (FQDN), the CCR name or DAG name is also in FQDN format.

- For restores of an Exchange stand-alone server, you must select for the source client name that NetBackup used for the VMware backup. For example, a particular Exchange Server has the real host name of `Exchangesv1`. You configure a VMware backup policy using the **VMware display name**, `Exchange_server1` and perform a backup. When you want to perform a restore, you browse for the backup using the source client name `Exchange_server1`.

- Select a destination client name that NetBackup recognizes. The destination client name must be a network name or computer name. This name must allow NetBackup to connect to the NetBackup client.

See the following topics for information on how to restore Exchange data from a VMware backup:

See "About restoring Exchange snapshot backups" on page 142.

See "About restoring individual Exchange mailbox and public folder items" on page 172.

See "About redirecting a restore of Exchange mailbox or public folder objects to a different path" on page 178.

Duplicating a VMware backup that protects Exchange

You cannot duplicate a VMware backup that protects Exchange through the NetBackup Administration Console. Use following command to generate a full Exchange catalog with granular information for the image:

```
bpduplicate -bc_only
```

Note that the mailbox user name is not cataloged with a VMware backup that protects Exchange.

If you use a granular proxy server with the bpduplicate command, the information for Exchange client and server privileges applies.

See "About Exchange client and server privileges" on page 66.

See "Configuring the granular restore proxy host" on page 73.

Recovering an Exchange database to a repaired or an alternate Exchange server

This chapter includes the following topics:

- About recovery of Exchange databases
- Recovering an Exchange database

About recovery of Exchange databases

Table 8-1 describes the steps to recover an Exchange database.

Table 8-1   Recovering Exchange databases

Step	Action	Description
Step 1	Repair the Exchange server or create an alternate Exchange server	If you need to recover an Exchange database, you can restore it to a repaired Exchange server or to an alternate Exchange server. For instructions on performing a diaster recovery of an Exchange server, see Table 8-2.
Step 2	Recover the Exchange database.	See "Recovering an Exchange database" on page 204.

	Table 8-1	Recovering Exchange databases *(continued)*
Step	**Action**	**Description**
Step 3	Extract mailbox or public folder data to the server.	After you restore to an alternate server, you then can extract mailbox or public folder data to that server. The following Technote explains how to configure an alternate server for restore operations: http://www.symantec.com/docs/TECH29816

Table 8-2 describes the resources available that describe how to recover an Exchange database.

	Table 8-2	Instructions for performing a diaster recovery of an Exchange server
Exchange 2010	http://technet.microsoft.com/en-us/library/dd876880(EXCHG.140).aspx	
Exchange 2007	http://technet.microsoft.com/en-us/library/aa998848.aspx	
Exchange 2003	*Exchange 2003 Disaster Recovery Operations Guide*	
	http://technet.microsoft.com/en-us/library/bb125070.aspx	
All versions of Exchange	www.microsoft.com/exchange	

See "Recovering an Exchange database" on page 204.

See "Prerequisites and operational notes for restoring Exchange individual mailboxes, mailbox folders, public folders, or messages" on page 173.

See "About restoring Exchange database data" on page 139.

Recovering an Exchange database

To recover an Exchange database

1   On an alternate or a repaired Exchange server, create databases (Exchange 2010) or storage groups (Exchange 2007 and earlier) that match the original databases or storage groups.

    You can use the Backup, Archive, and Restore interface on the master to view the correct logical names of the databases or storage groups you want to recover.

2   Mount and dismount each database store you want to restore.

    This action creates the data files NetBackup requires for restore.

3   Right-click the database store and click **Properties**.

4   On the **Database** tab, click **This database can be overwritten by a restore**.

5   Install the NetBackup client software on the alternate or the repaired Exchange server.

6   On the master server, open the Backup, Archive, and Restore interface.

7   Click **File > Specify NetBackup Machines and Policy Type**.

8   In the **Specify NetBackup Machines and Policy Type** dialog box, specify the following:

Server to use for backups and restores	Select the NetBackup server that performed the backup.
Source client for restores	Select the client from which the backup was performed. For a clustered or DAG environment, this client is the virtual DAG name or the virtual cluster name.
Policy type for restores	Select **MS-Exchange-Server**.
Destination clients for restores	Select the client where you want to direct the restore. This client is either the alternate or the repaired Exchange server.

9   Click **OK**.

10 Restore the databases and transaction logs.

See "Restoring storage groups or storage group databases from a streaming backup" on page 166.

11 Reconnect the mailboxes you recovered to their Active Directory user accounts.

12 If you recovered to an alternate Exchange server, Symantec recommends you restore mailbox data from a backup that used Granular Recovery Technology (GRT).

You can also use a third party tool such as EXMerge to move individual items from an alternate database or an RDB or RSG.

See the Microsoft Web site for more information about EXMerge.

See "About recovery of Exchange databases" on page 203.

See "Prerequisites and operational notes for restoring Exchange individual mailboxes, mailbox folders, public folders, or messages" on page 173.

See "About restoring Exchange database data" on page 139.

Troubleshooting backups and restores of Exchange Server

This chapter includes the following topics:

- **About NetBackup for Exchange debug logging**

- **Viewing Event Viewer logs on an off-host Exchange server**

- **About NetBackup status reports**

- **Exchange Server transaction log truncation errors**

- **Troubleshooting LCR, CCR, and Database Availability Group (DAG) recovery**

- **Troubleshooting an Exchange mailbox operation with a status 5 error with bprestore**

- **Dynamic enforcement of path length limit for Exchange backups and restores**

- **Troubleshooting Exchange snapshot operations**

- **Troubleshooting Exchange jobs that use Granular Recovery Technology (GRT)**

- **About concurrent restore of multiple storage groups**

- **Increased memory usage with Exchange 2010**

- **Finding the virtual Database Availability Group (DAG) node**

- **Displaying and resetting the Backup Status for a Database Availability Group (DAG)**

- Configuring the log on account for the NetBackup Legacy Network Service for Exchange 2010 database restores and restores that use Granular Recovery Technology (GRT)

- Troubleshooting VMware backups and restores of Exchange Server

About NetBackup for Exchange debug logging

The NetBackup master server and client software offers a comprehensive set of debug logs for troubleshooting problems that can occur during NetBackup operations. Debug logging is also available for Exchange Server backup and restore operations.

See the following topics for information on how to create the logs and how to control the amount of information written to the logs.

See "Enabling the debug logs for a NetBackup for Exchange client automatically" on page 208.

See "Debug logs for NetBackup for Exchange backup operations" on page 209.

See "Debug logs for NetBackup for Exchange restore operations" on page 210.

See "Setting the debug level on a NetBackup for Exchange Windows client" on page 212.

After you determine the cause of the problem, disable debug logging by removing the previously created debug logging directories. Details are available on the contents of these debug logs.

See the *NetBackup Troubleshooting Guide*.

Additional information about NetBackup client logs and NetBackup master server logs is available.

See the online help for the Backup, Archive, and Restore interface.

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

Note: When debug logging is enabled, the files can become large. The same files are used by normal file backups.

Enabling the debug logs for a NetBackup for Exchange client automatically

You can enable debug logging by running a batch file that creates each log directory. To create all log file directories automatically, run the following:

install_path\NetBackup\logs\mklogdir.bat

Debug logs for NetBackup for Exchange backup operations

After you perform a backup, debug logging information is placed in the *install_path*\Netbackup\logs directory. A subdirectory is created for each process. The debug log file is named *mmddyy*.log.

For details on logging, see the *NetBackup Troubleshooting Guide*.

Snapshot backups	Refer to the following logs:
	
	■ bpbkar
	  For off-host backups, the bpbkar log exists on the alternate client.
	■ bpfis
	  For off-host backups, the bpfis log exists on the alternate client and the primary client

Backups that use GRT	Refer to the following logs: ■ bpbkar ■ nbfsd This log appears on the client and the media server.
VMware backups	Refer to the following logs: ■ bpbkar ■ bpfis ■ ncfnbcs For ASC issues and failures, this log is created on the VM that is backed up.

Exchange 2010 backups	Refer to the following logs:
	
	■ bpbkar
	■ bpresolver
	  This log is written to the DAG node. To determine the active node, see the following:
	  See "Finding the virtual Database Availability Group (DAG) node" on page 218.

Mailbox(MAPI) backups	Refer to the following logs: ■ beds This log is used mailbox and public folder backups using MAPI. ■ bpbkar

See "About installing the Exchange System Management Tools on the remote server" on page 213.

Debug logs for NetBackup for Exchange restore operations

After you perform a restore, debug logging information is placed in the *install_path*\Netbackup\logs directory. A subdirectory is created for each process. The debug log file is named *mmddyy*.log. For legacy logging, the file is named *mmddyy*.log. For unified logging, the log file is in a format that is standardized across Symantec products.

For details on both unified and legacy logging, see the *NetBackup Troubleshooting Guide*.

All restores, except those with Granular Recovery Technology (GRT)	tar
Restores with GRT	Refer to the following logs: ■ beds ■ nbfsd 　This log appears on the client and the media server. ■ ncflbc 　This log is for nblbc.exe. It appears on the destination client or proxy client. ■ ncfgre 　This log is for nbgre.exe. It appears on the destination client.
Instant Recovery and off-host Instant Recovery	Refer to the following logs: ■ bpbkar 　For off-host Instant Recovery restores, bpbkar logs on the alternate client. ■ bpfis 　This log applies to Instant Recovery rollback restores. For off-host Instant Recovery restores, bpfis logs exist on both the primary and the alternate clients. ■ bppfi 　For off-host Instant Recovery restores, bppfi logs on both the primary and the alternate clients. ■ tar 　For off-host Instant Recovery, this log appears on the primary client.

Exchange 2010 restores	Refer to the following logs:
	■ bpbkar
	■ bpresolver
	This log is written to the DAG node. To determine the active node, see the following:
	See "Finding the virtual Database Availability Group (DAG) node" on page 218.
Restores from VMware backups	Refer to the following logs:
	■ bpbkar
	■ bppfi
	■ tar
Mailbox (MAPI) restores	Refer to the following logs:
	■ beds
	This log applies to mailbox and public folder restores with MAPI.
	■ tar

See "Exchange Server transaction log truncation errors" on page 214.

Symantec VSS provider logs

The Symantec VSS provider records its activities in Windows event logs. Debug logs are also available at the following locations:

```
\Program Files\Symantec\Backup Exec\BE VSS provider\logs
```

```
\Program Files\Symantec\Backup Exec\Windows\logs
```

To increase the log debug level modify both the pre-freeze-script.bat and post-thaw-script.bat files. Add the -log parameter to the script, at the line where BeVssRequestor.exe is called. VMware determines which script is invoked.

To increase the debug level, change the following line in the pre-freeze-script.bat:

```
BeVssRequestor.exe -pre2 -logscreen !SkipExReplica! !SkipSQL!
!VMBackupType! !ExcludeList!
```

to:

```
BeVssRequestor.exe -pre2 -logscreen !SkipExReplica! !SkipSQL!
!VMBackupType! !ExcludeList! -log
```

Also change the following line in the post-thaw-script.bat:

```
BeVssRequestor.exe -post2 -logscreen !SkipExReplica! !SkipSQL!
!VMBackupType! !ExcludeList!
```

to:

```
BeVssRequestor.exe -post2 -logscreen !SkipExReplica! !SkipSQL!
!VMBackupType! !ExcludeList! -log
```

Setting the debug level on a NetBackup for Exchange Windows client

To control the amount of information that is written to the debug logs, change the General, Verbose, and Database debug levels on the client(s). Typically, the default value of 0 is sufficient. However, technical support may ask you to set the value higher to analyze a problem.

The debug logs are located in *install_path*\NetBackup\logs.

To set the debug level on a NetBackup for Exchange client

1   From the Windows Start menu, choose **Programs > Symantec NetBackup > Backup, Archive, and Restore**.

2   Select **File > NetBackup Client Properties**.

3   Click the **Troubleshooting** tab.

4   Set the **General** debug level.

    Set this level as high as 2.

5   Set the **Verbose** debug level.

    Set this level as high as 5.

6   Click **OK** to save your changes.

Viewing Event Viewer logs on an off-host Exchange server

During the verification of an off-host backup, Exchange Server logs messages on the off-host server. These logs are helpful if you need to troubleshoot the verification stage of the backup. The application event logs are used for Exchange snapshot backup and restores and for consistency checks. If Exchange Server is not installed on the remote server, you cannot view the details of these logs.

You can view the logs on the remote server in one of the following ways:

- See "Connecting to the remote Exchange server from within Event Viewer" on page 213.

- See "About installing the Exchange System Management Tools on the remote server" on page 213.

See "Debug logs for NetBackup for Exchange backup operations" on page 209.

Connecting to the remote Exchange server from within Event Viewer

You can view the logs on the remote server by opening Event Viewer on a server that has Exchange Server installed. Then connect to the remote computer (the server that performed the off-host backup).

To connect to the remote server from within Event Viewer

1   Log in to a server that has Exchange Server installed.

2   Open the Event Viewer.

3   Click **Actions > Connect to another computer**.

4   In the Select Computer dialog box, click **Another computer**.

5   Type the name of the remote server or click **Browse** to select the server.

6   Click **OK**.

7   In the left-hand pane, click Application to view the Exchange logs related to the off-host backup.

See "Viewing Event Viewer logs on an off-host Exchange server" on page 212.

See "Debug logs for NetBackup for Exchange backup operations" on page 209.

About installing the Exchange System Management Tools on the remote server

To install the Exchange System Management Tools, refer to the following articles:

■   On the Microsoft Support Web site, refer to article 834121:
    http://support.microsoft.com

■   On the Microsoft TechNet Web site, refer to the Administration Guide for Exchange Server 2003:
    http://technet.microsoft.com

See "Debug logs for NetBackup for Exchange backup operations" on page 209.

About NetBackup status reports

NetBackup provides many standard status reports to verify the completion of backup and restore operations. In addition, users and the administrator can set up additional reports if a site requires them.

The administrator has access to operational progress reports through the NetBackup Administration Console. Reports can be generated for Status of Backups, Client Backups, Problems, All Log Entries, Media Lists, Media Contents, Images on Media, Media Logs, Media Summary, and Media Written. These reports can be generated for a specific time frame, client, or master server.

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

Progress reports on the client allow easy monitoring of user operations. When reports are created by the NetBackup client for each user-directed backup or restore operation, administrators can monitor these operations and detect any problems that may occur.

See "Viewing the progress report of a NetBackup for Exchange operation" on page 214.

Viewing the progress report of a NetBackup for Exchange operation

This topic describes how to view the progress report of a NetBackup for Exchange backup or restore operation.

To view the progress report of a NetBackup for Exchange operation

1   Choose **File** > **View Status**.

2   Click the task for which you want to check the progress.

3   Click **Refresh**.

    More information is available on progress reports and the meaning of the messages.

    See the *NetBackup Backup, Archive, and Restore Getting Started Guide*.

Exchange Server transaction log truncation errors

The Exchange server deletes transaction logs after a successful backup (for full and differential backup types). If the Exchange server encounters any errors during the deletion process, it logs this information in the application event log. Since the actual backup was successful, NetBackup exits with a status 0 (successful backup). Refer to the Microsoft Exchange Server documentation for information on any errors that are encountered with the transaction logs.

Troubleshooting LCR, CCR, and Database Availability Group (DAG) recovery

If you restore a backup which included only uncommitted logs, Exchange may report an error similar to the following:

```
Event Type:     Error
Event Source:   MSExchangeRepl
Event Category: Service
Event ID:       2059
```

Refer to the following Technote for information on how to resolve this issue:

http://www.symantec.com/docs/TECH88101

Troubleshooting an Exchange mailbox operation with a status 5 error with bprestore

If you start an Exchange mailbox restore operation with the bprestore command and encounter a status 5 error, check that the path is correct. The bplist command does not properly escape the "[" and "]" characters.

For example, bplist returns the following path for a mailbox:

```
/Microsoft Information Store/SG1/Mailbox1/backrest100 [backrest100]/
```

Instead, edit the path so it appears as follows:

```
/Microsoft Information Store/SG1/Mailbox1/backrest100 \[backrest100\]/
```

Dynamic enforcement of path length limit for Exchange backups and restores

The *NetBackup Administrator's Guide for Windows, Volume I* details that files and directories with path lengths greater than 1023 are automatically excluded from backups. For Exchange MAPI mailbox backups and for GRT-enabled backups, the path length limit applies to individual mailbox folders and messages. When a legacy mailbox backup encounters an item that exceeds the limit, the backup job reports a final status of 1. This status indicates that some items were not backed up, and the job details tell you which items were skipped. For granular backups NetBackup checks the pathname length limit and reports exceptions, during browsing and restoring of the granular backup image. It logs the pathnames

that exceed the limit in the unified logging `ncflbc` or `ncfgre` logs. Then it reports the items that were skipped during restore to the **View Status** window.

Troubleshooting Exchange snapshot operations

Note the following when you perform Exchange snapshot backup or restore operations:

- If you want to restore a snapshot backup from a multiplexed tape, restore the entire storage group. If you attempt to restore a single database from a storage group that contains multiple databases, the restore may fail. This issue will be fixed in a future release.

- If you want to restore from a snapshot image, the restore fails if an `Exxrestore.env` file exists in the transaction log folder for the database or the storage group. This temporary Exchange file can be left from a previously failed restore. A Windows application event log entry from Exchange tells you that this file is the problem. Remove this file manually before you attempt another restore.

- When you launch an Exchange off-host backup from the Backup, Archive, and Restore interface or from a node in a DAG, the progress log window does not display the usual progress messages as when a scheduled backup is executed. This lack of progress logging does not affect the backup operation. If you want detailed progress, use the NetBackup Administration Console to launch a manual backup operation of the Exchange policy.

Troubleshooting Exchange jobs that use Granular Recovery Technology (GRT)

Note the following when you use NetBackup to perform backup or restore operations using Granular Recovery Technology:

- Disable or uninstall Qlogic San Surfer software. It may conflict with the port mapper for Client for NFS.

- Before you install NFS on the media server or client(s), look for the ONC Portmapper service. If it exists, stop it and disable it. Otherwise, the installation of NFS Services for Windows fails.

- A status 1 error may occur for a GRT-enabled backup if the granular processing operations failed to complete successfully. The job details under the Activity

Monitor or error log should indicate if this failure is what caused the status 1. Do the following:

- Look at the bpbkar debug log for more information.

- A streaming backup still truncates transaction logs if the job ended with a status 1 because of a granular processing operation failure. In this situation, the backup image is suitable for database recovery.

- NetBackup must be able to contact the proxy client or destination client. If NetBackup cannot contact this client, then errors appear in the "Problems" or "All Log Entries" reports. The following error messages appear in the NetBackup error logs:

```
The granular proxy <clientname> for client <clientname> could not be
contacted.  Unexpected results may have occurred.  See bprd debug log for more
details.

Could not connect to <clientname> for virtual browse operation, errno=#,
bpcd_status=#
```

See "About Exchange client and server privileges" on page 66.

- Technical Support may want nbfsd logs from the media server. Use the Verbose setting carefully as the nbfsd log can grow very large.

About concurrent restore of multiple storage groups

When you use multiple backup streams, for example, one stream for each storage group, only the last storage group restored from the last restore job is properly mounted. Recovery of the remaining storage groups is not complete.

Take one of these corrective actions:

- If you want to restore from a snapshot backup, simply mount the unmounted storage groups.

- If you want to restore from a legacy (non-snapshot) backup, restore the logs from the last backup set for each storage group individually.

To avoid these steps, you can also restore the storage groups individually in separate restore operations.

Increased memory usage with Exchange 2010

As you increase the number of mailbox users with Exchange 2010, `MONAD.EXE` uses more memory during backup operations. Symantec is working with Microsoft to fix this problem.

Finding the virtual Database Availability Group (DAG) node

Finding the virtual Database Availability Group (DAG) node

1   Start **Programs > Administrative Tools > Failover Cluster Management** on one of the Exchange DAG servers.

2   In the left pane, select the DAG.

3   In the right pane, under **Summary of Cluster**, locate **Current Host Server**.

This server is where the virtual DAG resides.

Displaying and resetting the Backup Status for a Database Availability Group (DAG)

Use the following commands to display and reset the Backup Status for a DAG. More information is available about how the Backup Status is used to choose the node from which to perform the backup.

See "Backup status for Exchange Database Availability Groups (DAGs) and the preferred server list" on page 112.

Note: `-EXDB` is case sensitive

To display the Backup Status database, enter one of the following commands from the NetBackup master server:

```
bpclient -client host_name -EXDB
```

```
bpclient -All -EXDB
```

where *host_name* is the name of the DAG. The output from this command is as follows:

```
EX_DB: DAG_DB3    EX_SRVR: EXSRV3    EX_TIME: 1259516017   EX_COUNT: 1   EX_STATUS: 156
EX_DB: DAG_MBOX7 EX_SRVR: EXSRV3    EX_TIME: 1259516040   EX_COUNT: 2   EX_STATUS: 0
EX_DB: EXCHDB001 EX_SRVR: EXSRV2    EX_TIME: 1259516018   EX_COUNT: 1   EX_STATUS: 0
```

Note: `-exdb` is case sensitive

To reset the Backup Status database for a particular Exchange database, enter the following command:

```
bpclient -client host_name -update
-exdb <db_name:server_name[:timestamp:count:status]>
```

For example:

```
bpclient -client DAG_Name -update -exdb DAG_DB3:EXSRV1:0:0:0
```

Configuring the log on account for the NetBackup Legacy Network Service for Exchange 2010 database restores and restores that use Granular Recovery Technology (GRT)

By default, the NetBackup Legacy Network Service uses "Local System" account to log on. With this configuration, you may experience a status 5 error: `rai_resolvePathName: Server failed to be found`. In this case, a different account is required so NetBackup has the necessary local system privileges to perform Exchange 2010 database and GRT restores.

Change the log on account to the Windows domain account that you specified for the NetBackup Client Service.

Note: For Exchange 2010, perform the steps on each database node in the DAG and the CAS server.

To configure the log on account for the NetBackup Legacy Network Service

1 Open the Windows Services application.

2 Double-click on the **NetBackup Legacy Network Service** entry.

3 Click on the **Log On** tab.

4 Provide the name account that you specified for the NetBackup Client Service.

   See "Configuring the log on account for the NetBackup Client Service for NetBackup for Exchange on Windows" on page 60.

   The account must include the domain name, followed by the user account, *domain_name\account*. For example, **recovery\netbackup**.

5 Type the password.

6 Click **OK**.

7 Stop and start the NetBackup Legacy Network Service.

8 Close the Services control panel application.

Troubleshooting VMware backups and restores of Exchange Server

One Application State Capture job is created per VM, regardless of which applications are selected in policy.

Note the following when you perform VMware backups that protect applications:

- If the ASC job fails, the VMware snapshot or backup continues. Application-specific data cannot be restored.

- Failure results in the discovery job or parent job exiting with status 1.

- ASC messages are filtered to the ASC job details.

- If you enable recovery for a particular application but that application does not exist on the VM, the ASC job returns Status 0.

- Details on the ASC job can be found in the Activity monitor job details.

- If neither the Symantec nor the VMware VSS Provider is installed at the time of backup, the Exchange databases are not quiescent. In this case, the recovery of an Exchange database after it is restored may require manual steps using the Exchange `ESEUTIL` utility.

- `bpfis` is executed and simulates a VSS snapshot backup. This simulation is required to gain logical information of the application.

Index