Veritas NetBackup™ for Microsoft Exchange Server Administrator's Guide

for Windows

Release 8.1

VERITAS™

Veritas NetBackup™ for Microsoft Exchange Server Administrator's Guide

Last updated: 2017-09-25

Legal Notice

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

Technical Support

Technical Support maintains support centers globally. All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policies. For information about our support offerings and how to contact Technical Support, visit our website:

https://www.veritas.com/support

You can manage your Veritas account information at the following URL:

https://my.veritas.com

If you have questions regarding an existing support agreement, please email the support agreement administration team for your region as follows:

Worldwide (except Japan)	CustomerCare@veritas.com
Japan	CustomerCare_Japan@veritas.com

Documentation

Make sure that you have the current version of the documentation. Each document displays the date of the last update on page 2. The latest documentation is available on the Veritas website:

https://sort.veritas.com/documents

Documentation feedback

Your feedback is important to us. Suggest improvements or report errors or omissions to the documentation. Include the document title, document version, chapter title, and section title of the text on which you are reporting. Send feedback to:

NB.docs@veritas.com

You can also see documentation information or ask a question on the Veritas community site:

http://www.veritas.com/community/

Veritas Services and Operations Readiness Tools (SORT)

Veritas Services and Operations Readiness Tools (SORT) is a website that provides information and tools to automate and simplify certain time-consuming administrative tasks. Depending on the product, SORT helps you prepare for installations and upgrades, identify risks in your datacenters, and improve operational efficiency. To see what services and tools SORT provides for your product, see the data sheet:

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Contents

Chapter 1

Introducing NetBackup for Exchange

This chapter includes the following topics:

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. By default, NetBackup provides protection of the active databases in a DAG. You can restore Exchange databases and individual database objects from a VMware image. NetBackup provides support for VMware policies that use Replication Director to manage snapshots and snapshot replicas (storage lifecycle policy).
Exchange standalone server and DAG support	NetBackup for Exchange supports backups of Exchange standalone servers and Database Availability Groups (DAGs). VSS is the only backup Microsoft supports for Exchange 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 effect is reduced on the active Exchange server. NetBackup accesses the replicated data and leaves the active (or live) Exchange server alone. NetBackup can back up the passive copy on a specific server, based on the list of preferred servers.
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 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 Exchange backups and restores 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 96.
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 45.
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	Backups can be restored to another database on the local server or on a different server.
Redirection to the recovery database (RDB)	Backups can be redirected to the recovery database.
Support for NetBackup Accelerator with VMware backups	NetBackup Accelerator can potentially increase the speed of full VMware backups. By reducing the backup time, it is easier to perform the VMware backup within the backup window. Accelerator support for Exchange currently restricts backups to the full schedule type. This restriction also exists for a VMware backup that protects Exchange without Accelerator.

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

Feature	Description
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	The encryption feature 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 clustered Exchange servers; however, the agent is not cluster-aware. For information on the cluster solutions that are supported with Exchange Server, refer to your Exchange documentation.
Multi-tenant environments	Backup and recovery of Exchange Server databases are fully supported in a multi-tenant environment. NetBackup does not support restoring mailbox items into tenant mailboxes in a multi-tenant Exchange environment. To recover items pertaining to a tenant mailbox, redirect the recovery to a non-tenant mailbox.

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.
Microsoft consistency check API	Refers to the Microsoft CHKSGFILS API or interface.
Account for NetBackup Exchange operations	An Active Directory user account that is associated with a unique Exchange mailbox that has sufficient roles or group memberships to perform backups and restores.
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 nbtar images. This process is used with a client for 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”.

Table 1-2 NetBackup for Exchange terminology *(continued)*

Term	Definition or description
Snapshot	Refers to backups and restores performed with snapshot technology. In the NetBackup for Exchange Server documentation, “VSS” is synonymous with “snapshot”.
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”.

Chapter 2

Installing NetBackup for Exchange

This chapter includes the following topics:

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" on page 16.
Step 2	Verify the Exchange software requirements for NetBackup for Exchange.	See "Exchange server software requirements for NetBackup for Exchange" on page 18.

Table 2-1 Installation steps for NetBackup for Exchange *(continued)*

Step	Action	Description
Step 3	Verify NetBackup software requirements for NetBackup for Exchange.	See "NetBackup server requirements for NetBackup for Exchange" on page 16. See "NetBackup client requirements for NetBackup for Exchange" on page 17.
Step 4	For snapshot operations, verify the requirements for this type of backup.	See "Snapshot Client configuration and licensing requirements for Exchange snapshot backups" on page 18.
Step 5	Verify that master server has a valid license for NetBackup for Exchange and any NetBackup options or add-ons that you want to use.	See "About the license for NetBackup for Exchange" on page 19.

Verifying the operating system and platform compatibility

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 following webpage:

   http://www.netbackup.com/compatibility

2. In the list of documents, click on the following document:

   Application/Database Agent Compatibility List

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

   Snapshot Client Compatibility List

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

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

NetBackup server requirements for NetBackup for Exchange

To use the new features that are included with the NetBackup for Exchange Agent in NetBackup 8.1, you must upgrade your NetBackup for Exchange clients to

NetBackup 8.1. The NetBackup media server must use the same version as the NetBackup for Exchange client or a higher version than the client.

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.

NetBackup client requirements for NetBackup for Exchange

This topic describes where you need to install the NetBackup client and the version required to perform backups of Exchange server.

- To use the new features that are included in NetBackup for Exchange in NetBackup 8.1, you must upgrade your NetBackup for Exchange clients to NetBackup 8.1. The NetBackup media server must use the same version as the NetBackup for Exchange client or a higher version than the client.
- Install the NetBackup client software on the following:
  - The Exchange mailbox servers, or on all VMs that are Exchange mailbox servers
  - If you plan to use Granular Recovery Technology (GRT), install the NetBackup client on any mailbox servers that perform browse or restore operations.
  - Each node in the Exchange cluster or DAG
  - (Non-VMware backups) Any off-host clients
- For VMware operations, when you upgrade the client software you must install the latest version of the Veritas VSS provider. If you have an existing version of the provider, you must first uninstall the old 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 NetBackup software requirements for the Exchange server, see the following:
  See "NetBackup server requirements for NetBackup for Exchange" on page 16.
  See "NetBackup client requirements for NetBackup for Exchange" on page 17.
- If you plan to perform a VMware backup that protects Exchange, Granular recovery (GRT) is not supported if the Exchange data resides on a GPT (GUID partition table) disk.
- The Exchange Server does not need to be installed on the off-host client.

Snapshot Client configuration and licensing requirements for Exchange snapshot backups

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

- Confirm that the type of snapshot you want to configure is supported for your Exchange environment. See the following compatibility list:
  Snapshot Client Compatibility List
- 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 supported software level.
- The following snapshot options or Exchange configurations require a separate Snapshot Client license:
  - Instant recovery
  - Off-host backups
  - Backups using a hardware provider

  A Snapshot Client license is not required for any Exchange snapshot backups that use the Microsoft default provider or SFW.

- Additional installation requirements apply for Instant Recovery and off-host backups.
  See "Requirements for Exchange off-host backups" on page 19.
  See "Requirements for Exchange Instant Recovery backups" on page 19.
- If you want to restore individual items from database backups (granular recovery), additional installation requirements apply and other configuration is necessary.
  See "Configuring an Exchange backup that uses Granular Recovery Technology (GRT) (non-VMware backups)" on page 51.

Requirements for Exchange off-host backups

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

- Exchange does not need to be installed on the off-host client.
- For consistency checks of Exchange with the Microsoft consistency check API, Veritas 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 alternate client, you must install the VC9 run-time 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:
  See "Consistency checks on Exchange snapshot backups" on page 97.
  See "About consistency checks options for an Exchange backup" on page 27.
- For Instant Recovery off-host backups, see the following requirements:
  See "Requirements for Exchange Instant Recovery backups" on page 19.

Requirements for Exchange Instant Recovery backups

Instant Recovery backups require Storage Foundations for Windows (SFW) 5.1 SP1 if you use the SFW VSS provider.

About the license for NetBackup for Exchange

The NetBackup for Exchange agent is installed with the NetBackup client software. No separate installation is required. A valid license for the agent must exist on the master server.

More information is available on how to add licenses.

See the NetBackup Administrator's Guide, Volume I.

For a NetBackup cluster, a valid license for NetBackup for Exchange must exist on each node where NetBackup server resides.

Chapter 3

Configuring Exchange client host properties

This chapter includes the following topics:

Configuring Exchange client host properties

In the Exchange client host properties you configure settings for the Exchange clients you selected. The options available in this dialog box are based on the version of NetBackup installed on the client system. If you do not see all of these options after upgrading your client, close the NetBackup Administration Console and reopen it.

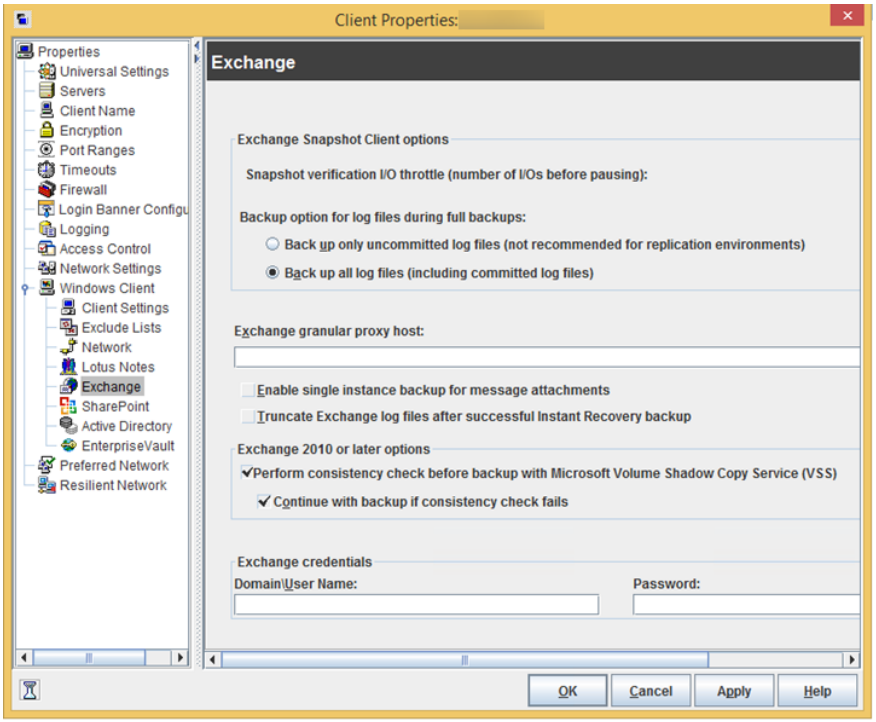
To configure Exchange client host properties

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.

   If the client does not appear in the list, click **Actions > Configure Client**.

   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 DAG host server is updated.

4. Click **Actions > Properties**.
5. Expand **Windows Client** and click **Exchange**.



6 Enable the options you want.

See "Exchange properties" on page 23.

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 DAG host server is updated.

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

Table 3-1 Exchange dialog box properties

Property	Description
Snapshot verification I/O throttle	This property only applies to **MS-Exchange-Server** backup policies with Exchange 2007. This version of Exchange is no longer supported.
Backup option for log files during full backups	**Note:** This property only applies to **MS-Exchange-Server** backup policies. Choose which logs to include with snapshot backups: ■ **Back up only uncommitted log files** ■ **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 25.
Truncate log after successful Instant Recovery backup	**Note:** This property only applies to **MS-Exchange-Server** backup policies. 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 27.

Table 3-1 Exchange dialog box properties *(continued)*

Property	Description
Exchange granular proxy host	**Note:** This property applies when you duplicate or browse a backup that uses Granular Recovery Technology (GRT). You can specify a different Windows system to act as a proxy for the source client when you duplicate or browse a backup (with `bplist`) that uses GRT. Use a proxy if you do not want to affect the source client or if it is not available. See "Configuring the Exchange granular proxy host" on page 25. See "Exchange granular clients and non-VMware backups " on page 47. See "Exchange granular clients and VMware backups" on page 49.
Enable single instance backup for message attachments	**Note:** This property only applies to **MS-Exchange-Server** backup policies with Exchange 2007. This version of Exchange is no longer supported.
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 a 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 backup" on page 27.
Exchange credentials	Note the following for this property: ■ This property applies to **MS-Exchange-Server** and **VMware** backup policies with Exchange recovery. ■ For Exchange 2013 and later, you must configure this property if you want to use GRT. Provide the credentials for the account for NetBackup Exchange operations. This account must have the necessary permissions to perform Exchange restores. The permissions that are required depend on the Exchange version that you have. The account also needs the right to "Replace a process level token." See "About the Exchange credentials in the client host properties" on page 28. See "About configuring the account for NetBackup Exchange operations" on page 30. See "About configuring the account for NetBackup Exchange operations with the right to Replace a process level token" on page 36.

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.

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 article:

http://www.veritas.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 Exchange client host properties” on page 21.

Configuring the Exchange granular 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 or browse a backup (with `bplist`) that uses GRT. Alternatively, you can specify a different Windows system to act as a proxy for the source client.

Specify a proxy host for a duplication or browse operation 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

An Exchange granular proxy host has the following requirements:

- Has the same NetBackup version as the Exchange hosts
- Uses the same NetBackup master server as the Exchange hosts
- Is included in the Exchange hosts
  You only need to add the proxy host to the list of Exchange hosts if the proxy host is not a NetBackup master or a media server.

The "-granular_proxy" option is included with the `bpduplicate` command and the `bplist` 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 149.

NetBackup determines the granular proxy host in the following order:

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

To specify a proxy, configure the **Exchange granular proxy host** in the Exchange properties for the client. More information is available about how to configure the client host properties.

See "Configuring Exchange client host properties" on page 21.

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 27.

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

See "Configuring Exchange client host properties" on page 21.

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.

About consistency checks options for an Exchange backup

By default, NetBackup is configured to run a consistency check on Exchange 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 a 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 topics:

See "Configuring Exchange client host properties" on page 21.

About the Exchange credentials in the client host properties

The Exchange credentials in the client host properties indicate the account that has necessary permissions to perform Exchange restores. The permissions that are required depend on the Exchange version that you have.

See the following topics:

See "Creating a privileged NetBackup user account for EWS access" on page 32.

See "Creating a minimal NetBackup account for Exchange operations" on page 33.

Note the following:

- The account that you configured for the **Exchange credentials** must also have the right to "Replace a process level token."
  See "About configuring the account for NetBackup Exchange operations with the right to Replace a process level token" on page 36.
- For database restores from VMware backups, the Exchange credentials that you provide must have permissions to restore VM files.
- If you want to restore from a VMware snapshot copy that was created with Replication Director, do the following:
  - Provide the Exchange credentials in the **Domain\user** and **Password** fields.
  - Configure the NetBackup Client Service with an account that has access to the CIFS shares that are created on the NetApp disk array.
- If you specify the minimal NetBackup account for the Exchange credentials in the client host properties, NetBackup can back up only active copies of the Exchange databases. If you select **Passive copy only** in the **Database backup source** field when you create a policy, any backups fail. The failure occurs

because the Microsoft Active Directory Service Interface does not provide a list of database copies for a minimal account.

Additional notes for Exchange 2013 and later

To use GRT, configure the Exchange credentials on all granular clients.

Alternatively, you can configure the Exchange credentials only on the granular clients that perform restores. In this case, for the entire domain add “Exchange Servers” to the “View-Only Organization Management” role group. Perform this configuration in the Exchange Administration Center (EAC) or in Active Directory. See the following Microsoft article for more information:

http://technet.microsoft.com/en-us/library/jj657492

Additional notes for Exchange 2010

These additional items apply to Exchange 2010:

- For granular restores from VMware backups, only the Exchange client that performs the granular restore requires configuration of the Exchange credentials. The Exchange credentials are not required for backup or browse operations.

Chapter 4

Configuring the account for NetBackup Exchange operations

This chapter includes the following topics:

About configuring the account for NetBackup Exchange operations

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 full database backups with **Enable granular recovery** selected.

NetBackup gains access to Exchange through the account for NetBackup Exchange operations, an Active Directory user account that is associated with a unique Exchange mailbox. This mailbox has sufficient roles or group memberships to

perform backups and restores. Use the account for NetBackup Exchange operations for the **Exchange credentials** in the Exchange client host properties.

Table 4-1 Steps to configure the account for NetBackup Exchange operations

Step	Action	Description
Step 1	Perform the following steps on the applicable Exchange granular clients.	In a cluster or replicated environment, perform the steps on each database node in the cluster. To determine which clients to configure for GRT operations, refer to the following topics: See "Exchange granular clients and non-VMware backups " on page 47. See "Exchange granular clients and VMware backups" on page 49.
Step 2	On the applicable Exchange granular clients, create an Exchange mailbox for NetBackup (or account for NetBackup Exchange operations).	Configure the account as follows: ■ Veritas recommends that you create a uniquely named mailbox. Verify that this mailbox is not hidden. ■ See the specific procedure for the Exchange version you have. See "Creating a privileged NetBackup user account for EWS access" on page 32. See "Creating a minimal NetBackup account for Exchange operations" on page 33.
Step 3	Configure the account with the right to "Replace a process level token."	See "About configuring the account for NetBackup Exchange operations with the right to Replace a process level token" on page 36.
Step 4	On the applicable Exchange granular clients, configure the **Exchange credentials** with the account you created previously.	See "About the Exchange credentials in the client host properties" on page 28.

About NetBackup and Microsoft Exchange Web Services

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

To use EWS to restore individual items, the client throttling policy should be modified for the resource credentials you specify for the restore job. The client throttling policy is located on the destination client and enforces connection bandwidth and activity limits on the Exchange server. When NetBackup executes under a highly privileged account, it automatically creates a throttling policy and assigns it to the account. NetBackup cannot perform these actions with an account with minimal privileges. In that case, you need to create and assign the throttling policy when you set up the account.

If the user account is a domain administrator or Exchange organization administrator, 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

A minimal NetBackup user account does not have the privilege to make these assignments. Follow the instructions to create this type of account.

Creating a privileged NetBackup user account for EWS access

This procedure provides an example of how to create a privileged account for NetBackup Exchange operations for EWS access. This account is used for the **Exchange credentials** in the Exchange client host properties, enabling NetBackup to perform operations with Granular Recovery Technology (GRT).

Note the following:

- Configure each Exchange mailbox server.
- Configure each client that performs granular operations. To determine which clients to configure, see the following topic:
  See “Exchange granular clients and non-VMware backups ” on page 47.
  See “Exchange granular clients and VMware backups” on page 49.
- In a cluster environment, perform the steps on each database node in the cluster. For an Exchange DAG, perform the steps on each database node in the DAG.

To create a privileged NetBackup user account for EWS access

1. In the Exchange Management Console, create a new Exchange mailbox for NetBackup.

   This process creates a new user that is automatically a domain user.

2. Double-click on the user account you created.
3. Select the **Member Of** tab.
4. Click **Add** and add this user to the **Organization Management** group.

   If permissions issues persist, try adding this user to the Domain Admins group. If the NetBackup Client Service logs on with this account, this account also needs to be a member of the Administrators group.

5. Provide the credentials for this account in the Exchange client host properties.

   See "About the Exchange credentials in the client host properties" on page 28.

   Veritas recommends that you configure the Exchange credentials in the Exchange client host properties. However, existing NetBackup customers can continue to configure the logon account for the NetBackup Client Service.

6. Configure this account with the right to "Replace a process level token."

   See "About configuring the account for NetBackup Exchange operations with the right to Replace a process level token" on page 36.

   If you configure the NetBackup Client Service with a logon account and configure the Exchange credentials in the Exchange client host properties, you must configure the "Replace a process level token" for both users.

Creating a minimal NetBackup account for Exchange operations

This procedure describes how to create a minimal account for NetBackup Exchange operations. This account is used for the **Exchange credentials** in the Exchange client host properties, enabling NetBackup to perform operations with Granular Recovery Technology (GRT).

Note the following:

- Configure each Exchange mailbox server.
- Configure each client that performs granular operations. To determine which clients to configure, see the following topic:
  See "Exchange granular clients and non-VMware backups " on page 47.
  See "Exchange granular clients and VMware backups" on page 49.

- In a cluster environment, perform the steps on each database node in the cluster. For an Exchange DAG, perform the steps on each database node in the DAG.

Note: If you specify the minimal NetBackup account for the Exchange credentials in the client host properties, NetBackup can back up only active copies of the Exchange databases. If you select **Passive copy only** in the **Database backup source** field when you create a policy, any backups fail. The failure occurs because the Microsoft Active Directory Service Interface does not provide a list of database copies for a minimal account.

If the policy specifies **Passive copy and if not available the active copy** in the **Database backup source** field, NetBackup backs up the active copy of each database.

To create a minimal NetBackup account for Exchange operations

1. In the Exchange Management Console, create a new Exchange mailbox for NetBackup.

   This process creates a new user that is automatically a domain user. This procedure refers to that user as *NetBackupUser*.

2. Double-click on the user account you created.
3. Select the **Member Of** tab.
4. Click **Add** and add this user to the **Administrators** group.
5. Create a new Role Group, make the account a member of this group, and assign roles. Use the Exchange Management Shell to run the following commands:

   Note: If the account does not have the necessary privileges, an administrator needs to perform these tasks.

```
New-RoleGroup -Name NetBackupRoles -Roles @("Database Copies", "Databases",
"Exchange Servers", "Monitoring", "Mail Recipient Creation", "Mail Recipients",
"Recipient Policies"

Add-RoleGroupMember -Identity NetBackupRoles -Member NetBackupUser
```

   Where *NetBackupUser* is the name of the Active Directory account you created in 1.

6 To perform restores with Granular Recovery Technology (GRT), also run the following commands with the Exchange Management shell:

For Exchange 2010:

```
New-ManagementRole -Name SymantecEWSImpersonationRole -Parent ApplicationImpersonation

New-ManagementRoleAssignment -Role SymantecEWSImpersonationRole -User NetBackupUser
-Name "NetBackupUser-EWSImpersonation"

New-ThrottlingPolicy -Name "SymantecEWSRestoreThrottlingPolicy" -EWSPercentTimeInCAS
$null -EWSPercentTimeInAD $null -EWSMaxConcurrency $null -EWSPercentTimeInMailboxRPC
$null -PowerShellMaxConcurrency $null

Set-Mailbox -Identity NetBackupUser -ThrottlingPolicy
"SymantecEWSRestoreThrottlingPolicy"
```

For Exchange 2013 and 2016:

```
New-ManagementRole -Name SymantecEWSImpersonationRole -Parent ApplicationImpersonation

New-ManagementRoleAssignment -Role SymantecEWSImpersonationRole -User NetBackupUser
-Name "NetBackupUser-EWSImpersonation"

New-ThrottlingPolicy -Name "SymantecEWSRestoreThrottlingPolicy" -EwsCutoffBalance
"Unlimited" -EwsMaxBurst "Unlimited" -EwsMaxConcurrency "Unlimited"
-ExchangeMaxCmdlets "Unlimited" -MessageRateLimit "Unlimited"
-PowerShellCutoffBalance "Unlimited" -PowerShellMaxBurst "Unlimited"
-PowerShellMaxCmdlets "Unlimited" -PowerShellMaxConcurrency "Unlimited"
-PowerShellMaxOperations "Unlimited" -RecipientRateLimit "Unlimited"
-ThrottlingPolicyScope "Regular"

Set-Mailbox -Identity NetBackupUser -ThrottlingPolicy
"SymantecEWSRestoreThrottlingPolicy"
```

7 Provide the credentials for this account in the Exchange client host properties.

See "About the Exchange credentials in the client host properties" on page 28.

8 Configure this account with the right to "Replace a process level token."

See "About configuring the account for NetBackup Exchange operations with the right to Replace a process level token" on page 36.

About configuring the account for NetBackup Exchange operations with the right to Replace a process level token

On each Exchange mailbox server you must assign the account for NetBackup Exchange operations the right to “Replace a process level token”. This right is necessary to pass the impersonation token to the NetBackup process that performs Active Directory and PowerShell commands.

Configuring the account for NetBackup Exchange operations with the right to Replace a process level token (Local Security Policy)

This procedure describes how to configure the **Local Security Policy** so that the account for NetBackup Exchange operations has the right to Replace a process level token.

To configure the account for NetBackup Exchange operations with the right to Replace a process level token (Local Security Policy)

1. Open the **Local Security Policy**.
2. Click **Local Policies**.
3. In the User Rights Assignment, add the account for NetBackup Exchange operations to the **Replace a process level token** property.
4. Run the group policy update command (group policy update) for this change to take effect:

   ```
   gpupdate /Force
   ```

Configuring the account for NetBackup Exchange operations with the right to Replace a process level token (on a domain controller)

This procedure describes how to configure the policy on a domain controller so that the account for NetBackup Exchange operations has the right to “Replace a process level token”.

To configure the account for NetBackup Exchange operations with the right to Replace a process level token (on a domain controller)

1. Open the **Group Policy Management**.
2. Under the domain, select **Group Policy Objects > Default Domain Controllers Policy**.
3. Click the **Settings** tab.

4. Expand **Security Settings > Local Policies**.
5. Right-click on **User Rights Assignment** and click **Edit**.
6. In the Group Policy Object Editor, expand **Computer Configuration > Policies > Windows Settings > Security Settings > Local Policies**.
7. In the User Rights Assignment, add the account for NetBackup Exchange operations to the **Replace a process level token** property.
8. Run the group policy update command (group policy update) for this change to take effect:

```
gpupdate /Force
```

Chapter 5

Configuring the Exchange hosts

This chapter includes the following topics:

Configuring mappings for restores of a distributed application, cluster, or virtual machine

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. Configure these mappings in the **Distributed Application Restore Mapping** host property on the master server. 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.

This configuration applies to the following situations:

- Any operations that use Granular Recovery Technology (GRT).
  Provide a list of the Exchange virtual and the physical host names. Any client that accesses the backup image for GRT operations must appear in the list. Also include the off-host client and the granular proxy host.
  See "Exchange granular clients and non-VMware backups " on page 47.
  See "Exchange granular clients and VMware backups" on page 49.
- An Exchange DAG
- A clustered Exchange server

- A Exchange granular proxy host
  See “Configuring the Exchange granular proxy host” on page 25.
- Off-host backups
- When you select a destination client other than the source client

Note the following:

- Provide the short name or the fully qualified domain name (FQDN) of the host. It is not necessary to provide both forms of the name.
- You only need to add the proxy host to the list if it is not a NetBackup master or a media server.
- (VMware policies) For a standalone server, the backup is cataloged under a different client name if you chose a **Primary VM identifier** other than **VM hostame**. In the list of hosts, you must add the NetBackup client name and the name that reflects the identifier that you chose on the **VMware** tab.

To configure mappings for restores of a distributed application, cluster, or virtual machine

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.

   The application host is the client name in the policy, or the DAG name if applicable in a VMware backup. The component host is the client that needs access to the backup image. See Table 5-1 and Table 5-2.

Example entries for Exchange hosts for a non-VMware backup

Table 5-1 Example entries for Exchange hosts for a non-VMware backup

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	Granular proxy host name

Table 5-1 Example entries for Exchange hosts for a non-VMware backup *(continued)*

Environment	Application host	Component host
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*
	Virtual cluster name	Granular proxy host name
Standalone	Client name in the policy	Granular proxy host name
Off-host	Primary client name	Off-host computer name

Example entries for Exchange hosts for a VMware backup

Table 5-2 Example entries for Exchange hosts for a VMware backup

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*
	Physical name of *Node 1*	Physical name of *Node 2*
	Physical name of *Node 1*	Physical name of *Node 3*
	Physical name of *Node 2*	Physical name of *Node 1*
	Physical name of *Node 2*	Physical name of *Node 3*
	Physical name of *Node 3*	Physical name of *Node 1*
	Physical name of *Node 3*	Physical name of *Node 2*
	Virtual name of DAG	Granular proxy host 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*
	Physical name of *Node 1*	Physical name of *Node 2*

Table 5-2 Example entries for Exchange hosts for a VMware backup *(continued)*

Environment	Application host	Component host
	Physical name of *Node 1*	Physical name of *Node 3*
	Physical name of *Node 2*	Physical name of *Node 1*
	Physical name of *Node 2*	Physical name of *Node 3*
	Physical name of *Node 3*	Physical name of *Node 1*
	Physical name of *Node 3*	Physical name of *Node 2*
	Virtual cluster name	Granular proxy host name
Standalone server	Client name under which NetBackup cataloged the backup	VM display name, VM BIOS UUID, or VM DNS name (Primary VM identifier other than **VM hostname**)
	Client name in the policy	Granular proxy host name

See "Configuring an Exchange backup that uses Granular Recovery Technology (GRT) (non-VMware backups)" on page 51.

Reviewing the auto-discovered mappings in Host Management

In certain scenarios, a NetBackup host shares a particular name with other hosts or has a name that is associated with a cluster. To successfully perform backups and restores with NetBackup for Exchange, you must approve each valid **Auto-Discovered Mapping** that NetBackup discovers in your environment. These mappings appear in the Host Management properties on the master server. You can also use the `nbhostmgmt` command to manage the mappings. See the Security and Encryption Guide for more details on Host Management properties.

Examples of the configurations that have multiple host names include:

- A host is associated with its fully qualified domain name (FQDN) and its short name or its IP address.
- If the Exchange server is clustered, the host is associated with its node name and the virtual name of the cluster.

- For an Exchange Database Availability Group (DAG), each node in the DAG is associated with the DAG name.

Auto-discovered mappings for a cluster

In a Exchange cluster environment, you must map the node names to the virtual name of the cluster if the following apply:

- If the backup policy includes the cluster name (or virtual name)
- If the NetBackup client is installed on more than one node in the cluster
  If the NetBackup Client is only installed on one node, then no mapping is necessary.

To approve the auto-discovered mappings for a cluster

1. In the NetBackup Administration Console, expand **Security Management > Host Management**.
2. At the bottom of the **Hosts** pane, click the **Mappings for Approval** tab.

   The list displays the hosts in your environment and the mappings or additional host names that NetBackup discovered for those hosts. A host has one entry for each mapping or name that is associated with it.

   For example, for a cluster with hosts `client01.lab04.com` and `client02.lab04.com`, you may see the following entries:

Host	Auto-discovered Mapping
client01.lab04.com	client01
client01.lab04.com	clustername
client01.lab04.com	clustername.lab04.com
client02.lab04.com	client02
client02.lab04.com	clustername
client02.lab04.com	clustername.lab04.com

3 If a mapping is valid, right-click on a host entry and click **Approve**.

For example, if the following mappings are valid for `client01.lab04.com`, then you approve them.

Auto-discovered Mapping	Valid name for
client01	The short name of the client
clustername	The virtual name of the cluster
clustername.lab04.com	The FQDN of the virtual name of the cluster

4 When you finish approving the valid mappings for the hosts, click on the **Hosts** tab at the bottom of the **Hosts** pane.

For hosts `client01.lab04.com` and `client02.lab04.com`, you see **Mapped Host Names/IP Addresses** that are similar to the following:

Host	Mapped Host Names/IP Addresses
client01.lab04.com	client01.lab04.com, client01, clustername, clustername.lab04.com
client02.lab04.com	client02.lab04.com, client02, clustername, clustername.lab04.com

5 If you need to add a mapping that NetBackup did not automatically discover, you can add it manually.

Click on the **Hosts** tab, then right-click in the **Hosts** pane and click **Add Shared or Cluster Mappings**. For example, provide the name of the virtual name of the cluster. Then click **Select Hosts** to choose the node names in the cluster to which you want to map that virtual name.

Table 5-3 Example mapped host names for Exchange configurations

Environment	Host	Mapped Host Names
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
Cluster	Physical name of *Node 1*	Virtual cluster name

Table 5-3 Example mapped host names for Exchange configurations *(continued)*

Environment	Host	Mapped Host Names
	Physical name of *Node 2*	Virtual cluster name
	Physical name of *Node 3*	Virtual cluster name

Chapter 6

Configuring Exchange Granular Recovery

This chapter includes the following topics:

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 databases. Or you can select individual folders or messages within a mailbox or public folder.

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

- Full or 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.
- VMware backups that protect Exchange
- 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 a Database Availability Group (DAG).

About mailbox discovery and Granular Recovery Technology (GRT)

To perform Exchange restores with Granular Recovery Technology (GRT), NetBackup needs certain information about the Exchange mailbox. For Exchange 2010, NetBackup obtains mailbox information by querying the Exchange database. This query is not sufficient for Exchange 2013, so NetBackup obtains the Exchange 2013 mailbox information through Exchange PowerShell. To save processing time during a GRT backup, the Exchange plug-in for the NetBackup Discovery Service starts local discoveries every 24 hours. It then sends the master server a list of the databases that it has discovered. The plug-in only gathers mailbox information for the most recent Exchange backup source for the database. It does not gather information from a server when a different server was the most recent backup source. If a database has no backup history, the plug-in gathers information for that database on each server that hosts a copy of the database. When the Discovery Service does not gather mailbox information for a database, NetBackup gathers the information in the snapshot job.

If you want to reset the backup status, see the following topic:

See “Displaying and resetting the backup status for a Database Availability Group (DAG)” on page 187.

For information on where NetBackup logs discovery and other information, see the following topic:

See “Debug logs for NetBackup for Exchange backup operations” on page 175.

Exchange granular clients and non-VMware backups

With snapshot backups (non-VMware backups), Exchange granular clients are those clients that perform backup or restore operations with Granular Recovery Technology (GRT). These clients have specific requirements that must be met to allow restores of individual mailbox and public folders from full database backups.

Exchange granular clients

Exchange granular clients include the following:

- All mailbox servers
- Mailbox servers in an Exchange DAG
- Mailbox servers in a clustered Exchange server
- An off-host client

Requirements for any Exchange granular clients that are mailbox servers

Each Exchange granular client that is a mailbox server requires configuration of the following:

- The NFS client. The NFS client must be installed. It also must have an unassigned drive letter for NetBackup to use to mount an NFS view of the backup image.
- An account for NetBackup Exchange operations (unique mailbox for NetBackup). This account must have the right to “Replace a process level token.”
  See “About configuring the account for NetBackup Exchange operations with the right to Replace a process level token” on page 36.
- The **Exchange credentials** in the Exchange client host properties. Use the credentials of the account for NetBackup Exchange operations.
  Alternatively for Exchange 2013 and 2016, you can add “Exchange Servers” to the “View-Only Organization Management” role group.
  See “About the Exchange credentials in the client host properties” on page 28.
- (Exchange 2010) If you configure the NetBackup Client Service with a logon account and configure the Exchange credentials in the Exchange client host properties, you must configure the “Replace a process level token” for both users.
- Mappings for distributed application restores.
  For virtual environments you need to create a map of the virtual names and physical names of the systems in the Exchange configuration. This mapping applies to any NetBackup client that mounts the backup image or initiates a

restore operation. Configure these mappings in the**Distributed Application Restore Mapping** host property on the master server.

If you use a proxy server and it is not a media or a master server, you also need to add the proxy server to this list.

See "Configuring mappings for restores of a distributed application, cluster, or virtual machine " on page 38.

- Auto-discovered mappings for the hosts in your environment.

  Approve each valid **Auto-Discovered Mapping** that NetBackup discovers in your environment. Perform this configuration in the **Host Management** properties on the master server.

  See "Reviewing the auto-discovered mappings in Host Management" on page 41.

- The client(s) must have the same version of Windows as the client from which the backup is made.
- If you use an Exchange granular proxy server, the mailbox servers and the proxy host must also meet the following additional requirements:
  - Have the same NetBackup version
  - Use the same NetBackup master server
  - Both use a Windows version that is supported for that version of Exchange For example, for Exchange 2010, the granular proxy host must be installed on Windows 2008 SP2 or R2 or on Windows 2012. See the Application/Database Agent Compatibility List for more information.

Requirements for a granular client that is an off-host client

An off-host client requires configuration of the following:

- The off-host client must have the NFS client installed. It also must have an unassigned drive letter for NetBackup to use to mount an NFS view of the backup image.
- Mapping of the primary client name and the off-host computer name.

  Perform this configuration in the Distributed Application Restore Mapping in the master server host properties.

  See "Configuring mappings for restores of a distributed application, cluster, or virtual machine " on page 38.

- The NetBackup client that performs the restore must have the same version of Windows as the off-host client from which the backup is made.

Exchange granular clients and VMware backups

Exchange granular clients are those clients that perform backup or restore operations with Granular Recovery Technology (GRT). This distinction is important because not all Exchange clients perform GRT operations with VMware browse and restore operations. Therefore, not all clients have the same configuration requirements.

Granular clients and a VMware backup that protects Exchange

With a VMware backup that protects Exchange, granular clients include following:

- Clients that browse for backups
- Mailbox servers that are used to browse into mailboxes to select items for restore
- An Exchange granular proxy host
  See "Configuring the Exchange granular proxy host" on page 25.

Requirements for Exchange granular clients

Each Exchange granular client requires configuration of the following:

- Configure all the mailbox servers.
- Every mailbox server that is used for granular browse or restore must have the NFS client installed. It also must have an unassigned drive letter for NetBackup to use to mount an NFS view of the backup image.
  Note that NFS is not needed for VMware backups.
- An account for NetBackup Exchange operations (unique mailbox for NetBackup)
  This account must have the right to "Replace a process level token."
  See "About configuring the account for NetBackup Exchange operations with the right to Replace a process level token" on page 36.
- In the Exchange client host properties, to the **Exchange credentials** add the credentials of the account for NetBackup Exchange operations.

  Configure the **Exchange credentials** on the following clients. Note that you do not need to configure the Exchange credentials on the mailbox servers that perform only backup or browse operations.

  - For Exchange 2013 and 2016, configure the credentials on all granular clients. Alternatively, add "Exchange Servers" to the "View-Only Organization Management" role group. Then configure Exchange credentials only on the destination client that performs restores.
  - For Exchange 2010, configure the credentials on the destination client that performs granular restores.

- (Exchange 2010) If you configure the NetBackup Client Service with a logon account and configure the Exchange credentials in the Exchange client host properties, you must configure the “Replace a process level token” for both users.
- Mappings for distributed application restores.
  For virtual environments you need to create a map of the virtual names and physical names of the systems in the Exchange configuration. This mapping applies to any NetBackup client that mounts the backup image or initiates a restore operation. Configure these mappings in the**Distributed Application Restore Mapping** host property on the master server.
  If you use a proxy server and it is not a media or a master server, you also need to add the proxy server to this list.
  See “Configuring mappings for restores of a distributed application, cluster, or virtual machine ” on page 38.
- Auto-discovered mappings for the hosts in your environment.
  Approve each valid **Auto-Discovered Mapping** that NetBackup discovers in your environment. Perform this configuration in the **Host Management** properties on the master server.
  See “Reviewing the auto-discovered mappings in Host Management” on page 41.
- The client that performs the restore must have the same version of Windows as the client from which the backup is made.
- If you use an Exchange granular proxy server, the mailbox servers and the proxy host must also meet the following additional requirements:
  - Have the same NetBackup version
  - Use the same NetBackup master server
  - Both use a Windows version that is supported for that version of Exchange
    For example, the granular proxy host must be installed on Windows 2008 SP2 or R2 or on Windows 2012 or R2. See the Application/Database Agent Compatibility List for more information.

Configuration for Replication Director

Note the following if you use Replication Director to manage your VMware snapshots and snapshot replication:

- Replication Director lets you browse and restore from a snapshot copy of the image. When NetBackup uses a snapshot rather than a disk storage unit for GRT operations, it does not use NFS or a new drive letter.
- Configure the NetBackup Client Service with a logon account that has access to the CIFS shares that are created on the NetApp disk array.

See "Configuring NetBackup with access to the CIFS share on the NetApp disk array" on page 167.

Exchange granular operations and the NetBackup media server

Certain requirements exist for the media server when you perform operations with Granular Recovery Technology (GRT).

The media server requires configuration of the following:

- Network File System (NFS)
  Note that operations on a snapshot copy of the image do not require NFS because it uses the primary copy.
- The client(s) must have the same version of Windows as the client from which the backup is made.
- If you use an Exchange granular proxy server, the mailbox servers and the proxy host must also meet the following additional requirements:
  - If you use a master or a media server as a proxy server you must add the proxy server to the Distributed Application Restore Mapping. (This configuration is in the master server host properties.) This list must also include any NetBackup client that mounts the backup image or initiates a restore operation.
  - Have the same NetBackup version
  - Use the same NetBackup master server

Configuring an Exchange backup that uses Granular Recovery Technology (GRT) (non-VMware backups)

Note: These steps are applicable for a backup in a non-virtual environment. To use GRT with a VMware backup, refer to the following topics:

See "Configuring Granular Recovery Technology (GRT) with a VMware backup that protects Exchange" on page 157.

Table 6-1 Configuring an Exchange backup that uses Granular Recovery Technology (GRT) with a backup in a non-virtual environment

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 Application/Database Agent Compatibility List. See the Software Compatibility List (SCL).
Step 2	Ensure that requirements are met for the NetBackup server and the Exchange Server software.	See "NetBackup server requirements for NetBackup for Exchange" on page 16. See "Exchange server software requirements for NetBackup for Exchange" on page 18.
Step 3	Determine which clients require configuration and ensure that requirements are met for the NetBackup clients.	See "Exchange granular clients and non-VMware backups " on page 47. See "NetBackup client requirements for NetBackup for Exchange" on page 17. In a cluster or replicated environment, perform the steps on each database node in the cluster. For an Exchange Database Availability Group (DAG), perform the steps on each database node in the DAG.
Step 4	On all granular clients, ensure that each node has an unassigned drive letter on which to mount the backup image.	
Step 5	Enable or configure NFS for your environment on the following: ■ All granular clients ■ The NetBackup media server	See "About configuring Services for Network File System (NFS) on Windows 2012, 2012 R2, or 2016" on page 54. See "About configuring Services for Network File System (NFS) on Windows 2008 and 2008 R2" on page 62. See "Configuring a UNIX media server and Windows clients for backups and restores that use Granular Recovery Technology (GRT)" on page 71.
Step 6	On all Exchange mailbox servers, create an account for Exchange operations (a unique mailbox) for NetBackup.	See "About configuring the account for NetBackup Exchange operations" on page 30.

Table 6-1 Configuring an Exchange backup that uses Granular Recovery Technology (GRT) with a backup in a non-virtual environment *(continued)*

Step	Action	Description
Step 7	On all Exchange mailbox servers, configure the Exchange credentials.	Use the credentials for the account for NetBackup Exchange operations. See "About the Exchange credentials in the client host properties" on page 28. Alternatively for Exchange 2013 and 2016, you can add "Exchange Servers" to the "View-Only Organization Management" role group. Perform this configuration in the Exchange Administration Center (EAC) or in Active Directory. See the following Microsoft article for more information: http://technet.microsoft.com/en-us/library/jj657492
Step 8	Create a MS-Exchange-Server policy as follows: ■ Select a supported disk storage unit. ■ Select **Enable granular recovery** on the **Attributes** tab.	See the NetBackup Hardware compatibility list. For more information on how to create a policy with GRT, see the following: See "About configuring snapshot backups of Exchange Server" on page 94.
Step 9	On the NetBackup server, configure the mappings for distributed application restores.	For backups in a DAG or cluster or if you use a proxy host or off-host client, you must map the application hosts and component hosts in your environment. For example, each DAG node must be able to access a backup image using the DAG name. Configure these mappings in the **Distributed Application Restore Mapping** host property on the master server. See "Configuring mappings for restores of a distributed application, cluster, or virtual machine " on page 38.
Step 10	On the NetBackup server, review the auto-discovered mappings for the hosts in your environment.	In certain scenarios, a NetBackup host has additional host names or shares a particular name with other hosts. For example, each DAG node must be mapped to the DAG name. Approve each valid **Auto-Discovered Mapping** that NetBackup discovers in your environment. Perform this configuration in the **Host Management** properties on the master server. See "Reviewing the auto-discovered mappings in Host Management" on page 41.

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 Windows 2012, 2012 R2, or 2016

To restore individual items from a database backup, you must configure Services for Network File System (NFS) on the NetBackup media server and the Exchange granular clients.

Table 6-2 Configuring NFS on Windows 2012, 2012 R2, or 2016

Step	Action	Description
Step 1	Configure NFS on the media server.	Before you configure NFS, review the requirements for the media server. See "Exchange granular operations and the NetBackup media server" on page 51. On the media server do the following: ■ Stop and disable the ONC/RPC Portmapper service, if it exists. ■ Enable NFS. See "Enabling Services for Network File System (NFS) on a Windows 2012, 2012 R2, or 2016 media server" on page 55. ■ Stop the Server for NFS service. See "Disabling the Server for NFS" on page 67. ■ Stop the Client for NFS service. See "Disabling the Client for NFS on the media server" on page 69. Note: If an Exchange granular client resides on the media server, do not disable the Client for NFS. ■ 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`.
Step 2	Configure NFS on the Exchange granular clients.	Determine which clients to configure. See "Exchange granular clients and non-VMware backups " on page 47. See "Exchange granular clients and VMware backups" on page 49. On the Exchange granular clients, do the following: ■ Enable NFS on the clients. See "Enabling Services for Network File System (NFS) on a Windows 2012, 2012 R2, or 2016 client" on page 59. ■ Stop the Server for NFS service. See "Disabling the Server for NFS" on page 67.

Enabling Services for Network File System (NFS) on a Windows 2012, 2012 R2, or 2016 media server

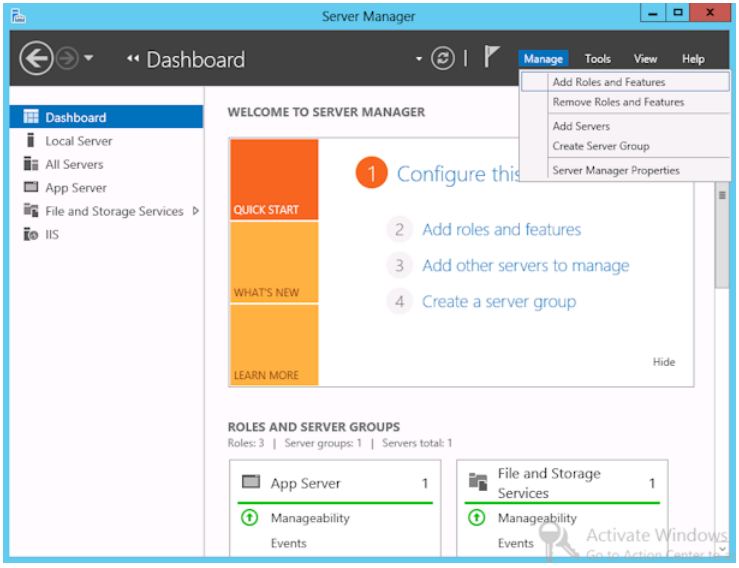
To restore individual items from a backup that uses Granular Recovery Technology (GRT), you must enable Services for Network File System (NFS). When this configuration is completed on the media server, you can disable any unnecessary NFS services. More information is available on requirements for the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

See “Exchange granular clients and non-VMware backups ” on page 47.

To enable Services for Network File System (NFS) on a Windows 2012, 2012 R2, or 2016 media server

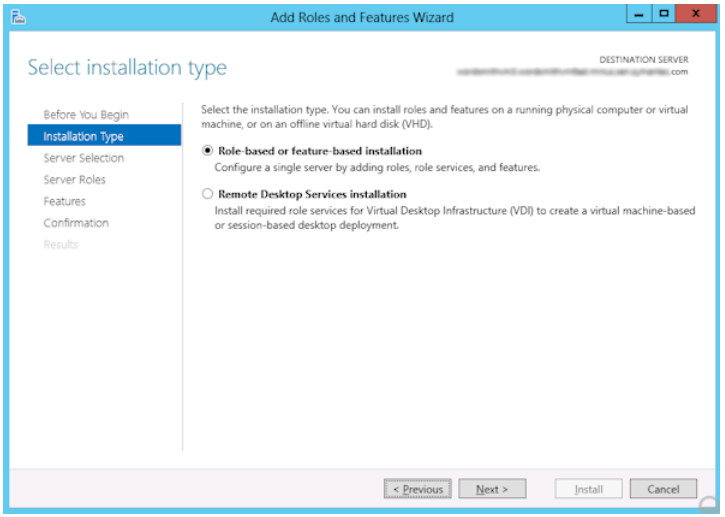
1 Open the Server Manager.

2 From the **Manage** menu, click **Add Roles and Features**.



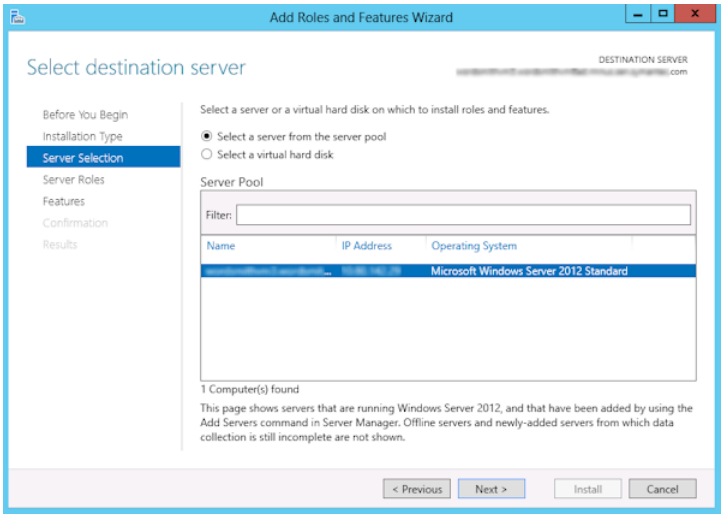
3 In the Add Roles and Features Wizard, on the **Before You Begin** page, click **Next**.

4 On the **Select installation type** page, select **Role-based or feature-based installation**.



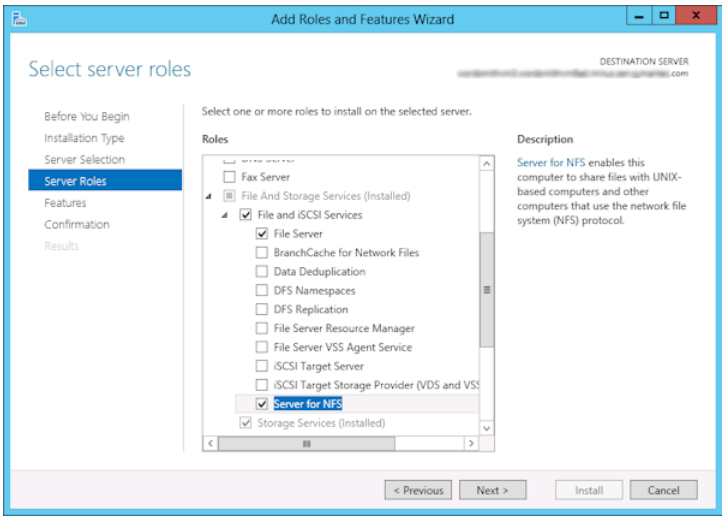
5 Click **Next**.

6 On the **Server Selection** page, click **Select a server from the server pool** and select the server. Click **Next**.

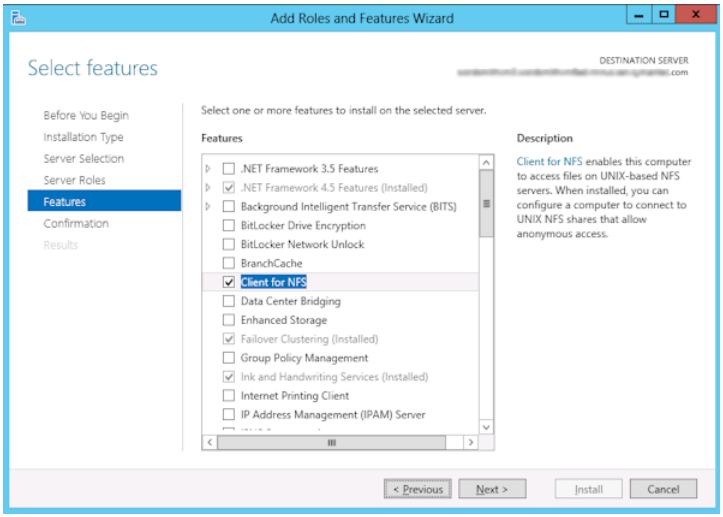


7 On the **Server Roles** page, expand **File and Storage Services** and **File and iSCSI Services**.

8 Click **File Server** and **Server for NFS**. When you are prompted, click **Add Features**. Click **Next**.



9 If the media server is also an Exchange client, on the **Features** page, click **Client for NFS**. Click **Next**.



10 On the **Confirmation** page, click **Install**.

11 Disable any unnecessary services, as follows:

- 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 service.
  See "Disabling the Server for NFS" on page 67.
- For a host that is only the NetBackup media server, you can disable the Server for NFS and the Client for NFS services.
  See "Disabling the Server for NFS" on page 67.
  See "Disabling the Client for NFS on the media server" on page 69.

Enabling Services for Network File System (NFS) on a Windows 2012, 2012 R2, or 2016 client

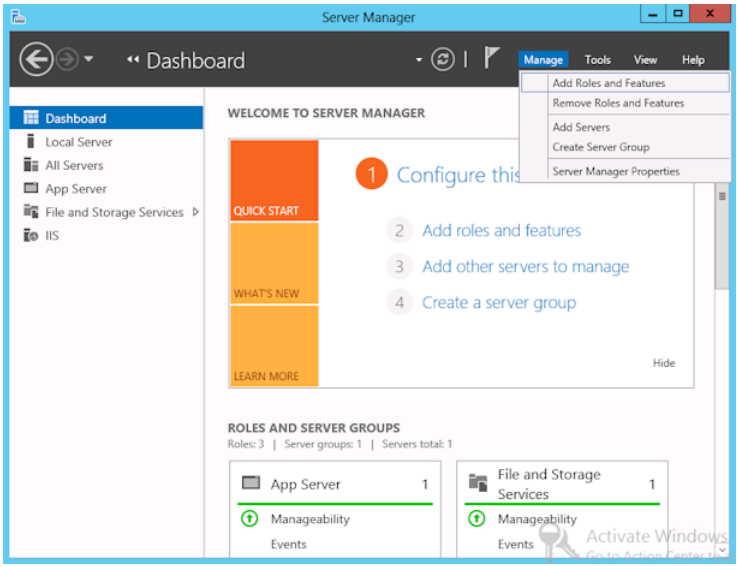
To restore individual items from a backup that uses Granular Recovery Technology (GRT), you must enable Services for Network File System (NFS). When this configuration is completed on the Exchange granular clients, you can disable any unnecessary NFS services. More information is available on which clients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

See "Exchange granular clients and non-VMware backups " on page 47.

See "Exchange granular clients and VMware backups" on page 49.

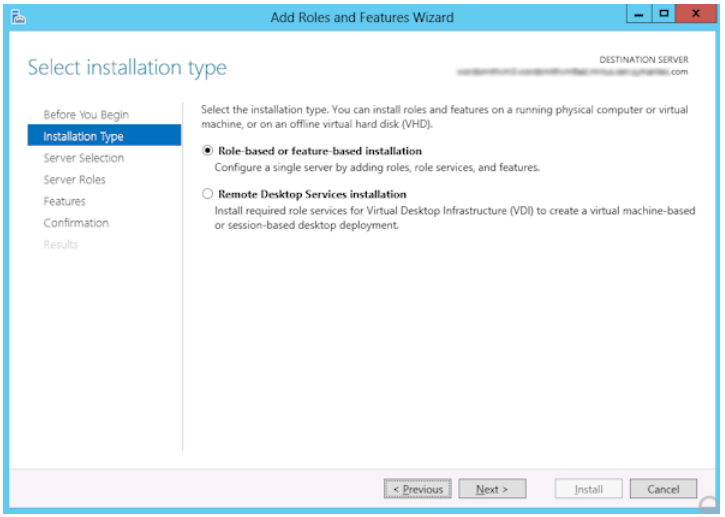
To enable Services for Network File System (NFS) on a Windows 2012, 2012 R2, or 2016 client

1. Open the Server Manager.
2. From the **Manage** menu, click **Add Roles and Features**.



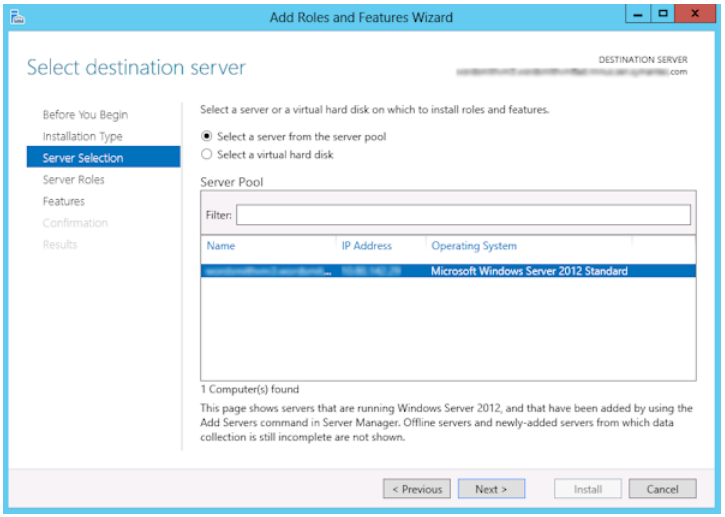
3. In the Add Roles and Features Wizard, on the **Before You Begin** page, click **Next**.

4 On the **Select installation type** page, select **Role-based or feature-based installation**.



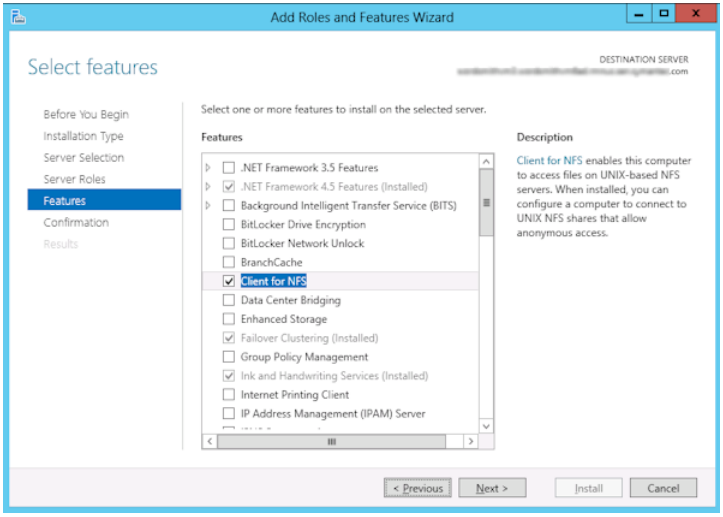
5 Click **Next**.

6 On the **Server Selection** page, click **Select a server from the server pool** and select the server. Click **Next**.



7 On the **Server Roles** page, click **Next**.

8 On the **Features** page, click **Client for NFS**. Click **Next**.



9 On the **Confirmation** page, click **Install**.

About configuring Services for Network File System (NFS) on Windows 2008 and 2008 R2

To restore individual items from a database backup, you must configure Services for Network File System (NFS) on the NetBackup media server and the Exchange granular clients.

Table 6-3 Configuring NFS in a Windows 2008 or 2008 R2 environment

Step	Action	Description
Step 1	Configure NFS on the media server.	Before you configure NFS, review the requirements for the media server. See "Exchange granular operations and the NetBackup media server" on page 51. On the media server do the following: ■ Stop and disable the ONC/RPC Portmapper service, if it exists. ■ Enable NFS. See "Enabling Services for Network File System (NFS) on Windows 2008 or 2008 R2" on page 64. ■ Stop the Server for NFS service. See "Disabling the Server for NFS" on page 67. ■ Stop the Client for NFS service. See "Disabling the Client for NFS on the media server" on page 69. Note: If an Exchange granular client resides on the media server, do not disable the Client for NFS. ■ 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`.
Step 2	Configure NFS on the Exchange granular clients.	Determine which clients to configure. See "Exchange granular clients and non-VMware backups " on page 47. See "Exchange granular clients and VMware backups" on page 49. On the Exchange granular clients, do the following: ■ Enable NFS. See "Enabling Services for Network File System (NFS) on Windows 2008 or 2008 R2" on page 64. ■ Stop the Server for NFS service. See "Disabling the Server for NFS" on page 67.

Table 6-3 Configuring NFS in a Windows 2008 or 2008 R2 environment *(continued)*

Step	Action	Description
Step 3	Install the hotfix for Client for NFS on the Exchange granular clients.	On the Exchange granular clients, install the hotfix for Client for NFS. The hotfix is available at the following location: http://support.microsoft.com/kb/955012 **Note:** Important Windows Vista hotfixes and Windows Server 2008 hotfixes are included in the same packages. However, the hotfix Request page lists only `Windows Vista`. To request the hotfix package that applies to one or both operating systems, select the hotfix that is listed under `Windows Vista` on the page. Always refer to the `Applies To` section in articles to determine the actual operating system for each hotfix.

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

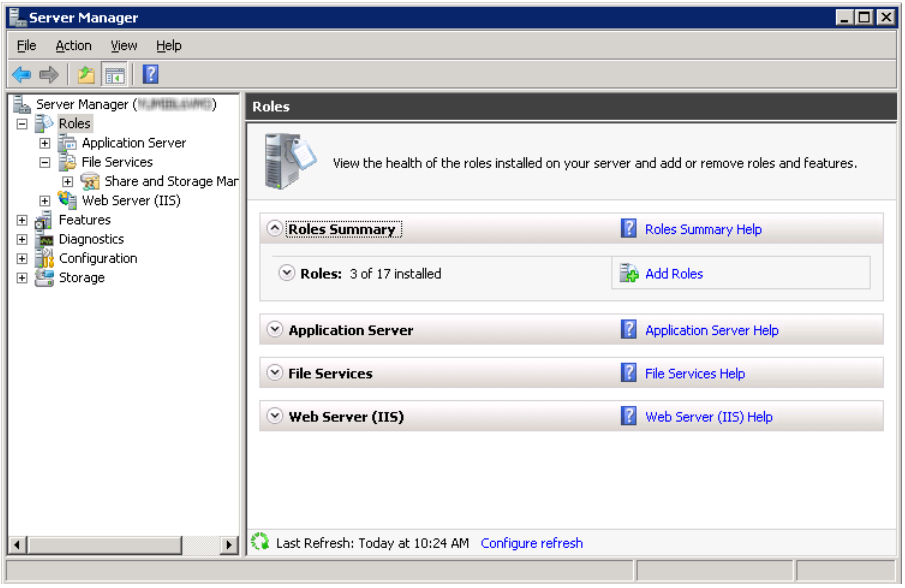
To restore individual items from a backup that uses Granular Recovery Technology (GRT), you must enable Services for Network File System (NFS). When this configuration is completed on the media server and the Exchange granular clients, you can disable any unnecessary NFS services. More information is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

See “Exchange granular clients and non-VMware backups ” on page 47.

See “Exchange granular clients and VMware backups” on page 49.

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

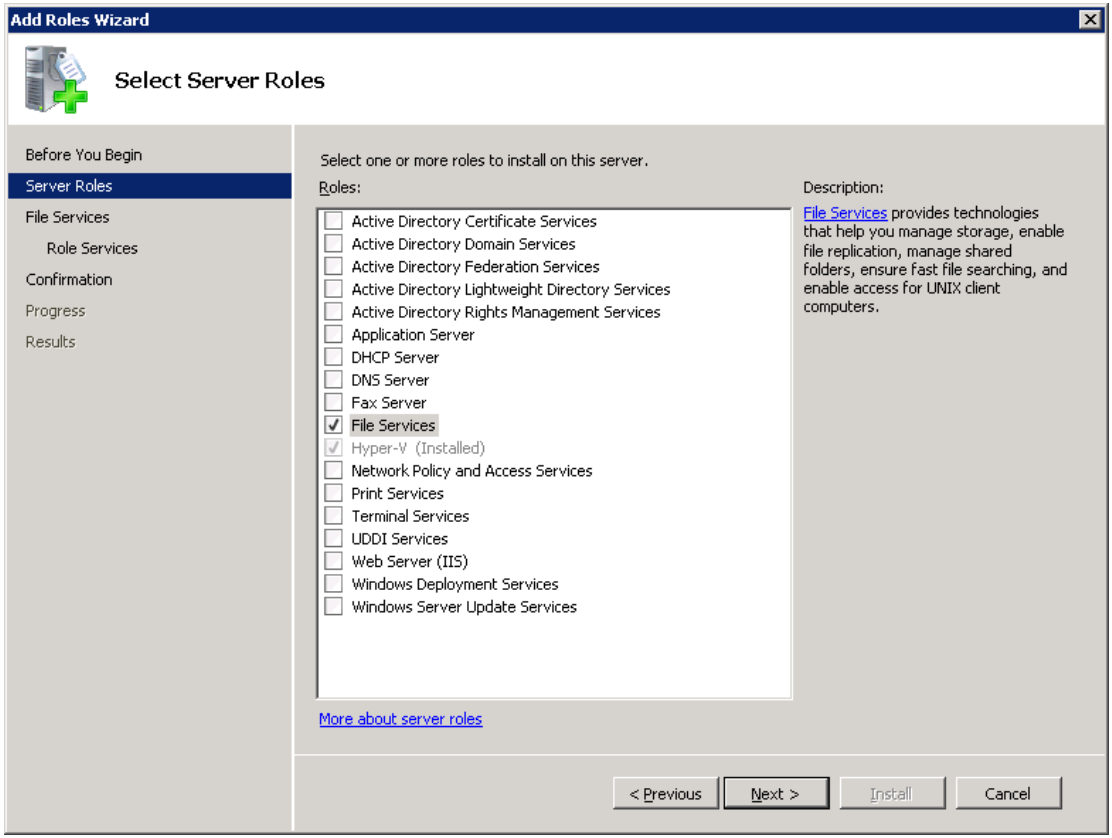
1. Open the Server Manager.
2. In the left pane, click **Roles** and, in the right pane, click **Add Roles**.



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. Click **Next**.

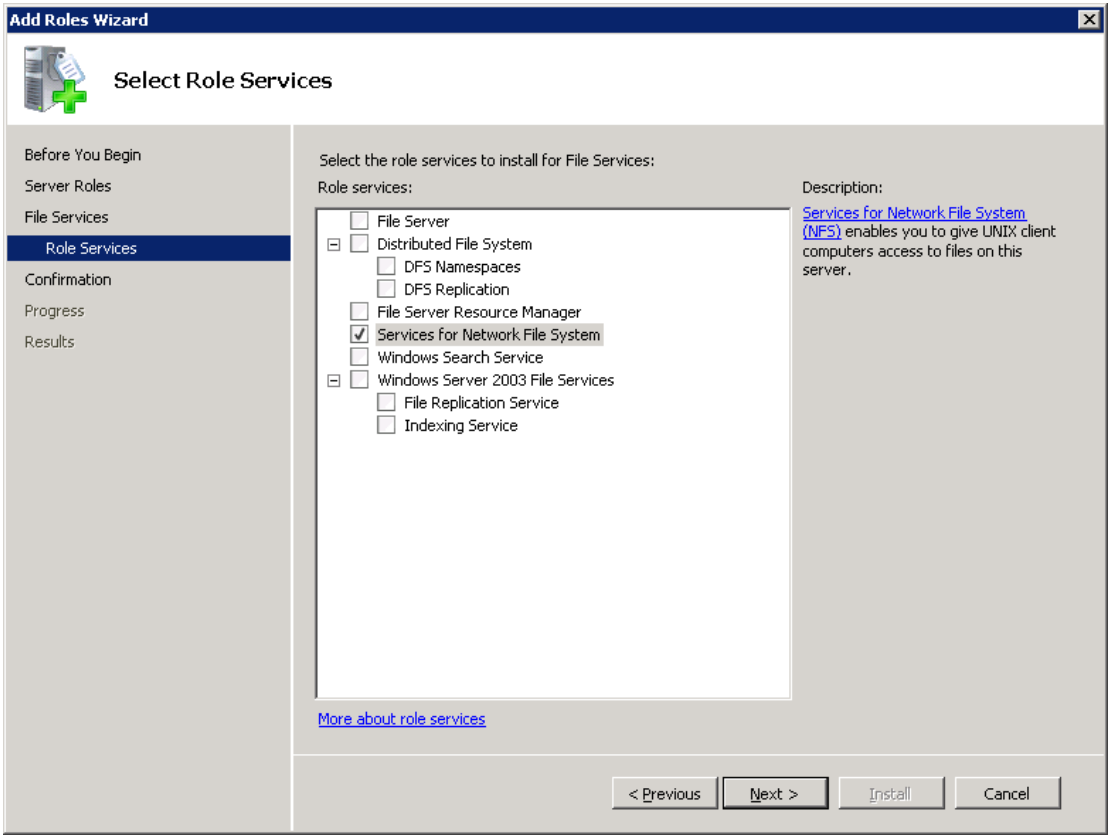
Note: If a role service is already installed for the File Services role, you can add other role services from Roles home page. In the File Services pane, click **Add Role Services**.



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

6 On the **Select Role Services** page, do the following:

- Uncheck **File Server**.
- Check **Services for Network File System**.
- Click **Next** and complete the wizard.



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

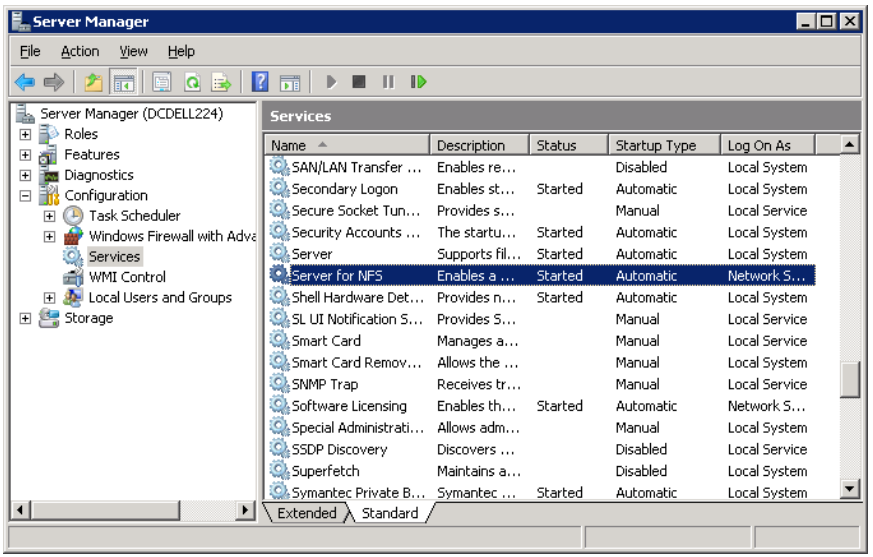
- If you have a single host that functions as both the media server and the Exchange granular client, you can disable the Server for NFS.
- For a host that is only the NetBackup media server, you can disable the Server for NFS and the Client for NFS.
- For a host that is only an Exchange granular client, 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.

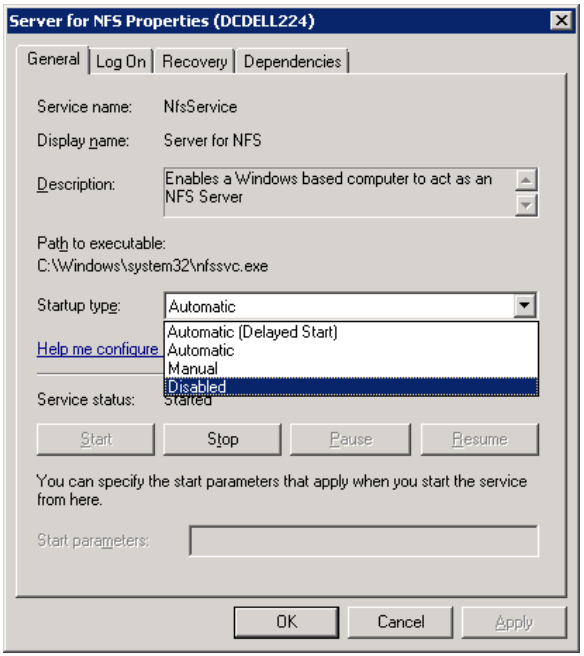
To disable the Server for NFS

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**.

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

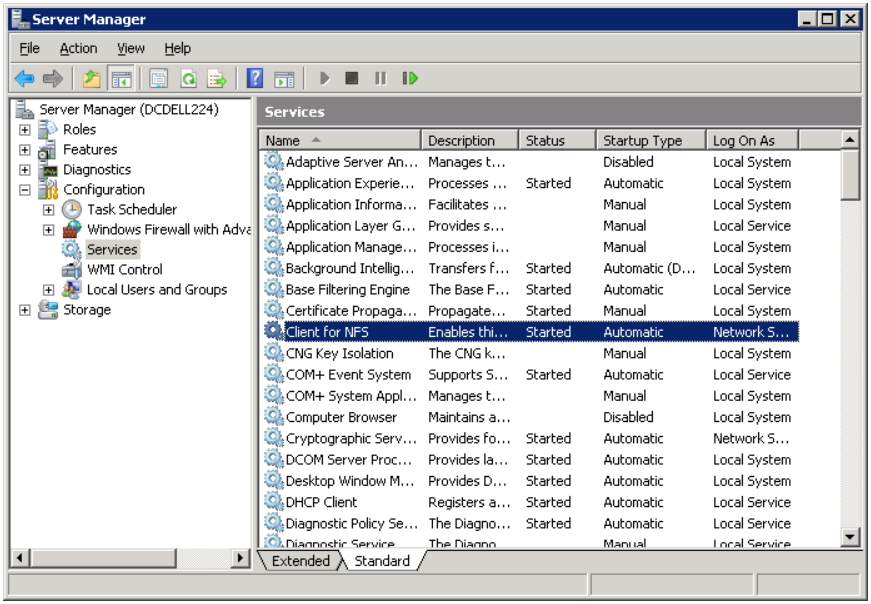
After you enable Services for Network File System (NFS) on a host that is only a NetBackup media server, you can disable the Client for NFS.

To disable the Client for NFS on the NetBackup media server

1 Open the Server Manager.

2 In the left pane, expand **Configuration**.

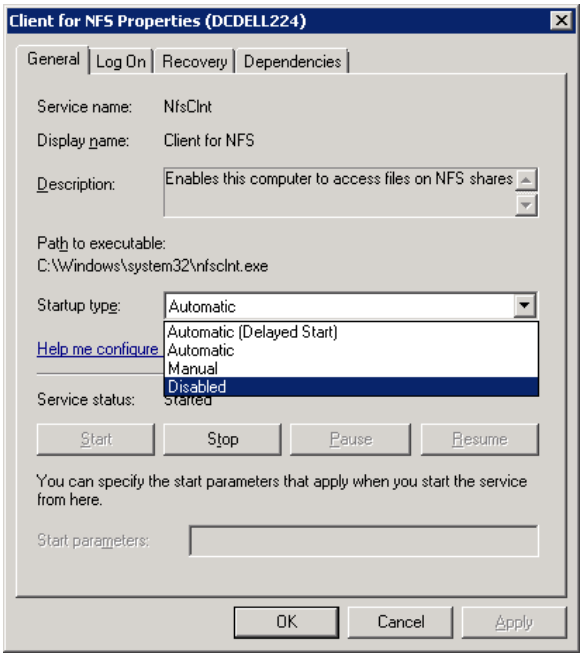
3 Click **Services**.



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**.

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



7 Click **OK**.

Configuring a UNIX media server and Windows clients for backups and restores that use Granular Recovery Technology (GRT)

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

- Confirm that your media server is installed on a platform that supports granular recovery.
  See the Software Compatibility List.
- No other configuration is required for the UNIX media server.
- Enable or install NFS on the Exchange granular clients.
  See “Enabling Services for Network File System (NFS) on a Windows 2012, 2012 R2, or 2016 media server” on page 55.
  See “Enabling Services for Network File System (NFS) on a Windows 2012, 2012 R2, or 2016 client” on page 59.

See "Enabling Services for Network File System (NFS) on Windows 2008 or 2008 R2" on page 64.

- You can configure a different network port for NBFSD.
  See "Configuring a different network port for NBFSD" on page 72.

Configuring a different network port for NBFSD

`NBFSD` runs on port 7394. If another service uses the standard `NBFSD` port in your organization, you 20can 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 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*

Disk storage units supported with Exchange Granular Recovery Technology (GRT)

Granular backups must be made to a supported disk device. During the backup operation, the mailbox name or top public folder is cataloged. When you duplicate (`-bc_only`) a backup, NetBackup catalogs the entire contents of the backup image and the duplication can be targeted to any media. When you perform a restore, the

primary backup image must exist on a supported disk media. You may need to perform another duplicate operation to copy the backup to disk.

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

See NetBackup Hardware compatibility list.

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

Note: This option does not apply to duplicating a VMware backup that protects Exchange. You cannot use the Administration Console to duplicate that kind of backup. You must use the command-line option `bpduplicate`.

Duplication of a backup that uses Granular Recovery Technology (GRT) 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 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 that use 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**.

Cataloging an Exchange backup or VMware backup that uses Granular Recovery Technology (GRT)

As an alternative to duplicating a backup image, you index or catalog the mailbox and public folder contents of the backup without creating a copy. The user can then more quickly browse the backup and perform restores. Use the following command to generate a full Exchange catalog with granular information for the image:

```
bpduplicate -bc_only
```

See the NetBackup Command Reference Guide for the options that may apply. For example, without options this command operates on all images within a default date range. This command works only on the primary copy of an Exchange image or Exchange view of a VMware image.

Note that for a VMware backup that protects Exchange, the mailbox user name is not cataloged at the time of the VMware backup.

If you specify a granular proxy host with the `bpduplicate` command, configure the Exchange hosts in the master server host properties.

See "Configuring mappings for restores of a distributed application, cluster, or virtual machine " on page 38.

Configuring the logon account for the NetBackup Client Service

Note: In previous versions of NetBackup, to perform Granular Recovery Technology (GRT) operations you configured the NetBackup Client Service on each granular client with a different logon account. This configuration is no longer required; configure the Exchange credentials in the client host properties.

See "About the Exchange credentials in the client host properties" on page 28.

Veritas recommends that you use the new configuration, though existing NetBackup customers that use GRT with Exchange 2010 can continue to configure the logon account for the NetBackup Client Service.

Note: (Exchange 2013 and later) To perform Granular Recovery Technology (GRT) operations, you must configure the Exchange credentials in the client host properties.

By default, the NetBackup Client Service uses “Local System” account to log on. A different account, called the account for NetBackup Exchange operations, is required for GRT operations. This account gives NetBackup permissions to perform Exchange backups and restores. See the following topics for information on how to create this account.

See “Creating a privileged NetBackup user account for EWS access” on page 32.

See “Creating a minimal NetBackup account for Exchange operations” on page 33.

Note the following when you configure the logon account for the NetBackup Client Service:

- Configure the NetBackup Client Service with the credentials for the account for NetBackup Exchange operations.
  See “About configuring the account for NetBackup Exchange operations” on page 30.
- Configure each client that performs granular operations. To determine which clients to configure, see the following topics:
  See “Exchange granular clients and non-VMware backups ” on page 47.
  See “Exchange granular clients and VMware backups” on page 49.
- If you use Replication Director to manage your VMware snapshots and snapshot replication, different configuration is required. You cannot configure the NetBackup Client Service with the credentials for the NetBackup Exchange operations account.
  See “About configuring a VMware backup that protects Exchange Server, using Replication Director to manage snapshot replication” on page 161.
- If you use NetBackup for Exchange on a SAN client, use the same account for the NetBackup Client Service and the SAN Client Fibre Transport Service. The account must also be a local administrator. Alternatively, you can provide the Exchange credentials in the client host properties. In that case, you do not need to use the same credentials for the SAN Client Fibre Transport Service.

To configure the logon 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. Provide the name of the account for NetBackup Exchange operations. To change the **Log on as** account, you must have administrator group privileges.

   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 Client Service.

8 Close the Services control panel application.

Chapter 7

Configuring Exchange backup policies (non-VMware)

This chapter includes the following topics:

About Exchange automatic, user-directed, and manual backups

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 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 150.

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
- 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.

Policy recommendations for Exchange Server

Note the following when you create policies for an Exchange Database Availability Group (DAG):

- Create a policy that backs up an entire DAG or backs up 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.
  This option lets you restore databases and individual mailbox and public folder items. You cannot restore individual mailbox and public folder items from any incremental backups.
- An MS-Exchange-Server policy by default backs up the passive copy of a database. This behavior provides an advantage over a VMware policy, which backs up only the active copy by default.
- The example policies include the basic policy settings for an Exchange backup. For information on how to create snapshot backup policies, see the following:
  See "About configuring snapshot backups of Exchange Server" on page 94.

Table 7-1 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.

Table 7-1 Example policy that backs up all databases in an Exchange DAG *(continued)*

Policy item	Configuration
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 7-2 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 standalone server:

- Create a policy that backs up the Information Store or individual databases. This policy supports full, incremental, and user-directed backups.
- To perform a backup with Granular Recovery Technology (GRT), select the **Enable granular recovery** option.
  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.
- The example policies include the basic policy settings for an Exchange backup. For information on how to create snapshot backup policies, see the following:
  See "About configuring snapshot backups of Exchange Server" on page 94.

Table 7-3 Example policy that backs up all database in an Exchange 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 7-4 Example policy that backs up a database in an Exchange 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	Recommended. 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.

About policy attributes

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

Table 7-5 describes some of the policy attributes available for a NetBackup for Exchange policy. For more information on policy attributes, see the NetBackup Administrator's Guide, Volume I.

Table 7-5 Policy attribute descriptions for NetBackup for Exchange policies

Attribute	Description
Policy type	Determines the types of clients that can be backed up with the policy. For Exchange databases, select the policy type MS-Exchange-Server.
Policy storage	Note that in a Database Availability Group (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. You can create multiple data streams at the database level.
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 "Disk storage units supported with Exchange Granular Recovery Technology (GRT)" on page 72. Exchange GRT-enabled backups do not support encryption or compression.
Keyword phrase	A textual description of a backup. Useful for browsing backups and restores.
Snapshot Client and Replication Director	For Exchange backups, you must enable the option **Perform snapshot backups** for all backup policies. For VMware backups, this option is enabled automatically. See "About snapshot backups with Exchange Server" on page 96. See "About configuring a VMware backup that protects Exchange Server" on page 154. See "Configuring a VMware policy to back up Exchange Server using Replication Director to manage snapshot replication" on page 165.

Table 7-5 Policy attribute descriptions for NetBackup for Exchange policies *(continued)*

Attribute	Description
Microsoft Exchange Attributes	Indicates what database backup source you want to use for a DAG. You can also indicate a preferred server list. See "Backup source for a Database Availability (DAG) backup " on page 102. See "Configuring a preferred server list for a Database Availability Group (DAG)" on page 103.

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**.

   See "NetBackup for Exchange backup types" on page 83.
5. Specify the other properties for the schedule.

   See "About schedule properties " on page 85.
6. Click **OK**.

NetBackup for Exchange backup types

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

Table 7-6 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 27. See "Truncating Exchange transaction logs by performing a backup to a storage unit" on page 27.
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 or the entire Information Store, the backup only includes the transaction logs. 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 or the entire Information Store, the backup only includes the transaction logs. 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.

Table 7-6 NetBackup for Exchange backup types *(continued)*

Type of backup	Description
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. 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 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 7-7 Description of schedule properties

Property	Description
Type of backup	Specifies the type of backup that this schedule can control. 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 83.
Schedule type	You can schedule an automatic backup in one of the following ways: ■ **Frequency** **Frequency** specifies the period of time that can elapse until the next backup operation begins on this schedule. For example, assume that the frequency is 7 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** The **Calendar** option lets you schedule the 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 112. See "Schedules settings in Exchange Instant Recovery policies" on page 113.

Table 7-7 Description of schedule properties *(continued)*

Property	Description
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

Additional requirements exist for any clients that use Granular Recovery Technology.

See "Exchange granular clients and non-VMware backups " on page 47.

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 click **Add**.

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

4. To add another client, repeat step 2.

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

6. In the **Policy** dialog box, click **Close**.

Using physical node names in the clients list

The most reliable method to back up mailbox servers in a cluster or DAG is to use the virtual Exchange name. However, if necessary you can use a node name (physical server name) in the policy rather than the virtual name. Granular Recovery Technology (GRT) is supported.

The following limitations and conditions exist when you use the physical node name:

- The backup of the databases is redirected to the server that hosts them and is cataloged under the host name. (Note: The databases are cataloged under the host name and not the DAG virtual name.)
- Use a node name that the NetBackup servers can contact.
- The backup selections list in the policy must contain `Microsoft Exchange Database Availability Groups:\`*`database name`*. The list can contain more than entry, but each database must be explicitly specified. The use of `Microsoft Exchange Database Availability Groups:\` or `Microsoft Exchange Database Availability Groups:\*` is not permitted.
- Restores can be redirected to either a DAG virtual name or the physical node name.

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 database. 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.

The following directives exist for database backups:

Table 7-8 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 standalone servers. See "About excluding Exchange items from backups" on page 91.

Table 7-8 NetBackup for Exchange Server directive sets and directives *(continued)*

Directive set	Directive(s)	Notes
MS_Exchange_ Database_ Availability_Groups	NEW_STREAM Microsoft Exchange Database Availability Groups:\	

Refer to the following topics when you add backup selections:

- See "Adding entries to the backup selections list by browsing" on page 88.
- See "Manually adding entries to the backup selections list" on page 89.
- See "Performing Exchange backups with multiple data streams" on page 89.
- See "About excluding Exchange items from backups" on page 91.

Adding entries to the backup selections list by browsing

You can browse for Exchange objects and add them to the backup selections list. Alternatively, you can add the objects manually.

See "Manually adding entries to the backup selections list" on page 89.

To add entries to the backup selections list by browsing

1. In the **Policy** dialog box, click the **Backup Selections** tab.
2. Click **New**.
3. Click **Browse**.
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 89.
     See "Using wildcards in an Exchange backup selections list" on page 90.
6. Click **OK**.

Manually adding entries to the backup selections list

This topic describes how to add database objects manually to the backup selections list. Alternatively, you can browse for the objects.

See "Adding entries to the backup selections list by browsing" on page 88.

To manually add entries to the backup selections list

1. In the **Policy** dialog box, click the **Backup Selections** tab.
2. Click **New**.
3. From the **Directive set** list select the applicable directive set.
4. From the **Pathname or directive** list, select the directive and click **Add**.
5. Edit the new entry if you want to define groups of objects or use multiple data streams.

   See "Performing Exchange backups with multiple data streams" on page 89.
6. To add other directives, repeat step 2 to step 4.
7. Click **OK** when you are finished creating the backup selections list.
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 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 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.

Backup jobs are divided 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 91.

See “Performing Exchange backups with multiple data streams” on page 89.

Using wildcards in an Exchange backup selections list

Wildcard characters can be used to define groups of databases. 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 option is not enabled, the backup fails.

See “Performing Exchange backups with multiple data streams” on page 89.

Table 7-9 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.
Left & right brackets ([...])	These wildcard characters are not supported for the `Microsoft Information Store:\` directive or for the `Microsoft Exchange Database Availability Groups:\` directive.

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. For example:

```
Microsoft Information Store:\*
Microsoft Information Store:\Database*
Microsoft Information Store:\Data??se
Microsoft Exchange Database Availability Groups:\*
Microsoft Exchange Database Availability Groups:\Database*
Microsoft Exchange Database Availability Groups:\Data??se
```

About excluding Exchange items from backups

If you do not want to back up certain databases, 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 "Configuring exclude lists for Exchange clients" on page 92.
- 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\*`

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.

Table 7-10 provides an example of an Exchange entries that you can add to an exclude list.

Table 7-10 Example Exchange 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.

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:

See "About excluding Exchange items from backups" on page 91.

The following figure shows an exclude list with two databases:

Note: For backups in a clustered or replicated environment, 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 server name, NetBackup updates only the DAG host server.

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 database in the following format:

     `Microsoft Information Store:\`*name*

     For *name*, specify the name of an Exchange database, as follows:

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

     When you specify an Exchange 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 DAG host server is updated. For the changes to be effective throughout the cluster, repeat the configuration steps on each node.

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 Information Store can have multiple separate databases, each of which has its own 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.

The database transaction log for the Information Store is named `E`*`XXYYYYYYYY`*`.log`. *XX* is the database number (in hex). *YYYYYYYY* is the log file number (in hex). The size of the transaction logs is 1 MB.

After every 1 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.

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.

Do not manually purge log files. Instead, purge logs through the backup process. For backups of a replicated copy (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 83.

See “Adding schedules for Exchange Instant Recovery” on page 112.

About configuring snapshot backups of Exchange Server

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

Table 7-11 Configuring a snapshot backup of Exchange Server

Step	Action	Description
Step 1	Review the configuration and the licensing requirements for snapshot backups.	See "Snapshot Client configuration and licensing requirements for Exchange snapshot backups" on page 18.
Step 2	Additional configuration is required if you want to restore mailbox items from a database backup (using Granular Recovery Technology or GRT).	See "Configuring an Exchange backup that uses Granular Recovery Technology (GRT) (non-VMware backups)" on page 51.
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 19.
Step 4	Review the general configuration requirements for snapshot operations.	See "Configuration requirements and recommendations for the Exchange Server when performing snapshot operations" on page 97. See "Limitations of Exchange snapshot operations" on page 97.
Step 5	Review the configuration requirements for Exchange Server.	See "Configuration requirements and recommendations for the Exchange Server when performing snapshot operations" on page 97.
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 25.
Step 7	Configure consistency checks.	See "Consistency checks on Exchange snapshot backups" on page 97. See "About consistency checks options for an Exchange backup" on page 27.
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 98.
Step 9	For a Database Availability Group (DAG), choose whether to back up the passive or the active copy. You can also define a preferred server list from which to back up the passive copy.	See "Backup source for a Database Availability (DAG) backup " on page 102. See "Configuring a preferred server list for a Database Availability Group (DAG)" on page 103.
Step 10	Configure the snapshot volume that you want to use during the backup process.	
Step 11	Disable circular logging for all databases.	

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 Snapshot Client 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 for non-clustered and non-replicated environments. Instant Recovery requires a separate Snapshot Client license. Makes the backups available for recovery from the local disk. The snapshot can also be the source for an additional backup copy to tape or other 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	Shifts the burden of backup processing onto a separate backup agent, reducing the backup impact on the client's computing resources. The backup agent sends the client's data to the storage device. NetBackup supports off-host backups of Exchange using an alternate client in non-clustered and non-replicated environments. Off-host backups require a separate Snapshot Client license. NetBackup also supports off-host Instant Recovery backups.

Limitations of Exchange snapshot operations

The following limitation exists 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.

Configuration requirements and recommendations for the Exchange Server when performing snapshot operations

Review the following requirements and recommendations before you perform snapshot backups:

- Complete the necessary installation and configuration for snapshot backups. See "Snapshot Client configuration and licensing requirements for Exchange snapshot backups" on page 18.
- Mount databases before you perform a backup.
- 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`).
- 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.

Consistency checks on Exchange snapshot backups

NetBackup is configured to run consistency checks for Exchange snapshot backups. Consistency checks are required for a standalone Exchange server. Consistency

checks are not required for an Exchange 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 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. Veritas 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:

- If you choose not to install the Exchange System Management Tools, the backup may fail. You must install the VC9 run-time 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.

See "About consistency checks options for an Exchange backup" on page 27.

Configuring a snapshot policy for Exchange Server

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

See "About configuring Instant Recovery backups of Exchange Server" on page 105.

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

See "Policy recommendations for Exchange Server" on page 79.

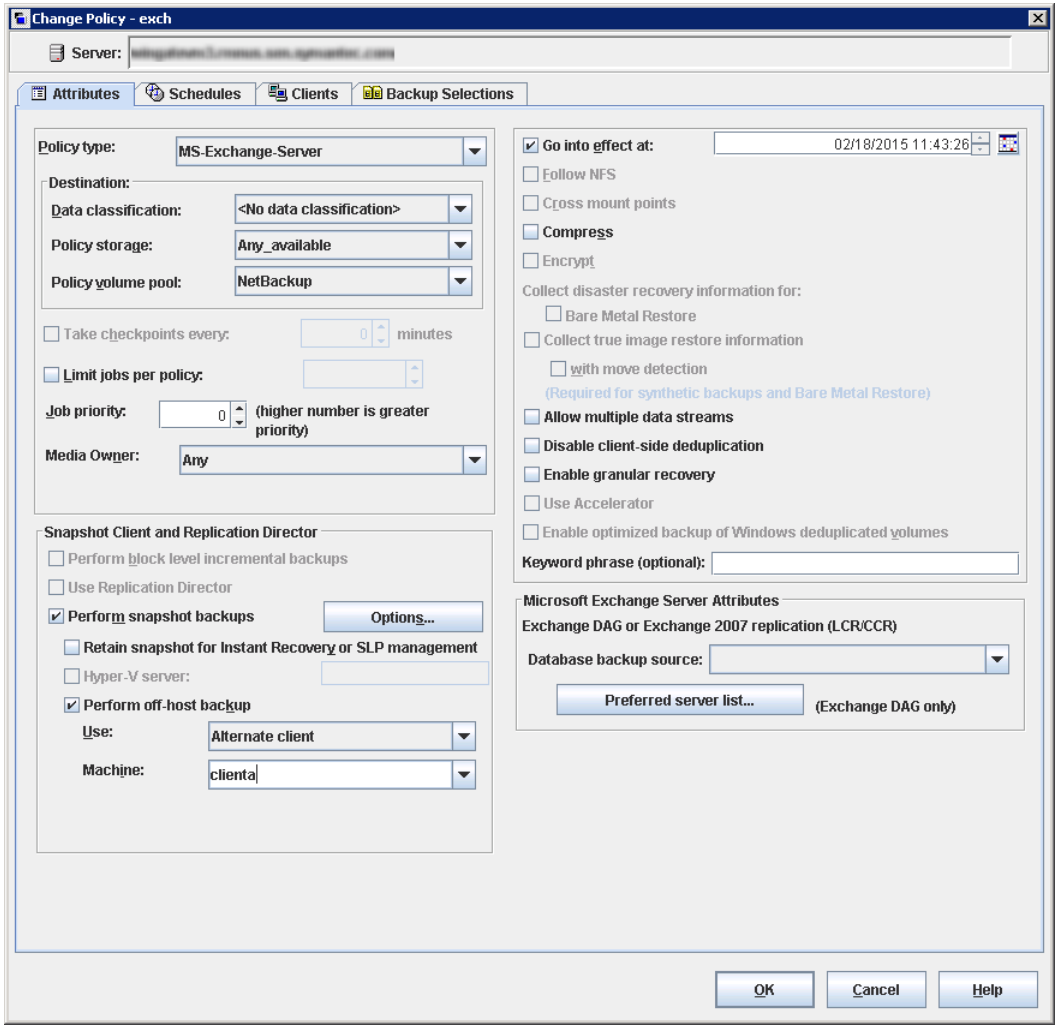
To configure a snapshot policy for Exchange Server

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 "Snapshot options for backups of Exchange Server" on page 101.
9. (Optional) To perform off-host backups with an Exchange 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 "Requirements for Exchange off-host backups" on page 19.

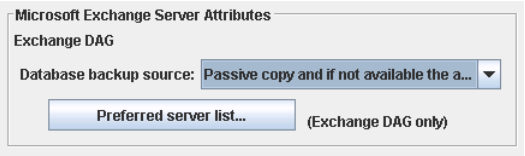


10 Optional: To divide backups into multiple jobs, click **Allow multiple data streams**.

11 To enable restores of individual items from database backups, click **Enable granular recovery**.

See "Configuring an Exchange backup that uses Granular Recovery Technology (GRT) (non-VMware backups)" on page 51.

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



See "Backup source for a Database Availability (DAG) backup " on page 102.

See "Configuring a preferred server list for a Database Availability Group (DAG)" on page 103.

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

See "Adding schedules to a NetBackup for Exchange policy" on page 83.

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 86.

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.

See "Configuring a preferred server list for a Database Availability Group (DAG)" on page 103.

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 the NetBackup Snapshot Client Administrator's Guide.

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

Off-host backups with the SFW VSS provider require that you back up objects only on the same SFW disk group.

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

Snapshot options for backups of Exchange Server

Table 7-12 lists the options that are available for snapshot backups.

Table 7-12 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.

Backup source for a Database Availability (DAG) backup

For backups of a Database Availability Group (DAG) you can choose whether to back up the active or the passive copy of the database. The client backs up and catalogs the selected database as if it were a local snapshot backup.

See "Configuring a preferred server list for a Database Availability Group (DAG)" on page 103.

On the **Attributes** tab of the policy, for the backup source select one of the following:

Passive copy only (or passive copy from preferred server list)	This option backs up the passive copy of a database or passive server if the database is all of the following: mounted, included in the backup selections list, and healthy. For a 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. If a database does not have any passive copies, then it is backed up on its active (and only) server. For example, the Public Folder database only has an active copy. A preferred server list is not required for any databases that only have an active copy.
Active copy only	This option backs up the active copy of a database or active server. 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 or the passive server that is all of the following: mounted, included in the backup selections list, and healthy. For a 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.

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

You can create preferred server configurations for an Exchange 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**, unless the database only has an active copy. The list 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 104.
- 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 a Database Availability (DAG) backup " on page 102.
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**.

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

In an Exchange 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
```

About configuring Instant Recovery backups of Exchange Server

Table 7-13 Configuring Instant Recovery backups of Exchange Server

Step	Action	Description
Step 1	Disable circular logging for all databases.	
Step 2	Review the configuration and the licensing requirements for snapshot backups.	See "Snapshot Client configuration and licensing requirements for Exchange snapshot backups" on page 18.
Step 3	Review the installation requirements for Instant Recovery backups.	See "Requirements for Exchange Instant Recovery backups" on page 19.

Table 7-13 Configuring Instant Recovery backups of Exchange Server *(continued)*

Step	Action	Description
Step 4	Review the general configuration requirements for snapshot operations.	See "Configuration requirements and recommendations for the Exchange Server when performing snapshot operations" on page 97. See "About Storage Foundations for Windows (SFW) and Exchange Instant Recovery" on page 109. See "About Exchange Instant Recovery with the Microsoft VSS Provider" on page 109.
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 109.
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 25.
Step 7	Review the backup policy recommendations for Instant Recovery backups.	See "Policy recommendations for Exchange Instant Recovery" on page 108.
Step 8	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 110.
Step 9	Configure one snapshot volume for each backup image that you need to retain on disk.	

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.

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 7-14 , see Schedules 1 and 2.)
  Granular Recovery Technology (GRT) is only supported with Instant Recovery if you also configure a backup to a storage unit.
- (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 7-14, 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 83.

Table 7-14 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.

About Storage 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.

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`).

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. Veritas recommends when you create a policy for an Exchange standalone server that you include only the databases that 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. 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.)

See “Adding schedules for Exchange Instant Recovery” on page 112.

See “Adding clients to a NetBackup for Exchange policy” on page 86.

See “Adding backup selections to an Exchange policy with Instant Recovery ” on page 114.

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

To configure a snapshot policy with Instant Recovery for Exchange Server

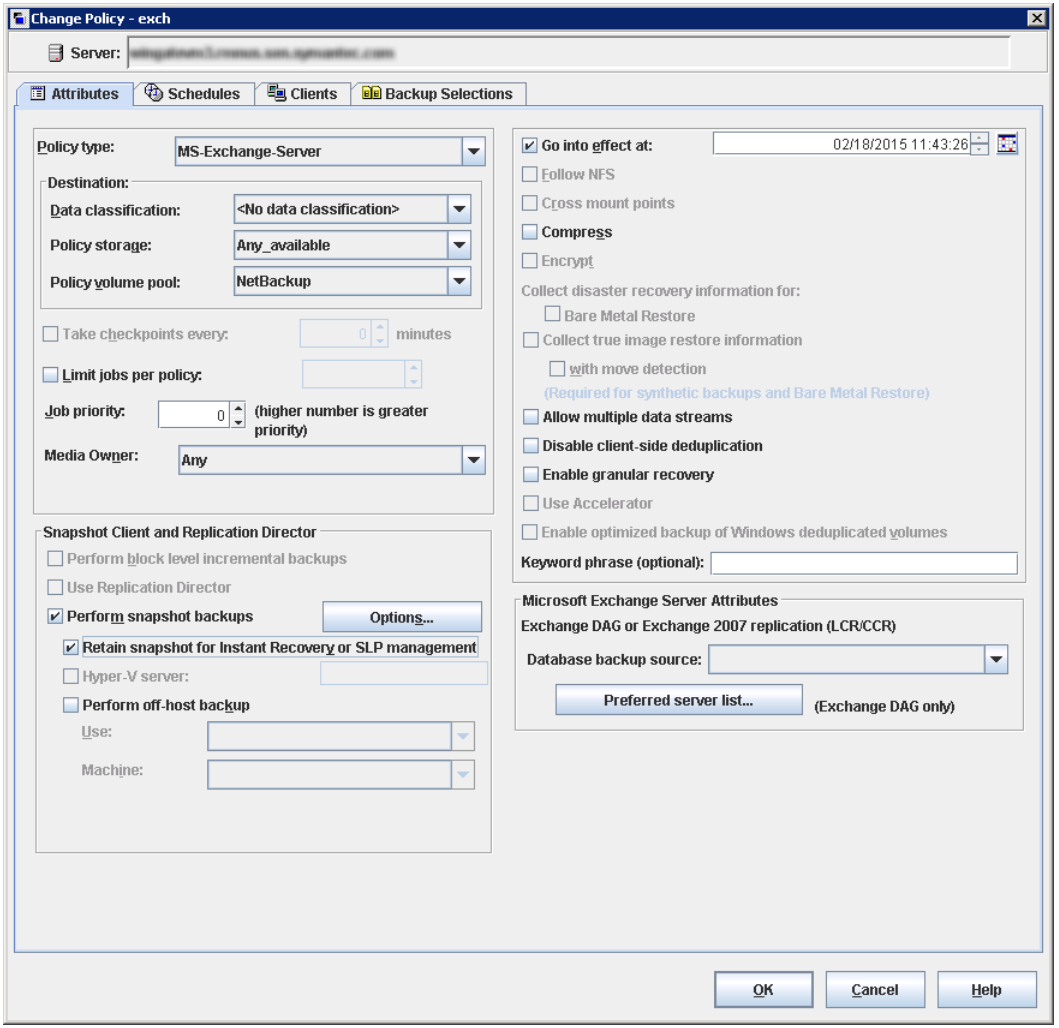
1. Create a new policy.
2. Click the **Attributes** tab.
3. In the **Policy type** drop-down list, click **MS-Exchange-Server**.
4. Select the **Policy storage**.
5. Click **Perform snapshot backups**.

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 112.

See "Schedules settings in Exchange Instant Recovery policies" on page 113.



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 backups of Exchange Server" on page 101.

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 89.

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 19.

12 Add other policy information as follows:

- Add clients to the policy.
  See "Adding clients to a NetBackup for Exchange policy" on page 86.
- Add backup selections to the policy.
  See "Adding backup selections to an Exchange policy with Instant Recovery " on page 114.

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

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**.

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 7-15 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.
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 114.

Table 7-15 Settings for schedules in Instant Recovery policies *(continued)*

Setting	Options	Description
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 27.

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 databases 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 database in one backup policy. Or you can choose to include a database 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 database.

When you configure an Exchange snapshot backup policy, the only valid directives are: `Microsoft Exchange Database Availability Groups:\` or `Microsoft Information Store:\` (a database can be appended) .

Performing a manual backup

After you configure the servers and clients in your environment, you can test the configuration settings with a manual backup. 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 Logging Reference Guide.

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

To perform a manual backup

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. In the **All Policies** pane, select the policy you want to test.
5. Select **Actions > Manual Backup**.
6. Select the schedule that you want to use for the manual backup.
7. Select the clients that you want to include for the manual backup.
8. To check the status of the backup, click **Activity Monitor** in the NetBackup Administration Console.

Chapter 8

Performing backups of Exchange Server, mailboxes, and public folders

This chapter includes the following topics:

About user-directed backups of Exchange Server data

With NetBackup for Exchange you can perform user-directed snapshot backups.

See "Performing user-directed snapshot backups of Exchange Server" on page 118.

You can also use NetBackup for Exchange to perform user-directed mailbox and public folder backups.

About selecting a source client for an Exchange Server backup operation

When you back up from a standalone server or non-virtual environment, you do not need to select or add a particular source client. However, for backups of an Exchange cluster or DAG environment to be successful, you must provide the virtual client name. When you use the NetBackup Administration Console or the Java-based Backup, Archive, and Restore client, log on with the virtual client name. Or if you use the Windows-based client, select the virtual client name in the **Specify NetBackup Machines and Policy Type** dialog box.

To select a source client for an Exchange Server backup operation in the NetBackup, Archive, and Restore interface (Windows)

1. Open the NetBackup Backup, Archive, and Restore interface.
2. Select **File > Specify NetBackup Machines and Policy Type**.
3. Select the source client as described in Table 8-1.

Table 8-1 Selecting a source client for an Exchange Server backup operation

To perform a backup of	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.

To log on to NetBackup using a virtual client name (Java)

1. Open the NetBackup Administration Console or the Backup, Archive, and Restore client.
2. Log on to NetBackup with the virtual client name or virtual DAG name.

   Select the virtual name as described in Table 8-2.

Table 8-2 Logging into NetBackup using a virtual client name

To perform a backup of	Log on with
An Exchange DAG	the DAG name.

Options for user-directed Exchange backups

Table 8-3 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 users can back up a Database Availability Group (DAG), the Information Store, or a database.

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 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 operation" on page 117.

8 In the **All Folders** pane, select the objects you want to back up.

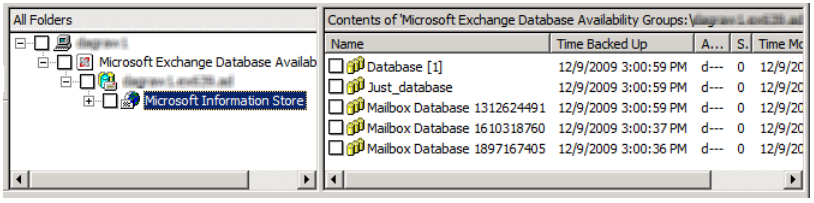
See Table 8-4 on page 120.

For a 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**.

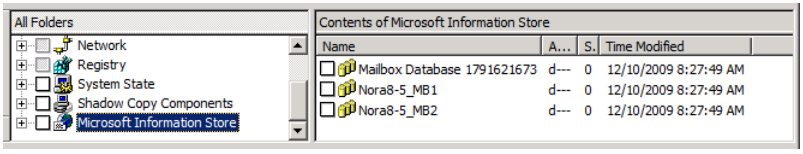
See "Backup source for a Database Availability (DAG) backup " on page 102.

All databases in the DAG, regardless of what server they reside on, are displayed.

The following figure shows a backup of an Exchange 2010 DAG.



The following figure shows a backup of an Exchange 2010 standalone server.



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 8-4 Selecting Exchange database objects for user-directed backups

Exchange version	Node	Objects to back up
Exchange DAG	**Microsoft Exchange Database Availability Groups**	DAG All databases in the DAG
Exchange standalone server	**Microsoft Information Store**	Microsoft Information Store All databases

Chapter 9

Performing restores of Exchange Server, mailboxes, and public folders

This chapter includes the following topics:

About Exchange server-directed and redirected restores

With the Backup, Archive, and Restore interface, the administrator can browse for Exchange Server backups and select the ones to restore. You can use this interface to perform restores from any NetBackup server or any NetBackup client that has permissions to view the source client's backup images. 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, Volume I 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)
- Another database

About selecting a destination client for an Exchange restore operation

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.

Requirements for redirecting Exchange objects

The following requirements must be met before you redirect the restore of 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 must exist on the target server.

- If you initiate a redirected restore from a NetBackup client, the destination client must have permission to restore from the source client. See the NetBackup Administrator's Guide, Volume I for the configuration that is needed for a redirected restore.
- The following situations require that the clients have the same version of Windows, as follows:
  - When you redirect a restore to a different client
  - When you select a destination client other than the source client when you browse the backup image

Selecting a destination client

To provide the name of the destination client, select **File > Specify NetBackup Machines and Policy Type**. If the client you want does not appear in the destination client list, you can add the client to the list.

If you want to perform a restore in a non-cluster environment to the original client that performed the backup, you do not need to change the destination client. In a cluster environment, you need to ensure that the destination client is virtual server name. It may not be possible to change the destination client value from a NetBackup client-only installation in a cluster. In that case, use the Backup, Archive, and Restore interface on a NetBackup server to change the destination client value to the virtual server name.

Select the destination client as described in Table 9-1.

Table 9-1 Destination client for an Exchange Server restore operation

To restore to...	For the destination client, select...
another database in the same DAG	the same destination client as the source client. NetBackup redirects the restore to the server that hosts the active copy of the database.
another database in a different DAG	the DAG name where the target database exists. NetBackup redirects the restore to the server that hosts the active copy of the database.
an RDB in a DAG	the DAG name
an RDB on a standalone server	the name of the standalone server
the original client that performed the backup	you do not need to change the client

Table 9-1 Destination client for an Exchange Server restore operation *(continued)*

To restore to...	For the destination client, select...
a different client	the client you want from the list. If necessary, first add the client name to the list.
a cluster environment	the virtual client name
a DAG node	the name of that node See "Using physical node names in the clients list" on page 87.
a specific mailbox server	the name of that server

About restoring Exchange database data

Review the following information before you perform restores of Exchange Server:

- The NetBackup for Exchange Agent supports a restore to the same Microsoft service pack (SP) or cumulative update (CU) on which the backup was originally created. Microsoft sometimes introduces database schema changes in SPs or CUs. If you restore to a different SP or CU level, the database server may not operate correctly.
- 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.
- You must dismount databases before you restore them.
- 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 full snapshot and a full VMware backups 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**.

- 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. 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.
- A restore of Exchange Server files always overwrites existing files. (For example, if `Pub.edb` already exists on the target server, 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 125.

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 deletes the current log files.

About restoring Exchange snapshot backups

From a snapshot backup you can restore the Microsoft Information Store or Exchange 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 138.

Note the following when you restore snapshot backups:

- All of the images you select for the restore must be from snapshot backups.
- Exchange allows a restore to the recovery database (RDB).
- 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

Options for Exchange snapshot restores

The following restore options are available when you perform snapshot restores.

Table 9-2 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 125.
Point-in-Time Recovery (Replay only restored log files)	Restores the database(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.
Temporary location for log files	Not applicable for snapshot restores.

Table 9-2 Snapshot restore options *(continued)*

Option	Description
Dismount database prior to restore	Dismounts the database(s) before the restore begins. By default this option is not selected. This option also sets the **Database can be overwritten by a restore** flag. **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	**Mount database after restore** is automatically selected if **Commit after last backup set is restored** is selected. Otherwise, this option is disabled.
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 operation" on page 117.

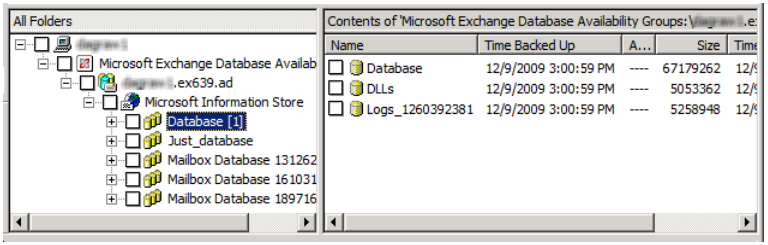
- For the policy type, select **MS-Exchange-Server**.

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, choose the objects you want to restore.

- For restores from a VMware policy, Exchange databases are displayed under the node **Microsoft Exchange Database Availability Groups**. You can restore the following objects:
  - The Database Availability Group.
    Expand **Microsoft Exchange Database Availability Groups** and select ***DAG_Name***. When you select this object, NetBackup restores all the databases.
  - Databases.
    Expand **Microsoft Exchange Database Availability Groups > *DAG_Name* > Microsoft Information Store**. Then select the database(s) and log files you want to restore.

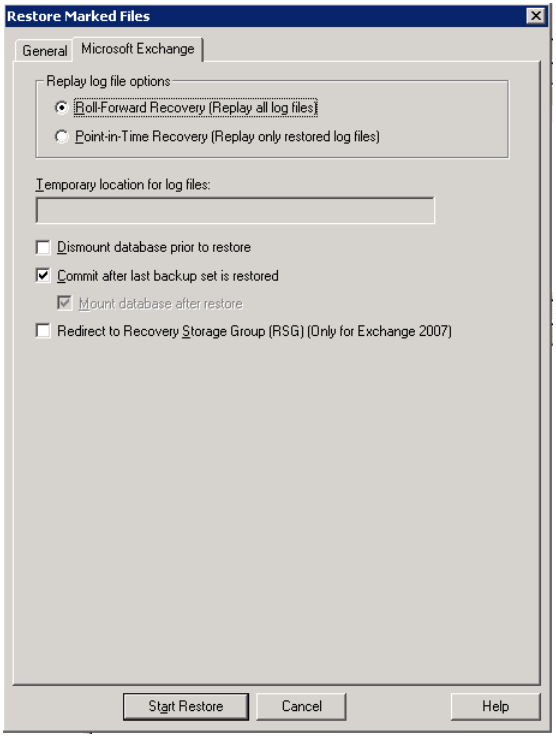


- For restores from an Exchange policy, Exchange databases are displayed under the node **Microsoft Information Store**. You can restore the following objects:
  - The Microsoft Information Store.
    Click the check box next to **Microsoft Information Store**.
  - Databases.
    Select **Microsoft Information Store**. Then select the database(s) and log files you want to restore.

9 Click **Actions > Restore**.

10 Click the **Microsoft Exchange** tab.

See "Options for Exchange snapshot restores" on page 126.



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 standalone server

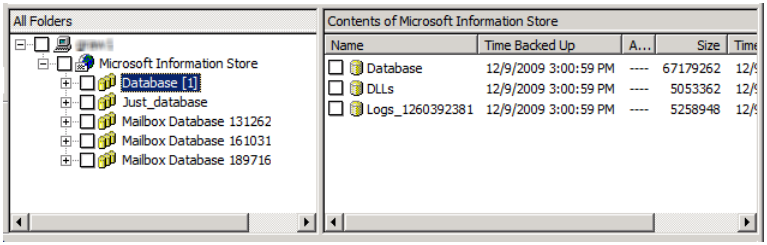
To perform a snapshot restore of an Exchange standalone server

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.
   - 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**.
   - Databases.
     Expand the **Microsoft Information Store** node. Then select the database(s) and log files you want to restore.

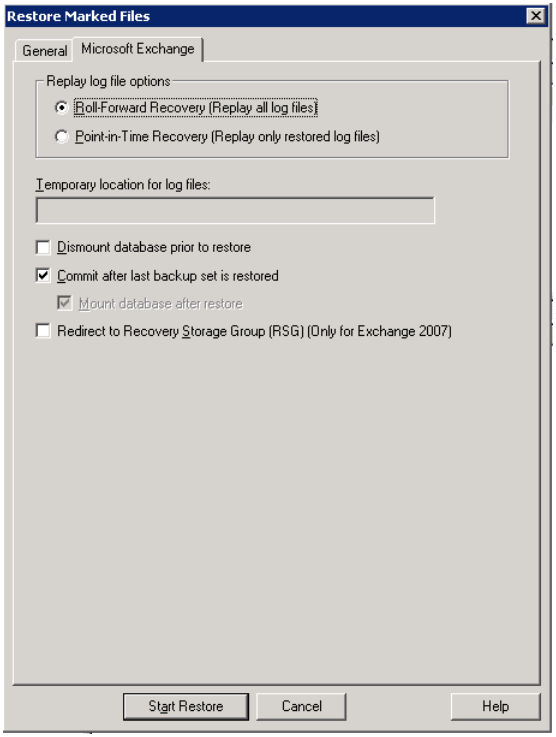
   The following figure shows a restore of Exchange 2010.



8 Click **Actions > Restore**.

9 Click the **Microsoft Exchange** tab.

See "Options for Exchange snapshot restores" on page 126.



10 Click **Start Restore**.

Redirecting a Database Availability Group (DAG) snapshot backup to another database or to the recovery database (RDB)

To redirect an Exchange snapshot backup to another database or to the recovery database

1 The following applies to suspending replication:

- If redirecting to another database, manually suspend replication. This step applies for any snapshot provider you use.
- If redirecting to the RDB, NetBackup suspends replication on the target server.

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 redirects the restore to the server that hosts the active copy of the database. To redirect the restore to a different DAG, indicate the DAG name where that database exists. To restore to a specific mailbox server, enter that server name. 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 restore operation" on page 122.
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

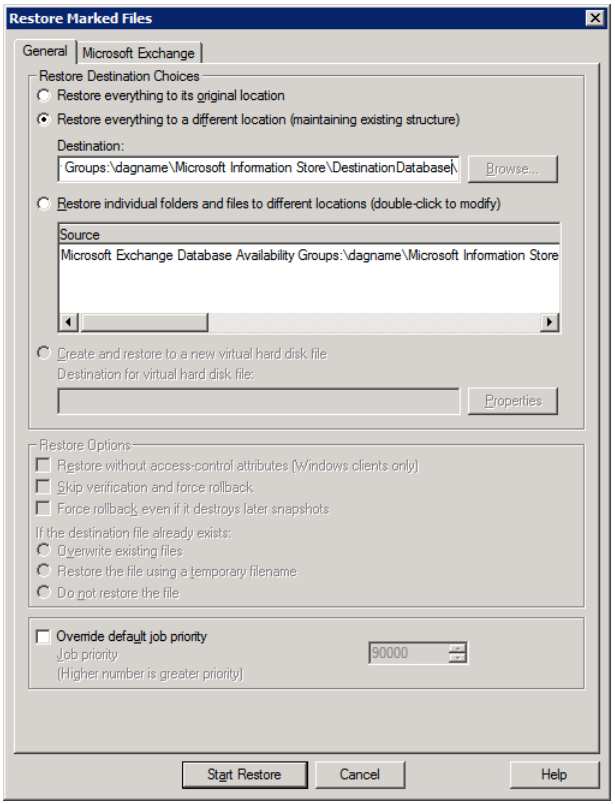
8 In the **All Folders** pane, expand **Microsoft Exchange Database Availability Groups > *Forest or domain name***.

9 Select the database you want to restore.

10 Click **Actions > Restore**.

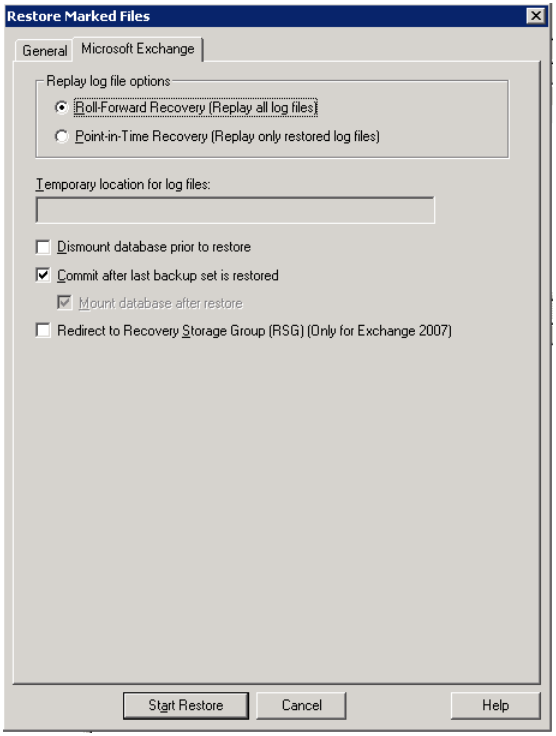
11 Change the destination path to another database or to the RDB:

- 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 does not automatically redirect a database to its RDB, if it exists.



12 Click the **Microsoft Exchange** tab.

See "Options for Exchange snapshot restores" on page 126.



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 137.

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

Redirecting an Exchange 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 standalone server to another database or the recovery database (RDB).

To redirect an Exchange 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 restore operation" on page 122. 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**.

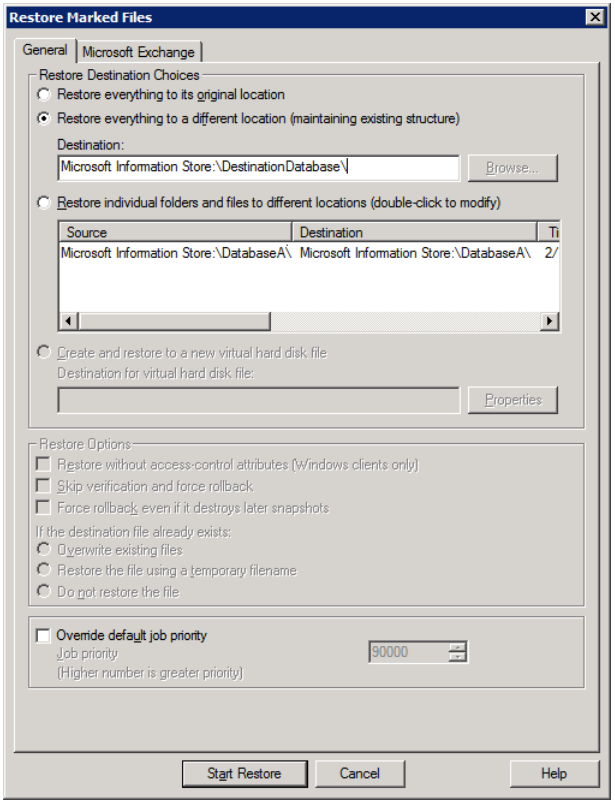
8 Select the database you want to restore.

9 Click **Actions > Restore**.

10 In the **Restore Marked Files** dialog box, click the **General** tab.

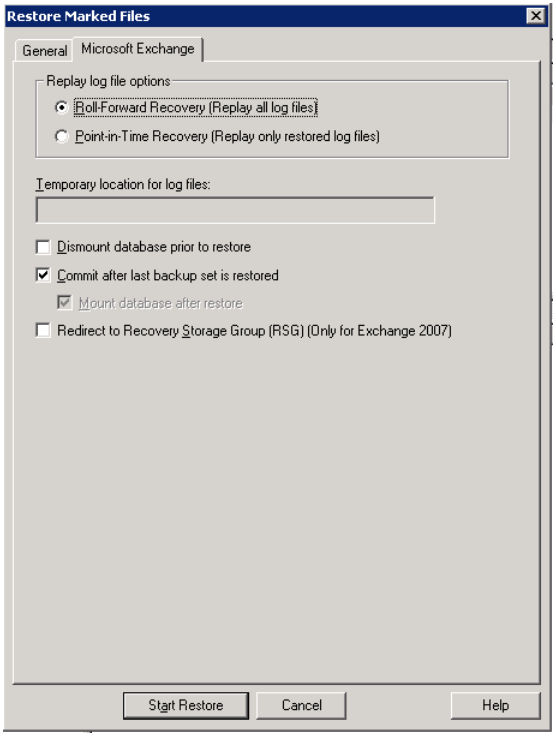
11 Change the destination path to another database or to the RDB:

- 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 does not automatically redirect a database to its RDB, if it exists.



12 Click the **Microsoft Exchange** tab.

See "Options for Exchange snapshot restores" on page 126.



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 137.

14 Click **Start Restore**.

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.
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.

About restoring individual Exchange mailbox and public folder items

You can restore individual mailbox or public folder items (folders, messages, and documents) from backups with Granular Recovery Technology (GRT) enabled. Refer to the following topics:

See "About special characters in Exchange mailbox folders and message subjects" on page 138.

See "Prerequisites and operational notes for restoring Exchange individual mailboxes, mailbox folders, public folders, or messages" on page 139.

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 9-3 to convert the translated characters back to the characters that appear in the restored items.

Table 9-3 Translation of special characters in mailbox folders and message subjects

Character	Translation
~	~0
/	~1
\	~2

Prerequisites and operational notes for restoring Exchange individual mailboxes, mailbox folders, public folders, or messages

Review the following information before you restore individual mailboxes, mailbox folders, public folders, or messages:

- The destination mailbox must exist to successfully restore a mailbox.
- 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.
- Restores that use Granular Recovery Technology (GRT) must be made from a disk storage unit. You cannot restore from the tape copy.
- NetBackup can back up the online archive mailbox for users. However, a restore from a backup using 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\`.
- 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.
- NetBackup does not support restoring mailbox items into tenant mailboxes in a multi-tenant Exchange environment. To recover items pertaining to a tenant mailbox, redirect the recovery to a non-tenant mailbox.

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 9-4 to indicate whether NetBackup should pass over or replace the pre-existing object.

Note: These options are ignored for a redirected restore.

Table 9-4 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 143.

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 in the same restore job any backups that use Granular Recovery Technology with any backups that do not.

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.

Veritas 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:

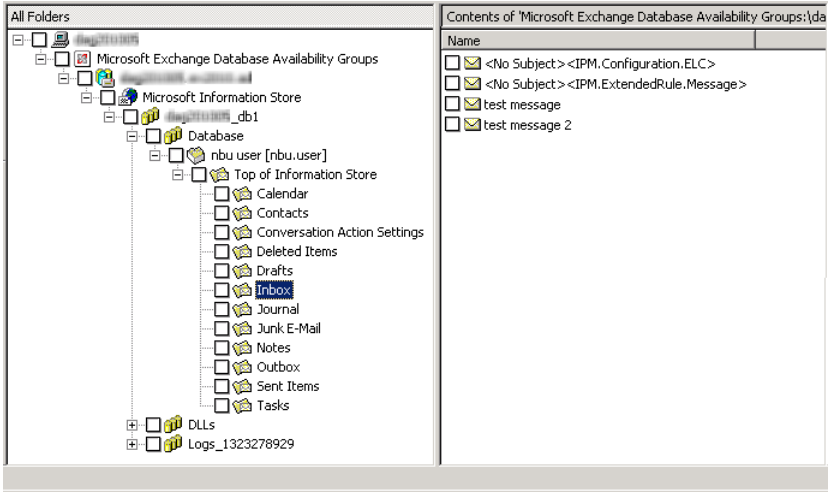
- **Microsoft Exchange Database Availability Groups > *Forest or Domain* > Microsoft Information Store > *Mailbox Database***
- **Microsoft Exchange Database Availability Groups > *Forest or Domain* > Microsoft Information Store > *Public Store***
- **Microsoft Information Store > *Mailbox Database***
- **Microsoft Information Store > *Public Store***

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).



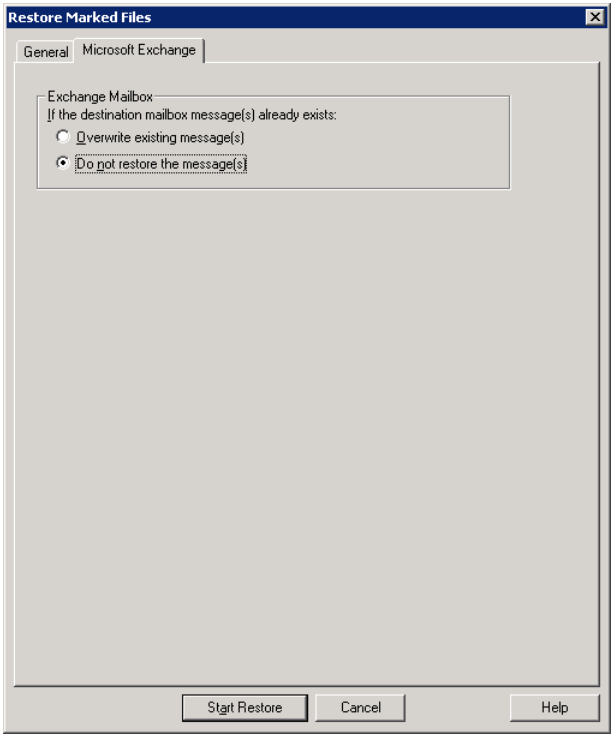
All objects appear as folders and messages. You can identify some non-message objects by the subject line. For example, if you create a Calendar event named Appointment1, that name appears in the subject line for that object.

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 "Options for restores of Exchange Server mailbox objects or public folder objects" on page 139.



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 143.

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 144.
- See "Redirecting the restore of an Exchange mailbox, mailbox folder, or public folder" on page 145.
- See "Redirecting a restore of an Exchange folder, message, or document to a different path" on page 147.

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:\
  ```

  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 a restore from a granular backup, consider the following example restore destinations:

```
Microsoft Exchange Database Availability Groups:\server1\My-database\Database\
John Q. Employee [JQEmployee]\Top of Information Store\Inbox\

Microsoft Information Store:\My-database\Database\John Q. Employee [JQEmployee]\
Top of Information Store\Inbox\
```

In the examples, note the following:

- *server1* can be the target server.
- *My-database*, must be valid database on target server (but is not directly accessed).
- *John Q. Employee*, must be a valid and an accessible mailbox.

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.

Caution: Public Folders require *Publisher Editor* permissions at the folder level on the **target** folder to allow restore to another folder.

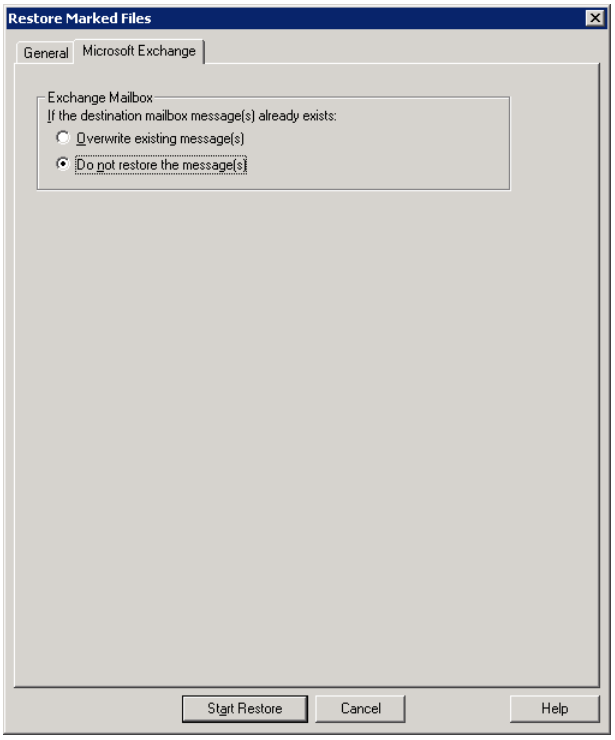
To redirect the restore of a mailbox, mailbox folder, or public folder

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 "Options for restores of Exchange Server mailbox objects or public folder objects" on page 139.



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:\DAG\Microsoft Information Store\
My-database\Database\mailbox2 [mailbox2]

Microsoft Information Store:\My-database\Database\mailbox2 [mailbox2]\
```

- 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 folder, message, or document to a different path

This topic describes how to restore a mailbox or a public folder object to a different path.

To redirect a restore of an Exchange folder, message, or document 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).

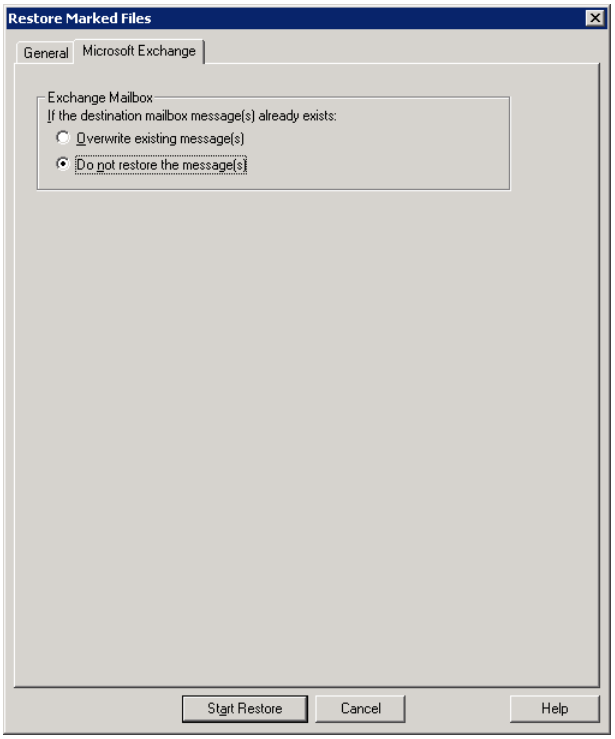
6 In the **Contents of** or right pane, click the folders, messages, or documents to restore.

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 "Options for restores of Exchange Server mailbox objects or public folder objects" on page 139.



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:\DAG\Microsoft Information Store\
My-database\Database\mailbox2 [mailbox2]\Other\

Microsoft Information Store:\My-database\Database\mailbox2 [mailbox2]\Other\
```

12 Click **OK**.

13 Click **Start Restore**.

About using the command line to browse or restore Exchange granular backup images

In addition to the NetBackup Administration Console, you can also 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 database. For example:

```
Microsoft Exchange Database Availability Groups:\server1\Microsoft Information Store\
My-database\Database\John Q. Employee [JQEmployee]\Top of Information Store\Inbox\

Microsoft Information Store:\My-database\Database\John Q. Employee [JQEmployee]\
Top of Information Store\Inbox\
```

- Use the "-granular_proxy" option with the `bpduplicate` command or the `bplist` command to specify a proxy host for a duplication operation
See "Configuring the Exchange granular proxy host" on page 25.
The following example shows how you can specify a proxy host with the `bplist` command:

```
bplist -t 16 -k exchgranpolicy -R -s 06/09/2016 16:00:00
-granular_proxy ProxyServerA "\Microsoft Information Store\My-database\
DeptA\EmployeeA\Top of Information Store\Inbox\*"
```

Chapter 10

Protecting Exchange Server data with VMware backups

This chapter includes the following topics:

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. From one VMware backup the following restore options are available: restore of the .vmdk (disk level), SFR restore (file-level recovery), Exchange database restore, or Exchange granular-level restore (GRT). You can also choose whether or not to truncate logs.

To protect a supported application with a VMware policy the 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-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 "Troubleshooting VMware backups and restores of Exchange Server" on page 188.

About the Veritas VSS provider for vSphere

The Veritas VSS provider is recommended instead of the VMware VSS provider in the following cases:

- You want VMware backups to truncate the logs on Exchange Server virtual machines. The Veritas VSS provider truncates logs for Exchange Server, by means of full VSS backups.
- The virtual machine you want to back up is a node in an Exchange DAG. 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 91.

When the Veritas VSS provider is installed and NetBackup starts a virtual machine snapshot, VMware Tools calls the Veritas VSS provider to quiesce the VSS writers for a file-level consistent backup. If log truncation is enabled in the policy, the Exchange VSS writer truncates the transaction logs when the VMware snapshot is complete.

Note: The Veritas VSS provider must be installed separately.

See "Installing the Veritas VSS provider for vSphere" on page 156.

Support for VMware backups that protect Exchange Server

Review the following requirements and information for VMware backups that protect Exchange Server:

- For details on the support for virtual environments, see the NetBackup Compatibility List.
- Either the Veritas VSS provider or the VMware VSS Provider is required. Without one of these providers, database recovery may require manual steps and granular recovery is not supported.

Veritas recommends the Veritas VSS provider for the virtual machines that host Exchange.

See "About the Veritas VSS provider for vSphere" on page 151.

- VMware backups are supported for standalone Exchange servers and DAGs.
- For DAG nodes, 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:

- This list is not a comprehensive list of VMware policy limitations. For additional information on support for NetBackup in virtual environments, see the following: http://www.veritas.com/docs/000006177
- VMware incremental backups of Exchange Server are not supported with this version of NetBackup. However, the use of Accelerator may increase the speed of full backups.
- Consistency checks of the Exchange databases are not performed with VMware backups.
- 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.
- Dismounted databases are not protected.
- 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 disk, the ASC job fails and no Exchange content is cataloged. All objects in the backup are not cataloged, including those that do not exist on the VHD.
- RAID volumes.
- An excluded Windows boot disk. The ASC job detects this type of 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:).

- VMware policies do not support exclude lists. If you want to exclude specific Exchange components, use a MS-Exchange-Server policy.

Notes for configuration of VMware policies that 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 NetBackup for VMware Administrator's Guide.

Truncating logs

For NetBackup to successfully truncate logs after a backup, the following apply:

- You must install the Veritas VSS provider.
  See “Installing the Veritas VSS provider for vSphere” on page 156.
- The ASC job must detect that the Veritas VSS provider is installed.
- You must first perform a full VMware backup without log truncation. Without this initial full backup, the ASC job fails. When this backup is complete, then enable log truncation in the policy.
- 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 152.

Operational notes

Note the following when you configure a VMware policy for Exchange Server backups:

- 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.
- The backup history is not saved for a VMware backup that protects 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 hostname** 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.

About configuring a VMware backup that protects Exchange Server

Use the following steps to configure a VMware backup that protects Exchange Server.

Table 10-1 Steps to configure a VMware backup that protects Exchange Server

Step	Action	Description
Step 1	Configure your VMware environment and add the necessary licenses.	See the NetBackup for VMware Administrator's Guide. On each ESX server that hosts the database, add the NetBackup for Exchange license and the Enterprise Client license. Install the NetBackup client software on the virtual machines that have Exchange running.
Step 2	Install the Veritas VSS provider.	See “Installing the Veritas VSS provider for vSphere” on page 156.

Table 10-1 Steps to configure a VMware backup that protects Exchange Server *(continued)*

Step	Action	Description
Step 3	If you want to restore individual mailbox and public folder items from the VMware backup, review the requirements for granular recovery.	See "Configuring Granular Recovery Technology (GRT) with a VMware backup that protects Exchange" on page 157.
Step 4	Configure a VMware policy.	See "Configuring a VMware policy to back up Exchange Server" on page 159. See the NetBackup for VMware Administrator's Guide. Note that if you want to truncate logs, you must first perform a full backup without log truncation. See "Notes for configuration of VMware policies that protect Exchange Server" on page 153. Additional information is available on how to use Accelerator to potentially increase the speed of full VMware backups. See "Using NetBackup Accelerator to increase speed of full VMware backups" on page 156.
Step 5	On the NetBackup server, configure the mappings for distributed application restores.	For backups in a DAG or cluster or if you use a proxy host, you must map the application hosts and component hosts in your environment. For example, each DAG node must be able to access a backup image using the DAG name. Configure these mappings in the **Distributed Application Restore Mapping** host property on the master server. See "Configuring mappings for restores of a distributed application, cluster, or virtual machine " on page 38.
Step 6	On the NetBackup server, review the auto-discovered mappings for the hosts in your environment.	In certain scenarios, a NetBackup host has additional host names or shares a particular name with other hosts. For example, each DAG node must be mapped to the DAG name. Approve each valid **Auto-Discovered Mapping** that NetBackup discovers in your environment. Perform this configuration in the **Host Management** properties on the master server. See "Reviewing the auto-discovered mappings in Host Management" on page 41.

Installing the Veritas VSS provider for vSphere

Note: You must install the latest version of the Veritas VSS provider. If you have an existing version of the provider, you must first uninstall the old version. Upgrading the NetBackup Client does not upgrade the Veritas VSS provider.

To use the Veritas 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 Veritas VSS provider

1. Browse to the following location:

   install_path\Veritas\NetBackup\bin\goodies\

2. Double-click on the **Veritas 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 Veritas VSS provider

1. In the Control Panel, open **Add or Remove Programs** or **Programs and Features**.
2. Double-click on **Veritas VSS provider for vSphere**.

   The uninstall program does not automatically reinstall the VMware VSS provider.

Using NetBackup Accelerator to increase speed of full VMware backups

Select the **Use Accelerator** option to use NetBackup Accelerator to potentially increase the speed of full VMware backups. By reducing the backup time, it is easier to perform the VMware backup within the backup window. To use this feature, you must first perform an initial backup with **Use Accelerator** enabled. Subsequent backup times can then be significantly reduced.

Accelerator support for Exchange currently restricts backups to the full schedule type. This restriction also exists for a VMware backup that protects Exchange without Accelerator.

See “About configuring a VMware backup that protects Exchange Server” on page 154.

To periodically establish a new baseline of change detection on the client, create a separate policy schedule with the **Accelerator forced rescan** option enabled.

This feature requires an MSDP or PureDisk storage unit and the Data Protection Optimization Option license. For more details on Accelerator with VMware backups, see the NetBackup for VMware Administrator's Guide.

Configuring Granular Recovery Technology (GRT) with a VMware backup that protects Exchange

This topic includes the steps to configure your NetBackup environment so that you can restore individual Exchange mailbox and public folder objects from a VMware backup.

Table 10-2 Configuring Granular Recovery Technology (GRT) with a VMware backup that protects Exchange

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 Application/Database Agent Compatibility List. See the Software Compatibility List (SCL).
Step 2	Ensure that requirements are met for the NetBackup server and the Exchange Server software.	See "NetBackup server requirements for NetBackup for Exchange" on page 16. See "Exchange server software requirements for NetBackup for Exchange" on page 18.
Step 3	Determine which clients require configuration and ensure that requirements are met for the NetBackup clients.	See "Exchange granular clients and non-VMware backups " on page 47. See "NetBackup client requirements for NetBackup for Exchange" on page 17. In a cluster or replicated environment, perform the steps on each database node in the cluster. For an Exchange Database Availability Group (DAG), perform the steps on each database node in the DAG.
Step 4	On all granular clients, ensure that each node has an unassigned drive letter on which to mount the backup image.	

Table 10-2 Configuring Granular Recovery Technology (GRT) with a VMware backup that protects Exchange *(continued)*

Step	Action	Description
Step 5	On all granular clients, enable or configure NFS for your environment.	In a cluster or replicated environment, perform the steps on each database node in the cluster. For an Exchange DAG, configure the nodes that browse for backups. This configuration is not needed to capture the data during backups of the virtual machine. See "About configuring Services for Network File System (NFS) on Windows 2012, 2012 R2, or 2016" on page 54. See "About configuring Services for Network File System (NFS) on Windows 2008 and 2008 R2" on page 62. See "Configuring a UNIX media server and Windows clients for backups and restores that use Granular Recovery Technology (GRT)" on page 71.
Step 6	On all granular clients, create an account for Exchange operations (a unique mailbox) for NetBackup.	Make sure that the account is a local administrator and has the right to replace a process level token on each server. See "About configuring the account for NetBackup Exchange operations" on page 30.
Step 7	On all granular clients, configure the Exchange credentials.	Use the credentials for the account for NetBackup Exchange operations. See "About the Exchange credentials in the client host properties" on page 28. Alternatively for Exchange 2013 and later, you can add "Exchange Servers" to the "View-Only Organization Management" role group. Perform this configuration in the Exchange Administration Center (EAC) or in Active Directory. See the following Microsoft article for more information: http://technet.microsoft.com/en-us/library/jj657492 In a cluster or replicated environment, perform the steps on each database node in the cluster.

Table 10-2 Configuring Granular Recovery Technology (GRT) with a VMware backup that protects Exchange *(continued)*

Step	Action	Description
Step 8	Create a policy as follows: ■ Select the **VMware** policy type. ■ Select a supported disk storage unit.	For complete details on how to configure Replication Director with VMware backups, see the NetBackup Replication Director Solutions Guide. See "Configuring a VMware policy to back up Exchange Server using Replication Director to manage snapshot replication" on page 165. Granular recovery is automatically provided for any VMware backups that protect Exchange. You do not need to enable it in the policy.
Step 9	On the NetBackup server, configure the mappings for distributed application restores.	For backups in a DAG or cluster or if you use a proxy host, you must map the application hosts and component hosts in your environment. For example, each DAG node must be able to access a backup image using the DAG name. Configure these mappings in the **Distributed Application Restore Mapping** host property on the master server. See "Configuring mappings for restores of a distributed application, cluster, or virtual machine " on page 38.
Step 10	On the NetBackup server, review the auto-discovered mappings for the hosts in your environment.	In certain scenarios, a NetBackup host has additional host names or shares a particular name with other hosts. For example, each DAG node must be mapped to the DAG name. Approve each valid **Auto-Discovered Mapping** that NetBackup discovers in your environment. Perform this configuration in the **Host Management** properties on the master server. See "Reviewing the auto-discovered mappings in Host Management" on page 41.

Configuring a VMware policy to back up Exchange Server

This topic describes how to configure a VMware policy to back up Exchange Server. Optionally, you can use NetBackup Accelerator.

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, select **VMware**.

For complete details on how to create a policy for VMware backups, see the NetBackup for VMware Administrator's Guide.

4 In the **Policy storage** box, select a disk storage unit.

If you want to use NetBackup Accelerator, select a PureDisk storage unit type (MSDP or PureDisk). The NetBackup device mapping files list all supported storage types.

5 To use NetBackup Accelerator, click **Use Accelerator**.

Accelerator uses the initial full backup to establish a baseline. Any subsequent backups that are performed with Accelerator can run significantly faster. You may want to create an additional policy schedule that enables the **Accelerator forced rescan** option. This option establishes a new baseline for the next Accelerator backup. For more details on NetBackup Accelerator, see the following:

See "Using NetBackup Accelerator to increase speed of full VMware backups" on page 156.

NetBackup for VMware Administrator's Guide.

When you enable Accelerator, on the **VMware** tab the **Enable block-level incremental backup** option is also selected and grayed out.

6 On the **Clients** tab, click **Select automatically through query**.

If you encounter problems using a query, on the **VMware** tab try changing the **Primary VM identifier** from **VM hostname** to **VMware display name**.

7 From the **NetBackup host to perform automatic virtual machine selection** list, select the host you want to use.

8 Use the Query Builder to create a rule(s) that selects the virtual machine(s) you want to back up.

For more details on the Query Builder, see the NetBackup for VMware Administrator's Guide.

9 Click the **Backup Selections** tab.

This tab displays the query you created on the **Clients** tab.

10 Click the **VMware** tab.

For details on the options in this dialog box, see the NetBackup for VMware Administrator's Guide.

11 Select the **Primary VM identifier** to use to catalog the backups.

12 Select **Enable file recovery from VM backup**.

This option must be enabled for application protection of Exchange Server.

13 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.

14 (Conditional) Choose whether or not truncate logs:

- If you do not want to truncate transaction logs, no further configuration is necessary for the policy.
  Continue with step 20.
- If you want to truncate transaction logs, you must first perform a full backup without log truncation. Without this initial full backup, the ASC job fails. When the backup is complete, then perform the full VMware backup with log truncation enabled.
  Continue with step 15.

15 Click **OK** to save the policy.

16 Perform a full backup.

17 When the backup completes, open the policy that you created in step 1.

18 Click the **VMware** tab.

19 Under **Enable Exchange Recovery**, select **Truncate logs**.

This option truncates the transaction logs when the VMware snapshot of the virtual machine is complete.

20 Click **OK** to save the policy.

About configuring a VMware backup that protects Exchange Server, using Replication Director to manage snapshot replication

Use the following steps to configure a NetBackup for VMware backup that protects Exchange Server and use Replication Director to manage snapshot replication. This feature requires the NetBackup Replication Director license.

Table 10-3 Steps to configure a VMware backup that protects Exchange Server, using Replication Director to manage snapshot replication

Step	Action	Description
Step 1	Configure your VMware environment and add the necessary licenses.	See the NetBackup for VMware Administrator's Guide. On each ESX server that hosts the database, add the NetBackup for Exchange license and the Enterprise Client license. Install the NetBackup client software on the virtual machines that have Exchange running.
Step 2	Install the Veritas VSS provider.	See "Installing the Veritas VSS provider for vSphere" on page 156.
Step 3	Create a storage lifecycle policy (SLP).	See the NetBackup Replication Director Solutions Guide.
Step 4	Configure the NetBackup Client Service to log on with an account that has access to the NetApp filer.	To browse and restore granular items in the VMware backup snapshot copy, you must configure the logon account for NetBackup Client Service. This account must have access to the CIFS shares that are created on the NetApp disk array. See "Configuring NetBackup with access to the CIFS share on the NetApp disk array" on page 167.
Step 5	If you want to restore individual mailbox and public folder items from the VMware backup, review the requirements for granular recovery.	See "Configuring Granular Recovery Technology (GRT) with a VMware backup that protects Exchange, using Replication Director to manage snapshot replication" on page 164.

Table 10-3 Steps to configure a VMware backup that protects Exchange Server, using Replication Director to manage snapshot replication *(continued)*

Step	Action	Description
Step 6	Configure a VMware policy with an SLP storage unit and enable Replication Director.	Create a policy as follows: ■ Select the **VMware** policy type. ■ Select the storage lifecycle policy (SLP) that you want to use. This SLP must be configured for snapshot replication. ■ Select **Use Replication Director**. ■ Note that if you want to truncate logs, you must first perform a full backup without log truncation. See "Notes for configuration of VMware policies that protect Exchange Server" on page 153. ■ Granular recovery is automatically provided for any VMware backups that protect Exchange. You do not need to enable it in the policy. See "Configuring a VMware policy to back up Exchange Server using Replication Director to manage snapshot replication" on page 165. For complete details on how to configure Replication Director with VMware backups, see the NetBackup Replication Director Solutions Guide.
Step 7	On the NetBackup server, configure the mappings for distributed application restores.	For backups in a DAG or cluster or if you use a proxy host, you must map the application hosts and component hosts in your environment. For example, each DAG node must be able to access a backup image using the DAG name. Configure these mappings in the **Distributed Application Restore Mapping** host property on the master server. See "Configuring mappings for restores of a distributed application, cluster, or virtual machine " on page 38.

Table 10-3 Steps to configure a VMware backup that protects Exchange Server, using Replication Director to manage snapshot replication *(continued)*

Step	Action	Description
Step 8	On the NetBackup server, review the auto-discovered mappings for the hosts in your environment.	In certain scenarios, a NetBackup host has additional host names or shares a particular name with other hosts. For example, each DAG node must be mapped to the DAG name. Approve each valid **Auto-Discovered Mapping** that NetBackup discovers in your environment. Perform this configuration in the **Host Management** properties on the master server. See "Reviewing the auto-discovered mappings in Host Management" on page 41.

Configuring Granular Recovery Technology (GRT) with a VMware backup that protects Exchange, using Replication Director to manage snapshot replication

This topic includes the steps to configure your NetBackup environment so that you can restore individual Exchange mailbox and public folder objects from a VMware backup.

Table 10-4 Configuring Granular Recovery Technology (GRT) with a VMware backup that protects Exchange, using Replication Director to manage snapshot replication

Step	Action	Description
Step 1	Verify that you have a supported Exchange Server configuration and have a media server platform that supports GRT.	Application/Database Agent Compatibility List Software Compatibility List (SCL)
Step 2	Ensure that requirements are met for the Exchange server software.	See "Exchange server software requirements for NetBackup for Exchange" on page 18.
Step 3	On all Exchange mailbox servers, create an Exchange mailbox for NetBackup (or account for NetBackup Exchange operations).	See "About configuring the account for NetBackup Exchange operations" on page 30.

Table 10-4 Configuring Granular Recovery Technology (GRT) with a VMware backup that protects Exchange, using Replication Director to manage snapshot replication *(continued)*

Step	Action	Description
Step 4	On all Exchange mailbox servers, configure the Exchange credentials.	Configure the Exchange credentials with the account you created in the previous step. In a cluster or replicated environment, perform the steps on each database node in the cluster. Perform the steps on each database node in the DAG. See "About the Exchange credentials in the client host properties" on page 28.

Configuring a VMware policy to back up Exchange Server using Replication Director to manage snapshot replication

This topic describes how to configure a VMware policy to back up Exchange Server using Replication Director to manage snapshot replication. Note that NetBackup must have access to the CIFS share on the NetApp disk array. For log truncation, the Veritas VSS provider must be installed.

See "Configuring NetBackup with access to the CIFS share on the NetApp disk array" on page 167.

See "Installing the Veritas VSS provider for vSphere" on page 156.

To configure a VMware policy to back up Exchange Server using Replication Director to manage snapshot replication

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, select **VMware**.

   For complete details on how to create a policy for VMware backups, see the NetBackup for VMware Administrator's Guide.
4. In the **Policy storage** list select the storage lifecycle policy (SLP) that you want to use. This SLP must be configured for snapshot replication.

   For complete details on how to configure Replication Director with VMware backups, see the NetBackup Replication Director Solutions Guide.
5. In the **Snapshot Client and Replication Director** group, click **Use Replication Director**.
6. Click the **Clients** tab.

7 Click **Select automatically through query**.

If you encounter problems using a query, on the **VMware** tab try changing the **Primary VM identifier** from **VM hostname** to **VMware display name**.

8 From the **NetBackup host to perform automatic virtual machine selection** list, select the host you want to use.

9 Use the Query Builder to create a rule(s) that selects the virtual machine(s) you want to back up.

For more details on the Query Builder, see the NetBackup for VMware Administrator's Guide.

10 Click the **Backup Selections** tab.

This tab displays the query you created on the **Clients** tab.

11 Click the **VMware** tab.

For details on the options in this dialog box, see the NetBackup for VMware Administrator's Guide.

12 Select the **Primary VM identifier** to use to catalog the backups.

13 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.

14 (Conditional) Choose whether or not truncate logs:

- If you do not want to truncate transaction logs, no further configuration is necessary for the policy.
  Continue with step 20.
- If you want to truncate transaction logs, you must first perform a full backup without log truncation. Without this initial full backup, the ASC job fails. When the backup is complete, then perform the full VMware backup with log truncation enabled.
  Continue with step 15.

15 Click **OK** to save the policy.

16 Perform a full backup.

17 When the backup completes, open the policy that you created in step 1.

18 Click the **VMware** tab.

19 Under **Enable Exchange Recovery**, select **Truncate logs**.

This option truncates the transaction logs when the VMware snapshot of the virtual machine is complete.

20 Click **OK** to save the policy.

Configuring NetBackup with access to the CIFS share on the NetApp disk array

You can use Replication Director to manage your VMware snapshots and snapshot replication, including the creation of snapshot copies and duplicating an image to disk. To browse and restore granular items from the VMware backup from a snapshot copy, you must configure the logon account for NetBackup Client Service. This account must have access to the CIFS shares that are created on the NetApp disk array.

Note the following when you configure the logon account for the NetBackup Client Service:

- You do not need to configure the logon account for the NetBackup Client Service if you restore databases. Nor do you need to configure the account if you browse or restore granular items from a disk image.
- Configure each client that performs granular operations. To determine which clients to configure, see the following topics:
  See "Exchange granular clients and VMware backups" on page 49.
- In a cluster environment, perform the steps on each database node in the cluster. Perform the steps on each database node in the DAG.

To configure NetBackup with access to the CIFS shared on the NetApp disk array

1 Open the Windows Services application.

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

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

4 Add the account that has access to the CIFS shares that are created on the NetApp disk array. To change the **Log on as** account, you must have administrator group privileges.

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 Client Service.

8 Close the Services control panel application.

About restoring Exchange data from a VMware backup

Exchange data is restored from a VMware backup like it is restored from a backup that was 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. See the following topics for information on how to restore Exchange data from a VMware backup:

See "About restoring Exchange snapshot backups" on page 126.

See "About restoring individual Exchange mailbox and public folder items" on page 138.

See "About redirecting a restore of Exchange mailbox or public folder objects to a different path" on page 143.

General notes

Note the following when you restore Exchange from a VMware backup:

- You cannot browse or recover granular items (GRT) from GPT (GUID Partition Table) disks.
- All the restore options are available. You can recover to any of the following:
  - A recovery database
  - Another database
  - An alternate server
    The target server can be a virtual computer or physical computer.

Selecting source and destination clients

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 the NetBackup Administrator's Guide, Volume I.

- For a restore of a cluster (including 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 DAG name is also in FQDN format.
- For a restore of an Exchange standalone server, you must select 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.

Restores from VMware backups, not using Replication Director

No additional requirements apply if you want to restore an Exchange database from a VMware backup. However, if you want to perform a granular browse and restore the following requirements apply:

- You must configure NFS on the client that you use to browse or restore.
- The client must have an unassigned drive letter on which to mount the backup image.
- For restore operations, for the destination client you must configure the **Exchange credentials** in the Exchange client host properties.

Restores from a snapshot copy that was created with Replication Director

No additional requirements apply if you want to restore an Exchange database from a snapshot copy that was created with Replication Director. However, if you want to perform a granular browse or restore from a snapshot copy, note the following:

- You must configure the logon account for the NetBackup Client Service. This account must have access to the CIFS shares that are created on the NetApp disk array.
- For a restore, you must configure the **Exchange credentials** in the Exchange client host properties.
- Note that when you browse or restore a snapshot copy, NetBackup does not require NFS. Nor does it require an unassigned drive letter on which to mount the backup image

Restores from a disk image that was created with Replication Director

If you use Replication Director to create a disk image and want to perform a granular browse or restore from that image, the following requirements apply

- You must configure NFS on the client that you use to browse or restore.
- The client must have an unassigned drive letter on which to mount the backup image.
- To restore from a disk image, you do not need to configure the logon account for the NetBackup Client Service with an account that can access the NetApp disk array. For granular restore, for the destination you must configure the Exchange credentials in the Exchange client host properties.

Enabling protection of passive copies of the Exchange database with VMware backups

For DAG nodes, only the active copies of the database on a VM selected for backup are cataloged. The passive copies of the databases are not cataloged. Log files are truncated for the passive copies as long as the Veritas VSS provider is installed.

To protect passive database copies, create the registry value that is described in the procedure. Designate a VM in the DAG to serve as the backup server in the DAG. Then set the registry value on that server. This backup server should have a passive copy of each database in the DAG.

To enable protection of passive copies of the Exchange database with VMware backups

1. On the VM that serves as the backup server, launch `regedit.exe`.
2. Open the following key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\VERITAS\NetBackup\CurrentVersion\Agents
```

3. Create a new String Value named **VM_Exchange_Backup_Passive_DBs**.
4. Right-click on the new value and click **Modify**.
5. In the **Value data** box, type **Yes**.
6. Click **OK**.

Chapter 11

Recovering an Exchange database to a repaired or an alternate Exchange server

This chapter includes the following topics:

About recovery of Exchange databases

Table 11-1 describes the steps to recover an Exchange database.

Table 11-1 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 11-2.
Step 2	Recover the Exchange database.	See "Recovering an Exchange database" on page 172.

Table 11-1 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 article explains how to configure an alternate server for restore operations: http://www.veritas.com/docs/TECH29816

Table 11-2 describes the resources available that describe how to recover an Exchange database.

Table 11-2 Disaster recovery resources

Exchange 2010	http://technet.microsoft.com/en-us/library/dd876880(EXCHG.140).aspx
All versions of Exchange	www.microsoft.com/exchange

Recovering an Exchange database

To recover an Exchange database

1. On an alternate or a repaired Exchange server, create databases that match the original databases.

   You can use the Backup, Archive, and Restore interface on the master server 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.

11 Reconnect the mailboxes you recovered to their Active Directory user accounts.

12 If you recovered to an alternate Exchange server, Veritas 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.

See the Microsoft website for more information about EXMerge.

Chapter 12

Troubleshooting backups and restores of Exchange Server

This chapter includes the following topics:

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 175.

See "Debug logs for NetBackup for Exchange backup operations" on page 175.

See "Debug logs for NetBackup for Exchange restore operations" on page 176.

See "Setting the debug level on a NetBackup for Exchange Windows client" on page 180.

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 Logging Reference 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 Logging Reference 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 ■ nbdisco This log applies to Exchange 2013 and later only. For discovery information, review this log on all mailbox clients. On the master server NetBackup logs information for the discovery database in *install_path*\NetBackup\db\discovery.
Backups that use GRT (non-VMware)	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 ■ nbdisco This log applies to Exchange 2013 and later only. For discovery information, review this log on all mailbox clients. On the master server NetBackup logs information for the discovery database in *install_path*\NetBackup\db\discovery. ■ ncfnbcs For ASC issues and failures, this log is created on the VM that is backed up.
All Exchange backups	Refer to the following logs: ■ bpbkar ■ bpresolver This log is written to the DAG node. To determine the DAG host server node, see the following: See "Finding the current host server of the Database Availability Group (DAG)" on page 187.

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 Veritas products.

For details on both unified logging and legacy logging, see the NetBackup Logging Reference Guide.

All restores, except those with Granular Recovery Technology (GRT)	Refer to the following logs: ■ `bpbrm` This log appears on the media server. ■ `bpdbm` ■ `bprd` ■ `tar`
Restores with GRT	Refer to the following logs: ■ `beds` ■ `bpcd` This log appears on the destination or the proxy client. It applies to GRT browse operations. ■ `bpdbm` ■ `bpbrm` This log appears on the media server. ■ `bprd` ■ `nbfsd` This log appears on the client and the media server. This log does not apply for browse and restore operations from VMware snapshot copies (using Replication Director). ■ `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. ■ `bpbrm` This log appears on the master server. ■ `bpdbm` ■ `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. ■ `bprd` ■ `tar` For off-host Instant Recovery, this log appears on the primary client.
All Exchange restores	Refer to the following logs: ■ `bpbkar` ■ `bpdbm` ■ `bprd` ■ `bpresolver` This log is written to the DAG node or other destination client, if specified. To determine the active node, see the following: See "Finding the current host server of the Database Availability Group (DAG)" on page 187.
Restores from VMware backups	Refer to the following logs: ■ `bpbkar` ■ `bpdbm` ■ `bppfi` ■ `bprd` ■ `tar`

Restores from snapshots using Replication Director	Refer to the following logs: ■ `bpbkar` This log is written to the backup host. ■ `bpdbm` ■ `bpfis` This log applies to GRT operations only. This log appears on the client where the browse or restore occurs. ■ `bprd` ■ `ncfnbhfr` This log is written to the backup host. ■ `tar` This log is written to the target Exchange server.

Veritas VSS provider logs

The Veritas VSS provider records its activities in Windows Event Logs. Debug logs are also available at the following location:

install_path`\Veritas VSS provider\logs`

Enabling Veritas VSS provider logging in the registry

Enable the Veritas VSS provider logging on the NetBackup computer where Exchange is installed.

To enable Veritas VSS provider logging in the registry

1. Log on as administrator on the computer where NetBackup is installed.
2. Open Regedit.
3. Open the following key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Backup Exec for Windows\Backup Exec\Engine\Logging`

4. Create a new DWORD value named **CreateDebugLog**.
5. Right-click on the new value and click **Modify**.
6. In the **Value data** box, enter **1**.
7. Click **OK**.

Increasing the Veritas VSS provider log debug level

To increase the log debug level modify both the pre-freeze-script.bat and post-thaw-script.bat files in the `C:\Windows` folder. Add the `-log` parameter to the

script, at the line where `BeVssRequestor.exe` is called. VMware determines which script is invoked.

To increase the Veritas VSS provider log debug level

1. 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
   ```

2. 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 for the legacy process on a NetBackup for Exchange client

1. Open the **Backup, Archive, and Restore** program
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.

To set the debug level for the processes that use unified logging on a NetBackup for Exchange client

1. Newer NetBackup processes such as `ncfgre` use unified logging (VxUL). To increase VxUL logging level, run the following:

   ```
   install dir\NetBackup\bin\vxlogcfg -a -p 51216 -o OID -s
   DebugLevel=6 -s DiagnosticLevel=6
   ```

   For a list of all OID values, see the NetBackup Logging Reference Guide.

2. To reset the VxUL logging level default value, run the following command:

   ```
   install dir\NetBackup\bin\vxlogcfg -a -p 51216 -o OID -s
   DebugLevel=1 -s DiagnosticLevel=1
   ```

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:

- Event Viewer
  See "Connecting to the remote Exchange server from within Event Viewer" on page 181.
- Exchange System Management Tools
  See "About installing the Exchange System Management Tools on the remote server" on page 182.

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.

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 website, refer to article 834121: http://support.microsoft.com

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.

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.

Troubleshooting Exchange restore operations

Review the following information to troubleshoot any issues with Exchange restore operations:

- Event ID 2059 is logged after a successful restore.
  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 article for information on how to resolve this issue:
  http://www.veritas.com/docs/TECH88101
- A restore of an Exchange database that contains a bracket in the name may fail.
  A restore of an Exchange database that contains a bracket in the name (for example, Exch_DB[Sales]), may fail if you select multiple images in the left pane of the Backup, Archive, and Restore (BAR) interface. To work around this issue, select the images to be restored one at a time.

Restores to different Exchange service pack or different cumulative update levels

The NetBackup for Exchange Agent supports a restore to the same Microsoft service pack (SP) or cumulative update (CU) on which the backup was originally created. Microsoft sometimes introduces database schema changes in SPs or CUs. If you restore to a different SP or CU level, the database server may not operate correctly.

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.

Dynamic enforcement of path length limit for Exchange backups and restores

The NetBackup Administrator's Guide, Volume I details that files and directories with path lengths greater than 1023 are automatically excluded from backups. For GRT-enabled backups, the path length limit applies to individual mailbox folders and messages. 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 from a snapshot image, the restore fails if an `Exxrestore.env` file exists in the transaction log folder for the database. 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.
- The memory usage of `bpfis.exe` grows when NetBackup processes a snapshot of multiple databases. In NetBackup testing, the `bpfis.exe` process memory usage grows by a few MB per storage group or database. If a single snapshot job processes a large number of databases, the process virtual memory size can exceed 1 GB. To work around this issue, make sure that you have sufficient virtual memory to accommodate this growth. Or, break up your backup into smaller snapshots.

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 SANSurfer software. It may conflict with the portmapper for Client for NFS.
- Before you install NFS on the media server or client(s), look for the ONC/RPC Portmapper service. If it exists, stop it and disable it. Otherwise, the installation of NFS Services for Windows fails.
- Exchange GRT operations can fail for the VM backup images that use display names that contain parenthesis. For example, a GRT live browse restore from the Backup, Archive, and Restore (BAR) interface fails with the following error:

  ```
  database system error
  ```
- (Exchange 2010) The “Company” information for task objects is not restored.
- 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. Look at the bpbkar debug log for more information.
- NetBackup must be able to contact the proxy host (if applicable) 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 “Exchange granular clients and non-VMware backups ” on page 47.
- For Exchange 2010, the following situations cause a restore to fail with a status 5:
  - Restores of a private mailbox item to a Public Folder
  - Restores of a Public Folder item to a private mailbox

  In the `ncfgre` log, the following error appears:

```
EWS Failed to get mailbox properties
```

- If you attempt to restore an Exchange 2010 Public Folder item to a subfolder that has not been previously created, the restore fails with a status 5. The following error appears in the progress log:

  ```
  MNR - error writing file: %1
  ```

  Use one of the following workarounds to resolve this issue:

  - Retry the restore operation. NetBackup receives an error when it attempts to create the new subfolder. However, the subfolder is created. A second restore attempt to the same subfolder location is successful.
  - Create the subfolder manually before you attempt the restore. If the subfolder exists, the restore is successful.
- Technical Support may want `nbfsd` logs from the media server. Use the Verbose setting carefully as the `nbfsd` log can grow very large.

Increased memory usage with Exchange 2010 and 2013

As you increase the number of mailbox users with Exchange 2010 or Exchange 2013, `MONAD.EXE` uses more memory during backup operations. Veritas is working with Microsoft to fix this problem.

Troubleshooting DAG backups and restores

The followings issues exist for DAG backups and restores:

- The status of a DAG backup can be empty if the restore is initiated from a node in the DAG.

  When you restore databases or granular items of a database availability group (DAG) backup, the restore status may appear empty from the Backup, Archive, and Restore (BAR) interface. The status is empty if the restore is initiated from a node in the DAG. You should initiate the restore from the active DAG node or a NetBackup server to properly see the activity status.
- User-initiated backups in a DAG environment fail if initiated from a node in the DAG that is not currently active.

  User-initiated backups in a DAG environment fail if initiated from a node in the DAG that is not currently active for the virtual DAG name. Initiate the user backup

from the active DAG node, or manually start the backup from the NetBackup master to properly start the backup.

Finding the current host server of the Database Availability Group (DAG)

To find the current host server of the Database Availability Group (DAG)

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**.

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 104.

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
```

Troubleshooting VMware backups and restores of Exchange Server

Note the following when you perform a VMware backup that protects an application:

- One Application State Capture job is created per VM, regardless of which applications are selected in policy.
- The ASC job can fail if the VMware disk layout has changed since the last discovery. In this situation, you must force NetBackup to rediscover virtual machines by lowering the value of the **Reuse VM selection query results for** option. See the NetBackup for VMware Administrator's Guide.
- 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 Veritas VSS provider 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.
- If you do not include the volume where Exchange is installed in a VMware backup, granular browse operations fail.
  If you perform a VMware backup with Exchange protection, ensure that you include the volume where the Exchange server is installed. For example, if NetBackup is installed on `F:\` and the Exchange server is installed on `C:\`, include `C:\` in the backup.

Appendix A

NetBackup Legacy Network Service (Exchange 2010)

This appendix includes the following topics:

Configuring the logon account for the NetBackup Legacy Network Service (Exchange 2010)

Note: Previous to NetBackup 7.6, for Exchange 2010 DAG configurations you had to configure the logon account for NetBackup Legacy Network Service. The logon account required permission to perform Exchange database operations and granular (GRT) operations. This configuration is no longer required; configure the Exchange credentials in the client host properties. Veritas recommends that you use this new configuration, though existing NetBackup customers can continue to configure the logon account for this service.

By default, the NetBackup Legacy Network Service uses “Local System” account to log on. A different account is required so NetBackup has the necessary local system privileges to perform Exchange 2010 DAG backups.

Note the following:

- Perform the steps on each mailbox server in the DAG.

- For restores with GRT, configure each client that performs granular operations. To determine which clients to configure, see the following topic:
  See "Exchange granular clients and non-VMware backups " on page 47.
  See "Exchange granular clients and VMware backups" on page 49.

To configure the logon 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 of the account for NetBackup Exchange operations that you previously created. To change the **Log on as** account, you must have administrator group privileges.

   See "Creating a privileged NetBackup user account for EWS access" on page 32.

   See "Creating a minimal NetBackup account for Exchange operations" on page 33.

   The account must include the domain name, followed by the user account, ***domain_name**account***. For example, **recovery\netbackup**.
5. Provide the password.
6. Click **OK**.
7. Stop and start the NetBackup Legacy Network Service.
8. Close the Services control panel application.

Index

P

R

S

T

U

V

W