Veritas NetBackup™ for Microsoft SharePoint Server Administrator's Guide

for Windows

Release 9.1

VERITAS™

Veritas NetBackup™ for Microsoft SharePoint Server Administrator's Guide

Last updated: 2021-05-27

Legal Notice

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 6   **Performing backups and restores of SharePoint Server and SharePoint Foundation** 68

Chapter 7   **Protecting SharePoint Server data with VMware backups** 91

Introducing NetBackup for SharePoint Server

This chapter includes the following topics:

- About NetBackup for SharePoint Server

- Features of NetBackup for SharePoint

- SharePoint Server backup operations

- SharePoint Server restore operations

- Limitations on SharePoint Server backups and restores

- NetBackup File System Daemon

About NetBackup for SharePoint Server

NetBackup for SharePoint extends the capabilities of NetBackup to include online backups and restores SharePoint Server. The NetBackup agent for Microsoft SharePoint Server is an optional, add-on component to the NetBackup for Windows client software. Because this product is tightly integrated with the Backup, Archive, and Restore interface, this manual provides only an overview of NetBackup functionality. Backup operations and restore operations for SharePoint Server are identical to other NetBackup file operations, except where noted.

Microsoft SharePoint Server or Microsoft Office SharePoint Server may be abbreviated to either SharePoint Server or to SharePoint. Unless otherwise noted, the text implies SharePoint Foundation when SharePoint is discussed.

Features of NetBackup for SharePoint

Table 1-1 describes the features for the NetBackup for SharePoint Agent.

Table 1-1 NetBackup for SharePoint Agent features

Feature	Description
Online backup	SharePoint Server objects can be backed up without taking the SharePoint Server offline. SharePoint services and data are available during the backup.
SharePoint Server backup methods	NetBackup supports full and differential-incremental backups of SharePoint.
Tight NetBackup integration	Tight integration with NetBackup means the following: ■ An administrator already familiar with NetBackup procedures and software can easily configure and use NetBackup to perform SharePoint Server backup and restore operations. ■ Features and strengths of the NetBackup product suite are available to the SharePoint Server backup user. These features include scheduled and user-directed operations, backups of multiple data streams, and in-line tape copy. These features are described in detail. See the NetBackup Administrator's Guide, Volume I.
Central administration	You can administer the backup and recovery of multiple SharePoint Server installations from a central location.
Media management	SharePoint Server backups are saved directly to a wide variety of storage devices that NetBackup supports.
Automated backups	Administrators can set up schedules for automatic, unattended backups for local or remote clients across the network. These backups are managed entirely by the NetBackup server from a central location. The administrator can also manually back up the clients. Auto discovery is used for SharePoint Server installations. The topology is read from the SharePoint front-end Web server and the backup selection list is automatically built.
User-directed backups	A user can perform backups of SharePoint Server resources through the Backup, Archive, and Restore client interface on the front-end Web server.
Backups and restores of standalone SharePoint Foundation or Windows SharePoint Services (WSS)	NetBackup can back up and restore standalone installations of SharePoint Foundation or Windows SharePoint Services.
Support for VMware backups that protect SharePoint	VMware backups that protect SharePoint Server provide granular recovery, complete protection of the farm, and protection of the SharePoint components in the Windows files system.

Table 1-1   NetBackup for SharePoint Agent 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 compression of the backups that use Granular Recovery Technology (GRT).
Encryption	When the Encryption attribute is enabled, the server encrypts the backup for the clients that are listed in the policy. NetBackup does not support encryption of any backups that use GRT.
Restore operations	An administrator who uses the Backup, Archive, and Restore interface can browse SharePoint Server backups and select the ones to restore.
Support for NetBackup Accelerator with VMware backups	NetBackup Accelerator can reduce by up to 90% the time it takes to perform a VMware backup that protects SharePoint. By reducing the backup time, it is easier to perform the VMware backup within the backup window. Accelerator support for SharePoint currently restricts backups to the full schedule type. This restriction also exists for a VMware backup that protects SharePoint without Accelerator.
Restores of individual items and document sets using Granular Recovery Technology (GRT)	When a backup uses GRT, users can restore individual lists, items, and documents sets directly from any full database backup of a Web application. This feature adds an extra step that identifies the items within the database. This step lets you recover individual items later. (Note that you must create a separate backup for the full farm.)
Support for claims-based authentication	Claims-based authentication (CBA) is now supported for web applications in SharePoint. The following providers are supported: ■ Windows authentication (LDAP) ■ Facebook ■ LinkedIn ■ Live Id ■ Forms-based authentication (FBA), using SQL Server ■ ADFS 2.0
Redirected restore	You can redirect the restore of the following: ■ SharePoint web application within a farm. ■ SharePoint web application to another farm. ■ SharePoint Content database to another SQL instance, to take advantage of data recovery from an unattached content database.
Multi-tenant environments	Backup and recovery of SharePoint Server databases are fully supported in a multi-tenant environment. NetBackup does not support GRT with Microsoft SharePoint Server backups in a multi-tenant SharePoint environment.

Table 1-1	NetBackup for SharePoint Agent features *(continued)*
Feature	**Description**
Support for any backups that were created with previous NetBackup versions	You can restore the backups that were created with previous versions of NetBackup. However, features in the current release are not supported with any backups that were created with previous versions.

SharePoint Server backup operations

You can use the NetBackup for SharePoint Server agent to back up the entire SharePoint Server farm or individual components. NetBackup provides the following methods to perform backups:

- Automatic

- Manual

- User-directed

The NetBackup administrator can schedule the backups that occur automatically and unattended under the control of the NetBackup Server. The following types of automatic backups are available:

Full schedule	The entire contents in the backup selections list are backed up.
Differential incremental	Only the contents that have been added or changed since the previous full or incremental are included in the backup.

Manual backup may be used for special events. A manual backup includes all the items in the backup selections list of the policy you selected for backup.

User directed backups require a User Backup schedule to be defined on a SharePoint policy on the NetBackup Server. A user-directed backup includes the entire contents of the items that are selected for backup. This type of backup is only supported from the SharePoint application host, not on other hosts where only SharePoint objects are present.

SharePoint Server restore operations

Use the Backup, Archive, and Restore interface to initiate SharePoint Server restore operations. This interface lets you select the NetBackup Server from which the objects are restored and the client whose backups you want to browse. Based upon these selections, you can browse the backup history, select individual items and

launch a restore. The NetBackup Recovery Assistant lets you restore SharePoint resources with one click and determines the sequence in which the resources are restored.

An administrator can browse for and restore databases and individual items. Users also can restore the security settings on a selected item. Objects that users can restore include the following:

- One or more databases

- Individual documents in a Document library

- Entire sites

- Subsites

- Entire lists or libraries

- Document sets

- Individual list items or documents

Limitations on SharePoint Server backups and restores

The following limitations exist when you perform backups and restores of SharePoint Server:

- Due to Microsoft API limitations, NetBackup does not support backups of the Application Registry service application.

- Project Server databases are not protected.

- Reporting Services are not supported.

- The FAST Search service application under SharePoint is not protected.

- The following cannot be redirected to another web application:

    - Documents and folders

    - Farm Configuration database and Single Sign-on database

    - Index Files or Index database

- NetBackup does not support restores of customized SharePoint Solution Packages (`.wsp`) or third-party Web Part customizations.

- Web Parts on the home page of the site collection and subsite do not retain their formatting when you restore with GRT at the site collection and subsite level.

- NetBackup does not support GRT restores of deleted lists and PerformancePoint Dashboards. For example, Microsoft OneDrive sync fails after you perform the GRT restore of the list or the OneDrive web app that is deleted.

- Restoring a SharePoint Help Search database and index files results in a successful restore. However, the SharePoint Help Search is not extended to use the restored database and index files.

- When you direct items to a file system, any list items you selected are not restored and appear as 0-KB files.

- In SharePoint 2016 and 2019, restore jobs related to the **Basic Search Center** template fail with an error message.

- For limitations on operations with Granular Recovery Technology (GRT), see the following topic:
  See "Limitations and conditions for restores that use SharePoint Granular Recovery Technology (GRT)" on page 37.

NetBackup File System Daemon

The NetBackup File System Daemon (NBFSD) on the NetBackup media server is a process that allows NetBackup clients to mount, browse, and read NetBackup (tar) images. This process is used with a client for Granular Recovery Technology (GRT) operations. These operations include backups, browsing for backup images, restores, and duplication.

Installing NetBackup for SharePoint Server

This chapter includes the following topics:

- Planning the installation of NetBackup for SharePoint

- Verifying the operating system and platform compatibility

- NetBackup server and client requirements

- SharePoint server software requirements

- Requirements for installing the SQL Server back-end servers in a cluster

- About the license for NetBackup for SharePoint

Planning the installation of NetBackup for SharePoint

Perform the following tasks before you use NetBackup for SharePoint.

Table 2-1   Installation steps for NetBackup for SharePoint

Step	Action	Description
Step 1	Verify the operating system and platform compatibility.	See "Verifying the operating system and platform compatibility" on page 15.
Step 2	Verify the NetBackup server and client requirements for NetBackup for SharePoint.	See "NetBackup server and client requirements" on page 15.

	Table 2-1	Installation steps for NetBackup for SharePoint *(continued)*
Step	**Action**	**Description**
Step 3	Verify that master server has a valid license for NetBackup for SharePoint and any NetBackup options or add-ons that you want to use.	See "About the license for NetBackup for SharePoint" on page 17.

Verifying the operating system and platform compatibility

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

To verify operating system and compatibility

1   Go to the NetBackup compatibility list site.

     http://www.netbackup.com/compatibility

2   Click on the following document:

     Application/Database Agent Compatibility List

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

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

NetBackup server and client requirements

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

- The NetBackup server software is installed and operational on the NetBackup server.
  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 that are used and storage capacity of the media

  - 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

- The length of retention of the backup images
  See the NetBackup Administrator's Guide, Volume I.

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

- The NetBackup client software is installed on all SharePoint servers, except the Search server or Job server. In a VMware environment, the NetBackup client software must be installed on the virtual machines that are part of a SharePoint farm.

- To use the new features that are included in NetBackup for SharePoint in NetBackup 9.1, you must upgrade your NetBackup for SharePoint clients to NetBackup 9.1. The NetBackup media server must use the same version as the NetBackup for SharePoint client or a higher version than the client.

SharePoint server software requirements

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

- SharePoint server software must be installed and operational.

- The Microsoft .NET Framework 3.5 is installed on the SharePoint servers.

- When you use multiple front-end SharePoint servers, all front-end server web sites must be uniformly identified in IIS. Identify the sites with either host headers or IP addresses, but not both. An environment that mixes host headers and IP addresses across multiple front-end servers is not supported.

- To prevent restore failures, the IIS Default Application Pool identity must be a valid SharePoint user ID.

- The SharePoint user should be an administrator user account.

See "NetBackup server and client requirements" on page 15.

Requirements for installing the SQL Server back-end servers in a cluster

NetBackup supports clustering of a back-end SQL Server in a Windows Server Failover Clustering (WSFC) environment. The same version of NetBackup must be used on each node in the cluster.

For more information, see your WSFC documentation.

About the license for NetBackup for SharePoint

The NetBackup for SharePoint 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.

Installing and configuring NFS for SharePoint Granular Recovery

This chapter includes the following topics:

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

- Requirements for SharePoint Granular Recovery

- Configurations that are supported for SharePoint Granular Recovery

- About configuring Services for Network File System (NFS)

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

- Configuring a different network port for NBFSD

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

NetBackup uses Granular Recovery Technology (GRT) and Network File System (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

The NetBackup client mounts and accesses a mapped drive over a secure connection to the NetBackup media server. The NetBackup media server handles the client requests through the NetBackup File System (NBFS) service, or NBFSD.

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

Requirements for SharePoint Granular Recovery

Table 3-1   Requirements for SharePoint Granular Recovery

Step	Action	Description
Step 1	You have a supported SharePoint Server configuration.	See the Application/Database Agent Compatibility List.
Step 2	You have a media server platform that supports GRT.	See the Software Compatibility List (SCL).
Step 3	On all SQL back-end servers and the media server, ensure that each node has an assigned drive letter on which to mount the backup image.	
Step 5	Enable or configure NFS for your environment: ■ Windows media server and clients ■ UNIX media server and Windows clients	See "About configuring Services for Network File System (NFS)" on page 20. See "Configuring a UNIX media server and Windows clients for backups and restores that use Granular Recovery Technology (GRT)" on page 30.

Configurations that are supported for SharePoint Granular Recovery

For information on the SharePoint and SQL Server back-end versions and the Windows Server releases that are supported for Granular Recovery Technology (GRT) see the Application/Database Agent Compatibility List.

For information on the media server platforms that are supported for Granular Recovery Technology (GRT) see the Software Compatibility List (SCL).

About configuring Services for Network File System (NFS)

To restore individual items from a database backup, you must configure Services for Network File System (NFS) on the NetBackup media server and on the SQL back-end servers.

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

Table 3-2 Configuring NFS on Windows 2012, 2012 R2, or later

Step	Action	Description
Step 1	Configure NFS on the media server.	**Note:** For VMware backups that protect SharePoint, you do not need to configure NFS on the media server. 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 media server" on page 21. ■ Stop the Server for NFS service. See "Disabling the Server for NFS" on page 28. ■ Stop the Client for NFS service. See "Disabling the Client for NFS on the media server" on page 26. Note: If a SQL back-end server 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 SQL back-end servers.	On the SQL back-end servers, do the following: ■ Enable NFS on the clients. See "Enabling Services for Network File System (NFS) on a client" on page 24. ■ Stop the Server for NFS service. See "Disabling the Server for NFS" on page 28.

Enabling Services for Network File System (NFS) on a media server

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

To enable Services for Network File System (NFS) on a media server

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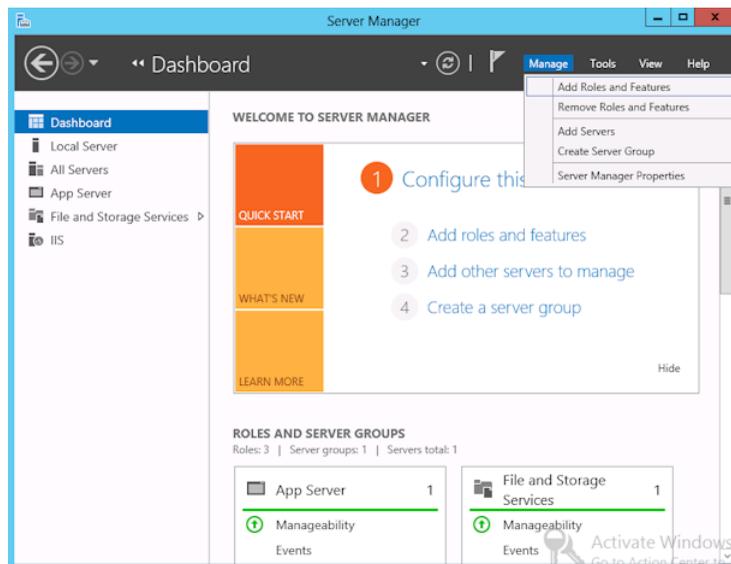
2   From the **Manage** menu, click **Add Roles and Features**.

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**.
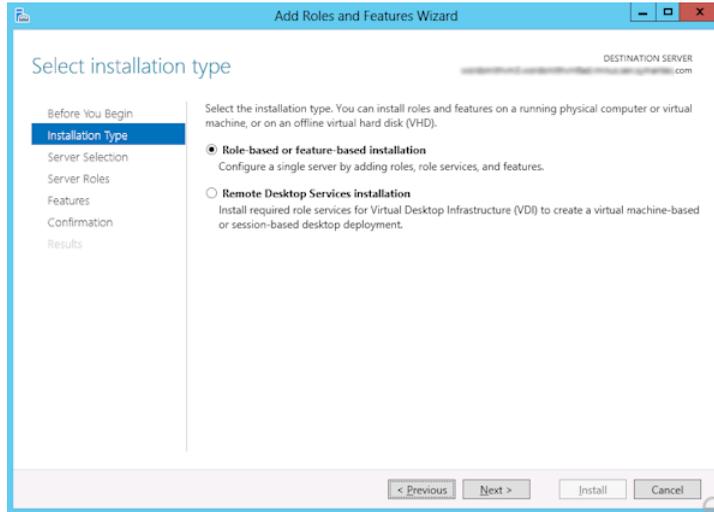
5 Click **Next**.

6 On the **Server Selection** page, click **Select a server from the server pool** and select the server. Click **Next**.
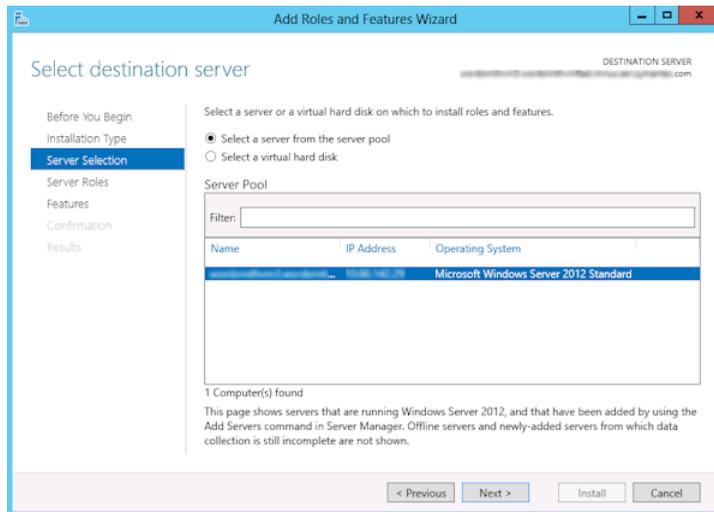
7 On the **Server Roles** page, expand **File and Storage Services** and **File and iSCSI Services**.

8 Click **File Server** and **Server for NFS**. When you are prompted, click **Add Features**. Click **Next**.
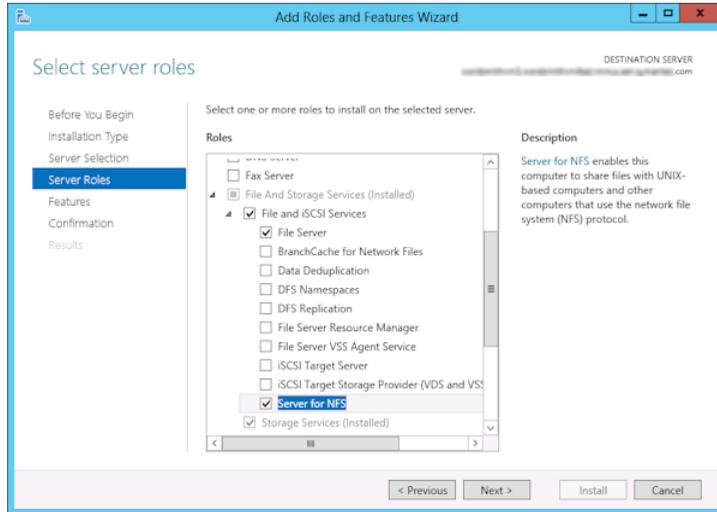
9 If the media server is also an SQL back-end server, on the **Features** page, click **Client for NFS**. Click **Next**.
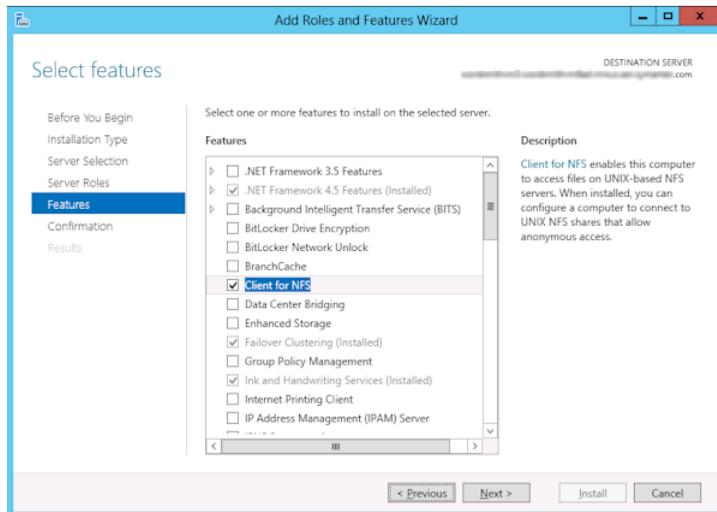
10 On the **Confirmation** page, click **Install**.

11 Disable any unnecessary services, as follows:

- If you have a single host that functions as both the media server and the SQL back-end server, you can disable the Server for NFS service.
  See "Disabling the Server for NFS" on page 28.

- 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 28.
  See "Disabling the Client for NFS on the media server" on page 26.

Enabling Services for Network File System (NFS) on a 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 SQL back-end servers, you can disable any unnecessary NFS services.

To enable Services for Network File System (NFS) on a Windows client

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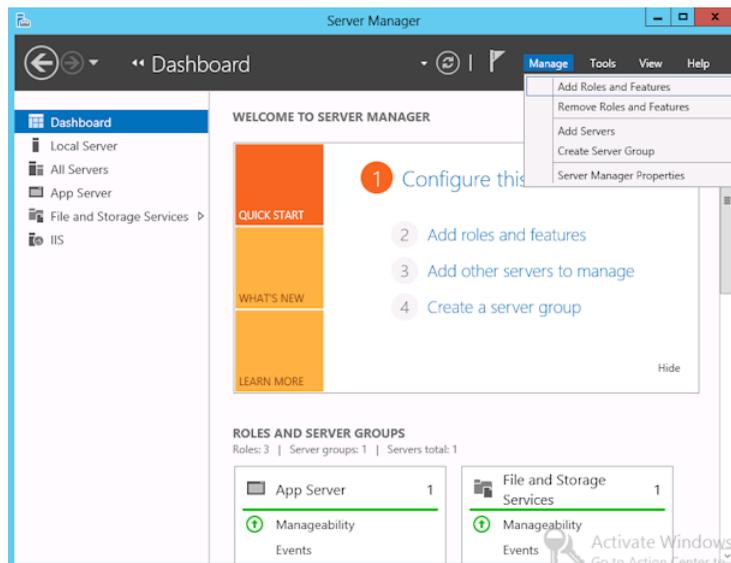
2 From the **Manage** menu, click **Add Roles and Features**.

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**.
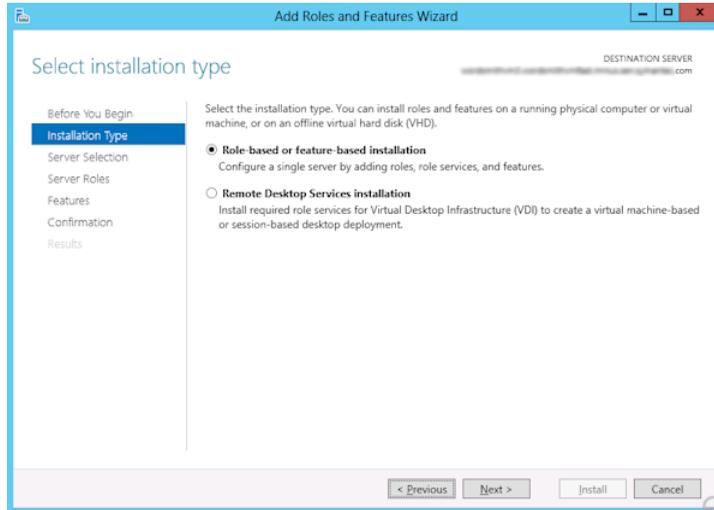
5 Click **Next**.

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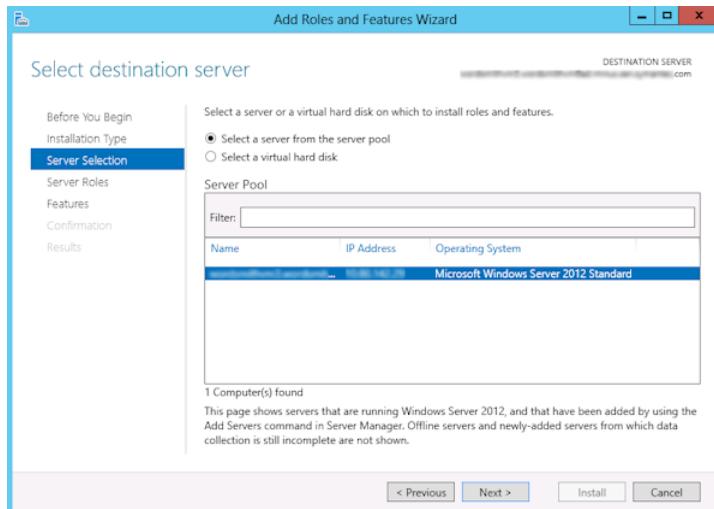
7 On the **Server Roles** page, click **Next**.

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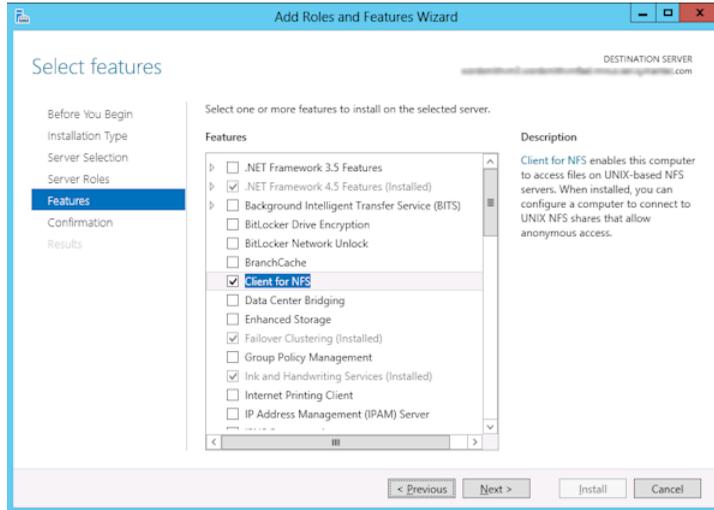
9 On the **Confirmation** page, click **Install**.

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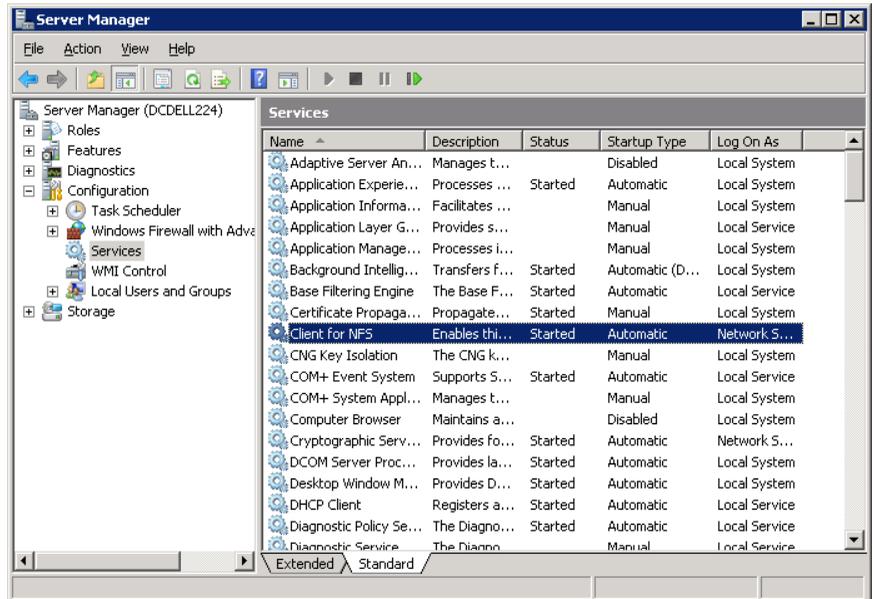
4   In the right pane, right-click on **Client for NFS** and click **Stop**.

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**.
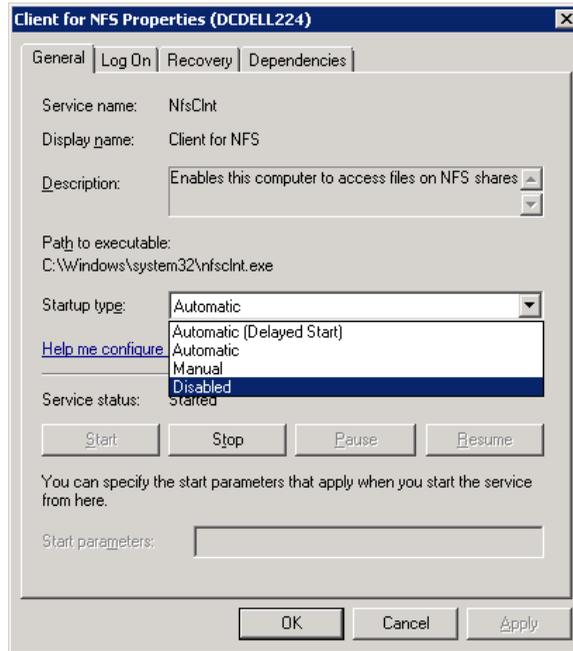
7 Click **OK**.

Disabling the Server for NFS

After you enable Services for Network File System (NFS) on the media server and on the SQL back-end servers, 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**.

Installing and configuring NFS for SharePoint Granular Recovery | 30
**Configuring a UNIX media server and Windows clients for backups and restores that use Granular Recovery
Technology (GRT)**

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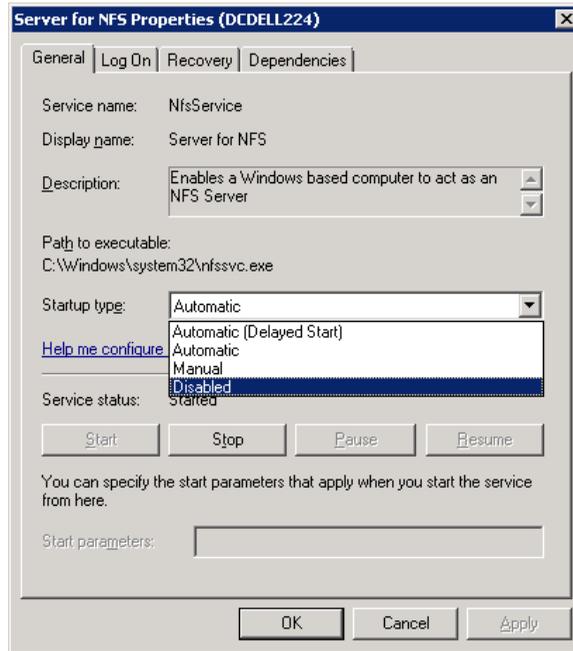
7   Click **OK**.

8   Repeat this procedure for the media server and for each SQL back-end server.

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.
    For more information about supported platforms, see the *NetBackup Enterprise
    Server and Server - OS Software Compatibility List* at the following URL:

■   No other configuration is required for the UNIX media server.

- Enable or install NFS on the SQL back-end servers.
  See "Enabling Services for Network File System (NFS) on a media server" on page 21.
  See "Enabling Services for Network File System (NFS) on a client" on page 24.
- You can configure a different network port for NBFSD.
  See "Configuring a different network port for NBFSD" on page 31.

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*

Configuring NetBackup for SharePoint Server

This chapter includes the following topics:

- About configuring NetBackup for SharePoint

- About a SharePoint non-granular backup vs. a backup that uses Granular Recovery Technology (GRT)

- Configuring a SharePoint backup that uses Granular Recovery Technology (GRT)

- Configuring the logon account for the NetBackup Client Service for NetBackup for SharePoint

- Configuring the logon account for the NetBackup Legacy Network Service and the NetBackup Legacy Client Service

- Configuring SharePoint client host properties

- Configuring mappings for restores of a distributed applications, clusters, or virtual machines

- Reviewing the auto-discovered mappings in Host Management

- Performing a manual backup

About configuring NetBackup for SharePoint

To successfully perform backups and restores of SharePoint Server, complete the following steps. For additional information on how to configure NetBackup in preparation of VMware backups that protect SharePoint, refer to the following topics.

See "About protecting an application database with VMware backups" on page 91.

Table 4-1   Configuring NetBackup for SharePoint

Step	Action	Description
Step 1	Review the information for configuring the backup and the restore operations that use Granular Recovery Technology (GRT).	GRT lets you restore individual documents, etc., from a database backup. GRT is an option limited to certain versions of SharePoint Server and Windows Server. GRT is included in VMware backups that protect SharePoint. See "Configuring a SharePoint backup that uses Granular Recovery Technology (GRT)" on page 35.
Step 2	Configure the NetBackup Client Service.	Required if you want to restore individual items with GRT. See "Configuring the logon account for the NetBackup Client Service for NetBackup for SharePoint " on page 38.
Step 3	Configure the NetBackup Legacy Network Service and (optionally) the NetBackup Legacy Client Service.	See "Configuring the logon account for the NetBackup Legacy Network Service and the NetBackup Legacy Client Service" on page 39.
Step 4	Configure the host properties for SharePoint clients.	See "Configuring SharePoint client host properties" on page 39.
Step 5	Configure the mappings for distributed application restores.	Map the application hosts and component hosts in your environment. Configure these mappings in the **Distributed Application Restore Mapping** host property on the master server. See "Configuring mappings for restores of a distributed applications, clusters, or virtual machines " on page 45.
Step 6	On the NetBackup server, review the 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 46.

Table 4-1   Configuring NetBackup for SharePoint *(continued)*

Step	Action	Description
Step 7	Select the backup and the recovery strategies that fit your environment.	See "About backup policies for granular backup and recovery of SharePoint Server " on page 50.
		See "About backup policies for SharePoint farm backup and recovery" on page 51.
		See "About backup policies for disaster recovery of SharePoint Server" on page 53.
		See "About VMware backup policies that protect SharePoint Server" on page 55.
Step 8	Test your configuration settings.	See "Performing a manual backup" on page 48.

About a SharePoint non-granular backup vs. a backup that uses Granular Recovery Technology (GRT)

Non-granular backups allow the restore of SharePoint objects at the level of a Web Application. This type of backup also allows the restore at the level of the Single Sign-on database. Individual items cannot be restored from non-granular backups.

To restore individual items using Granular Recovery Technology (GRT), NetBackup performs a granular-level backup of the SharePoint Web Application. You can restore the entire database or you can restore items individually. Items can then be restored to the existing Web Application.

Note: The farm databases (Configuration, Single Sign-on, Index Files and their Search databases) cannot be backed up with a policy that is enabled for individual item restores (GRT). For comprehensive farm disaster recovery, back up those databases with a separate policy where granular recovery is disabled.

Table 4-2 describes what SharePoint objects can be restored with non-granular and granular-level backups.

Table 4-2   SharePoint Server non-granular backup vs. a backup that uses Granular Recovery Technology

Object	Can be restored from a non-granular backup	Can be restored from a backup that uses Granular Recovery Technology
Configuration database	Yes*	No
Single Sign-on database	Yes*	No
Global Settings	Yes*	No
Index Files and their Search databases	Yes*	No
Web Applications or Content databases	Yes	Yes
Site collections	No	Yes
Subsites	No	Yes
Individual lists or libraries	No	Yes
Individual documents or list items	No	Yes

* Only restore these items as part of a farm restore.

Configuring a SharePoint backup that uses Granular Recovery Technology (GRT)

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

See "Requirements for SharePoint Granular Recovery" on page 19.

Table 4-3 Configuring a SharePoint backup that uses Granular Recovery Technology (GRT)

Step	Action	Description
Step 1	Review the limitations and conditions.	See "Disk storage units supported with SharePoint Granular Recovery Technology (GRT)" on page 36. See "Limitations and conditions for restores that use SharePoint Granular Recovery Technology (GRT)" on page 37.
Step 2	On all SQL Server back-end servers, configure the NetBackup services log on accounts: - NetBackup Client Service as the SharePoint administrator - NetBackup Legacy Network Service as the Local System account (Optional) NetBackup Legacy Client Service as the Local System account	See "Configuring the logon account for the NetBackup Client Service for NetBackup for SharePoint " on page 38. See "Configuring the logon account for the NetBackup Legacy Network Service and the NetBackup Legacy Client Service" on page 39.
Step 3	On each SharePoint server in the farm assign the local security privileges.	See "Configuring local security privileges for the SharePoint Servers" on page 43.
Step 4	For backups in non-virtual environments, select **Enable granular recovery** in the backup policy.	Granular recovery is automatically provided for a VMware backup that protects SharePoint Server. You do not need to enable it in the policy. See "Adding a NetBackup for SharePoint policy" on page 56.

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

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

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

See NetBackup Enterprise Server and Server - Hardware and Cloud Storage Compatibility List.

Limitations and conditions for restores that use SharePoint Granular Recovery Technology (GRT)

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

- The feature is limited to certain versions of SharePoint Server and Windows Server. See the Software Compatibility List (CL) and the Application/Database Agent Compatibility List.

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

- NetBackup does not support Granular Recovery Technology (GRT) with Microsoft SharePoint Server backups in a multi-tenant SharePoint environment.

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

- Backups with GRT do not support any content databases that exist on multiple servers in a farm.

- Granular Recovery with Remote BLOB Storage providers is not supported; however, you can backup and restore the entire farm or databases. Refer to the following TechNote.
  Remote BLOB Storage (RBS) and NetBackup

- When you perform a granular recovery of documents, pictures, or list items that are part of a workflow, the state of these items is not preserved.

- NetBackup does not support backups and restores with GRT if you use a third-party document management software to manage your SharePoint documents. For example, NextDocs.

- (SharePoint 2016 and later) If you edit the title of a list item, SharePoint creates a new version for those list items. When you select all list item versions for restore, NetBackup creates a new list item for only those versions whose title is different than the original list item title. As a workaround, restore the list.

- (SharePoint 2016 and later) If the list item version you selected for restore has a different title than the original list item title and the **Restore over existing items option** is also enabled, the restore job fails with an error message. As a workaround, restore the list.

- (SharePoint 2016 and later) When you use Granular Recovery Technology (GRT) to restore ghosted or uncustomized aspx pages from any template, the restore job is successful, but the restored pages appear with the default content

when it was created. This issue is not seen if the aspx pages are uploaded to SharePoint. Such pages are treated as customized pages.

To work around this issue, restore the SharePoint web application content database. See "Redirecting the restore of a SharePoint Server Web application content database to an alternate SQL Server instance" on page 89.

- For backups that use GRT, a redirected restore to a file system is not supported.

- The Restore GRT Basic Meeting Workspace shows errors when you restore even though the restore completed.

- The following site templates are not supported with SharePoint restores that use GRT:

  - Product Catalog

  - Community Site

- If you perform a restore with Granular Recovery Technology (GRT), any SharePoint user ratings and tags are synchronized to the current settings of the user rating and tags in the respective metadata databases.

- Dependent items of blog posts (including comments and images) are not restored with restores that use Granular Recovery Technology (GRT).

- When you restore a list item from a localized subsite, the job is reported as successful. However the list item fails to appear in the SharePoint user interface. To work around this issue, restore the item to a file system and upload the item to SharePoint.

Configuring the logon account for the NetBackup Client Service for NetBackup for SharePoint

The NetBackup Client Service must log on with an account that has local administrator and SharePoint farm administrator privileges.

Configure the service for the hosts where the Index Files or Index databases and where the document libraries reside. For any backups that use Granular Recovery Technology (GRT), configure this service on all SQL back-end servers.

Note: For VMware backups and restores, configure the NetBackup Client Service on the systems that you use to browse for backups and the systems you use to perform restores.

To configure the logon account for the NetBackup Client Service for NetBackup for SharePoint

1   In the Windows Services application, open the **NetBackup Client Service** entry.

2   On the **Log On** tab, provide the following:

   - For the **Log on as** account, provide the account name that has local administrator and SharePoint farm administrator privileges.

   - Type the password.

3   Stop and start the NetBackup Client Service.

Configuring the logon account for the NetBackup Legacy Network Service and the NetBackup Legacy Client Service

The NetBackup Legacy Network Service must log on with the Local System account. Optionally, you can also configure the NetBackup Legacy Client Service with the Local System account.

Configure the service for the hosts where the Index Files or Index databases and where the document libraries reside. For the backups that use Granular Recovery Technology (GRT), configure the service on all SQL back-end servers.

To configure the logon account for the NetBackup Legacy Network Service and the NetBackup Legacy Client Service

1   In the Windows Services application, open the **NetBackup Legacy Network Service** entry.

2   On the **Log On** tab, provide the following:

   - For the **Log on as** account, select **Local System account**.

   - Type the password.

3   Stop and start the NetBackup Legacy Network Service.

4   (Optional) Follow the same process for the NetBackup Legacy Client Service.

Configuring SharePoint client host properties

In the SharePoint client host properties you configure settings for the SharePoint clients you selected. Configure the host properties for all servers in the SharePoint farm. 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 SharePoint 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 SharePoint client(s) you want to configure.

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

4   Click **Actions > Properties**.

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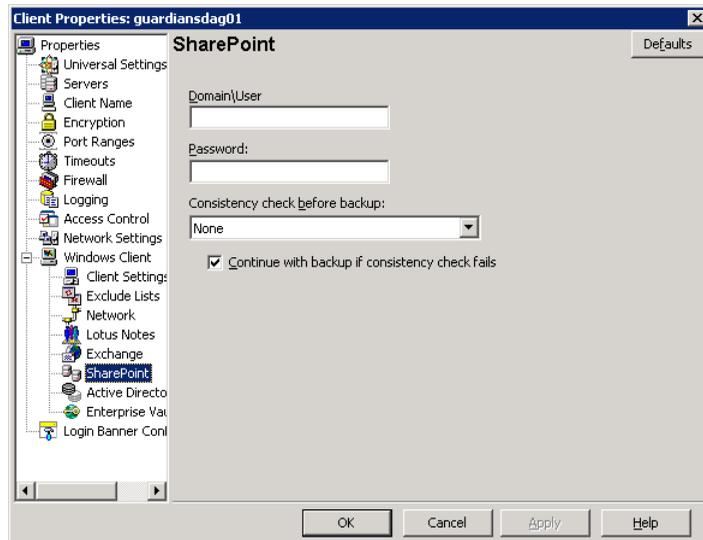
6   Enable the options you want.

    See "SharePoint properties" on page 40.

7   Click **OK**.

SharePoint properties

The **SharePoint** properties apply to currently selected Windows clients to protect SharePoint Server installations.

Figure 4-1   SharePoint dialog box
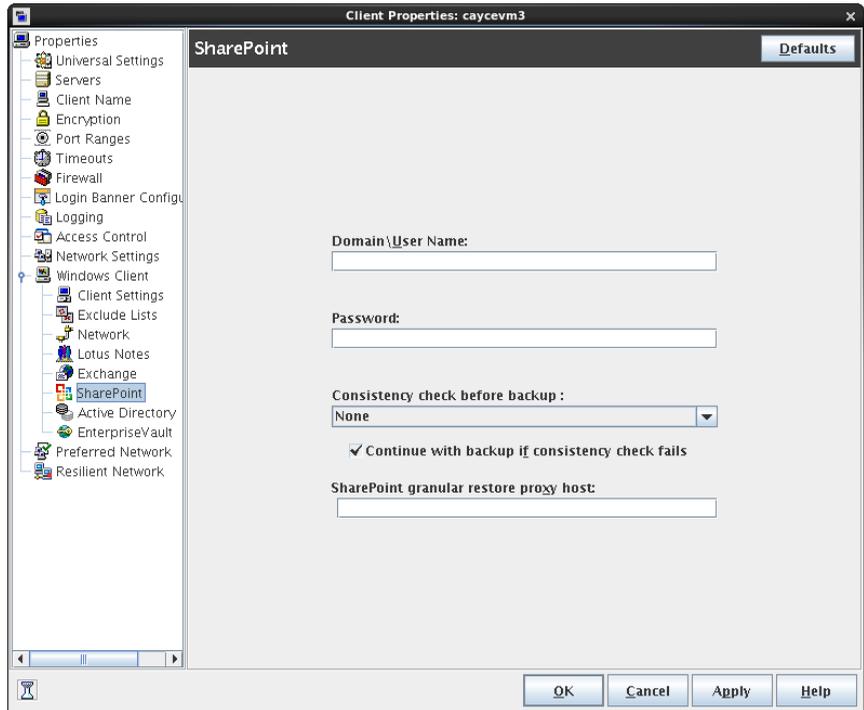
The **SharePoint** dialog box contains the following properties.

Table 4-4   SharePoint dialog box properties

Property	Description
Domain\User name	Specifies the domain and the user name for the account you want to use to log on to SharePoint (DOMAIN\user name). See "Specifying the account that logs on to the SharePoint application server" on page 42.
Password	Specifies the password for the account.

Table 4-4   SharePoint dialog box properties *(continued)*

Property	Description
Consistency check before backup	Specifies the consistency checks to perform on the SQL Server databases before NetBackup begins a backup operation. These checks are performed for both server-directed and user-directed backups.
	If you choose to perform a consistency check, you can select **Continue with backup if consistency check fails**. NetBackup then continues to perform the backup if the consistency check fails.
	See "Performing consistency checks with NetBackup for SharePoint backups" on page 44.
	See "Consistency check options for SharePoint Server" on page 44.
SharePoint granular restore proxy host	For VMware backups that protect Federated SharePoint configurations, provide the name of the back-end SQL server. This server acts as the granular restore proxy host for the catalog hosts (front-end servers in the farm).
	See "Configuring the granular proxy host for Federated SharePoint configurations with VMware" on page 96.

Specifying the account that logs on to the SharePoint application server

To perform backups and restores, NetBackup must know the user name and password of the account for the SharePoint administrator. NetBackup also requires this information so you can browse for SharePoint objects when you create a backup policy. NetBackup validates the user name and password you provide.

This account must meet the following requirements:

- Have the following rights on the servers where the SharePoint components are installed: Local administrative privileges and site collection administration rights.

- SharePoint farm administrator account.

- The front-end server must have registry access to the back-end database servers.

- Have certain local security privileges on the servers which have the content of the SharePoint farm.
  See "Configuring local security privileges for the SharePoint Servers" on page 43.

- Internet Information Services (IIS) rights can affect database backups and restores. Ensure that the logon account that is used for backups and restores has rights to access the IIS sites. Integrated Windows Security should be enabled within the IIS rights.

To specify the logon account for the SharePoint application server

1. Open the NetBackup Administration Console.

2. Expand **NetBackup Management > Host Properties > Clients**.

3. In the right pane, right-click on the client and click **Properties**.

4. In the left pane, expand **Windows Client** and click **SharePoint**.

5. In the **Domain\User** box and the **Password** box, specify the user ID and password of the SharePoint Application Server.

6. Click **OK** to save your changes.

7. Repeat this configuration for all servers in the SharePoint farm.

8. Configure the local security privileges for the SharePoint Servers.

   See "Configuring local security privileges for the SharePoint Servers" on page 43.

Configuring local security privileges for the SharePoint Servers

On each SharePoint server in the farm you must assign certain local security privileges. These privileges are necessary since the NetBackup for SharePoint Agent logs on as the SharePoint user when it accesses data.

To configure the local security privileges

1. Open the Local Security Policy.

2. Click **Local Policies**.

3. In the User Rights Assignment, add the account to the following policies:

   - Allow log on locally

   - Debug programs

   - Log on as a service

   - Replace a process level token

4. Run the group policy update command (group policy update) for this change to take effect:

   ```
   gpupdate /Force
   ```

Performing consistency checks with NetBackup for SharePoint backups

You can perform consistency checks of the SQL Server database(s) before NetBackup begins a SharePoint backup operation. These checks are performed for both server-directed and user-directed backups.

To perform consistency checks with NetBackup for SharePoint backups

1   Open the NetBackup Administration Console.

2   Expand **NetBackup Management > Host Properties > Clients**.

3   In the right pane, right-click on the client and select **Properties**.

4   In the left pane, expand **Windows Client** and click **SharePoint**.

5   From the **Consistency check before backup** list, choose which check NetBackup should perform before backups.

See "Consistency check options for SharePoint Server" on page 44.

If you choose to perform a consistency check, you can select **Continue with backup if consistency check fails**. NetBackup then continues to perform the backup if the consistency check fails.

6   Click **OK** to save your changes.

7   Repeat this configuration for all servers in the SharePoint farm.

Consistency check options for SharePoint Server

The following consistency checks can be performed before a SharePoint Server backup.

Table 4-5   Consistency check options

Option	Description
None	Do not perform consistency checking.
Full check, excluding indexes	Select this option to exclude indexes from the consistency check. If indexes are not checked, the consistency check runs significantly faster but is not as thorough. Only the data pages and clustered index pages for each user table are included in the consistency check. The consistency of the non-clustered index pages is not checked.
Full check, including indexes	Include indexes in the consistency check. Any errors are logged.

See "Performing consistency checks with NetBackup for SharePoint backups" on page 44.

Configuring mappings for restores of a distributed applications, clusters, or virtual machines

NetBackup catalogs backup images under the SharePoint front-end server name. To allow NetBackup to restore content to each server in the farm, you must map the SharePoint Central Administration server with the SQL back-end servers. Configure these mappings in the Distributed Application Restore Mapping host property on the master server.

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 SharePoint Central Administration server. The component host is the client that needs access to the backup image. See Table 4-6.

Example entries for a single front-end SharePoint server with a clustered SQL back-end server

Table 4-6   Example entries for a single front-end SharePoint server with a clustered SQL back-end server

Application host	Component host
SharePoint Central Administration server	sql-virtualname
SharePoint Central Administration server	sql-db1
SharePoint Central Administration server	sql-db2

See "Configuring a SharePoint backup that uses Granular Recovery Technology (GRT)" on page 35.

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 SharePoint, 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 NetBackup Administrator's Guide, Volume I 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.

- For SharePoint Server, the nodes in a clustered back-end SQL Server are associated with the virtual name of the SQL Server.

Auto-discovered mappings for a cluster

If you have a clustered back-end SQL Server, 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.

In FCI is a SQL Server failover cluster instance.

Table 4-7 Example mapped host names for a single front-end SharePoint server with a clustered back-end SQL Server

Environment	Host	Mapped Host Names
FCI (cluster with two nodes)	Physical name of *Node 1*	SQL Server cluster virtual name
	Physical name of *Node 2*	SQL Server cluster virtual name

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.

To perform a manual backup

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

2 In the **All Policies** pane, select the policy you want to test.

3 Select **Actions > Manual Backup**.

4 Select the schedule that you want to use for the manual backup.

5 Select the clients that you want to include for the manual backup.

A parent job contains the whole file list and one or more child jobs. A child job is automatically launched for each host that contains SharePoint data. For example, assume that a SharePoint farm consists of four separate hosts. In this case, one parent job and four child jobs appear in the Activity Monitor. The front-end web server is listed as the client name for all jobs.

Configuring NetBackup for SharePoint backup policies

This chapter includes the following topics:

- About backup policies for granular backup and recovery of SharePoint Server
- About backup policies for SharePoint farm backup and recovery
- About backup policies for disaster recovery of SharePoint Server
- About VMware backup policies that protect SharePoint Server
- About configuring a backup policy for SharePoint

About backup policies for granular backup and recovery of SharePoint Server

A SharePoint granular backup provides you with the ability to restore individual items from the backup using Granular Recovery Technology (GRT). This type of backup does not provide protection for the full farm or disaster recovery. GRT only supports full 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.

> **Note:** The `Microsoft SharePoint Resources:\AllWebs` directive includes the SharePoint administration sites in a backup. However, granular recovery of the SharePoint Central Administration website and the Shared Services Administration website is not supported.

Create an **MS-SharePoint** policy for each individual web application or create a policy with the `Microsoft SharePoint Resources:\AllWebs` directive. Enable the **Enable granular recovery** option in the policy. (See Table 5-1, see Policy A or B.)

See "Configuring a SharePoint backup that uses Granular Recovery Technology (GRT)" on page 35.

Table 5-1   NetBackup for SharePoint policy examples for granular recovery

Policy and policy type	Backup selections	Auto backup frequency	Enable granular recovery	Other configuration
Policy A MS-SharePoint	Microsoft SharePoint Resources:\AllWebs	Weekly Full	Yes	The backup image must reside on a disk storage unit.
Policy B MS-SharePoint	Microsoft SharePoint Resources:*Web application name*	Weekly Full	Yes	The backup image must reside on a disk storage unit.

About backup policies for SharePoint farm backup and recovery

A farm-level backup provides a complete backup of the SharePoint installation. It does not, however, provide for disaster recovery, as some components must be backed up with an **MS-Windows** policy. Granular recovery is not available from this type of backup. If you enable granular recovery with this policy, NetBackup backs up *only* SQL Server objects in the farm.

SharePoint farm backups

You can back up a SharePoint farm in one of following ways:

- Create a **MS-SharePoint** policy to back up the entire farm, but exclude the Index Files and Search databases from incremental backups. Optionally, you can create another policy if you want to back up the Index Files and Search databases more frequently. See Table 5-2.

■ Create two **MS-SharePoint** policies. One policy backs up the entire farm and excludes the Index Files and Search from full and incremental backups. The other policy backs up the Index Files and Search databases. See Table 5-3.

Table 5-2   NetBackup for SharePoint policy example for full farm backups

Policy and policy type	Backup selections	Auto backup frequency	Enable granular recovery	Other configuration
Policy A MS- SharePoint	Microsoft SharePoint Resources:*	Weekly Full Daily Incremental	No	Exclude the Index Files and Search databases from the incremental backups. For the incremental schedule, add the following directive to the exclude list: Microsoft SharePoint Resources:\Shared Services\Shared Services Applications*Search Service Application name*
(Optional) Policy B MS-SharePoint	Microsoft SharePoint Resources:\Shared Services\Shared Services Applications*Search Service Application name*	More than once a week	No	This policy is optional. If a weekly full backup does not provide adequate protection, adjust the schedule accordingly. Ensure that Policy A and Policy B run at different times, ideally on different days.

Table 5-3   NetBackup for SharePoint full farm backup, with separate policy for Index Files and Search databases

Policy and policy type	Backup selections	Auto backup frequency	Enable granular recovery	Other configuration
Policy A MS-SharePoint	Microsoft SharePoint Resources:*	Weekly Full Daily Incremental	No	Exclude the Index Files and Search databases from the full and the incremental backups. Add the following directive to the exclude list: Microsoft SharePoint Resources:\Shared Services\Shared Services Applications*Search Service Application name*

NetBackup for SharePoint full farm backup, with separate policy for Index Files and Search databases *(continued)*

Policy and policy type	Backup selections	Auto backup frequency	Enable granular recovery	Other configuration
Policy B MS-SharePoint	Microsoft SharePoint Resources:\Shared Services\Shared Services Applications*Search Service Application name*	Weekly Full	No	If a weekly full backup does not provide adequate protection, adjust the schedule accordingly.

About backup policies for disaster recovery of SharePoint Server

To provide for full disaster recovery of SharePoint Server, you must create a farm-level backup and a Windows backup of certain file system components. The Windows backup should include the file system where SharePoint Web Parts can be installed and System State directive (Shadow Copy Components). A backup of the System State protects the IIS metadata.

SharePoint backups for disaster recovery

You can create backup policies for disaster recovery of a SharePoint in one of following ways:

- Create a **MS-SharePoint** policy and an **MS-Windows** policy. The first policy backs up the entire farm, but excludes the Index Files and Search databases from incremental backups. The second policy backs up the components that reside outside of SharePoint.
  See .
  Optionally, you can create another policy if you want to back up the Index Files and Search databases more frequently.

- Create two **MS-SharePoint** policies and an **MS-Windows** policy. One SharePoint policy backs up the entire farm and excludes the Index Files and Search from full and incremental backups. The other SharePoint policy backs up the Index Files and Search databases. The **MS-Windows** policy backs up the components that reside outside of SharePoint. See .

Table 5-4   NetBackup for SharePoint backup for disaster recovery

Policy and policy type	Backup selections	Auto backup frequency	Enable granular recovery	Other configuration
Policy A MS- SharePoint	Microsoft SharePoint Resources:*	Weekly Full Daily Incremental	No	Exclude the Index Files and Search databases from the incremental backups. For the incremental schedule, add the following directive to the exclude list: Microsoft SharePoint Resources:\Shared Services\Shared Services Applications*Search Service Application name*
Policy B MS-Windows	Shadow Copy Components:\ ALL_LOCAL_DRIVES	Weekly Full Daily Incremental	No	Exclude any databases from this policy. Add the paths for any databases to the exclude list.
(Optional) Policy C MS-SharePoint	Microsoft SharePoint Resources:\Shared Services\Shared Services Applications*Search Service Application name*	More than once a week	No	This policy is optional. If a weekly full backup does not provide adequate protection, adjust the schedule accordingly. Ensure that Policy A and Policy C run at different times. Ideally these policies should run on different days.

Table 5-5   NetBackup for SharePoint backup for disaster recovery, with a separate policy for Index Files and Search databases

Policy and policy type	Backup selections	Auto backup frequency	Enable granular recovery	Other configuration
Policy A MS- SharePoint	Microsoft SharePoint Resources:*	Weekly Full Daily Incremental	No	Exclude the Index Files and Search databases from the full and the incremental backups. Add the following directive to the exclude list: Microsoft SharePoint Resources:\Shared Services\Shared Services Applications*Search Service Application name*

| | Table 5-5 | | NetBackup for SharePoint backup for disaster recovery, with a separate policy for Index Files and Search databases *(continued)* |

Policy and policy type	Backup selections	Auto backup frequency	Enable granular recovery	Other configuration
Policy B MS-SharePoint	Microsoft SharePoint Resources:\Shared Services\Shared Services Applications*Search Service Application name*	Weekly Full	No	If a weekly full backup does not provide adequate protection, adjust the schedule accordingly.
Policy C MS-Windows	Shadow Copy Components:\ ALL_LOCAL_DRIVES	Weekly Full Daily Incremental	No	Exclude any databases from this policy. Add the paths for any databases to the exclude list.

About VMware backup policies that protect SharePoint Server

VMware backups that protect SharePoint Server provide granular recovery, complete protection of the farm, and protection of the SharePoint components in the Windows files system. These system components include SharePoint Web Parts and the System State directive (Shadow Copy Components). This version of NetBackup does not support a VMware incremental backup that protects SharePoint Server.

More information is available on how to configure a VMware backup that protects SharePoint.

See "About protecting an application database with VMware backups" on page 91.

See the NetBackup for VMware Administrator's Guide.

About configuring a backup policy for SharePoint

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

See "Adding a NetBackup for SharePoint policy" on page 56.

Adding a NetBackup for SharePoint policy

This topic describes how to add a new backup policy for a database.

To add a new NetBackup for SharePoint policy

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

2   Start the NetBackup Administration Console.

    If your site has more than one master server, choose the one on which you want to add the policy.

3   Select **NetBackup Management** > **Policies**. Then select **Actions > New > Policy**.

4   Type a unique name for the new policy and click **OK**.

5   From the **Policy type** list, select **MS-SharePoint**.

    The MS-SharePoint policy type does not appear in the drop-down list unless your master server has a license for the database agent.

6   (Optional) To enable restores of individual items from database backups, click **Enable granular recovery**.

    See "Configuring a SharePoint backup that uses Granular Recovery Technology (GRT)" on page 35.

7   Complete the entries on the **Attributes** tab.

    See "About policy attributes" on page 57.

8   Add other policy information as follows:

    - Add schedules.
      See "Adding schedules to a NetBackup for SharePoint policy" on page 58.

    - Add clients.
      See "Adding clients to a policy" on page 61.

    - Add database objects to the backup selections list.
      See "Creating a backup selections list for a SharePoint Server policy" on page 62.

9   For backups that use Granular Recovery Technology (GRT), configure the list of SharePoint hosts.

See "Configuring mappings for restores of a distributed applications, clusters, or virtual machines " on page 45.

10   When you have added all the schedules, clients, and backup selections you need, click **OK**.

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.

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

Table 5-6   Policy attribute for NetBackup for SharePoint policies

Attribute	Description
Policy type	Determines the types of clients that can be backed up with the policy. For SharePoint databases, select the policy type MS-SharePoint.
Limit jobs per policy	Limits the number of jobs that NetBackup performs concurrently with this policy. Set this option to **1** for the policies that are used to back up SharePoint databases.
Take checkpoints every	Checkpoint restart is not supported with NetBackup for SharePoint policies.
Enable granular recovery	Allows restores of individual items using Granular Recovery Technology (GRT). Documents external to the document library such as lists, calendars, and discussion boards cannot be restored individually. Users can only restore individual items from a full 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 SharePoint Granular Recovery Technology (GRT)" on page 36.
	SharePoint GRT-enabled backups do not support encryption or compression.
Keyword phrase	A textual description of a backup. Useful for browsing backups and restores.

Table 5-6	Policy attribute for NetBackup for SharePoint policies *(continued)*

Attribute	Description
Use Accelerator	Select this 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 SharePoint currently restricts backups to the full schedule type. This restriction also exists for a VMware backup that protects SharePoint without Accelerator. 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 the Data Protection Optimization Option license. For supported storage types, see NetBackup Enterprise Server and Server - Hardware and Cloud Storage Compatibility List. For more details on Accelerator with VMware backups, see the NetBackup for VMware Administrator's Guide.

Adding schedules to a NetBackup for SharePoint 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 SharePoint 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 SharePoint Server backup types" on page 59.

5 Choose a frequency level appropriate for the type of backup.

6 Specify the other properties for the schedule.

See "About schedule properties " on page 59.

7 Click **OK**.

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 5-7   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 SharePoint Server backup types" on page 59.
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.
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.

NetBackup for SharePoint Server backup types

Table 5-8 describes the type of backups that are available with the SharePoint Agent.

Table 5-8   Description of types of backups

Type of Backup	Description
Full Backup	Select this back up type to back up the entire SharePoint component database(s). Granular-level backups must be backed up with a full backup. A list is available for the objects that support full backups. See Table 5-9.
User Backup	A user backup is not automatically scheduled and is initiated from the front-end web server. This schedule allows for granular recovery. You may want a separate policy for User Backup schedule types. With a separate policy, you can easily separate user-directed and scheduled backups when you restore files. If you create a separate policy 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 before the backup begins.
Cumulative Incremental backup	This type of backup is not supported for SharePoint Server.
Differential Incremental backup	Select this backup type to only back up the changes that are made to the database since the last full backup or previous incremental backup. You cannot restore individual items from an incremental restore. A list is available for the objects that support incremental backups. See Table 5-9. **Note:** The SharePoint Index Files only support full backups. To minimize storage unit space consumption, it is recommended that you back up the Index Files and their corresponding Search databases with a different policy. **Note:** Incremental backups are not supported for granular-level backups.

Table 5-9 describes the schedule types that are supported for SharePoint Server and SharePoint Foundation objects.

Table 5-9   Schedule types supported for SharePoint Server and SharePoint
                     Foundation objects

SharePoint/SharePoint Foundation objects	Schedule type
Configuration DB	Full backup, Differential Incremental backup
Global Settings	Full backup, Differential Incremental backup
Single Sign-On	Full backup, Differential Incremental backup
Web Application/Content DB/ (including individual document restores)	Full backup
Shared Services/Services DB	Full backup, Differential Incremental backup
Shared Services/Shared Search Index/Index Files	Full backup
Shared Services/Shared Search Index/ Search DB	Full backup
Shared Services/Web App/Content DB	Full backup, Differential Incremental backup

Adding clients to a 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.

The NetBackup client software must be installed on each of the following: the front-end web server, the SQL Server database host, and the Index Files or the Index database host. The client software does not need to be installed on the Search or the Job servers. If the SQL Server is clustered,

To add clients to a policy

1   Open the policy you want to edit or create a new policy.

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

2   Click the **Clients** tab and click **New**.

3   Type the name of the client and select the hardware and operating system of the client.

Alternatively, you can also click the browse icon to browse for the clients available in the network

Only add the client that is the front-end web server and that runs the Central Administration Service to the policy list.

Note: You must perform additional configuration if the SQL back-end servers are clustered and you installed NetBackup on more than one node in the cluster.

See "Reviewing the auto-discovered mappings in Host Management" on page 46.

See "Configuring mappings for restores of a distributed applications, clusters, or virtual machines " on page 45.

---

4   Select the **Detect client operating system** check box to automatically detect the client computer's operating system and hardware.

5   Choose one of the following:

- To add another client, click **Add**.

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

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

Creating a backup selections list for a SharePoint Server policy

The backup selections list defines the SharePoint objects to be backed up and the grouping of SharePoint objects for multiple data streams. You can specify the entire farm or back up individual SharePoint components, such as a Single Sign-on, Configuration, or Content database. You can also use wildcards to specify a group of objects.

Veritas recommends that you create backup selections with the browse feature. Because SharePoint objects have long names, it is easy to mistype the object name when you create backup selections by adding and editing directives. One exception is the `Microsoft SharePoint Resources:\AllWebs` directive. Use this directive to back up all Web applications. You do not need to add a separate backup selection for each Web application.

To browse for the SharePoint objects, you must provide the credentials for the account that logs on to the SharePoint Server.

See

To perform backups with multiple data streams, you must enable this feature on the **Attributes** tab for the policy and define the backup streams with the `NEW STREAM` directive.

Creating a backup selections list to back up SharePoint Server objects

To create a backup selections list to back up SharePoint Server objects

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

2   Click **New**.

3   Click the **Browse** option to browse for a SharePoint object.

4   In the left pane, expand the client and select the object you want to back up.

     If you selected **Enable granular recovery** on the **Attributes** tab, the display is limited to Web applications.

5   Click **OK**.

6   Repeat step 2 through step 5 for each object you want to add.

Creating a backup selections item for all Web applications

To create a backup selections item for all Web applications

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

2   Click **New**.

3   From the **Pathname of directive** drop-down list, select **Microsoft SharePoint Resources:\AllWebs**.

     This directive works for both Web applications.

Performing SharePoint backups with multiple data streams

NetBackup lets you divide a backup so that each job backs up only a part of the backup selections list. To divide the backup into multiple jobs, insert the `NEW_STREAM` directive at a certain point or points in the backup selections list to define where each stream begins.

Backup jobs are divided as follows:

- When you specify `NEW_STREAM` directives in your policy, NetBackup creates a new job for each `NEW_STREAM` directive in the policy.

- If you use wildcard characters to define SharePoint objects in the backup selections list, those objects are backed up in the same stream.

- When you back up multiple SharePoint databases, NetBackup groups the backup jobs by the selected server.

For more information on the multiple data streams feature, see the NetBackup Administrator's Guide, Volume I.

Using wildcards in a SharePoint 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. For example, you may have a farm with a large number of Web applications or have Web applications with many content databases. You can use wildcard characters to indicate groups of Web applications and use the NEW_STREAM directive to divide the backup into multiple jobs, as follows:

Backup Selections
- Microsoft SharePoint Resources:\Microsoft SharePoint Foundation Web Application\SharePoint - 1*
- Microsoft SharePoint Resources:\Microsoft SharePoint Foundation Web Application\SharePoint - 3*
- Microsoft SharePoint Resources:\Microsoft SharePoint Foundation Web Application\SharePoint - 4*
- Microsoft SharePoint Resources:\Microsoft SharePoint Foundation Web Application\SharePoint - 5*

Table 5-10   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 eighth characters.

Table 5-10   Supported wildcard characters *(continued)*

Wildcard character	Action
Left & right brackets ([...])	Use to match any one character that is enclosed in square brackets. A minus (–) can be used to indicate a range of consecutive characters; for example, [0-9] is equivalent to [0123456789]. **Note:** The minus (-) loses this special meaning if it occurs last in the string. **Note:** The right square bracket (]) does not terminate such a string when it is the first character within it. For example, `[] a-f]` matches either a right square bracket (]) or one of the ASCII letters a through f inclusive. Asterisk (*) and Question Mark (?) stand for themselves within such a string of characters.

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

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

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

- Wildcard patterns are honored only in the final segment of the path name.
  Correct
  ```
  Microsoft SharePoint Resources:\WebApp*
  Microsoft SharePoint Resources:\WebApp[A-D]
  Microsoft SharePoint Resources:\WebAppDept?
  ```
  Incorrect
  ```
  Microsoft SharePoint Resources:\Shared Services\*\Content DB
  ```

Configuring exclude lists for SharePoint clients

If you need to exclude certain SharePoint objects, you can create an exclude list. When NetBackup runs a NetBackup for SharePoint 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 the NetBackup Administrator's Guide, Volume I.

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

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

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

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

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

You can exclude any SharePoint object from a backup. You can specify the exclude list entry under **All Policies** or under a specific policy or schedule.

SharePoint object names can be lengthy. You can type an object name in the exclude list manually. Or it may be easier to locate the object through a remote browse (from the NetBackup policy window). Then copy the object name from there to the exclude list.

The following figure shows an exclude list with one SharePoint Web application:

Figure 5-1   Exclude list for two SharePoint databases
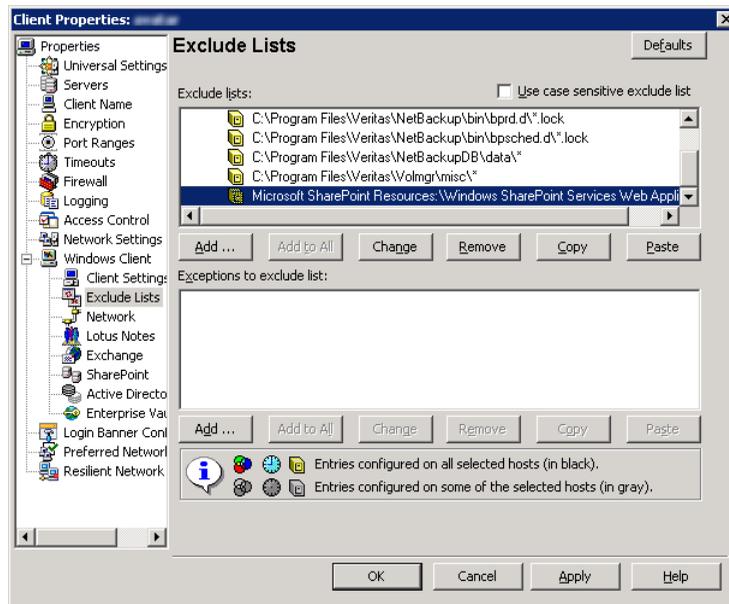
Note: For SQL Servers in a cluster, you must select each node and perform the configuration procedure on each node. You must configure the same settings on each node. If you change the attributes for the virtual name of the client, NetBackup updates only the active node or current node.

To configure a SharePoint 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 SharePoint 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 SharePoint object in the following format:
  For Web applications:
  ```
  Microsoft SharePoint Resources:\Windows SharePoint Foundation
  Web Application\app name
  ```

  - To exclude a specific database, type the name of a specific database after the Web application name.

  - To exclude Index Files and their Search databases, use one of the following directives.
    Microsoft SharePoint Resources:\Shared Services\Shared Service Applications*Search Service Application name*

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

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

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

Performing backups and restores of SharePoint Server and SharePoint Foundation

This chapter includes the following topics:

- About user-directed backups of SharePoint Server and SharePoint Foundation
- About restores of SharePoint Server and SharePoint Foundation

About user-directed backups of SharePoint Server and SharePoint Foundation

User-directed backups of SharePoint Server must be performed from the front-end Web server. Back up the Content, Services, and User profile databases together.

If the policy that has a user backup schedule enables consistency checks, these checks are also performed before user-directed backups.

Note: If you open multiple backup windows (in the NetBackup client) to browse SharePoint resources, the windows may unexpectedly terminate. Instead, use a single backup window to browse SharePoint resources for backup.

Specifying the server and client for a SharePoint Server backup operation

When you perform user backups of a SharePoint Server, you can specify the server that you want to perform the backups.

To specify the server and client for a backup operation

1   Log onto the server as Administrator.

2   Open the Backup, Archive, and Restore interface.

3   Select **File > Specify NetBackup Machines and Policy Type**.

4   In the **Specify NetBackup Machines and Policy Type** dialog box, provide the following information:

Server to use for backups and restores	Select the server you want to perform the backup.
Source client for restores (or virtual client for backups)	Not applicable for SharePoint backups.

5   Click **OK**.

About backup options for NetBackup for SharePoint

Table 6-1 lists the options that are available when you perform backups of a SharePoint Server.

Table 6-1   Backup options

Option	Description
Backup to NetBackup server	Identify the NetBackup server that you want to perform the backup.
Items marked to be backed up	Contains a list of objects to be backed up.
Keyword phrase to associate with the backup or archive	Specify a keyword phrase, up to 128 characters in length, that NetBackup can associate 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.

Performing a user-directed backup of SharePoint Server and SharePoint Foundation

This topic describes how to perform a user-directed backup of SharePoint Server and SharePoint Foundation.

To back up SharePoint resources

1   Log onto the server as Administrator.

2   Open the Backup, Archive, and Restore interface.

3   Choose **File > Select Files and Folders to Back Up**.

4   In the **Backup** window, in the **All Folders** pane, expand **Microsoft SharePoint Resources**.

5   Select the object(s) to back up.

6   Choose **Actions > Backup**.

    See "About backup options for NetBackup for SharePoint" on page 69.

7   In the **Backup Files** dialog box, click **Start Backup**.

    If you want to view the progress of the backup, click **Yes**. If you do not want to view the progress of the backup, click **No**.

See "About user-directed backups of SharePoint Server and SharePoint Foundation" on page 68.

See "Restoring individual SharePoint items from full database backups" on page 80.

About restores of SharePoint Server and SharePoint Foundation

Note the following when you perform restores:

- The NetBackup for SharePoint 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.

- Administer restores from the NetBackup master server or the SharePoint front-end server.

- When you select an item for restore, do not select (or mark) items in the **All Folders** pane. In the **All Folders** pane, click on, but do not select the check box for the parent folder. Then, in the **Contents of** pane, select the specific object you want to restore.

- The Configuration database contains all of the configuration information for the entire SharePoint server farm. Use caution when you restore this database; upon restore, any changes are lost that you made to the farm topology after the backup was performed.

- When you select for restore some but not all Content databases for a Web application, the Web application is not provisioned. After you restore the selected Content databases, those databases are re-attached.

- Even if SharePoint components exist on multiple computers, all the backups are cataloged under the same SharePoint server name. Once you select that server name, all available backup images for your SharePoint environment are displayed.

- When you redirect a restore to a file system, any list items you selected are not restored and appear as 0-KB files.

- Restores that use GRT must be made from a disk storage unit. You cannot restore from the tape copy.

- When you restore a site collection, any non-default theme you applied is not restored with the site collection. You must reapply the theme manually after the restore. This limitation does not affect restores of sub sites.

See "Limitations and conditions for restores that use SharePoint Granular Recovery Technology (GRT)" on page 37.

Specifying the server, client, and the policy type for a SharePoint Server restore operation

When you perform restores, you select the following information:

- The master server that performed the backup
- The SharePoint front-end client that was backed up
- The SharePoint policy type

To specify the server, client, and policy type for a SharePoint Server restore operation

1   Log onto the server as Administrator.

2   Open the Backup, Archive, and Restore interface.

3   Click **File > Specify NetBackup Machines and Policy Type**.

4   In the **Specify NetBackup Machines and Policy Type** dialog box, from the **Server to use for backups and restores** list, select the NetBackup server that performed the restore.

5   From the **Source client for restores** list, select the client.

    The source client is the SharePoint Server front-end client whose backup images you want to browse.

6   From the **Policy type for restores** list, choose **MS-SharePoint**.

7   Click **OK**.

Restore options for SharePoint Server on the Microsoft SharePoint tab

On this tab you can choose to bring databases online after a restore job. You can also specify a different location to which to redirect a web application. The farm and the web application to which you want to redirect the restore must already exist.

Table 6-2   Microsoft SharePoint tab

Option	Description
Bring restored databases online and reconnect previous database links	Select this option to bring the databases online after a restore job. This option also re-establishes the link between the restored databases and their corresponding web applications.
Preserve existing Internet Information Services (IIS) Web site and application pool	If the website and the application pool for the SharePoint web application that you restore already exists in IIS, this option preserves them during restore. If you do not check this option, the website and the application pool are deleted from IIS during the restore. After they are deleted, they are recreated in the default location that SharePoint specifies.

Table 6-2   Microsoft SharePoint tab *(continued)*

Option	Description

If versioning is enabled on the restore destination	If versioning is enabled on the destination to which you want to restore an individual item or document, select one of the following options:
	
	■ **Add as a new version**
	NetBackup restores the existing item or document as a new version, which makes it the most recent version of the existing item. For example, assume that you have five versions of `testfile.doc` and choose to restore version 2.0 of the file. When the file is restored, it is added as `testfile.doc` 6.0 and is the most recent version.
	■ **Skip if the item exists**
	NetBackup does not restore the item if an identical item or document exists in the restore destination. NetBackup notes that the file was skipped in the job log.
	■ **Restore over existing items**
	NetBackup restores the existing item as a new version and deletes the existing version. For example, assume that the version history is as follows:
	
	`testfile.doc version 3.0`
	`testfile.doc version 2.0`
	`testfile.doc version 1.0`
	
	`testfile.doc` version 3 is the most recent version. If you choose to restore `testfile.doc` version 2.0, the restore adds `testfile.doc` version 4.0 and deletes `testfile.doc` version 2.0. So the version history appears as follows:
	
	`testfile.doc version 4.0`
	`testfile.doc version 3.0`
	`testfile.doc version 1.0`
	
	`testfile.doc` version 2.0 is now version 4.0 of the file.
	
	Note: The version of the restored file depends on the **Versioning Settings** selected for that library or list in SharePoint.

If versioning is not enabled on the restore destination	If versioning is not enabled on the destination to which you want to restore an individual item, select one of the following options: ■ **Skip if the item exists** NetBackup does not restore the item if an identical item exists in the restore destination. NetBackup indicates that the file was skipped in the log. ■ **Restore over existing items** NetBackup replaces the existing item with the restored item.
Restore only the most recent version of an item	Check this option to only restore the most recent version of an item. Note that NetBackup restores the most recent version of the versions you selected for restore. If a more recent version exists, but you did not select it for restore that version is not restored.

Table 6-2   Microsoft SharePoint tab *(continued)*

Option	Description

Include security information	Check this option to restore any applicable security information with the item. Note that security information is restored only if you select a parent folder and not when you select individual items. For example, security information is restored when you select Shared Documents, but not if you select an individual document. However, an individual object can have user permissions that are defined with a level of "limited access." In this case, permissions for those users are not restored with that object.
	
	You can restore different levels of security based on the SharePoint item you restore:
	
	■ Sites
	   User and SharePoint Group information and security ACL are restored for top-level sites.
	■ Subsites
	   Security ACL is restored.
	■ Lists
	   Security ACL and other security-related information are restored.

Redirect SharePoint Resources	Check this option to redirect a Web application. Then click one of the following: ■ **Web application** ■ **Alternate SQL instance** ■ **Individual SharePoint sites, documents, lists, or items** Note that you can only redirect documents or pictures to a path.
Web application	Select this option to redirect a Web application to another Web application. ■ In the **URL** box, specify the URL of the destination site. For example: http://*URL to Web application* ■ In the **Front end web server name** box, indicate the host name of the web server to which you want to redirect. The web server must already exist on the destination location. See "Redirecting a restore of a SharePoint web application within a farm" on page 85. See "Redirecting a restore of a SharePoint Web application to another farm" on page 87.
Alternate SQL instance	**Note:** Select only one database to redirect. If you select multiple databases, all databases are written to the target database. Select this option to redirect a web application to an alternate SQL instance. In the **SQL Server\Instance** box, indicate the name of the target SQL Server and the target instance name. In the **Target Database** box, indicate the name of the target database. See "Redirecting the restore of a SharePoint Server Web application content database to an alternate SQL Server instance" on page 89.

Table 6-2   Microsoft SharePoint tab *(continued)*

Option	Description
Individual SharePoint sites, documents, lists, or items	**Note:** This feature applies only to SharePoint 2010.

How the NetBackup Recovery Assistant restores SharePoint Server and SharePoint Foundation

The NetBackup Recovery Assistant launches a restore job for each database in a Web application. Databases are restored in the proper order to ensure that a working Web application exists when the restore is complete. After all the databases are restored any items you selected are restored in a single job.

The Recovery Assistant restores objects in the following order:

- Configuration databases (only if assistant is run in disaster recovery mode)

- Content databases

- Services databases

- Index Files

- Document sets, documents, lists, etc.

Objects are skipped if they are not found in the database configuration. Each restore may only restore a portion of the components depending on what objects you select and the backup image you select. When you restore an item, it does not restore an entire Content database or Document library.

Restoring SharePoint Server and SharePoint Foundation

Multiple SharePoint Server resources can be restored together. The NetBackup Recovery Assistant determines the order in which the resources must be restored. You can restore any of the SharePoint resources in separate restore operations.

Note: NetBackup does not prevent you from restoring placeholders. NetBackup also lets you restore any object that can hold a document, even if it does not contain a document.

Restoring SharePoint Server

1   Enable the front-end Web server to redirect restores to the SQL Server hosts in the farm.

A redirected restore is performed since backups are cataloged under the front-end client name for the Federated SharePoint farm.

See "Configuring mappings for restores of a distributed applications, clusters, or virtual machines " on page 45.

2   Log on as Administrator.

3   Open the Backup, Archive, and Restore interface.

4   Choose **File > Select Files and Folders to Restore > from Normal Backup**.

5   Select the **MS-SharePoint** policy type.

See "Specifying the server, client, and the policy type for a SharePoint Server restore operation" on page 71.

6   Click **OK**.

NetBackup browses for SharePoint Server backup images.

7   From the **NetBackup History** pane, select the image(s) that contain the objects you want to restore:

- The last full backup, or

- The last full backup and all subsequent differential backups

8   In the **All Folders** pane, expand **Microsoft SharePoint Resources**.

Note: When you select items to restore, do not check the checkbox for an item in the **All folders** pane. Only check the checkbox for an item in the **Contents of** pane.

---

9   In the **Contents of** pane, check the checkbox for the SharePoint resources to restore.

To select a database, click on (but do not check the checkbox for) the parent folder in the **All Folders** pane. Then check the checkbox for the database in the **Contents of** pane.

If you want to restore a subsite, expand the site collection in the **All Folders** pane. Then check the checkbox for the subsite in **Contents of** pane.
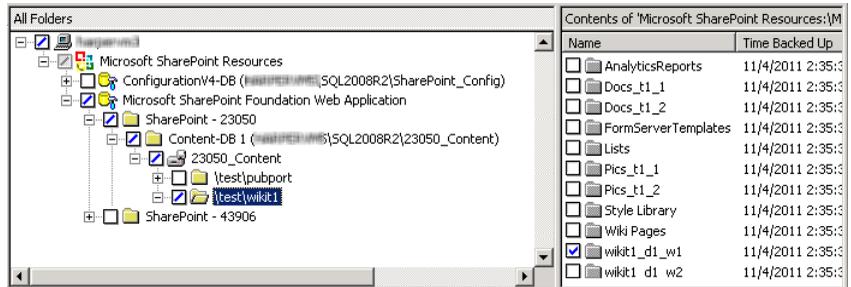
Note: For a successful restore, you must select the Index Files folder(s) exactly
as described here.

If you want to restore the SharePoint Index Files, do the following:

- In the **All Folders** pane, click on the folder for the Shared Services
  Application but do not select the checkbox for it.

- In the **Contents of** pane, select each Index Files folder.
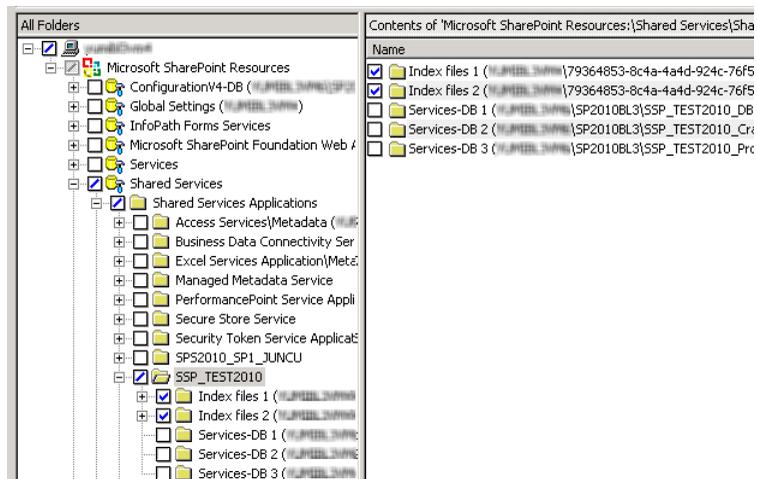
10   Choose **Actions** > **Restore**.

11   In the **Restore Marked Files** dialog box, click the **Microsoft SharePoint** tab.

See "Restore options for SharePoint Server on the Microsoft SharePoint tab"
on page 72.

12   Click **Start Restore**.

Restoring the SharePoint Search Service Application

The following instructions describe how to restore the Shared Services Application. Select all of the components of the Search Service application for recovery. The SharePoint Agent un-provisions the Search service application, restores the components, and recovers the Search service application.

To restore the SharePoint Search Service Application

1   Open the NetBackup Backup, Archive, and Restore interface.

2   Open a **Restore** window.

3   Select the full backup that contains the shared services.

4   In the **All Folders** pane, expand **Microsoft SharePoint Resources** > **Shared Services** > **Shared Services Applications**.

5   Select each Index Files folder for restore as follows:

Note: For a successful restore, you must select the Index Files folders exactly as described here.

- In the **All Folders** pane, click on the folder for the Shared Services Application but do not select the checkbox for it.

- In the **Contents of** pane, select each Index Files folder.
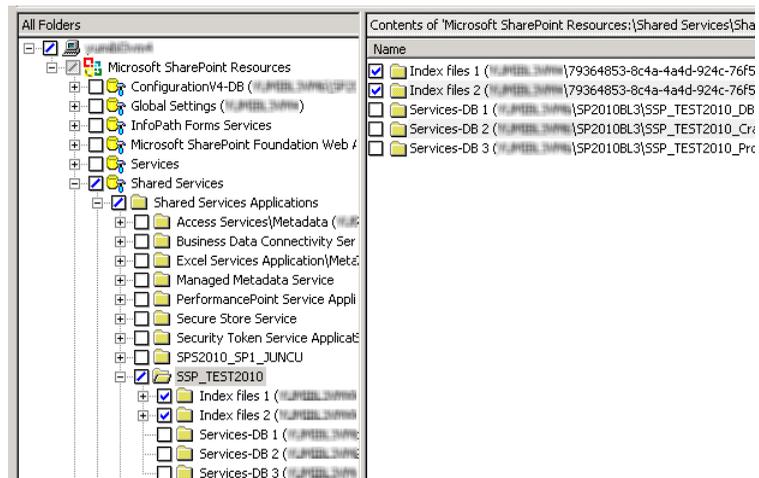
6   Select each Shared Services database for restore as follows:

Note: For a successful restore, you must select the databases exactly as described here.

- In the **All Folders** pane, click on the folder for the Shared Services database but do not select the checkbox for it.

- In the **Contents of** pane, select the Shared Services database.
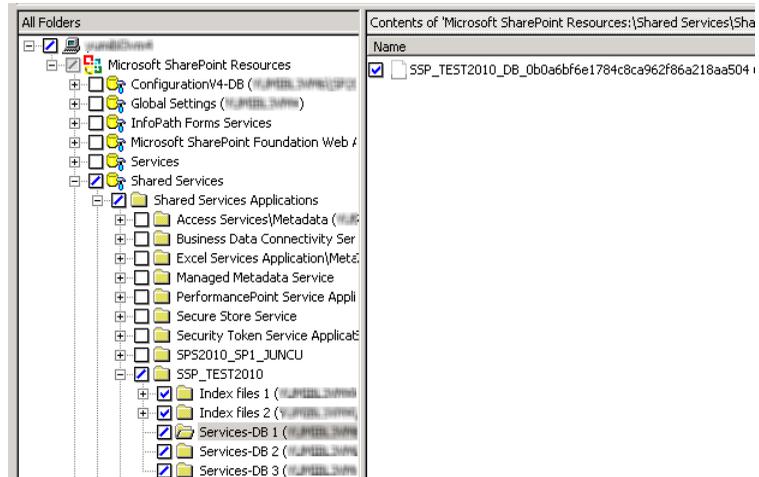
7   Choose **Actions > Restore**.

8   In the **Restore Marked Files** dialog box, click the **Microsoft SharePoint** tab.

9   Uncheck **Bring restored databases online and reconnect previous database links**.

10 Click **Start Restore**.

11 Restore any incremental backups. Do not select **Bring restored databases online and reconnect previous database links** except for the *last* incremental backup.

About requirements for restores of individual SharePoint items using Granular Recovery Technology (GRT)

The following requirements must be met to restore individual items from full database backups Granular Recovery Technology (GRT):

- The administrator has configured NetBackup to allow for restores of individual items (**Enable granular recovery**). This option is on the **Attributes** tab for the backup policy.

See "About policy attributes" on page 57.

- The user must restore from a full backup image.

- You can only restore an individual item when the backup image resides on a disk storage unit.
  See "Disk storage units supported with SharePoint Granular Recovery Technology (GRT)" on page 36.

Restoring individual SharePoint items from full database backups

You can restore individual sites, subsites, documents, images, and list items from the full SharePoint database backup jobs that use Granular Recovery Technology (GRT).

Note: Granular recovery of the SharePoint Central Administration web site and the Shared Services Administration web site is not supported.

Note: When you restore an item, it is safe to ignore certain `bprd` errors in the Activity Monitor similar to the following:

```
7/12/2007 11:01:39 AM - Error bpdm (pid=2928) did not receive EXIT
STATUS from bprd, all blocks may not have been restored
```

Instead, rely on the final status that is reported in the Activity Monitor to determine the true success or failure of the restore operation.

To restore individual SharePoint items from full database backups

1 Enable the SharePoint front-end Web server to restore to the SQL Server hosts in the farm.

See "Configuring mappings for restores of a distributed applications, clusters, or virtual machines " on page 45.

2 Log on as Administrator.

3 Open the Backup, Archive, and Restore interface.

4 Choose **File > Select Files and Folders to Restore > from Normal Backup**.

5 Select the **MS-SharePoint** policy type.

See "Specifying the server, client, and the policy type for a SharePoint Server restore operation" on page 71.

6 Click **OK**.

NetBackup browses for SharePoint Server backup images.

7 From the **NetBackup History** pane, select the full backup image that contains the items you want to restore.

8 In the **All Folders** pane, expand **Microsoft SharePoint Resources**.

Note: When you select items to restore, do not check the checkbox for an item in the **All folders** pane. Only check the checkbox for an item in the **Contents of** pane.

---

9 In the **Contents of** pane, select the items to restore.

Note that security information is restored only if you select a parent folder and not when you select individual items. For example, security information is restored when you select Shared Documents, but not if you select an individual document. However, an individual object can have the user permissions that are defined with a level of "limited access." In this case, permissions for those users are not restored with that object.

10 Choose **Actions > Restore**.

11 In the **Restore Marked Files** dialog box, click the **Microsoft SharePoint** tab.
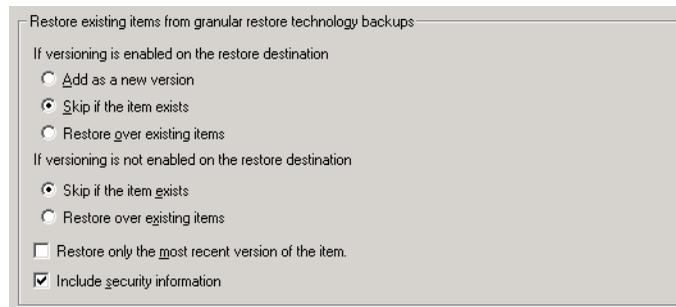
12 Choose your restore options, as follows:

If versioning is enabled on the restore destination	Select one of the following options: ■ **Add as a new version** NetBackup restores the existing item as a new version, making it the most recent version of the existing item. ■ **Skip if the item exists** NetBackup does not restore the item if an identical item exists in the restore destination. NetBackup notes that the file was skipped in the job log. ■ **Restore over existing items** NetBackup restores the existing item as a new version and deletes the existing version.
If versioning is not enabled on the restore destination	Select one of the following options: ■ **Skip if the item exists** NetBackup does not restore the item if an identical item exists in the restore destination. NetBackup notes that the file was skipped in the job log. ■ **Restore over existing items** NetBackup replaces the existing item with the restored item.
Restore only the most recent version of an item	Check this option if you only want to restore the most recent versions of any individual items you have selected for restore.
Include security information	Check this option if you want to restore the SharePoint security information that is attached to the items you restore.

13 Select the other restore options you want.

14 Click **Start Restore**.

Recovering a SharePoint Web application in a farm with multiple front-end servers

To restore a deleted web application in a Network Load Balanced (NLB) farm, you may need to perform a manual operation using the SharePoint Central Administration interface. After the restore operation is successful, if the Web application on the NLB farm is offline, perform the following steps.

Note: After you complete the following steps, a change is reflected in the IIS attributes for the primary configured balanced node. The new balanced load server contains two sites: the original site and the name of the latest site that you create in step 13. However, both sites link to the original site and there is no effect on the environment.

To recover a SharePoint Web application in a farm with multiple front-end servers

1 Log on as Administrator.

2 Open the Backup, Archive, and Restore interface.

3 Choose **File > Select Files and Folders to Restore > from Normal Backup**.

4 Select the **MS-SharePoint** policy type.

See "Specifying the server, client, and the policy type for a SharePoint Server restore operation" on page 71.

5 Click **OK**.

NetBackup browses for SharePoint Server backup images.

6 From the **NetBackup History** pane, select the images that contain the objects you want to restore:

- The last full backup, or

- The last full backup and all subsequent differential backups

7 In the **All Folders** pane, expand **Microsoft SharePoint Resources** and the Web application.

Note: When you select items to restore, do not check the checkbox for an item in the **All folders** pane. Only check the checkbox for an item in the **Contents of** pane.

---

8 In the **Contents of** pane, select the Content database.

9 Restore the database to the primary front end.

Note that you only need to perform this action once.

10 Open the SharePoint Central Administration interface.

11 Under **Central Administration**, click **Application Management**.

12 Under **SharePoint Web Application Management**, click **Create or extend Web application**.

13 Select **Extend an existing Web application**.

14 Do the following to extend the Web application:

- Click on the link for the Web application and select **Change Web Application**. Fill in the values to extend the restored Web application.

- Select **Create a new IIS web site** and fill in the information to match the original Web application. However, you cannot use the same port number.

- In the **Load Balanced URL** section, provide the node name of the load balanced server. (For example, http://VMSP-3:new port.)

15 After you complete step 14, all other configured front-ends may be automatically updated with IIS entries. If so, no further action is required.

If other front-ends require load balancing, then repeat step 12 through step 14.

Restoring a deleted SharePoint list

To restore a list that you deleted, you need to restore the list and `default.aspx` in separate restore jobs.

To restore a deleted list

1 Log on as Administrator.

2 Open the Backup, Archive, and Restore interface.

3 Choose **File > Select Files and Folders to Restore > from Normal Backup**.

4 Select the **MS-SharePoint** policy type.

See "Specifying the server, client, and the policy type for a SharePoint Server restore operation" on page 71.

5 Click **OK**.

NetBackup browses for SharePoint Server backup images.

6 From the **NetBackup History** pane, select the images that contain the objects you want to restore:

- The last full backup, or

- The last full backup and all subsequent differential backups

7 In the **All Folders** pane, expand **Microsoft SharePoint Resources**.

Note: When you select items to restore, do not check the checkbox for an item in the **All folders** pane. Only check the checkbox for an item in the **Contents of** pane.

---

8 From the **Contents of** pane, select the list item you deleted or the library container for the list.

9 Click **Start Restore**.

When the restore completes, continue with the next step.

10 In the **All Folders** pane, expand **Microsoft SharePoint Resources**.

11 From the **Contents of** pane, in the subsite or the site collection, select `default.aspx`.

12 Click **Start Restore**.

Redirecting a restore of a SharePoint web application within a farm

A web application restore can be redirected within the same farm or to a different farm. For instructions on how to redirect to a different farm, see the following topic:

See "Redirecting a restore of a SharePoint Web application to another farm" on page 87.

Note the following when you redirect a web application within a farm:

- The source web application cannot be a live web application.

- The web application target to which you want to redirect the restore must already exist on the specified web server.

- The target must have the same database structure as the source web application.

- You can only redirect a web application from a full backup. Redirection is not supported from differential backups.

- You can restore configuration databases and single sign-on databases back to the original location only. Document sets and individual SharePoint items must be restored to their original site.

- You can redirect a restore of a web application within the same farm. The SQL Server database host and the SharePoint host must be the same. A redirected restore is not supported if the SQL Server databases exist across multiple SQL hosts.

- You must restore all SQL Server databases in one operation at the same time.

To redirect a restore of a SharePoint web application within a farm

1 Log on as Administrator.

2 Create the target web application on the target web server. The target site must have the same database structure as the source site.

3 Remove the source web application.

If you attempt the redirected restore without removing the source, the restore completes successfully, but the databases are not properly connected to the virtual server.

4 Open the Backup, Archive, and Restore interface.

5 Click **File > Select Files and Folders to Restore > from Normal Backup**.

6 Select the **MS-SharePoint** policy type.

See "Specifying the server, client, and the policy type for a SharePoint Server restore operation" on page 71.

7 From the **NetBackup History** pane, select the full backup image that contains the objects you want to restore.

8 In the **All Folders** pane, expand **Microsoft SharePoint Resources**.

Note: When you select items to restore, do not check the check box for an item in the **All folders** pane. Only check the check box for an item in the **Contents of** pane.

---

9 In the **Contents of** pane, select the web application to redirect.

10 Click **Actions > Restore**.

11 In the **Restore Marked Files** dialog box, click the **Microsoft SharePoint** tab.

12 Check **Redirect SharePoint Resources**.

13 Click **Web application**.

14 In the **URL** box, type the URL of the destination site:

http://*webapp*

15 In the **Front end web server name** box, indicate the host name of the web server.

16 For information on other restore options in this dialog box, see the following topic:

See "Restore options for SharePoint Server on the Microsoft SharePoint tab" on page 72.

17 Click **Start Restore**.

Redirecting a restore of a SharePoint Web application to another farm

A Web application restore can be redirected within the same farm or to a different farm. For instructions on how to redirect within a farm, see the following topic:

See "Redirecting a restore of a SharePoint web application within a farm" on page 85.

Note the following when you redirect a Web application to another farm:

- The Web application target to which you want to redirect the restore must already exist on the specified Web server. It also must have the same number of content databases as the source Web application.

- The target Web application and SQL Server database name must have new names (different from original names).

- The SharePoint version from the source farm must match the SharePoint version of the destination farm.

- You can only redirect a Web application from a full backup. Redirection is not supported from differential backups.

- The Web applications must be restored at the database level.

- The destination SharePoint farm nodes must be in the NetBackup domain.

- In the host properties for the master server, configure the **Distributed Application Restore Mapping** settings.
  These settings must contain the mapping for the destination farm. A distributed application must have all the farm nodes of the destination SharePoint farm mapped as components of the source SharePoint front end.

- The Windows **Client Properties** for the destination farm nodes must be set for SharePoint for all nodes in the farm.

- A NetBackup client must be installed on all nodes of the destination farm.

- You cannot complete a redirected restore if the SQL Server databases exist across multiple SQL hosts.

- You must restore all redirected Web application SQL Server databases in one operation at the same time.

- You cannot redirect a Web application to the same farm more than once. This restriction ensures SQL Server database ID uniqueness.

- The SharePoint version of the source and destination must be the same.

- The SQL version of the source and destination must be the same.

- You must manually restore from the MS-Windows backup image any custom Web parts that were created on the file system. These components are not backed up with the MS-SharePoint policy. (For example, you must manually restore `C:\inetpub\wwwroot\wss\VirtualDirectories\`*`port number`*.)

To redirect a restore of a SharePoint Web application to another farm

1   Log on as Administrator.

2   Create the target Web application on the target Web server.

3   Open the Backup, Archive, and Restore interface.

4   Click **File > Select Files and Folders to Restore > from Normal Backup**.

5   Select the **MS-SharePoint** policy type.

    See "Specifying the server, client, and the policy type for a SharePoint Server restore operation" on page 71.

6   From the **NetBackup History** pane, select the full backup image that contains the objects you want to restore.

7   In the **All Folders** pane, expand **Microsoft SharePoint Resources**.

    ***

    Note: When you select items to restore, do not check the checkbox for an item in the **All folders** pane. Only check the checkbox for an item in the **Contents of** pane.

    ***

8   In the **Contents of** pane, select the Web application to redirect.

9   Click **Actions > Restore**.

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

11 Check **Redirect SharePoint Resources**.

12 Click **Web application**.

13 In the **URL** box, type the URL of the destination site:

    http://*webapp*:*port*

    Use the URL that appears in SharePoint Central Administration.

14 In the **Front end web server name** box, indicate the host name of the *target* Web server.
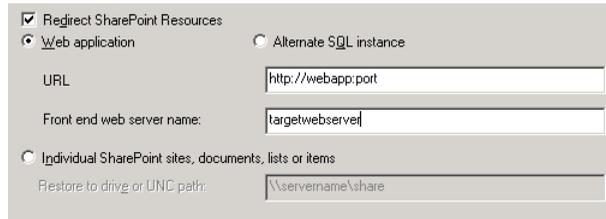
See "Restore options for SharePoint Server on the Microsoft SharePoint tab" on page 72.

15 Click **Start Restore**.

Redirecting the restore of a SharePoint Server Web application content database to an alternate SQL Server instance

You can redirect a SharePoint Web application content database to an alternate SQL Server instance to take advantage of SharePoint data recovery from an unattached content database. The target database must be a new database.

For information on how to redirect individual items to a file path, see the following topic:

To redirect the restore of a SharePoint Server database to an alternate SQL Server instance

1 Open the Backup, Archive, and Restore interface.

2 Click **File > Select Files and Folders to Restore > from Normal Backup**.

3 Select the **MS-SharePoint** policy type.

See "Specifying the server, client, and the policy type for a SharePoint Server restore operation" on page 71.

4 From the **NetBackup History** pane, select the full backup image that contains the objects you want to restore.

5 In the **All Folders** pane, expand **Microsoft SharePoint Resources**.

Note: When you select items to restore, do not check the checkbox for an item in the **All folders** pane. Only check the checkbox for an item in the **Contents of** pane.

6   In the **Contents of** pane, select the Web application content database to redirect.

7   Click **Actions > Restore**.

8   In the **Restore Marked Files** dialog box, click the **Microsoft SharePoint** tab.

9   Click **Redirect SharePoint Resources**.

10   Select **Alternate SQL Instance**.

11   In the **SQL Server\Instance** box, type the name of the SQL Server and the instance name to which you want to redirect the Web application content database.

12   In the **Target Database** box, indicate the name of the target database.
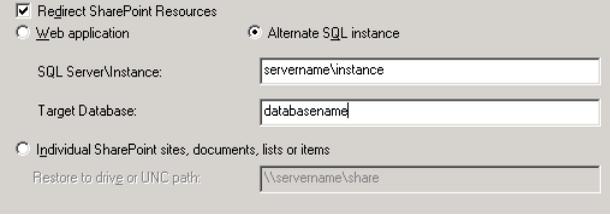
For information on other restore options in this dialog box, see the following topic:

See "Restore options for SharePoint Server on the Microsoft SharePoint tab" on page 72.

13   Click **Start Restore**.

Protecting SharePoint Server data with VMware backups

This chapter includes the following topics:

- About protecting an application database with VMware backups
- About configuring a VMware backup that protects SharePoint Server
- Restoring SharePoint data from a VMware backup

About protecting an application database with VMware backups

With a VMware backup policy and the Veritas VSS provider, NetBackup can create consistent, full backups of an application database that resides on a virtual machine.

VMware application backups let you:

- Use the existing database restore process to restore and recover data from VMware backups.
- From one VMware backup, choose from these restore options: Disk-level restore, file-level recovery, database restore, or granular-level restore (GRT).
- Restore and recover databases from VMware backups to alternate clients. The target destination client can be a physical computer or a virtual machine.

Supported environments and configuration

See the following information on virtual systems compatibility:

https://www.veritas.com/content/support/en_US/doc/NB_70_80_VE

Veritas VSS provider

Veritas recommends the Veritas VSS provider. VMware Tools calls the provider to quiesce the VSS writers for a file-level consistent backup.

See "Installing the Veritas VSS provider for vSphere" on page 93.

Limitations of VMware application backups

Databases are cataloged and protected only if they exist in a configuration that is supported for VMware backups. Make sure to store databases on supported storage.

VMware application backups do not support the following policy options and configurations:

- Incremental backups. Instead, you can create an MS-SharePoint policy for SharePoint Server incremental backups

- Consistency checks of the SharePoint Server.

- SQL Server clusters or SQL Server availability groups.

- SQL Server back-end servers that service multiple SQL Server instances for multiple SharePoint farms.

- SharePoint Server databases are not cataloged and backed up if they exist on the following:

  - Virtual machines that use raw device mapping (RDM).

  - Virtual Machine Disk (vmdk) volumes that are marked as independent.

  - Mount point volumes.

  - Virtual hard disks (VHDs).

  - RAID volumes.

  - ReFS file systems.

  - An excluded Windows boot disk.

- Any components that reside on a physical computer are not backed up with the VMware backup.

- SharePoint configurations that have any SQL Server back-end servers that service multiple SQL Server instances for multiple SharePoint farms are not supported with SharePoint application-enabled VMware policies.

Installing the Veritas VSS provider for vSphere

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**.

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

About configuring a VMware backup that protects SharePoint Server

To successfully perform VMware backups and restores of SharePoint Server, complete the following steps.

Table 7-1   Configuring a VMware backup that protects SharePoint Server

Step	Action	Description
Step 1	Configure your VMware environment and NetBackup.	See the NetBackup for VMware Administrator's Guide. Install the NetBackup client software on the virtual machines that are part of a SharePoint farm.
Step 2	Install the Veritas VSS provider.	See "Installing the Veritas VSS provider for vSphere" on page 93.

Table 7-1   Configuring a VMware backup that protects SharePoint Server
(continued)

Step	Action	Description
Step 3	Configure the NetBackup Client Service.	See "Configuring the logon account for the NetBackup Client Service for NetBackup for SharePoint " on page 38.
Step 4	Configure the NetBackup Legacy Network Service and optionally the NetBackup Legacy Client Service.	See "Configuring the logon account for the NetBackup Legacy Network Service and the NetBackup Legacy Client Service" on page 39.
Step 5	Configure the local security privileges.	See "Configuring local security privileges for the SharePoint Servers" on page 43.
Step 6	On the NetBackup server, configure the mappings for distributed application restores.	Map the application hosts and component hosts in your environment. Configure these mappings in the **Distributed Application Restore Mapping** host property on the master server. See "Configuring mappings for restores of a distributed applications, clusters, or virtual machines " on page 45.
Step 7	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. 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 46.
Step 8	Review the requirements granular restores.	See "Requirements for SharePoint Granular Recovery" on page 19. See "Configuring a SharePoint backup that uses Granular Recovery Technology (GRT)" on page 35.
Step 9	For Federated SharePoint configurations, configure the granular proxy on the master server.	See "Configuring the granular proxy host for Federated SharePoint configurations with VMware" on page 96.
Step 10	Configure the host properties for each SharePoint client.	See "Configuring SharePoint client host properties" on page 39.

	Table 7-1	Configuring a VMware backup that protects SharePoint Server *(continued)*

Step	Action	Description
Step 11	Create a VMware backup policy.	See "Configuring a VMware backup policy to protect SharePoint Server" on page 95.
Step 12	Test your configuration settings.	See "Performing a manual backup" on page 48.

Configuring a VMware backup policy to protect SharePoint Server

Through a VMware backup policy, NetBackup can create full application-consistent backups of a SharePoint Server that resides on a virtual machine. Optionally, you can use NetBackup Accelerator. VMware policies let you exclude certain virtual disks from the VMware backup. If you want to exclude specific SharePoint components, use a MS-SharePoint policy.

Note that before you create a policy, you must perform additional configuration requirements:

- Configure all storage options.

- Configure the logon account for the NetBackup services.

- Review the auto-discovered mappings for the hosts in your environment.

More information on Accelerator is available:

See "About policy attributes" on page 57.

See the NetBackup Administrator's Guide, Volume I.

To configure a VMware backup policy to protect SharePoint Server

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

2 Click the **Attributes** tab.

- From the **Policy type** list, select **VMware**.

- In the **Policy storage** list, select a disk storage unit.
  If you want to use NetBackup Accelerator, select a supported storage unit type. The NetBackup device mapping files list all supported storage types.

- If you want 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.

       Perform block level incremental backups is automatically selected and grayed out. On the **VMware** tab, the **Enable block-level incremental backup** option is also selected and grayed out.

3   On the **Clients** tab, do the following:

- Click **Select automatically through query**.

- Select **NetBackup host to perform automatic virtual machine selection** and the host you want to use.

- Use the Query Builder to create the rules that select the virtual machines you want to back up.

4   Select the **VMware** tab:

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

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

- Select **Enable SharePoint Recovery**.
  This option allows recovery of the databases 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 individually.
  Alternatively, you can select **Enable SQL Recovery**. Do not select both recovery options.

5   If you want to exclude certain disks from the VMware backup, click the **Exclude Disks** tab.

    NetBackup excludes those disks from the VMware backup that protects SharePoint Server. Be sure that any disks that you exclude do not contain database data.

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

Configuring the granular proxy host for Federated SharePoint configurations with VMware

For a VMware backup that protects Federated SharePoint configurations, you need to configure the back-end SQL server as the granular restore proxy host for the catalog hosts (front-end servers in the farm). You can perform this configuration on the master server from the NetBackup Administration Console or from the command line.

To specify the SharePoint granular restore proxy host from the NetBackup Administration Console

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

2   Expand **NetBackup Management > Host Properties > Clients**.

3   In the right pane, right-click on the client and select **Properties**.

4   In the left pane, expand **Windows Client** and click **SharePoint**.

5   In the **SharePoint granular restore proxy host** box, type the name of the SQL back-end host.

6   Click **OK** to save your changes.

7   Repeat this configuration for all servers in the SharePoint farm.

To specify the SharePoint granular restore proxy host from the command line

◆   Use the following command to indicate the granular proxy host that you want to use:

```
bpclient -add -client SharePoint front-end server -granular_proxy
SQL back-end server
```

To verify that the granular restore proxy host is set, use the following command:

```
bpclient -client SharePoint front-end server -G
```

Restoring SharePoint data from a VMware backup

SharePoint data is restored from a VMware backup in the same manner that it is restored from a backup that is performed with the SharePoint Agent. Though you use a VMware policy type to back up the data, you still use the MS-SharePoint policy type for the restore. NetBackup displays the SharePoint data in the VMware backup image that is available for restore.

When you perform a granular restore of SharePoint from multiple VMware application-aware backup images, browse and restore from one image at a time.

Note: NetBackup only supports full VMware backups that protect SharePoint. In a VMware environment, you cannot restore NetBackup for SharePoint (MS-SharePoint) differential restores.

To restore SharePoint data from a VMware backup

1 For the policy type, select **MS-SharePoint**.

2 For the source client, select the name of the SharePoint front-end server.

Select the server that is listed first alphabetically in the list of front-end servers.

Even if SharePoint components exist on multiple computers, all the backups are cataloged under the same SharePoint server name. Once you select that server name, all available backup images for your SharePoint environment are displayed.

3 Follow the instructions for a SharePoint restore from a non-VMware environment.

See "About restores of SharePoint Server and SharePoint Foundation" on page 70.

Disaster recovery

This chapter includes the following topics:

About disaster recovery of a SharePoint Server

Disaster recovery of a SharePoint server cannot be separated from the disaster recovery of windows because SharePoint server uses the Windows security for authentication. You must recover the Windows server before you recover the SharePoint Server.

If you purchased the NetBackup Bare Metal Restore option. Refer to NetBackup Bare Metal Restore Administrator's Guide for more information. If you do not have BMR, see the "Disaster Recovery" chapter in the NetBackup Troubleshooting Guide.

Requirements for disaster recovery of a SharePoint Server

The following requirements exist for disaster recovery of a SharePoint Server:

- A copy of NetBackup for Windows

- The master server has a license for NetBackup for SharePoint Server

- The latest backup of the SharePoint Server you want to recover

- The SharePoint Server CD

- Any service packs that have been applied to the original installation

Recovering a SharePoint server (without BMR)

This topic describes how to recover a SharePoint server installation without Bare Metal Restore (BMR).

To recover a SharePoint server (without BMR)

1   Prepare the SharePoint host for restore. Configure it the same as the original host.

    This configuration may involve new hardware and reinstalling the OS, Windows services packs, and the software that is needed to restore SharePoint from backup.

2   Install any prerequisite software and SharePoint.

    This installation includes running the SharePoint Products Configuration Wizard.

3   Create a new farm configuration database using the SharePoint Products Configuration Wizard.

4   Open your Web browser and verify that you can access the SharePoint Central Administration pages and that the configuration includes the original farm members.

    Run the Farm Configuration Wizard, if applicable.

5   Configure the NetBackup master server and the SharePoint client hosts so you can restore SharePoint from the backup.

6   From the front-end server open the NetBackup Backup, Archive, and Restore interface.

7   Verify that the **Microsoft SharePoint Resources:** are visible.

8   Restore the components of the SharePoint Server in the following order:

    ■   Web application(s), one at a time

    ■   Services (State Service database, metadata, and State Service Proxy)

    ■   Shared Services databases (Service application and metadata), one at a time

    ■   SharePoint Foundation Help Search (WSS_Search)

    ■   InfoPath Forms Services (Metadata)

    ■   Index files

Shared Services Proxies should not be restored. (When NetBackup restores
the Service application it generates new URIs and proxies for the Service
application.)

9   Ensure that all the SharePoint and the SQL services are restarted on the
    SharePoint and the SQL Server, including the IIS service.

10 Use the SharePoint Central Administration, IIS, or the NetBackup Backup,
    Archive, and Restore interface to browse the Web application sites. Verify that
    the Web application sites you restored are accessible and were restored
    properly.

Troubleshooting

This chapter includes the following topics:

- About NetBackup for SharePoint debug logging

- About NetBackup status reports

- Restores to different SharePoint service pack or different cumulative update levels

- Modified system files or ghost files are not cataloged or restored during a site collection restore

- Troubleshooting SharePoint jobs that use Granular Recovery Technology (GRT)

- About troubleshooting SharePoint restore operations

- About NetBackup for SharePoint and client-side deduplication

- Troubleshooting VMware backups and restores of SharePoint Server

About NetBackup for SharePoint 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 SharePoint 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 SharePoint client automatically" on page 103.

See "Enabling the debug logging for NetBackup for SharePoint manually" on page 103.

See "Setting the debug level on a NetBackup for SharePoint Windows client" on page 105.

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 SharePoint 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

Enabling the debug logging for NetBackup for SharePoint manually

To turn on debug logging, create the log directories in the following location:

install_path\NetBackup\logs

Create the following log directories on the SQL Server, the front-end web server, the media server, and the master server.

After you create these directories and perform a backup or restore, debug logging information is placed in a subdirectory that has the name of the process directory. 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. To view the logs that use unified logging, use lv.exe or vxlogview.

For more information about unified logging, see the NetBackup Administrator's Guide, Volume I. For information on how to use the log commands, see the NetBackup Troubleshooting Guide.

Master server

bprd   All restores

Media server

bpbrm	All backups & restores
nbfsd	SharePoint GRT backups & restores

Front-end web server

beds	SharePoint managed code on the SharePoint front-end server
bpbkar	All backups
bpfis	Snapshot backups, VMware backups
bpresolver	SharePoint Granular Recovery Technology (GRT) backups and restores
ncflbc	SharePoint live browse if the image type is VMware
ncfnbcs	VMware Application State Capture (ASC) jobs
SPSV2Recovery Asst	Recovery Assistant unified log. This log does not have its own directory. NetBackup creates this log file in the `NetBackup\logs` folder with the following format: `51216-254-*.log`.
spsv2ra	Recovery Assistant legacy log
tar	Non-GRT restores

SQL Server

bpbkar	All backups
bpfis	Snapshot backups, VMware backups
nbfsd	SharePoint GRT backups and restores
ncfgre	SharePoint GRT restores. Increase the `ncfrai` logging level to add detail.
ncfnbcs	VMware ASC jobs
tar	Non-GRT restores

Setting the debug level on a NetBackup for SharePoint 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 SharePoint 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 SharePoint client

1   Newer NetBackup processes such as `ncfgre` use Veritas 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`

Replace the OID as follows:

`ncfrai` = 158

`ncflbc` = 351

`ncfgre` = 352

`ncfnbcs` = 366

`SPSV2RecoveryAsst` = 254

`spsdkservice` = 479

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`

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 SharePoint 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\Veritas\NetBackup\CurrentVersion\Config`

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
```

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 SharePoint operation

This topic describes how to view the progress report of a NetBackup for SharePoint backup or restore operation.

To view the progress report of a NetBackup for SharePoint 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.

Restores to different SharePoint service pack or different cumulative update levels

The NetBackup for SharePoint 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.

Modified system files or ghost files are not cataloged or restored during a site collection restore

Modified system files or modified ghosted files are neither cataloged nor restored during a site collection restore. This issue is observed in SharePoint 2013 and 2016.

To work around this issue, restore the SharePoint web application content database.

Troubleshooting SharePoint 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.

- SharePoint 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
  ```

- In the Local Security Settings, the Users group must have User Rights Assignment "Allow log on locally". By default, the Users group is included. If the Users group does not have this right, the following error occurs:
  1385 -- Logon failure: the user has not been granted the requested logon type at this computer.

- Backups of the SharePoint web applications that use Granular Recovery Technology (GRT) and that contain a larger number of content databases (100+) may timeout. In this situation, increase the default "Client read timeout" setting to 900 seconds.

- NetBackup supports GRT restores of large documents for SharePoint with SQL Server using SQL Server Native Client 10.0 or later.

- Technical Support may want `nbfsd` logs from the media server. Use the Verbose setting carefully as the `nbfsd` log can grow very large.

About troubleshooting SharePoint restore operations

Note the following when you perform restores:

- NetBackup does not prevent you from restoring placeholders.

- NetBackup lets you restore any object that can hold a document, even it does not contain a document.

The following issues also exist for SharePoint:

- For a SharePoint survey list, after a restore the "Time Created" value reflects the value at the time of the granular restore. This behavior is by design.

- If you restore a deleted report, the report ID is incremented upon restore. If you want to maintain the original report ID value, restore the entire report container. In SharePoint 2016 and later, if you select the entire report container for restore, the report IDs post restore are not from the original set and new IDs are created.

- NetBackup does not start a GRT restore job from a UNIX NetBackup master server. Initiate the restore job from the SharePoint client under which the backup is cataloged.

- If you use a SQL Server local RBS provider and want to take a SharePoint data backup, then you must create a file system policy for file-level backups of SharePoint databases on the SQL Server.
  You can use this backup for database level restores (full and differential)

- When you restore a web application a new application pool is created for each restore. The original application also remains and can be deleted.
  See Figure 9-1.

Figure 9-1   New application pool after a web application restore

About NetBackup for SharePoint and client-side deduplication

When you use the NetBackup for SharePoint with client-side deduplication, the job details only show that deduplication occurs on the front-end Web server. The job is reported this way even if client-side deduplication is enabled for the SQL client

and the other SharePoint farm hosts. Deduplication is performed if you choose **Prefer to use client-side deduplication** or **Always use client-side deduplication**.

The bpbrm logs contain information on the deduplication process (shown as "Client Direct"). For example, the log for a SQL back-end server is as follows:

```
15:49:13.947 [4892.8600] <2> bpbrm main: bpbrm.c.2767: Client Direct is using
alternate client: FABLE
15:49:13.947 [4892.8600] <2> initiate_proxy_server: Calling bpcr_start_proxy
with hostname:FABLE
```

Troubleshooting VMware backups and restores of SharePoint Server

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

- The Application State Capture (ASC) job contacts the NetBackup client on the guest virtual machine and catalogs the application data for recovery.
- One ASC job is created per VM, regardless of which applications are selected in policy.
- ASC messages are filtered to the ASC job details in the Activity Monitor.
- The ASC job can result in status 1 (partially success). For example, if SharePoint was protected, but SQL Server failed to be protected.
- Failure results in the discovery job or parent job exiting with status 1.
- If you enable recovery for a particular application but that application does not exist on the VM, the ASC job returns Status 0.
- bpfis is run and simulates a VSS snapshot backup. This simulation is required to gain logical information of the application.

Table 9-1   Issues with using a VMware policy to protect databases

Issue	Explanation
A database backup fails.	Databases are cataloged and protected only if they exist in a configuration that is supported for VMware backups. The following disks are not supported: raw device mapping (RDMs), Virtual Machine Disk (vmdk) volumes that are marked as independent, mount point volumes, virtual hard disks (VHDs), RAID volumes, ReFS file systems, or an excluded Windows boot disk.
	NetBackup is installed on an excluded Windows boot disk. The ASC job detects this type of disk and treats it like an independent disk. Do not select the **Exclude boot disk** option if NetBackup is installed on the boot drive (typically C:).

Table 9-1 Issues with using a VMware policy to protect databases
(continued)

Issue	Explanation
ASC job produces a status 1 (partially successful).	You selected databases for backup that exist on both supported and on unsupported disks. See "A database backup fails" for unsupported disk information.
	Full-text catalog files exist on the mounted folders. The databases are not cataloged.
The Application State Capture (ASC) job fails and the databases are not protected.	When the ASC job fails, the VMware snapshot or backup continues. Application-specific data cannot be restored.
	You disabled the **Virtual Machine quiesce** option.
	Database objects are on a VHD disk. No objects in the backup are not cataloged, including those that do not exist on the VHD.
	You excluded any data disks from the VMware policy, on the **Exclude Disks** tab. Be sure that any disks that you exclude do not contain database data.
	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.
	You cannot use a VMware incremental policy to protect SharePoint Server. However, the VMware backup job is successful.
	There is a Content database with no site collections present. To avoid this issue, remove the empty Content database or create a site collection in the Content database.
	The policy included SQL Servers that host multiple SharePoint farms.
You can recover the entire virtual machine from the backup, but you cannot recover the databases individually.	You did not select **Enable SharePoint Recovery**, which allows recovery of the databases from the virtual machine backups
VMware job fails with error 2804.	A media server was not added in the **Additional Servers** list.

Table 9-1   Issues with using a VMware policy to protect databases
(continued)

Issue	Explanation
GRT live browse error for an application-aware VMware image.	The **Primary VM identifier** is not a NetBIOS name (for example, display name or UUID). For example, a client name like `client SP2016` becomes `client%20SP2016`. The live browse fails with a database system error because the client name is not recognized as a valid client name. Add an entry to the **Distributed Application Restore Mapping** settings. The **Primary VM identifier** is the name of the application host. The front-end client name is the name of the component host. Alternatively for UNIX master servers, add the `SPS_REDIRECT_ALLOWED` entry to the `bp.conf file`. Or for Windows master servers, add an `SPS_REDIRECT_ALLOWED` registry entry.
The SQL snapshot preparation fails.	In the VMware policy, you select both **Enable SharePoint Recovery** and **Enable SQL Recovery**. Only select one of these recovery options.