

BrightStor® ARCserve® Backup for Windows

Agent for Microsoft SharePoint Guide

r11.5



Computer Associates®

D01184-2E

This documentation and related computer software program (hereinafter referred to as the "Documentation") is for the end user's informational purposes only and is subject to change or withdrawal by Computer Associates International, Inc. ("CA") at any time.

This documentation may not be copied, transferred, reproduced, disclosed or duplicated, in whole or in part, without the prior written consent of CA. This documentation is proprietary information of CA and protected by the copyright laws of the United States and international treaties.

Notwithstanding the foregoing, licensed users may print a reasonable number of copies of this documentation for their own internal use, provided that all CA copyright notices and legends are affixed to each reproduced copy. Only authorized employees, consultants, or agents of the user who are bound by the confidentiality provisions of the license for the software are permitted to have access to such copies.

This right to print copies is limited to the period during which the license for the product remains in full force and effect. Should the license terminate for any reason, it shall be the user's responsibility to return to CA the reproduced copies or to certify to CA that same have been destroyed.

To the extent permitted by applicable law, CA provides this documentation "as is" without warranty of any kind, including without limitation, any implied warranties of merchantability, fitness for a particular purpose or noninfringement. In no event will CA be liable to the end user or any third party for any loss or damage, direct or indirect, from the use of this documentation, including without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised of such loss or damage.

The use of any product referenced in this documentation and this documentation is governed by the end user's applicable license agreement.

The manufacturer of this documentation is Computer Associates International, Inc.

Provided with "Restricted Rights" as set forth in 48 C.F.R. Section 12.212, 48 C.F.R. Sections 52.227-19(c)(1) and (2) or DFARS Section 252.227-7013(c)(1)(ii) or applicable successor provisions.

© 2005 Computer Associates International, Inc.

All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

Contents

Chapter 1: Introducing the Agent	7
Agent Features.....	7
Supported SharePoint Data.....	8
How the Agent Works	9
SharePoint Router Agent.....	10
SharePoint External Data Agent	11
SharePoint Database Agent.....	11
Server Roles.....	11
Consolidated View	12
Chapter 2: Installing the Agent	13
Installation Prerequisites.....	13
Installation Considerations	13
Agent Installation	14
Agent Configuration	14
Environmental Considerations	14
Install and Configure the Agent	15
Uninstall the Agent.....	17
Chapter 3: Backing Up	19
Backup Overview.....	19
Backup Operations.....	19
Backup Types	20
Backup Strategy Recommendations.....	21
Required Full Backup.....	22
Differential Backups.....	22
File and FileGroup Backups.....	23
Transaction Log Backups.....	24
Database Consistency Checks.....	25
Back Up Data	26
Back Up Databases	27
Backup Considerations.....	28
Rotation Schemes and Global Options	28
Dynamic and Explicit Job Packaging	29
Dynamic Job Packaging	30
Mark Objects for Dynamic Job Packaging	30

Explicit Job Packaging	31
Mark Objects for Explicit Job Packaging	32
Chapter 4: Restoring	33
Restore Overview.....	33
Restore Operations	33
SharePoint Database Restores	34
SharePoint Non-Database Data Restores	35
Restore Types	36
Differential Backup Restores.....	37
Transaction Log Restores.....	37
File and FileGroup Restores	38
Restore Options.....	38
Automatic Selection Option	39
Restore Type Option	39
Force Restore Option.....	40
Recovery Completion State Option.....	40
Log Point in Time Restore Option.....	41
Restore Database Files As Option	42
Database Consistency Check (DBCC) Options	43
Restricted User Access After Restore Option.....	43
Keep Replication Settings Option.....	43
SQL Agent Filter Option	44
Restore Methods.....	44
Restore Data	45
Restore Using the Restore by Tree Method.....	45
Restore Using the Restore by Session Method.....	47
Restore to Alternate Disk Locations Using Automatic Selection	50
Restore to Alternate Disk Locations by Individual Session.....	50
Appendix A: Disaster Recovery	53
Front-End Web Server Restore	53
Restore a Front-End Web Server	54
Restore a Search Index Server.....	54
Restore a Backward-Compatible Document Library Server	54
Restore the Database Server	55
Restore a Single-Server Installation Using MSDE.....	56
Appendix B: Configuring Microsoft SQL Server Security Settings	57
Types of Microsoft SQL Authentication.....	57

Authentication Requirements	57
How User Authentication Is Changed.....	58
Check or Change the Microsoft SQL Server Authentication Method.....	58

Index**59**

Chapter 1: Introducing the Agent

BrightStor® ARCserve® Backup is a comprehensive, distributed storage solution for applications, databases, distributed servers, and file systems. It provides backup and restore capabilities for databases, business-critical applications, and network clients.

Among the agents BrightStor ARCserve Backup offers is the BrightStor® ARCserve® Backup Agent for Microsoft SharePoint. This agent provides the ability to back up and restore Microsoft SharePoint Portal Server 2003 and Microsoft Windows SharePoint Services data.

Although SharePoint environments can be complex and distributed across a number of machines, the agent provides full protection of SharePoint installations by consolidating all SharePoint data into a single node in the interface on the BrightStor ARCserve Backup server. SharePoint content consists of distributed SharePoint databases, backward-compatible document libraries, Single Sign-On (SSO), and search indexes. The agent lets you use the features of BrightStor ARCserve Backup to easily manage the backup and restore of all SharePoint data on your network.

Note: Throughout this guide, backward-compatible document libraries, Single Sign-On (encryption key component only), and search indexes are referred to as *non-database data* to distinguish this type of data from SharePoint database data.

Agent Features

The Agent for Microsoft SharePoint offers a number of features to facilitate your backup and restore operations:

- Provides backup and restore capabilities for both Microsoft SharePoint Portal 2003 and Microsoft Windows SharePoint Services installations
- Supports backup and restore functionality for Microsoft SQL databases, and Microsoft SQL Server 2000 Desktop Engine (MSDE) and Microsoft SQL Server 2000 Desktop Engine Windows (WMSDE) databases
- Provides protection to search indexes, backward-compatible document libraries, and Single Sign-On for Microsoft SharePoint Portal Server 2003 installations

- Supports database complete, database differential, Files/FileGroups differential, and Transaction log backups for SharePoint databases
Note: Only Database Complete backups are supported for non-database data (such as search indexes).
- Enables SharePoint data to be restored to its original location or to an alternate destination

Supported SharePoint Data

The Agent for Microsoft SharePoint requires Windows 2003 and supports the backup of the following SharePoint data:

- Microsoft SharePoint Portal Server 2003
 - SharePoint Portal 2003 databases
 - Single Sign-On database
 - Search indexes
 - Backward-compatible document libraries
- Microsoft Windows SharePoint Services
 - Windows SharePoint Services databases

Note: You must protect customized template and configuration files stored on front-end web servers with a file system backup. The agent does not provide support for these files, including:

- IIS (Internet Information Server) metabase
- SharePoint extended virtual server root directories
- Custom web part assemblies
- Custom SharePoint templates and configuration files
- Any add-on software used by the SharePoint sites

You can fully protect this information by using the BrightStor® ARCserve® Backup Client Agent for Windows. For more information about using this agent, see the *Client Agents Guide*.

How the Agent Works

BrightStor ARCserve Backup and the Agent for Microsoft SharePoint work together to back up and restore SharePoint data. When BrightStor ARCserve Backup backs up data, it sends a request to the agent. The agent retrieves the data from the server and sends it to BrightStor ARCserve Backup, where the data is backed up to media. During a restore operation, the agent functions in a similar way and helps transfer the backed up data from BrightStor ARCserve Backup to the server.

Because SharePoint data can be distributed across multiple servers, the Agent for Microsoft SharePoint includes the following subagents to manage the various servers:

- SharePoint Router Agent
- SharePoint External Data Agent
- SharePoint Database Agent

Note: For more information on each of these subagents, see the sections SharePoint Router Agent, SharePoint External Data Agent, and SharePoint Database Agent in this chapter.

By providing a consolidated view of the SharePoint data, these subagents work together as a unit to protect SharePoint data that is distributed across multiple servers.

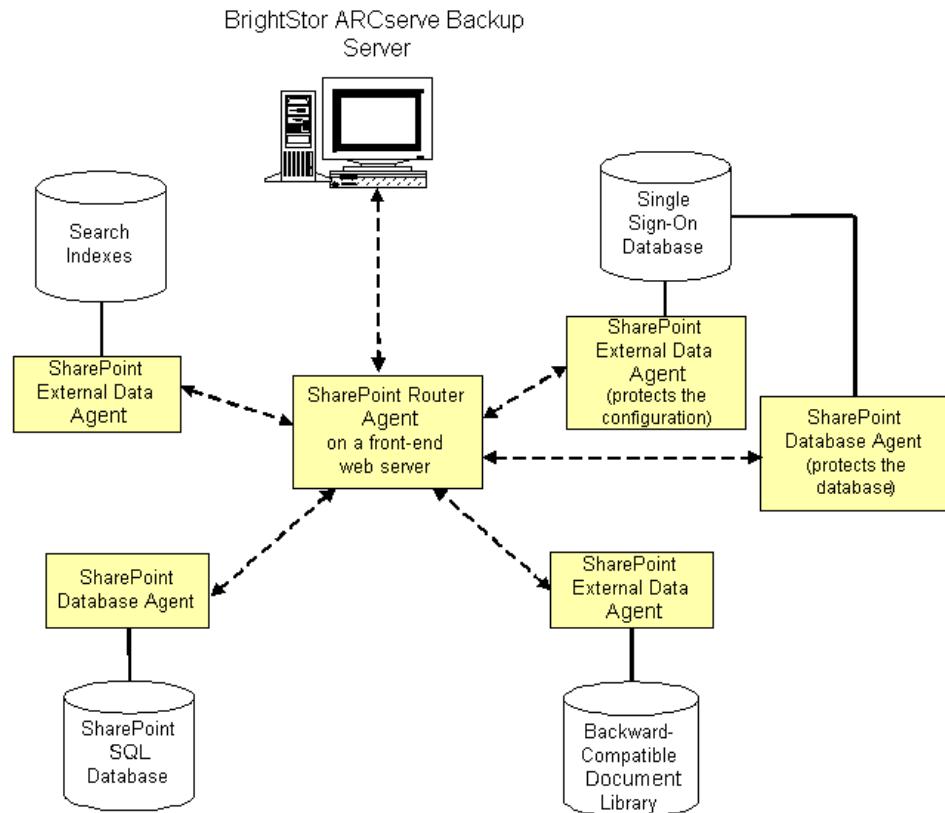
In addition, the subagents save time by routing backup data directly from the data source to the destination in environments with multiple SharePoint servers.

To begin protecting SharePoint data, install the BrightStor ARCserve Backup for Microsoft SharePoint Configuration wizard component on a BrightStor ARCserve Backup server and use the configuration wizard to install the SharePoint Router Agent on the front-end web server. The SharePoint Router Agent reads the configuration information, determines where the other components are located, and then installs the remaining subagents on the appropriate SharePoint servers, as follows:

- The SharePoint External Data Agent functions on the following servers:
 - Search indexes server
 - Backward-compatible document library server
 - Single Sign-On server (protects the encryption key component of the database)

- The SharePoint Database Agent is installed on the following servers:
 - SharePoint databases server
 - Single Sign-On database server (protects the database portion only)

The following diagram illustrates where the subagents are installed:



Note: Multiple subagents can be installed on a single server when that SharePoint server fills multiple roles.

SharePoint Router Agent

The SharePoint Router Agent is the central management component of the Agent for Microsoft SharePoint, and is installed on a front-end web server. The SharePoint Router Agent provides the following functionality:

- Consolidates browser requests from a distributed SharePoint server farm into a single administrative view. The backup browse view shows all SharePoint data under a single backup node.

- Communicates the physical and logical information for the SharePoint data when requested. It obtains the browse information directly from the subagents, which are installed on SharePoint servers.
- Manages the backup server requests, although it is not directly involved with the backup and restore data. To enhance performance, backup and restore tasks are sent directly to the appropriate backup server, and data is sent directly from the data source to the backup destination.

SharePoint External Data Agent

The SharePoint External Data Agent is a subagent of the Agent for Microsoft SharePoint. It protects SharePoint data that is external to SharePoint databases, including the following SharePoint data:

- Backward-compatible document libraries
- Encryption key component of Single Sign-On
- Search indexes

SharePoint Database Agent

The SharePoint Database Agent is a subagent of the Agent for Microsoft SharePoint. The SharePoint Database Agent is installed on one or more SharePoint servers hosting the following SharePoint databases:

- Microsoft SQL Server
- Microsoft SQL Server 2000 Desktop Engine Windows (WMSDE 2000 or MSDE)

The SharePoint Database Agent is similar to the BrightStor® ARCserve® Backup Agent for Microsoft SQL Server, with the following differences:

- SharePoint databases protected by the SharePoint Database Agent appear under the SharePoint backup node.
- The browse interface detects only SharePoint data and ignores any other Microsoft SQL databases that exist outside of the SharePoint server farm.

Server Roles

Each server in the SharePoint server farm must be assigned at least one role to perform. Use the configuration wizard to query the machines about the roles each of the servers have been assigned. The configuration wizard installs the appropriate agent or subagent on each server. If the SharePoint server farm configuration changes, use the configuration wizard to modify or remove the subagents.

Consolidated View

The Backup Manager displays all SharePoint data under the Agent for Microsoft SharePoint node, even though the SharePoint data may exist on multiple machines in a distributed environment.

The following SharePoint data appears directly under the Agent for Microsoft SharePoint node:

- Backward-compatible document library

Note: If you have not installed or configured this optional library, it does not appear in the tree.

- One SharePoint configuration database

Note: If the configuration database is the only database to appear and is marked as inaccessible, it indicates that the agent was unable to browse the SharePoint information and cannot access the data. Ensure that SharePoint and Microsoft SQL Server are running correctly.

- SharePoint portals

- Search indexes

- Single Sign-On

- Windows SharePoint Services content databases

Note: In a portal environment these databases may not appear at the top level, but under the host portal.

The following SharePoint items can be expanded to display all instances on the SharePoint server farm:

- SharePoint portals - Expand to show the databases.

- Search indexes - Expand to show the Index servers.

- Single Sign-On - Expand to show the Single Sign-On database and the configuration file.

Note: If you have not installed or configured this optional component, it does not appear in the tree.

To view the physical location of a SharePoint backup item, select a SharePoint backup item and view the property set in the Properties pane.

Chapter 2: Installing the Agent

This chapter provides the information you need to install and configure the Agent for Microsoft SharePoint. The information in this chapter assumes you are familiar with the characteristics and requirements of your Microsoft SharePoint server farm.

Installation Prerequisites

Before installing the Agent for Microsoft SharePoint, you must satisfy the following prerequisites:

- Verify that your system meets the minimum requirements needed to install the Agent for Microsoft SharePoint. For a list of requirements, see the Readme file.
- Ensure that you have administrator privileges or the proper authority to install software on the computers where you will be installing the product.
- Verify that you have access rights to all SharePoint data.
- Verify that you have installed Microsoft Windows SharePoint Services or Microsoft SharePoint Portal on the front-end web server.

Installation Considerations

Consider the following when you install the agent and subagents:

- You must install the BrightStor ARCserve Backup for Microsoft SharePoint Configuration wizard on the BrightStor ARCserve Backup server.
- The BrightStor ARCserve Backup server must be able to ping all machines in the SharePoint environment by name. If you do not use DNS (Domain Name System) in your SharePoint environment, you must add all the machines in the SharePoint environment into the hosts file on the BrightStor ARCserve Backup server.
- After installing the configuration wizard, use the wizard to configure and install the subagents on the appropriate machines.

Agent Installation

Before you begin the installation, ensure that you have met the installation prerequisites and reviewed the installation considerations. For information about installing the Agent for Microsoft SharePoint, see the *Getting Started* guide.

Agent Configuration

During installation, the setup program installs the configuration wizard. Use the configuration wizard to configure and install the subagents on your servers. The subagents are installed after the configuration is complete.

Note: You must configure the subagents to complete the agent installation process.

The configuration wizard also lets you uninstall the subagents from your servers.

Environmental Considerations

SharePoint environments can be complex and distributed across a number of machines. The server farm configuration must be supported by Microsoft. As an example, a distributed SharePoint environment could contain the following components:

- A server configured as a BrightStor ARCserve Backup server
- A front-end web server for the SharePoint server farm that is also a Search Server
- A second front-end web server for the SharePoint server farm that is also a Search server.
- A server configured as the Index and Job Server that also hosts the Single Sign-on configuration file
- The SQL Server database server used by the SharePoint server farm
- A server hosting the backward-compatible document library

Install and Configure the Agent

To install and configure the agent, you must ensure that you have the required privileges to install software on each of the machines in the server farm and have access rights to all the SharePoint data.

After you have installed the Agent for Microsoft SharePoint on the BrightStor ARCserve Backup server, perform the following procedure to configure and install the subagents for the Agent for Microsoft SharePoint.

1. Start the configuration wizard.

When you install the agent, the configuration wizard starts automatically. To run the configuration wizard again, use the Agent for SharePoint Configuration shortcut.

2. The Server Selection dialog appears, prompting you to select a front-end web server on which to install the SharePoint Router Agent.

If this is the first time you are running this configuration, check the Install router onto machine option and click Next.

If you are reconfiguring an existing installation, leave this check box empty and click Next.

3. The Configuration Type dialog appears, allowing you to select one of the following configuration types:

- **Automatic:** This option automatically generates the necessary information to configure the installation of the agents required to protect the current SharePoint configuration.
- **Custom:** This option allows you to manually select the machines on which to install the agent required to protect your data. You must manually protect each server role (Search Index, Document Library, Single Sign-On, and Portal DB). In addition, the Custom option allows you to uninstall agents from your machines.

Select one of the configuration options and click Next.

4. If you selected the Custom Configuration Type, select the machine names in the Unprotected list in the Search Index dialog and click Add to move these machine names to the Protected list. During the installation stage of the configuration wizard, the agent required to protect the data is installed on all machines in the Protected list.

Repeat this step for each server role (Document Library, Single Sign-On, and Portal DB) and click Next.

If you selected the Automatic Configuration Type, go on to the next step.

5. The Selected Configuration dialog displays the configuration to be installed.

Note: To set the installation path for any of the subagents, select the machine name, change the path in the Agent Install Path field, and click Apply.

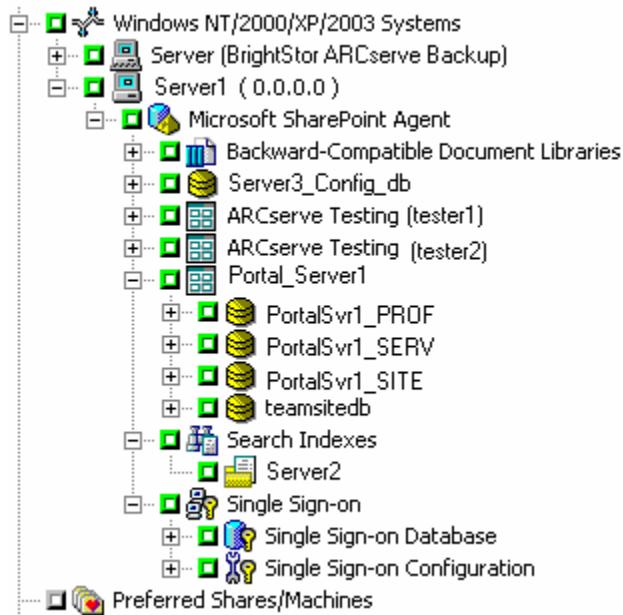
If you do not want to set the installation paths, click Next to begin the installation process.

A progress dialog allows you to track the installation of the components installed throughout the process. When the installation is complete, a summary dialog appears, allowing you to view the status of each of the servers in the server farm.

If you run the Configuration wizard as part of the setup process, click Finish to return to the Install Summary. Check marks in the Install Summary screen indicate the agents that have been successfully installed and configured.

If you run the Configuration wizard at any time after the setup process, click Finish to end the configuration.

6. From the Backup Manager, browse to the machine and expand the agent to view a consolidated view of all the servers:



Everything appears under a single node although the data can be spread over multiple machines.

Uninstall the Agent

To uninstall the Agent for Microsoft SharePoint or one of its subagents, you can use one of the following methods:

- Configuration wizard (does not remove the SharePoint Router Agent)
- Add or Remove Programs option in Windows (removes everything, including the SharePoint Router Agent)

The simplest way to uninstall subagents (with the exception of the SharePoint Router Agent) in a distributed environment is to use the configuration wizard. Select the Custom Configuration Type and move each subagent from the Protected list to the Unprotected list in the configuration wizard.

Alternatively, you can use Add or Remove Programs in Windows and select CA BrightStor ARCserve Backup Agent for Microsoft SharePoint.

Note: To remove the SharePoint Router Agent, you **must** use Windows Add or Remove Programs.

In addition to removing the agent and subagents, you can remove the configuration wizard and the SPIImages directory from the BrightStor ARCserve Backup server. To remove these items, use Add or Remove Programs in Windows and select CA BrightStor ARCserve Backup Agent for Microsoft SharePoint Admin GUI.

Chapter 3: Backing Up

This chapter contains information about backing up SharePoint data using BrightStor ARCserve Backup and the Agent for Microsoft SharePoint.

Backup Overview

To *back up* is to create a copy of the SharePoint database or non-database data objects. Use the Agent for Microsoft SharePoint to perform backups.

When a SharePoint database or non-database data object backup is started in BrightStor ARCserve Backup, the Agent for Microsoft SharePoint initiates a dynamic backup of the database and data. This backup can take place while the database is active. The backup captures the state of the data at the moment the statement is executed. No partial transactions are captured. Any data changes made after the backup begins are not captured in the backed up database or non-database data.

Backup Operations

Back up SharePoint data using the Backup Manager interface on a BrightStor ARCserve Backup server. All SharePoint data can be accessed from a single point, regardless of the physical locations of the SharePoint servers.

Use the Backup Manager to perform the following backup tasks:

- Browse SharePoint data
- Set backup options at job level and database level
- Back up selected SharePoint data

Note: For SharePoint database data, the lowest level element that can be independently backed up is the database. Individual tables cannot be backed up.

Backup Types

The Agent for Microsoft SharePoint supports the following types of database backups:

- **Database Complete** - Use full backups to back up your SharePoint database. You can also use full backups to back up all your SharePoint non-database data (such as search indexes).
Note: For non-database data, the agent supports only complete backups.
- **Database Differential** - Backs up database data that has changed since the last complete backup. For example, if you ran a complete backup of your database on Sunday night, you can run a differential backup on Monday night to back up only the data that changed on Monday.
- **Transaction Log** - Backs up the Transaction log. Transaction log backups provide the following options:
 - **Remove inactive entries from transaction log** - Truncates the log files. This is the default option.
 - **Do not remove inactive entries from transaction log** - Retains inactive log entries after backup. These entries are included in the next Transaction log backup.
 - **Back up only the log tail and leave the database in unrecovered mode** - Backs up the log and leaves the database data in a restoring state. Use this option to capture activity since the last backup, and take the database offline to restore it.
- **Files and FileGroups** - Backs up selected files in a database. Use this option to back up a file or FileGroup when the database size and performance requirements make it impractical to perform a full database backup.
- **Files and FileGroups; Differential** - Backs up database data changed in selected files since the last file and FileGroup backup. Differential file backups reduce recovery time by reducing the number of transactions from the Transaction log that must be restored.

Backup Strategy Recommendations

To establish a good backup strategy for database and non-database data, follow these recommendations:

- If your database activity is low to medium, schedule your backups with the following frequency:
 - Full backups: once per week
 - Differential backups: once per day
 - Transaction Log backups: every two to four hours
- If your database activity is high and your database is of small to medium size, schedule your backups with the following frequency:
 - Full backups: twice per week
 - Differential backups: twice per day
 - Transaction Log backups: every 60 minutes
- If your database activity is high and you have a large database using the Full or Bulk-Logged Recovery model, schedule your backups with the following frequency:
 - Full backup: once per week
 - Differential backup: once per day
 - Transaction Log backup: every 20 minutes
- If your database activity is high and you have a large size database using the Simple Recovery model, schedule your backups with the following frequency:
 - Full backup: once per week
 - Differential backup: twice per day
- For non-database data (such as the backward-compatible document library), schedule or plan your backups according to the frequency of your data changes. For instance, if the activity level for your backward-compatible document library activity is high, you should perform a full backup twice a week. If it is low, you may want to perform a full backup only once a week. Remember that you can back up non-database data only with a full backup.

Required Full Backup

After you perform certain database management actions, your next backup **must** be a full database backup. If you perform one of these actions and then perform a differential backup, Transaction log backup, or files and FileGroups backup, you may be unable to use that backup with your last full database backup to restore the database successfully.

To prevent this problem, always perform a full database backup immediately after you have performed any of the following actions:

- Changed the SharePoint configuration
- Added new search indexes
- Created a new database
- Changed the recovery model of the database
- Changed the number of files or FileGroups in the database
- Changed the arrangement of files among the FileGroups
- Canceled a full backup job while it is running
- Restored the database from backups

Differential Backups

A differential backup records only the data that has changed since the last full database backup. On average, these backups are smaller and typically take less time to complete than full database backups, although they are typically larger and take more time to complete than Transaction log backups. To restore a database, a differential backup requires only the last full backup, and does not need any of the other differential or Transaction log backups performed since the last backup. A differential backup is also faster to restore than a Transaction log backup because transactions do not need to be reprocessed.

Note: If a database is very active or if a long time has passed since the last full backup, a differential backup could take as long as a full backup.

Differential Backup Timing

Perform differential backups as a supplement to full backups. Because they are usually faster and smaller, you can perform them more often than full database backups. They are also typically more efficient because they require less space on media and have a briefer impact on database performance than frequent, full database backups. Additionally, you can use them to minimize the number of Transaction logs you need to recover during a restore, because you need to restore only those Transaction log backups performed since the differential backup.

Differential backups are most beneficial under the following circumstances:

- A relatively small portion of the data in the database has changed since the last database backup. Differential database backups are most efficient if the same data is modified frequently.
- You are using the Simple Recovery model, which does not permit Transaction log backups, and you want to perform backups more frequently than is practical for full database backups.
- You are using the Full or Bulk-Logged Recovery model and want to minimize the time it takes to roll forward Transaction log backups when restoring a database.

Note: After you have modified the structure or configuration of the database (for example, by adding more data or log files or changing the recovery model), you must perform a full database backup before performing a differential or Transaction log backup.

File and FileGroup Backups

You can choose to back up one or more FileGroups or individual files when the database size and performance requirements make it impractical to perform a full database backup.

If you choose to back up an individual file instead of the full database, put procedures in place to ensure that all files in the database are backed up regularly, and perform separate Transaction log backups for the databases whose files or FileGroups you back up individually. After restoring a file backup, you must apply the Transaction log to roll the contents of the file forward to make it consistent with the rest of the database. For more information, see the Microsoft SQL Server documentation.

Transaction Log Backups

Transaction logs contain the record of Microsoft SQL Server database activity; back them up frequently. To back them up, run self-contained Transaction log backups separately from database backups. Transaction log backups offer the following advantages over other types of backups:

- Generally faster than differential backups
- Typically faster and smaller than full database backups (unless they have not been truncated recently)
- Typically, less impact on database performance while running
- Normally able to be restored to a specific point in time, rather than only to the time the backup was made

Important! *Transaction logs are not backed up during full or differential database backups. You must back them up by running separate Transaction log backups.*

After you have modified the structure or configuration of the database (for example, by adding more data or log files, or changing the recovery model), you must perform a full database backup before performing a differential or Transaction log backup.

Restore Requirements for Transaction Log Backups

To restore a Transaction log backup, you must first restore the following:

- The last full database backup performed
- The last differential backup performed since that full database backup, if any
- Any other Transaction log backups performed since the last full database or differential backup

It takes longer to recover a database when you restore the database and several Transaction logs than it does when you restore only the database. Finding the correct strategy depends on your environment. You must consider the time required to perform backups in relation to the time required to restore.

Important! *Do not perform a Transaction log backup until you have performed at least one full database backup.*

Truncate Transaction Logs

You can truncate Transaction logs when you back them up. To truncate a Transaction log, select the Remove inactive entries from transaction log option when you configure the backup. If the Transaction log is not truncated, it may eventually grow large.

Database Consistency Checks

When your database activity is low, you should run a database consistency check (DBCC), particularly with a large database. Although it takes some time, it is important to determine that your Microsoft SQL Server database is functioning well.

A DBCC tests the physical and logical consistency of a database. When you enable the Database Consistency Check option for a backup, the DBCC performs the following tests:

- **DBCC CHECKDB:** Checks the allocation and structural integrity of all objects in the specified database. By default, the CHECKDB performs a check for indexes that can increase the overall execution time.
Note: The system table indexes are checked regardless of whether you select this option.
- **DBCC CHECKCATALOG:** Checks for consistency in and between system tables in the specified database.

Database Consistency Check (DBCC) Options

DBCC provides the following options:

- **Before Backup:** Checks consistency before the backup of the database.
- **After Backup:** Checks consistency after the backup of the database.
- **Continue with backup, if DBCC fails:** Performs a database backup even if the consistency check fails.
- **After restore:** Performs DBCC after the restore of the database.

- **Do not check indexes:** Checks the database for consistency without checking indexes for user-defined tables.
- **Check only the physical consistency of the database:** Detects torn pages and common hardware failures. In addition, it checks the integrity of the physical structure of the page and record headers, and the consistency between the page's object ID and index ID.

All error messages that are generated during the DBCC are displayed in the Agent for Microsoft SharePoint directory on the machine where the SharePoint Database Agent is installed. The dbasql.log is located in the Backup Agent directory.

Back Up Data

Use the Backup Manager in BrightStor ARCserve Backup to back up SharePoint data. To perform a backup of SharePoint data, follow these steps:

1. In the Backup Manager, browse the left pane and expand the Microsoft SharePoint Agent backup node.
The SharePoint data appears in the browse tree.
2. Select the entire SharePoint backup node or the SharePoint data you want to back up.
3. Set or select any backup options.

Note: For more information about backup options, see the *Administrator Guide*.

4. Click Start.

If you have selected SharePoint databases, the Security and Agent Information dialog appears. If required, provide the proper authentication for the selected databases.

Note: Authentication is packaged with the backup job. You do not need to provide this when the backup job runs.

5. Click OK on the Submit Job dialog.

The selected SharePoint data is backed up.

Back Up Databases

To back up a database, follow these steps:

1. Ensure that Microsoft SQL Server is running on your server. The Microsoft SQL Server service must be started.
2. Start the CA BrightStor Backup Agent RPC Server service and CA BrightStor Backup Agent Remote Service, if necessary.

Note: These services are started automatically when the agent is installed and are set to start automatically if the machine is restarted.

3. Open the Backup Manager, and expand the Microsoft SharePoint Agent node to display a list of databases.
4. Follow these steps for each database you are backing up for this job:

- a. Choose a database under the Microsoft SharePoint Agent node. Information about the selected database appears in the right pane of the Backup Manager.

Note: For information about selecting a database to apply options properly for backup, see Dynamic and Explicit Job Packaging in this chapter.

- b. Right-click the database object and select Backup Agent Options from the pop-up menu. The Backup Agent Options opens.
- c. Select the type of backup you want to perform. For more information about backup types, see Backup Types in this chapter.
- d. If you chose the Files/FileGroups or Files/FileGroups-Differential backup type, click the Browse or Browse Files/FileGroups button. The Specify FileGroups and Files dialog opens.

Select the specific files and FileGroups you want to back up, and click OK.

- e. (Optional) Enable a Database Consistency Check and select the Database Consistency Check options. For more information about Database Consistency Checks, see Database Consistency Checks in this chapter and your Microsoft SQL documentation. Click OK.

5. On the Destination tab in the Backup Manager, select a backup destination.

Note: You can use the * symbol in the Group or Media fields to create partial wildcards when you select a backup destination. For example, if you have two sets of device groups, one with all members beginning GroupA and the other with all members beginning GroupB, you can select all the GroupA members by entering GroupA* in the Group field. For more information about selecting devices and media, see the *Administrator Guide*.

6. On the Schedule tab, select the scheduling options for this backup. For information about scheduling backups, see the *Administrator Guide*.
7. Click Start. The Security and Agent Information dialog opens.

Note: In this dialog, the column and button labeled Agent refer to the Client Agent for Windows. You can edit client agent information at this time. For more information about client agents, see the *Administrator Guide*.
8. Verify the user name and password for the target machine and for Microsoft SQL Server. To change the security information for Microsoft SQL Server, click Security and change the information in the dialog.
9. After verifying or changing the security information, click OK. The Submit Job dialog opens.
10. (Optional) Use the Submit Job dialog to select the job execution time, submit the job on hold, add an optional description for the backup job, or select source priority.
11. Click OK. The Job Status window opens. Use this window to monitor the current status of your job. For more information about the Job Status window, see the *Administrator Guide*.

Backup Considerations

You should back up a database immediately after you create it and continue to back it up on a regular schedule to ensure smooth recovery from a database or media failure. Be sure to maintain regular backups of all databases and content.

Rotation Schemes and Global Options

BrightStor ARCserve Backup can use incremental and differential global backup methods when backing up the Agent for Microsoft SharePoint, allowing you to use a rotation scheme to perform differential and Transaction log backups of SharePoint databases, dynamically adjusting for the limitations of each individual database.

Note: For more information about rotation schemes and automatic backups, see the *Administrator Guide*.

You can use the following backup methods:

- **Full Backup Method** - If you specified backup options for the target database, these options are applied. Otherwise, a full database backup is performed by default.

- **Differential Backup Method** - The following rules apply to a differential backup:
 - If you are backing up a system database (for example, master, model, or msdb), a full database backup is always performed.
 - If the Microsoft SQL Server has no record of a prior full database backup of the target database, a full database backup is performed.
 - If the backup options selected for the target database include a selection of specific database files and FileGroups, a File-and-FileGroup differential backup is performed.
 - In all other circumstances, a differential database backup is performed.
- **Incremental Backup Method** - The following rules apply to an incremental backup:
 - If you are backing up a system database (for example, master, model, or msdb), a full database backup is always performed.
 - If the Microsoft SQL Server has no record of a prior full database backup of the target database, a full database backup is performed.
 - If the database uses the Simple Recovery Model, a differential database backup is performed.
 - In all other circumstances, a Transaction log backup with truncation is performed.

Important! *Performing a backup can slow the system down. Run backups when the database is not being heavily updated.*

Dynamic and Explicit Job Packaging

BrightStor ARCServe Backup provides two ways to package or set up your backup jobs:

- Dynamic job packaging
- Explicit job packaging

Dynamic Job Packaging

If you mark a parent object for dynamic job packaging when defining a backup job, BrightStor ARCserve Backup automatically selects and protects, at the time the backup job runs, all the components of the object for backup.

For example, if you choose to back up at the Microsoft SharePoint Agent level and you mark the agent object for dynamic job packaging and then you add a new component, the new component is included when you run the next backup job.

Important! *When you mark a parent object for dynamic job packaging, all of its associated (or child) objects are also marked for dynamic job packaging and are selected for backup. Child objects of an object marked for dynamic packaging lose any separate options you have assigned them when the job is submitted.*

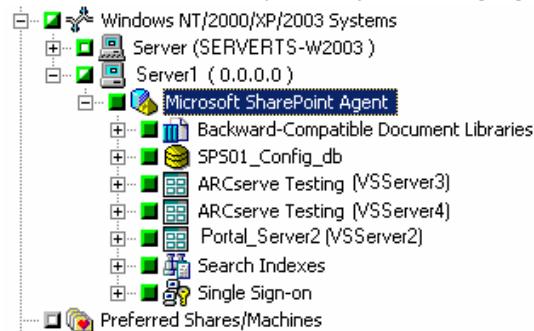
Mark Objects for Dynamic Job Packaging

To mark an object for dynamic job packaging, follow these steps:

1. On the Source tab in the Backup Manager, expand the directory tree until the object you want to mark for dynamic job packaging appears.
2. Click the square next to the object.

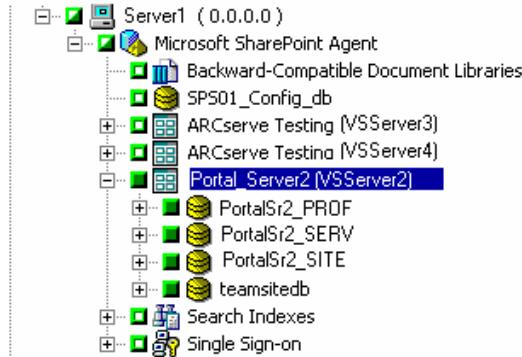
The square next to the object, and the squares next to all the children of the object, become completely green.

In the following example, Microsoft SharePoint Agent has been marked for dynamic job packaging. All of the child items in the following illustration are also marked for dynamic job packaging:



When you select a backup object at this level, even if you add a new item, for example a new portal, the new item is protected without requiring you to modify the job.

You can also protect at an individual level. For example, the following illustration shows that an individual portal has been selected for dynamic job packaging, which means that if more databases are added to this portal, they will be included dynamically in this job:



Explicit Job Packaging

If you mark a database or non-database object for explicit job packaging when defining your backup job, you mark some or all of its child objects for dynamic job packaging, but do not mark the parent.

For example, if you select the Microsoft SharePoint Agent node, which is the parent, it is packaged dynamically. If you then deselect the teamsitedb node under the Portal_Server2 node, all three nodes (that is, teamsitedb, Portal_Server2, and Agent) are packaged explicitly. This means that if you add a new database to the Portal_Server2 node or a new item to the Microsoft SharePoint Agent node, the new item or database is not included automatically in the backup job.

Explicit job packaging gives you the ability to customize local backup options. For example, if you run a backup job for which you have dynamically packaged the Microsoft SharePoint Agent on your server (which is explicitly packaged), you can select one set of options for one component, such as the teamsitedb, and another set of options for another component, such as the configuration database.

Important! *To customize database options, you must package the database items explicitly.*

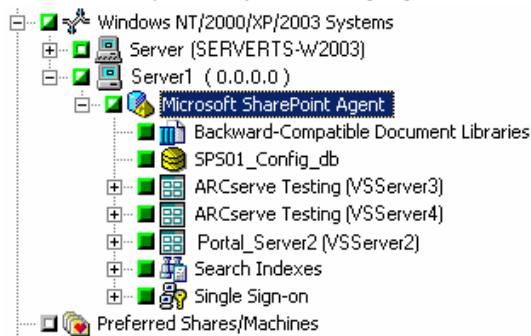
Mark Objects for Explicit Job Packaging

To mark an object for explicit job packaging, follow these steps:

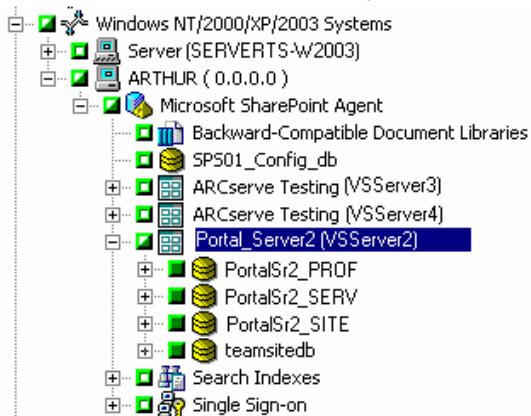
1. On the Source tab in the Backup Manager, expand the directory tree until the object you want to mark for explicit job packaging appears.
2. Click the squares next each of the items below the object.

The squares next to the child objects become completely green and the square next to the parent object becomes half green and half white.

In the following example, the Microsoft SharePoint Agent node has been marked for explicit job packaging, and all the items below have been marked for dynamic job packaging:



You can also protect at an individual level. For example, the following illustration shows that the **Portal_Server2** node has been selected for explicit job packaging, which means that if more databases are added to this node or are removed, they will not be included in this job:



Chapter 4: Restoring

This chapter contains information about restoring SharePoint data using BrightStor ARCserve Backup and the Agent for Microsoft SharePoint.

Restore Overview

To *restore* is to load a database or one or more non-database data objects from a backup of that database or the objects. If a database or non-database data object is lost or damaged, you can restore it by reloading the most recent database or non-database data object backup. A restore job overwrites any information in the database with the backed up information.

When restoring a SharePoint database, exclusive access to the database must be granted during the restore process. If users or applications attempt to access a database during the restore process, the restore process will fail. One way to prevent users from accessing the database is to stop the following Microsoft SharePoint-related services on all machines in the SharePoint installation:

- Microsoft SharePointPS Search Service
- SharePoint Timer Service
- SharePoint Portal Alert Service
- SharePoint Portal Administration Service
- Microsoft Single Sign-on Service (if using Single Sign-On)

For more information about stopping these services, see the *Microsoft Office SharePoint Portal Server 2003 Administrator's Guide* or *Microsoft Windows SharePoint Services 2.0 Administrator's Guide*.

Restore Operations

Use the Restore Manager to perform restore operations for SharePoint data. The Restore Manager lets you perform the following tasks:

- Browse the data that has been backed up
- Set restore options
- Queue a restore job

In addition, you can restore SharePoint data to an alternate location.

SharePoint Database Restores

Different databases need to be restored in different ways. The following sections describe the different types of databases and some recommended ways to restore them.

Configuration Database Restore

Each SharePoint installation includes one configuration database. Without this database (for example, if it becomes corrupted), Windows SharePoint Services (WSS) or SharePoint Portal 2003 cannot function properly.

You cannot restore this database to its original location while SharePoint is running because the database is in use, and exclusive access is required when restoring. Use one of the following methods to avoid getting a failed error message while restoring:

- Stop all SharePoint services, restore the database, and then restart the services.
- Restore the database with a new name. Using the SharePoint administration tools, detach the SharePoint machines from the old database and attach them to the restored one with the new name.

Portal Databases Restore

Three databases are created for each portal site:

- *Portal_SERV*
- *Portal_PROF*
- *Portal_SITE*

Note: Microsoft recommends that you restore these databases as a group, unless you know specifically that there is a problem with only one of them.

If you encounter difficulty gaining exclusive access to the databases to allow the restore operation to complete successfully, use one of the following methods:

- Stop all SharePoint services, restore the databases, and then restart the services.
- Delete the existing portal. Restore the databases, and follow the "Restoring a Portal Site" procedure in the *Microsoft Office SharePoint Portal Server 2003 Administrator's Guide*.

WSS and Portal Content Database Restore

When restoring the Windows SharePoint Services (WSS) and Portal Content databases, follow these steps to avoid exclusive access problems:

1. Use the Manage Content Databases window in SharePoint Administration to detach the database from SharePoint.
2. Restore the database.
3. Use the Manage Content Databases window to reattach the database to SharePoint.

SharePoint Single Sign-On Database

To avoid exclusive access problems when restoring the Single Sign-On database, use one of these methods:

- Stop the Microsoft Single Sign-On Service, restore the database, and then restart the service.
- Restore the database with a new name. Use the SharePoint Sign-On Administration tool to use the new database.

SharePoint Non-Database Data Restores

SharePoint non-database data restores are less restrictive than SharePoint database restores. Non-database data includes the following types of data:

- **Backward-Compatible Document Library Restore** - You can restore the backward-compatible document library to its original location or to another backward-compatible document library. You do not need to stop any services.
- **Single Sign-On Configuration File Restore** - You can restore the Single Sign-On configuration file to its original location or to another SharePoint Single Sign-on configuration file. You do not need to stop any services.
- **Search Indexes Restore** - You can restore Search Indexes to its original location or to another SharePoint Search Index Server. You do not need to stop any services.

Note: When restoring to an alternate location, you must select a destination item of the same type to prevent the job from failing. For example, a backward-compatible document library can be restored only to another backward-compatible document library.

Restore Types

The Agent for Microsoft SharePoint supports different restore types for non-database data restores and for database restores.

- For SharePoint non-database data restores, the agent supports only Complete database restore.
- For database restores, the agent supports the following types of restores:
 - **Complete database restore** - Restores the entire SharePoint database.
 - **Differential backup restore** - Restores the database to the point in time when you created the differential backup. Typically, you would supplement differential backups by creating multiple Transaction log backups after each database backup. To use this restore type, you must restore the last complete database backup before restoring the differential backup. Using a combination of full-database, differential, and Transaction log backups, you can minimize the time of database recovery and the amount of data loss due to failure.
 - **Transaction log restore** - Restores the Transaction log. Restoring a Transaction log is also referred to as *applying* a Transaction log. When you restore a Transaction log, the Microsoft SQL server re-executes the changes contained in the log and rolls back any transactions that were uncommitted when you backed up the Transaction log.

After you have restored a database, you can load the differential backup (if any) and the Transaction log backups you created after backing up that database. Loading Transaction logs lets you recover as much of a database as possible.

You must load backups of the Transaction log in the sequence in which they were created. The Microsoft SQL checks the timestamps on each backed up database and each backed up Transaction log to verify that the sequence is correct.

After the Microsoft SQL server has loaded the entire sequence of Transaction log backups, the database is restored to its state at the time of the last Transaction log backup, excluding any uncommitted transactions. The only uncommitted transaction that the Microsoft SQL server does not roll back is the Microsoft SQL Backup Log transaction, which is completed as part of the restore process.

- **File and FileGroup restore** - Restores files or FileGroups. You can restore files and FileGroups from either a file or FileGroup backup or from a full database backup. When restoring files or FileGroups, you must apply all of the differential file or FileGroup backup sessions, followed by all of the Transaction log backup sessions performed after the file or FileGroup backup. When you restore a file or FileGroup, you must apply the Transaction log to the database files immediately after the last file or FileGroup operation.

- **Partial restore** - A partial restore always restores the primary FileGroup and other files you specify and their corresponding FileGroups. The result is a subset of the database. FileGroups that are not restored are marked as offline and are not accessible.

Differential Backup Restores

A differential backup contains only the data that has changed since the last full backup. If you have performed multiple differential backups after a full backup, you need only the last differential backup and the last full backup to restore the database to its most recent state.

When you have selected a differential backup session to restore, the Automatic Selection option automatically selects the appropriate full-database backup session and the proper options. Automatic Selection ensures that the correct sessions are restored in your job. Although you can package the appropriate sessions manually, Automatic Selection can save time and prevent errors.

When you restore a differential backup, the database must not be in use. Any data in the specified database is replaced by the restored data. If you are not using Automatic Selection, the database must be in a Loading state from a Full Database restore.

Unlike Transaction log restores, differential restores restore your data only to the point in time when you created the differential backup, not to the exact point of failure.

Transaction Log Restores

When restoring from a Transaction log backup, you must apply the Transaction log backup to the appropriate full database, differential backup, or FileGroup backup. When restoring, you must restore your data in the following order:

- Restore the full database backup
- Restore the latest differential backup, if any
- Restore the Transaction log backups made since the full or differential backup

When you select a Transaction log backup to restore, the Automatic Selection option automatically selects the appropriate Transaction log backup, differential backup, and database backups, and the proper options. Automatic Selection ensures that the correct sessions are restored in your job. Although you can package the appropriate sessions manually, Automatic Selection can save time and prevent errors.

File and FileGroup Restores

You can restore individual files or FileGroups from either a file or FileGroup backup or from a full database backup. When using this option, you must apply the Transaction log to the database immediately after the last file or FileGroup restore operation. This allows the contents of the file to roll forward, making it consistent with the rest of the database.

When you have selected a file or FileGroup backup to restore and selected Automatic Selection, the Automatic Selection option automatically selects all of the Transaction log backups needed to run the restore successfully. Automatic Selection ensures that your job restores the correct sessions. Although you can package the appropriate sessions manually, Automatic Selection can save time and prevent errors.

When you have selected a file or FileGroup differential backup and Automatic Selection, the Automatic Selection option selects the file or FileGroup backup session on which the differential was based and all of the Transaction log backups needed to run the restore successfully.

Restore Options

The Agent for Microsoft SharePoint provides the following database restore options:

- Automatic Selection
- Restore Type
- Force Restore Over Existing Files
- Recovery Completion State
- Log Point in Time Restore
- Restore Database Files As
- Database Consistency Check (DBCC)
- Restricted User Access After Restore
- Keep Replication Settings
- SQL Agent Filter

Note: These restore options are available for restoring databases and are not applicable to restoring non-database components.

Automatic Selection Option

The Automatic Selection option automatically selects:

- Other sessions that must be restored with the session you are restoring for the restore job to be successful
- Appropriate options for the restore job

The Automatic Selection option is enabled by default for every database restore job. Using Automatic Selection saves you time and prevents errors in packaging restore jobs.

Restore Type Option

The Restore Type option lets you select the type of restore from the following choices:

- **Database option:** Use the Database option to restore complete databases, differential backups, and Transaction log backups.
- **Files or FileGroups option:** Use the Files or FileGroups option to restore file or FileGroup backups or files that belong to database backups, but not files that belong to log backups or differential backups. After you have selected the Files or FileGroups option, you must select the files you want to restore.
- **Partial Restore option:** Use the Partial Restore option to perform the following actions:
 - Restore part of a database to its original location
 - Restore part of a database to another location so you can copy damaged or missing data back to the original database

You can use this option with full database backup sessions only.

Requirements to Restore Files or FileGroups

After restoring a file or FileGroup, you must apply a Transaction log session to roll the contents of the file forward to make it consistent with the rest of the database. Therefore, each time you back up a file or FileGroup, you should perform a Transaction log backup immediately afterwards.

Microsoft SQL Server requires that you restore all FileGroups, in a single operation, for which you created indexes since their last backup. You must fulfill this requirement whether you are restoring from a FileGroup backup or from a full database backup. Microsoft SQL Server detects the FileGroup index and compiles a list of the FileGroups you must restore. If you do not fulfill this requirement, Microsoft SQL Server reports this information to you when the restore is run. See the Agent for Microsoft SharePoint Activity log for the complete results.

For more information about the requirements for restoring files and FileGroups, see the Microsoft SQL Server documentation.

Force Restore Option

The Force Restore Over Existing Files option lets Microsoft SQL Server overwrite files it does not recognize as part of the database it is restoring. Use this option only if you receive a message from Microsoft SQL Server prompting you to use the With Replace option.

Microsoft SQL Server supports this option for database restore and file or FileGroup restore operations.

Recovery Completion State Option

The Recovery Completion State option lets you specify the final state of a session restore using the following options:

- **Leave database operational. No additional transaction logs can be restored:** This option instructs the restore operation to roll back any uncommitted transactions. After the recovery process, the database is ready for use.

Note: If you use Automatic Selection, you do not have to choose any of the Recovery Completion State selections manually because BrightStor ARCserve Backup performs the selection of sessions and the necessary options automatically. If you do not choose Automatic Selection, you must follow Microsoft SQL Server rules regarding the restore flow. For more information, see Microsoft SQL Server documentation.
- **Leave database nonoperational, but able to restore additional transaction logs:** This option instructs the restore operation **not** to roll back any uncommitted transactions. You must choose either this option or the Leave database read-only option to apply another differential backup or Transaction log. Microsoft SQL Server requires that you use this option for all but the final session. You must also use this option for database restores with multiple Transaction log restores or when a restore requires multiple sessions (for example, a full database backup followed by a differential backup).

- **Leave database read-only and able to restore additional transaction logs:** This option prepares a standby (warm backup) server. A standby server is a second server that you can bring on line if the primary production server fails. It contains a copy of the databases on the primary server. For more information about standby servers, see Microsoft SQL Server documentation.

Log Point in Time Restore Option

The Log Point in Time Restore option restores a database to the state it was in at a date and time that you have specified. You should use Automatic Selection with this option.

Important! *You cannot use the Log Point in Time Restore option if the database you are recovering uses the Bulk-Logged recovery model.*

To find the correct log when you have selected the Log Point in Time Restore option, Microsoft SQL Server restores the record in each Transaction log backup containing the start and finish time of the backup. Microsoft SQL Server then searches this record for the time you have specified.

- If Microsoft SQL Server finds the specified time, it restores the log to the point in the record that contains the time you submitted. The agent then signals BrightStor ARCserve Backup to stop restoring and the database is fully recovered. If there are other logs with the same time, those logs are ignored and the subsequent sessions are skipped.
- If the specified time occurs after those contained in the log, Microsoft SQL Server restores the log and leaves the database in a restoring state, waiting for the next log restore operation.
- If the specified time occurs before those contained in the log, Microsoft SQL Server cannot restore the log.

The Log Point in Time Restore option has limitations. For example, if you choose the Force Restore Over Existing Files option rather than the Automatic Selection option, and you restore one or more logs belonging to the same database, but do not select the appropriate database, differential backup, and FileGroup sessions to be restored first, the job will be incomplete and the subsequent sessions for that database will be ignored.

The following options are available for Log Point in Time Restore:

- **Stop at time:** This option includes date and time fields in which you can enter a specific date and time. The option recovers the database to the specified date and time. This is the default option.
- **Stop before log mark:** This option includes date and time fields in which you can set a specific date and time mark. The option recovers the database to the specified mark but does not include the transaction that contains the mark. If you do not select the After Time option, recovery stops at the first mark with the specified name. If you select the After Time option, recovery stops at the first mark with the specified name exactly at or after the date and time.
- **Stop at log mark:** This option includes date and time fields in which you can set a specific date and time mark. The option recovers the database to the specified mark, including the transaction that contains the mark. If you do not select the After Time option, recovery stops at the first mark with the specified name. If you select the After Time option, recovery stops at the first mark with the specified name exactly at or after the date and time.
- **After Time:** This option includes date and time fields in which you can set a specific date and time mark. The recovery stops at the specified mark only when the timestamp for the log mark is later than the specified time. Use this option with the Stop at log mark or Stop before log mark option.

Restore Database Files As Option

Using the Restore Database Files As option, you can perform the following actions:

- View the list of files for the database and related information.
- Select the files to be restored in a file or FileGroup backup session or in a file or FileGroup or Partial Restore of a database backup session.
- Change the location or file name of files during a restore. Use the location change function only with complete database restores or when using Automatic Selection.

Database Consistency Check (DBCC) Options

When you enable the database consistency check option for a restore, it performs the following test:

- **DBCC CHECKDB:** Checks the allocation and structural integrity of all the objects in a specified database. By default, the CHECKDB performs a check for indexes that can increase the overall execution time.
Note: The system table indexes are checked regardless of whether you select this option.
- **DBCC CHECKCATALOG:** Checks for consistency in and between system tables in the specified database.

Restricted User Access After Restore Option

The Restricted User Access after Restore option restricts access to a newly restored database to members of the db_owner, dbcreator, or sysadmin roles. This option requires the Leave database operational, no additional transaction logs can be restored option.

Keep Replication Settings Option

The Keep Replication Settings option instructs the restore operation to preserve replication settings when restoring a published database to a server other than the one on which it was created. As a result, it prevents Microsoft SQL Server from resetting the replication settings when it restores a database or log backup on a warm standby server and recovers the database. Use the Keep Replication Settings option when setting up replication to work with log shipping.

You cannot select this option when restoring a backup with the Leave database non-operational, but able to restore additional transaction logs option. Use this option only with the Leave database operational, no additional transaction logs can be restored option.

SQL Agent Filter Option

You can use the SQL Agent Filter option in the Restore Manager to display backup sessions of a particular database belonging to a particular server name and a particular instance. This option is available when you are using the Restore by Session method.

To display backup sessions of a database belonging to a server name, follow these steps:

1. Open the Restore Manager and select Filter from the Restore menu.
2. In the Filter dialog, select the SQL Agent Filter tab.
3. Enter a machine name and a database name, or a machine name, instance name, and database name.
Note: If you have several databases with the same matching character set in the name, they all display.
4. Click OK.

Note: After you apply the Microsoft SQL filter settings, you can expand media items to view the results. If a media item was expanded already, you must collapse it and expand it again to see the results.

Restore Methods

Use the Restore Manager to perform restore operations for SharePoint data. The Agent for Microsoft SharePoint supports the following restore methods:

- **Restore by Session** - Displays a list of all media used in backups and the files contained in them. This method lets you select objects for restore jobs based on backup sessions.
- **Restore by Tree** - Lets you select objects for restore jobs based on the source machine from which the data was backed up. If you select this method, you cannot restore the entire contents of the server as a whole but must select all subordinate objects individually. Use this method when you do not know which media contains the data you need but you have a general idea of what you need to restore and which machine it came from. This is the default method for the Restore Manager.

Note: The Restore by Query method is not supported.

Restore Data

Use the Restore Manager to perform restore operations for SharePoint data. To restore SharePoint data, follow these steps:

1. In the Restore Manager, select the source data using the Restore by Session or Restore by Tree method.
Note: The Restore by Query method is not supported.
2. Select the restore destination.
3. Set any restore options.
4. Define your restore schedule.
5. Submit your restore job.

Restore Using the Restore by Tree Method

To restore databases and non-database data using the Restore by Tree method, follow these steps:

1. On the Restore Manager Source tab, select Restore by Tree from the drop-down list.
2. In the navigation tree, expand the Agent for Microsoft SharePoint node and select the node you want to restore.
3. (Optional) To use a backup other than the most recent one, click Version History. The Version History dialog opens.

Version History provides information on the media name attached to each backup session, its backup session number, backup method, and the date and time the backup was made. You can select the session to restore from the backup media using Version History.

4. If this is a database session, right-click the node you selected, and choose Backup Agent Options from the pop-up menu.

The Backup Agent Restore Options dialog appears. The dialog varies depending on the restore sessions selected.

Important! *The Automatic Selection option on the Backup Agent Restore Options dialog automatically selects the restore options appropriate for your backup.*

5. Select restore options using one of the following methods:
 - Click OK to allow the Automatic Selection option to select the appropriate restore options for the restore job. The Automatic Selection option is the default option for every restore job.
 - Manually select the options you want to use for this restore session, and click OK.
6. On the Source tab, ensure that the session you want to restore is selected.
7. On the Destination tab and select a destination using the appropriate method:
 - For SharePoint databases, select one of these destinations:
 - The original location - Select the Restore files to their original locations option.
 - The SQL instance - You can rename the database or change the storage location. Clear the Original Location check box, and select the destination.
 - An existing SharePoint database - When you chose to restore to an existing database, the content of the destination database is overwritten by the restored data. Clear the Restore files to their original locations option, select the destination server, and select the database to overwrite.
 - For SharePoint non-database data, select one of these destinations:
 - The original location - Select the Restore files to their original locations option.
 - An alternate Agent for Microsoft SharePoint location of the same type - When you select this destination, you must select a destination item of the same type to prevent the job from failing. For example, a backward-compatible document library can be restored only to another backward-compatible document library. Keep in mind that selecting this destination location causes your data to be overwritten.
8. Click Start.

The Session User Name and Password dialog opens.

9. Verify or change the user name or password for the Windows computer on which Microsoft SQL Server is loaded. To verify or change the user name or password, follow these steps:
 - a. On the Machine tab, select a session, and click Edit.

The Enter User Name and Password dialog opens.

 - b. Enter or modify the user name and password.
 - c. If a session password was assigned to this session, enter the session password.

- d. To apply the user name, password, and session password you entered to all the sessions you are restoring, select the **Apply [User Name and Password]** to all rows option.
 - e. Click **OK**.
10. Verify or change the user name or password for the database servers to which you are restoring. To verify or change the user name or password for the database servers, follow these steps:
 - a. On the **DBAgent** tab, select a session, and click **Edit**.
The **Enter User Name and Password** dialog opens.
 - b. Enter or modify the user name and password.
 - c. To apply the user name, password, and session password you entered to all the sessions you are restoring, select the **Apply [User Name and Password]** to all rows option.
 - d. Click **OK**.
11. Click **OK** on the **Session User Name and Password** dialog.
The **Submit Job** dialog opens.
12. (Optional) Use the **Submit Job** dialog to select the job execution time, submit the job on hold, add an optional description for the backup job, or select a source priority.
13. Click **OK** to submit this job.
If you selected **Run Now**, the **Job Status** window opens. Use this window to monitor your job. For more information about the **Job Status** window, see the *Administrator Guide*.

Restore Using the Restore by Session Method

To restore databases and non-database data using the **Restore by Session** method, follow these steps:

1. On the **Restore Manager** Source tab, select **Restore by Session** from the drop-down list.
A list of the media you have used when backing up with BrightStor ARCserve Backup opens.
2. Choose the media containing the backup you want to restore, and select the session containing the specific database or log you want to restore.
Note: You must perform a separate session restore for each database and non-database data component you want to restore.

If you are restoring a non-database data component, skip to Step 4.

3. (Optional) If you are restoring a database, perform the following procedures:
 - a. Right-click the session containing the database or log you want to restore, and choose Backup Agent Options from the pop-up menu.
The Backup Agent Restore Options dialog appears. This dialog varies depending on the restore sessions selected.
- b. Click OK to allow the Automatic Selection option to select the appropriate restore options for the restore job. Alternatively, manually select the options you want to use for this restore job, and click OK.
4. On the Source tab, verify that the session you want to restore is selected.
5. On the Destination tab, select a destination using the appropriate method:
 - For SharePoint databases, select one of these destinations:
 - The original location - Select the Restore files to their original locations option.
 - The SQL instance - You can rename the database or change the storage location. Clear the Original Location check box, and select the destination.
 - An existing SharePoint database - When you chose to restore to an existing database, the content of the destination database is overwritten by the restored data. Clear the Restore files to their original locations option, select the destination server, and select the database to overwrite.
 - For SharePoint non-database data, select one of these destinations:
 - The original location - Select the Restore files to their original locations option.
 - An alternate Agent for Microsoft SharePoint location of the same type - When you select this destination, you must select a destination item of the same type to prevent the job from failing. For example, a backward-compatible document library can be restored only to another backward-compatible document library. Keep in mind that selecting this destination location causes your data to be overwritten.
6. Click Start.

The Session User Name and Password dialog opens.

7. Verify or change the user name or password for the Windows computer on which Microsoft SQL Server is loaded. To verify or change the user name or password, follow these steps:
 - a. On the Machine tab, select a session, and click Edit.
The Enter User Name and Password dialog opens.
 - b. Enter or modify the user name and password.
 - c. If a session password was assigned to this session, enter the session password.
 - d. To apply the user name, password, and session password you entered to all the sessions you are restoring, select the Apply [User Name and Password] to all rows option.
 - e. Click OK.
8. Verify or change the user name or password for the database servers to which you are restoring. To verify or change the user name or password for the database servers, follow these steps:
 - a. On the DBAgent tab, select a session, and click Edit.
The Enter User Name and Password dialog opens.
 - b. Enter or modify the user name and password.
 - c. To apply the user name, password, and session password you entered to all the sessions you are restoring, select the Apply [User Name and Password] to all rows option.
 - d. Click OK.
9. Click OK on the Session User Name and Password dialog.
The Submit Job dialog opens.
10. (Optional) Use the Submit Job dialog to select the job execution time, submit the job on hold, add an optional description for the backup job, or select a source priority.
11. Click OK to submit this job.
If you selected Run Now, the Job Status window opens. Use this window to monitor your job. For more information about the Job Status window, see the *Administrator Guide*.

Restore to Alternate Disk Locations Using Automatic Selection

You can restore a database to a different location on a disk (for example, to a different drive letter or directory path, or with a different file name) while using Automatic Selection only if the Backup Agent Restore Options dialog displays file path entries for the data files.

To determine whether you can use Automatic Selection to restore a database or session to a different location, follow these steps:

1. Right-click the database, if you are using Restore by Tree, or the last backup session for this database, if you are using Restore by Session.
2. Choose Backup Agent Options from the pop-up menu. The Backup Agent Restore Options dialog opens.
3. If the FileGroups and data files appear in the section called Restore database files as, you can use Automatic Selection.

Restore to Alternate Disk Locations by Individual Session

If the FileGroups and data files are not displayed in the section called Restore database files as, you must restore the sessions individually to restore them to an alternative disk location. To restore sessions to an alternative disk location individually, use one of the following methods:

- Restore by Session using a single restore job
- Restore by Session using a separate job for each session
- Restore by Tree

For information on these restore methods, see the sections Restore by Session Using a Single Restore Job, Restore by Session Using a Separate Job for Each Session, and Restore Using the Restore by Tree in this chapter.

Restore by Session Using a Single Restore Job

To restore databases by session using a single restore job, follow these steps:

1. On the Restore Manager Source tab, select Restore by Session from the drop-down menu. A list of the media you have used when backing up with BrightStor ARCserve Backup opens.
2. Choose the media containing the backup you want to restore, expand the session containing that backup, and select the current backup session.
3. Right-click the backup session and select Backup Agent Options from the pop-up menu. The Backup Agent Restore Options dialog opens.

4. Clear the Automatic Selection check box and select the Leave database nonoperational, but able to restore additional transaction logs option under Recovery Completion State.
Note: No additional transaction logs can be restored if this option is not selected.
5. Click OK.
6. For each additional required backup of the database, select the next most recent session, open the Backup Agent Restore Options dialog, clear Automatic Selection, and select the Leave database nonoperational, but able to restore additional transaction logs option under Recovery Completion State. Click OK.
7. For the earliest of these backup sessions (the full backup on which the others depend), make the appropriate changes to the file paths and names.
Important! *Do not edit the file names or paths for any of the sessions except the full backup session.*
8. Complete the restore job packaging, and submit the restore job. For instructions on restoring by session, see the appropriate section in this guide.

Restore by Session Using a Separate Job for Each Session

If you restore databases using a separate job for each session, you can submit each job on hold and then make each job ready individually as the previous one finishes. To package the database restore job as separate jobs, follow these steps:

1. On the Restore Manager Source tab, select Restore by Session from the drop-down menu. A list of the media you have used when backing up with BrightStor ARCserve Backup opens.
2. Choose the media containing the backup you want to restore, expand the session containing that backup, and select the most recent full database backup of the database you want to restore. This is the full backup on which the more recent backup sessions depend.
3. Right-click the backup session and select Backup Agent Options from the pop-up menu. The Backup Agent Restore Options dialog opens.
4. Clear the Automatic Selection option and edit the file names or paths as appropriate.
5. Select the Leave database nonoperational, but able to restore additional transaction logs option under Recovery Completion State.
6. Click OK to close the Backup Agent Restore Options dialog and submit the restore job.
7. Select the next backup session for the database you want to restore.

8. Right-click the backup session and select Backup Agent Options from the pop-up menu. The Backup Agent Restore Options dialog opens.
9. Clear the Automatic Selection option.
10. If this is **not** the last session to be restored, select the Leave database nonoperational, but able to restore additional transaction logs option under Recovery Completion State.
If this **is** the last session to be restored, confirm that the Leave database operational. No additional transaction logs can be restored option is selected under Recovery Completion State.
11. Click OK to close the Backup Agent Restore Options dialog and submit the restore job. For instructions about restoring by session, see the appropriate section in this chapter.
12. Repeat the preceding steps from the point at which you close the Backup Agent Restore Options dialog and submit the restore job until all backup sessions have been submitted for the restore.

Note: You must clear your previous selections before selecting options for the next job.

Appendix A: Disaster Recovery

A typical disaster recovery scenario may require you to rebuild your machines and reinstall Windows and BrightStor ARCserve Backup before you reinstall the Agent for Microsoft SharePoint.

The Agent for Microsoft SharePoint protects user data only; it does not protect the software or configuration of the computer or computers on which the SharePoint installation is hosted. In a disaster recovery situation, you must recover these machines and ensure that the Agent for Microsoft SharePoint is running before you can restore the SharePoint data.

In a SharePoint installation, different servers can fulfill different roles:

- Front-end web server
- Search index server
- Backward-compatible document library server
- Database server

These roles can be assigned to different servers, or in the case of a single-server configuration, one computer. The role or roles performed by a server determine what is required to support disaster recovery.

Front-End Web Server Restore

Front-end web servers store customized data required for recovery of a SharePoint installation that is not protected by the Agent for Microsoft SharePoint. To allow full recovery in the event of a disaster, this information should be protected. The files and data that should be backed up include:

- IIS metabase
- SharePoint extended virtual server root directories
- Custom web part assemblies
- Custom SharePoint templates and configuration files
- Any add-on software used by the SharePoint sites

All of this information can be fully protected using the Client Agent for Windows. For more information about using this agent, see the *Client Agents Guide*.

Restore a Front-End Web Server

To restore a front-end web server, follow these steps:

1. Restore or rebuild the server.
2. Restore the IIS metabase and the other files listed above it on the tree.
3. Install the SharePoint Portal Server software.
4. Connect to the server farm configuration database, and add the new server to the topology as a web server.
5. If this server was the front-end web server that had the SharePoint Router Agent installed, use the BrightStor ARCserve Backup for Microsoft SharePoint Configuration wizard to install the SharePoint Router Agent.

If the server must be rebuilt, install the operating system, Windows SharePoint Services or SharePoint Portal 2003, and all SharePoint service packs before restoring these items. Then you can connect the server to the existing configuration database for the server farm and add the rebuilt server to the SharePoint server topology as a web server.

Restore a Search Index Server

To restore a search index server, follow these steps:

1. Remove the server from the server farm topology.
2. Restore or rebuild the server, and install the SharePoint Portal Server software and all SharePoint service packs.
3. Connect to the server farm configuration database, and add the new server to the topology as an index server.
4. Using the BrightStor ARCserve Backup for Microsoft SharePoint Configuration wizard, install the SharePoint External Data Agent.
5. Restore the SharePoint search index files to the new server.

Restore a Backward-Compatible Document Library Server

To restore a backward-compatible document library server, follow these steps:

1. Delete all the document libraries using SharePoint Portal Server Central Administration.
2. Remove the document library server from the server farm topology.

3. Restore or rebuild the server, and install the backward-compatible document library component.
4. Add the server to the SharePoint topology.
5. Create a new backward-compatible document library using the same backward-compatible document library name.
6. Use the BrightStor ARCserve Backup for Microsoft SharePoint Configuration wizard to install the SharePoint External Data Agent.
7. Restore the backward-compatible document library.

Restore the Database Server

To restore the Microsoft SQL Server 2000 server, follow these steps:

1. Restore or rebuild the server so that Microsoft SQL Server 2000 is configured in the same way as it was prior to the failure.
2. Use the SharePoint Central Administration tool to create a new configuration database.
3. Connect all the SharePoint machines to the new configuration database and set the SharePoint topology back to the state it was in before the failure.
4. Use the BrightStor ARCserve Backup for Microsoft SharePoint Configuration wizard to install the SharePoint SQL Agent on the recovered Server.
5. Perform one of the following two options:
 - Restore all the SharePoint databases, including the old configuration database.
 - Restore all of the SharePoint databases except for the configuration database.

Microsoft does not recommend the first option because the configuration database may become out-of-sync with the other SharePoint databases. However, if no sites or portals were being created or deleted when the backup was being performed, the restore should work correctly.

If you use the second option, after restoring the SharePoint databases you must restore the SharePoint portals and virtual servers using the **procedures described in the Microsoft SharePoint Portal Server 2003 Administrator's Guide and the Microsoft Windows SharePoint Services 2.0 Administrator's Guide**.

Restore a Single-Server Installation Using MSDE

The procedure for a single-server installation using MSDE is slightly different if you cannot restore the machine so that MSDE is running correctly. In this situation, follow these steps:

1. Restore or rebuild the server.
2. Reinstall SharePoint Portal 2003 or Windows SharePoint Services and all SharePoint service packs to recreate the MSDE installation and create the configuration database.
3. Use the BrightStor ARCServe Backup for Microsoft SharePoint Configuration wizard to install the required Agent for Microsoft SharePoint components.
4. Restore all the SharePoint databases except the configuration database.

Use the procedures described in the *Microsoft SharePoint Portal Server 2003 Administrator's Guide* or the *Microsoft Windows SharePoint Services 2.0 Administrator's Guide* to recreate the SharePoint Portal or Windows SharePoint Services sites.

Note: As previously mentioned, if you know that the configuration of SharePoint was stable when the backup was performed, it may be possible to recover the configuration database. However, this option is not supported by Microsoft.

Appendix B: Configuring Microsoft SQL Server Security Settings

This appendix explains how to configure Microsoft SQL Server security settings for BrightStor ARCserve Backup.

Types of Microsoft SQL Authentication

Microsoft SQL Server provides two types of user authentication:

- Apply the Windows login identification
- Use separate user credentials specific to Microsoft SQL Server

Although Microsoft recommends using only Windows authentication wherever possible, in certain instances it is appropriate, or even necessary, to enable Microsoft SQL Server-based authentication. For example, you must use Microsoft SQL Server authentication for Microsoft SQL Server 2000 when the database is running in a cluster.

Authentication Requirements

For Microsoft SQL Server authentication, you must specify a user account with system administrator access privileges. By default, Microsoft SQL Server creates an account with this level of access, called **sa**, but the Agent for Microsoft SharePoint can use any account with equivalent privileges.

For Windows authentication, any account with administrator equivalency for the machine on which the database is running typically has system administrator access privileges for the database.

Note: A Windows or domain administrator does not automatically have system administrator access privileges for the database if the BUILTIN\Administrators login entry in Microsoft SQL Server has been removed or does not have this role, or if a separate login entry for this user in Microsoft SQL Server does not have this role.

How User Authentication Is Changed

Regardless of the authentication option you choose, you must configure both Windows and BrightStor ARCserve Backup. In addition, if you change the option, you must update settings so that both Windows and BrightStor ARCserve Backup reflect the change. If you are using Microsoft SQL Server 2000, you must make the change separately for each instance of the server.

To change user authentication and update the settings for both Windows and BrightStor ARCserve Backup so that this change is reflected, you must check and change the Microsoft SQL Server authentication method. See the following section for more information regarding this process.

Check or Change the Microsoft SQL Server Authentication Method

To check or change the Microsoft SQL Server authentication method, follow these steps:

1. On the system where Microsoft SQL Server is running, open the SQL Server Enterprise Manager.
2. In the Tree pane, expand the entries below Console Root until you reach the database server.
3. Right-click the server name, and select Properties from the drop-down menu. The Properties dialog opens.
4. In the Properties dialog, click the Security tab.
5. Under Authentication, select either Microsoft SQL Server and Windows, to enable Microsoft SQL server-based authentication, or Windows Only, to enable only Windows user names and passwords.
6. Click OK.

Index

A

agent

- architecture • 9
- configuration • 14
- install • 13
- uninstall • 17

B

backup

- differential • 22
- file and filegroups • 23
- overview • 19
- perform • 26
- supported backup types • 20
- transaction log • 24

C

configuration

- configuration wizard • 9, 13, 14, 15, 17

D

disaster recovery

E

External Data Agent

I

installation

- considerations • 13
- install the agent • 13
- prerequisites • 13
- uninstall the agent • 17

N

non-database data, defined

R

restore

- by session using a separate job for each session • 51
- by session using a single restore job • 50
- differential backup • 37
- methods • 44

operations

- options • 38
- overview • 33
- perform • 45
- transaction log • 37
- types • 36
- Router Agent • 10
- uninstall • 17

S

server roles

- SharePoint Database Agent • 11
- SPImages Directory, uninstall • 17
- subagents • 9
 - External Data Agent • 11
 - Router Agent • 10
 - SharePoint Database Agent • 11

U

uninstall