

CA ARCserve® Backup for Windows

Agent for Microsoft SharePoint Guide

r12.5



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

This Documentation may not be copied, transferred, reproduced, disclosed, modified or duplicated, in whole or in part, without the prior written consent of CA. This Documentation is confidential and 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 the Documentation for their own internal use, and may make one copy of the related software as reasonably required for back-up and disaster recovery purposes, 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 provisions of the license for the Product are permitted to have access to such copies.

The right to print copies of the Documentation and to make a copy of the related software is limited to the period during which the applicable 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 certify in writing to CA that all copies and partial copies of the Documentation have been returned to CA or destroyed.

EXCEPT AS OTHERWISE STATED IN THE APPLICABLE LICENSE AGREEMENT, 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 the Documentation is governed by the end user's applicable license agreement.

The manufacturer of this Documentation is CA.

Provided with "Restricted Rights." Use, duplication or disclosure by the United States Government is subject to the restrictions set forth in FAR Sections 12.212, 52.227-14, and 52.227-19(c)(1) - (2) and DFARS Section 252.227-7014(b)(3), as applicable, or their successors.

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

Copyright © 2009 CA. All rights reserved.

CA Product References

This documentation set references the following CA products:

- BrightStor® ARCserve® Backup for Laptops and Desktops
- BrightStor® CA-Dynam®/TLMS Tape Management
- BrightStor® CA-Vtape™ Virtual Tape System
- BrightStor® Enterprise Backup
- BrightStor® High Availability
- BrightStor® Storage Resource Manager
- CA Antivirus
- CA ARCserve® Backup Agent for Advantage™ Ingres®
- CA ARCserve® Backup Agent for Novell Open Enterprise Server for Linux
- CA ARCserve® Backup Agent for Open Files on NetWare
- CA ARCserve® Backup Agent for Open Files on Windows
- CA ARCserve® Backup Client Agent for FreeBSD
- CA ARCserve® Backup Client Agent for Linux
- CA ARCserve® Backup Client Agent for Mainframe Linux
- CA ARCserve® Backup Client Agent for NetWare
- CA ARCserve® Backup Client Agent for UNIX
- CA ARCserve® Backup Client Agent for Windows
- CA ARCserve® Backup Enterprise Option for AS/400
- CA ARCserve® Backup Enterprise Option for Open VMS
- CA ARCserve® Backup for Microsoft Windows Essential Business Server
- CA ARCserve® Backup for Windows
- CA ARCserve® Backup for Windows Agent for IBM Informix
- CA ARCserve® Backup for Windows Agent for Lotus Domino
- CA ARCserve® Backup for Windows Agent for Microsoft Exchange
- CA ARCserve® Backup for Windows Agent for Microsoft SharePoint
- CA ARCserve® Backup for Windows Agent for Microsoft SQL Server
- CA ARCserve® Backup for Windows Agent for Oracle
- CA ARCserve® Backup for Windows Agent for Sybase
- CA ARCserve® Backup for Windows Agent for Virtual Machines

- CA ARCserve® Backup for Windows Disaster Recovery Option
- CA ARCserve® Backup for Windows Disk to Disk to Tape Option
- CA ARCserve® Backup for Windows Enterprise Module
- CA ARCserve® Backup for Windows Enterprise Option for IBM 3494
- CA ARCserve® Backup for Windows Enterprise Option for SAP R/3 for Oracle
- CA ARCserve® Backup for Windows Enterprise Option for StorageTek ACSLS
- CA ARCserve® Backup for Windows Image Option
- CA ARCserve® Backup for Windows Microsoft Volume Shadow Copy Service
- CA ARCserve® Backup for Windows NDMP NAS Option
- CA ARCserve® Backup for Windows Serverless Backup Option
- CA ARCserve® Backup for Windows Storage Area Network (SAN) Option
- CA ARCserve® Backup for Windows Tape Library Option
- CA Dynam®/B Backup for z/VM
- CA VM: Tape for z/VM
- CA XOssoft™ Assured Recovery™
- CA XOssoft™
- CA 1® Tape Management
- Common Services™
- eTrust® Firewall
- Unicenter® Network and Systems Management
- Unicenter® Software Delivery
- Unicenter® VM: Operator®

Contact CA

Contact Technical Support

For your convenience, CA provides one site where you can access the information you need for your Home Office, Small Business, and Enterprise CA products. At <http://ca.com/support>, you can access the following:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Provide Feedback

If you have comments or questions about CA product documentation, you can send a message to techpubs@ca.com.

If you would like to provide feedback about CA product documentation, complete our short [customer survey](#), which is also available on the CA support website, found at <http://ca.com/support>.

Contents

Chapter 1: Introducing the Agent	11
Introduction	11
Agent Features	11
SharePoint Server 2007 Features	12
SharePoint Portal Server 2003 Features	12
Supported SharePoint Data	13
How the Agent Works on SharePoint Server 2007 Systems	14
Consolidated View	14
How the Agent Works on SharePoint Server 2003 Systems	15
SharePoint Router Agent	17
SharePoint External Data Agent	17
SharePoint Database Agent	17
Server Roles	18
Consolidated View	18
Chapter 2: Installing the Agent	21
Environmental Considerations	21
Installation Considerations for SharePoint Server 2007	22
Installation Prerequisites	23
Configure the Agent on SharePoint 2007 Systems	24
Install the Agent	26
Uninstall the Agent on SharePoint 2007 Systems	26
Installation Considerations for SharePoint Server 2003	26
Installation Prerequisites	28
Configure the Agent on SharePoint 2003 Systems	29
Install Subagents	31
Uninstall the Agent on SharePoint 2003 Systems	32
Chapter 3: Backing Up SharePoint 2007 Systems	33
Backup Overview	33
Database-Level Backup Prerequisites	33
How to Perform a Full Backup	34
Backup Considerations	34
Database-Level Agent Backup Option Dialog	35
Default Backup Dump Location	35
Backup Dump Path	36

Backup Methods	36
Perform a Database-Level Backup	37

Chapter 4: Backing Up SharePoint 2003 Systems **39**

Backup Overview	39
Backup Operations	39
Backup Types	40
Backup Strategy Recommendations	41
Required Full Backup	42
Differential Backups	43
File and FileGroup Backups	44
Transaction Log Backups	44
Database Consistency Checks	46
Backup Considerations	48
Rotation Schemes and Global Options	49
Back Up Data	50
Back Up Databases	51
Dynamic and Explicit Job Packaging	53
Dynamic Job Packaging	53
Mark an Object for Dynamic Job Packaging	53
Explicit Job Packaging	54
Mark an Object for Explicit Job Packaging	55

Chapter 5: Restoring SharePoint 2007 Systems **57**

Restore Overview	57
Database-Level Restore Sets	57
Database-Level Restore Option Dialog	58
Default Restore Dump Location	58
Restore Dump Path	59
Restore Configuration Settings	59
Database-Level Restore Prerequisites	60
Perform a Database-Level Data Restore	62

Chapter 6: Restoring SharePoint 2003 Systems **65**

Restore Overview	65
Restore Operations	66
Database Restores	66
Nondatabase Data Restores	68
Restore Types	68
Complete Database Restore	69
Differential Backup Restores	69

Transaction Log Restores	69
File and FileGroup Restores	70
Partial Restore	70
Restore Options	70
Automatic Selection Option	71
Restore Type Option	71
Force Restore Option	72
Recovery Completion State Option	73
Log Point in Time Restore Option	73
Restore Database Files As Option	75
Database Consistency Check (DBCC) Options	75
Restricted User Access After Restore Option	76
Keep Replication Settings Option	76
Restore Methods	76
Restore Data	77
Restore Data Using the Restore by Tree Method	77
Restore Data Using the Restore by Session Method	80
Restore Data to Alternate Disk Locations Using Automatic Selection	82
Restore to Alternate Disk Locations by Individual Session	83
Restore Database to Alternate Microsoft SQL Systems	85

Chapter 7: Using Best Practices **87**

How to Select the Proper Location	87
Set Access Permission on Dump Location	88

Appendix A: Disaster Recovery **89**

How the Agent Supports Disaster Recovery on SharePoint 2003 Systems	89
Restore a Front-End Web Server	90
Restore a Backward-Compatible Document Library Server	90
Restore a Search Index Server	91
Restore a Database Server	92
Restore a Single-Server Installation Using MSDE	92
How to Perform a Database-Level Disaster Recovery on SharePoint 2007 Systems	93

Appendix B: Configuring Microsoft SQL Server Security Settings **95**

Types of Microsoft SQL Authentication	95
Authentication Requirements	95
How User Authentication Is Changed	96
Check or Change the Microsoft SQL Server Authentication Method	96

Appendix C: Troubleshooting	99
Index	101

Chapter 1: Introducing the Agent

This section contains the following topics:

[Introduction](#) (see page 11)

[Agent Features](#) (see page 11)

[Supported SharePoint Data](#) (see page 13)

[How the Agent Works on SharePoint Server 2007 Systems](#) (see page 14)

[How the Agent Works on SharePoint Server 2003 Systems](#) (see page 15)

Introduction

CA 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 CA ARCserve Backup offers is the CA ARCserve Backup Agent for Microsoft SharePoint 2007 and CA ARCserve Backup Agent for Microsoft SharePoint 2003. These agents let you back up and restore Microsoft Office SharePoint Server 2007, Microsoft Office SharePoint Portal Server 2003, and Microsoft Windows SharePoint Services 3.0 and 2.0 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 CA ARCserve Backup server. SharePoint content consists of distributed SharePoint databases, Single Sign-On (SSO), and search indexes. The agent lets you use the features of CA ARCserve Backup to easily manage the backup and restore of all SharePoint data on your network.

Agent Features

The Agent for Microsoft SharePoint offers a number of features to facilitate your backup and restore operations. It provides backup and restore capabilities for Microsoft Office SharePoint Server 2007, Microsoft Office SharePoint Portal Server 2003, and Microsoft Windows SharePoint Services 3.0 and 2.0 installations.

SharePoint Server 2007 Features

The agent supports the following features for SharePoint Server 2007:

- Backup and restore of the following SharePoint Server 2007 Farm and Farm components:
 - Web Application
 - SharePoint Services Provider with associated search indexes
 - Single Sign-On (SSO) databases
 - Windows SharePoint Services Help Search
 - Global Search settings
- Enables SharePoint data to be restored to its original location or to an alternate destination.
- Supports backup to a wide array of storage devices.

SharePoint Portal Server 2003 Features

The agent supports the following features for SharePoint Server 2003:

- Supports backup and restore functionality for Microsoft SQL databases, Microsoft SQL Server 2000 Desktop Engine (MSDE), and Microsoft SQL Server 2000 Desktop Engine Windows (WMSDE).
- Provides protection to search indexes and Single Sign-On for SharePoint Portal Server 2003 installations.
- Supports database complete, database differential, Files/File Groups differential, and Transaction log backups for SharePoint databases.
Note: Only Database Complete backups are supported for nondatabase 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 Server 2007
 - SharePoint server farm
 - Web Applications
 - Web Application content database
 - Single Sign-On database
 - Windows SharePoint Services Help Search
 - Shared Services Provider
 - Shared Services Provider content database
 - Global Search Settings
- Microsoft Office SharePoint Portal Server 2003
 - SharePoint Portal 2003 databases
 - Single Sign-On database
 - Search indexes
 - Backward-compatible document libraries
 - Windows SharePoint Services 2.0 databases

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.

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 CA ARCserve Backup Client Agent for Windows. For more information about using this agent, see the *Client Agents Guide*.

How the Agent Works on SharePoint Server 2007 Systems

CA ARCserve Backup and the Agent for Microsoft SharePoint work together to back up and restore SharePoint 2007 data. When CA ARCserve Backup backs up data, the server connects to the agent and sends a request. The agent retrieves the data from the SharePoint Server 2007 and exports the data to a shared folder on the disk and then sends it to CA 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 CA ARCserve Backup to the server.

Consolidated View

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

The following SharePoint data appears under the Farm object of the Agent for Microsoft SharePoint 2007 object:

- One SharePoint configuration database
- Windows SharePoint Services Web Application
- WSS Administration
- Shared Services Providers
- Global Search Settings
- Windows SharePoint Services Help Search
- Single Sign-On (SSO) database

Note: If you have not configured SSO, it does not appear in the tree.

You can expand the following SharePoint items to display all instances on the SharePoint server farm:

Windows SharePoint Services Web Application

Shows web applications and their content databases.

WSS Administration

Shows Farm administration web Application and its content databases.

Shared Services Providers

Shows several SSP components like SSP administration web applications, SSP databases, User Profile Application, Session State, SSP Search index files.

Windows SharePoint Services Help Search

Shows Windows SharePoint Services Search Instance.

How the Agent Works on SharePoint Server 2003 Systems

CA ARCserve Backup and the Agent for Microsoft SharePoint work together to back up and restore SharePoint 2003 data. When CA ARCserve Backup backs up data, it sends a request to the agent. The agent retrieves the data from the server and sends it to CA 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 CA 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](#) (see page 17).
- [SharePoint External Data Agent](#) (see page 17).
- [SharePoint Database Agent](#) (see page 17).

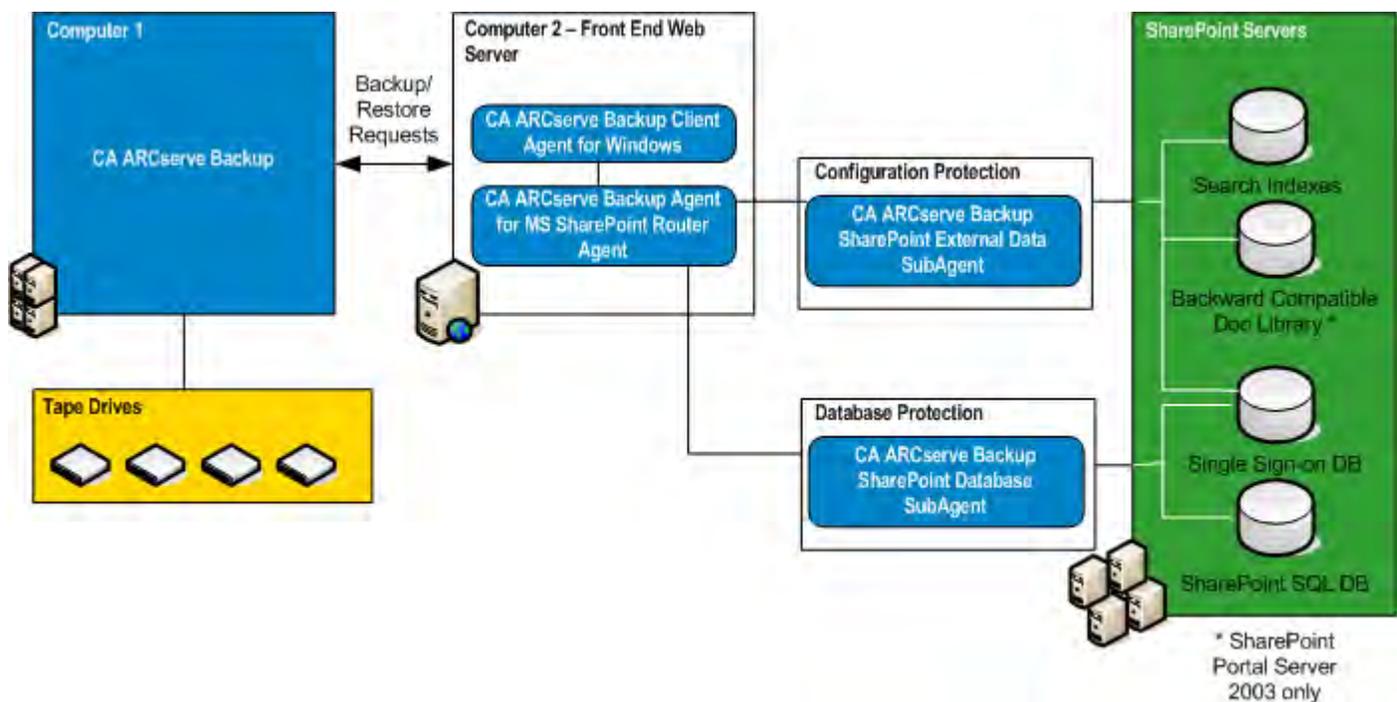
By providing a consolidated view of the SharePoint data, these subagents work together as a unit to protect SharePoint data that is distributed across multiple servers.

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 CA ARCserve Backup for Microsoft SharePoint Configuration wizard component on a CA 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 backing up and restoring of 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 and also protects SharePoint Portal Server 2003, 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 2000 or 2005
- Microsoft SQL 2005 Express
- Microsoft SQL Server 2000 Desktop Engine Windows (WMSDE 2000 or MSDE)

The SharePoint Database Agent is similar to the CA 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.

Note: If the Agent for Microsoft SQL Server and the database component of the Agent for Microsoft SharePoint are both deployed on the same machine, the SharePoint databases are included in any whole-instance backups performed by the Agent for Microsoft SQL Server.

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 (SharePoint Portal Server 2003 only)

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

Note: If the single sign-on service is started on the job server of a SharePoint 2003 distributed Farm, the SSO encryption key will be displayed as inaccessible in the CA ARCserve Backup base browser. This does not occur in a Standalone farm of SharePoint 2003.

- Shared Services Provider (Microsoft Office SharePoint Server 2007 only)
- Windows SharePoint Services content databases

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

You can expand the following SharePoint items to display all instances on the SharePoint server farm:

SharePoint portals

Shows the databases.

Search indexes

Shows the Index servers.

Single Sign-On

Shows 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 on SharePoint 2007 and SharePoint 2003 systems. The information in this section assumes you are familiar with the characteristics and requirements of your Microsoft SharePoint server farm.

Note: You cannot install the Agent for Microsoft SharePoint for SharePoint 2007 and the Agent for Microsoft SharePoint 2003 on the same machine.

This section contains the following topics:

[Environmental Considerations](#) (see page 21)

[Installation Considerations for SharePoint Server 2007](#) (see page 22)

[Install the Agent](#) (see page 26)

[Uninstall the Agent on SharePoint 2007 Systems](#) (see page 26)

[Installation Considerations for SharePoint Server 2003](#) (see page 26)

[Uninstall the Agent on SharePoint 2003 Systems](#) (see page 32)

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 CA 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 (SharePoint Portal Server 2003 only).

Installation Considerations for SharePoint Server 2007

Consider the following when you install the agent:

- Microsoft Office SharePoint Server 2007 or Microsoft Windows Shared Service 3.0 must be installed before you install the Agent for Microsoft SharePoint 2007. The agent is supported on all operating systems on which Microsoft Office SharePoint Server 2007 is supported.
- The CA 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 CA ARCserve Backup server.
- You must run the Microsoft SQL Server Windows service as a domain account or a local system account.
- If you are running Microsoft SharePoint 2007 on a Windows Server 2008 system, you must install the Agent for Microsoft SharePoint on the same machine on which central administration is running or your search index backups will fail.
- Jobs may not complete successfully when the CA ARCserve Backup server and the agent server reside in different time zones. To ensure that jobs complete successfully, you must synchronize the time zone on the agent server with the CA ARCserve Backup server.
- There is a known Microsoft issue that could lead to SharePoint 2007 behaving differently depending on how you deployed Windows SharePoint Services 3.0 and Microsoft Office SharePoint Server 2007 on Windows Server 2008 systems.
 - If you upgrade Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007 with Service Pack 1, you must install the CA ARCserve Backup Agent for SharePoint on machines on which the Central Administration Service is running. Before you submit a backup or restore job, you must ensure this service is running on the target machine or the jobs may fail.
 - If you install Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007 including Service Pack 1, you can install the CA ARCserve Backup Agent for SharePoint on any machine on which the Central Administration Service is running. It is not a prerequisite to have Central Administration Service running on the target machine for backup and restore jobs in this situation.

- If you choose Server Farm Installation when upgrading the CA ARCserve Backup Agent for Microsoft SharePoint 2007 from r12 or r12.1 to this release, you must use the same Farm Administrator used to create the Farm, or you will need to launch the SharePoint 2007 Agent configuration and repeat configuration. This restriction affects Server Farm Installations (Complete and Web Front End) only. It does not affect SharePoint Single Server (standalone) installations.

Installation Prerequisites

Before installing the Agent on SharePoint 2007 systems, 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.
- The user name entered in the Agent for Microsoft SharePoint Configuration Wizard must have administrative access to all machines in the SharePoint Server farm.
- Ensure that you are aware of the account which belongs to the Microsoft SharePoint 2007 farm administrator group.
- Verify that you have installed Microsoft Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007.
- If you are running Windows Server 2008, you must install the Agent for Microsoft SharePoint on the same system on which central administration is running or jobs will fail.

Configure the Agent on SharePoint 2007 Systems

After you have installed the Agent for Microsoft SharePoint on the CA ARCserve Backup server, SharePoint 2007 agent installs SPSO12, an agent COM+ component into the system. This component interacts with SharePoint 2007 to backup and restore the data.

Important! When configuring the Agent for SharePoint 2007, make sure the Pagefile usage size does not exceed the physical memory, or configuration will fail.

To configure the Agent on SharePoint 2007 systems

1. From the Windows Start menu, select All Programs, CA, ARCserve Backup, and Backup Agent Admin.

The CA ARCserve Backup Agent Admin dialog opens.

2. From the drop-down list, select CA ARCserve Backup Agent for Microsoft SharePoint 2007 and click Configuration.

The Configuration dialog opens.

3. Select one of the following options as the default backup dump location under Default Backup / Restore Dump Location:

Note: The same location will be used when you restore a backup job.

Use agent default configuration setting

Enabled by default. This option makes use of the backup dump location that you selected while configuring the agent.

CA ARCserve Server

Exports SharePoint 2007 data to a shared folder on the ARCserve server before it is saved to a tape.

CA ARCserve SharePoint Agent (Local Machine)

Exports SharePoint 2007 data to a shared folder on a local computer where the Agent is installed. The data is then saved on a tape through the network.

Other (NAS, File) Server Name

Exports SharePoint 2007 data to a NAS device or a public shared folder. You need to specify the server name, if you select this option.

Note: You must specify the host name instead of an IP address.

- Specify the Share name and Physical Path under the Backup / Restore Dump Path as follows:

Share Name

Specifies the shared folder where the data must be backed up, if you selected the Other (NAS, File) Server Name as the backup/restore dump location. You must grant the necessary permissions to the folder.

Note: The name should not contain the special character '\$' at the end.

Physical Path

Specifies the path where you want the data to be backed up, if you select the CA ARCserve Server or CA ARCserve SharePoint Agent as the backup or restore dump location.

- Select one of the following options as the backup method under Backup Methods:

Use Global or Rotation setting

Enabled by default. If you do not disable this, you must select a backup method on the Schedule tab.

Full

Backs up the entire database and marks all of the files that have been backed up in preparation for a subsequent incremental or differential backup.

Note: Always perform a full backup when running the agent for the first time, after upgrading to a Service Pack, and after performing a restore.

Differential

Backs up the files that have changed since the last backup.

Note: The Backup Method options on the Schedule tab do not apply if you select the Full or Differential backup methods. SharePoint 2007 does not support the Incremental Backup method. If you select Incremental Backup on the Schedule tab, it will still consider it as a Differential Backup.

- Click OK.

The Agent for SharePoint Server 2007 is configured.

Install the Agent

The Agent for Microsoft SharePoint 2007 and Agent for Microsoft SharePoint 2003 follows the standard installation procedure for the system components, agents, and options of CA ARCserve Backup.

For detailed procedures about installing CA ARCserve Backup, see the Implementation Guide.

Note: After you complete the installation procedure, be sure to restart your computer, if prompted.

Uninstall the Agent on SharePoint 2007 Systems

To uninstall the Agent for Microsoft SharePoint on SharePoint 2007 systems, select Add or Remove Programs in Windows and select CA ARCserve Backup Agent for Microsoft SharePoint.

Installation Considerations for SharePoint Server 2003

Consider the following when you install the agent and subagents:

- You must install the CA ARCserve Backup for Microsoft SharePoint Configuration wizard on the CA ARCserve Backup server.
- The CA 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 CA ARCserve Backup server.

- During the installation process, 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. CA ARCserve Backup must be installed before you install the Agent for Microsoft SharePoint Configuration Wizard. The Configuration Wizard is supported on all operating systems on which CA ARCserve Backup is supported.

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

- Jobs may not complete successfully when the CA ARCserve Backup server and the agent server reside in different time zones. To ensure that jobs complete successfully, you must synchronize the time zone on the agent server with the CA ARCserve Backup server.
- When upgrading from a prior release to this release of CA ARCserve Backup, use the Agent for Microsoft SharePoint Configuration Wizard to upgrade all CA ARCserve Backup SharePoint agents, including the Router Agent, External Data Agent, and Embedded SQL Agent. Uninstall all previous agents first, then install the Agent for Microsoft SharePoint.
- If the Agent for Microsoft SQL Server and the database component of the Agent for Microsoft SharePoint are both deployed on the same machine, the SharePoint databases are included in whole-instance backups performed by the Agent for Microsoft SQL Server. This issue also applies to the Agent for Microsoft SQL Server.
- To install and configure the Agent for Microsoft SharePoint in an environment with a firewall provided by Windows Server 2003 Service Pack 1 enabled, you must perform the following procedure:

Note: This procedure refers only to ports for the Agent for Microsoft SharePoint. You may have to open other ports to allow Microsoft SharePoint Portal to work properly. Verify that the Microsoft SharePoint Portal is working correctly before performing the following procedure.

1. Ensure that the firewalls on any remote computers hosting the SharePoint installation are configured to allow exceptions.
2. Install the Agent for Microsoft SharePoint from the CA ARCserve Backup installation media. The Agent for Microsoft SharePoint Configuration wizard starts automatically.
3. Complete the Server Selection information and click Next. Although the SharePoint Router Agent is installed, you may receive the following error message, indicating that the firewall is blocking access to the SharePoint Router Agent:

The router was not found on the selected machine. Check that the router is running.

4. Add the UnivAgent.exe executable to the Windows Firewall exception list on the machine on which the SharePoint Router Agent has been installed. This executable is found in the following directory:

c:\Program Files\CA\SharedComponents\ARCserve Backup\UniAgent

5. In the wizard, clear the Install router onto machine checkbox and click Next. The wizard obtains the SharePoint topology information, allowing you to proceed with either an Automatic or Custom installation type. Proceed to the Install screen of the wizard and click Next to install the required agents.
6. A list of computers and the agents installed on them appears. Before you can use the Agent for Microsoft SharePoint, these agents must be added to the Windows Firewall exception list on those machines.
7. If you have the CA ARCserve Backup External Data Agent installed on any computers, add the UnivAgent.exe executable to the Windows exception list. This executable is found in the following directory:
c:\Program Files\CA\SharedComponents\ARCserve Backup\UniAgent
8. If you have the Agent for Microsoft SQL Server installed on any computers, add the following to the Windows Firewall exception list:
 - Select File and Printer Sharing and choose TCP 139
 - dbasvr.exe, found in the following directory:
c:\Program Files\CA\SharedComponents\ARCserve Backup\DBACommon

The Agent for Microsoft SharePoint can now be used successfully from the CA ARCserve Backup server.

Installation Prerequisites

Before installing the Agent for Microsoft SharePoint on SharePoint 2003 systems, 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.
- Note that performance may be slow when backing up or restoring search indexes, as such operations can consume 100% of your CPU resources if the SharePoint server used satisfies only minimum hardware requirements. See the Microsoft documentation for more information hardware requirements.
- Ensure that you have administrator privileges or the proper authority to install software on the computers where you will be installing the product.
- The user name entered in the Agent for Microsoft SharePoint Configuration Wizard must have administrative access to all machines in the SharePoint Server farm.

- Ensure that you are aware of the account which belongs to the Microsoft SharePoint 2007 farm administrator group.
- Verify that you have installed Microsoft Windows SharePoint Services 3.0 or Microsoft Office SharePoint Server 2007.
- If you are running Windows Server 2008, you must install the Agent for Microsoft SharePoint on the same system on which central administration is running or jobs will fail.

Configure the Agent on SharePoint 2003 Systems

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

To configure the agent on SharePoint 2003 systems

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.

Note: 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.

The Configuration Types dialog opens.

3. Select one of the following configuration types:

Automatic

Automatically generates the necessary information to configure the installation of the agents required to protect the current SharePoint configuration.

Custom

Lets you 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 lets you to uninstall agents from your machines.

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 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 lets you track the installation of the components installed throughout the process. When the installation is complete, a summary dialog appears where you can 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.

Install Subagents

If you want to install other subagents instead of the SharePoint Router, use the Configuration wizard.

To install the subagents

1. Start the Configuration wizard. The following screen appears:

The screenshot shows a dialog box titled "CA ARCserve Backup Agent for Microsoft SharePoint Configuration". The main window is titled "Server Selection" and contains the following text: "This is a previously installed CA Router or a server on which you wish to install the CA Router." On the left, there is a "Page:" list with the following items: Welcome, Server Selection (highlighted), Configuration, Search Index, Document Library, Single Sign On, Portal DB, and Install. On the right, there is a "Router selection/install" section with the following fields: "Domain:" with the value "domain"; "Router:" with a dropdown menu showing "SPSWebServer"; "User name:" with the value "user"; "Password:" with a masked field (XXXXXXXXXXXXXXXXXX); an unchecked checkbox labeled "Install router onto machine"; and "Install path:" with an empty text box. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

2. On the Server Selection dialog, clear the Install router onto machine check box.

Click Next.

The other subagents will be installed. The subagents will have the same SharePointVersion value as that of the SharePoint Router.

Note: If you want to switch from one version to another, you may also need to install SharePoint External Data Agent or External SQL agents on some nodes where those agents were never installed. In this scenario, you must first manually change the SharePointVersion for the SharePoint Router and then run the Configuration wizard to install the SharePoint External Data Agent or External SQL agent.

Uninstall the Agent on SharePoint 2003 Systems

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

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

The simplest way to uninstall subagents (except 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 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 CA ARCserve Backup server. To remove these items, use Add or Remove Programs in Windows and select CA ARCserve Backup Agent for Microsoft SharePoint Admin GUI.

Important! You cannot uninstall Microsoft SharePoint Portal Server 2003 while the agent on SharePoint 2003 is still running. You must stop the agent or uninstall it before you can uninstall Microsoft SharePoint Portal Server 2003.

Chapter 3: Backing Up SharePoint 2007 Systems

This chapter provides information for backing up data on SharePoint 2007 systems.

This section contains the following topics:

[Backup Overview](#) (see page 33)

[Database-Level Backup Prerequisites](#) (see page 33)

[How to Perform a Full Backup](#) (see page 34)

[Backup Considerations](#) (see page 34)

[Database-Level Agent Backup Option Dialog](#) (see page 35)

[Perform a Database-Level Backup](#) (see page 37)

Backup Overview

Database-level backup protects the SharePoint Server 2007 database files. It is the fundamental backup for your SharePoint Server, and you should always use it if you use one of the other granular backup types. You can use database-level backups to restore SharePoint Server in the event of a system failure, database corruption, or a disaster recovery scenario.

Database-Level Backup Prerequisites

Before performing a database-level backup on SharePoint Server 2007, you must satisfy the following requirements:

- Ensure that the Windows SharePoint Services Administrative service is running on the front-end web server and the Application Server.
- Ensure that Microsoft SQL Server is running.

How to Perform a Full Backup

If you want to take a full backup of the database you need to ensure certain Farm management actions. If you perform one of these actions and then perform a differential backup, you may not be able to successfully restore the database that you backed up fully, earlier. To avoid this problem, always perform a full database backup immediately after you have performed any of the following actions:

- Any change in the topology of SharePoint 2007 Farm or Windows SharePoint 3.0 Farm such as the following:
 - Adding a new web application, a new SharePoint Service Provider, a new database into a normal web application or SharePoint Service Provider Administration web application.
 - Renaming the SharePoint Service Provider.
 - Deleting the SharePoint Service Provider so that its Administration web application is detached from the SharePoint Service Provider.
 - Canceling a full backup job while it is running.
 - Restoring the database from any backup.

Backup Considerations

To run successful backups consider the following:

- On backup, operation is not allowed. If you perform a full backup of component A, and then a full backup of A's child component B, the differential backup of component A would fail. In other words, a Farm-level full backup can be followed by a Farm-level differential. However, you cannot do a Farm-level full backup followed by a SharePoint Provider Service full backup, and then a Farm Differential backup. In this case, the differential job would fail with an error message.
- You cannot perform a backup by using both SharePoint Server 2007 and tools such as Microsoft SQL Server tools, Central Administration website, and so on. For example, if you perform a full backup using these tools, you may not be able to restore the differential backup job.
- If you try to protect SharePoint Server 2007 using the Agent for SharePoint and other agents, such as Client Agent and Agent for SQL server, the SharePoint 2007 data may be backed up more than once. To avoid this situation, you should exclude the SharePoint 2007 database and files from the Client Agent and Agent for SQL Server backup job.

SharePoint Server 2007 does not support the following:

- Data encryption and compression at the agent side under the Global Options.
- Multiplexing and Multistreaming backup jobs.
- Backup agent data on two different machines that are in different CA ARCserve Backup domain.

Database-Level Agent Backup Option Dialog

The following sections give options that the CA ARCserve Backup Agent for Microsoft SharePoint Server 2007 offers when performing database-level backups.

To configure the database-level backup options, right-click on a Farm object and click Agent Option. The SharePoint 2007 DB Level Agent Backup Option dialog appears.

Default Backup Dump Location

When you submit a backup job, you must select a backup dump location. The backup dump location tells CA ARCserve Backup where you want your data to be stored temporarily before saving it to a tape.

You can select from the following backup dump locations:

Use Agent default configuration setting

Enabled by default. This option makes use of the backup dump location that you selected while configuring the agent.

CA ARCserve Server

Exports the SharePoint 2007 data to a shared folder on CA ARCserve Backup.

CA ARCserve SharePoint Agent

Exports the SharePoint 2007 data to a shared folder where the SharePoint Agent is installed.

Other (NAS, File) Server Name

Exports the SharePoint 2007 data to a specified shared folder on the NAS server or File server.

Note: You must specify the host name instead of an IP address.

Backup Dump Path

You need to specify the share name and physical path.

Share Name

If you select the Other (NAS, File) Server Name as the backup dump location, you need to specify the share name where the data must be exported. You must grant the necessary permissions to the folder.

Note: The share name should not contain the special character '\$' at the end.

Physical Path

If you select the CA ARCserve Server or CA ARCserve SharePoint Agent as the backup dump location, you need to specify the path where you want the data to be exported.

Backup Methods

When you submit a backup job, you must select a backup method. The backup method tells CA ARCserve Backup how you want your data to be backed up.

You can select from the following backup methods:

Use Global or Rotation setting

Enabled by default. If you do not disable this, you must select a backup method on the Schedule tab.

Full

It backs up the entire database and marks all of the files that have been backed up in preparation for a subsequent incremental or differential backup.

Note: Always perform a full backup when running the agent for the first time, after upgrading to a Service Pack, and after performing a restore.

Differential Backup

Backs up the files that have changed since the last backup.

Note: The Backup Method options on the Schedule tab do not apply, if you select the Full or Differential backup methods. SharePoint 2007 does not support the Incremental Backup method. If you select Incremental Backup on the Schedule tab, it will still consider it as Differential Backup.

For more information on these options and how you can configure them, see [Configure the Agent on SharePoint 2007 Systems](#).

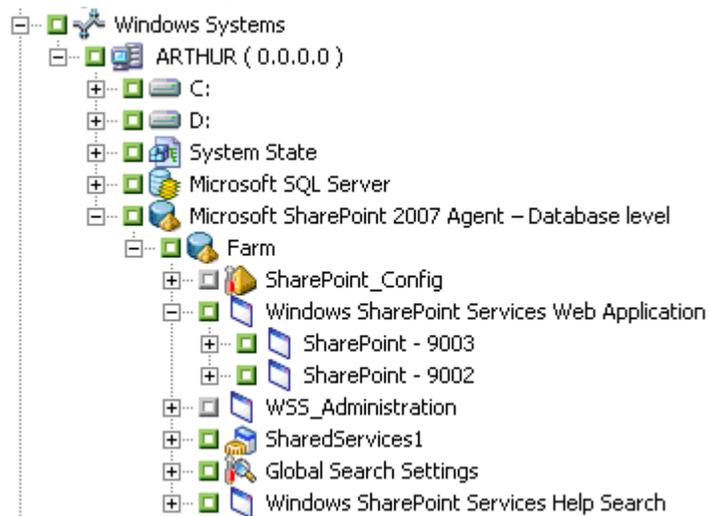
Perform a Database-Level Backup

Use the Backup Manager in CA ARCserve Backup to perform database-level backup on SharePoint 2007 systems.

To perform a Database-level backup on SharePoint 2007 Systems

1. From the CA ARCserve Backup Home Page, select Backup from the Quick Start menu.

The Backup Manager window opens, as shown in the following graphic:



2. From the Backup Manager window, select the Database-Level objects you want to back up (Microsoft SharePoint 2007 - Database level). If you want to back up only certain components in the farm, expand the farm and select the components.
3. Right-click the Farm object you are including in this job and select Agent Option to select a backup method to use and click OK.

Note: Always perform a full backup when running the agent for the first time so that you can store a complete set of SharePoint Server databases.

4. Click the Destination tab and select a backup destination.
5. Click the Schedule tab.

If you want to use a Custom Schedule, select a Repeat Method. If you want to use a rotation scheme, select the Use Rotation Scheme option and set up your scheme. For more information on scheduling jobs and rotation schemes, see the online help or the *Administration Guide*.

6. Click Start in the toolbar.

The Security and Agent Information dialog opens.

7. From the Security and Agent Information dialog, ensure that the correct user name and password are filled in for each object. If you need to enter or modify a user name or password, click the Security button, make your changes, and then click OK.
8. Click OK.
The Submit Job dialog opens.
9. From the Submit Job dialog, select Run Now to run the job immediately, or select Run On and select a future date and time when you want the job to run.
10. Enter a description for your job.
If you selected multiple sources to back up and want to set the priority in which the job sessions initiate, click Source Priority. Use the Top, Up, Down, and Bottom buttons to change the order in which the jobs are processed. When you finish setting priorities, click OK.
11. Click OK.
The backup job is submitted.

Chapter 4: Backing Up SharePoint 2003 Systems

This chapter provides information for backing up data on SharePoint 2003 systems.

This section contains the following topics:

[Backup Overview](#) (see page 39)

[Backup Considerations](#) (see page 48)

[Rotation Schemes and Global Options](#) (see page 49)

[Back Up Data](#) (see page 50)

[Back Up Databases](#) (see page 51)

[Dynamic and Explicit Job Packaging](#) (see page 53)

Backup Overview

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

When a SharePoint Server 2003 database or nondatabase data object backup is started in CA 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 nondatabase data.

Backup Operations

Back up SharePoint Server 2003 data using the Backup Manager interface on a CA ARCserve Backup server. All SharePoint Server 2003 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 Server 2003 data
- Set backup options at job-level and database-level
- Back up selected SharePoint Server 2003 data

Note: For SharePoint Server 2003 database data, the database is the lowest-level element that can be independently backed up. You cannot back up individual tables.

Backup Types

The Agent for Microsoft SharePoint backup options dialog allows you to choose the following methods of database protection:

Database Complete

Use full backups to back up your SharePoint Server 2003 database. You can also use full backups to back up all your SharePoint Server 2003 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.

Important! Do not use this option when backing up the SharePoint 2003 configuration database. It is not supported. However, you may use this option when backing up other SharePoint 2003 databases.

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 nondatabase 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 nondatabase 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 nondatabase 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

More information:

[Backup Types](#) (see page 40)

[Backup Strategy Recommendations](#) (see page 41)

Differential Backups

A differential backup records only the data that has changed since the last full backup of the same part of the data/same data files/same database subset. Usually, these backups are smaller and faster than full backups, but larger and longer than Transaction log backups. To restore a database, a differential backup requires only the last full backup as a prerequisite, and does not need any of the other differential or Transaction log backups performed between it and the last full 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.

More information:

[Backup Types](#) (see page 40)

[Backup Strategy Recommendations](#) (see page 41)

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 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 the 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 replay 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. For more information, refer to Required Full Backups.

File and FileGroup Backups

You can 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 back up an individual file instead of the full database, create procedures 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.

More information:

[Backup Types](#) (see page 40)

[Backup Strategy Recommendations](#) (see page 41)

Transaction Log Backups

Transaction logs record Microsoft SQL Server database activity. When using the Full or Bulk-Logged Recovery Models, they should be backed 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 have less impact on database performance while running
- Normally able to be restored to a specified point in time, rather than only to the time the backup was made

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. For more information, refer to Required Full Backup.

It is sometimes possible to perform a Transaction Log backup of a damaged database. If the database is in the Suspect or Damaged state, and its transaction log files are intact, you will be able to perform a Transaction Log backup without Truncation. This will allow you to recover the database to the point in time immediately before the failure.

Important! Transaction logs are not backed up during full or differential database backups. You must back them up by running separate Transaction log backups or using the Backup Transaction Log After Database option. Transaction logs are only Truncated as part of a Transaction Log backup. If they are not backed up and truncated, they may grow until the disk is full. If this happens, you must perform a Transaction Log backup With Truncation, and then shrink the Transaction Log files to reclaim disk space. In SQL 2005 and later, multiple log backups with Truncation may be needed before log files can be significantly shrunk.

Note: Databases which use the Simple Recovery Model do not permit or require Transaction Log backups. Microsoft SQL Server manages the maintenance of the Transaction Logs for these databases automatically.

More information:

[Backup Types](#) (see page 40)

[Backup Strategy Recommendations](#) (see page 41)

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 database backup performed since that full database backup and before the selected Transaction Log backup, if any
- Any other Transaction log backups performed since the last full database or differential backup and before the selected Transaction Log backup

You can alternatively also restore the following:

- A prior full database backup
- Optionally, a differential database backup that is newer than the full backup selected, and older than the next full database backup, if any
- Every Transaction Log backup performed since the selected full database or differential database 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 against 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.
- **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.

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.

Do not disable Catalog Database when performing backup and restore jobs with this release.

To run successful backups consider the following:

- On backup, operation is not allowed. If you perform a full backup of component A, and then a full backup of A's child component B, the differential backup of component A would fail. In other words, a Farm-level full backup can be followed by a Farm-level differential. However, you cannot do a Farm-level full backup followed by a SharePoint Provider Service full backup, and then a Farm Differential backup. In this case, the differential job would fail with an error message.
- The user name entered in the Agent for Microsoft SharePoint Configuration Wizard must have administrative access to all machines in the SharePoint Server farm.
- You cannot perform a backup by using both SharePoint Server 2007 and tools such as Microsoft SQL Server tools, Central Administration website, and so on. For example, if you perform a full backup using these tools, you may not be able to restore the differential backup job.
- If you try to protect SharePoint Server 2007 using the Agent for SharePoint and other agents, such as Client Agent and Agent for SQL server, the SharePoint 2007 data may be backed up more than once. To avoid this situation, you should exclude the SharePoint 2007 database and files from the Client Agent and Agent for SQL Server backup job.
- If you back up a Microsoft SQL database using both the Agent for Microsoft SQL Server and the Agent for Microsoft SharePoint, the backup history for the database in the SharePoint branch of Restore by Tree will only include backups performed using the Agent for Microsoft SharePoint, while the backup history for the database in the Microsoft SQL Server branch of Restore by Tree lists all backups performed using both agents. This also happens when using the Agent for Microsoft SQL Server.
- If the Agent for Microsoft SQL Server and the database component of the Agent for Microsoft SharePoint are both deployed on the same machine, the SharePoint databases are included in whole-instance backups performed by either the Agent for Microsoft SQL Server or the Agent for Microsoft SharePoint.

SharePoint Server 2007 does not support the following:

- Data encryption and compression at the agent side under the Global Options. Encryption of SharePoint 2003 and 2007 data is supported only on the CA ARCserve Backup server.
- Multiplexing and Multistreaming backup jobs.
- Backup agent data on two different machines that are in different CA ARCserve Backup domains.

SharePoint 2003 does not support the following:

- When backing up the SharePoint 2003 configuration database, you cannot use the Backup only the log tail and leave the database unrecovered option. You may, however, use this option for other SharePoint 2003 database backups.

More information:

[Backup Strategy Recommendations](#) (see page 41)

Rotation Schemes and Global Options

CA ARCserve Backup can use incremental and differential global backup methods when backing up the Agent for Microsoft SharePoint, enabling 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. Encryption for SharePoint 2003 or 2007 data is supported only on the CA ARCserve Backup server.

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

More information:

[Backup Strategy Recommendations](#) (see page 41)

Back Up Data

Use the Backup Manager in CA ARCserve Backup to back up data on SharePoint 2003 systems.

To back up data on SharePoint 2003 systems

1. In the Backup Manager, browse the left pane and expand the Microsoft SharePoint Agent backup node.
The SharePoint data appears in the directory 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 *Administration Guide*.

4. Click Start.

If you have selected SharePoint databases, the Security and Agent Information dialog opens. 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.

More information:

[Consolidated View](#) (see page 18)

Back Up Databases

Use the Backup Manager in CA ARCserve Backup to back up databases on SharePoint 2003 systems.

To back up databases on SharePoint 2003 systems

1. Ensure that Microsoft SQL Server is running on your server. The Microsoft SQL Server service must be started.
2. Start the CA Backup Agent RPC Server service and CA 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.
 - b. Right-click the database object and select Backup Agent Options from the pop-up window. The Backup Agent Options opens.

- c. Select the type of backup you want to perform. For more information about backup types, see [Backup Types](#) (see page 40).
 - 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](#) (see page 46) 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 asterisk (*) 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 *Administration Guide*.
 6. On the Schedule tab, select the scheduling options for this backup. For information about scheduling backups, see the *Administration 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 *Administration 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. This window displays the information when the database is backed up.

For more information about the Job Status window, see the *Administration Guide*.

More information:

[Consolidated View](#) (see page 18)

Dynamic and Explicit Job Packaging

CA ARCserve Backup provides the following two ways to package or set up your backup jobs:

- [Dynamic job packaging](#) (see page 53).
- [Explicit job packaging](#) (see page 54).

Dynamic Job Packaging

If you mark a parent object for dynamic job packaging when defining a backup job, CA 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 back up at the Microsoft SharePoint Agent level, 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 an Object for Dynamic Job Packaging

Use the Backup Manager in CA ARCserve Backup to mark objects for dynamic job packaging.

To mark an object for dynamic job packaging

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.

All of the child items in the object 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, when 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 nondatabase 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.

Example: Explicit Job Packaging

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 an Object for Explicit Job Packaging

Use the Backup Manager in CA ARCserve Backup to mark objects for dynamic job packaging

To mark an object for explicit job packaging

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 to 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.

You can also protect at an individual level. When a 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 5: Restoring SharePoint 2007 Systems

This chapter provides information for restoring data on SharePoint 2007 systems.

This section contains the following topics:

[Restore Overview](#) (see page 57)

[Database-Level Restore Sets](#) (see page 57)

[Database-Level Restore Option Dialog](#) (see page 58)

[Database-Level Restore Prerequisites](#) (see page 60)

[Perform a Database-Level Data Restore](#) (see page 62)

Restore Overview

The following sections include information on the prerequisites you must meet before you perform a restore, the features that the CA ARCserve Backup Agent for Microsoft SharePoint Server 2007 offers when restoring from a database level backup, and the procedure for how to perform a restore.

Database-Level Restore Sets

To restore a SharePoint Server, you must restore all of the sessions that, when combined, completely restore the data. These sessions are called your restore set, and it includes the following sessions:

- If you backed up using only the full backup method, your restore set includes only this full session.
- If you backed up using both full and differential backups, your restore set includes your full session and one differential session. For example, in the following backup scenario, your restore set can be full and differential 1, full and differential 2, full and differential 3, or full and differential 4:

Full	Differential 1	Differential 2	Differential 3	Differential 4
-------------	-----------------------	-----------------------	-----------------------	-----------------------

- If you want to restore from a differential backup, you need to select only that differential backup session. CA ARCserve Backup will find the previous full backup automatically, and then both the full and selected differential backup sessions.

Database-Level Restore Option Dialog

When you create a restore job, you can specify restore options to customize the job.

Default Restore Dump Location

Before you restore data, you must select a restore dump location. The restore location tells CA ARCserve Backup where you want your data to be stored temporarily before restoring it to the SharePoint server.

Note: If you configure the restore location using the restore option, the location configured using Agent Configuration option does not apply. You can select the following restore dump locations:

Use Agent default configuration setting

Enabled by default, this option makes use of the location that you selected while configuring the agent.

CA ARCserve Server

Restores the SharePoint 2007 data to a shared folder on CA ARCserve Backup.

CA ARCserve SharePoint AGENT

Restores the SharePoint 2007 data to a shared folder where the SharePoint Agent is installed.

Other (NAS, File) Server Name

Restores the SharePoint 2007 data to a specified shared folder on the NAS server or File server.

Note: You must specify the host name instead of an IP address.

Restore Dump Path

Share Name

If you select the Other (NAS, File) Server Name as the default restore dump location, you need to specify the Server name where the data must be restored. You must grant the necessary permissions to the folder.

Note: The share name should not contain the special character '\$' at the end.

Physical Path

If you select the CA ARCserve Server or CA ARCserve SharePoint Agent as the restore dump location, you need to specify the path where you want the data to be restored.

For more information on these options and how you can configure them, see [Configure the Agent on SharePoint 2007 Systems](#).

Restore Configuration Settings

You can configure the restore settings using the Start button in the Restore Manager.

The dialog contains the following information:

Type of restore

Lets you to keep the same restore Name and Location after restore or a different one.

Login names and passwords

Lets you to configure who can login to the Farm, Web Application, and SharePoint Service Provider. This credential information is always required to restore the data.

Name and Location

Lets you configure so that the name or location or both so that of one or more components will have new name or location after a backup job has been restored

Different components have different configuration items for name and location. The following table lists the components and their configuration items:

Component Type	Configuration Item	Comment
Database	New database Server Name	The SQL database server you want to restore the database to. It could be an alias name.
	New directory name	The new physical path that

		stores the SQL database files.
	New database name	The new name of the database after restore.
UserProfileApplication	New server name	The new My Site address of UserProfileApplication after restore.
Shared Search Index	New server name	The computer name where the Office Search Index service is running.
	New directory name	The new physical path where the index files are stored.
Web Application	New web application URL	The URL of the Web Application website
	New web application Name	The new name of the web application that is displayed in IIS.

Database-Level Restore Prerequisites

Before performing a database-level restore on SharePoint Server 2007, you must satisfy the following requirements:

- Ensure that the Windows SharePoint Services Administrative service and Windows SharePoint Services Timer service are running on all the Front-End Web servers and Application servers.
- Ensure to restart the Timer service on stand-alone installations.
- If you are restoring search services and indexes to a new location, ensure that the search service is running before you start the restore.
- Ensure that the Application Server Administration Service Timer Job, Application Server Timer Job and Shared Services Provider Synchronizing Job are disabled using SharePoint 2007 Central Admin Utility before restoring any Web Applications.
- Ensure that all web application content databases have unique names. If a database with the same name is used by two web applications and then restored, data in the second database is overwritten with data from the first database.

- Ensure that you do not perform more than one restore at the same time.
- Ensure that all servers in Farm have the same time zone and daylight savings time settings.
- For stand-alone installations, please add the following accounts into the Local Administrators Group before performing a restore job. Once the restore job is completed, delete the accounts:
 - NT AUTHORITY\LOCAL SERVICE
 - NT AUTHORITY\NETWORK SERVICE

To add these accounts

1. Open Control Panel and expand Administration Tools, Computer Management, System Tools, Local Users and Groups, Groups, Administrators.
2. Click Add.
3. Enter NETWORK SERVICE and LOCAL SERVICE.
4. Click OK.

Perform a Database-Level Data Restore

Use the Backup Manager in CA ARCserve Backup to perform a Database-level data restore.

Important! Treat all content database names as unique. Before you restore a content database, make sure the name of the database does not exist in any other web application. If you restore a content database whose name is used by two different applications using the Restore by Session method, the database restore job is listed as 'successful', but occurs under the second application, overwriting whatever content existed in that database.

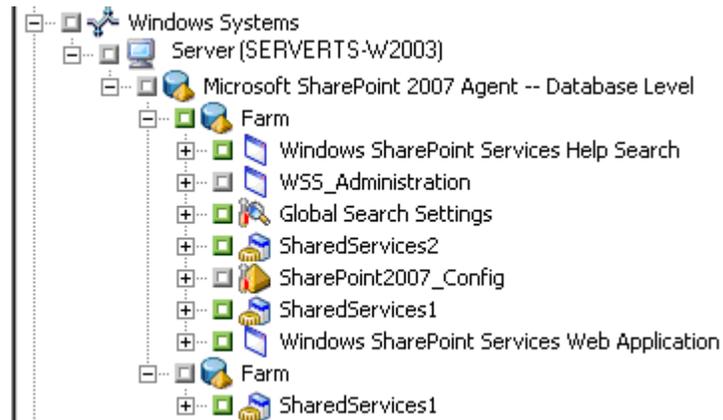
To restore a SharePoint Server 2007 database

1. From the CA ARCserve Backup Home Page, select Restore from the Quick Start menu.

The Restore Manager window opens.

2. From the Restore Manager window, select Restore by Tree in the drop-down list below the Source tab as shown in the following graphic.

Note: Both Restore by Tree and Restore by Session are supported for Database-Level restore.

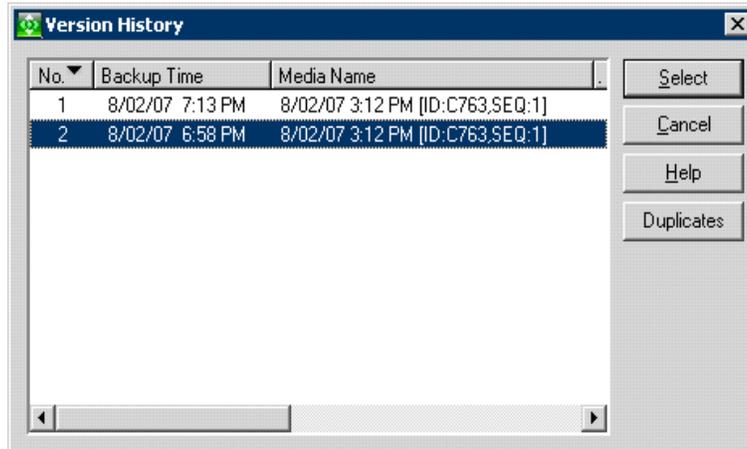


Under the Microsoft SharePoint 2007 Agent - Database Level node there may be more than one Farm object.

If you select multiple components under a Farm for a single backup job, you see multiple Farm objects. Each node is associated with a component selected to backup. For example, if you select a Web Application and a SharePoint Provider service, two Farm objects are generated. One Farm object has the Web Application and the other Farm object has the SharePoint Provider service.

If you back up the same Farm or component several times, you see only one Farm object which displays the latest backup of this component.

- From the directory tree, expand the Windows Systems object, expand the farm containing the database that you backed up, and select the farm object.
- If the most recent backup is not the backup you want to restore, click Version History as shown in the following graphic, select the version you want to restore, and click Select:

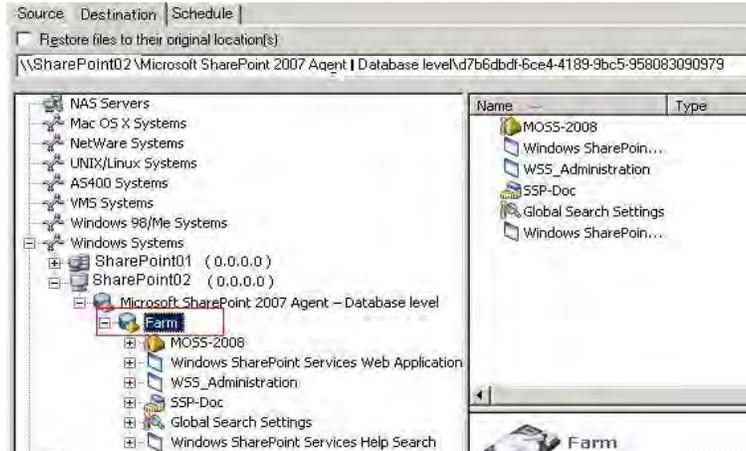


Note: Version History is enabled for SharePoint 2007 Database-Level objects and Farm objects and displays the backup history of the selected components. SharePoint 2007 identifies the Farm component based on its ID, which is unique. This ID does not change even if the component is renamed.

- Right-click each farm object you are including in this job and select Agent Option to select restore options. For more information about restore options, see Database-Level Restore Options.
- Click the Destination tab. You can restore the database objects to their original location (the default) or you can restore the database objects to an alternative location.

7. If you want to restore to an alternative location, clear the check mark from the Restore files to their original locations check box, expand the Windows Systems object, expand the server you want to restore to, and select the Microsoft SharePoint 2007 – Database Level object.

Note: If you want to restore to an alternative location, you must select the Farm object as the destination:



8. Click Start in the toolbar. Enter the required information in the Restore Configuration dialog.

If you are restoring to an alternative location, when the Security dialog appears, enter the user name and password for the destination server and click OK.

9. When the Session User Name and Password dialog opens, verify or change the user name and password for the destination server. To change the user name or password, select the session, click Edit, make your changes, and then click OK.

Note: You must enter the user name in the following format:

DOMAIN\USERNAME

10. Click OK.
11. When the Submit Job dialog opens, select Run Now to run the job immediately, or select Run On and select a future date and time when you want the job to run.
12. Enter a description for your job and click OK.

Important! After you perform a restore, you must restart the Internet Information Services (IIS).

Chapter 6: Restoring SharePoint 2003 Systems

This chapter provides information for restoring data on SharePoint 2003 systems.

This section contains the following topics:

[Restore Overview](#) (see page 65)

[Restore Types](#) (see page 68)

[Restore Options](#) (see page 70)

[Restore Methods](#) (see page 76)

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 try to access a database during the restore process, the 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.

For Microsoft SharePoint Portal Server 2003:

- 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)
- SharePoint Portal Server Document Management Services (if using External Document Library)

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*.

More information:

[Restore Options](#) (see page 70)

[Restore Methods](#) (see page 76)

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.

Database Restores

Different databases are 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 mentioned above.
- Stop World Wide Web Publishing Service on all the Front-End Web Server and Application Servers.
- Shutdown the RouterManagement COM+ component and EDA COM+ component.
- 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 following 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 procedure to restore a portal site 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 the steps in this process to avoid exclusive access problems.

To restore WSS and portal content databases

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
- Restart the service
- Restore the database with a new name.
- Use the SharePoint Sign-On Administration tool to use the new database.

Nondatabase Data Restores

SharePoint nondatabase data restores are less restrictive than SharePoint database restores. Nondatabase 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 (SharePoint Portal Server 2003 only).

Important: If you do not keep the SharePoint Portal Server Document Manager service running, the restore will fail.

- **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.

Important! If you do not keep the Single Sign-On service running, the restore will fail. Also, do not restore the Single Sign-On Configuration File and the Single Sign-On database together. You should restore these separately.

- **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.

Important! If you do not keep the SharePoint Portal Server Search service running, the restore will fail.

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 nondatabase data restores and for database restores.

- For SharePoint nondatabase data restores, the agent supports complete database restores only.
- For database restores, the agent supports the following types of restores:
 - [Complete database restore](#) (see page 69)
 - [Differential backup restore](#) (see page 69)
 - [Transaction log restore](#) (see page 69)
 - [File and FileGroup restore](#) (see page 70)
 - [Partial restore](#) (see page 70)

Complete Database Restore

A complete database restore always restores the entire SharePoint Server 2003 database.

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 chooses the appropriate full-database backup session and the proper options for you. 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 when you created the differential backup. They cannot be used to restore the database to the exact point of failure or to a specific time.

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, partial, or files-and-FileGroups) 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 chooses the appropriate Transaction log, differential, and database backups, and automatically sets the proper options for each. 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 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 chooses all of the Transaction log backups you need 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 chooses the file or FileGroup backup session on which the differential was based and all of the Transaction log backups you need to run the restore successfully.

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.

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 but do not apply to restoring non-database components.

More information:

[Restore Overview](#) (see page 65)

[Restore Methods](#) (see page 76)

Automatic Selection Option

The Automatic Selection option chooses the following options:

- 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

Note: 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.

Important! Check this option before restoring a database to Microsoft SQL 2005 Server.

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

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 CA 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

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

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 and does one of the following actions:

- 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 CA 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 the ones specified 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 instead of 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 nonoperational, 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.

Restore Methods

Use the Restore Manager to perform restore operations for SharePoint Server 2003 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.

More information:

[Restore Overview](#) (see page 65)

[Restore Options](#) (see page 70)

Restore Data

Use the Restore Manager in CA ARCserve Backup to restore SharePoint data.

To restore SharePoint data

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 Data Using the Restore by Tree Method

Use the Restore Manager in CA ARCserve Backup to restore databases and nondatabase data.

To restore databases and nondatabase data using the Restore by Tree method

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 Agent Options from the pop-up window.

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 one of the following methods:
 - For SharePoint databases, select one of the following 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 nondatabase data, select one of the following 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 *Administration Guide*.

Notes:

If a Microsoft SQL database is backed up using both the Agent for Microsoft SQL Server and the Agent for Microsoft SharePoint 2003, the backup history for the database in the SharePoint branch of Restore by Tree will only include backups performed using the Agent for Microsoft SharePoint, while the backup history for the database in the Microsoft SQL Server branch of Restore by Tree lists all backups performed using both agents.

You must use Restore by Session to perform a differential restore of the configuration database. In SharePoint 2003, the Agent cannot automatically select the previous full backup needed to perform the differential restore in Restore by Tree.

Restore Data Using the Restore by Session Method

Use the Restore Manager in CA ARCserve Backup to restore databases and nondatabase data.

To restore databases and nondatabase data using the Restore by Session method

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 CA 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 nondatabase data component you want to restore.

If you are restoring a nondatabase data component, go 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 window.

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 one of the following methods:
 - For SharePoint databases, select one of the following 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 was 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 nondatabase data, select one of the following 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 *Administration Guide*.

Restore Data 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

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 window. 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](#) (see page 84).
- [Restore by Session Using a Separate Job for Each Session](#) (see page 83).

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

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 CA 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 window. 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 window. 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.

Restore by Session Using a Single Restore Job

Use the Restore Manager in CA ARCserve Backup to restore databases by session using a single restore job.

To restore databases by session using a single restore job

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 CA 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 window. 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: You cannot restore any additional transaction logs 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 Database to Alternate Microsoft SQL Systems

Use the Restore Manager to restore databases to another machine installed with Microsoft SQL Server.

To restore a database to another machine with Microsoft SQL Server

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 CA ARCserve Backup opens.
2. Choose the media containing the backup you want to restore, and select the session containing the specific database you want to restore.
3. Right-click the session containing the database you want to restore, and choose Backup Agent Options from the pop-up window.
4. On the Source tab, verify that the session you want to restore is selected.
5. On the Destination tab, clear the Restore files to their original location(s) check box.
6. From the directory tree, expand the Windows Systems object and select the destination server.
7. Expand the Microsoft SharePoint Agent node, expand the farm containing the database that you backed up, and select the farm object.

The destination location under the Restore files to their original location(s) is displayed incorrectly.

8. Enter the correct destination location in the following format:

```
\\<DatabaseServerMachineName>\dbasql@<SQLServerInstanceName>\<DatabaseName>
```

If the SQL server instance name is the default name, then the destination would be

```
\\<DatabaseServerMachineName>\dbasql@MSSQLSERVER\<DatabaseName>
```

9. Click Start.

The Session User Name and Password dialog opens.

10. 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.

11. 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.

12. Click OK on the Session User Name and Password dialog.

The Submit Job dialog opens.

13. (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.

14. 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 *Administration Guide*.

Chapter 7: Using Best Practices

This section recommends best practices for using CA ARCserve Backup Agent for Microsoft SharePoint on SharePoint 2007 systems.

This section contains the following topics:

[How to Select the Proper Location](#) (see page 87)

[Set Access Permission on Dump Location](#) (see page 88)

How to Select the Proper Location

You must select a proper location both for backup as well as restore. The following considerations apply:

- Available disk size—The Agent for SharePoint 2007 stores some data in a dump location during backup and restore. You should ensure that there is enough disk space to hold all the components that will be backed up. If you want to know how much disk space is required for the backup job, open the Backup Manager, select the component to be backed up, and then check the disk space required.

Object Disk Size Required	3,318,633,869 Bytes
---------------------------	---------------------

- Available Network Band-You must select an available network band for the differential dump location depending on your network traffic and costs involved. Consider the following:
 - CA ARCserve Server costs less because the data is transferred once.
 - CA ARCserve SharePoint Agent (Local Machine) and Other (NAS, File) Server Name cost more as the data maybe transferred twice.
- ARCserve Server and SharePoint 2007 Agent Location-CA ARCserve SharePoint Agent (Local Machine) and Other (NAS, File) Server Name support all of the following four scenarios:
 - Agent and server are installed in a single windows domain.
 - Agent and server are installed in two different domains and one domain trusts another.
 - Agent and server are installed in different Windows domains, and there is no trust relationship.
 - Either the agent or the server is installed in a workgroup and the other is installed in a domain.

Note: CA ARCserve Server supports only the first two scenarios mentioned above.

Set Access Permission on Dump Location

The accounts in the following table can access the shared folder:

Account	Dump Location Access Permission for Backup	Dump Location Access Permission for Restore
Database server's SQL Account	All permissions except Full Control	Read permission
The Timer service account	All permissions except Full Control	Read permission
Central Administrator pool account	All permissions except Full Control	All permissions except Full Control

If the database server's SQL account is on a Local system, you must grant the required permission to the SQL server computer. If you want to know who has been assigned permissions to the shared folder, open the Backup Manager, select the account, and then check the list of users who have permission to the shared folder.

Backup Restore Shared Folder Permission User List	Arthur (Arthur-W3S-2)
---	-----------------------

Appendix A: Disaster Recovery

This section contains the following topics:

[How the Agent Supports Disaster Recovery on SharePoint 2003 Systems](#) (see page 89)

[Restore a Front-End Web Server](#) (see page 90)

[Restore a Backward-Compatible Document Library Server](#) (see page 90)

[Restore a Search Index Server](#) (see page 91)

[Restore a Database Server](#) (see page 92)

[How to Perform a Database-Level Disaster Recovery on SharePoint 2007 Systems](#) (see page 93)

How the Agent Supports Disaster Recovery on SharePoint 2003 Systems

A typical disaster recovery scenario may require you to rebuild your machines and reinstall Windows and CA 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 the following roles:

- [Front-end web server](#) (see page 90).
- [Backward-compatible document library server](#) (see page 90).
- [Search index server](#) (see page 91).
- [Database server](#) (see page 92).

You can assign these roles 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.

Restore a Front-End Web Server

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, you should protect this information. The files and data that you should back up include the following:

- 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

You can fully protect all of this information using the Client Agent for Windows. For more information about using this agent, see the *Client Agents Guide*.

To restore a front-end web server

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 CA 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 Backward-Compatible Document Library Server

You can restore a backward-compatible document library server using CA ARCserve Backup.

To restore a backward-compatible document library server

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 CA ARCserve Backup for Microsoft SharePoint Configuration wizard to install the SharePoint External Data Agent.
7. Restore the backward-compatible document library.

Note: Restoring the backward-compatible Document Library to an alternative location on a remote machine running a different version of Exchange Storage Engine than the Source machine causes SharePoint Portal Server Document Management service on the remote machine to fail. To avoid this, you must ensure that the version of the Exchange Storage Engine running on the remote machine is same as the version running on the source machine.

Restore a Search Index Server

You can restore a search index server using CA ARCserve Backup.

To restore a search index server

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 CA ARCserve Backup for Microsoft SharePoint Configuration wizard, install the SharePoint External Data Agent.
5. Restore the SharePoint search index files to the new server.

Note: Performance may be slowed when backing up or restoring search indexes, as these operations may consume 100% of your CPU resources if the SharePoint server used satisfies only the minimum hardware requirements for Microsoft SharePoint Portal Server. See the Microsoft SharePoint Portal Server Administrator's Guide for more information about hardware requirements.

Restore a Database Server

You can restore Microsoft SQL Server 2000 or 2005 using CA ARCserve Backup.

To restore a Microsoft SQL Server 2000 or 2005

1. Restore or rebuild the server so that Microsoft SQL Server 2000 or 2005 is configured in the same way it was before 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 CA 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 or SQL 2005 Express is slightly different if you cannot restore the machine so that MSDE or SQL 2005 Express is running correctly. In this situation, perform the following steps.

To restore a single-server installation using MSDE or SQL 2005 Express

1. Restore or rebuild the server.
2. Reinstall SharePoint Portal 2003 or Windows SharePoint Services and all SharePoint service packs to recreate the MSDE or SQL 2005 Express installation and create the configuration database.

3. Use the CA 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 re-create the SharePoint Portal or Windows SharePoint Services sites.

Note: If you know that the configuration of SharePoint was stable when the backup was performed, you might recover the configuration database. However, this option is not supported by Microsoft.

How to Perform a Database-Level Disaster Recovery on SharePoint 2007 Systems

If one or more computers in a farm crash, it can corrupt the entire farm or a few components. If a disaster occurs, you must follow this process to restore the SharePoint 2007 data:

- Restore the operating system on your computer. The CA ARCserve Backup Disaster Recovery Option provides an automated and efficient way for you to complete these tasks. For more information, see the *Disaster Recovery Option Guide*.
- Ensure that the required applications are operational. SQL Server should be running on the computer where Microsoft SQL Server is installed. The front-end web server and Application server require SharePoint 2007.
- If you want to recover the entire farm, you must create the new farm using SharePoint Products and the Technologies Configuration wizard.
- After creating the new Farm, make sure that the following services in the SharePoint 2007 Central Admin are running:
 - Windows SharePoint Services Help Search, Office SharePoint Server Search, and Excel Calculation Services for SharePoint 2007 Farm
 - Windows SharePoint Services Search for Windows SharePoint Services 3.0 Farm
- If the new Farm is a stand-alone setup, you must rename the default Shared Service Provider (SharedService1) to a new name that does not exist in the original Farm. After you perform the restore, you can delete the Shared Service Provider.
- Restore the Farm or its components. For instructions on how to restore the databases to SharePoint 2007, see Perform a Database-Level Data Restore.

Appendix B: Configuring Microsoft SQL Server Security Settings

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

This section contains the following topics:

[Types of Microsoft SQL Authentication](#) (see page 95)

[Authentication Requirements](#) (see page 95)

[How User Authentication Is Changed](#) (see page 96)

[Check or Change the Microsoft SQL Server Authentication Method](#) (see page 96)

Types of Microsoft SQL Authentication

Microsoft SQL Server provides the following 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 or 2005 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 CA ARCserve Backup. In addition, if you change the option, you must update settings so that both Windows and CA ARCserve Backupv 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 CA ARCserve Backup so that this change is reflected, you must check and change the Microsoft SQL Server authentication method.

Check or Change the Microsoft SQL Server Authentication Method

You can check or change the Microsoft SQL Server authentication method using CA ARCserve Backup.

To check or change the Microsoft SQL Server authentication method

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 list.
The Properties dialog opens.

4. In the Properties dialog, click the Security tab.
5. Under Authentication, select one of the following options:

Microsoft SQL Server and Windows

Enables Microsoft SQL server-based authentication.

Windows Only

Enables only Windows user names and passwords.

6. Click OK.
The user authentication process is now set.

Appendix C: Troubleshooting

The following information is provided for troubleshooting backup and restore issues using the CA ARCserve Backup Agent for Microsoft SharePoint:

This section contains the following topics:

[AE9972](#) (see page 99)

AE9972

If you receive an AE9972 Object <Component Name> failed error in event OnRestore, perform the following tasks:

1. Start the SPAdmin Windows Service, displayed as Windows SharePoint Services Administration.
2. Go the SharePoint 3.0 Central Administration website and select Operations, Topology and Services, Services on Server.
3. Choose the agent machine server and select the Custom radio box.
4. Click Central Administration.
5. Click Start.
6. Run the job that previously failed, again.

Index

A

agent

- agent, architecture • 15
- agent, SharePoint database • 17
- agent, SharePoint external data • 17
- agent, SharePoint Router • 17
- configuration • 29
- disaster recovery support • 89
- features • 11
- uninstallation • 32

B

back up databases, procedure • 51

backup

- backing up databases • 51
- differential backup • 43
- file and filegroup backups • 44
- full backup • 42
- incremental backups • 49
- job packaging • 53, 54
- overview • 39
- procedure • 51
- strategy • 41
- supported backup types • 40
- transaction log • 44

Backup Manager • 50

backward-compatible document library server,
restoring • 90

C

- configuring the agent • 29
- consolidated view • 18
- contacting technical support • v
- customer support, contacting • v

D

- database consistency checks • 46, 75
- database server, restoring using disaster
recovery • 92
- differential backup • 43
- differential backup restores • 69
- directory structure, Backup Manager • 18
- disaster recovery • 89
- dynamic job packaging • 53

E

encryption

- encryption, single sign-on key • 13, 17, 18,
49
- encryption, support • 34, 48, 49
- explicit job packaging • 55

F

- file and filegroup backups • 44
- file and filegroup restores • 70
- force restore option • 72
- front-end web server, restoring • 90

G

global backup options • 49

I

- incremental backups • 49
- installation
 - considerations • 26
 - prerequisites • 28

K

keep replication settings • 76

L

log point in time restore • 73

R

- recovery completion state • 73
- restore database files as • 75
- restoring data
 - by session • 80
 - by tree • 77
 - disaster recovery • 90, 91, 92
 - methods • 76
 - options • 70, 71, 72, 73, 75, 76
 - overview • 65
 - restoring data, backward-compatible
document library server • 90
 - restoring data, database server • 92
 - restoring data, front-end web server • 90
 - restoring data, partial restore • 70

- restoring data, search index server • 91
- restoring differential backups • 69
- restoring transaction logs • 69
- supported databases • 66
- transaction log • 69
- using automatic selection • 71, 82
- using restore type • 71

restricted user access after restore • 76

rotation schemes • 49

S

- search index server, restoring • 91
- server roles • 18
- SharePoint data
 - environments • 11
 - server roles • 18
 - types supported • 13
- SharePoint Database Agent • 17
- SharePoint External Data Agent • 17
- SharePoint Router Agent • 17
- Single Sign-on
 - Single Sign-on, configuration • 12, 21, 29, 68, 89
 - Single Sign-on, database • 12, 13, 21, 67
 - Single Sign-on, encryption key • 14, 17, 18
 - Single Sign-on, server • 11, 15, 65
- SQL Agent filter • 76
- SQL Server, authentication • 95
- strategy for backing up data • 41
- support, contacting • v
- supported backup types • 40

T

- technical support, contacting • v
- transaction log backups • 44
- transaction log restores • 69

U

- uninstalling the agent • 32