

SnapManager® 2.0 for Microsoft® Office SharePoint® Server

Installation and Administration Guide

NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089 USA
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: <http://www.netapp.com>

Part number: 215-04396_A0
December 2008

Copyright and trademark information

Copyright information

Copyright © 1994–2008 NetApp, Inc. All rights reserved. Printed in the U.S.A.

No part of this file covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted material of NetApp, Inc. is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication or disclosure by the government is subject to restrictions set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp, the Network Appliance logo, the bolt design, NetApp—the Network Appliance Company, Cryptainer, Cryptoshred, DataFabric, DataFort, Data ONTAP, Decru, FAServer, FilerView, FlexClone, FlexVol, Manage ONTAP, MultiStore, NearStore, NetCache, NOW NetApp on the Web, SANscreen, SecureShare, SnapDrive, SnapLock, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapValidator, SnapVault, Spinnaker Networks, SpinCluster, SpinFS, SpinHA, SpinMove, SpinServer, StoreVault, SyncMirror, Topio, VFM, and WAFL are registered trademarks of NetApp, Inc. in the U.S.A. and/or other countries. gFiler, Network Appliance, SnapCopy, Snapshot, and The evolution of storage are trademarks of NetApp, Inc. in the U.S.A. and/or other countries and registered trademarks in some other countries. The NetApp arch logo; the StoreVault logo; ApplianceWatch; BareMetal; Camera-to-Viewer; ComplianceClock; ComplianceJournal; ContentDirector; ContentFabric; EdgeFiler; FlexShare; FPolicy; Go Further, Faster; HyperSAN; InfoFabric; Lifetime Key Management, LockVault; NOW; ONTAPI; OpenKey, RAID-DP; ReplicatorX; RoboCache; RoboFiler; SecureAdmin; Serving Data by Design; SharedStorage; Simplicore; Simulate ONTAP; Smart SAN; SnapCache; SnapDirector; SnapFilter; SnapMigrator; SnapSuite; SohoFiler; SpinMirror; SpinRestore; SpinShot; SpinStor; vFiler; VFM Virtual File

Manager; VPolicy; and Web Filer are trademarks of NetApp, Inc. in the U.S.A. and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of NetApp, Inc. in the U.S.A.

IBM, the IBM logo, AIX, and System Storage are trademarks and/or registered trademarks of International Business Machines Corporation.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the U.S.A. and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the U.S.A. and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the U.S.A. and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks. NetApp, Inc. NetCache is certified RealSystem compatible.

Table of Contents

	Preface	vii
Chapter 1	Overview	1
Chapter 2	Preparing to Install SnapManager for Microsoft Office SharePoint Server	3
	Windows host system requirements	4
	Determining storage space needs	7
Chapter 3	Installing SnapManager for Microsoft Office SharePoint Server	11
	Where to Install SnapManager for Microsoft Office SharePoint Server components	12
	Installing SnapManager for Microsoft Office SharePoint Server Manager . .	13
	Installing SnapManager for Microsoft Office SharePoint Server Agent . . .	17
Chapter 4	Upgrading SnapManager for Microsoft Office SharePoint Server	21
	Upgrading SnapManager for Microsoft Office SharePoint Server Manager. .	22
	Upgrading SnapManager for Microsoft Office SharePoint Server Agent . . .	24
Chapter 5	Verifying the SnapManager for Microsoft Office SharePoint Server	
	Installation	27
Chapter 6	Accessing SnapManager for Microsoft Office SharePoint Server	29
Chapter 7	Uninstalling SnapManager for Microsoft Office SharePoint Server	31
Chapter 8	General Administrative Services	33
	Control Service	34
	Data Retention	36
	Device Manager	37

	Verification Server	41
	Account Manager	42
	System Recovery	47
	Log Manager	50
	E-mail Notification	52
	License Manager	54
Chapter 9	Preparing and Managing SharePoint Data	55
	Database and index migration	56
Chapter 10	Backup Builder	59
	Backup of SharePoint components	67
	Limitations for backup	68
Chapter 11	Restore Controller.	69
	Common restore options	71
	Granular level restore.	73
	Farm component level restore options	77
	Farm component level restore considerations	80
	Disaster recovery	83
	Full farm restore	86
	Restore from alternate storage location.	92
	Restore limitations	94
Chapter 12	Job Monitor	95
	Log Viewer	96
	Job Monitor	97

Preface

About this guide

This guide describes how to install the SnapManager® 2.0 for Microsoft® Office SharePoint® Server (SMMOSS) Manager and Agent software, use the Control Panel features, and back up and restore SharePoint data.

This guide does not explain how to install, configure, and use the SnapDrive® features that enable creation and connection to LUNs. Also, the guide does not explain how to install the SnapManager for Microsoft SQL Server™ software, which must be installed before using SnapManager for Microsoft Office SharePoint Server. For information about this installation and details on how to configure the storage system volumes and enable storage system access, see the *SnapDrive Installation and Administration Guide* for the version of SnapDrive that is running on the Microsoft SQL Server. See the *SnapManager for Microsoft SQL Server Installation and Administration Guide* for more information about using SnapManager for Microsoft SQL Server.

This guide also does not cover basic system or network administration topics, such as IP addressing, routing, and other network topology.

Audience

This guide is for system and SharePoint administrators who possess a working knowledge of Microsoft Office SharePoint Server 2007 and Windows Server (2003 and 2008). The audience must be familiar with following topics:

- ◆ Microsoft Office SharePoint Server administration
- ◆ Network functions and operations
- ◆ Operating system, network, and storage systems

Command, keyboard, and typographic conventions

This document uses command, keyboard, and typographic conventions that help you enter commands.

Command convention: In examples that illustrate commands executed on a UNIX workstation, the command syntax and output might differ, depending on your version of UNIX.

Keyboard conventions: The following list describes keyboard conventions used in this document:

- ◆ When describing key combinations, this document uses the hyphen (-) to separate individual keys. For example, “Ctrl-D” means pressing the “Control” and “D” keys simultaneously.

- ◆ This document uses the term “Enter” to refer to the key that generates the digital equivalent of a carriage return, although the key is named “Return” on some keyboards.

Typographic conventions: The following table describes typographic conventions used in this document.

Convention	Type of information
<i>Italic font</i>	Words or characters that require special attention. Placeholders for information you must supply. For example, if the guide says to enter the arp -d hostname command, you enter the characters “arp -d” followed by the actual name of the host. Book titles in cross-references.
Monospaced font	Command names, option names, keywords, and daemon names. Information displayed on the system console or other computer monitors. The contents of files.
Bold monospaced font	Words or characters you type. What you type is always shown in lowercase letters, unless you must type it in uppercase letters.

Special messages

This document might contain the following types of messages to alert you to conditions you need to be aware of. Danger notices and caution notices only appear in hardware documentation, where applicable.

Note

A note contains important information that helps you install or operate the system efficiently.

Attention

An attention notice contains instructions that you must follow to avoid a system crash, loss of data, or damage to the equipment.

DANGER

A danger notice warns you of conditions or procedures that can result in death or severe personal injury.

CAUTION

A caution notice warns you of conditions or procedures that can cause personal injury that is neither lethal nor extremely hazardous.

About SnapManager for Microsoft Office SharePoint Server

SnapManager for Microsoft Office SharePoint Server is an enterprise strength backup, recovery, and content management solution for Microsoft SharePoint versions including Windows SharePoint Services 3.0 and Microsoft Office SharePoint Server 2007.

Operating on NetApp's latest distributed software platform, SnapManager for Microsoft Office SharePoint Server Manager is accessible from anywhere in the network through Internet Explorer®, and can monitor multiple SharePoint environments across the network. SnapManager for Microsoft Office SharePoint Server Manager's main features include the following:

- † The ability to centrally manage SharePoint backup and recovery jobs, including scheduling, monitoring, reporting, user account management, and software agent management across multiple SharePoint farms from a single accessible-from-anywhere Web interface
- † Fast backup speeds leveraging Snapshot backups, as well as real-time granular restore of items, item versions, lists, libraries, sites, and site collections, directly onto the production server (or an alternate location)
- † Backup coverage of all SharePoint databases, including the content, search, configuration, Single Sign-On (SSO), and Shared Services Provider (SSP) databases
- † Backup of SharePoint search index files
- † Backup of various SharePoint component settings, SharePoint solutions, and IIS settings on front-end servers
- † SnapMirror replication for backups of SharePoint databases and search indexes, and verification of SnapMirror database targets
- † SnapVault/data set backup for backups of SharePoint databases, and verification of SnapVault targets
- † Multiple schedules for different restore granularity levels in a single backup plan
- † Separately scheduled verification jobs apart from backup or restore jobs
- † Different retention settings for the same backup components in multiple plans

Modules required for the installation

SnapManager for Microsoft Office SharePoint Server consists of two modules: SnapManager for Microsoft Office SharePoint Server Manager and SnapManager for Microsoft Office SharePoint Server Agent. Both modules must be installed in order to run SnapManager for Microsoft Office SharePoint Server.

This section describes the tasks that you must complete before installing SnapManager 2.0 for Microsoft Office SharePoint Server:

- † [“Windows host system requirements”](#)
- † [“Determining storage space needs”](#)

Windows host system requirements

SnapManager for Microsoft Office SharePoint Server Manager requirements

The following table lists the hardware and software requirements for SnapManager for Microsoft Office SharePoint Server Manager.

Component	Requirement
Computer and processor	PC with an Intel® Pentium® III-compatible 700-MHZ processor (dual Intel Xeon® 3.0 GHz or faster recommended)
Memory	2 GB of RAM minimum, 3 GB recommended
Hard disk	2 GB minimum, 5 GB or more recommended
Operating system	One of the following: • Windows Server 2003 Standard Edition with SP1 or SP2 (x86, x64) • Windows Server 2003 Enterprise Edition with SP1 or SP2 (x86, x64) • Windows Server 2003 R2 Standard Edition (x86, x64) • Windows Server 2003 R2 Enterprise Edition (x86, x64) • Windows Server 2003 R2 Standard Edition with SP2 (x86, x64) • Windows Server 2003 R2 Enterprise Edition with SP2 (x86, x64) • Windows Server 2008 Standard Edition (x86, x64) • Windows Server 2008 Enterprise Edition (x86, x64) Note_____ Only IPv4 is supported. _____
Framework	.NET Framework v2.0 required

SnapManager for Microsoft Office SharePoint Server Agent requirements

The following table lists the hardware and software requirements for the SnapManager for Microsoft Office SharePoint Server Agent.

Component	Requirement
Computer and processor	PC with an Intel Pentium III-compatible 700-MHZ processor (dual Intel Xeon 3.0 GHz or faster recommended)
Memory	1GB of RAM minimum, 2 GB recommended
Hard disk	1 GB minimum, 3 GB recommended
Operating system	One of the following: • Windows Server 2003 Standard Edition with SP1 or SP2 (x86, x64) • Windows Server 2003 Enterprise Edition with SP1 or SP2 (x86, x64) • Windows Server 2003 R2 Standard Edition (x86, x64) • Windows Server 2003 R2 Enterprise Edition (x86, x64) • Windows Server 2003 R2 Standard Edition with SP2 (x86, x64) • Windows Server 2003 R2 Enterprise Edition with SP2 (x86, x64) • Windows Server 2008 Standard Edition (x64, x86, IA64) • Windows Server 2008 Enterprise Edition (x64, x86, IA64) Note _____ Only IPv4 is supported. Also, only the SnapManager for Microsoft Office SharePoint Server Member Agent supports IA64. _____
Framework	.NET Framework v2.0 required

Component	Requirement
Microsoft SQL Server	The following list shows the requirements for Microsoft SQL Server. • SQL Server 2008 Standard Edition (x86, x64, IA64) • SQL Server 2008 Enterprise Edition (x86, x64, IA64) • SQL Server 2005 Standard Edition with SP1 or SP2 (x86, x64, IA64) • SQL Server 2005 Enterprise Edition with SP1 or SP2 (x86, x64, IA64) • SQL Server 2000 Standard Edition SP4 (x86) • SQL Server 2000 Enterprise Edition SP4 (x86)
SnapManager for Microsoft SQL Server version	SnapManager for Microsoft SQL Server must be installed. Note_____ This requirement only pertains to the SnapManager for Microsoft Office SharePoint Server Member Agent. _____
Microsoft Office SharePoint Server	SnapManager 2.0 for Microsoft Office SharePoint Server requires the installation of the front-end Web server for Microsoft Office SharePoint Server (MOSS) 2007 or Windows SharePoint Services (WSS) 3.0. Note_____ These platforms can be used with or without Service Pack 1 installed. _____

Determining storage space needs

Storage space requirements

The required storage space for content databases, indexes, and other storage requirements are specific to each SharePoint environment and must be estimated for every specific environment.

You can assess the general volume size requirements for SnapManager for Microsoft Office SharePoint Server in the same way as it is done for SnapManager for Microsoft SQL Server. For more information, see the section Assessing volume size in the *SnapManager for Microsoft SQL Server Installation and Administration Guide*.

The general guidelines for sizing NetApp volumes, storage devices, content databases, and indexes are described in the following table.

Component	Size	Description
Recommended maximum content database size	50 GB	This is not the absolute maximum size but a general recommendation for performance and scalability.
Recommended maximum number of content databases per storage device	10	This is a recommendation and not a limitation.

Component	Size	Description
Maximum number of content databases per NetApp volume	35	All databases located on a NetApp volume might be backed up in a single backup operation. In this case, the SQL Server must be able to manage all the databases while they are being backed up. Each database that is being backed up requires SQL Server resources. The SQL Server might not be able to manage more than 35 databases. If the database server does not have enough RAM, then even 35 databases might be too many for the SQL Server to manage.
Note_____ The recommendations in the following five rows are based on the information found in the following Microsoft article: http://technet2.microsoft.com/Office/en-us/library/5465aa2b-aec3-4b87-bce0-8601ff20615e1033.msp?mfr=true		
Database log files		Disk space needs for log files vary based on log settings and the number of databases. For more information, see the following article: http://go.microsoft.com/fwlink/?LinkId=78853&clcid=0x409
Configuration database	1.5 GB	Most configuration databases do not grow beyond this size. This is an estimated maximum size, not a hard limit.
Content databases		Estimate the initial volume of content that will be stored in content databases. Multiply the value of the size of the initial content by 1.2 to get the value of the size of stored content in an SQL Server database. If versions are used for documents, a copy of each version is stored in the database.
Future growth		You should plan for twice the amount of data that you initially plan to store. Enter a number that is appropriate for your environment.

Component	Size	Description
Content index		Add the amount of content in content databases that will be indexed by the index server. Thirty percent of the resulting number is the maximum estimated size of the content index.

This section describes how to install the SnapManager for Microsoft Office SharePoint Server Manager and Agents. The following topics are covered:

- † [“Where to Install SnapManager for Microsoft Office SharePoint Server components”](#)
- † [“Installing SnapManager for Microsoft Office SharePoint Server Manager”](#)
- † [“Installing SnapManager for Microsoft Office SharePoint Server Agent”](#)

Where to Install SnapManager for Microsoft Office SharePoint Server components

Where to install SnapManager for Microsoft Office SharePoint Server Manager

SnapManager for Microsoft Office SharePoint Server Manager can be installed on any machine on the network meeting the requirements described in [Chapter 2, "System Requirements"](#). The machine it is installed on serves as the interface to access the SnapManager for Microsoft Office SharePoint Server application from other machines. Therefore, you should install SnapManager for Microsoft Office SharePoint Server Manager on a machine with high availability. This can be on the same machine where SnapManager for Microsoft Office SharePoint Server Control Agent is installed.

Where to install SnapManager for Microsoft Office SharePoint Server Agent

There are two kinds of agents in SnapManager for Microsoft Office SharePoint Server Agent, which can either be deployed separately or on the same server depending on the need:

Control Agent: This should be installed on the SharePoint front-end Web server.

Member Agent: This should be installed on Microsoft SQL Server (for database backups), the SharePoint index server (for search index backups), or the SharePoint front-end server (for front-end resource backups such as IIS backups).

SQL cluster support

SnapManager for Microsoft Office SharePoint Server supports SQL clustering. If cluster failover support is required, a member agent must be installed on each SQL cluster node, otherwise, a member agent needs to be installed only on the active node.

Installing SnapManager for Microsoft Office SharePoint Server Manager

Installation prerequisites

Before installing SnapManager for Microsoft Office SharePoint Server Manager, complete the following steps.

Step	Action
1	Install SnapDrive and SnapManager for Microsoft SQL Server on all machines containing Microsoft SQL Server.
2	Install .NET Framework v2.0 on all machines.
3	Verify that the installation account has local administrator rights.

Installation steps

To install SnapManager for Microsoft Office SharePoint Server Manager, complete the following steps.

Step	Action	
1	Install the software from the CD-ROM or download it.	
	If...	Then...
	You are obtaining the software from the network	1. Download the SnapManager for Microsoft Office SharePoint Server Manager package from the network. 2. Save it on the Windows host system. 3. Launch the SnapManager for Microsoft Office SharePoint Server Manager installation package by double-clicking setup.exe in the Explorer window.
	You are installing the software from the CD-ROM	Browse to the SnapManager for Microsoft Office SharePoint Server Manager installation package and double-click setup.exe on the CD drive.

Step	Action
2	The SnapManager for Microsoft Office SharePoint Server Manager Install Wizard launches. Click Next in the bottom right side of the window to begin the installation process.
3	Review the license agreement for SnapManager for Microsoft Office SharePoint Server. Read the terms of the agreement and click the radio button to select “I accept the terms in the license agreement.” Click Next.
4	Enter the desired User Name and Organization name in the Customer Information window.
5	Select Change to install the package to a drive or a path other than the default path.

Step	Action
6	After the installation is complete, review the SnapManager for Microsoft Office SharePoint Server Manager configuration details. SMMOSS Control Service Address: Specify the current machine's host name or IP address. The Control Service manages internal configuration data, user access control, scheduling, and job monitoring. SMMOSS Control Service Port: The default port number is 12000. SMMOSS Media Service Address: Specify the current machine's host name or IP address. The Media Service manages backup job data (for example, job metadata and backup index). SMMOSS Media Service Control Port: The default port number is 12001. SMMOSS Web Service Address: Specify the current machine's host name or IP address. The Web Service is the display engine for the browser console. SMMOSS Web Service Port: The default port number is 8080 for HTTP, and 8443 for HTTPS. SMMOSS Web Network Port: This is the internal communication port from the Control Service to the Web Service. By default, this value is 12002. Enable HTTPS: Selecting the check box enables users to access the SnapManager for Microsoft Office SharePoint Server interface over HTTPS. By default, this box is not selected. Enable Active Directory: Select this check box to integrate with Active Directory (AD) and add existing AD users to the SnapManager for Microsoft Office SharePoint Server platform. Enter the user name and password of an Active Directory account. The user does not need to be an administrator. If SnapManager for Microsoft Office SharePoint Server Manager is installed without this option selected, only local SnapManager for Microsoft Office SharePoint Server accounts can be created and added to SnapManager for Microsoft Office SharePoint Server.

Step	Action
7	Change the settings according to your needs and click Next button. Note_____ It is recommended that you use the default settings unless a known conflict with an existing port exists. _____
8	The installer configures SnapManager for Microsoft Office SharePoint Server Manager with the chosen name and port designations.
9	Click Finish to exit SnapManager for Microsoft Office SharePoint Server Manager Install Wizard.

Installing SnapManager for Microsoft Office SharePoint Server Agent

Installation prerequisites

Before installing SnapManager for Microsoft Office SharePoint Server complete the following steps.

Step	Action
1	Install Microsoft Office SharePoint Server 2007 or Windows SharePoint Services 3.0 on a server in the environment (SnapManager for Microsoft Office SharePoint Server Control Agent will be installed on this server).
2	Install SnapManager for Microsoft SQL Server on all machines containing Microsoft SQL Server (SnapManager for Microsoft Office SharePoint Server Member Agent will be installed on this server).
3	Install .NET Framework v2.0.
4	Verify that the installation account has local administrator rights.

Installation steps

To install SnapManager for Microsoft Office SharePoint Server Agent, complete the following steps.

Step	Action	
1	Install the software from the CD-ROM or download it.	
	If...	Then...
	You are obtaining the software from the network	1. Download the SnapManager for Microsoft Office SharePoint Server Agent package from the network. 2. Save it on the Windows host system. 3. Launch the SnapManager for Microsoft Office SharePoint Server Agent installation package by double-clicking setup.exe in the Explorer window.
	You are installing the software from the CD-ROM	Browse to the SnapManager for Microsoft Office SharePoint Server Agent installation package and double-click setup.exe.
2	The SnapManager for Microsoft Office SharePoint Server Agent Install Wizard launches. Click Next in the bottom right side of the window to begin the installation process.	
3	Review the license agreement for SnapManager for Microsoft Office SharePoint Server. Read the terms of the agreement and click the button to select "I accept the terms in the license agreement." Click Next.	
4	Enter the desired User Name and Organization name in the Customer Information window.	
5	Select Change to install the package to a drive or a path other than the default path.	

Step	Action
6	After the installation is complete, review the SnapManager for Microsoft Office SharePoint Server Agent configuration details. SMMOSS Control Service Address: Specify the host name or the IP address of the server where the SnapManager for Microsoft Office SharePoint Server Control Service is installed. SMMOSS Control Service Port: This is the port used for communication with the Control Service and should match the information provided during the Manager configuration. By default, this value is 12000. SMMOSS Agent Address: Specify the current server's host name, IP address or fully qualified domain name (FQDN). SMMOSS Agent Port: The port specified here is used by the Manager or other Agents for communication. By default, its value is 10103. User Account: Specify the agent account under which the Agent activities are performed. The detailed permissions are as follows: † On the Control Agent, an account with Farm Admin permissions and ViewServerState permission on SQL server is required. † On the SQL Member Agent, an account with DBO permission to SharePoint databases is required. In both the Agent types, local administrator rights is recommended. Agent Type: The Control Agent must be installed on the SharePoint front-end Web server, and the SnapManager for Microsoft Office SharePoint Server Member Agent must be installed on the SQL database server. It is recommended that the Member Agent is installed on the SharePoint index server and the front-end server as well. At least one Control Agent and one Member Agent are required, but these can reside on the same box if the above conditions are met.

Step	Action
7	Change the settings according to your needs and click Next. Note_____ It is recommended that you use the default settings unless a known conflict with an existing port exists. _____
8	Click Finish to exit SnapManager for Microsoft Office SharePoint Server Agent Install Wizard.

This section describes how to upgrade the SnapManager for Microsoft Office SharePoint Server Manager and Agents. The following topics are covered:

- † [“Upgrading SnapManager for Microsoft Office SharePoint Server Manager”](#)
- † [“Upgrading SnapManager for Microsoft Office SharePoint Server Agent”](#)

Upgrading SnapManager for Microsoft Office SharePoint Server Manager

Preparing to upgrade

Before upgrading your SnapManager for Microsoft Office SharePoint Server Manager, we recommend performing a System Recovery backup for rollback purposes. See the previous *SnapManager for Microsoft Office SharePoint Server Installation and Administration Guide*.

Note

This option is only available in SnapManager for Microsoft Office SharePoint Server 1.1 and later.

Upgrade steps

To upgrade SnapManager for Microsoft Office SharePoint Server Manager, complete the following steps.

Step	Action	
1	Install the software from the CD-ROM or download it.	
	If...	Then...
	You are obtaining the software from the network	1. Download the SnapManager for Microsoft Office SharePoint Server Manager package from the network. 2. Save it on the Windows host system. 3. Launch the SnapManager for Microsoft Office SharePoint Server Manager installation package by double-clicking setup.exe in the Explorer window.
	You are installing the software from the CD-ROM	Browse to the SnapManager for Microsoft Office SharePoint Server Manager installation package and double-click setup.exe.
2	A pop-up window appears and prompt you to upgrade. Click Yes and the SnapManager for Microsoft Office SharePoint Server Manager Install Wizard launches.	

Step	Action
3	Click Next to begin the installation process.
4	Enter the desired User Name and Organization name in the Customer Information window. Click Next.
5	Click Install to begin the installation.
6	After the installation is complete, review the SnapManager for Microsoft Office SharePoint Server Manager configuration details. By default, the configuration information is the same as that of SnapManager 1.0 and later. For details on these fields, see the Manager installation instructions in the previous chapter. After you are satisfied with the configuration settings, click Next.
7	The installer will configure the SnapManager for Microsoft Office SharePoint Server Manager with the chosen name and port designations.
8	Click Finish to exit SnapManager for Microsoft Office SharePoint Server Manager Install Wizard.

Upgrading SnapManager for Microsoft Office SharePoint Server Agent

Upgrade steps

To upgrade the SnapManager for Microsoft Office SharePoint Server Agent, complete the following steps.

Step	Action	
1	Install the software from the CD-ROM or download it.	
	If...	Then...
	You are obtaining the software from the network	1. Download the SnapManager for Microsoft Office SharePoint Server Agent package from the network. 2. Save it on the Windows host system. 3. Launch the SnapManager for Microsoft Office SharePoint Server Agent installation package by double-clicking setup.exe in the Explorer window.
	You are installing the software from the CD-ROM	Browse to the SnapManager for Microsoft Office SharePoint Server Agent installation package and double-click setup.exe.
2	A pop-up window appears and prompts you to upgrade. Click Yes and the SnapManager for Microsoft Office SharePoint Server Agent Install Wizard launches.	
3	Click Next to begin the installation process.	
4	Enter the desired User Name and Organization name in the Customer Information window.	
5	Click Install to begin the installation.	
6	After the installation is complete, review the SnapManager for Microsoft Office SharePoint Server Agent configuration details. By default, the configuration information is the same as that of SnapManager 1.0 and later. For more information on these fields, see the Agent installation instructions in the previous section.	

Step	Action
7	After you are satisfied with the configuration settings, click Next.
8	Click Finish to exit SnapManager for Microsoft Office SharePoint Server Agent Install Wizard.

Verifying the installation

To verify the installation, complete the following steps.

Step	Action
1	Open the Services tool on the machine where SnapManager for Microsoft Office SharePoint Server Manager is installed. This is located under Administrative Tools of the Windows Control Panel.
2	Verify that the following services are listed and started: † SnapManager for Microsoft Office SharePoint Server Communication Service (Agent) † SnapManager for Microsoft Office SharePoint Server Control Service (Manager) † SnapManager for Microsoft Office SharePoint Server Media Service (Manager) † SnapManager for Microsoft Office SharePoint Server Web Service (Manager)
3	To change some configuration settings, for example, an address or a port number, use the Configuration tool. This tool is available for both the Manager and the Agent and is located in the SnapManager for SharePoint Server group in the Start menu of each machine.
4	To restart any of the services that are down, use the Restart Services tool, which is available for both the Manager and the Agent. This tool is located in the Programs folder for SnapManager for Microsoft Office SharePoint Server.
5	To ensure proper communication between SnapManager for Microsoft Office SharePoint Server Manager and Agent, the ports listed in the table below must be open and available if a firewall is in place.

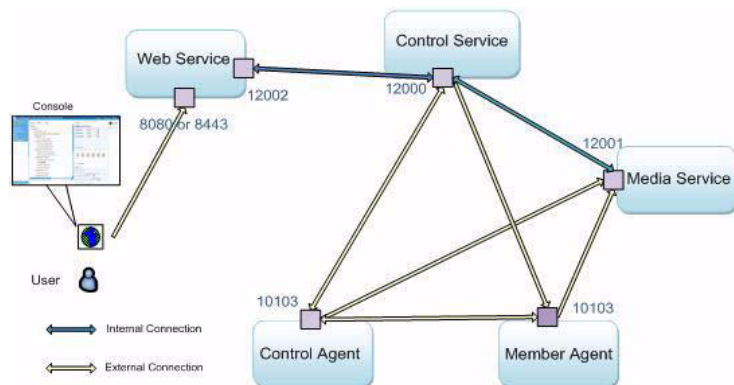
Ports used by SnapManager for Microsoft Office SharePoint Server Manager and Agent

The following ports should be open and available to ensure proper communication.

Component	Service name	Default port	Description	Public
Manager	Web Service	8080	Web server for the interface when HTTP is used	Y
		8443	Web server for the interface when HTTPS is selected	Y
		12002	Web Service communication port	N
	Control Service	10103	Control Service communication port	Y
	Media Service	12001	Media service control messages and data transfer port	Y
Agent	Communication Service	10103	Agent communication port	Y

Topology diagram for ports

The following diagram illustrates all the internal and external connections that are used.



Accessing the Server

To access SnapManager for Microsoft Office SharePoint Server, complete the following steps.

Step	Action
1	In the Internet Explorer address bar, enter the following: <i>http://machine:8080/smmoss</i> or <i>https://machine:8443/smmoss</i> Where <i>machine</i> is the host name or IP address of the machine running SnapManager for Microsoft Office SharePoint Server Manager, and <i>8080</i> or <i>8443</i> represents the Web Service port defined during the configuration of the Manager (which depends on whether HTTP or HTTPS is configured). Note_____ Another method to access SnapManager for Microsoft Office SharePoint Server is through the link titled Start SMMOSS for Manager Application. By default, this link is located in the Start menu on the machine containing SnapManager for Microsoft Office SharePoint Server Manager.
2	At the Login screen, select Local System, enter the initial login information and click Login. The initial login information is as follows: Login ID: admin Password: admin

Note_____

The ability to access the SnapManager for Microsoft Office SharePoint Server control panel should be limited to users with the highest level of administrative privileges.

Types of login modes

There are two kinds of login modes that you can specify:

Local User Login: A local user is also called a SnapManager for Microsoft Office SharePoint Server user; the local user should be created and added to a group first in the control panel. This account is pre-stored on the local database because the installation of the system is owned by the SnapManager for Microsoft Office SharePoint Server Administrators group, and cannot be deleted. When you log in as a local user, choose the Local System mode in the login page.

Active Directory (AD) User Login: This will make a separate domain available in the drop-down list where Local System is selected when you log in to the platform. If you want the system to support the domain user login mode, you need to first enter a domain user account during the SnapManager for Microsoft Office SharePoint Server Manager installation, or from the Manager Configuration Tool. After logging in to the Local System for the first time, you can add AD users to the platform to log in later.

See the Account Manager section of this guide for details on setting up new local users or adding AD users.

Uninstall steps

Both SnapManager for Microsoft Office SharePoint Server Manager and Agent can be removed using the Microsoft Windows Add or Remove Programs tool. To uninstall SnapManager for Microsoft Office SharePoint Server Manager and Agent, complete the following steps.

Step	Action
1	Open the Add or Remove Programs tool from the Windows Control Panel.
2	To uninstall SnapManager for Microsoft Office SharePoint Server Agent, locate the SnapManager for Microsoft Office SharePoint Server Agent entry, and click Remove.
3	To continue with the uninstalling of SnapManager for Microsoft Office SharePoint Server Agent, click Yes to verify removal, and SnapManager for Microsoft Office SharePoint Server Agent is removed.
4	To uninstall SnapManager for Microsoft Office SharePoint Server Manager, locate SnapManager for Microsoft Office SharePoint Server Manager, and click Remove.
5	To continue with the uninstalling of SnapManager for Microsoft Office SharePoint Server Manager, click Yes to verify removal, and SnapManager for Microsoft Office SharePoint Server Manager is removed.
6	To remove the configuration data, select the Remove the Configuration Data check box on the last screen of the uninstall interface (before clicking Finish). If the configuration data is not removed, it is possible to reinstall the same version of the SnapManager for Microsoft Office SharePoint Server Manager software and use the existing configurations. Note _____ The backup data from jobs managed by the Media Service is not deleted when you uninstall, even if the configurations are removed. You can manually delete these files from the system, if needed.

This chapter describes the following general administrative services available in SnapManager for Microsoft Office SharePoint Server:

- † “Control Service”
- † “Data Retention”
- † “Device Manager”
- † “Verification Server”
- † “Account Manager”
- † “System Recovery”
- † “Log Manager”
- † “E-mail Notification”
- † “License Manager”

Control Service

About Server Monitor

Server Monitor provides a central interface to monitor SnapManager for Microsoft Office SharePoint Server Media Service, Web Service, and Control Service. You can also view the Port information, the Hostname for the machine, product Version, and the Status for these services in the appropriate columns. The services are as follows:

- † SnapManager for Microsoft Office SharePoint Server Media Service is the component responsible for storing backup job data.
- † SnapManager for Microsoft Office SharePoint Server Web Service provides an interface for sessions opened through browser consoles.
- † SnapManager for Microsoft Office SharePoint Server Control Service maintains internal SnapManager for Microsoft Office SharePoint Server data such as backup plans and configurations, coordinates with the Agent during operations of this platform, maintains backup schedules, and performs other tasks relating to the management of this platform.

About Agent Monitor

Agent Monitor provides a central interface to monitor and restart multiple SnapManager for Microsoft Office SharePoint Server Agent hosts, and enables you to adjust other settings.

You can use the Restart, Disable, and Uninstall buttons under the Control column to perform the following functions:

Restart: This restarts SnapManger for Microsoft Office SharePoint Server Agent Service on the Agent machine (Communication Service). This does not reset all services, only those pertaining to this platform.

Disable: This suspends all backup or restore jobs corresponding to this Agent. All plans that were scheduled are skipped if an agent is disabled, but they will still be visible from all the modules.

Remove: This removes the specific Agent from SnapManager for Microsoft Office SharePoint Server Manager. The plans for this Agent no longer run and this Agent is not available from either the Backup or Restore modules. This also means that the Agent Monitor no longer shows this agent in the interface. This option should be used in only in instances when uninstalling an Agent does not remove it from the Agent Monitor.

Configure: To configure the Agent information, complete the following steps.

Step	Action
1	Click Configure and a window pops up.
2	On the top-left of the pop-up window, select the log level from the drop-down list. There are four options: Error, Warn, Info and Debug. The default option is Info. Note_____ When troubleshooting issues, the recommended setting for the log level is Debug. _____
3	On the bottom-left of the interface, select the Account Configuration you want to use to connect to the SharePoint environment. Local System Account: This is typically only used in instances of an “all in one” configuration with the SharePoint front-end Web and the SQL Server installed on the same server. It is not the recommended option. This Account: This is the default option, and uses the Domain Name, User Name, and Password specified when installing the Agent. The Control Agent account should be a Farm administrator and should have the server status permission in SQL. The SQL Member Agent should have database operator (DBO) permissions to the SharePoint database.
4	The Cache Location Setting section in the configuration window enables you to specify a temporary location for use during backup and restore jobs. The default location is on the SnapManager for Microsoft Office SharePoint Server Agent host machine: <SMMOSS Installation Directory>\Agent\temp This data is typically small in size, but varies based on deployment.
5	After modifying any of the fields described in the previous steps, click Save. Click Cancel if you do not want to keep your changes.

Data Retention

About Data Retention

The Data Retention component of SnapManager for Microsoft Office SharePoint Server enables you to define data retention and expiration policies. Retention policies are a method of pruning old backup data to make room for new backups. A Data Retention Rule specifies the number of backup process cycles that trigger data pruning as well as the number of backup sets to keep of a given backup management group.

To specify a data retention rule, complete the following steps.

Step	Action
1	Enter a data retention Profile Name in the field provided.
2	Enter the number of backups to run before data retention begins to prune data and the type of backup management group to prune. For example, if you set the data retention rule to '2 weeks', only the two newest backup sets of type 'weekly' will be kept.
3	Click Save, located on the bottom of the screen. The profile appears on the right of the screen. You can click the title of this profile later to modify it, or use the red 'X' sign to delete it.
4	After saving your data retention rule, you can select it from the Backup Builder module.

Device Manager

Overview

In SnapManager for Microsoft Office SharePoint Server, by default, backup data is saved under the path:

```
C:\Program Files\NetApp\SnapManager for SharePoint Server\VaultServer\
SMMOSSMedia\data
```

The SharePoint databases and SharePoint index are stored in the storage system as Snapshot copies, but the following data is stored in the physical device:

- † Job metadata
- † Backup index
- † SharePoint component properties
- † SharePoint solutions
- † SharePoint front-end resources

As large amounts of index data can be generated in some environments, you should store the index data on a separate drive, typically a LUN. Under Device Manager, you can specify a Physical Drive (either a local and network shared drive) for storage location.

Data Manager also enable you to see the Hostname, Port, Status, and other information regarding Media Services.

Creating a local device

To create a local device, complete the following steps.

Step	Action
1	Input a name for the new device in the Device Name text box on the right.
2	Select the Local option from the Device Type drop-down list.

Step	Action
3	Input a valid path. Note_____ If the path does not exist in the system, it will create the path automatically. For example, if the backup path is set to “d:\backupdata,” and there is no “backupdata” folder on the ‘d’ drive, the folder will be created automatically after the storage drive is saved. _____
4	Click Test on the bottom of the screen to test the new device. If the information set is valid, a window pops up to confirm that the test is successful.
5	Click Save to save the profile for the new physical device. It is listed under the Physical Device column on the left.

Creating a network device

The Device Manager can also use a network path to build a network drive to any UNC path accessible from SnapManager for Microsoft Office SharePoint Server Manager. To create a network device, complete the following steps.

Step	Action
1	Input a name for the new device in the Device Name text box on the right.
2	Select the Network option from the Device Type drop-down list.
3	Enter a UNC path in the format: \\<server>\<share>\<path>. Note_____ The specified path needs to exist already; a new path will not be created automatically. _____
4	Input the Username, Domain, and Password to set up access to the network path.
5	Click the Test button on the bottom to test the new device. If the information set in the previous steps is valid and the path exists, a window pops up to confirm that the test is successful.

Step	Action
6	Click Save to save the profile for the new physical device. It is then listed under the Physical Device columns on the left.

Storing data on a LUN

To put the previously mentioned data on a LUN, complete the following steps.

Step	Action
1	Input a name for the new device in the Device Name text box on the right.
2	Select the Local option from the Device Type drop-down list.
3	Input a valid path on the LUN. Note _____If the LUN of the path you entered has SnapMirror enabled, SnapManager for Microsoft Office SharePoint Server automatically updates SnapMirror after finishing any backup job.
4	Click the Test button on the bottom to test the new device. If the information set is valid, a window pops up to confirm that the test is successful.
5	Click Save to save the profile for the new physical device. It is then listed under the Physical Device column.

Note_____You should use a LUN with SnapMirror enabled. This automatically replicates all related data to the SnapMirror target site for disaster recovery (DR) situations automatically. If you use a regular storage location or UNC path without SnapMirror enabled, you have to move the backup data to a remote site manually for DR protection.

Deleting a device

To delete a device, select a device from the drive list and click the red 'X' sign or the Delete button to remove it. There must always be at least one drive in the Physical Device column.

Note

If there is backup data stored in the device that you are deleting, a warning message is displayed. However, only the link between the path and the Media Service is removed; the actual data is not deleted and can be restored at a later time by re-creating the device.

Verification Server

Defining a Verification Server

You can define a Verification Server to be used in Backup Builder Module or Restore Controller Module for verifying SQL databases using SnapManager for SQL Server.

To define or create a Verification Server profile, complete the following steps.

Step	Action
1	Enter a Profile Name in the space provided at the top of the Verification Server interface.
2	Input an SQL Server to be used as Verification Server in the Server Name field. Note_____ SnapManager for SQL Server should be installed on this SQL Server and an SQL virtual server should not be used in an Microsoft Cluster Service (MSCS) environment.
3	Select an authentication from the corresponding drop-down list. You can select either Windows Authentication or SQL Server Authentication. If you select the SQL Server Authentication option, enter the User Name and the Password of the SQL Server in the corresponding fields.
4	Click Save to save the profile.

After saving your verification server rule, you can select it from the verification server section of the Backup Builder and Restore Controller modules.

For pre-existing profiles, you can edit the information by clicking the name on the right side of the screen. After editing any information, click Save to save the changes. You can also delete a pre-existing profile by using the red ‘X’ sign next to the name in the profile list.

Account Manager

Overview

In SnapManager for Microsoft Office SharePoint Server, you can create users and assign specific rights to the users. Account Manager enables you to easily control and maintain the access rights to SnapManager for Microsoft Office SharePoint Server from a central point, which ensures the integrity of the account. You can add users to certain groups that are categorized by specific permissions. The following paragraphs describe the use of SnapManager for Microsoft Office SharePoint Server's Account Manager.

About users

To log in and use SnapManager for Microsoft Office SharePoint Server, a Username and corresponding Password is needed. The default system has only one user name and password named admin and admin, respectively. The admin user has full rights and this account cannot be deleted, though the password and information can be edited. Logging in as the administrator user enables you to create other users and assign specific rights to those new users. New users can also have the same rights as an administrator or they can be restricted from certain actions by limiting their rights.

Note

You cannot directly assign rights to an individual user. You must first create a group and assign some rights to that group. After adding a user to that group, you can assign the corresponding rights to the user.

About groups

You can create groups in SnapManager for Microsoft Office SharePoint Server and assign a series of rights to the group. You can then add specific users to a certain group. This is the only way you can assign rights to users.

There are several built-in groups, including Administrators, Managers, and Operators. These have pre-defined permission levels and cannot be deleted. SnapManager for Microsoft Office SharePoint Server administrators have full access rights to the Account Manager (view and update) and can view all the items in the Control Panel.

Two types of groups can be created: local groups and AD groups. A local group is managed within SnapManager for Microsoft Office SharePoint Server only. An AD group is defined and maintained in Active Directory. To use an AD

group, a domain user account must be specified during the installation of SnapManager for Microsoft Office SharePoint Server Manager, or through the Manager Configuration Tool.

You can view all members in a local group by clicking the Members tab when the group is selected from the list. This is not available for AD groups.

Creating a new group

To create a new group or add an AD group, complete the following steps.

Step	Action
1	Click the Account Manager tab on the left of the window.
2	Click the Add Group icon () and a window pops up where you can add a new group. By default, a local group is created. An AD group can also be added by using the AD radio button. When an AD group is defined, all AD users in that group can log in to the SnapManager for Microsoft Office SharePoint Server platform and perform actions as allowed by that AD group's permissions.
3	Input the group name and a brief description of this group. If you are adding a pre-existing AD group, you can use the Find button to locate the name specified.
4	Click Save to save the group.

All the groups created or added in the Account Manager are added to the User Defined tab on the left, represented by a group icon in the Account Type column. For a list of groups pre-defined by SnapManager for Microsoft Office SharePoint Server (including the Administrators group), click the System Defined tab.

Assigning permissions to a group

After a group is created, you must define its permissions. Permissions are separated into two groups: the permission to access the backup and restore controllers and the permission to access or view the Control Panel.

To change the access rights of a group, complete the following steps.

Step	Action
1	Click the Group name on the list on the left to load the group's information.
2	Click the Permission tab under the group name on the right. There are two tabs under the Permissions tab.
3	Click the MOSS 2007 tab. This shows the permissions for Backup Builder and Restore Controller. Check if the group should have permission to either of these, or use the Select All and Clear buttons on the bottom of the interface.
4	Click the Control Panel tab to set the permissions for the available actions. For each permission item, you have at least two options: View and Update. Some items have a third option: Control. Control enables the user to take action from these modules (that is, restart services on an Agent). Choose which permissions to apply, or use the Select All and Clear buttons on the bottom.
5	Click Apply to assign the selected permissions to this group.

Note

Be aware that only the user in a group with the right to update Account Manager has the right to use Account Manager to edit other users and groups profiles. The users in SnapManager Administrators group have the right to update the Account Manager. Therefore, the members of the SnapManager Administrators group have the right to edit other users and groups profiles.

Creating a new local user

To add a new user to a previously created group, complete the following steps.

Step	Action
1	Click the Add Users icon () and a window pops up to add a new user. By default, the Local radio button is selected.
2	Input a User name, Password, Confirm Password and E-mail in the text boxes provided. Click Save to save the user, or click Cancel to cancel the configuration. If you save the user, the user appears under the User Defined tab on the left.

All users created in the Account Manager are added to the User Defined tab on the left, represented by a single-user icon in the Account Type column.

Note

The Admin user is the only pre-defined SnapManager for Microsoft Office SharePoint Server user and cannot be removed. To edit the password for this account, click the System Defined tab and click the Admin entry.

Adding a new AD user

To add an AD user, complete the following steps.

Step	Action
1	Click the Add Users and a window pops up where you can add a new user.
2	Click the AD radio button.
3	Enter the Username and click Find to find the user.
4	Choose to make them a member of a pre-existing group using the drop-down list.
5	Click Save to save the user, or click Cancel to cancel the configuration.

Editing a user or a group

To edit a user or group's attributes, click the corresponding name on the left, and the detailed information appears on the right of the screen. Modify the information, and click Save to save the modification.

Deleting a user or a group

To delete a user or group, click the red 'X' sign or Delete icon next to the name on the right. Note that the system-defined accounts and users cannot be removed.

System Recovery

Overview

SnapManager for Microsoft Office SharePoint Server System Recovery enables you to set up a manual or automatic backup job for the SnapManager for Microsoft Office SharePoint Server system and then restore the system when needed. SnapManager for Microsoft Office SharePoint Server System Recovery can also be used to configure a new SnapManager for Microsoft Office SharePoint Server deployment.

There are two parts in the SnapManager for Microsoft Office SharePoint Server System Recovery: System Backup and System Restore.

System Backup

The System Backup tab enables you to execute a backup job of the system settings in this SnapManager for Microsoft Office SharePoint Server deployment. System Backup saves the system settings into a flat file to the location defined under backup destination. Before a backup job can be executed, the backup schedule and backup destination settings must be configured.

To perform a backup, complete the following steps.

Step	Action
1	Specify the location where the System Recovery backup job file should be stored by selecting either Local Drive or Network Drive. The Local Drive option stores data locally in the SnapManager for Microsoft Office SharePoint Server Control Service machine.
2	If you select Local Drive, you need to input a path such as “C:\data”. The default path is “C:\Program Files\NetApp\SnapManager for SharePoint Server\SMMOSSData”.
3	If you select Network Drive, you need to input a path in standard UNC or “\\server\data” format. On the network drive, input the domain name, a user name, and password with write permissions.

Step	Action
4	You can specify a LUN for these options. If the LUN is SnapMirror enabled, system backup data will be automatically replicated to the SnapMirror destination after a system backup job is completed. If you intend to keep a copy of the system recovery backup data on another location for disaster recovery purposes, you will need to manually copy the backup data to a remote site. For this reason, you should set this destination to a LUN with SnapMirror enabled.

To set up the backup schedule, complete the following steps.

Step	Action
1	Select the “Enable Schedule” check box to activate the backup schedule. This is not required if you only intend to create a manual backup. Note that you can only specify one schedule.
2	Click the calendar icon next to the Start Time field and a calendar opens. Use the calendar to specify when the backup should begin.
3	Specify the interval at which an automatic or recurring backup should occur: Only Once, By Hour, By Day, By Week, or By Month.

To test the settings, complete the following steps.

Step	Action
1	After specifying the backup destination, click the Test Drive button. If there is no problem accessing the backup location, you receive a ‘Test Drive OK’ message. Otherwise, an alert window prompts you to check the backup drive and try again.
2	Click Save and Run Now to execute the backup job, or click Save to save the backup plan to run at a later scheduled time and date. If the backup job is saved, it will be reloaded the next time this interface is opened.

Monitoring a Backup Job: After finishing the backup job, you can monitor it through the Backup Job Report at the bottom of the GUI. Click the green arrow on the right of the tool bar to expand and collapse this. The report includes the Start Time, the backup Path, the User who initiated the job, the Status, the backup Data Size, and the Progress. You can delete the job report by clicking the Delete button.

System Restore

After the backup is completed, it is listed with the Backup Time in the System Restore Job browser. You can restore to any point-in-time by choosing the radio button next to the appropriate job and clicking the Restore button.

Because the system settings are backed up to a file, the backup file can be physically transported and restored to a new SnapManager Server in a disaster recovery scenario. To restore the backup plans and SnapManager Control Panel profiles to a new SnapManager Server, use the System Backup File browser on the new machine to load the backup file. Click Restore to begin the restore process after selecting a file.

Note

Because the system settings are highly coupled with the topology of the environment, the new environment should have the same topology for the restored system settings to work as before.

Monitoring a restore job: You can monitor the restore job through Restore Job Report. The report includes the Start Time, the Path the data is loaded from, the User who initiated it, the Status, the Data Size restored, and the Progress. You can delete the job report by clicking the Delete button.

Note

In case multiple users are logged on to SnapManager for Microsoft Office SharePoint Server System during a System Restore, when other users attempt any type of operation during the system restore, SnapManager for Microsoft Office SharePoint Server displays a message stating that a system restore is executing.

Log Manager

About Log Manager

SnapManager for Microsoft Office SharePoint Server Log Manager provides several options for managing the logs associated with the SnapManager for Microsoft Office SharePoint Server components. Logs are stored as:

System logs: These include all actions performed under SnapManager for Microsoft Office SharePoint Server Manager services. These are stored in the internal Manager databases and can be viewed from Job Monitor > Log Viewer.

Manager logs: Detailed log files of each Manager service are stored on the Manager machine.

Agent logs: Detailed logs of each Agent are stored on the Agent machine's event viewer called "SMMOSS".

You can set the amount of logs to record from the Log Level Setting panel and the number of system log entries to retain from the System Log Setting panel. Additionally, you can send these logs from the E-mail Notification Settings panel.

Downloading logs

Log Data Download is used to centrally download logs from multiple SnapManager for Microsoft Office SharePoint Server components, including the Control, Media, and Web services, as well as any Agents. Select all agents or services that you require logs from and click Download. You can save the consolidated zip file to any destination you choose.

Pruning logs with System Log Setting

System Log Setting is used to specify the maximum Log count for the SnapManager for Microsoft Office SharePoint Server system log to keep on the system. By default, 5000 logs are kept, but you can change this number and click Apply to save the setting. If the specified value is smaller than the current log size, all older log messages are pruned.

Setting log levels

Log Level Settings are used to set log levels for log recording for the following services:

- † SnapManager for Microsoft Office SharePoint Server Web Service
- † SnapManager for Microsoft Office SharePoint Server Media Service

† SnapManager for Microsoft Office SharePoint Server Control Service

To make these changes, choose one of the services from the drop-down list and the appropriate log level setting (either Debug, Info, Warning, Error, or Fatal). Click Apply to save your changes. Because there is only one Control Service, you do not need to select a service to apply the new setting.

Note

To change the log level of an Agent, use the Agent configuration page in the Agent Monitor.

Setting up e-mail notification

You can use E-mail Notification Settings to send the logs to a specified recipient directly from the GUI. Within the panel you can add a subject or write a description for the log.

E-mail Notification

Overview

The E-mail Notification manager enables you to create various e-mail profiles containing different mailing lists. Backup plans can then be configured to e-mail different profiles for error, success, or warning conditions. This enables you to effectively control which personnel gets notified under which conditions.

E-mail Notification also enables you to specify what is reported, from simple summary reports to detailed URL-specific reports. The e-mail report sent out from SnapManager for Microsoft Office SharePoint displays the backup status and the reason for failure if the backup job fails.

Configuring a mailing list profile

To configure a mailing list profile, complete the following steps.

Step	Action
1	Input the E-mail notification name.
2	Enter your POP3 or Microsoft Exchange Outgoing Mail Server (SMTP) address.
3	Specify a port. The default port is 25.
4	Under the Sender field, enter the e-mail address you want to use as the source of the e-mail notifications, as well as the login credentials for this address (Username, Password, Confirm password) in the applicable fields.
5	Enter the e-mail recipients under the Summary Report Recipients and Detailed Report Recipients. Note _____ Multiple recipients can be added to the recipient text box, separated by a semicolon “;”. _____

Step	Action
6	Select a notification level from both “Summary Report Notification Level” and “Detailed Report Notification Level”: either All Levels, Success, Failure or Warning. Depending on the results of each job, these reports are sent out according to the level set here. Note _____ Notification levels can be customized by profile. For instance, you might want a specific person or group of people to only receive reports for backups that have failed. You can manage this by adding a new e-mail notification for each person or group based on their needs.
7	Select the format in which the message will be delivered: HTML or Plain Text.
8	Select the Send All Logs to Recipient check box if you want to see all error logs when a job has failed. These are not included for successful jobs.
9	Click the Test button to ensure that your notification profile is configured properly. All e-mail recipients entered in the Summary and Detailed Report fields receive a test message from the e-mail address you specified in the Sender field.
10	Click Save As, create a notification name for this profile, and click OK. The new profile is added to the list on the right of the screen. All e-mail notification profiles are selectable from the Backup Builder module.
11	To modify a profile, click the name of the profile in the list on the left. It is loaded in the fields on the right. After you finish your modifications, click Save. If you want to clear the configuration, click Clear.

License Manager

Overview

SnapManager for Microsoft Office SharePoint Server License Manager controls the license that is in use by SnapManager for Microsoft Office SharePoint Server. The license controls the number of agents available as well as the version of SnapManager for Microsoft Office SharePoint Server. Applying a full enterprise edition license to a SnapManager for Microsoft Office SharePoint Server Demo Server Package converts the demonstration package into the full enterprise edition.

Note

By default, each license of SnapManager for Microsoft Office SharePoint Server allows the registration of five member agents, which can be deployed on either SQL servers, SharePoint index servers, or SharePoint front-end Web servers. Additional member agents can be purchased to expand the capability.

Viewing current license information

To view the permissions granted in the current license, open License Manager under Control Panel. By selecting the various features and solutions SnapManager for Microsoft Office SharePoint Server provides from the list on the left of the interface, you can view all information.

Applying a license file

To apply a license file, complete the following steps.

Step	Action
1	Click Browse and locate the license file you want to import.
2	Click Apply to load the selected license file.
3	For the license update to take effect, you have to re-login to the SnapManager for Microsoft Office SharePoint Server interface.

Planning for volumes and LUNs in NetApp storage

It is important to understand the implications of NetApp storage volume and LUN during the backup and restore process. During the backup process, a Snapshot backup is created for SharePoint databases and SharePoint search index files located in a NetApp storage volume. The backup set can contain one or multiple Data ONTAP® LUNs with multiple databases.

If a LUN in a backup set contains multiple databases but only a subset of databases needs to be restored, a stream-based database restore is performed. If all databases contained in the LUN are restored, the LUN restore is performed (which is more efficient than the stream-based method). For optimal restore speed, this means that each database should ideally be on its own LUN. However, depending on the number of databases, this is not always possible because of the maximum number of LUNs that the system can have. In that case, putting the large database on its own LUN, and keeping other related databases on the same LUN (that is, the content databases pertaining to one SharePoint Web application) are the preferred methods.

For the SharePoint search index, a similar recommendation applies. It is recommended that the SharePoint index for each SharePoint Shared Services Provider (SSP) reside on its own dedicated LUN. If the SharePoint search index is not the only folder on the LUN, the stream-based restore is used.

During backup, SharePoint databases use SnapManager for Microsoft SQL Server to generate the Snapshot backup, and the SharePoint search index LUNs use SnapDrive to generate the Snapshot backup. To minimize the number of snapshots created during backup, it is recommended to use different volumes for database LUNs and search index LUNs.

Note

If SharePoint databases share a LUN with SQL Server system databases, only stream-based backup and restore can be utilized. SnapManager for Microsoft Office SharePoint Server does not support this configuration. Always put SharePoint databases on different LUNs different from the SQL server system database LUN.

For more information, see the *SnapManager for Microsoft SQL Server Installation and Administration Guide*.

Database and index migration

Database migration SharePoint databases must be located on Data ONTAP storage systems (LUNs) to be backed up by SnapManager for Microsoft Office SharePoint Server. If SharePoint databases are not located on Data ONTAP storage systems, they need to be migrated to Data ONTAP storage systems. SnapManager for Microsoft SQL Server needs to be used to perform these operations. SMMOSSDBTool can also be used to facilitate this process. This tool is included in the SnapManager for Microsoft Office SharePoint Server Agent installation, and can be used to attach and detach SharePoint related databases for migration onto Data ONTAP storage systems.

Finding SharePoint databases To find the SharePoint databases that need to be migrated onto the Data ONTAP storage system, you can use the `listdbs` command under SMMOSSDBTool. To list the databases using SMMOSSDBTool, execute the following command on the SharePoint front-end Web server:

```
%PROGRAMFILES%\NetApp\SnapManager for SharePoint  
Server\VaultClient\bin\SMMOSSDBtool.exe -cmd listdbs
```

Initial migration SharePoint services access SharePoint databases constantly. For the initial database migration onto the Data ONTAP storage system, it is recommended that you shut down SharePoint related services on all SharePoint servers before the migration. The SharePoint related services include the following:

- † World Wide Web Publishing Service
- † Windows SharePoint Services Administration
- † Windows SharePoint Services Timer
- † Windows SharePoint Services Search
- † Office SharePoint Server Search
- † Microsoft Single Sign-on Service

You can start these services again after the database migration is complete.

Migrating a content database

After the initial migration process is done, a content database might need to be moved to a LUN located on a NetApp Storage system. Because SharePoint can access the content database during the move process, you can use SMMOSSDBTool to temporarily detach (`detachdb` command) the content database from SharePoint and re-attach it (`reattachdb` command) after the operation is complete.

To detach the database, enter the following command on the SharePoint front-end web Server:

```
%PROGRAMFILES%\NetApp\SnapManager for SharePoint  
Server\VaultClient\bin\SMMOSSDBtool.exe -cmd detachdb -dbserver  
server[\instance] -db dbname -statefile filepath
```

where *Server[\instance]* represents the database location, *dbname* is the name of the database, and *filepath* is the location and file name for the database state information that is saved.

To re-attach the database to SharePoint, enter the following command on the SharePoint front-end web:

```
%PROGRAMFILES%\NetApp\SnapManager for SharePoint  
Server\VaultClient\bin\SMMOSSDBtool.exe -cmd reattachdb -statefile  
filepath
```

Where *filepath* is the location and file that contains the last state information of the database before it was detached.

Note

You must ensure that there is no activity on the database before detaching. If SMMOSSDBTool detects that there are open connections to the content database, it will not detach the database. If you are sure that there is no activity on the content database, you can specify the `closedbconnections` option to force the detach operation to proceed. To use the `closedbconnections` option, add `closedbconnections` to the end of the detach database command specified previously.

Creating a new content database

To create a new content database, create a new empty SQL database using the 'LATIN1_General_CI_AS_KS_WS' collation and move it onto the Data ONTAP storage system. Then in Microsoft SharePoint, choose to create new content databases and point to the pre-created databases. For more information regarding this option, consult the Microsoft SharePoint documentation. This is the recommended approach to create new content databases.

Migrating the SharePoint OSearch and SPSearch index files to LUN

To migrate the index files of Office SharePoint Server Search (OSearch) and Windows SharePoint Services Search (SPSearch) to LUN, you can use the command under SMMOSSIndexTool. To migrate the index files using SMMOSSIndexTool, execute the following command from your SharePoint index server:

```
%PROGRAMFILES%\NetApp\SnapManager for SharePoint  
Server\VaultClient\bin\SMMOSSIndexTool.EXE [-o|-s] [-ssp sspname] -  
d mountpoint
```

Where *-o* is the path of the Office SharePoint Server Search (OSearch) index files, *-s* is the path of the Windows SharePoint Services Help Search (SPSearch) index files, and *-ssp sspname* is the name of the specific ssp, and *-d mountpoint* is the destination of the index files.

Note

The *-ssp sspname* flag is only needed when the *-o* option is used. If this parameter is not specified, all SSPs are processed.

Deploying SharePoint with DBA-created databases

If the Data ONTAP storage system has already been allocated, but the SharePoint environment has not been created, the SharePoint databases can be set up first and then SharePoint can be deployed using the DBA-created databases later. For instructions, go to the following Microsoft site:

<http://technet2.microsoft.com/Office/en-us/library/798aa915-7025-4adc-a210-4f6ff14c43fc1033.mspx?mfr=true>

Overview of backup

SnapManager for Microsoft Office SharePoint Server provides full SharePoint farm-level backup and restore for different levels of SharePoint components from a single document version to the entire farm.

The SharePoint components covered are:

- † All SharePoint databases
- † SharePoint search index
- † SharePoint Web applications, SSP, SSO settings
- † SharePoint solutions
- † SharePoint front-end resources (including IIS sites and the SharePoint hive)

SnapManager for Microsoft SQL Server is used to perform database Snapshot backups, SnapDrive is used to perform Snapshot backups of search index, and backup data of other SharePoint component is sent to the SnapManager for Microsoft Office SharePoint Server Media Service, stored together with backup job metadata and index.

For Disaster Recovery purposes, this backup data can be replicated to a SnapMirror destination volume automatically. For longer retention of the backup data, database backups can be archived to a SnapVault destination when Protection Manager is configured for SnapManager for Microsoft SQL Server.

General actions you can perform

From SnapManager for Microsoft Office SharePoint Server Backup Builder, you can perform the following actions:

- † Set up scheduled or immediate backups for any SharePoint environment (as long as SnapManager for Microsoft Office SharePoint Server Agents are installed)
- † Select e-mail notifications created in the Control Panel's E-mail Notification manager
- † Choose a designated SnapManager media server to manage backup work
- † Monitor real-time progress of any backup or restore jobs (through the Job Monitor)

Plan options you can specify

SnapManager operates on the concept of backup plans, where each backup plan allows you to specify the following:

- † What SharePoint components to back up through a tree view of the farm

- † When to perform backups (up to six schedules can be customized per plan)
- † Where to store backup data (through Media Services which then writes data to the designated network, local disk drives or LUNs)
- † How to handle backing up data in terms of data retention or restore granularity level

SnapManager backup plans do not lock up SharePoint SQL database and index files, and therefore can be scheduled to run during normal production hours.

Verifying the SharePoint storage layout

To verify the SharePoint storage layout, complete the following steps.

Step	Action
1	Expand the SharePoint farm tree by selecting an agent from the Agent Host drop-down list.
2	Click the SnapManager for Microsoft Office SharePoint Server Agent name. By default, the Verify Storage Layout option is selected, which means that the SnapManager for Microsoft Office SharePoint Server tries to obtain information for all the database and search index components regarding storage from SnapManager for Microsoft SQL Server and SnapDrive, respectively. Sometimes this process might take a while to complete depending on the number of databases on the SQL servers. When the Verify Storage Layout option is not selected, SnapManager will retrieve only the farm tree structure from SharePoint, which means that the farm tree loads faster. However, because the storage layout is unknown in this case, you must ensure that all the components are correctly configured on the LUN. A warning appears if a component with unknown storage layout is included in backup plan.

When the Verify Storage Layout option is selected, some special icons are displayed to indicate the storage status, as shown in the following table.

Type	Database	Index
In LUN with SnapMirror and SnapVault enabled		N/A
In LUN with SnapMirror enabled		
In LUN with SnapVault enabled		N/A
In LUN		
Invalid		
Unknown		
No Agent is installed, the database cannot be backed up		N/A

Common backup option profiles

When you are constructing a new backup plan, there are many options that can be configured. Some of the options available here should be configured ahead of time in the Control Panel.

To configure a backup, complete the following steps.

Step	Action
1	Click the drop-down box to specify an Agent Host. The drop-down box contains a list of SnapManager for Microsoft Office SharePoint Server Control Agents currently connected to the Manager. The Control Agent represents the SharePoint front-end Web Server where SnapManager retrieves the farm structure for the tree (from which you can select the data to be backed up).
2	Specify a Media Service from the drop-down box under the Backup tab. This contains a list of all Media Services that designate where the backup data is stored. For more information about configuring the location for backup data, see the Device Manager section within the Control Panel.
3	Select an E-mail Notification profile from the drop-down box. The E-mail Notification drop-down box contains a list of profiles that have been associated with both a sender and a list of recipients. These profiles are set in the E-mail Notification section within the Control Panel. Specifying an E-mail Notification profile is optional.
4	Select a data retention rule from the corresponding drop-down box. The Data Retention policies enable you to specify the pruning policy for the data generated by this backup plan. By picking a data retention profile, you can specify how long the data generated by this plan is kept on the disk. Specifying data retention profile is optional but highly recommended. Note _____ A SharePoint component can be saved in multiple backup plans, but the retention type (Backups, Days, Weeks, and so on) must be different.

About data retention

Retention of backup data is configured based on the number of backups or the amount of time to keep backup data, and is automatically triggered when a backup job is completed that fits the pre-set criteria.

When a retention policy is configured, SnapManager for Microsoft Office SharePoint Server checks with SnapManager for Microsoft SQL Server to see if a local or remote copy of that Snapshot backup set still exists (the remote instance is only when SnapVault is used). If a copy of the backup data still exists, the metadata and index for this plan are not be deleted. In this way, you can always browse backup data and restore even if local backups are deleted due to retention. After both the local and remote backups are deleted, the corresponding backup data information in SnapManager for Microsoft Office SharePoint Server is deleted as well.

Retention of backup sets is dependent on a combination of databases. This can create problems when a backup set contains multiple databases. For example, suppose a backup set contains three databases db1, db2, and db3. The retention policy is configured to keep the three most recent backup sets (DbSet1, DbSet2, and DbSet3). Each time the three databases are backed up as a set, a new backup set (DbSet4) is created and the oldest backup set (DbSet1) is deleted.

However, if db2 is deleted, the next backup set contains only two databases (db1 and db3). As a result of this inconsistency the retention policy, which automatically keeps only the three most recent backups and deletes the older ones, does not work. Therefore to delete the older backups, you need to explicitly delete the backup data. This can be done by deleting the related backup jobs from Job Monitor, which deletes the backup job information as well as the Snapshot backup of the database and index.

For more information about the retention details when multiple databases are involved, see the *SnapManager for Microsoft SQL Server Installation and Administration Guide*.

Creating a backup plan

After completing the configuration of the common backup options in the Control Panel, proceed to the Backup Builder to create a backup plan.

Step	Action
1	Enter a Plan Name in the provided field.
2	Select an Agent Host. The Agent Host name reflects the machine name of the server from which to extract data to be backed up. The name of the agent host selected is displayed in the Backup Builder below the common settings, ready for browsing.

Step	Action
3	Click the name of the selected agent host. This expands the host to display the SharePoint farm structure, including the various SharePoint components such as SSP, Web applications, content databases and front-end server resources. There is a check box corresponding to each SharePoint component on the Backup Builder tree. Selecting this box indicates that the component is to be included in the backup plan. Select the check-boxes for the components to be included in this plan.

Note

The selected databases and search index must be in NetApp Storage. If the storage layout for a selected component is unknown, the Verify Storage Layout option has not been selected, or the Manager failed to obtain its status, a window pops up to remind you that the selected component should be in a storage system.

Setting up the backup schedules

After selecting the components to be backed up and selecting any maintenance options you might need, you can determine when and at what frequency the backup job plan should run. You can select multiple schedules, accessed by cycling through the schedule clocks. Select the Schedule check box to activate a new schedule. An active schedule is highlighted in blue, and inactive schedules are in yellow. You can also see the schedule name (A - F) beneath the clocks.

There are several options available under the Data tab of the schedule:

Verify Backup: If you select this option, the Verify On Available SnapMirror Destination Volumes and the Verify Archive Backup On Secondary Storage check boxes are activated. If your environment has SnapMirror enabled, you can select this option to verify both the data in the source and the data that is mirrored to the destination. Select a verification server from the drop-down list, defined in the Control Panel.

Update SnapMirror After Operation: If your environment has SnapMirror enabled for databases and the search index, you can select this option to automatically update the SnapMirror destination after backup. Only the default SnapMirror target is updated.

Archive Backup to Secondary Storage: If your environment has SnapVault enabled for databases, you can select this option to archive the backup data to the SnapVault storage system.

Restore Granularity Level: This option enables you to set the level of granularity on restore. Choosing the Item or Item Version level enables you to restore individual files and file versions. Different restore granularity levels can be used in different schedules. Choosing the level of indexing is a trade-off between backup performances and restore granularity.

Check Old Backups to be Deleted: When this option is selected, the data retention process is triggered after the backup. By default, this option is selected. If SnapVault is used, it is possible that many backups cannot be deleted until the remote backups are deleted. In this case, the data retention process takes longer to complete and you can select this option only in certain backup schedules.

To set up a start time for you backup, complete the following steps.

Step	Action
1	Click the calendar icon next to the Start Time field. A calendar pops up. Use the calendar to specify when the backup should begin.
2	Specify the interval at which the backup occurs: Only Once, By Hour, By Day, By Week, By Month, or Advanced.
3	After successfully scheduling the time and frequency at which the backup plan should run, save the plan by clicking Save.

After the plan has been saved successfully, it is displayed in the narrow column area on the right. The plan will be executed according to the set schedule. You can edit these options later by clicking the plan name. You can delete a plan by using the red 'X' sign next to the name.

To manually execute a scheduled plan at any time, click the Backup Now button. After you click the Backup Now button, a pop-up window appears, enabling you to select the options specified.

Backup maintenance

For large SharePoint environments, database verification during the backup job might create too much overhead on the production environment and slow down the completion time for the backup job. You can elect to perform data verification at a different time from the backup schedule.

To schedule data verification, complete the following steps.

Step	Action
1	Go to the Backup Maintenance tab to select the options to verify the backup data.
2	Select the Verify Last... option and enter a positive integer in the provided field to specify how many unverified backup jobs to verify. If SnapMirror or SnapVault is enabled, you can also select the Verify On Available SnapMirror Destination Volumes or the Verify Archive Backup On Secondary Storage check boxes.
3	Choose a Verification Server from the drop-down list. See the Control Panel section of this guide for instructions on defining a Verification Server.
4	If SnapMirror is enabled in your environment and you did not enable the SnapMirror update at backup time, you can use the Update SnapMirror After Operation option to trigger SnapMirror replication for the Snapshot backups of SharePoint databases and search index.
5	If SnapVault is enabled through Protection Manager in your environment and you did not select the archive backup option at backup time, you can use the Archive Backup To Secondary Storage option to archive the Snapshot backups of SharePoint databases to the SnapVault storage.
6	You can also set up a schedule for the verification by clearing the No Schedule check box. Using the calendar icon next to the Start Time field, select a date and time for the backup maintenance job to run. Also, set an interval for recurring rules based on Only Once, Hourly, Daily, Weekly, or Monthly schedules. If you want to run this job immediately, click the Run Now button.

Synchronizing the farm data

After the SharePoint farm structure is changed (that is new content databases are created), you can load the saved backup plan and click the Sync Farm Data button to show the latest SharePoint structure. Then you can add these new components to the backup plan.

Backup of SharePoint components

SharePoint components

SnapManager for Microsoft Office SharePoint Server can back up the following SharePoint components:

All SharePoint databases: The configuration database, central administrator content database, content databases, SSO database, SSP database and search database are included. These databases are backed up on SQL Member Agent using SnapManager for Microsoft SQL Server Snapshot backup.

SharePoint search index: This include the OSearch index and SPSearch index. The search index files are backed up on Index Member Agent using SnapDrive Snapshot copies.

SharePoint components and settings: This includes Web applications, SSO, SSP, InfoPath Forms, and Global Search Settings. This data is backed up to the Media Service specified in the backup plan, along with backup job data.

SharePoint solutions: This includes any SharePoint customizations deployed to SharePoint in the form of solutions. These solutions and their deployment status are backed up to the Media Server specified in backup plan.

SharePoint front-end resources: The front-end Member Agent backs up the IIS sites (both metadata and files) and SharePoint 12 hive files to the Media Server specified in the backup plan.

Some components have multiple related sub-components that need to be backed up together. For example, OSearch and SPSearch index files need to be backed up with their corresponding search database.

The SSP database, the Web application hosting the SSP admin site, and OSearch can be backed up together. If OSearch is not selected for backup, the search setting needs to be re-configured and the index needs to be re-crawled after SSP restore.

Note

To back up SSO, the account specified in the Agent needs to be able to back up and restore the master key.

Limitations for backup

SnapMirror and SnapVault limitations

For integration with SnapMirror and SnapVault, you must use other methods to check the status because the actual operations are performed outside of SnapManager and the status information is not available:

- † **SnapMirror Update and Verification Results:** Use Data ONTAP FilerView to check the SnapMirror status and replicated Snapshot copies.
- † **SnapVault Archiving and Retention:** Use Protection Manager to check SnapVault backup and retention status. You can also use Protection Manager to delete SnapVault backups.
- † **Archive Backup to Secondary Storage:** This feature does not support archiving of any SharePoint data that is not managed by the SQL Server.

About SharePoint customizations

SnapManager for Microsoft Office SharePoint Server does not replace system backups like AD, File System, and System State backups. Therefore, customizations with external dependencies are not backed up. Typically, such customizations are deployed through an installer or manually and require the use of some binaries, registry entries, or other databases.

SharePoint customizations deployed using the SharePoint solution framework can be backed up and restored to the deployed state. You might need to reconfigure them after restoring.

Simple customizations that involve only some self-contained files in the SharePoint hive folder can be covered by the Front-End Member Agent backup of the SharePoint hive. You can select the related files for restore.

Overview of restore

From the SnapManager for Microsoft Office SharePoint Server Restore Controller screen, you can perform the following actions:

- † Browse and search the backup data contents displayed on a timeline, representing all available restore points
- † Set up scheduled or immediate restores for any SharePoint environment (as long as a SnapManager for Microsoft Office SharePoint Server Agent is installed)
- † Selectively restore SharePoint components, from the whole farm down to specific document versions, with all security, metadata, and original properties preserved
- † Monitor real-time progress of any restore jobs (through the Job Monitor)

After a backup job is completed successfully, the backup data is ready for browsing. To perform a restore, click Restore Controller to begin browsing the backup data.

Loading the timeline

To select content to populate the Timeline Browser, complete the following steps.

Step	Action
1	Open the Restore Controller interface and locate the options section on the top of the screen.
2	Select a SnapManager for Microsoft Office SharePoint Server Agent from the drop-down list. This contains all Agents that have a successful backup stored in the Media Service.
3	Select a specific plan from the drop-down list, or select All Plans to load data for this Agent that has been backed up in multiple plans.
4	Specify a time range in the Time Window field by clicking the calendar icon to the right of From. This enables you to specify a start time for the search. In the window that pops up, select a date and time and click OK.

Step	Action
5	Click the calendar icon to the right of the To field to choose an end time and use the calendar pop-up to specify a date and time. Click OK to set this time. By default, the To field is populated with the current time when the interface is loaded.
6	If you want to hide the incomplete jobs from the Timeline, including any that are still being indexed, select the Hide Incomplete Jobs box.
7	Click the Load Timeline button. The time points at which the backup jobs were run are displayed on the timeline. When you hover your mouse over each available point, details about the backup time and plan name, restore granularity level, plan status, and verification status are shown in the pop-up bubble. Additionally, verified jobs are shown with a check mark over the point-in-time icon.
8	Click a plan's point-in-time icon to load the data for this plan. You can review the contents of the job in the tree mode on the bottom-left of the screen.
9	Browse through the backup data in the tree by clicking the name of the Agent host or the SharePoint instance to expand the backup content.

Restore level

There are two restore levels available:

Farm component level: Under the Farm Browser tab, the SharePoint backup farm structure is displayed. Multiple farm components, such as content databases, Web applications, SSP, or even the entire farm and its settings can be selected for restore.

Granular level: If granular indexing options were selected during backup, individual site collections, sites, lists, folders, items, or item versions can be restored from the content databases.

The restore options available for each restore level are different and are described in the following sections.

Common restore options

Scheduling the restore job

By default, all restore jobs are set to run Now. If you want to run a restore job later, you can fill out the Start Time schedule in the Restore Option section of the interface. Click the calendar icon to set the time to run the job.

Restore option types

Another common setting for restores is the type of Restore Option to use: Not Overwrite, Overwrite, and Append.

Not Overwrite: SnapManager for Microsoft Office SharePoint Server does not restore the content if it already exists on the destination. For example, if an entire folder's content is selected for restore but only one document was removed from the destination folder, only the one document is restored.

Overwrite: This option restores the content over whatever exists on the destination. Essentially this deletes the content on the destination and replaces it with the content selected to be restored.

Append: The Append option updates the destination with the selected data to be restored. Data that already exists is not deleted, but an additional copy is added. Also, any data that is not already present is added.

Note

The Append option is unavailable at the Farm Component level because SharePoint does not allow two identical farm components to coexist in the same farm. This is because their internal IDs would conflict with each other.

Restore from SnapVault

By integrating with SnapVault, it is possible to have longer retention for backup data. The restore process from SnapVault backup data is the same as the features listed in the previous section.

In the background of a restore from SnapVault, SnapManager for Microsoft Office SharePoint Server checks if a local backup for the selected object exists. The SnapVault backup data (or the remote backup data) is used only when local backup is already deleted. However, restoring from SnapVault data is much slower than SnapRestore from local backup data.

Note

Only database backup to SnapVault is supported. Restoring the SharePoint search index from SnapVault is not supported.

Running a restore job

After configuring the settings, click the Go button for SnapManager to initiate the restore process immediately or to assign the schedule for the restore job to be run later.

Granular level restore

Selecting content for restore

To choose site collections, sites, or any other SharePoint content to restore from a content database, you must first load the contents using the tree in the lower left of the interface.

Step	Action
1	To choose SharePoint site collections to restore from (and any contents contained beneath these), you can either search for the site collection directly, or load the tree from the main SharePoint farm tree. To perform a site collection search, click the Find Site Collection button at the top of the SharePoint tree and enter the search criteria for the site collection in the pop-up provided (including wildcards “*”). Click Search to open an additional tab called DB Browser to list the databases that the site collections are in. For case-sensitive searches, select the Case Sensitive check box.
2	Click the Detail button next to the selected content database either in the site collection search results or in the main SharePoint tree. This opens a new Detail tab, which displays the contents of this database.
3	Click the site collection name to expand the tree. You can continue to expand the tree further to show all subsites, lists, libraries, and folders located beneath that specific site collection. Note_____ The tree can only expand to the level set by the Restore Granularity level during backup.
4	Select the content to restore by using the check box next to each node. By default, after you select the container, all items in it are also selected. If some items are not selected, the check box for this node becomes a dash symbol. To view items or item versions available for restore, click the Content Browser icon (ⓘ) to view the content of a list, library, or folder, and select the corresponding check box to select the content to restore.

Searching for the backup data to restore

For large backups that contain a significant amount of content, browsing through a large content database for the data needed for the restore can be inefficient. In such situations, the Search icon () is recommended.

To search for the data to restore, complete the following steps.

Step	Action
1	Expand the Backup Data Browser tree and locate the node you want to search under.
2	As you hover your mouse over the node, the Search icon appears to the right of the node. Click this icon to open the search pop-up.
3	Enter the type of search criteria. You can search on any level beneath the current node. For instance, searching from a site collection node enables you to search on the site, list or library, folder, or item level. Searching on a list or library level enables you only to define criteria for a folder or an item.
4	Enter a search term in the Criteria field. Wildcards (*) are accepted (that is, *.ZIP). You can select the Case Sensitive check box at the bottom of the window if you want to limit the search further.
5	Click the Add button. You can continue to add multiple search terms, and the search is performed based on AND logic. You can also delete terms using the Delete button.
6	Click OK to load a list of search results. These open in a new tab called Search Result. You can select contents from this search result using the check boxes available.

Performing granular level restore

When a granular level restore is performed, choose one of these restore types: In Place or Out of Place.

In Place Restore: Restores backup data to the original location.

Out of Place Restore: Restores backup data to any alternate SharePoint location either in the same farm or across different farms.

After you select one of the restore types, in this case Out of Place Restore, complete the following steps.

Step	Action
1	After selecting the Out of Place restore option, click the Set Destination button.
2	Choose a destination in the new window that appears. Select the Agent Name for the destination location from the drop-down list at the top of the window. The destination must already have a SnapManager for Microsoft Office SharePoint Server Agent installed to be selectable from this list.
3	Click the farm name to expand the tree. You can continue to click each node to expand the tree to the destination you want to restore to.
4	Use the radio button next to the destination node to select a location to restore to. If you want to restore to a location that does not exist in SharePoint, you can use the blank box at the bottom of each level in the SharePoint tree. To create a new site collection, the full URL is needed, but for other levels (from site down to folder), only the name needs to be specified. Note _____ You should always select a container for the content either on the same level or one level higher than what is being restored. For example, a site should always be restored either to a site or a site collection, and a list or library should always be restored either to a site or another list or library. _____
5	Click OK. The Farm Name and Destination information is populated below the Out of Place restore option.

Restore options for items

For both In Place and Out of Place restores, the detailed contents of each container object can be displayed in a new window by clicking the Details icon as described previously. In the items details window, you can select individual items in the resulting table listing all restorable items. You can use the following options for the selected items and container:

- † **Container Security:** Select this option to restore the security settings of the container object, if unique permission is used.
- † **Container Property:** Select this option to restore the container properties. For example, if the container is a list, this includes all the columns, settings, and other options.
- † **Item Security:** Use the check boxes in the last column of the item pop-up to restore the security settings of the items. This is useful if unique permissions are used.

If Item Version restore granularity was used during backup, item versions are listed in the item details window. History versions are displayed as Item Name Version Number. The most current version is displayed as the item name without any version information. You can either choose to restore a single version or only the most current version.

Farm component level restore options

Restoring a database to its most recent state

This option enables you to use SnapManager for Microsoft Office SharePoint Server to restore a SharePoint database to its most recent state.

Note

To use this option, you must select the latest backup data.

If this option is not used, a point-in-time restore is performed, which creates multiple recovery paths for the database. A later up-to-the-minute restore using the same backup data will fail. In that case, the SnapManager for Microsoft SQL Server interface can be used for up-to-the-minute restores. A detailed explanation of this limitation is documented in the following section.

After the database is restored, it must be reattached to the SharePoint environment before SharePoint Services can access it. To reattach the database, enter the following command:

```
%COMMONPROGRAMFILES%\microsoft shared\web server  
extensions\12\bin\stsadm.exe -o addcontentdb -url URL name -  
databasename database name
```

Where the *URL name* entry is a valid URL (such as `http://server_name`) and *database name* is a valid content database name. For more details about the SharePoint Team Services **ADM**inistration (STSADM) command, visit the Microsoft TechNet Web site:

<http://technet.microsoft.com/en-us/library/cc263422.aspx>

Note

The preceding STSADM command can be used only on a content database. For other SharePoint databases, the Restore From Alternate Storage Location option can be used for the manual restore process.

Restoring a database to a point in time

In a point-in-time restore, databases are restored only to a point in time selected from the timeline browser.

A point-in-time restore occurs in two restore scenarios:

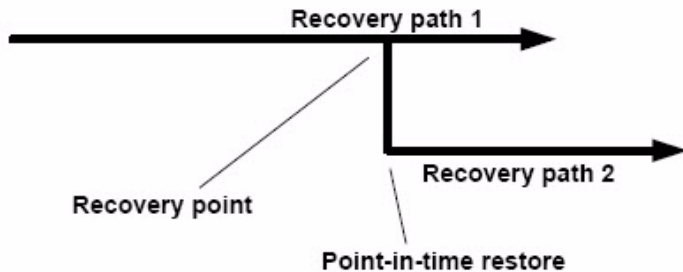
- † The database is restored to a given time from a backed up transaction log.

- ‡ The database is restored but only a subset of backed up transaction logs are applied to it.

Note

Performing a point-in-time database recovery results in a new recovery path.

The following image illustrates the potential problems when a point-in-time restore is performed.



In this image, Recovery path 1 consists of a full backup followed by a number of transaction log backups (a point-in-time backup). New transaction log backups are created after the point-in-time restore takes place, which results in Recovery path 2. It is not possible to tie the transaction logs created in Recovery path 2 to the full backup belonging to Recovery path 1.

Therefore, to preserve database integrity, the only way to restore the database to its most current state after a point-in-time restore is to complete a new full backup that has only one recovery path.

Note

To avoid the problems listed previously, ensure that you always create a full backup after restoring a database to a point in time.

Verifying backup data before restoring

This option enables you to verify backup data before restoring it to ensure that the restore is successful. Select a Verification Server from the drop-down list, defined previously in the Control Panel. The Default option uses the Verification Server configured in the SnapManager for Microsoft SQL Server interface.

Restore databases only

When this option is used, only the selected databases are restored with no attempt to connect them to the SharePoint environment. This is useful in the instance when a SharePoint environment has not yet been set (that is, during a whole farm restore). This can also be used in cases where you want to perform manual steps to bring up or down a specific environment after the database is restored.

Note _____
Configuration databases and Central Administration databases can only be restored by selecting this option.

Restore front-end file security

This option only applies to the front-end files backed up, including IIS site files and SharePoint 12 hive files. When the option is used, both file contents and securities are restored. Otherwise, only the file content is restored.

Restore front-end files to alternate location

This option enables you to select a location to restore the front-end files and templates files.

Step	Action
1	Click the Browser button, and a pop-up window appears.
2	Select an Agent from the drop-down box.
3	Expand the destination tree by clicking the Agent name. Click each node to expand the tree further.
4	Select the location for the files you want to restore by clicking the corresponding radio button.
5	Click OK to save this destination, or use Cancel to clear the settings.

Farm component level restore considerations

Supported farm level components for restore

For a list of all the farm components available for restore, see the following list.

Farm component	Notes
Configuration Database	Can only be restored during a whole farm restore
Central Administrator Web Application	Can only be restored during a whole farm restore
Admin Content Database	
Web Application	
Content Databases	Allows granular restore of individual items
Shared Services Provider (SSP)	SSP properties, SSP database, and search index
SSP Search Index	Must be backed-up and restored together with SSP
Global Search Settings	Farm-level search settings and crawler impact rules
SharePoint Help Search	
InfoPath Form Services	InfoPath Forms Services Settings and InfoPath Forms Services form templates
Single Sign On (SSO)	SSO database and configurations
Windows SharePoint Solutions	SharePoint solutions and their deployment status
Front-End Resources	IIS settings and files, SharePoint 12 Hive folder

Note

SharePoint components that are not listed in the preceding table are not supported. For example, custom Web parts not deployed through SharePoint solution.

**Restore details
about specific farm
components**

Some of the details and conditions pertaining to restoring each farm component type are as follows:

Configuration database: This is the core component of the SharePoint farm. It can only be restored during a whole farm restore. See the full farm restore section of this guide for details regarding this process.

Web applications: Web applications can be selected from the farm tree and restored, including the settings and associated IIS sites. Content databases under the Web applications are also restored if selected. However, if there are any changes on the IIS sites (resulting from manual changes or 3rd party software) the IIS site backup on the front-end Member Agent will also need to be restored.

Content databases: Content databases include SharePoint data such as site collections, sites, lists, libraries, and all items. When a content database is restored, SnapManager for Microsoft Office SharePoint Server automatically reattaches them to the original Web application on restore.

SSO: To back up and restore the Single Sign-On encryption key, the control agent must be the encryption key server. The encryption key, SSO database, and SSO settings are restored.

SSP and search index: Shared Services Provider has multiple sub-components including the SSP database, search index files, search database, and SSP admin site collection hosting Web application. In addition, other Web applications might be related to SSP, such as the Web application hosting the MySites site collections. Before the SSP is restored, the following must be restored:

- † Any related Web applications must be restored before the SSP can be restored.
- † The OSearch service must be started in the SharePoint Central Administrator interface.
- † In addition, the search index must be restored together with SSP.

SharePoint solutions: When a SharePoint solution is restored, it is deployed to the related Web applications as of the state of the backup. Depending on the customizations contained in the SharePoint solution, it might need to be re-configured after the deployment.

Front-end resources: If only out-of-the-box SharePoint features are used, there is no need to restore the front-end resources, because everything is covered by the other farm components. If there are manual customizations applied to the IIS site (including web.config), the IIS site should be restored.

If customizations are self-contained within the SharePoint 12 hive folder, they can be restored as well by restoring the files. Both IIS site files and 12 hive files can be restored out-of-place to another location for further examination.

Note

Front-end resources cannot be restored together with other farm components. They need to be restored separately after any other farm components are restored.

Deleting SnapManager for Microsoft SQL Server restore copies

SnapManager for Microsoft SQL Server creates a snapshot copy of LUNs as part of restoring SQL server databases to the original location. These snapshot copies of LUNs cannot be deleted by SnapManager for Microsoft Office SharePoint Server. You must use SnapManager for Microsoft SQL Server to delete these copies.

To delete these copies, complete the following steps.

Step	Action
1	Launch the SnapManager for Microsoft SQL Server interface.
2	Select the Action menu, and choose the Delete Backup option.
3	Select the option to Delete Snapshot Copy of LUN Created During Restore to delete these copies. You can also select any additional options at this point.

Note

This situation only applies to the restore of farm components, because granular level restore only clones the original snapshot backup and does not restore the database.

Disaster recovery

Prerequisites for performing a disaster recovery

This section describes how to perform a disaster recovery (DR) using backup data from SnapMirror from the perspective of SharePoint and SnapManager for Microsoft Office SharePoint Server. It does not cover how to recover Active Directory (AD) or any other components not covered by SnapManager for Microsoft Office SharePoint Server.

The following are some prerequisites to performing this restore:

- † The SharePoint database and search index backups must be available. Typically these are automatically replicated through SnapMirror.
- † SnapManager for Microsoft Office SharePoint Server backup jobs data and system backup data must be available. If Media Service and System Backup locations are using SnapMirror enabled LUNs, it should be automatically replicated.
- † At the DR site, all server topology should be identical to the production site, which includes both the SharePoint farm topology and SnapManager for Microsoft Office SharePoint Server topology.
There are several ways to achieve this. For example, a separate AD domain for the DR site can be used to keep the same server topology, or if the DR site does not need to coexist with the production site, disk imaging or virtualization technology can be used to ensure the same topology is used.
- † If a separate AD domain is used at DR site, that domain should have a trusted relationship with the primary site's AD so that users can still access SharePoint content. This can also be run if the DR site is in the same AD domain as the original location.

Preparing the DR site for recovery

After the servers are rebuilt and the preceding prerequisites are met, complete the following steps for disaster recovery.

Step	Action
1	Install all required software components, including SnapDrive, SQL server, and SnapManager for Microsoft SQL Server.

Step	Action
2	Install SharePoint. If only farm components like Web applications or SSP need to be restored, a new farm can be created. Otherwise, SharePoint can be left unconfigured when performing an entire farm restore.
3	Install SnapManager for Microsoft Office SharePoint Server Manager according to the steps listed in this guide. Note_____ Make sure all software versions and patch levels are the same as the original production site. Also ensure that all the users and permissions are created and set to the same production site.
4	Perform a SnapManager for Microsoft Office SharePoint Server system restore using the System Recovery backup data.
5	Connect the SnapMirror LUN containing the Media Service backup job data, or manually copy this data to a location that the DR site Media Server can access. Note_____ The DR site's Media Service location can be changed to point to the new location.
6	Install SnapManager for Microsoft Office SharePoint Server Agents according to the steps listed in this guide.

Performing the DR restore

After you install SnapManager for Microsoft Office SharePoint Server in the DR site and complete the preceding steps, you can continue with the full farm restore as described in the following steps.

Step	Action
1	Navigate to Restore Controller in SnapManager for Microsoft Office SharePoint Server.

Step	Action
2	Browse for the backup data and choose the Restore From Alternate Storage Location option. How to use this option is described later in this guide.
3	Use SnapManager for Microsoft SQL Server to restore any related databases.
4	Reconnect the SharePoint search index LUN using SnapDrive.
5	Complete the manual restore wizard.
6	If the whole farm restore was performed, follow the procedure described in the full farm restore section to reconnect SharePoint servers and complete other post-restore steps.
7	After the restore is complete, you can make a DNS switch to redirect users to the DR site.

Full farm restore

Overview

SnapManager for Microsoft Office SharePoint Server Backup and Restore solution enables you to back up your entire SharePoint farm, including all of the SharePoint farm components listed previously.

Prerequisites for a full farm restore

To do a full farm level restore, the following requirements need to be met:

- † A backup copy of the data for the entire farm (including the SharePoint configuration database and the central administration database) must be available.
- † The SharePoint server topology should be identical to the topology at the time of backup. The system platform should also match the platform at the time of backup. For example, a x64 system should be used if an x64 system was used at the time of backup.
- † All related software installed on the destination should be the identical version and the patch level as before. Examples of related software are: SharePoint, SQL Server, SnapManager for Microsoft SQL Server, SnapManager for Microsoft Office SharePoint Server, as well as .NET Framework.
- † User permissions on both the local server and SQL Server should be set to the same as before.
- † Configure the same LUN storage layout as before.
- † SnapManager for Microsoft Office SharePoint Server Control Agent should be installed on the SharePoint Central Administration server.
- † Also, to restore Single Sign-On, SnapManager for Microsoft Office SharePoint Server Control Agent must be on the SSO master key managing server.

Performing a full farm restore

To perform a full farm restore, complete the following steps.

Step	Action
1	Because this restore using Restore Controller must be performed as an “in place” restore (same farm), evaluate the status of the farm: † If the farm where all data is being restored to has either been currently or recently deployed (including re-installed environments), disconnect all front-end servers using the SharePoint Products and Technologies Configuration Wizard. See your SharePoint user guide for more details. † If the farm you are using for the restore is a new installation, proceed to the next step.
2	Using Restore Controller (described in the previous sections), load the backup plan and data for this farm. Using the tree, choose the Configuration DB and Admin Content DB. Note If the Configuration DB and Admin Content DB were not backed up, any missing configurations need to be put back manually. You can create a new farm and continue from Step 7.
3	Choose the Restore Databases Only option, next to the restore options. This option is used because the SharePoint environment is not available at this time, therefore it is not required to connect the databases yet.
4	Click Go to start the restore process.

Step	Action
5	Connect all of the SharePoint front-end Web servers to the Config DB restored in the previous step. You can use the SharePoint Products and Technologies Configuration Wizard to perform this action. Note_____ At least one front-end Web server should be used to host the Central Administration Web Application. When using the SharePoint Products and Technologies Configuration Wizard, select the Use This Machine To Host The Web Site option under Advanced Settings: Host Central Administration Web Application. _____ After connecting all front-end Web servers to the Config DB using the preceding steps, complete all the following additional steps to finish the restore.
6	Under certain circumstances, front-end resources backed up by a SnapManager for Microsoft Office SharePoint Server Front-End Member Agent need to be restored. For example, IIS site settings or files (that is, web.config) might have been changed after the Web application was created, either manually or through third-party software. Note_____ Front-end resources should be restored separately from the farm component restore. They cannot be selected at the same time with farm components in Restore Controller. _____
7	To ensure that all solutions have been properly deployed, select the Windows SharePoint Solutions node in the restore tree and run a restore. Note_____ The Database Only option should not be used in this case. _____

Step	Action
8	For the features that apply to your environment, check that the following services are running in the Services tool for Windows (located under Administrative Tools in the Control Panel). Single Sign-On (SSO): Restart the Microsoft Single Sign-On Service under the Services window. SPHelpSearch: Restart Windows SharePoint Services Search in the Services window. Shared Services Provider (SSP): All features except the search index are already available. To restore this, make sure the Office SharePoint Server Search (OSearch) has been restarted in the Services window. You also need to restart the SSP service in the SharePoint Central Administration > Operations > Services setting on the Server list.
9	To complete the restore of the index data for the SSP, select the corresponding nodes and children in the tree of the Restore Controller tree and perform an in-place restore. Make sure you are not using the “Database Only” restore option. If this SSP is the parent of an inter-farm deployment, all children take 5-10 minutes to establish a connection after the restore is complete. This happens automatically. Note _____ You can also manually re-crawl the SharePoint index. From Central Administration, choose to edit the properties and specify an index server for the SSP. Navigate to the SSP admin site and choose Search Setting > Restart Crawl Index Files.
10	If any customizations have been installed using a third-party install wizard, re-run those installations to complete the restore.
11	Using the instructions provided in the Granular and Farm Component Restore sections above, restore the SharePoint content databases back to the environment.

Restoring front-end Web settings

You can restore customizations to your front-end Web server for your farm by using Restore Controller. You can also use this to restore the IIS settings and the SharePoint hive.

Using Restore Controller, perform an in-place restore of any of the nodes listed under the front-end Web servers level. For instance, if you only want to restore the IIS settings for a single Web application (that is, the only one with customizations), you can restore a single front-end resource node from this tree. You can also remove all the customizations and return these to the original settings.

General troubleshooting tips for full farm restore

Some of the most common problems when performing a full farm backup and restore are detailed in the following sections.

SharePoint Central Administration cannot be accessed after restore:

You can recover Central Administration by using one of the following methods:

- † Make sure that the front-end Web servers were used to host the Admin Web (described previously). If not, disconnect a front-end server and reconnect it using the Use To Host Admin Web option. Consult your SharePoint guide for more information about this process.
- † Reset the application pool for Central Administration.

If index data is not accurate or corrupted: You can use one of the following methods to restore the index data.

- † Use Restore Controller (without the “Database Only” option) to restore the index records from the last available backup.
- † Restart the Office SharePoint Server Search Services and set the index server for the SSP and re-crawl the environment.

If a Web application cannot be accessed after restore: If you want to fix this issue, make sure you perform the following first.

- † If customized features or site-definitions were used, verify that all prerequisite steps for the front-end Web server were performed before performing the restore.
- † Make sure that Web Site Status is started in IIS Manager with the proper settings.
- † Reset the password for the application pool and perform an IIS reset.

If there are problems with user profiles and properties or search settings in SSP: Perform the following steps if you are having trouble with the SSP.

- ‡ Restart the Office SharePoint Server Search Services in SharePoint.
- ‡ Restore the SSP using Restore Controller.

Restore from alternate storage location

About restoring from alternate storage location

By using this option, you can restore data from an alternate storage location other than your primary storage. For example, your data might be stored on a SnapMirror copy or as a SnapVault backup. A wizard within the SnapManager for Microsoft Office SharePoint Server interface guides you through the restore process and the data is restored manually using other tools (like SnapManager for Microsoft SQL Server).

To restore from an alternate storage location, complete the following steps.

Step	Action
1	From Restore Controller, select the content you need to restore.
2	Select the Restore From Alternate Storage Location option under Restore Options.
3	Click the Go button to launch the wizard.
4	Click Next to continue. SnapManager for Microsoft Office SharePoint Server begins the process to prepare for the restore. During this process, the following processes occur: † If the SSP was selected for restore, the SSP is deleted and all the related databases are detached from SharePoint. The search index is also deleted as part of the SSP deletion process. † For any other SharePoint components, the related databases are detached from SharePoint.
5	After the restore preparation has completed successfully, the detailed information regarding all related components for manual restore is listed, including the detached databases and the location of the search index.
6	Perform a manual restore of the listed components. For instructions regarding a restore from an alternate source, see the <i>SnapManager for SQL Server Administrator's Guide</i>.

Step	Action
7	After the manual restore is completed, click the Verify button to continue the restore process. SnapManager attempts to verify the manually restored components and completes the restore. If the verification or the restore fails, a list of errors detected is displayed.

Granular level restore

You can also perform a granular level restore using the backup data in the alternate storage location.

Step	Action
1	In the granular restore interface, select the objects you want to restore.
2	Select the Restore From Alternate Storage Location check box.
3	Click Go. A GUI wizard opens to guide you through the manual restore process.
4	Follow the prompt to manually restore the content database backup to the temporary database, then click Verify.
5	SnapManager uses the manually restored temporary database to complete the restore process. After the restore is completed, the detailed information about the restore is displayed.

Note

After the granular restore, you need to delete the temporary database and disconnect the LUN.

Restore limitations

SharePoint component restore limitations

SnapManager for Microsoft Office SharePoint Server has some limitations in performing a restore of SharePoint components:

- † Only SharePoint components explicitly available for backup are covered; all other components that store information externally are not covered. For example, the Form-Based-Authentication (FBA) user database cannot be backed up or restored.
- † Customizations deployed by SharePoint solutions can be restored to its deployed state. Similar to the previous limitation, if the specific customization stores information externally, these cannot be backed up or restored. If the original state was not restored for this reason, additional configurations of these features and solutions might need to be done after the restore.
- † Customizations not deployed as SharePoint solutions (either deployed manually or through a separate installer) are not supported. If the customization is self-contained within the SharePoint 12-hive scope, you can restore it from the 12-hive backup, but this is not supported.

Granular restore limitations

For the granular restore option, SnapManager for Microsoft Office SharePoint Server does not support the following.

- † Workflows are not supported at the site collection level granular restore and below. Only SharePoint built-in workflows can be restored from the content database level and the site collection level granular restore.

Overview of the Job Monitor

From the SnapManager for Microsoft Office SharePoint Server Job Monitor module, you can monitor the progress of any backup, backup maintenance, or restore job and view the detailed information at the completion of any successful or failed job.

The SnapManager for Microsoft office SharePoint Server Job Monitor module has two sections: Log Viewer and Job Monitor, which are described in the following sections.

Log Viewer

About the Log Viewer

To monitor the detailed processes involved in the SnapManager for Microsoft Office SharePoint Server platform, use the Log Viewer to view the logs generated during any job process. You can customize the Log Viewer to show different services and log levels to narrow your search.

Using the Log Viewer

When troubleshooting errors in SnapManager for Microsoft Office SharePoint Server, you can use the Log Viewer to track down each step that led to a failure. You can configure the view in the Log Viewer by setting up the following four options.

Level: In this drop-down box, you can select to view all the levels or Fatal, Error, Warning, Info, or Debug levels.

Service: You can select to view logs for all the services or for just the Media Service, Web Service, or Control Service.

Refresh: You can use this option to update the Log Viewer with the latest logs. There are four options available: 3s, 10s, 30s, and 120s (measured in seconds). You can also refresh the view immediately by clicking the Refresh button.

Per Page: You can customize the number of logs that appear per page by selecting either 5, 10, or 20 items to list from the drop-down menu.

If you click the Log ID number located in the first column for any log, you can see the detailed information for each log, including the Message generated, the ID number, the Date and time generated, the Service that generated the log, and the Host that the service was located on.

To view all logs, you can either page through the main list of logs or you can click the ID of a log and use the Previous and Next buttons to navigate through the logs one at a time.

Job Monitor

About the Job Monitor

Through the SnapManager for Microsoft Office SharePoint Server Job Monitor screen, you can monitor the progress of any backup, backup maintenance or restore job. Additionally, detailed information about the job is listed on completion.

You can view the following information for each job from the default view: the Status, the Plan Name, the unique Job ID, the Progress, the Agent Name for the farm that is being backed up, the Start Time, the Finish Time, the User who initiated the job, the Restore Granularity level chosen, the Index Status if a granular restore level is chosen, and a Detail field to download a detailed job report. Additional columns might be available depending on the type of job.

Loading the Job Monitor

To launch the Job Monitor, you can either navigate to the menu on the side of SnapManager for Microsoft Office SharePoint Server, or you can click the Go To Job Report button that appears when a job is run. This automatically loads the screen showing the job information when you run a job.

If you want to change the view to show either a Restore, a Backup, or a Backup Maintenance job, select the corresponding options on the upper-left of the interface.

To sort the Job Monitor table, click any of the column titles. If there are many jobs, you can also use the page navigation controls.

Downloading detailed job reports

To download a detailed job report, scroll to the Detail column and click the View Detail Report button. A window appears showing a brief summary of the details regarding this job. You can save the detailed job report by clicking the Download button and selecting a location to save the zip file. This is useful for cases where advanced troubleshooting is required.

For backup and backup maintenance jobs, the related SnapDrive and SnapManager for Microsoft SQL Server API outputs will be recorded for download as well. This option will appear as a second Download option in the pop-up window.

Note

When a backup job is deleted, its associated backup job data and snapshot backups in storage system will also be deleted. Therefore, restore from that backup job is no longer possible after the deletion
