NETAPP TECHNICAL REPORT

SNAPMANAGER FOR MICROSOFT OFFICE SHAREPOINT SERVER 2007: BEST PRACTICE GUIDE

Sourav Chakraborty, Jai Desai Network Appliance, Inc

January 2008 | TR-3638

CONTENTS

1 ENABLING COMPREHENSIVE DATA MANAGEMENT SERVICES

This document is an overview of how SnapManager® for Microsoft® Office SharePoint® Server can be used to automatically manage the backup and restore of critical Microsoft Office SharePoint Server resources. This document describes SnapManager for Microsoft Office SharePoint Server and provides information about how this application differs from other solutions available in the same space.

2 WHAT IS SNAPMANAGER FOR MICROSOFT OFFICE SHAREPOINT SERVER?

Microsoft Office SharePoint Server 2007 includes content management, information search, portal services, and other capabilities in a single software package. SharePoint Server 2007 combines the features of SharePoint Portal Server 2003 and a content management server with new capabilities, extending the functionality of the Microsoft Office suite to centralize storage of documents and other content for simplified management and improved Web-based collaboration.

SharePoint Server 2007 offers many advantages over SharePoint 2003, and its usage is accelerating rapidly. IT teams are deploying it to centralize important content from remote locations and to get documents off of individual desktops and laptops for improved accessibility as well as better data protection and security. SharePoint Server 2007 search capabilities make it easier to locate data, including specific versions of stored files. In fact, Microsoft is actively encouraging customers to move away from Exchange public folders for sharing Office documents and other files.

Naturally, the more corporate documents you pull together in a single location, the more business critical the repository becomes. As customers move to SharePoint for business-critical collaboration and content management, storage availability, accessibility, and performance are becoming critical, as is data protection—a particular pain point for SharePoint Server 2007.

With the newly released SnapManager for Microsoft Office SharePoint Server, NetApp helps streamline data management in SharePoint Server 2007 environments through:

- Fast backup of the SharePoint content database, including metadata
- Granular recovery of content, from a single item version to the entire content database
- A user interface based on SharePoint that simplifies data management tasks for a SharePoint administrator

3 SNAPMANAGER FOR MICROSOFT OFFICE SHAREPOINT SERVER BENEFITS

In today's business environment, two things are constant for customers:

- Growth in end-user and business data
- The dynamic nature of the business, which leads to a dynamic environment

Protecting the vast and growing amount of data is critical to keep the business running. Over the years, data protection infrastructures have become solid and are evolving further to meet the speed and reliability needs of the business. Individually, each of these technologies is getting easier to set up and use. In this environment, customers mention the following key data protection challenges:

- Guaranteeing the recoverability of the data
- Efficiently managing the data protection environment

In most IT environments today, the process of setting up the backup part for new data coming online is fairly streamlined. This process is considered essential to getting the data online, but it is expensive because of the manual steps required to map the end-user data to the actual storage that needs to be backed up and the multiple independent configurations that must be set up to complete the total data protection lifecycle setup.

Data environments are constantly evolving and changing. Most organizations do not have a rigid process to tie the changes in environment to the data protection process. This can lead to a situation where not all of the current data is getting backed up. The biggest risk in this whole process is that customers will find out the real impact only when the data is requested to be restored. This uncertainty leads to sleepless nights for backup managers who commit to service-level agreements (SLAs).

To eliminate the sleepless nights and to deliver confidence to business, backup managers need to determine what data is getting backed up and what is not. In today's complex data management scenario, the backup team has to go through lots of manual inventory, scripted queries, and manual correlations to find out the current backup status. The amount of time it takes reduces the currency of the gathered information.

Even when the changes in data environments are identified, the process of doing the mapping and finding the right kind of backup infrastructure is manual and time consuming. Customers have spent a lot of resources in optimizing their primary storage for excellent storage utilization. However, they have had very few tools to optimize their data protection infrastructure utilization. In most IT environments, the data protection resources are 5 to 50 times more than what the storage administrator maintains in primary data. Even incremental optimization in this area would lead to tremendous savings.

The primary reasons for lack of optimal utilization of resources are the complex planning and manual configurations required to keep efficiency high. With data growth exceeding IT personnel resource growth, customers are forced to take actions that create solutions that are fast but not the most efficient.

SnapManager for Microsoft Office SharePoint Server provides the tools to help customers meet all of these challenges. The value propositions are as follows:

- Dramatically simplifies the addition of data protection to new and existing user and project data.
- Enables backup organizations to determine and demonstrate data protection compliance with ease.
- Optimizes utilization of data protection resources.
- Automatically detects existing data protection relationships and imports them, making it easy to deploy in legacy environments.
- Employs an easy-to-use interface for backup and restore management.
- Policy-based management using templates enables consistent data protection SLAs to be performed.
- Automated data protection reduces the risk of human error.
- Maximized secondary storage resource utilization reduces capital expenditures to purchase new storage.
- Role-based access controls enable a secure environment.
- Integration with Operations Manager enables centralized reporting, event management, configuration management, and so on.

4 SNAPMANAGER FOR MICROSOFT OFFICE SHAREPOINT SERVER CONCEPTS AND SYSTEM ARCHITECTURE

The Network Appliance item-level backup and restore product, SnapManager for Microsoft Office SharePoint Server, addresses all of the shortcomings inherent in the native backup and restore functionality of Microsoft Office SharePoint Server 2007 and further extends the administrator’s ability to efficiently manage the SharePoint environment. SnapManager for Microsoft Office SharePoint Server expands from a backup and recovery tool to a full management platform because it utilizes a scalable client-server deployment strategy that allows deployment across multiple SharePoint instances, while enabling management and control from a single centralized browser-based interface.

As shown in Figure 1, SnapManager for Microsoft Office SharePoint Server clients can be deployed on a front-end Web server in each SharePoint environment. These clients are a light systems process and do not use a significant amount of resources. The clients communicate with the SnapManager for Microsoft Office SharePoint Server server, which can be accessed via a Web browser. Although the figure shows the SnapManager for Microsoft Office SharePoint Server client and server installed on separate machines, they could be installed on the same machine.

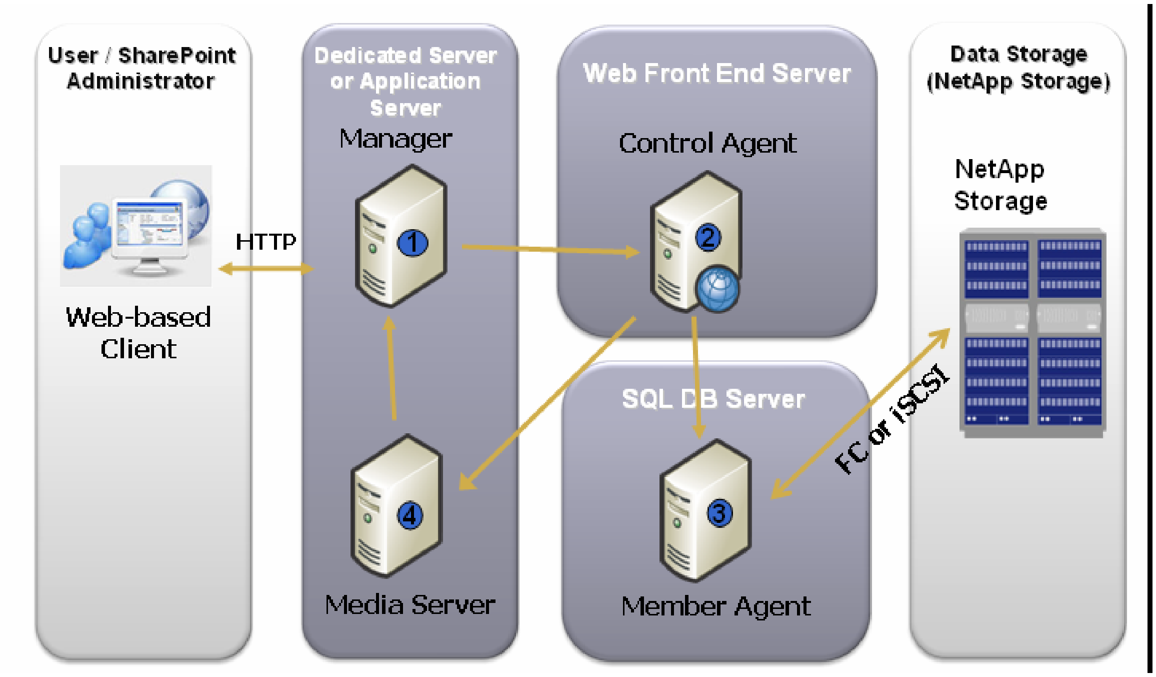
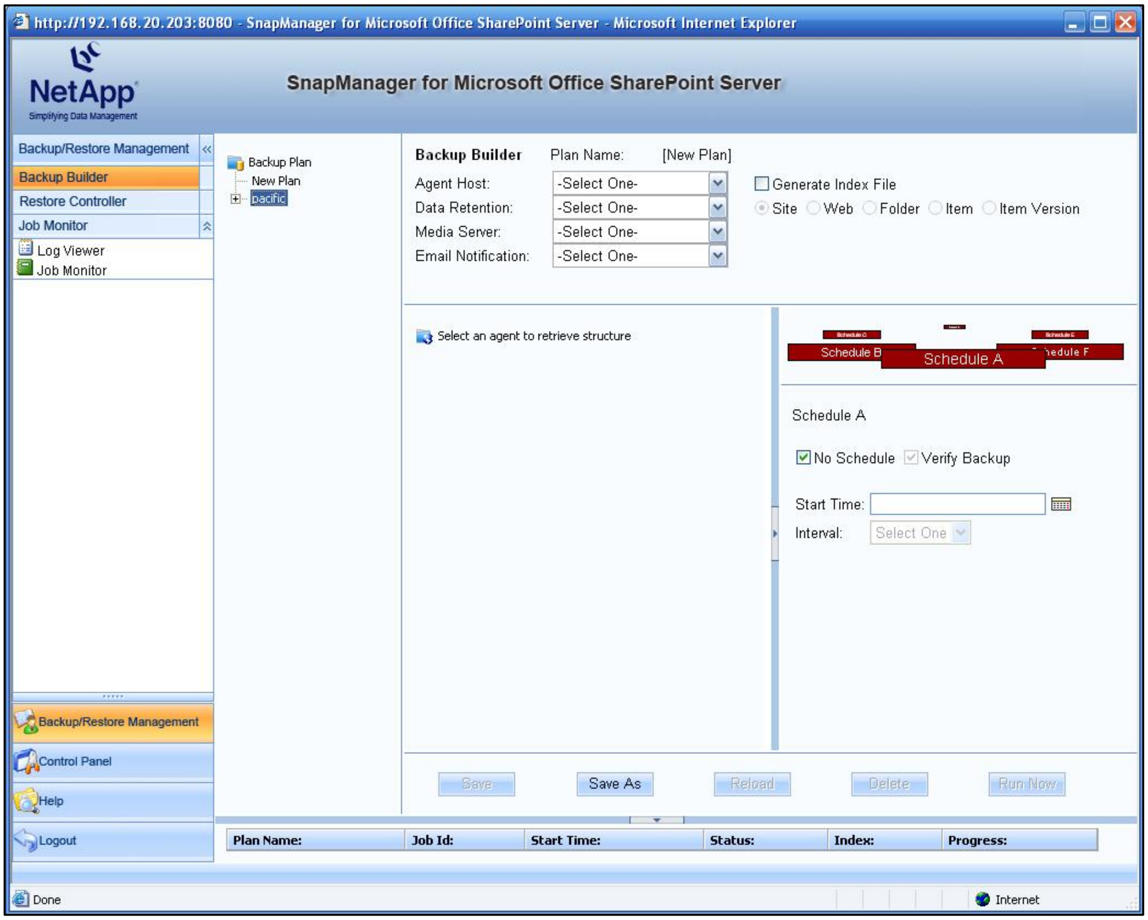


Figure 1) Architectural overview of SnapManager for Microsoft Office SharePoint Server.

Optionally, a dedicated SnapManager for Microsoft Office SharePoint Server media server may be provided to facilitate additional computing resources. Each SnapManager for Microsoft Office SharePoint Server installation includes installation of the SnapManager for Microsoft Office SharePoint Server Web service, SnapManager for Microsoft Office SharePoint Server network service, SnapManager for Microsoft Office SharePoint Server database service, and SnapManager for Microsoft Office SharePoint Server media service. Each of these services can be run on a separate dedicated machine, and thus there can be multiple dedicated media servers. The media servers perform the actual SharePoint data backup, effectively distributing the backup workload across multiple physical servers. Backup data on the media server supports full text indexing and search and can also be encrypted and compressed.

The SnapManager for Microsoft Office SharePoint Server server can also direct two SnapManager for Microsoft Office SharePoint Server clients to communicate with each other, allowing the transfer of SharePoint contents between SharePoint environments. Special care was taken in the SnapManager for Microsoft Office SharePoint Server software architecture to enable this communication to survive over very noisy or even intermittent data channels. Strenuous quality assurance tests on data packet fault tolerance included performing backups and restores of SharePoint data across the Pacific Ocean for a period of three days, where Ethernet cables were intermittently unplugged to simulate disrupted data communications. Successful results from such data transfer tests showcased the reliability of the data packet–level fault tolerance features of SnapManager for Microsoft Office SharePoint Server.

To address the shortcomings of the native backup and restore options in SharePoint, SnapManager for Microsoft Office SharePoint Server provides granularity down to the item level in both backup and restore. The manager window contains modules for performing a site-, subsite-, or item-level backup, as shown in Figures 2 and 3. Each of these modules enables you to perform a full backup of the entire SharePoint environment; the differentiation is in the granularity of the restore. For example, if a full backup of a SharePoint farm were performed utilizing the item-level module, the granularity of a restore from that backup would be down to a single individual item, such as a single version of a document, within that farm. If a full backup of a SharePoint farm were performed utilizing the site-level module, the granularity of a restore from that backup would be available down to an individual site within that farm.



Plan Name: [New Plan]

Agent Host: -Select One-

Data Retention: -Select One-

Media Server: -Select One-

Email Notification: -Select One-

□ Generate Index File

● Site ○ Web ○ Folder ○ Item ○ Item Version

Select an agent to retrieve structure

Schedule A

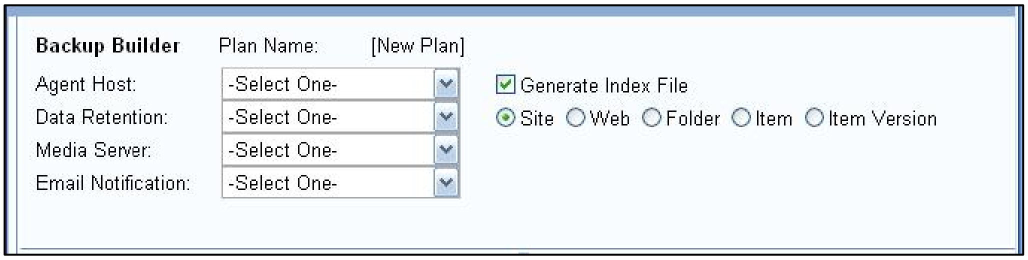
☑ No Schedule ☑ Verify Backup

Start Time:

Interval: Select One

Figure 2) SnapManager for Microsoft Office SharePoint Server GUI.

A natural question that arises is why one should use the site-level module, if the item-level module provides more functionality. One reason is speed. The item-level module has been tested to perform at approximately 30GB per hour per plan; a site-level backup is slightly faster, at 35GB per hour per plan. Another common use of site-level backup is to move or promote a site. This is accomplished by performing a restore to an alternate location. An administrator might also choose to perform a site-level backup only on less mission-critical sites or site collections. In addition, the site-level module can be used to supplement the item-level module. For example, site-level backups of content could be performed every few hours, while item-level backups might be performed once per day. The subsite-level backup provides even more flexibility in developing backup strategies.



Backup Builder Plan Name: [New Plan]

Agent Host: -Select One-

Data Retention: -Select One-

Media Server: -Select One-

Email Notification: -Select One-

☑ Generate Index File

● Site ○ Web ○ Folder ○ Item ○ Item Version

Figure 3) SnapManager for Microsoft Office SharePoint Server backup granularity level.

5 CONFIGURING SNAPMANAGER FOR SHAREPOINT ARCHITECTURE

The previous section presented a high-level overview of the SnapManager for Microsoft Office SharePoint Server architecture. It also discussed the connection between the different components of SnapManager for Microsoft Office SharePoint Server. This section discusses the considerations for configuring SnapManager for Microsoft Office SharePoint Server.

5.1 CONFIGURING THE SNAPMANAGER FOR MICROSOFT OFFICE SHAREPOINT SERVER MANAGER

Figure 4 shows the fields that you use in configuring the SnapManager for Microsoft Office SharePoint Server manager. The configuration dialog box opens at the time of installation. It can also be accessed at any time from Manager Configuration Tool on the Start menu.

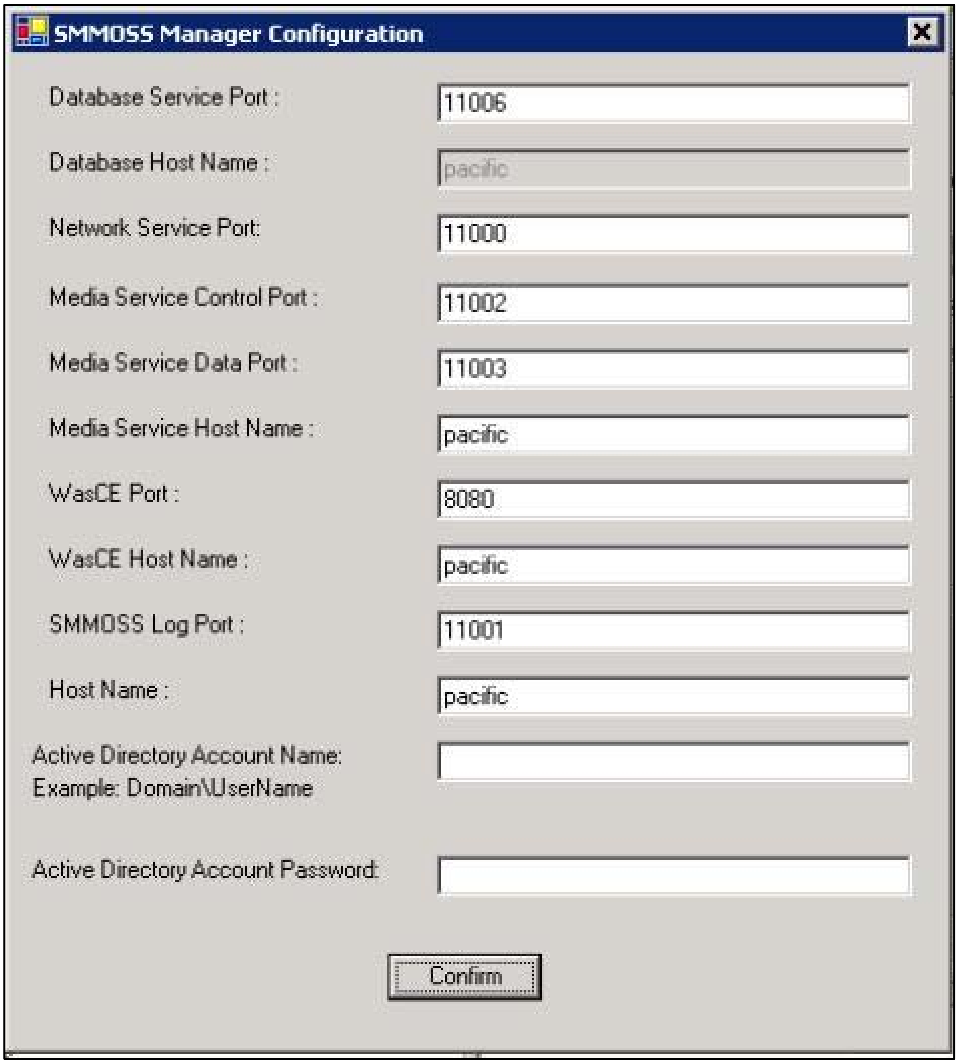
Tip: Always install the SnapManager for Microsoft Office SharePoint Server manager before installing the control and member agents. This will save time in having to configure these agents later to associate them with the correct SnapManager for Microsoft Office SharePoint Server manager. In addition, you can be assured of having the correct port numbers that the agents and the manager will use to communicate with each other. Also, you can test these port numbers.

Best practice: It is always advisable to leave the port settings and database hostname settings at the default values. This is because the same port numbers are also used to populate the settings for the agents. Unless there is a conflict in port numbers, leave them as default values.

Best practice: The account specified here allows the software to enumerate Active Directory® accounts so that they have access to the SnapManager for Microsoft Office SharePoint Server software. The Active Directory accounts must be associated with SnapManager for Microsoft Office SharePoint Server before they can be used to log in to the software. The initial login after installing SnapManager for Microsoft Office SharePoint Server manager is:

```
USERNAME  :  admin
PASSWORD  :  admin
```

It is recommended that the default password be changes immediately after installation. Moreover, this username is not a domain user, and it is highly recommended that domain logins be added and subsequently used to log in to the SnapManager for Microsoft Office SharePoint Server manager.



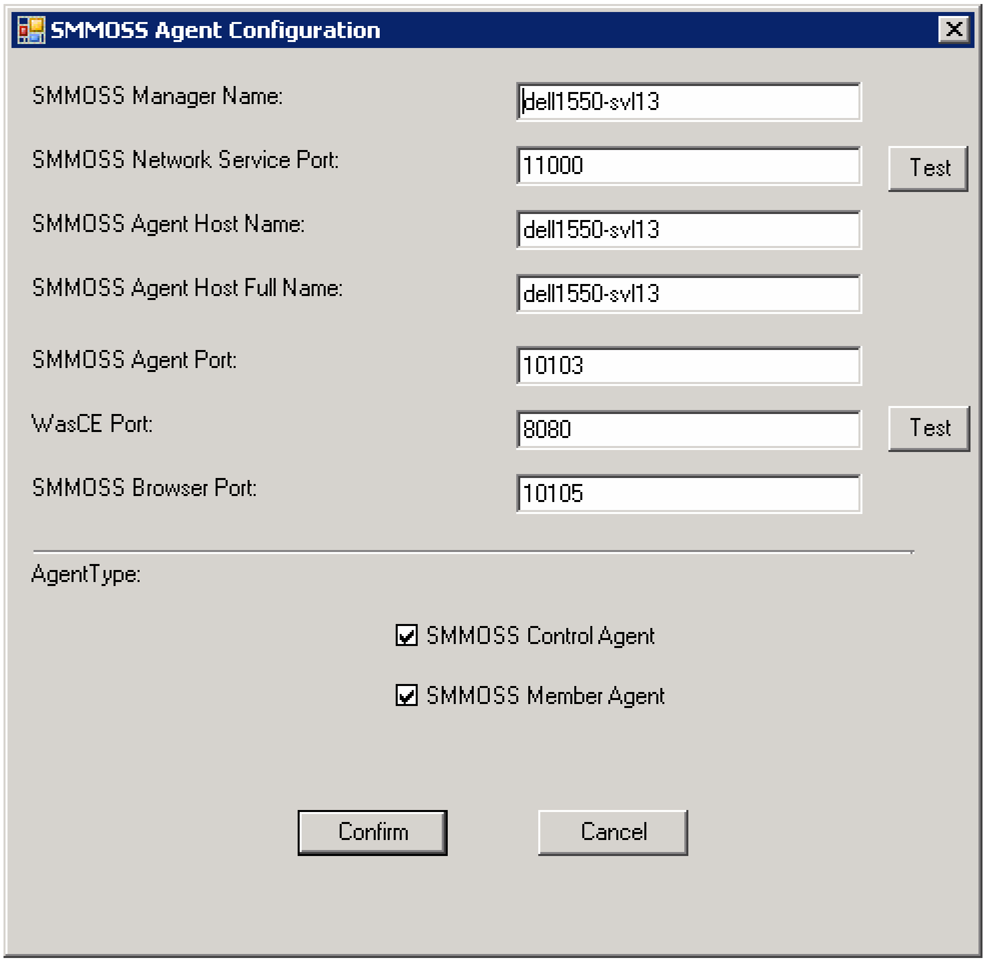
SMMOSS Manager Configuration

Database Service Port :	11006
Database Host Name :	pacific
Network Service Port:	11000
Media Service Control Port :	11002
Media Service Data Port :	11003
Media Service Host Name :	pacific
WasCE Port :	8080
WasCE Host Name :	pacific
SMMOSS Log Port :	11001
Host Name :	pacific
Active Directory Account Name: Example: Domain\UserName	
Active Directory Account Password:	

Figure 4) SnapManager for Microsoft Office SharePoint Server manager configuration screen.

5.2 CONFIGURING CONTROL AND MEMBER AGENTS

Figure 5 shows the fields that you use in configuring the SnapManager for Microsoft Office SharePoint Server control and member agents. The configuration dialog box opens at the time of installation. In addition, it can also be accessed at any time from the Agent Configuration Tool on the Start menu.



SMMOSS Agent Configuration

SMMOSS Manager Name: dell1550-svl13

SMMOSS Network Service Port: 11000

SMMOSS Agent Host Name: dell1550-svl13

SMMOSS Agent Host Full Name: dell1550-svl13

SMMOSS Agent Port: 10103

WasCE Port: 8080

SMMOSS Browser Port: 10105

AgentType:

☑ SMMOSS Control Agent

☑ SMMOSS Member Agent

Figure 5) SnapManager for Microsoft Office SharePoint Server agent configuration screen.

Best practice: When specifying the domain account under which the control and member agents will work, ensure that it has enough permission to query Microsoft Office SharePoint Server 2007 in order to discover the SharePoint layout. In addition, this account must have enough rights to access the content databases on SQL Server™. This means that the account can either have sysadmin rights on SQL Server or database owner rights on multiple content databases. It is best to create a special domain account or a special domain user group for this purpose to ease administrative overhead.

Best practice: Always install the control agents on a server that is separate from the one on which the SnapManager for Microsoft Office SharePoint Server manager is installed. The manager needs resources to handle multiple control agents (disk, CPU, network bandwidth, and so on). Moreover, this arrangement presents a layout that is more resilient to single points of failure.

Tip: It is best to have the member agent installed on a different box too, but this depends on the location of the SQL Server instance that houses the content databases of a Microsoft Office SharePoint Server 2007 farm.

The location of the member agent is governed by the placement of the SQL Server instance that houses the content databases. It is therefore evident that at least one control agent and one member agent are needed per SharePoint farm. The number of member agents is directly related to the number of SQL Server instances in the farm. One SnapManager for Microsoft Office SharePoint Server manager on its own can handle multiple control and member agents.

5.3 CONFIGURING THE MEDIA SERVER

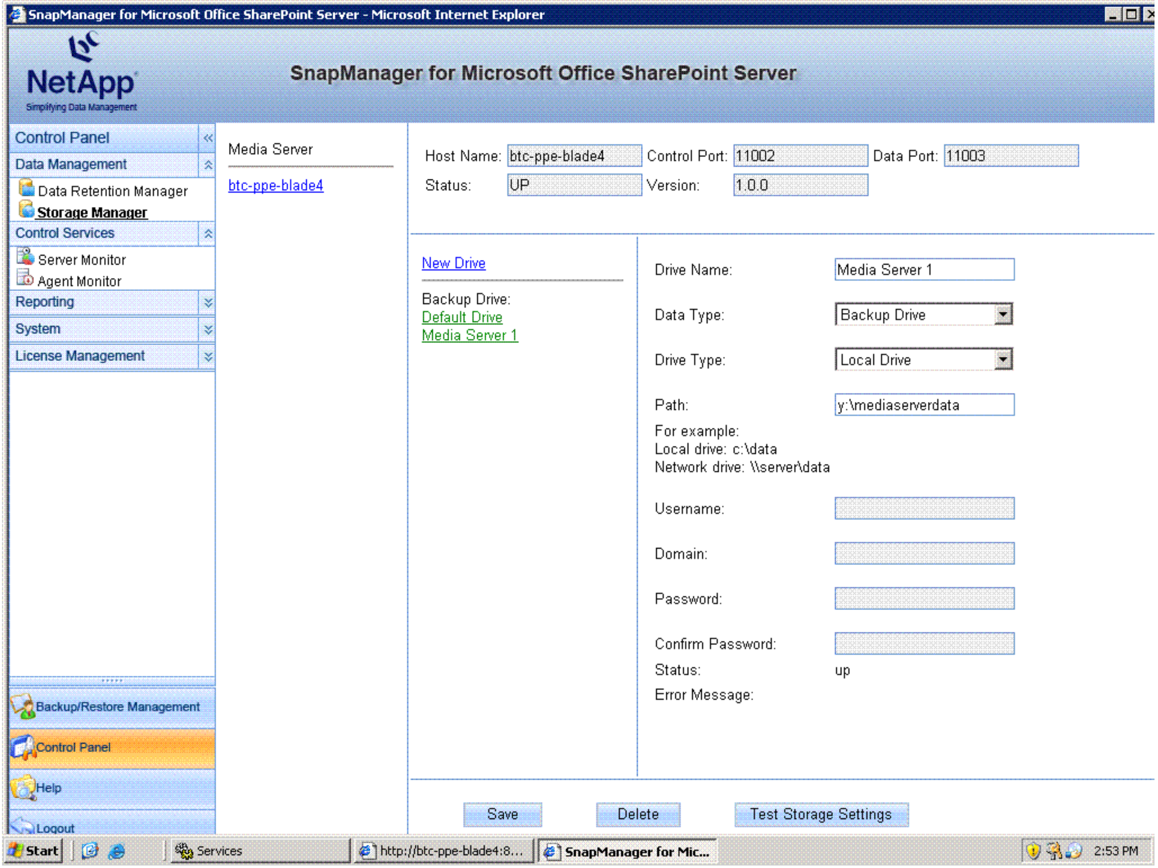
The media server is at the heart of the SnapManager for Microsoft Office SharePoint Server technology; it provides the ability to create backups at multiple levels of granularity. This means that the media server fulfills the following tasks in the overall SnapManager for Microsoft Office SharePoint Server functionality:

- Indexing the backup set to provide appropriate levels of granularity
- Storing the metadata related to backup sets and their corresponding indexing

The key aspect of the media server is the location that the administrator chooses to store the metadata. Figure 6 shows the GUI that is used to configure the storage.

The metadata stored on the media server is the most crucial piece of data for restore operations in SnapManager for Microsoft Office SharePoint Server. In fact, the restore process uses the media server’s metadata to locate all of the backup sets created for a specific SharePoint Web application. Moreover, the backup set’s index provides the ability to browse a data set and choose the correct granularity of restore. Therefore the media server’s data store is the most crucial element of all SnapManager for Microsoft Office SharePoint Server operations and needs to be given the highest possible level of data protection.

The media server’s data store can be located on either a local drive or a shared folder. By default it is located at C:\Program Files\NetApp\SnapManager for SharePoint Server\VaultServer\SMMOSSMedia\data. However, it can also be configured to reside on NetApp volumes on which a LUN is created.



Host Name: btc-ppe-blade4 Control Port: 11002 Data Port: 11003

Status: UP Version: 1.0.0

Drive Name: Media Server 1

Data Type: Backup Drive

Drive Type: Local Drive

Path: y:\mediaserverdata

For example:
Local drive: c:\data
Network drive: \\server\data

Username:

Domain:

Password:

Confirm Password:

Status: up

Error Message:

Figure 6) Configuring the media server drive.

Best practice: It is best to create the media server drive on a NetApp volume on which a LUN is created. This enables the administrator to enforce data protection and data recovery strategies by using SnapMirror®, rolling Snapshot™ copies, and so on. This allows effortless recovery of the media server metadata in case the primary storage location fails.

6 THE PROBLEM AND THE SOLUTION

Microsoft SharePoint products and technologies are widely popular and have helped everyone from entire organizations to virtual teams to communities of users, to collaborate and communicate more efficiently and effectively than ever before. Because of this, Windows® SharePoint Services and SharePoint Portal Server are at the top of the list of mission-critical tools.

Unfortunately, very few organizations have well-documented SharePoint backup and recovery plans. Those that do have such plans generally focus on full disaster scenarios that involve the loss of an entire environment. These plans usually do not focus on item-level backup and recovery, despite the fact that item-level problems are significantly more commonplace and much more likely to occur than a full disaster.

When item recovery does become necessary, it is usually accomplished by the reuploading of content. However, such reuploading causes loss of content history, along with other metadata issues, and destroys many of the benefits that formed the basis of putting the content in a SharePoint environment in the first place.

There has been much buzz about the enhanced features available in Microsoft Office SharePoint Server 2007, particularly in the areas of backup and recovery. Although enhanced backup and recovery tools such as a recycle bin and differential backups have been introduced, they do not completely satisfy the needs of SharePoint administrators. Administrators require tools that allow fast restore capabilities at the portal, site and item level. Because of these requirements, a third-party backup and restore tool is still necessary in most Microsoft Office SharePoint Server 2007 environments.

Use Case 1: Fast, Space-Efficient Backup

With almost any application, two things are critical when it comes to backup:

- **Speed:** You can’t afford to have your SharePoint application off line for extended periods during backups.
- **Space efficiency:** The less space your backup takes, the more backups you can retain.

A unique advantage of the new SnapManager for SharePoint application is the ability to leverage NetApp Snapshot technology to back up only those data blocks that have actually changed.

To create a Snapshot copy, SnapManager first ensures that the SharePoint repository resides on NetApp storage and that all cached data and metadata has been flushed from memory to disk (a consistency check point). Then SnapManager initiates a Snapshot copy to rapidly back up the underlying SQL Server data as well as associated metadata. The Snapshot process takes only a few seconds, so normal operations should not be disrupted. (By comparison, the native backup capability in SharePoint Server 2007 is very resource intensive, and Microsoft doesn’t recommend running it while a system is handling transactions.)

A NetApp Snapshot copy doesn’t consume additional disk space until changes are made to the repository. For example, suppose that an existing file is modified and saved to disk. A Snapshot backup keeps file system pointers to the old unchanged blocks and to the new blocks representing the changed data. These blocks are protected until the Snapshot copy that depends on them has been deleted. Because unchanged blocks are not recopied to disk for backup, the NetApp approach to Snapshot copies is very space efficient and can enable 250+ Snapshot copies in a single storage volume.

Once a Snapshot copy is created you have multiple options:

- You can retain the Snapshot copy on primary storage.
- You can back up the Snapshot copy to tape.
- NetApp SnapVault® can be used to back up the Snapshot copy to secondary disk storage.

- NetApp SnapMirror can be used to replicate the Snapshot copy to a disaster recovery site for end-to-end data protection.

All of these options occur on the storage system with no impact on the SharePoint application. By moving the protection of the SharePoint data off the application server, NetApp minimizes risk of unforeseen downtime.

As an example of the benefit of fast and nondisruptive backup, suppose that a user accidentally infects the SharePoint document repository with a virus. Recovery from a traditional nightly backup might result in the loss of up to a day's worth of changes and could take hours. Having hourly backup Snapshot copies enables you to revert to the backup set created immediately before the infection occurred or to simply recover an uninfected version of the affected file or files (depending on the severity of the problem), all in minutes.

Use Case 2: Granular Recovery

The native SharePoint Server 2007 recovery capability is limited to restoration of the content database at the SharePoint site level. Even if you want to recover only a single file, you must restore the content database to a nonproduction server and then manually copy the file back to the production server, a time-consuming process that results in loss of the SharePoint metadata.

SnapManager enables SharePoint Server 2007 recovery at *any* level of granularity, from the database level all the way down to a single item, nondisruptively, while the SharePoint application server is online. For instance, suppose that you lost a particular version of a file from several months ago. SnapManager enables you to search for the file by name. When you search on the file name, all of the Snapshot copies that contain the file are displayed so that you can choose the appropriate version of the file and recover it. The file metadata is recovered along with the file, and the whole process is nondisruptive to other SharePoint activity.

Similarly, if you are restoring a particular folder or subsite, you can navigate to it in a SharePoint tree structure in the user interface and select the object to be recovered. Because you are restoring the data from a Snapshot copy on disk, the recovery proceeds much faster than with other alternatives.

If you are mirroring to a remote site for disaster recovery, breaking the SnapMirror relationship makes the destination writable. User access can be shifted to SharePoint volumes at the remote site until activity is restored at the primary site. This minimizes user disruption and data loss.

Best practice: It is best to use site-level granularity only for weekly or nightly backups. For intraday backups, choose either item-level or item version–level granularity in the backup set. This practice localizes the impact on a particular SharePoint site to just the concerned document library, in case only a few documents need to be restored,

Best practice: Always mirror the content database volume to enable disaster recovery. This also ensures that the backup sets created for the content database are available even if the primary storage fails completely.

Best practice: Ensure that nightly backups are always verified. Verification is an expensive process and uses a fair amount of computation resources. Therefore it is best to configure a separate verification server for SnapManager for SQL Server to ensure faster verification of the content database backups.

Use Case 3: Single Interface Based on SharePoint

Another benefit of SnapManager is that its centralized interface is very familiar to SharePoint administrators; you don't have to know how the Microsoft SQL Server database that underlies SharePoint Server 2007 is laid out or anything about the underlying NetApp storage system. The look and feel of the GUI are the same as if you were browsing your SharePoint environment. You simply locate and select the items you want to back up or recover. SnapManager translates those actions to the appropriate underlying actions on the database server and storage system.

In addition to backup and recovery, SnapManager also provides the ability to create backup and retention policies as well as create and manage SharePoint users, groups, and permissions. You can create up to six backup schedules and associate a retention policy with each schedule. For instance, you might have a separate schedule with a separate retention policy for hourly, daily, weekly, and monthly Snapshot copies. A verify option instructs SnapManager to verify any backup after it is created.

From the centralized SnapManager GUI, you can also manage a SharePoint infrastructure spanning multiple sites. A plan can be defined for each site that includes site-specific backup and retention policies with six unique backup schedules per site, as described earlier. A built-in logging mechanism enables you to run reports on the success of all backup and recovery jobs.

7 RESTRICTIONS AND LIMITATIONS

7.1 STORAGE SYSTEMS

- Automatic provisioning via resource pools requires Data ONTAP® 7.0 or later for flexible volumes and Data ONTAP 6.5 or later for traditional volumes.
- Mirroring prefers that source and destination run the same Data ONTAP version.
- Backup and mirroring require Data ONTAP 6.5.6 or later.
- SnapManager for Microsoft Office SharePoint Server adds no new Data ONTAP licensing requirements: the storage system still needs SnapVault and SnapMirror licenses to enable vaulting or mirroring.

7.2 SNAPMANAGER FOR MICROSOFT OFFICE SHAREPOINT SERVER LIMITATIONS

- The current version of SnapManager for Microsoft Office SharePoint Server does not allow out-of-place restore of SharePoint sites. This means that the restore operations overwrite the appropriate contents of the current site (depending on level of granularity).
- The current version of SnapManager for Microsoft Office SharePoint Server is not integrated with SnapMirror or SnapVault.
- SnapManager for Microsoft Office SharePoint Server does not allow a specific content database to be a part of more than one backup plan.

8 MICROSOFT OFFICE SHAREPOINT SERVER BEST PRACTICES

- Manage content growth through site quotas and monitoring solutions such as Microsoft Operations Manager 2005 or the newer System Center Operations Manager 2007.
- Use site collections to scale SharePoint to varying groups with different security needs.
- Use IIS virtual servers (IIS Web sites) to manage varying types of Web-based access to SharePoint sites, such as SSL encryption or different host headers.
- If clustering is not an option, consider SQL Server 2005/2000 log shipping for simple redundancy of SharePoint data.
- If the full level of scalability with SQL Server 2005/2000 is required, use the Enterprise Edition of the software and the Windows Server 2003 operating system.
- Utilize SharePoint farms to provide scalability beyond single server SharePoint environments.
- Don’t deploy more than four search or four index servers in a single SharePoint farm.
- Consider the use of network load-balancing failover technology on the front-end SharePoint Web servers of midsize to large SharePoint deployments.
- Deploy Microsoft Cluster Server clustering technology for the database servers of large SharePoint deployments.
- Use Office 2007 components at the client level for the best integration with SharePoint technology.
- Deploy Microsoft Office SharePoint Server 2007 with Exchange Server 2007 for the most robust messaging and collaboration environment.
- Integrate SharePoint with BizTalk® Server 2006 to control, manage, and centralize access to business process data, allowing intelligent business decisions to be made more easily.
- Use SharePoint document libraries to address the problems of redundant creation of documents and inefficient document collaboration in an environment.
- Utilize the SharePoint search and indexing capabilities to efficiently search across different types of content.

- Use SharePoint document libraries and versioning to avoid excessive use of e-mail attachments during document collaboration.
- Utilize metadata in document libraries to organize or classify content.
- When users need to collaborate on a project, deploy and utilize the features of a Windows SharePoint Services team site, such as document libraries, meeting workspaces, task lists, and discussions.
- Use Microsoft Office SharePoint Server 2007 to index external content sources for creating a corporate intranet solution that provides centralized access to information and processes.
- Utilize the extranet features of Microsoft Office SharePoint Server 2007 to manage content directed to customers outside an organization.

9 SUMMARY

SnapManager for Microsoft Office SharePoint Server is backup and replication management software for a NetApp disk-based data protection environment. SnapManager for Microsoft Office SharePoint Server delivers assured data protection and higher productivity by providing policy-based management, including automated data protection setup.

With an automated policy in place, administrators can move and manage data in a logical rather than a physical way and are provided a long-term solution to the growing problem of storage device backup and migration.

APPENDIX: ADDITIONAL REFERENCES

Microsoft Office SharePoint Server 2007

www.microsoft.com/sharepoint/default.mspx

Microsoft Office SharePoint Server 2007 Home Page

TechNet Webcast: Disaster Recovery Planning for Office SharePoint Server 2007 (Level 200)

SnapManager for Microsoft Office SharePoint Server
NetApp SnapManager for Microsoft Office SharePoint Server 1.0 Installation and Administration Guide
SnapManager for SQL Server Best Practices Guide

SnapDrive for Windows
SnapDrive® for Windows 5.0 Installation and Administration Guide

SnapDrive for Windows Best Practices Guide

Data ONTAP
Data ONTAP System Administration Guide

Data ONTAP Storage Management Guide

NetApp SnapMirror
SnapMirror How-To Guide

SnapMirror Best Practices Guide

Database Layout with Data ONTAP 7G