NETAPP TECHNICAL REPORT

SnapManager for Microsoft Office SharePoint Server: Backup and Recovery Guide

Sourav Chakraborty, NetApp
October 2008 | TR-3715

EXECUTIVE SUMMARY

Innovative NetApp® technologies enable organizations to extract benefits out of their SharePoint® deployments in the area of backing up and restoring these. The various technologies empower the SharePoint administrator to design a robust backup management strategy to protect the organization's SharePoint resources.

NetApp provides industry-leading solutions in the areas of data protection; thin storage provisioning; data deduplication; file-based backups; instantaneous SharePoint site backup and restores; and nondisruptive restores, application development, and training purposes.

The intent of this document is to educate users in the internals of SnapManager® for Microsoft® Office SharePoint Server (SMMOSS) to enable them to fully harness its full potential as an effective backup management utility for Microsoft Office SharePoint Server (MOSS).

TABLE OF CONTENTS

1 INTRODUCTION TO SNAPMANAGER FOR MICROSOFT OFFICE SHAREPOINT SERVER

SnapManager for Microsoft Office SharePoint Server (SMMOSS) software is a complete backup and restore solution for SharePoint sites. It couples the power of NetApp Snapshot™ technology with one of the most flexible site restoration features. SMMOSS not only allows for the backups to be extremely fast and space efficient, it also provides for a restore functionality that allows the SharePoint administrator to perform item-level restore.

The value propositions for SMMOSS are as follows:

- Provides a unified management platform for managing backup and restore for multiple SharePoint farms.
- Performs auto-discovery of SharePoint infrastructure inside SharePoint farms. This involves discovering the Web applications and their corresponding content databases.
- Allows the user to perform item-level restore that localizes the business impact of a restore operation to the items being recovered.
- Allows out-of-place restore, which allows the backup created for a particular SharePoint site to be restored to a completely different SharePoint farm.
- Both backup and restore operations use NetApp Snapshot technology, which empowers SMMOSS with speed, reliability and robustness.
- Role-based access controls enable secure environment.
- SMMOSS allows great flexibility in scheduling both backups and restores.

Primarily, SnapManager for Microsoft Office SharePoint Server addresses all of the shortcomings inherent in the native backup and restore functionality in Microsoft Office SharePoint Server 2007. SMMOSS further extends the administrator's ability to efficiently manage the SharePoint environment.

2 THE SMMOSS ARCHITECTURE AND LICENSING PROCEDURE

2.1 DEFINITION OF SMMOSS COMPONENTS

In this section we will look at the architecture of SMMOSS and the different components that it includes.

SMMOSS has been designed from ground up with two major objectives:

- Centralized management of backup and recovery for multiple SharePoint farms
- Minimal need for manual actions and maximal automation of the backup and recovery process

In order to fulfill the above aims, SMMOSS makes use of an agent-based architecture. These agents not only help provide centralized management but automate most of the mundane tasks of backup and recovery.

SMMOSS consists of the following components:

- SMMOSS Manager
- SMMOSS Media Server
- SMMOSS Control Agent

1. SMMOSS Member Agent

Let us now define each of the above components, discuss their roles, and understand the core architecture of SMMOSS. The following are the brief definitions of each component:

- **SMMOSS Manager:** The centerpiece of the SMMOSS suite is called the SMMOSS Manager. It is responsible for providing a central backup/restore management by utilizing the services of the control and member agents (discussed later). It also provides the central graphical user interface (GUI) for that the user to initiate backup and restore tasks for SharePoint Web applications.

- **SMMOSS Media Server:** This component generates and stores various artifacts related to a SharePoint Web application's backup set. Primarily this includes backup set indexes and backup set metadata.

- **SMMOSS Control Agent:** This is a component that runs as a service on each MOSS Web front-end (WFE) server and is responsible for discovering the SharePoint Web applications that run on that WFE. It also is responsible for initiating backup and restore tasks for the Web applications on its respective WFE server. It does this with the help of member agents.

- **SMMOSS Member Agent:** This is the component that actually performs the backup or restore task by using commands based on SnapManager® for SQL Server® (SMSQL). The reason SMSQL is needed is because only SMSQL is capable of backing up or restoring SQL Server databases and SharePoint Web applications use a special SQL Server database (content database) to store all their contents.

From the pervious definitions, the idea that one tends to get is that SMMOSS is an agent-based solution. This in fact is the reason why SMMOSS is able to provide a reasonably automated solution for backup and recovery of MOSS sites.

2.2 THE SMMOSS ARCHITECTURE

In this section we have a look at how all the components come together and communicate with each other. In Figure 1 we present the overall architecture of the SMMOSS software that depicts all its components and their relationships.

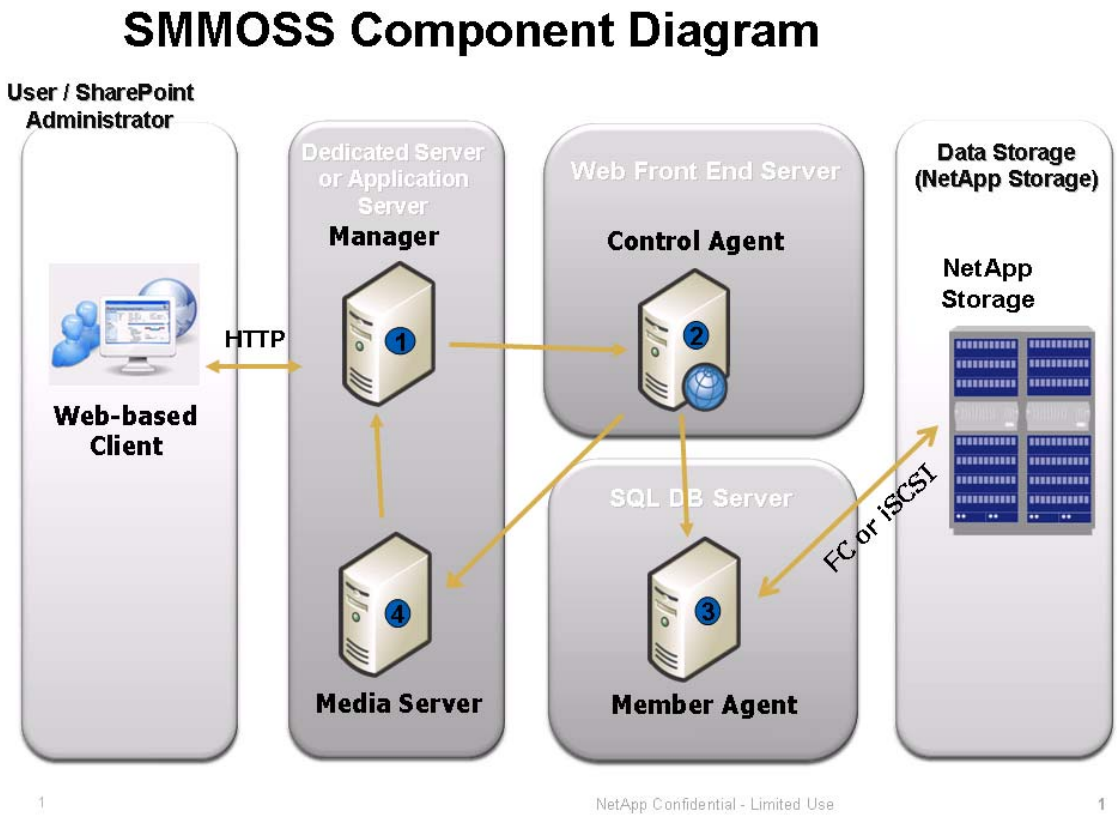

Figure 1) The SMMOSS architecture.

The central piece of the SMMOSS software is the SMMOSS Manager that is used to manage multiple SharePoint WFEs. This is the most unique feature of SMMOSS since it provides a truly centralized

management system for backup and recovery of SharePoint sites. The user initiates backup/recovery of SharePoint sites and performs other administrative tasks related to SMMOSS through this central GUI. As shown in the picture, one or more control agents communicate with the SMMOSS manager through the use of TCP/IP ports.

The media server is the component that is responsible for the generation and storage of various artifacts related to a SharePoint Web application's backup set. Primarily this includes backup set indexes and backup set metadata. The information stored on the media server is extremely crucial to make sure that the backup set is useful for restore operations. Media server might or might not reside on the same host as the SMMOSS manager. Further sections will discuss the best practices around this.

As mentioned before, the component that is responsible for discovering the layout of SharePoint Web applications on a WFE is the control agent. SMMOSS deployment needs exactly one control agent per SharePoint WFE server. The control agent performs the following two major tasks:

- Discover the number of Web applications running on the WFE server and discover their content databases and which SQL Server instance they are located on.
- To communicate with the member agents as a part of initiating backup and restore of the SharePoint Web application.

The control agent uses TCP/IP ports to communicate with the member agent and the media server.

The last piece of the SMMOSS software is the member agent. The member agent accepts a backup/restore request from the control agent, forms the appropriate SMSQL command, and then passes it to the SMSQL instance on the SQL Server host. SMMOSS deployment needs exactly one member agent per SQL Server host. The SMSQL software must also be installed on the SQL Server host.

The control agent uses TCP/IP ports to communicate with the control agent.

Hence, we can summarize by saying that SMMOSS is a completely agent-based solution. Agents are specific in their functionality and interactions and maximize automation of the tasks performed by SMMOSS.

2.3 HOW LICENSING WORKS FOR SMMOSS

Due to its architecture, SMMOSS has a slightly more involved licensing procedure than most other SMAI products. This complexity is primarily due to the large number of components and services that SMMOSS is dependent on. In this section we present a complete discussion on all aspects of SMMOSS licensing.

As discussed in the previous section, SMMOSS primarily comprises of the following components: SMMOSS Manager, Control Agent, and Member Agent. Furthermore, SMMOSS is dependent on the following services for its operations: SMSQL, SDW, and SnapRestore®. Hence, it may be stated early on that all the above components and dependencies have to be accounted for in the licensing procedure for SMMOSS.

To make sure that SMMOSS is completely licensed, we need the following licenses:

SMMOSS license
SMSQL license
SDW license
SnapRestore license

In this section we will discuss each of the above licenses that are required for SMMOSS to run successfully.

Let's begin our discussion by looking at the SMMOSS license. A single SMMOSS license consists of one SMMOSS Manager license and five agent licenses. Five agent licenses implies that using one SMMOSS license, we can make sure that at most five agents are licensed. The key aspect is that the sum of control and member agents cannot exceed five but may be present in any combination that leads to their total to five.

As of the present release, SMMOSS has only server-side licensing, and no storage system-based licenses exist. This is understandably so because all the SMMOSS components live on the server side and do not use any storage system-based services directly. NetApp also provides a 30-day trial version of SMMOSS.

Further to our discussion about satisfying all the licensing requirements, we will have a look at the licensing needs for SMSQL, SDW, and SnapRestore. SMSQL can be licensed either in the per server mode or the per storage system mode. Typically it is common to license SMSQL in the per server mode since SQL Server instances on the same host can use different storage systems.

Licensing SMSQL on clustered Windows® hosts and for clustered SQL Server instances is somewhat of a gray area. It is important to understand that in Windows, any clustered service and the cluster service itself always run in the active-passive mode. The reason for this is that Windows cluster does not allow shared usage of cluster resources such as quorum disks, shared drives, and so on. This means that a clustered SQL Server instance will be alive on at most one of the cluster nodes. In this scenario, in case of per server licensing, only one SMSQL license is needed to manage the clustered SQL Server instance. However, for all nonclustered SQL Server instances running on individual cluster nodes, we need one license per node depending on which nodes these SQL Server instances run on.

In the last portion of this section, the licensing needs for SDW and SnapRestore are discussed along with a discussion on the different product bundles that available for SMMOSS. SDW always uses the per server license mode and needs to be licensed on every host that wants to use LUNs. In an SMMOSS deployment this would typically be the SQL Server host and in some cases the media server host. SnapRestore is a Data ONTAP® component and has to be licensed per storage system. SnapRestore needs to be licensed on all the storage systems that are being used by SQL Server to store data and also on the storage system that is being used by the media server to store data.

In order to enable first time users of SMAI products to use SMMOSS of the shelf, NetApp offers the SMMOSS solution bundle. This package contains one SMMOSS license, one SMSQL license, and 1 SDW license. Furthermore, NetApp also offers the NetApp Select™ package that contains one SMMOSS license, one SMSQL license, one SDW license, and one SnapRestore license.

2.4 EXAMPLE OF SMMOSS LICENSING

Let us assume we have a MOSS environment that has four Web front-end servers and six SQL Server host machines. Let us assume that the content databases are spread over four storage systems. For this example we will consider that media server data resides on a separate storage system and is accessed by mapping a LUN to the media server host.

So by the above definitions of components and their licensing requirements, we will need the following licenses:

Number of control agents = 4
Number of member agents = 6
Hence, total number of agents = 4 + 6 = 10

Therefore, number of SMMOSS licenses needed is two. This is because each SMMOSS license covers only five agents. Note that two SMMOSS licenses will cover two SMMOSS Managers/Media Server licenses and hence, we need no extra licenses here.

Number of SQL Server hosts = 6
Number of storage systems being used by the SQL Server hosts = 4

Therefore, number of SMSQL licenses needed is four (for per-storage system licensing) or six (for per-server licensing).

Number of SDW licenses needed = 7 (6 + 1)
This is because we will need one SDW license per SQL Server host, which makes six SDW licenses and one extra SDW license for the media server host.

Number of SnapRestore licenses needed = 5 (4 + 1)
This is because we will need one SnapRestore license for each of the four storage systems being used by the SQL Server hosts and one extra SDW license for the storage system being used by the media server host.

3 DEPLOYING SMMOSS

In this section we focus on three major areas of SMMOSS deployment: common SMMOSS deployments, port communication architecture for SMMOSS components, and security provisions in SMMOSS.

3.1 COMMON SMMOSS DEPLOYMENTS

In this subsection, we will examine important patterns that exist in MOSS deployments. The subsection will then discuss the corresponding deployment of SMMOSS components for each of the MOSS deployments. Although there might be other examples of MOSS deployments, this section aims to discuss the most prevalent of these, and it is hoped that the key concepts behind SMMOSS deployments will be understood by the reader.

CASE 1: SINGLE SHAREPOINT SERVER

In this scenario, all the components of MOSS—Web FSE, IIS, SQL Server 2000/2005, and indexing server—are present on one physical host. Normally, this sort of a deployment exists in lightly loaded (for example, smaller departments) or test/dev environments.
In this case, the following SMMOSS components have to be on the same host as the one that has MOSS installed on it:

- SMMOSS Control Agent
- SMMOSS Member Agent

The SMMOSS Manager and Media Server might or might not reside on the same host mentioned above. The decision for this will depend on the following factors:

- Number of SharePoint farms that are being managed using the SMMOSS manager
- Backup schedules
- Whether backup-set Indexing is regularly done and the corresponding sizes of the SharePoint Web applications

CASE 2: WELL-DEFINED SERVER ROLES IN A SHAREPOINT FARM

In this scenario, all the components of MOSS—Web FSE, IIS, SQL Server 2000/2005, and indexing server—are present on different physical hosts. Different hosts may talk to one another as a part of forming a large SharePoint infrastructure. Such deployments are more commonly used in large enterprises that use SharePoint.

In this case, the following SMMOSS components have to be on the same host as the one that has the MOSS WFE installed on it:

- SMMOSS Control Agent

Furthermore, the following SMMOSS components have to be on the same host as the one that has the SQL Server instances installed on it and houses the content databases:

- SMMOSS Member Agent
- SnapDrive® for Windows

Note that the two components mentioned above have to be installed on each node in a cluster for clustered SQL Server instance. In case the setup only has a Windows cluster with standalone SQL Server instances on some of the nodes, then the two components mentioned above need to be installed on each host that has a SQL Server instance that houses content databases.

Preferably, the SMMOSS Manager and Media Server should be put on a dedicated host. The decision for this will depend on the following factors:

- Number of SharePoint farms that are being managed using the SMMOSS manager
- Backup schedules

- Whether backup-set Indexing is regularly done and the corresponding sizes of the SharePoint Web applications

Case 3: Demilitarized Zone-Based Installations
In this case, the only limitation is the presence of some of MOSS components, in most cases the MOSS Web FSE, in an external public domain that has sufficient trust relationships established with the internal corporate domain. Generally the IIS and SQL Server hosts are in the corporate domain.

Note that apart from the presence of two distinct Windows domains, this deployment will be similar to case 2 in how the different MOSS components are placed. In this case, the only care that must be taken is that the adequate ports must be opened on each host and allowed to pass through the firewall that exists between the external and internal domains.

Section 3.2 discusses the ports that are used by the different components of SMMOSS.

3.2 PORT COMMUNICATION ARCHITECTURE OF SMMOSS

All SMMOSS components use TCP/IP ports to communicate between each other. This method of communication makes sure that communication between the agents can flow easily even with complex deployment scenarios such as demilitarized zone (DMZ) deployments where the MOSS WFE server is typically present in an external public domain and the application and database servers are in the internal private domain.

As discussed before, there are four major components of SMMOSS: SMMOSS Manager, Media Server, Control Agent, and Member Agent. The following figure shows the major information exchanges that happen between SMMOSS components.

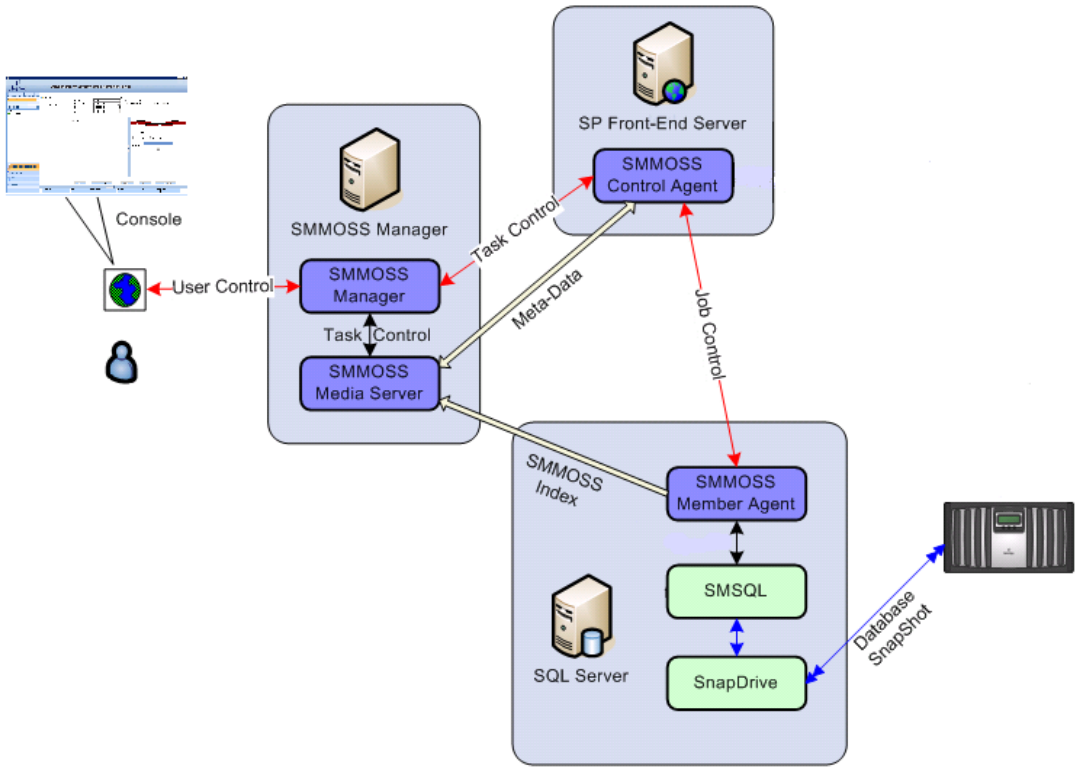

Figure 2) Flow of Information between the different SMMOSS components.[[NOTE: In figure 2, please change "SnapShot" to "Snapshot" (twice).]]

The default ports that are used by SMMOSS are as follows:

- SMMOSS Manager default ports: 11000, 11001, 11002, 11003, 8080
- SMMOSS Agents default port: 10103

All the above ports are configurable and can be assigned other values depending on availability of free ports. The port values can be changed from the SMMOSS Manager and Agent configuration tools. However, it is generally a best practice to use as many default ports as possible to make sure of minimal intervention while installing and configuring the SMMOSS manager and agent tools.

The following are the definitions of the ports which are used by SMMOSS to enable communication between its components:

- **Database service port:** This is the port that is used by the SMMOSS DB service to receive messages. The internal database is used by SMMOSS to store configuration information and other metadata. The default value for this port is 11006. This port needs to be open at the host where the SMMOSS manager is installed.

- **Network service port:** This port is used by the SMMOSS Manager to receive messages. The default value for this port is 11000 from agents. This port needs to be opened on the host where the SMMOSS manager is installed.

- **Media service control and data port:** These ports are used by the media server service to receive control and data messages. The default values for these ports are 11002 and 11003 for the control and data port, respectively. These ports need to be opened on the host where the media server service is installed. In most cases this is the same host as the SMMOSS Manager.

- **WasCE port:** This port is used by the Apache application server service to present the SMMOSS GUI to the user. The default value for this port is 8080. This port needs to be opened on the host where the SMMOSS manager is installed.

- **SMMOSS log port:** This port is used by the SMMOSS Service to write events to its logs. The default value for this port is 11001. This port needs to be opened on the host where the SMMOSS manager is installed.

- **SMMOSS agent port:** This is used by the SMMOSS agent services (control and member agents) to send and receive messages amongst themselves. The SMMOSS Manager also uses this port to send messages to the agent. The default value for this port is 10103. This port needs to be opened on the host where the SMMOSS agent is installed.

To summarize, we need the ports as mentioned in Table 1.

Table 1) Ports used by different SMMOSS components.

Component	Service Name	Default Port	Description	Internal
Manager	Web Service	8080	Web server for admin console	N
	Media Service Control	11002	Media service control messages port	Y
	Media Service Data	11003	Media service data transfer port	N
	Database Service	11006	Internal database server port	Y
	Net Service	11000	Communication port with agent	N
	Log Service	11001	Logger interface	Y
	Patch Service	11004	Patch update	Y
Agent	Communication Service	10103	Communication port with manager and other agents	N
	Browser	10105	Serve SharePoint structure browse requests	Y

Further, we may state the following about the port usage of SMMOSS components:

- Most of the ports are configurable and can assume user-defined values. However, it is best to keep as many default values as possible.
- The above mentioned ports need to be opened on the corresponding hosts and have to be opened on the firewalls as well.
- Following ports are used for communications between the manager and the agents:
  - Manager to agent: 10103
  - Agent to manager: 11000, 11003
  - Agent to agent: 10103

3.3 SECURITY IN SMMOSS

SMMOSS has a very comprehensive security model. It presently supports two security models:

- SMMOSS-based security: Here the logins are specific to SMMOSS and are internal to it. This is referred to as the local system mode of authentication.

- AD-based security: Here the logins used are domain-level logins and hence are authenticated by the active directory. This is referred to as the active system mode of authentication.

The SMMOSS security principles are categorized as follows:

- User: These are logins that are used to gain access to the SMMOSS interface. As discussed before, logins can either be SMMOSS-based (local) or AD-based (domain).

- Groups: Groups are specialized roles within SMMOSS that have certain specific access rights. There are three types of groups within SMMOSS: SMMOSS administrators, SMMOSS operators, and SMMOSS managers. Each user needs to be a part of any one of these three groups. SnapManager administrators is the group that has superuser privileges, and the initial default local login admin is also a member of this group.

Security in SMMOSS is managed through the Account Manager portion of the SMMOSS GUI, and this occurs under the Control Panel panel. Figure 3 presents the Account Manager section.

The SMMOSS-based user admin (password is also admin) is the default login that is present whenever SMMOSS is installed. This login is a member of the SMMOSS administrators group. This login is the only one that can be used to log into SMMOSS Manager for the first time. Subsequently, other users can be created and adequately placed in one of the three user groups that are mentioned above.

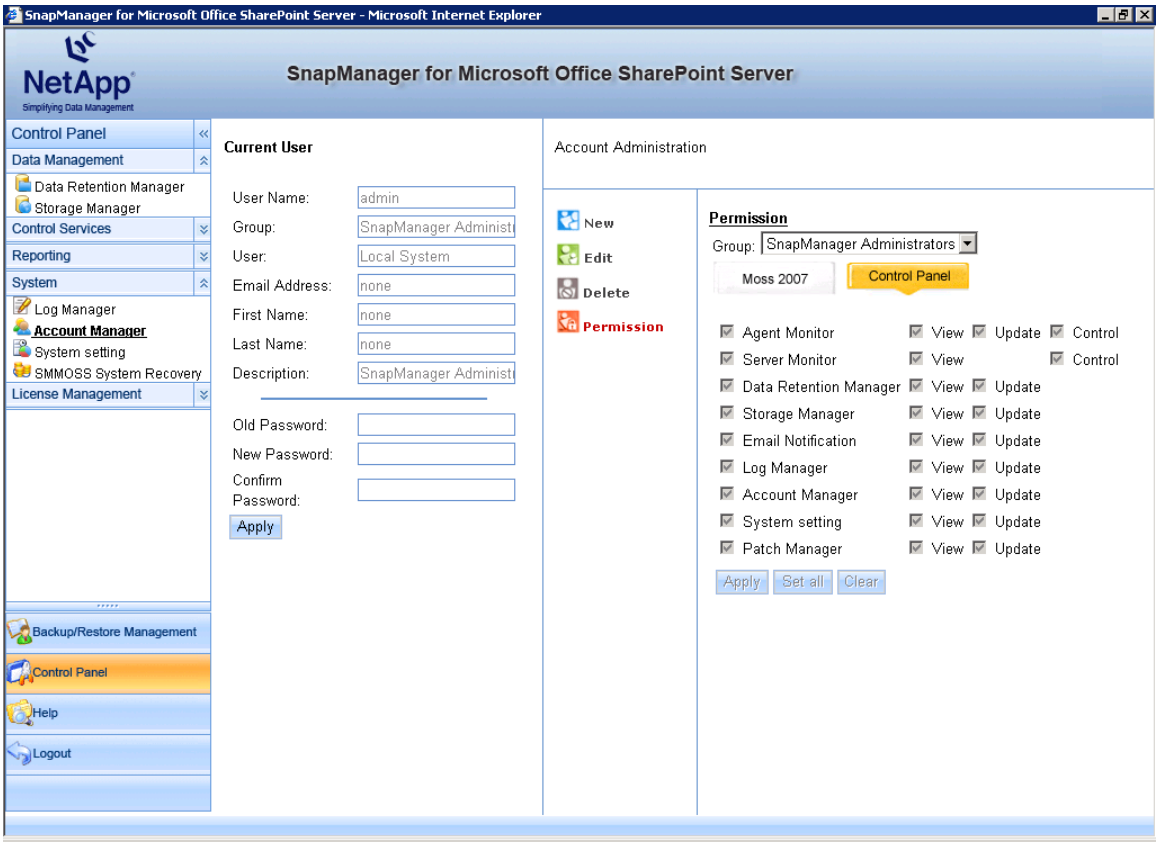

Figure 3) Account Manager.

4 SMMOSS SIZING

The most commonly asked question around any deployment of SnapManager products is how to size storage for the key components of SnapManager. In this section, we discuss the storage needs of the following components of SMMOSS:

- SMMOSS Media Server

Note that we will not discuss the storage sizing for MOSS since an in-depth discussion on this topic is presented in the TR titled **"**SnapManager for Microsoft SharePoint Server."

Similarly, the following TR talks in depth about sizing the SMSQL SnapInfo directory and the content database volumes: **"**Best Practices Guide: Microsoft SQL Server 2000/2005 and NetApp Solutions."

4.1 SIZING THE MEDIA SERVER

The media server is basically responsible for two major tasks:

- Indexing the backup set to enable granular restore
- Storing the indexes that are created above and storing the backup set metadata

The size of the indexes created by the media server depends on the level of granularity chosen while creating the backup set. There are five levels of granularity in SMMOSS, and these are site, web, folder, item, and item version. The definitions of each of these levels of granularity are as follows:

- Site: This level of granularity makes sure that individual root level sites within the SharePoint Web application can be recovered.

- Web: This level of granularity makes sure that subsite under the root level sites can be recovered.
- Folder: This level of granularity makes sure that document libraries and lists can be recovered.
- Item: This level of granularity makes sure that each item in the SharePoint Web application can be individually recovered. This includes lists, announcements, documents, calendars, events, and so on.
- Item version: This level of granularity makes sure that all versions of each item (especially documents) in the SharePoint Web application can be individually recovered. This includes lists, announcements, documents, calendars, events, and so on.

In a normal SharePoint Web application, as the level of granularity becomes finer, the number of objects that will have to be indexed will increase. This means that the size of the index increases as the granularity level becomes finer.

Normally, it is difficult to get a count of the number of objects at each level of granularity, and hence sizing the media server is very difficult. However, the size of each entry in the index is roughly 300 bytes. This information can be used to size the media server data store accordingly by observations. Note that the change in the number of objects increases as the level of granularity becomes finer. This means that we can closely determine the size of the media server indexes up till the folder granularity level by taking a few runs of the backup plan set at the required granularity levels and then checking the size of the index folder that is created.

The folder where SMMOSS stores the index created as a part of running a backup plan is located at <Media Server data path>\<Plan ID>\<Job ID>.
The PlanID of a backup plan may be found by clicking the View hyperlink of the job status row (in the BackupJob monitor) for the job. The same row also contains the JobID column.

If you choose to keep the SMMOSS Media Server on a NetApp LUN, then please size the volume accordingly. As of now, SMMOSS does not create Snapshot copies of the Media Server volume by itself. Hence, if you choose to create Snapshot copies of this volume manually, then the formula to size the Media Server volume will be as follows:

Volume size = (<LUN size * 2> + < change rate (adjusted to time between Snapshot copy creation) * number of Snapshot copies>)

It is advisable to have a dedicated volume for the SMMOSS Media Server to make sure that in the event of a disaster, the LUN can be easily and quickly recovered. The most important factor in the formula mentioned above is to calculate the data change rate (in MB per second). Although there is no direct method or tool to determine the change rate, one may do this by careful observation and following the steps below:

1. Determine the Index size of each backup plan by running it once and observing the size of the folder located at <Media Server data path>\<Plan ID>\<Job ID>.

2. Determine the time interval between creation of two Snapshot copies. Let's call this T.

3. Let the initial change rate C = 0.

4. For each backup plan do C = C + (index size for this backup plan as obtained in step 1) x (number of runs of this backup plan in T).

The final value of C (obtained from above) is the change rate between creation of two Snapshot copies. Different variations of this idea may be used as well.

5 BACKUP AND RESTORE USING SMMOSS

The key functionality of SMMOSS is to back up and restore SharePoint Web applications. All its components assist in various steps of this process. In this section we will discuss the way backup and restore work in

SMMOSS and the concepts associated with it. In addition, this section will also describe use cases of two new features in SMMOSS 1.1, out-of-place restore and system state backup.

5.1 HOW THE BACKUP PROCESS WORKS

The backup process in SMMOSS is a highly automated process and allows SharePoint administrators to easily back up a SharePoint Web application by either scheduling a backup or starting one on the fly.

In SMMOSS, a backup plan is the container for all backup related attributes for a given SharePoint Web application. This includes things like the content database being backed up, media server to be used, backup set retention policy, and so on. In addition, SMMOSS also allows six different schedules to be specified for a given backup plan. Note that as of now it is not possible to vary the granularity level of the backup for each of the six schedules.

Backups in SMMOSS are always full backups followed by a TLOG backup. In addition, up-to-the-minute restore capability is also maintained while creating the backup. The backup set may be verified or unverified depending on the option you choose while running the backup plan. In addition, backup sets are deleted as per the retention policy set for the backup plan.

The steps involved in completing a backup request for a SharePoint Web application are as follows:

1. A backup request is initiated by the user or by a scheduled backup plan.
2. The SMMOSS Manager then sends a backup request message to the appropriate control manager.
3. The control manager then queries the SharePoint Web application and finds out its content database(s) and the SQL Server instance and hostname on which it resides.
4. The control manager then initiates a backup request to the appropriate member agent that is present on the concerned SQL Server host.
5. The member agent then initiates an SMSQL based backup of the content database by forming the corresponding SMSQL command.
6. The SMSQL command prepared in step 5 is run by SMSQL, and a full backup of the content database along with a TLOG backup is taken.
7. If the Generate Index File option has been selected then the control agent instructs the SMMOSS Media Server to generate indexes for the backup set.
8. Subsequently, the metadata about the backup, for example, date-time, whether backup was verified, whether backup was completed, indexing level, and so on, is written to the media server.
9. As steps 1-8 proceed, entries are made to the SMMOSS log, and these can be viewed through the job status in the Job Monitor.

5.2 HOW THE RESTORE PROCESS WORKS

Although the restore process in SMMOSS is just the reverse of the backup process in a couple of ways, there are some differences in case backup set indexing is selected. In this subsection, we will discuss the restore process in detail.

The steps involved in completing a backup request for a SharePoint Web application are as follows:

1. The user initiates the restore process.
2. The SMMOSS Manager then presents the user with the media server and all the control agents that are tied to it. The reason for this is that the metadata for a backup is stored on the media server and backup plans are created with respect to a control agent.
3. When the user selects the appropriate control agent and expands it, a list of all the backup plans tied to it is shown. The user then selects the backup to use.

NOTE: Steps 2 and 3 depend on the media server to fetch all the metadata that is displayed.

4. As soon as the backup set is chosen, the backup set browser is enabled in the pane below. Now the user has two options:
    a. To choose to use the backup set index to navigate to and choose the particular object(s) to restore.
    b. Restore the complete content database.
5. If option a is chosen above then the following happens:
    i. SMMOSS Manager locates the correct control agent and sends it a restore request.
    ii. The control agent then sends a restore request to the concerned member agent and initiates an SMSQL restore of the database.

iii. Once, the member agent initiates an SMSQL based restore operation, SMSQL mounts the concerned Snapshot copy as a virtual disk.
iv. SMSQL then maps SMSQL to a free drive letter and restores the original content database (named “XXX”) as “XXX_temp.”
v. The control agent then streams out the contents from the “XXX_temp” database to the original content database named “XXX.” This is the reason why the restore does not affect the operations of any parts of the SharePoint Web application.

6. If option b is chosen, then the following happens:
   i. SMMOSS Manager locates the correct control agent and sends it a restore request.
   ii. The control agent then sends a restore request to the concerned member agent and initiates an SMSQL restore of the database.
   iii. Once the member agent initiates an SMSQL based restore operation, SMSQL first backs up the current transaction log to make sure of an up-to-the-minute recovery. Hence, it is important to have a verification server configured in SMSQL or the restore will fail.
   iv. Then SMSQL initiates a verification of the database in the Snapshot copy.
   v. Thereafter, if the verification is successful, SMSQL performs a standard database restore and applies the TLOG backup taken above.

5.3 BACKING UP CONTENT DATABASE WITH SMSQL AND SMMOSS

Backups in SMMOSS are essentially full backups of the content database, and hence, it is this full backup that forms the centerpiece of all discussions around SMMOSS backups. Since it is possible to take full backups from both SMMOSS and SMSQL, there are a number of questions around the practice of mixing the usage of SMSQL and SMMOSS in taking content database backups. This section analyzes and describes the facets of such a practice.

It is important to note that the best, most advantageous and strongly recommended practice is to use SMMOSS only for backing up SharePoint Web applications and thus the content database. Choosing to back up the content database using SMSQL has disadvantages as compared to using SMMOSS. The disadvantages are as follows:

- No notion of granularity of backup. This means that the restores will render the entire SharePoint Web application unavailable for the period of the restore.
- Not a centralized approach as the backup and restore needs to be initiated specifically from the SMSQL installed on the concerned SQL Server host.
- Auto-discovery of the SharePoint layout (specifically SQL Server related) cannot be availed. Hence, the user must have prior knowledge about the SQL Server layout that forms the back end for the SharePoint farm.

However, if a user still chooses to use both SMSQL and SMMOSS to back up a content database, the following best practices should be kept in mind:

- If TLOG backups are being taken through SMSQL and full backups through SMMOSS then note that all the TLOG backups that are taken after the full backup taken by SMMOSS are applicable to only that full backup.

- TLOG backups cannot be used by SMMOSS to do point-in-time restores. Hence, if you want to restore additional TLOG backups, then these will have to be done manually.

- In case you are using SMSQL to take full backups of a content database in addition to using SMMOSS then please be aware that SMMOSS is unaware of SMSQL-initiated backups and hence will not list these.

- In case SMSQL is used to perform a point-in-time restore outside of SMMOSS then it is recommended that a full backup be initiated from SMMOSS right after the PIT restore completes.

- Make sure that backup schedules between SMMOSS and SMSQL do not overlap since this might cause both backups to take longer to finish.

5.4 OUT-OF-PLACE RESTORE

The out-of-place restore feature is one of the new features that have been introduced in SMMOSS Version 1.1. By definition, the out-of-place restore feature allows the user to use the backup created for a SharePoint Web application at a particular SharePoint farm and restore from it to a completely different SharePoint farm.

This means that the backup set that is created by SMMOSS becomes independent of the SharePoint farm that it is associated with and extends the restorability of MOSS Web applications. The most important requirement for out-of-place restore to work is that the SMMOSS Control Agent should be installed on the MOSS WFE server of the destination MOSS farm. This allows for automated discovery of the destination farm to be done when out-of-place restore is chosen.

The way in which out-of-place restore works is as follows:

1. As a part of the process, the user specifies the target SharePoint site and the objects to restore from the source backup.
2. SMMOSS Manager then sends a restore request to the control agent of the source MOSS Web application.
3. The source control agent (from step 2) then sends a restore request to the concerned member agent and initiates an SMSQL restore of the database.
4. Once the member agent initiates an SMSQL based restore operation, SMSQL mounts the concerned Snapshot copy as a virtual disk.
5. SMSQL then maps SMSQL to a free drive letter and restores the original content database (named “XXX”) as “XXX_temp.”
6. The control agent then streams out the contents from the “XXX_temp” database to the content database located at the destination MOSS Web application.

Two very interesting use cases of out-of-place restore are:

- Moving MOSS sites up or down the site hierarchy
- Site migration of a MOSS site to an alternate SharePoint farm

In the first use case, the destination remains as the original SharePoint farm. Note that the out-of-place restore does not remove the original site or SharePoint object. It simply creates a copy of that at a new location. Hence, the deletion (if needed) of the original object has to be done manually through the site interface by an administrator. These use cases are very beneficial for design changes, site migrations to test/dev environment, creating redundant site deployments, and so on.

5.5 SMMOSS SYSTEM RESTORE

The SMMOSS system recovery feature is one of the new features that have been introduced in SMMOSS Version 1.1. The main usage of this feature is to make sure that critical data elements that constitute the SMMOSS software are backed up and can be restored in the future.

SMMOSS stores almost all critical configuration and operational data in an internal database named Derby. Therefore, the SMMOSS system recovery creates a backup of this database itself.

The default path for the SMMOSS system backup is C:\Program Files\NetApp\SnapManager for SharePoint Server\SMMOSSData. This is a configurable path, and the best practice is to make sure that the backup path exists on a NetApp LUN to make sure of maximum protection from disasters.

The SMMOSS system backup allows you to recover all the original system settings even if the SMMOSS manager is reinstalled on the host. The only requirement is that the backup path that existed in the previous installation be presented to the system recovery part of the software. Hence, this is another reason to make sure that the system backup path exists on a NetApp LUN so that the data is protected even if the SMMOSS Manager is uninstalled or gets corrupted.

6 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.

6.1 SHAREPOINT DISASTER RECOVERY USING SMMOSS

Most of today's businesses need high degrees of collaboration between different entities. Such collaborations involve a lot of document exchange, shared document access, Web-portal based information interchange, and document management. Microsoft Office SharePoint Server (MOSS) presents a technology that solves all the challenges of inter- and intraorganizational collaboration. Hence, it forms the backbone of many organizations in terms of providing a technical framework to drive such complex collaborations and workflows.

In order to deliver its objectives, MOSS uses the services of multiple components such as IIS, SQL Server, and so on. Of these components, SQL Server is an important one since it houses all the databases that are used by MOSS to store Web application data, configuration data, and so on. Hence, the core data repository for MOSS is SQL Server.

A technical report (TR-3714) has been published to deliver solutions related to disaster recovery model or Microsoft Office SharePoint server user sites using SnapManager for Microsoft Office SharePoint Server (SMMOSS) and SnapManager for Microsoft SQL Server (SMSQL).

APPENDIX A: 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