NETAPP TECHNICAL REPORT

Disaster Recovery Solutions for Microsoft Office SharePoint Server User Sites Using SnapManager for Microsoft Office SharePoint Server

Sourav Chakraborty, NetApp
October 2008 | TR-3714

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 de-duplication; file-based backups; instantaneous SharePoint site backup and restores; and non-disruptive restores, application development, and training purposes.

This technical report presents two solutions to enable SharePoint sites to have disaster recovery capabilities using NetApp technologies.

TABLE OF CONTENTS

1 INTRODUCTION

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.

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.

This technical report delivers an overview of a disaster recovery model for Microsoft Office SharePoint server user sites using SnapManager® for Microsoft Office SharePoint Server (SMMOSS) and SnapManager for Microsoft SQL Server (SMSQL).

2 GENERAL INTRODUCTION TO SMMOSS AND ITS COMPONENTS

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

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
- 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 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 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.

3 PURPOSE AND SCOPE

Disaster recovery and business continuance have different connotations and implementations based on the environment for they are being designed. The definition of disaster recovery that will be used in this paper is as follows:

3.1 DISASTER RECOVERY (DR)

A process of regaining access to the data, hardware, and software necessary to resume critical business operations after a disaster. A disaster recovery plan should also include methods or plans of copying necessary mission-critical data to a recovery site to regain access to such mission-critical data after a disaster.

3.2 PROBLEM DEFINITION AND SCOPE

The particular disaster recovery problem that is addressed in this paper is as follows:

Given a SharePoint Web application that might have one or more content databases and one or more site collections, we aim to replicate the content databases to a secondary site. The replica of the content database at the secondary site will be used to recover the contents (site, subsites, document libraries, and so on) of the original SharePoint Web application.

The paper presents two solutions of achieving the above mentioned goal of replicating the content databases. The paper discusses all the pertinent steps and components needed to implement the DR strategy defined above. The solutions are completely based on NetApp technology and are designed to achieve acceptable RPO/RTO objectives.

The scope of the discussed solution is limited to the following:

- The paper only covers the recovery of SharePoint user sites.
- Recovery of the content database only. Customized portions such as WebParts need to be reinstalled and reconfigured manually at the DR site.
- The solutions only use backups that are created by SnapManager for Microsoft Office SharePoint Server (SMMOSS).
- Additionally, the solutions also use SnapMirror® and SnapManager for SQL Server (SMSQL).

1. SnapManager for SQL Server restore option at the secondary site is limited to recovery from a full-backup using volume SnapRestore® to recover database and transaction log volumes at the secondary location.
    - SnapMirror replication discussed in this solution is limited to content databases of user sites only and does not cover other databases such as config database, central administration console database, and so on.

The technical report will not cover the following:

- Recovery of MOSS databases that are outside the purview of SMMOSS
- Synchronous SnapMirror
- Semisynchronous SnapMirror

4 INTENDED AUDIENCE

This technical report is intended for information technology professionals, storage professionals, and MOSS administrators responsible for corporate SharePoint site infrastructure management. For methods and procedures mentioned in this technical report, it is assumed that the reader has working knowledge of the following:

- Service-level expertise of Microsoft Office SharePoint Server
- Working knowledge of SMMOSS
- Working knowledge of SMSQL

- Working knowledge of NetApp storage
- Working knowledge of NetApp solutions including the following:
  - Data ONTAP®
  - SnapDrive® for Windows®
  - SnapMirror

5 TERMS USED IN THIS PAPER

The following terms related to business continuance and disaster recovery have been used in the paper:

- **Recovery point objective (RPO)**: The recovery point objective (RPO) describes a point in time to which data must be restored/recovered in order to be acceptable to the organization's process supported by the data.
- **Recovery time objective(RTO)**: The recovery time objective (RTO) is the frontier of time and service level within which service availability must be accomplished to avoid undesirable consequences associated with a break in continuity of a service/process.
- **Service level agreement (SLA)**: A formal negotiated agreement between a service provider and a user (typically customers), specifying the levels of availability, serviceability, performance, and operation of a system, service, or application.

6 NETAPP DR SOLUTION FOR MICROSOFT OFFICE SHAREPOINT SERVER

Based on our experimentations, the following are the key advantages of using NetApp solutions to create a DR plan for SharePoint user sites:

- **Ease of configuration**: The most user-friendly aspect of NetApp solutions is the ease with which one can deploy the discussed DR plan. Note that through the SMMOSS GUI and a few Data ONTAP commands, one can guarantee a robust DR solution. This reduces administrative overhead in complex SharePoint environments.
- **Speed and performance**: Since SMSQL backups are based on volume Snapshot™ technology (Data ONTAP), the duration for which the database being backed up remains frozen is minimized. This means that for very large content databases, there is minimal interference with transaction processing.
- **Simplified SharePoint serverwide DR**: Note that using the simplified SMMOSS GUI, an administrator can opt for extending DR capabilities to each and every SharePoint Web application. There are no special or extra steps that one needs to take for controlling the SharePoint Web applications to which DR capability needs to be imparted.

7 DISASTER RECOVERY SOLUTIONS FOR MOSS 2007 USER SITES

7.1 TECHNOLOGY COMPONENTS

To implement the DR solutions that will be proposed in further sections of the paper, there some core components need to be used. These components are as follows:

NETAPP SNAPMANAGER FOR MICROSOFT OFFICE SHAREPOINT SERVER

NetApp SnapManager for Microsoft Office SharePoint Server allows SharePoint administrators to back up SharePoint Web applications using NetApp Snapshot technology. SMMOSS presents a centralized GUI to manage multiple SharePoint farms with minimal manual intervention. It also includes features such as "out-of-place restore" and backup-set indexing to allow fast and nondisruptive restore operations.

NETAPP SNAPDRIVE FOR WINDOWS

NetApp SnapDrive for Windows is an enterprise-class storage and data management solution for Microsoft Windows Server environments. SnapDrive enables storage and system administrators to quickly and easily manage, map, and migrate data.

NETAPP SNAPMANAGER FOR SQL SERVER

NetApp SnapManager for SQL Server speeds and simplifies SQL Server data management. It empowers DBAs to utilize the capabilities of NetApp storage systems from an approach centered around SQL Server. It automates and simplifies the complex, manual, and time-consuming process associated with backup and recovery of SQL Server databases leveraging the NetApp technology stack to create fast and space-efficient Snapshot copies.

NETAPP SNAPMIRROR

NetApp SnapMirror delivers the disaster recovery and data replication solution that today's global enterprises need. By replicating data at high speeds over LAN and WAN, SnapMirror provides the highest possible data availability and fastest recovery for mission-critical applications.

7.2 DISASTER RECOVERY SOLUTIONS

The primary objective of this disaster recovery solution is to achieve the highest degree of operational continuance at the primary site with no single points of failure and to have a recovery site and replicate the content databases pertaining to the SharePoint Web applications for recovery in case of a disaster. Two scenarios were tested with the above discussed NetApp components to achieve two different levels of RPO/RTO objectives outlines below.

SOLUTION ONE (OVERVIEW)

To meet a near zero-minute RTO and 24-hour RPO, the "out-of-place" restore feature is used to restore the user Web application from the primary site onto a standby Web application at the DR site.

SOLUTION TWO (OVERVIEW)

To meet a one-hour RPO and a 1-minuten RTO, full backups of the content database that are created by SMMOSS are replicated to the DR site every hour using SnapDrive rolling Snapshot updates of the content database volumes (data and transaction logs) and the SMSQL SnapInfo volume. The concerned volumes at the primary site were mirrored to the DR site using asynchronous SnapMirror relationship.

TEST ENVIRONMENT

The proposed solutions were tested in the following environment and found to be working as per RTO/RPO objectives defined above:

- Windows Server 2003 Enterprise Edition
- Microsoft Office SharePoint Server (MOSS) 2007
- Microsoft SQL Server 2005 RTM
- SnapManager for Microsoft Office SharePoint Server v1.1
- SnapDrive 5.0
- Data ONTAP 7.2.4 (with SnapMirror license)
- The primary (production) and secondary (disaster recovery) hosts must be in the same domain

Table 1 shows the storage layout at the primary site that was used for testing the proposed DR solution:

Table 1) Storage layout at the primary site.

	Volume Name	File Size	LUN
ContentDB data file (MDF)	ContentDB_Vol	50GB	M:\
ContentDB log file (LDF)	ContentDB_Vol	1GB	M:\

SMSQL SnapInfo folder	SnapInfo_Vol		N:\

Table 2 shows the storage layout at the secondary site that was used for testing the proposed DR solution.

Table 2) Storage layout at the secondary site.

	Volume Name	File Size	LUN
ContentDB data file (MDF)	ContentDB_Vol2	50GB	M:\
ContentDB log file (LDF)	ContentDB_Vol2	1GB	M:\
SMSQL SnapInfo folder	SnapInfo_Vol2		N:\

8 SOLUTION ONE: 24-HOUR RPO/NEAR ZERO-MINUTE RTO

The following section will demonstrate a disaster recovery solution for MOSS user Web applications using SMMOSS to achieve a near zero-minute RPO and five-minute RTO.

8.1 SETTING UP THE DR SOLUTION

To set up this DR solution, the following steps need to be performed:

1. Create a backup plan for the appropriate MOSS Web application using the SMMOSS Backup Builder UI.
2. Make sure that the backup plan is scheduled to run at least once a day.
3. Go to the restore controller and choose the latest backup set that exists for the backup plan created above.
4. In the backup browser section of the Restore Controller, click the “Detail” button.
5. In the new backup browser that opens, choose each of the site collections that are listed. Note that there is no need to expand the site collections.
6. Now choose the “Out of Place” restore option and then select the appropriate SMMOSS control agent and the target Web application. Note that the SMMOSS control agent needs to be the one that exists on the MOSS WFE server at the DR site. The configuration looks like this:

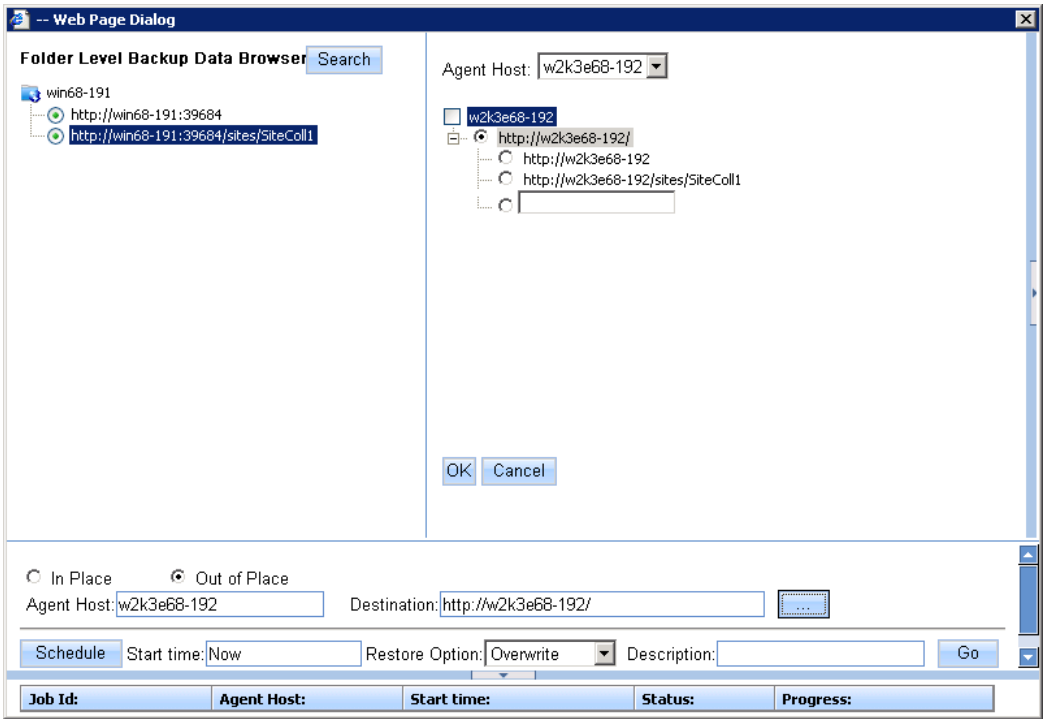

Figure 1) Configuration.

7. Now either run the restore right away or schedule it to run at a future time.

8.2 FAILOVER TO THE DR SITE

To resume operations at the DR site use one of the following options :

- Use the same URL (http://<machine-name>:<port number>/….) to access the different sites from the MOSS WFE at the DR site. Note that “machine-name” refers to the hostname of the MOSS WFE at the DR site.

OR

- Use the steps mentioned in Appendix-xxx**[[NOTE: Please complete x-ref.]]** to map the above URL to a common universally accepted URL.

8.3 FAILBACK TO THE PRIMARY SITE

To conclude the DR solution, the failback strategy is an important piece. To perform a failback, one needs to perform an out-of-place restore with the currently running MOSS Web application at the DR site as the source and the original MOSS Web application at the primary site as the target. Note that due to the nondisruptive nature of the restore, there will be absolutely no downtime. The users can start using the MOSS Web application at the primary site once the restore is complete.

BEST PRACTICES

1. The backup plan should be scheduled to run more than once a day, preferably two or three times during off-peak hours (for example, early morning, lunchtime, and closing time). This allows for more than one backup set to be present for each day of work.
2. This solution is specifically meant for small and low-activity MOSS Web applications. Note that it is best to restore the site to an alternate location each day after close of business so that the standby copy of the sites is maintained.
3. In case the number of site collections (selected items on the left pane of the browser window as shown above) are too large, then the following three-part strategy can be used:

i. Back up and do an “out of place” restore of all the site collections only once at the beginning of each week.

ii. During rest of the days, select groups of site collections and then restore them to the DR location.

9 SOLUTION TWO: ONE-HOUR RPO/20-MINUTE RTO

The following section will demonstrate a disaster recovery solution for MOSS user Web applications using SMMOSS to achieve a near zero-minute RPO and five-minute RTO.

9.1 SETTING UP THE DR SOLUTION

The following setup needs to be implemented in order to achieve a DR strategy:

1. Establish an asynchronous SnapMirror relationship between the following volumes of the primary and secondary sites:

   ContentDB_Vol <-> ContentDB_Vol2
   SnapInfo_Vol <-> SnapInfo_Vol2

   We now describe the steps involved in setting up a SnapMirror relationship. As an example, the setting up of the SnapMirror relationship between the “ContentDB_Vol” volume (primary site) and the “ContentDB_Vol2” (secondary site) is shown.

   Note: The destination volume must always be equal to or greater than the source.

   For this example, the following are the source and destination volumes:

   - Source storage system: SS1
   - Source volume: ContentDB_Vol
   - Destination storage system: SS2
   - Destination volume: ContentDB_Vol2

   a) On both source and destination storage systems, make sure that SnapMirror is licensed. In case it is not, run the following command:

      `license add <license key>`

   b) On SS1 run the following command:

      `options snapmirror.access host=SS2`

   c) On both SS1 and SS2 run the following command:

      `options snapmirror.enable on`

   d) On SS2 edit the snapmirror.conf file as follows:

      i. Type:

         `wrfile /etc/snapmirror.conf`

      ii. Type the following command:

         `SS1:ContenDB_Vol SS2:ContenDB_Vol2 - - - - -`

      iii. Press Enter followed by ctrl-c to exit.

      iv. Verify the contents of the file by running

         `rdfile /etc/snapmirror.conf`

   e) On SS2 run the following command:

      `vol restrict ContentDB_Vol2`

   f) On SS2 run the following command:

      `snapmirror initialize –S SS1:ContentDB_Vol SS2:ContentDB_Vol2`

g) On SS2 run the following command:

```
snapmirror status
```

h) Create a backup plan at the primary site for the appropriate MOSS user site using the SMMOSS manager GUI. The backup plan should be schedule to run every hour. Do not use backup indexing since this will cause the backup to take more time to complete, whereas indexed backup is not needed for the DR solution.

Note: The following screenshots show the configuration of the SMMOSS backup plan.

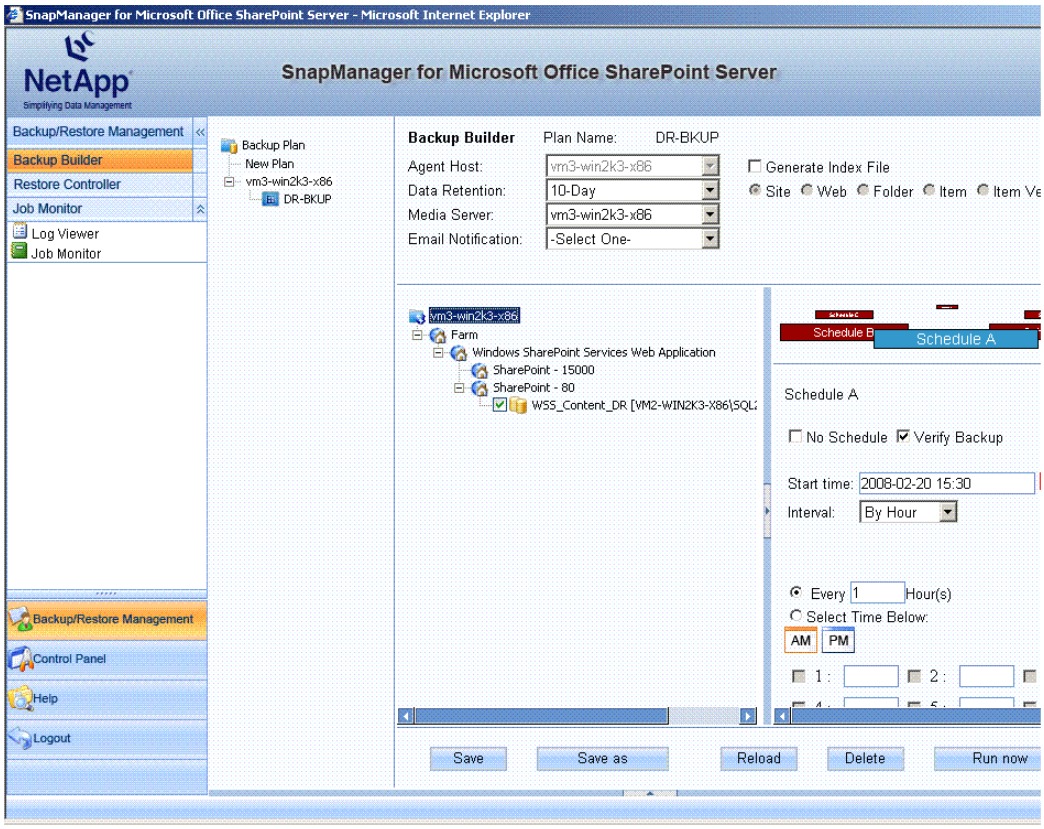

Figure 2) Configuration of SMMOSS backup.

i) Create a Windows scheduled task on the SQL Server host that updates the SnapMirror relationship for the ContentDB volume every 30 minutes. This process is termed rolling Snapshot copies with SnapMirror update. The SnapDrive command line that is used for this task is as follows:

```
sdcli snap update_mirror –m HostName -d DriveLetter
```

Note that the “DriveLetter” parameter above corresponds to the drive on which the ContentDB exists. In our example the ContentDB was placed on a NetApp LUN that was mapped to M: and the hostname was “VM2-WIN2K3-X86”**.** Hence, the command used was as follows:

```
sdcli snap update_mirror –m VM2-WIN2K3-X86 -d M
```

The output of the run is as follows:

```
VM2-WIN2K3-X86 : Checking policies
VM2-WIN2K3-X86 : Preparing virtual disks for snapshot creation
VM2-WIN2K3-X86 : Ready to create Snapshot
VM2-WIN2K3-X86 : Creating a snapshot for the virtual disk
```

```
VM2-WIN2K3-X86 : Initiating snapmirror update for any source volumes.
The operation completed successfully.
```

j) Follow the instructions in step 3 to create a Windows scheduled task on the SQL Server host that updates the SnapMirror relationship for the SnapInfo directory every 30 minutes.

In our example the SnapInfo directory was placed on a NetApp LUN that was mapped to N:, and the hostname was "VM2-WIN2K3-X86"**.** Hence, the command used was as follows:

sdcli snap update_mirror –m VM2-WIN2K3-X86 -d *N*

k) For the first time, manually run the SMMOSS backup plan, created in step 2, after it is created. Subsequently, manually run the Windows scheduled tasks, created in steps 3 and 4, after they are created. Note that this is only a one-time manual run. From here on the automated schedules for both the tasks will make sure that the jobs are run as intended. The reason for this step is to have a fresh SnapMirror ContentDB backup to start with.

9.2 FAILOVER TO THE DR SITE

To initiate a recovery of the user MOSS Web application at the DR site, make sure that the following components are present at the DR site:

- Microsoft Office SharePoint Server 2007 Web front-end server
- SQL Server 2005 which hosts the content databases
- SnapManager for SQL Server Version 2.1.1
- NetApp storage system with SnapMirror license
- DATA ONTAP 7.2.4

Subsequently, the following steps should be performed to recover the user sites at the secondary site:

1. Break the SnapMirror relationship between all the existing SnapMirror relationships as described in the previous section. To do this run the following command on SS2 (destination storage system):

   snapmirror break *<vol_name>*

   For example, to break the SnapMirror relationship between the ContentDB volumes we ran the following command at SS2:

   snapmirror break ContentDB_vol2

2. Bring the SnapMirror volumes, as described in the previous section, on SS2 online with the following command:

   vol online <vol_name>

   For example, to bring the ContentDB volume online we ran the following command at SS2:

   vol onlines ContentDB_vol2

3. Remove any LUN mappings carried over from the primary site for the volume. This can be done from the SS view GUI.

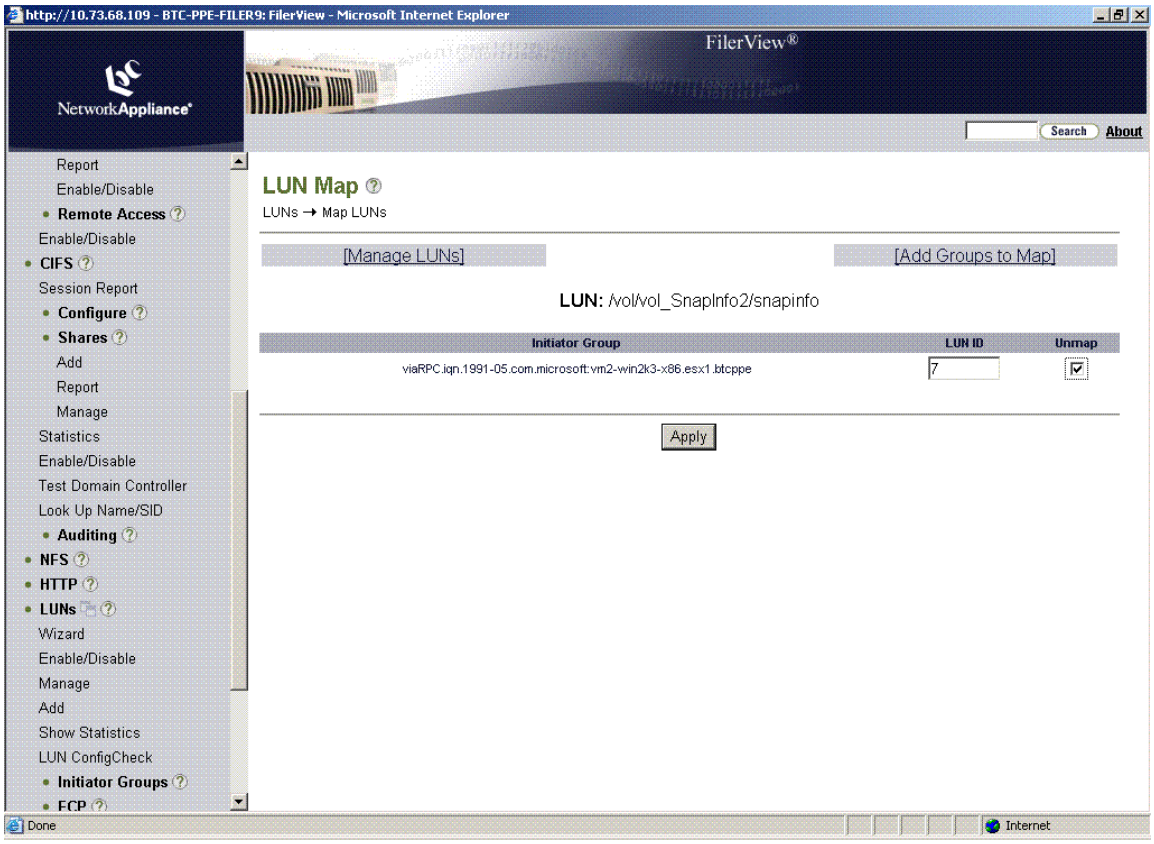

Figure 3) Map LUNs.[[NOTE: Figure 4 has same title - please change one of them.]]

4. At the secondary site, map the LUNs that exist on the ContentDB and SnapInfo volumes to the same drive letters as on the primary site. To do this, use SnapDrive for Windows to connect to the LUNs on the two volumes, the SnapInfo and ContentDB volumes, using the same drive letters as existed at the primary site:

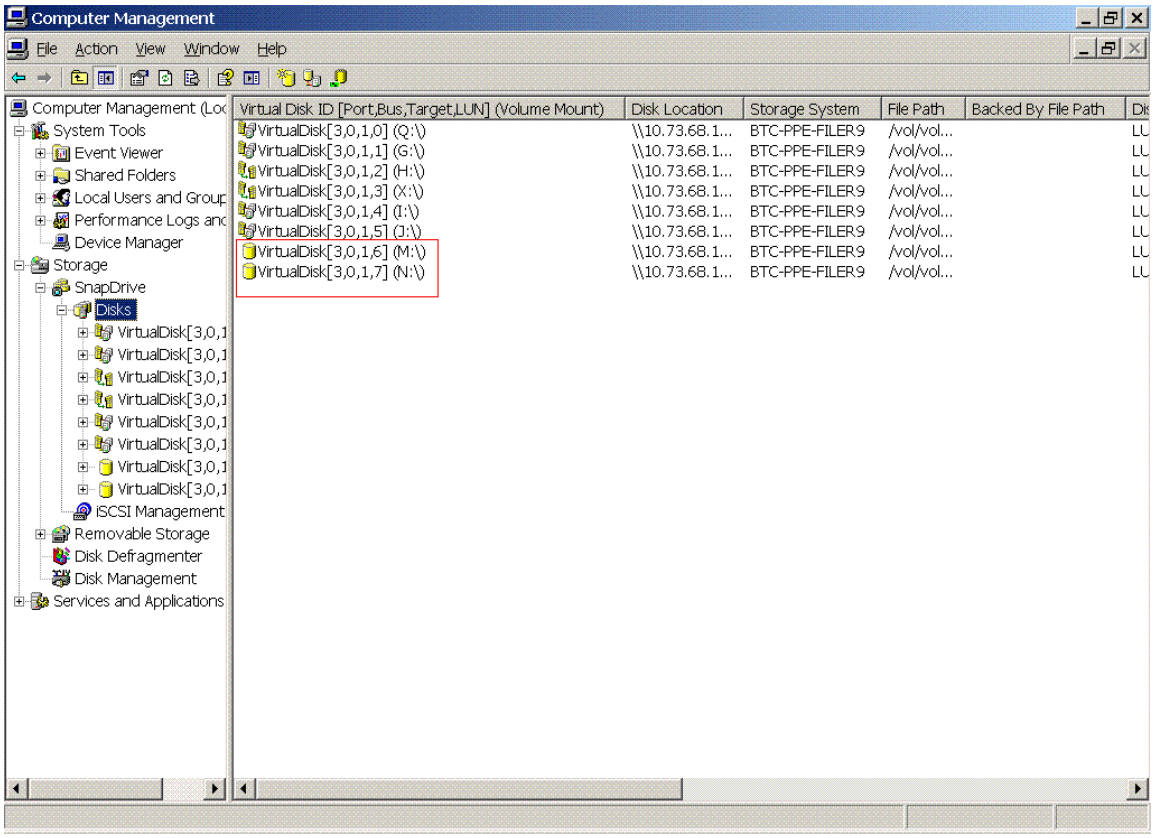

Figure 4) Map LUNs.

5. Use the SMSQL instance at the secondary site to recover the content database at the SQL Server instance present on the secondary site.

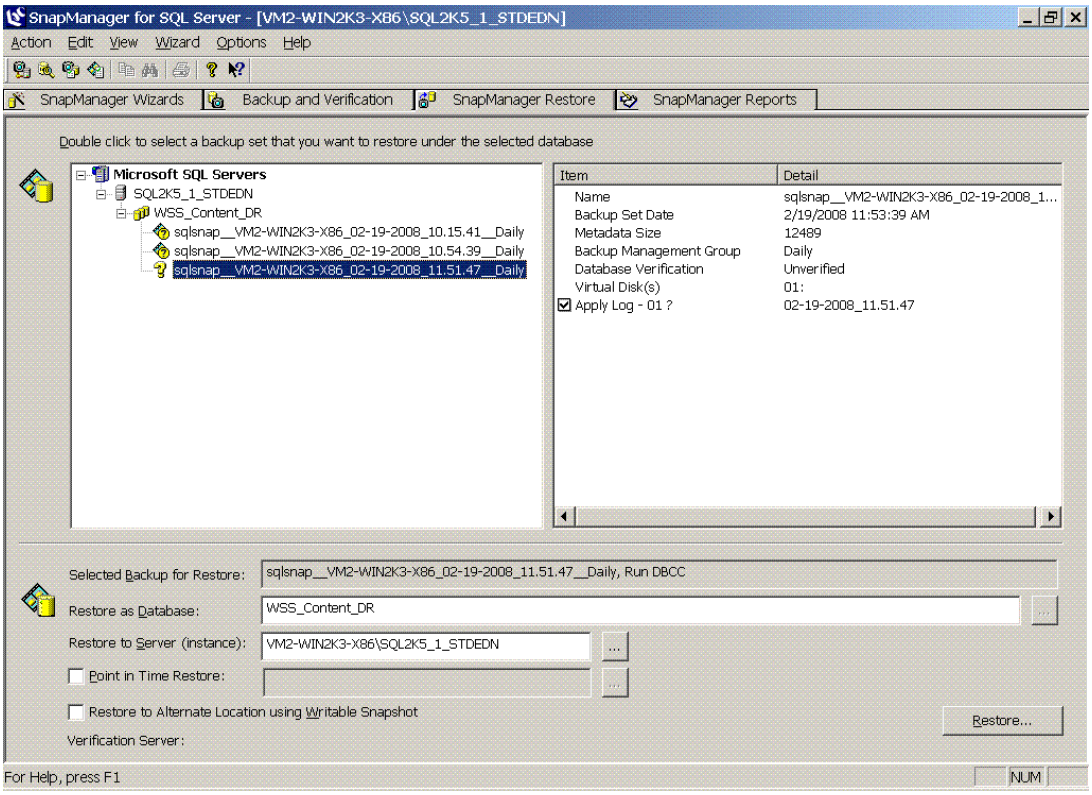

Figure 5) Recovering content database.

Note: Please make sure that the “Create Transaction Log backup before Restore” option is unchecked in the “Restore Settings” under “Options” menu item.

6. Use the SQL Server management studio at the secondary site to verify that the content database is online.

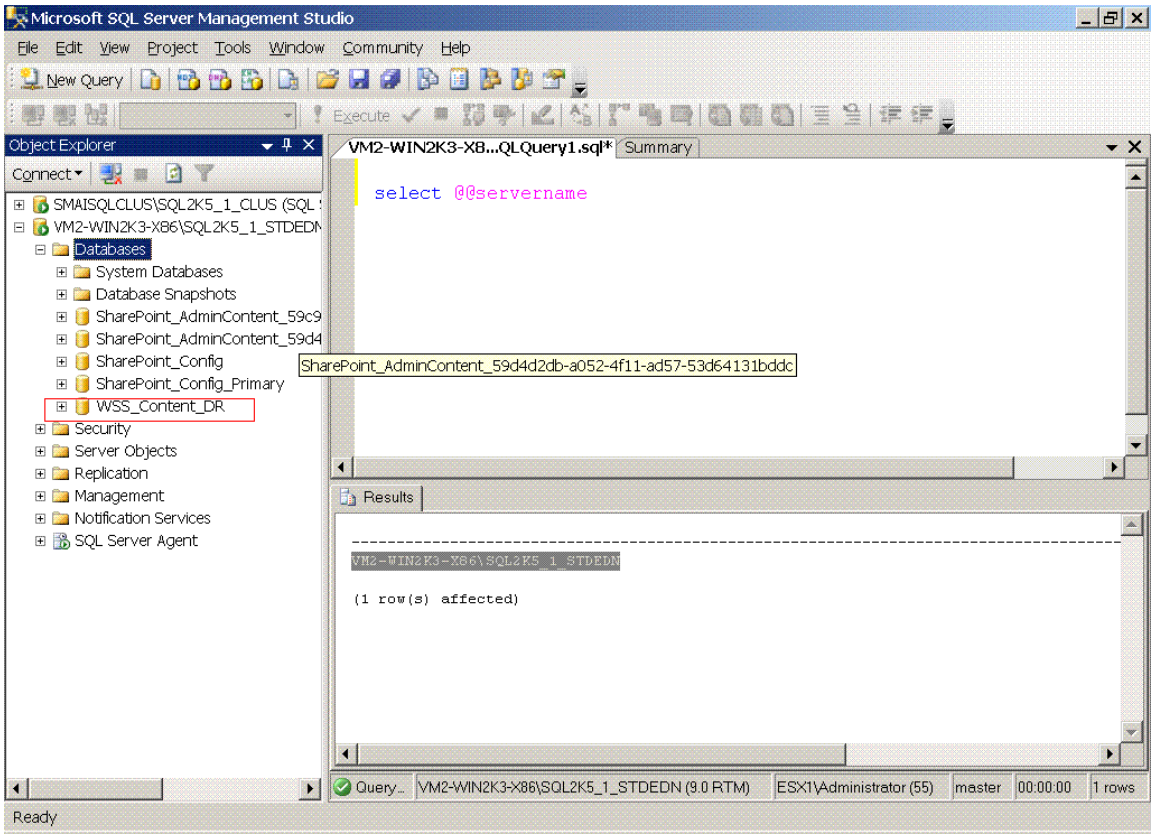

Figure 6) Verifying if data is online.

7. Open the MOSS 2007 Central Administration portal.
8. Go to "Central Administration > Application Management > Content Databases > Manage Content Database Settings" and remove the existing content database.
9. Now go to "Central Administration > Application Management > Content Databases" and add the database restored in step 2 as the new content database.

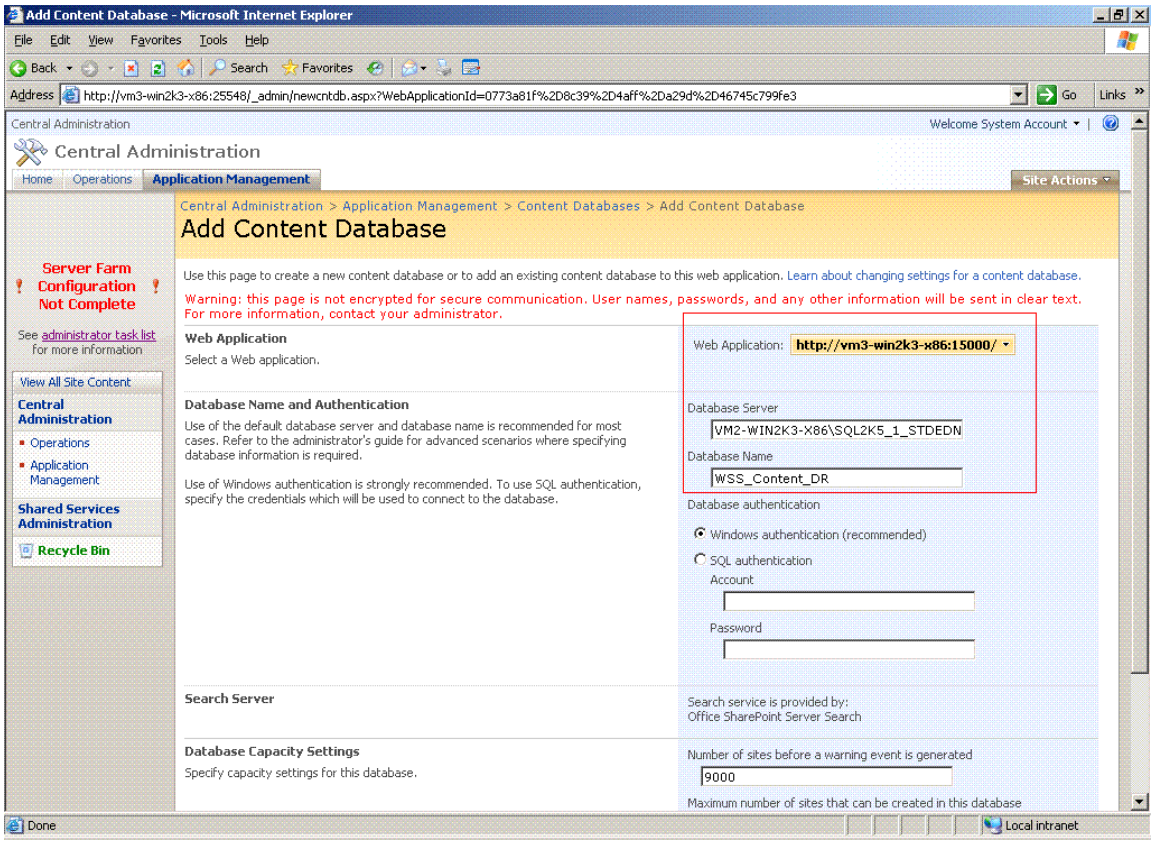

Figure 7) Adding content database.

As noted in the previous solution, the access to the new Web application can be done as follows:

- Use the same URL (http://<machine-name>:<port number>/….) to access the different sites from the MOSS WFE at the DR site. Note that “machine-name” refers to the hostname of the MOSS WFE at the DR site.

OR

- Use the steps mentioned in Appendix A to map the above URL to a common universally accepted URL.

9.3 FAILBACK TO THE PRIMARY SITE

To conclude the DR solution, the failback strategy is an important piece. To perform a failback one needs to perform an out-of-place restore with the currently running MOSS Web application at the DR site as the source and the original MOSS Web application at the primary site as the target. Note that due to the nondisruptive nature of the restore, there will be absolutely no downtime. The users can start using the MOSS Web application at the primary site once the restore is complete.

10 COMPARISON OF THE SOLUTIONS: HOW TO CHOOSE THE RIGHT APPROACH

Table 2 explains the advantages and the disadvantages of the two solutions presented above and will help the reader in selecting the most appropriate solution.

Table 3) Solution comparision.

Parameters	Solution 1	Solution 2
RPO	24 hours (maybe more if “out of place” restores are not done daily)	1 hour
RTO	Near zero	15–20 minutes
Ease of Configuration	Limited configuration required	Needs configuring: SnapMirror relationship SDW rolling updates SMSQL at the DR site
Level of Automation	User interface based	Scripted
Target Web Application Size	Small and low-activity Web applications related to small user groups, test and dev environments, and so on	Large and high-activity Web applications.
NetApp Components Used by the Solution	SMMOSS	SMMOSS, SDW, SMSQL, SnapMirror
Network Resource Usage	High	Low

APPENDIX A: UNIVERSAL ACCESS MAPPING

Alternate access mapping is the feature that allows a site to be published to users on multiple networks, where clients on each network might address the site with different URLs.

CONFIGURATION

You can specify alternate access mapping settings in SharePoint Central Administration by doing the following:

1 Click Start, Administrative Tools, and select SharePoint Central Administration.
2 Click the Application Management section.
3 Click Alternate access mappings under the SharePoint Web Application Management section.
4 Click Edit Outbound URLs in the task pane to specify alternate access mapping for an existing Web application.
5 Click the Change link on the top-right of the Web page. A popup is displayed asking you to choose the Web application for which you want to configure alternate access mapping.
6 Select the Web application and click OK.
7 Specify the URLs for intranet, extranet, Internet, and custom URLs.
8 Click Save on the Web page.

APPENDIX B: REFERENCES

SnapManager for Microsoft Office SharePoint Server 2007: Best Practice Guide

SMMOSS Advanced Demo 1 (Out-of-Place Restore)

SMMOSS Advanced Demo 2 (DR Demo for MOSS Sites)