Technical Report

NetApp SnapManager for Microsoft SharePoint Server

Disaster Recovery Guide

Cheryl George, NetApp

January 2015 | TR-4372

Executive Summary

This guide discusses how to protect data by using the NetApp® SnapManager® for Microsoft® SharePoint® Server solution to maximize application availability and reduce planned and unplanned downtime during disaster recovery.

Note: This guide pertains specifically to NetApp clustered Data ONTAP® deployment scenarios.

TABLE OF CONTENTS

1 Overview 4

2 Disaster Recovery Overview 4

3 Business Use Case 5

4 Failure Scenarios 7

5 Disaster Recovery Strategies 9

5.1 High-Availability Options 9

5.2 Failback Options 16

5.3 Advantages of Using NetApp Solutions 16

6 Protecting SharePoint Using SMSP 18

7 Restoring Microsoft SharePoint Content 19

8 Archiving Options 19

9 Best Practices While Using SMSP with SharePoint Server 19

10 Summary 20

Appendix: Implementation Details 20

References 21

Version History 22

LIST OF TABLES

Table 1) Disaster recovery objectives. 5

Table 2) Failure scenarios. 7

Table 3) Solution and technology components. 8

Table 4) Recovery prerequisites. 13

Table 5) Business goals. 17

Table 6) Example SMSP backup schedule. 18

Table 7) Implementation details. 20

LIST OF FIGURES

Figure 1) SMSP data protection of SharePoint farm. 6

Figure 2) SMSP data protection of virtualized SharePoint farm. 7

Figure 3) NetApp software and technology used in SharePoint farm. 8

Figure 4) SharePoint farm failover within primary site. 11

Figure 5) Initialize SnapMirror relationship. 12
Figure 6) SharePoint farm failover to recovery site leveraging NetApp SnapMirror technology. 13
Figure 7) Virtualized SharePoint farm failover to recovery site leveraging NetApp SnapMirror technology. 16
Figure 8) SnapManager for SharePoint with storage optimization. 18

1 Overview

Microsoft SharePoint is used extensively by enterprise businesses to create and maintain intranet and extranet websites, facilitate document collaboration, and improve business intelligence. The availability of SharePoint farm resources is critical to organizations. Therefore, it is important to develop an effective disaster recovery (DR) plan and set recovery goals based on your business drivers and acceptable latency periods.

This technical report provides an overview of disaster recovery strategies for Microsoft SharePoint Server 2013 by using the comprehensive NetApp suite of hardware and software solutions. Some key benefits of the NetApp SnapManager for Microsoft SharePoint Server solution include:

- **Reduced infrastructure costs.** The NetApp disaster recovery solution enables storage efficiency by using NetApp Snapshot® and NetApp FlexClone® technologies, thin provisioning, deduplication, NetApp SnapManager for SharePoint (SMSP) and NetApp SnapMirror® compression to realize savings at both the primary site and the secondary site (also known as the DR site). This solution meets challenging business needs with a single platform that offers multiprotocol SAN (FC, FCoE, and iSCSI) and NAS (SMB-CIFS) data access.
- **Simplified disaster recovery processes.** Leverage the SMSP built-in recovery features, such as NetApp backup, restore, and archiving technologies, to quickly and easily recover SharePoint farm content at the secondary site.
- **Application consistency.** After failover to the secondary site, SMSP technology consistently recovers Microsoft SharePoint applications. The SMSP solution integrates Microsoft SharePoint with NetApp technologies by using SMSP agents for advanced, application-aware data protection of SharePoint databases, BLOB storage, SharePoint search indexes, and SMSP stub databases, all of which can be replicated to the secondary site by using SnapMirror technology.

2 Disaster Recovery Overview

A successful disaster recovery plan requires a secondary, redundant site (also known as a recovery site) to make sure that SharePoint servers can continue operating when the primary site becomes temporarily or permanently unavailable.

To architect a solution for high availability (HA) and business continuity, you should be familiar with the following terms:

- **Availability.** Availability is defined as the continuous operation of services or systems designed for zero data loss and zero downtime.
- **Disaster recovery.** Disaster recovery is the process of regaining access to the data, hardware, and software necessary to resume critical business operations after a disaster. A disaster recovery plan should include methods or plans for copying necessary mission-critical data to a secondary site, as well as procedures for regaining access to mission-critical data after a disaster.
- **High availability.** High availability is a design implementation that enables continuous data availability for business operations. High-availability planning should include strategies to prevent single points of failure that could potentially disrupt the availability of mission-critical business operations.

The primary objective of a disaster recovery solution is to achieve the highest degree of operational continuance at the primary site with no single point of failure and also to have a secondary site to which the SharePoint farm can be replicated and recovered in case of disaster.

Table 1 describes the objectives of a well-planned disaster recovery solution.

Table 1) Disaster recovery objectives.

Objective	Description
Recovery point objective (RPO)	The RPO is the maximum amount of acceptable data loss, in terms of latency, between the last committed data transaction before the failure and the most recent data recovered after the failure.
Recovery time objective (RTO)	The RTO is the duration of the outage before the application is available to its users, with the primary goal of restoring full service so that new transactions can take place.
Service-level agreement (SLA)	An SLA is a formal, negotiated agreement between a service provider and a user (typically a customer), specifying the levels of availability, serviceability, performance, and operation of a system, service, or application.

3 Business Use Case

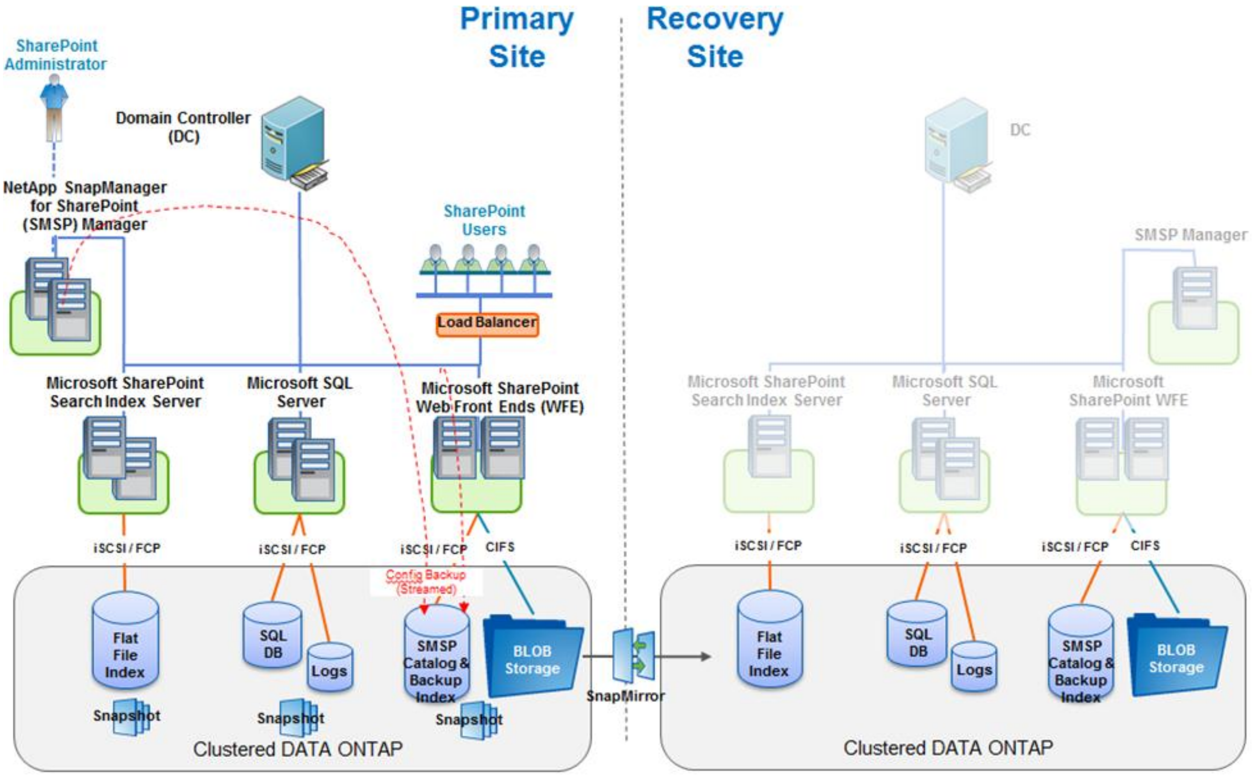
NetApp SnapManager for SharePoint (SMSP) is a high-availability disaster recovery solution that you can use to back up and restore your entire SharePoint environment in the event of a disaster. With SMSP storage optimization, content such as binary large object (BLOB) data can be moved or externalized from SharePoint content databases to NetApp CIFS shares.

NetApp Snapshot technology creates backups of SharePoint databases, BLOB data, and SharePoint index files stored on NetApp storage. This backed-up data is then sent to the configured SMSP storage policy and stored together with the backup job metadata and index files.

SMSP leverages NetApp SnapMirror technology, which effectively uses network bandwidth to replicate SharePoint Server data to NetApp storage at the recovery site. SnapMirror employs network compression to speed up transfers, reduce bandwidth utilization, and control network costs between locations. Furthermore, SMSP installs its own services, such as control and media services, and you can choose to load balance these services.

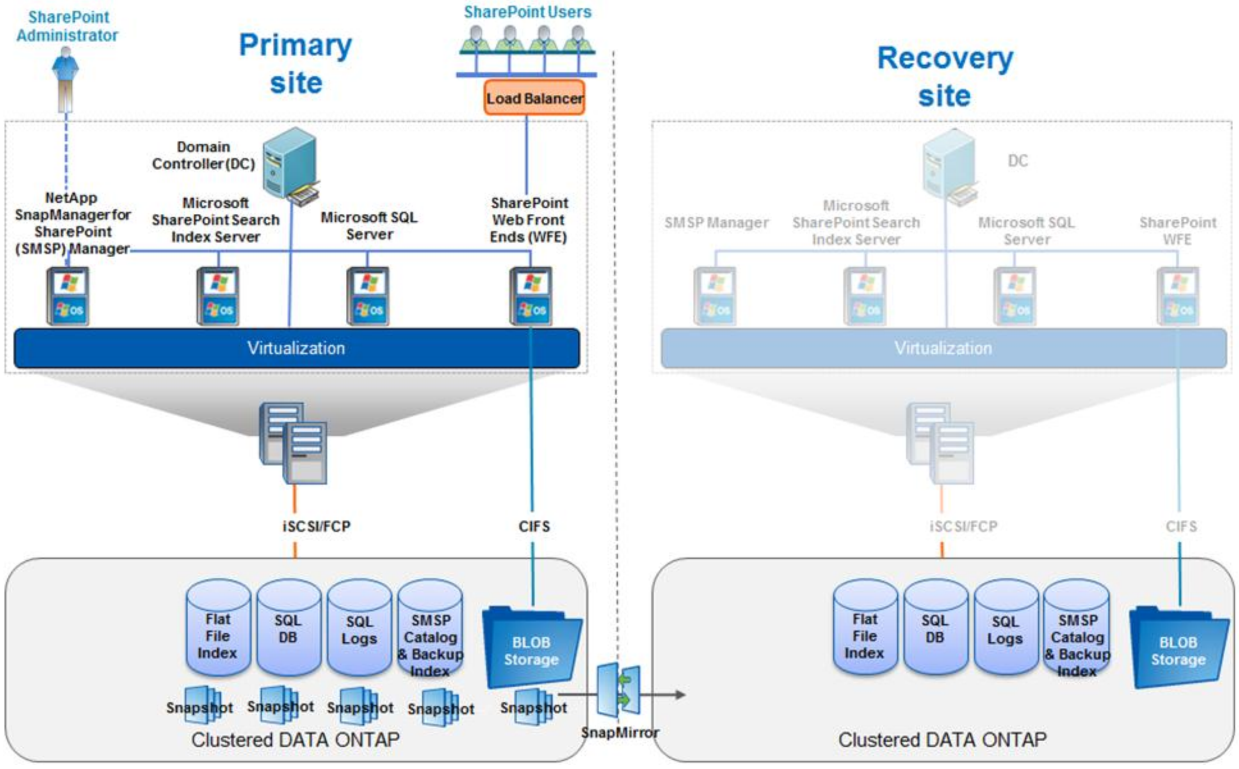
Figure 1 shows the SMSP solution using SnapMirror technology to protect SharePoint farm data.

Figure 1) SMSP data protection of SharePoint farm.



As customers move toward virtualized data centers, they increasingly look for ways to bring the benefits of virtualization to their mission-critical SharePoint Server application. Virtualizing SharePoint on NetApp unified storage provides enhanced data protection and disaster recovery capabilities with greater flexibility and streamlined recovery in the event of a disaster. Figure 2 shows the SMSP solution using SnapMirror technology to protect a virtualized SharePoint farm.

Figure 2) SMSP data protection of virtualized SharePoint farm.



4 Failure Scenarios

Table 2 lists SharePoint farm failure scenarios and recovery methods.

Table 2) Failure scenarios.

Failure Scenario	Possible Causes	Recovery Method
Application-level failure	SharePoint farm failure, including: • Web front-end (WFE) or application server failure • SQL Server® failure	Application-level recovery through SMSP backups
Storage-level failure	• LUN failure • Volume failure • Aggregate failure	Storage-level and application-level recovery through SMSP backups
	• Controller node failure • Controller interface failure • Cluster interconnect failure	Storage-level recovery
Site-level failure	• Natural disaster	Site-level recovery

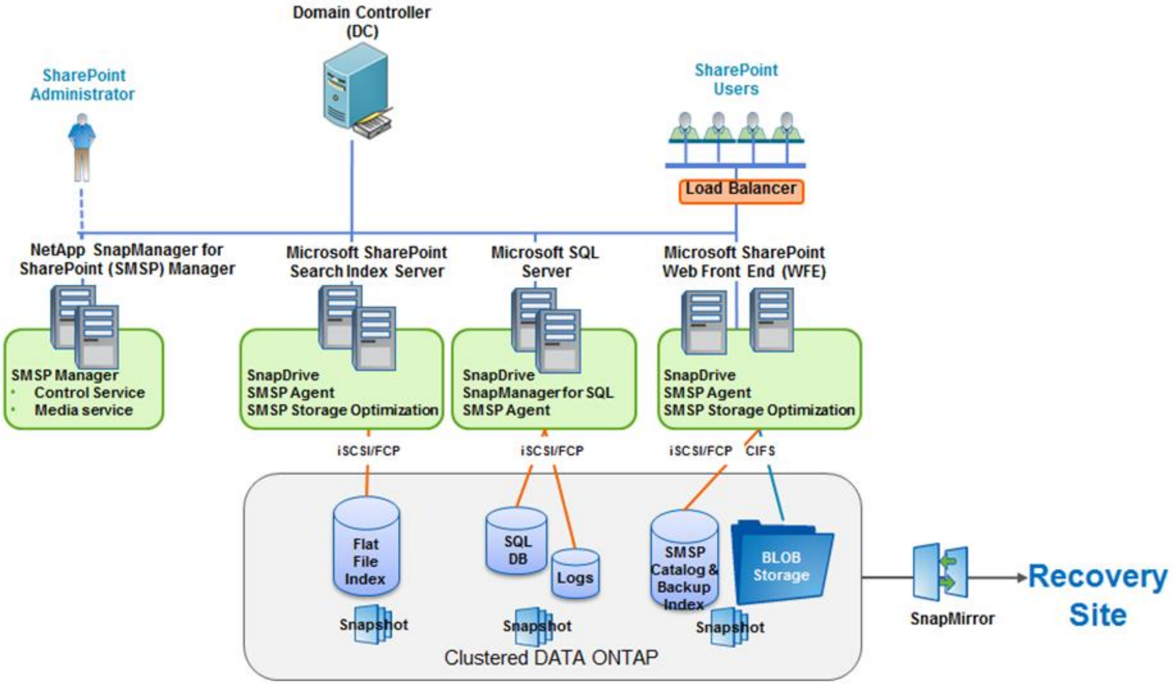
Table 3 lists the solution and technology components used in this disaster recovery solution.

Table 3) Solution and technology components.

Component	Software/Technology
Storage (primary and disaster recovery data centers)	• Operating system: NetApp Data ONTAP • Storage protocols: FC, iSCSI, and CIFS shares (used by SMSP Storage Optimization module such as Storage Manager, Archive Manager, and Connector) • NetApp technology: Snapshot copies, thin provisioning, compression, and SnapMirror data replication • Licenses: FlexClone, NetApp SnapRestore®, SnapMirror, SnapManager suite, and SnapManager for SharePoint optional modules
NetApp management software (primary and disaster recovery data centers)	• Backup and restore: NetApp SnapDrive® for Windows®, SnapManager for Microsoft SQL Server, and SnapManager for SharePoint Server
Application virtual machine operating system	• Windows Server®
Microsoft application	• SharePoint Server • SQL Server

Figure 3 shows the NetApp software and technology used by the SMSP solution.

Figure 3) NetApp software and technology used in SharePoint farm.



5 Disaster Recovery Strategies

Disaster recovery planning for SharePoint farms is critical, which is why you need a well-designed plan. The first step in developing a SharePoint disaster recovery plan is to know exactly what components exist in your environment. Take complete inventory of the following:

- Physical architecture, such as the servers, databases, and networks
- Logical architecture, such as web applications, service applications, service accounts, and apps
- Customized software installed on SharePoint farm servers

You should also record SMSP topology details such as:

- SMSP Manager server
  - Control database used and the SQL Server on which it resides
- Various NetApp software installed on servers in the SharePoint farm
  - SnapDrive for Windows (SDW)
  - SnapManager for SQL Server (SMSQL)
  - SMSP Manager
  - SMSP Agents
  - SMSP additional module: Storage Manager configuration details
- SnapManager for SharePoint backup of the entire SharePoint farm, including SMSP control database (added in SMSP backup as a custom database) and SMSP stub database
- LUN storage layout used for SharePoint databases
- CIFS storage location used for BLOB storage

Your DR plan, defined by current SLAs derived from RPOs/RTOs, should include provisions for the different types of failures that could affect operations. These failures can range from natural calamities, such as earthquakes, to component failures, such as a disk failure.

A disaster recovery plan identifies the types of failures and countermeasures required to help you resume operations, and it also includes planning for high availability within your local site.

5.1 High-Availability Options

The following sections outline the primary and secondary site availability options that are available when SharePoint is deployed on NetApp storage.

In the event of a disaster, two types of restores can be performed:

- Full-farm recovery at the primary site in which the servers in the SharePoint farm are disconnected and then reconnected
- Full-farm recovery at a secondary site (the destination of the data replicated by SnapMirror) in which the servers in the SharePoint farm are disconnected and then reconnected

Note: The WFE server data that you have backed up explicitly (including the IIS settings, SharePoint hive, global assembly cache, custom features, SharePoint site definitions, and file system folders) will not be restored as a result of using either of these methods. After the farm rebuild, restore WFE data explicitly by selecting the desired WFE server nodes from corresponding backups. For more information, refer to “Options for Restoring Backed-Up Web Front-End Files” in the SnapManager 8.1 for Microsoft SharePoint Platform Backup and Restore User’s Guide.

Local Site Availability Options

Local availability is high availability within a data center, site, or local area network (LAN). This section reviews local availability options for Microsoft SharePoint environments that use NetApp technologies.

High availability for servers in a SharePoint farm can be achieved by distributing and configuring different parts of a SharePoint environment. For example, WFE HA can be achieved by enabling the SharePoint Foundation web application service on the WFE servers. Therefore, even if one of the WFE servers fails, clients browsing to load-balanced URLs will still be able to access the SharePoint site.

Microsoft SQL Server HA can be achieved using a failover cluster instance (FCI) or availability group (AG), which leverages Windows Server failover clustering (WSFC). Both contain an instance of SQL Server running across multiple WSFC nodes, allowing for failover of the WSFC resource group from one node to another in case the primary becomes unavailable. SQL Server FCI provides redundancy at the server-instance level; AG provides redundancy at the database level. Therefore, when a SQL Server failure occurs, SQL Server automatically fails over to the available node in the FCI or the AG synchronous secondary replica within the primary site. This operation is transparent to the SharePoint farm that uses SQL Server; therefore, there is no application downtime.

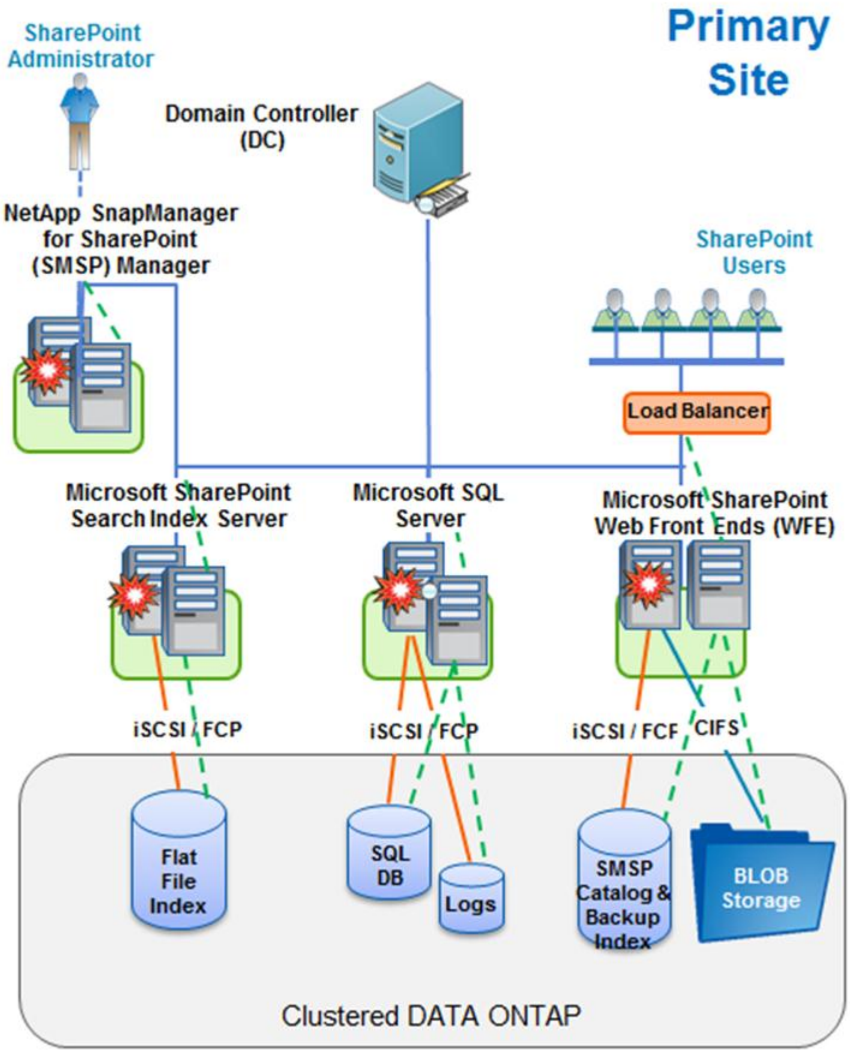
For more information, refer to Failover Clustering and AlwaysOn Availability Groups (SQL Server) and Supported high availability and disaster recovery options for SharePoint databases (SharePoint 2013).

The proven efficiency of NetApp storage and SnapManager for SharePoint complements Microsoft SharePoint to provide high availability within the local site. SMSP leverages NetApp Snapshot technology to provide quick, space-efficient, and application-consistent backups and rapid restores, even at the granular level, such as site collection, document libraries, lists, items, and item versions.

In case of minor issues in the SharePoint farm at the primary site, perform an SMSP farm repair job. A farm repair job is typically performed when the SharePoint farm is connected but experiencing minor issues, such as unavailable services, deficiency of permissions in the SharePoint registry, and so on. A farm repair is much quicker than a farm rebuild because a farm repair does not require any servers in the farm to be disconnected.

To recover the entire SharePoint farm, perform a farm rebuild to restore the original SharePoint farm and recover availability. This operation requires all servers in the farm to be disconnected and then reconnected. For more information about the complete procedure, refer to the SnapManager 8.1 for Microsoft SharePoint Disaster Recovery User’s Guide.

Figure 4) SharePoint farm failover within primary site.



Secondary Site Availability Options

The following sections describe high-availability options for secondary sites.

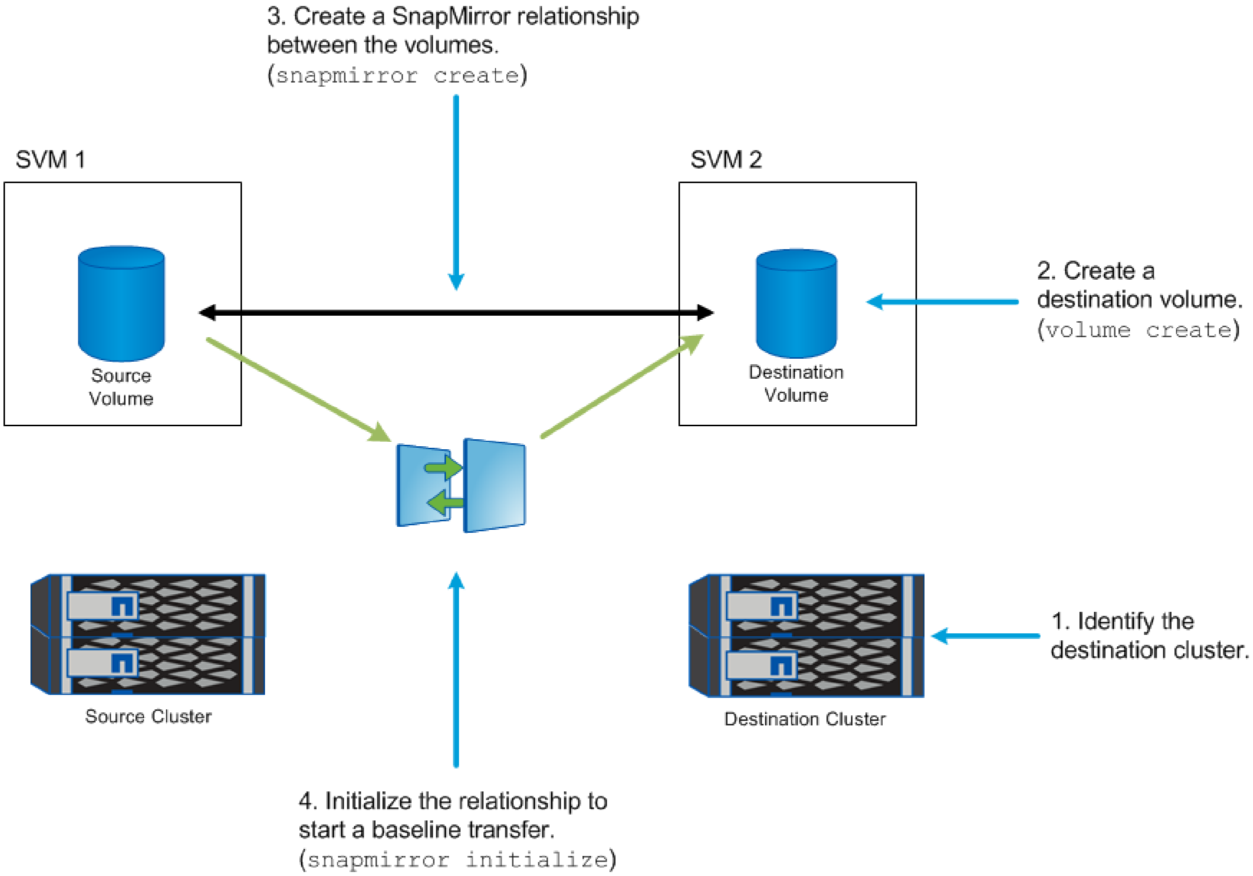
NetApp SnapMirror Technology

NetApp SnapMirror is an asynchronous, thin replication solution based on NetApp Snapshot technology that enables customers to build an incredibly efficient disaster recovery solution. SnapMirror makes disaster recovery rapid, reliable, and manageable. It helps organizations to reduce the risk and concern related to disaster recovery. SnapMirror technology is used to mirror data between NetApp storage systems across a LAN or WAN. Its storage deduplication and network compression capabilities put SnapMirror on the leading edge of replication technology.

With SnapMirror, disaster recovery can be implemented to protect the entire data center. By using NetApp SnapMirror technology, volumes can be incrementally mirrored to an off-site location. SMSP provides native integration with SnapMirror technology, thereby enabling you to easily ship backups to the remote DR site as soon as failover has been initiated on the primary site. SnapMirror performs incremental, block-based replication as frequently as the required RPO. The block-level updates reduce bandwidth and time requirements, and data consistency is maintained at the DR site. SMSP then allows data to restore from an alternative storage location (the SnapMirror destination), thereby enabling an SMSP farm rebuild to restore data to a point in time before data corruption occurred.

Figure 5 illustrates the procedure to initialize a SnapMirror relationship.

Figure 5) Initialize SnapMirror relationship.


3. Create a SnapMirror relationship between the volumes. (snapmirror create)
SVM 1
SVM 2
Source Volume
Destination Volume
2. Create a destination volume. (volume create)
Source Cluster
Destination Cluster
1. Identify the destination cluster.
4. Initialize the relationship to start a baseline transfer. (snapmirror initialize)

The first and most important step for setting up a SnapMirror relationship is to conduct a one-time baseline transfer of the entire dataset. This is required before incremental updates can be performed. This operation includes creating a Snapshot copy (also called a baseline copy) at the source and transferring all of the data blocks referenced by it to the destination file system. After the initialization is complete, scheduled or manually triggered updates can occur. Each update transfers only the new and changed blocks from the source to the destination file system.

SMSP backups can integrate with SnapMirror, which replicates Snapshot copies to mirrored volumes. SnapMirror coordinates with SnapManager for SQL Server (SMSQL) and SnapDrive for Windows (SDW) to perform asynchronous replication of SharePoint databases, BLOB data on CIFS share, SharePoint search indexes, and SMSP backup data.

The schedule defined for SMSP backup plans can trigger an asynchronous mirror replication update when SMSP runs the backup job. If this schedule is optimized, the time between two SnapMirror replications can be minimized to achieve the desired RPO. After a SnapMirror relationship is configured and an SMSP backup is complete, a SnapMirror update is initiated by SMSP to reflect the incremental changes of the source volume to the destination volume.

Because the replication is periodic, SnapMirror consolidates the changed blocks and conserves network bandwidth, which minimizes the effect on write throughput and write latency. After SnapMirror replicates the data, disaster recovery of SharePoint farm data on the secondary site can begin. The following sections describe disaster recovery scenarios.

Full-Farm Rebuild from Alternative Storage Location

In this scenario, prior to the disaster, SnapManager for SharePoint backups of the SMSP control database, SharePoint databases, SMSP stub databases, SharePoint search indexes, connector BLOB data, and Storage Manager BLOB data must be replicated to the DR site by using NetApp SnapMirror technology. The SMSP farm Snapshot copy can be restored to a standby SharePoint farm at the recovery site on which the SharePoint configuration wizard has not been run.

An SMSP full-farm backup backs up all SharePoint databases and other components, including search index data, at the same point in time. Similarly, the SMSP farm rebuild that uses the SMSP backup recovers of all these components to the same point in time. The farm rebuild also synchronizes each SharePoint server with the restored configuration database to make sure that the SharePoint server and cache are consistent with the configuration database.

Figure 6) SharePoint farm failover to recovery site leveraging NetApp SnapMirror technology.

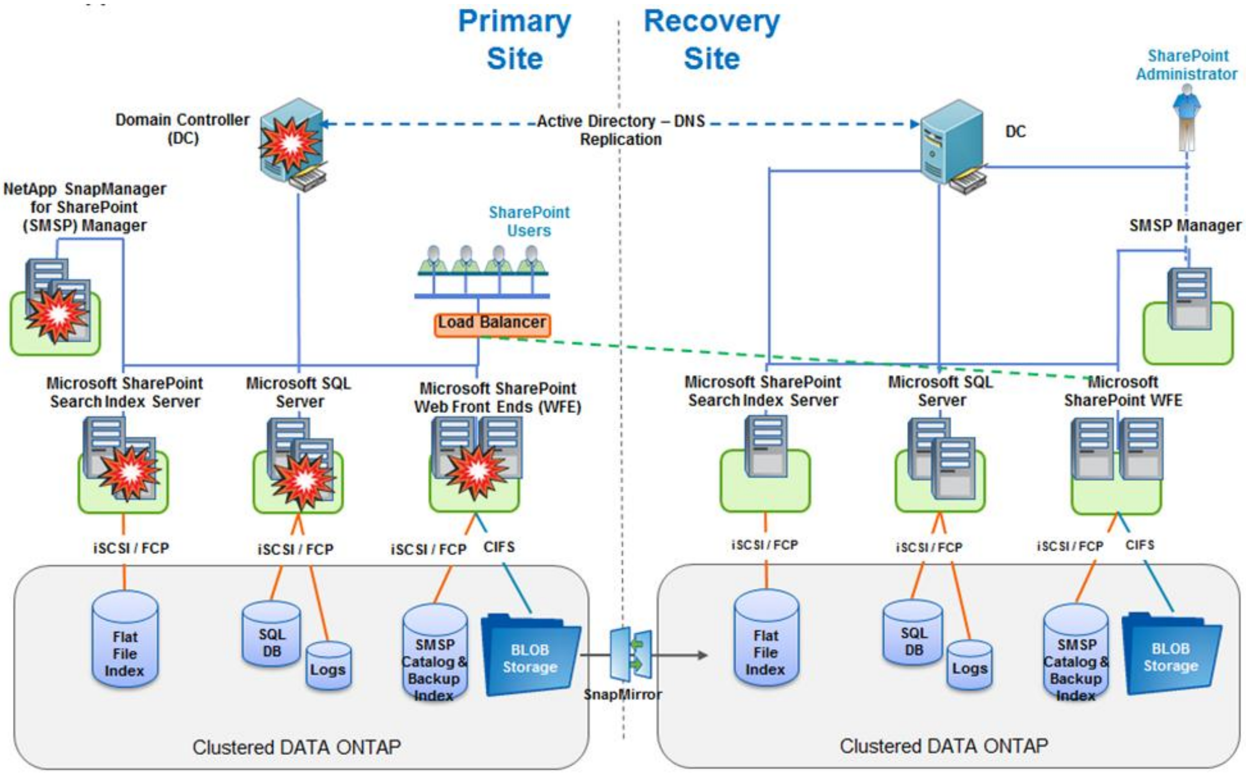


Table 4 lists the prerequisites that must be met at the secondary SharePoint farm before you perform a recovery operation.

Table 4) Recovery prerequisites.

Description
The domain controller must be recovered. For more information about how to recover the domain controller, refer to Domain Controller Recovery.
SQL Server must be set up by using the FCI. Alternatively, if you are using AGs, leverage the asynchronous replica at the secondary site.

Description
A secondary SharePoint farm with servers that have SharePoint installed is required. **Note:** The SharePoint configuration wizard must not have been run on these servers.
Where applicable, all required software components, such as Windows Host Utility Kit, SDW, and SMSQL, must be installed on the secondary servers.
All customizations from the production server must be deployed.
The failover components and systems in the secondary data center must match the primary site's components and systems in all ways. These components include, but are not limited to, the following: • Platform • Hardware • Number of servers • Server names • Operating system version and updates • Microsoft SQL Server versions and updates • Microsoft SharePoint versions and updates • NetApp software stack, including SDW, SMSQL, and SMSP

Restore SharePoint Farm at Secondary Site

In the event of a disaster at the primary site, complete the following steps to restore SharePoint farm data on the secondary site from the SnapMirror destination volumes:

1. Break the SnapMirror relationships set up between the primary and secondary storage systems.
2. Verify that the servers in the farm are properly connected to the SnapMirror destination storage through either iSCSI or FCP.
3. Use SDW to connect to the LUNs for flat file index, SQL Server database, logs, and SMSP catalog and backup index in the SnapMirror destination, including the SnapInfo LUN that contains details about backup jobs.

   Note: Use the same drive letters and mount points used on the original server.
4. Run the SMSQL configuration wizard to use the SnapInfo LUN from the SnapMirror destination.
5. Recover the SMSP Manager first at the secondary site. Use SMSQL to manually restore the SMSP Control database from backup. Verify that the SMSP Manager component installation connects to the restored SMSP Control database.
6. Confirm that the SMSP settings for the storage system profile and the physical and logical devices for LUNs and CIFS share point to the SnapMirror destination storage system.
7. Verify that the SMSP agents installed on various SharePoint servers point back to the SMSP Manager.
8. Use the farm rebuild function to restore the SMSP farm from an alternative storage location. For more information, refer to the SnapManager 8.1 for Microsoft SharePoint Platform Backup and Restore User's Guide.
9. Validate the SharePoint environment to make sure that all content has been restored from the SnapMirror destination.

Recover SharePoint Farm in Virtualized Environment

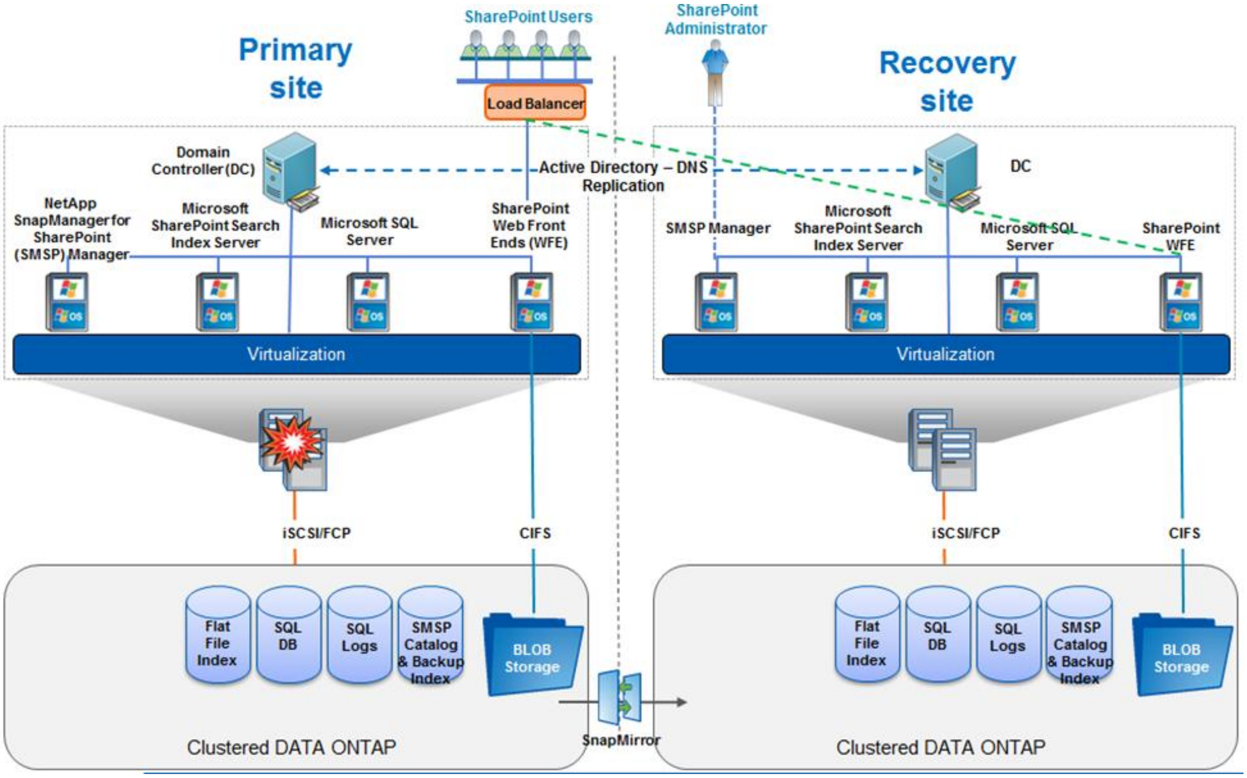
In this scenario, prior to the disaster, the volumes that contain the Microsoft SharePoint farm virtual machines (VMs) must be replicated to the disaster recovery site by using SnapMirror technology.

To recover a SharePoint farm in a virtualized environment, complete the following steps:

1. Configure SDW to communicate with the Microsoft Hyper-V® server or VMware® ESX® server on the recovery site.
2. Verify that the virtualization host is connected to the SnapMirror secondary storage.
3. On the virtualization host, do one of the following:
   - If you are using Hyper-V, use SnapDrive for Windows to connect to the LUN where the SharePoint farm VMs are located on the secondary storage. Then import the SharePoint farm VMs into the Hyper-V server and power on the VMs.
   - If you are using an ESX server, initiate site failover by using VMware Site Recovery Manager integrated with NetApp Site Recovery Adapter.
4. Configure the SharePoint farm VMs to be on the network at the disaster recovery site and update the DNS, if required.

   Note: Because the VMs are backed up outside of SMSP, be sure to run the SharePoint configuration wizard first to disconnect from the previous configuration database at the point of backup.
5. Use SDW on the SharePoint server and SQL Server VMs to connect to the LUNs for flat file index, SMSP catalog and backup index, SQL Server database, logs, and SnapInfo in the SnapMirror destination.
6. Confirm that the SMSP settings for the storage system profile and the physical and logical devices for LUNs and CIFS share point to the SnapMirror destination storage system.
7. Use the farm rebuild function to restore from the SMSP farm from an alternative storage location. For more information, refer to the SnapManager 8.1 for Microsoft SharePoint Platform Backup and Restore User's Guide.
8. Validate the SharePoint environment to make sure that all content has been restored from the SnapMirror destination.

Figure 7) Virtualized SharePoint farm failover to recovery site leveraging NetApp SnapMirror technology.



5.2 Failback Options

The failback procedure is similar to the failover procedure except for the SnapMirror resynchronization operation. If the primary storage is intact, a failback can be performed by resynchronizing the mirrors in the reverse direction of that used by the original production storage resources by using NetApp OnCommand® System Manager.

Note: Confirm that the previous SharePoint disks in the destination are disconnected or removed before running the resync operation.

If the primary storage is destroyed, a new disaster recovery plan can be created to fail over the SharePoint storage resources to the production site. The primary site cluster must be rebuilt, and the necessary storage controllers must be reconnected to confirm that the resources are presented to the cluster. SharePoint and SQL Server FCI or AG, with the required service packs and hotfixes, must be installed on all the servers in the SharePoint farm and be configured at the primary site. The same recovery procedures described earlier can be used for failback.

Note: If new SnapMirror relationships must be configured in the reverse direction, create and initialize the SnapMirror relationships by using OnCommand System Manager.

5.3 Advantages of Using NetApp Solutions

NetApp technologies complement Microsoft SharePoint to provide data protection for disaster recovery purposes, for example:

- Key NetApp technologies such as thin provisioning and NetApp SnapMirror compression help reduce infrastructure costs.
- Using NetApp SnapMirror technology simplifies DR operations and allows customers to lower their RTO while achieving RPO based on their SLAs.

- By replicating only the changed blocks of data after the initial baseline transfer, NetApp SnapMirror decreases the replication time across sites and reduces network usage and storage costs.
- NetApp SnapMirror can be deployed with no additional IT resources, and it also supports frequent testing of your DR plan.
- The SnapManager suite can be used to create application-consistent backups by using NetApp Snapshot technology. NetApp SnapMirror can be used to extend the protection by replicating these consistent backups either to a different storage system located within the primary data center or to another data center located at a remote DR site.
- Microsoft SharePoint data can be protected by using SMSP, which leverages NetApp Snapshot technology. With SMSP, customers can use the restore option to help recover lost or damaged data and databases quickly and easily from the periodic backups.
- The backups created by SMSP are application consistent and can be mirrored to the DR site by using SnapMirror technology. This enables customers to meet or exceed their stringent SLAs through rapid recovery of SharePoint databases to a consistent state after failover to the DR site.
- SMSP allows you to recover granular items from SMSP Snapshot copies.

Table 5 lists business goals and how they are addressed at the primary site to provide a resilient architecture.

Table 5) Business goals.

Business Goal	Resolution Method	Details
No single point of failure	Windows Failover Clustering (WFC) and NetApp storage	WFC addresses server resiliency, and NetApp storage cluster addresses resiliency on the storage. Together, they eliminate single points of failure on applications, server hardware, and storage.
Fast backup and recovery	SMSP	SMSP automates complex, manual backup processes by creating fast and space-efficient Snapshot copies and providing faster recovery.
Disaster recovery	SMSP, SMSQL, SDW, SnapMirror, and SnapManager for Hyper-V (SMHV) or Virtual Storage Console (VSC)	SnapMirror replicates the database and log volumes, and SMSP provides faster backups and granular restores. SMHV or VSC can be used in a virtualized environment to back up and recover VMs.
Low RPO	SnapMirror	Scheduled SnapMirror operations upon completion of full backups of the SharePoint farm allow you to meet the RPO requirements.
Low RTO	SMSP, SMSQL, and SDW	SMSP provides instantaneous full farm or granular restores to meet the required RTO.

6 Protecting SharePoint Using SMSP

SnapManager for SharePoint (SMSP) is an enterprise-strength backup, recovery, and data management solution for SharePoint. SMSP leverages the SharePoint Volume Shadow Copy Service Writer in conjunction with the Windows Volume Shadow Copy Service to create consistent, point-in-time Snapshot copies of the SharePoint farm, including SharePoint databases and search index files, which are also mirrored by using SnapMirror technology.

In addition, SMSP Storage Optimization (Storage Manager, Connector, and Archive Manager) helps dramatically improve the scalability and performance of SharePoint Server by moving BLOB data outside of the SQL Server content database used by SharePoint, as shown in Figure 8.

Figure 8) SnapManager for SharePoint with storage optimization.

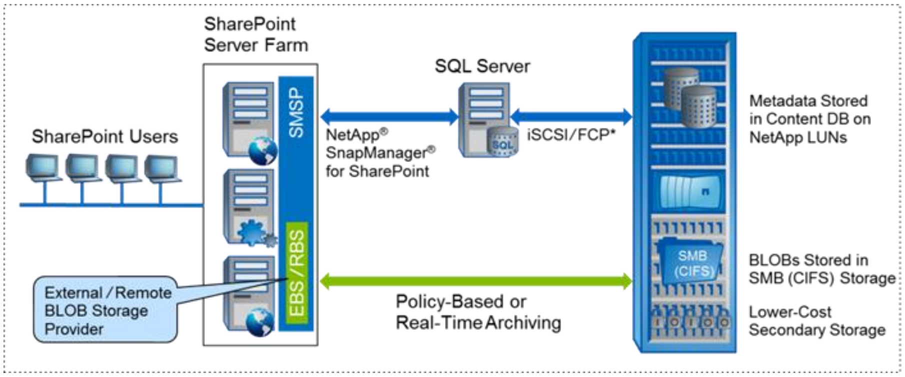

SharePoint Server Farm
SharePoint Users
SMSP
EBS/RBS
External/Remote BLOB Storage Provider
SQL Server
SQL
NetApp® SnapManager® for SharePoint
iSCSI/FCP*
Policy-Based or Real-Time Archiving
Metadata Stored in Content DB on NetApp LUNs
SMB (CIFS)
BLOBs Stored in SMB (CIFS) Storage
Lower-Cost Secondary Storage

Figure 8 shows metadata stored in a SQL Server database along with smaller files and large files (BLOBs) stored in NetApp SMB (CIFS) storage.

The backup strategy is determined by the backup requirements, which are typically identified according to how much data you can afford to lose (RPO) and how long you can take to recover lost or corrupted data (RTO). Make sure you have a proper backup schedule established that meets application and business requirements. Table 6 provides an example backup schedule for meeting required recovery objectives.

Note: Different backup and SnapMirror schedules can be set up for different service tiers.

Table 6) Example SMSP backup schedule.

Backup Schedule	Full-Farm Backup (Including BLOB Content)	SnapMirror Operation
Daily backup	Every 2 hours	Upon completion of every full backup

When planning a DR solution, the data to be recovered can be prioritized by using a hierarchical storage mechanism for tiered storage that is transparent to SharePoint end users. The storage hierarchy is defined as follows:

- Tier 1 storage is high-end, faster access SAN storage that provides high IOPS and low latency and hosts the SharePoint content databases.
- Tier 2 storage is less expensive, NAS-based storage that contains BLOB data externalized through the SMSP Storage Manager module, which significantly improves SharePoint performance and SQL Server efficiency because content database size is reduced.
- Tier 3 storage is archived data for retention.

The NetApp SnapManager for SharePoint Server solution uses SnapMirror technology for replication and DR because of its proven efficiency, simplicity, and modest cost when compared with the other DR solutions. SnapMirror also provides all of the benefits of storage efficiency offered by NetApp.

Note: Together, the SharePoint database backup and BLOB content backup create a complete backup set of SharePoint content. This backup set can be used to restore the SharePoint content databases with externalized content. Therefore, when planning a backup and restore strategy, plan for and factor in remote BLOB storage (RBS) recovery and make sure that the SharePoint documents are available to end users.

7 Restoring Microsoft SharePoint Content

SMSP Snapshot copies can be used to restore an entire SharePoint farm or granularly restore individual site collections, sites, libraries, lists, folders, items, or file/item versions provided granular indexing options were selected during backup. This restore operation can be performed in either of the following ways:

- In-place restore in which SharePoint data (database or granular content) is restored to the original location in the SharePoint farm
- Out-of-place restore in which SharePoint data can be restored to another location within the original SharePoint farm or to a separate SharePoint farm

For more information, refer to the SnapManager 8.1 for Microsoft SharePoint Platform Backup and Restore User’s Guide.

8 Archiving Options

SMSP also allows you to archive backup Snapshot copies to the secondary storage by using NetApp SnapVault® technology, thereby enabling the retention of weeks’ worth of SMSP Snapshot copies of databases, BLOB data, search indexes, and storage policy devices. These SnapVault relationships are created by using OnCommand System Manager.

The SMSP backup retention of SharePoint databases is mapped to SMSQL, which actually creates database Snapshot copies. The retention of search indexes, BLOB data, and storage policy devices relies on the database backup retention policy. The remote, archived Snapshot copies of search indexes and BLOB CIFS volumes are deleted automatically when SMSQL returns the related database backup. Local Snapshot copies of the storage policy device, however, must be deleted manually.

To restore from SnapVault, use the load remote backup option in the SMSP restore wizard to load the remote SnapVault Snapshot copies and perform a restore, if the local Snapshot copy does not exist. For more information, refer to the “Restore from Alternate Storage Location” section of the SnapManager 8.1 for Microsoft SharePoint Platform Backup and Restore User’s Guide.

9 Best Practices While Using SMSP with SharePoint Server

When using SMSP with SharePoint Server, NetApp recommends the following best practices:

- Database layout planning is critical to making sure that the SMSP backups are not stored in the same volume as the SharePoint content databases. NetApp also recommends using SnapMirror to replicate the backup volume to separate storage for redundancy.
- Leverage SMSP verification (at the end of a backup job or deferred verification) to make sure you have created consistent database backups.
- For DR purposes, make sure that you periodically use SnapMirror to replicate the following volumes:
  - SMSP Snapshot copies that contain SharePoint content databases and search index data
  - NetApp CIFS shares that contain externalized BLOB data

    - The SMSP Control database used by SMSP Manager
    - The stub database used by SMSP Agent for BLOB access
- Make sure that you periodically test the restore functionality of these SMSP backups to verify that the backups can be used in the event of a disaster.

10 Summary

Microsoft SharePoint is an enterprise-level collaboration application that can cripple productivity if it becomes unavailable. This technical report provides a validated business case for using NetApp SnapManager for SharePoint, which complements the high-availability and disaster recovery capabilities of SQL Server FCI. The key benefits of this solution include:

- **Ease of configuration.** The most user-friendly aspect of NetApp solutions is the ease with which the disaster recovery strategy can be implemented through SMSP. SMSP reduces administrative overhead in complex collaboration environments.
- **Speed and performance.** SMSP backups leverage NetApp Snapshot technology to create application-consistent database copies. This means that for very large SharePoint databases, client request latency is not affected. In addition, SnapMirror updates are also reasonably fast and enable healthy RPOs and RTOs.
- **SharePoint restoration options.** SMSP offers varying degrees of restore capabilities that range from full-farm recovery to granular restoration of individual items.
- **Virtualizing SharePoint.** Virtualizing a SharePoint farm on NetApp unified storage accelerates the deployment time in addition to providing high-level performance and availability to simplify IT operations.

Appendix: Implementation Details

Table 7 lists the DR plan implementation details validated for this solution. The setup considered for this solution was a SharePoint farm that used SQL Server FCI on the primary site with a total of 1TB of SharePoint data.

Table 7) Implementation details.

Stage	Details
Prior to a disaster	A SnapMirror relationship was initialized between the controllers at the primary and secondary sites for volumes containing the databases and CIFS shares containing the BLOB data. Data was generated on the primary site. This data was then replicated incrementally by SnapMirror with no administrator interference. Full-farm backups were scheduled for every 2 hours. Upon completion of the SMSP backups, the databases, BLOB data, and storage policy were replicated to the DR site using SnapMirror technology.
Simulating the disaster	The servers in the primary site were abruptly powered down.

Stage	Details
Recovering from the disaster	SharePoint data was recovered successfully on the secondary site by using the DR procedures described in this document. The RPO was 2 hours with SnapMirror replication of the SharePoint farm backups to the DR site. The total recovery time was approximately 40 minutes. The following time-related metrics were collected: • Break the SnapMirror relationship: 30 seconds • Clear all the LUN mappings and connect and mount all the LUNs from SnapMirror destination storage on the recovery server by using SnapDrive for Windows: 5 minutes • Attach the SharePoint databases by using SQL Server Management Studio: 2 minutes • Configure SMSP (map to existing Control database from SnapMirror destination): 3 minutes • Rebuild the SMSP farm: 25 minutes
Failing back to the primary site	The servers in the primary site were powered on. After the primary site was operational, to fail back the SharePoint databases, the SnapMirror relationship was reinitialized from secondary to primary storage. After the initialization was complete, the data was recovered using the methods described in this document.

Note: The recovery time listed in Table 7 is based on NetApp internal testing; this time may vary based on your environment’s setup and configuration.

References

This section lists useful resources to assist you in planning and managing your SharePoint Server on NetApp storage.

- Choose a disaster recovery strategy for SharePoint 2013
- High availability and disaster recovery concepts in SharePoint 2013
- Plan for high availability and disaster recovery for SharePoint 2013
- SharePoint 2013 for IT pros
- SnapDrive 7.0 for Windows Administration Guide for SAN Environments
- SnapDrive 7.0.1 for Windows Installation Guide
- SnapManager 8.1 for Microsoft SharePoint Installation Guide
- Supported high availability and disaster recovery options for SharePoint databases (SharePoint 2013)
- TR-3437: Storage Subsystem Resiliency Guide
- TR-3450: High-Availability (HA) Pair Controller Configuration Overview and Best Practices
- TR-4015: SnapMirror Configuration and Best Practices Guide for Clustered Data ONTAP
- TR-4228: SnapDrive 7.0 for Windows for Clustered Data ONTAP 8.2 Best Practices Guide for SAN Environments
- TR-4297: Microsoft SharePoint and SnapManager for SharePoint Deployment Guide

Version History

Version	Date	Document Version History
Version 1.0	January 2015	Initial release

Refer to the Interoperability Matrix Tool (IMT) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer's installation in accordance with published specifications.

Copyright Information

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

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

Trademark Information