



Technical Report

Microsoft SharePoint Server and SnapManager for SharePoint Deployment Guide

Cheryl George, Niyaz Mohamed NetApp
July 2014 | TR-4297

Executive Summary

This deployment guide assists customers in deploying solutions as per best practices to meet specific business requirements. It is based on the experiences of existing NetApp customers, on real-world simulations, and on NetApp engineering lab validations. The deployment guide helps customers through the entire project lifecycle, including requirement assessment, solution design, installation, and administration.

Note: This guide specifically focuses on NetApp® clustered Data ONTAP® deployment scenarios.

TABLE OF CONTENTS

1	Business Requirements	5
2	Solution Deployment Details	5
2.1	SharePoint Server Roles	5
2.2	Storage Environment	6
2.3	Additional NetApp Software Used	6
2.4	Database Layout Planning	9
2.5	SharePoint LUN Sizing	10
2.6	Installation and Configuration	12
2.7	Installing NetApp SnapDrive for Windows on SharePoint Servers in the Farm	13
2.8	Test and Validate Solution	24
3	Solution Operation	26
3.1	Capacity Management	26
3.2	Backup and Recovery Operations	27
4	Conclusion	28
	Appendix A: Installation and Configuration Details	29
	Detailed Steps to Install SnapDrive for Windows	29
	Set Transport Protocol Settings in SDW	33
	Accessing and Managing SnapDrive for Windows	33
	Enable vCenter or ESX Logon from SDW	33
	Create LUNs in VMware Environments	34
	Create LUNs for Hyper-V	35
	Appendix B: Build SharePoint 2013 Farm Using SQL Server 2012 AlwaysOn Availability Group Solution for High Availability and Disaster Recovery	39
	Set Up Windows Network Load Balancing for SharePoint Web Front-End Servers	39
	Configure Network Load Balancing	39
	Set Up Failover Clustering Feature for SQL Server 2012	39
	Create a New Windows Failover Cluster	40
	Set Up Quorum Mode Configuration	40
	Set NodeWeight Property	40
	Install a Standalone Instance of SQL Server 2012 on Each Cluster Node	41
	Install and Configure SharePoint 2013	42
	Install SnapDrive for Windows	42

Install SnapManager for SQL Server.....	42
Install SnapManager 8.0 for SharePoint on Server in SharePoint Farm.....	42
SMSP Migration Procedures	42
Enable AlwaysOn Availability Group Feature	43
Create Initial Database Backup Using SMSQL.....	43
Create SQL Server 2012 Availability Group	44
Create Availability Group Listener	47
Create SharePoint Farm Backup Using SMSP.....	47
Basic Tests to Validate the Solution	48
Appendix C: Solution Operation Details	51
Backup and Restore	51
References.....	60
Additional Documentation Available from NetApp Support Site	60
Version History	61

LIST OF TABLES

Table 1) Details of SharePoint servers in this environment.	5
Table 2) Additional NetApp software used.	6
Table 3) SharePoint implementation protocols.....	8
Table 4) Installation and configuration procedure.....	12
Table 5) Required components.	13
Table 6) Prerequisites for SnapDrive for Windows.....	15
Table 7) Prerequisites for SnapManager for SQL Server.....	16
Table 8) Prerequisites for SnapManager for SharePoint.....	17
Table 9) SMSP components mapped to SharePoint farm hosts.	18
Table 10) SnapManager for SharePoint configuration prerequisites.	19
Table 11) SMSP readiness tests performed.....	25
Table 12) Connectivity and validation tests performed.....	25
Table 13) SMSP backup and recovery tests.	25
Table 14) SnapManager for SharePoint backup test.....	26
Table 15) SnapManager for SharePoint restore test.....	26
Table 16) Settings for SQL Server 2012 AlwaysOn replica.....	44
Table 17) SharePoint 2013 databases supported for SQL Server 2012 AlwaysOn availability group.....	45

LIST OF FIGURES

Figure 1) NetApp SnapManager for SharePoint solution for SharePoint environment.....	7
Figure 2) NetApp SnapManager for SharePoint solution with storage optimization.....	8

Figure 3) SMSP volume layout.....10
Figure 4) Enable TCP/IP protocol for MSSQLSERVER.41
Figure 5) Enable AlwaysOn availability group feature.43

1 Business Requirements

The scope, scale, and complexity of today's data-driven world create new demands for agility in the data center. To increase collaboration and productivity across the enterprise, many of today's businesses deploy content management and collaboration systems. Microsoft® SharePoint® Server is a leading enterprise content management and collaboration platform, one that is expanding rapidly across many organizations. For IT managers, this development poses a number of challenges:

- Cost-effectively keeping pace with storage requirements
- Managing rapidly growing SharePoint Server farms
- Seamlessly scaling SharePoint deployments to manage large data files and more users
- Protecting SharePoint data efficiently
- Meeting archive, compliance, and governance requirements

2 Solution Deployment Details

This section discusses the details of the various components used in the solution. It also discusses the roles of SharePoint Server followed by the NetApp storage layout used by the SharePoint environment. In addition, it highlights the solution components and the overall architecture.

2.1 SharePoint Server Roles

The roles of a Microsoft SharePoint Server 2013 farm can be deployed as a standalone server or across many servers. The roles of the servers include:

- **Web server role.** This server responds to user requests for SharePoint web pages. The web front end (WFE) can typically be load balanced by using either the Windows Server® network load-balancing feature or other third-party software or hardware.
- **Application server role.** This server provides SharePoint services and features that can be load balanced. A few examples of the services/features provided include central administration, access services, Excel® services, user profile service, and secure store service. For a full list of services that can be configured with SharePoint 2013, refer to [Configure services and service applications in SharePoint 2013](#).
- **Database server role.** This server stores content, configuration, administration, and service data. For details on high-availability and disaster recovery options for various SharePoint 2013 databases, refer to the Microsoft TechNet article [Supported high availability and disaster recovery options for SharePoint databases \(SharePoint 2013\)](#).

Table 1 lists the details of various components installed on each server in the SharePoint farm.

Table 1) Details of SharePoint servers in this environment.

Host Name	Application	Roles
DC	Windows 2008 R2 domain	Domain controller for domain demo.netapp.com, which contains the SharePoint farm
APPMED1	Microsoft SharePoint Server 2013	Application server that also hosts the SharePoint Central Administration
WFE1, WFE2	Microsoft SharePoint Server 2013	Web front end (WFE)—Load balanced using Windows® network load balancing (NLB)

Host Name	Application	Roles
SQL1	Microsoft SQL Server® 2012	Hosts all databases related to SharePoint for configuration, administration, service, and content databases

2.2 Storage Environment

NetApp FAS Storage Controllers

The NetApp FAS series is the storage platform used in this solution. This platform offers the following advantages for this solution.

- Capacity management that provides the ability to grow as demands on collaboration increase
- Integration of the layers of storage, Microsoft Windows, and Microsoft SharePoint to simplify and automate data backup and granular restore
- Data protection to meet the high-availability requirements of SharePoint

2.3 Additional NetApp Software Used

Table 2 lists the array of NetApp software used to augment the storage platform to assist in deployment, backup, recovery, replication, management, and data protection.

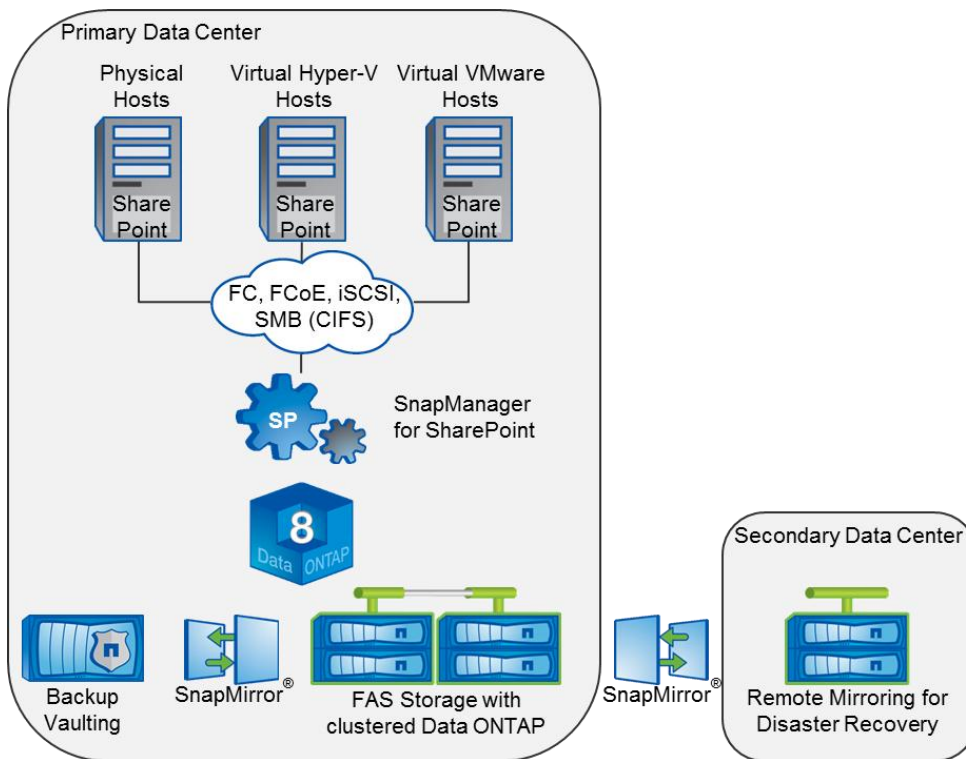
Table 2) Additional NetApp software used.

Name	Description
Data ONTAP	Clustered Data ONTAP operating system
SnapDrive® for Windows	Storage provisioning
SnapManager® for Microsoft SQL Server	Backup and recovery using application-consistent Snapshot™ copies of SharePoint databases stored in Microsoft SQL Server
SnapManager for Microsoft SharePoint Server	Application-consistent Snapshot copies during platform backups; performs granular content restore and enables application-aware disaster recovery

The solution presented in this deployment guide not only meets business requirements, but it offers additional benefits compared to other solutions that use a standard direct-attached storage implementation or a similar SAN implementation. This section describes how the solution meets the requirements stated earlier and discusses additional benefits as well.

Figure 1 illustrates the NetApp SnapManager for SharePoint solution for a SharePoint environment.

Figure 1) NetApp SnapManager for SharePoint solution for SharePoint environment.

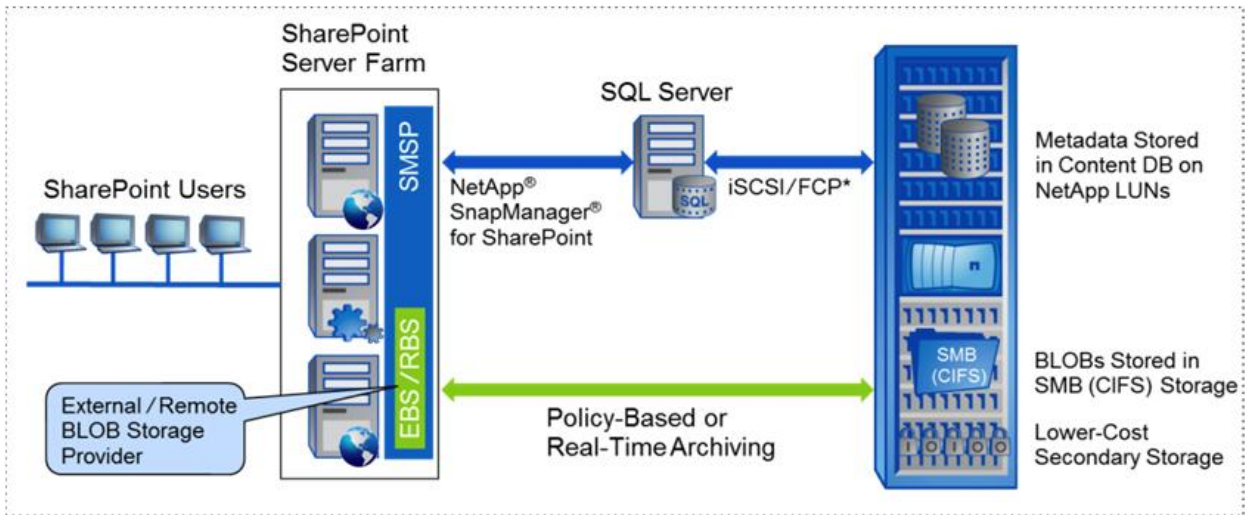


As organizations adopt SharePoint as a central repository for enterprise content, the increased data integration from multiple sources can cause unstructured BLOB data to consume up to 95% of the SQL Server storage space on SharePoint. A binary large object (BLOB) is unstructured data (such as a file or an attachment) stored in SQL Server content databases. By default, any file or attachment that is uploaded to SharePoint is stored as BLOB data in the content database. Typically, as much as 80% of the data consists of file-based data streams that are stored as BLOB data that comprise data associated with SharePoint files. However, maintaining large quantities of BLOB data in a SQL Server database is a suboptimal use of SQL Server resources.

By configuring BLOB Provider, BLOB data is externalized from a content database to a user-specified NetApp storage system. The BLOB Provider feature intercepts SharePoint database traffic and redirects all of the BLOB traffic to the external BLOB storage, leaving only a stub of the data in SharePoint. Remote BLOB Storage (RBS) is the only method of BLOB externalization supported in SharePoint 2013. RBS is implemented by SQL Server and is available in SharePoint 2013 as a set of application programming interfaces (APIs) supported by SQL Server 2008, SQL Server 2008 R2, and SQL Server 2012. RBS provides much tighter integration with SQL Server 2008 R2 Enterprise than external BLOB storage (EBS). Microsoft recommends using RBS for any new deployments because EBS will not be supported beyond SharePoint 2010.

Figure 2 illustrates the SMSP solution in a SharePoint environment with BLOB externalization.

Figure 2) NetApp SnapManager for SharePoint solution with storage optimization.



For more information, refer to [SnapManager for Microsoft SharePoint](#).

Virtualization

Server virtualization is a major component of data center virtualization and plays a key role in the virtualization initiative. NetApp has been on the forefront of solving complex business problems with its innovative technology breakthroughs and end-to-end solutions approach. The virtualization platform, through its ability to virtualize SharePoint, assists in efficient use of hardware resources that can be combined with the other key advantages of server virtualization, which include better availability, lower cost, and increased flexibility. You can realize multiple benefits from using SharePoint in a virtualized environment with NetApp storage technology, including:

- **Effective use of server hardware.** Migrating the entire SharePoint farm from dedicated physical servers that have relatively low utilization rates can lead to significantly higher server utilization.
- **Savings.** You save on power and space.
- **Reduced server hardware requirements.** The number of physical servers required to support SharePoint can also be reduced.

SharePoint supports virtualization using Hyper-V® or VMware®. SnapManager for SharePoint (SMSP) is qualified with guest initiator LUNs and pass-through disks in Hyper-V environments. In VMware environments, SnapManager for SharePoint is validated with guest initiator LUNs (easy for deployment) and iSCSI/FC RDMS or VMFS or NFS.

Table 3 lists the five protocols that SharePoint can use to communicate between server and storage.

Table 3) SharePoint implementation protocols.

Environment Type	Fibre Channel (FC)	Fibre Channel over Ethernet (FCoE)	Internet Small Computer System Interface (iSCSI)	Network File System (NFS)	Server Message Block (SMB)
Physical	Yes	Yes	Yes	No	Yes

Environment Type	Fibre Channel (FC)	Fibre Channel over Ethernet (FCoE)	Internet Small Computer System Interface (iSCSI)	Network File System (NFS)	Server Message Block (SMB)
VMware Guest	Raw Device Mapping (RDM)	RDM	Guest or RDM	VMware Disk (VMDK)	Yes
Hyper-V Guest	RDM	RDM	Guest or RDM	No	Yes

To understand the key design considerations and options for a virtual architecture that can support your SharePoint 2013 farm, refer to [Overview of arm virtualization and architectures for SharePoint 2013](#).

2.4 Database Layout Planning

This section describes how the storage from the NetApp storage controller will be configured. FlexVol® volumes will be provisioned for the SQL Server instance used for the SharePoint environment.












The typical design uses the following FlexVol volumes per SQL Server instance to store the SharePoint data:

- Volume `san_sql_InstanceName__SystemDB` contains a single LUN for the system databases—master, model, msdb. Keeping system databases in a separate LUN and FlexVol volume is done because colocating system databases with user databases in a single LUN performs a stream-based copy backup and prevents Snapshot backups of the user databases.
- Volume `san_sql_InstanceName__TempDB` contains a single LUN for the SQL Server system database tempdb. No backup will be configured for tempdb databases since this database is always rebuilt upon SQL Server restart.
- Volume `san_InstanceName_ContentDB` contains a single LUN for all the SharePoint content database data files (*.mdf).
- Volume `san_InstanceName_ContentDBLog` contains a single LUN for SharePoint content database transaction log files (*.ldf).
- Volume `san_InstanceName_NonContentDB` contains a single LUN for all the non-SharePoint database data files (*.mdf).
- Volume `san_InstanceName_NonContentDBLog` contains a single LUN for non-SharePoint database transaction log files (*.ldf).
- Volume `san_InstanceName_Search` contains a single LUN for SharePoint Search Service application databases such as Crawl, Link, Analytics Reporting, and Search Administration.
- Volume `san_InstanceName_ConfigDB` contains a single LUN for all the SharePoint configuration and database data files (*.mdf).
- Volume `san_InstanceName_ConfigDBLog` contains a single LUN for SharePoint configuration database transaction log files (*.ldf).
- Volume `san_InstanceName_SMSPStubDB` contains two LUNs for SMSP Stub database data file and transaction log files (*.ldf), respectively.
- Volume `san_InstanceName_snapinfo` contains a single LUN for SharePoint configuration database transaction log files (*.ldf).

Note: Placing all data files (.mdf) in a different FlexVol volume from the log files (.ldf) separates the random I/O of the data files from the sequential I/O to the log files and can improve SQL Server performance.

Figure 3 illustrates the volume layout for SharePoint databases on NetApp storage.

Figure 3) SMSP volume layout.

<div style="border: 1px solid black; border-radius: 10px; padding: 5px; width: fit-content;"> <p>Note Configuration per SQL Server Instance</p> </div>	<p>SQL System Databases (Master, MSDB, Model and Resource) Volume Design 1 LUN for SQL System databases</p>	 <p>Mount point Label: SystemDB FlexVol : sql_InstName_SystemDB</p>
	<p>SQL System Database - TempDB Volume Design 1 LUN for TempDB 1 LUN for TempDB Log</p>	 <p>Mount Point : TempDB FlexVol : sql_InstName_TempDB</p>
	<p>Content Database MDF Volume Design 1 LUN where the SP Content database MDF files are located</p>	 <p>Mount Point : ContentDB FlexVol : sql_InstName_ContentDB</p>
	<p>Content Database LDF Volume Design 1 LUN where the SP Content database LDF files are located</p>	 <p>Mount Point : ContentDBLog FlexVol : sql_InstName_ContentDBLog</p>
	<p>Non-Content Database MDF Volume Design 1 LUN where the other database MDF files are located</p>	 <p>Mount Point : NonContentDB FlexVol : sql_InstName_NonContentDB</p>
	<p>Non-Content Database LDF Volume Design 1 LUN where the other database LDF files are located</p>	 <p>Mount Point : NonContentDBLog FlexVol : sql_InstName_NonContentDBLog</p>
	<p>Search Databases Volume Design 1 LUN for Search databases</p>	 <p>Mount Point : Search FlexVol : sql_InstName_Search</p>
	<p>SharePoint Configuration Database and Admin database Volume Design 1 LUN where the SP Configuration database MDF files are located</p>	 <p>Mount Point : ConfigDB FlexVol : sql_InstName_ConfigDB</p>
	<p>Configuration Database LDF Volume Design 1 LUN where the SP Configuration database LDF files are located</p>	 <p>Mount Point : ConfigDBLog FlexVol : sql_InstName_ConfigDBLog</p>
	<p>SMSP Stub Database and Log Volume Design 1 LUN for StubDB 1 LUN for StubDB Log</p>	 <p>Mount Point : SMSPStubDB FlexVol : sql_InstName_SMSPStubDB</p>
	<p>SnapInfo 1 LUN containing SnapInfo directory content, SnapInfo Metadata, streaming backup of all system databases except TempDB.</p>	 <p>Mount Point : SnapInfo FlexVol : sql_InstName_SnapInfo</p>

2.5 SharePoint LUN Sizing

SQL Server System Database FlexVol Volume and LUN Sizing

System databases are not configured for Snapshot-based backups; backups of these databases are streamed to the SnapInfo area on a separate LUN. Snap Reserve can be set to 0% and the LUN in the FlexVol volume can be almost as large as the FlexVol volume itself.

A 100GB LUN for a system database in a 120GB FlexVol volume will be set up for each SQL Server instance.

Content Database Sizing

Use the following formula to estimate the size of your content databases:

Database size = ((D × V) × S) + (10KB × (L + (V × D)))

Note: The value 10KB in the formula is a constant that approximately estimates the amount of metadata required by SharePoint Server 2013. If your system requires significant use of metadata, you might want to increase this constant.

Where:

- D - Expected number of documents. This value typically depends on the features (such as Recycle bins and auditing) that you use.
For example, for My Sites or collaboration sites, we recommend that you calculate the expected number of documents per user and multiply by the number of users.
For records management or content publishing sites, you may calculate the number of documents that are managed and generated by a process.
- S - Average size of the documents.
- L - Estimate the number of list items in the environment. We generally use an estimate of three times the number of documents (D), but this will vary based on how you expect to use your sites.
- V - Average number of versions any document in a library will have.

SharePoint Configuration FlexVol Volume and LUN Sizing

We recommend that you allocate 2GB for the Configuration database and 1GB for the Central Administration content database.

SMSP Stub Database Sizing

The minimum unit for assigning StubDB is content database. The stub DB size is small (for a content DB with a maximum of 60 million document BLOBs, the stub DB size will be less than 20GB).

SMSQL SnapInfo FlexVol Volume and LUN Sizing

The SnapInfo LUN will contain the following:

- Streaming backups of system databases, except TempDB, which is not backed up
- Backups of the active portion of user database transaction logs
- SnapManager for SQL Server (SMSQL) backup set metadata

The data in the SnapInfo LUN is arranged in a folder structure beneath a SnapInfo folder in the root of the drive. The amount of data in the SnapInfo area depends on the size of a backup and the number of days' backups that are retained online.

The size of the SnapInfo LUN is calculated as follows:

= ((system database size + (Maximum DB LDF size X Daily log change rate %)) X Snapshot retention)/(1-LUN overhead space %)

The SnapInfo LUN sizing calculation above assumes the following:

- System databases backup. TempDB is not included because it is recreated every time SQL Server is restarted and is not backed up.
- Backups (online Snapshot-based backups) are retained for 7 days on primary storage.
- 10% LUN overhead space.

The size of the SnapInfo FlexVol volume is calculated as follows:

= ((Size of SnapInfo LUN) x (1+Fractional Reserve)) + (System database Size+ (Maximum DB LDF size X Daily log change rate %)) X Snapshot retention)

Note: The fractional reserve is set to 0% for all the volumes and will not be used.

2.6 Installation and Configuration

This section provides an overview of the installation sequence as well as specific configuration parameters, with a focus on the NetApp components of the solutions.

Table 4 lists the primary tasks for installing and configuring the solution.

Table 4) Installation and configuration procedure.

Steps	Task	Description
1.	Review the solution design	<ul style="list-style-type: none"> Review and sign off on the requirements and design Make sure that business objectives and IT deliverables are aligned
2.	Prepare data centers	<ul style="list-style-type: none"> Rack space and power preparations Cabling, network ports, and SAN ports TCP/IP address and DNS host names <p>Note: The power supply requirements are relevant to the hardware that is used. For information about power supply requirements specific to the customer environment, refer to the appropriate technical specification documentation.</p> <p>Note: For detailed information about the site preparation requirements, refer to the NetApp Site Requirements Guide.</p>
3.	Install server hardware	<ul style="list-style-type: none"> Install server hardware Comply with both internal standards and hardware vendor best practices
4.	Install and configure FAS storage arrays	<ul style="list-style-type: none"> Provide physical installation Install Data ONTAP Create aggregates, storage virtual machine (SVM), and volumes
5.	Install and configure Microsoft Windows servers	<ul style="list-style-type: none"> Validate Microsoft Windows operating system prerequisites for SharePoint 2013; refer to System requirements for SharePoint 2013 Perform any required updates and patches
6.	Install and configure Microsoft SQL Server	<ul style="list-style-type: none"> Validate Microsoft prerequisites for Microsoft SQL Server 2012 used by the SharePoint 2013 farm Hardware and Software Requirements for Installing SQL Server 2012 Install SQL Server 2012 from the Installation Wizard (Setup) Perform any required updates and patches
7.	Install and configure Microsoft SharePoint Server	<ul style="list-style-type: none"> Install SharePoint 2013 on respective servers of the SharePoint farm Also refer to: Hardware and software requirements for SharePoint 2013 prior to the installation Deployment guide for SharePoint 2013 provides

Steps	Task	Description
		deployment instructions for SharePoint 2013 <ul style="list-style-type: none"> Configure service applications and web applications in the SharePoint farm
8.	Install NetApp SnapDrive for Windows on various servers in the SharePoint farm	<ul style="list-style-type: none"> Install SnapDrive prerequisites Install SnapDrive software and provision LUNs from FAS controller
9.	Install NetApp SnapManager for SQL Server	<ul style="list-style-type: none"> Install SnapManager for SQL Server on all nodes in the SQL Server 2012 Availability Group
10.	Install NetApp SnapManager for SharePoint in the SharePoint farm	<ul style="list-style-type: none"> Install SnapManager for SharePoint Manager Install SnapManager for SharePoint Agent on all SharePoint servers in the farm Configure and schedule backups
11.	Test and validate the solution	<ul style="list-style-type: none"> Pretest of solution readiness Test and validation – Refer to Appendix B Validation of backup and restore – Refer to Appendix C

For detailed installation and configuration steps, refer to [Appendix A: Installation and Configuration Details](#) in this guide.

2.7 Installing NetApp SnapDrive for Windows on SharePoint Servers in the Farm

The Microsoft SharePoint 2013 server roles depend heavily on storage for a stable and reliable configuration. NetApp offers many advantages over other storage vendors for SharePoint, most notably the ability to capture the state of the SharePoint 2013 databases and index at various points in time, called Snapshot copies. You must confirm that your storage system and your Windows system meet at least the minimum requirements to properly install and run SnapDrive.

Before setup begins, verify the compatibility of all hardware and software involved using the [NetApp Interoperability Matrix Tool](#).

1. Prepare the Windows Host part of the Microsoft SharePoint farm in the SnapDrive configuration.
2. Verify that the host meets the minimum requirements for use with SnapDrive.
3. Determine whether the Microsoft iSCSI Software Initiator program is installed.
4. Determine whether SnapDrive was previously installed.
5. Determine which FC or iSCSI HBA or MPIO components are already installed.

SnapDrive supports three protocols for creating and managing LUNs: iSCSI, FC, and FCoE. Before installing SnapDrive for Windows, install these components on the host computer, as listed in Table 5.

Table 5) Required components.

Scenario	Tasks
The iSCSI protocol and software initiator will be used to create and manage LUNs.	<ul style="list-style-type: none"> Install the Microsoft iSCSI Software Initiator. Install the iSCSI Host Utilities on the hosts. <p>Note: NetApp highly recommends installing Data ONTAP DSM for Multipathing.</p>

Scenario	Tasks
The iSCSI protocol and hardware initiator will be used to create and manage LUNs.	<ul style="list-style-type: none"> • Install the iSCSI HBA. • Install the iSCSI HBA driver and firmware. <p>Note: NetApp highly recommends installing Data ONTAP DSM for Multipathing. Install the iSCSI Host Utilities on the hosts if Data ONTAP DSM is not installed.</p>
The FC protocol will be used to create and manage LUNs.	<ul style="list-style-type: none"> • Install FCP HBA or CNA for FCOE. • Install the FC driver and firmware. <p>Note: NetApp highly recommends installing Data ONTAP DSM for Multipathing. Install the Windows Host Utilities on the hosts if Data ONTAP DSM is not installed.</p>
A Common Internet File System (CIFS) protocol for CIFS shares is used by SMSP storage optimization modules.	<ul style="list-style-type: none"> • License CIFS and set it up and start it on the NetApp storage system. • Create a CIFS share.

For detailed SDW installation steps, refer to [Appendix A: Installation and Configuration Details](#).

Prepare Each Storage System in SnapDrive Configuration

1. After verifying that licenses for FC, iSCSI, or both are enabled on the storage system, start the services by entering the `fc start` command or the `iscsi start` command at the storage system command line.

Note: For more information, refer to the appropriate Data ONTAP administration guide on the [NetApp Support](#) site.

2. Prepare a volume on the storage system to hold SnapDrive LUNs.

SnapDrive Prerequisites in Clustered Data ONTAP Environments

For help with supported configurations for NetApp, refer to the [NetApp Interoperability Matrix Tool](#).

Before installing SnapDrive for Windows, the following prerequisites in Table 6 must be met.

Table 6) Prerequisites for SnapDrive for Windows.

Description of Prerequisites
<p>The following licenses are required on the storage system:</p> <ul style="list-style-type: none"> • Fibre Channel Protocol (FCP) or iSCSI (depending on the configuration) - Use FC/iSCSI-accessed LUNs. • FlexClone[®] technology - Enable volume clone functionality on flexible volumes. • SnapRestore[®] technology - Restore LUNs from Snapshot copies. • SnapDrive or SnapManager_Suite (either on the host or on the system) - Use whichever license enables SnapDrive functionality when the SDW license is not on the host. • SnapVault[®] technology (optional). • SnapMirror technology (optional). <p>To determine which licenses are enabled on a storage system, complete these steps:</p> <ol style="list-style-type: none"> 1. Log in to the storage system through the console or telnet. 2. Type <code>license</code> to display the list of licenses installed. <p>Note: This can also be done through System Manager.</p>
<p>A SnapDrive user service account on the storage system is required.</p> <p>Note: This account is required to connect SnapDrive to the storage system.</p>
<p>The transport protocol (HTTP, HTTPS, or RPC) that SnapDrive will use to communicate with the storage system must be determined.</p> <p>Note: NetApp recommends using HTTPS. The HTTPS protocol allows using the Data ONTAP interface for all interactions between the storage system and the host, including sending passwords securely. For SnapDrive to use the HTTP or HTTPS protocol, the <code>httpd.admin.enable</code> option must be set on the storage system.</p> <p>Note: The RPC protocol is not supported by SnapDrive on clustered Data ONTAP systems.</p>
<p>NET Framework 4.0 is required.</p>
<p>NetApp Windows Host Utilities 6.0.2 or later is required.</p>
<p>The required hotfix for Windows 2012 is 2859162 and for Windows 2008 R2 the hotfixes are 2522766, 2528357, 2494016, 2520235, 2531907, and 974930.</p>
<p>Cluster- and node-management logical interfaces (LIFs) are required.</p>
<p>An SVM with the following settings and configurations is required:</p> <ul style="list-style-type: none"> • Data volumes with junction paths are defined. • An SVM management LIF has the following parameter settings: <code>data=role, protocols=none, firewall policy=management</code> • Vsadmin password is set and the account is unlocked. • On each node in the cluster, there is a data LIF for SAN protocols that is separate from any data LIFs.

Note: Set appropriate storage controller options for the volume.

Note: Synchronize the storage controller clocks with the Active Directory[®] servers and configure DNS settings on the storage controller. Verify that name resolution is working before installing SnapDrive for Windows on the hosts.

Install SnapManager for SQL Server

NetApp SnapManager for SQL Server provides the underlying host intelligence required to present storage and to coordinate SharePoint 2013–aware backups using NetApp Snapshot technology.

Prior to installing SMSQL, verify that the prerequisites in Table 7 are met.

Table 7) Prerequisites for SnapManager for SQL Server.

Description of Prerequisites
The Microsoft SQL Server application has been installed on the host where NetApp SnapManager for SQL Server (SMSQL) will be installed.
SQL Server Browser service is running on the host on which SMSQL will be installed.
The installation account used to install SMSQL is a member of the local administrators group on the host where SnapManager for SQL Server will be installed.
The following components must be installed or configured on the storage system: <ul style="list-style-type: none">• iSCSI or Fibre Channel (FC) protocols• SnapManager license• SnapRestore license• SnapMirror license• FlexClone license• CIFS license
SnapDrive for Windows (SDW) has been installed on the SQL Server host on which SnapManager will be installed. Note: For more information about installing SnapDrive, refer to the SnapDrive for Windows Installation and Administration Guide .
The SnapDrive-preferred IP address (if the storage system has multiple IP addresses), Microsoft iSCSI Software Initiator, and SnapDrive for Windows must be installed.
Storage must be configured and the LUNs must be presented to the Windows servers.
The SMSQL service account must have a SQL Server login and sysadmin role assigned to the SQL Server login for the SQL Server instance on which SMSQL will be installed.
.NET Framework 4.0 has been installed on the host on which SMSQL will be installed.

For help with supported configurations for NetApp, refer to the [NetApp Interoperability Matrix Tool](#).

Prior to installing SMSQL, refer to the section “Preparing to install or upgrade SnapManager” in the [SnapManager 7.0 for Microsoft SQL Server Installation and Administration Guide](#).

Download the SnapManager for SQL Server software from <http://support.netapp.com/> and follow the installation steps outlined in [Appendix A: Installation and Configuration Details](#).

Install SnapManager for SharePoint

NetApp SnapManager for SharePoint allows the migration and data protection of SharePoint 2013 content (databases and index). Prior to installing SMSP, verify that the prerequisites in Table 8 are met. For prerequisites and supported configurations, refer to the [Interoperability Matrix Tool](#).

Table 8) Prerequisites for SnapManager for SharePoint.

Description of Prerequisites
Microsoft Prerequisites
Windows Server 2012 is installed.
SQL Server 2012 is installed.
Windows PowerShell® 2.0 or later is installed.
.NET Framework 3.5 SP1 or later (excluding .NET Framework 4.0) is installed.
For Windows Server 2012, the following Windows features must be installed: .NET Framework 3.5.1, HTTP activation, non-HTTP activation, WCF services, and TCP port sharing.
More than 1GB of disk space is available.
Net.TCP Port Sharing Service is started.
Windows Process Activation Service (WAS) is started and the process model, the .NET environment, and the configuration application programming interfaces (APIs) are enabled.
World Wide Web Publishing Service (W3SVC) is started.
The following Windows features and tools are installed: <ul style="list-style-type: none"> • Web server • Common HTTP features, such as static content and default document • For Windows Server 2012: application development (ASP.NET 3.5, .NET extensibility 3.5, ISAPI extensions and ISAPI filters) • Management tools, such as Internet Information Services (IIS) Management Console, IIS 6 Management Compatibility, and IIS 6 Metabase Compatibility
IIS Admin Service is started.
NetApp Prerequisites
SnapDrive for Windows is installed.
SnapManager for SQL Server is installed.
Clustered Data ONTAP 8.2 is installed
Network Configuration Prerequisites
The following ports must be open: <ul style="list-style-type: none"> • 14000: Control Service port • 14001: Media Service port • 14002: Media Service data port • 14003: Report Service port • 14004: SMSP Agent port
Application Pool Prerequisites

Description of Prerequisites
<p>The following IIS7 advanced settings are required:</p> <ul style="list-style-type: none"> • .NET Framework Version is set to v2.0 or v4.0. • Enable 32-Bit Applications is set to <code>False</code>. • Managed Pipeline Mode is set to <code>Integrated</code> (<code>Classic</code> is not supported with .NET Framework 4.0). • Load User Profile is set to <code>True</code>. • Start Automatically is set to <code>True</code>.
<p>The following local permissions are required:</p> <ul style="list-style-type: none"> • <code>IIS_WPG</code> (for IIS 6.0) or <code>IIS_IUSRS</code> (for IIS 7.0 and IIS 8.0). • Full control to <code>HKEY_LOCAL_MACHINE\SOFTWARE\Network Appliance\SnapManager 7 for SharePoint</code>. • Full control to SMSP Manager folder. • Member of the Performance Monitor Users group. • Full control to SMSP certificate private keys.

Table 9 lists the SMSP components that need to be installed on each server in the SharePoint farm.

Table 9) SMSP components mapped to SharePoint farm hosts.

Host Name	Microsoft Software	NetApp Software	Optional SMSP Modules
APPMED1	Microsoft SharePoint Server 2013 Application Server Role	SnapDrive for Windows (SDW)—to perform SharePoint search index Snapshot backups SMSP Manager—to control, Media and Reporting Services	
SQL1	Microsoft SQL Server 2012 named instance that manages all SharePoint configuration, administration, and service and content databases	SnapManager for SQL Server (SMSQL)—to perform database Snapshot backups of SharePoint databases SMSP Agent—to communicate with SQL Server used by the SharePoint farm, based on commands it receives from the SMSP Manager's Control Service	

WFE1	Microsoft SharePoint Server 2013 Web Front-End Role	<p>SnapDrive for Windows (SDW)—to perform SharePoint backups of 14/15 hives</p> <p>SMSP Agent—to communicate with SharePoint based on the commands it receives from the SMSP Manager's Control Service</p>	<ol style="list-style-type: none"> 1. Storage Manager—enable only to perform stub-based externalization of documents to NetApp CIFS share 2. Archive Manager—for policy-based archiving of SharePoint data <p>Connector—to ingest content from a network file share into SharePoint directly through SharePoint without migration</p>
WFE2	Microsoft SharePoint Server 2013 Web Front-End Role	<p>SnapDrive for Windows (SDW)—to perform SharePoint backups of 14/15 hives</p> <p>SMSP Agent—to communicate with SharePoint based on the commands it receives from the SMSP Manager's Control Service</p>	<ol style="list-style-type: none"> 1. Storage Manager 2. Archive Manager 3. Connector

For detailed SMSP installation steps, refer to [Appendix A: Installation and Configuration Details](#).

It is important to migrate the SharePoint database to NetApp LUNs to enable the backup of SharePoint content through the SnapManager for SharePoint platform backup feature. Before you migrate the SharePoint-related databases, verify that all of the prerequisites in Table 10 are met.

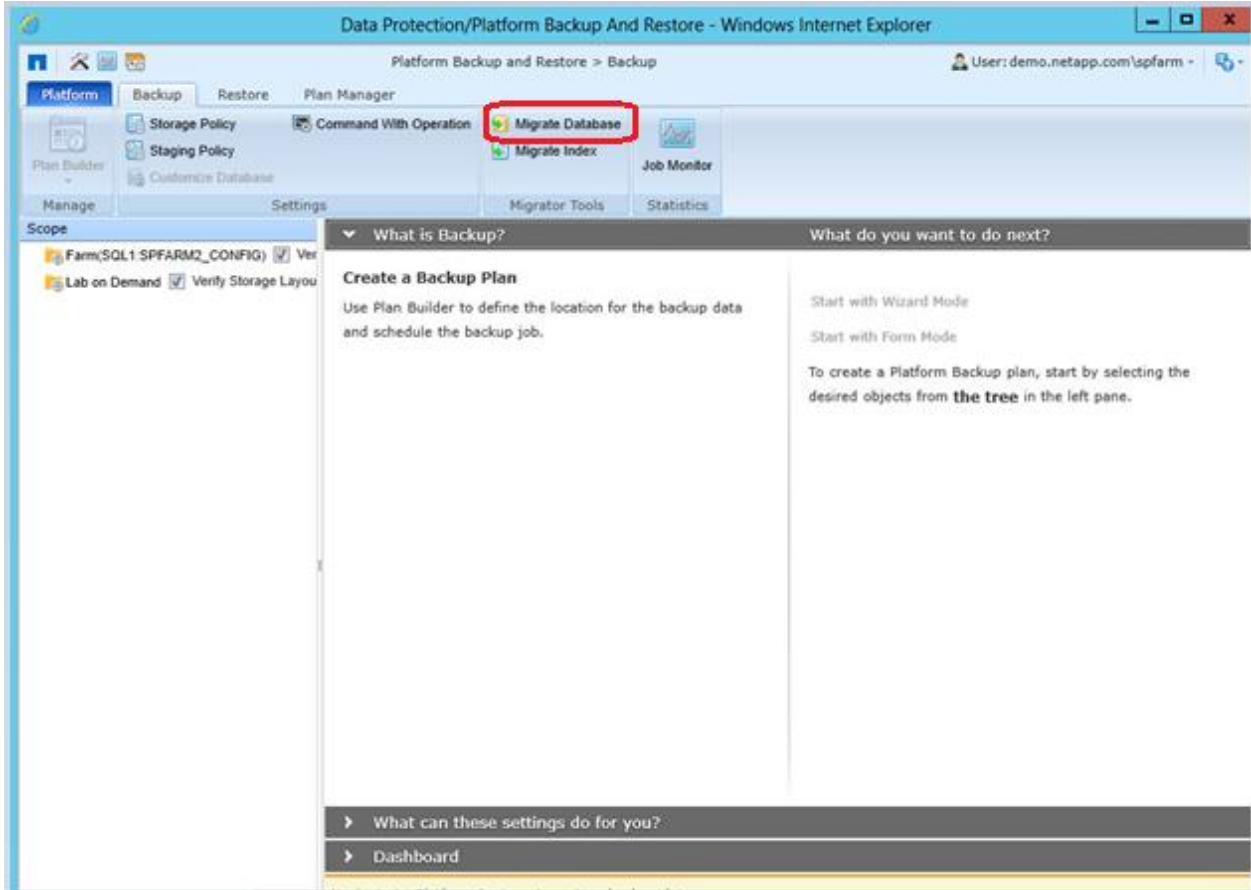
Table 10) SnapManager for SharePoint configuration prerequisites.

Description of Prerequisites
<p>The following web applications must be running in SharePoint before their databases are migrated:</p> <ul style="list-style-type: none"> • SharePoint Configuration database • SharePoint Central Administration database • Content database • Custom databases <p>Note: The database list can be accessed by selecting Manage Database in the SharePoint Central Administration page.</p>
<p>A Common Internet File System (CIFS) share must be created and the CIFS protocol must be set up and started on the storage system.</p>
<p>Signing must be enabled on the NetApp storage system by running the <code>options cifs.smb2.signing.required</code> on command.</p>

NetApp SnapManager Database Migration/Configuration

After installation of SnapManager for SharePoint, use the SMSP Migrate Database tool to migrate SharePoint database to a NetApp LUN in order to be backed up by SnapManager for SharePoint.

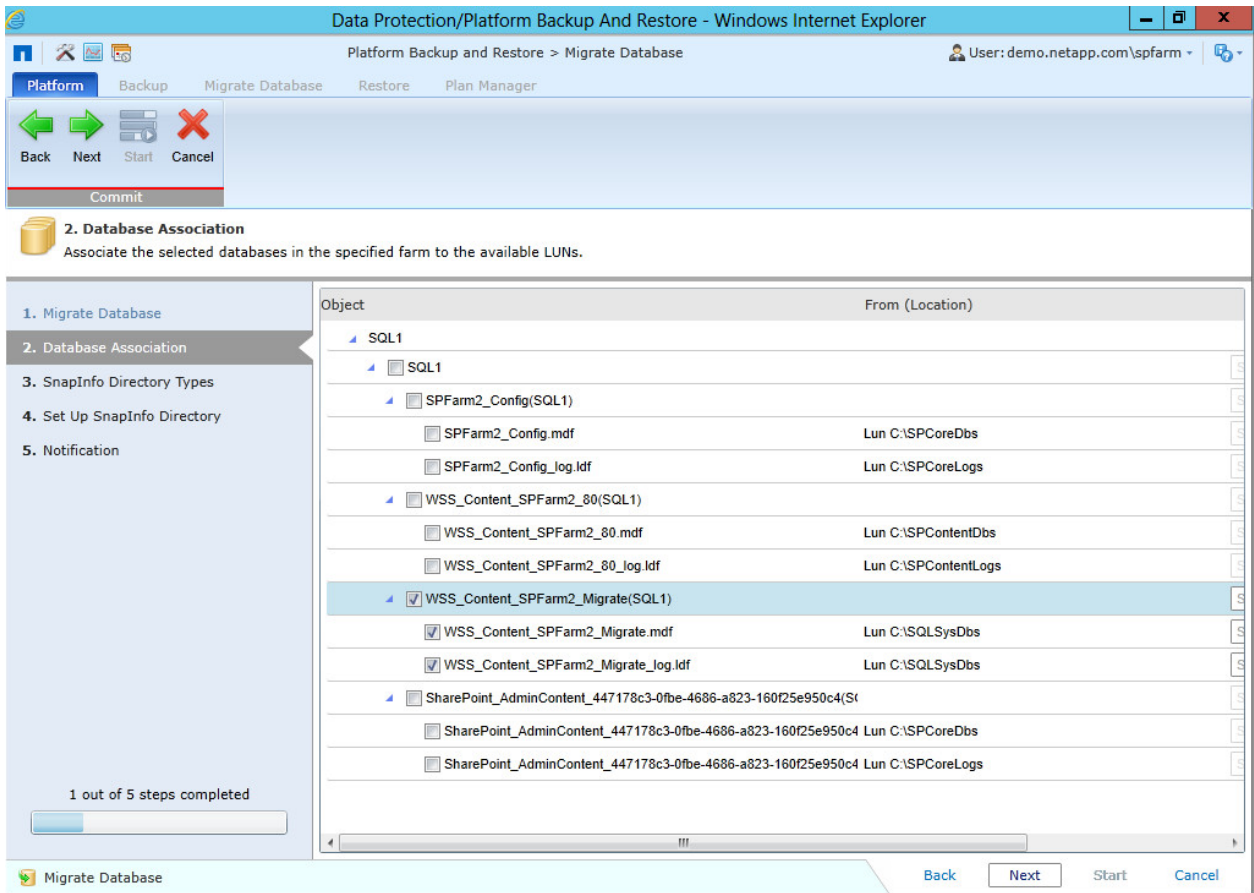
1. Log in to the SnapManager for SharePoint Manager. By default, it will land on the Data Protection section. Click Platform Backup & Granular Restore.
2. Click the Backup tab, then click Migrate Database.



3. In the Migrate Database page, select the farm that contains the SharePoint database you want to migrate for the Farm Selection field. Choose the Agent from the Agent selection drop-down list to migrate the database on the specified Agent server. Click Next.

Note: All of the SnapManager for SharePoint Agents installed on the SQL Server instances of the specified farm are loaded in the Agent Selection field.

4. In the Database Association page, select the checkbox of the SharePoint database to migrate.



5. Scroll to the right where the To (Available Disk) field becomes enabled. Then select the LUN from the drop-down list for the .mdf file.

Platform Backup and Restore > Migrate Database User: demo.netapp.com\spfarm

Platform Backup Migrate Database Restore Plan Manager

Back Next Start Cancel

Commit

2. Database Association

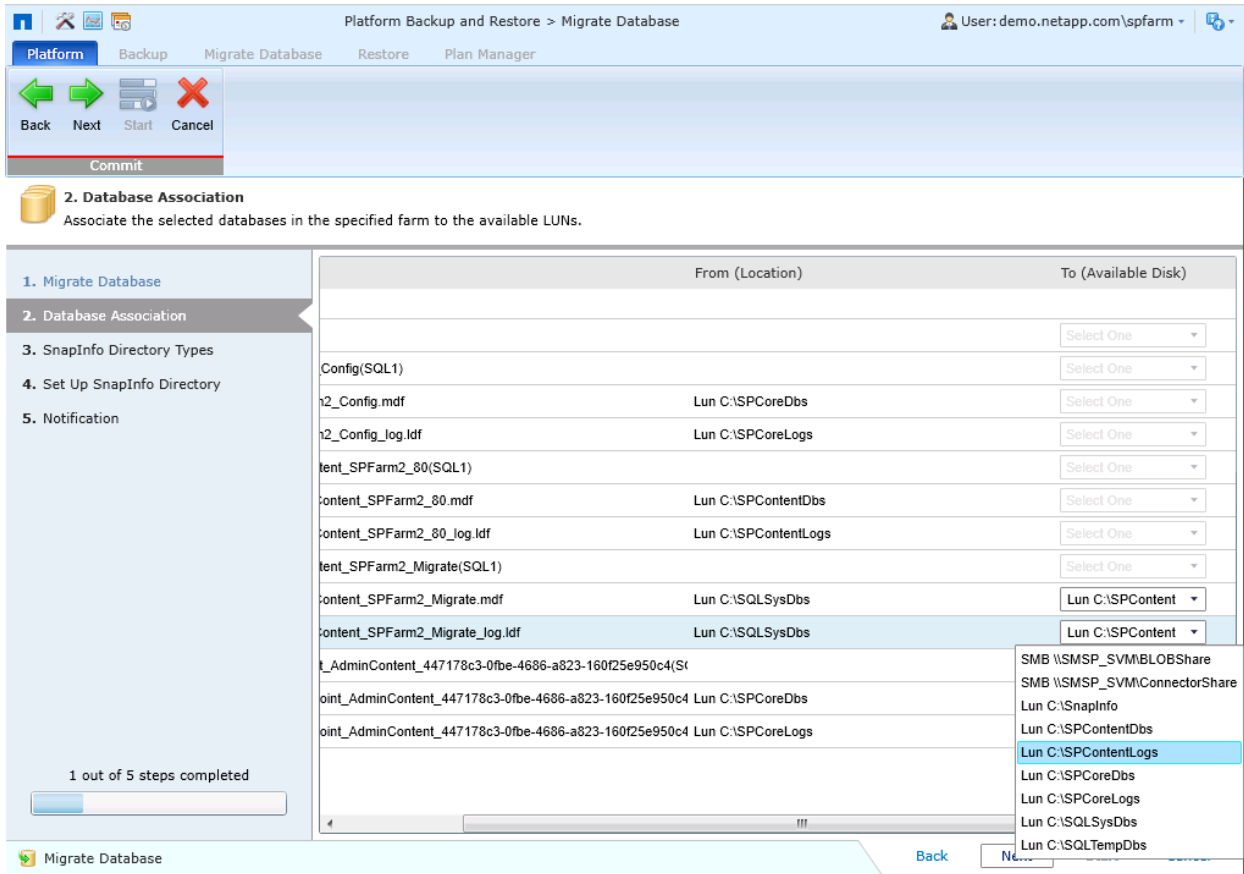
Associate the selected databases in the specified farm to the available LUNs.

	From (Location)	To (Available Disk)
		Select One
		Select One
Config(SQL1)		Select One
2_Config.mdf	Lun C:\SPCoreDbs	Select One
2_Config_log.ldf	Lun C:\SPCoreLogs	Select One
ent_SPFarm2_80(SQL1)		Select One
ontent_SPFarm2_80.mdf	Lun C:\SPContentDbs	Select One
ontent_SPFarm2_80_log.ldf	Lun C:\SPContentLogs	Select One
ent_SPFarm2_Migrate(SQL1)		Lun C:\SPContent
ontent_SPFarm2_Migrate.mdf	Lun C:\SQLSysDbs	Lun C:\SPContent
ontent_SPFarm2_Migrate_log.ldf	Lun C:\SQLSysDbs	SMB \SMSP_SVMBLOBShare SMB \SMSP_SVM\ConnectorShare Lun C:\SnapInfo
oint_AdminContent_447178c3-0fbe-4686-a823-160f25e950c4(S		Lun C:\SPContentDbs
oint_AdminContent_447178c3-0fbe-4686-a823-160f25e950c4	Lun C:\SPCoreDbs	Lun C:\SPContentLogs
oint_AdminContent_447178c3-0fbe-4686-a823-160f25e950c4	Lun C:\SPCoreLogs	Lun C:\SPCoreDbs
		Lun C:\SPCoreLogs
		Lun C:\SQLSysDbs
		Lun C:\SQLTempDbs

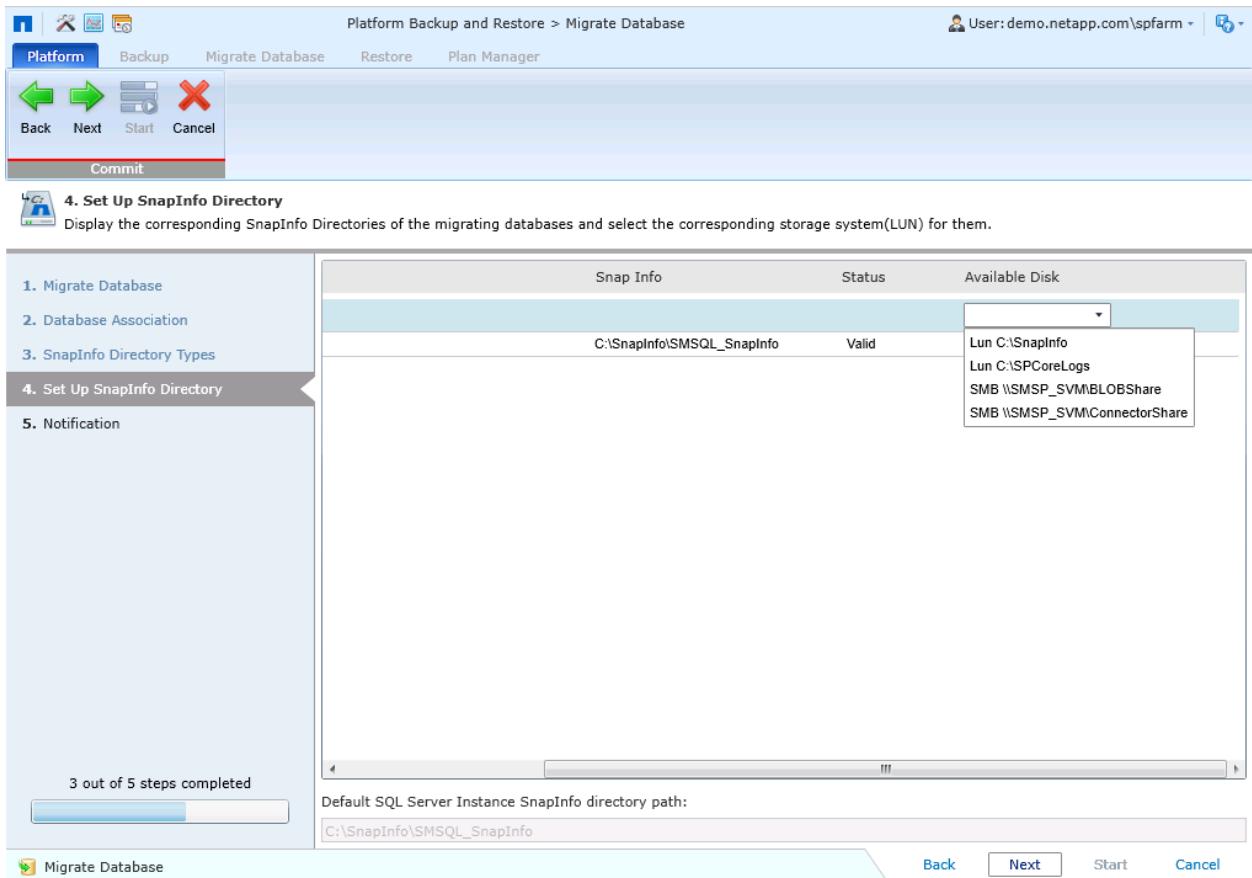
1 out of 5 steps completed

Migrate Database Back Next Start Cancel

6. Similarly, select the LUN from the drop-down list for the .ldf file. Click Next.



7. Select the Single SnapInfo directory for SnapInfo Types field. Click Next.
8. In the Set Up SnapInfo Directory page, check the checkbox for the SQL Server instance.
9. Scroll to right to select the SnapInfo directory LUN for the specified SQL Server instance in the Available Disk drop-down. Click Next.



10. Leave the default as None on the Notification page and click Start.
11. The migration of the database will stop all the SharePoint services on all the servers in the farm. Click OK.
12. The job will now start and you can view it by clicking Job Monitor.

Note: To confirm that the database has been moved to the NetApp LUN, open SQL Management Studio > Database > Content database > Properties > Files > Path to confirm the location of the data files.

2.8 Test and Validate Solution

This phase entails validating solution readiness using various backup and restore operations.

Pretest of Solution Readiness

After setting up and configuring the designed SharePoint environment in this deployment guide, it is important to test every component for its readiness in terms of functionality, resiliency, and availability.

Table 11 lists tests that can be performed at each level to check the readiness of the architecture to meet its design specifications.

Table 11) SMSP readiness tests performed.

Operations	Basic	Functionality
Windows user logon.	x	
SMSP Manager Login functionality.		x
Verify Storage Configuration settings in SMSP Control Panel that allow you to create and configure a storage system profile, physical and logical devices, or storage policies for certain SnapManager for SharePoint modules to store backup data.		x

Storage Connectivity and Validation Tests

Table 12 lists the tests performed to verify that the basic storage connectivity is tested and validated before stress testing the solution.

Table 12) Connectivity and validation tests performed.

Operation	Functionality
SnapDrive Create LUN	x
SnapDrive Destroy LUN	x
SnapDrive Expand LUN	x
SnapDrive LUN Connect	x
SnapDrive LUN Disconnect	x
SnapDrive Create Snapshot	x
SnapDrive Delete Snapshot	x

Backup and Recovery Tests

Table 13 summarizes the backup and recovery tests validated with the solution. Table 14 contains detailed backup tests, and Table 15 contains detailed restore tests.

Table 13) SMSP backup and recovery tests.

Operation	Functionality	High Availability
Periodic backups of SharePoint farm with granularity set to item level using SnapManager for SharePoint Snapshot copies (with frequency as twice per day, 1 daily backup, and 1 weekly	x	

Operation	Functionality	High Availability
backup)		
Backup of SharePoint farm with backup verification enabled using SnapManager for SharePoint	x	x
Granular restore of items in SharePoint	x	
Clone restore of database to different SharePoint farm	x	

Table 14) SnapManager for SharePoint backup test.

Step	Description
Task	To test the backup of SnapManager for SharePoint backup and data retention: <ul style="list-style-type: none"> Perform and verify SharePoint farm backup using SMSP Data Protection to include hourly, daily, and weekly copies with granular and configurable retention of each. Monitor the time to do the average backup tasks.
Observed Results	Observe the backup of the SharePoint farm, retention, and total backup time.

Table 15) SnapManager for SharePoint restore test.

Step	Description
Task	To test the granularity and scalability of SnapManager for SharePoint backup and data retention: <ul style="list-style-type: none"> Perform point-in-time restoration of an entire SharePoint content database. Perform a granular restore of SharePoint items from a successful backup job. Monitor time to do the restoration.
Observed Results	Observe the point-in-time restore and granular recovery of individual SharePoint items.

3 Solution Operation

3.1 Capacity Management

This section describes how to grow and manage the capacity of the NetApp storage systems as business needs grow.

FlexVol Volume Management

Flexible volumes can be sized according to capacity requirements. The size of a flexible volume can be increased or decreased. The resize can be accomplished from the command line (RSH, telnet, console) or from System Manager.

To resize the volume from the command line, enter the following command:

```
vol size -vserver <vserver name> -volume <vol_name> -new-size [+ | -] <New size>
```

In this command, `vol_name` is the name of the volume and `size` is the space to be added to or removed from the volume. `Size` also includes a modifier to identify whether the space added is in kilobytes (k), megabytes (m), gigabytes (g), or terabytes (t). The plus or minus sign indicates whether space will be added to or subtracted from the volume.

Example: The volume name is `vol_SPDbvol1` and the size is 250GB. The new desired size is 300GB. The command to change the size of the volume is:

```
vol size -vserver <vserver name> -volume vol_SPDbvol1 -new-size +50g
```

Expand LUNs

To expand the LUNs, follow these steps:

1. Under SnapDrive in the left MMC pane, expand the instance of SnapDrive you want to manage, then expand Disks and select the disk you want to manage.
2. From the menu choices at the top of MMC, navigate to Action > Resize Disk.
3. Next to Maximum size in the Resize Disk window, leave selected Reserve space for at least one Snapshot copy.

Note: When you select this option, the disk size limits displayed are accurate only when they first appear on the Select LUN Properties panel.

4. In the New size box, either type a value or use the slider bar to increase or decrease the amount of space the disk uses.
5. Select the Take a Snapshot before resizing the LUN checkbox to take a Snapshot copy before you resize your disk.
6. Click OK.
7. Create a new Snapshot copy of the resized disk.

If you increase the size of the LUN, you might need to close and reopen the computer management MMC (`compmgmt.msc`) before the increased LUN size becomes visible in the Disk Management snap-in.

3.2 Backup and Recovery Operations

Configuring Backups by Using SnapManager for SharePoint

SharePoint database backup and BLOB storage backup serve different purposes in SMSP. Database backup is applicable to both disaster recovery (DR) and item-level recovery (non-DR). BLOB storage backup is only for DR. The frequency of the SharePoint database backup and the BLOB data backup can be matched to the same hourly schedule; however, this is not usually necessary. For example, consider the following scenario:

1. The user creates a document that is changed to `stub1 + BLOB1`.
2. The user changes the document and saves it again; overwriting `stub1` (versioning is not enabled). The new document is changed to `stub2 + BLOB2`.
3. The user now wants to get the previous version back and uses the previous database backup to restore `stub1` (if versioning is enabled, the previous version can be used by accessing the version history).
4. Because `BLOB1` is still in the BLOB store, the restore of the user data works.

Note: Use caution when removing orphaned BLOBs. BLOBs are not automatically removed immediately after the stub is deleted from SharePoint.

The following components are backed up when submitting an SMSP backup of the SharePoint farm:

- SharePoint content databases

- Custom databases
- SharePoint search indexes
- SharePoint components and settings
- SharePoint solutions
- SharePoint front-end resources, including IIS settings, `inetpub` folder, SharePoint Hive, and Global Assembly Cache (GAC)

SMSQL performs Snapshot copy backups of the SharePoint database, and SnapDrive performs Snapshot copy backups of the search index. Backup data of other SharePoint components is sent to SMSP Media Service where it is stored with the backup job metadata and index.

For restore, these restore levels are available in SMSP:

- **Farm-component level.** Multiple farm components can be selected for restore, such as content databases, web applications, service applications, and even the entire farm and its settings.
- **Granular level.** If granular indexing options are selected during backup, individual site collections, sites, lists, folders, items, and item versions can be restored from the content databases.
- **Clone restore to another farm.** The clone to another farm feature restores backed-up web applications and content databases only to a separate SharePoint farm. If BLOB data or a stub database is being backed up with the selected web application or content database, the BLOB data and the stub database will be cloned to the destination farm as well.

For detailed SnapManager for SQL Server backup configuration steps and restore steps, see [Appendix C: Solution Operation Details](#).

4 Conclusion

Microsoft SharePoint Server is a powerful and cost-effective collaboration solution that has been deployed to meet a wide variety of enterprise and departmental needs. NetApp delivers an agile storage solution for Microsoft SharePoint Server environments through:

- A unified architecture supporting SAN for SharePoint database content and SMB or CIFS for binary and large object files or BLOBs.
 - Data ONTAP, a unified storage platform that provides the following advantages:
 - Nondisruptive operations allow you to maintain storage access during routine maintenance and upgrades.
 - Data deduplication is available on both primary and secondary storage.
 - Our multi-tenant platform enables sharing of physical resources across departments or organizations.
- SnapManager for Microsoft SharePoint Server offers up additional benefits, such as:
- NetApp's policy-based intelligent management helps you automate storage management.
 - NetApp supports more frequent recovery points, as many as one per minute.
 - We deliver granular SharePoint data recovery.
 - Deep integration with AvePoint DocAve is available for industry-leading compliance and governance capabilities.

Appendix A: Installation and Configuration Details

Detailed Steps to Install SnapDrive for Windows

Download SnapDrive for Windows

Download SnapDrive for Windows from the following link:

<http://support.netapp.com/NOW/cgi-bin/software?product=SnapDrive&platform=Windows>

Consult your NetApp systems engineer to acquire a license to start using SnapDrive capabilities.

Install SnapDrive for Windows

Install SnapDrive for Windows on all the Microsoft SQL Server nodes to provision and manage storage LUNs and also the SharePoint Search Index server. Before setup begins, verify the compatibility of all hardware and software involved by using the [NetApp Interoperability Matrix Tool](#).

To install SnapDrive for Windows (SDW), complete the following steps:

1. Browse to the location of the SnapDrive installation package and double-click the executable file to launch the SnapDrive installation wizard.
2. On the Welcome to the SnapDrive installation wizard, click Next.
3. Read and accept the license agreement and click Next.
4. On the SnapDrive License page, select the type of licensing to use.
5. Enter the license key. If host-side licensing is used, enter the license key per server. Click Next.

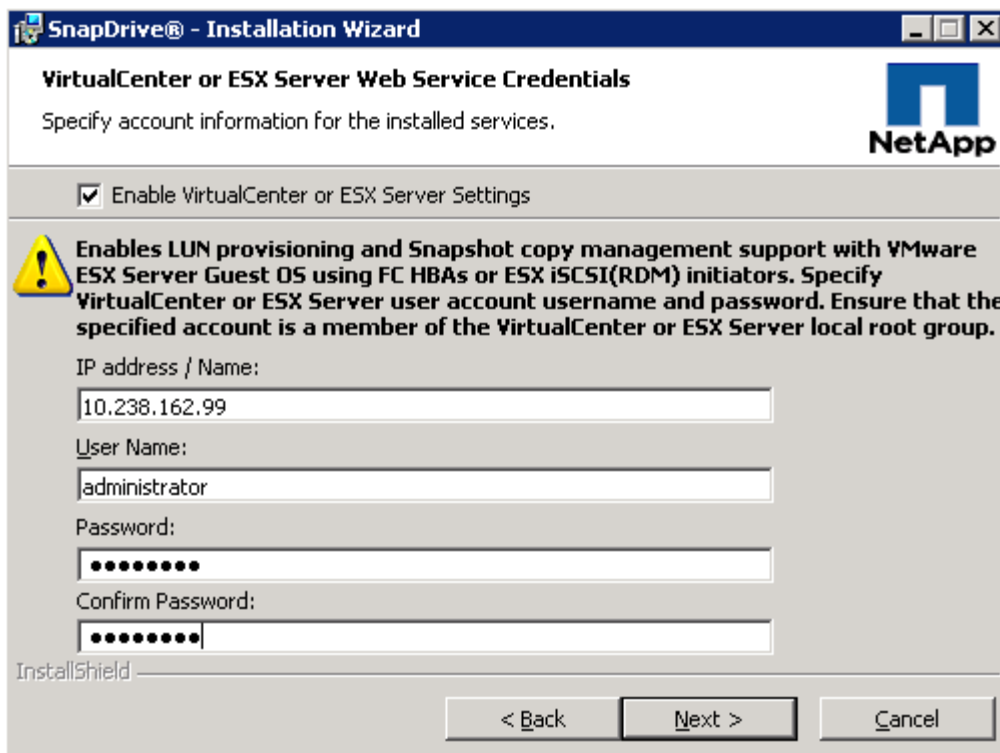
Note: When storage system licensing is selected, SnapDrive can be installed without entering a license key. SnapDrive operations can be performed only on storage systems that have a SnapDrive or SnapManager license installed.

Note: With cluster-based systems, the storage system licensing for SnapDrive is bundled with the other SnapManager product licenses. The bundle is a single license called the SnapManager_suite license.

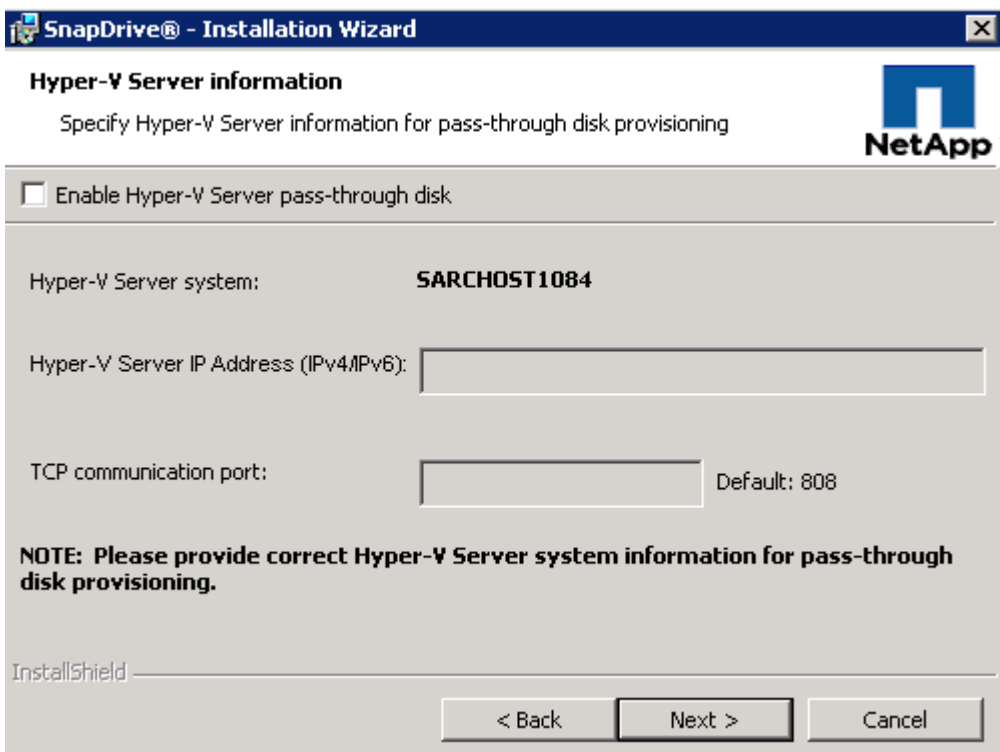
6. On the Customer Information page, enter the user name and organization name. Click Next.
7. On the Destination Folder page, select a host directory in which to install SnapDrive.

Note: By default, this directory is C:\Program Files\NetApp\SnapDrive\.

8. If the VMware ESX[®] guest OS is detected, the Installation Wizard prompts for the IP address and a user name with the appropriate vCenter[™] or ESX server privileges. On the VirtualCenter or ESX Server Web Service Credentials screen, type the IP address of the vCenter or ESX server and the user name and password for SnapDrive to authenticate for web service. To use vMotion[®], be sure to use vCenter. Selecting Enable VirtualCenter or ESX Server Settings enables SnapDrive to use RDM pass-through LUNs. Select this option to use RDM pass-through disks. By default, this option is not selected.



9. If the Hyper-V guest OS is detected, the Installation Wizard prompts for the IP address and a user name with the appropriate Hyper-V server privileges. Type the IP address of the Hyper-V server.



10. On the SnapDrive Service Credentials page, enter the account credentials. Alternatively, click Add to select a specific user account from Active Directory. Click Next.

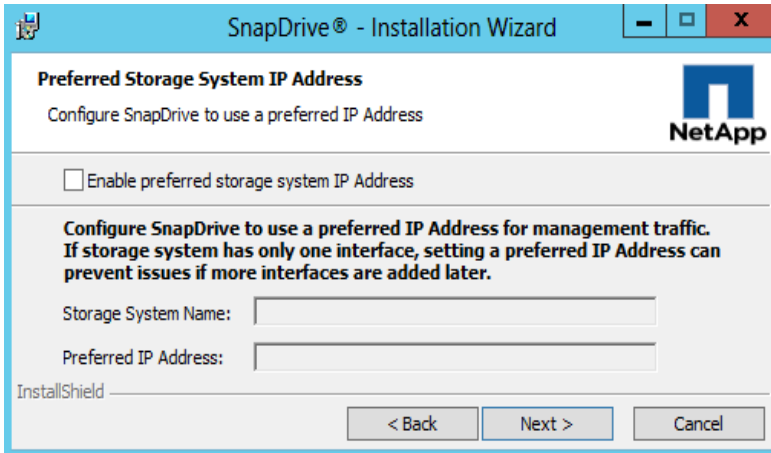
The screenshot shows the 'SnapDrive Service Credentials' page of the SnapDrive Installation Wizard. The window title is 'SnapDrive® - Installation Wizard'. The page header includes the NetApp logo and the text 'Specify account information for the installed services.' A warning icon and text state: 'Ensure that the specified account is a member of the local administrators group of this system. See the SnapDrive for Windows Installation Guide for more details about service account requirements. Please provide the Account information as "Domain Name\User Name" format.' Below this, a note says: 'Note: NetApp VSS hardware provider registration also requires user account information.' There are three input fields: 'Account:' with an 'Add...' button, 'Password:', and 'Confirm Password:'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

Note: The specified account must be a member of the local administrators group on this system.

11. On the SnapDrive Web Service Configuration page, keep the default port settings and click Next.

The screenshot shows the 'SnapDrive Web Service Configuration' page of the SnapDrive Installation Wizard. The window title is 'SnapDrive® - Installation Wizard'. The page header includes the NetApp logo and the text 'Specify SnapDrive Web Service Configuration'. There are three input fields for port numbers: 'SnapDrive Web Service Tcp/Ip Endpoint (Port)' with the value '808', 'SnapDrive Web Service HTTP Endpoint (Port)' with the value '4094', and 'SnapDrive Web Service HTTPS Endpoint (Port)' with the value '4095'. At the bottom, there are buttons for '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

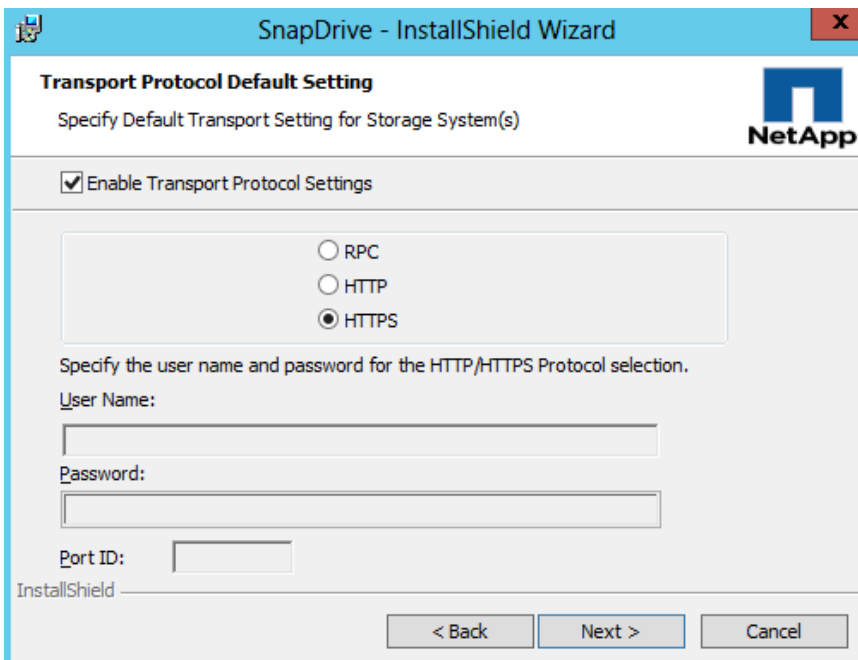
12. On the Preferred Storage System IP Address page, you can specify the IP address you want to use to communicate with the storage system. Then click Next.



13. In the Transport Protocol Default Setting page, select HTTPS and click Next.

Note: NetApp recommends using HTTPS. The HTTPS protocol allows the use of the Data ONTAP interface for all interactions between the storage system and host, including sending passwords securely.

Note: The RPC protocol is not supported for SnapDrive when clustered systems are used.



14. On the OnCommand® configuration page, clear the Enable Protection Manager Integration checkbox and click Next.

Note: Protection Manager can be configured after the SnapDrive installation is complete, if required in the customer environment.

15. On the Server Information page, clear the Configuration Option checkbox and verify that all of the fields are unavailable. Click Next.

Note: VMware integration and pass-through disk setup for Hyper-V can be configured after the SnapDrive installation is complete. Refer to [SnapDrive Documentation](#) for enabling and

disabling the vCenter or ESX logon from SnapDrive MMC if using VMware or to enable the Hyper-V Server pass-through disk if using a Hyper-V configuration.

16. On the Ready to Install page, click Install.
17. When the SnapDrive Installation Completed page is displayed, click Finish.

Set Transport Protocol Settings in SDW

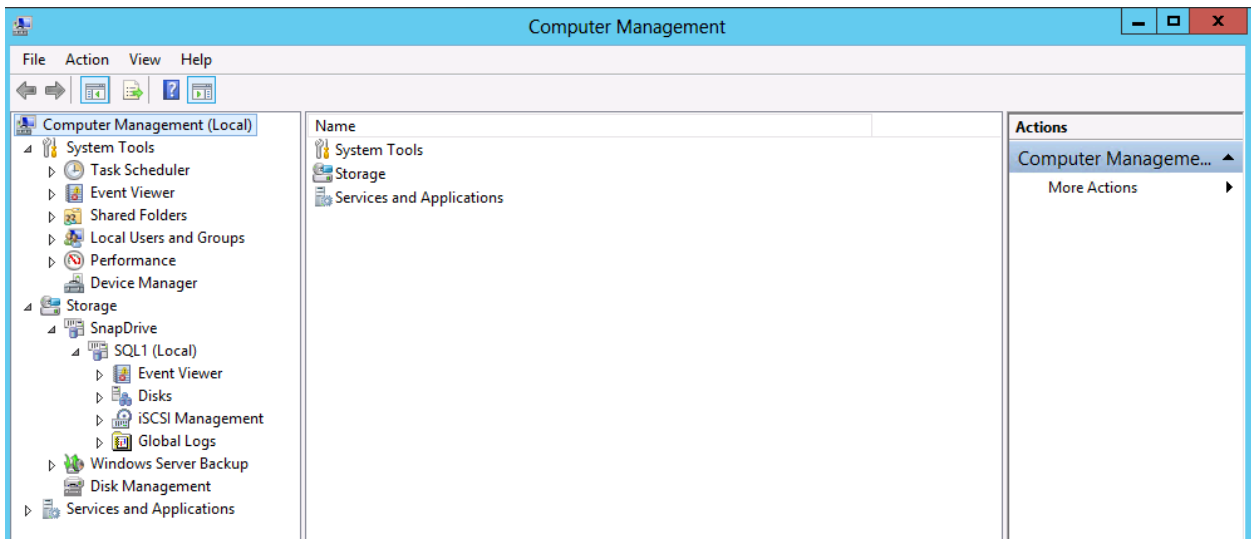
To configure Transport Protocol Settings in SDW, complete the following steps:

1. Log in to the host system and launch SDW.
2. From the SnapDrive console, right-click the host name and select Transport Protocol Settings.
3. From the Storage Systems tab, click Add.
4. In the Add Storage System dialog box, add the IP address of the storage virtual machine (SVM) and click OK.
5. Verify that the SVM has been successfully added to the SnapDrive host.

Accessing and Managing SnapDrive for Windows

SnapDrive for Windows can be managed from the Microsoft Windows Computer Management MMC console.

1. From the Start menu, select Control Panel > Administrative Tools > Computer Management. Or select Start > Run, enter `compmgmt.msc`, and click OK.
2. In the left panel under Storage, select SnapDrive to list the SnapDrive options.



Enable vCenter or ESX Logon from SDW

In the SnapDrive for Windows pane, select the instance of SnapDrive for which you want to enable vCenter or ESX logon. From the menu choices at the top, navigate to Action > vCenter Server or ESX Server Login Settings.

1. The vCenter Server or ESX Server Log On window is displayed.
2. To enable vCenter or ESX logon, in the vCenter Server or ESX Server Log On window, select the Enable vCenter Server or ESX server settings checkbox.
3. Type the IP address or host name, user name, and password for the vCenter or ESX to which you want to log in.

4. Click OK.

Create LUNs in VMware Environments

You can use SnapDrive to create LUNs in VMware environments.

1. Before creating datastores, you must install and configure any adapters that your storage requires.
2. Rescan the adapters to discover newly added storage devices.

Create an RDM LUN on a Guest OS

A Raw Disk Mapping (RDM) can be used to present a LUN directly to a virtual machine from a SAN. You can use SnapDrive to create FC, iSCSI, or ESX iSCSI–accessed RDM LUNs on a guest OS.

To add an RDM to a virtual machine, this VM first needs to be shut down.

1. Log in to the VMware vSphere® Client and select the host from Hosts and Clusters in the Inventory Panel.
2. Right-click that selected host and click Edit Settings.
3. On the Hardware tab, click Add and choose Hard Disk.
4. Select Raw Device Mapping (RDM) on the page for Select a Disk. Click Next.
5. On the Select Target LUN page, choose the appropriate LUN. Click Next.
6. Choose Store with virtual machine or, if you want, store the link to the RDM in a specific datastore. Click Next.
7. On the Compatibility Mode page, select the Physical compatibility mode, which allows the VM to pass SCSI commands directly to the storage system LUN. This allows it to leverage SAN-specific features such as interaction with the SAN's own Snapshot copy functions.
8. For Advanced Options, choose a Virtual Device Node that is on a different SCSI bus from the current virtual disks. The RDM must be located on a separate SCSI controller. Click Next.
9. Confirm the settings and choose Finish on the Ready to complete screen.
10. A new SCSI controller and hard disk are added to the virtual machine configuration.

Note: Upon VM boot, the OS checks for new disk and formats/mounts the disk.

Create VMDK on VMFS Datastore

1. Log in to the VMware vSphere Client and select the host from Hosts and Clusters in the Inventory panel.
2. Click the Configuration tab and click Storage in the Hardware panel.
3. Click Datastores and click Add Storage.
4. Select the Disk/LUN storage type to create a datastore on a Fibre Channel, iSCSI, or local SCSI disk, or mount an existing VMFS volume. Click Next.

Note: Adding a datastore on FC or iSCSI will add this datastore to all hosts that have access to the storage media.

5. Select a device to use for your datastore and click Next.

Note: Select the device that does not have a datastore name displayed in the VMFS Label column. If a name is present, the device contains a copy of an existing VMFS datastore.

6. If the disk you are formatting is blank, the Current Disk Layout page automatically presents the entire disk space for storage configuration. If the disk is not blank, review the current disk layout in the top panel of the Current Disk Layout page and select a configuration option. Use all available partitions from the bottom panel. Click Next.
7. In the Properties page, enter a datastore name and click Next.

8. If needed, adjust the file system and capacity values. By default, the entire free space on the storage device is available. Click Next.
9. In the Ready to Complete page, review the datastore configuration information and click Finish.

Create VMDK on NFS Datastore

1. Log in to the VMware vSphere Client and select the host from Hosts and Clusters in the Inventory panel.
2. Click the Configuration tab and click Storage in the Hardware panel.
3. Click Datastores and click Add Storage.
4. Select the Network File System as the storage type and click Next.

Note: Adding a datastore on FC or iSCSI will add this datastore to all hosts that have access to the storage media.

5. Enter the server name, the mount point folder name, and the datastore name.
6. (Optional) Select Mount NFS read only if the volume is exported as read only by the NFS server. Click Next.
7. In the Network File System Summary page, review the configuration options and click Finish.

Create LUNs for Hyper-V

Before starting to provision LUNs by using SnapDrive, make sure that the FCP or iSCSI service is started on the storage system.

Note: You might need to license FCP or iSCSI protocol based on your requirements. See your NetApp systems engineer or your NetApp software subscription package for license details.

Two types of LUNs can be provisioned to the host by using SnapDrive for Windows:

- Dedicated
- Shared

Dedicated LUNs are dedicated to the server to which they are connected or mapped. Shared LUNs are used with Microsoft Cluster Service (MSCS). SnapDrive for Windows is cluster aware and allows all the cluster nodes to connect to a single LUN when a shared LUN is provisioned.

1. Open the Computer Management Console.
2. Expand SnapDrive and expand the server name.
3. Right-click Disks and select Create Disk.
4. Enter the storage system name or IP address in the Create Disk Wizard. If you have already added the storage system in the storage systems management window, you can select the storage system from the drop-down list.
5. Select the volume where this LUN will be hosted. Enter a LUN name in the LUN Name field and enter a meaningful description for the LUN. Click Next.
6. Select Dedicated in the LUN type panel and click Next.
7. In the Select LUN Properties window, select a drive letter or mount point.
8. Select Limit or Do Not Limit for the option Do you want the maximum disk size to accommodate at least one Snapshot copy. In this case, we selected Do Not Limit to make the best use of thin provisioning. Enter the size of the disk to be created and click Next.
9. In the Select Initiators window, select the initiators. If you need to achieve multipathing, select all the initiators. The selected initiators must be of the same protocol. (A selection cannot have one FC initiator and one iSCSI initiator.) Click Next.
10. In the Select Initiator Group Management window, select Automatic and then click Next.
11. Click Finish to create the SnapDrive-provisioned LUN.

12. From the SnapDrive GUI, you can locate the drive that you just created.

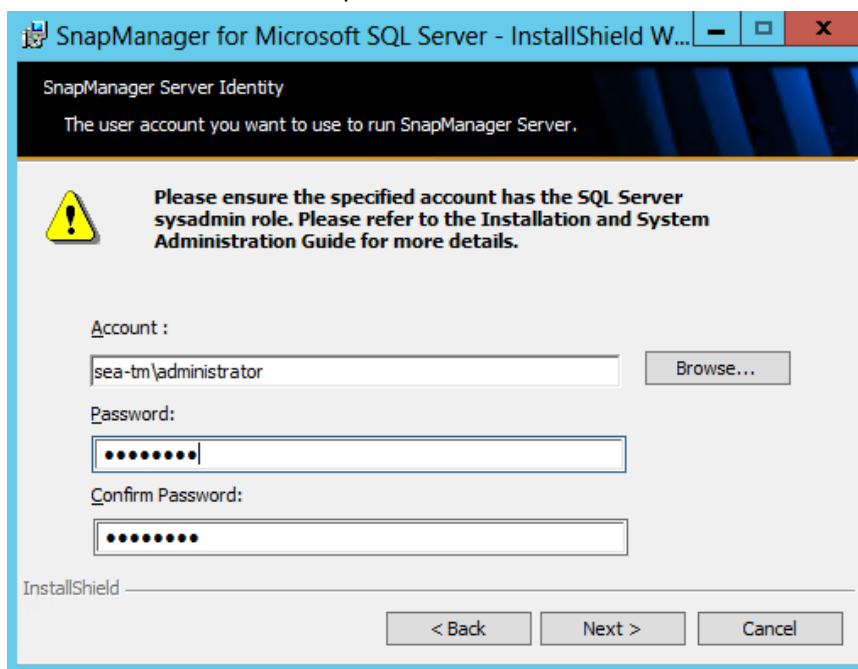
Detailed Steps to Install and Configure SnapManager for SQL Server

To install SMSQL, complete the following steps:

1. Download the SMSQL software installation package from the NetApp Support site [Software Downloads](#) page.
2. From the host, right-click the SMSQL installation package and select Run as Administrator to start the SMSQL installation.
3. On the Welcome page of the SnapManager for Microsoft SQL Server – InstallShield Wizard, click Next.
4. Specify the following customer information and click Next:
 - User name
 - Optional: Information about the organization
 - License type

Note: If a storage-based SMSQL license is used, select the Per Filer license type. If a host-based SMSQL license is used, select the Per Server license type and enter the license key string.

5. Accept the default folder location for the installation or click Change to specify an alternate folder location. Click Next.
6. On the SnapManager Server Identity page, complete the following steps and click Next:
 - a. Enter a user name for the SMSQL service account. To select a different service account, click Browse.
 - b. Enter and confirm a password for the SMSQL service account.



7. Click Install.
8. Click Finish to complete the installation.

Add Server in SnapManager for SQL Server

1. Right-click SnapManager for SQL Server and select Add Servers to Be Managed.

2. Enter SQL1 and press Add.

Install SMSP Manager

To install SMSP Manager, complete the following steps:

1. From the host, right-click the SMSP installation package and select Run as Administrator to start the SMSP installation.
2. On the Welcome page of the Installation wizard, click Next.
3. On the About SnapManager for SharePoint page, click Next.
4. Enter the appropriate customer information and click Next.
5. Read and accept the license agreement. Click Next.
6. Select Yes to install optional SharePoint products. Click Next.
7. Select Yes to install optional DocAve products. Click Next.
8. Read and accept the license agreement. Click Next.
9. Specify the installation location. Click Next.
Note: The default installation location is C:\Program Files\NetApp\SMSP8.
10. Verify that the Control Service and Media Service options are selected. Click Next.
Note: Report Service is an optional DocAve module.
11. After SMSP verifies that all installation prerequisites are met, click Next. To set up the Control Service configuration, enter the following information and click Next:
 - a. Enter the name of the Control Service host.
 - b. Select Create a New IIS Web Site and enter the appropriate information.
 - c. Select Create a New Application Pool and enter the appropriate information.**Note:** NetApp does not recommend using an existing application pool. To use an external application pool, the application pool settings must be configured.
12. To configure the Control Service database settings, enter the following information and click Next:
 - a. Select a database type.
 - b. Enter the database server name.
 - c. Enter the Control Service database name.
 - d. Enter the database credentials.**Note:** Under Advanced Database Settings, you can specify failover policies to be used in conjunction with SQL Server database mirroring.
Note: The built-in database (SQL Server Express) supports only an all-in-one installation on 64-bit operating systems. After the SMSP Manager installation completes, the database type cannot be changed through the Change function in the Windows uninstaller.
13. If a message appears indicating that the database does not exist, click OK to create the database.
14. Enter the Control Service passphrase and click Next.
Note: The passphrase entered on this page is required during the SMSP Agent installation.
15. Review the Media Service configuration default settings. Click Next.
16. Review the Report Service configuration default settings. Click Next.
17. To configure the Report Service database settings, enter the following information and click Next:
 - a. Enter the Report Service database name.
 - b. Enter the database credentials.

- c. When a message appears indicating that the database does not exist, click OK to create the database.
18. To configure the Report Service auditor database settings, enter the following information and click Next:
 - a. Enter the auditor database name.
 - b. Enter the database credentials.
 - c. When a message appears indicating that the database does not exist, click OK to create the database.
19. On the Advanced Configuration page, select Built-in Certificate as the method of SSL certification. Click Next.

Note: The built-in certificate is a certificate generated automatically from the server on which SMSP Manager is installed.

Note: Selecting the User-Defined Certificate option requires a certificate from a valid certificate authority (CA).
20. On the Ready to Install SnapManager for SharePoint Manager page, verify the selections. Click Install.
21. After the SMSP Manager installation completes, click Finish.

Install SMSP Agent on Server

To install SMSP Agent on the server, complete the following steps:

1. Browse to the location of the SnapManager for SharePoint Agent installation package and double-click the executable file to launch the SnapManager for SharePoint Agent installation wizard.
2. On the Welcome page of the Installation wizard, click Next.
3. Enter the appropriate customer information and click Next.
4. Read and accept the license agreement. Click Next.
5. Specify the installation location. Click Next.
6. After SMSP verifies that all of the installation prerequisites are met, click Next.

Note: Click the status of each rule to display detailed information about the scan results.
7. To configure the Communication Configuration page, enter the following information and click Next:
 - a. Enter the SMSP Agent host name.
 - b. Enter the SMSP Agent port number.
 - c. Enter the name of the Control Service host.
 - d. Enter the Control Service port number.
 - e. Select the appropriate SSL certificate.
8. To set up the Agent configuration, enter the following information and click Next:
 - a. Enter the manager passphrase.
 - b. Enter the Agent account credentials.

Note: Specify the user name and password of the Agent account under which the Agent activities are performed.
9. On the Ready to Install SnapManager for SharePoint Agent page, verify the selections. Click Install.
10. After the SMSP Agent installation completes, click Finish.

Appendix B: Build SharePoint 2013 Farm Using SQL Server 2012 AlwaysOn Availability Group Solution for High Availability and Disaster Recovery

This section discusses the steps required to set up a SharePoint 2013 farm with load-balanced web front end (WFE) using SQL Server 2012 availability groups for a local high-availability and remote disaster recovery solution with this design pattern using nonshared storage for each SQL Server instance.

Set Up Windows Network Load Balancing for SharePoint Web Front-End Servers

Following are the prerequisites:

- Each WFE part of the cluster uses a unique dedicated (private) IP address.
- A cluster (public) IP that is a virtual IP, used by all nodes within the network load-balancing (NLB) cluster.
- Private (dedicated) IPs and cluster IP must be on the same subnet mask (network) to function properly.

Configure Network Load Balancing

The NLB feature allows distributing end-user web requests across the WFE servers in the cluster. The section "[Failover Clustering Overview](#)" describes the Failover Clustering feature and provides links to additional guidance about creating, configuring, and managing failover clusters.

Note: Because we are using virtual machines on Hyper-V, select the Enable spoofing of MAC addresses checkbox in the Properties of each virtual machine.

Install the NLB Feature

To install the NLB feature on all of the WFE servers, which will be load balanced in the SharePoint farm, follow the instructions given in [Installing Network Load Balancing](#).

Create an NLB Cluster

To create a new NLB cluster, refer to [Create a New Network Load Balancing Cluster](#).

Note: Verify that NLB failover cluster FQDN URL can be resolved by your domain name server (DNS) for this URL to work from the client's machines.

Add the Second Web Server

To add a second WFE to an existing NLB cluster, refer to [Add a Host to the Network Load Balancing Cluster](#). For additional information, visit <http://support.microsoft.com/kb/896861>.

Set Up Failover Clustering Feature for SQL Server 2012

Windows Server Failover Clustering (WSFC) provides infrastructure features that support the high-availability and disaster recovery scenarios for Microsoft SQL Server used in the SharePoint 2013 farm. Add the Failover Clustering feature to SQL 1 and SQL 2 in the primary data center and SQL 3 located in the secondary data center. For the AlwaysOn availability groups, the availability group and the availability group listener are registered as the WSFC cluster resources.

To install the Failover Clustering feature, refer to [Install the Failover Clustering Feature](#) and [Understanding Requirements for Failover Clusters](#).

Note: Confirm that the Windows Server edition supports the Windows Failover Clustering feature.

Note: All the cluster nodes must be in the same Active Directory Domain Services domain.

Note: The domain user also needs to be a member of the local administrators group, and this domain account should also have administrator permissions on each cluster node and Create Computer Objects and Read All Properties permissions for the container used for the domain computer accounts. For more information, refer to the [Failover Cluster Step-by-Step Guide: Configuring Accounts in Active Directory](#).

Create a New Windows Failover Cluster

Use the procedure listed in [Create a New Failover Cluster](#) to create a new Windows cluster and add nodes SQL 1, SQL 2, and SQL 3 to the new cluster.

Note: Confirm that the Remote Registry and Server services are started on each node to successfully add remote nodes to the Windows cluster.

Set Up Quorum Mode Configuration

WSFC uses a quorum-based approach for monitoring overall cluster health and maximizing node-level fault tolerance. WSFC supports four quorum models. However, only two quorum models (Node Majority and Node and File Share Majority) apply when using a nonshared-storage solution in which there is a total of two nodes in the primary data center. Hence, you can use the Node and File Share Majority quorum model (with one vote assigned to each node in the primary data center and a file share witness where this remote file share is also configured as a voting witness, and connectivity from any node to that share is also counted as an affirmative vote). Hence, more than half of the possible votes must be affirmative for the cluster to be healthy.

The section “To change the quorum configuration in a failover cluster by using failover cluster snap-in” in the [Failover Cluster Step-by-Step Guide: Configuring the Quorum in a Failover Cluster](#) provides the steps to set Node and File Share Majority as the quorum model for this Windows cluster.

Note: For the folder that the file share uses, confirm that the administrator has Full Control share and NTFS permissions. As a best practice, the witness file share should not reside on any node in the cluster and should be visible to all nodes in the cluster.

Note: Also, after the Quorum Configuration Wizard is run, the computer object for the Cluster Name will automatically be granted read and write permissions to the file share.

Set NodeWeight Property

The NodeWeight property of the WSFC node represents the vote for that particular node. Adjust each node’s NodeWeight setting (a value of 0 or 1) so that the node’s vote is not counted toward the quorum.

Following is the voting scheme, and it means that only the two nodes in the primary data center and the file share witness will then have votes:

- One vote to each node (SQL 1 and SQL 2) in the primary data center.
- Zero votes to node SQL 3 in the disaster recovery data center because you do not want node SQL 3 from the secondary site to contribute to a decision to take the cluster offline when no glitch has occurred at the primary site.

To configure the NodeWeight from a node in a WSFC using Windows PowerShell, on SQL 3, click Start > Administrative Tools > Windows PowerShell Modules.

To set node SQL 3’s vote to 0, enter the following.

```
(Get-ClusterNode "SQL 3").NodeWeight=0
```

Note: Confirm that the other servers, SQL 1 and SQL 2, have the NodeWeight set as 1.

For more information on adjusting node votes, refer to the [Configure Cluster Quorum NodeWeight Settings](#).

Recommendations for quorum voting for AlwaysOn high-availability and disaster recovery solutions are provided in the [Recommended Adjustments to Quorum Voting](#) in the [WSFC Quorum Modes and Voting Configuration](#).

Install a Standalone Instance of SQL Server 2012 on Each Cluster Node

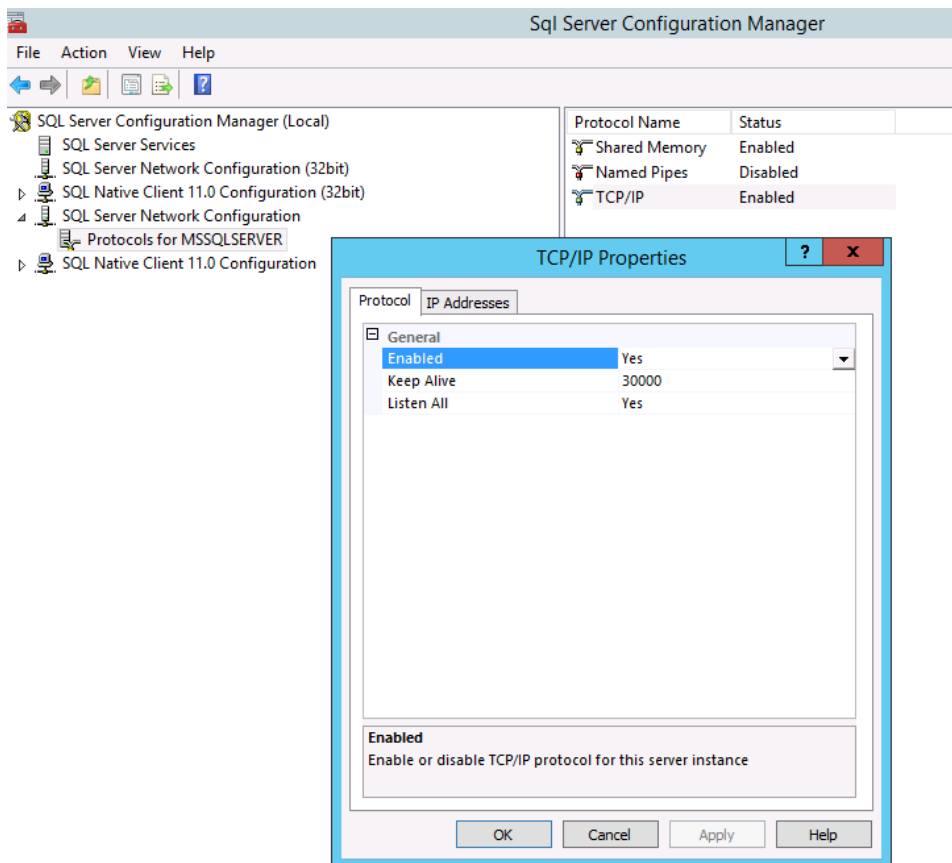
Prior to installing SQL Server 2012, confirm that the necessary prerequisites have been met on each cluster node. For more information, refer to “[Prerequisites, Restrictions, and Recommendations for AlwaysOn Availability Groups \(SQL Server\)](#).” Then install SQL Server 2012 Enterprise edition to leverage the AlwaysOn availability group feature with the standalone instance. For more information, refer to [Installation for SQL Server 2012](#). The SMSP Storage Manager module also requires SQL Server Enterprise edition because it relies on the RBS provider to process RBS BLOB, and the RBS provider requires the SQL Server enterprise version to enable RBS.

Note: In the database engine configuration step of the installation, NetApp recommends using identical file paths on each node.

Note: Also, confirm that all of the SQL Server instances use the same SQL Server collation in order to host the availability group replicas.

By default, SQL Server does not accept remote connections. To change this default setting, click Start > Programs > Microsoft SQL Server 2012 > Configuration Tools > SQL Server Configuration Manager. Expand SQL Server Network Configuration, click Protocols for MSSQLSERVER, and double-click the TCP/IP entry. Change the Enabled option to Yes and click OK.

Figure 4) Enable TCP/IP protocol for MSSQLSERVER.



Install and Configure SharePoint 2013

Refer to [Hardware and software requirements for SharePoint 2013](#) before you [Install and configure SharePoint 2013](#) on respective servers of the SharePoint farm. Also, [Deployment Guide for SharePoint 2013](#) provides deployment instructions for SharePoint 2013.

Note: This web-balanced FQDN <http://netapp.com> needs to be configured for Alternate Access Mapping in SharePoint Central Administration page > Application Management > Web Applications > Configure alternate access mappings.

Note: Select the web application that you want the network load balancing to configure.

Note: Click the Add internal URL and type <http://netapp.com>.

Install SnapDrive for Windows

SnapDrive for Windows (SDW) needs to be installed on each node of the WSFC cluster and SharePoint index server to be able to perform a backup of the SharePoint search index.

For more information, refer to the “[Detailed Steps to Install SnapDrive for Windows.](#)”

Install SnapManager for SQL Server

SnapManager for SQL Server (SMSQL) needs to be installed on each node of the SQL Server 2012 WSFC cluster.

For more information, refer to the “[Detailed Steps to Install SnapManager for SQL Server.](#)”

Install SnapManager 8.0 for SharePoint on Server in SharePoint Farm

SnapManager for SharePoint (SMSP) needs to be installed on each server in the SharePoint farm.

For more information, refer to the “[Detailed Steps to Install SnapManager for SharePoint.](#)”

The same SMSP Manager is used to manage the primary and disaster recovery data centers in this lab scenario.

Note: If you choose to leverage the SMSP Storage Optimization modules such as Storage Manager and Connector to externalize Binary Large Objects (BLOB) onto a CIFS share in NetApp storage system, you have to use the Remote BLOB Storage (RBS) Provider binaries installed during SMSP Agent installation. You do not need to separately install the RBS component from the feature pack for SQL Server 2012/2008 R2, unless you choose to use the supplied SQL Server FILESTREAM provider.

Note: These SMSP Add-on modules for Storage Manager, Archive Manager, and Connector are licensed per web front end (WFE) and Application server in the SharePoint farm.

SMSP Migration Procedures

SMSP Migrate Database

When you create a SharePoint 2013 web application, the corresponding content databases get created in the default SQL Server database location, and this needs to be migrated to NetApp storage. Use the SMSP Migrate Database tool to migrate SharePoint databases to Data ONTAP storage systems (LUNs).

For more details, refer to the section “Migrate Database” in the [SnapManager for Microsoft SharePoint Platform Backup and Restore User's Guide](#).

Note: SharePoint services on all of the servers in the farm will automatically be stopped during the migration process. Services are restarted after completion of the migration. For servers in the farm that do not have SnapManager for SharePoint Agents installed, you must stop the services before you click Start and then restart the services manually after the migration job has finished.

SMSP Migrate Index

Similarly, leverage the SMSP Migrate Index tool to migrate the SharePoint Foundation Help Search index and Search Service Application index to a LUN.

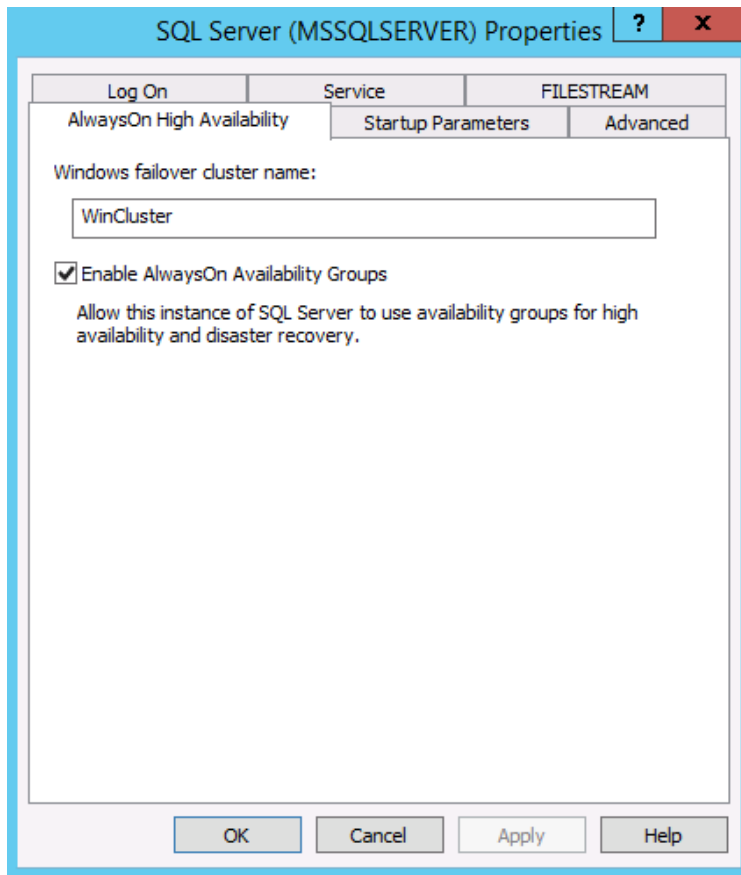
For more details, refer to the Migrate Index of [SnapManager for Microsoft SharePoint Platform Backup and Restore User's Guide](#).

Enable AlwaysOn Availability Group Feature

To enable the AlwaysOn availability groups feature on each node, refer to the [Enable and Disable AlwaysOn Availability Groups](#).

Note: Verify that the Windows failover cluster name field contains the name of the local failover cluster. If this field is blank, this server instance currently does not support AlwaysOn availability groups. Either the local computer is not a cluster node, the WSFC cluster has been shut down, or this edition of SQL Server 2012 does not support AlwaysOn availability groups.

Figure 5) Enable AlwaysOn availability group feature.



Create Initial Database Backup Using SMSQL

In order to create an availability group, the database must be in full recovery mode, and at least one full backup must have been performed, for which we use SnapManager for SQL Server (SMSQL). SMSQL uses NetApp Snapshot technology to deliver near-instantaneous and space-efficient backups. After SMSQL has been installed, it needs to be configured to perform a full database and log backup. For details on how to perform a full database backup, refer to Create SQL Server Database Backup in

Appendix: Installation and Configuration Details of [TR-4302: Microsoft SQL Server and SnapManager for SQL Server Deployment Guide](#).

Create SQL Server 2012 Availability Group

Log in to the server SQL 1 that will host the primary replica and follow the procedure listed in the article [Use the Availability Group Wizard \(SQL Server Management Studio\)](#) to create a SQL Server 2012 availability group with databases added only in the primary instance SQL 1.

Then you can leverage NetApp SnapManager for SQL Server (SMSQL) to restore databases to secondary replica servers as follows:

Leverage NetApp Technology to Servers in the Same Primary Data Center

Typically, the backup and restore process for large databases during the creation of SQL Server 2012 availability groups can take a long time, and the backup file takes up a large amount of disk space. SMSQL can provide faster backup and restore for these databases (in norecovery mode) by using NetApp Snapshot and FlexClone technologies onto the secondary replica SQL 2. For additional information, refer to the section “Back Up and Restore Database to Replica Instance in Same Data Center” in [TR-4106: Accelerate SQL Server 2012 AlwaysOn Availability Groups Deployment on NetApp Storage](#).

Leverage NetApp Technology to Server in Disaster Recovery Data Center

Network bandwidth limitations make it more challenging to back up and restore databases between the SQL Server instances in separate data centers. SMSQL and NetApp SnapMirror® make this task faster and simpler to secondary replica SQL 3. For procedures that need to be performed on SQL 3, refer to the section “Back Up and Restore Database to Replica Instance in Different Data Centers” in [TR-4106: Accelerate SQL Server 2012 AlwaysOn Availability Groups Deployment on NetApp Storage](#).

Note: SnapMirror relationship of the database volumes (database, log, and SnapInfo volumes) must be created.

Note: When SMSP runs backup of a SharePoint farm that uses SQL Server AlwaysOn availability groups, it detects the backup preferred replica first, then SMSP passes the parameter to the new backup and uses the preferred replica copy for backup purposes. If the preferred replica is not found, then the primary replica will be used. In case the SQL Server instance containing this replica fails, NetApp recommends using SnapManager for SQL Server (SMSQL) to back up the SQL Server availability group because it backs up all the replicas.

Table 16 lists the configured replica settings.

Table 16) Settings for SQL Server 2012 AlwaysOn replica.

Data Center	Replica	Role	Availability Mode	Failover Mode
Primary data center	SQL 1	Primary	Synchronous commit	Automatic
Primary data center	SQL 2	Secondary	Synchronous commit	Automatic
Disaster recovery data center	SQL 3	Secondary	Asynchronous commit	Forced Manual

Table 17 lists all of the SharePoint 2013 databases that can participate in SQL Server 2012 AlwaysOn availability groups. For additional information, refer to [Supported high availability and disaster recovery options for SharePoint databases \(SharePoint 2013\)](#).

Table 17) SharePoint 2013 databases supported for SQL Server 2012 AlwaysOn availability group.

Database	Description	SQL Server AlwaysOn Availability Group with Synchronous-Commit for Availability	SQL Server AlwaysOn Availability Group with Asynchronous-Commit for Disaster Recovery
SharePoint_Config	Contains data about the following: <ul style="list-style-type: none"> • SharePoint databases • Internet Information Services (IIS) websites • Web applications • Trusted solutions • Web Part packages • Site templates • Default quota settings • Blocked file types 	Yes	No. This is a farm-specific database.
SharePoint_Admin_Content	Stores all configuration data for the Central Administration site collection.	Yes	No. This is a farm-specific database.
WSS_Content	Stores all of the content for a site collection, document libraries and lists, Web Part properties, audit logs, and apps for SharePoint data if the apps are installed, in addition to user names and rights and user data for SharePoint Power Pivot.	Yes	Yes
AppManagement	Stores app licenses and permissions that are downloaded from the SharePoint Store or App Catalog.	Yes	Yes
Secure Store	Stores and maps credentials, such as account names and passwords.	Yes	Yes
Subscription Settings	Stores features and settings for hosted customers.	Yes	Yes
Word Automation	Stores information about pending and completed document conversions.	Yes	Yes
Managed Metadata	Stores managed metadata and syndicated content types.	Yes	Yes

Database		Description	SQL Server AlwaysOn Availability Group with Synchronous-Commit for Availability	SQL Server AlwaysOn Availability Group with Asynchronous-Commit for Disaster Recovery
Translation Services		Stores information about pending and completed batch document translations with enabled file name extensions.	Yes	Yes
Business Data Connectivity		Stores external content types and related objects.	Yes	Yes
Project Server		Each Project Web App database contains the following data: <ul style="list-style-type: none"> All Project and Portfolio Management (PPM) data Time tracking and Timesheet data Aggregated SharePoint project site data 	Yes	Yes
PerformancePoint Services		Stores temporary objects and saved user comments and settings.	Yes	Yes
Search	Search Administration	Stores the Search application configuration and system access control list (SACL) for the crawl component.	Yes	No. Taking a copy of the Search Administration database and using it to recreate the Search service application is supported.
	Analytics Reporting	Stores the results for usage analysis reports and extracts information from the Link database when it is needed.	Yes	No
	Crawl	Stores the state of the crawled data and the crawl history.	Yes	No
	Link	Stores the information that is extracted by the content processing component and click through information.	Yes	No
User Profile	Profile	Stores and manages users and associated information. It also stores information about user's social network	Yes	Yes

Database		Description	SQL Server AlwaysOn Availability Group with Synchronous-Commit for Availability	SQL Server AlwaysOn Availability Group with Asynchronous-Commit for Disaster Recovery
		in addition to memberships in distribution lists and sites.		
	Synchronization	Stores configuration and staging data for use when profile data is being synchronized with directory services, such as Active Directory.	Yes	No
	Social Tagging	Stores social tags and notes created by users, alongside their respective URLs.	Yes	Yes
Usage and Health Data Collection		Stores health monitoring and usage data temporarily and can be used for reporting and diagnostics.	Yes, but not recommended	No. This database is farm-specific. However, you can copy it to a disaster recovery environment for data mining.
Power Pivot Service		Stores data refresh schedules and Power Pivot usage data that is copied from the central usage data collection database.	NA because it is not tested.	NA because it is not tested.
State Service		Stores temporary state information for InfoPath Forms Services, Exchange Server, the chart Web Part, and Visio Services.	Yes	No

Create Availability Group Listener

In order to have fast application failover access to SQL Server, an availability group listener must be created on the current primary node. Refer to [Create or Configure an Availability Group Listener \(SQL Server\)](#).

Create SharePoint Farm Backup Using SMSP

A successful SharePoint farm backup needs to be taken using the SnapManager for SharePoint (SMSP) Data Protection feature, which in turn leverages SMSQL, which uses NetApp Snapshot technology.

For details on how to perform a SharePoint farm backup, refer to the section “Perform SharePoint Farm Backup” of [TR-4297: Microsoft SharePoint Server and SnapManager for SharePoint Deployment Guide](#).

Note: You can alternatively choose to restore from SMSQL backups of SharePoint databases onto backed-up VMs (with SQL Server content mapped). However, when compared with the SMSP, these backups will not provide the required granular recovery features.

Basic Tests to Validate the Solution

This section outlines the test procedures for the basic tests that should be performed to validate the deployment.

Windows User Logon

Task

To test whether users are able to log on to the Windows domain:

- Create a Windows user and log on to the Windows domain using the created account.

SMSP Manager Login

Task

To log in to SMSP, complete the following steps:

1. Run SnapManager for SharePoint Manager by double-clicking the SnapManager for SharePoint shortcut on Appmed1.
2. Microsoft Internet Explorer will start, and you will be presented with a security certificate warning. Click Continue to This Website (Not Recommended) to proceed.

Note: This warning is due to the fact that a custom security certificate has not been installed. NetApp recommends that customers install their own certificates when implementing SMSP.

3. In the SMSP Login window, enter the login ID and password and then click Login.

Storage System Profile

Task

To create a new storage system profile, complete the following steps:

1. Start SnapManager for SharePoint Manager and select Control Panel > Storage Configuration > Storage System Profile.
2. Click Create a New Storage System Profile.
3. Configure the following settings for the storage system profile:
 - a. Enter a name and a description for the profile.
 - b. Enter the IP address of the storage controller in the Storage System Address field.
 - c. Select a connection type from the Connection Type list.
 - d. Enter the user name, password, and port used to access the storage system.
 - e. Select the appropriate connection mode. If the system is running Data ONTAP 8.2, select the Cluster-Mode option.
 - f. Enter the preferred IP address to access the CIFS share.
 - g. Click Test to verify the connection type, account information, and mode.
 - h. If the test is successful, click OK to save the configuration and return to the Storage Configuration page.
4. Verify that the new storage system profile is listed in the Storage System

Storage System Profile

Profile tab.

Note: After the storage system profile has been created, the CIFS share devices can be set up.

Create Physical Device for LUNs

Task

To create a new physical device for LUNs, complete the following steps:

1. Start SnapManager for SharePoint Manager and select Control Panel > Storage Configuration > Physical Device.
2. Click Create a New Physical Device.
3. Configure the following settings for the physical device:
 - a. Enter a name and a description for the device.
 - b. Select Data ONTAP as the storage type.
 - c. Select LUN from the Data ONTAP list.
 - d. Select a previously configured media device from the Media Service list.
 - e. Select the appropriate LUN from the LUN list.
 - f. Select the farms that can use the storage device or keep the default value in the Farm list.
 - g. Select a space threshold for the storage type or keep the default value.
 - h. To test the connection to the selected LUN, click Validation Test.
 - i. To verify that enough free space is available, click Test.
 - j. If both tests are successful, click OK to save the configuration and return to the Storage Configuration page.
4. Verify that the physical device is listed in the Physical Device tab.

Create Physical Device for CIFS

Task

To create a new physical device for a CIFS share, complete the following steps:

1. Start SnapManager for SharePoint Manager and select Control Panel > Storage Configuration > Physical Device.
2. Click Create a New Physical Device.
3. Configure the following settings for the physical device:
 - a. Enter a name and a description for the device.
 - b. Select Data ONTAP as the storage type.
 - c. Select CIFS Share from the Data ONTAP list.
 - d. Select the storage system profile from the list.
 - e. Select CIFS from the Share Name list.
 - f. Select the farms that can use the physical device or keep the default value.
 - g. Select a space threshold for the storage type or keep the default value.

Create Physical Device for CIFS

- h. To verify the login credentials, click Validation Test.
 - i. To verify that enough free space is available, click Test.
 - j. If both tests are successful, click OK to save the configuration and return to the Storage Configuration page.
4. Verify that the physical device is listed in the Physical Device tab.

Create Logical Device for LUN

Task

To create a new logical device for a LUN, complete the following steps:

1. Start SnapManager for SharePoint Manager and select Control Panel > Storage Configuration > Logical Device.
2. Click Create a New Logical Device.
3. Configure the following settings for the logical device:
 - a. Enter a name and a description for the device.
 - b. Select Data ONTAP as the storage type.
 - c. Select Logical Device as the data storage type.
 - d. Select LUN as the Data ONTAP device type.
 - e. From the Physical Device list, select a physical device to be added to the logical device and click Add.
 - f. Click OK to save the configuration and return to the Storage Configuration page.
4. Verify that the device is listed in the Logical Device tab.

Create Logical Device for CIFS

Task

To create a new logical device for CIFS, complete the following steps:

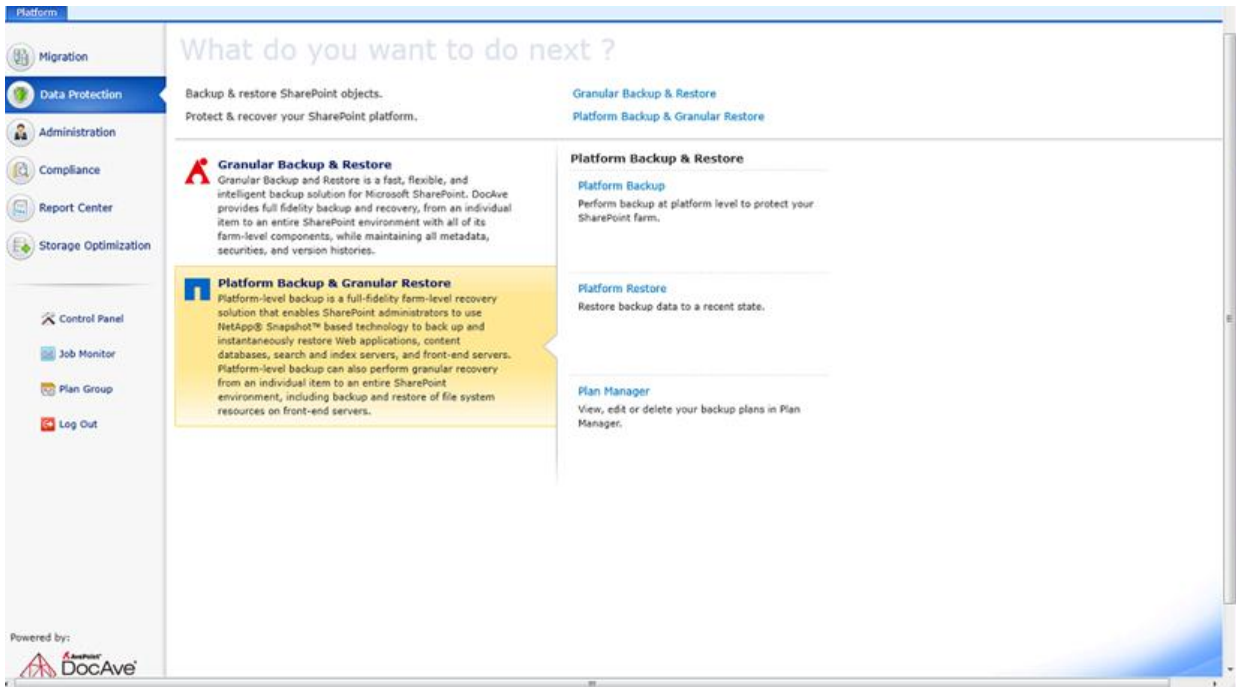
1. Start SnapManager for SharePoint Manager and select Control Panel > Storage Configuration > Logical Device.
2. Click Create a New Logical Device.
3. Configure the following settings for the logical device:
 - a. Enter a name and a description for the device.
 - b. Select BLOB Storage Device as the data storage type.
 - c. Select Data ONTAP as the storage type.
 - d. Select CIFS Share as the Data ONTAP device type.
 - e. Select a physical device and click Add.
 - f. Select the Create Storage Path for Contents Using the Following Structure checkbox and select the relevant format for the storage path from the drop-down list.
 - g. Click OK to save the configuration and return to the Storage Configuration page.

Create Logical Device for CIFS	
	4. Verify that the device is listed in the Logical Device tab.
Task	<p>To create a new storage policy, complete the following steps:</p> <ol style="list-style-type: none"> 1. Start SnapManager for SharePoint Manager and select Control Panel > Storage Configuration > Storage Policy. 2. Click Create a New Storage Policy. 3. Configure the following settings for the storage policy: <ol style="list-style-type: none"> a. Enter a name and a description for the policy. b. From the Logical Device list, select the primary logical device for the storage policy. c. Select a Media Service to add to the storage policy and click Add. d. To verify the successful connection to the logical device, click Test. e. Select Enable Retention Rule, if appropriate. f. Select Backup Type for Storage Policy Type. g. Select None for Notification. h. Select appropriate details for Backup Retention Rule. i. Click OK to save the configuration and return to the Storage Configuration page. 4. Verify that the storage policy is listed in the Storage Policy tab.

Appendix C: Solution Operation Details

Backup and Restore

Following are the actions performed using the SnapManager for SharePoint Manager > Data Protection.



1. Perform SharePoint Farm backup.
2. Perform in-place item-level restore.

Perform SharePoint Farm Backup

To perform a SharePoint farm backup by using SnapManager for SharePoint (SMSP) Data Protection, complete the following steps:

1. Start SnapManager for SharePoint Manager by selecting Start > All Programs > SnapManager for SharePoint.
2. Click Platform > Data Protection > Platform Backup & Restore.
3. In the Scope pane on the left, select the components to back up from the SharePoint tree.
4. Click Plan Builder and select Wizard Mode.
5. Enter a plan name and a description and select either Create a New Plan or Copy Saved Plan Settings from Template. Click Next.
6. On the Storage Policy page, select a storage policy for the backup. Click Next.

Note: If a storage policy has not previously been selected, create a new storage policy by clicking New Storage Policy and enter the following details: name, logical device, and media service.
7. On the Advanced page, select an associated plan group and a notification profile for the backup plan. Click Next.

Note: The associated plan group provides an interface for collecting and grouping plans according to the setup parameters. The plans run simultaneously or in sequence. The selected notification profile should already be configured with report settings and report recipients.
8. On the Schedule page, select Configure the Schedule Myself and click Add Schedule.
9. Click the Options tab and do the following:
 - a. Select Item Level from the Restore Granularity Level list.
 - b. Keep the default selections for the remaining fields or update as necessary.

- c. Select Backup Storage Manager BLOB.
- d. Select Backup Connector BLOB.
10. Click the Time tab and then specify a schedule for running the job. Click OK.
11. On the Schedule page, click Next.
12. On the Maintenance page, select the appropriate maintenance options based on your organization's backup policies. Click Next.
13. On the Overview page, verify the selections and select Finish and Run Now.
14. Verify that the backup plan is listed in the Plan Manager.

Note: If SharePoint databases share a LUN with SQL Server system databases, only stream-based backup and restore can be used. However, SMSP does not support this configuration. SharePoint databases should be placed on separate LUNs from the SQL Server system database.

Perform In-Place Item-Level Restore

To perform an item-level restore of a document deleted from the SharePoint site, complete the following steps:

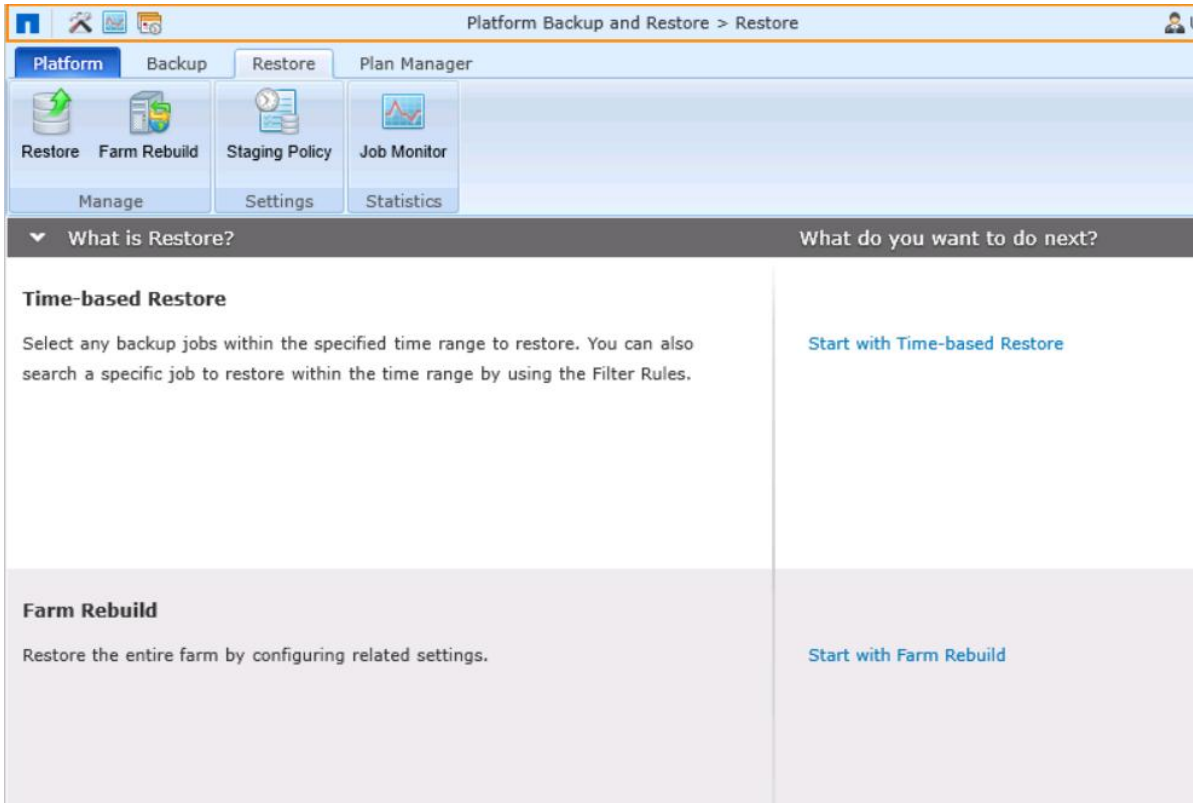
1. Start SMSP Manager.
2. Click Platform > Data Protection > Platform Backup & Granular Restore > Platform Restore.

The screenshot shows the NetApp SMSP Manager interface. The breadcrumb path is 'Platform Backup and Restore > Restore > Time-based Restore'. The ribbon includes 'Platform', 'Backup', 'Restore', 'Time-based Restore', and 'Plan Manager'. The left navigation pane shows 'Data Protection' selected. The main content area has a heading 'What do you want to do next?' and two main sections: 'Granular Backup & Restore' and 'Platform Backup & Restore'. The 'Platform Backup & Restore' section is highlighted in yellow and contains the following text:

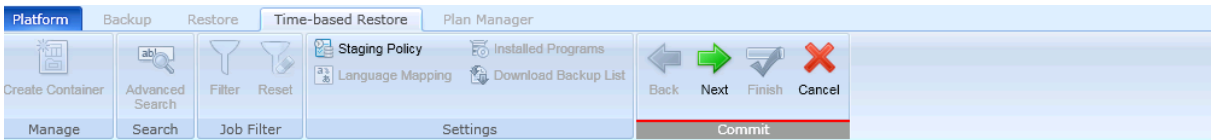
Platform Backup & Granular Restore
 Platform-level backup is a full-fidelity farm-level recovery solution that enables SharePoint administrators to use NetApp® Snapshot™ based technology to back up and instantaneously restore Web applications, content databases, search and index servers, and front-end servers. Platform-level backup can also perform granular recovery from an individual item to an entire SharePoint environment, including backup and restore of file system resources on front-end servers.

On the right side of the interface, there are links for 'Granular Backup & Restore', 'Platform Backup & Granular R', 'Platform Backup', 'Platform Restore', and 'Plan Manager'.

3. Click Restore in the ribbon.

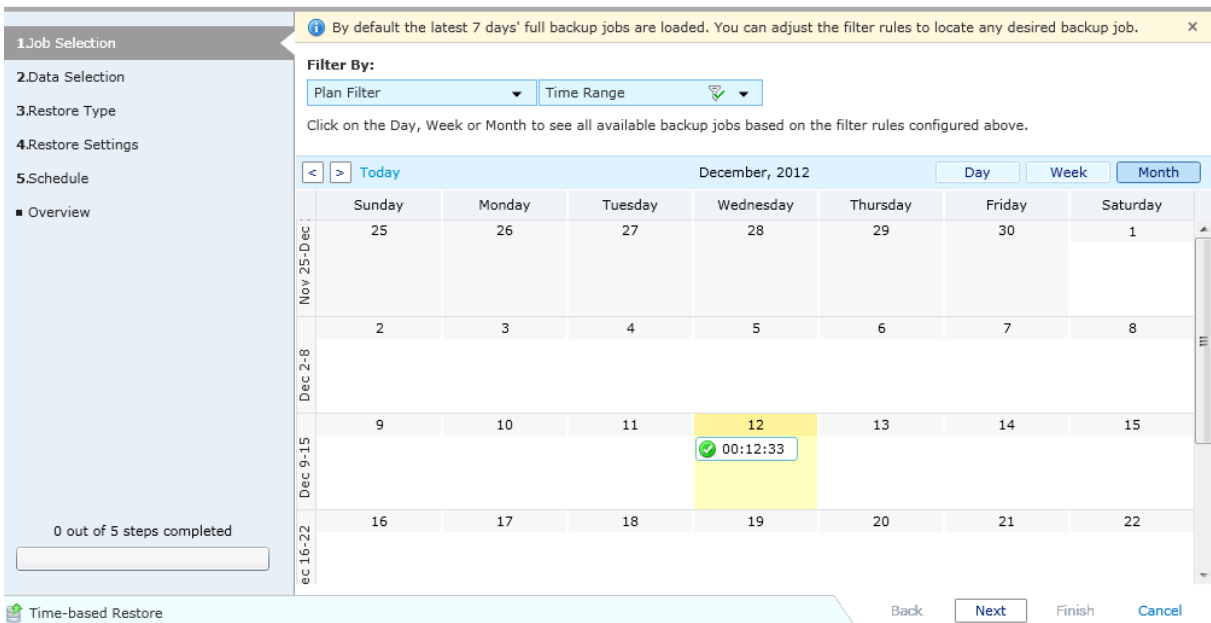


4. On the Job Selection page, select the backup job to restore. Click Next.

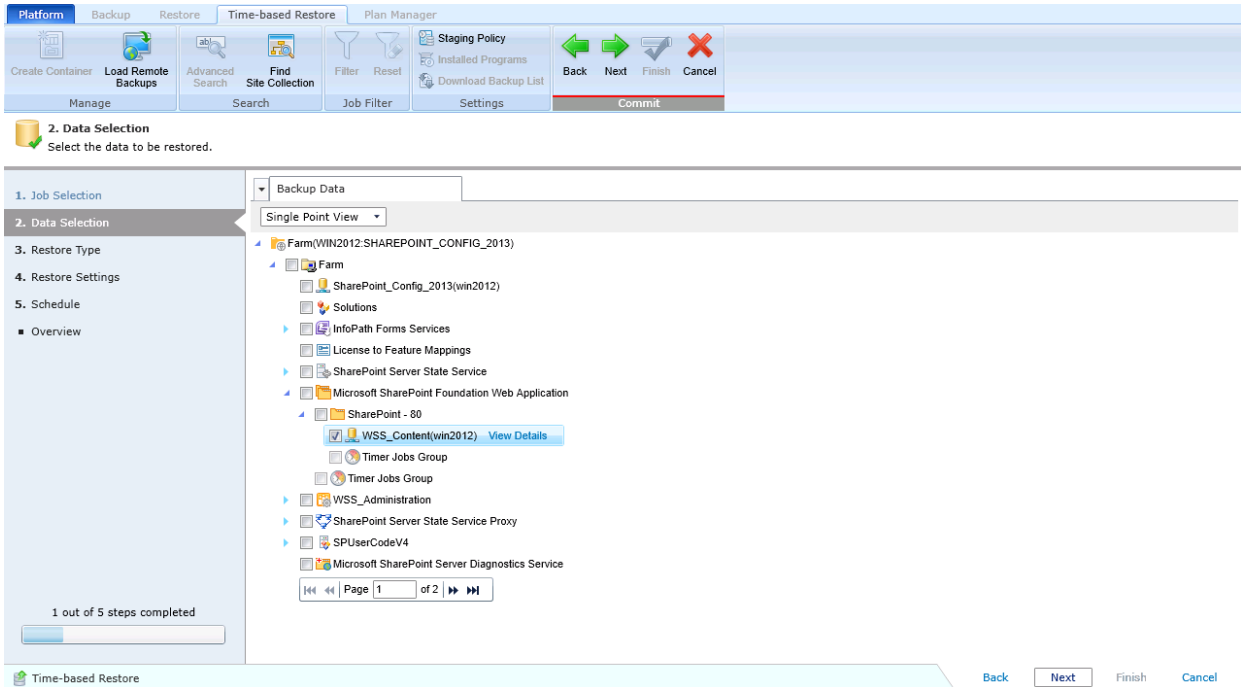


1. Job Selection

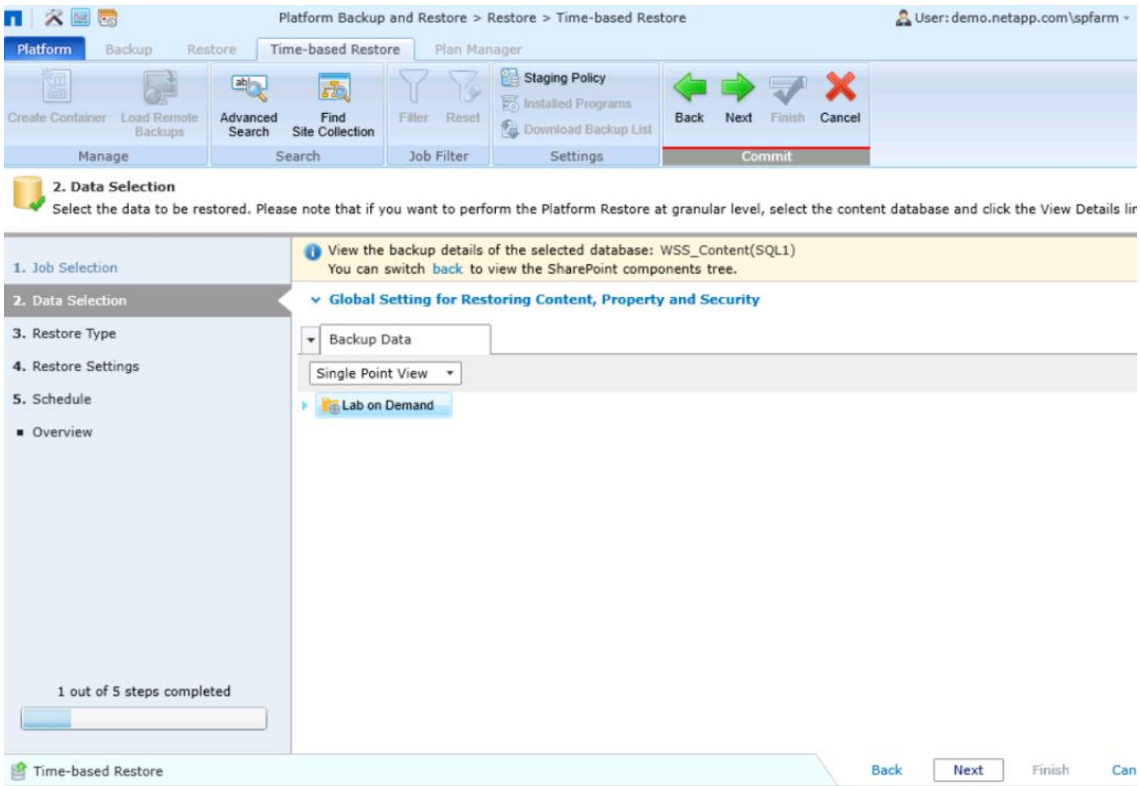
The latest 7 days' full backup jobs are loaded. You can adjust the filter rules below to search any desired job and select one job to proceed to the next step.



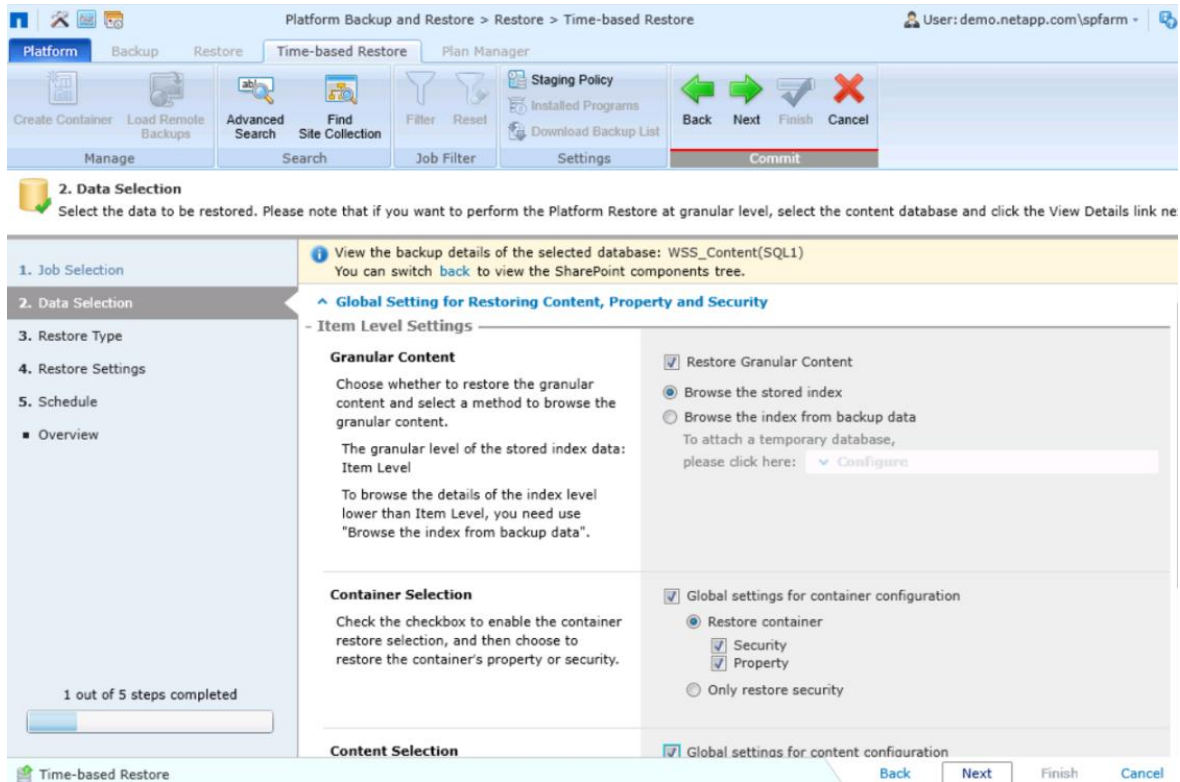
- Expand the farm and select the content to be restored. Click View Details to view detailed information about the selected database.



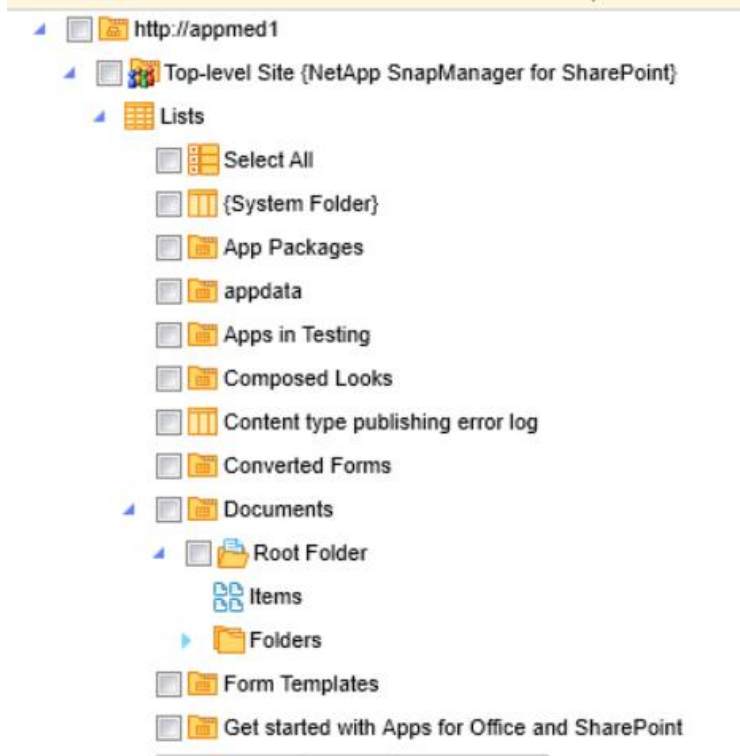
- Click Global Setting for Restoring Content, Property, and Security to configure the item-level settings for the restore.



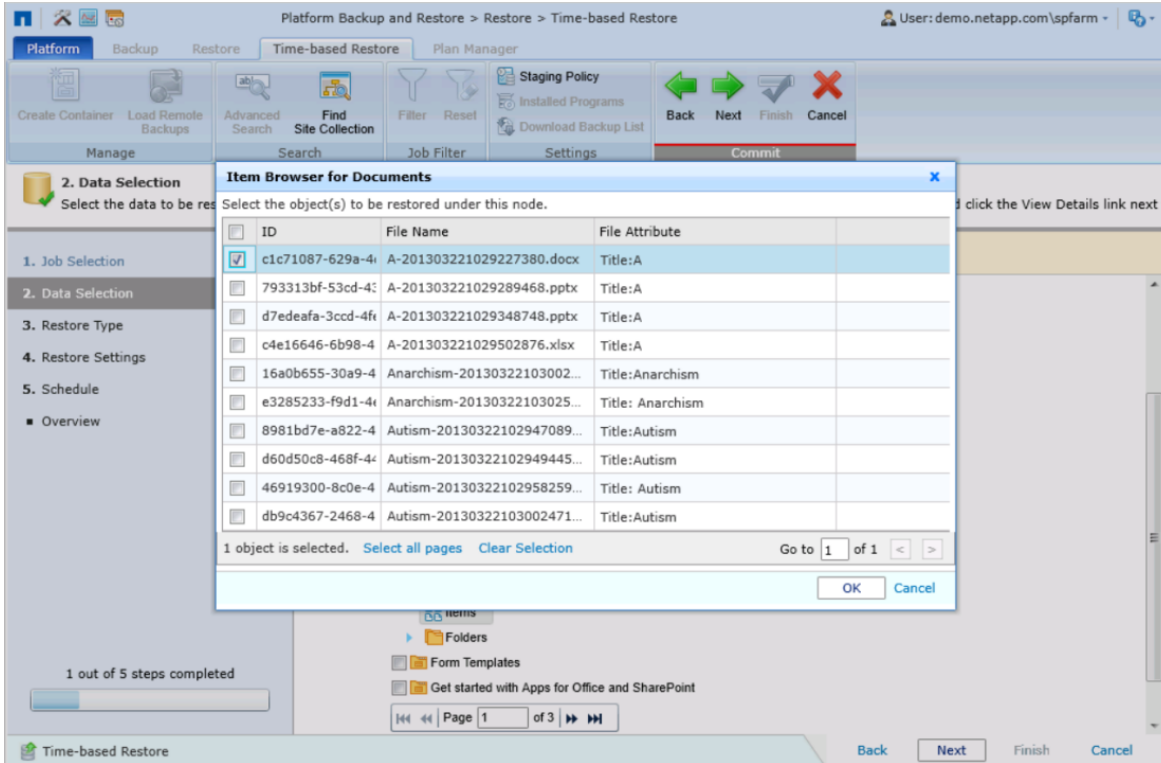
7. Select the Restore Granular Content checkbox and the following relevant settings.



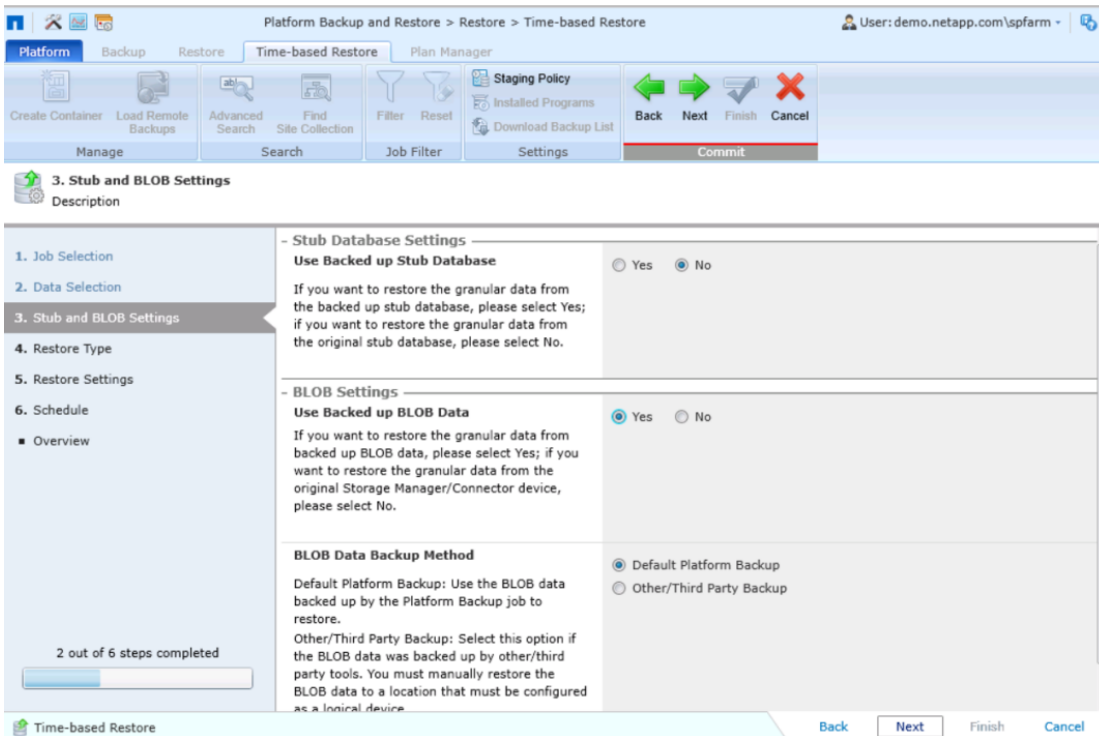
8. Expand the farm tree in the Backup Data pane and locate the content to be restored.



- Select Items to open the Item Browser for Documents, which allows you to select individual items to restore.



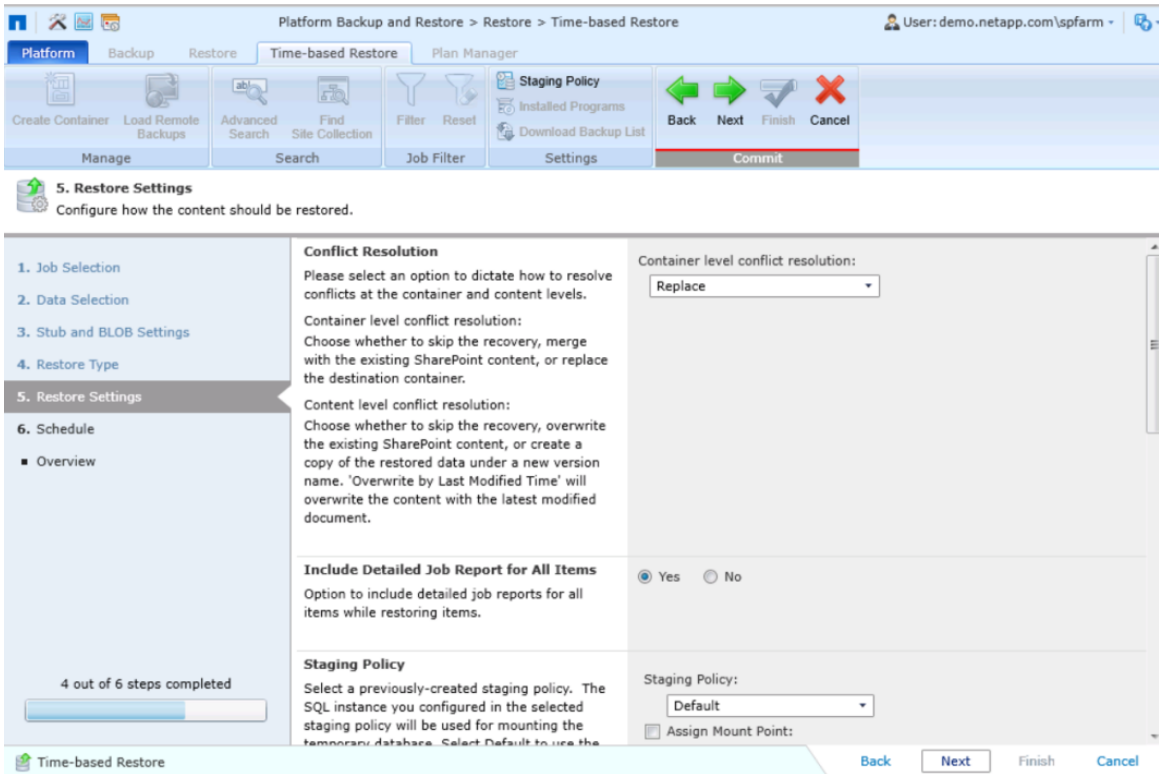
- Select Yes to Use backed up BLOB data.



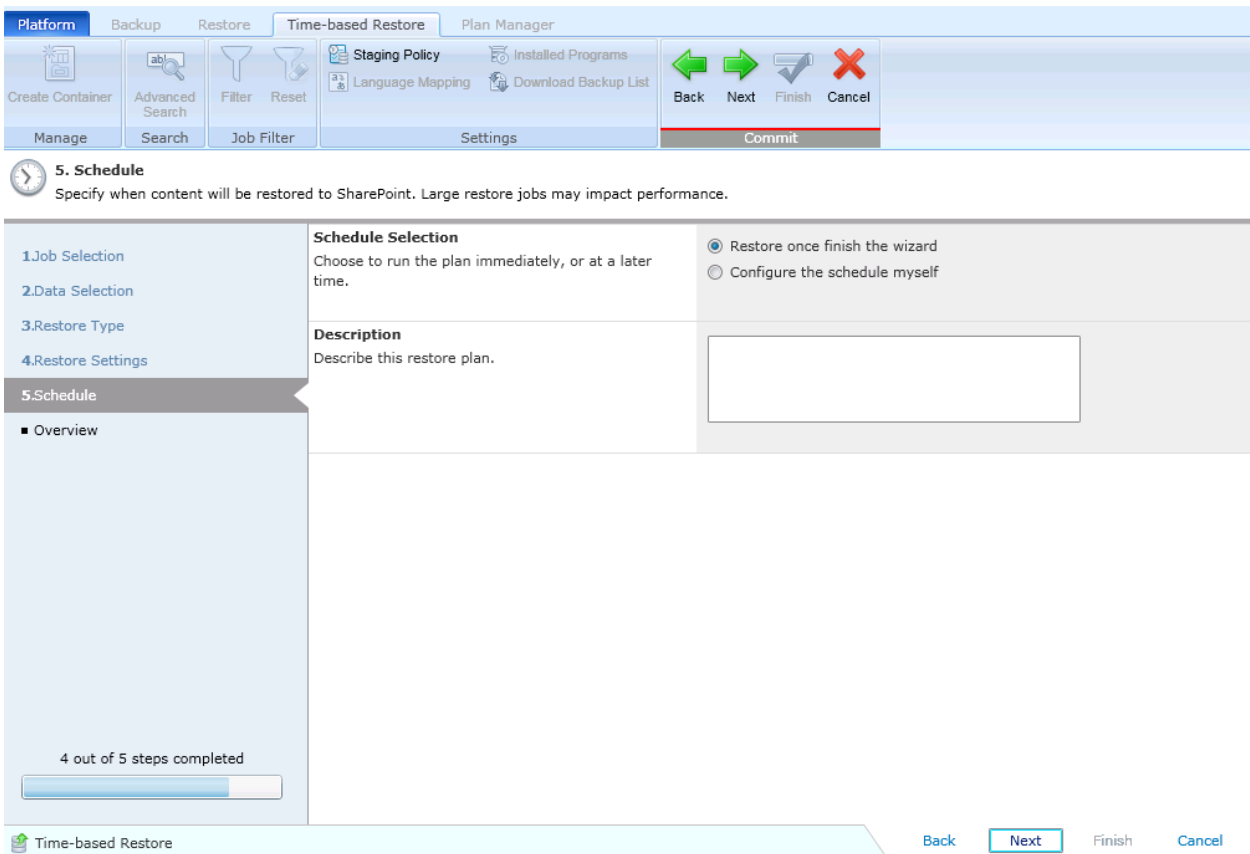
11. Select the restore type, the restore location (if different from the original location), and the agent group to be used to restore the data. Click Next.

The screenshot displays the 'Time-based Restore' wizard in the SnapManager for SharePoint interface. The current step is '3. Restore Type', which involves choosing how to restore the selected data. The interface includes a top navigation bar with tabs for Platform, Backup, Restore, Time-based Restore, and Plan Manager. Below the navigation bar are various tool icons and buttons like 'Back', 'Next', 'Finish', and 'Cancel'. The main content area is divided into a left-hand navigation pane and a right-hand configuration area. The navigation pane lists five steps: 1. Job Selection, 2. Data Selection, 3. Restore Type (current), 4. Restore Settings, and 5. Schedule. A progress bar at the bottom of the navigation pane shows '2 out of 5 steps completed'. The configuration area contains three sections: 'Restore Type' with radio buttons for 'In place restore' (selected) and 'Out of place restore'; 'Restore From Alternate Storage Location' with a checkbox; and 'Agent Group' with a dropdown menu set to 'DEFAULT_AGENT_GROI'. At the bottom of the wizard, there are 'Back', 'Next', 'Finish', and 'Cancel' buttons.

12. On the Restore Settings page, select Replace for Container level conflict resolution setting for the restore job. Click Next.



13. On the Schedule page, select a schedule for restoring the data (if applicable). Click Next.



14. On the Overview page, review and edit the job selections and click Finish.

Platform Backup and Restore > Restore > Time-based Restore

User: demo.netapp.com\spfarm

Platform Backup Restore Time-based Restore Plan Manager

Create Container Load Remote Backups Advanced Search Find Site Collection Filter Reset Staging Policy Installed Programs Download Backup List

Manage Search Job Filter Settings Commit

Back Next Finish Cancel

Overview
Review and edit the settings on this page.

1. Job Selection
2. Data Selection
3. Stub and BLOB Settings
4. Restore Type
5. Restore Settings
6. Schedule

Overview

6 out of 6 steps completed

Time-based Restore

Back Next Finish Cancel

Data selection Edit	
View:	Details view

Restore Type Edit	
Restore Type:	In place restore
Restore From Alternate Storage Location:	No
Agent Group:	DEFAULT_AGENT_GROUP_FOR_Farm(SQL1:SHAREPOINT_CONFIG)

Restore Settings Edit	
Container Level Conflict Resolution:	Replace
Content Level Conflict Resolution:	None
Include Detailed Job Report for All Items:	Yes
Staging Policy:	Default
Restore Workflow State:	No
Item Dependent Columns and Content Types:	Overwrite the columns and content types
Exclude User/Group Without Permission:	No
Notification:	None

Schedule Edit	
-------------------------------	--

References

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

- [NetApp Storage Systems](#)
- [Data ONTAP Documentation](#)

Additional Documentation Available from NetApp Support Site

- [NetApp SnapDrive for Windows](#)
- [SnapManager for Microsoft SQL Server \(SMSQL\)](#)
- [SnapManager for Microsoft SharePoint](#)
- [Install Prerequisites from a Network Share](#)
- [Deploy a Single Server with SQL Server](#)
- [Deploy a Single Server with a Built-In Database](#)
- [Multiple Servers for a Three-Tier Farm](#)
- [Deploy a Virtual Environment](#)
- [Configure Services](#)
- [Configure Farm Settings](#)
- [Create Web Applications \(Classic Mode Authentication\)](#)
- [Create Web Applications \(Claims-Based Authentication\)](#)

Version History

Version	Date	Document Version History
Version 1.0	May 2014	Initial release
Version 1.0.1	July 2014	Updated with deployment procedure

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.

NetApp provides no representations or warranties regarding the accuracy, reliability, or serviceability of any information or recommendations provided in this publication, or with respect to any results that may be obtained by the use of the information or observance of any recommendations provided herein. The information in this document is distributed AS IS, and the use of this information or the implementation of any recommendations or techniques herein is a customer's responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. This document and the information contained herein may be used solely in connection with the NetApp products discussed in this document.

[Go further, faster®](#)



www.netapp.com

© 2014 NetApp, Inc. All rights reserved. No portions of this document may be reproduced without prior written consent of NetApp, Inc. Specifications are subject to change without notice. NetApp, the NetApp logo, Go further, faster, Data ONTAP, FlexClone, FlexVol, OnCommand, SnapDrive, SnapManager, SnapMirror, SnapRestore, Snapshot, and SnapVault are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries. Active Directory, Excel, Hyper-V, Microsoft, SharePoint, SQL Server, Windows, Windows PowerShell, and Windows Server are registered trademarks of Microsoft Corporation. ESX, VMware, VMware vMotion, and VMware vSphere are registered trademarks and vCenter is a trademark of VMware, Inc. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. TR-4297-0714