Dell EMC NetWorker Module for Microsoft for SQL and SharePoint VSS

Version 19.1

User Guide

302-005-512

REV 01

Published May 2019

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.“ DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Published in the USA.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

FIGURES

TABLES

Preface

As part of an effort to improve product lines, periodic revisions of software and hardware are released. Therefore, all versions of the software or hardware currently in use might not support some functions that are described in this document. The product release notes provide the most up-to-date information on product features.

If a product does not function correctly or does not function as described in this document, contact a technical support professional.

Note

This document was accurate at publication time. To ensure that you are using the latest version of this document, go to the Support website https://www.dell.com/support.

Purpose

This guide contains information about using the NetWorker Module for Microsoft (NMM) 19.1 software to back up and recover SQL Server and SharePoint Server using the Volume Shadow Copy Service (VSS) technology.

Note

The *NetWorker Module for Microsoft Administration Guide* supplements the backup and recovery procedures described in this guide and must be referred to when performing application-specific tasks. Download a copy of the *NetWorker Module for Microsoft Administration Guide* from the Support website (https://support.emc.com) before using this guide.

Audience

This guide is part of the NMM documentation set, and is intended for use by system administrators during the setup and maintenance of the product. Readers should be familiar with the following technologies used in backup and recovery:

- NetWorker software
- Microsoft Volume Shadow Copy Service (VSS) technology

Revision history

The following table presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
01	May 20, 2019	First release of this document for the NetWorker Module for Microsoft 19.1 Beta release.

Related documentation

The NMM documentation set includes the following publications:

- *NetWorker Module for Microsoft Release Notes*
- *NetWorker Module for Microsoft Administration Guide*
- *NetWorker Module for Microsoft Installation Guide*
- *NetWorker Module for Microsoft for SQL and SharePoint VSS User Guide*
- *NetWorker Module for Microsoft for SQL VDI User Guide*
- *NetWorker Module for Microsoft for Exchange VSS User Guide*
- *NetWorker Module for Microsoft for Hyper-V User Guide*
- *ItemPoint for Microsoft SQL Server User Guide*
- *ItemPoint for Microsoft Exchange Server User Guide*
- *ItemPoint for Microsoft SharePoint Server User Guide*
- NetWorker documentation set

Special notice conventions that are used in this document

The following conventions are used for special notices:

NOTICE

Identifies content that warns of potential business or data loss.

Note

Contains information that is incidental, but not essential, to the topic.

Typographical conventions

The following type style conventions are used in this document:

Table 2 Style conventions

Bold	Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window.
Italic	Used for full titles of publications that are referenced in text.
`Monospace`	Used for: • System code • System output, such as an error message or script

Table 2 Style conventions (continued)

	• Pathnames, file names, file name extensions, prompts, and syntax • Commands and options
Monospace italic	Used for variables.
Monospace bold	Used for user input.
[ ]	Square brackets enclose optional values.
|	Vertical line indicates alternate selections. The vertical line means or for the alternate selections.
{ }	Braces enclose content that the user must specify, such as x, y, or z.
...	Ellipses indicate non-essential information that is omitted from the example.

You can use the following resources to find more information about this product, obtain support, and provide feedback.

Where to find product documentation

- https://www.dell.com/support
- https://community.emc.com

Where to get support

The Support website https://www.dell.com/support provides access to product licensing, documentation, advisories, downloads, and how-to and troubleshooting information. The information can enable you to resolve a product issue before you contact Support.

To access a product-specific page:

1. Go to https://www.dell.com/support.
2. In the search box, type a product name, and then from the list that appears, select the product.

Knowledgebase

The Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Knowledge Base**.
3. In the search box, type either the solution number or keywords. Optionally, you can limit the search to specific products by typing a product name in the search box, and then selecting the product from the list that appears.

Live chat

To participate in a live interactive chat with a support agent:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Contact Support**.
3. On the **Contact Information** page, click the relevant support, and then proceed.

Service requests
To obtain in-depth help from Licensing, submit a service request. To submit a service request:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Service Requests**.

Note

To create a service request, you must have a valid support agreement. For details about either an account or obtaining a valid support agreement, contact a sales representative. To get the details of a service request, in the `Service Request Number` field, type the service request number, and then click the right arrow.

To review an open service request:

1. Go to https://www.dell.com/support.
2. On the **Support** tab, click **Service Requests**.
3. On the **Service Requests** page, under **Manage Your Service Requests**, click **View All Dell Service Requests**.

Online communities
For peer contacts, conversations, and content on product support and solutions, go to the Community Network https://community.emc.com. Interactively engage with customers, partners, and certified professionals online.

How to provide feedback
Feedback helps to improve the accuracy, organization, and overall quality of publications. You can send feedback to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

Introduction

This chapter includes the following sections:

SharePoint Server overview

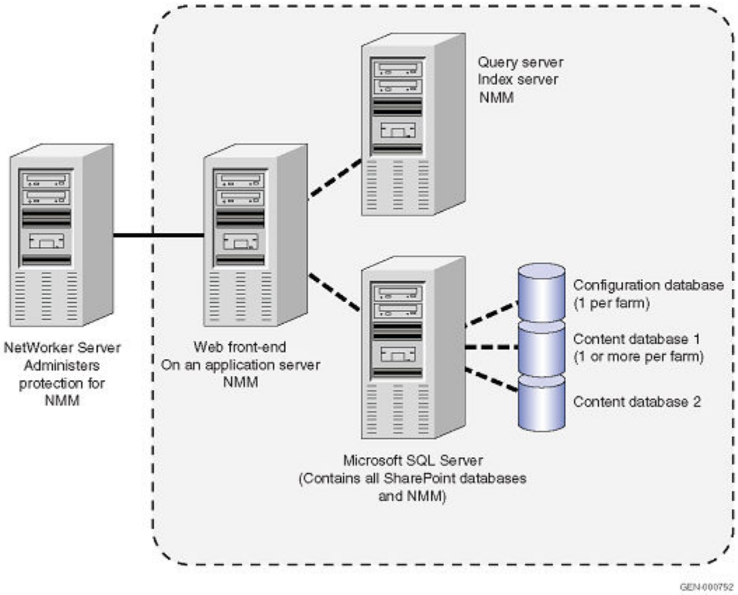
You can use the NetWorker Module for Microsoft (NMM) to back up and recover a Microsoft SharePoint Server.

Microsoft SharePoint environments

NMM uses the Microsoft Volume Shadow Copy Service (VSS) framework and the Microsoft Office SharePoint Server VSS Writers for consistent point-in-time snapshots to back up the entire SharePoint farm.

NMM supports backup and recovery of a Microsoft Office SharePoint Server farm in a distributed configuration. A distributed configuration includes a collection of servers that host separate services.

Figure 1 SharePoint Server distributed farm configuration



NOTICE

Configure SharePoint farm to the SQL alias that has been created only by using `cliconfg.exe`.

To back up the entire distributed SharePoint Server farm, ensure that NetWorker client and NMM are installed on each server that hosts SharePoint data, including servers that host the content index and search index.

Note

If there are multiple query servers, you cannot include index servers with them.

The following table lists the services and servers in a SharePoint Server farm.

Table 3 Services and servers in a SharePoint Server farm

Services and servers	Description
Central Administration site and shared services	The services that are usually installed on a web front-end server. The Central Administration in the SharePoint Server is used to perform administration tasks from a central location. For example: The Application Management manages web applications, site collections, service applications, and databases.
Web front-end server	A web server that handles web page requests from users, processes the requests, and then returns the data.
Application server	A server that provides software applications with services, such as security, data services, transaction support, load balancing, and management of large distributed systems. For example, Excel Calculation Services.
SQL Server	The server that contains SharePoint databases: • Configuration database (only one per farm) • Content databases (one or more per farm) • Search database (one or more per farm)
Index server	An Index server is assigned the task of 'crawling' the user content and building up an index of key words and phrases. A Search Server then uses this index to respond to user searches and suggest results.
Query server	An application server with only the search service role enabled (in this case the query role). If there is more than one query server, the index server cannot be included on a query server.

NMM backs up the following SharePoint farm components:

- Configuration database—SharePoint configuration database
- Content database—SharePoint content database
- Microsoft Office Search—Microsoft Office search indexes and associated databases
- Service applications—(Only for Microsoft SharePoint Server 2013, 2016, and 2019) You can configure individual services independently, and third-party companies can add services to the platform. Services that are deployed are named service applications. A service application provides a resource that can be shared across sites throughout a farm, and that users can through a hosting web

application. Service applications are associated to web applications by service application connections. Some services can be shared across farms.

Supported SharePoint Server VSS Writers

This section lists the VSS Writers that SharePoint Server supports.

Table 4 Supported SharePoint Server VSS Writers

VSS Writers	Description	Found in SharePoint Server versions
SharePoint Services Writer	Writer for SharePoint Server	• SharePoint Server 2019 • SharePoint Server 2016 • SharePoint Server 2013
OSearch15 VSS Writer	Writer for Microsoft Office Server Search	SharePoint Server 2013
OSearch16 VSS Writer	Writer for Microsoft Office Server Search	• SharePoint Server 2019 • SharePoint Server 2016

Note

NMM backs up the SharePoint Server using the SharePoint VSS Writer. The SharePoint Server VSS Writer is dependent on the SQL Server VSS Writer, and SharePoint Server OSearch Writer.

Supported special characters

NMM supports the following special characters in SharePoint web application, site collection, and content databases:

- @
- !
-)
- $

NMM also supports SharePoint backups and recoveries of data that contain these special characters.

SharePoint Server backups

NMM supports SharePoint farm level backup for SharePoint Server distributed farm. All the SharePoint Servers and dependent data across all the servers in a farm are backed up. A pure WFE in the SharePoint farm is not part of a farm-level backup and you must separately backup the pure WFE node for disaster cases.

SharePoint Server recovery

NMM supports the following recovery types for a SharePoint Server distributed farm.

- SharePoint farm-level recovery: Recovers all the SharePoint Servers and dependent data across all the SharePoint WFE nodes in the farm.

You can start a farm-level recovery only from the SharePoint WFE's. However, the SQL data can be restored from any SharePoint or SQL Server node of the farm.

- Content database recovery: Recovers only the content databases.
- Single web application recovery: Recovers only one web application that has been backed up as part of a full-farm backup.
  You must back up any new web application as part of a full-farm backup.
- Granular level recovery: Recovers files and folders from a single full backup.
  You can perform granular level recovery by using NMM with ItemPoint for SharePoint Server. The "Microsoft SharePoint Server Granular Level Recovery" chapter and the ItemPoint for SharePoint Server documentation provides information.

SQL Server overview

You can use NMM to back up and recover a Microsoft SQL Server with Volume Shadow Copy Service (VSS) technology.

Note

Do not use both the NMM VSS and NMM Virtual Backup Device Interface (VDI) together to back up and recover a SQL Server. NMM SQL VSS backups are always full backups. NMM VSS backups promote NMM SQL VDI incremental backups to full backups. The *NetWorker Module for Microsoft for SQL Server VDI User Guide* provides information about backup and recovery by using the VDI technology.

The *NetWorker E-LAB Navigator* , which is available at https://elabnavigator.emc.com/eln/elnhome, provides the most up-to-date information about supported SQL Server and Windows Server versions.

NMM does not support backup and recovery of the following SQL Server versions:

- SQL Server running on IA64
- SQL Server 2000 and SQL Server 2005
- SQL Server Express Editions

Note

To perform a SQL Server Express Edition backup, use the VDI technology workflow, as described in the *NetWorker Module for Microsoft for SQL VDI User Guide*.

SQL Server backup and recovery

NMM supports full backups and full recoveries of the SQL VSS Server. NMM supports full backups at instance level and database level.

NMM treats a SQL Server database that is configured as AlwaysOn as a normal database. Back up the database as Performing federated backups on SQL setups that have AlwaysOn Availability Group configured on page 50 describes.

NMM does not support the following types of SQL VSS backups:

- SQL transaction log backups
- SQL database differential backups
- SQL backup of individual filegroups, files, or logs

The "Supported backup settings for SQL Server 2012 and later Availability Group" section provides information about the AUTOMATED_BACKUP_PREFERENCE and

BACKUP PRIORITY settings for SQL Server 2012 and later Availability Group that are supported by NMM.

NMM 19.1 compatibility with NetWorker 8.2.3 or 8.2.4 servers

NMM supports backup and recovery with NetWorker client version 19.1 and NetWorker server version 8.2.3 or 8.2.4.

The *NetWorker Module for Microsoft Installation Guide* contains the NMM support matrix for NetWorker server and client versions. For more details, see the individual NMM release sections of the *NetWorker E-LAB Navigator* , which is available at https://elabnavigator.emc.com/eln/elnhome.

Note the following limitations when you configure NMM backup and recovery with an NMM 19.1 client and a NetWorker 8.2.3 or 8.2.4 server:

- Dedicated Storage Node: NetWorker 8.2.3 and 8.2.4 servers do not support NetWorker storage node 19.1. As a result, you cannot configure a dedicated storage node when you use NetWorker 19.1 client with NetWorker 8.2.3 or 8.2.4 server.
- Backup levels: NetWorker 8.2.3 and 8.2.4 servers use NetWorker server 8.x backup-level definitions, and do not support the NetWorker server version 9.x and later backup levels.

Using NetWorker server 8.2.3 or later and NMM 19.1

If you are using NetWorker server 8.2.3 and NMM 19.1:

- Configure a regular NetWorker backup group. Do not enable the **Snapshot** option in the NetWorker backup group.
- For the Client Backup Configuration wizard to properly function, ensure that JRE is installed on the host, where the NetWorker Management Console (NMC) is used. The NMC for NetWorker 8.2.3 supports JRE 7, and the NMC for NMM 19.1 supports JRE 8 and 9.
- After upgrading the NMM version to 19.1, ensure that you use the **Client Backup Configuration** wizard to modify client resources for SharePoint federated backups. The client resources of all the nodes except the client resource of the backup primary WFE node are converted to dummy clients. If you perform a backup without modifying the client resource, the backup fails.
- To modify a client resource that was created by using NMM 8.2.x, before you run the NMM 19.1 Client Backup Configuration wizard, ensure that the **Snapshot** option of the NetWorker group, to which the client resource belongs, is clear. If the **Snapshot** option is selected, you cannot select the NetWorker group in the wizard, and you are prompted to create or select another group.
- To upgrade a SharePoint environment from non-federated to federated, use the **Modify** option in the **Client Backup Configuration** wizard.
- Do not use NetWorker strong authentication (nsrauth) to communicate with other hosts, such as NMC server, NetWorker server, and NetWorker client. The NetWorker 19.1 Administration Guide provides more information about nsrauth.

CHAPTER 2

Microsoft SharePoint Server Scheduled Backups in a Federated Workflow

This chapter includes the following sections:

Overview

In NMM 9.1 and later, the scheduled backup workflow is simplified and is known as federated backup. You can perform SharePoint federated backups of an entire SharePoint farm including the web front ends (WFE), SQL Server, dedicated Search Servers, and SQL Server AlwaysOn Availability Group (AAG) databases. To perform SharePoint disaster recovery, you must ensure that all the data is backed up.

NOTICE

NMM 19.1 does not support SharePoint with SQL Server 2017 VSS read-scale (clusterless) availability group and domain independent (domainless) availability group configurations.

- NMM 9.0 and later provide support for SQL AAG configurations between SQL standalone setups.
- NMM 9.1 and later provide support SQL Server AAG configured between SQL virtual servers and SQL Server standalone.
- NMM SharePoint backups ensure synchronous backup of client file indexes and SQL databases. Therefore, the backups do not go out-of-sync with each other. A backup is scheduled against a single WFE that automatically discovers the dependencies that must be backed up from other WFEs and SQL Servers. This WFE is known as the backup primary WFE. The Client Configuration Wizard enables you to select the backup primary WFE from the list of WFEs in a farm.
- The backup of the entire farm is indexed against the primary WFE node. If the backup fails on any node, the entire backup fails.

Note

You must separately backup the WFEs that are not part of a farm-level backup. Backing up these WFEs helps in the case of a disaster.

Prerequisites for SharePoint Server backups

Ensure that you meet the following prerequisites:

- Provide the required permission for the SharePoint Server so that the SYSTEM user can run SharePoint PowerShell. The `nsrnmmsv` command runs under the security context of the Domain\Remote username that is specified in the **Remote Username** field during client configuration. The `nsrnmmra` command runs under the security context of the SYSTEM user.

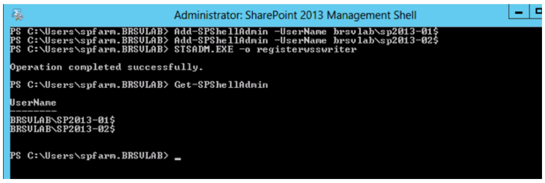
  1. In the SharePoint Management Shell, add the SYSTEM account and Domain \UserName to SPShellAdmin, by typing the following command for each web front-end server and the Search Server:

     ```
     Add-SPShellAdmin -UserName DOMAIN\HOSTNAME$
     ```

     ```
     Add-SPShellAdmin -UserName DOMAIN\USERNAME
     ```

  2. Verify that the SYSTEM account is added to SPShellAdmin by typing the command `Get-SPShellAdmin` and viewing the details in the Object Explorer of the SQL Server Management Studio (SSMS).

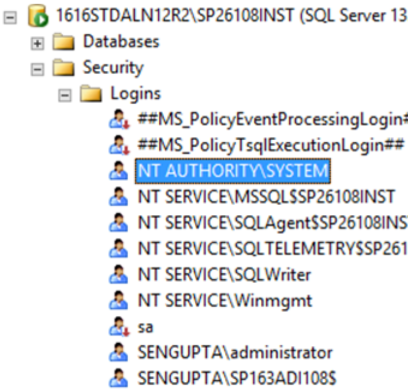
Figure 2 Expected output after using the Add-SPShellAdmin and Get-SPShellAdmin commands



Administrator: SharePoint 2013 Management Shell

```
PS C:\Users\spfarm.BRSVLAB> Add-SPShellAdmin -UserName brsvlab\sp2013-01$
PS C:\Users\spfarm.BRSVLAB> Add-SPShellAdmin -UserName brsvlab\sp2013-02$
PS C:\Users\spfarm.BRSVLAB> STSADM.EXE -o registerwsswriter

Operation completed successfully.

PS C:\Users\spfarm.BRSVLAB> Get-SPShellAdmin

UserName
--------
BRSVLAB\SP2013-01$
BRSVLAB\SP2013-02$


PS C:\Users\spfarm.BRSVLAB> _
```

Figure 3 View SYSTEM account in the Object Explorer



```
⊟ 1616STDALN12R2\SP26108INST (SQL Server 13
  ⊞ Databases
  ⊟ Security
    ⊟ Logins
        ##MS_PolicyEventProcessingLogin#
        ##MS_PolicyTsqlExecutionLogin##
        NT AUTHORITY\SYSTEM
        NT SERVICE\MSSQL$SP26108INST
        NT SERVICE\SQLAgent$SP26108INS
        NT SERVICE\SQLTELEMETRY$SP261
        NT SERVICE\SQLWriter
        NT SERVICE\Winmgmt
        sa
        SENGUPTA\administrator
        SENGUPTA\SP163ADI108$
```

3. Configure the user roles, groups, and permissions that following table lists:

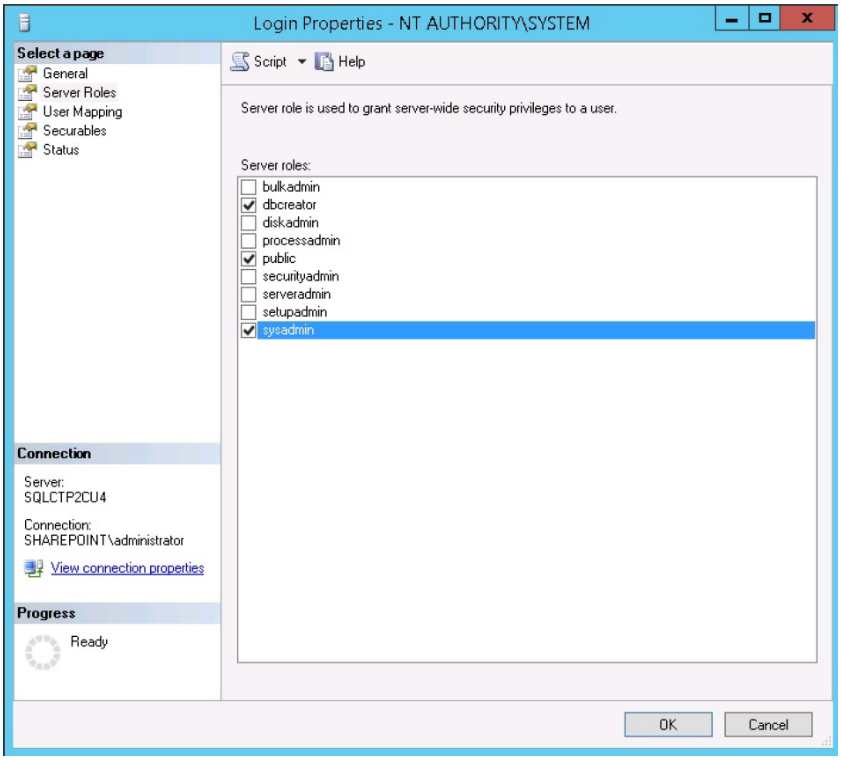
Table 5 User roles, groups, and permissions

User account or role	Add the user to the Backup Operators group	Add the user to the local Administrators group	Add the user to the Remote Desktop Users group	Add the user to the Farm Administrators group	Applicable nodes	Set the Public, DB Creator, Sys Admin permissions in the SQL Server Management Studio	Need Domain Admin privileges
SP Farm Admin	Yes	Yes	Yes	Yes	SP	Yes	No
SP Search Admin	Yes	Yes	Yes	Yes	SP	Yes	No
SQL Admin	No	No	No	No	SQL	Yes	No
Backup Admin	Yes	Yes	Yes	Yes	SP and SQL	Yes	No

4. On the **Microsoft SQL Server Management Studio** > **Security** > **Login** > **Login Properties** page, grant the SQL Server system dbcreator, public, and

system administrator permissions to the Windows login account. Provide these permissions to the *NTAUTHORITY\SYSTEM* user and the *DOMAIN \HOSTNAME$* user and the *Domain\UserName* user on a distributed farm.

Figure 4 Granting permissions to view subcomponents in SSMS



Login Properties - NT AUTHORITY\SYSTEM

Select a page
- General
- Server Roles
- User Mapping
- Securables
- Status

Script ▾ Help

Server role is used to grant server-wide security privileges to a user.

Server roles:

- □ bulkadmin
- ☑ dbcreator
- □ diskadmin
- □ processadmin
- ☑ public
- □ securityadmin
- □ serveradmin
- □ setupadmin
- ☑ sysadmin

Connection

Server:
SQLCTP2CU4

Connection:
SHAREPOINT\administrator

View connection properties

Progress

Ready

OK Cancel

- If the OSearch Writer service is running with a different user permission, perform the following steps:
  1. Add the OSearch account to the following groups:
     - Backup Operators
     - Remote Desktop Users
     - Local Administrators
  2. On each SharePoint node, to the groups that are mentioned in step 1, add the following user accounts:
     - **SP-FARM**: A SharePoint administrator account that you can use to configure or deploy SharePoint.
     - **SP-Search**: A user account that is not a SharePoint administrator account, and you configured the SharePoint Search service to use it.
     - **SP-Backup**: A user account that you can use to configure a SharePoint client on a Networker server.
- You use the correct NetWorker server and client versions. The *NetWorker Module for Microsoft Installation Guide* contains the NMM support matrix for NetWorker server and client versions. For more specific details, see the individual NMM release sections of the *NetWorker E-LAB Navigator* , which is available at https://elabnavigator.emc.com/eln/elnhome.
- Install the NetWorker client and NMM on all the SharePoint farm components with data that must be backed up.

- If you select a WFE that was not used to create client resources in the farm as the backup primary WFE, manually register the WSS Writer on the selected backup primary WFE.
- When you select a SharePoint WFE as the backup primary WFE, ensure that the WFE has Microsoft SharePoint Foundation Web Application service running. To check whether the Microsoft SharePoint Foundation Web Application service is running, run the following command:

  ```
  Get-SPServiceInstance -Server <WFE node> | where-object
  {$_.TypeName -eq "Microsoft Sharepoint Foundation Web
  Application"}
  ```

  Output:

  ```
  TypeName Status Id

  Microsoft SharePoint Foundati... Online
  ae749c81-6469-4777-96f9-7e1adc5ca567
  ```

- Mount all the SharePoint Server databases before backing up the application server. Unmounted SharePoint Server databases are not backed up.
- After you install SharePoint Server, do not move the Search administration component within the SharePoint Server because the SharePoint Search Index service can stop working.
- If any major change is made to the SharePoint Server configuration or database structure, reconfigure the clients and ensure that all dependencies are reflected in the dependent clients. For example, if you perform a farm backup on Monday, and add a content database on Tuesday, perform a fresh backup of the complete farm to keep the backup up-to-date.
- Before starting a backup, ensure that the following services are enabled and started:
  - Windows SharePoint VSS Writer that is running the web front-end host
  - SPSearch Writer and OSearch Writer
  - SQL Server VSS Writer that is running on the host that contains the configuration database or content databases

  Note

  After you configure SharePoint Search, the services automatically start. If the services do not automatically start, manually start them. Before you perform a backup, ensure that all the relevant configured services for SharePoint are started. Otherwise, backup fails.

- On SharePoint Server 2013, ensure that an IP address always resolves to only one domain and one hostname.
  If an IP address resolves to multiple domains or hostnames, a federated backup fails, because the backup appends all the relevant domain names to the configured hostname in the following invalid format:

  ```
  <hostname>.<domain>.<domain_1>.<domain_2>....<domain_n>
  ```

  Because of this reason, NMM does not support the following configurations for SharePoint Server 2013 federated backups:
  - Disjoint namespace configuration
  - SharePoint Apps or setting up the App domain for the SharePoint Server

Creating SharePoint Server client resources

Before you create the client resources, set the appropriate attribute values for the Policy and Group resources. You must be an administrator to perform this task. You can create a client resource by either using the Client Backup Configuration wizard or manually performing the process by using the NetWorker Administration page of the NMC.

When you use the Client Backup Configuration wizard, configure a single SharePoint WFE as the backup primary WFE, and create a client resource for it. The **Client Backup Configuration** wizard automatically detects all the components in the SharePoint farm, and then creates a client resource for the backup primary WFE and dummy client resources for the other components in the SharePoint farm. The backup primary WFE contains the top level save set "APPLICATIONS:\Microsoft Office SharePoint Services" and the rest of the dummy clients contain the dummy save set "ALL."

Note

Before you remove a backup primary WFE from a farm, select one of the other WFEs as the backup primary WFE. If you accidentally delete a backup primary WFE from either a SharePoint farm or a Networker server, before you perform a backup, you must delete all the dummy clients, and then reconfigure the clients.

Creating a client resource by using the Client Backup Configuration wizard

When you create a client resource for the backup primary WFE by using the Client Backup Configuration wizard, only the top level save set is used. To view the top level save set, run the `nsrnmmsv -P` command. To view the detailed list of all the save sets, run the `nsrnmmsv -v -P` command.

Procedure

1. In the **NetWorker Administration** window, click **Protection**.
2. In the expanded left panel, right-click **Clients**, and then select **New Client Wizard**.
3. On the **Specify Client Information** page:

   a. In the **Client Name** field, type either the host name or the Fully Qualified Domain Name (FQDN) of the WFE that you used to configure SharePoint farm backup.

      Note

      Do not type the IP address of the WFE.

   b. In the **Comment** field, type a description for the client resource.

   c. (Optional) In the **Tag** field, type one or more tags that identify this client resource as one to include in the dynamic client groups for data protection policies.

      Dynamic client groups automatically generate a list of clients for a data protection policy based on the tags assigned to the client and group.

   d. From the **Group** menu, select the protection group to which the client resource for the primary node must be added. The *NetWorker Administration Guide* provides information about how to create a protection group.

   Note

   You may also create a group later and assign the client resource to it.

   e. Select **Traditional NetWorker client**.

   f. Click **Next**.

4. On the **Specify Backup Configuration Type** page:

   a. From the **Available Application** list, select **SharePoint Server**.

   b. If the **Enable NetWorker Snapshot Management on the selected application** option is selected, clear it.

   c. Click **Next**.

5. On the **Specify the NetWorker Client Properties** page:

   a. From the **Priority** list, select the priority level.

   b. From the **Parallelism** list, select the level of parallelism.

   c. In the **Remote Access** field, type the required attributes.

   You can control client recover access with the attributes in the **Remote Access** field during in the client resource configuration. The **Remote Access** attribute displays a list of the users that can recover save sets for a client. Add or remove user names depending on the level of security the files require.

   d. From the **Data Domain Interface** list, select the device type.

   e. If the **Block Based Backup** option is selected, clear it.

   SharePoint Server does not support block based backups.

   f. Click **Next**.

6. On the **Specify the SharePoint Login Credentials** page:

   a. In the **Remote User Name** field, type the username of the SharePoint Server.

   The username format must be either `Domain\username` or `username@domain.com`.

   b. In the **Password** field, type the password of the SharePoint Server.

   Note

   The user must have administrator privileges on the SharePoint and SQL Servers.

   c. Click **Next**.

7. On the **Select SharePoint Primary WFE** page:

   a. From the list of WFEs, select the backup primary WFE.

If the selected backup primary WFE is different from the WFE that was used to configure SharePoint farm backup, manually register the WSS writer on the selected backup primary WFE.

   b. Click **Next**.

8. On the **Select SharePoint Backup Objects** page, click **Next**.
9. On the **Backup Configuration Summary** page:

   a. Verify whether all configuration settings are correct.

      To revise details on previous pages, click **Back**.

      To reconfigure client resources, click **Create**.

   b. Click **Next**.

10. On the **Client Configuration Results** page, click **Finish**.
11. (Optional) In NMC:

    a. To verify the details of the client resource, right-click the client resource, and then select **Properties**.

       The **Client Properties** dialog box displays the details of the client resource.

    b. To change the client resource, right-click the client resource, and then select **Client Backup Configuration** > **Modify Client Wizard**.

Manually creating client resources by using the Client Properties dialog box

To manually create client resources, use the Client Properties dialog box of the NetWorker Administration program. Create client resources for all the clients that are part of the SharePoint farm. For example, if the farm has two dependent WFEs and two SQL nodes, manually create client resources for all four clients.

Ensure that you have the list of all the save sets that must be backed up when performing the steps to create the client resources. When you manually create client resources for the entire SharePoint farm, only the top level save set is used. To view the top level save set, run the `nsrnmmsv -P` command. To view the detailed list of all the save sets, run the `nsrnmmsv -v -P` command.

Procedure

1. Open NMC.
2. In the **NetWorker Administration** window, click **Protection**.
3. In the expanded left panel, right-click **Clients**, and then select **New**.

   The **Create Client** dialog box appears.

4. On the **General** tab:

   a. In the **Name** field, type either the hostname or the FQDN of the WFE that you used to configure SharePoint farm backup.

      Note

      Do not type the IP address of the WFE.

   b. In the **Comment** field, type a description for the client resource.

If you are creating multiple client resources for the same WFE, use this field to differentiate the purpose of each resource.

c. In the **Save Set** field, type the save sets that you want to back up:

- For the backup primary WFE, type `APPLICAITONS:\Microsoft Office SharePoint Services`.
- For all other nodes, type `ALL`.

d. From **Protection Group List**, select the protection group, to which you want to add the client resource for the backup primary WFE.

Do not add the dummy clients to **Protection Group List**.

5. On the **Apps & Modules** tab:

a. In the **Backup command** field, type **nsrnmmsv.exe**.

b. To enable client-side Data Domain Boost deduplication backups, select **Data Domain backups**.

c. (Optional) To pause the SharePoint crawl component before you take a snapshot, and then resume the component after you take the snapshot, specify the following value in the **Application Information** field in the **Client Properties** dialog box:

```
NSR_PAUSE_RESUME_SSA=YES
```

Note

This application information variable can affect the performance of the index component if the number of items in the search index is large. It is recommended that you do not specify this application information variable.

6. On the **Globals (2 of 2)** tab, in the **Remote Access** field, add or remove user names according to the level of security that the files require.

The field displays a list of the users, who can recover save sets for a client.

7. On the other tabs, specify the fields according to your requirements, and then click **OK**.

Special backup scenarios

Review the following information about special backup scenarios.

Copy-Only full backups of databases on secondary replicas
Because full backups are not supported on the secondary replica, NMM performs a copy-only full backup instead of a full backup on the secondary replica when `AUTOMATED_BACKUP_PREFERENCE` is configured for backup of secondary replica.

The http://msdn.microsoft.com/en-us/library/hh245119.aspx page provides details about backup types that are supported on secondary replicas.

Backups of asynchronous secondary replicas
Backups of asynchronous secondary replicas do not support disaster recovery. These backups support Content Database recovery and item-level recovery using SharePoint GLR.

Table 6 Supported high availability and disaster recovery options for SharePoint Server

	Configuration database	Central Admin content database	Content database	Search Service database
Supports SQL Server AlwaysOn Availability Group with synchronous-commit for high availability	Yes	Yes	Yes	Yes
Supports SQL Server AlwaysOn Availability Group with asynchronous-commit for disaster recovery	No	No	Yes	No

The http://technet.microsoft.com/en-us/library/jj841106.aspx page provides details for supported high availability and disaster recovery options for SharePoint Server 2013 and 2016 databases.

Backups of a SharePoint database that is configured with AG listener but is not joined to an AlwaysOn Availability Group

If a SharePoint database is configured with AG Listener:

- The database is created on the SQL instance that is the primary replica.
- The database is not added to AlwaysOn Availability Group. So, the database is inaccessible from SharePoint after an AlwaysOn AG fails over to another node. The SharePoint Writer does not report this database after the failover, which results in data loss because unreported databases are not backed up.

CHAPTER 3

Microsoft SharePoint Server Recovery

This chapter includes the following sections:

SharePoint Server restore recommendations

Before you perform any restore procedures, review the following recommendations:

- You can restore federated backups of a SharePoint farm from any web front-end that is part of the SharePoint farm. The backups also include SharePoint databases on SQL Servers.

  Note

  SharePoint farm-level restore from a SQL node is not supported. Only SharePoint database restore is supported from a SQL node. Do not separately restore the SharePoint configuration database. Restore it only by performing a full farm restore.

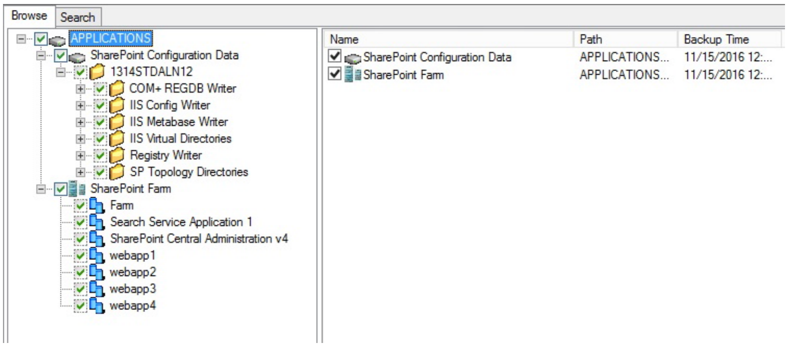
- When you restore a SharePoint configuration database as part of an entire SharePoint farm restore, ensure that all the content databases in that farm are restored for the SharePoint Writer. This is a Microsoft requirement to ensure consistency. You can separately restore a content database without restoring the entire farm.

Restoring a SharePoint full farm

Procedure

1. On the WFE server, open the NetWorker User for Microsoft GUI.
2. In the left panel, click **Recover**.
3. In the middle panel, expand **APPLICATIONS**, and then select the **SharePoint Configuration Data** and **SharePoint Farm** save sets.

   Figure 5 Select SharePoint Configuration Data and SharePoint Farm



Name	Path	Backup Time
☑ SharePoint Configuration Data	APPLICATIONS...	11/15/2016 12:...
☑ SharePoint Farm	APPLICATIONS...	11/15/2016 12:...

4. To view required volumes of a selected web application to recover, right-click the web application, and then select **Required volumes**.

   In the **Required NetWorker Volumes** dialog box, review the list of volumes, and then click **OK**.

5. To select a particular version or backup time of a web application:

   a. Right-click the web application, and then select **Versions**.

   b. In the **NetWorker Versions** dialog box:

      a. Select the backup time.

   b. Select **Use selected item backup time as new browse time**.

   c. Click **OK**.

6. In the NetWorker User for Microsoft GUI, click **Recover**.
7. On the **Recovery Summary** page, review the settings, and then click **Start Recover**.
8. In the **SharePoint Configuration Data Restore** dialog box, click **Yes**.
9. After the restore completes, go to the SharePoint Central Administration, and verify whether the SharePoint full farm is restored.

Restoring content databases

Procedure

1. Open the NetWorker User for Microsoft GUI on the web front-end server.
2. Select **Options** > **Recover Session Options**.
3. In the **Recover Options** dialog box:

   a. On the **NetWorker** tab, clear the **Use Microsoft Best Practices for selecting the SharePoint Configuration Data** option.

   b. click **OK**.
4. In the NetWorker User for Microsoft GUI, in the left panel, click **Recover**.
5. In the middle panel, on the **Browse** tab, expand **APPLICATIONS** > **SharePoint Farm**, and then select the web applications that contain the content databases that you want to restore.
6. To view required volumes of a selected web application to recover, right-click the web application, and then select **Required volumes**.

   In the **Required NetWorker Volumes** dialog box, review the list of volumes, and then click **OK**.
7. To select a particular version or backup time of a web application:

   a. Right-click the web application, and then select **Versions**.

   b. In the **NetWorker Versions** dialog box:

      a. Select the backup time.

      b. Select **Use selected item backup time as new browse time**.

      c. Click **OK**.
8. In the NetWorker User for Microsoft GUI, click **Recover**.
9. In the **Recover Summary** dialog box, review the settings, and then click **Start Recover**.
10. After the restore completes, go to SharePoint Central Administration, and then verify whether the content databases are restored.

Restoring single web application and content databases

With NMM 9.2 or earlier, when a web application corrupts, you must restore the entire farm. The full farm restore operation overwrites the web applications that are created since the last backup.

NMM 18.1 and later enable you to restore single web application, which includes all site collections and databases. The single web application restore does not cause any data loss to other web applications.

When you restore single web application, consider the following limitations:

- You cannot restore a web application to an alternate farm.
  You must restore a web application only to the source farm.
- You cannot restore SharePoint Central Administration web application and extended web applications, that is, web applications that are extended to other zones, such as intranet, extranet, and internet.
  To restore an extended web application, perform single web application restore, and then manually extend the web application.
- You cannot concurrently restore multiple web applications.
- You cannot restore a backup that was performed by using NMM 9.2 or earlier.
  You can only restore a backup that is performed by using NMM 18.1 or later.
- You cannot back up and restore soft and hard links of a virtual directory.

Procedure

1. On the WFE server, open the NetWorker User for Microsoft GUI.
2. In the left panel, click **Recover**.
3. In the middle panel, on the **Browse** tab, expand **APPLICATIONS** > **SharePoint Farm**, and then select the web application that you want to restore.

   Note

   Do not select either the SharePoint Central Administration web application or an extended web application.

4. To view required volumes of a selected web application to recover, right-click the web application, and then select **Required volumes**.

   In the **Required NetWorker Volumes** dialog box, review the list of volumes, and then click **OK**.

5. To select a particular version or backup time of a web application:

   a. Right-click the web application, and then select **Versions**.

   b. In the **NetWorker Versions** dialog box:

      a. Select the backup time.

      b. Select **Use selected item backup time as new browse time**.

      c. Click **OK**.

6. In the NetWorker User for Microsoft GUI, click **Recover**.
7. In the **Recovery Item** dialog box, perform one of the following steps:
   - To restore the web application that you have selected:

     a. Select **Single web application recovery**.

     b. Click **Recover**.

     c. Perform steps 5 and 6.
   - To restore only the databases (content databases) of the web application that you have selected:

   a. Select **Database recovery**.

   b. Click **Recover**.

   c. Perform step 6.

8. In the **Recover Options** dialog box, perform the following steps:

   a. On the **NetWorker** tab, clear the **Use Microsoft Best Practices for selecting the SharePoint Configuration Data** option.

   b. On the **SharePoint** tab, specify the following fields:

   - **UserName**: The username that was used to perform the backup automatically appears in this field. However, you can specify a different username that has farm administrator rights.
   - **Password**: Type the corresponding password for the username that you have specified.

   c. Click **OK**.

9. In the **Recover Summary** dialog box, review the settings, and then click **Start Recover**.

Restoring SQL Server AlwaysOn Availability Group databases

Before you begin

Restore SharePoint full farm.

Note

Before you restore a SharePoint farm, in which the SQL Server has AlwaysOn Availability Group preference set to secondary, fail over the SQL secondary to make it the primary node. You must perform this task because during a SharePoint full farm recovery, the WFE node connects only to the SQL primary node, and cannot recognize the secondary node.

Procedure

1. Ensure that the AlwaysOn Availability Group is a primary replica on the host, from which the AlwaysOn Availability Group database was backed up.

   The NetWorker User for Microsoft GUI displays the host, from which a particular database was backed up. If the backed up host instance is not a primary replica, fail over the AlwaysOn database to the replica, from which the database was backed up.

2. Restore the database.
3. Delete the **Recovering** mode database on all secondary replicas.
4. Join or re-add the database to the AlwaysOn Availability Group by using the **full join** method.

Restoring SharePoint Server and SQL Server VSS backups that are performed by using NMM 8.2.3 and 8.2.4

This procedure applies to the customers, who upgrade NMM from 8.2.3 or 8.2.4 to 9.1 or later.

To restore SharePoint Server and SQL Server VSS backups that are performed by using NMM 8.2.3 and 8.2.4, use NMM 9.1 or later.

Before you perform the restore, ensure that you meet the following requirements:

1. You installed NMM 9.1 or later by selecting the **Restore of NMM 8.2.x and Earlier Backups (VSS workflows)** option in the installer.
2. You installed all the necessary packages.

The *NetWorker Module for Microsoft Installation Guide* provides information.

The *NetWorker Module for Microsoft for SQL and SharePoint VSS 8.2 User Guide* describes the procedure to perform restore.

CHAPTER 4

Microsoft SharePoint Server Granular Level Recovery

This chapter includes the following sections:

Overview

You can perform Granular Level Recovery (GLR) of SharePoint application backups that are performed by using NMM. GLR enables you to recover specific items, such as files and folders, from a single full backup. You do not need to recover the full backup. GLR reduces storage space requirements and recovery time according to the sizes of content databases. You can recover content databases of SharePoint Server 2013 SP1, 2016, and 2019. SharePoint Server 2016 and 2019 include KB3128014 update.

Performing GLR of SharePoint farms

Performing a GLR of a SharePoint farm includes the following tasks:

1. Mounting backups
2. Performing GLR
3. Dismounting backups

Prerequisites

Before you perform a GLR, ensure that you meet the following prerequisites:

- You selected the **SharePoint Granular Recovery** option during the NMM installation.
- Only one NetWorker Virtual File System (NWFS) is active at any particular time. If you mount another backup to restore, NWFS dismounts the mounted backup. So, you cannot access the dismounted backup contents till you remount the backup.
- You did not select a tape as a backup device.
- If the type of the device that you use to perform a GLR is non-AFTD, non-Data Domain, or non-Cloud Boost, ensure that the backup is cloned to an Advanced File Type Device (AFTD), a Data Domain device, or a Cloud Boost device.
- To use an AFTD to perform a GLR, you created or configured the AFTD by specifying the UNC path.
  This requirement prevents inadvertent usage of the storage node data path, and performance and timeout issues.
- All backup devices are Direct File Access (DFA)-enabled.
- You started the ItemPoint Agent for Content Transfer Service (ACTS) on the target SharePoint Server.
  The *NetWorker Module for Microsoft Installation Guide* provides information about installing ItemPoint for SharePoint Server, and ACTS. The *ItemPoint for Microsoft SharePoint Server User Guide* provides information about ItemPoint for SharePoint Server.

Prerequisites to use ItemPoint for SharePoint Server

Before you use ItemPoint for SharePoint Server to perform GLR, ensure that the environment meets the following requirements:

Table 7 ItemPoint for SharePoint Server requirements

Component	Requirement
Operating Systems	The following operating systems are supported: • Windows Server 2008 • Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows 7 • Windows 8 • Windows 10 **Note** 32-bit and 64-bit versions, virtual and physical, of the listed operating systems are supported. Dell EMC ItemPoint can only be run by users with administrative privileges and in administrative mode.
Microsoft Office SharePoint Server/ Microsoft SQL Server	Dell EMC ItemPoint for Microsoft SharePoint Server can open the following source data: • Microsoft Office SharePoint Server 2013 up to SP1 data stored on: ▪ Microsoft SQL Server 2008 R2 up to SP2 ▪ Microsoft SQL Server 2012 up to SP1 ▪ Microsoft SQL Server 2014 • Microsoft Office SharePoint Server 2016 data stored on: ▪ Microsoft SQL Server 2014 ▪ Microsoft SQL Server 2016 SP1 and later ▪ Microsoft SQL Server 2017 • Microsoft Office SharePoint Server 2019 data stored on: ▪ Microsoft SQL Server 2016 ▪ Microsoft SQL Server 2017 Dell EMC ItemPoint for Microsoft SharePoint Server can connect to the following target servers: • Microsoft Office SharePoint Server 2013 through SP1 • Microsoft Office SharePoint Server 2016 • Microsoft Office SharePoint Server 2019 Remote Blob Stores (RBS): • FILESTREAM Provider • Metalogix StoragePoint Provider (v4.2.1 through v5.4)

Table 7 ItemPoint for SharePoint Server requirements (continued)

Component	Requirement
	• StorSimple SharePoint Database Optimizer
Virtual environments	**Note** Virtual operation of tape devices may have restrictions imposed by virtual operating systems.
Additional software	Microsoft .NET Framework • 3.5 SP1 • 4.0 • 4.5 • 4.5.2 **Note** In order for Dell EMC ItemPoint for Microsoft Exchange Server to operate fully, you must ensure the Dell EMC software is correctly licensed for use and the source files are located on Dell EMC storage. If not, attempts to open a source database will produce an error message.

Limitations of ItemPoint for SharePoint Server

The following are the limitations of ItemPoint for SharePoint Server:

- ItemPoint for SharePoint Server can copy the following data:
  - SharePoint Server 2013 (2013 Experience) data to SharePoint Server 2013 with the 2013 Experience
  - SharePoint Server 2013 data that contains only items and folders to SharePoint Server 2013 with the 2013 Experience
  - SharePoint Server 2016 data to SharePoint Server 2016
  - SharePoint Server 2019 data to SharePoint Server 2019
- After you restore data from the source server, you must use the Copy Progress dialog box to verify the links, security settings, and Web Parts on the target server.
- ItemPoint for SharePoint Server does not support the following Microsoft SharePoint Server 2013 site collection templates:
  - eDiscovery Case Site Template
  - Developer Site Template
  - Project Site Template
  - Community Site Template
  - Community Portal Template
  - Product Catalog Template

- ItemPoint for SharePoint Server does not support the following Microsoft SharePoint Server 2016 and 2019 site collection templates:
  - eDiscovery Portal Site Template
  - In Place Hold Policy Center
  - Point Publishing Hub
  - Point Publishing Topic
  - Microsoft Project Site
- After you copy a Microsoft SharePoint Server 2013 site collection that contains the Enterprise Search Center, Enterprise Wiki, Business Intelligence Center, or Publishing Portal site collection templates to a new site collection, the site displays an error on the web page.
- When you copy a Microsoft SharePoint Server 2013 site or site collection that contains the Project Functionality feature, the same feature is not enabled on the target.
- When you copy a Microsoft SharePoint Server 2013 site or site collection that contains the Site Notebook feature, the same feature is not enabled on the target.
- When you copy a Microsoft SharePoint Server 2013 blog site to the target, sometimes the posts list switches from like ratings to star ratings.
- When you copy a Microsoft SharePoint Server 2013 site or site collection that contains the BICenterSampleData hidden feature, the same feature is not enabled on the target.
- When you copy a Microsoft SharePoint site or site collection that contains the GBWProvision hidden feature, the same feature is not enabled on the target.
- When you copy a site collection that contains the community feature enabled as the SharePoint farm account, sometimes an extra System Account user appears in the Community Members list.
  Workaround:

  Manually remove the extra user from the list.
- When you copy a site or site collection, inactive users become active users on the target.
- When you copy tasks with multiple versions, the Predecessors property, which appears in the version history, can be incorrect.
- When you copy an Image list, picture thumbnails do not appear.
- If you enabled the Record Center feature, sometimes thumbnails for some of the copied items do not appear.
- When you copy a project tasks item or list, the Attachment icon is not displayed in the default view.
- Fast site collection creation is not supported. Sites masters are hidden in the tree view.
- Fields from list templates must exist on both the source and target to be copied.

Mounting backups by using the NetWorker User for Microsoft GUI

Procedure

1. Open the NetWorker User for Microsoft GUI.
2. Select **Options** > **Recover Session Options**.

3. In the **Recover Options** dialog box, perform the following steps:

   a. On the **NetWorker** tab, clear the **Use Microsoft Best Practices for selecting the SharePoint Configuration Data** option.

   b. On the **SharePoint Granular Level Recovery** tab, specify the following fields:

   Note

   The **SharePoint Granular Level Recovery** tab appears only if the backups of SharePoint content databases are GLR-compatible.

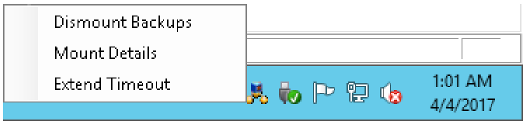
   - **Specify drive letter or path where SharePoint backup will be mounted**: In this field, the default mount path of the content databases that was created in the registry during the installation appears. To specify a different path, either type the path or click **Browse**, and then select a folder. Databases that are mounted for GLR include the original folder hierarchy from the NWFS-based virtual drive.
   - **Specify amount of time to leave SharePoint backup mounted**: From this list, select the number of hours, after which the mounted SharePoint backup must be dismounted. The default value is **8** hours.

   c. Click **OK**.

4. In the NetWorker User for Microsoft GUI, on the **Recover** tab page, click the **Browse** tab.
5. Expand **APPLICATIONS**, expand **SharePoint Farm**, and then select the web application that contains the content database that you want to mount.
6. In the right panel, right-click the content database that you want to mount, and then select **Mount SharePoint backup for Granular Level Recovery**.

   If the mount operation succeeds, the Mount Service icon is added to the system tray.

   Figure 6 Mount Service system tray icon

7. To view the status of the mount operation, in the NetWorker User for Microsoft GUI, click the **Monitor** tab.

Viewing mount details

You can view the mount details by using either the NetWorker User for Microsoft GUI or the Mount Service system tray icon. The Mount Service icon appears in the system tray only if the databases or backups are mounted by using the **Mount SharePoint backup for Granular Level Recovery** or **Mount/Launch EMC ItemPoint for Granular Level Recovery** options. Mounting backups by using the NetWorker User for Microsoft GUI on page 41 and Performing GLR by using the EMC ItemPoint for Microsoft SharePoint Server GUI on page 43 provide information about these options.

Viewing mount details by using the NetWorker User for Microsoft GUI

Procedure

1. Open the NetWorker User for Microsoft GUI.
2. On the **Recover** tab page, click the **Browse** tab.
3. Expand **APPLICATIONS**, expand **SharePoint Farm**, and then select the web application that contains the content database, the mount details of which you want to view.
4. In the right panel, right-click the content database, the mount details of which you want to view, and then select **Mount Details**.
5. In the **Mount Details** dialog box, review the information, and then click **OK**.

   Note

   In the **Mount Details** dialog box, the **MountPath** column provides the complete mount path that you can specify in the ItemPoint for SharePoint Server GUI when you manually start it to perform a GLR.

Viewing mount details by using the Mount Service system tray icon

Procedure

1. In the system tray, right-click the Mount Service icon, and then select **Mount Details**.
2. In the **Mount Details** dialog box, review the information.

   To refresh the information, click **Refresh**.

3. Click **OK**.

Performing GLR by using the EMC ItemPoint for Microsoft SharePoint Server GUI

To perform SharePoint GLRs, use the EMC ItemPoint for Microsoft SharePoint Server GUI. ItemPoint uses a SQL Server database that is restored by using NMM directed recovery or mounted by using NetWorker virtual file system as the source for GLR. You can open the EMC ItemPoint for Microsoft SharePoint Server GUI either manually after mounting backups or by using NMM. You cannot use the NetWorker User for Microsoft GUI till you close the EMC ItemPoint for Microsoft SharePoint Server GUI.

Before you begin

Ensure that you meet the following prerequisites:

- You started the ItemPoint ACTS on the target SharePoint Server.
- The temporary file path contains sufficient storage space.
  You specify the temporary file path in the **Data Wizard** of the EMC ItemPoint for Microsoft SharePoint Server GUI. The temporary file path is used during the copy operation of the restore.

Procedure

1. Open the NetWorker User for Microsoft GUI.
2. On the **Recover** tab page, click the **Browse** tab.

3. Expand **APPLICATIONS**, expand **SharePoint Farm**, and then select the web application that contains the content database that you want to mount and perform GLR.
4. In the right panel, right-click the content database that you want to mount and perform GLR, and then select **Mount/Launch EMC ItemPoint for Granular Level Recovery**.

   If the database or backup is mounted, this step only opens the **Data Wizard** in the EMC ItemPoint for Microsoft SharePoint Server GUI. Otherwise, this step mounts the database or backup, and then opens the **Data Wizard** in the EMC ItemPoint for Microsoft SharePoint Server GUI.

5. On the **Source Path Selection** page:

   a. If the **Temporary File Path** field is empty, type the path to temporarily stage the restored data before moving it to the target SharePoint Server.

      ItemPoint saves the path. For subsequent GLRs, the path automatically appears in the **Temporary File Path** field.

      ItemPoint automatically adds the source files from the NMM GUI to the **Source Files** field.

   b. Click **Next**.
6. On the **Target Server Selection** page:

   a. In the **SharePoint Server Site URL** field, type the URL of the target SharePoint Server.

      You can also select the URL from the list. However, validate the URL that you select because it can change.

      The most recently used URL appears in this field by default.

   b. Specify the authentication information.

   c. Click **Next**.

Extending timeout of a mounted backup

You can extend the timeout of a mounted backup or database by using either the NetWorker User for Microsoft GUI or the Mount Service system tray icon. The Mount Service icon appears in the system tray only if the databases or backups are mounted by using the **Mount SharePoint backup for Granular Level Recovery** or **Mount/ Launch EMC ItemPoint for Granular Level Recovery** options. Mounting backups by using the NetWorker User for Microsoft GUI on page 41 and Performing GLR by using the EMC ItemPoint for Microsoft SharePoint Server GUI on page 43 provide information about these options.

Extending timeout of a mounted backup by using the NetWorker User for Microsoft GUI

Procedure

1. Select **Options** > **Recover Session Options**.
2. In the **Recover Options** dialog box, click the **SharePoint Granular Level Recovery** tab.
3. From the **Specify amount of time to leave SharePoint backup mounted** list, select the number of hours, for which you want to extend the timeout of the mounted backup. The default value is **8** hours.

Extending timeout of a mounted backup by using the Mount Service system tray icon

Procedure

1. In the system tray, right-click the Mount Service icon, and then select **Extend Timeout**.
2. In the **Extend Timeout** dialog box, from the **Extend Timeout** list, select the number of hours, for which you want to extend the timeout of the mounted backup. The default value is **8** hours.
3. Click **OK**.
4. In the **Change Expire Time** dialog box, click **Yes**.

Dismounting backups

After a recovery completes, you can either manually dismount backups or leave them to be dismounted after the timeout. The **Specify amount of time to leave SharePoint backup mounted** field on the **SharePoint Granular Level Recovery** tab of the **Recover Options** dialog box in the NetWorker User for Microsoft GUI contains the timeout value.
The backups are automatically dismounted under any of the following circumstances:

- The NetWorker server or client is changed.
- The NetWorker User for Microsoft GUI is refreshed.
- The backup time is changed.
- The mount is timed out.
- The host is restarted.

Dismounting backups by using the NetWorker User for Microsoft GUI

Procedure

1. Open the NetWorker User for Microsoft GUI.
2. On the **Recover** tab page, click the **Browse** tab.
3. Expand **APPLICATIONS**, expand **SharePoint Farm**, and then select the web application that contains the content database that you want to dismount.
4. In the right panel, right-click the content database that you want to dismount, and then select **Dismount SharePoint backup**.
5. In the **SharePoint Granular Level Recovery** dialog box, click **Yes**.

Dismounting backups by using the Mount Service system tray icon

Procedure

1. In the system tray, right-click the Mount Service icon, and then select **Dismount Backups**.
2. In the **Dismount Backups** dialog box, click **Yes**.

Performing a GLR of a Remote BLOB Storage

A Remote BLOB Storage (RBS) enables you to store BLOB data, such as streaming videos, image files, and sound clips, outside a SQL Server database. When you enable an RBS for SQL Server data in a SharePoint environment, and then back up the data by using NMM, you can perform a GLR of the data by using NMM and ItemPoint for SharePoint Server.

Before you perform a GLR of an RBS, ensure that you meet the following prerequisites:

- Configure the content database to use the RBS with the FILESTREAM.
  To configure the RBS, you must enable the FILESTREAM provider on the SQL Server.
- Install the RBS provider on the SQL Server.
- Install the RBS provider on all the SharePoint Servers.
- Run the required PowerShell cmdlets to enable the content database to use the RBS.

Note

Microsoft documentation and RBS vendor documentation provide information about how to perform these tasks.

To perform a GLR of the RBS, perform the following tasks:

1. Back up the RBS by using the NetWorker File System plug-in.
   The *NetWorker Administration Guide* provides information.
2. Perform a full backup of SharePoint databases by using NMM.
3. Perform a directed recovery of content databases by using NMM.
4. Perform a GLR by using the EMC ItemPoint for Microsoft SharePoint Server GUI.
   The *ItemPoint for SharePoint Server User Guide* provides information.

CHAPTER 5

Microsoft SQL Server Scheduled Backups

This chapter includes the following sections:

Prerequisites

Review the prerequisites in this section before performing a SQL Server VSS scheduled backup.

- Start the SQL Server VSS Writer service and ensure that all the databases are online. Offline databases are not backed up, and if a database is offline, no warning appears during the backup operation.
- Ensure that a database name in a SQL Server VSS instance does not contain either leading or trailing spaces. Use the following command to locate the presence of spaces in front or at the end of database names:

  ```
  SELECT database_id as DatabaseID, '##'+name+'##' as DatabaseName
  from sys.databases
  ```

  Example output:

  ```
  DatabaseID DatabaseName

  8 ##AdventureWorks## -- DB name is fine

  15 ##  DBWithLeadingSpace## -- DB name contains leading
  spaces

  17 ##DBWithTrailingSpace ## -- DB name contains trailing
  spaces
  ```
- View the valid application data save sets by using the `nsrnmmsv -P` command.

Supported backup settings for SQL Server 2012 and later Availability Group

NMM supports the **AUTOMATED_BACKUP_PREFERENCE** and **BACKUP PRIORITY** settings for AlwaysOn Availability Groups of SQL Server 2012 and later. You can configure the settings by using either the Microsoft SQL Server Management Studio or the Transact-SQL commands. The Microsoft SQL Server documentation provides information about the settings, and how to configure them.

Configuring scheduled backups

To configure a scheduled backup, you must configure a client resource. Before you configure a client resource, perform the following tasks:

- Configure a backup pool
- Configure a backup schedule
- Configure a protection policy

The *NetWorker Module for Microsoft Administration Guide* provides information about scheduled backups and data protection policies.

Note

If you use NetWorker Server 8.2.3 or later and NMM 9.1 or later, perform the steps that the "Microsoft SQL Server Scheduled Backups" chapter in the *NetWorker Module for Microsoft for SQL and SharePoint VSS 8.2 SP1 User Guide* describes. NMM 19.1 compatibility with NetWorker 8.2.3 or 8.2.4 servers on page 20, Using NetWorker server 8.2.3 or later and NMM 19.1 on page 20, and the *NetWorker 8.2 SP1 Administration Guide* provide additional information.

Configuring client resources

The *NetWorker Module for Microsoft Administration Guide* provides information.

Procedure

1. Open NMC.
2. In the **Administration** page, click **Protection**.
3. In the expanded left pane, select **Clients**.
4. From the **File** menu, select **New**.
5. Click the **General** tab.
6. In the **Name** field, type the fully qualified hostname of the NetWorker client.

   If you are backing up a SQL clustered instance, use the virtual SQL Server name here. Create client resources for all the physical cluster nodes where the SQL clustered instance is being run.

7. In the **Comment** field, type a description. If you are creating multiple client resources for the same NetWorker client host computer, use this attribute to differentiate the purpose of each resource.
8. For the **Retention Policy** field, select a retention policy from the list. The retention policy determines the time period during which the rolled-over data is available, although not necessarily quickly.
9. Select the **Scheduled Backups** field.
10. In the **Save Set** field, specify the save set name listed in the table.

Table 8 Backup type and save set name

Backup type	Save set
SQL Server full backup	`APPLICATIONS:\SqlServerWriter`

SQL Server named instance backup	`APPLICATIONS:\SqlServerWriter\host%5Cinstance`
	For example, to back up a SQL Server that is named instance MT11\BU, type the following:
	`APPLICATIONS:\SqlServerWriter\MT11%5CBU\`

SQL Server individual database backup	`APPLICATIONS:\SqlServerWriter\host%5Cinstance\<database name>` For example, to back up an individual database TestDB12, type the following:

Table 8 Backup type and save set name (continued)

Backup type	Save set
	`APPLICATIONS:\SqlServerWriter` `\MT11%5CBU\TestDB12`

11. In the **Group** field, select the backup group that was configured.
12. Click the **Apps & Modules** tab.
13. In the **Access** area:
    - For cluster setups of all SQL Server versions and stand-alone setups of SQL Server 2012, type the **Remote user** and **Password**.
    - For stand-alone setups for SQL Server versions other than SQL Server 2012, leave the **Remote user** and **Password** fields empty.
14. In the **Backup command** field, type the backup command: `nsrnmmsv.exe`.
15. In the **Globals (1 of 2)** tab:
    - Click **OK**. The alias names are automatically listed in the **Aliases** field.
    - Complete the other attributes, as required.
16. Click **OK**.

Performing federated backups on SQL setups that have AlwaysOn Availability Group configured

You can use NMM to perform federated backup not only for databases configured with AAG but also for databases not configured with AAG. The backups are taken using a single client (cluster host) so that multiple backups are not spawned on the same client. However, non-AAG databases are indexed against the host name, and the AAG databases are indexed against the AG listener name.

Create client resources for the federated backups by using the NMC, as described in the "Configuring client resources" section. Use the AG listener as the backup resource. Create client resources for SQL nodes and SQL virtual server. Ensure that the client resources do not belong to any group. You can use these client resources to create indexes of non-AAG databases.

NOTICE

NMM 19.1 does not support SQL Server 2017 VSS read-scale (clusterless) availability group and domain independent (domainless) availability group configurations.

Procedure

1. On the SQL host that hosts the primary replica, run the following command:

   ```
   nsrnmmsv -P
   ```

2. Create a client resource for the Windows Cluster name that hosts the SQL instances.
3. Add all the listed save sets that belong to the AlwaysOn Availability Group instance to the client resource by running the `nsrnmmsv -P` command.

4. In the **Application Information** field of the client resource, type `NSR_FEDERATED_BACKUP=yes`.

CHAPTER 6

Microsoft SQL Server Recovery

This chapter includes the following sections:

Restoring SQL Server data in a stand-alone environment

During a system databases recovery, NMM automatically detects and stops the SQL Server services for the SQL database instances. After the system databases recovery completes, NMM automatically starts the SQL Server services for the SQL Server database instances.

Procedure

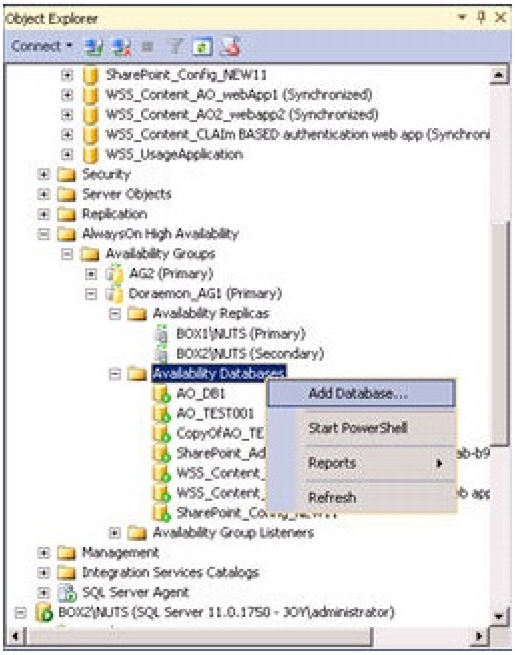
1. Open the NetWorker User for Microsoft GUI.
2. From the navigation tree, expand the **Applications** folder and the **SQLServerWriter** folder.
3. Select the databases to recover.
4. From the **SharePoint and SQL Server Recover Session** toolbar, click **Start Restore**.

Restoring SQL Server Always-On Availability Group databases

Federated backups are indexed against the Availability Group Listener. The indexing enables you to consolidate backups from multiple clients under a single client.

1. Ensure that the AlwaysOn Availability Group is a primary replica on the host, from which the AlwaysOn Availability Group databases were backed up. The hostname or the replica for the relevant SQL Server instance, from which the databases were backed up, appears in the **Path** field in the NMM GUI.
   If the backed up host instance is not a primary replica, fail over the AlwaysOn Availability Group to the replica, from which the databases were backed up.
2. Restore the databases.
3. On the servers that host the secondary replicas of the AlwaysOn Availability group, delete the restored databases that are in the restoring state.
4. Join or re-add the databases to the AlwaysOn Availability Group by using the **full join** method:
   a. Open the Microsoft SQL Server Management Studio.
   b. In the **Object Explorer** panel, right-click the **Availability Databases**, and then select **Add Database to Availability Group**.
      The **Add Database to Availability Group** dialog box appears.

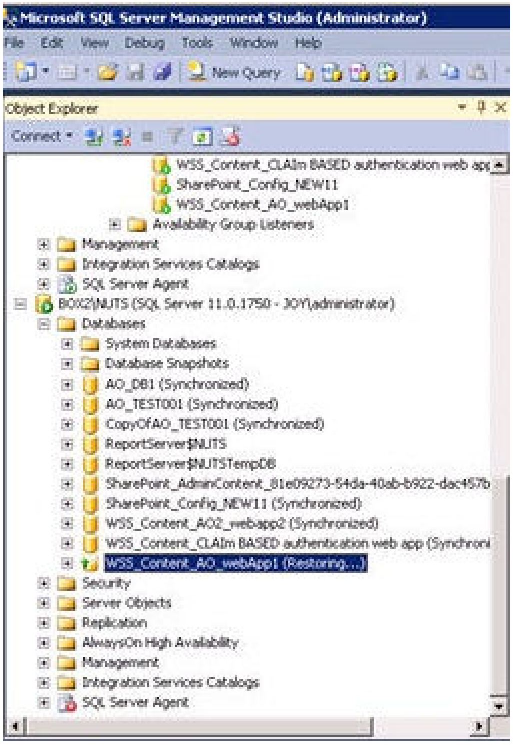
Figure 7 Add Database to Availability Group dialog box



c. On the **Select Databases** page, select the databases, and then click **Next**.

d. On the **Select Initial Data Synchronization** page, select **Full**, specify the synchronization location, and then click **Next**.
If a secondary replica copy with the same name exists, the synchronization can fail. If the synchronization fails, delete the secondary replica copy that is in the restoring mode, and then validate.

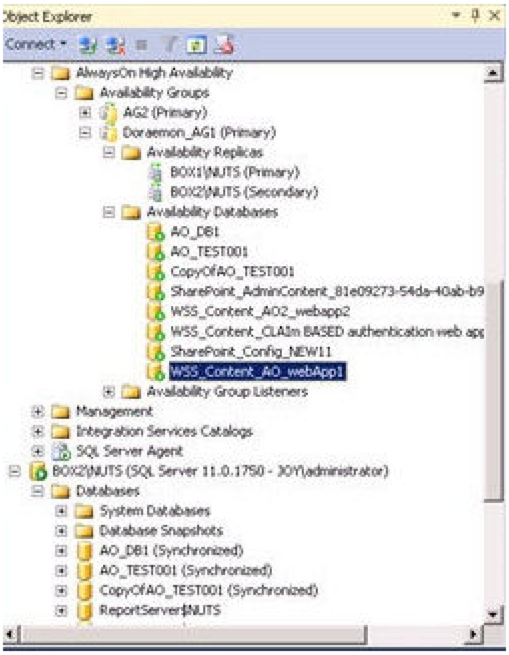
Figure 8 Secondary replica copy in restoring mode


Microsoft SQL Server Management Studio (Administrator)
File Edit View Debug Tools Window Help
New Query
Object Explorer
Connect

```
            WSS_Content_CLAIm BASED authentication web app
            SharePoint_Config_NEW11
            WSS_Content_AO_webApp1
          Availability Group Listeners
    Management
    Integration Services Catalogs
    SQL Server Agent
  BOX2\NUTS (SQL Server 11.0.1750 - JOY\administrator)
    Databases
      System Databases
      Database Snapshots
      AO_DB1 (Synchronized)
      AO_TEST001 (Synchronized)
      CopyOfAO_TEST001 (Synchronized)
      ReportServer$NUTS
      ReportServer$NUTSTempDB
      SharePoint_AdminContent_81e09273-54da-40ab-b922-dac457b
      SharePoint_Config_NEW11 (Synchronized)
      WSS_Content_AO2_webapp2 (Synchronized)
      WSS_Content_CLAIm BASED authentication web app (Synchroni
      WSS_Content_AO_webApp1 (Restoring...)
    Security
    Server Objects
    Replication
    AlwaysOn High Availability
    Management
    Integration Services Catalogs
    SQL Server Agent
```

The databases are added to the AlwaysOn Availability Group.

Figure 9 Content database added back to the AlwaysOn Availability Group



```
    AlwaysOn High Availability
      Availability Groups
        AG2 (Primary)
        Doraemon_AG1 (Primary)
          Availability Replicas
            BOX1\NUTS (Primary)
            BOX2\NUTS (Secondary)
          Availability Databases
            AO_DB1
            AO_TEST001
            CopyOfAO_TEST001
            SharePoint_AdminContent_81e09273-54da-40ab-b9
            WSS_Content_AO2_webapp2
            WSS_Content_CLAIm BASED authentication web app
            SharePoint_Config_NEW11
            WSS_Content_AO_webApp1
          Availability Group Listeners
    Management
    Integration Services Catalogs
    SQL Server Agent
  BOX2\NUTS (SQL Server 11.0.1750 - JOY\administrator)
    Databases
      System Databases
      Database Snapshots
      AO_DB1 (Synchronized)
      AO_TEST001 (Synchronized)
      CopyOfAO_TEST001 (Synchronized)
      ReportServer$NUTS
```

CHAPTER 7

Microsoft SQL Server Directed Recovery

This chapter includes the following sections:

Overview of SQL Server directed recovery

You can perform a SQL Server directed recovery to either of the following destinations that must have NMM installed:

- The same host, which is in either the same location or a different location
- A different host

When you perform a SQL Server directed recovery to a different host, the host can:

- Be a SQL server, web front-end server, or a file server.
- Be either part of or separate from the farm where the backup was performed.
- Either have or not have SharePoint or SQL services.

NMM does not support the following types of directed recovery:

- Directed recovery of:
  - Filestream database
  - Transparent Data Encryption (TDE) enabled database
- Directed recovery to:
  - Encrypted target
  - Compressed drive
    Although the recovery takes place, the database attachment fails.
- Directed recovery of SQL system databases to a different host

Prerequisites

- When performing a directed recovery to a different host:
  - Recover all database files to a single drive.
  - Ensure that the SQL database is marked on the client host, where directed recovery browsing is performed. Otherwise, the SQL tab does not appear for directed recovery browsing.
  - Ensure that you have added the source and target hosts as client resources in NMC.
- Ensure that the recovery drive is available, and has sufficient disk space to accommodate the data.
- For directed recovery of multiple databases, recover one database at a time. You can specify separate recovery paths for each database.
- For non-system database directed recovery, the SQL Server service can be in either the stop or start state.

Performing SQL Server directed recovery

Procedure

1. On the host where you perform the recovery, open the NetWorker User for Microsoft GUI.

   The NetWorker server that contains SQL backups is selected.

2. To select a different NetWorker server:

a. Click the icon beside **NetWorker server: <server_name>**.

The **Change NetWorker Server** dialog box appears.

b. To refresh the list of NetWorker servers, click **Update Server List**.

c. Select the NetWorker server, and then click **OK**.

3. Specify the target location to perform a directed recovery:
   - To perform a directed recovery to another host, specify the alternate SQL Server client:
     a. Click **Options** > **Configure Options**.
     b. In the **Configure Options** dialog box, click the button beside the **Client name** field.
     c. In the **Select Viewable Clients** dialog box, from the **Available clients on** list, select the SQL Server client, and then click **Add** to move the SQL Server client to the **Clients to list on menu bar** list.
     d. Click **OK**.
     e. From the **Client** list, select the SQL Server client that you added.
   - To perform a directed recovery to the same host, specify the same SQL Server client.
4. In the middle panel, on the **Browse** tab, expand **APPLICATIONS** > **SqlServerWriter**, and then select the databases that you want to recover.
5. Click **Recover Options**.
6. In the **Recover Options** dialog box, on the **SQL** tab:

   a. Select **Perform SQL Directed Restore**.

   b. Select one of the following options:
   - **Restore SQL files to local machine using their original directory path**: Performs the directed recovery to the source path.
   - **Specify the file system path where the SQL database(s) should be restored**: Performs the directed recovery to the path that you specify in the text box.
     To specify the path, click **Browse**.

     In the **Browse for Folder** dialog box, select the path, and then click **OK**.

   Note

   You cannot perform a directed recovery to the same source location.

   c. Click **OK**.
7. Click **Recover**.
8. On the **Recovery Summary** page, review the summary, and then click **Start Recover**.
9. To view the status of the recovery, click the **Monitor** tab.

After you finish

1. Copy the recovered database files, such as .mdf, .ldf, and .ndf files to the required location, which can be on either the same drive or a different drive.

2. Attach the database files to the databases:
   a. Open the SQL Server Management Studio.
   b. Connect to the SQL Server instance.
   c. In the Object Explorer pane, right-click the databases node, and then select **Attach**.
      The **SQL Attach Database** dialog box appears.
   d. Specify the primary database file to attach.
      After the primary database file is attached, if all the other database files are in the same location, the SQL Server automatically identifies them.

      If the other database files are not in the same location, specify their corresponding locations.
   e. Click **OK**.

Examples of log messages in the NMM log file and the Monitor page

This section contains example messages that appear in the NMM log file and the **Monitor** page.

Example messages that appear in the NMM log file and the **Monitor** page for recovery to the original location are as follows:

- `Command line:\n C:\Program Files\EMC NetWorker\nsr\bin \nsrnmmrc.exe -A RESTORE_TYPE_ORDER=conventional -A BR_ELEVATED_WARNING=true -s mb-nwsvr-1.baker.legato.com -c mb-clnt-3.belred.legato.com -A NSR_SNAP_TYPE=vss -A NSR_SQL_RECOVER_MODE=alt_location -A NSR_SQL_TARGET_ORIG=yes -I -`
- `nsrnmmrc: flag=A arg=NSR_SQL_RECOVER_MODE=alt_location`
- `nsrnmmrc: flag=A arg=NSR_SQL_TARGET_ORIG=yes`
- `NMM .. Performing SQL directed restore.`
- `NMM .. SQL directed restore will relocate database files to their original locations.`

Example of messages that appear in the NMM log file and the **Monitor** page for recovery to a user-defined location are as follows:

- `Command line:\n C:\Program Files\EMC NetWorker\nsr\bin \nsrnmmrc.exe -A RESTORE_TYPE_ORDER=conventional -A BR_ELEVATED_WARNING=true -s mb-nwsvr-1.baker.legato.com -c mb-clnt-3.belred.legato.com -A NSR_SNAP_TYPE=vss -A NSR_SQL_RECOVER_MODE=alt_location -A NSR_SQL_TARGET_DIR=E:\ -I -`
- `nsrnmmrc: flag=A arg=NSR_SQL_RECOVER_MODE=alt_location`
- `nsrnmmrc: flag=A arg=NSR_SQL_TARGET_DIR=E:\`
- `NMM .. Performing SQL directed restore.`
- `NMM .. SQL directed restore will relocate database files to path[E:\].`

- `NMM .. SQL directed restore relocating database files for database [APPLICATIONS:\SqlServerWriter\MB-CLNT-3\AcmeBank].`
- `NMM .. SQL directed recover, relocating file [C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA\AcmeBank.mdf] to [E:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA\AcmeBank.mdf].`
- `NMM .. SQL directed recover, relocating file [C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA\AcmeBank_log.ldf] to [E:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA\AcmeBank_log.ldf].`
- `NMM .. SQL directed recover, relocating file [C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA\AcmeBank2.mdf] to [E:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA\AcmeBank2.mdf].`

CHAPTER 8

Windows Bare Metal Recovery Solution

This chapter includes the following sections:

SQL Server in a stand-alone environment

This section provides the BMR backup and recovery procedures for SQL Server in a stand-alone environment.

Backing up a SQL Server for BMR

Configure a SQL Server client resource to back up SQL Server for BMR.

Creating client resources by using the NetWorker Client Backup Configuration Wizard

Create separate client resources to back up the application data and the file system data. The client resource for the file system data must include the `ALL` save set.

Creating a client resource by using the Client Backup Configuration wizard on page 26 provides information about how to create a client resource to back up the application data.

The "Creating a client resource with the Client Backup Configuration Wizard" section in the *NetWorker Administration Guide* provides information about how to create a client resource to back up the file system data.

Creating client resources by using the Client Properties dialog box

Create separate client resources to back up the application data and the file system data. The client resource for the file system data must include the `ALL` save set.

Procedure

1. In the Administration view of NMC, create a policy, a workflow, a group, and an action for SQL Server.

   The "Data Protection Policies" chapter in the *NetWorker Administration Guide* provides information.

2. Create a client resource to back up the `ALL` save set:

   a. In the **NetWorker Administrator** window, click **Protection**.

   b. In the expanded left panel, right-click **Clients** and select **New**.

   The **Create Client** dialog box appears.

   c. On the **General** tab:

      a. In the **Name** field, type the hostname of the client resource.

      b. In the **Group** list, select the group that you created in step 1.

      c. In the **Save set** field, type **`ALL`**.

   d. On the **Apps & Modules** tab, ensure that the **Backup command** and **Application information** fields are clear.

   e. Specify other fields according to the requirements.

   f. Click **OK**.

3. Perform the backup.

   Ensure that the backup successfully completes.

4. Create a client resource to back up the `APPLICATIONS:\SqlServerWriter` save set:

   a. In the **NetWorker Administrator** window, click **Protection**.

   b. In the expanded left panel, right-click **Clients** and select **New**.

      The **Create Client** dialog box appears.

   c. On the **General** tab:

      a. In the **Name** field, type the hostname of the client resource.

      b. In the **Group** list, select the group that you created in step 1.

      c. In the **Save set** field, type **`APPLICATIONS:\SqlServerWriter`**.

   d. On the **Apps & Modules** tab, in the **Backup command** field, type **`nsrnmmsv`**.

   e. Specify other fields according to the requirements.

   f. Click **OK**.

5. Perform the backup.

   Ensure that the backup successfully completes.

Performing BMR of a standalone SQL Server

The BMR process recovers only the `C:` drive. It does not recover the SQL data, quorum and SQL cluster drives, or the system databases such as master, msdb, and model.

Procedure

1. Perform the procedures that the "Performing a Windows BMR recovery to physical or virtual computers" section in the *NetWorker Administration Guide* describes.
2. Start the NMM GUI.
3. Select the server and click **Recover**.
4. Under the `APPLICATIONS` save set, select **SqlServerWriter**.
5. Perform the recovery.
6. Ensure that the SQL Server service starts for the recovered instance.
7. To verify whether you have recovered the databases, open SQL Server Management Studio and connect to the instance. The databases that belong to the instance appear.
8. Build the msdb and model databases:

   a. Start the physical nodes of the cluster.

   b. Ensure that you have the SQL Server installation software on the active node.

   c. In the software, go to the folder where the SETUP file exists and run the following command:

      ```
      Setup/QUIET/ACTION=REBUILDDATABASE/INSTANCENAME=SQL Server
      instance name/SQLSYSADMINACCOUNTS=Domain\administrator
      username/IAcceptSQLServerLicenseTerms
      ```

Refer to Microsoft documentation for information about how to rebuild the SQL Server system databases:

Table 9 Rebuilding SQL Server system databases

SQL Server version	Microsoft article
SQL Server 2016	https://msdn.microsoft.com/en-us/library/dd207003(v=sql.130).aspx
SQL Server 2014	https://msdn.microsoft.com/en-us/library/dd207003(v=sql.120).aspx
SQL Server 2012	https://msdn.microsoft.com/en-us/library/dd207003(v=sql.110).aspx
SQL Server 2008 R2 SQL Server 2008	https://msdn.microsoft.com/en-us/library/dd207003(v=sql.100).aspx

SQL Server in a cluster environment

This section provides the bare-metal recovery (BMR) backup and recovery procedures for SQL Server by using the VSS technology in a cluster environment.

Backing up a SQL Server for BMR

Configure a SQL Server client resource to back up SQL Server for BMR.

Creating client resources by using the NetWorker Client Backup Configuration Wizard

Create separate client resources to back up the application data and the file system data. The client resource for the file system data must include the `ALL` save set.

The section Creating a client resource by using the Client Backup Configuration wizard on page 26 provides information about how to create a client resource to back up the application data.

The "Creating a client resource with the Client Backup Configuration Wizard" section in the *NetWorker Administration Guide* provides information about how to create a client resource to back up the file system data.

Creating client resources by using the Client Properties dialog box

Create separate client resources to backup the application data and the file system data. The client resource for the file system data must include the `ALL` save set.

This procedure uses the following sample SQL Server configuration:

- You have installed SQL Server on cluster volume `P:\`.
- The cluster quorum drive is `E:\`.
- You have clustered all the drives except the `C:\` drive in the cluster.

Procedure

1. In the Administration view of NMC, create a policy, a workflow, a group, and an action for SQL Server.

   The "Data Protection Policies" chapter in the *NetWorker Administration Guide* provides information.

2. Create a client resource to back up the `ALL` save set on the active node:

   a. In the **NetWorker Administrator** window, click **Protection**.

   b. In the expanded left panel, right-click **Clients** and select **New**.

   c. In the **Create Client** dialog box:

      a. In the **Name** field, type the name for the active node.

      b. In the **Group** list, select the group that you created in step 1.

      c. In the **Save set** field, type **`ALL`**.

      d. Specify other fields according to the requirements.

      e. Click **OK**.

3. Perform the backup.

   Ensure that the backup successfully completes.

4. Perform steps 2 and 3 for the passive node.

   Note

   When you perform step 2ca, in the **Name** field, type the name for the passive node.

5. Perform steps 2 and 3 for the quorum drive.

   Note

   When you perform step 2ca, in the **Name** field, type the name for the Windows cluster.

6. Perform steps 2 and 3 for the SQL cluster drives.

   Note

   When you perform step 2ca, in the **Name** field, type the SQL virtual name.

7. Create a client resource with SQL virtual name to back up the SQL application data:

   a. In the **NetWorker Administrator** window, click **Protection**.

   b. In the expanded left panel, right-click **Clients** and select **New**.

      The **Create Client** dialog box appears.

   c. On the **General** tab:

      a. In the **Name** field, type the SQL virtual name.

      b. In the **Group** list, select the group that you created in step 1.

      c. In the **Save set** field, type **`APPLICATIONS:\SqlServerWriter`**.

   d. On the **Apps & Modules** tab, in the **Backup command** field, type **`nsrnmmsv`**.

   e. Specify other fields according to the requirements.

f. Click **OK**.

8. Create dummy client resources for the physical nodes of the cluster.
9. Perform the backup.

   Ensure that the backup successfully completes.

Performing BMR of a SQL Server cluster

The BMR process recovers `C:` drive only. It does not recover the SQL data, the quorum and SQL cluster drives, and the system databases such as master, msdb, and model.

Procedure

1. Separately recover the active and passive nodes by performing the procedures that the "Performing a Windows BMR recovery to physical or virtual computers" section in the *NetWorker Administration Guide* describes.
2. Recover the cluster quorum database:

   a. After you have started the active and passive nodes, ensure that the cluster disks are online on the active node in the Disk Management Console of the Windows GUI.

   b. Add the quorum drive to Failover Cluster Management of the Cluster Configuration UI.

   c. Select the storage node in Failover Cluster Management and ensure that the quorum disk is online.

   d. On the SQL Server active node, start the NetWorker User program.

   e. Click **Recover**.

   f. In the **Source Client** dialog box, select the source client with the Windows cluster name, and click **OK**.

   g. In the **Destination Client** dialog box, select the destination client with the active node name, and click **OK**.

   h. Select the quorum drive and recover the drive.
3. Recover the SQL cluster drives:

   a. Add the SQL drives to Failover Cluster Management of the Cluster Configuration UI.

   b. Ensure that the disk is online.

   c. Configure the drive mount points between the drives so that the mount points are the same as the mount points during the backup.

   d. On the SQL Server active node, start the NetWorker User program.

   e. Click **Recover**.

   f. In the **Source Client** dialog box, select the source client with the SQL virtual name and click **OK**.

   g. In the **Destination Client** dialog box, select the destination client with the active node name and click **OK**.

   h. Select all the SQL cluster drives and recover the drives.
4. Build the msdb and model databases:

a. Start the physical nodes of the cluster.

b. Ensure that you have the SQL Server installation software on the active node.

c. In the software, go to the folder where the SETUP file exists and run the following command:

```
Setup/QUIET/ACTION=REBUILDDATABASE/INSTANCENAME=SQL Server
instance name/SQLSYSADMINACCOUNTS=Domain\administrator
username/IAcceptSQLServerLicenseTerms
```

Refer to Microsoft documentation for information about how to rebuild the SQL Server system databases. The following table provides links to relevant Microsoft documentation for various versions of SQL Server.

Table 10 Rebuilding SQL Server system databases

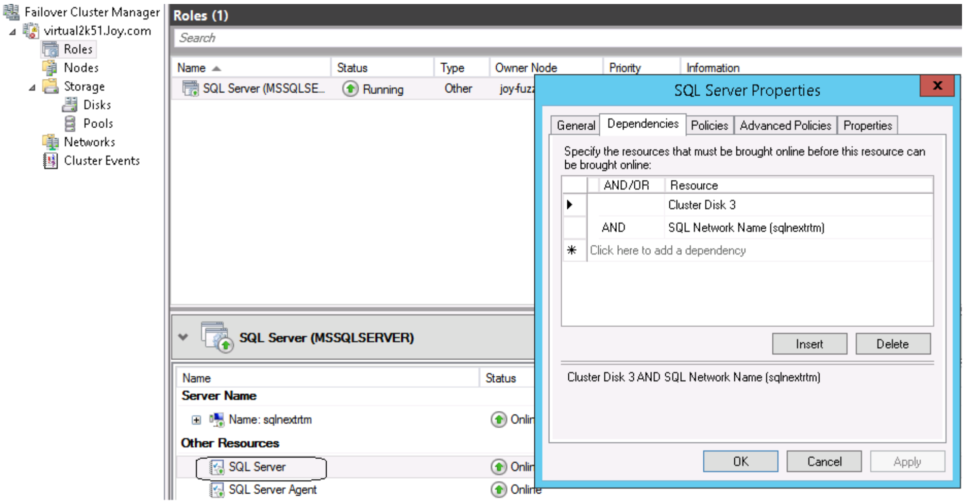
SQL Server version	Microsoft article
SQL Server 2016	https://msdn.microsoft.com/en-us/library/dd207003(v=sql.130).aspx
SQL Server 2014	https://msdn.microsoft.com/en-us/library/dd207003(v=sql.120).aspx
SQL Server 2012	https://msdn.microsoft.com/en-us/library/dd207003(v=sql.110).aspx
SQL Server 2008 R2 SQL Server 2008	https://msdn.microsoft.com/en-us/library/dd207003(v=sql.100).aspx

5. In the **Failover Cluster Management** window of the Cluster Configuration UI, perform the following steps:

a. Open the **SQL Server Properties** dialog box.

The following figure shows the **SQL Server Properties** dialog box.

Figure 10 SQL Server Properties dialog box



Specify the resources that must be brought online before this resource can be brought online:

	AND/OR	Resource
▶		Cluster Disk 3
	AND	SQL Network Name (sqlnextrtm)
✳	Click here to add a dependency	

Cluster Disk 3 AND SQL Network Name (sqlnextrtm)

b. On the **Dependencies** tab, add all the SQL Server dependencies that you must bring online before you bring the SQL Server online. For example, add any dependent cluster disk.

c. Bring the SQL virtual resources online.

d. Bring the SQL Server online.

e. Perform the failover and ensure that the failover is successful.

6. Restore the databases by using the NetWorker User for Microsoft GUI:

a. Open the NetWorker User for Microsoft GUI.

b. Select the SQL Server and relevant SQL virtual server instance, and then click **Recover**.

c. On the **Recover** tab page, click the **Browse** tab.

d. Expand **APPLICATIONS**, and then select **SqlServerWriter**.

e. Perform the restore operation.

f. After the restore operation completes, ensure that the SQL Server service starts for the recovered instance.

SharePoint Server BMR

This section provides the BMR backup and recovery procedures for SharePoint Server 2013, SharePoint Server 2016, and SharePoint Server 2019. The backup and recovery procedures for all these SharePoint versions are the same.

Note

NMM 9.1 and later do not support the BMR backup and recovery of SharePoint stand-alone server with SQL embedded and SQL Server Express Edition.

Sample SharePoint farm configuration

Use the NetWorker Administrator program to create SharePoint Server client resources to back up SharePoint Server for BMR.

The following table provides the sample SharePoint 2013 farm configuration that the procedures use.

Table 11 Sample SharePoint Server 2013 configuration

Components	Operating system	Application version	Critical volume	NetWorker build
SQL Server	Windows Server 2012 R2 SP1	SQL Server 2014	• SQL application is installed on the C: drive. • Databases reside on the C: drive.	NetWorker 9.1 and later
Web front-end server 1		SharePoint Server 2013 SP1	SharePoint Server 2013 Application is installed on C: drive.	

Table 11 Sample SharePoint Server 2013 configuration (continued)

Components	Operating system	Application version	Critical volume	NetWorker build
Web front-end server 2		SharePoint Server 2013 SP1	SharePoint Application is installed on the `E:` drive. So, the critical volumes are the `C:` and `E:` drives.	

The SharePoint Server 2013 backup includes SQL Server, Web front-end server 1, and Web front-end server 2 backups.

Backing up SharePoint Server

This section provides information about how to backup SharePoint Server.

Backing up SharePoint Server comprises backing up the following servers:

- SQL Server in a SharePoint Server environment
- Web front-end server 1
- Web front-end server 2

Backing up SQL Server in a SharePoint Server environment

Procedure

1. By using the NetWorker Administration GUI, create the first policy, workflow, group, and action for the SQL Server.

   The "Data Protection Policies" chapter in the *NetWorker Administration Guide* provides information.

2. Create the first client resource for the SQL Server:

   a. In the **NetWorker Administrator** window, click **Protection**.

   b. In the expanded left panel, right-click **Clients** and select **New**.

   c. In the **Create Client** dialog box:

      a. In the **Name** field, type the name for the client resource.

      b. Ensure that you have selected **Scheduled backup**.

      c. In the **Group** list, select the group that you created in step 1.

      d. In the **Save set** field, type **`ALL`**.

      e. Specify other fields according to the requirements.

      f. Click **OK**.

3. In the **NetWorker Administrator** window, select the **View** tab and select **Diagnostic Mode**.

4. Perform the backup.

   Ensure that the backup successfully completes.

5. By using the NetWorker Administration GUI, create the second policy, workflow, group, and action for the SQL Server.

   The "Data Protection Policies" chapter in the *NetWorker Administration Guide* provides information.

6. Create the second client resource for the SQL Server.

   a. In the **NetWorker Administrator** window, click **Protection**.

   b. In the expanded left panel, right-click **Clients** and select **New**.

      The **Create Client** dialog box appears.

   c. On the **General** tab:

      a. In the **Name** field, name for the client resource.

      b. Ensure that you have selected **Scheduled backup**.

      c. In the **Group** list, select the group that you created in step 5.

      d. In the **Save set** field, type `APPLICATIONS:\SqlServerWriter`.

   d. On the **Apps & Modules** tab, in the **Backup command** field, type `nsrnmmsv`.

   e. Specify other fields according to the requirements.

   f. Click **OK**.

7. In the **NetWorker Administrator** window, select the **View** tab and select **Diagnostic Mode**.

8. Perform the backup.

   Ensure that the backup successfully completes.

Backing up web front-end server 1

Perform the steps that Backing up SQL Server in a SharePoint Server environment on page 71 describes.

Note

When you perform step 6cd, in the **Save set** field, type `APPLICATIONS:\Microsoft Office SharePoint Services` instead of `APPLICATIONS:\SqlServerWriter`.

Backing up web front-end server 2

The steps to perform the BMR backup of web front-end server 2 are the same as the steps in Backing up web front-end server 1 on page 72.

Performing BMR of SharePoint Server

This section describes the recovery procedures for SQL Server, web front-end server 1, and web front-end server 2.

Recovering SQL Server in a SharePoint Server environment

Note

The failure of a SQL master database recovery leads to the failure of the SharePoint disaster recovery. To continue with recovery, move, rename, or delete the specified database files and perform the recovery from that point. The associated files are the master database file `master.mdf`, and the master log file `mastlog.ldf`.

Procedure

1. Perform the procedures that the "Performing a Windows BMR recovery to physical or virtual computers" section in the *NetWorker Administration Guide* describes.
2. After SQL Server restarts:
   a. Start the NMM GUI.
   b. Select the server and click **Recover**.
   c. In the **APPLICATIONS** save set, select **SqlServerWriter**.
   d. Perform the recovery.
   e. Restart the host if prompted.
   f. Start the SQL Server service and verify whether all instances have started.

Recovering the web front-end servers

Procedure

1. Perform the procedures in the "Performing a Windows BMR recovery to physical or virtual computers" section of the *NetWorker Administration Guide*.
2. Use the NetWorker client to recover any other backed up file system drives. Ensure that the `DISASTER_RECOVERY:\` save set is visible in the NetWorker client GUI.
3. After web front-end server restarts:
   a. Start the NMM GUI.
   b. Select the server, and click **Recover** to recover the SharePoint configuration data.
   c. In the **APPLICATIONS** save set, select the SharePoint save sets, and perform the recovery.
   d. Restart the host if prompted.

APPENDIX A

Example Procedure for SharePoint Server Backup and Recovery

This appendix includes the following sections:

Example save sets for SharePoint farm backups

Review the examples in this section for save sets that you can use for backup of SharePoint farm components.

To view a list of the SharePoint Server 2013, SharePoint Server 2016, and SharePoint Server 2019 save sets that are available for backup, run the following command on the application server:

```
nsrnmmsv -P
```

Example 1 SharePoint Server standalone farm

A stand-alone farm, in which the host contains SharePoint Server 2013 and SQL Server Enterprise Edition. The NetWorker server backs up the following save set on the same client:

```
APPLICATIONS:\Microsoft Office SharePoint Services
```

Example 2 SharePoint Server distributed farm with two servers

A distributed farm with two servers, of which one contains the web front-end and Central Admin, and the other contains the SQL Server.

The NetWorker server has two client resources, one for each server. The WFE client resource is the primary WFE resource, and the SQL client resource is the dummy resource that are needed for successful backup and restore.

- SharePoint web front-end host save set for resource 1: `APPLICATIONS:\Microsoft Office SharePoint Services`
- SQL Server host is not configured with any save set and is not configured under any group.

Example 3 SharePoint Server distributed farm with four servers

A distributed farm with four servers:

- Server A: Runs the web front-end and the search components
- Server B: Runs only search components
- Server C: Runs only the web front-end
- Server D: SQL Server

In this example, the following save sets are backed up on each web front-end.

Table 12 Example: Required save sets to be backed up

Type of backup data	Required save sets to be backed up
Server A Server B	Take individual backups of all these save sets: `APPLICATIONS:\Microsoft Office SharePoint Services`

Example 3 SharePoint Server distributed farm with four servers (continued)

Table 12 Example: Required save sets to be backed up (continued)

Type of backup data	Required save sets to be backed up
Server C	
Server B Server C SQL Server	These nodes are created as dummy nodes for successful backup and recovery. They are not configured with any save set and are not configured under any group.

Microsoft Office SharePoint Services internally backs up the SharePoint Configuration Data, SQL Server, and Search service indexes.

Note

It is recommended that you perform backups of the NMM and the operating system in different schedules.

Recovery examples for SharePoint Server 2013

This section provides example procedures that supplement the information on SharePoint Server recovery in Microsoft SharePoint Server Recovery. The procedures with detailed step-by-step instructions help you through the recovery process for SharePoint Server 2013.

In the example procedure, the SharePoint distributed farm has a SharePoint Server 2013 SP1 and a SQL Server, and consists of:

- An application server `SP2013-WFE1`, which contains:
  - SharePoint Server 2013 SP1 and Central Administration
  - NMM client
- A web front-end server `SP2013-WFE3`, which contains:
  - SharePoint Server 2013 SP1
  - NMM client
- A supported version of SQL Server that contains NMM client

In a SharePoint distributed farm that has a SharePoint Server 2013 SP1 and a SQL Server 2014 configured with the AlwaysOn Availability Group functionality, there are two additional nodes - `clus107` and `clus109` of a SQL Server 2014 cluster. Each node contains SQL Server 2014 with AlwaysOn Availability Group functionality and NMM client. `clus107` is configured as the primary replica. `clus109` is configured as the secondary replica.

`http://sp2013-wfe1:1/sites/site1` is the website, for which a SharePoint farm is used.

Considerations for Microsoft SharePoint

Review the following considerations when recovering Microsoft SharePoint data from save sets:

- Microsoft SharePoint farm level recovery: If you are performing a Microsoft SharePoint farm level restore, restoring from any WFE node in the farm restores the data for entire SharePoint farm.
- Microsoft SharePoint content database level recovery: If you are performing a Microsoft SharePoint content database level restore, perform the following steps:
  1. Select **Recover options**, select **NetWorker** tab.
  2. Clear the **Use Microsoft best practices for selecting the SharePoint Configuration Data** option.
  3. Select the relevant content database from any node of the SharePoint farm and restore.

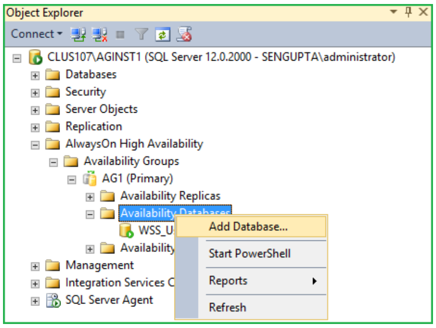
Configuring SQL Server 2014 AlwaysOn Availability Groups

Perform the required steps before you restore of the content database, for example `WSS_Content_1`, on the SQL Server node.

Procedure

1. Perform recoveries as described in the following sections:
   - Restoring deleted individual items from document library
   - Restoring deleted search service application
   - Restoring deleted web application
2. After the recoveries succeed, go to the SQL Server Management Studio, and then add `WSS_Content_1` back to Availability Group.

   Figure 11 Add database

3. Right-click the **Availability Databases** and select the **Add Database to Availability Group** option.

   The **Add Database to Availability Group** dialog box appears.
4. On the **Select Databases** page, select `WSS_Content_1`, and then click **Next**.
5. On the **Select Initial Data Synchronization** page, select the **Full** option, specify the synchronization location, and then click **Next**.
6. If a secondary replica with same name exists, the synchronization fails, and displays an error.
7. Delete the secondary replica that is in restoring mode.
8. Rerun the validation.

   `WSS_Content_1` is added back to Availability Group.

9. Return to the NMM GUI on the application server or web front-end as applicable, and then click **Continue** in the dependency dialog box. Perform the remaining steps as described in the following sections:
    - Restoring deleted individual items from document library for list item.
    - Restoring deleted search service application
    - Restoring deleted web application

Restoring deleted individual items from document library

In this example, the content database `WSS_Content_1` that contains the list item is deleted from the website `http://sp2013-wfe1:1/sites/site1`, and then restored.

Microsoft SharePoint Server Scheduled Backups provides information about backing up a SharePoint farm.

Deleting a list item
Use the Central Administration to delete the content database `WSS_Content_1` that contains the list item. The content database and its list item are deleted.

Restoring individual items that were deleted from document library
You must perform the required steps to restore the list item that is deleted.

1. Open the NetWorker User for Microsoft GUI on the application server `sp2013-wfe1` to start the recovery.
2. Select the **Recover** options, select **NetWorker** tab. Clear the **Use Microsoft best practices for selecting the SharePoint Configuration Data**. Select the relevant content database from any node of the SharePoint farm and restore.
3. Click **Recover**.
4. Configuring SQL Server 2014 AlwaysOn Availability Groups on page 78 provides steps to restore SharePoint Server 2013 SP1 by using SQL Server 2014 that is configured with the AlwaysOn Availability Group.
5. After the recovery, go to the Central Administration, and check whether the list item is restored to the website `http://sp2013-wfe1:1/sites/site1`.

Restoring deleted search service application

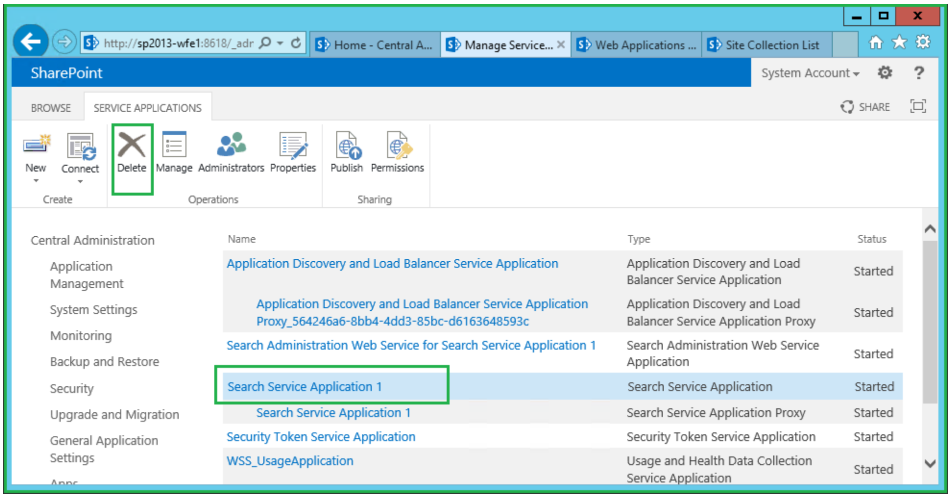
In this example, the search service application is deleted and then restored. When the search service application is deleted, the associated content database and website are also deleted.

Microsoft SharePoint Server Scheduled Backups provides information about backing up a SharePoint farm.

Deleting a search service application
Perform the required steps on the application server.

1. Go to the **SharePoint Central Administration** > **Application Management** > **Service Applications**.
2. Delete the search service application "Search Service Application 1" by using the **Delete** button.

Figure 12 Delete search service application



Name	Type	Status
Application Discovery and Load Balancer Service Application	Application Discovery and Load Balancer Service Application	Started
Application Discovery and Load Balancer Service Application Proxy_564246a6-8bb4-4dd3-85bc-d6163648593c	Application Discovery and Load Balancer Service Application Proxy	Started
Search Administration Web Service for Search Service Application 1	Search Administration Web Service Application	Started
Search Service Application 1	Search Service Application	Started
Search Service Application 1	Search Service Application Proxy	Started
Security Token Service Application	Security Token Service Application	Started
WSS_UsageApplication	Usage and Health Data Collection Service Application	Started

3. Note the name of the search index.

Restoring the deleted Search Service Application

Perform the required steps to restore the Search Service Application that is deleted.

1. Open the NetWorker User for Microsoft GUI on the application server 2010farm-cnadm to start the recovery process.
2. Select **SharePoint Configuration Data** and **SharePoint Farm**.
3. Click **Recover**.
4. On the **Recovery Summary** page, click **Start Recover**.
   After the recovery completes, a dialog box that contains the message "`The system must be rebooted to complete the recovery process. Would you like to reboot now?`" appears.
5. Click **Yes**.
6. Go to the SharePoint Central Administration and check that the search service application is restored.
7. Go to the SharePoint Central Administration and check that the deleted data is restored.

Restoring deleted web application

This section provides an example procedure to delete and restore a SharePoint Server 2013 SP1 web application.

Configuring SQL Server 2014 AlwaysOn Availability Groups on page 78 provides steps to restore SharePoint Server 2013 SP1 by using SQL Server 2014 that is configured with the AlwaysOn Availability Group.

Microsoft SharePoint Server Scheduled Backups provides information about how to back up a SharePoint farm.

Deleting a web application

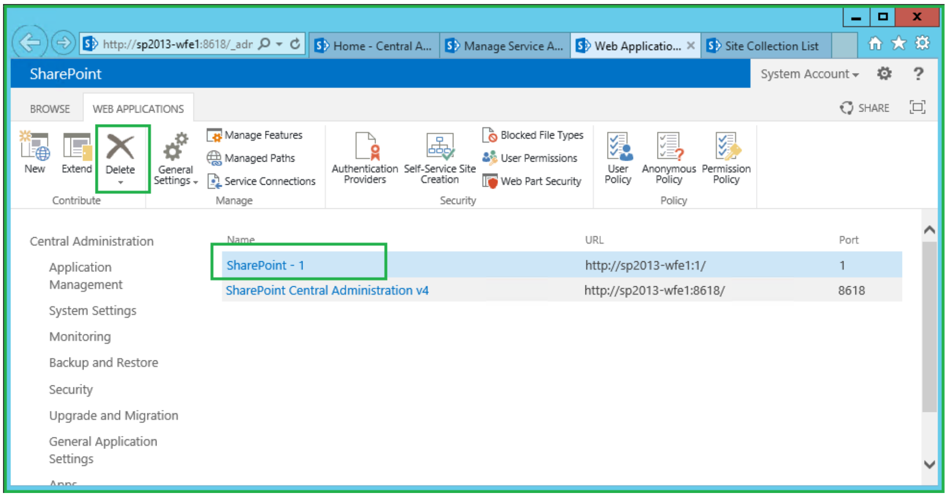
Perform the required steps on the application server.

Procedure

1. Go to **Central Administration** > **Application Management** > **Web Applications**.

2. Select the web application `SharePoint - 1`, and then click **Delete**. When the web application is deleted, the associated content database and website are also deleted.

Figure 13 Delete web application



Name	URL	Port
SharePoint - 1	http://sp2013-wfe1:1/	1
SharePoint Central Administration v4	http://sp2013-wfe1:8618/	8618

Restoring a deleted web application

Perform the required steps to restore the web application, and associated content database and website.

Procedure

1. Open the NetWorker User for Microsoft GUI on the application server `SP2013-WFE1` to start the recovery process.
2. Select **Options** > **Recover Session Options**.
3. In the **Recover Options** dialog box, on the **NetWorker** tab, select the **Use Microsoft Best Practices for selecting the SharePoint Configuration Data** option, and then click **OK**.
4. In the NetWorker User for Microsoft GUI, on the navigation tree:

   a. Expand `APPLICATIONS:\SharePoint Farm`.

   b. Select the deleted web application.

   c. Click **Recover**.
5. In the **Recovery Summary** dialog box, click **Start Recover**.
6. Configuring SQL Server 2014 AlwaysOn Availability Groups on page 78 provides steps to restore SharePoint Server 2013 SP1 by using SQL Server 2014 that is configured with the AlwaysOn Availability Group.
7. After the recovery, go to the Central Administration, and then check whether the web application is restored.

APPENDIX B

Example Procedure for SharePoint Web Application Directed Recovery

This appendix includes the following sections:

Introduction

The current NMM software design does not support recovery of `C:\Inetpub/IIS` for a web application. A full recovery of a farm results in recovery of all the web applications to a point-in-time. However, the user may want to recover only one web application.

This can be achieved by performing additional steps during directed recovery of web applications. By performing these additional steps, one web application can be recovered without affecting the data of another web application.

The instructions in the appendix are applicable for SharePoint Server 2013, SharePoint Server 2016, and SharePoint Server 2019.

In the example procedure, the SharePoint distributed farm has two SharePoint Server 2013 nodes and a SQL Server 2014 cluster, and consists of:

- An application server `2013farm-cnadm`
- A pure web front-end server `2013farm-wfe`
- A SQL Server active node `clus16`
- A SQL Server passive node `clus18`

NetWorker client and NMM are installed on the application server, web front-end server, SQL Server active node, and SQL Server passive node.

In the example procedure, two web applications that are named **`SharePoint - 3`** and **`SharePoint - 4`**, are created. **`SharePoint - 4`** is corrupted and must be recovered. A new web application that is named **`SharePoint - dr`** is created and through directed recovery, the data of the corrupted web application **`SharePoint - 4`** is recovered to **`SharePoint - dr`**.

Performing a directed recovery of a web application

This section provides an example procedure for directed recovery of a web application.

Procedure

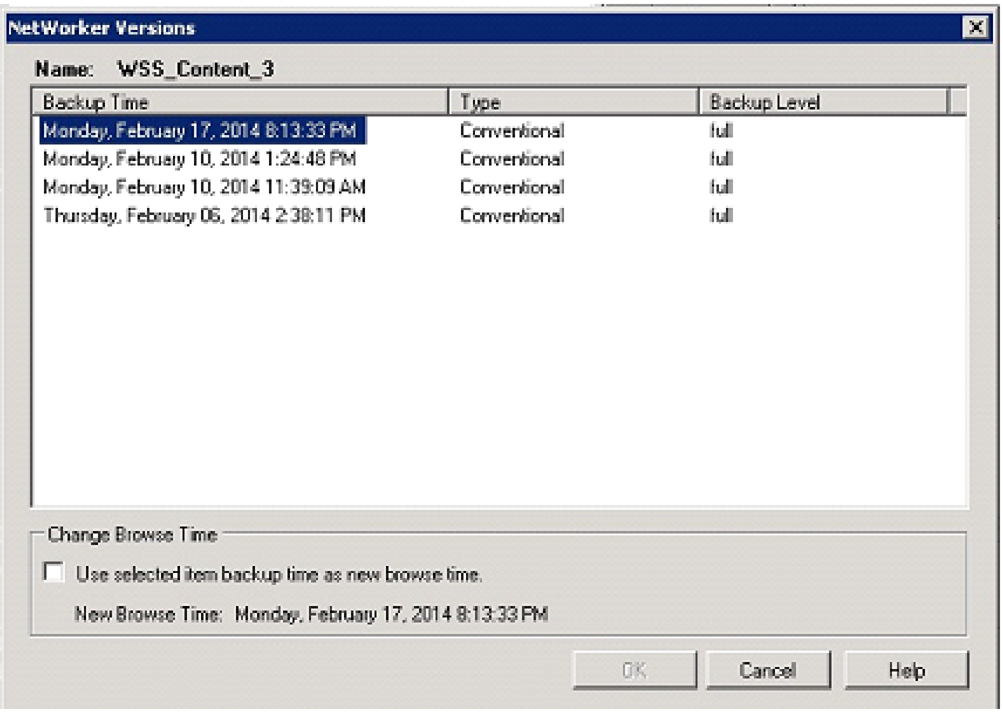
1. Create two web applications: **`SharePoint - 3`** and **`SharePoint - 4`**.

   Back up the SharePoint data with 706 documents each in five site collections of size 300 KB each in SharePoint - 3 web application and 353 documents each in 10 site collections of size 300 KB each in **`SharePoint - 4`** web application.

   The content databases for **`SharePoint - 3`** and **`SharePoint - 4`** web applications are respectively **`WSS_Content_3`** and **`WSS_Content_4`**.

   The highlighted text shows the backup version.

Figure 14 The backed up content database



Name: WSS_Content_3

Backup Time	Type	Backup Level
Monday, February 17, 2014 8:13:33 PM	Conventional	full
Monday, February 10, 2014 1:24:48 PM	Conventional	full
Monday, February 10, 2014 11:39:09 AM	Conventional	full
Thursday, February 06, 2014 2:38:11 PM	Conventional	full

☐ Use selected item backup time as new browse time.

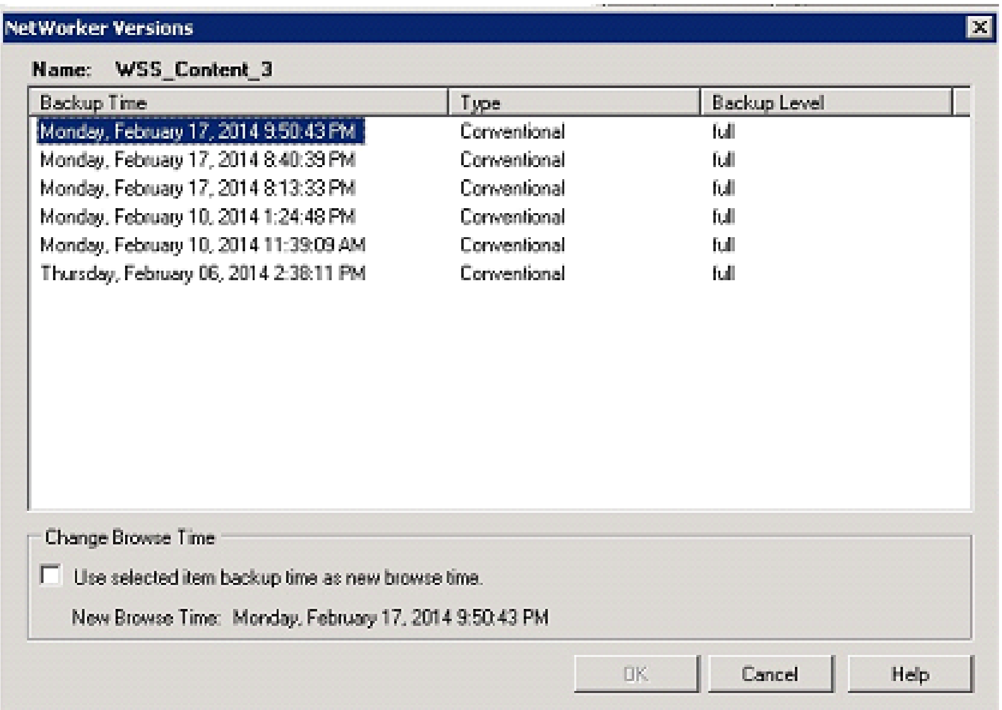
New Browse Time: Monday, February 17, 2014 8:13:33 PM

2. Upload five additional documents to one site collection in each of the two web applications and perform a second full backup.

   Similarly, upload five additional documents to one site collection in each of the two web applications and perform a third full backup.

   There are now three backups (dated February 17, 2014) for `SharePoint - 3` web application.

Figure 15 Three backups for SharePoint - 3 web application



Name: WSS_Content_3

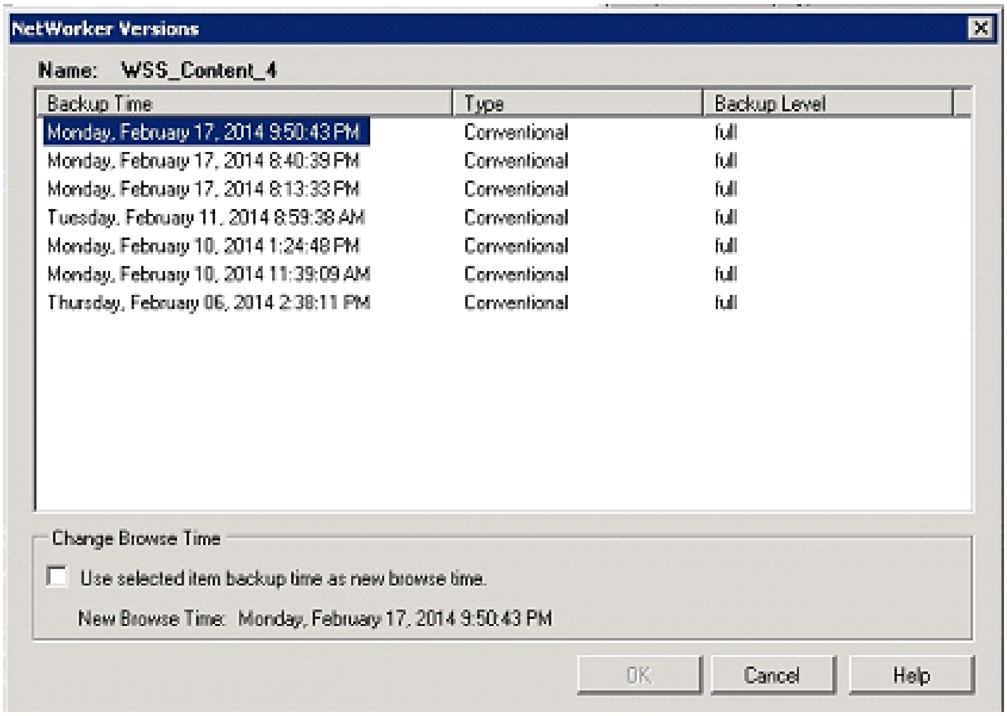
Backup Time	Type	Backup Level
Monday, February 17, 2014 9:50:43 PM	Conventional	full
Monday, February 17, 2014 8:40:39 PM	Conventional	full
Monday, February 17, 2014 8:13:33 PM	Conventional	full
Monday, February 10, 2014 1:24:48 PM	Conventional	full
Monday, February 10, 2014 11:39:09 AM	Conventional	full
Thursday, February 06, 2014 2:38:11 PM	Conventional	full

☐ Use selected item backup time as new browse time.

New Browse Time: Monday, February 17, 2014 9:50:43 PM

There are three backups (dated February 17, 2014) for `SharePoint - 4` web application.

Figure 16 Three backups for SharePoint - 4 web application



Name: WSS_Content_4

Backup Time	Type	Backup Level
Monday, February 17, 2014 9:50:43 PM	Conventional	full
Monday, February 17, 2014 8:40:39 PM	Conventional	full
Monday, February 17, 2014 8:13:33 PM	Conventional	full
Tuesday, February 11, 2014 8:59:38 AM	Conventional	full
Monday, February 10, 2014 1:24:48 PM	Conventional	full
Monday, February 10, 2014 11:39:09 AM	Conventional	full
Thursday, February 06, 2014 2:38:11 PM	Conventional	full

Change Browse Time

☐ Use selected item backup time as new browse time.

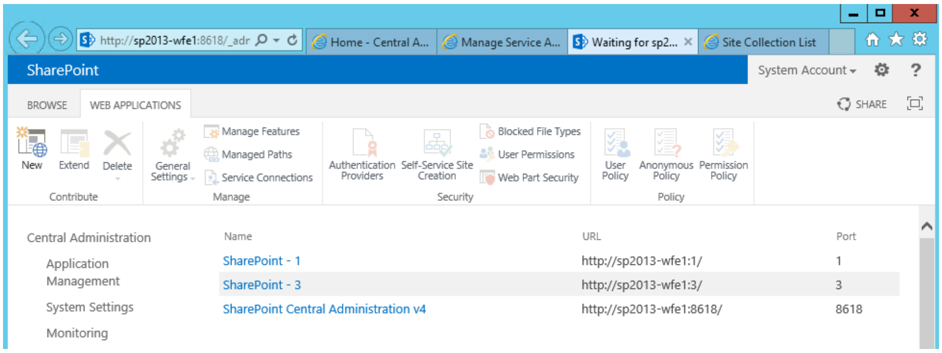
New Browse Time: Monday, February 17, 2014 9:50:43 PM

3. Upload additional five documents to the same site collection of the web application `SharePoint - 4`.

   Disaster strikes `SharePoint - 4` web application, and the IIS site is lost, the web application is not accessible from SharePoint Central Administration. However, the content database is available.

   The web application is not accessible from SharePoint Central Administration.

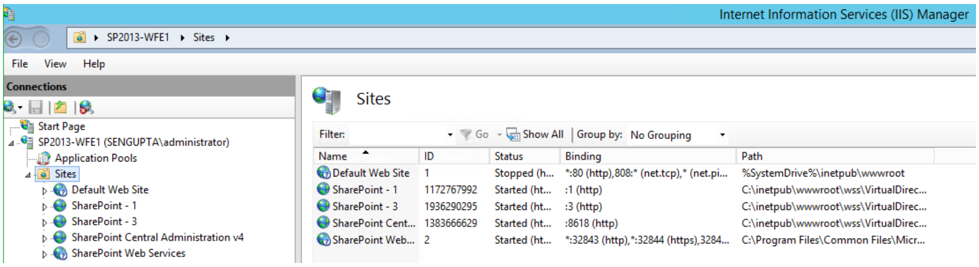
Figure 17 Web application is not accessible



Name	URL	Port
SharePoint - 1	http://sp2013-wfe1:1/	1
SharePoint - 3	http://sp2013-wfe1:3/	3
SharePoint Central Administration v4	http://sp2013-wfe1:8618/	8618

The IIS site for `SharePoint - 4` is not available.

Figure 18 IIS site for SharePoint - 4 is not available



Internet Information Services (IIS) Manager

SP2013-WFE1 ▸ Sites ▸

Connections

- Start Page
- SP2013-WFE1 (SENGUPTA\administrator)
  - Application Pools
  - Sites
    - Default Web Site
    - SharePoint - 1
    - SharePoint - 3
    - SharePoint Central Administration v4
    - SharePoint Web Services

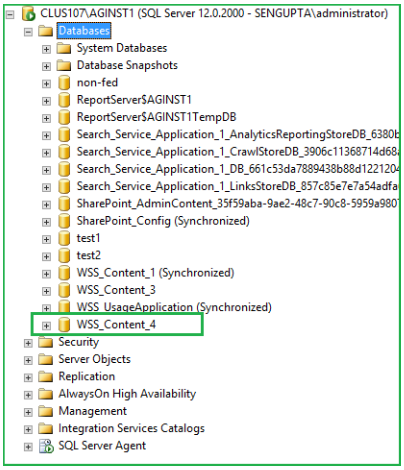
Sites

Filter: Go Show All | Group by: No Grouping

Name	ID	Status	Binding	Path
Default Web Site	1	Stopped (h...	*:80 (http),808:* (net.tcp),* (net.pi...	%SystemDrive%\inetpub\wwwroot
SharePoint - 1	1172767992	Started (ht...	:1 (http)	C:\inetpub\wwwroot\wss\VirtualDirec...
SharePoint - 3	1936290295	Started (ht...	:3 (http)	C:\inetpub\wwwroot\wss\VirtualDirec...
SharePoint Cent...	1383666629	Started (ht...	:8618 (http)	C:\inetpub\wwwroot\wss\VirtualDirec...
SharePoint Web...	2	Started (ht...	*:32843 (http),*:32844 (https),3284...	C:\Program Files\Common Files\Micr...

The content database is available for `SharePoint - 4` web application.

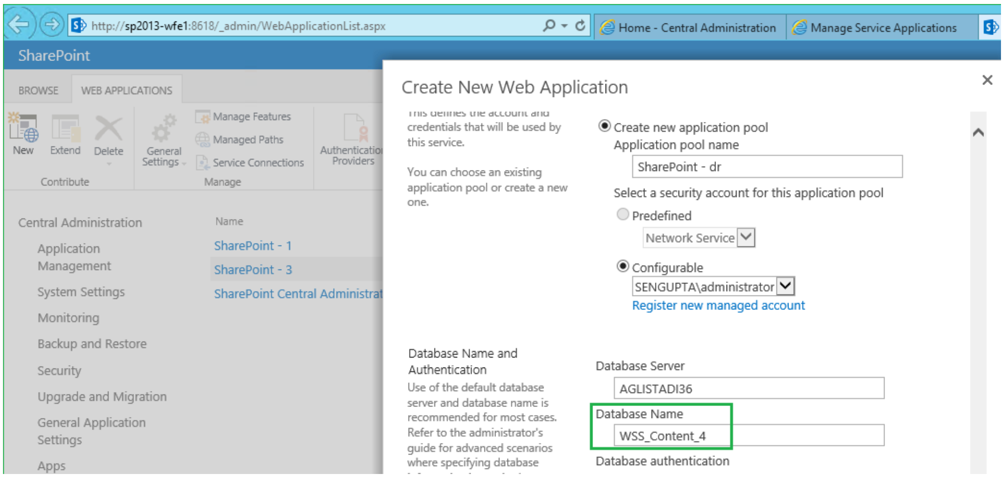
Figure 19 Content database is available



- CLUS107\AGINST1 (SQL Server 12.0.2000 - SENGUPTA\administrator)
  - Databases
    - System Databases
    - Database Snapshots
    - non-fed
    - ReportServer$AGINST1
    - ReportServer$AGINST1TempDB
    - Search_Service_Application_1_AnalyticsReportingStoreDB_6380b
    - Search_Service_Application_1_CrawlStoreDB_3906c11368714d68
    - Search_Service_Application_1_DB_661c53da7889438b88d1221204
    - Search_Service_Application_1_LinksStoreDB_857c85e7e7a54adfa
    - SharePoint_AdminContent_35f59aba-9ae2-48c7-90c8-5959a980
    - SharePoint_Config (Synchronized)
    - test1
    - test2
    - WSS_Content_1 (Synchronized)
    - WSS_Content_3
    - WSS_UsageApplication (Synchronized)
    - WSS_Content_4
  - Security
  - Server Objects
  - Replication
  - AlwaysOn High Availability
  - Management
  - Integration Services Catalogs
  - SQL Server Agent

4. Create a web application, `SharePoint - dr`, and attach the database `WSS_Content_4` to this web application. The new web application `SharePoint - dr` is created with the `WSS_Content_4` content database.

   Figure 20 New web application created

   http://sp2013-wfe1:8618/_admin/WebApplicationList.aspx

   Create New Web Application

   This defines the account and credentials that will be used by this service.

   You can choose an existing application pool or create a new one.

   ● Create new application pool

   Application pool name: SharePoint - dr

   Select a security account for this application pool

   ○ Predefined: Network Service

   ● Configurable: SENGUPTA\administrator

   Register new managed account

   Database Name and Authentication

   Use of the default database server and database name is recommended for most cases. Refer to the administrator's guide for advanced scenarios where specifying database

   Database Server: AGLISTADI36

   Database Name: WSS_Content_4

   Database authentication

5. Select the latest backup version in NetWorker User for Microsoft GUI of the application server `2013farm-cnadm`.

6. Select **Yes** when the prompted **System must be rebooted to complete the recovery process. Would you like to reboot now?**

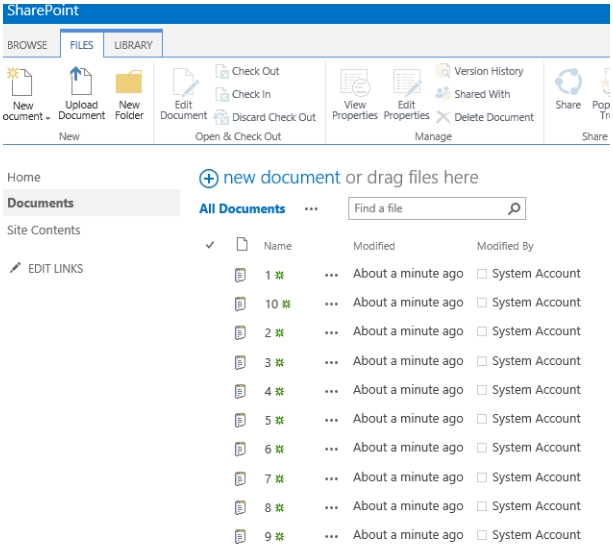
   The system is restarted after recovery of SharePoint Configuration Data.

7. Select the **Recover** options, select **NetWorker** tab. Clear the **Use Microsoft best practices for selecting the SharePoint Configuration Data**. Select the relevant content database from any node of the SharePoint farm and restore.
8. Select the content database `WSS_Content_4` and `SharePoint_Config`, and start the recovery process.

   The recovery of the content database of corrupted web application succeeds.

9. You can access the corrupted web application until the point the backup was taken. However, the last five documents that were added before disaster struck cannot be accessed.

Figure 21 SharePoint documents



Name	Modified	Modified By
1	About a minute ago	System Account
10	About a minute ago	System Account
2	About a minute ago	System Account
3	About a minute ago	System Account
4	About a minute ago	System Account
5	About a minute ago	System Account
6	About a minute ago	System Account
7	About a minute ago	System Account
8	About a minute ago	System Account
9	About a minute ago	System Account

APPENDIX C

SharePoint BLOB Backup and Recovery by using NMM and Metalogix StoragePoint

This appendix includes the following sections:

Overview of using NMM for SharePoint RBS externalized by Metalogix StoragePoint software

This appendix describes the procedure for backing up and restoring by using NMM for SharePoint RBS externalized by Metalogix StoragePoint software.

NMM supports SharePoint granular recovery for sites and items by using ItemPoint for SharePoint Server, which is aware of SharePoint RBS. ItemPoint for SharePoint Server supports recovery of SharePoint site collections, sites, and items that have BLOB content and have been externalized to tiered file system storage by using SharePoint RBS.

NOTICE

ItemPoint for SharePoint Server supports Metalogix StoragePoint 4.2.1 through 5.4.

A SharePoint farm stores both the configuration data and the content data in the SQL database. Use the RBS Metalogix software solution to externalize the BLOB store to a file system share. The RBS Metalogix software solution reduces the size of the content database that participates in the externalization process in the SQL database.

You can also use NMM SQL VSS writer, SharePoint VSS writer, and NetWorker File System technologies to provide a recovery solution for SharePoint web applications, site collections, list items, and external BLOB stores.

NMM generally supports backup and restore of SharePoint by using VSS writers only. You can extend the NetWorker File System technology to SharePoint with a few manual and additional steps. BLOB externalization reduces the size of a content database by 90-95 percentage.

RBS deployed SharePoint disaster restore solution by using NetWorker and NMM

The sample setup described in this section consists of a distributed SharePoint farm environment with the following configuration:

- SharePoint Central Administration, named 2013farm-cnadm.abc.com
- WFE, named 2013farm-wfe.abc.com
- SQL Server, named sql14vdisona.abc.com

The hostnames and external BLOB store name that are used in this sample setup are validated in the Dell EMC lab. You can configure hostnames, IP addresses, and external BLOB store name according to your requirement. You can also externalize the BLOB store outside a SQL Server.

NOTICE

It is recommended that soon after any data modification, you back up SharePoint farm, SQL Server, and BLOB store to help in disaster protection.

Configuring client resources

Procedure

1. Open the NMC.

2. Configure client resources for the SharePoint farm.
3. Configure three workflows, each containing one group and one backup action. One for the SharePoint server farm, one for the StoragePoint content database on the SQL Server, and the other to backup the BLOB store and run after a client backup completes.

   Note

   Schedule the workflows in such a way that backups on the SharePoint farm nodes are not overlapped.
   If the BLOB store is built on a non-SQL node, you must back up the non-SQL node.

4. Configure the SharePoint farm backup in one group by using the Client Backup Configuration Wizard.

   Use the SharePoint Central Administration server as the backup primary.

5. Configure another group for SQL Writer backup of StoragePoint, other databases that do not belong to the SharePoint farm, and file system backup of the BLOB store.
6. For SQL Server 2014 standalone (sql14vdisona.abc.com), configure the NMM backups for the Metalogix StoragePoint database by specifying the following fields:
   - Save set: `APPLICATIONS:\SqlServerWriter\SQL14VDISONA %5CSP13SQL14RBSM\StoragePoint`
   - Backup Command: `nsrnmmsv.exe`

   NOTICE

   In the case of data protection against a disaster, perform a SQL writer-level backup.

7. For SharePoint pure WFE (2013farm-wfe.abc.com), use the following information when configuring the NMM backups:
   - Save set: `APPLICATIONS:\Microsoft Office SharePoint Services`
   - Backup Command: `nsrnmmsv.exe`

   Note

   Back up SharePoint pure WFE only in the case of data protection against a disaster. You do not need to back up a SharePoint pure WFE as part of federated backups.

8. For each client resource that is created, configure NetWorker traditional save backups:
   - For SQL Server 2014 standalone (sql14vdisona.abc.com) external BLOB store, use the save set G:\ExtBLOBStore.
   - For SQL Server 2014 standalone (sql14vdisona.abc.com) disaster recovery backup, use the save set DISASTER_RECOVERY:\.

- For SharePoint Central Administration (2013farm-cnadm.abc.com) disaster recovery backup, use the save set DISASTER_RECOVERY:\.
- For SharePoint pure WFE (2013farm-wfe.abc.com) disaster recovery backup, use the save set DISASTER_RECOVERY:\.

Performing backups

Perform backups after you create client resources:

Procedure

1. Perform a full backup of SharePoint farm and SQL Server. The SharePoint Writer includes the SharePoint Configuration Data, SharePoint Content databases. The SQL Server backup includes the SQL and StoragePoint databases for the relevant SQL Server instance.
2. Configure a file system backup of the external BLOB store by using the file system configuration wizard.
3. Configure file system backup of the file system save sets and DISASTER_RECOVERY:\ save set on SharePoint Central Administration, SharePoint pure WFE, and SQL Server.

Restoring RBS Metalogix BLOB store

Procedure

1. Open the NetWorker User GUI.
2. Connect to the client that contains the file share.
3. Select the BLOB store that you want to restore.
4. Restore the selected BLOB store.

Performing SharePoint GLR with Metalogix RBS deployed and configured for externalizing BLOB store by using the EMC ItemPoint for Microsoft SharePoint Server GUI

This section describes the procedure to perform a GLR of an RBS-enabled content database. Ensure that you installed ItemPoint for Microsoft SharePoint Server on the SharePoint Central Administration.

The *ItemPoint for Microsoft SharePoint Server User Guide* supplements the information in this section.
The procedure in this section assumes that the BLOB store is present. Otherwise, restore the BLOB store by performing the steps that the Restoring RBS Metalogix BLOB store on page 92 describes.

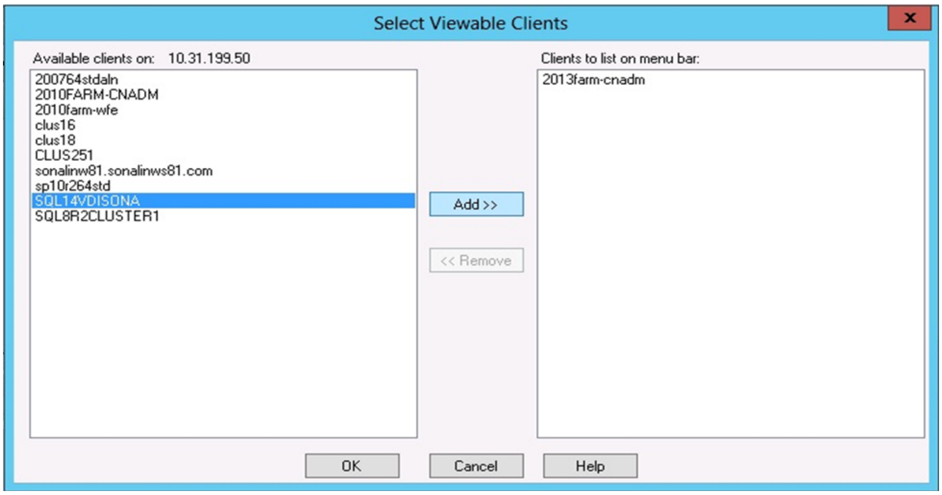
Procedure

1. Open the NetWorker User for Microsoft GUI on the host, on which you want to perform SharePoint GLR.

   In this example, you start the NetWorker User for Microsoft GUI on the SharePoint Central Administration.

2. Navigate to the **Select Viewable Clients** page and add the available SharePoint primary WFE hostname to the **Clients to list on menu bar** list to browse the SharePoint content database on the destination host. Click **OK**.

Figure 22 Select viewable clients



Available clients on: 10.31.199.50

200764stdaln
2010FARM-CNADM
2010farm-wfe
clus16
clus18
CLUS251
sonalinw81.sonalinws81.com
sp10r264std
SQL14VDISONA
SQL8R2CLUSTER1

Clients to list on menu bar:

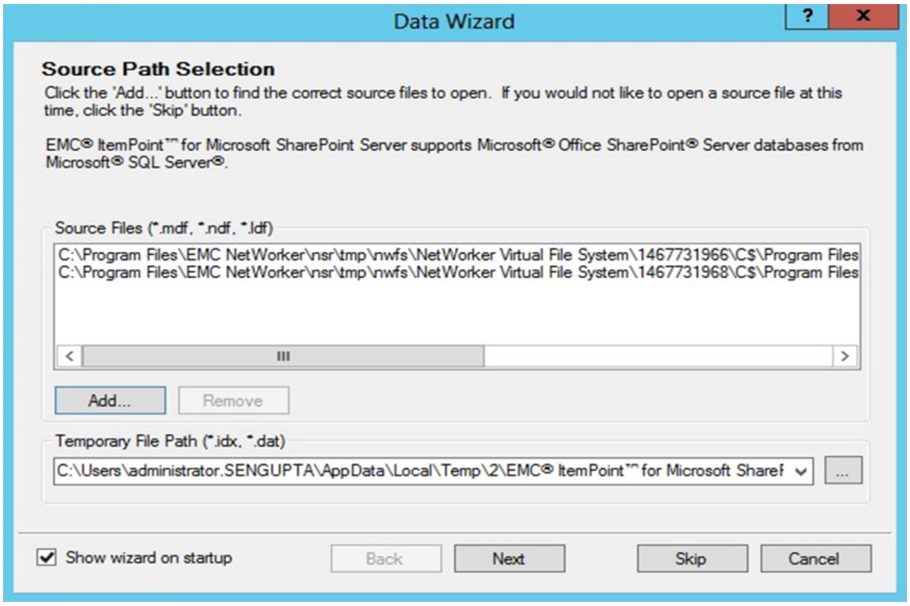
2013farm-cnadm

3. Right click the content database CD1_100, which is RBS-enabled and added to the storage profile, and select **Mount/Launch EMC ItemPoint for Granular Level Recovery.**.

   The **Data Wizard** appears.

4. On the **Source Path Selection** page, review the relevant source mdf, ldf, and ndf files, and then click **Next**.

Figure 23 Source path selection



Source Path Selection

Click the 'Add...' button to find the correct source files to open. If you would not like to open a source file at this time, click the 'Skip' button.

EMC® ItemPoint™ for Microsoft SharePoint Server supports Microsoft® Office SharePoint® Server databases from Microsoft® SQL Server®.

Source Files (*.mdf, *.ndf, *.ldf)

C:\Program Files\EMC NetWorker\nsr\tmp\nwfs\NetWorker Virtual File System\1467731966\C$\Program Files
C:\Program Files\EMC NetWorker\nsr\tmp\nwfs\NetWorker Virtual File System\1467731968\C$\Program Files

Temporary File Path (*.idx, *.dat)

C:\Users\administrator.SENGUPTA\AppData\Local\Temp\2\EMC® ItemPoint™ for Microsoft Sharef

☑ Show wizard on startup

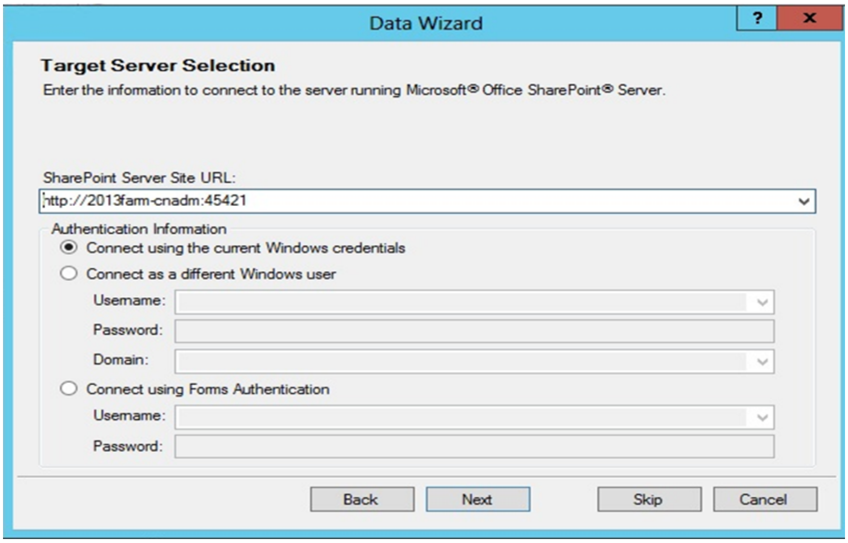
5. On the **Target Server Selection** page:

   a. From the **SharePoint Server Site URL** menu, select the URL of the SharePoint Server site.

   b. Select **Connect using the current Windows credentials**.

c. Click **Next**.

Figure 24 Target server selection



Target Server Selection

Enter the information to connect to the server running Microsoft® Office SharePoint® Server.

SharePoint Server Site URL: http://2013farm-cnadm:45421

Authentication Information

● Connect using the current Windows credentials

○ Connect as a different Windows user

Username:

Password:

Domain:

○ Connect using Forms Authentication

Username:

Password:

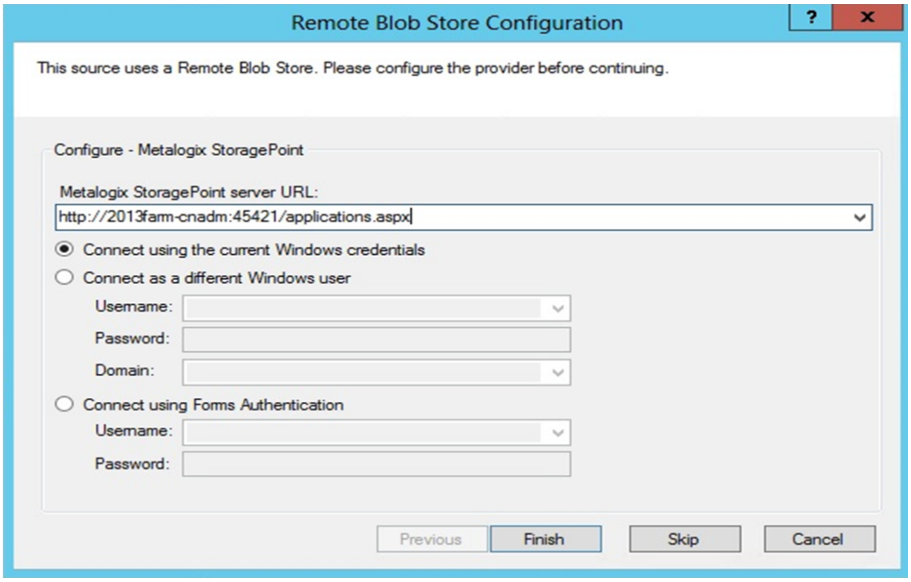
6. On the **Remote Blob Store Configuration** page:

   a. From the **Metalogix StoragePoint server URL** menu, select the URL of the Metalogix StoragePoint Server.

   b. Select **Connect using Windows credentials**.

   c. Click **Next**.

Figure 25 Remote BLOB store configuration



This source uses a Remote Blob Store. Please configure the provider before continuing.

Configure - Metalogix StoragePoint

Metalogix StoragePoint server URL: http://2013farm-cnadm:45421/applications.aspx

● Connect using the current Windows credentials

○ Connect as a different Windows user

Username:

Password:

Domain:

○ Connect using Forms Authentication

Username:

Password:

If the Metalogix StoragePoint Server URL is correct, the EMC ItemPoint for Microsoft SharePoint Server GUI appears.

7. In the EMC ItemPoint for Microsoft SharePoint Server GUI, click **File** > **Open Target**.

8. On the **Target Path Selection** page:

   a. From the **Metalogix StoragePoint server URL** menu, select the URL of the Metalogix StoragePoint Server.

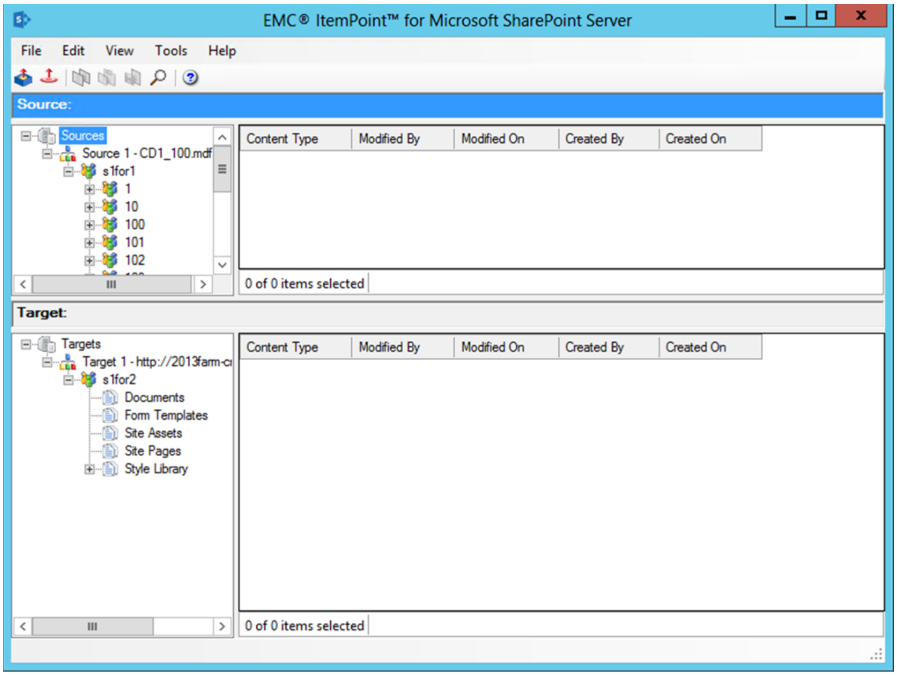
b. Select **Connect using Windows credentials**.

c. click **Next**.

9. In the EMC ItemPoint for Microsoft SharePoint Server GUI:

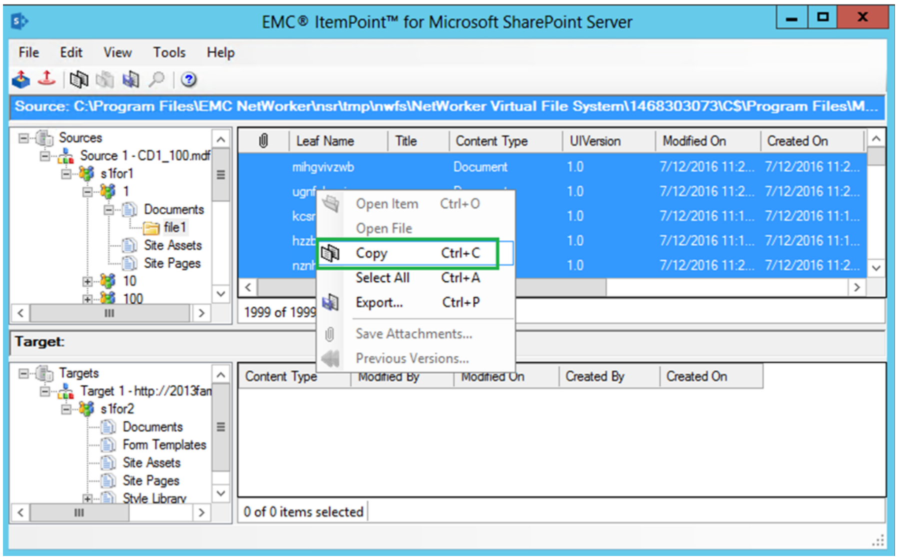
a. View the target.

Figure 26 Viewing the target



b. Copy the items from the source to a location on the target.

Figure 27 Copying items from the source



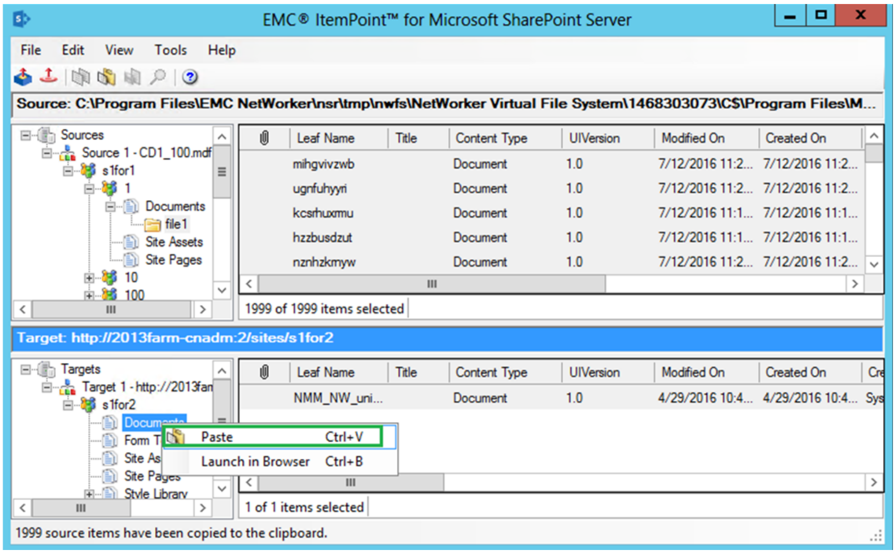
Source: C:\Program Files\EMC NetWorker\nsr\tmp\nwfs\NetWorker Virtual File System\1468303073\C$\Program Files\M...

	Leaf Name	Title	Content Type	UIVersion	Modified On	Created On
	mihgvivzwb		Document	1.0	7/12/2016 11:2...	7/12/2016 11:2...
	ugnf			1.0	7/12/2016 11:2...	7/12/2016 11:2...
	kcsr			1.0	7/12/2016 11:1...	7/12/2016 11:1...
	hzzb			1.0	7/12/2016 11:1...	7/12/2016 11:1...
	nznh			1.0	7/12/2016 11:2...	7/12/2016 11:2...

1999 of 1999

c. Paste the items to the target.

Figure 28 Pasting items to the target



Source: C:\Program Files\EMC NetWorker\nsr\tmp\nwfs\NetWorker Virtual File System\1468303073\C$\Program Files\M...

Leaf Name	Title	Content Type	UIVersion	Modified On	Created On
mihgvivzwb		Document	1.0	7/12/2016 11:2...	7/12/2016 11:2...
ugnfuhyyri		Document	1.0	7/12/2016 11:2...	7/12/2016 11:2...
kcsrhuxmu		Document	1.0	7/12/2016 11:1...	7/12/2016 11:1...
hzzbusdzut		Document	1.0	7/12/2016 11:1...	7/12/2016 11:1...
nznhzkmyw		Document	1.0	7/12/2016 11:2...	7/12/2016 11:2...

1999 of 1999 items selected

Target: http://2013farm-cnadm:2/sites/s1for2

Leaf Name	Title	Content Type	UIVersion	Modified On	Created On	Cre
NMM_NW_uni...		Document	1.0	4/29/2016 10:4...	4/29/2016 10:4...	Sys

1 of 1 items selected

1999 source items have been copied to the clipboard.

The **Copy progress** window appears.

10. After the selected number of items are successfully copied, you can close, save, or print the report.

Restoring SharePoint content databases

Perform the following steps to restore a SharePoint farm by using NMM and NetWorker file system.

Procedure

1. Delete the documents from the site collection that contains the content database CD1_100.
2. Delete the BLOB store from the share location.
3. Restore the SharePoint farm by using NMM.
4. Restore the BLOB store by using NetWorker file system.

   Restoring RBS Metalogix BLOB store on page 92 provides information.

5. On the SharePoint node, restore the relevant RBS-enabled content database to restore the relevant site collection, with which the web application under test is associated.

   Restoring single web application and content databases on page 33 provides information.

6. Verify whether all the documents are restored, the site collection is started, and the data is online.

Restoring a SharePoint farm with RBS Metalogix deployed and externalized BLOB store

Procedure

1. Delete the web application, with which the content database CD1_100 is associated.

   Delete all entries and references.

2. Delete the BLOB store from the shared location, `G:\ExtBlobStore`.
3. Restore the BLOB store.

   Restoring RBS Metalogix BLOB store on page 92 provides information.

4. On the SharePoint Server host, open the NetWorker User for Microsoft GUI, and then restore the relevant web application.

   Restoring single web application and content databases on page 33 provides information.

Note

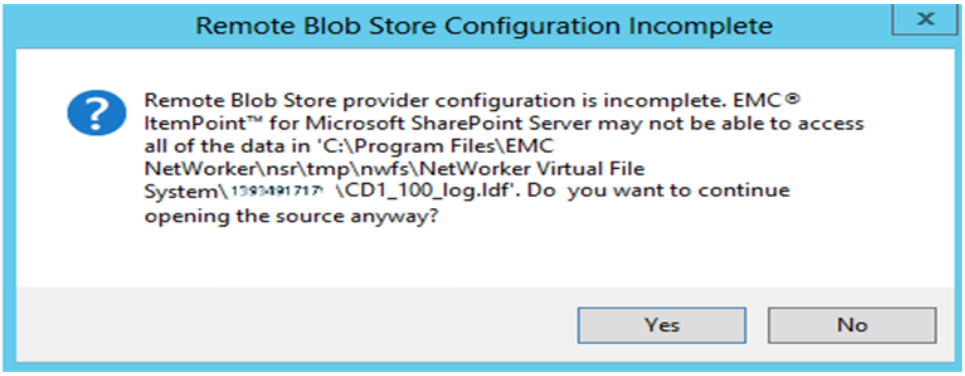
In the case of a complete disaster, where the Metalogix data is lost, restore the Metalogix StoragePoint database also.

Troubleshooting tips

This section lists the common issues with backing up and recovering SharePoint BLOB by using NMM and Metalogix StoragePoint, and provides workarounds for these issues.

- An error may occur after you have selected the target server during a granular restore by using the EMC ItemPoint for Microsoft SharePoint Server GUI.

  Figure 29 Error during a granular restore



Remote Blob Store Configuration Incomplete

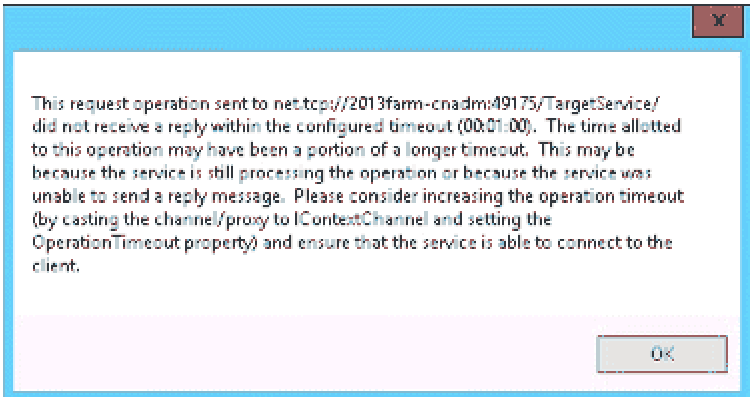
Remote Blob Store provider configuration is incomplete. EMC® ItemPoint™ for Microsoft SharePoint Server may not be able to access all of the data in 'C:\Program Files\EMC NetWorker\nsr\tmp\nwfs\NetWorker Virtual File System\1393491717\CD1_100_log.ldf'. Do you want to continue opening the source anyway?

Figure 29 Error during a granular restore (continued)

Solution: Provide the correct Metalogix StoragePoint server URL on the Remote BLOB store configuration page.

- When you have started the copy operation from a source to a target, the operation can be timed out.

Figure 30 Copy operation time out



This request operation sent to net.tcp://2013farm-cnadm:49175/TargetService/ did not receive a reply within the configured timeout (00:01:00). The time allotted to this operation may have been a portion of a longer timeout. This may be because the service is still processing the operation or because the service was unable to send a reply message. Please consider increasing the operation timeout (by casting the channel/proxy to IContextChannel and setting the OperationTimeout property) and ensure that the service is able to connect to the client.

Solution: Click OK in the message box and start the copy operation.

APPENDIX D

SharePoint Content Database Log Truncation

This appendix includes the following sections:

Issue with truncating SharePoint content database logs

SharePoint or SQL VSS backups do not truncate SQL logs. This known Microsoft SQL VSS Writer behavior can lead to no disk space on hard disks that leads to SQL server crash.

A mix of SQL VDI and SharePoint farm backups can act as a workaround for the issue. However, after each SharePoint farm backup, the subsequent SQL VDI backup is promoted to a full backup. Regardless of the existence of a SQL VDI full backup before the SharePoint farm backup, or the backup level that you set to perform the SQL VDI backup, the backup is promoted to a full backup. This known NMM behavior can lead to no disk space on hard disks.

Solution to truncate SharePoint content database logs

This section provides a solution, that is, a procedure to truncate SharePoint content database logs. After a SharePoint farm backup, to disable promoting a SQL VDI backup to a full backup, and save disk space, use the *NSR_BACKUP_PROMOTION* application information variable.

Before you begin

By using NMC, create the following policies:

- Policy 1 to perform the SQL VDI full backup
- Policy 2 to perform the SharePoint farm VSS backup

The procedure applies to a SharePoint farm that is configured with default SQL Server instance, named SQL Server instance, SQL virtual instance, or SQL AlwaysOn Availability Group.

Procedure

1. In policy 1, perform the SQL VDI full backup.
2. In policy 2, perform the SharePoint farm VSS backup.
3. Perform the SQL VDI tLog backup by specifying either `NSR_BACKUP_PROMOTION=NONE_WITH_WARNINGS` or `NSR_BACKUP_PROMOTION=NONE` application information variable in the **Client Properties** dialog box of the **NetWorker Administration** window.

   The application information variable disables promoting the tLog backup to a full backup after the SharePoint farm backup, and saves the disk space.

4. Perform the VSS backup of the SharePoint farm that you backed up in step 2.
5. Restore the SharePoint farm from the backup that you performed in either step 2 or step 4.

   The restore operation succeeds.

Limitation

Using either `NSR_BACKUP_PROMOTION=NONE_WITH_WARNINGS` or `NSR_BACKUP_PROMOTION=NONE` application information variable to perform a SQL VDI backup causes a log gap when you restore the backup. However, this limitation and the procedure do not affect the subsequent SharePoint farm backups and restores.

Restoring SharePoint content databases from SQL VDI backups

Restore SharePoint content databases from SQL VDI backups either if SharePoint backups are unavailable or to intentionally perform the task.

Before you begin

By using NMC, create the following policies:

- Policy 1 to perform the SQL VDI full backup of the SharePoint content databases and the other databases that do not pertain to SharePoint
- Policy 2 to perform the SharePoint farm VSS backup

Procedure

1. In policy 1, perform the SQL VDI full backup of the SharePoint content databases and the other databases that do not pertain to SharePoint.
2. In policy 2, perform the SharePoint farm VSS backup.
3. Perform the SQL VDI tLog backup of the databases that you backed up in step 1 by specifying either `NSR_BACKUP_PROMOTION=NONE_WITH_WARNINGS` or `NSR_BACKUP_PROMOTION=NONE` application information variable in the **Client Properties** dialog box of the **NetWorker Administration** window.

   The application information variable disables promoting the tLog backup to a full backup after the SharePoint farm backup, and saves the disk space.

4. Perform the VSS backup of the SharePoint farm that you backed up in step 2.
5. Perform the SQL VDI tLog backup of the databases that you backed up in step 1 by specifying either `NSR_BACKUP_PROMOTION=NONE_WITH_WARNINGS` or `NSR_BACKUP_PROMOTION=NONE` application information variable in the **Client Properties** dialog box of the **NetWorker Administration** window.
6. Restore the SharePoint content databases from the backup that you performed in step 1, 3, or 5.

   The restore operation succeeds.

   The *NetWorker Module for Microsoft for SQL VDI User Guide* provides information about SQL VDI restore operation.

Limitation

Using either `NSR_BACKUP_PROMOTION=NONE_WITH_WARNINGS` or `NSR_BACKUP_PROMOTION=NONE` application information variable to perform a SQL VDI backup causes a log gap when you restore the backup.

Sample configuration and test steps to truncate SharePoint content database logs

This section provides the sample configuration and the test steps to truncate SharePoint content database logs.

Before you begin

By using NMC, create the following policies, workflows, and backup actions:

- Policy 1, workflow 1, and backup action 1 that contains SharePoint 2013 Application Server as primary WFE
- Policy 2, workflow 2, and backup action 2 that contains SQL AlwaysOn Availability Group client (Windows cluster resource that uses SQL VDI)

The procedure to truncate SharePoint content database logs has been tested with the following sample configuration:

- SharePoint Server 2013 is configured with SQL Server 2014 AlwaysOn Availability Group.
- Promotion logic is disabled for SQL VDI AlwaysOn Availability Group backup.
- SharePoint 2013 Application Server, SharePoint 2013 Search Server, and SQL AlwaysOn Availability Group are configured on two SQL Servers.

Procedure

1. By using workflow 2, perform the SQL VDI full backup.
2. By using workflow 1, perform the SharePoint farm VSS backup.
3. By using workflow 2, perform the SQL VDI tLog backup by specifying either `NSR_BACKUP_PROMOTION=NONE_WITH_WARNINGS` or `NSR_BACKUP_PROMOTION=NONE` application information variable in the **Client Properties** dialog box of the **NetWorker Administration** window.

   The application information variable disables promoting the tLog backup to a full backup after the SharePoint farm backup, and saves the disk space.

4. By using workflow 1, perform the VSS backup of the SharePoint farm that you backed up in step 2.
5. Delete the SharePoint web application, and then restore the SharePoint farm from the backup that you performed in either step 2 or step 4.

   The restore operation succeeds.

APPENDIX E

Troubleshooting

This appendix includes the following sections:

Generic troubleshooting issues

Review the issue descriptions and corresponding solutions to troubleshoot the following issues.

Insuffiencient privileges for SharePoint Writer and SQL Writer
Check that the SharePoint Writer and SQL Writer are functional on their respective machines. If the custom writer or express writer creation fails, check if the user has sufficient privileges.

Run the `vssadmin list writers` command to check the Writers and also whether the user has sufficient privileges.

Grant the the SharePoint users 'NT AUTHORITY\SYSTEM' and 'DOMAINNAME \HOSTNAME$' the dbcreator, public, and system permissions on the SQL Server.

Windows Management Instrumentation (WMI) should be enabled on all machines in the farm for backup and restore to work. To enable WMI go to Windows Firewall, and allow an application or feature through windows firewall. Scroll down and check the domain and private profiles for WMI. Both the NMM Installer and the System Configuration Checker provide checks for this condition.

If a backup fails on one node, the entire backup fails. Similarly, if restore fails on one node, the entire restore fails.

Failure to establish a Client Direct session during GLR
The Client Direct feature must be enabled to perform GLR. To verify that the environment has Client Direct enabled, perform the following steps:

1. Validate that the NetWorker device is enabled for Client Direct.
   This verification must only be performed for AFTD devices. Data Domain is automatically enabled for Client Direct. The *NetWorker Administration Guide* provides more information about Client Direct.
2. Validate that the client has name resolutions for the systems.
   If Data Domain is being used, ensure the client has name resolution for the Data Domain device. If an AFTD storage node is being used, ensure the client has name resolution for the storage node.
3. Check the application logs directory in the NetWorker Virtual File System (NWFS) log file, `nwfs.raw`, and look for messages confirming that a Client Direct session was established.
   - The message "`Performing Direct File Access Restore`" confirms that a Client Direct session is successfully established.
   - The following messages indicate that a Client Direct session could not be established:
     - `Configured to perform Immediate recover, exiting`
     - `Configured to perform Non-Immediate recover, exiting`
4. Run the following `save` command from the command prompt:
   ```
   PS C:\Program Files\EMC NetWorker\nsr\bin> save -D1 -a
   DIRECT_ACCESS=yes -b networker_pool 'C:\Windows\System32\drivers
   \etc\hosts'
   ```
   Where *networker_pool* is the NetWorker pool containing the volumes where the savesets for recovery reside.

5. Check the output for messages indicating the Client Direct session is established:

```
10/16/16 23:59:27.094472 Default DFA handling by client is
'Fallback'
10/16/16 23:59:27.094472 DIRECT_ACCESS=yes: Client direct set to
'Yes'
10/16/16 23:59:27.129477 Device attribute block size is 262144
10/16/16 23:59:29.185589 libDDBoost version: major: 3, minor: 3,
patch: 0, engineering: 2, build: 545054
10/16/16 23:59:29.197590 load ddp_get_file_segment_type
129292:save: Successfully established Client direct save session
for save-set ID '889485007' (mb-vm-sql-2.dpsg-sea.emc.c
om:C:\Windows\System32\drivers\etc\hosts) with Data Domain volume
'ddveselssemccom.002'.
10/16/16 23:59:29.299596 using DFA save for ssid = 889485007
10/16/16 23:59:29.299596 ssid 889485007 using DFA save to `mb-vm-
nw-2'
10/16/16 23:59:29.299596 Successfully setup direct saves
```

6. (Optional) If the `save` command fails:

   a. Run the `save` command again after replacing `-D1` to `-D3`:

      ```
      PS C:\Program Files\EMC NetWorker\nsr\bin> save -D3 -a
      DIRECT_ACCESS=yes -b networker_pool 'C:\Windows\System32\drivers
      \etc\hosts'
      ```

      Where *networker_pool* is the NetWorker pool containing the volumes where the savesets for recovery reside.

   b. Check for output messages indicating the Client Direct session is established.

   c. If a Client Direct session is not established, find the messages indicating the cause of the failure, and fix the problem as required.

Cannot enable a Client Direct session and GLR failing as a result

Client Direct is required for SharePoint GLR, including GLR of backups taken with a previous version of NMM. If you cannot enable Client Direct for either policy or technical reasons, use the following workaround to allow GLR to continue without Client Direct.

1. Create a folder and name it "debug" in the `\nsr\` directory, if the folder does not already exist.
2. Within the "debug" folder, create an empty file and name it "nodirectfile" with no file name extension.
   You may be required to create the "nodirectfile" file from a DOS Shell command line.

Note

This workaround disables Client Direct for all client operations, including subsequent backups. This workaround is against NMM best practices and you may run into timeout and other restore issues if you do not enable Client Direct.

SharePoint Server issues

Review the issue descriptions and corresponding solutions to troubleshoot SharePoint Server related issues.

Client Backup Configuration wizard issues

Review the descriptions and corresponding solutions to troubleshoot the following Client Backup Configuration wizard issues.

- When using the Client Backup Configuration wizard to create a client resource, if the page after the authentication window does not appear or the clients are not being listed after authentication, perform the following steps:
  - Check if SPShellAdmin is present.
  - If SPShellAdmin is missing, add the SPShellAdmin and provide access privileges like SQL system dbcreator, public, and system administrator permissions.
  - Provide the same access permissions to the NT Authority\System login in SQL Server Management studio.

  Note

  These steps are important because the Client Backup Configuration wizard accesses the SharePoint Configuration Database. You are recommended to perform these steps before running the Client Backup Configuration wizard. The "Prerequisites" section in the Microsoft SharePoint Server Scheduled Backups in a Federated Workflow chapter provides the steps you must perform before running the Client Backup Configuration wizard.

- SQL nodes are not added. Only SQL virtual cluster or SQL AG listener are added as SQL client.
  Run the following PowerShell script and check if the node names are being displayed:

  -
    ```
    Get-WmiObject -q "Select name from mscluster_node" -
    Namespace <root\mscluster> -ComputerName "Name of the
    virtual cluster or AG Listener"
    ```

  -
    ```
    Get-WmiObject -q "Select name from mscluster_node" -
    Namespace <root\mscluster> -ComputerName "Name of Windows
    cluster name"
    ```

  Where **`Name of the virtual cluster or AG Listener`** and **`Name of Windows cluster name`** are user inputs.

  If errors like access denied, RPC Server not found, or so on occur when the PowerShell script is run, run the cluster validation wizard again.

  Note

  Such issues mostly occur due to improper cluster configuration.

If crawling content produces more traffic on the web front-end servers than user requests

You can use a dedicated web front-end server for crawling with NMM, if the crawling content produces more traffic on the web front-end servers than a user requests. You can specify any web front-end server in the farm for crawling.

The Microsoft TechNet website provides more details about dedicated web front-end crawling.

You must perform the required steps to configure a dedicated web front-end server.

Procedure

1. Back up the existing host file.
2. Open SharePoint Central Administration, and configure dedicated web front-end crawling.

   After the configuration is complete, the SharePoint Central Administration creates a new host file.
3. Append the information from the backed-up host file to the newly created host file.
4. Configure NMM backups.

Perform manual steps to associate a web application to the original SSP after recovery

After performing a backup if you change the association of a web application to the original Shared Service Provider (SSP) and then perform a recovery, although recovery is successful, the association of a web application to the original SSP is not restored after a recovery.

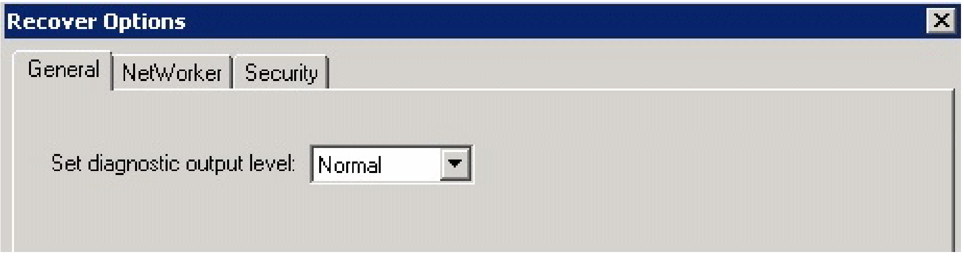
Solution

1. In the SharePoint Central Administration, select **Shared Services Administration**.
2. On the **Manage this farm's shared services** page, select **Change association**.
3. Complete the required fields. You should have already restored the SSP on the site.
4. Specify the web application and database to which the SSP was restored.

Missing SQL tab during SharePoint GLR

The SQL tab is not displayed at the target location in the NetWorker User for Microsoft GUI for a redirected recovery if the SQL Server databases are not selected for recovery.

Figure 31 Missing SQL tab

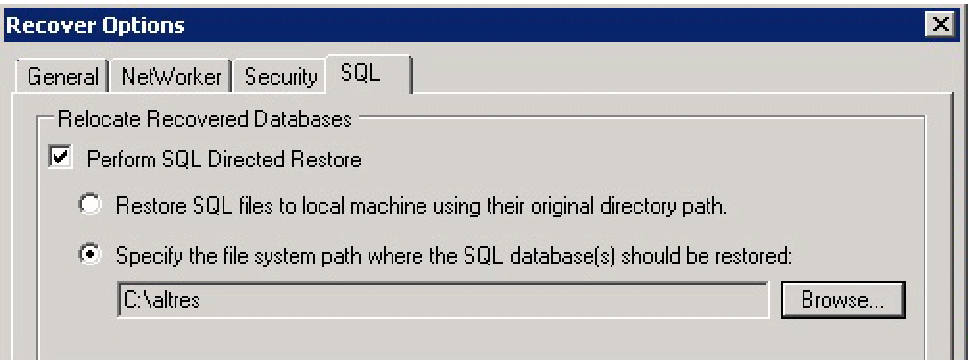


Set diagnostic output level: Normal

Solution

Select the SQL Server databases for recovery. The SQL tab appears. Provide the recovery location for the databases in the SQL tab.

Figure 32 Available SQL tab



Recover Options

General | NetWorker | Security | SQL

Relocate Recovered Databases

☑ Perform SQL Directed Restore

○ Restore SQL files to local machine using their original directory path.

● Specify the file system path where the SQL database(s) should be restored:

C:\altres

Locating the content database for directed recovery during SharePoint Server GLR

In some SharePoint Server configurations, the data is stored in multiple content databases. Before performing a recovery of a content database, you must know which content database contains the SharePoint data (SharePoint site or lists).

Solution
To locate the content database that contains the SharePoint data for recovery, use either the Command Line or the SharePoint Central Administration GUI.

Locating a content database by using the Command Line:

- If you know the site URL information, you can obtain information about the content database that contains the SharePoint data by running the following command:

```
C:\Program Files\Common Files\Microsoft Shared\Web Server
Extensions\14\BIN>stsadm.exe -o enumcontentdbs -url "http://
sqlsrv1vmsp10:8081"

<Databases Count="2">

<ContentDatabase Id="62ad9807-00c9-4494-9ba0-642e86b18b3d"
Server="sqlsrv1vmsql08.nmmperf.com" Name="WSS_Content_8081"

/>

<ContentDatabase Id="e31561b5-5843-40a2-96ac-2063775e41aa"
Server="sqlsrv1vmsql08.nmmperf.com" Name="WSS_Content_SR Re

quest Portal" />

</Databases>
```

- If you do not know the site URL information, you can obtain information about the site URL and the content database by running the following command:

```
C:\Program Files\Common Files\Microsoft Shared\Web Server
Extensions\14\BIN>stsadm.exe -o enumcontentdbs -url "http://
sqlsrv1vmsp10:8081"

<Database SiteCount="1" Name="WSS_Content_SR Request Portal"
DataSource="sqlsrv1vmsql08.nmmperf.com">

<Site Id="2998fdfd-56ba-4031-983e-18bb640e45f4"
OwnerLogin="NMMPERF\user" InSiteMap="True">

<Webs Count="7">
```

```
<Web Id="580174de-1818-490c-9a21-57ab18d4703a" Url="/"
LanguageId="1033" TemplateName="STS#0" TemplateId="1" />

<Web Id="c6768e65-1857-401e-8a68-f3885be76dee" Url="/
qcdefcts" LanguageId="1033" TemplateName="STS#0"
TemplateId="1" />

<Web Id="c467e967-c615-45dd-88ff-cc337efb775c" Url="/
qcdefcts/srrequest2013" LanguageId="1033"
TemplateName="STS#0" TemplateId="1" />

<Web Id="f6ff88b6-7456-4852-96c0-60b908743708" Url="/Qcesc"
LanguageId="1033" TemplateName="STS#0" TemplateId="1" />

<Web Id="87fe65ea-a8b6-4b9f-b5c4-20b0ad84740c" Url="/
srrequest" LanguageId="1033" TemplateName="STS#0"
TemplateId="1" />

<Web Id="b4239a41-ed7a-4f57-ba4d-f19dfb1ec7de" Url="/
srrequest/srrequest2013" LanguageId="1033"
TemplateName="STS#0" TemplateId="1" />

<Web Id="e92443e7-d73a-48c5-aafb-a4ac13fd9d7f" Url="/
srrequest/srrequest2011" LanguageId="1033"
TemplateName="STS#0" TemplateId="1" />

</Webs>

</Site>

</Database>
```

Locating a content database by using the SharePoint Server Central Administration GUI:

1. Open the SharePoint Central Administration.
2. Select the **Application Management** tab.
3. Under **SharePoint Site Management**, select **Site collection list**.
4. Select the web application to view the site collection list and the content database name that stores the site collection data.
5. Identify the correct content database.

Agent for Content Transfer Service error during SharePoint GLR

An error message appears if the Agent for Content Transfer Service is not installed or running when performing SharePoint GLR by using ItemPoint for SharePoint Server.

Solution

The Agent for Content Transfer Service does not start automatically and must be manually started by either using `services.msc` or by using the Command Line.

Run the SetupACTS.exe installer, which is packaged with the NMM binaries, to install the Agent for Content Transfer Service.

The nsrnmmsv -P command does not list the save set

An NMM backup cannot be performed unless the save set for a backup is available.

Solution

If the `nsrnmmsv -P` command does not list the save set, register the Windows SharePoint Services by using the `stsadm.exe -o registerwsswriter` command.

Sometimes save sets are not listed correctly when a SharePoint client resource is created by using the Client Backup Configuration wizard

This error occurs when there is an issue in the SharePoint setup. Either the SharePoint configuration database is missing from the SQL database or is not connected.

Solution

Perform the following steps:

1. Disconnect and reconnect the SharePoint farm.
2. In the SQL Configuration Manager, check if the SharePoint configuration database is missing. If missing, reattach the SharePoint configuration database from SQL install directory.

Slow SharePoint Server GLR performance when using a DD device

The GLR performance for SharePoint Server may be extremely slow when using a DD device.

In such situations, enable the "EnableDirectIO" registry value of the "NWFS Direct IO" feature to improve GLR performance. The NWFS Direct IO" feature is enabled by default.

Note

Do not use this solution if the SharePoint backups are AES encrypted because the NMM software behavior is undefined when AES encryption is used.

SharePoint backups fail, and display an error that is similar to "Unable to connect to the SQL Server" or "Failed to login to SQL Server"

This is a special scenario, where you cannot connect to the SQL Server without the static port number.

Ensure that there is network connectivity to the SQL Server instance, and correct network protocols are enabled on the SQL Server. To quickly check the connection to the SQL Server instance, perform the following steps:

1. Create a text file, and rename its extension from **.txt** to **.udl**.
2. Open the file by double-clicking it.
   The **Data Link Properties** dialog box appears.
3. On the **Provider** tab, select either **Microsoft OLE DB Provider for SQL Server** or **SQL Server Native Client 11.0**.
4. On the **Connection** tab:
   a. In the **Select or enter a server name** field, type the SQL Server name in one of the following formats:

  - `<SQL_Server_name>\<SQL_Server_instance_name>`, when you use a named SQL Server instance.
    For example, SharePointSQL\SharePointSQLInstance.
  - `<SQL_Server_name>`, when you use the default SQL Server instance.
    For example, SharePointSQL.

b. Select **Use Windows NT Integrated security**.

c. Click **Test Connection**.

d. If the connection fails, perform the following steps:

  a. In the **Select or enter a server name** field, type the SQL Server name and the port number in one of the following formats:

    - `<SQL_Server_name>\<SQL_Server_instance_name>,<Port_number>`, when you use a named SQL Server instance.
      For example, SharePointSQL\SharePointSQLInstance,423487.
    - `<SQL_Server_name>,<Port_number>`, when you use the default SQL Server instance.
      For example, SharePointSQL,423487.

  b. Click **Test Connection**.

e. If the connection succeeds when you specify the port number with the SQL Server name, and fails when you do not specify the port number with the SQL Server name, perform the steps that the following "Solution" section describes.

Solution
Create a Multi-String Value "SPSQLConnections" in the Windows Registry, and then add all the SQL Servers that you need:

1. Open the Windows Registry Editor.
2. In the left pane, go to **HKEY_LOCAL_MACHINE** > **SOFTWARE** > **Legato** > **NetWorker**.
3. Right-click **VSSClient**, and then select **New** > **Multi-String Value**.
   The string appears in the right pane.
4. Change the string name to `SPSQLConnections`.
5. Either double-click the string or right-click the string, and then select **Modify**.
6. In the **Edit Multi-String** dialog box, in the **Value data** field, type the SQL Server name and the port number in one of the following formats:
   - `<SQL_Server_name>\<SQL_Server_instance_name>,<Port_number>`, when you use a named SQL Server instance.
     For example, SharePointSQL\SharePointSQLInstance,423487.
   - `<SQL_Server_name>,<Port_number>`, when you use the default SQL Server instance.
     For example, SharePointSQL,423487.

   In the same format, specify the other SQL Servers that you need, each in a separate line.

   Click **OK**.

NOTICE

Whenever you install NMM, perform these steps.

SharePoint backups fail, and display an error that is similar to "Unable to connect to the SQL Server" or "Failed to login to SQL Server" 111

SQL Server issues

Review the issue descriptions and corresponding solutions to troubleshoot SQL Server issues.

Recovery of SQL Server database fails when the database is renamed after backup

If you perform recovery of a SQL Server database that is renamed after a backup is complete, the recovery of the database fails. This feature is not supported in NMM.

Solution
To rename a SQL Server database and its datafiles after backup, perform the following steps.

1. Open the Microsoft SQL Management Studio on the database.
2. Select the **Tasks and Copy Database** options.
3. Rename the SQL Server database and datafiles.
   The wizard also offers a choice to move rather than copy the database.

SQL Server services stop during recovery of SQL Server master database

During recovery of SQL Server master databases, the SQL services to stop.

Solution

1. Stop the SQL Server Reporting Service (SSRS).
2. Open the NetWorker User for Microsoft GUI.
3. Perform recovery of the SQL Server.
4. Once the recovery is complete, restart the SQL Server Reporting Service.

Back up the SQL Server resource database during file system backup by using the NetWorker client

The SQL Server resource database must be protected for a full recovery of a SQL Server environment, but the SQL Server resource database is not backed up during the backup of the SQL Server.

Solution
You must back up the resource database as part of the file system backup by using the NetWorker client.

The SQL Server documentation and Microsoft Knowledge Base article http://msdn.microsoft.com/en-us/library/ms190940.aspx provide more information.

Freeing up disk space by shrinking the SQL log files

A transaction log file might contain unused space that you can reclaim by reducing the size of the transaction log. This process, which is known as shrinking the log file, helps in freeing up disk space.

Solution
Shrinking can occur only while the database is online. Run the following native SQL command (T-SQL) to avoid the log file from becoming full:

```
DBCC SHRINKFILE ( DBNAME_LOG, TARGET FILE SIZE)
```

The SQL Server documentation and Microsoft Knowledge Base article http://msdn.microsoft.com/en-us//library/ms189493.aspx provide more information.