EMC® NetWorker® Module for Microsoft for Hyper-V VSS
Version 9.1

User Guide

302-003-216
REV 02
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>Recoveries</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>58</td>
</tr>
<tr>
<td></td>
<td>Hosting the recovered virtual systems</td>
<td>58</td>
</tr>
<tr>
<td></td>
<td>Specifying the destinations for the Hyper-V configuration files and virtual system</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>Selecting the Hyper-V recovery destination</td>
<td>59</td>
</tr>
<tr>
<td></td>
<td>Performing Hyper-V recovery to the original machine and location</td>
<td>60</td>
</tr>
<tr>
<td></td>
<td>Performing a directed Hyper-V recovery to a different host or location</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>Recovering Hyper-V CSV virtual machines</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>CSV virtual machine recovery</td>
<td>63</td>
</tr>
<tr>
<td></td>
<td>Recovering with a Windows Server 2012 and 2012 R2 proxy CSV server</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>Recovering multiple CSV VMs to the original location</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>Recovering an individual CSV Hyper-V virtual machine to a different location</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>Using NMM 9.1 to recover a backup created by using an NMM 8.2.x release</td>
<td>68</td>
</tr>
<tr>
<td>4</td>
<td>Granular Level Recoveries</td>
<td>71</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>Recovering Hyper-V files and folders</td>
<td>72</td>
</tr>
<tr>
<td>5</td>
<td>File Level Recoveries</td>
<td>75</td>
</tr>
<tr>
<td></td>
<td>Introduction</td>
<td>76</td>
</tr>
<tr>
<td></td>
<td>Required ports for Hyper-V File Level Restore GUI</td>
<td>76</td>
</tr>
<tr>
<td></td>
<td>Performing a browser-based file level restore</td>
<td>76</td>
</tr>
<tr>
<td></td>
<td>Performing a directed file level restore</td>
<td>78</td>
</tr>
<tr>
<td></td>
<td>Monitoring file level restores</td>
<td>79</td>
</tr>
<tr>
<td></td>
<td>Hyper-V FLR web UI log files</td>
<td>80</td>
</tr>
<tr>
<td>6</td>
<td>EMC Data Protection Add-in for SCVMM</td>
<td>81</td>
</tr>
<tr>
<td></td>
<td>Overview</td>
<td>82</td>
</tr>
<tr>
<td></td>
<td>Recoveries</td>
<td>82</td>
</tr>
<tr>
<td></td>
<td>Backups</td>
<td>82</td>
</tr>
<tr>
<td></td>
<td>Supported versions</td>
<td>82</td>
</tr>
</tbody>
</table>
Software dependencies................................................................. 83
Required privileges........................................................................ 83
Installation and configuration overview..........................................84
How the Data Protection Add-in works with SCVMM....................... 84
Workflows overview...................................................................... 85
GUI overview............................................................................... 86
SCVMM user roles and allowed actions......................................... 86
Supported scopes and contexts.....................................................87
Installation and uninstallation........................................................ 87
Installing SCVMM and the SCVMM console................................. 88
Installing the Data Protection Add-in............................................88
Importing the Data Protection Add-in.......................................... 89
Activating the Data Protection Add-in.......................................... 89
Uninstalling the Data Protection Add-in........................................90
Upgrading the Data Protection Add-in......................................... 91
Preferences........................................................................................ 92
Adding NetWorker servers............................................................ 92
Removing NetWorker servers....................................................... 93
Setting the refresh interval...........................................................93
Including debug output for logging purposes................................. 94
Using multiple NetWorker Servers that define the same clients and
virtual machine savesets.............................................................94
Data Protection Add-in overview data............................................94
Recoveries........................................................................................ 100
Viewing available virtual machines..............................................102
Recovering a virtual machine to the original location......................102
Redirected recoveries.................................................................. 103
Recovering a deleted virtual machine........................................... 106
Monitoring........................................................................................ 106
Troubleshooting...............................................................................107
Recovered virtual machine does not start.................................... 107
Installation fails due to access issue............................................. 108
The Data Protection Add-in for SCVMM displays an incorrect
NetWorker Server version..........................................................108
Importing fails due to access issue.............................................. 108
Virtual machine attributes might display incorrect values......... 108
Redirected recovery appears to succeed but no virtual machine
appears in Hyper-V Manager....................................................109
Checks for redirected recovery failures .................................... 109
Avoid virtual machine names with the same name within an SCVMM
context....................................................................................109
Cluster virtual machine backups do not display on the Recover page
............................................................................................109
Redirected recovery is not supported when the virtual machine
name or virtual machine configuration path contains special
characters..................................................................................110

Chapter 7  Windows Bare Metal Recovery Solution  111
Microsoft Hyper-V Backup and BMR.............................................112
    Backing up Hyper-V for BMR.................................................112
    Performing BMR of Hyper-V.................................................112
Microsoft System Center Virtual Machine Manager backup and BMR...113
    Backing up System Center Virtual Machine Manager for BMR.... 113
    Performing BMR of a System Center Virtual Machine Manager... 115
## Chapter 8  
**Best Practices and Recommendations**  
117

- Non-ASCII files and directories.................................................................118
- Required AFTD DFA device settings for Hyper-V environments..............118
- Hyper-V Server backup and recovery best practices......................................118
- Microsoft application backup and recovery within a Hyper-V virtual machine best practices.................................................................................................................................119
- Improving backup performance in Windows Server 2012 and 2012 R2 clusters with CSV.........................................................................................................................119
- Data mining using Hyper-V granular level recovery..................................120
- Restrictions and requirements for relocating and recovering data to a different location.................................................................................................................................121
- Restrictions for backup and recovery of Hyper-V virtual machines in a Windows Server Failover Cluster.................................................................121
- Restrictions for Hyper-V virtual machine granular-level recovery..............122

## Chapter 9  
**Troubleshooting**  
123

- Troubleshooting backups........................................................................124
- Troubleshooting recovery........................................................................126

## Appendix A  
**Recovering SQL Server, Exchange Server, and SharePoint Server Items from a Hyper-V Virtual Machine**  
129

- Overview....................................................................................................130
- Recovering items that are stored on a Hyper-V virtual machine..............130
  - Recovering SQL Server items from a Hyper-V virtual machine....132
  - Recovering Exchange Server items from a Hyper-V virtual machine .................................................................................................................................133
- Recovering SharePoint Server items.......................................................134
<table>
<thead>
<tr>
<th>FIGURES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>16</td>
</tr>
<tr>
<td>17</td>
</tr>
<tr>
<td>18</td>
</tr>
<tr>
<td>19</td>
</tr>
<tr>
<td>20</td>
</tr>
<tr>
<td>21</td>
</tr>
<tr>
<td>22</td>
</tr>
<tr>
<td>23</td>
</tr>
<tr>
<td>24</td>
</tr>
<tr>
<td>25</td>
</tr>
<tr>
<td>26</td>
</tr>
<tr>
<td>27</td>
</tr>
<tr>
<td>28</td>
</tr>
<tr>
<td>29</td>
</tr>
</tbody>
</table>
FIGURES
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Revision history...........................................................................................................12</td>
</tr>
<tr>
<td>2</td>
<td>Style conventions........................................................................................................13</td>
</tr>
<tr>
<td>3</td>
<td>Comparison of guest and image-level backup and recovery........................................17</td>
</tr>
<tr>
<td>4</td>
<td>VSS Writer and VSS Provider used.............................................................................19</td>
</tr>
<tr>
<td>5</td>
<td>Access privileges needed for SMB backup and recovery ...........................................22</td>
</tr>
<tr>
<td>6</td>
<td>NMM backup types....................................................................................................25</td>
</tr>
<tr>
<td>7</td>
<td>Virtual machine files included in backups...........................................................25</td>
</tr>
<tr>
<td>8</td>
<td>The GUIs used for various types of recoveries........................................................32</td>
</tr>
<tr>
<td>9</td>
<td>Special characters supported in NMM........................................................................37</td>
</tr>
<tr>
<td>10</td>
<td>Backup tasks for Hyper-V..........................................................................................42</td>
</tr>
<tr>
<td>11</td>
<td>Hyper-V save set syntax.............................................................................................52</td>
</tr>
<tr>
<td>12</td>
<td>Hyper-V application information variable settings................................................53</td>
</tr>
<tr>
<td>13</td>
<td>SCVMM user roles and actions allowed by the Data Protection Add-in......................87</td>
</tr>
<tr>
<td>14</td>
<td>Virtual machine IDs after redirected recovery.......................................................103</td>
</tr>
<tr>
<td>15</td>
<td>Backup types............................................................................................................130</td>
</tr>
</tbody>
</table>
As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function correctly or does not function as described in this document.

Note

This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose

This guide contains information about using the NetWorker Module for Microsoft (NMM) 9.1 software to back up and recover Hyper-V virtual machines 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. Ensure to download a copy of the NetWorker Module for Microsoft Administration Guide from EMC Online Support (https://support.emc.com) before using this guide.

Audience

This guide is part of the NetWorker Module for Microsoft 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:

- EMC NetWorker software
- EMC NetWorker data protection policy management
- EMC NetWorker block based backup (BBB) technology
- Microsoft Volume Shadow Copy Service (VSS) technology
- Microsoft Hyper-V server technology
- Microsoft Failover Cluster technology
Revision history
The following table presents the revision history of this document.

Table 1 Revision history

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>02</td>
<td>May 2, 2017</td>
<td>The &quot;Troubleshooting recovery&quot; section in the &quot;Troubleshooting&quot; chapter has been updated with content on the following topics:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Failure to establish a Client Direct session during GLR</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Cannot enable a Client Direct session and GLR failing as a result</td>
</tr>
<tr>
<td>01</td>
<td>December 22, 2016</td>
<td>First release of this document for EMC NetWorker Module for Microsoft release 9.1. Information on the following new features are added:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Hyper-V Server 2016</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Windows Server 2016</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Data Protection Add-in support with System Center 2016 Virtual Machine Manager</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Disabling incremental backups and enabling only full backups with NMM for Hyper-V Server</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The &quot;Disabling incremental backups and enabling only full backups&quot; section in the Backup chapter is added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The <strong>Disable Change Block Tracking</strong> option in the Client Backup Configuration Wizard to disable incremental backups and enable only full backups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• The <strong>NSR_DISABLE_INCREMENTAL</strong> Application Information variable that can be used when manually creating client resources with the NetWorker Management Console to disable incremental backups and enable only full backups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• General information pertaining to the 9.1 release.</td>
</tr>
</tbody>
</table>

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 VSS 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**
EMC uses the following conventions 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**
EMC uses the following type style conventions in this document:

<table>
<thead>
<tr>
<th>Table 2 Style conventions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bold</strong></td>
</tr>
<tr>
<td>Used for names of interface elements, such as names of buttons, fields, tab names, and menu paths (what the user specifically selects or clicks)</td>
</tr>
<tr>
<td><strong>Italic</strong></td>
</tr>
<tr>
<td>Used for full titles of publications that are referenced in text</td>
</tr>
<tr>
<td><strong>Monospace</strong></td>
</tr>
<tr>
<td>Used for:</td>
</tr>
<tr>
<td>• System code</td>
</tr>
<tr>
<td>• System output, such as an error message or script</td>
</tr>
<tr>
<td>• Pathnames, file names, prompts, and syntax</td>
</tr>
<tr>
<td>• Commands and options</td>
</tr>
<tr>
<td><strong>Monospace italic</strong></td>
</tr>
<tr>
<td>Used for variables</td>
</tr>
<tr>
<td><strong>Monospace bold</strong></td>
</tr>
<tr>
<td>Used for user input</td>
</tr>
<tr>
<td>[ ]</td>
</tr>
<tr>
<td>Square brackets enclose optional values</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Vertical bar indicates alternate selections - the bar means &quot;or&quot;</td>
</tr>
<tr>
<td>{ }</td>
</tr>
<tr>
<td>Braces enclose content that the user must specify, such as x or y or z</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>Ellipses indicate non-essential information that is omitted from the example</td>
</tr>
</tbody>
</table>

**Where to get help**
EMC support, product, and licensing information can be obtained as follows:

**Product information**
For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at [https://support.emc.com](https://support.emc.com).

**Technical support**
Go to EMC Online Support at [https://support.emc.com](https://support.emc.com), and click Service Center. Several options for contacting EMC Technical Support appear on the site. Note that
to open a service request, you must have a valid support agreement. Contact your
EMC sales representative for details about obtaining a valid support agreement or with
questions about your account.

**Online communities**
Go to the EMC Community Network at [https://community.emc.com](https://community.emc.com) for peer
contacts, conversations, and content on product support and solutions. Interactively
engage online with customers, partners, and certified professionals for all EMC
products.

**Your comments**
Your suggestions help to improve the accuracy, organization, and overall quality of the
user publications. Send your opinions of this document to
[DPAD.Doc.Feedback@emc.com](mailto:DPAD.Doc.Feedback@emc.com).
CHAPTER 1

Introduction

This chapter includes the following sections:

- Overview ............................................................................................................ 16
- NMM protection methods for Hyper-V ............................................................... 16
- Using NMM with Hyper-V in stand-alone and clustered environments over Server Message Block 3.0 .............................................................................................. 18
- Required privileges ............................................................................................. 22
- Backup overview ................................................................................................ 23
- Recovery overview ............................................................................................. 31
- NMM 9.1 compatibility with NetWorker 8.2.3 or later servers ......................... 34
Overview

Microsoft Hyper-V is a hypervisor-based server virtualization product for Microsoft Windows Server. Hyper-V enables you to create multiple virtual machines (VMs) on a standalone server or Windows cluster server to consolidate workloads.

EMC® NetWorker® Module for Microsoft (NMM) supports backup, recovery, and granular recovery of Hyper-V virtual machines that run on the Hyper-V role installed on Windows Server 2012 and 2012 R2 and on Server Core installations for Windows Server 2012 and 2012 R2.

Note

The Microsoft Hyper-V documentation provides a complete and updated list of system requirements and supported guest operating system versions. The NetWorker Online Software Compatibility Matrix, available at http://compatibilityguide.emc.com:8080/CompGuideApp/, provides the most up-to-date and accurate listing of hardware, operating system, service pack, and application versions that the NMM client supports.

NMM protection methods for Hyper-V

You can perform Hyper-V guest-level or image-level backup and recovery depending on certain criterion, such as the Windows operating system that is running on the guest and where the NMM software is installed.

Guest-level backup and recovery

For guest-level backup and recovery, install an NMM client on each virtual machine that hosts databases or specific applications, for example, Exchange Server or SharePoint Server. To NMM, each virtual machine is a separate client, and you can perform individual backups of each virtual machine and Microsoft application.

The following figure illustrates Hyper-V guest-level backup and recovery with NMM.

![Figure 1 Guest-level backup and recovery environment](image-url)
Image-level backup and recovery

For image-level backup and recovery, install an NMM client on the Hyper-V Server. You can perform a full and incremental image-level backup of the virtual machines. The following figure illustrates the image-level backup and recovery environment. Figure 2 Image-level backup and recovery environment

Comparing NMM protection methods for Hyper-V

The following table compares guest-level and image-level backup and recovery.

Table 3 Comparison of guest and image-level backup and recovery

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Guest-level</th>
<th>Image-level</th>
</tr>
</thead>
<tbody>
<tr>
<td>NMM</td>
<td>Install on each virtual machine</td>
<td>Install only on the Hyper-V Server</td>
</tr>
<tr>
<td>NetWorker client</td>
<td>Install on each virtual machine</td>
<td>Install only on the Hyper-V Server</td>
</tr>
<tr>
<td>NetWorker server network connection</td>
<td>Required for each virtual machine</td>
<td>Required only on the Hyper-V Server</td>
</tr>
<tr>
<td>iSCSI/pass-through disk support</td>
<td>Required</td>
<td>Not required</td>
</tr>
<tr>
<td>Windows Bare Metal Recovery (BMR) backup</td>
<td>Can be performed (by using the NetWorker client DISASTER RECOVERY save set)</td>
<td>Can be performed</td>
</tr>
<tr>
<td>Virtual machine status for backup</td>
<td>Virtual machine must be online</td>
<td>Virtual machine can be online, offline, or saved state</td>
</tr>
<tr>
<td>Customized backup, including exclusion of certain files or file types</td>
<td>Can be performed</td>
<td>Cannot be performed</td>
</tr>
</tbody>
</table>
Table 3 Comparison of guest and image-level backup and recovery (continued)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Guest-level</th>
<th>Image-level</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(by using the NetWorker client DISASTER RECOVERY save set)</td>
<td></td>
</tr>
<tr>
<td>Application-aware backup and</td>
<td>Can be performed, for applications such as:</td>
<td>Cannot be performed</td>
</tr>
<tr>
<td>recovery</td>
<td>• Exchange Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SharePoint Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SQL Server</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Active Directory</td>
<td></td>
</tr>
<tr>
<td>Application-consistent backup and</td>
<td>Can be performed</td>
<td>Can be performed (for applications with VSS Writer and VSS integration component)</td>
</tr>
<tr>
<td>recovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Individual files and folders</td>
<td>Can be performed</td>
<td>Can be performed using granular-level recovery</td>
</tr>
<tr>
<td>recovery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disaster recovery</td>
<td>Can be performed by performing:</td>
<td>Can be performed with NMM</td>
</tr>
<tr>
<td></td>
<td>• Recover the operating system state critical volumes through the NetWorker client BMR wizard.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Recover applications and non-critical volume data with NMM.</td>
<td></td>
</tr>
</tbody>
</table>

Using NMM with Hyper-V in stand-alone and clustered environments over Server Message Block 3.0

You can use NMM with Hyper-V in stand-alone and clustered environments and over Server Message Block (SMB) 3.0.

NMM supports the following Hyper-V configurations:

- Local volumes on a stand-alone server with Windows Server 2012 and 2012 R2
- Cluster Shared Volumes (CSV) on a cluster with Windows Server 2012 and 2012 R2
- Server Message Block (SMB) 3.0 file shares on the following Windows Server 2012 and 2012 R2 file servers:
  - Stand-alone file server
  - Scale-Out File Server (SOFS)

The *EMC NetWorker Module for Microsoft Installation Guide* lists the Hyper-V hardware requirements.

Microsoft Volume Shadow Copy Service (VSS) is a framework that enables volume backups to be performed while applications on a system continue to write to the volumes. NMM uses the Hyper-V VSS Writer and Clustered Shared Volumes (CSV) VSS Writer on the host to back up and recover Hyper-V data.
The following table provides a list of types of Hyper-V environments and the corresponding VSS Writers and VSS Providers.

**Table 4 VSS Writer and VSS Provider used**

<table>
<thead>
<tr>
<th>Type of environment</th>
<th>VSS Writer used</th>
<th>VSS Provider used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stand-alone</td>
<td>Hyper-V VSS Writer</td>
<td>Microsoft Software Shadow Copy Provider</td>
</tr>
<tr>
<td>CSV</td>
<td>Hyper-V VSS Writer and CSV Writer</td>
<td>Microsoft CSV Shadow Copy Provider</td>
</tr>
<tr>
<td>Server Message Block (SMB) 3.0</td>
<td>Hyper-V VSS Writer</td>
<td>Microsoft File Share Shadow Copy Provider</td>
</tr>
</tbody>
</table>

**Using NMM in a stand-alone environment**

The Hyper-V role can be installed on a stand-alone machine. On a stand-alone Hyper-V Server, NMM uses the Hyper-V VSS Writer to take VSS snapshots of virtual machines.

**Using NMM in a Clustered Shared Volumes environment**

Cluster Shared Volumes (CSV) is a Windows Server feature that enables all nodes within a failover cluster to concurrently access shared disks.

Microsoft and NMM refer to the node in the cluster, where a CSV is locally mounted as the coordinating node. NMM provides the option to move the CSV ownership among the various nodes to provide the best backup and recovery performance.

NMM supports physical and virtual proxy nodes for Hyper-V CSV backups. When you specify a Preferred Server Order List (PSOL) in the Application Information attribute when configuring a client resource for the Cluster Server Name, NMM performs a snapshot on the cluster primary node, and then each proxy node backs up the snapshots in parallel.

With NMM, you can use virtual machines on a Hyper-V cluster as proxy nodes for CSV backups. NMM reassigns and distributes the backup workload to selected virtual proxy nodes. All virtual proxy nodes perform backups in parallel, which increases backup performance. At the same time, because the proxies are virtual machines, the hypervisor governs their compute, disk, and network resource utilization to ensure they do not unnecessarily impact other virtual machine workloads.

You may also run NMM as a proxy on the physical Hyper-V node where the system resource utilization may not be governed by the Hypervisor. These virtual proxies must be highly available cluster Hyper-V virtual machines, and the virtual proxies must be connected to the same domain as the physical nodes. A mix of physical and virtual machines is supported. NMM automatically excludes the virtual machines for the virtual proxies from backups.

**Note**

For Hyper-V cluster and CSV environments, including proxy environments, EMC recommends that you install the NetWorker client and NMM on all nodes in the cluster and the virtual proxies because the cluster ownership (and cluster alias) can failover to any cluster node within the cluster and NMM schedules backups against the cluster alias.
In a failover cluster, all servers (nodes) run Hyper-V and can host one or more virtual machines. A clustered virtual machine is only active on one node but can be configured to fail over to other nodes. Microsoft supports failover clustering for Hyper-V through CSV.

NMM implements the following snapshot features to protect the Hyper-V CSV environment during a backup:

- Single snapshot feature—A snapshot of each CSV is created on the active (master) node of the cluster and data is rolled over from proxy nodes.
- Multiple snapshot feature—A snapshot is taken of one CSV at a time.

Hyper-V CSV in a failover cluster

The following figure illustrates a Hyper-V failover cluster with two nodes. There are four virtual machines that can fail over between the nodes, and a fifth virtual machine that runs exclusively on the second node.

**Figure 3** Two-node Hyper-V failover cluster

---

**Using NMM with Hyper-V virtual machines over SMB 3.0**

You can use NMM to back up Hyper-V virtual machines over SMB 3.0 file shares on Windows Server 2012 and Windows Server 2012 R2 file servers.

The SMB file shares are supported on the following file servers:

- Stand-alone file server
- Scale-Out File Server (SOFS)
- Clustered file server

*Required SMB privileges* on page 22 describes the required permissions for SMB backup and recovery.
Windows Server Hyper-V stand-alone configurations with SMB file shares

For stand-alone Hyper-V Server with virtual machines on SMB storage, install NMM on the Hyper-V Server.

Windows Server Hyper-V clusters with SMB file shares

If you store virtual machines on SMB 3.0 file shares for use by a Hyper-V cluster, you can configure NMM to perform federated backup and restore of the virtual machines. The SMB file shares can be on either a Scale-Out File Server (SOFS) or on a clustered file server.

To perform backups of virtual machines on SMB file shares, install NMM on each node in the Hyper-V cluster.

The federated cluster client receives backup and restore requests from the NetWorker server and forwards the requests to the NMM client on the cluster nodes. The NMM client performs the backup and returns the backup data and metadata to the NetWorker server. The federated cluster client manages all NMM client requests and ensures that you can back up all virtual machines on SMB file shares in the cluster.

The following figure illustrates a Windows Server cluster where the federated cluster client enables image-level backups of virtual machines on SMB file shares. Figure 4 Image-level backups in a Windows Server cluster with SMB

Note

The Microsoft TechNet website provides instructions on configuring an SMB file share.
Required privileges

The *NetWorker Module for Microsoft Administration Guide* lists the required privileges for backup and recovery of Hyper-V virtual machines. These privileges are common for all Microsoft applications that are backed up and recovered through NMM.

Backup and recovery of Hyper-V virtual machines in a CSV environment or over SMB 3.0 require additional privileges.

**Note**

SMB and CSV backups and recoveries in NetWorker Restricted Datazone (RDZ) environments require additional permissions and configuration. The *NetWorker Module for Microsoft Administration Guide* provides details about the required permissions and configuration. The *NetWorker Administration Guide* provides detailed information about the NetWorker RDZ feature.

Required SMB privileges

SMB backup and recovery require privileges beyond Hyper-V backup and recovery privileges.

The following table describes the required privileges for SMB backup and recovery.

<table>
<thead>
<tr>
<th>SMB configuration</th>
<th>Required privileges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stand-alone file server</td>
<td>Perform one of the following steps:</td>
</tr>
<tr>
<td>Scale-Out File Server</td>
<td>• Add backup permissions for the backup user on all file servers in the cluster.</td>
</tr>
<tr>
<td>Cluster File Server</td>
<td>• Add the backup user as the cluster administrator (domain administrator).</td>
</tr>
<tr>
<td></td>
<td>• When Windows is used as the file server, add server accounts for all cluster nodes and virtual proxies to the local Administrators account of each server in the file server tier.</td>
</tr>
<tr>
<td>Scale-Out File Server</td>
<td>In the Local Backup operator group of each SMB node, configure the application server as a member of the Backup Operators group.</td>
</tr>
<tr>
<td>Cluster File Server</td>
<td>Add each Cluster File Server node to the SMB nodes of the Local Backup Operator group.</td>
</tr>
</tbody>
</table>

Verify that the Hyper-V Server and the file server are in the same domain. Recoveries require the same permissions as backups.

To enable communication between the SMB host and clients, install the File Share Shadow Copy Agent on the file server that hosts the SMB file shares.

Required Hyper-V CSV privileges

During client resource configuration for Hyper-V CSV backups, you must provide the Domain User account and password, instead of providing a Domain Administrator account and password. Perform the following steps to create a domain user and provide the required privileges.

**Procedure**

1. Create a Domain User.
2. Add the following Active Directory security groups to the newly created Domain User:
   - Backup Operators
   - Hyper-V Administrator
   - Windows Authorization Access Group
   - Users
   - Remote Desktop Users
   - Group Policy User Control
   - Group Policy Creator Owners

3. On each cluster node, log in, and then add the Domain User account to the following groups on the local node:
   - Users
   - Administrators
   - Hyper-V Administrators

4. Provide local administrator privileges to the Domain User.

5. Provide access for cluster management to each group. Open Windows PowerShell and type the following command:

   ```powershell
   PS C:\....\NMMEMC> Grant-ClusterAccess -User domain\user -Full
   ```

   This command grants the Domain User account full access to the cluster, which provides access for cluster management to each group.

---

## Backup overview

You can perform full and incremental backups of virtual machines. Perform backups regularly with NMM through NetWorker scheduling.

The backup strategy for a Hyper-V environment must include:

- Stand-alone Hyper-V Servers and Hyper-V images
- Clustered Shared Volumes
- Hyper-V virtual machines over SMB 3.0

NMM does not back up the management operating system. To protect the Hyper-V management operating system, perform a disaster recovery backup with the NetWorker client. The Windows Bare Metal Recovery Solution chapter provides details.

### Note

NMM 9.1 does not support backups of Hyper-V nodes of Windows Server 2012 R2 and Windows Server 2016 in the same cluster. To perform a backup of Windows Server 2012 R2 and Windows Server 2016, you must have separate clusters for Windows Server 2012 R2 and Windows Server 2016. Microsoft provides limited support for server versions of different operating systems in the same cluster, and especially during migration of Windows Server 2012 R2 to Windows Server 2016. Microsoft recommends you not to plan for any backup and recovery activity during an operating system migration. A full backup is recommended before and after migration of operating system.
**Block Based Backups with NMM**

Hyper-V Block Based Backup (BBB) enables faster backups and recoveries. You can perform block based backups as synthetic full and incremental forever for NMM Hyper-V. For details on BBB, refer to the *NetWorker Module for Microsoft Administration Guide*.

NMM 9.0 and later support synthetic full and incremental forever BBB backups:

- **Synthetic full backup**—A synthetic full backup combines a full backup and subsequent incremental backups to form a new full backup. A synthetic full is equivalent to a traditional full backup and can be used in the same ways as a traditional full backup.

- **Incremental forever backup**—An incremental forever backup backs up files that have changed since the last full or incremental backup.

Incremental backups reduce storage consumption, network traffic, and backup time. NMM Hyper-V incremental backups rely on changed block tracking (CBT) in the virtual machine. To enable incremental backup of a virtual machine, Windows Server 2012 and later use the "IncrementalBackupEnabled" property of the "Msvm_VirtualSystemSettingData" data type in WMI v2. Setting this property to "true" enables incremental backups of the virtual machines.

It is a best practice to create the following schedule policies to leverage these backup levels:

- Incremental forever, which is used to perform BBB backups to Double Data Rate (DDR) target.

- Incremental forever full on the first day of the month, which performs a full backup on the first day of each month. This is a best practice for a BBB to an AFTD target because it limits the depth of the differencing chain.

When you create a client, NMM enables incremental backups by default. NMM automatically enables incremental backups for a virtual machine the first time it is backed up. If you disable incremental backups later, NMM re-enables them. No Application Information attribute is available to control this behavior.

NMM promotes incremental backups to full backup under the following circumstances:

- NMM does not find a previous full backup of the virtual machine.

- The required Recovery Snapshot cannot be validated.

- Incremental backup is not enabled for the virtual machine.

When one virtual machine backup is promoted to full, NMM does not promote other virtual machines in the backup set. NMM uses multiple shadow copy sessions by a single backup operation to perform full and incremental backups.

**Adding a virtual machine to an existing incremental backup**

The first instance of all virtual machines backups must be a full backup. When you add a virtual machine to a Hyper-V Server or a failover cluster that is scheduled for writer-level incremental backups, NMM determines that the newly added virtual machine is not enabled for incremental backups because a full backup of the virtual machine does not exist. During the next incremental backup of the writer-level incremental save set, NMM splits the virtual machines into two sets, creates a snapshot for each set, and then backs up each set separately.

- Set of virtual machines for which full backups are available, only incremental backup is performed.
- Set of virtual machines that contains the newly added virtual machine, first a full backup is performed, followed by incremental backup. The backup for this set of virtual machines might take longer to complete.

**VSS backup consistency types with NMM**

The Hyper-V Writer in the management operating system determines if the backup image is application-consistent or crash-consistent. You do not need to select these backup types when performing scheduled backups of virtual machines with NMM.

A crash-consistent backup is performed when Microsoft VSS Integration component (IC) is not installed on the virtual machine. In a crash-consistent backup, the virtual machine is paused before shadow copy creation and resumed after the shadow is created.

An application-consistent backup is performed when IC is installed on the virtual machine. Ensure that the virtual machine is online and VSS-capable. In an application-consistent backup, the IC runs in-guest and freezes the operating system and all application states.

The Microsoft Technet website provides more information about Microsoft application-consistent or crash-consistent backups.

**NMM backup types**

The following table contains descriptions for the supported types of backup.

<table>
<thead>
<tr>
<th>Type of backup</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federated Hyper-V CSV cluster backup</td>
<td>The backup includes virtual machines that are stored on clustered shared volumes.</td>
</tr>
<tr>
<td>Federated Hyper-V CSV cluster over SMB 3.0 backup</td>
<td>The backup includes all cluster virtual machines that are stored on SMB 3.0 file servers.</td>
</tr>
<tr>
<td>Hyper-V Servers standalone backup</td>
<td>The backup includes all virtual machines and the host component.</td>
</tr>
<tr>
<td>Hyper-V Servers standalone over SMB 3.0 backup</td>
<td>The backup includes all standalone virtual machines that are stored on SMB 3.0 file servers.</td>
</tr>
</tbody>
</table>

**Note**

NMM 9.1 supports all these backup types for Hyper-V Server 2016.

**Files included in backups**

NMM backs up the virtual machine files that are listed in the following table:

<table>
<thead>
<tr>
<th>File type</th>
<th>File name extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual hard disk files</td>
<td>.VHDX</td>
<td>For the virtual machines that are created with Windows Server 2012 and later, Hyper-V uses the Microsoft Virtual Hard Disk (VHDX) specification to</td>
</tr>
</tbody>
</table>
### Table 7 Virtual machine files included in backups (continued)

<table>
<thead>
<tr>
<th>File type</th>
<th>File name extension</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Differencing virtual hard disk</td>
<td>.AVHDX</td>
<td>Store virtual hard disks for virtual machines. A virtual machine can have one or more virtual disks.</td>
</tr>
<tr>
<td>disk files</td>
<td></td>
<td>A virtual machine snapshot creates one differencing VHDX file per VHDX.</td>
</tr>
<tr>
<td>Virtual machine configuration</td>
<td>.XML</td>
<td>Hyper-V uses a virtual machine configuration file in XML format to store virtual machine settings (for example, CPU, memory, VHDXs).</td>
</tr>
<tr>
<td>configuration snapshots</td>
<td>.XML</td>
<td>A virtual machine snapshot creates a copy of the current virtual machine configuration and saves it to enable rollback.</td>
</tr>
<tr>
<td>Virtual machine configuration</td>
<td>.BIN .VSV</td>
<td>Hyper-V uses a virtual machine configuration file in XML format to store virtual machine running state (memory) files.</td>
</tr>
<tr>
<td>data files</td>
<td>.vmcx</td>
<td>For Windows 2016, virtual machine configuration data files use a .vmcx file name extension.</td>
</tr>
<tr>
<td>Runtime state data files</td>
<td>.vmrs</td>
<td>For Windows 2016, runtime state data files use a .vmrs file name extension.</td>
</tr>
</tbody>
</table>

### Backup process workflow

The workflow for Hyper-V backups with NMM differs depending on the backup type.

#### VSS backup workflow

The VSS Writer enables the creation of backups for virtual machines by quiescing the Windows operating system and applications within the guest for operating system and application consistency.

The following figure illustrates the workflow for a VSS backup. The workflow is explained in the steps that follow the figure.
During a VSS backup, the following events occur:

1. The NetWorker server sends a request to the NMM client on the Hyper-V management operating system to start the backup for the specified virtual machines.

2. The NMM client sends a request to the VSS framework to create a point-in-time consistent backup for the virtual machine.

3. The VSS framework contacts the Hyper-V Writer and requests that the Writer prepare for volume shadow copy for the specified virtual machine.

4. The Hyper-V Writer establishes a communication path with Hyper-V VSS Integration Components (IC) on the virtual machines that are being backed up.

5. The Hyper-V IC requests a volume shadow copy from VSS inside the virtual machine.

6. Inside the virtual machine, VSS sends a volume shadow copy preparation request to all applications within the virtual machine. All the applications are quiesced, and then control is returned to VSS.

7. VSS creates a volume shadow copy (VSC) inside the virtual machine.

8. VSS returns control to the VSS IC requestor.
9. When the volume shadow copy completes, the Hyper-V VSS IC requestor notifies the Hyper-V VSS writer and CSV VSS writer on the management operating system.

10. The Hyper-V VSS writer returns control to VSS.

11. VSS creates a volume shadow copy (VSC) on the management operating system for the required volumes.

12. The post volume shadow copy process synchronizes the changes between the volume shadow copies created on the virtual machine and the physical host.

13. VSS returns control to NMM.

14. NMM performs a backup from the volume shadow copy.

Ensure that the IC versions for the backup Hyper-V Server and the guest virtual machine match. If you plan to recover the guest virtual machine to an alternate Hyper-V Server, ensure that the alternate Hyper-V Server uses the same version of IC.

Saved state backup workflow

During backup, the virtual machine is put into a saved state and is returned to the previous state after the backup. The backup performed during the saved state is also called an offline backup.

The following figure illustrates the workflow for a saved state backup. The workflow is explained in the steps that follow the figure.
During a saved state backup, the following events occur:

1. The NetWorker server sends a request to the NMM client on the Hyper-V management operating system to start the backup for the specified virtual machines.

2. The NMM client sends a request to the VSS framework to create a point-in-time consistent backup for the virtual machine.

3. The VSS framework contacts the Hyper-V VSS writer and requests a preparation request for a VSC for the specified virtual machine.

4. The Hyper-V VSS Writer sends a request to the hypervisor to put the specified virtual machines into a pause state to freeze the I/O.

5. The Hyper-V VSS Writer returns control to VSS.

6. VSS creates a volume shadow copy (VSC) on the management operating system for the required volumes.

7. The Hyper-V VSS Writer returns the specified virtual machine to running state.

8. VSS returns control to NMM.
9. NMM performs a backup from the volume shadow copy.

Federated backups workflow

NMM supports failover clusters through a federated architecture that manages backup and recovery across the Hyper-V cluster. The federated architecture complies with Microsoft CSV and Hyper-V cluster rules. The federated architecture provides failover resiliency for Hyper-V virtual machines by determining which physical cluster node is running a virtual machine at the time of a backup or recovery operation.

The federated architecture includes two roles:

- **Primary role**—Provides the point of communication for the NetWorker browse, backup, and recovery jobs. The primary role also controls the high-level virtual machine image backup and recovery workflow across the cluster nodes.

- **Secondary role**—Provides a low-level virtual machine image backup and recovery workflow on specific cluster nodes.

You use the Client Backup Configuration wizard to configure the NMM Windows CSV client. After you configure the CSV client, NMM issues browse, backup, and recovery jobs against the NMM CSV client name.

The NMM process starts when NetWorker issues a job (work order) to the NMM Windows CSV client that is operating in the primary role. For virtual machine image backup and recovery operations, the primary role determines which cluster nodes run the virtual machines that are specified in the job (workorder), and then dispatches sub-jobs to the cluster nodes. The sub-job starts an NMM process on the target cluster node, and that process operates in the secondary role. The secondary role manages the CSVs and interacts with the Hyper-V VSS writer for backup and recovery operations.

The following figure illustrates the primary and secondary CSV backup workflows in Hyper-V federated backups.

*Figure 7 Primary and secondary CSV backup workflows in Hyper-V federated backups*
CSV federated backup with no proxy node

This topic describes the process for a Hyper-V federated backup with no proxy node.

1. The NMM client receives the save sets, which list the virtual machines to back up, from the NetWorker Server.
2. The NMM client calls the Clustered Shared Volumes (CSV) API to discover the required CSV.
3. The NMM client calls the Hyper-V VSS Writer and CSV VSS Writer to select the virtual machines for the image backup and to create a shadow copy with the point-in-time copy of the virtual machine files.
4. The NMM client backs up the virtual machine files from the shadow copy to the NetWorker server.

CSV federated backup with proxy node

During a CSV federated backup with a proxy node, the following events occur:

1. The NMM client receives the save sets, which list the virtual machines and the proxy servers to back up, from the NetWorker Server.
2. The primary NMM client starts the backup on the proxy server.
   a. The Windows cluster master node creates a primary NMM backup process that moves the CSV to the proxy nodes and takes a snapshot of the CSV.
   b. A secondary NMM backup process, which copies data from the snapshot to backup media, starts on the proxy nodes.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>If no proxy node is specified, the primary node acts as the proxy.</td>
</tr>
</tbody>
</table>

3. The virtual machine files are backed up from the shadow copy to the NetWorker server.

SMB 3.0 federated backup

During a SMB federated backup, the following events occur:

1. The NMM client receives the save sets, which list the virtual machines to back up, from the NetWorker Server.
2. The Hyper-V and cluster APIs determines the node where the virtual machine is running.
3. The secondary job on the node takes the snapshot of the VM using Hyper-V writer.
4. The data is copied from the snapshot using the proxy nodes.

Recovery overview

The following recovery options are available when you perform regular backups as discussed in Backup overview on page 23:

- Perform a recovery of a virtual machine to its original location on the original Hyper-V Server.
- Perform a redirected recovery of a virtual machine to a different location on the original Hyper-V server.
Perform a redirected recovery of a virtual machine to an alternate Hyper-V server.
Perform a granular level recovery (GLR) of individual files and folders.

Types of supported recovery

NMM supports two types of recoveries:

- Recovery of the virtual machine
- Recovery of the files and folders in the virtual machine (Granular or file level recovery)

<table>
<thead>
<tr>
<th>Type of recovery</th>
<th>GUIs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery of the virtual machine:</td>
<td>Using the NetWorker User for Microsoft GUI</td>
</tr>
<tr>
<td>- When multiple virtual machines are recovered to original location</td>
<td></td>
</tr>
<tr>
<td>- When only one virtual machine is recovered at a time to the alternate location</td>
<td></td>
</tr>
<tr>
<td>Recovery of the files and folders in the virtual machine (granular or file level recovery)</td>
<td>- Using the NetWorker User for Microsoft GUI</td>
</tr>
<tr>
<td></td>
<td>- Using a browser based interface</td>
</tr>
<tr>
<td>Recovery of all System Center Virtual Machine Manager (SCVMM) managed virtual machines that have NMM conventional backups</td>
<td>Using the EMC Data Protection Add-in for SCVMM GUI</td>
</tr>
</tbody>
</table>

Note

NMM 9.1 does not support:

- Any new feature of Hyper-V 2016 for backup and recovery, for example Production Checkpoints, Export/Import based backup.

While you can perform either import based or VSS based recovery for Windows Server 2012 R2, you can perform only import based recovery for Windows Server 2016.

Recovering to the original Hyper-V Server

You might need to recover a virtual machine to its original location or a different location on the original Hyper-V Server from which the backup was performed.

Note

When you recover a virtual machine to its original location, the recovery process deletes or overwrites all files on the virtual machine. If the recovery is performed to an alternate location on the original Hyper-V server then the files are not over-written.

Recover to the original location when:
- You must roll back the virtual machine because a patching or virus issue occurred.
- You must perform disaster recovery of the virtual machine after a disk failure.
- The virtual machine was accidentally deleted.

Performing Hyper-V recovery to the original machine and location on page 60 describes how to recover a virtual machine to the original location.

**Redirected recovery of a virtual machine to an alternate Hyper-V Server**

You can recover a virtual machine to an alternate Hyper-V server.

To perform the recovery:

- Select a different Hyper-V server for the virtual machine recovery process.
- Select a different file system location for the files on the original Hyper-V Server.
- In a clustered environment, select the CSV where the files will be placed during a recovery.

NMM supports redirected recoveries to a host running the same or later operating system version. For example: NMM supports redirected recovery from a Windows Server 2012 R2 source host to a Windows Server 2012 R2 destination host, but NMM does not support redirected recovery from a Windows Server 2012 R2 source host to a Windows Server 2012 destination host.

Performing a directed Hyper-V recovery to a different host or location on page 61 describes how to recover a virtual machine to an alternate Hyper-V Server.

**Granular level recovery**

Hyper-V Granular Level Recovery (GLR) provides the ability to recover specific files from a virtual machine image backup without recovering the full virtual machine, reducing the recovery time. The NMM GLR feature uses Networker Block Based Backup (BBB) APIs to mount the virtual machine that contains the items to recover.

- You can only use GLR for virtual machines running Windows operating systems.
- User files or folders from a virtual machine backup can be restored using GLR as flat files.
- GLR can be used to recover SQL Server, Exchange Server, and SharePoint Server data that are stored in Hyper-V virtual machine.

The following figure illustrates an environment where NMM is installed on a virtual machine to perform a GLR.
NMM 9.1 compatibility with NetWorker 8.2.3 or later servers

NMM supports backup and recovery with NetWorker client version 9.1 and NetWorker 8.2.x server.


Note the following limitations when you configure NMM backup and recovery with a NMM 9.1 client and a NetWorker 8.2.3 server or later:

- Dedicated Storage Node—NetWorker 8.2.x server does not support NetWorker storage node 9.1. As a result, you cannot configure a dedicated storage node when you use NetWorker 9.1 client with NetWorker 8.2.x server.

- Volume affinity—NetWorker 8.2.x server does not support the volume affinity feature. NetWorker server 9.0 and later support the volume affinity feature. For NMM Exchange and Hyper-V, if the same volume or a volume from the same Data Domain device and taken from a prior backup cannot be obtained, an incremental-level backup is promoted to level full.

- Backup levels—NetWorker 8.2.x server uses NetWorker server 8.x backup-level definitions, and it does not support the NetWorker server version 9.0 and later backup levels.
CHAPTER 2

Backups

This chapter includes the following sections:

- Planning backups ................................................................. 36
- Configuring backups .......................................................... 41
- Performing cluster-level and CSV virtual machine backups .......... 43
- Configuring multi-proxy backups ......................................... 43
- Creating multiple snapshots of CSV volumes in Hyper-V scale-out environments .............................................................. 47
- Configuring a client resource by using the Client Backup Configuration Wizard ................................................................. 47
- Configuring a client resource manually by using the NetWorker Management Console ................................................................. 52
Planning backups

This section contains information and considerations to review before backing up Hyper-V virtual machines.

Viewing valid application data save sets

When manually configuring a client resource in the NMC, type the save sets in the Save Set attribute.

To view the list of the application data save sets that is available for backup:

Procedure

1. Open a command prompt on the Hyper-V Server and type the required command.
2. If the Hyper-V Server is a stand-alone host, then type the following command and press Enter:
   \nsrnmmsv -P
3. If the Hyper-V Server is configured as a cluster, then type the following command and press Enter:
   - For SMB configurations:
     \nsrnmmsv -P -A NSR_FEDERATED_BACKUP=yes -A NSR_FEDERATED_TYPE=smb
   - For CSV configurations:
     \nsrnmmsv -P -A NSR_FEDERATED_BACKUP=yes -A NSR_FEDERATED_TYPE=csv

The following examples show the application data (Hyper-V guest virtual machine) save sets that are available on a Hyper-V system with two virtual machines, virtual_machine_name_1 and virtual_machine_name_2, on stand-alone and cluster virtual hosts:

- On a stand-alone virtual host:
  "APPLICATIONS:\Microsoft Hyper-V"
  "APPLICATIONS:\Microsoft Hyper-V\Host Component"
  "APPLICATIONS:\Microsoft Hyper-V\virtual_machine_name_1"
  "APPLICATIONS:\Microsoft Hyper-V\virtual_machine_name_2"

- On a cluster virtual host:
  "APPLICATIONS:\Microsoft Hyper-V"
  "APPLICATIONS:\Microsoft Hyper-V\Host Component"
  "APPLICATIONS:\Microsoft Hyper-V\non-csv"
  "APPLICATIONS:\Microsoft Hyper-V\vm27_rename1"
Note
Remove the leading and trailing quotes (""") when copying the save set name from the output to the Save Set attribute in the client resource. Each line of output corresponds to a save set entry that you can add to the Save Set attribute of a client resource. Type each entry that you add to the Save Set attribute on a separate line.

Integration services components version

Ensure that the IC version that runs inside the virtual machine is the same as the version of Hyper-V on the host. A mismatch in versions may lead to backup failures.

Check the Hyper-V version on the server by starting the Hyper-V Manager and then selecting About Hyper-V Manager from the Help menu.

Check the IC version:
1. In the Device Manager application inside the guest virtual machine, on System Devices, select Device Manager.
2. Right-click the entry Microsoft Hyper-V Volume Shadow Copy.
4. Check the IC version on the Driver tab.

If the IC version does not match the Hyper-V version, insert the integration services disk by choosing that option under the Action menu in the virtual machine console. Install the integration components, and then restart the virtual machine.

Special character considerations

You can use all foreign language characters and certain special characters in virtual machine names and virtual machine configuration paths, for stand-alone, CSV, and SMB 3.0 configurations.

You must use the NetWorker User for Microsoft GUI to recover backups of virtual machines with special characters and unicode characters in virtual machine name, VHD Paths, VHD name, and so on. The NMM Hyper-V File Level Restore (FLR) GUI and EMC Data Protection Add-in for SCVMM GUI cannot be used for this.

Note
NMM has been qualified with German, Spanish, French, Simplified Chinese, Traditional Chinese, and Japanese.

The following table lists the special characters that are supported by NMM Hyper-V:

<table>
<thead>
<tr>
<th>Special character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A–Z, a–z, 0–9</td>
<td>Alphanumeric</td>
</tr>
<tr>
<td>-</td>
<td>Dash</td>
</tr>
<tr>
<td>.</td>
<td>Period</td>
</tr>
</tbody>
</table>
### Table 9 Special characters supported in NMM (continued)

<table>
<thead>
<tr>
<th>Special character</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>_</code></td>
<td>Underscore</td>
</tr>
<tr>
<td><code>{ }</code></td>
<td>Curly brackets</td>
</tr>
<tr>
<td><code>+</code></td>
<td>Plus</td>
</tr>
<tr>
<td><code>=</code></td>
<td>Equal</td>
</tr>
<tr>
<td><code>~</code></td>
<td>Tilde</td>
</tr>
<tr>
<td><code>!</code></td>
<td>Exclamation</td>
</tr>
<tr>
<td><code>#</code></td>
<td>Hash</td>
</tr>
<tr>
<td><code>$</code></td>
<td>Dollar</td>
</tr>
<tr>
<td><code>%</code></td>
<td>Percentage</td>
</tr>
<tr>
<td><code>)</code></td>
<td>Right parenthesis</td>
</tr>
<tr>
<td><code>(</code></td>
<td>Left parenthesis</td>
</tr>
<tr>
<td><code>&amp;</code></td>
<td>Ampersand</td>
</tr>
<tr>
<td><code>^</code></td>
<td>Carat</td>
</tr>
<tr>
<td><code>@</code></td>
<td>At sign</td>
</tr>
<tr>
<td><code>&lt;</code></td>
<td>Less-than sign</td>
</tr>
<tr>
<td><code>&gt;</code></td>
<td>Greater-than sign</td>
</tr>
<tr>
<td><code>*</code></td>
<td>Asterisks</td>
</tr>
<tr>
<td><code> </code></td>
<td>Space</td>
</tr>
<tr>
<td><code>;</code></td>
<td>Semi colon</td>
</tr>
<tr>
<td><code>:</code></td>
<td>Colon</td>
</tr>
<tr>
<td><code>,</code></td>
<td>Comma</td>
</tr>
<tr>
<td>`</td>
<td>`</td>
</tr>
<tr>
<td><code>\</code></td>
<td>Backtick</td>
</tr>
</tbody>
</table>

Examples of usage of special characters:
- Virtual machine name: VM@emc%1%
- VHD paths: C:\folder\&^%
- VHD names: C:\folder\VM@emc(1).vhd
- Files and folders inside virtual machine: samplefile!@#.txt
- Folder paths: C:\folder\&^\sample.txt
- Mount paths: C:\mountSpicharvms\!@#$%
Backups are skipped if:

- Double quotes ("), single quotes ('), square brackets ([ ]), forward slash (/), or question mark (?) is used in virtual machine names.
- The path of a mount point location contains a special character, for example C: \GLRmnt_!@#$^^;,. 

The system hangs if back slash (\) is used in virtual machine names.

**Windows Server 2012 and 2012 R2 Hyper-V CSVs**

For Windows Server 2012 and 2012 R2, Microsoft has released several special requirements and special APIs to support backup applications. A backup application can back up all the CSVs from a single node. CSVs are not required to be put in I/O Redirection Mode as with previous Microsoft OS releases, and CSVs can be backed up in parallel.

The Windows Server 2012 and 2012 R2 interoperability backup application is CSV-aware because the CSV writer metadata information must be updated to its component name by querying the primary server for CSV resources.

In Windows Server 2012 and 2012 R2, the new CSV VSS writer can report the backup components on the behalf of a different cluster node. This CSV VSS Writer can also take the snapshots of volumes on the remote node. These features enable NMM to back up not only the local image of a Hyper-V virtual machine, but also to back up the image that is on a remote node. This allows for more configuration options. For example, you can dedicate a single node to back up the cluster.

**Manually configuring highly available backups (cluster-aware backups)**

Due to enhancements in Windows Server 2012 and 2012 R2 CSVs, you can back up CSV virtual machines as part of a highly available (cluster-aware) backup or a physical proxy node backup. Cluster-aware backups are highly available because you install NMM on each node in the cluster. If one node is not available, NMM starts the backup from the node that resolves to the cluster server name at runtime.

The following procedure describes how to configure the backup manually.

**Procedure**

1. Install NMM on each node in the cluster.
2. Create an empty (placeholder) NetWorker client resource for each node in the cluster.
3. Create a client resource for the cluster server name and specify the save sets to back up. Add this client to a backup group.
4. At runtime, the cluster server name resolves to one of the nodes in the cluster. This node becomes the master backup node.

**Windows Server 2012 R2 shared VHDX files**

In Windows Server 2012 R2, NMM does not support VHDX backups when the Microsoft option "Enable virtual hard disk sharing" is enabled. Virtual machines with shared VHDX virtual machines are ignored and the back-up continues with the rest of...
the save set. To protect the data in a VHDX that is virtual hard disk sharing enabled, install the NMM software on the guest virtual machine and run the backup inside the guest virtual machine.

Backups over SMB 3.0

NMM supports Hyper-V virtual machines residing on Windows Server 2012 and 2012 R2 SMB 3.0. You back up stand-alone servers and non-CPS failover clusters over SMB the same way you back up local virtual machines. To backup SMB 3.0 Hyper-V cluster, NMM uses a federated backup architecture.

Hyper-V incremental backup and differencing disks

Hyper-V VSS Writer uses differencing disks to capture changed blocks between backups.

A differencing disk is a VHD that contains changes for another VHD or the guest operating system. Differencing disks are stored in the same subdirectory as the parent VHDx for the virtual machine. This location is not configurable.

Incremental changes since the last checkpoint or backup are written to a new differencing disk. This differencing disk gets merged to its parent disk after the backup completes. When a snapshot occurs as part of a backup, a new differencing disk is created. This new differencing disk receives all the writes until the next backup starts. The backup saves the differencing disk as part of an incremental backup. If you create checkpoints, then multiple differencing disks can be present on the system. If you do not create checkpoints, there is one differencing disk present along with parent disk.

To estimate the required additional primary storage for differencing disks, consider the rate of changes happening inside the virtual machine. As a virtual machine grows, it requires more storage space on the primary disk. NMM logs how much data it has backed up for each backup.

Disabling incremental backups and enabling only full backups

By default, when Hyper-V backups are performed by using NMM, the first instance of the backup is always full and subsequent backups are incremental. Hyper-V enables Change Block Tracking (CBT) for all the VHDXs associated with a virtual machine. After the first instance of the backup, that is full backup, NMM performs an incremental backup and Hyper-V creates a differencing Virtual Hard Disk (AVHD). All data changes to the virtual machine during the backup and after the backup go to the differencing disk. The AVHD can grow in size if there are a number of changes in the virtual machine between two backups, which may require extra space on the production storage, for example, CSV, SMB shares, or local disk.

The "Hyper-V incremental backup and differencing disks" section describes how differencing disks are created between backups when CBT is enabled.

NMM 9.1 provides the user with the option to perform only full backups, instead of full and incremental backups. To ensure that only full backups are performed, the user must disable CBT. When CBT is disabled, the differencing disk is not created. A user has the option to enable CBT or disable CBT at anytime as per their business needs.

When a user disables CBT in an existing environment, the previously created differencing disks are merged after the backup.

The "Configuring a client resource by using the Client Backup Configuration Wizard" section and the "Configuring a client resource manually by using the NetWorker
Management Console” provide details about how enable or disable incremental backups for Hyper-V when creating a client resources for backups.

**Hyper-V virtual machine checkpoints merged after backup**

Hyper-V checkpoints are of two types: Backup checkpoints and user created checkpoints.

Hyper-V users can use the Hyper-V management interface to create checkpoints for a virtual machine to capture the virtual machine state at strategic points of their own choice.

Both these types of checkpoints create differencing disks that provide roll back capabilities to these strategic points.

When NMM performs either full or incremental backup of the Hyper-V virtual machine, the differencing disks that are created for the backup checkpoints are merged by NMM on the backup media. The Hyper-V management interface continues to display the checkpoints even after the backup is complete. Because the differencing disks are merged on the backup media after backup is complete, the checkpoints are not displayed in Hyper-V management interface after restore.

Currently, the shipping versions of Hyper-V do not recommend user created checkpoints for production virtual machines.

---

**Note**

When a user disables CBT, the differencing disks that are created for the virtual machine checkpoints are not merged on the backup media after the backup.

---

**Client Direct to AFTD or Data Domain Boost storage devices**

The Client Direct feature reduces bandwidth usage and bottlenecks at the storage node and provides highly efficient backup data transmission.

NMM performs Hyper-V Server backups by using Client Direct, which enables clients with network access to AFTD or Data Domain Boost storage devices to send their backup data directly to these devices, bypassing the NetWorker storage node. The storage node manages the devices for the NetWorker clients, but does not handle the backup data. Ensure that the clients have the required permissions or accessibility to the target device, otherwise backups fail.

---

**Note**

When using an AFTD device, configure the device using UNC path.

When you create a client resource, NetWorker enables the Client Direct feature by default. The `nsrnmmsv.raw` backup log displays details about the Client Direct activity for the Hyper-V server.

The *NetWorker Administration Guide* provides details about the Client Direct to AFTD and Data Domain Boost storage devices.

---

**Configuring backups**

When configuring backups, the backup tasks differ depending on the items to back up.

The following table describes the backup tasks you must perform when using NetWorker server 9.1 and NMM 9.1 to back up Hyper-V parent and virtual machines.
The *EMC NetWorker Release Administration Guide* provides detailed information about how to perform the tasks in the table.

**Table 10 Backup tasks for Hyper-V**

<table>
<thead>
<tr>
<th>Items to back up</th>
<th>Backup tasks to perform</th>
</tr>
</thead>
</table>
| **On the server**                      | 1. Configure the NetWorker devices for backup storage.  
2. Configure a backup group.  
3. Configure one or more client resources for each client. Configuring a client resource by using the Client Backup Configuration Wizard on page 47 and Configuring a client resource manually by using the NetWorker Management Console on page 52 provide details.  
4. Configure a data protection policy for scheduled backups, including selecting a group, policy, policy workflow, and backup action.  
**Note**  
When using NetWorker server 8.2.3 or later, configure a regular NetWorker backup group instead of configuring a data protection policy. Do not enable the Snapshot option in the Group Properties page.  
5. Configure required NetWorker privileges.  
6. Configure backup proxies.                                                                                                                                                                                                                                                                 |
| **Hyper-V on the server**              | 1. Configure the backup storage resources.  
2. Configure a backup group.  
3. Configure one or more client resources for each client. Configuring a client resource by using the Client Backup Configuration Wizard on page 47 and Configuring a client resource manually by using the NetWorker Management Console on page 52 provide details.  
4. Configure a data protection policy for scheduled backups, including selecting a backup group, policy, policy workflow, and backup action.  
**Note**  
When using NetWorker server 8.2.3 or later, configure a regular NetWorker backup group instead of configuring a data protection policy. Do not enable the Snapshot option in the Group Properties page. |
| **Hyper-V virtual machines and Host Component file** | Install NMM on the virtual machine operating system and configure application backups with NMM installed within the virtual machine operating system:  
- Configure Windows application backups.  
- Configure Windows Server cluster backups.  
Specific instructions for the Microsoft application are provided in the application-specific user guides.                                                                                                                                                                                                                       |
Performing cluster-level and CSV virtual machine backups

NetWorker performs CSV virtual machine backups through a client resource that is created for the cluster virtual server only. You create client resources for all the nodes in the cluster and for the cluster server. However, the backup is scheduled against the cluster virtual server client resource only. NetWorker indexes the backup against the cluster server name.

NMM supports backups for all CSV virtual machines as well as individual CSV virtual machines. Configuring backups on page 41 provides details about how to perform Hyper-V backups.

Note
A Hyper-V CSV distributed backup supports only conventional backups from a temporary shadow copy (rollover). NMM does not support proxy host backups and instant backups that use persistent point-in-time shadow copies.

Performing a CSV-level federated backup

To perform a CSV-level federated backup, you must set the Application Information attributes for the cluster virtual server and the client resource.

Apply the following settings:

- Set the save set attribute Applications: Microsoft Hyper-V in the client resource for the cluster virtual server to back up all the CSV virtual machines in the cluster.
- Add NSR_FEDERATED_BACK=YES and NSR_FEDERATED_TYPE=CSV to the Application Information attribute in the client resource.

Performing a CSV virtual machine backup

To perform a CSV virtual machine backup, set the save set attribute APPLICATIONS: Microsoft Hyper-V in the client resource for the cluster virtual server to back up the CSV virtual machine in the cluster.

NMM supports backup of non-clustered virtual machines that run on specific cluster nodes. NMM excludes virtual machines that do not reside on the CSV from the CSV backup. Backup and recovery of non-clustered virtual machines is managed through the individual physical node name, not the cluster virtual server client resource. The physical node name is the client resource name.

Configuring multi-proxy backups

To meet backup windows for larger Hyper-V environments, you can improve performance by scaling out the Hyper-V CSV backups to multiple cluster nodes or proxies.

When you create multiple proxies, NMM should be installed on all cluster nodes and virtual proxies. There must be client resources for all the cluster nodes, virtual proxies, and cluster alias.

You add secondary roles, which must be physical or virtual cluster nodes. You specify the proxy host by setting NSR_FEDERATED_PSOL in the Application Information for the client resource of the cluster, or by using the Preferred Server Order List (PSOL) in...
the Client Configuration Wizard. The PSOL distributes the backup workload across all servers in the PSOL. You schedule the backups against the cluster alias, and the primary role runs on the cluster node that owns the cluster alias. The recovery process for virtual machines that are backed up as part of a multi-proxy setup is the same as the recovery process for traditional backups.

In a multi-proxy architecture, you can select multiple cluster nodes to act as proxy nodes to perform parallel backups on all proxy nodes. An NMM CSV algorithm is used to intelligently reassign virtual machines to proxies and, if the `NSR_MOVE_CSV_OWNERSHIP` application information attribute is set to `Yes`, assign CSVs to proxies. The backup load is evenly split between multiple nodes. All proxy nodes perform backups in parallel, significantly increasing backup performance compared with single proxy backups in a normal distributed CSV environment. You can add or remove proxy nodes as needed.

NMM takes a single snapshot of the Windows Server 2012 and 2012 R2 Hyper-V cluster from the controlling node. NMM mounts the snapshot on the primary node and shares it among the secondary nodes. This makes the snapshot process faster.

If all the selected proxy nodes are unavailable, then NMM performs the backup on the node to which the cluster alias is resolved.

**Hyper-V intelligent proxies**

NMM allows you to use virtual machines on a Hyper-V cluster as proxy nodes for CSV backups. NMM intelligently reassigns and load balances the virtual machines in the backup to the selected virtual proxy nodes. All virtual proxy nodes will perform backups in parallel, thus increasing backup performance. These virtual proxies must be highly available cluster Hyper-V virtual machines, and they must be connected to the same domain as the physical nodes. A mix of physical and virtual machines is supported. NMM automatically excludes the virtual machines for the virtual proxies from backups.

The NMM controller node is the cluster node on which the cluster alias is active. All servers in the PSOL are treated as proxies. Before starting the distribution of CSVs, the controller validates all the servers in the PSOL and excludes any unavailable nodes from the PSOL. It is a best practice to configure more proxies in the PSOL so that a spare node will always be available. Because NMM uses the cluster alias to schedule cluster backups, NMM is immune to node failures. If the currently active node fails, the cluster alias moves to a different node.

The CSV ownership distribution algorithm logic tries to distribute the CSVs among the proxies equally. For example, in an 8-node cluster with 4 CSVs:

- If two servers are in the PSOL, then NMM backs up two CSVs per proxy.
- If four servers are in the PSOL, then NMM moves the CSV ownership for maximum performance and backs up one CSV per proxy.
- If five servers are in the PSOL, then NMM backs up one CSV per proxy for four of the servers.

**Multi-proxy backup components**

In addition to the existing single proxy client components, NMM uses the following software components in multi-proxy backups:

- **Main proxy client**—NMM schedules and browses backups against the cluster server name (cluster alias). The NMM process that starts on the active node of the cluster alias is the main proxy client. The main proxy client node acts as the primary node in the cluster.
- **Client software**—You must install the NetWorker and NMM client software on all secondary proxy nodes. This ensures tolerance for node failures, because the cluster alias ownership can change.
• CSV ownership distribution algorithm—When the **NSR_MOVE_CSV_OWNERSHIP** value is **Yes**, NMM changes the coordinator node of the CSV.
  - The CSV coordinator node owns the storage stack for the CSV. Although other nodes might read and write files on the CSV through the SCSI stack, all metadata operations go to the coordinator node.
  - The CSV coordinator node also owns the VSS software shadow copy for the CSV. In this case, I/O on the coordinator node is local, but I/O of the shadow copy volume from other nodes is redirected to the coordinator node over the network.
  - When CSV ownership moves, the software shadow copies for that CSV also move.
  - NMM evenly distributes the backup load across the proxy nodes you select, and the proxy nodes perform backups in parallel to maximize the backup performance. Also, if you want to have an optimized I/O path to the CSV shadow copy for the proxy nodes, select to move CSV ownership.

• Application Information attributes—You can configure Hyper-V CSV options by using the Client Configuration wizard or by using the NetWorker Management Console to edit the client resource for the cluster alias. To enable multi-proxy backups by using the NetWorker Management Console, add the following Application Information attributes on the main proxy client:
  - **NSR_FEDERATED_PSOL**—Enables multi-proxy backups and distributes the backup workload across all servers in the PSOL.
    
    For example:
    ```
    NSR_FEDERATED_PSOL=server1, server2, server 3
    where server1, server2, and server3 acts as proxy servers.
    ```

    **Note**
    
    If you do not specify **NSR_FEDERATED_PSOL**, NMM performs the backup from the current active node and substitutes the cluster master node as the proxy node. If you specify values for **NSR_FEDERATED_PSOL**, NMM performs backups from all the valid, available nodes in the list. If the number of nodes is greater than the number of CSVs, NMM excludes the nodes that exceed this number.

  - **NSR_MOVE_CSV_OWNERSHIP**—Uses the CSV ownership distribution algorithm to allow or disallow CSV ownership change during multi-proxy backups for best backup performance. After you initially create the client resource, you can allow or disallow CSV ownership changes as needed.
    
    For example:
    ```
    NSR_MOVE_CSV_OWNERSHIP=Yes
    NSR_MOVE_CSV_OWNERSHIP=No
    ```
    
    The default value is **Yes**. If you set the value of this attribute to **Yes**, then NMM changes the CSV ownership. If you set this attribute value to **No**, then NMM does not change the CSV ownership.

    **Note**
    
    To achieve the highest levels of performance with software snapshots on a CSV, it is recommended to scale up the bandwidth of intra-node communication.
Configuring multi-proxy backups in an SMB configuration

To achieve better backup performance for Hyper-V over SMB Cluster environments on Windows Server 2012 R2, you can use parallel federated, multiple proxy-based backups.

In a parallel federated multi-proxy architecture, you can select multiple SMB cluster nodes to act as proxy nodes. These nodes perform parallel VSS snapshots and parallel federated data backups on all the selected proxy nodes. The backup load is evenly distributed between all proxy nodes (as much as possible) to perform backups in parallel, thus significantly increasing backup performance compared to the existing "federated or single proxy" backup method. NMM also supports virtual machines running on a Hyper-V cluster as proxy nodes for performing Hyper-V over SMB cluster backups on Windows Server 2012 R2.

To use this backup method, add NSR_FEDERATED_BACKUP=yes, NSR_FEDERATED_TYPE=SMB, and NSR_FEDERATED_PSOL=node1, node2, node3 to the client resource of the cluster.

Best practices for configuring multi-proxy backups

You can improve multi-proxy backup performance by following best practices for configuring and allocating Hyper-V proxies.

The following section describes the components that affect multi-proxy backup performance. This section also describes best practices for configuring these components to achieve best backup performance.

Load balance virtual machine data on CSVs

To attain maximum backup performance, load balance virtual machine data on all the available CSVs as much as possible.

NMM performs load balancing by running a correlational factor of the number of virtual machines residing on the CSVs and the common size share. NMM calculates a 'set of CSV' for a 'set of virtual machine' whose maximum common share resides on those CSVs.

NMM moves this set of CSV to one proxy and backs up the set of corresponding virtual machines from that node. Maintaining proper CSV load balance results in fewer CSV ownership changes.

Allocate the number of proxy nodes and CSVs

When determining how many proxy nodes to use, you should allocate the maximum number of proxy nodes to gain maximum backup performance. Increasing the number of proxy nodes can improve backup performance. However, this maximum number of proxy nodes should be less than or equal to the maximum number of CSVs.

For best performance, the number of CSVs should be multiples of the number of proxy nodes. Each virtual machine should be contained within a single CSV only, rather than distributed across multiple CSVs.

Allow CSV ownership change

To achieve maximum backup performance, change CSV ownership to the nodes with less CSV data. CSV ownership change allows the NMM CSV algorithm to intelligently
change CSV ownership to the proxy nodes you selected, thus correctly load balancing the backup data. NMM performs the data split per CSV, not per virtual machine.

Select proxy nodes with good system resources

Backups can be an intensive operation on system resources. To attain the best backup performance, select cluster nodes with maximum resources available as proxy nodes. Select nodes with minimal live data movement, so that the backup operation does not disturb the day-to-day production activities.

Creating multiple snapshots of CSV volumes in Hyper-V scale-out environments

NMM 9.0 and earlier uses the "single snapshot" feature as the default method for protecting Hyper-V CSV environments. The Client Backup Configuration wizard enables the user to create client resources for the single snapshot feature.

In Hyper-V scale-out environments, the CSV Writer might fail to create a single snapshot of all the virtual machines. In single snapshot, the CSV Writer from the cluster owner node performs a snapshot of all virtual machines running on different nodes of the cluster.

In NMM 9.0.1 and later, a number of snapshots can be created instead of a single snapshot of the entire CSV environment. To achieve this, the virtual machines are grouped by the CSV volumes on which they are present. The CSV Writer then creates a snapshot for each group of virtual machines.

To create multiple snapshots, the user must specify an additional Application Information attribute to create multiple snapshots of CSV volumes. Manually create the client resource by using the NMC, and type the attribute NSR_MAX_CSV_PER_SNAPSHOT=<number of CSVs in the cluster> in the Application Information field. Where the value of the attribute NSR_MAX_CSV_PER_SNAPSHOT can be one to the number CSVs in the cluster.

Configuring a client resource manually by using the NetWorker Management Console provides the procedure on manually creating a client resource.

Configuring a client resource by using the Client Backup Configuration Wizard

The Client Backup Configuration wizard for Hyper-V simplifies configuration of scheduled backups for Hyper-V servers. The NMM client must be installed on all Hyper-V cluster nodes for the Client Backup Configuration wizard to function correctly. The wizard automatically configures Hyper-V save sets, backup commands, Application Information attributes, and backup options. Use the wizard to configure client resources for stand-alone and federated environments.

Before you begin

Before you use the wizard, review the following requirements:

- Ensure that the NetWorker server host is listed in the servers file on the client computer.
- Ensure that the communication between the NMC server, NetWorker client, and NetWorker server uses nsrauth strong authentication.
- Ensure that the user who runs the wizard meets the following requirements:
- Root (UNIX) or Administrator (Windows) privileges.
- A member of a User Group on the NetWorker server that has Configure NetWorker privileges.

- Ensure that multiple wizard hosts are not trying to access the same client computer simultaneously.
- Ensure that the NetWorker server host is listed in the servers file on the client computer.
- Ensure that the communication between the NMC server, NetWorker client, and NetWorker server uses nsrauth strong authentication.
- Ensure that the user who runs the wizard meets the following requirements:
  - Root (UNIX) or Administrator (Windows) privileges.
  - A member of a User Group on the NetWorker server that has Configure NetWorker privileges.
- Ensure that multiple wizard hosts are not trying to access the same client computer simultaneously.

**Note**
If using NetWorker server 8.2.3 or later and NMM 9.1:

- Ensure that JRE 8 is installed on the system where NMC is used for the Client Backup Configuration wizard to function properly. While the NetWorker Management Console (NMC) for NetWorker 8.2.3 and later is compiled with JRE 7, NMM 9.1 Java plugin for NMC is compiled with JRE 8.
- The procedure used to create a client resource when using NetWorker server 8.2.3 and later is different from the procedure used to create a client resource when using NetWorker server 9.1. Follow the procedure provided in the Scheduled Backup chapter of each application user guide.
- Prior to running the NMM 9.1 Client Backup Configuration wizard to modify a client resource that was created by using NMM 8.2.x, ensure that the Snapshot attribute of the NetWorker group that this client resource belongs to is clear. If the Snapshot attribute is left selected, the NetWorker group cannot be selected in the wizard and you are prompted to create or select another group.

**Note**
This requirement does not apply to SQL Server VDI and Active Directory.

**Procedure**

1. Use NMC to connect to the NetWorker server.
2. In the Administration window, click Protection.
3. In the expanded left pane, right-click Clients, and then select New Client Wizard.
   
   The Client Backup Configuration wizard appears, starting on the Specify the Client Name page.
4. In the Client Name field, type the name of the client where NMM is installed:
   - For federated backups, type the cluster server name.
   - For non-federated backups, type the stand-alone Hyper-V server name.
5. Optionally, in the **Comment** box, type a description of the client. If you are creating multiple client resources for the same NetWorker client host, then use this attribute to differentiate the purpose of each resource.

6. In the **Tag** box, type one or more tags to identify this Client resource for the creation of dynamic client groups for data protection policies. Place each entry on a separate line.

7. In the **Type** box, select **Traditional NetWorker client**.

8. Optionally, from the **Group** list, select a group for the Client resource. The group to which the client belongs determines the workflow that is used to back up the client.

   **Note**
   
   You can also assign the client to one or more groups after you create the Client resource.

9. Click **Next**.

10. On the **Specify the Backup Configuration Type** page, select **Hyper-V Server** and click **Next**.

11. On the **Select the NetWorker Client Properties** page:
   - Select the priority level in the **Priority** field.
   - Select the level of parallelism in the **Parallelism** field.
   - Leave the **Remote Access** field empty.
   - Select the device type from the **Data Domain Interface** list.
   - Select the **Parallel Save Streams** option to enable multiple save streams for each save set during backup.

   **Note**
   
   To use the default NetWorker Client settings, do not update the options that are provided on the page.

12. Click **Next**.

   The **Select the Hyper-V Backup Objects** page appears. The **Select the Hyper-V Backup Objects** page automatically discovers the save sets depending on the operating system type and client name. By default, all save sets are selected for backup.

13. To exclude a save set from the backup, perform the following steps:
   a. Select the top level save set.
   b. Select the **Exclude Component List** option that appears at the bottom of the page.
   c. Clear the save set that you want to exclude from the backup.

14. Click **Next**.

   The **Specify Backup Options** page appears.

15. On the **Specify Backup Options** page:
- For federated setups—The wizard creates empty (placeholder) client resources for all nodes that are not used to perform the backup. The wizard also creates a client resource with the cluster name and specifies the NSR_FEDERATED_BACKUP=yes attribute. In the Remote user field, specify an administrator user account of the administering computer in the format of username@hostname. In the Password field, specify the password for the user account.

- For stand-alone setups—The wizard creates a client resource with the physical name using the selected save sets. If you select both CSV and non-CSV virtual machines, the backup fails.

- For CSV configurations, you can select Move CSV ownership to allow or disallow CSV ownership to change during multi-proxy backups for best backup performance. After you initially create the client resource, you can allow or disallow CSV ownership changes as needed. By default, federated backups are performed as CSV.

- For SMB configurations, select Perform backup of virtual machines over SMB3, which clears the Move CSV ownership option.

- To support partial backup failure, select Perform partial writer backup. When you select this option, if snapshot creation fails for some virtual machines, the backup continues for other virtual machines. The Hyper-V VSS Writer reports the virtual machines that failed to back up.

- To take a full backup and then take incremental backups, select Force VSS COPY-FULL backup type to specify the VSS COPY-FULL backup type. By default, this box is unchecked and the backup type is VSS FULL.

- To perform copy-level backups inside the virtual machine, select Perform copy-level backup inside VM.

- To disable incremental backups and make sure that only full backups are performed, select the Disable Change Block Tracking option. The section "Disabling incremental backups and enabling only full backups" in the Backups chapter provides details about this feature.
16. Click Next.
   
The Backup Configuration Summary page appears.

17. On the Backup Configuration Summary, do one of the following:
   
   • Click Back to revisit the previous pages.
   
   • Click Create to configure the client resources.
     The Client Configuration Results page appears. This page provides details about the client resources that have been created.

18. To change the configuration that you created earlier, in the NetWorker Management Console, select the client, right-click, and select Modify Client Wizard.

19. To verify the details for the client, on the Administration window, select the client, right-click, and select Modify Client Properties.

20. Optionally, to modify remote user access:
   
   a. On the Administration window, select the client, right-click, and select Modify Client Properties.
   
   b. On the Globals (2 of 2) tab, type the hostname of the proxy client in the Remote Access attribute.
      If the NMM client is part of a cluster, type the names of the physical nodes of the cluster in the Remote Access attribute.
Configuring a client resource manually by using the NetWorker Management Console

You can manually create a Hyper-V client resource by using the Client Properties dialog box.

**Note**

If using NetWorker server 8.2.3 or later and NMM 9.1:

- The procedure used to create a client resource when using NetWorker server 8.2.3 is different from the procedure used to create a client resource when using NetWorker server 9.1. Keep the following considerations in mind when following the NMM 8.2 SP1 procedure:

- Configure a regular NetWorker backup group instead of configuring a data protection policy. Do not enable the **Snapshot** option in the Group properties page.

- Type `nsrnmmsv.exe` in the **Backup Command** field.

**Procedure**

1. In the **Administration** window, click **Protection**.
2. In the expanded left pane, select **Clients**.
3. Right-click **Clients** and select **New**.
4. Click the **General** tab.
5. On the **General** tab:
   a. In the **Name** attribute, type the hostname of the NetWorker client computer.
   b. 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.
   c. In the **Save Set** attribute, specify the components to be backed up. Place multiple entries on separate lines. The following table provides the save set syntax.

<table>
<thead>
<tr>
<th>Type of backup data</th>
<th>Save set syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hyper-V Manager</td>
<td>APPLICATIONS:\Microsoft Hyper-V</td>
</tr>
<tr>
<td>The Hyper-V Host Component file and</td>
<td>The Hyper-V Writer does not support offline backup of the configuration file.</td>
</tr>
<tr>
<td>each virtual machine.</td>
<td></td>
</tr>
<tr>
<td>Hyper-V Host Component file</td>
<td>APPLICATIONS:\Microsoft Hyper-V\Host Component</td>
</tr>
<tr>
<td>There is one configuration file in</td>
<td>The Hyper-V Writer does not support offline backup of the configuration file.</td>
</tr>
<tr>
<td>the Hyper-V Manager installation.</td>
<td></td>
</tr>
<tr>
<td>This file lists the Hyper-V settings</td>
<td></td>
</tr>
<tr>
<td>for the host operating system and the</td>
<td></td>
</tr>
<tr>
<td>guest operating systems.</td>
<td></td>
</tr>
</tbody>
</table>

- Type `nsrnmmsv.exe` in the **Backup Command** field.
Table 11 Hyper-V save set syntax (continued)

<table>
<thead>
<tr>
<th>Type of backup data</th>
<th>Save set syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Hyper-V Host Component</td>
<td>save set in a proxy backup group.</td>
</tr>
<tr>
<td>Hyper-V virtual machine There are usually multiple virtual machines on the host operating system.</td>
<td>APPLICATIONS:\Microsoft Hyper-V \virtual_machine_name Child pertains or virtual machines can be in a proxy backup group.</td>
</tr>
</tbody>
</table>

6. Click the Apps & Modules tab and do the following:

a. In the Remote user and Password fields respectively, type the domain administrator username and password.

For guest virtual machines hosted over SMB 3.0 and CSV, the backup fails if you do not provide the domain administrator credentials.

b. In the Backup command attribute, type the following backup command:

nsrnmmsv.exe

c. In the Application Information attribute, specify the attributes for the backup. The following table lists the variables that can be specified in the Application Information attribute of the client resource.

Table 12 Hyper-V application information variable settings

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSR_FEDERATED_BACKUP</td>
<td>Marks the backup for CSV and SMB recovery.</td>
<td>Yes</td>
</tr>
<tr>
<td>NSR_FEDERATED_TYPE</td>
<td>Specifies whether the backup is federated CSV or SMB.</td>
<td>• SMB (required) • CSV (optional)</td>
</tr>
<tr>
<td>NSR_FEDERATED_PSOL</td>
<td>Optional. Distributes the backup workload across physical and virtual servers in the PSOL. If a server is not available or down, then NMM performs the backup from the node to which the cluster server name resolves, including virtual proxies.</td>
<td>Type a comma-separated list of the server names. For example: NSR_FEDERATED_PSOL=server1, server2, server3</td>
</tr>
<tr>
<td>NSR_EXCLUDE_SMB</td>
<td>Optional. Excludes virtual machines that have data that is stored on SMB file servers. By default, SMB virtual machines are in the writer level backup.</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Note
A Hyper-V CSV backup fails if the same host name is added twice in PSOL list.
Table 12 Hyper-V application information variable settings (continued)

<table>
<thead>
<tr>
<th>Attribute name</th>
<th>Description</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSR_VSS_FULL_BACKUP</td>
<td>Default value is Yes. When the value is Yes, NMM initially performs a full backup and later performs incremental backups. If the value is No, then NMM performs a copy full backup and does not merge the recovery snapshot with the base VHDX.</td>
<td>Yes, No</td>
</tr>
<tr>
<td>NSR_VM_COPY_BACKUP</td>
<td>If the value is Yes, NMM performs a VSS copy backup in guest virtual machines, which means there is no log truncation for applications running in guest virtual machines. If the value is No, NMM performs a VSS full backup in guest virtual machines. By default, all Hyper-V virtual machine backups are VSS copy type.</td>
<td>Yes</td>
</tr>
<tr>
<td>NSR_PARTIAL_BACKUP</td>
<td>Optional. Supports partial backup failure. If snapshot creation fails for some virtual machines, the backup continues for other virtual machines. The Hyper-V VSS Writer reports the virtual machines that failed to backup.</td>
<td>Yes</td>
</tr>
<tr>
<td>NSR_EXCLUDE_COMPONENTS</td>
<td>Optional. Excludes a virtual machine from the backup. Specify the writer level save set and the components to exclude from the backup. NMM logs the excluded components in the <code>nsrnmmsv.raw</code> log file for references.</td>
<td>Type a comma-separated list of the server names. For example: <code>NSR_EXCLUDE_COMPONENTS=VM1, VM2, VM3</code></td>
</tr>
<tr>
<td>NSR_MAX_CSV_PER_SNAPSHOT</td>
<td>Creates multiple snapshots for scale-out Hyper-V environments. The maximum value of the attribute is the number of CSVs in the scale-out environment.</td>
<td></td>
</tr>
<tr>
<td>NSR_DISABLE_INCREMENTAL</td>
<td>By default, when Hyper-V backups are performed by using NMM, the first instance of the backup is always full and subsequent backups are incremental. The <code>NSR_DISABLE_INCREMENTAL=yes</code> attribute disables incremental backups and enables only full backups. When incremental backups are disabled using this parameter, the recovery snapshots, that is .AVHDX files, are merged prior to the full backup.</td>
<td>Use the value is Yes to disable change block tracking (CBT) and perform only full backups. Use the value is No to enable change block tracking (CBT) and perform both full and incremental backups. You have the option to enable CBT or disable CBT at any time depending on your business needs.</td>
</tr>
</tbody>
</table>

7. Click the **Globals (1 of 2)** tab and, in the **Aliases** attribute, type the NETBIOS name for the client.

NMM client uses the host computer NETBIOS or “short” name when connecting to the NetWorker server to browse backups. If the NETBIOS name is not found, NMM cannot display backups.
8. To set up remote access, click the **Globals (2 of 2)** tab and do one of the following:
   - If you are setting up a proxy client for the NMM client, type the hostname of the proxy client in the **Remote Access** attribute.
   - If the NMM client is part of a cluster, type the names of the physical nodes of the cluster in the **Remote Access** attribute.

9. Click OK.
Backups
CHAPTER 3

Recoveries

This chapter includes the following sections:

- Overview ............................................................................................................. 58
- Hosting the recovered virtual systems .............................................................. 58
- Specifying the destinations for the Hyper-V configuration files and virtual system ........................................................... 59
- Selecting the Hyper-V recovery destination .................................................... 59
- Recovering Hyper-V CSV virtual machines .................................................... 63
- Using NMM 9.1 to recover a backup created by using an NMM 8.2.x release .... 68
Overview

Depending on what you specified in the backup save set, you can recover the following from a Hyper-V virtual machine backup by using the NetWorker User for Microsoft GUI:

- All Hyper-V components
- The Host Component file
- Individual or multiple virtual machines
- Granular level recoveries for individual files and folders

In circumstances when you are unable to use the NetWorker User for Microsoft GUI, you can use the NMM Support Tools for recovery. The *EMC NetWorker Module for Microsoft Release Administration Guide* provides details about these tools.

**NOTICE**

To recover backups that were created using an NMM release earlier than 9.0, click **Start > EMC NetWorker > NetWorker Tools > Restore previous NMM release backups** to start the NetWorker Module for Microsoft GUI. Browse the backups and perform the recovery from the GUI that appears.

Hosting the recovered virtual systems

The *Destination Host* page allows you to recover the virtual system to the original location.

**Procedure**

1. Open the NMM client software and select the NetWorker server on which the NMM client software was configured for backup.
   
   If the NMM client is part of a cluster, select the physical client to which you are recovering data. The physical client can be selected from the **Client List** attribute in the application toolbar.
   
   If the client does not appear in the list of available clients, add the client by clicking on **Options > Configure Options > Client name** (click on the icon beside), and then add the client from the **List of available clients** section to the **Clients to list on menu bar** section.

2. From the left pane, select **Recover > Hyper-V Recover Session > Image Recovery**.

3. From the navigation tree, select a single virtual machine under the Microsoft Hyper-V writer.

4. From the **Hyper-V Recover Session** toolbar, click **Advanced Recovery**.

   The Hyper-V Recovery wizard starts and the **Destination Host** page appears.

5. Select **Recover (Overwrite) Virtual System to original location**.

   The **Finish** button is available and **Next** button is unavailable when you select this option.

6. Click **Finish**.

   The **Finish** button validates the server location and displays the **Hyper-V Recovery Options** page.
7. Click **Start Recover**.

**Specifying the destinations for the Hyper-V configuration files and virtual system**

The **Destination Host** page allows you to specify the destination directory for the Hyper-V configuration files and the destination host for each virtual system.

**Procedure**

1. Open the NMM client software and select the NetWorker server on which the NMM client software was configured for backup.
   If the NMM client is part of a cluster, select the physical client to which you are recovering data. The physical client can be selected from the **Client List** attribute in the application toolbar.

   If the client does not appear in the list of available clients, add the client by clicking on **Options > Configure Options > Client name** (click on the icon beside), and then add the client from the **List of available clients** section to the **Clients to list on menu bar** section.

2. From the left pane, select **Recover > Hyper-V Recover Session > Image Recovery**.

3. From the navigation tree, select a single virtual machine under the Microsoft Hyper-V writer.

4. From the **Hyper-V Recover Session** toolbar, click **Advanced Recovery**.
   The Hyper-V Recovery wizard starts and the **Destination Host** page appears.

5. In the **Destination for Hyper-V configuration files** dialog box, click **Browse** to change the destination path.
   The **Select Virtual System Destination** list displays the destinations for each virtual system VHD/VHDX. The specified host must have the NMM client installed.

6. To change the destination path:
   a. Select a virtual system.
   b. Click **Change Destination**.
      The **Remote Directory Browser** dialog box appears.

7. To validate the settings click **Finish**.
   If the destinations are valid, then the **Hyper-V Recovery Options Summary** dialog box appears.

8. Click **Start Recover**.
   NMM validates all the pages. If the pages are all valid, NMM starts the recovery.

**Selecting the Hyper-V recovery destination**

You can select the destination of the Hyper-V recovery to the original host or to a different host or location.

When you perform a Hyper-V recovery on Windows Server Core, the recovery is a directed recovery. Because the Server Core installation does not provide a GUI, you
must use another host to start the recovery. To recover a Windows Server Core virtual machine through directed recovery, you must use the No Proxy option.

Restrictions and requirements for relocating and recovering data to a different location on page 121 provides details about other restrictions.

Performing Hyper-V recovery to the original machine and location

You might need to recover virtual machines to their original location if the virtual machines have been corrupted or deleted.

When you recover virtual machines to the original Hyper-V server, the original drive letters or mount points for the virtual machines must exist on the system, and the directory paths are automatically created. If any of the files from the virtual machines are still on the Hyper-V Server, then the recovery deletes or overwrites the files.

If the recovered virtual machine was a clustered virtual machine, then the recovery creates the virtual machine on one of the cluster nodes. However, you must use Microsoft Cluster Manager to make the virtual machine highly available.

Because Hyper-V recognizes virtual machines by an internal GUID, you cannot move or rename the current virtual machine during the recover if the virtual machine exists on the Hyper-V Server.

The Host Component file contains the authorization configuration for Hyper-V. If the file has become corrupted or you need to roll back the authorization settings, you might need to recover the Host Component to the original Hyper-V Server. The NMM System Component backups also include the Host Component.

Procedure

1. Open the NMM client software and select the NetWorker server on which the NMM client software was configured for backup.

   If the NMM client is part of a cluster, select the physical client to which you are recovering data. The physical client can be selected from the Client List attribute in the application toolbar.

   If the client does not appear in the list of available clients, add the client by clicking on Options > Configure Options > Client name (click on the icon beside), and then add the client from the List of available clients section to the Clients to list on menu bar section.

2. From the left pane, select Recover > Hyper-V Recover Session > Image Recovery.

3. From the navigation tree, select the Hyper-V Writer or individual virtual machines under the Hyper-V Writer.

4. From the Hyper-V Recover Session toolbar, click Recover.

   The Hyper-V Recover Session Summary dialog box appears.

5. If all the options are correct, then go to 9 on page 60. If you want to change options, then go to 6 on page 60.

6. Click Recover Options.

7. On the General tab, specify the Diagnostic Output Level.

8. On the Security tab, specify pass phrases if any are needed.

9. Click OK to close the Hyper-V Recover Session Options dialog box.

10. Click Start Recover.
Results

NMM validates all pages. If all pages are valid, then the recovery begins.

Performing a directed Hyper-V recovery to a different host or location

You can recover a virtual machine to the original Hyper-V Server, but move the virtual machine files to different file system locations. This type of recovery is necessary if the virtual machine files were moved after the selected backup time and you want to preserve the new locations. If the original virtual machine is present, then the virtual machine is overwritten during the recovery.

Procedure

1. Open the NMM client software and select the NetWorker server on which the NMM client software was configured for backup.

   If the NMM client is part of a cluster, select the physical client to which you are recovering data. The physical client can be selected from the Client List attribute in the application toolbar.

   If the client does not appear in the list of available clients, add the client by clicking on Options > Configure Options > Client name (click on the icon beside), and then add the client from the List of available clients section to the Clients to list on menu bar section.

2. From the left pane, select Recover > Hyper-V Recover Session > Image Recovery.

3. From the navigation tree, select a single virtual machine under the Microsoft Hyper-V writer.

4. From the Hyper-V Recover Session toolbar, click Advanced Recovery.

   The Hyper-V Recovery wizard starts and the Destination Host page appears.

5. Specify the destination host server for the Virtual System recovery:

   • To recover to the same location as the original:
     a. Select Recover (Overwrite) Virtual System to original location.
     b. Perform the steps in 6 on page 62.

   • To recover to a different path on the same Hyper-V Server:
     a. Select Recover Virtual System to a different path and then click Next. The Destination Path page appears, and you can specify a destination for each Virtual System. The specified host must have the NMM client installed.
     b. Click Browse to specify the destination location for the configuration files. After you select the destination location for the configuration files, you can change the destination location for the virtual machine’s virtual disks.
     c. To change the destination location for a virtual disk, select the virtual machine’s virtual disk in the list, and then click Change Destination. Repeat as needed for each virtual disk destination that you want to change.
     d. When you have completed changing destinations, go to 6 on page 62.
The destinations that are provided on this page are Microsoft's default configuration file locations and might not match the Hyper-V configuration. Change the destination as needed.

When you try a directed recovery to a different path on the same Hyper-V server, the recovery process takes the recovery virtual machine offline and then recovers the data to the alternate location. NMM registers the virtual machine pointing to the data in the new location.

You can remove the Virtual Hard Disk (VHD) files of the original virtual machine manually after the recovered Hyper-V child components are up and running.

• To recover to a different Hyper-V server:
  a. Click **Recover Virtual System to a different Hyper-V Server**.
  b. From the **Select Remote Host** list, click the server that you want to recover to.
  c. Click **Next**.
  d. The **Destination Path** page appears, where you can specify a destination for each Virtual System.
  e. On the **Destination Path** page, click **Browse** to specify the destination location for the configuration files. After you select the destination location for the configuration files, you can change the destination location for the virtual machine’s virtual disks.
  f. To change the destination location for a virtual disk, select the virtual machine’s virtual disk in the list, and then click **Change Destination**. Repeat as needed for each virtual disk destination that you want to change.
  g. When you have completed changing destinations, go to 6 on page 62.

The destinations that are provided on this page are Microsoft’s default configuration file locations and might not match the Hyper-V configuration. Change the destination as needed.

When you try a directed recovery to a different Hyper-V Server and the destination Hyper-V Server has an existing virtual machine with the same name as the one being recovered, the recovery process takes the virtual machine offline and recovers the data to the alternate location. NMM registers the virtual machine pointing to the data in the new location.

If you are recovering a virtual machine with same name to different Hyper-V server, you can remove the VHD files of the original virtual machine present earlier with the same name manually after the recovered Hyper-V child components are up and running.

6. To validate and start recovery, click **Finish**.

NMM validates the recovery and does the following:

• If the validation is not successful, then NMM displays an error message.

• If the validation is successful, then NMM displays a summary page that lists the Hyper-V and NetWorker Recover options that you specified.

• If you must change any of the options, click **Recover Options** or **Back**.

7. Click **Start Recover**.

NMM validates all pages. If all pages are valid, NMM starts the recovery.
Recovering Hyper-V CSV virtual machines

The following sections describe the supported types of Hyper-V CSV recoveries. Ensure that the NMM client is installed on all the cluster nodes before performing Hyper-V non-proxy recovery option.

Note

NMM does not support redirected recovery of virtual machines over SMB 3.0.

CSV virtual machine recovery

NMM supports recoveries for Hyper-V CSV virtual machines at the cluster level and at the individual CSV virtual machine level. NMM supports recoveries only on supported NMM hosts that run the Hyper-V service. This host might be outside of the cluster.

NMM recovers the CSV virtual machines that you select on the cluster node where the virtual machine is active. If a CSV virtual machine does not exist at the time of recovery, then NMM recovers the virtual machine to the majority node.

If no virtual machines exist in the cluster, then for the deleted virtual machine:

- If the winclient is started within the cluster, then the recovery operation starts on the node that runs the winclient.
- If the winclient is started from outside cluster, then NMM recovers the deleted virtual machine to the cluster owner node.

Redirected recovery of a clustered virtual machine to a node where it is not active is not allowed on the cluster where the virtual machine resides. If you request a relocated recovery of a virtual machine to a node on a cluster, but the virtual machine is already active on another cluster node, then the recovery fails. EMC recommends that you move the virtual machine to the desired node first and then start the virtual machine recovery.

When you select a single virtual machine, NMM supports the following types of recoveries:

- Default recovery (Recover on the cluster node where the virtual machine is active) — This is the default recovery when you click Recover... NMM recovers the selected virtual machine to the cluster node where it is active. If the virtual machine does not exist, NMM recovers it to the owner node.
- Advanced recovery — When you click the Advanced Recover... option, you can select one of the following options:
  - Recover Virtual System to active virtual system cluster node — If the virtual machine is already active on the destination cluster node, then you can recover the virtual machine to a path that differs from the path at the time of the backup.
  - Recover Virtual System to a different cluster node — If the virtual machine does not exist in the cluster, you can recover the selected virtual machine to an alternate node in the cluster. If the virtual machine exists in the cluster but is not active on the destination node, then the recovery fails. In this case, first migrate the virtual machine to the destination node and then perform either a default recovery or an advanced recovery.
  - Recover Virtual System to a different Hyper-V server — You can recover the selected virtual machine to a Hyper-V server outside of the cluster.

You can choose to recover all CSV virtual machines or multiple CSV virtual machines. NMM cannot recover the selected CSV virtual machines on their respective cluster.
nodes when the virtual machine is active. If a CSV virtual machine does not exist at the time of recovery, NMM recovers the virtual machine to the owner node.

After you recover a virtual machine, confirm that the recovery process registers the virtual machine. If the virtual machine is not registered as a cluster resource, use Failover Cluster Manager to register the virtual machine as cluster resource.

**Recovering with a Windows Server 2012 and 2012 R2 proxy CSV server**

You can select a proxy node for the CSV recovery operation.

**Procedure**

1. Open the NMM client software.
2. From the left pane, select **Recover > Hyper-V Recover Session**.
3. Click the **CSV Proxy Server** tab.

---

**Note**

The **CSV Proxy Server** tab is available only when performing recovery of virtual machines running on CSV, and not for SMB and standalone environments.

4. When using Windows Server 2012 R2, you can perform either import based or VSS based recovery.

**Figure 10 CSV Proxy Server tab for Windows Server 2012 R2**
5. When using Windows Server 2016, you can perform only import based recovery. The VSS based recovery option is not available.

**Figure 11** CSV Proxy Server tab for Windows Server 2016

6. Click **OK**.

7. Click **Recover**.

8. Click **Start Recover**.

   NMM validates the information on all pages. If all pages are valid, then NMM starts the recovery.

9. To validate and start recovery, click **Finish**.

   NMM validates the recovery and does the following:
   
   - If the validation is not successful, then NMM displays an error message.
   - If the validation is successful, then NMM displays a summary page that lists the Hyper-V and NetWorker Recover options that you specified.
   - If you must change any of the options, click **Recover Options** or **Back**.
Recovering multiple CSV VMs to the original location

You can recover multiple clustered Hyper-V VMs to the same location as the original CSV VM.

Procedure

1. Open the NMM client software.
2. From the left pane, select Recover > Hyper-V Recover Session.
3. From the navigation tree, select Image Recovery.
4. Select the cluster name from the Client menu.
5. Select the VMs you want to recover.
6. Click Recover.
7. Click Start Recover.

   NMM validates the information on all pages. If all pages are valid, then NMM starts the recovery.
8. To validate and start recovery, click Finish.

   NMM validates the recovery and does the following:
   - If the validation is not successful, then NMM displays an error message.
   - If the validation is successful, then NMM displays a summary page that lists the Hyper-V and NetWorker Recover options that you specified.
   - If you must change any of the options, click Recover Options or Back.

Recovering an individual CSV Hyper-V virtual machine to a different location

You can recover an individual CSV virtual machine to a different location. Only single virtual machine recovery to different location is supported.

Procedure

1. Open the NMM client software.
2. From the left pane, select Recover > Hyper-V Recover Session.
3. From the navigation tree, select Image Recovery.
4. Select the cluster name from the Client menu.
5. Click Advanced Recover.

   The Hyper-V Advance Recovery wizard starts and the Destination Host page appears. Select the destination to recover the CSV virtual machine.

   - To recover the virtual machine to the node on which it is active:
     a. Click Recover Virtual System to Active Virtual System Cluster Node.
     b. Click Next.
     c. Click OK.
     d. Click Recover Options.
     e. Select the CSV Proxy Server tab.
Note

The CSV Proxy Server tab is available only when performing recovery of virtual machines running on CSV, and not for SMB and standalone environments.

f. To recover the virtual machine to a different Hyper-V Server:
   a. Click Import based recovery (Select a server from cluster).
   b. Select the remote host to which you will recover the CSV virtual machine.
   c. Click Next.
   d. Specify the destination path for the configuration files.

When using Windows Server 2012 R2, you can perform either import based or VSS based recovery.

Figure 12 CSV Proxy Server tab for Windows Server 2012 R2

When using Windows Server 2016, you can perform only import based recovery. The VSS based recovery option is not available.
g. Click OK.

NMM performs the validation. If the validation is not successful, then NMM displays an error message. If the validation is successful, then NMM displays a Summary page that lists the specified Hyper-V and NetWorker Recover options.

6. If you must change any of the options, click the **Recover Options** or **Back** button.

7. Click **Start Recover**.

   NMM validates the information on all pages. If all pages are valid, then NMM starts the recovery.

**Using NMM 9.1 to recover a backup created by using an NMM 8.2.x release**

To recover backups that were created by using NMM 8.2.x, you must make certain changes to the existing client resource. Make these changes for all existing client resources.

The *EMC NetWorker Module for Microsoft Installation Guide* provides information about the "Restore of NMM 8.2.x and Earlier Backups (VSS workflows)" option in the installer.

The "Scheduled Backup" chapter in the *EMC NetWorker Module for Microsoft Release Administration Guide* provides the information on editing client resources that were created using NMM 8.2.x release, and information about the NetWorker Management Console bulk edit feature.
Note

Ensure that the Snapshot attribute of the NetWorker group that this client resource belongs to is clear or create a new group that does not have the snapshot option checked.

Procedure

1. In the Administration window, click Protection.
2. Right-click Clients in the navigation tree or right-click the required client in the Clients table.
3. Select Modify Client Properties.
4. In the Backup Command field, delete the nsrsnap_vss_save command and type the nsrnmsv.exe command. Perform this change for all existing client resources.
5. If the NSR_VSS_FULL_BACKUP variable is not specified in the Application Information field, then all Hyper-V VSS backups are automatically performed as Copy type backups. To continue with this default behavior, specify NSR_VSS_FULL_BACKUP=no in the Application Information field. Not using NSR_VSS_FULL_BACKUP or using NSR_VSS_FULL_BACKUP=yes enables Hyper-V virtual machine backups.
6. Make other changes, if required.
7. Click OK.
Recoveries
CHAPTER 4

Granular Level Recoveries

This chapter includes the following sections:

- **Overview** .......................................................................................................................... 72
- **Recovering Hyper-V files and folders** ........................................................................... 72
Granular level recovery (GLR) provides the ability to recover specific files from a single backup without recovering the full virtual machine, which drastically reduces the recovery time.

NMM can perform a GLR for backups of Hyper-V virtual machines that you created with NMM. You can only perform GLR for virtual machines running Windows operating systems. Hyper-V GLR functionality is supported in the NMM client software.

The NMM GLR feature uses BBB to mount the virtual machine that contains the items to recover. When the Hyper-V GLR completes, you can choose to unmount the virtual machine or perform another Hyper-V GLR operation. You can only use Hyper-V GLR to recover data that has been rolled over to backup media that supports GLR.

NMM only allows browsing and recovery of one virtual machine at a time, and NMM does not support the recovery of the same backup to multiple clients simultaneously. If you try to mount another virtual machine while you use the Hyper-V GLR, NMM unmounts the first virtual machine and you lose access to the contents of the first virtual machine until you remount it.

EMC recommends that you provision a system to act as the NMM Hyper-V GLR proxy. The Hyper-V GLR proxy has the required setup so that you can granularly recover files from a Hyper-V image backup. NMM supports the use of a 64-bit Windows Server virtual machine or physical server as the GLR proxy system.

Using this GLR proxy setup, you can recover files from any NMM Hyper-V backup of a Hyper-V virtual machine with a supported operating system installed. After NMM recovers the files or folders that are local to the proxy server, you must manually move or data mine the files as needed. The NetWorker administrator configures the NetWorker authentication to allow the NMM Hyper-V GLR proxy client the rights to recover any save set that NMM must mount.

NMM supports the following Windows Server 2012 Hyper-V GLR features:

- Recovery of data from a VHDX hard disk
- Recovery of FAT32, NTFS, and ReFS volume data
- GLR of Hyper-V VMs over SMB

NMM does not support the following Windows Server 2012 Hyper-V GLR features:

- Recovery of data from a Windows Server 2012 Storage Spaces disk on a virtual machine
- Differencing disk with parent and child hard disk on different hard drives
- Recovery of deduplicated data

Recovering Hyper-V files and folders

While you perform the steps in the following procedure, you can switch to the Monitor pane to see the progress of the recovery operation and to check for error messages. NMM displays any problems attaching hard disks, recognizing virtual machines, or expanding virtual machines in the Monitor window.

**Procedure**

1. On the GLR proxy server, open the NMM client.
If the GLR proxy server is not available, open the NMM client on the physical host where the backup was taken. This option requires you to install GLR on the physical host.

2. From the left pane, click Recover > Hyper-V Recover Session > Granular Level Recovery.

   NMM displays the GLR-capable virtual machines for the selected client.

3. In the navigation tree, locate the Hyper-V virtual machine that contains the folders or items you want to recover.

   To search for a particular item within the save set, right-click the virtual machine and then click Search for.

   **Note**

   The Search for option is enabled only when the source virtual machine is mounted.

4. Right-click the target virtual machine and then click Mount.

   NMM mounts the virtual machine. If another virtual machine is already mounted for GLR recovery, NMM notifies you that it will unmount the first virtual machine. Click OK to continue the mounting process with the second virtual machine, or click Cancel to leave the first virtual machine mounted.

5. Click a VHD to display a list of the virtual machines it contains in the right pane. If a VHD does not mount, NMM displays an error message. You can continue to work with the other available VHDs. Hyper-V GLR cannot mount raw VHDs (hard disks that have not been formatted).

6. Locate the folders or items that you want to recover by completing one of the following steps:

   - Expand the virtual machines to view a list of their contents.
   - Right-click a virtual machine and then click Search for to search for a specific folder or item.

      Depending on virtual machine size, loading a virtual machine can take awhile. You can start other operations in the Recover pane while waiting for a virtual machine to load. After the virtual machines load, you can perform data mining.

7. Select the checkbox beside each item to recover. If you select a folder for recovery, then NMM also selects the folder contents for recovery.

   You can specify a destination file path to recover the files. NMM retains the files in their original folder hierarchy. NMM overwrites files that exist on the destination path. If you do not specify a destination path, NMM uses a default recovery path.

8. To specify a destination path to recover the items to, click Recover Options in the Hyper-V Recover Session toolbar.

9. In the Hyper-V Recover Session Options window, click the Granular tab and specify a destination path to recover the items to.

10. Close the Hyper-V Recover Session Options window.

11. Click Recover in the Hyper-V Recover Session toolbar.

12. In the Hyper-V Recover Summary window, click Start Recover to start the recovery. NMM recovers the files in the destination path by creating the original folder hierarchy.
13. Close the Hyper-V Recover Session Summary window.

To view the recovery progress, click Monitor in the left pane. When a recovery is in progress, you cannot perform other tasks in the Recover pane. After a recovery completes, you can perform browse and recovery actions on the mounted virtual machine.
CHAPTER 5

File Level Recoveries

This chapter includes the following sections:

- Introduction................................................................. 76
- Performing a browser-based file level restore.............................. 76
- Performing a directed file level restore...................................... 78
- Monitoring file level restores................................................ 79
- Hyper-V FLR web UI log files................................................. 80
Introduction

The NMM Hyper-V File Level Restore (FLR) user interface allows NetWorker administrators to restore files that are stored on any Hyper-V virtual machine that is configured for NetWorker protection. As a NetWorker administrator, you can select Hyper-V backups to restore from, browse and search for files, select files and folders, and perform either browser-based or directed recoveries. The Hyper-V FLR user interface is fully web-based and runs in a web browser.

The Hyper-V FLR web UI supports two restore workflows:

- Browser-based restore—Download the backup to a local folder or network location.
- Directed restore—Restore items to a specific virtual machine and location.

The Hyper-V FLR web UI requires NetWorker 9.0 or later, and NetWorker Authentication Service must be configured.

To access the Hyper-V FLR web UI, you can log in as a NetWorker administrator who is part of the NetWorker Security Administrator and Application Administrator user groups. Note that the Hyper-V FLR web UI provides access to any Hyper-V data that has been backed up on the NetWorker server.

To perform Hyper-V FLR recoveries without logging in as a NetWorker administrator:

- Add the remote client to the Backup Operators group on the Hyper-V Server host
- Install Hyper-V Integrated Services on all virtual machines on the remote host
- In PowerShell, run the `enable-psremoting` cmdlet. During redirected recovery, NMM requires this cmdlet so that it can fetch the list of running VMs and open live VMs from the remote Hyper-V server.

The Hyper-V FLR web UI also requires the NMM Recovery Agent (NMM RA), which is installed as part of the standard NMM installation package. To perform recoveries to a Hyper-V virtual machine, install NMM Proxy RA. The NetWorker Module for Microsoft Installation Guide provides details.

The proxy server communicates with NW Adapter, mounts virtual machine backups, and serves data for browser-based and directed restores. The proxy server also queries Hyper-V servers to get a list of running VMs on each Hyper-V server. The proxy server can be any host that has required permissions on the NetWorker server to access virtual machine backups from the different Hyper-V servers that it manages. The proxy server requires Failover Clustering to mount virtual machines on a CSV.

Required ports for Hyper-V File Level Restore GUI

The Hyper-V FLR service uses the following ports:

- 10000 HTTP
- 11000 Secure HTTPS
- 10099 Cache Service
- 10024 Persistence Service
- 9090 NetWorker Authentication Service

Performing a browser-based file level restore

The Hyper-V FLR web UI browser-based file level restore process follows a step-by-step, wizard-like workflow similar to the directed file level restore process. You can
use the browser-based restore option to select items to recover and then download the recovered files.

**Procedure**

1. From a supported web browser, type the URL of the Hyper-V FLR web UI:

   \[\text{http://server\_name:service\_port}\]

   where:

   - `server_name` is the name of the Hyper-V FLR web UI.
   - `service_port` is the port for the embedded HTTP server. The default HTTP port is 10000.

   For example: `http://houston:10000`

2. Log in using NetWorker administrator credentials.

   The **Proxy URL** dialog box appears. This dialog box appears the first time you log in.

3. In **Proxy URL** dialog box, provide the cluster name that was used for Hyper-V cluster level backup. Provide Hyper-V server name for standalone.

4. In the **Select the Hyper-V Server** area, select the Hyper-V server that contains the virtual machine you want to restore from by using one of the following options:

   - Select a server from the **Select the Hyper-V Server** list.
   - Click the sort button to sort the list of servers alphabetically.
   - Type a search term in the search field. The results display in the **Select the Hyper-V Server** list. Select a server from this results list. To clear the search term, click the "x" in the search field.

5. In the **Select the Virtual Machine** area, select the virtual machine that you want to restore from by using one of the following options:

   - Select a virtual machine from the list that is displayed in the **Select the Virtual Machine** list.
   - Click the sort button to sort the list of VMs alphabetically.
   - Type a search term in the search field. The results display in the **Select the Virtual Machine** list. Select a virtual machine from this results list. To clear the search term, click the "x" in the search field.

6. In the **Select a backup containing the items for restore** area, select the backup that you want to restore from by using one of the following options:

   - Select a backup that is displayed in the list.
   - To sort the list of backups alphabetically, click the sort button.
   - To filter the list of backups by date, Click the filter button, select the **Date filtered view**, select Before or After, and then select a backup date. To clear the filter, Click the filter button and select None. Dates are displayed in GMT time.

7. On the **Restore Items** page, browse or search for items to restore.

8. Select an item to restore by doing one of the following:

   - Double-click the item. The item displays in the **Items to Restore** area.
   - Drag and drop the item into the **Items to Restore** area.

   To remove items from the **Items to Restore** area, click the "x" next to the item.
9. On the Restore Options page, verify that the Restore to a browser download location setting is Yes and then click Finish.

10. Check the restore status in the Restore Monitor pane.
    To cancel a pending restore, click or tap Cancel.

11. After the download completes, click the Download button on the restored items status pane.

12. In the Save As window that displays, browse to a location to save the restored items and click Save.

Results
The restored items are downloaded to the location you specified.

Performing a directed file level restore

The Hyper-V FLR web UI directed file level restore process follows a step-by-step, wizard-like workflow similar to the browser-based file level restore process. Use the Hyper-V FLR web UI to select items to restore and then specify a destination file path for the restored items.

Procedure

1. Log in using NetWorker administrator credentials.
   The Proxy URL dialog box appears. This dialog box appears the first time you log in.

2. In Proxy URL dialog box, provide the cluster name that was used for Hyper-V cluster level backup. Provide Hyper-V server name for standalone.

3. In the Select the Hyper-V Server area, select the Hyper-V server that contains the virtual machine you want to restore from by using one of the following options:
   • Select a server from the Select the Hyper-V Server list.
   • Click the sort button to sort the list of servers alphabetically.
   • Type a search term in the search field. The results display in the Select the Hyper-V Server list. Select a server from this results list. To clear the search term, click the "x" in the search field.

4. In the Select the Virtual Machine area, select the virtual machine that you want to restore from by using one of the following options:
   • Select a virtual machine from the list that is displayed in the Select the Virtual Machine list.
   • Click the sort button to sort the list of VMs alphabetically.
   • Type a search term in the search field. The results display in the Select the Virtual Machine list. Select a virtual machine from this results list. To clear the search term, click the "x" in the search field.

5. In the Select a backup containing the items for restore area, select the backup that you want to restore from by using one of the following options:
   • Select a backup that is displayed in the list.
   • To sort the list of backups alphabetically, click the sort button.
   • To filter the list of backups by date, Click the filter button, select the Date filtered view, select Before or After, and then select a backup date. To clear
the filter. Click the filter button and select None. Dates are displayed in GMT time.

6. On the Restore Items page, browse or search for items to restore.
7. Select an item to restore by doing one of the following:
   • Double-click the item. The item displays in the Items to Restore area.
   • Drag and drop the item into the Items to Restore area.
   To remove items from the Items to Restore area, click the "x" next to the item.
8. On the Restore Options page, verify that the Restore to a browser download location setting is No and then click Finish.
9. In the Select the Virtual Machine area, select the destination virtual machine by doing one of the following:
   • Select a virtual machine from the list that is displayed in the Select the Virtual Machine list.
   • Click the sort button to sort the list of virtual machines alphabetically.
   • Type a search term in the search field. The results display in the Select the Virtual Machine list. Select a virtual machine from this results list. To clear the search term, click the "x" in the search field.
10. In the Restore to location area, browse to the wanted destination file path for the restored items by doing one of the following:
    • Select a location in the list that is displayed.
    • Select a location in the Restore to location list, then type a search term in the search field and click Go. The results display in the Restore to location list. To clear the search term, click the "x" in the search field.
11. Click Finish.
12. Check the restore status in the Restore monitor pane.
   To cancel a pending restore, click Cancel.

Results
The items are restored to the specified destination file path.

Monitoring file level restores
You can monitor Hyper-V FLR restores from any page in the web UI by using the Status bar. Collapse or expand the Status bar to hide or display the Restore Monitor toolbar. The Restore Monitor toolbar allows you to view restore details in tile or list view and display an expanded view of a restore status.

Status bar
When collapsed, the Status bar displays condensed information about running, pending, successful, and failed restores. Clicking or tapping the Status bar displays the Restore Monitor toolbar.

Restore Monitor toolbar
The Restore Monitor toolbar displays restore statuses in either tile view or list view. To change the view, select Change View and then select a view. To refresh the Restore Monitor with the latest restore information, click or tap Refresh. You can also filter the restore statuses to display only successful, failed, or running restores, and you can sort the restore statuses by start time, end time, progress, or status.

Clicking or tapping a restore status displays an expanded view, which provides additional details and available actions. Only one restore status can be expanded at a
time. To close the expanded view, double-click or tap the expanded item, or click or tap another item.

Hyper-V FLR web UI log files

If you encounter errors while using the Hyper-V FLR web UI, you can check various Hyper-V FLR web UI, NMM, and NetWorker log files.

Check the log files in the following order:

1. Hyper-V FLR UI
   - Linux: /nsr/logs/hyperv-flr-ui/hyperv-flr-ui.log
   - Windows: C:\Program Files\EMC NetWorker\nsr\logs\hyperv-flr-ui\hyperv-flr-ui.log

2. NMM RA (Windows only)
   - C:\Program Files\EMC NetWorker\nsr\logs\nsrnmmra.log
   - C:\Program Files\EMC NetWorker\nsr\logs\nsrnmmproxyra.log

3. NetWorker adapter
   - Linux: /opt/nsr/nsrmq/logs/nsrmq.log
   - Windows: C:\Program Files\EMC NetWorker\nsr\nsrmq\logs\nsrmq.log

4. RabbitMQ message bus
   - Linux: /opt/nsr/rabbitmq-server-3.2.4/var/log/rabbitmq/rabbitmq.log
   - Windows: C:\Windows\System32\config\systemprofile\AppData\Roaming\RabbitMQ\log\rabbit.log

5. NetWorker Server
   - UNIX: /nsr/logs/daemon.raw
   - Windows: C:\Program Files\EMC NetWorker\nsr\logs\daemon.raw

6. NetWorker authentication service
   - Linux: /opt/emc/authc/tomcat/logs/catalina.out
   - Windows: C:\Program Files\EMC\Authc\tomcat\logs\catalina.out
This chapter includes the following sections:

- Overview ............................................................................................................ 82
- How the Data Protection Add-in works with SCVMM ........................................ 84
- Installation and uninstallation ............................................................................. 87
- Preferences ....................................................................................................... 92
- Data Protection Add-in overview data ............................................................... 94
- Recoveries ........................................................................................................ 100
- Monitoring ........................................................................................................ 106
- Troubleshooting .............................................................................................. 107
Overview

The EMC Data Protection Add-in for SCVMM leverages the System Center Virtual Machine Manager (SCVMM) Add-in extension support to enable NetWorker client Hyper-V virtual machine recoveries within the SCVMM console.

The Data Protection Add-in enables you to perform NMM Hyper-V recoveries within the SCVMM console. You can view and recover all current SCVMM-managed virtual machines that have NMM conventional backups. The Data Protection Add-in supports recoveries of Hyper-V virtual machines in cloud, cluster, host, host group, and virtual machine contexts.

You can perform recoveries of Hyper-V virtual machines to the original location or to an alternate host location.

Recoveries

The Data Protection Add-in feature set supports recovery of Hyper-V virtual machines protected by NetWorker servers. The Data Protection Add-in supports recoveries of conventional backups to the original Hyper-V server on which the virtual machine was backed up or to an alternate Hyper-V server. The Data Protection Add-in does not support recoveries of VMware virtual machines or recoveries from persistent snapshots.

The Data Protection Add-in can be used in the following SCVMM configurations:

- SCVMM console on the same host as the SCVMM server
- SCVMM console on a different host from the SCVMM server

To perform recoveries by using the Data Protection Add-in, you must have the required privileges for the client to which you recover the virtual machine. Required privileges on page 83 provides details about SCVMM privileges. The NetWorker Administration Guide provides details about the required NetWorker server privileges.

Backups

The SCVMM user cannot perform backups from the Data Protection Add-in. A NetWorker administrator must create and configure NetWorker client resources for the Hyper-V servers from which the SCVMM can recover virtual machines.

After the Hyper-V server has been added to a NetWorker client, the basic workflow for a scheduled backup of a virtual machine that is managed by SCVMM is the same as the workflow of a standard physical host. If the NetWorker administrator does not create and configure a NetWorker client for the Hyper-V server, then the NetWorker server cannot protect the SCVMM virtual machine and therefore the virtual machine is not available for recovery.

The "Backups" chapter and the NetWorker Administration Guide provide details on scheduling and managing backups.

Supported versions

The Data Protection Add-in supports System Center 2016 and System Center 2012 R2 Virtual Machine Manager.
Note

The NetWorker Online Software Compatibility Matrix on EMC Online Support lists the most up-to-date information about the Windows Server versions that NMM supports. The Data Protection Add-in version must match the NetWorker and NMM client versions.

The Data Protection Add-in is compatible with the following operating systems when imported into the System Center 2016 Virtual Machine Manager Console:

- Windows Server 2016 (64 bit) Standard and Datacenter
- Windows 7 SP1 or later (64 bit or 32 bit) Professional, Enterprise, and Ultimate
- Windows 8 (64 bit or 32 bit) Professional and Enterprise
- Windows 8.1 (64 bit or 32 bit) Professional and Enterprise

The Data Protection Add-in is compatible with the following operating systems when imported into the System Center 2012 R2 Virtual Machine Manager Console:

- Windows Server 2012 (64 bit) Standard and Datacenter
- Windows Server 2012 R2 (64 bit) Standard and Datacenter
- Windows 7 SP1 or later (64 bit or 32 bit) Professional, Enterprise, and Ultimate
- Windows 8 (64 bit or 32 bit) Professional and Enterprise
- Windows 8.1 (64 bit or 32 bit) Professional and Enterprise

Note

Hyper-V Server with Window Server 2016 can not be imported to System Center 2012 R2 Virtual Machine Manager Console.

Software dependencies

The Data Protection Add-in requires the following software:

- The Data Protection Add-in and the NetWorker base and extended client software must be installed on the SCVMM console host. The Data Protection Add-in must match the NetWorker and NMM client versions.
- The NetWorker and NMM 9.0 or later client software must be installed on the Hyper-V server to which the virtual machine is recovered.
- The Data Protection Add-in requires access to a NetWorker 9.0 or later server.

Required privileges

To perform recoveries, you must be a member of certain SCVMM roles and have certain privileges.

To perform recoveries, you must:

- Be a member of the SCVMM Administrator or Fabric Administrators SCVMM roles.
- Have write access to the folder where the cached datafiles are stored. For example: C:\Users\%current user%\AppData\Local\EMC\NetWorker\SCVMM.
- Have NetWorker directed recovery privileges, which requires the following:
The Data Protection Add-in host is a client of the NetWorker server that contains the backup information. This administering client can be a different platform from the source and destination clients.

Use the local root or Administrator account to start the recovery. Ensure that the user account is a member of one of the following:

- The Operators, Application Administrators, Database Administrators, or Database Operators User Group.
- A customized User Group with the following privileges on the NetWorker server:
  
  - Remote Access All Clients
  - Operate NetWorker
  - Monitor NetWorker
  - Operate Devices and Jukeboxes
  - Backup Local Data
  - Recover Local Data
  - Recover Remote Data

Installation and configuration overview

To install the Data Protection Add-in, an SCVMM administrator and each user must perform required steps.

Procedure

1. An SCVMM administrator must perform the following steps:
   a. Installing SCVMM and the SCVMM console on page 88
   b. Installing the Data Protection Add-in on page 88

2. Each user must perform the following steps:
   a. Importing the Data Protection Add-in on page 89
   b. Activating the Data Protection Add-in on page 89

After you finish

To uninstall the Add-in, an SCVMM administrator, and each user must perform the steps that are described in Uninstalling the Data Protection Add-in on page 90.

How the Data Protection Add-in works with SCVMM

The NetWorker client and NMM client software must be installed on each Hyper-V physical host. The SCVMM console can be installed on a separate server or on the SCVMM server. However, the NetWorker client must be installed on the SCVMM console host.

Note

The EMC Data Protection Add-in uses a hostname, as displayed on the SCVMM console, when it tries to identify corresponding NetWorker clients on the NetWorker servers. If the hostname in SCVMM does not match its actual server name, then the Add-in is unable to find the corresponding NetWorker Client. Ensure that the hostnames in SCVMM match their actual server names.

The following figure illustrates the Data Protection Add-in architecture.
Workflows overview

The following sections describe common workflows for the Data Protection Add-in.

Initialize the SCVMM console or change context

When you launch the SCVMM console or change context within the console, the Data Protection Add-in does the following:

**Procedure**

1. Accesses the SCVMM server to obtain a list of virtual machines for the context you selected.
2. Displays virtual machines for the selected context that have been backed up on servers in the Preferred NetWorker servers list.

Refresh the Data Protection Add-in display

When you click the Refresh button on any page in the Data Protection Add-in, the Data Protection Add-in does the following:

**Procedure**

1. Accesses the SCVMM server to obtain a list of all hosts.
2. Accesses the NetWorker server to obtain a list of all clients and save sets.
3. Accesses the SCVMM server to obtain a list of all virtual machines in the current context.
4. Displays the updated protection information on the Overview page and virtual machines available for recovery on the Recover page.
Perform a recovery

When you perform a recovery, the following occurs:

Procedure

1. The Data Protection Add-in passes the virtual machine, backup time, and destination options you selected to the NWRecover service. The NWRecover service starts the recovery process.

2. The NWRecover service runs a remote agent on the Hyper-V server and passes the required information.
   
   The NWRecover service posts recover messages to the **Data Protection Add-in Monitor** page

3. The remote agent performs the requested recovery.
   
   During the recovery process, the NWRecover service updates the log shown in the **Monitor** page as well as the Windows event log under **Applications and Services > NetWorker Recovery Service**.

Results

The NWRecover service posts the recover success message in the monitor log and the Windows event log.

GUI overview

The Data Protection Add-in consists of the **Overview**, **Preferences**, **Recover**, and **Monitoring** pages.

- Overview—Displays the protection status for all virtual machines in the current SCVMM context.

- Preferences—Allows you to specify NetWorker servers, set the refresh rate, and set the debug level.

- Recover—Allows you to perform recoveries and view virtual machines available for recovery.

- Monitoring—Allows you to view in-progress and completed operations.

After you import the Data Protection Add-in, when you select the **All Hosts** or **Cloud** scope in the SCVMM console, the EMC Data Protection Add-in button displays in the SCVMM ribbon within the **VMs and Services** context.

If you select a non-supported scope (within the **VMs and Services** context), the Data Protection Add-in button is disabled.

SCVMM user roles and allowed actions

The Data Protection Add-in is cloud and tenant-aware, so you can only recover virtual machines to which you have access. You cannot direct a recovery to a Hyper-V server to which you do not have access.

The following table lists the supported SCVMM User Roles and the actions that the Data Protection Add-in allows for each supported role.
Table 13 SCVMM user roles and actions allowed by the Data Protection Add-in

<table>
<thead>
<tr>
<th>Role</th>
<th>Actions allowed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fabric Administrator (Delegated Administrator)</td>
<td>Can see all virtual machines, hosts, and clouds. Can recover all virtual machines managed by SCVMM to original and alternate locations.</td>
</tr>
<tr>
<td>Tenant Administrator</td>
<td>Can see and recover virtual machines within the private cloud they manage. Only recovery to original location is supported. On the Recover page, unable to see the Hyper-V Host and Recover Destination columns.</td>
</tr>
<tr>
<td>Read-Only Administrator</td>
<td>Can see the virtual machines and hosts within the private cloud they manage. No recovery operations are allowed.</td>
</tr>
<tr>
<td>Application Administrator (Self-Service Administrator)</td>
<td>Can see and recover virtual machines within the private cloud they manage. Only recovery to original location is supported. On the Recover page, unable to see the Hyper-V Host and Recover Destination columns.</td>
</tr>
</tbody>
</table>

**Supported scopes and contexts**

The Data Protection Add-in supports the following SCVMM scopes:

- Cloud
- Cluster
- Host (clustered and stand-alone)
- HostGroup
- Virtual machine

The Microsoft website provides more information about SCVMM scopes.

**Installation and uninstallation**

This section describes the Data Protection Add-in required components and the order in which they must be installed and configured.

The SCVMM administrator must install the components in the following order:

1. SCVMM and SCVMM console
2. SCVMM update rollups
3. NetWorker base client kit
4. NetWorker extended client kit
5. Data Protection Add-in

**Note**

The NetWorker base and extended client kits must be installed on the SCVMM console host and must be the same version as the Data Protection Add-in.

After the SCVMM administrator has installed these components, each user imports and activates the Data Protection Add-in.
To uninstall the Data Protection Add-in, each user removes the Data Protection Add-in from the SCVMM console, and an SCVMM administrator uninstalls the Data Protection Add-in.

Installing SCVMM and the SCVMM console

Download and install SCVMM from the Microsoft website. Install the SCVMM console so that it is available for all users. This installation requires system administrator privileges.

Installing the Data Protection Add-in

To install the Data Protection Add-in, you access the installation files from a DVD disk or EMC Online Support. To install the Data Protection Add-in on the SCVMM server, you must have local administrator privileges.

NetWorker client packages and the Data Protection Add-in must be installed on the SCVMM console host. The Data Protection Add-in requires the NetWorker base client and extended client packages to be installed on the SCVMM console host before installing the Add-in itself. The Data Protection Add-in must match the NetWorker and NMM client versions. The NetWorker Installation Guide provides details about the NetWorker client package installations.

Because the Data Protection Add-in does not have built-in foreign language support, only install the English language pack on the NetWorker client for use with the SCVMM add-in.

Procedure

1. To access the Data Protection Add-in software from a local DVD disk:
   a. Log in as an administrator or equivalent on the NetWorker client.
   b. Insert the Data Protection Add-in DVD disk into the DVD drive.
   c. Run EMC_Data_Protection_UI_Addin_for_SCVMM.msi directly from the DVD.
   d. Accept the default values during the installation.

2. To access the Data Protection Add-in software from EMC Online Support:
   a. Log in as administrator or equivalent on the NetWorker client.
   b. Browse to EMC Online Support (http://support.emc.com).
   c. Browse to the Downloads for NetWorker Module for Microsoft page.
   d. Download the 32-bit or 64-bit Data Protection Add-in software Zip file to a temporary folder that you create.
   e. Extract the Zip file to the temporary folder.
   f. Run EMC_Data_Protection_UI_Addin_for_SCVMM.msi.
   g. Accept the default values during the installation.

Results

The installer places a Data Protection Add-in Zip file in the public user documentation folder and installs the required NWRecover Service. The NWRecover Service automatically starts during the installation process.

The default installation path for the Data Protection Add-in Zip file is: C:\Users\Public\Documents\EMC NetWorker\nsr\addins\VMM_DataProtection\. If you encounter any issues while installing or importing
the Data Protection Add-in, then ensure that you have read and write permission for all folders in this path.

Make note of the Data Protection Add-in .zip file installation path as it is used in Importing the Data Protection Add-in on page 89. The default installation path for the NWRecover Service is:

C:\Program Files\EMC Networker\nsr\addins\VMM_DataProtection.

**Importing the Data Protection Add-in**

Each Data Protection Add-in user must import the Data Protection Add-in. The users must have write access to the folder where the cached datafiles are stored. For example:

C:\Users\%current_user%\AppData\Local\EMC\NetWorker\\SCVMM.

**Procedure**

1. Launch the SCVMM console and connect to a Virtual Machine Manager server. The console opens.
2. In the workspaces pane, click **Settings**.
3. In the navigation pane, click **Console Add-ins**.
4. If a previous version of the Data Protection Add-in exists, select it and click **Remove** on the SCVMM ribbon.
5. On the SCVMM ribbon, click **Import Console Add-in**.
6. In the **Import Console Add-in** wizard, browse to the folder in which you installed the Data Protection Add-in Zip file.
7. Select **EMC.DP.ScvmmAddIn.zip** and click **Open**. For example:

C:\Users\Public\Documents\EMC NetWorker\nsr\addins\VMM_DataProtection.

8. To continue installing, select the checkbox and click **Next**.
9. Click **Finish** and then click **Close** to close the **Jobs** window that displays.

**Results**

If an error message displays, delete the pre-existing add-in folder. For example:

C:\Program Files\Microsoft System Center 2016\Virtual Machine Manager\bin\AddInPipeline\AddIns\<domain_username>.

**Activating the Data Protection Add-in**

After you install SCVMM, the SCVMM console, the SCVMM update rollups, and the Data Protection Add-in, you must activate the Data Protection Add-in.

**Procedure**

1. In the workspace pane of the SCVMM console, click **VMs and Services**.
2. In the navigation pane, select a host or cluster.
3. On the SCVMM ribbon, click **EMC Data Protection**.

After about 5-10 seconds, the main content area of the console will be replaced by the Data Protection Add-in.
When a user launches the Data Protection Add-in for the first time, the Preferences page displays. After initial configuration and refresh, subsequent launches of the Add-in display the Overview page first.

Uninstalling the Data Protection Add-in

To uninstall the Data Protection Add-in, each user must remove the Data Protection Add-in from the SCVMM console, and an SCVMM administrator must uninstall the Data Protection Add-in. If no users perform other NetWorker operations on this computer, you can also uninstall the NetWorker software. These tasks can be performed in any order.

Removing the Data Protection Add-in from the SCVMM console

Each user must remove the Data Protection Add-in from the SCVMM console. Removing the Data Protection Add-in from the SCVMM console removes all components that are copied to the SCVMM AddIn folder during the import process, but not the originally downloaded Data Protection Add-in .zip file itself.

Note

Removing the Data Protection Add-in only affects individual users. Other users who imported the Add-in are not affected.

Procedure

1. In the SCVMM console, click the Settings workspace.
2. Click the Console Add-ins setting.
3. In the list of installed Add-ins, select EMC Data Protection Add-in.
4. On the top ribbon, click **Remove**.
5. On the confirmation window that displays, click **Yes**.

**After you finish**

The Data Protection Add-in creates persistent data cache files during the refresh operation. These files are created for each user. If a user removes the Add-in and is not expected to upgrade or otherwise re-import the add-in in the future the files can be manually removed from the following folder: `C:\User\<user name>\AppData\Local\EMC\NetWorker\SCVMM`.

**Uninstalling the Data Protection Add-in by using Windows Program and Features**

An SCVMM administrator must uninstall the Data Protection Add-in from the SCVMM server. Uninstalling the Data Protection Add-in ensures the Data Protection Add-in (.zip file) is removed from the SCVMM console host and ensures that the Data Protection service is stopped and uninstalled.

---

**Note**

This step affects all users who imported the Data Protection Add-in. If the Data Protection Add-in is uninstalled, no users can perform a recovery by using the Data Protection Add-in. Verify that each SCVMM console user has removed the Data Protection Add-in before uninstalling.

**Procedure**

1. For Windows Server 2012 or Windows 8 or later: Click **Control Panel** and then click **Programs and Features**.
2. For Windows 7 or earlier: Click **Control Panel** and then click **Uninstall a program**.
3. Select **EMC Data Protection UI Addin for SCVMM**.
4. Click **Uninstall**.

**Upgrading the Data Protection Add-in**

To upgrade the Data Protection Add-in, you must complete the uninstallation procedures to uninstall the current version and then complete the installation procedures to install the new version.

**Before you begin**

Before upgrading the Data Protection Add-in, ensure that the NetWorker and NMM client software and the NetWorker Server software are compatible with the Data Protection Add-in. The Data Protection Add-in version must match the NetWorker and NMM client versions. The *NetWorker Online Software Compatibility Matrix* on EMC Online Support lists the most up-to-date information about supported versions.

**Procedure**

1. Obtain the new Data Protection Add-in installer MSI file from the EMC Support site.
2. For all users, remove the existing Data Protection Add-in from the SCVMM console.
3. Follow the steps that are described in **Uninstalling the Data Protection Add-in** on page 90.
4. Follow the steps that are described in **Installing the Data Protection Add-in** on page 88.
5. Follow the steps that are described in Importing the Data Protection Add-in on page 89.
6. Follow the steps that are described in Activating the Data Protection Add-in on page 89.
7. In the Upgrade Successful window, click OK.
8. Click Refresh to repopulate the Data Protection Add-in.

Preferences

After completing the installation process, you must configure the Data Protection Add-in to access the NetWorker servers that contain virtual machine backups for recovery. You can also set the refresh frequency and specify the logging debug level. After making any configuration changes to the SCVMM environment, perform a Refresh operation in the Data Protection Add-in to ensure that the Add-in is displaying current information.

Figure 16 Data Protection Add-in

Adding NetWorker servers

You can search for virtual machine backups on multiple NetWorker servers. Contact the NetWorker administrator to learn which NetWorker servers protect the virtual machines you manage, and then add them to the Data Protection Add-in.

Procedure

1. In the workspaces pane of the SCVMM console, click VMs and Services.
2. In the left navigation pane, select the host or cloud you want to manage.
3. In the SCVMM ribbon, click EMC Data Protection.
4. In the Data Protection Add-in, click Preferences.

5. In the text box next to the Preferred NetWorker servers list, type the FQDN or IP address of a NetWorker Server and click Add.

The preferred NetWorker servers list is displayed.

**Note**

Do not use IPv6 addresses, localhost, or 127.0.0.1 as the NetWorker server in the Preferences page.

6. In the notification that displays, click OK.

7. Follow the directions in the notification.

8. Click Refresh to view the newly added NetWorker server virtual machine protection status on the Overview page and the available virtual machine backups on the Recover page.

**Note**

If adding more than one NetWorker server at a time, it is recommended to add all servers before starting the Refresh operation.

### Removing NetWorker servers

**Procedure**

1. In the workspaces pane of the SCVMM console, click VMs and Services.
2. In the navigation pane, select the host or cloud you want to manage.
3. In the SCVMM ribbon, click EMC Data Protection.
4. In the Data Protection Add-in, click Preferences.
5. In the Preferred NetWorker servers list, select a server and click Remove.

The Data Protection Add-in automatically performs a Refresh operation to display virtual machine data for the remaining NetWorker servers.

### Setting the refresh interval

On the Preferences page, the Data Protection Add-in provides two options for scanning the SCVMM environment for changes:

- **Use manual refresh only**—This is the default setting. When you select this option, you must manually scan for changes by clicking the Refresh button on any Data Protection Add-in page. With this setting, the Data Protection Add-in does not scan for changes automatically.

- **Use specified refresh interval**—You can specify the interval at which the Data Protection Add-in automatically refreshes the data. When you select this option, type a refresh interval and click anywhere in the SCVMM console to apply the change. The refresh rate should correspond to how often a virtual machine is backed up in the environment and the amount of time a refresh process takes to complete. If the refresh process does not complete within the interval you specify, lengthen the interval accordingly.
Including debug output for logging purposes

You can choose to include debug output in log files. This can be especially helpful for troubleshooting purposes. To include debug level output, on the Preferences page, select the Include debug level output checkbox.

Using multiple NetWorker Servers that define the same clients and virtual machine save sets

The Data Protection Add-in learns about protected virtual machines by querying the NetWorker servers that are specified on the Preferences page. If there is conflicting data regarding a Hyper-V server and its virtual machine protection because the Hyper-V server is a client of multiple NetWorker servers, the Data Protection Add-in might display inconsistent data.

Therefore, if you are using multiple NetWorker servers that define the same Hyper-V clients and virtual machine save sets, it is best to change the Preferences page to one NetWorker server at a time. This reduces NMM data protection metric inconsistency on the Overview page and protected virtual machine listings on the Recover page.

In scenarios where the Preferences page does include NetWorker servers that define the same Hyper-V clients and virtual machine save sets, then the Data Protection Add-in arbitrarily chooses information from one NetWorker server if conflicts exist. This prevents scenarios where a virtual machine is mis-counted for protection metrics or shows twice on the Recover page.

Data Protection Add-in overview data

The Overview page summarizes the current NMM data protection metrics for the managed virtual machines in the currently selected SCVMM context. For Administrator, Fabric Administrator, and Read-Only Administrator user roles, the Data Protection Add-in displays virtual machine protection status. For Tenant Administrator and Application Administrator (Self-Service Administrator) user roles, the Data Protection Add-in displays virtual machine backup status.

Overview page for Administrator, Fabric Administrator, and Read-Only Administrator user roles

For Administrator, Fabric Administrator, and Read-Only Administrator user roles, the Overview page displays multiple sub-panes:

- Clouds, Clusters, Hosts, and Virtual machines sub-panes—These sub-panes list the number of clouds, clusters, hosts, and virtual machines the user role manages within the currently selected SCVMM context.
- Configured for protection—This sub-pane provides protection characteristics for the virtual machines that are protected on the NetWorker servers that are listed on the Preferences page.

The pie chart provides the following data about virtual machines:

- VMs excluded from protection—These virtual machines are currently listed in the NSR_EXCLUDE_COMPONENTS attribute for a NetWorker client resource and not protected by another client resource.
- VMs not protected—These virtual machines are not configured for a scheduled backup as part of a NetWorker client resource and not explicitly excluded for backup. Virtual machines with missing status are shown under 'VMs not protected' and can be viewed in the pie chart under VMs not protected section of Overview page.
The tool tip on the "VMs not protected" slice of the pie chart lists the virtual machines names that are not configured in the NetWorker server and have a status of 'Missing' in the SCVMM.

- VMs protected—These virtual machines are configured for scheduled backup as part of a NetWorker client resource.

A virtual machine is protected when it is configured for scheduled backups as part of a NetWorker client resource. A virtual machine that is configured for scheduled backups but does not have existing backups is considered protected. Conversely, a virtual machine that is not configured for scheduled backups but has existing backups is not considered protected.

**Note**

The Data Protection Add-in is unable to distinguish between multiple virtual machines with the same name on the same host. If a host has multiple virtual machines with the same name, and any of these virtual machines are backed up, the Data Protection Add-in shows all the virtual machines as backed up.

The following figure shows the Data Protection Add-in Overview page for Administrator, Fabric Administrator, and Read-Only Administrator user roles.

**Figure 17 Data Protection Add-in Overview page for Administrator, Fabric Administrator, and Read-Only Administrator user roles**

When you position the mouse over a protection category in the pie chart, a tooltip lists the first 10 virtual machines for that protection category. If there are more than 10 virtual machines in that category, the list is truncated with an ellipsis. To view the full list, click the wanted section of the pie chart. If the virtual machine name is more than 40 characters in length, the tooltip truncates the virtual machine name with an ellipsis.

The following figure shows the pie chart and tooltip for Administrator, Fabric Administrator, and Read-Only Administrator user roles.
When you click a protection category in the pie chart, the virtual machine Protection Details window displays. This window contains a table that lists the name, host, and ID for each virtual machine in the selected protection category. To copy data for all the virtual machines to the clipboard, click the Copy All to Clipboard button. To copy data for specific virtual machines, select the wanted rows in the table and click the Copy Selected to Clipboard button. You can press Ctrl or Shift to select multiple rows, similar to other Windows applications.
**Overview page for Tenant Administrator and Application Administrator user roles**

For Tenant Administrator and Application Administrator user roles, the Overview page displays multiple sub-panes:

- Clouds, Clusters, and Hosts sub-panes—These sub-panes display "NA", since Tenant Administrator and Application Administrator user roles do not have access to other clouds, clusters, or hosts.

- Virtual machines sub-panes—This sub-pane lists the number of virtual machines that the Tenant Administrator and Application Administrator user roles can access.

The pie chart provides the following data about virtual machines:

**VMs not backed up**

These virtual machines are not currently backed up as part of a NetWorker client resource.

**VMs backed up**

These virtual machines are currently backed up as part of a NetWorker client resource.

---

**Note**

The Data Protection Add-in is unable to distinguish between multiple virtual machines with the same name on the same host. If a host has multiple virtual machines with the same name, and any of these virtual machines are backed up, the Data Protection Add-in shows all the virtual machines as backed up.

---

The following figure shows the Data Protection Add-in Overview page for Tenant Administrator and Application Administrator user roles.
When you position the mouse over a backup status category in the pie chart, a tooltip lists the first 10 virtual machines for that backup status category. If there are more than 10 virtual machines in that category, the list is truncated with an ellipsis. To view the full list, click the wanted section of the pie chart. If the virtual machine name is more than 40 characters in length, the tooltip truncates the virtual machine name with an ellipsis.

The following figure shows the pie chart and tooltip for Tenant Administrator and Application Administrator user roles.
When you click a backup status category in the pie chart, the virtual machine Protection Details window displays. This window contains a table that lists the virtual machine name and virtual machine ID for each virtual machine in the selected backup status category. To copy data for all the virtual machines to the clipboard, click the Copy All to Clipboard button. To copy data for specific virtual machines, select the wanted rows in the table and click the Copy Selected to Clipboard button. You can press Ctrl or Shift to select multiple rows, similar to other Windows applications.
Recoveries

The Recover page displays a list of all VMs managed by SCVMM that are backed up by a NetWorker server in the Preferred Servers list and in the current selected context and match the date filtering criteria. When you access the Recover page for the first time, click Refresh to populate the grid with backups performed on the VMs in the current context.

NOTICE

To recover backups that were created using an NMM release earlier than 9.0, click Start > EMC NetWorker > NetWorker Tools > Restore previous NMM release backups to start the NetWorker Module for Microsoft GUI. Browse the backups and perform the recovery from the GUI that appears.
If you change the SCVMM environment, such as adding a virtual machine, adding a NetWorker server on the Preferences page, or performing a redirected recovery, click Refresh to update the list of VMs on the Recover page.

When performing virtual machine recoveries by using the Data Protection Add-in, consider the following:

- The Data Protection Add-in supports recoveries only from conventional backups. You cannot use the Data Protection Add-in to recover virtual machines from NMM Hyper-V persistent snapshots.
- The Data Protection Add-in is unable to distinguish between multiple VMs with the same name on the same host. If a host has multiple VMs with the same name, the Data Protection Add-in shows incorrect recovery options.
- The Data Protection Add-in does not support recoveries of VMs that have differencing disks.
- The Data Protection Add-in does not perform multiple operations simultaneously, such as recovering multiple VMs or refreshing the list of VMs during a recovery. The Recover and Refresh buttons are disabled while a recovery or refresh operation is in progress.
- The recovery progress log messages are reported in the following locations:
  - On the Monitoring page in the Data Protection Add-in.
  - On the Hyper-V server where the actual recovery is performed.
  - Open the Windows Event Viewer on the server that is hosting the SCVMM console. To access the event logs, browse to Application and Services Logs > Networker Recovery Service.
- When recovering to a Windows Server 2016 destination host, the Data Protection Add-in for SCVMM performs import based recovery or proxy based recovery.
- For highly available VMs in cluster configurations, recovery to the original location is always to the active node of the cluster, regardless of the existing virtual machine physical host location. Before starting the recovery, confirm that the cluster active node is the same as the virtual machine physical host. After the...
recovery is complete, you might need to use Microsoft Cluster Manager to make the virtual machine highly available again.

**Note**

If this practice is not followed, the resulting conflict of the same virtual machine on different nodes can be very difficult to repair and might require a cluster restart.

- For highly available virtual machine recoveries, when you recover to a cluster physical node rather than to the cluster virtual server, you must use Microsoft Cluster Manager to make the virtual machine highly available after the recovery completes.
- For recoveries of VMs on Hyper-V servers over SMB 3.0 configurations, the Data Protection Add-in supports recovery of stand-alone and clustered configurations.

**Note**

Because the Data Protection Add-in performs Hyper-V recoveries by using NMM, the NMM Hyper-V considerations that are described in the documentation also apply to performing Hyper-V recoveries by using the Data Protection Add-in.

### Viewing available virtual machines

The Recover page displays a list of all virtual machines that match the following criteria:

- Reside within the currently selected context of the SCVMM navigation pane
- Have been backed up by a NetWorker server in the Preferred Servers list
- Have at least one backup date that matches the current date filter

You can sort the list by VM Name, Hyper-V Host, or Availability.

You can further filter virtual machine names by typing a search string in the Enter a VM name to filter field and clicking Filter.

**Note**

The search string can be the full virtual machine name or a sub string of the virtual machine name; The search is case in-sensitive; The search filter is based on the virtual machine name only; Regular expressions are not allowed as part of the search string.

By default, the Recover page shows all virtual machines that were backed up on or before the current date. You can filter the virtual machines by selecting one of the date criteria options and choosing a date on the calendar. Only virtual machines with backup times that match the specified date filtering criteria are displayed. If you select criteria that results in no matching backup dates for a particular virtual machine, then that virtual machine does not display in the table.

### Recovering a virtual machine to the original location

The recovery operation runs on the Hyper-V server that is hosting the virtual machine or, if the virtual machine is highly available, on the active node of the cluster. The Monitoring page displays the status of the recovery.

**Procedure**

1. In the SCVMM console, ensure the Home tab is selected.
2. In the workspaces pane of the SCVMM console, click VMs and Services.
3. In the navigation pane, select the host or cloud that contains the virtual machine you want to recover.
4. On the SCVMM ribbon, click **EMC Data Protection**.
5. In the Data Protection Add-in, click the **Recover** tab.
6. On the **Recover** page of the Data Protection Add-in, select the virtual machine in the table.
7. Select the **Date Backed Up** cell, click again to activate the drop-down list, and select the backup date and time.
8. Click the **Recover** button.

**Redirected recoveries**

The Data Protection Add-in supports redirected recovery of virtual machines to an alternate host to which you have access in the SCVMM console, provided the host is protected with NetWorker Server.

In the SCVMM host, the virtual machine placement path properties contain one or more paths. The redirected recovery location is the first location in this list.

The Data Protection Add-in recovers to the default SCVMM placement path that the Hyper-V administrator configured during the Hyper-V role installation.

The Data Protection Add-in does not support redirected recoveries of Hyper-V backups that were taken before an NMM 8.2 upgrade.

The Data Protection Add-in supports redirected recoveries to a host running the same or later operating system version. For example: The Data Protection Add-in supports redirected recovery from a Windows Server 2016 source host to a Windows Server 2016 destination host, but the Data Protection Add-in does not support redirected recovery from a Windows Server 2016 source host to a Windows Server 2012 R2 destination host.

The Data Protection Add-in does not support virtual machine redirected recovery to an SMB path location. If a virtual machine placement path property specifies a path to an SMB location as the first item in the path list, then a redirected virtual machine recovery to this Hyper-V server is not supported.

**Virtual machine IDs after redirected recovery**

NMM assigns a new virtual machine ID in certain redirected recovery scenarios. The redirected recovery continues normally, regardless of whether NMM assigns a new ID or uses the existing ID. If NMM assigns a new ID during redirected recovery, then the virtual machine appears in both the source and destination hosts.

The following table provides details about whether NMM assigns the existing virtual machine ID or a new virtual machine ID during a redirected recovery:

<table>
<thead>
<tr>
<th>Source operating system</th>
<th>Destination host</th>
<th>Destination virtual machine ID assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 R2</td>
<td>Windows Server 2008 R2</td>
<td>Existing</td>
</tr>
</tbody>
</table>
Table 14  Virtual machine IDs after redirected recovery (continued)

<table>
<thead>
<tr>
<th>Source operating system</th>
<th>Destination host</th>
<th>Destination virtual machine ID assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Operating system</td>
<td>Configuration type</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>Windows Server 2012 or 2012 R2</td>
<td>CSV</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>Windows Server 2012 or 2012 R2</td>
<td>Stand-alone</td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>Windows Server 2012 or 2012 R2</td>
<td>CSV</td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>Windows Server 2012 or 2012 R2</td>
<td>Stand-alone</td>
</tr>
<tr>
<td>Windows Server 2012 R2</td>
<td>Windows Server 2012 or 2012 R2</td>
<td>CSV</td>
</tr>
<tr>
<td>Windows Server 2012 R2</td>
<td>Windows Server 2012 or 2012 R2</td>
<td>Stand-alone</td>
</tr>
</tbody>
</table>

File paths for redirected recovery virtual machines and VHDs

For a redirected recovery, the Data Protection Add-in uses the SCVMM placement path property as the default location for recoveries. The Data Protection Add-in extends the default SCVMM placement path property value by appending the virtual machine name and the recovery time (vmname_timestamp) to create a unique subfolder.

If you recover multiple virtual machines with the same name on different source hosts to the same destination host, the Data Protection Add-in recovers these virtual machines to two different folders with unique subfolders by appending vmname_timestamp to the folder names. For example, if two virtual machines that are both named Virtual_Machine are recovered to the default SCVMM placement path property "C:\ProgramData\Microsoft\Windows\Hyper-V", the virtual machines are recovered to the following unique subfolders:

- C:\ProgramData\Microsoft\Windows\Hyper-V \Virtual_Machine_20140917143500\
- C:\ProgramData\Microsoft\Windows\Hyper-V \Virtual_Machine_20140917152205\

If the virtual machine has multiple disks with the same name, the Data Protection Add-in recovers these disks to separate folders. For example, if a virtual machine with two VHDs that are both named DualDisk.vhd are recovered to the default SCVMM placement path property "C:\ProgramData\Microsoft\Windows\Hyper-V", the virtual machines are recovered to the following unique subfolders:

- C:\ProgramData\Microsoft\Windows\Hyper-V \DualDisk_20140625133500\1\DualDisk.vhd
- C:\ProgramData\Microsoft\Windows\Hyper-V \DualDisk_20140625133500\2\DualDisk.vhd
Microsoft limits virtual machine file paths to 260 characters. If the appended file path exceeds 260 characters, the recovery fails.

Performing a redirected recovery

Redirected recovery of NMM 8.2 and later save sets cannot be performed to a NMM 9.1 Hyper-V Server and vice-versa.

Procedure

1. Take the original virtual machine offline to avoid conflicts during the recovery operation.
2. In the SCVMM console, ensure the **Home** tab is selected.
3. In the **workspaces** pane of the SCVMM console, click **VMs and Services**.
4. In the left navigation pane, select the host or cloud that contains the virtual machine you want to recover.
5. On the SCVMM ribbon, click **EMC Data Protection**.
6. In the Data Protection Add-in, click the **Recover** tab.
7. On the **Recover** page of the Data Protection Add-in, select the virtual machine in the table.
8. Select the **Date Backed Up** cell, click again to activate the drop-down list, and select the relevant backup date and time.
9. Select the **Recover Destination** cell, click again to activate the drop-down list, and select the destination host.
   - The **Recover Destination** drop-down list shows physical Hyper-V hosts that are NetWorker clients and that are visible in SCVMM for the current user. The **Recover Destination** drop-down list does not list the NetWorker virtual server clients representing the clusters.
10. Click the **Recover** button.
11. If an **Action Needed** message displays, click **OK** to clear the message.
12. Confirm that the virtual machine is successfully recovered by verifying that the virtual machine appears in the hypervisor on the Hyper-V server where you recovered the virtual machine.
13. If the **Action Needed** message displayed, delete the original virtual machine from its original host by using the SCVMM console. Alternatively, delete the virtual machine by using Hyper-V Manager or PowerShell, and then refresh the SCVMM console.
14. In the navigation pane of the SCVMM console, right-click the destination host and click **Refresh Virtual Machines**.
15. If a new ID was assigned to the virtual machine as described in Virtual machine IDs after redirected recovery on page 103, in the navigation pane of the SCVMM console, right-click the source host and click **Refresh Virtual Machines**.
16. Ask the NetWorker administrator to perform a backup of the virtual machine from its new Hyper-V host.
Viewing virtual machines after a redirected recovery

If you perform a redirected recovery of a virtual machine to a Hyper-V host, then the virtual machine will not meet the criteria that are listed in Viewing available virtual machines on page 102 until after a new backup of the virtual machine is completed. Therefore, the Recover page does not immediately display the redirected virtual machines. After you perform a redirected recovery for a virtual machine, ask the NetWorker administrator to perform a backup of the Hyper-V host where the virtual machine currently resides.

Because the Data Protection Add-in displays only backups for the current Hyper-V host of the virtual machine, if you want to recover a virtual machine from a backup that was taken before a redirected recovery, you must use NMM.

Recovering a deleted virtual machine

The Data Protection Add-in does not support recovering virtual machines that have been deleted from SCVMM. The NetWorker administrator must perform the recovery by using NMM.

Monitoring

The Monitoring page provides information about Data Protection Add-in events and operations.

The Monitoring page displays:

- Status of recovery operations in progress
- Details of queries to the NetWorker servers and the SCVMM server
- All logging entries from previous uses of the Data Protection Add-in (if any)
The Monitoring page shows three columns, all of which can be sorted:

- DataTime
- EventType
- Message

The monitor log information is updated in real-time as operations occur. To manually scan for updated protection information, click Refresh.

You can export the log file by clicking Export at the bottom of the Monitoring page. NMM logs are stored on the destination host, where the virtual machine is restored. The exported log file name is MonitorExportFile and is at C: \Users\<current user>\AppData\Local\EMC\NetWorker\SCVMM.

Troubleshooting

This section includes information about how to resolve general issues you might encounter while using the Data Protection Add-in. The NetWorker Administration Guide and the NetWorker Module for Microsoft Administration Guide provide additional troubleshooting details.

Recovered virtual machine does not start

If a recovered virtual machine does not start, perform the following steps:

**Procedure**

1. Select the recovered virtual machine, then right-click the virtual machine and select Discard Saved State.
2. Right-click the recovered virtual machine and then select Properties.
3. In the **Properties** dialog box, click **Hardware Configuration** and verify the Network Adapter settings of the virtual machine.

**Installation fails due to access issue**

When you install the Data Protection Add-in, you need access to the following path:

```
C:\Users\Public\Documents\EMC NetWorker\nsr\addins\VMM_DataProtection
```

**Note**

This path applies to environments in which the system drive is **C:**.

**Solution**

Before you install the Data Protection Add-in, verify that you have read/write access permissions to the paths previously noted.

**The Data Protection Add-in for SCVMM displays an incorrect NetWorker Server version**

If the NetWorker Server software is updated, the Data Protection Add-in for SCVMM displays the previous version number until you remove and re-add that NetWorker server in the Add-in.

**Importing fails due to access issue**

To import the Data Protection Add-in, you need access to the following paths:

- `C:\Program Files\Microsoft System Center 2016\Virtual Machine Manager\bin\AddInPipeline\AddInViews`
- `C:\Program Files\Microsoft System Center 2016\Virtual Machine Manager\bin\AddInPipeline\AddIns`

**Note**

These paths apply to environments in which SCVMM was installed in the default location of `C:\Program Files`.

If you do not have access to the required paths, you receive the following error:

The assembly

`Microsoft.SystemCenter.VirtualMachineManager.UIAddIns.dll` referenced by the add-in assembly `EMC.BRS.ScvmmAddIn.AddInView` could not be found in the add-in package. Ensure that this assembly was included with the add-in package.

**Solution**

Before you import the Data Protection Add-in, verify that you have read/write access permissions to the previously noted paths.

**Virtual machine attributes might display incorrect values**

On the **Monitoring** page of the Data Protection Add-in, the **VM Availability** attribute might occasionally show an incorrect value.

To show the correct information:
1. In the SCVMM navigation pane, refresh the virtual machine.
2. In the Data Protection Add-in, click **Refresh**.

**Redirected recovery appears to succeed but no virtual machine appears in Hyper-V Manager**

If a redirected recovery appears to succeed but no virtual machine appears in Hyper-V Manager, the network of the target host might be incompatible. For example, if the target host is in a non-trusted domain, redirected recovery to this target host fails.

If the network of the target host is incompatible, then the virtual machine is disconnected from the network. The recovery succeeds according to the Data Protection Add-in monitor log and the `nsrnmmsv.raw` log, and the virtual machine files are stored on the target host and volume, but Hyper-V Manager does not display or recognize the virtual machine.

**Solution**

Reconnect the existing switch of the host by using the SCVMM GUI or by using the following PowerShell command:

```
$sw=Get-virtual machineswitch;get-vm -Id <vmID> | Get-VMNetworkAdapter | Connect-VMNetworkAdapter -SwitchName $sw.Name
```

After reconecting the existing switch, re-attempt the redirected recovery.

**Checks for redirected recovery failures**

Redirected recovery of a virtual machine might fail due to virtual machine network or saved state incompatibility between the original Hyper-V host and the target Hyper-V host. The Hyper-V writer cannot register the virtual machine because of errors in virtual machine configuration files which the writer cannot resolve.

If you suspect this is the problem for a failed redirected recovery, then examine the target host destination location for the virtual machine files. Look in the Monitor logs for the redirected restore cmd line options: output. If the virtual machine files are there, then try to register the virtual machine manually by using the SCVMM UI.

**Avoid virtual machine names with the same name within an SCVMM context**

The Data Protection Add-in primarily uses the virtual machine name, as displayed in Hyper-V Manager or Failover Cluster Manager, as an identifier for the virtual machines. If multiple virtual machines have the same name in the same SCVMM context, then the Add-in is unable to distinguish between the virtual machines. Although not required, it is considered best practice for virtual machine names to be unique.

**Cluster virtual machine backups do not display on the Recover page**

If a cluster virtual machine backup does not display on the Recover page, check that the cluster is configured as highly available in Microsoft Cluster Manager.

If a virtual machine is removed from Microsoft Cluster Manager and is no longer shown by PowerShell as highly available, the backups for that virtual machine do not display on the Recover page.
Redirected recovery is not supported when the virtual machine name or virtual machine configuration path contains special characters

NMM Hyper-V restricts the use of special characters in virtual machine names and virtual machine configuration paths.

When you try to recover a Hyper-V save set, virtual machine name, or file path that contains a character that is not listed above, the Data Protection Add-in checks the name and path of the virtual machine objects and displays a warning message stating that the virtual machine contains unsupported characters and cannot be recovered to an alternate location.

You can use SCVMM to perform the following workaround:

Procedure

1. Recover the virtual machine to the original location of the backup.
2. Use SCVMM to export the virtual machine to a temporary location.
3. Copy the virtual machine files to an appropriate location on the target host.
4. Use SCVMM to import the virtual machine.
CHAPTER 7

Windows Bare Metal Recovery Solution

This chapter includes the following sections:

- Microsoft Hyper-V Backup and BMR .............................................................. 112
- Microsoft System Center Virtual Machine Manager backup and BMR ........... 113
Microsoft Hyper-V Backup and BMR

Ensure that the Hyper-V Server is backed up before performing BMR.

Backing up Hyper-V for BMR

Configure a Hyper-V client resource to back up Hyper-V for BMR.

Review the "Configuring a client resource by using the Client Backup Configuration Wizard" and "Configuring a client resource manually by using the NetWorker Management Console" sections in the Backups chapter for detailed information about how to create a client resource.

Note

Separately create a client resource to back up the application data and the file system data which includes the DISASTER_RECOVERY:\ save set.

Performing BMR of Hyper-V

Ensure that the cluster service account is enabled. Otherwise, the explorer stops responding when you browse CSVs and the recovery fails.

To enable the cluster service computer account, log in to the Domain Controller with the domain administrator credentials, and use the Active Directory Users and Computer snap-in.

Procedure

1. Perform the procedures that the "Performing a Windows BMR recovery to physical or virtual computers" section in the NetWorker Administration Guide describes.

   After the recovery completes, the status of Hyper-V VMs in the Failover Cluster Manager window are either Pending or Failed.

2. Reconfigure quorum and cluster storage (CSV and non-CSV volumes):
   a. Create or configure the quorum, CSV, and non-CSV shared volumes.
   b. Ensure that you have documented the drive letters for quorum and non-CSV (shared volume) and used here.
   c. Ensure that you have configured the same CSV volume name as the original.

3. Recover all Hyper-V cluster nodes by using the NMM client.

4. Reconfigure the VMs with either the Pending or the Failed status.

5. Recover the Hyper-V VMs that the CSV volumes host with the virtual node as the client resource, by using the NMM client.

6. Recover the Hyper-V VMs that the non-CSV volumes host with the physical node as the client resource, by using the NMM client.
Microsoft System Center Virtual Machine Manager backup and BMR

Ensure that the System Center Virtual Machine Manager is backed up before performing BMR.

Backing up System Center Virtual Machine Manager for BMR

Back up and recover the following key components of VMM to ensure a protected VMM environment:

- **VMM server**: The VMM server is the central component of a VMM deployment. The server contains the core Windows service that includes the VMM engine.
- **VMM database**: The VMM database resides on either the VMM server or on a remote database server. You must regularly save the VMM database to quickly recover the VMM environment.
- **VMM library**: The VMM library is either one file server or multiple file servers with file shares that index specific file types that the VMM uses. The VMM library shares include VHD, VMDK, ISO, PS1, INF, VFD, FLP, and XML files besides stored virtual machines.

You must frequently back up the data such as, the data on the virtual machines, which VMM manages, that often changes. NMM supports the Microsoft Hyper-V VSS writer to protect Hyper-V virtual machines. The *NetWorker Module for Microsoft for Hyper-V VSS User Guide* provides information about how to back up the environment’s virtual machines.

You must perform BMR backups for the Hyper-V servers also.

If you have installed any component of VMM on a Hyper-V virtual machine, you can protect it by using the NMM client’s Hyper-V. Use NMM to protect the VMM server, the VMM library, or the VMM database on a virtual machine. NMM takes image backups of Hyper-V virtual machines. You do not need to install an NMM client on the virtual machine. Instead, install an NMM client on the Hyper-V server and configure NMM client resources to back up the virtual machines. Use the NMM GUI Hyper-V plug-in to recover a virtual machine that contains a VMM component.

The *NetWorker Module for Microsoft for Hyper-V VSS User Guide* provides information about how to protect a Hyper-V server’s information.

Backing up the VMM library for BMR

The VMM library is a catalog of resources that enables you to store objects that are not running or associated with a host. The library contains the files that are present on library shares, templates, operating system profiles, and hardware profiles.

**Procedure**

- Use the NMM backup and recovery techniques for Windows files servers to back up and recover a VMM library server.
- Use the NetWorker client to back up the VMM library by specifying the `ALL save` set to perform a Windows BMR backup of the VMM library. The `ALL save set` enables you to back up the local file systems and the `DISASTER_RECOVERY:\` save set of the VMM library.

Configuring a client resource by using the Client Backup Configuration Wizard on page 47 and Configuring a client resource manually by using the NetWorker
Management Console on page 52 provide information about how to create client resources to back up the application data and the file system data respectively.

Backing up the VMM server for BMR

The VMM server relies on the VMM database to store data. The VMM database uses the server account to encrypt that data.

You must perform a full backup of the VMM server host to ensure that you meet the following requirements:

- The same host account is available to interact with the VMM database after recovery.
- All virtual machine hosts associates and communicates with the VMM server.
- You can recover any communication certificates so that the existing agents continue to work as you expected.

You can protect the VMM server by performing a NetWorker Windows BMR backup along with an NMM backup of local file systems and application-specific data, such as the data associated with Hyper-V Server, SQL Server, or SharePoint Server. The advantage of a Windows BMR backup and recovery capability for a VMM server is that the backup includes the system state. When you perform recovery, the system state recovers the computer security identifier (SID) that uniquely identifies the computer to the network. The computer-recovered SID enables the VMM server to quickly and easily interact with any existing VMM database, VMM library, and managed servers without additional post-recovery operations. The Windows BMR backup captures the VMM authorization datafile which is typically `%ProgramData%\Microsoft\Virtual Machine Manager\HyperVAuthStore.xml` when protecting the critical system drive.

Procedure

1. Use the NetWorker client to back up the VMM server non-application files by specifying the `ALL` save set. This setting enables the backup of the local file systems and the `DISASTER_RECOVERY:` save set of the VMM server.

2. Use an NMM client resource specification to perform a full backup of any application data on the VMM server.

Backing up the VMM database for BMR

The VMM database is a SQL Server database that contains all the configuration information for VMM. Give the highest priority to protect the VMM database.

The default installation of VMM uses Windows Internal Database (WID), a version of Microsoft SQL Express, on the same host as the VMM server. The database name is `MICROSOFT$VMM$\Virtual Manager DB`. However, the VMM database can also reside on either an existing Microsoft SQL Server Standard or SQL Server Enterprise server. To find out the location of the database for VMM, inspect the Registry values entries under the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Microsoft System Center Virtual Machine Manager Server\Settings\Sql` key.

NMM clients support the backup and restore of SQL databases.

Back up the VMM database that is part of a SQL Server installation.
The NetWorker Module for Microsoft for SQL VDI User Guide provides information about how to protect a SQL server.

**Procedure**
1. Configure an NMM SQL Server client resource for the system with the VMM database.
2. Include the VMM databases when you schedule a backup.
3. In the Client Properties dialog box, in the Save set field, specify the VMM database. You can save either the entire SQL Server or named instances and individual databases.

**Performing BMR of a System Center Virtual Machine Manager**

The VMM components have interdependencies. Recover the entire VMM environment for a disaster recovery.

**Procedure**
1. Recover the library file server.
   a. Recover the physical VMM library file server with a Windows BMR save set.
   b. Use the NetWorker client file system plug-in to recover the file system that you shared as the VMM library.
2. Recover the VMM database.
   a. Recover the physical SQL server with a Windows BMR save set.
   b. Stop the VMM services.
   c. Use the NMM GUI SQL plug-in to restore the VMM database.
   d. Start the VMM services.
3. Recover the VMM host.
4. After the operating system and VMM server are stable, perform the required post-recovery VMM steps that the Microsoft documentation describes.

**Performing BMR of the VMM server**

Perform the procedures described in the "Performing a Windows BMR recovery to physical or virtual computers" section in the NetWorker Administration Guide.

**Performing BMR of the VMM library**

**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 you recover the file share directories, either adjust the VMM Library Refresher interval or manually trigger the Library Refresher to enable VMM to refresh the contents of the file server share.
   The VMM Administrator Console embedded help describes how to set the Library Refresher interval and perform a manual refresh.

**Performing BMR of the VMM database**

Perform the procedures that the "Performing a Windows BMR recovery to physical or virtual computers" section in the NetWorker Administration Guide describes.
If you only back up and recover the VMM database, then you must use the same instance of the VMM server component for the restore. This is important to reduce VMM post-restore steps. Microsoft VMM documentation provides more information.

You must manually stop the VMM Windows service before you restore the VMM database. After you restore the database, start the service. After you restore the VMM database and start the VMM Windows service, VMM synchronizes the database with the VMM server and VMM library computers.

**Note**

You must reapply any changes that you made to the VMM environment between the time of the backup and the restore. For example, you must re-create the templates that you created in VMM after performing the backup that you use to perform the restore.

Before you restore a SQL database, verify whether all the SQL services have started. To perform a SQL Server recovery as part of BMR, perform the steps that the Bare Metal Recovery chapter in the *NetWorker Module for Microsoft for SQL VDI User Guide* describes.
CHAPTER 8
Best Practices and Recommendations

This chapter includes the following sections:

- Non-ASCII files and directories ................................................................. 118
- Required AFTD DFA device settings for Hyper-V environments .......... 118
- Hyper-V Server backup and recovery best practices ........................... 118
- Microsoft application backup and recovery within a Hyper-V virtual machine best practices ................................................................. 119
- Improving backup performance in Windows Server 2012 and 2012 R2 clusters with CSV ................................................................. 119
- Data mining using Hyper-V granular level recovery ............................... 120
- Restrictions and requirements for relocating and recovering data to a different location ........................................................................ 121
- Restrictions for backup and recovery of Hyper-V virtual machines in a Windows Server Failover Cluster ............................................ 121
- Restrictions for Hyper-V virtual machine granular-level recovery ........ 122
Non-ASCII files and directories

If you create a Client resource with the Client Properties dialog box and the Save set attribute contains non-ASCII characters, you must edit the Save operations attribute on the Apps & Modules tab for the Client resource.

On Windows clients, specify the following value in the Save operations attribute:

I18N:mode=utf8path

On UNIX/Linux clients, specify the following value in the Save operations attribute:

I18N:mode=nativepath

You must enable diagnostic mode view by selecting View > Diagnostic Mode in the Administration window to access the Save operations attribute in the Client Properties dialog box.

Required AFTD DFA device settings for Hyper-V environments

For Hyper-V environments, when creating a NetWorker AFTD DFA device on an NTFS or ReFS volume, Microsoft requires certain settings.

If the NetWorker AFTD DFA device is created on an NTFS volume, virtual hard disk files must be uncompressed and unencrypted. If the NetWorker AFTD DFA device is created on an ReFS volume, virtual hard disk files must not have the integrity bit set.

Hyper-V Server backup and recovery best practices

This type of backup uses the Hyper-V Writer on the Hyper-V server:

- To get the most benefit from the Hyper-V role, create separate virtual machines for each application, so that the application-type backup and recovery that is performed at the host level is only for Hyper-V.
- After disaster recovery of the Hyper-V server, you might need to recover applications within each virtual machine if:
  - You are performing separate virtual machine backups.
  - These backups are more recent than the complete Hyper-V server backups.
- This type of backup is best used for Bare Metal Recovery of a guest and for recovery of operating system roles.
- Best practice for Host Component file backup is to back up when Hyper-V configuration changes are made. You do not need to back up the Host Component file each time a virtual machine guest is backed up.
- In NMM, the Hyper-V Writer does not support backup of the Host Configuration file to a proxy client.
- The primary purpose for recovering the Host Component file in NMM is for disaster recovery of the Hyper-V Server.
- Roll-forward recovery is not available for virtual machine level disaster scenarios. From a Hyper-V server, a roll-forward recovery of a virtual machine is not possible. Recoveries from a Hyper-V server are point-in-time (disaster recovery).
- Virtual machine pass-through disks are skipped during Hyper-V Server backups.
- Basic disks are supported only within virtual machines. NMM does not support backups of dynamic disks within virtual machines. NMM mounts the guest snapshot during the Hyper-V backup process, and this changes the disk signature on dynamic disks in a guest.
- NMM supports Windows Server Failover Clustering, which allows you to configure a failover of virtual machine.
- EMC storage that is connected to Fibre Channel or iSCSI storage can be used in the parent to host virtual machines.
- Do not take a Hyper-V VSS server snapshot of Hyper-V virtual machines that are part of a SharePoint farm. To back up SharePoint on the Hyper-V virtual machine:
  1. Install the NMM client on the virtual machine.
  2. Perform the SharePoint backup locally within the virtual machine.

The Microsoft website provides recommendations and requirements about using SharePoint and Hyper-V together.

**Microsoft application backup and recovery within a Hyper-V virtual machine best practices**

Microsoft applications backup and recovery are performed within the Hyper-V virtual machine and use application and system component writers that are available on the virtual machine.

- Microsoft recommends using backups within the virtual machine as the preferred method for Exchange backup and recovery.
- NMM supports roll-forward recovery for Exchange.
- NMM applies standard application backup and recovery rules and capabilities, including roll-forward recoveries.
- NMM skips virtual machine pass-through disks in Hyper-V backups. NMM supports pass-through disks backups within the virtual machine.
- NMM supports Windows Server Failover Clustering with iSCSI storage.
- NMM does not support virtual machine Windows Server failover clustering with Fibre Channel storage because SCSI-3 is not supported in Hyper-V virtual machines.

**Improving backup performance in Windows Server 2012 and 2012 R2 clusters with CSV**

When a cluster node is used as the proxy client, and you use the cluster proxy client to perform image-level backups of the virtual machines in a Windows Server 2012 or 2012 R2 cluster, NMM performs the backup of the data from the cluster node that owns the CSV where the virtual machine files reside.

For example, Cluster Node 1 owns CSV1 on which the virtual machine 1 files reside, and the cluster proxy client runs on Cluster Node 2. When the cluster proxy node backs up virtual machine 1, the backup process:

- Creates a shadow copy of CSV1.
- Streams the backup data from Cluster Node 1 to Cluster Node 2.
Routes the backup data to the NetWorker server. In this example, the backup performance depends on network performance between the cluster nodes. The performance for this backup is slower than backups where the CSV node ownership is co-resident with the cluster proxy client.

When using a cluster proxy client for virtual machine backups, consider the following recommendations to improve performance for image-level backups:

- Maximize the network bandwidth between the cluster nodes.
- Move the CSV ownership to the proxy cluster client so that the shadow copies of these volumes are local to the backup process.

To maximize the backup performance, ensure that the cluster node that runs the NMM proxy cluster client owns the targeted CSVs. Before you move the CSVs, consider the following recommendations:

- Ensure that the cluster node with the cluster client proxy has the capacity to own all physical nodes.
  
  The CSV owner node is responsible for file system metadata updates to the NTFS partition. If you change the ownership of a CSV volume to a single node, the performance of all the associated virtual machines on the CSV may be impacted. The cluster proxy client node must have the capacity to be the owner of all the CSVs.

- Ensure that any CSV you move is in the “healthy state”, online, and in full access mode.

  There are two ways to change the CSV ownership to the proxy node:
  - Use the Failover Cluster Manager GUI.
  - Use the PowerShell Module FailoverClusters cmdlet Move-ClusterSharedVolume.

  The Microsoft Failover Cluster document provides additional instructions for moving CSV ownership.

**Data mining using Hyper-V granular level recovery**

NMM can perform granular level recovery for backups of Hyper-V virtual machines that were created with NMM 3.0 or above. NMM with Hyper-V also supports data mining the information from the virtual machine image drives by using a tool such as EMC ItemPoint.

To prepare to mine the data, use the NMM GUI to mount the virtual machine, attach the VHDs, and load the virtual machines.

For example, if the virtual machine guest is running SharePoint, first use the NMM GUI to mount the Hyper-V virtual machine image, attach the VHSs, and load the virtual machines. Then use EMC ItemPoint for SharePoint to recover SharePoint sites, lists, libraries, and items.

You must keep the NMM GUI open while you explore and recover files on the mounted virtual machine VHDs. If you close or change the focus of the NMM GUI, you lose access to the mounted VHDs. A warning is displayed when a closure or focus change causes loss of access to a mounted virtual machine image.
Restrictions and requirements for relocating and recovering data to a different location

Hyper-V has several restrictions on relocating and recovering to other locations. NMM does not support directed recoveries of virtual machines to a Hyper-V Server that is a later version than the source Hyper-V Server. Although you can restore a virtual machine to a destination Hyper-V Server that runs a Hyper-V Server version later than the source Hyper-V server, the virtual machine may not fully function on that server. For mixed environments, you might be unable to perform a redirected restore of a virtual machine from one type of environment to another. Mixed environments include the following configurations:

- Environments with both stand-alone and clustered Hyper-V Servers
- Cluster environments with different operating systems and types of virtual machine storage (CSV and SMB file shares)

Hyper-V does not support:

- Recovering Hyper-V virtual machines to non-Hyper-V Servers.
- Recovering the Host Component file to a different location.
- Relocating or redirecting Hyper-V backups that were taken before an NMM upgrade.

Before you relocate or recover Hyper-V backups, review these requirements:

- The parent partition must run Windows Server 2012 or later to recover, with relocation of files, a virtual machine that has Hyper-V snapshots.
- The destination host must have the NMM client installed.
- When you perform a directed recovery of a virtual machine to a Hyper-V Server that differs from the source, you must update the Network Adapter settings of the virtual machine with the Hyper-V Manager before you start the virtual machine.

Restrictions for backup and recovery of Hyper-V virtual machines in a Windows Server Failover Cluster

When a Hyper-V virtual machine resides on a physical host, which is part of a Windows Server Failover Cluster, you cannot back up or recover the virtual machine as part of the cluster virtual server.

For example, consider the following Failover Cluster setup:

- A cluster, Cluster_Virtual_Name, contains two physical hosts, Physical_Machine_1 and Physical_Machine_2.
- Physical_Machine_1 contains two virtual machines, VM1 and VM2.

You want to back up and recover VM1.

If you create a NetWorker client resource for:

- Cluster_Virtual_Name, NMM does not support backup and recovery of VM1 through that client resource.
- Physical_Machine_1, you can specify the following values in the save set attribute:
  - APPLICATIONS: \Microsoft Hyper-V—To back up the Hyper-V application. This save set includes all virtual machines on the physical host.
APPLICATIONS:\Microsoft Hyper-V\VM1—to back up an individual virtual machine, such as VM1.

You can recover VM1 from a backup of the NetWorker client resource of the physical host, Physical_Machine_1. Performing Hyper-V recovery to the original machine and location on page 60 describes how to perform this type of recovery.

You can perform a directed recover to recover VM1 from the NetWorker client resource of the physical host, Physical_Machine_1 to the Physical_Machine_2. Performing a directed Hyper-V recovery to a different host or location on page 61 describes how to perform this type of recovery.

Restrictions for Hyper-V virtual machine granular-level recovery

The following restrictions apply when you perform a granular-level recovery of a Hyper-V virtual machine.

Windows Server does not support:

- Recovery of deduplicated data. To recover deduplicated volume data, enable the Deduplication role.
- Recovery of ReFs volume data.

Hyper-V GLR does not support differencing disk with parent and child hard disk on different hard drives.
CHAPTER 9

Troubleshooting

This chapter includes the following sections:

- Troubleshooting backups
- Troubleshooting recovery
Troubleshooting backups

The following topics explain issues that might occur during the backup process for a Hyper-V environment and provide steps to resolve or work around the issues.

Redirected I/O status does not update after CSV backup

Problem
During a CSV backup, the CSV is in redirected I/O status. Other nodes cannot directly write to disks. Instead, the I/O is redirected over the LAN to the owner node that is performing the backup.

Solution
If the redirected I/O status does not update correctly after the CSV backup is complete, clear the status by performing one of the following procedures:

1. Type the following commands at the Windows PowerShell command prompt to delete the stale shadows:
   ```
   diskshadow
   DISKSHADOW> list shadows all
   DISKSHADOW> delete shadows all
   Test-ClusterResourceFailure "volume name"
   ```
   Note
   This command might clear the "backup in progress" status.

2. If the "redirected access" status is not cleared after performing step 1, change the coordinator node by moving the volume to another node in the cluster and verifying that the volume is online.
   Type the following command at the Windows PowerShell command prompt to clear the backup state for the affected volume:
   ```
   nsrcsvutil -c <csv_volume_path>
   For example: nsrcsvutil -c "c:\ClusterStorage\Volume1"
   ```

Hyper-V pass-through disks are not backed up in a child partition backup

Problem
For Hyper-V backups, the child partition pass-through disks are skipped in the Hyper-V parent partition backup, and child partition pass-through disks are supported by backups within the child partition. However, sometimes the Hyper-V parent partition backup of a child partition with a pass-through disk might fail completely.

Solution
If this failure occurs, contact Microsoft support for assistance because the problem might be with the hardware configuration or the Microsoft Hyper-V writer.
Hyper-V configuration requirements for backing up a virtual machine that contains multiple volumes

Problem
When the guest contains multiple virtual hard disks, the backup of the associated virtual machine from the Hyper-V server might fail because of a Microsoft limitation. When multiple volumes exist on the guest, VSS determines the shadowstorage area for the snapshots, based on the volume that has more space. This can cause snapshots of two volumes to reside on the volume that has more space. For example, the snapshots of volume C and volume D may reside on volume D because VSS has determined that volume D contains more space. During the snapshot revert stage, PostSnapshot, the snapshot of volume C may be lost if the snapshot of volume D is reverted first.

Solution
To prepare a multiple volume guest for backup:

1. Use the `vssadmin` command to force the shadowstorage of each volume to occur on the same volume. Run the following commands from inside each guest, not the parent physical Hyper-V Server.

   ```bash
   vssadmin Add ShadowStorage /For=C:/On=C:
   vssadmin Add ShadowStorage /For=D:/On=D:
   ```

2. Repeat as needed for each volume in the virtual machine.

Hyper-V CSV virtual machine backups fail when the VHDX is stored in the root of the CSV volume

Problem
Due to a Microsoft limitation, Hyper-V CSV virtual machine backups fail when the VHDX is stored in the root of the CSV volume. For example: `C:\ClusterStorage\Volume1\Test Lab.Vhdx`

Solution
Move the virtual machine to a subfolder. For example: `C:\ClusterStorage\Volume1\Test Lab\Test Lab.Vhdx`.

Backup of an online virtual machine might reset the uptime value of the virtual machine

Problem
After an Application-Aware backup of an online virtual machine, Hyper-V Manager might display an inaccurate system uptime. System uptime inside the guest operating system is accurate.

Solution
Contact Microsoft for help with this issue.

Hyper-V backups that are backed up in a crash-consistent state

Problem
When the guest contains multiple virtual hard disks, the backup of the associated virtual machine from the Hyper-V server might fail because of a Microsoft limitation. When multiple volumes exist on the guest, VSS determines the shadowstorage area for the snapshots, based on the volume that has more space.
This can cause snapshots of two volumes to reside on the volume that has more space. For example, the snapshots of volume C and volume D may reside on volume D because VSS has determined that volume D contains more space. During the snapshot revert stage, PostSnapshot, the snapshot of volume C may be lost if the snapshot of volume D is reverted first.

Solution
To prepare a multiple volume guest for backup:

1. Use the **vssadmin** command to force the shadowstorage of each volume to occur on the same volume. Run the following commands from inside each guest, not the parent physical Hyper-V Server.
   
   ```
   vssadmin Add ShadowStorage /For=C: /On=C:
   vssadmin Add ShadowStorage /For=D: /On=D:
   ```

2. Repeat as needed for each volume in the virtual machine.

**Troubleshooting recovery**

The following topics explain issues that might occur while performing a Hyper-V recovery and provide steps to resolve or work around the issues.

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

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

   ```bash
   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 Hyper-V 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.

**When recovering multiple Hyper-V CSV virtual machine through proxy, all the
virtual machines are recovered but all the virtual machines are not registered**

**Problem**

In a Hyper-V CSV setup, when you recover multiple Hyper-V CSV virtual
machines through proxy, all the virtual machines are recovered although only one
virtual machine is registered.

**Solution**

After recovery of multiple Hyper-V CSV virtual machines through proxy is
complete, NMM recovers the .vhd and .xml files. Manually run the following
PowerShell command to register the virtual machines that are not registered:

```powershell
PS C:\Users\administrator.CONTOSO> Import-VM -path "C:\ClusterStorage
\Volume3\CSV-VM-013\CSV-VM-013\Virtual Machines\E45E8DBB-
```
Troubleshooting

After Hyper-V CSV disaster recovery, application data recovery fails and CSV mount point is not browsable

**Problem**
After disaster recovery, if NMM is used to recover Hyper-V data, the following issues are observed:

- Hyper-V recovery of virtual machines that are located in a shared disk (but non-CSV volume) fails.
- The CSV volumes are not browsable, and recovery of virtual machines that are on the CSV volume fails.

**Solution**
Perform the following steps:
1. Remove stale entries from the cluster resource.
2. In the Domain Controller, start the Active Directory Users and Computers Snap-In, and ensure that the failover cluster virtual network name account of Hyper-V Virtual Server is enabled.

Through Advanced Recovery option, recovery of online virtual machine to other node in same cluster setup completes

**Problem**
In a Hyper-V CSV setup, when a child partition is running, the same child partition can be recovered to another node using the Advanced Recovery option. This creates multiple virtual machines in different CSV nodes.

**Solution**
If the virtual machine is online or active, recover the virtual machine to the same node.

NMM registers corrupted Hyper-V child partition to Hyper-V Server

**Problem**
Although a recovery operation for a Hyper-V child partition fails, NMM registers the corrupted Hyper-V child partition to the Hyper-V Server.

**Solution**
After receiving a confirmation about a failed recovery operation, the Hyper-V system administrator must delete the following:
1. The corrupted Hyper-V child by using the Hyper-V Manager.
2. The corresponding child partition .vhd files.
APPENDIX A

Recovering SQL Server, Exchange Server, and SharePoint Server Items from a Hyper-V Virtual Machine

This appendix includes the following sections:

- Overview.......................................................................................................... 130
- Recovering items that are stored on a Hyper-V virtual machine....................... 130
Overview

This appendix describes how to perform granular-level recovery (GLR) of Microsoft SQL Server, Exchange Server, and SharePoint Server items that are stored in Hyper-V virtual machines.

The Hyper-V Writer of Microsoft Hyper-V Server supports only full backups (VSS_BT_FULL). The Hyper-V requestor performs a full backup of virtual machines that run a Microsoft application (SQL Server, Exchange Server, or SharePoint Server). If a requestor specifies VSS_BT_COPY, the Hyper-V Writer performs a full backup, according to the VSS MSDN documentation.

The following table shows the backup types that the requester can set by using the SetBackupState on the host and the backup type set by the Hyper-V requestor inside the guest.

Table 15 Backup types

<table>
<thead>
<tr>
<th>Backup type set by requestor through SetBackupState on the host</th>
<th>Backup type set by Hyper-V's requestor inside the guest</th>
</tr>
</thead>
<tbody>
<tr>
<td>VSS_BT_FULL</td>
<td>VSS_BT_FULL</td>
</tr>
<tr>
<td>VSS_BT_COPY</td>
<td>VSS_BT_FULL</td>
</tr>
</tbody>
</table>

Virtual machine image backups are copy-type backups in-guest for applications. Log grooming requires separate in-guest application backups. The Microsoft documentation provides information about the VSS_BT_FULL backup type.

Recovering items that are stored on a Hyper-V virtual machine

Procedure

1. Configure the Hyper-V client resources on the NetWorker server and choose the Hyper-V Writer save set for backup.
2. Perform a full backup.
3. Open the NetWorker User for Microsoft GUI on the FLR proxy server that you configured for GLR.
4. Select the NetWorker server where you performed the Hyper-V Server backup. Click the icon next to NetWorker server to view the list of NetWorker servers in the Change NetWorker Server window.
5. Under **Options**, select the **Configure Option** and click the icon next to the **Client name** field in the **Select Viewable Clients** window to view the Hyper-V Server client resources.

**Figure 26 Select Viewable Clients window**

6. Click **Recover > Hyper-V Recover Session > Granular Level Recovery**.
Figure 27 Selecting granular level recovery

Recovering SQL Server items from a Hyper-V virtual machine

Procedure

1. Mount the virtual machine that hosts the SQL Server, attach the hard disk, and then browse to the folder that contains the database and logs from which you will recover the items.

   The following figure provides an example:

   Figure 28 Selecting SQL Server items for recovery from a Hyper-V virtual machine

2. Select the database (mdf) and logs (ldf) files.

3. Perform the recovery to the folder of your choice.

   If the database is offline in SQL Server Management Studio, perform the following steps:

   a. Copy the recovered database and logs files to the actual path.
b. Bring the database online.

c. Check that the recovered data is intact.

If the database is online in SQL Server Management Studio with some data corruption or loss, perform the following steps:

a. Bring the database offline.

b. Replace the existing database and logs with the recovered database and logs files.

c. Bring the database online.

d. Check that the recovered data is intact.

Recovering Exchange Server items from a Hyper-V virtual machine

Procedure

1. Mount the virtual machine that hosts the Exchange Server, attach the hard disk, and browse to the folder that contains the database and logs from which you will recover the items.

The following figure provides an example:

Figure 29 Selecting Exchange Server items for recovery from a Hyper-V virtual machine

2. Select the database and log files.

3. Perform the recovery to the folder of your choice.

If the database is online in the Exchange Management Console with some data corruption or loss, perform the following steps:

a. Bring the database offline.

b. Replace the existing database and logs folder with the recovered database and logs folder in the actual path.

c. Bring the database online.

d. Check that the recovered data is intact.
If the database is offline in the Exchange Management Console, perform the following steps:

a. Replace the existing database and logs folder with recovered database and logs folder in the actual path.

b. Bring the database online.

c. Check that the recovered data is intact.

Recovering SharePoint Server items

Use EMC ItemPoint for SharePoint Server to perform SharePoint GLR.

Procedure

1. Mount the virtual machine that hosts the SharePoint database, attach the hard disk, and browse to the folder that contains the database and logs from which you will recover the items.

2. Select the database and log files.

   NMM mounts the Hyper-V VHD file in a location that you define during GLR recovery. The default location is C:\Program Files\EMC NetWorker\nsr\tmp.

3. Use EMC ItemPoint for SharePoint Server to perform the SharePoint GLR.

   Install EMC ItemPoint for SharePoint Server on the SharePoint Server and on the FLR proxy server where you mount the Hyper-V virtual machine. These steps are similar to the procedure described in the NetWorker Module for Microsoft for SQL and SharePoint VSS User Guide. In this document, you directly mount the database under SharePoint and SQL Server Recover Session.

   However, to recover items from a virtual machine that hosts the SharePoint Server, you must configure EMC ItemPoint for SharePoint Server differently. In Add the Source Path for the database, select the path where the Hyper-V VHD is mounted and then browse through the folder to select the database.

   For example: C:\Program Files\EMC NetWorker\nsr\tmp\HyperVMountPoints\SQL2010\Hard Disk 0\Partition1\sqlfirstins\MSSQL11.FIRSTINSTANCE\MSSQL\DATA.

4. Provide the target SharePoint Server with credentials.

   EMC ItemPoint for SharePoint Server configures itself with the SharePoint Server and FLR proxy server by scanning the logs, pre-scanning the logs, hashing the logs, and retrieving the content database.

5. After the EMC ItemPoint for SharePoint Server configuration completes, copy the content to be recovered from the source to the target location.