EMC²
RELEASE NOTES

EMC® NetWorker®
Module for Microsoft Applications
Release 2.1

Release Notes
P/N 300-007-793
REV A07

September 8, 2009

These release notes contain supplemental information about this release of EMC NetWorker Module for Microsoft Applications. Topics include:

Revision history

Table 1 on page 2 presents the revision history of this document.

Table 1 Revision history

Revision	Date	Description
A07	September 8, 2009	• Added information about "Client security vulnerability hotfix 5.2.0.1 in NMM 2.1 SP1 build 165 (LGTsc30291)" on page 7. • Added note in "NMM 2.1 hotfixes in build 143" on page 8.
A06	March 11, 2009	Added to Known problems and limitations: • "Windows SharePoint Services 3.0 cumulative update package required to fix backup issues (LGTsc27991)" on page 53 • "NMM incremental backup fails for document in SharePoint Data Connection Library (LGTsc27989)" on page 53
A05	March 2, 2009	Added revision history.
A04	February 27. 2009	Service Pack 1. The following sections are new: • "Improved NMM performance and scalability" on page 4 • "NetWorker support for Linux" on page 5 • "Disaster recovery procedures" on page 9 The following sections have been updated: • "Known problems and limitations" on page 23 • "Technical notes" on page 53 In "Unsupported Windows features" on page 23, removed "EMC VSS Hardware Provider with Windows Server 2008," it is now supported.
A03	November 28, 2008	• Added "NMM 2.1 hotfixes in build 143" on page 8 • Updated "Known problems and limitations" on page 23 • Removed "Active Directory only recovers objects 1 level deep (LGTsc20936)"
A02	October 25, 2008	• Added to NMM 2.1 fixes: "NMM 2.1 includes resource vulnerability fix (LGTsc19158)" on page 8 • Added to Known problems and limitations: "Recovery of multiple databases in Recovery Storage Group fails (LGTsc21107)" on page 36
A01	September 26, 2008	First version of this document for new NetWorker® Module for Microsoft Applications 2.1 release.

Product description

The EMC® NetWorker® Module for Microsoft Applications 2.1 (NMM) uses Microsoft VSS technology to provide backup and recovery services for file systems, application data, and operating system data.

The NMM software allows for the creation of a point-in-time snapshot (copy) of data. Instead of backing up data directly from the physical file system, data is backed up from the snapshot. The snapshot includes exact copies of files and all open files. For example, databases and files that are open due to operator or system activity are included in a snapshot. In this way, files changed during the backup process are copied correctly.

Snapshot backups ensure that:

- Applications can continue to write data to the volume during a backup.
- Open files are no longer omitted during a backup.
- Backups can be performed at any time, without locking out users.

The NMM software enables one to manage snapshots on disk to maximize backup and recovery performance.

NMM Features

This section describes briefly the backup and recovery features of the NMM software. The *EMC NetWorker Module for Microsoft Applications Release 2.1 Administration Guide* provides more details about all NMM features.

NMM backups

Backups are configured as scheduled snapshot backups on the NetWorker server. Ad hoc (manual) backups, from either the command line or from the NMM, are not supported at this time. However, one can manually start a scheduled snapshot backup at any time.

The NMM supports three types of snapshot backups:

- Nonpersistent backup (also referred to as a live backup)
- Instant backup with or without rollover
- Serverless backup (also referred to as proxy backup or an off-host backup)

Proxy client support

A proxy client is used to offload the processing requirements associated with serverless backups. Serverless backups free the backup client from much of the processing involved in an instant backup. These backups are particularly useful when there is additional processing involved in a scheduled backup. For example, to determine whether a snapshot of an Exchange database is consistent, the Exchange utility, **eseutil**, must be run against the snapshot. Running **eseutil** can be disk intensive. Therefore, offloading the work from the Exchange server to a proxy client frees resources on the Exchange server.

NMM recoveries

There are three types of recoveries:

- Conventional recovery
- Instant recovery
- Rollback recovery

By default, recoveries are performed from a conventional backup. If a conventional backup is unavailable for the selected browse time, an instant recovery is performed. The default recovery method can be specified in the NetWorker Recovery Options dialog box.

New features and changes

NMM 2.1 provides the following new and expanded features:

Improved NMM performance and scalability

This section describes the features for improved NMM performance and scalability.

Internal use of mount points (LGTpa53035 and LGTsc22818)

This eliminates several drive letter issues where backup mounting may fail because all of the drive letters are used up.

Parallel rollovers of VSS volume snapshots to improve backup performance (LGTsc22529)

Previously, live save set backups to tape were being performed sequentially (one after another), even though the clients were parallel. With the improvements in NMM 2.1 SP1, these backups are now performed in parallel (simultaneously). This provides significant improvements in backup time and performance. All sizes of environments will show performance improvements, but especially so in very large environments.

Reduce NMM memory consumption and CPU utilization when thousands of files are backed up (LGTsc20995)

Some backups of Exchange Server 2007 environments would fail, or take a long time. The save operations in NMM have been improved, reducing Exchange memory consumption and CPU utilization by NMM.

Improve SharePoint optimized backup performance by removal of packaging and unpackaging processes (LGTsc22189)

Previously, whether the backup was optimized or non-optimized, the backups were packaged into a file similar to zip or .cab compression. This packaging is necessary for non-optimized SharePoint backup, but not for optimized SharePoint backup. The packaging and unpackaging processes have been removed from the optimized backup, which reduces backup time and improves performance.

Allow throttling of Exchange consistency checks to improve Exchange server performance (LGTsc23898)

Several command line switches have been added that allow user input to throttle Exchange consistency checks. "Consistency check parameters added to set threading and throttling to handle performance issues (LGTsc26634)" on page 39 lists and describes these switches in detail.

Improve SharePoint Granular Backup Performance (LGTsc22708 and LGTsc23647)

Using new NMM 2.1 SP1 custom algorithms, instead of Microsoft SharePoint APIs, the total backup window for granular backups of large sites is significantly reduced. For example, under the old method a large 10GB site, with 50,000 objects took approximately 16 hours for backup. Using the new NMM backup algorithms, the backup time was reduced to 1.5 hours.

Additional NMM 2.1 SP1 features and improvements

This section describes the additional NMM 2.1 SP1 features and improvements.

NetWorker support for Linux

NMM 2.1 SP1 has been tested and qualified to work with NetWorker Server and NetWorker Storage Node, running NetWorker 7.4 SP3 or later on Linux.

Additional documentation of disaster recovery procedures

"Disaster recovery procedures" on page 9 supplements the disaster recovery procedures in the *EMC Module for Microsoft Applications Release 2.1 Administration Guide* with procedures for the following disaster recovery scenarios:

- "Microsoft Exchange Server 2007 (standalone) disaster recovery" on page 10
- "Microsoft Exchange Server 2007 disaster recovery for Exchange CCR to a 2 node cluster in a production environment" on page 12
- "Microsoft Exchange Server 2007 disaster recovery for Exchange CCR in a production environment" on page 14
- "Microsoft SQL Server 2005 (standalone) disaster recovery on Windows Server 2008" on page 16
- "Microsoft SQL Server 2005 (standalone) disaster recovery on Windows Server 2003" on page 17
- "Windows Server 2008 Active Directory disaster recovery" on page 21
- "Microsoft SQL Server 2005 cluster disaster recovery on Windows Server 2003" on page 20
- "Windows Server 2008 Active Directory disaster recovery" on page 21

Previous release new features and changes

NMM 2.1 provides new and expanded support for the following Microsoft applications and features:

I18N Support:

- NMM supports non-English characters to the extent that they are supported in the programs NMM protects: Microsoft Exchange Server, Microsoft SQL Server, Microsoft Office SharePoint Server, Microsoft DPM, EMC NetWorker, and the Microsoft Windows operating systems.

GUID Partition Table disks:

- No disk size limit on Windows environments with CLARiiON storage (SnapView clone, SnapView snap, and SAN Copy technologies only)
- Disk size limit of less than 2 TB on Windows environments with Symmetrix storage

Directed Recovery

Application Support:

- Windows Server 2008 Hyper-V Host and In-Guest backup and recovery
- Microsoft Data Protection Manager granular recovery and disaster recovery

- Microsoft SharePoint 2003
- Microsoft SharePoint 2007 granular backup and recovery
- Microsoft Exchange Server 2007 recovery to Recovery Storage Group

NMM 2.0 succeeds EMC NetWorker VSS Client for Windows Server 2003 7.3, First Edition.

NMM 2.0 features new and expanded support for many Microsoft applications, including:

New Operating System Support:

- Support for Windows Server 2008 x86/x64
- Support for Windows Server 2003 x64
- Support for Windows Dynamic Disks

New Application Support:

- Microsoft Exchange Server 2007 x64
  - Exchange Server 2007 Cluster Continuous Replication (CCR) Secondary Node Backups
  - Exchange Server 2007 Local Continuous Replication (LCR) Compatible
- Microsoft Office SharePoint Server 2007
  - Disaster Recovery for standalone and distributed farms
- Microsoft System Center Data Protection Manager 2007
  - Protection of DPM Server and DPM Protected Server Replicas

New NetWorker Support:

- Support for AES Encryption

New VSS Hardware Provider Support:

- EMS Celerra with Celerra VSS Hardware Provider
- qualLogic PS Series Arrays with EqualLogic Integration Toolkit

Expanded VSS writer support for Microsoft SQL Server 2005

Fixed problems

This section describes additional fixes in current and previous releases.

Note: The most up-to-date product issues for *EMC NetWorker Module for Microsoft Applications* are detailed online in the EMC Issue Tracker available on the EMC Powerlink website: http://Powerlink.EMC.com.

Client security vulnerability hotfix 5.2.0.1 in NMM 2.1 SP1 build 165 (LGTsc30291)

This hotfix contains the solution for issue LGTsc30291: Security Fix for RMAPI Service, ZDI-CAN-451, ESA-09-010.

To access this hotfix from the EMC Support website:

1. Go to http://Powerlink.EMC.com.
2. Select **Support** > **Software Downloads and Licensing** > **Downloads J-O** > **NetWorker Module**.
3. In the table of **NetWorker Module Software Downloads**, click the **NetWorker Module for Microsoft Applications Release 2.1 SP1**.

   The NMM SP1 build now available on Powerlink is 165 and includes the fix for the client security vulnerability. The previous build of NMM 2.1 SP1 has been replaced by build 165.

   Build 165 is available as a zipped file and the contents must be extracted.

IMPORTANT

All previous installations of NMM must be uninstalled before NMM 2.1 SP1 build 165 is installed.

To install the hotfix, follow the installation instructions provided in *EMC Module for Microsoft Applications Release 2.1 Installation Guide*.

To access notes and articles about this hotfix:

1. Go to http://Powerlink.EMC.com.
2. On the **Support** menu, select **Search Support.**
3. Type **emc219663** in the search field, and click **Search**.
4. Select the **ESA-09-010: EMC Replication Manager Remote Code Execution vulnerability** link to learn more about the issue impacting NMM 2.1.

In addition to resolving issue LGTsc30291, this hotfix also contains the following fixes that were resolved in NMM 2.2:

- Microsoft Office SharePoint Server: Recovery of custom permission level fails (LGTsc27822)
- Microsoft Office SharePoint Server: NMM SharePoint granular backup fails when parent site is larger in size than the staging space (LGTsc27321)
- Backup of Exchange 2007 Single Copy Cluster (SCC) using NMM fails (LGTsc22388)
- NMM breaks when using a backup NIC (LGTsc29075)
- NMM Exchange CCR Active Directory backup fails (LGTsc30109)

NMM 2.1 hotfixes in build 143

Table 2 on page 8 provides a list of bug fixes included in build 143.

Table 2 Fixed problems in NMM 2.1 Build 143

Number	Description
LGTsc20936	Active Directory only recovers objects 1 level deep.
LGTsc21805	Data Protection Manager: Recover fails to skip replicas not in the "Allocated" state
LGTsc22189	SharePoint Performance: Backup fails when backing up 10GB site
LGTsc20995	Exchange backup: NMM fails to create snapshot of Exchange Server 2007 cluster on Windows Server 2008
LGTsc22032	Exchange rollback fails with nsr_snap_recover.exe crash

IMPORTANT

The bug fixes present in build 143 are now included in build 165. "Client security vulnerability hotfix 5.2.0.1 in NMM 2.1 SP1 build 165 (LGTsc30291)" on page 7 provides details about build 165.

NMM 2.1 fixes

This section provides details about the NMM 2.1 fixes.

NMM 2.1 includes resource vulnerability fix (LGTsc19158)

The initial release of NMM 2.1 includes a fix for a resource exhaustion vulnerability in Networker's nsrexecd.exe process. The vulnerability could be exposed through the usage of a crafted request through a TCP connection to the nsrexecd process, which then consumes all available system memory, resulting in a denial of service. The vulnerability has been eliminated by ensuring that the length of the RPC request is validated. This issue does not affect the integrity or confidentiality of the data.

EMC strongly recommends downloading NMM 2.1, available through Powerlink® at **Home > Support > Software Downloads and Licensing > Downloads J-O > NetWorker Module**. More details on the security vulnerability can be found in the knowledge base article **esg99768**, available at http://Powerlink.EMC.com.

Additional steps required for configuring SharePoint 2007 backups (LGTsc15836)

The additional steps have been added to the *EMC Module for Microsoft Applications Release 2.1 Administration Guide*.

SharePoint recovery of Configuration database requires restore of all Content Databases (LGTsc15837)

The additional information has been added to the *EMC Module for Microsoft Applications Release 2.1 Administration Guide* in the section "Performing SharePoint 2007 recovery".

Previous fixes in NMM 2.0 QuickFix releases with build numbers of 183 or higher

This section describes the fixes in NMM 2.0 QuickFix releases.

Security fix for RPC vulnerability (LGTsc14258)

Installing this NMM hotfix resolves a previously discovered RPC security vulnerability.

Fix to recover Windows Server 2008 Hive Registry database correctly (LGTsc15312)

NetWorker System State restores on Windows Server 2008 did not correctly recover the Hive Registry database. This issue has been fixed, and the Windows Server 2008 Hive Registry is recovered correctly in a full system recovery.

Environment and system requirements

The *EMC NetWorker Module for Microsoft Applications Release 2.1 Installation Guide* lists hardware and software requirements for the NMM software.

Note: NetWorker Module for Microsoft SQL Server (NMSQL) 5.1 SP1x64 installation does not recognize that NetWorker Module for Microsoft Applications is installed (LGTsc15511). If installing both modules on a Windows Server 2003 x64, contact EMC Customer Support for NMSQL 5.1 SP1 266_QuickFix to enable the modules to run together. This issue does not apply to NMSQL 5.2.

Disaster recovery procedures

The *EMC Module for Microsoft Applications Release 2.1 Administration Guide* provides documentation of disaster recovery for the following Microsoft applications and operating system features:

- Microsoft Hyper-V parent partition
- Microsoft Data Protection Manager
- Microsoft SharePoint Server 2007
- Microsoft Windows Server 2003 Active Directory
- Microsoft Windows Server 2003 Cluster
- Microsoft Window Server 2008 Cluster authoritative and nonauthoritative restore

This release note includes procedures for the following disaster recovery scenarios:

- "Microsoft Exchange Server 2007 (standalone) disaster recovery" on page 10
- "Microsoft Exchange Server 2007 disaster recovery for Exchange CCR to a 2 node cluster in a production environment" on page 12
- "Microsoft Exchange Server 2007 disaster recovery for Exchange CCR in a production environment" on page 14
- "Microsoft SQL Server 2005 (standalone) disaster recovery on Windows Server 2008" on page 16

- "Microsoft SQL Server 2005 (standalone) disaster recovery on Windows Server 2003" on page 17
- "Windows Server 2008 Active Directory disaster recovery" on page 21
- "Microsoft SQL Server 2005 cluster disaster recovery on Windows Server 2003" on page 20
- "Windows Server 2008 Active Directory disaster recovery" on page 21

Microsoft Exchange Server 2007 (standalone) disaster recovery

The process for performing this disaster recovery follows these steps:

1. The Exchange data must have already been backed up with the save set Applications:\Microsoft Exchange 2007.
2. Rebuild the Exchange Server hardware, following the instructions provided by Microsoft.
3. After the Exchange Server is rebuilt, make sure with the name, account information, and configuration, and other information is the same as the old server that is being replaced.
4. Reinstall NMM.
5. In NMM, perform an Exchange Server point-in-time recovery.

The following procedure describes the process in more detail.

To perform a disaster recovery of a standalone installation of Microsoft Exchange Server 2007:

1. Back up all Exchange data with the save set

   Applications:\Microsoft Exchange 2007
2. Build new machine hardware for an Exchange Server, following Microsoft's instructions on TechNet:

   "Moving Exchange Servers to New Hardware and Keeping the Same Server Name"

   http://technet.microsoft.com/en-us/library/bb332343.aspx
3. Capture all of your manually set Internet Information Services (IIS) virtual directory configurations. Run the following Exchange Management Shell command:

   ```
   Get-OwaVirtualDirectory "owa (default web site)" | export-clixml
   Owa.xml - depth
   ```
4. Copy the Owa.xml file to a location that can be accessed by the new server after it is available and the old server is shut down.
5. Shut down the existing Exchange 2007 Server. (The backup should have already been taken, at step 1 of this procedure.
6. Reset the computer account for the existing Exchange 2007 server.
7. Bring the new computer online, and then confirm that the new computer is running the same operating system that was installed on the existing Exchange 2007 server.

8. Rename the new server to the same name as the original server that you are replacing, and then join this computer to the domain.
9. For drives that contained Exchange 2007 data, configure drive letters on the new server to map to or match the configuration of the old server.
10. Verify that the drives have sufficient space to accommodate the restored data.
11. Run Exchange Server 2007 Setup with the following parameter:

    ```
    Setup.com /M:RecoverServer
    ```

12. Reboot the machine.
13. Restore your manually set IIS virtual directory configurations, by running the following Exchange Management Shell script:

    ```
    Restorevdir.ps1 Owa.xml
    ```

    The Microsoft Exchange Server should come online with all previous storage groups.
14. Install NMM.

    The *EMC Module for Microsoft Applications Release 2.1 Installation Guide* provides instructions for installing NMM, including Exchange Server-specific configuration settings.
15. In NMM, perform an Exchange Server point-in-time recovery.

    These recovery steps are provided in detail in the "Microsoft Exchange Server Backup and Recovery" chapter of the *EMC Module for Microsoft Applications Release 2.1 Administration Guide.*

Microsoft Exchange Server 2007 disaster recovery for Exchange CCR to a 2 node cluster in a production environment

Prior to disaster recovery, use NMM to perform regular backups of volumes, System Components, and application save sets.

The following save sets should be backed up regularly:

1. Back up the following with the snapshot policy “all.”

   C:

   System Components:

   The backup of C:\ automatically includes the following:

   - Windows Boot Volume
   - Windows System Volume
   - Application software.

   Note: If the system has been set up with a separate file system for the Windows boot\system partition and separate file system for application installation, then along with C:\ drive, back up the file system that includes the Windows Boot Volume, Windows System Volume, and application software.

   The *NetWorker Module for Microsoft Applications Administration Guide* provides more information about configuring snapshot policies for SYSTEM COMPONENTS backup.

2. Back up application data for Exchange CCR on the NetWorker server on the passive node using the following save set with snapshot policy "all."

   Applications:\Microsoft Exchange 2007

The steps in this disaster recovery scenario are based on the following host details for the production environment you are recovering, and the isolated environment you are recovery to.

Production environment setup:

- Domain Controller, 1 physical machine
- CCR setup with an active node and a passive node, 2 physical machines

Isolated environment setup:

- Domain Controller setup with the same hardware and software configuration as the production environment
- CCR setup with only a passive node, 1 physical machine

To perform a disaster recovery of Microsoft Exchange Server 2007 to a 2 node cluster in a CCR environment:

1. Configure an AD domain setup in an isolated environment, using the same operating system version, machine IP and machine name as the production Active Directory Domain setup.

   Note: There should not be any communication between the production environment and the isolated environment.

2. Configure the AD domain on the isolated environment with the same domain name as the production AD domain name.

   Make sure that both environments use the same make and model of hardware.

3. Install all Windows updates, and applications such as Exchange, in the isolated environment AD domain setup, to match the production Active Directory Domain setup.

4. Disconnect the NetWorker server from the production environment, and connect the NetWorker server to the isolated environment.

   Note: In this scenario, the backup was taken on the file system, not on tape. Since the backup is not on tape, to move the backup to the isolated environment you must connect isolated environment to the NetWorker server which is storing the backup.

5. Install NMM on the isolated environment AD domain machine.

6. Restart the machine in "Directory Service Restore Mode" and start recovery of C:\ and System Components:\ using NMM recovery.

   Note: Make sure that "legato" and "RMagentPS" folders are not selected before starting C:\ recovery.

7. When recovery completes, you will be prompted to restart the machine. Restart the machine.

   This recovers all production AD domain objects into the isolated AD domain. This also recovers all application information.

8. On the isolated environment AD domain setup, reset the computer account for the existing Exchange Virtual Server, or Clustered Mailbox Server (CMS), or virtual Exchange Server.

9. Rebuild another standalone server in the isolated environment with the same operation systemversion as the production CCR setup.

10. Provide this new machine with a new IP address and new Network name, and bring it online in the isolated environment.

11. Install all roles required for Exchange setup to run.

12. Create the same drive letters and paths for Storage Groups (SG) and databases as the production CCR SGs and databases.

13. Install the cluster feature and configure a new cluster with Quorum.

    Note: The Majority Node Set (MNS)/Quorum shared folder must be different from the old.

14. Run Exchange setup in “Custom” mode, and only install the Passive Cluster Role.

15. Run the following command, using the CMS name and IP address from the Production CCR server:

    Setup.com /recoverCMS /CMSName:<name> /CMSIPaddress:<ip>

    This puts the production virtual server online on this new node.

Note: All Storage Groups which were created in the CCR are recreated in this installation. Verify that all drive letters and paths for Storage Groups and databases are recreated the same as those in the production CCR server.

16. All databases will be in dismounted state, which is required for recovery from NMM.
17. Install NMM on the new CCR machine.
18. Browse through Production CCR EVS index and perform PIT recovery of Exchange.
19. Install Microsoft Exchange on the new CCR machine. Run Exchange setup in Custom mode and install only the Passive Cluster Role.
20. Reseed the passive cluster node to get it in sync with the active node.

Microsoft Exchange Server 2007 disaster recovery for Exchange CCR in a production environment

Prior to disaster recovery, use NMM to perform regular backups of volumes, System Components, and application save sets.

The following save sets should be backed up regularly:

1. Back up the following with the snapshot policy “all.”

   C:

   System Components:

   The backup of C:\ automatically includes the following:

   - Windows Boot Volume
   - Windows System Volume
   - Application software.

   Note: If the system has been set up with a separate file system for the Windows boot\system partition and separate file system for application installation, then along with C:\ drive, back up the file system that includes the Windows Boot Volume, Windows System Volume, and application software.

   The *NetWorker Module for Microsoft Applications Administration Guide* provides more information about configuring snapshot policies for SYSTEM COMPONENTS backup.

2. Back up application data for Exchange CCR on the NetWorker server on the passive node using the following save set with snapshot policy "all."

   Applications:\Microsoft Exchange 2007

The steps in this disaster recovery scenario are based on the following host details for the production environment you are recovering, and the production environment you are recovery to.

Production environment setup:

- Domain Controller, 1 physical machine
- CCR setup with an active node and a passive node, 2 physical machines

Recovery site setup (in the same network as the production setups):

- Domain Controller setup with the same hardware and software configuration as the production environment
- CCR setup with only a passive node, 1 physical machine

In this disaster recovery procedure, the machines are referred to as follows:

Production:

- MC1:Domain controller
- CL1:cluster node 1
- CL2:Cluster node 2

R**ecovery site (in the same network as the production setups):**

- CL11:cluster node 1
- CL21: cluster node 2

To perform a Microsoft Exchange Server 2007 CCR disaster recovery in production to a 2 node cluster:

1. Shut down the Exchange CCR setup.Shutdown both CCR nodes, assuming the Exchange Cluster is lost or crashed.
2. Reset the computer account for the existing Exchange Virtual Server, or Clustered Mailbox Server (CMS), or virtual Exchange Server.
3. Reset the computer account for CL1 and CL2 if you want the base cluster names to be the same as those in original production setup.
4. Rebuild 2 machines CL21 and CL11 with the same operating system version as the old server.
5. Assign the new machine with a new IP address and new Network name, and bring it online in the same domain.

   --or--

   If you want the same IP address and Network name as the production machine, assign the same IP and name.
6. Install all roles required for Exchange setup to run on both CL11 and CL21.
7. Install cluster feature and create a new cluster with Quorum

   Note: The Majority Node Set (MNS)/Quorum shared folder must be different from the old.
8. Make sure the host has all of the drive letters created as those that were on the original Exchange server.
9. Run Exchange setup in Custom mode and install only Passive Cluster Role on CL11.
10. Run the following command, using the CMS name and IP address from the old CCR server:

    Setup.com /recoverCMS /CMSName:<name> /CMSIPaddress:<ip>

When this command is run:

- It puts the old virtual server online on this new node.
- All Storage Groups which were created in CCR are recreated in this installation.
- All databases will be in a dismounted state, which is required to recover from NMM.

11. Install NMM.
12. Browse through OLD CCR EVS index and perform PIT recovery of Exchange.
13. On CL211, install Exchange passive node. Run Exchange setup in custom mode and install only the Passive Cluster Role.

Microsoft SQL Server 2005 (standalone) disaster recovery on Windows Server 2008

Prior to disaster recovery, use NMM to perform regular backups of volumes, System Components, and application save sets.

The following save sets should be backed up regularly:

1. Back up the following with the snapshot policy "all."

   C:

   System Components:

   The backup of C:\ automatically includes the following:

   - Windows Boot Volume
   - Windows System Volume

   Note: If the system has been set up with a separate file system for the Windows boot\system partition and separate file system for application installation, then along with C:\ drive, back up the file system that includes the Windows Boot Volume, Windows System Volume, and application software.

   The *NetWorker Module for Microsoft Applications Administration Guide* provides more information about configuring snapshot policies for SYSTEM COMPONENTS backup.

2. Back up application data for Microsoft SQL Server 2005 with the following save set:

   Applications:\SqlServerWriter

To perform a disaster recovery of Microsoft SQL Server 2005 on a Windows Server 2008 machine:

1. Install Microsoft SQL Server 2005 and SP2, including the SQL Server Instances which were running on the machine before the disaster.

   Note: The Instance names must be exactly the same as the previous ones.

2. Perform a recover of the System Components and volumes.

3. After restore of System Components, enter the following command at the command line:

   ```
   >bcdedit /export c:\Boot\savebcd.txt
   ```

4. Reboot the machine.

5. Enter the following command at the command line:

   ```
   >bcdedit /import c:\Boot\savebcd.txt
   ```

6. Verify that the import was successful by entering the following command:

   ```
   >bcdedit /store c:\boot\bcd
   ```

   This will display the changed file. It should NOT show the values below:

   ```
   Windows Boot Manager
   --------------------
   device            unknown

   Windows Boot Loader
   -------------------
   device          unknown
   osdevice        unknown
   resumeobject     GUID THAT DOESN'T MATCH THE TARGET SYSTEM
   ```

7. Perform a recovery of the SQL Server 2005 data for all previous instances.

   Note: In the NMM GUI, make sure to clear the checkmarks for all of the system databases, or the recovery will fail.

Microsoft SQL Server 2005 (standalone) disaster recovery on Windows Server 2003

Prior to disaster recovery, use NMM to perform regular backups of volumes, System Components, and application save sets.

The following save sets should be backed up regularly:

1. Back up the following with the snapshot policy "all."

   C:

   System Components:

   The backup of C:\ automatically includes the following:

   - Windows Boot Volume
   - Windows System Volume

   Note: If the system has been set up with a separate file system for the Windows boot\system partition and separate file system for application installation, then along with C:\ drive, back up the file system that includes the Windows Boot Volume, Windows System Volume, and application software.

   The *NetWorker Module for Microsoft Applications Administration Guide* provides more information about configuring snapshot policies for SYSTEM COMPONENTS backup.

2. Back up application data for Microsoft SQL Server 2005 with the following save set:

   Applications:\SqlServerWriter

To perform a Microsoft SQL Server 2005 (standalone) disaster recovery on Windows Server 2003:

1. Set up a Windows 2003 new machine, to match the machine name, IP address, and domain status of the old machine.
2. Recover SYSTEM COMPONENTS:\ and the local file system volumes.
3. Reboot the machine.
4. Sign into the machine as local administrator, unjoin the domain, and then rejoin the domain.
5. Recover the APPLICATIONS:\SqlServerWriter save set.
6. Reboot, and then recovery will be complete.

Microsoft SQL Server 2005 cluster disaster recovery on Windows Server 2008

Prior to disaster recovery, use NMM to perform regular backups of volumes, System Components, and application save sets.

The SQL Server cluster should be backed up regularly, the following will be required when a disaster recovery occurs:

1. Back up the following on both Cluster nodes. Use the snapshot policy "all" for each node backup:

   C:

   System Components:

   The backup of C:\ automatically includes the following:

   - Windows Boot Volume
   - Windows System Volume

   Note: If the system has been set up with a separate file system for the Windows boot\system partition and separate file system for application installation, then along with C:\ drive, back up the file system that includes the Windows Boot Volume, Windows System Volume, and application software.

2. Back up application data for Microsoft SQL Server 2005 with the following save set:

   Applications:\SqlServerWriter

   Note: You must specify a separate Applications save set for each SQL Cluster instance.

To perform a Microsoft SQL Server 2005 cluster disaster recovery on Windows Server 2008:

1. Set up each new cluster machine to match the machine name, IP address, and domain status of the corresponding old machine.
2. On each cluster machine, install Microsoft SQL Server 2005 and all updates that were installed on the old machines, and all Instances that were installed on the old machines.
3. Recover each node's SYSTEM COMPONENTS:\ and local file system volumes.
4. Reboot each new machine.
5. On each machine, sign into the machine as local administrator, unjoin the domain, and then rejoin the domain.
6. After restore of System Components, enter the following command at the command line:

   >bcdedit /export c:\Boot\savebcd.txt

7. Reboot the machine.
8. Enter the following command at the command line:

   >bcdedit /import c:\Boot\savebcd.txt

9. Verify that the import was successful by entering the following command:

   >bcdedit /store c:\boot\bcd

   This will display the changed file. It should NOT show the values below:

```
Windows Boot Manager
--------------------
device            unknown

Windows Boot Loader
-------------------
device          unknown
osdevice        unknown
resumeobject     GUID THAT DOESN'T MATCH THE TARGET SYSTEM
```

10. On the active node:
    a. Stop SQL Instance Services
    b. Restore APPLICATIONS:\SQLServerWriter
    c. Start SQL Instance Services.

Microsoft SQL Server 2005 cluster disaster recovery on Windows Server 2003

Prior to disaster recovery, use NMM to perform regular backups of volumes, System Components, and application save sets.

The SQL Server cluster should be backed up regularly, the following will be required when a disaster recovery occurs:

1. Back up the following on both Cluster nodes. Use the snapshot policy "all" for each node backup:

   C:

   System Components:

   The backup of C:\ automatically includes the following:

   - Windows Boot Volume
   - Windows System Volume

   Note: If the system has been set up with a separate file system for the Windows boot\system partition and separate file system for application installation, then along with C:\ drive, back up the file system that includes the Windows Boot Volume, Windows System Volume, and application software.

2. Back up Cluster Management.
3. Back up application data for Microsoft SQL Server 2005 with the following save set:

   Applications:\SqlServerWriter

   Note: You must specify a separate Applications save set for each SQL Cluster instance.

To perform a Microsoft SQL Server 2005 2 node cluster disaster recovery on Windows Server 2003:

1. Set up each new cluster machine to match the machine name, IP address, and domain status of the corresponding old machine.
2. Recover each node's SYSTEM COMPONENTS:\ and local file system volumes.
3. Reboot each new machine.
4. On each machine, sign into the machine as local administrator, unjoin the domain, and then rejoin the domain.
5. On each machine, recover the APPLICATIONS:\SqlServerWriter save set.
6. Reboot each machine.

   Cluster status recovery is complete.

Windows Server 2008 Active Directory disaster recovery

Prior to disaster recovery, use NMM to perform regular backups of volumes, System Components, and application save sets.

The following save sets should be backed up regularly:

1. Back up the following with the snapshot policy "all."

   C:

   System Components:

   The backup of C:\ automatically includes the following:

   - Windows Boot Volume
   - Windows System Volume
   - Application software.

   Note: If the system has been set up with a separate file system for the Windows boot\system partition and separate file system for application installation, then along with C:\ drive, back up the file system that includes the Windows Boot Volume, Windows System Volume, and application software.

2. Back up the domain controller on the Active Directory machine.

   The *NetWorker Module for Microsoft Applications Administration Guide* provides more information about configuring snapshot policies for SYSTEM COMPONENTS backup.

In the following procedure, Machine A is the current Active Directory machine, the system that requires a disaster recovery. Machine B is the new machine set up to replace Machine A. The disaster recovery will restore the Active Directory to the new machine, Machine A.

To perform a disaster recovery of Active Directory on Windows Server 2008:

1. Back up the domain controller on Machine A. Do this regularly along with backing up the machine in general, *long before you actually need to perform a disaster recovery.*
2. Shut down Machine A.
3. Install w2k8 on Machine B.
4. Name Machine B the same as Machine A, and use the same IP address as Machine A.
5. Install NMM and update the hosts file.

   For Active Directory applications, install the AD role before proceeding with the disaster recovery

6. Boot Machine B into DSRM.
7. Locate your 'Boot\bcd' file. This file is usually found on the C: or System drive.
8. In a Command window, navigate to the location of the Boot\bcd file.

9. Run the following command:

   ```
   C:\windows\system32\bcdedit /export  exportBCD.txt
   ```

   This saves the Boot Configuration Data to the file exportBCD.txt.

   The following message is displayed if the command completes successfully:

   "The operation completed successfully."

10. Move the exportBCD.txt file to a known temporary location you will be able to access after the restore.
11. Perform the NMM System Components restore. If the restore is successful reboot.
12. Perform the File System restore.
13. When the restore successfully completes, locate the saved exportBCD.txt file and move it back to the \Boot directory.
14. In a command window, navigate the folder path to the \Boot directory and run the following command:

    ```
    C:\windows\system32\bcdedit /import  exportBCD.txt
    ```

15. Run the following command to display the contents of the Boot Configuration Data:

    ```
    C:\windows\system32\bcdedit /store C:\Boot\bcd
    ```

    The contents should look like the output below. Verify that the lines in bold have a volume letter and do not say **unknown**. These steps are only required with the first reboot.

    ```
    Windows Boot Manager
    --------------------
    identifier              {bootmgr}
    device                  partition=C:
    description           Windows Boot Manager
    locale                   en-US
    inherit                  {globalsettings}
    default                 {default}
    displayorder         {default}
    toolsdisplayorder {memdiag}
    timeout                 30
    Windows Boot Loader
    -------------------
    identifier              {default}
    device                  partition=C:
    path                     \Windows\system32\winload.exe
    description           Microsoft Windows Server 2008
    locale                    en-US
    inherit                 {bootloadersettings}
    osdevice              partition=C:
    systemroot           \Windows
    resumeobject       {99d5f867-cab4-11dd-9306-d52aac68c2b6}
    nx                         OptOut
    ```

14. Reboot. The machine should boot normally.

Known problems and limitations

This section describes known problems and limitations for this release:

Unsupported NetWorker features

The following NetWorker features are not supported:

- NetWorker Clone, Staging and Archive.
- Localization (L10N).
- Installation of dedicated Storage Node on NMM client host. NMM does support proxy storage node. The *EMC NetWorker Module for Microsoft Applications Release 2.1 Administration Guide* provides more information.
- Adhoc/Manual Backups.
- De-duplication.

Unsupported Windows features

The following Windows Server versions are not supported:

- Windows Server 2008 Core installation
- Windows IA64 editions.

The following Windows features are not supported:

- BitLocker encryption.
- LAN-based Proxy Client or LAN-free backups, if dynamic disks are used.
- EMC VSS Provider for Celerra with Windows Server 2008.
- VSS Hardware Providers with Windows dynamic disks.
- Microsoft Software Shadow Copy provider to perform persistent snapshots of clustered disks.
- Windows Automated System Recovery (ASR).
- Windows Storage Server Single Instance Storage (SIS) is supported, but recoveries will recover file data for all duplicate file—data will not be lost if there is sufficient disk space to hold the duplicate copies.

The *EMC Information Protection Software Compatibility Guide* contains additional and the most up-to-date information about NMM compatibility.

Latest VSS patches and hotfixes from Microsoft are required (LGTsc27378)

There are several known issues with VSS on Microsoft Windows Server 2003 that may lead to snapshot or backup errors. The following Microsoft Hotfix kits are required for NMM to work correctly:

- KB940349 Availability of a Volume Shadow Copy Service (VSS) update rollup package for Windows Server 2003 to resolve some VSS snapshot issues
- KB951568 VSS-based backup operations may fail if VSS tracing is enabled on a Windows Server 2003-based computer that has hotfix 940349 applied
- KB949391 When Volume Shadow Copy Service (VSS) tries to delete hardware support snapshots on a computer that is running Windows Server 2003 or an x64 version of Windows XP, the operation may fail
- KB943545 Error returned by the IOCTL_SCSI_GET_INQUIRY_DATA operation on a Windows Server 2003-based computer: "STATUS_INVALID_DEVICE_REQUEST"

These fixes can be downloaded from the Microsoft web site.

NetWorker Server

This section describes the known problems and limitations in NetWorker Server.

NO_SUPPRESS option can cause backup operations to report failures (LGTsc13731)

In the NetWorker software release 7.3.x and later, savegroup does not support the NO_SUPPRESS option. This means there will be no extra output obtained in the messages file if you create the NO_SUPPRESS file in\nsr\debug and in \nsr\tmp. In NMM this can also cause backup operations to report failures.

Workaround

Do not use the NO_SUPPRESS option.

Microsoft Windows Server and clustering

This section describes the known problems and limitations in Microsoft Windows Server and clustering.

Active Directory attribute value for msNPAllowDialin not recovered under Windows Server 2003 SP1 (LGTpa95417)

For NMM clients running Windows Server 2003 SP1, the value for the Active Directory attribute **msNPAllowDialin** is unrecoverable. NMMs that run Windows Server 2003 R2 are unaffected.

Workaround

After recovering Active Directory, update the value for the **msNPAllowDialin** attribute if necessary. To edit this attribute use a Microsoft tool such as ADSI Edit, which is available by installing the Windows Server 2003 family Support Tools from the Windows Server 2003 family CD.

Snapshot cannot include both hardware and software snapshot volumes for clustered NetWorker VSS clients (LGTsc05386)

A NetWorker VSS client resource running on a cluster cannot include both hardware and software volumes in the same save set. Additionally, save set **All** cannot be specified for such a client resource. If both hardware and software volumes are included in a save set, the backup will fail.

Workaround

If a NMM client on a cluster has both hardware and software volumes, create at least two client resources: one for hardware volumes and one for software volumes. Additionally, do not specify save set **All** in any of the client resources for the NMM client. When using a hardware provider with a NMM client, you must configure a proxy client and the snapshot volume must be exported to a proxy outside of the cluster.

NPS Writer fails if not configured properly on Windows Server 2008 (LGTsc13843)

If Network Policy and Access Services (NPS) Role is installed, but is not configured properly, will not create the file "c:\windows\system32\ias\ias.xml," which is in the NPS Writer file list.

Workaround

Run NPS configuration, which will create "c:\windows\system32\ias\ias.xml." Or, do not use NPS.

Failed Cluster Database recovery of legacy VSS backups may fail without displaying error message (LGTsc06190)

The NMM client can recover legacy VSS backups of the cluster database (VSS SYSTEM SERVICES) created prior to the upgrade to or installation of the NMM client. The Cluster Writer Service files may be successfully recovered, but the cluster database recovery may fail without displaying a recovery failure message.

Workaround

When recovering the cluster database, make sure that the cluster is not running on the other node.

Backup of Windows Server 2008 with proxy host fails (LGTsc11828)

If a Windows Server 2003 system is used as the proxy mount host for Windows Server 2008 production host, backup will fail.

Recovery failure after .NET 3.5 framework installation (LGTsc19814)

Volume and SYSTEM COMPONENTS restore fails if the system previously had .NET Framework 3.5 installed, and the OS was reinstalled but the .NET Framework 3.5 was not re-installed before attempting recovery. When recovery fails, an error is displayed: "The directory is not empty..."

Workaround

To restore the Volume and SYSTEM COMPONENTS on a system that previously had .NET Framework 3.5 installed at the time of the backup:

1. Reinstall the operating system.
2. Reinstall .NET Framework 3.5.
3. Install NMM.
4. Recover the volume and SYSTEM COMPONENTS.

Groups left offline after failure of Windows Server 2008 Cluster Writer authoritative restore (LGTsc14540)

At the start of an authoritative restore of the Windows Server 2008 Cluster Writer, NMM sets the cluster group offline. If the authoritative restore happens to fail, the recovery will leave the groups offline.

Workaround

Perform both of the following actions:

- Manually restart the cluster services.
- Manually restart all of the cluster groups.

SYSTEM COMPONENTS failure after McAfee uninstall (LGTsc18766)

If a program does not uninstall cleanly, some program files may still remain after uninstallation. This may cause SYSTEM COMPONENTS:\ backups to fail. This has been known to occur with McAfee VirusScan 8.5i, but may occur with other programs.

Workaround

Microsoft has identified this as an issue with the VSS System Writer. Microsoft Support KB article 955078 describes this issue and provides several solutions.

Installation of Microsoft Windows Server 2008 does not grant correct permissions to nsr\tmp directory (LGTsc15258)

During installation of the NMM client on Windows Server 2008, the networker_install_dir\tmp directory does not have the correct permissions. The Administrator account needs write permissions to this directory.

Workaround

Manually change the permissions to the *networker_install_dir*\tmp directory:

1. In **Windows Explorer**, right-click on the *networker_install_dir*\tmp directory and select **Properties**.
2. Select the **Security** tab.
3. Temporarily change the ownership to the Administrators group.
4. Grant Read/Write permissions to the Administrators group.
5. Change the ownership back to the system.

Note: The most up-to-date product issues for *EMC NetWorker Module for Microsoft Applications* are detailed online in the EMC Issue Tracker available on the EMC Powerlink website: http://Powerlink.EMC.com.

Windows Server 2008 COM+ Registry database is not recovered correctly (LGTsc15380)

NetWorker System State restores on Windows Server 2008 do not correctly recover the COM+ Registry database. There is a workaround that enables you to do a full system recovery.

Workaround

1. Log on to the system as a local system administrator.
2. Open a command window:

   Click **Start**, click **Run**, type **cmd**, and then press **Enter**.
3. Change the working directory to the COM+ catalog files folder:

   cd %windir%\registration
4. Delete all the COM+ catalog files that are not in use, except for the R000000000001.clb file. The following command will prompt you to confirm the deletion of each file; select N for the R000000000001.clb file if it exists.

   del /p *.clb

Application and NMM upgrades may need to be reinstalled after System Writer recovery (LGTsc15889)

When recovering an older backup of the System Writer in Windows Server 2008, any application or NMM upgrades, service packs, or hot fixes that were installed since the backup may need to be reinstalled after the recovery.

NMM client does not support the NetWorker pathownerignore cluster functionality (LGTsc15116)

The pathownerignore cluster functionality is not supported in NMM. This restriction is not enforced by NMM code. In some circumstances the path owner may be ignored by NMM so that the data from a clustered disk is backed up under the indices of the physical node. But recovers of that data will fail.

Clustered disks must be backed up under a virtual cluster client (which is configured with an IP address). The *EMC Module for Microsoft Applications Release 2.1 Administration Guide* provides more information about backing up a clustered NMM client.

Workaround

Do not attempt to use the pathownerignore functionality. Ensure that a nsr\bin\pathownerignore file does not exist.

FRS writer fails to recover during Windows Server 2008 AD disaster recovery (LGTsc25314)

When performing a disaster recovery of a domain controller to a new machine, the FRS writer fails to recover.

Use of the newsid.exe utility is not supported. This utility is not supported if it is used originally to create the source machine. It is not supported if it is used to subsequently create the target machine.

Disaster recovery fails for Dell 2850 running Windows Server 2008 (LGTsc26386)

Disaster recovery will fail when a Dell 2850 running Windows Server 2008 is recovered to an alternate machine of the same type. According to the manufacturer's web site, the Dell 2850 is designed for Windows Server 2003, but should support basic Windows Server 2008 features and functionality. The Dell web site provides more information about supported hardware for Windows Server 2008:

http://www.dell.com/content/topics/global.aspx/alliances/en/os_certifications?c=us&cs=19&l=en&s=dhs&~tab=5

NetWorker Module for Microsoft Applications

This section describes the known problems and limitations in NetWorker Module for Microsoft Applications.

Conventional incremental backup does not save renamed files (LGTsc00665)

If, after performing a conventional full backup of a drive, you rename files and then perform a conventional incremental backup of the drive, the renamed files will not be saved and will not be browsable for recover in the NMM client window.

Invalid temporary path created during Event Log writer recovery (LGTpa96400)

When you recover a writer such as the System Components Event Log writer, an empty subdirectory is created at C:\temp\nsr_recover\timestamp\...\ ServiceState\EventLogs, where timestamp indicates the time and date of the recover operation. The creation of this subdirectory does not create any performance issues, but does cause the nsr_recov directory to not be removed after rebooting the system.

Workaround

After the client is rebooted, manually delete the nsr_recover directory.

Unable to browse save sets created by NMM client after downgrading from NMM client software to non-NMM client (LGTpa96395)

If, after installing the NMM software, you perform a save or rollover save operation and then decide to downgrade to a non-NMM client, you cannot browse the save sets created by the NMM client on the downgraded client software. This is because the format of the client file index entries changed with the NMM client, and previous NetWorker clients do not recognize this format.

Mounting one volume will mount all volumes in snapshot (LGTpa94348)

When mounting a volume for restore, all volumes included in that snapshot are also mounted. For example, if drives C:, D:, and E: are included in the snapshot and then you mount a directory from drive C: for restore, drives D: and E: also get mounted. The mounting of all volumes in the snapshot causes drive letters to be used up.

Rollover backups do not occur in parallel (LGTpa85933)

Rollover backups for multiple save sets in the client resource occur sequentially instead of in parallel, causing backups to take longer than normal. However, if any save sets are writer save sets (for example, SQL writer) and the writer has files on multiple volumes, the rollover of this save set occurs in parallel, with multiple streams for each of the volumes containing the writer files. Conventional backups (nonsnapshot) occur in parallel.

Recovering files to a deleted mount point (LGTpa95055)

To recover data to a deleted mount point, manually re-create the mount point before recovering the data. Re-creating the mount point enables the data to be recovered to the remote mount point location. Otherwise, the data is recovered to a local directory and the local directory name is the deleted mount point.

Limit of eight volumes included in save set for a client resource (LGTpa94348)

There is a limit of eight volumes included in a snapshot that is supported with the EMC VSS Provider.

Workaround

To back up more than eight volumes for a NMM host:

1. Create separate client resources for the host and limit the save set for each client resource to eight volumes.
2. Ensure that client resources are assigned to different backup groups so that no backup group contains more than eight volumes for a particular NMM host.

Note: Other hardware providers have their own limit for volumes included in the snapshot. Consult your provider's documentation for specific limits.

Character support for names of backup files and directories (LGTpa89319)

The backup of files and directories fail if they have file and directory names containing:

- Extended ASCII characters such as those in French or Spanish.

  Note: Some extended ASCII characters not symbol related may not display properly.

- Unicode characters. These characters are often used in Asian languages.

Behavior of local directives in NMM (LGTpa94805)

Local directives specified in a nsr.dir file cannot refer to a nested directory.

Workaround

Place the directive file, nsr.dir, in the nested directory to which the directive applies. For example, the following directive specifies that all files with a .dll extension under the C:\Windows\system32 directory must be skipped when a backup is performed.

```
<<"C:\Windows\system32">>
skip: *.dll
```

To enable the previous directive, place the directive file, nsr.dir, in the C:\Windows\system32 directory. If the directive is placed in the root of the C: drive, it is not executed upon backup.

Celerra snapshot failure due to inadequate file system size (LGTsc12292)

The file system size needs to be set correctly to accommodate snapshots.

The Celerra document *Configuring iSCSI targets on Celerra* describes how to set the file size correctly in the section "Planning considerations for iSCSI."

Recovery of large number of items fails if one or more items in a folder is deselected (LGTsc05792)

If one or more items is deselected in a folder that has been selected for recovery, then recovery may fail if the number of items in that folder is very large.

This scenario has occurred when testing the recovery of 50 K items in a folder.

Workaround

Select all items or the entire folder, and then perform recovery. After recovery, delete any unwanted items.

Multiple client resources with the same name cannot be combined in the same group (LGTsc15014)

If two or more client resources with the same name are in the same snapshot group, then some of the save sets will not be recoverable. NMM does not support combining multiple client resources with the same name in the same group.

Workaround

Either combine the client resources into a single client resource, or create separate groups and backup the individual clients in separate groups.

The *EMC NetWorker Module for Microsoft Applications Release 2.1 Administration Guide* provides more information about best practices and considerations for application backups, including using different policies for application server data and host operating system data and volumes.

Backup fails when using short client name, after previously using the FQDN for the client device (LGTsc19707)

If you create a client resource using the machine's short name, such as the NETBIOS name, and you have previously used the FQDN in the client resource for that machine, backup will fail.

Workaround

There are two recommended workarounds:

- Delete the media associated with the old client.

  — or —

- Use the FQDN name, so that media records match.

Multiple folder level save sets from the same volume are not displayed in the NMM recovery window (LGTsc20121)

When multiple folder save sets from the same volume are specified in a save set list, only one folder will be displayed in the NMM recovery window. This only occurs with a point-in-time backup with no rollover.

Workaround

To back up multiple folders from the same volume, specify the volume as the save set. Or, create a separate backup job for each folder to be backed up from the same volume.

When GUI is minimized during rollover, the GUI does not open again (LGTsc06558)

If a rollover is started from the GUI, and then the GUI is minimized, then the GUI cannot be opened to check monitoring status. The GUI may appear to be hung.

Workaround

Wait until rollover is complete, and then open the GUI.

Unable to create a Windows Firewall exception for irccd.exe (LGTsc20123)

An error may be displayed during NMM installation:

"Unable to create a Windows Firewall exception for C:\Program Files\EMC\rmagentps\client\bin\irccd.exe. File not found."

Workaround

If this occurs, manually configure the firewall setting, and then validate the configuration.

To configure the firewall:

1. Click **Start**, and then click **Control Panel**.
2. Open **Add or Remove Programs**, select **NetWorker Module for Microsoft Applications**, and then click **Change**.
3. When the **Welcome to NetWorker User Module for Microsoft Applications Maintenance** dialog box appears, click **Next**.
4. In the **Windows Firewall** screen, select **Configure the Windows Firewall**.
5. Click **Next** until you finish the configuration wizard.
6. Click **Start**, and then click **Control Panel**.
7. Open **Windows Firewall**.
8. Click the **Exceptions** tab.
9. In the **Programs and Services** list, verify that **EMC Replication Manager Client for RMAgentPS** appears and is selected.
   - If the checkbox is not selected, select it.
   - If there is no entry for **EMC Replication Manager Client for RMAgentPS,** manually add it:
     a. Click **Add Program**.
     b. Click **Browse**.
     c. Type **C:\Program Files\EMC\rmagentps\client\bin\irccd.exe**.

        If NMM was installed on an another drive letter other than C:\, specify the correct path to irccd.exe as needed.
     d. Click **OK**.

Search results return everything from root node when searching from a subnode (LGTsc20731)

In the NMM System Recover Session window, if you use the context menu to search from within a folder several levels deep in the navigation tree, the search operation displays results from the root node down. This may occur when you right-click a sub node in the Browse pane and then click **Search for**. NMM switches to the Search tab, and the search path correctly displays the selected sub node. But when a search is performed, the results are from the root node down, not the selected sub node.

VSS_E_WRITERERROR_RETRYABLE (LGTsc20827)

This error may occur during backup. In some cases it occurs if a savegroup is rerun, and it was stopped previously while a replica was being taken and the replica did not complete. This error may also occur if the shadow copy storage limit is exceeded.

Workaround

Try one or more of the following:

- Wait ten minutes, and then repeat the backup, restore or shadow copy creation operation up to three times.

- Stop EMC VSS provider, Microsoft VSS service, and Replication Manager service. Then restart these services and try the backup again.
- Delete unnecessary shadow copies on the system to free up shadow copy storage.
- When this error occurs with a Hyper-V backup, the Hyper-V VSS writer will be in an inappropriate state for backup, and the **Hyper-V Virtual Machine Management** service must be restarted before attempting another backup.

Data cannot be recovered from multiple snapshots at a time (LGTsc26194)

When there are multiple snapshots with different save times, the snapshot recovery will fail for one of the drives if data is selected from multiple snapshots at a time.

The following example describes one way this recovery failure might occur:

1. A snapshot policy is configured as 4/4/day/none.
2. A backup is performed of a local drive, C:\ .
3. A backup is performed of a local drive, I:\ .
4. After the backups, a recover session is opened in NMM, and the C and I drives are mounted for browsing the data.
5. Data is selected for recovery from both drives, for example C:\Test1 and I:\Test2.
6. The "snapshot restore" option is selected, and then the recovery operation is performed.
7. The result: *recovery of data from one of the drives, either C or I, will fail*.

Workaround

Use a conventional restore to recover data from multiple drives or save sets that are from different times.

At least one drive letter must be available for rollover of a snapshot (LGTsc27316)

When performing a rollover of a snapshot of the drive that contains the NMM binaries, at least one drive letter must be available to use as the temporary location for the mounted snapshot.

For example, the default installation folder for the NMM binaries is C:\Program Files\Legato\nsr. When performing a rollover of a snapshot of the C drive, at least one drive letter must be available to use as the temporary location of the mounted snapshot.

CLARiiON, Symmetrix, and providers

This section describes the known problems and limitations in CLARiiON, Symmetrix, and providers.

Snapshot cannot include both CLARiiON and Symmetrix volumes (LGTpa91221)

A client resource cannot include both CLARiiON and Symmetrix volumes in the same save set. Additionally, save set **All** cannot be specified for such a client resource. If both CLARiiON and Symmetrix volumes are included in a save set, the backup will fail.

Workaround

If a NMM has both CLARiiON and Symmetrix volumes, create at least two client resources: one for CLARiiON volumes and one for Symmetrix volumes. Additionally, do not specify save set **All** in any of the client resources for the NMM.

EMC VSS Provider cannot take a snapshot of the volume on which Solutions Enabler is installed (LGTpa90841)

A CLARiiON or Symmetrix volume supported with the EMC VSS provider cannot take a snapshot of the volume on which Solutions Enabler is installed. Additionally, the volume on which Solutions Enabler is installed cannot be included in the same client resource and backup group with a CLARiiON or Symmetrix volume.

More information about this issue is provided in the EMC Solutions Enabler documentation.

Workaround

To protect a NMM using CLARiiON or Symmetrix storage:

- Install Solutions Enabler on a local volume (a volume that is not a CLARiiON or Symmetrix volume). When Solutions Enabler is installed on a local volume, the snapshot is taken with the software-based VSS System provider.
- Do not specify save set **All**.
- Create at least two client resources for the NMM. Create one client resource for the local volume on which Solutions Enabler is installed and create another client resource for the CLARiiON or Symmetrix volumes. Local volumes without Solutions Enabler installed can be included in any client resource.
- Ensure that the client resource for the local volume on which Solutions Enabler is installed and the client resource for the CLARiiON or Symmetrix volumes are not assigned to the same backup group.

Snapshot may fail to import when QLogic SanSurfer running (LGTpa90724)

Snapshots supported with a hardware provider may fail to import if the QLogic Management Suite Java Agent service running, and return a getoperation error.

Workaround

Use the QLogic SanSurfer utility to stop the QLogic Management Suite Java Agent service. Manually start the service only when required and then manually stop the service. The Primus eServer Solution article, emc129473, provides more information.

Hardware import failures and freeing up LUN resources (LGTpa88834)

When an import operation succeeds, LUN resources reserved for the import operation are freed automatically. When an import operation fails, the NMM cannot free resources when the snapshot is deleted through retention policy on hardware storage systems such as CLARiiON or Symmetrix.

Workaround

Free the LUN resources manually using the Microsoft **vshadow** utility or vendor supplied utilities.

The Microsoft **vshadow** utility is available in the Microsoft Volume Shadow Copy Service SDK 7.2, which is available for download from http://www.microsoft.com/downloads/.

Information about freeing resources with vendor utilities is available in the array of management utilities provided with your hardware storage systems.

Reclaiming array storage after an import failure (LGTsc03522)

When there is an import failure in CLARiiON snapshots or clones, or Symmetrix BCVs or VDEV, the snapshot session must be destroyed, synchronized, or terminated, depending on the hardware type, prior to the next backup.

Use the following examples as general descriptions of the process or procedure. Refer to the product documentation for more detailed steps and information to perform these on your system.

Workaround

For CLARiiON Snapshots (DIFF):

1. In **Navisphere Manager**, locate the snapshot name and session based on the timestamp.
2. If the snapshot belongs to a Storage Group(s), remove the snapshot from the Storage Group(s).
3. Select the session and then click **Stop Session**.
4. Select the snapshot and then click **Destroy Snapshot**.

The index entry "destroy, snapshot" in the *Navisphere Manager Help* provides more detailed steps and information.

For CLARiiON Clones (PLEX)

1. In **Navisphere Manager**, locate the clone group for the source LUN.
2. Right-click the clone group you want to synchronize, and then click **Synchronize**.

The topic "Synchronizing a fractured clone" in the *Navisphere Manager Help* provides more detailed steps and information.

For Symmetrix BCVs (PLEX)

- Make the BCVs *not ready*, using EMC Solutions Enabler Symmetrix CLI (SYMCLI)

For example:

```
symdev -sid SymmID [not_ready] <BCV#>
```

The *EMC Solutions Enabler Symmetrix CLI Command Reference* and the *EMC Solutions Enabler Symmetrix TimeFinder Family CLI Product Guide* provide detailed information about using the symdev command and options.

For Symmetrix VDEV (DIFF)

- Terminate the snap session using the symsnap command with the terminate option.

The *EMC Solutions Enabler Symmetrix CLI Command Reference* and the EMC *Solutions Enabler Symmetrix TimeFinder Family CLI Product Guide* provide more information about using the symsnap command and options.

If the hardware provider is in a cluster, the proxy host cannot be a member (LGTsc26983)

The *EMC NetWorker Module for Microsoft Applications Administration Guide* provides instructions for performing Windows Server Cluster backups. One of the tasks listed for Windows Server Cluster backups, Task 7: Configure a proxy client, states that when setting up hardware provider such as the EMC VSS Provider, a proxy client must be configured for a clustered NMM client.

There is an additional consideration for backing up a clustered Client resource: The proxy client is not allowed to be a member of the cluster. This is by Microsoft design, it is not supported by the Windows Cluster service. Microsoft describes this restriction in a MSDN article at http://msdn.microsoft.com/en-us/library/aa384600(VS.85).aspx, in the subsection "Auto-Import Hardware Shadow Copies Are Not Supported on Windows Cluster Service."

Microsoft Exchange Server and Microsoft SQL Server

This section describes the known problems and limitations in Microsoft Exchange Server and Microsoft SQL Server.

SQL 2005 databases in recovery state are not skipped during backup or restore (LGTsc00754)

SQL 2005 databases in the recovery state are not skipped during a conventional backup or snapshot restore; the SQL Server Writer does not list database files in the recovery of the file system. This problem only occurs when you perform a file system backup of the file systems that contain these SQL database files. As a result, when you restore the file system where these databases reside, the files are overwritten.

Workaround

If the databases were participating in SQL Log Shipping, recreate the database from a fresh backup of the source, then reenable log shipping.

SQL backups with the MSDE Writer fail if a database is in suspect mode (LGTpa94615)

If any of the databases belonging to a SQL instance are in suspect mode, and a backup of the SQL instance is attempted with the Microsoft MSDE Writer, the snapshot backup will fail with the following error:

```
[3844] [S]  10/27/06 11:19:24 RM .. 027121 ERROR: MSDEWriter has
failed at prepare snapshot. The error is
VSS_E_WRITERERROR_NONRETRYABLE.  The code is: 0x800423f4. Check the
application event log for more information.
[3844] [S]  10/27/06 11:19:24 RM .. 026003 ERROR: Application Agent
operation thaw has failed with an error...
```

Workaround

Either delete or repair the suspect databases.

Rollback recovery fails if there is a public folder in Exchange (LGTsc20347)

If an attempt is made to perform rollback recovery of Exchange and there is a public folder, rollback will fail.

Workaround

There are several options available:

- **Option 1**: Attempting a rollback implies that you have a point-in-time (PIT) on hardware supported by EMC VSS Provider, because NMM does not support rollback in any other configuration. Instead of performing rollback from the PIT Management plug-in, use the System plug-in and request a recover from there. If there has been no rollover to NetWorker, or you have selected the option to try a point-in-time recover first, then NMM will perform a "file system" recovery. In this file system recovery, the .edb and log files will be selected from the point-in-time recovery and copied back to the production volume.

  If there is also a rollover, then you can recover from there as well.

- **Option 2**: The storage group that contains the public folder database can be set up on a separate volume from the storage group that contains the mailbox databases.

Backing up data for a Microsoft Exchange or SQL application (LGTpa91971)

When backing up data for a Microsoft Exchange or SQL application, ensure that all databases are mounted. Unmounted databases are not backed up, and no warning appears during the backup operation to indicate if any databases are unmounted.

Exchange Storage Groups must be in the same locale as the Microsoft Exchange Server (LGTsc17699)

Microsoft requires Exchange Server 2003 Storage Group names to be in the same locale as the Microsoft Exchange Server.

Exchange backup requires that the System Path and Transaction Log be set to the same location (LGTpa93254)

When performing a backup of Microsoft Exchange, specify the same directory location (such as E:\) for both the System path and the Transaction log under the Storage Group properties in Microsoft Exchange System Manager.

Recovery of multiple databases in Recovery Storage Group fails (LGTsc21107)

When recovery of multiple databases in a Recovery Storage Group (RSG) is configured through Database Recovery Management in Exchange Management Console, restore of one or more of the database files may fail. This issue has been identified as a bug in Microsoft Exchange, not EMC NetWorker Module for Microsoft Applications. Microsoft is working on a fix for this issue.

Microsoft provides more information about this issue and workarounds in the Knowledge Base (KB) article 959065 "Wrong database name is added to Recovery Storage Group when more than one database exists in a Storage Group," available at:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;959065

Workaround

Use the Exchange Management Shell at the command line to configure an RSG. The *EMC NetWorker Module for Microsoft Applications Release 2.1 Administration Guide*" provides detailed steps for this task in the "Microsoft Exchange Server Backup and Recovery" chapter, in the section "Creating an RSG and adding target databases."

NMM installation fails with irccd failure on Exchange Server 2003 (LGTsc26630)

Exchange backup may fail after NMM installation because the IRCCD.exe and nwexinfo.exe services must be run manually after installation. During any NMM installation, the IRCCD.exe service may need to be manually started. This issue is discussed elsewhere in the Release Notes in "Unable to create a Windows Firewall exception for irccd.exe (LGTsc20123)" on page 30.

In addition to manually starting the IRCCD services, in Exchange installations an additional step is required.

Workaround

At the command line, run the following command to update the Exchange domain information: **nwexinfo.exe**.

Exchange backup fails if some logs and databases are under normal path and some are under volume mount path (LGTsc22968)

Exchange backup may fail if it contains some Exchange Storage Group logs and databases that reside under a normal path, without a mount point, and some Exchange Storage Group logs and databases that reside under a volume mount point path.

Backup may fail, and display the following message:

```
---------------------------------------------------------------------
RM .. 026420 ERROR:An unexpected internal error occurred: IRD:
mountRestoreState::handleFinalStatusMsg() :
validateState::runState() failed.
---------------------------------------------------------------------
```

Workaround

In the save set, use the volume mount path to specify all Exchange Storage Group logs and databases.

NMM does not support RSG configuration where the RSG system path restore location and RSG logs restore location are different (LGTsc23889)

Microsoft Exchange server supports an RSG configuration where the RSG system path restore location and RSG logs restore location can be different.

NMM does not currently support that configuration.

Workaround

Specify the same location for the RSG system path and the RSG log path.

Exchange backup fails with VSS_E_MAXIMUM_NUMBER_OF_VOLUMES_REACHED (LGTsc26385)

Attempting to perform a backup of more than 32 storage groups results in an error:

VSS_E_MAXIMUM_NUMBER_OF_VOLUMES_REACHEDVSS_E_MAXIMUM_NUMBER_OF_VOLUMES_REACHED

This is a known Microsoft error described at:
http://msdn.microsoft.com/en-us/library/aa382650(VS.85).aspx

Workaround

You can back up 32 storage groups in a single save set at a time.

NMM installation fails for Proxy Storage Node because RMExchangeInterfaceComponent is not installed (LGTsc26558)

On an NMM Proxy installation over a NetWorker Storage Node, NMM installation does not install RMExchangeInterfaceComponent, and consistency checking fails. For Proxy Storage Node configurations that will be used in an Exchange Proxy Backup configuration, the RMExchangeInterface service is required on the Proxy Storage Node. Installing NMM on the Proxy Storage Node will not currently register this service on the system. However, the binaries for the service are installed, and the RMExchangeInterface service may be manually registered once NMM is installed.

Note: This issue only impacts Proxy Storage Node configurations. It does not impact Proxy Node (non-Storage) node configurations, where the RMExchangeInterface service should be installed and registered properly.

To manually register the RMExchangeInterface service and COM component:

1. At the command line, change directories to C:\Program Files\EMC\rmagentps\client\bin:

   cd C:\Program Files\EMC\rmagentps\client\bin

2. Type the following command (all on one line):

   rm_exchangeinterface /debug /service /user "DOMAIN\USERNAME" /password "clear text password"

3. Type: **Install.log**

   The existence of this log confirms that the COM component was registered and the service was installed.

Troubleshooting steps for RMExchangeInterface component (LGTsc26559)

If there appear to be problems with the RMExchangeInterface component, try one or more of the following:

- Check that the service is installed.
- Check service account. It should not be local system. It should be an account that has Exchange Administrator privileges.

  Note: The service is not running by default, it runs on demand.

- Check the Install.log in C:\Program Files\EMC\rmagentps\client\bin\Install.log. The file itself does not contain much information. What is important is that the existence of this log confirms that the COM component was registered and the service was installed.
- Validate COM entry is present using the Component Services manager.
- Check the event log for any errors.

RM service CPU utilization is increased while doing parallel consistency checking (LGTsc26585)

If multiple consistency checks are run in parallel without setting proper throttle limits, it may cause performance problems on the proxy system. In extreme cases, this can cause I/O bottlenecks so severe that consistency checks will fail and other operations with the system are adversely affected.

Workaround

Set threading and throttling as described in "Consistency check parameters added to set threading and throttling to handle performance issues (LGTsc26634)" on page 39.

Consistency check parameters added to set threading and throttling to handle performance issues (LGTsc26634)

NMM 2.1 SP1 adds the ability to set threading and throttling to handle performance issues through the use of the -A attribute values to pass on to Replication Manager for eseutil configuration settings.

The following attributes have been added:

- **NSR_ESE_UTIL_SEQUENTIAL** - set to true or false to specify if eseutil should be run sequentially (single threaded) or in parallel against multiple SG's (multi-threaded)
- **NSR_ESE_UTIL_THROTTLE** - set to true or false to specify if eseutil should be throttled
- **NSR_ESE_THROTTLE_IOS** - number of I/O's between pauses when throttling, value range of 100 < 10000
- **NSR_ESE_THROTTLE_DURATION** - duration of pause in milliseconds when throttling, value range of 1000 < 60000

For example:

-A NSR_ESE_UTIL_SEQUENTIAL=false -A NSR_ESE_UTIL_THROTTLE=true -A NSR_ESE_THROTTLE_IOS=500 -A NSR_ESE_THROTTLE_DURATION=5000

Exchange snapshot recovery failing with ImportCopy error (LGTsc25761)

For Exchange backup in NMM, it is highly recommended to avoid using persistent software shadow copy or copy-on-write backups. Due to the way data is distributed in Exchange databases, those types of snapshots may not remain valid long enough for recovery to be successful.

To ensure a valid and successful backup of Exchange, always use the setting backup=all when configuring the Client Resource. The EMC NetWorker Module for Microsoft Applications Administration Guide provides complete instructions for configuring a Client Resource in the Microsoft Exchange Backup and Recovery chapter.

NMM does support temporary software shadow copy or copy-on-write for Exchange, which may be necessary if your system does not use a CLARiiON or similar hardware storage array. For persistent snapshot support in an Exchange environment, use a hardware storage array in your Exchange backup and recovery strategy.

If a persistent software copy or copy-on-write backup is performed on an Exchange database, recovery may fail with an error message similar to the following:

```
%sERR: Error calling importCopy, status=%d:'%s' 3 0 35 PS:
(CPSImportService::ImportCopy) 1 2 15 24 107 Error obtaining volume
name (s) for snapshot; Microsoft ShadowCopy Service has no knowledge
of the snapshot.
```

Workaround

Always follow these recommended practices:

- Do not use persistent software shadow copy or copy-on-write for Exchange backup.
- Configure the NMM backup Client Resource snapshot policy to use the **backup=all** setting.
- Use a hardware storage array to handle backup, recovery, and storage operations. This minimizes the load on the Exchange server storage and resources by moving these operations to separate hardware.

Backups should be grouped with no more than 10 Storage Groups at a time (LGTsc27318)

When backing up Exchange 2007, backups should be grouped with no more than 10 Storage Groups at a time. This is especially important when parallel consistency checking has been turned on. Grouping more than 10 Storage Groups consumes the available resources of the CPU, I/O and memory, which can lead to backup failures.

Microsoft Hyper-V and Data Protection Manager

This section describes the known problems and limitations in Microsoft Hyper-V and Data Protection Manager.

Save of DPM data with data mover fails with import error (LGTsc12128)

When performing a save operation of DPM database and replica without using data mover, save operation is successful.

If the DPM database and replica is saved with data mover, the save operation fails with an error similar to the following:

```
2007 12 12 16:52:02 (5628) main.

000551 ERROR:Import of dynamic disk group(s) cannot proceed
because Replication Manager was unable to determine the
existing dynamic disk groups on this system (Call to vxdg
list failed). Check to make sure that Volume Manager is
installed properly. /*e*/
```

Workaround

NMM does note support dynamic disks with data mover (transportable snapshots).Perform save operations of DPM database and replica without using data mover.

NMM incorrectly reports replica recovery failure (LGTsc15805)

When recovering a single replica from among several replicas that were backed up, the recovery job may be reported as failing.

Nsrsnap_vss_recover.exe will report failures for any replicas that were not targeted for recovery.

Workaround

No action is required for the replicas selected for recovery. The targeted replicas will recover successfully, and if failures are reported for replicas that were not selected for recovery, the recovery failure messages can be ignored.

Granular recovery of replica on Hyper-V guest leaves extra folder behind (LGTsc20357)

When a granular recovery of a DPM replica is performed, NMM recreates in the recovery folder the exact path to the replica as it appeared when backed up from the DPM server. This path includes the installation path of the DPM application and the subfolders containing replica data, similar to the following:

<recovery folder>\C\Program Files\Microsoft DPM\DPM\Volumes\Replica\<replica data>

Following replica recovery, NMM attempts to remove the unnecessary DPM application folders, so the resulting path becomes:

<recovery folder>\<replica data>

When such a recovery is performed on a Hyper-V guest, NMM is unable to remove the DPM application folders.

Workaround

After a Hyper-V guest replica recovery, verify the recovery, and then manually delete the extra folders created in the replica path.

Data Protection Manager 2007 rollup installation requires resetting account permissions (LGTsc19637)

For compatibility on all supported platforms — Windows Server 2003 (x86 and x64) and Windows Server 2008 (x86, x64) — NMM requires that the initial installation of Data Protection Manager 2007 be followed by installation of the DPM 2007 rollup "System Center Data Protection Manager 2007 Feature Pack (x86)," available from the Microsoft downloads web site. However, installing the rollup also removes account permissions essential for recovery of the DPM configuration database, resulting in failed recoveries.

Workaround

Currently Microsoft has no service pack or hot fix available to fix this issue. The following steps are required to manually restore the permissions:

1. Install Data Protection Manager 2007.
2. Install the DPM 2007 Rollup.
3. Open the **Windows Registry**.
4. Locate the registry key:

   HKLM/Software/Microsoft/Microsoft Data Protection Manager/Setup/DatabasePath

5. Get the value of the database path. For example:

   C:\Program Files\Microsoft DPM\DPM\DPMDB

6. Close the **Windows Registry**.
7. Go to the folder obtained from the registry entry. For example:

   The **DPMDB** folder at **C:\Program Files\Microsoft DPM\DPM\DPMDB**.

8. Assign a full control permission to the folder, for the user: **MicrosoftDPMAcct**

After successful DPM backup, NMC occasionally displays the save group as failed (LGTsc20732)

Sometimes the NetWorker Management Console (NMC) displays the DPM backup save group as failed, even though the backup was successful.

Workaround

You can verify whether the save group backup succeeded or failed by either of the following methods:

- Check the nmm.raw file. This is the NMM log file and it is cumulative, so it is appended each time a backup or recover operation is performed. This file is located in the Applogs folder. For example, C:\Program Files\Legato\nsr\applogs\.
- Check the NMM GUI. If the save set is available in the DPM Recover Session window, then the save group backup was successful.

Defaults for disaster mode and granular mode on Hyper-V guest or physical machine (LGTsc20284)

The default recovery mode depends on whether it is a Hyper-V guest or physical machine:

- For Hyper-V guests, the default is disaster mode with directed recovery.
- For physical machines, the default is granular mode.

Hyper-V configuration requirements for backing up a virtual machine that contains multiple volumes (LGTsc18796)

When there are multiple volumes on the guest, backup may fail. When there are multiple volumes on the guest, VSS decides the shadowstorage area for the snapshots based on which volume has more space. This can lead to a condition where the snapshot of volume C and the snapshot of volume D both reside on volume D, since volume D has more space. During the snapshot revert stage in PostSnapshot, the snapshot of volume C may be lost if the snapshot of volume D is reverted first.

Workaround

To prepare a multiple volume guest for backup, use the *vssadmin* command to force the shadowstorage of each volume to be on the same volume:

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

Repeat as needed for each volume in the virtual machine.

Unable to recover DPM database through System Recover Session (LGTsc20971)

To recover a DPM database, use DPM Recover Session. In the NMM GUI, when you select a DPM server and then select Recover, the submenu lists both System Recover Session and DPM Recover Session. Because the DPM database is a SQL database, it may appear selectable for recovery in System Recover Session. An attempt to recover a DPM database through System Recover Session will fail in the recovery operation.

Workaround

Always use the DPM Recovery Session UI to recover DPM databases.

Incorrect Hyper-V save set name for configuration file in Administration Guide (LGTsc26529)

In the NetWorker Module for Microsoft Applications Release 2.1 Administration Guide, one of the references to the Hyper-V save set name for backing up the configuration file is incorrect. In the "Microsoft Hyper-V Backup and Recovery" chapter, in the procedure "To create a Hyper-V Client resource," there is an error in step 9. The save set to back up the configuration file (Initial Store) incorrectly listed Information Store in the syntax, APPLICATIONS:\Microsoft Hyper-V*Information* Store. The text should say:

To back up the configuration file (Initial Store), specify:

```
APPLICATIONS:\Microsoft Hyper-V\Initial Store
```

DPM support requires DPM 2007 SP1 (LGTsc25460)

DPM support in NMM requires the installation of DPM 2007 SP1. Otherwise, replicas may not successfully recover.

The DPM 2007 SP1 download is available from Microsoft at:

- 32 bit: http://www.microsoft.com/downloads/details.aspx?FamilyID=43cef22c-f027-4c0b-8fad-b081485c3efe
- 64 bit: http://www.microsoft.com/downloads/details.aspx?FamilyID=8ae5edac-4de8-44e0-a6f9-8afbb3e23585

Microsoft SharePoint

This section describes the known problems and limitations in Microsoft SharePoint.

Restore of SharePoint web applications fails if a web application is deleted (LGTsc20028)

If a web application is deleted, NMM cannot restore the web sites that belonged to the deleted web application.

Workaround

Create a web application, and do an alternate restore of the web sites to the newly created web application.

SharePoint search does not display Farm or File objects (LGTsc20823)

In the NMM SharePoint Recovery window, when a search is performed from the Search tab for a Farm or File in the Object type field, no search results are displayed.

Workaround

Locate Farm or File objects by navigating to them through the Browse tab.

SharePoint 2007 granular recovery does not recover correct permission level for List (LGTsc20108)

After recovering a list, the permissions applied to the recovered list may be incorrect. When the **WSS only** or **All** option is selected in the recovery **Security** options, those settings may be ignored and the original permission levels for the list are not recovered correctly. The wrong permission levels may be applied to the recovered list, or, in some cases the permission levels are inherited from the parent website.

SharePoint 2007 granular backup does not support multiple save sets at the same time (LGTsc20071)

NMM does not support running multiple SharePoint 2007 save sets in a save set at the same time.

Workaround

To back up more than one save set:

- Schedule each save set to run at a different time.
- Specify only one save set within a savegroup.

Backup of a large SharePoint farm requires inactivity timeout set to zero (LGTsc20555)

During the backup of a large or complete SharePoint farm, some web applications or websites may not be backed up if the inactivity timeout is not set to zero (0). Backup errors may be noted in the log file, but the backup may appear to be okay in the NetWorker Management Console.

Workaround

When configuring the NetWorker Client resource, set the inactivity timeout to zero (0) for the save group.

Required Volumes information is not displayed correctly in Microsoft SharePoint Services node (LGTsc13670)

In NMM, when you select and right-click the **Microsoft Office SharePoint Services** node or an item within that node, and then click **Required Volumes**, the volume information is not displayed. Instead, a message box is displayed:

```
NetWorker was not able to display required volumes information for
the selected Microsoft Office SharePoint Services component. Please
query the following node(s):
```

The message lists the nodes where the required volumes information can be found. The message may point to a local or remote host name, depending on where the SQL Server database for this Microsoft Office SharePoint Services is located.

Workaround

Query the nodes listed in the message:

1. In **NetWorker Module for Microsoft Applications**, navigate to the backup you want to check.
2. Select and right-click the **Microsoft Office SharePoint Services** node or an item within that node, and then click **Required Volumes**.

   A NetWorker message box is displayed, with instructions to query the nodes that are listed in the message box.
3. Note the nodes listed in the message box, and click **OK**.
4. For each node that was listed, select and right-click the node, and then click **Required Volumes**.

Incorrect Author information is displayed when browsing or searching SharePoint recovery sets (LGTsc20175)

When browsing or searching SharePoint recovery sets, the Author column in the results pane may display numbers or other incorrect information.

Some SharePoint list items are not recovered after they were deleted from SharePoint (LGTsc20334)

Some list items are not recovered after they are deleted from SharePoint. This issue has been observed with the following types of lists:

- Annoucements
- Custom List
- Survey
- Contacts
- Calender
- Task

Workaround

Try one of the following:

- Check the SharePoint Recycle Bin. If the deleted item exists in the Recycle Bin, it can be restored from there.

  The default storage for the SharePoint Recycle Bin is 90 days, but this setting can be changed by the SharePoint administrator.

- Recover the list from an optimized backup of the top level site which contains the lists noted in this issue.

  With an optimized backup, all items in the web application and top level site can be backed up and restored. An optimized backup is a non-granular backup, and cannot be recovered in a granular way. The optimized backup does not back up the entire SharePoint farm, and cannot be used for disaster recovery.

  To perform an optimized backup, follow the steps in "Configuring a SharePoint 2007 Client resource for granular backup" in the "Microsoft SharePoint 2007 Granular Backup and Recovery" chapter in the *EMC NetWorker Module for Microsoft Applications Release 2.1 Administration Guide* through step 13. At step 14, in the **Application information** attribute, type the following variable and value: *OPTIMIZED*=true.

- Recover the list from a full VSS-based backup.

  Schedule regular full backups of the SharePoint farm, so that all items in the site collection are backed up and can be restored. The "Microsoft SharePoint Server Backup and Recovery" chapter in the *EMC NetWorker Module for Microsoft Applications Release 2.1 Administration Guide* provides complete steps for full backup and recovery of a SharePoint farm. Typically a backup plan for SharePoint includes regular full backups, for disaster recovery, and granular backups for granular recovery of specific SharePoint sites, subsites, lists, or objects.

SharePoint credentials are not set during installation (LGTsc20424)

When installing NMM on non-English versions of Windows Server 2008 x64, an error message may be displayed during NetWorker SharePoint Service Configuration. The error message may contain the following text:

"Error while modifying credentials of service" or "Unable to start the service"

Workaround

Manually set the username and password for the SharePoint service. Before assigning any user to start any service, assign permission of type "Log on as service" for each user account. For more information about "Log on as service," consult Microsoft Server 2008 documentation.

SharePoint 2007 granular search and recovery limitations (LGTsc20363)

There are several known issues and limitations with granular recovery of SharePoint 2007 items:

- SharePoint granular search items that are marked will not appear in the summary results pane like Browse tab items do.
- You can select items from either the Browse tab or the Search tab, but not both at the same time. If an attempt is made to select from both, a warning message will be displayed.
- Within the Search tab, you can only search for one type of object.
- With leaf objects (items that are not containers), you can select multiple objects, but not the same objects from different backup times. If you try to select different versions of the same object, a warning message will be displayed.
- With container objects, you can only select one object at a time. If you try to select more than one container object, a warning message will be displayed.
- You can prevent additional messages from being displayed in this session by selecting the **Do not show this again for this session** checkbox. A session is defined as starting when the NMM client is opened, through the NMM operations, and ending when the NMM client is closed. Each time a new session is started, this checkbox is restored to the cleared (unselected) state.
- The **Update Version**, **Overwrite** option for in the Pre-Recovery Options dialog box does not always overwrite items if they already exist on the target. If the old version of the item is not overwritten, delete the file from the target and perform recovery of the file again.

SharePoint disaster recovery fails with SQL database recovery failure (LGTsc20972)

SQL master database recovery may fail, which causes SharePoint disaster recovery to fail. An error is displayed similar to the following:

```
63688:nsrsnap_vss_recover: NMM Cannot replace file C:\Program
Files\Microsoft SQL Server\MSSQL.1\MSSQL\Data\master.mdf in
comp master in writer SqlServerWriter. Database must be put
into overwrite state.
```

Workaround

If this error occurs, then the specified files database needs to be moved, renamed, or deleted, and the recovery steps rerun from that point. The associated files are the master database file master.mdf and master log file mastlog.ldf.

Incorrect item names displayed in NMM granular backup of SharePoint 2007 (LGTsc19177)

In the NMM Recover view, NMM may display the wrong names in the item list for the following SharePoint list items:

- Custom list
- Custom list in datasheet view

- Import spreadsheet

When one of these lists is clicked in the navigation page, instead of displaying list item name, a number is displayed for each item name. For example: 1_.00, 2_.00, 3_.00. There is no data loss; all of the items in the list are displayed and available for selection and only the name of the item is displayed wrong.

When the item is actually recovered, the name of the item is not changed and will appear correctly in SharePoint with the original name of the item backed up.

SharePoint allows multiple items with the same name under one list (LGTsc20571)

With some types of lists, SharePoint allows multiple versions of the same item from different backups to be recovered to the same list. Duplicate items may be appended to the list instead of overwriting the item.

SharePoint assigns a unique id (GUID) to every item, so when an item is changed, it is assigned a new GUID even though the name of the item is the same. When the item is recovered, SharePoint uses the GUID, not the item name, to determine whether the recovered item is added to the list or replaces an item in the list. Multiple versions of the same item may appear in the list because they have different GUIDs.

This behavior occurs with items in the following types of lists:

- Announcement
- Calendar
- links
- Calendar
- Project tasks
- Task
- Issue tracking
- Custom list
- Custom list in Datasheet view
- Languages and Translators
- Import Spreadsheet

Workaround

After recovering items from these types of lists, check the recovered documents and delete or remove any extraneous files that may have been recovered.

SharePoint backup hangs after adding space to write NetWorker index (LGTsc27197)

If there is not enough space on the NetWorker server to write the index, a warning is displayed:

```
NetWorker index: (warning) Filesystem containing file index for
client '...' is getting full.
```

Even if you provide additional space on the NetWorker server after seeing the warning, backup fails to proceed, and no more warnings are displayed.

Workaround

1. Clear sufficient space for the index on the NetWorker server.
2. Stop the currently running backup.
3. Restart the backup.

SharePoint recovery of site fails for certain templates (LGTsc27196)

With some SharePoint site or library templates, complete site recovery may fail after individual items in those sites are updated and the site is backed up.

This may occur with sites created using one of the following site or library templates:

- Wiki Site
- Blog
- Document Center
- Report Center
- Search Center with tabs
- Site Directory
- Collaboration portal

If individual list items are updated in these sites, and then the site is backed up, the backup will be successful. But when the complete site is selected for recovery, recovery fails. However, individual list items can be recovered successfully.

Workaround

Create a blank site with the same name and URL, and then perform recovery.

Note: The recovery will be successful, but an error message will be displayed in the event viewer:

```
Error loading and running event receiver
Microsoft.SharePoint.Portal.WebControls.ReportLibraryItemEventRecei
ver in
Microsoft.SharePoint.Portal, Version=12.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c. Additional information is below.:
: The object specified does not belong to a list.
```

This message can be ignored.

Changing the temporary storage location for the SharePoint backup (LGTsc22283)

During NMM installation, the NetWorker SharePoint Service Configuration dialog box is displayed. This dialog box allows you to specify the staging area for SharePoint granular backups. Neither the NMM 2.1 Installation Guide or the Administration Guide describe how to change the staging area after installation.

To change the temporary storage location for staging SharePoint backups:

1. At the command line, type:

   C:\Program Files\Legato\nsr\bin\nwmossinst.exe

   The **NetWorker SharePoint Service Configuration** dialog box is displayed.

2. In **Temporary Storage Location**, specify the path for the staging area for SharePoint granular backups.

The Temporary Storage Location must contain a valid drive and folder name, and cannot have a terminating '\' at the end of the path.

3. Click **OK** to save your changes.

   The NetWorker SharePoint Service Configuration safely saves the staging location to the Windows Registry.

The temporary storage location must contain a valid drive and folder (LGTsc27380)

When specifying the temporary path in the SharePoint Recovery Options dialog box in NMM, and in the NetWorker SharePoint Service Configuration setup utility run at the end of installation, the temporary path must contain a valid drive and folder name.

For example, "C:\folder" provides the minimum requirement for a valid temporary path by specifying the drive "C:\" and folder "folder." The path can be deeper but cannot be just the volume itself. Do not put a terminating '\' at the end of the path, or backups will fail with an error, "Illegal characters in path."

NetWorker SharePoint Service credentials must match credentials of SharePoint Server Administrator (LGTsc24189)

During NMM installation, the NetWorker SharePoint Service Configuration dialog box provides fields to specify the Domain/User Name and Password for SharePoint Service credentials. By default, *LocalSystem* is specified for the User Name. If you leave this value as is and do not fill in the fields to specify the same credentials as those of the SharePoint Server administrator, backup of SharePoint data will fail with a Windows E_ACCESSDENIED error.

If you have already completed installation and want to test whether your credentials are correct, you can run the following commands at the command line on the SharePoint machine:

```
nsr_moss_save.exe -f

nsr_moss_save.exe -w

nsr_moss_save.exe -w "<Web Application Name>"

nsr_moss_save.exe -u
```

If these queries run without any triggering any error messages, your credentials are probably specified correctly.

Workaround If you have been getting error messages or failures with SharePoint backups, you can update the NetWorker SharePoint Service credentials.

To update or correct SharePoint Credentials:

1. At the command line, type:

   C:\Program Files\Legato\nsr\bin\nwmossinst.exe

   The **NetWorker SharePoint Service Configuration** dialog box is displayed.

2. In **Domain\User Name**, specify the domain and user name you use for your Microsoft SharePoint Server administrator account.

3. In **Password** and **Confirm Password**, specify the password you use for your Microsoft SharePoint Server administrator account.

4. Click **OK** to save your changes.

Optimized SharePoint granular backups must be specified in the backup command (LGTsc22537)

The NetWorker Module for Microsoft Applications Release 2.1 Administration Guide on page 162 specifies to use the Optimized=true command attribute in the Application Information section when configuring the Client resource. However, this does not work correctly and it creates a full granular backup.

This will be fixed in a future NMM release.

Workaround

Add the Optimized=true command attribute to the Backup command instead of the Application Information section.

To add the Optimized=true command:

1. In the Client resource, click the **Apps & Modules** tab.
2. In the **Backup command** attribute, include the **Optimized=True** value in the backup command.

   For example:

   ```
   Nsr_moss_save.exe -A OPTIMIZED=True
   ```

SharePoint backup fails when host and proxy client do not match (LGTsc24206)

When using Data Mover to perform a SharePoint backup, the application host and proxy client must use the same operating system release, patch level and processor architecture:

- The application host and proxy client must be same operating system release.

  For example both are Windows Server 2003 or both are Windows Server 2008.

- The application host and proxy client must be same operating system patch or service pack level.

  For example, both are Windows Server 2003 R2 or both are Windows Server 2003 SP3.

- The application host and proxy client must be same processor architecture.

  For example, both are x86 or both are amd64/x64.

SharePoint backup and recover commands NSR_MOSS_RECOVER and NSR_MOSS_SAVE are not documented (LGTsc26417)

The command line options for the backup and recover commands NSR_MOSS_RECOVER and NSR_MOSS_SAVE were not documented in the *NetWorker Module for Microsoft Applications Release 2.1 Administration Guide*.

NSR_MOSS_SAVE

To view all of the command line options available for the save command, type:

```
nsr_moss_save.exe -?
```

Save set syntaxes

Table 5 on page 51 describes the save set syntaxes for nsr_moss_save.exe command.

Table 5 Save set syntaxes for nsr_moss_save.exe

Save set syntax	Description
NMMOSS:/<FARM_NAME>	Backup entire SharePoint Farm.
NMMOSS:/<FARM_NAME>/<WEB_APPLICATION>	Backup a single web application.
NMMOSS:/URL=<url>	Backup a SharePoint Object (Site-collection, Site or Sub-site) specified by URL.

Commands to query SharePoint

Table 6 on page 51 describes the save set syntaxes to query SharePoint.

Table 6 Commands to query SharePoint

Commands	Description
nsr_moss_save.exe [-f]	Displays Current SharePoint farm name.
nsr_moss_save.exe [-w]	Displays all web applications.
nsr_moss_save.exe [-w webapplication]	Displays all site-collections of a web application.
nsr_moss_save.exe [-u site-collectionl url]	Displays all sub-sites of a site-collection.

Usage:

nsr_moss_save.exe [-s *server*] **[-c** *client*] **[-N** *saveset*] **[-b** *pool*] **[-g** *group*] **[-l (***full | incr***)]**

Additional flags:

Optimized=(*True|False***)**

NSR_MOSS_RECOVER

To view all of the command line options available for the recover command, type: **nsr_moss_recover.exe -?**

Usage:

nsr_moss_recover.exe [-fnqu] [-i {nNyYrR}] [-s *server*] **[-c** *client*] **[-t <***date | "l locale_date***">] [-d** *staging-location*] **[-W** *web-application*] **[-T** *site-url*] **[-w** *web-url*] **[-g** *web-guid*] **[-O** *retain-identity <0|1>*] **[-V** *update-versions <1|2|3|4>*] **[-U** *update-user <0|1|2>*] **[-S** *update-security <0|1|2>*] **[-E** *halt-onwarning <0|1>*] **[-F** *halt-onnonfatal <0|1>*] **[-l** *apply-locks <0|1|2|3>*] **[dir]**

or

nsr_moss_recover.exe [-fnqu] [-i {nNyYrR}] [-I *input-file*] **[-s** *server*] **[-c** *client*] **[-t** *<date | "l locale_date">*] **[-d** *staging-location*] **[-W** *web-application*] **[-T** *site-url*] **[-w** *web-url*] **[-g** *web-guid*] **[-O** *retain-identity <0|1>*] **[-V**

update-versions <1|2|3|4>] [-U *update-user <0|1|2>*] [-S *update-security <0|1|2>*] [-E *halt-onwarning <0|1>*] [-F *halt-onnonfatal <0|1>*] [-l *apply-locks <0|1|2|3>*] [path...]

Where,

site-url: url of the site-collection

web-application: name of the destination web application in the case of recovery to alternate location

web-url: url of the web-site

web-guid: guid of the web-site

retain-identity: 0(default) - No, 1 - Yes

update-versions: 1(defualt)- Append, 2- Overwrite, 3- Ignore, 4- Error

update-user: 0(default) - None, 1 - Replace, 2- ImportAll

update-security: 0(default) - None, 1 - WssOnly, 2- All

halton-warning: 0(default) - No, 1 - Yes

halton-nonfatal: 0(default) - No, 1 - Yes

apply-locks: 0(default) - Read Unlocked/Write Unlocked, 1 - Read Unlocked/Write Locked, 2 - Read Locked/Write Unlocked, 3 - Read Locked/Write Locked

Search for 'Object type=Folder' in SharePoint backup does not display all the folders (LGTsc26494)

When using the NMM GUI to search a SharePoint backup for an Object type=Folder, using the wild card * in the name field, only the lowest, most nested folder in the folder hierarchy is displayed. This may prevent you from locating and selecting folders within the folder hierarchy because they are not displayed. There are two workarounds available.

Workaround #1

This workaround allows you to see and select the items for recovery

1. Browse for the folder object in the NMM UI, and select it for recovery.
2. Click **Start Recovery**.

Workaround #2

This workaround allows you to select and mark items for recovery, but you will not be able to see all of the folders.

1. Perform a search for the item, selecting **Folder** as the object type and * as the search criteria.

   The search results will display the lowest nested folder.
2. Select this item. When you select this item, the parent folders will automatically be selected.
3. Click **Start Recovery**.

NMM incremental backup fails for document in SharePoint Data Connection Library (LGTsc27989)

In some circumstances an incremental backup of a document in a Data Connection Library may fail with an error, "Could not find objects to back up."

This error may occur in the following circumstance:

1. A user creates a Data Connection Library list.
2. The user creates a folder, and uploads one or more documents to that folder.
3. The user performs a backup of the top level site.
4. The user uploads another document into the same folder.
5. The user performs an incremental backup and it fails with the error, "Could not find objects to back up."

This error only appears to occur when performing an incremental backup of a document added to a folder in a Data Connection Library, after backup of the top level site.

Workaround

If this error occurs, perform a full backup of the Data Connection Library or top level site.

Windows SharePoint Services 3.0 cumulative update package required to fix backup issues (LGTsc27991)

A Windows SharePoint Services 3.0 cumulative update package must be installed to correct backup performance and error issues. Failure to install this package may lead to unusually long backup times for large sites, and backup timeout errors.

You can download the KB961755 hotfix from Microsoft support, at http://support.microsoft.com/kb/961755. The Microsoft support article "Description of the Windows SharePoint Services 3.0 cumulative update package: February 24, 2009" provides more information and download instructions.

Technical notes

NetWorker Module for Microsoft Applications and EMC CLARiiON Implementing Proxy Node Backups Technical Notes provides details on how to deploy EMC NetWorker Module for Microsoft Applications in a proxy backup configuration with EMC CLARiiON.

Documentation

Related documents include:

- *EMC Module for Microsoft Applications Release 2.1 Administration Guide*
- *EMC Module for Microsoft Applications Release 2.1 Installation Guide*
- *EMC NetWorker Administration Guide*
- *EMC NetWorker Installation Guide*
- *EMC NetWorker Release Notes*
- *EMC Information Protection Software Compatibility Guide*

- *EMC License Manager Installation and Administration Guide*
- *EMC Symmetrix Solution Enabler Quick Reference Guide*

Note: For updated disaster recovery information, consult the *EMC Module for Microsoft Applications Release 2.1 Administration Guide*.

Software media, organization, and files

Information on software media, organization, and files is provided in the *EMC Module for Microsoft Applications Release 2.1 Installation Guide.*

Installation

The *EMC Module for Microsoft Applications Release 2.1 Installation Guide* contains details on installation of the NMM Client.

Note: Before performing a NMM client software upgrade, remove all existing snapshots. Also, ensure that PowerSnap snapshot entries are deleted before upgrading. Delete PowerSnap entries using the PowerSnap Client SnapManager or **nsrnapadmin**.

Troubleshooting and getting help

EMC support, product, and licensing information can be obtained as follows.

Product information — For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the EMC Powerlink™ website (registration required) at:

`http://Powerlink.EMC.com`

Technical support — For technical support, go to EMC Customer Service on Powerlink. To open a service request through Powerlink, you must have a valid support agreement. Please contact your EMC sales representative for details about obtaining a valid support agreement or to answer any questions about your account.