

SnapManager® 3.1.1 for Microsoft® Exchange Release Notes

Network Appliance, Inc.
495 East Java Drive
Sunnyvale, CA 94089 USA
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: <http://www.netapp.com>

Part number 215-01578_A0
October 2005

Copyright and trademark information

Copyright information

Copyright © 1994—2005 Network Appliance, Inc. All rights reserved. Printed in the U.S.A.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted Network Appliance material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETWORK APPLIANCE “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL NETWORK APPLIANCE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

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

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

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp, the Network Appliance logo, the bolt design, NetApp—the Network Appliance Company, DataFabric, FAServer, FilerView, MultiStore, NearStore, NetCache, SecureShare, SnapManager, SnapMirror, SnapMover, SnapRestore, SnapVault, SyncMirror, and WAFL are registered trademarks of Network Appliance, Inc. in the United States, and/or other countries. Data ONTAP, gFiler, Network Appliance, SnapCopy, Snapshot, and The Evolution of Storage are trademarks of Network Appliance, Inc. in the United States and/or other countries and registered trademarks in some other countries. ApplianceWatch, BareMetal, Camera-to-Viewer, Center-to-Edge, ComplianceClock, ComplianceJournal, ContentDirector, EdgeFiler, FlexClone, FlexVol, FPolicy, HyperSAN, InfoFabric, LockVault, Manage ONTAP, NOW, NOW NetApp on the Web, ONTAPI, RAID-DP, RoboCache, RoboFiler, SecureAdmin, Serving Data by Design, SharedStorage, Simulate ONTAP, Smart SAN, SnapCache, SnapDirector, SnapDrive, SnapFilter, SnapLock, SnapMigrator, SnapSuite, SnapValidator, SohoFiler, vFiler, VFM, Virtual File Manager, VPolicy, and Web Filer are trademarks of Network Appliance, Inc. in the United States and other countries. NetApp Availability Assurance and NetApp ProTech Expert are service marks of Network Appliance, Inc. in the United States. Spinnaker Networks, the Spinnaker Networks logo, SpinAccess, SpinCluster, SpinFS, SpinHA,

SpinMove, SpinServer, and SpinStor are registered trademarks of Spinnaker Networks, LLC in the United States and/or other countries. SpinAV, SpinManager, SpinMirror, SpinRestore, and SpinShot are trademarks of Spinnaker Networks, LLC in the United States and/or other countries.

Apple is a registered trademark and QuickTime is a trademark of Apple Computer, Inc. in the United States and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the United States and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the United States and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

Network Appliance is a licensee of the CompactFlash and CF Logo trademarks.

Network Appliance NetCache is certified RealSystem compatible.

Topics covered

These release notes describe SnapManager® 3.1.1 for Microsoft® Exchange. The following topics are covered:

- ◆ “[Product overview](#)” on page 2
- ◆ “[System requirements](#)” on page 4
- ◆ “[Upgrade information](#)” on page 6
- ◆ “[New features](#)” on page 7
- ◆ “[Bug fixes](#)” on page 14
- ◆ “[Known issues](#)” on page 15
- ◆ “[Disaster recovery by relocating Exchange virtual servers to a different Windows cluster](#)” on page 22

Product overview

This section provides an overview of SnapManager 3.1.1 for Microsoft Exchange.

Features and enhancements

SnapManager 3.1.1 for Microsoft Exchange includes all the features of SnapManager 3.1, plus several new features and bug fixes.

New features: SnapManager 3.1.1 introduces the following new features:

- ◆ Support for Microsoft Exchange 2003 Service Pack 2
- ◆ Option to throttle Eseutil.exe database checksum verification
This feature requires Exchange 2003 Service Pack 2 and is described in “[New features](#)” on page 7.
- ◆ Ability to restore databases in a clustered Exchange virtual server without taking offline the cluster physical disk resource or the Exchange virtual server
This feature requires SnapDrive 3.2 and is described in “[New features](#)” on page 7.

Previously, SnapManager 3.1 introduced the following features:

- ◆ Support for Microsoft Exchange 5.5 on Windows® 2000 Server
- ◆ Support for Microsoft Exchange 2003 Service Pack 1
- ◆ Support for Microsoft Windows Server 2003 Standard Edition
- ◆ Enhanced physical integrity verification to include transaction log verification in addition to database verification
- ◆ Optional rather than mandatory transaction log sequence verification, for faster restores

Bug fixes: This release of SnapManager fixes several bugs, listed and briefly described in “[Bug fixes](#)” on page 14.

Known issues and their workarounds are described in “[Known issues](#)” on page 15.

New information

These release notes include a description of “[Disaster recovery by relocating Exchange virtual servers to a different Windows cluster](http://now.netapp.com/NOW/cgi-bin/software/)” on page 22. The same information is also available in NetApp Knowledge Base article KB10542, available on the NetApp on the Web (NOW) site at <http://now.netapp.com/NOW/cgi-bin/software/>.

Limitations

SnapManager 3.1.1 for Microsoft Exchange does not support the following:

- ◆ Backup and recovery of the Exchange recovery storage group
- ◆ 64-bit Windows
- ◆ NT 4.0
- ◆ Windows 2000 Server with SP3 (SP4 is now required)

System requirements

The following table shows the system requirements for SnapManager 3.1.1 for Microsoft Exchange.

Note

For the most current list of system requirements, see the SnapManager 3.1.1 for Microsoft Exchange Product Description Page on the NOW site at <http://now.netapp.com/NOW/cgi-bin/software/>.

Component	Requirement for hosts running Windows 2000 Server	Requirement for hosts running Windows Server 2003
Operating system on the NetApp storage system	See the SnapDrive system requirements.	See the SnapDrive and NetApp VSS Hardware Provider system requirements.
SnapDrive	One of the following versions of SnapDrive: ◆ SnapDrive 3.0R2 ◆ SnapDrive 3.1, 3.1.1, or 3.1.1R1 ◆ SnapDrive 3.2 Note SnapDrive 3.2 is required to support the new SnapManager ability restore databases in a clustered Exchange virtual server without taking offline the cluster physical disk resource or the Exchange virtual server. For detailed information about enabling this feature, see “Ability to restore databases in a clustered Exchange virtual server without taking offline the cluster physical disk resource or the Exchange virtual server” on page 13.	
NetApp VSS Hardware Provider	N/A	NetApp VSS Hardware Provider 1.0 NetApp VSS Hardware Provider, a separate installation package for use with SnapDrive 3.0R2, is included with SnapDrive version 3.1 and later.

Component	Requirement for hosts running Windows 2000 Server	Requirement for hosts running Windows Server 2003
Microsoft Exchange	One of the following Standard or Enterprise editions of Microsoft Exchange: ◆ Exchange 2003 with SP2 ◆ Exchange 2003 with SP1 ◆ Exchange 2003 ◆ Exchange 2000 with SP 3 ◆ Exchange 5.5 with SP4	One of the following Standard or Enterprise editions of Microsoft Exchange: ◆ Exchange 2003 with SP2 ◆ Exchange 2003 with SP1 ◆ Exchange 2003
Host operating system	One of the following versions of Microsoft Windows: ◆ Windows 2000 Server with SP4 ◆ Windows 2000 Advanced Server with SP4	One of the following versions of Microsoft Windows: ◆ Windows 2003 Server Standard Edition ◆ Windows 2003 Server Standard Edition with SP1 ◆ Windows 2003 Server Enterprise Edition ◆ Windows 2003 Server Enterprise Edition with SP1
Microsoft Windows hotfixes	See the SnapDrive system requirements.	See the SnapDrive and NetApp VSS Hardware Provider system requirements.
Other host system requirements	The host system used to run SnapManager 3.1.1 for Microsoft Exchange must meet the hardware and software system requirements for SnapDrive. Note These requirements are not necessary for SnapManager installations used for remote administration only. See your SnapDrive documentation for complete details about the following system requirements: ◆ Host hardware platform ◆ LUN access protocol software	

Upgrade information

If you are upgrading to SnapManager 3.1.1 from a previous release of SnapManager for Microsoft Exchange, read the information in this section.

Upgrade paths

There are two basic upgrade paths to SnapManager 3.1.1:

Upgrading from release 1.1 or newer: You can upgrade directly to SnapManager 3.1.1 for Microsoft Exchange from SnapManager for Microsoft Exchange 2000 1.1, after you have upgraded your NetApp storage system software and host system software to meet the SnapManager system requirements.

Upgrading from a release earlier than 1.1: If you are running a release earlier than 1.1, you need to upgrade to release 1.1 first and then upgrade to release 3.1.1. For information about upgrading to release 1.1, read the documentation for the SnapManager 1.1 release on the NOW site at <http://now.netapp.com/NOW/cgi-bin/software>.

Changes to the Run Command After Operation feature

If you are upgrading from SnapManager 3.0 for Microsoft Exchange, and you have been using the Run Command After Operation feature, you might need to update your default Run Command After Operation command arguments.

In SnapManager 3.0 for Microsoft Exchange, each SnapManager variable was enclosed in double quotes automatically. However, this could cause problems when used with `rsh` or other environments that do not handle double quotes.

After you upgrade from SnapManager 3.0 for Microsoft Exchange, you will notice a change to the syntax of the SnapManager variables contained in your default Run Command After Operation command arguments: the SnapManager variables other than `$SnapInfoPath` are no longer enclosed in quotes. If this causes problems (for example, if you have spaces in your SnapInfo pathname), you can open the Run Command After Operation window and add the quotes manually to the Command Arguments string.

When you create a brand new Command Argument string by selecting the appropriate SnapManager variable and clicking Select, the double quotes will be automatically added to the SnapInfoPath variable only. The double quotes will be visible in the Command Arguments field; you can manually edit them if necessary.

New features

SnapManager 3.1.1 introduces the following new features:

- ◆ [“Option to throttle Eseutil in checksum verification mode”](#)
- ◆ [“Ability to restore databases in a clustered Exchange virtual server without taking offline the cluster physical disk resource or the Exchange virtual server”](#)

Option to throttle Eseutil in checksum verification mode

When installed with Exchange 2003 SP2, SnapManager 3.1.1 supports the ability to decrease the throughput rate of database checksum verification operations. For more information, see the following topics:

- ◆ [“About database verification load”](#) on page 7
- ◆ [“Requirements”](#) on page 7
- ◆ [“How the database verification throttling feature works”](#) on page 8
- ◆ [“The effect of using different throttling values”](#) on page 8
- ◆ [“How to choose the sleep interval”](#) on page 8
- ◆ [“How to configure the throttling option”](#) on page 11

About database verification load: Database verification can place a significant load on both the Exchange server and the NetApp filer. For this reason, verification can degrade Exchange Server response, particularly during peak work hours. With previous releases of SnapManager, there are two options for distributing this load by separating database verification database backup operations: **deferred database verification** and **remote database verification**. These options are described in the *SnapManager 3.1 for Microsoft Exchange Installation and Operations Guide*.

SnapManager 3.1.1 supports a third option for managing database verification, that you can combine with either or both of the existing options, to reduce the load even further. When installed with Microsoft Exchange 2003 Service Pack 2, SnapManager 3.1.1 supports the ability to throttle Eseutil (the Microsoft Exchange consistency checker utility) in database checksum verification mode.

Requirements: SnapManager 3.1.1 supports this feature only if installed with **Exchange 2003 SP2** or later.

Note

Attempting to use the throttling feature with earlier versions of SnapManager or Exchange will have no effect.

How the database verification throttling feature works: Exchange 2003 Service Pack 2 added a feature to `Eseutil.exe`, the Microsoft Exchange consistency checker utility, to insert artificial 1-second pauses periodically during the database physical consistency check. To support this feature, a new input parameter `/px` has been added to the checksum verification mode (`Eseutil /k`):

- ◆ The default behavior of `Eseutil /k` is unchanged.
- ◆ When the `/px` option is defined with x specified as any integer value from 1 to 2000, `Eseutil /k` artificially pauses for one second after every x I/O operations.

The effect of using different throttling values: `Eseutil.exe` reads 512 KB for each database checksum verification I/O operation. Therefore, when the `/px` option is defined with `Eseutil /k`, the maximum throughput rate for database checksum verification is decreased to the following:

$$512 \text{ KB per I/O} \times x \text{ I/Os per second} = 512 \times x \text{ KB/second}$$

The following examples illustrate the effect of using throttling values of 100, 150, 200, and 250 for x .

One-second pause interval x	Maximum possible database verification speed	
	Calculation	Maximum speed
100	$512 \text{ KB/I/O} \times 100 \text{ I/O/sec} = 51,200 \text{ KB/sec}$	50 MB/sec
150	$512 \text{ KB/I/O} \times 150 \text{ I/O/sec} = 76,800 \text{ KB/sec}$	75 MB/sec
200	$512 \text{ KB/I/O} \times 200 \text{ I/O/sec} = 102,400 \text{ KB/sec}$	100 MB/sec
250	$512 \text{ KB/I/O} \times 250 \text{ I/O/sec} = 128,000 \text{ KB/sec}$	125 MB/sec

Note

Decreasing the `Eseutil.exe` database verification throughput causes the database checksum verification to take longer to complete. This also means that a backup job that is configured with verification will also take longer to complete. However, decreasing verification throughput does not cause a backup job without verification configured to take any longer to complete.

How to choose the sleep interval: Calculate the appropriate sleep interval value to use *for each Exchange server*. This entails monitoring the read and write

performance of the LUNs on which the Exchange databases reside and then adjusting the verification throttle setting so that the average and peak physical disk performance is below the maximum values determined by Microsoft.

To calculate the Eseutil throttling value for a specific Exchange server, complete the following steps.

Step	Action
1	Launch the Windows Performance Monitor utility (also known as “perfmon”) on the machine that is the Exchange server.
2	Add the following perfmon counters for each NetApp LUN that contains an Exchange database: ◆ PhysicalDisk\Average Disk sec/Read ◆ PhysicalDisk\Average Disk sec/Write Note_____ Monitor the LUNs containing the live Exchange databases, not the LUN in snapshot that is mounted and verified by the verification process.
3	Monitor these pairs of values while a SnapManager verification job or a backup job with verification is in progress. Follow these guidelines: ◆ To monitor the SnapManager progress, watch the Backup Status window that is displayed during a manually launched backup job. ◆ If monitoring a backup with verification job, be sure to monitor the counters during the <i>verification portion</i> of the job. ◆ Multiple databases on the same Exchange server are verified sequentially, so be sure to monitor the counters for <i>all</i> of the database verifications. ◆ Monitor the counters during the busiest time of day that a verification or backup with verification job might occur.
4	The throttle setting is global, so select the reading from the database that exhibits the worst performance (highest readings).

Step	Action
5	Compare the measured values to the maximum values recommended by Microsoft. PhysicalDisk\Average Disk sec/Read: The average physical disk performance times determined by Microsoft are as follows: ◆ Average read time should be below 20ms. ◆ Maximum peak read time should be below 50ms. PhysicalDisk\Average Disk sec/Write: The maximum physical disk performance times determined by Microsoft are as follows: ◆ Average write time should be below 20ms. ◆ Maximum peak write time should be below 50ms. Note_____ These values are good guidelines during peak Exchange usage hours. During off-peak Exchange hours, higher latencies may be acceptable.
6	If the measured values exceed the maximum values recommended by Microsoft, adjust the throttle setting to decrease the verification throughput rate.

How to configure the throttling option: To configure database verification throttling, complete the following steps.

Step	Action
1	Determine which of your Windows host systems need to be configured with the <code>Eseutil</code> throttling option: ◆ Create the new <code>EseUtilThrottle</code> registry key value on every system that will be used to perform database verification. Note _____ The Windows host system that will be performing database verification is not necessarily the Exchange server itself. ◆ If a remote verification server is used, also create the <code>EseUtilThrottle</code> registry key value on the Windows host that is configured to perform the remote verifications. You can create this registry key value on <i>all</i> systems involving database verification.
2	Run the Windows registry editor.
3	Locate the following key: <pre>HKEY_LOCAL_MACHINE\SOFTWARE\Network Appliance\SnapManager for Exchange\Server</pre>
4	Under that key, create a <code>REG_DWORD</code> value with the following name: <pre>EseUtilThrottle</pre>

Step	Action
5	Double-click the newly created registry value so that the value can be changed, and then set it to a value from 0 to 2000 (decimal). Refer to the formula and example calculations in “The effect of using different throttling values” on page 8. Network Appliance has observed that using a value in the range of 100 to 250 is suitable for most environments, and 150 is often the optimum value. A value that is too low will have little to no effect on Exchange server performance. A value that is too high will shift the bottleneck to the filer. The throttling feature is disabled if the value is 0 or if the DWORD value does not exist.
6	Save the new registry setting and exit the registry editor. The setting will take effect at the next database verification operation or at the next backup operation configured with database verification.

Before each database verification, the SnapManager backup and verification report indicates whether the feature is enabled (that is, whether the registry is set and the Eseutil version is newer than 6,5,7582,0):

- ◆ If the feature is enabled, the report includes the following entry:
ESEUTIL throttling feature is enabled.
- ◆ If the feature is not enabled, the report includes the following entries:
ESEUTIL throttling feature is disabled.
ESEUTIL output will show the throttling parameter.

Ability to restore databases in a clustered Exchange virtual server without taking offline the cluster physical disk resource or the Exchange virtual server

When installed with SnapDrive 3.2, SnapManager supports the ability to restore databases in a clustered Exchange virtual server without taking offline the cluster physical disk resource or Exchange virtual server. This feature is disabled by default. To enable this feature, you can configure your environment so that LUNs are kept online during the LUN restore operation.

This feature, when enabled, applies to LUN restore operations that use the single-file SnapRestore (SFSR) method as well as to those that use the LUN clone split restore method supported with Data ONTAP™ 7.1. Keeping the LUNs online during a SnapManager restore operation minimizes downtime during restore for databases in storage groups that share a cluster group but are not being restored.

Requirement: SnapManager 3.1.1 supports this feature only if installed with SnapDrive 3.2.

To keep LUNs online during the LUN restore operation: Set the registry variable so that SnapDrive can restore the MSCS LUN without taking the LUN resource offline. For detailed instructions, see the NetApp Knowledge Base article KB10590 “Restoring a Clustered LUN Resource without Taking the LUN Resource Offline” on the NOW site, located at <http://now.netapp.com/NOW/knowledge/docs>.

Note

This must be done on all nodes of the cluster.

Bug fixes

The following table lists bugs that were fixed in SnapManager 3.1.1 for Microsoft Exchange. For more information about any of these bugs, launch your Web browser, navigate to <http://now.netapp.com/NOW/cgi-bin/bol>, type the bug ID into the “Enter Bug IDs” field, and then click Go.

Bug ID	Description
133515	When running SnapManager database verification on a remote verification server, the operation might fail.
152066	A point-in-time restore operation with Exchange 2003 on Windows Server 2003 might fail if the transaction log file directory is missing.
152161	A restore from archive operation might fail if the transaction log file directory was not restored or is missing.
157764	A backup operation that uses the unique naming convention and is configured to update SnapMirror after the backup operation might not execute the SnapMirror update and log.

Known issues

The following table lists issues known to exist in SnapManager 3.1.1 for Microsoft Exchange. For the latest information about workarounds, launch your Web browser, navigate to <http://now.netapp.com/NOW/cgi-bin/bol>, type the bug ID into the “Enter Bug IDs” field, and then click Go.

Bug ID	Description and workaround
61756	Exchange databases not remounted after a restore or being brought offline and back online. For an Exchange server in a Windows cluster, SnapManager must offline the physical disk resource that will be restored from snapshot as part of the SnapManager Restore operation. The Exchange databases that will be restored by this SnapManager Restore operation are configured temporarily not to be automatically mounted at startup. After these Exchange databases are restored from snapshot, SnapManager again configures them for automatic mount at startup. If the Active Directory object that controls the startup properties for the Exchange databases does not get updated properly, the Exchange databases remain unmounted after the completion of the SnapManager Restore operation or after the Exchange Information Store resource is brought offline and back online. Workaround: Manually mount the Exchange databases after the SnapManager Restore operation has been completed. Disable (uncheck) the “Do not mount this store at startup” option for the restored Exchange databases using the Exchange System Manager.

Bug ID	Description and workaround
80426	Server throws an exception after SnapDrive dismounted the snapshot during database verification. SnapManager server might throw an exception during database verification. This problem might occur after SnapDrive dismounts the LUN backed by a snapshot. If you are using SnapManager for Exchange 2000 version 1.1 or earlier, you see the following error: “Failed to create report file. Error Code: 0x80070020. The process cannot access the file because it is being used by another process.” Workaround: Reboot the Exchange Server if it happens repeatedly. The SMESrvr.exe process might become orphaned and contribute to this problem. SMESrvr.exe should not be running on the Exchange server without SnapManager.exe or Snapbackup.exe also running. Use the following procedure to determine whether the SMESrvr.exe process has become orphaned: Close the SnapManager application and start Task Manager. If SMESrvr.exe is running, identify whether the following conditions are true: ◆ SMESrvr.exe 0% CPU utilization for several minutes ◆ SnapManager.exe process is not running ◆ SnapBackup.exe process is not running ◆ There are no SnapManager backup or restore jobs scheduled to run at this time If all four of the above items are true, it is likely that the SMESrvr.exe process is orphaned. Use Task Manager to end the SMESrvr.exe process or reboot the Exchange server.
96624	If a SnapManager backup is stopped before it is complete, an SMTP notification is never sent. This is expected behavior, because it is at the end of the process that a success or failure notification is sent. Workaround: To prevent the job from being killed by the scheduler, ensure that the scheduler allows the job to run for at least the amount of time that it takes to be completed, plus a little extra time.

Bug ID	Description and workaround
113227	Restores might fail with error code c00413E3 or 8000ffff with MExchangeIS Event ID 9518 if there are more than 1008 logs to be recovered. Restores might fail with SnapManager error c00413E3 and error message “Error Code 8000ffff Description: The action could not be completed because the Microsoft Exchange Information Store service is unavailable. Be sure the service is running and you have network connectivity to the Microsoft Exchange Server computer. ID no: c1041721 Microsoft CDO for Exchange Management” in the SnapManager report. From Application Event Log, an MExchangeIS event id 9518 is logged with “Error 0xfffffd9a (-614) Initialization of Jet failed.” Workaround: 1. Make sure that all the databases are in a clean shutdown state. You can do this by running <code>eseutil /mh</code> on each database file and checking the database state in the <code>eseutil.exe</code> output. 2. Rename the transaction log folder for the affected storage group to a new name and create a new transaction log directory with the original name. (Alternatively, you can move all the transaction logs in this transaction log directory to a new location.) 3. Use Exchange System Manager to mount all the databases in the storage group. Note This behavior is due to a bug in Microsoft Exchange Server. See Microsoft KB Article 834154 for more information.
133645	For both Microsoft Exchange 2000 and Microsoft Exchange 2003 installed on Windows 2000, the Time of Last Full Backup field is not updated when SnapManager performs a backup. Workaround: None.

Bug ID	Description and workaround
135029	The <i>SnapManager for Exchange Installation and Administration Guide</i> for SnapManager 3.0 and 3.1 does not explain how to differentiate between a filer-side license and a server-side license in SnapManager for Microsoft Exchange. The missing information is relevant to the “SnapManager license options” paragraphs in the <i>SnapManager for Microsoft Exchange Installation and Administration Guide</i>. For version 3.0, see page 19. For version 3.1, see page 20. There are two types of license codes, described next, that can be used with SnapManager for Microsoft Exchange version 3.0 and 3.1. You only need to use one of the two license code types. The two license code types are entered in different ways, and the codes cannot be interchanged. Per-server licensing: If you purchased a per-server SnapManager license, enter the 14-character license code into the SnapManager user interface; you do not need to add a per-filer license unless you upgrade your license type. This type of license can be entered in either of two places in the user interface: ◆ You can enter the per-server license code into the Installation Wizard at installation time. ◆ After installation, you can enter the per-server license code by following these steps: a. In the SnapManager main window, go to the menu bar and then select Help > About SnapManager. b. In the About SnapManager dialog box, select Update License. c. In the Update Server-Side License dialog box, enter the license code in the Server-Side License field and then click OK. Filer licensing: If you purchased a per-filer SnapManager license, enter the seven-character license code directly on the filer using the filer's <code>license add</code> command; you do not need to enter a per-server license code in the SnapManager GUI or Installation Wizard. For detailed information about the license commands, see the <i>Data ONTAP Software Setup Guide</i> and the <i>Data ONTAP System Administration Guide</i> for your version of Data ONTAP.

Bug ID	Description and workaround
140646	The <i>SnapManager for Exchange Installation and Administration Guide</i> does not explain that, for versions 3.0 and 3.1, the log volume can contain two snapshots per backup when used with Microsoft Exchange 2003 on Windows Server 2003. When SnapManager for Exchange is used in conjunction with Microsoft Exchange Server 2003 on a Windows Server 2003, it uses the Microsoft Volume Shadow Copy Service (VSS) subsystem to provide backup and restore functionality. If, in this environment, the SnapInfo directory has been configured on the same volume as the transaction log, then a single SnapManager backup creates two snapshots on that volume instead of just one: 1. A VSS snapshot in the transaction log This <code>exchsnap__*</code> snapshot is created at the same time as the corresponding database snapshot of the same name. 2. The SnapInfo backup snapshot for protecting the SnapInfo directory This is the <code>eloginfo__*</code> snapshot created at the end of the SnapManager backup. This snapshot is used for transaction log verification and for backup protection. If the backup set was archived, this snapshot can be used for a SnapManager restore operation. Creation of these two snapshots is expected behavior when SnapManager uses VSS for backup and restore functionality and SnapInfo is on the same volume as the transaction log. Note _____ Volume size is unchanged because the backup set still captures the same total number of changed blocks on the filer, even though there are two snapshots created instead of one. _____

Bug ID	Description and workaround
140646 (cont.)	For example, suppose the SnapInfo directory is on the same LUN as the transaction log in an Exchange Server 2003 environment with Windows Server 2003. The console output shows that the transaction log volume contains snapshots with the same name as the Exchange database snapshot: <pre>Volume netappnj1_logs working... date name ----- Aug 30 01:04 eloginfo__mailnj1__recent Aug 30 01:00 exchsnap__mailnj1__recent Aug 29 13:03 eloginfo__mailnj1_08-29-2004_13.00.00__daily Aug 29 13:00 exchsnap__mailnj1_08-29-2004_13.00.00__daily Aug 29 01:04 eloginfo__mailnj1_08-29-2004_01.00.00 Aug 29 01:00 exchsnap__mailnj1_08-29-2004_01.00.00 Aug 28 13:03 eloginfo__mailnj1_08-28-2004_13.00.00__daily Aug 28 13:00 exchsnap__mailnj1_08-28-2004_13.00.00__daily Aug 28 01:04 eloginfo__mailnj1_08-28-2004_01.00.00 Aug 28 01:00 exchsnap__mailnj1_08-28-2004_01.00.00 Aug 27 15:36 eloginfo__mailnj1_08-27-2004_15.30.15 Aug 27 15:30 exchsnap__mailnj1_08-27-2004_15.30.15 Aug 20 15:35 eloginfo__mailnj1_08-20-2004_15.27.35 Aug 20 15:27 exchsnap__mailnj1_08-20-2004_15.27.35</pre> If you are not aware of the configuration details, you might expect to see only the “eloginfo__” snapshots and not the “exchsnap__” snapshots. Workaround: None.

Bug ID	Description and workaround
146295	The <i>SnapManager 3.1 for Exchange Installation and Administration Guide</i> does not explain that two unassigned drive letters are needed to perform remote verification for more than one storage group in a single job. In all other situations, only one unassigned drive letter is required. The missing information is relevant to the last paragraph of the section “Drive letter limitations and individual database restoration” on page 25. The extra drive letter is for mounting the LUN in a snapshot that stores the SnapInfo directory for the purpose of transaction log verification (a feature introduced in SnapManager 3.1 for Microsoft Exchange). After SnapManager verifies the transaction logs for the first backup set, it does not dismount the LUN or release the assigned drive letter for this LUN. This saves an unnecessary LUN-mounting operation for the verification of the transaction log for the second backup set. Workaround: There are two options: ◆ Free a second drive letter. ◆ Schedule backup or verification jobs to verify one backup set at a time.
173498	The <i>SnapManager 3.1 for Exchange Installation and Administration Guide</i> contains a misleading statement regarding the total number of storage groups that can be configured on a Windows cluster. The misleading information is in the fourth bullet of the section “Data storage requirements for Exchange 2000 and 2003.” The bullet begins on page 25 and reads as follows: “In a Windows cluster, there are one or more Exchange virtual servers. The totals for the entire clustered system cannot exceed the specified limits. For example, there could be four Exchange virtual servers with one storage group each, or one Exchange virtual server with four storage groups, or any combination in between, as long as the maximum number of storage groups is not exceeded.” Instead, the bullet should read as follows: “In a Windows cluster, there are one or more Exchange virtual servers. The totals for the entire clustered system cannot exceed the specified limits. For example, there could be four Exchange virtual servers with one storage group each, or one Exchange virtual server with four storage groups, or any combination in between, as long as each Exchange virtual server conforms to the maximum of four storage groups per server.”

Disaster recovery by relocating Exchange virtual servers to a different Windows cluster

This section describes a disaster recovery method that consists of relocating Exchange virtual servers to a different Windows cluster. See the following topics for more information:

- ◆ [“About this method”](#) on page 22
- ◆ [“Preparing to configure the production and DR sites”](#) on page 23
- ◆ [“Configuring the production and DR sites”](#) on page 24
- ◆ [“Bringing the production site online”](#) on page 27
- ◆ [“Bringing the DR sites online”](#) on page 32
- ◆ [“Failing over to a DR site”](#) on page 34
- ◆ [“Failing back to the production site”](#) on page 39
- ◆ [“Changing the IP addresses of SMTP and HTTP virtual server cluster resources”](#) on page 55

About this method

The following paragraphs summarize a disaster recovery scenario that uses SnapManager and SnapMirror in a clustered environment.

The configuration consists of a Windows cluster with Microsoft Exchange and NetApp products at a production site along with a different but similarly configured cluster at a disaster recovery (DR) site. There are likely to be numerous DR sites, geographically remote from one another.

The Exchange data is stored on NetApp LUNs, which are asynchronously mirrored from the production site to the DR sites using NetApp SnapMirror. NetApp SnapManager for Exchange is used for Exchange backup and recovery as well as to drive the SnapMirror replication schedule. NetApp SnapDrive is used for LUN provisioning and management.

In the event of a disaster, an Exchange virtual server can fail over from the production site to a DR site and then, after the original production site has been repaired, the DR site can fail back to the production site. Exchange data that changed while running at the DR site is mirrored back to the production site and retained.

Preparing to configure the production and DR sites

Before you begin configuring your production and DR sites, ensure that you complete the prerequisite tasks described in this section.

Windows host systems: Each Windows host system must be installed with the following:

- ◆ One of the following versions of Windows:
 - ❖ Windows 2000 Advanced Server
 - ❖ Windows Server 2003 Enterprise Edition
- ◆ Exchange Server 2003
- ◆ SnapManager for Exchange 3.1 or newer
- ◆ SnapDrive 3.2D1
- ◆ A version of Data ONTAP that is supported by SnapDrive 3.2D1

Note

For faster restore times, use Data ONTAP 7.1 or later.

Windows clusters: Each Windows cluster must meet the following requirements:

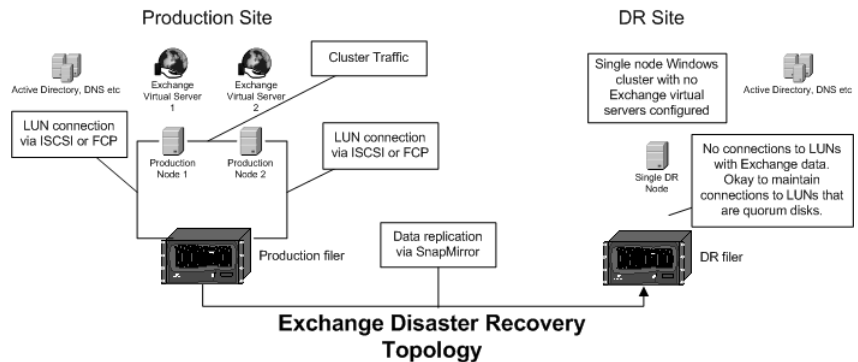
- ◆ The production and DR clusters must be in the same Active Directory site.
- ◆ The Exchange virtual server name must be maintained.

Supporting documentation: Although this document describes how to move an Exchange virtual server from one Windows cluster to another in a Microsoft and NetApp environment, it does *not* describe how to restore the supporting Windows infrastructure. For more information about Exchange disaster recovery and its dependencies, see the following Microsoft articles:

- ◆ For Exchange 2000, see Microsoft article KB326052, *White Paper - Disaster Recovery for Microsoft Exchange 2000 Server*.
- ◆ For Exchange Server 2003, see Microsoft article KB867704, *The “Exchange Server 2003 Disaster Recovery Operations Guide” is available*.

Configuring the production and DR sites

The production and DR sites can consist of one or more Windows clusters running one or more Exchange virtual servers where each cluster has one or more nodes (two nodes or more are recommended). Data storage for Exchange is provided by one or more filers. The following example shows a two-node production Windows cluster running one Exchange virtual server on each node. The DR Windows cluster contains a single node. There is one filer at each site.



The production and DR sites are set up with filer volumes of identical sizes. Initially, SnapMirror relationships are configured between the source volumes on the production site and destination volumes on the DR sites. While in production, data is mirrored from SnapMirror source volumes at the production site to SnapMirror destination volumes at each of the DR sites.

If a disaster occurs at the production site, you can fail over operations to one of the DR sites. After the original production site is repaired, the DR site can fail back to the production site and the data will be mirrored back in the opposite direction using SnapMirror.

Where to locate the quorum disks: To properly configure Windows clusters, you need to understand the proper location of quorum disks:

- ◆ Because the Windows clusters at the production site and at the DR sites are each autonomous clusters, each cluster requires its own quorum disk.
 - If you use a Data ONTAP LUN as a quorum disk, that LUN must reside on a filer at the same site where the Windows cluster itself resides:
 - ❖ For the production Windows cluster, locate the quorum disk LUN on the filer at the production site.
 - ❖ For a DR Windows cluster, locate the quorum disk LUN on a filer at that DR site.
- ◆ There is no need to mirror the quorum disk from the production filer to the DR filer. Therefore, to avoid transferring unnecessary data across a WAN, locate the quorum disk LUNs on non-mirrored filer volumes.

Tip for creating and mapping LUNs: Standardizing across all clusters (at the production site and at all DR sites) on an identical mapping of **LUN names** to **drive letters** can simplify disaster recovery activities, from initial configuration through maintenance, failover, and failback.

For example, the following mapping of LUN names and drive letters could be adopted by the database administrators at the production site and each DR site.

Drive letter	LUN name	LUN storage purpose
I:	db.lun	Microsoft Exchange databases
L:	logs.lun	Microsoft Exchange transaction logs
T:	data.lun	Microsoft Exchange “data directory”
N:	snapinfo.lun	NetApp SnapManager SnapInfo directory

Note

If you adopt the best practice of keeping detailed and up-to-date notes about your DR plans, remember to keep a printed hardcopy.

NetApp filer performance considerations: Exchange performance might be significantly lower at the DR site than at the production site:

- ◆ If the filer at the DR site is a less powerful model than the one at the production site, it will yield lower performance than the filer at the production site.
- ◆ In the event of a disaster, a single DR cluster could potentially host multiple Exchange virtual servers from more than one production cluster.

Because of this, you should be aware that Exchange performance at the DR site could be significantly lower than would be expected at the production site.

Configuration procedure: To configure the production and DR sites, complete the following steps.

Step	Action
1	At the production site, create the filer volumes. Typically, the size and number of volumes will be determined with the help of Network Appliance during the sales cycle. Volume sizing information is also available in the <i>SnapManager for Exchange Installation and Administration Guide</i> and in the <i>Exchange Best Practices Guide</i> (TR3233).
2	At the DR site, create the filer volumes. Note The SnapMirror source and destination volumes must be identical in size. The supporting infrastructure required for the Exchange virtual server, the Windows cluster, and the NetApp filer must be in place, up to date, and functioning at the DR site. This includes, but is not limited to, Active Directory, DNS, WINS, and Network connectivity.
3	Configure SnapMirror with a non-schedule. This is described in the <i>SnapDrive Installation and Administration Guide</i>, in the section “Using SnapMirror with SnapDrive.”
4	To minimize data loss, you can configure SnapDrive to replicate the transaction log volume more frequently in between SnapManager backups. This is described in the <i>SnapManager Installation and Administration Guide</i>, in the section “Using SnapMirror with SnapManager.”

Bringing the production site online

Complete the following steps at the production site.

Step	Action
1	Configure a Windows cluster and then install Windows Server on all nodes of the cluster, but do <i>not</i> install or configure Exchange yet. Note_____ The quorum disk can be a Data ONTAP LUN, but this is not a requirement. For more information, see “Where to locate the quorum disks” on page 24. For details about configuring the cluster, refer to Microsoft documentation.
2	Using the Cluster Administrator, create a cluster resource group named “Exchange” for the Exchange cluster resources. Note_____ The cluster group names of “Exchange” and “Exchange DR” are used in this document for clarity and only as examples. Using these cluster group names is not a requirement.
3	Create a new “IP address” cluster resource in the Exchange DR cluster group. Note_____ Due to the TCP/IP subnet configuration at the DR site, this IP address will probably be different from that of the production site.
4	Create a new “Network Name” cluster resource in the Exchange DR cluster group. Note_____ Later, in the procedure “Bringing the DR sites online” on page 32, you will use the same network name for the Exchange virtual server at the DR site as was in use at the production site.
5	Install SnapDrive on all cluster nodes, following the instructions in the <i>SnapDrive Installation and Administration Guide</i>.

Step	Action
6	If using iSCSI, establish an iSCSI connection from one of the production site cluster nodes to the production filer.
7	On a SnapMirror source volume on the production filer, create LUNs to store the following: ◆ Exchange databases ◆ Exchange transaction logs ◆ SnapManager SnapInfo directory To do this, complete the following steps: a. Using SnapDrive, create “shared” LUNs on a SnapMirror source volume on the filer at the production site. Refer to “Tip for creating and mapping LUNs” on page 25. b. When prompted by SnapDrive, select the Exchange cluster resource group you created in Step 2. This creates the shared physical disk resources on the cluster nodes of the production site.

Step	Action
8	On a SnapMirror source volume on the production filer, create a separate LUN to store the “Exchange data directory”: a. Using SnapDrive, create another “shared” LUN on a SnapMirror source volume on the filer at the production site. Again, refer to “Tip for creating and mapping LUNs” on page 25. b. When prompted by SnapDrive, select the Exchange cluster resource group you created in Step 2. This places the LUN in the Exchange cluster resource group created in Step 7. Later, when you create the Exchange System Attendant cluster resource for the first time, you will be prompted for this LUN. This LUN will also be used for the Exchange SMTP and MTA queues and Microsoft Search. SnapManager can be used later to configure the SMTP and MTA locations, if desired. Note_____The Microsoft Search Directory can be moved manually, as described in the Microsoft TechNet document “Working with Exchange Server 2003 Stores.”
9	Install Exchange on all nodes in the cluster and then apply any Exchange service packs to all nodes in the cluster. Note_____Install the same version of Exchange and apply the same Exchange service pack to all nodes in the production cluster. In the next procedure, “Bringing the DR sites online” on page 32, you will use this same version and service pack on all nodes in the DR cluster.

Step	Action
10	Using the Cluster Administrator, do the following: - Create a new Exchange System Attendant cluster resource in the Exchange cluster resource group. This automatically creates all of the other Exchange cluster resources. - When prompted for the Exchange “data directory,” use the separate LUN you created in Step 7. The prompt will include a drive letter and path. The drive letter will simply be the first available drive letter within the cluster resource group. Only the drive letter needs to be changed. The path can remain unmodified.
11	Install and configure SnapManager on all nodes of the cluster.
12	Make the cluster node you are working on the owner of the Exchange cluster resource group: - Use the Cluster Administrator to perform a “move group” operation. - When SnapManager prompts for a location for the MTA and SMTP files, place them on the separate LUN you created for the Exchange “data directory” in Step 7. These files need to be kept on a separate LUN from the Exchange database, transaction logs, and the SnapManager SnapInfo directory.
13	Verify that the Exchange virtual server at the production site is up and running: - Use the Cluster Administrator to make sure that the cluster resources are online. - Use the Exchange System Manager to make sure that the database is mounted.
14	Create a SnapManager backup and confirm that SnapMirror is functioning properly. There are three ways to check that SnapMirror replication occurred: ◆ View the backup report in the “SnapManager Reports tab”. ◆ View the events logged in the “Windows Application Event log”. ◆ View the SnapMirror information on the “Storage system”.

SnapManager Reports tab: Look at the backup report for the backup that was just run. The following text will appear toward the end of the report:

```
*** REQUEST SNAPMIRROR UPDATE AFTER BACKUP ***
```

```
Starting SnapMirror update...
```

```
Querying disk list for SnapMirror update...
```

```
Requesting SnapMirror update for LUN [I:] on volume [exch_db] of  
filer [exch-dr-filer]...
```

```
Request for SnapMirror update for LUN [I:] was completed  
successfully.
```

```
Requesting SnapMirror update for LUN [L:] on volume [exch_logs] of  
filer [exch-dr-filer]...
```

```
Request for SnapMirror update for LUN [L:] was completed  
successfully.
```

Windows Application Event log: This is an example of the events that might be seen when there are two volumes in use:

```
Event Type: Information  
Event Source: SnapDrive  
Event Category: SnapMirror event  
Event ID: 144
```

```
Date: 7/14/2005
```

```
Time: 2:08:47 PM
```

```
User: N/A
```

```
Computer: EXCHANGE
```

```
Description:
```

```
A SnapMirror update request to destination (exch-filer:exch_db) was  
successfully sent.
```

```
Event Type: Information  
Event Source: SnapDrive  
Event Category: SnapMirror event  
Event ID: 144
```

```
Date: 7/14/2005
```

```
Time: 2:08:50 PM
```

```
User: N/A
```

```
Computer: EXCHANGE
```

```
Description:
```

```
A SnapMirror update request to destination (exch-filer:exch_logs)  
was successfully sent.
```

Storage system: Using a web browser, bring up FilerView on the filer that is the SnapMirror destination:

- a. To bring up FilerView, enter `http://filename/na_admin` into the address field of the web browser, where *filename* is the name of the filer at the production site.

Example: `http://dr_filer/na_admin`

- b. When the page loads, click the FilerView link.
- c. Click SnapMirror and then click Manage. Information about the SnapMirror relationships is displayed.

Bringing the DR sites online

There can be numerous DR sites around the globe. To prepare the DR sites for disaster recovery, complete the following steps *at each DR site*.

Attention

Only one Exchange virtual server with a given network name can be online at a time, otherwise connectivity issues will arise.

Step	Action
1	Install Windows Server on all nodes of the cluster and then configure the default cluster group, but do <i>not</i> install or configure Exchange yet. Note_____ The quorum disk can be a Data ONTAP LUN, but this is not a requirement. For more information, see “Where to locate the quorum disks” on page 24. _____ For details about configuring the cluster, refer to Microsoft documentation.
2	Install SnapDrive on all cluster nodes, following the instructions in the <i>SnapDrive Installation and Administration Guide</i>.

Step	Action
3	If using iSCSI, establish an iSCSI connection from one of the cluster nodes at this DR site to the DR filer. Note_____ Do <i>not</i> connect to any of the LUNs that will be used by the Exchange virtual server yet. This is done later as part of the recovery procedure.
4	Install Exchange on all nodes in the cluster and then apply any Exchange service packs to all nodes in the cluster. Note_____ Be sure to use the same Exchange version and service pack that you installed on the nodes of the production cluster, described in the “Bringing the production site online” on page 27. Install the same version of Exchange and apply the same Exchange service pack to all nodes in the DR cluster.
Create the cluster resource group and install SnapManager for Exchange	
Although it saves time if you create this cluster resource group and the cluster resources prior to disaster, it is not a requirement. You can choose to postpone performing the remaining steps in this procedure until you need to fail over to this DR site.	
5	Using the Cluster Administrator, create a cluster resource group named “Exchange DR” for the Exchange cluster resources. Note_____ The cluster group names of “Exchange” and “Exchange DR” are used in this document for clarity and only as examples. Using these cluster group names is not a requirement.
6	Create a new “IP address” cluster resource in the Exchange DR cluster group. Note_____ Due to the TCP/IP subnet configuration at the DR site, this IP address will probably be different from that of the production site.

Step	Action
7	Using the Cluster Administrator, do the following: - Create a new “Network Name” cluster resource in the Exchange DR cluster group. Use the same network name for the Exchange virtual server at the DR site as was in use at the production site. - Leave the Exchange DR cluster group (or just the Network Name cluster resource) offline. It will be brought online at a later time as part of the recovery procedure. The Network Name cluster resource at the DR site <i>cannot</i> be online while the same Network Name cluster resource is online at the production site.
8	Do <i>not</i> add Exchange cluster resources yet. This is done later, as part of the recovery procedure.
9	Install SnapManager for Exchange on all nodes of the cluster, but do <i>not</i> configure it yet.

Failing over to a DR site

At the DR site to which you want to fail over, perform the following steps.

Step	Action
1	Ensure that the Exchange cluster group at the production site is offline. Note_____ Only one Exchange virtual server with a given network name can be online at a time. This is required because the virtual Exchange server on the DR cluster will be brought online with the same network name. _____

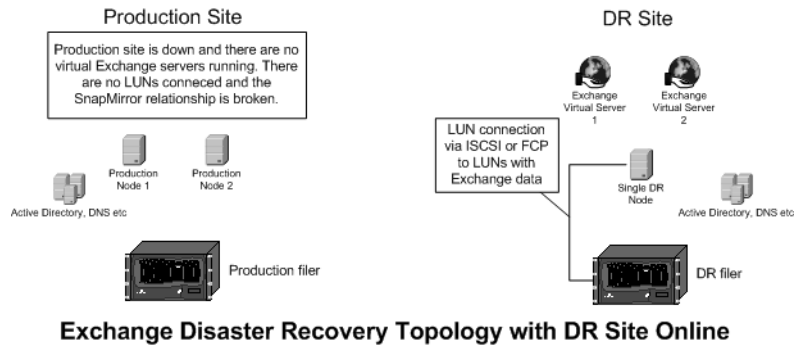
Step	Action
2	If the DR cluster will take over the Exchange services <i>within one hour</i> of the time that the production site went offline, use the Active Directory Users and Computers MMC to reset the machine account for the Exchange virtual server. If you fail to do this, you might encounter client authentication issues. Attention ————— Do <i>not</i> delete and re-create this account. Doing so will make it impossible to recover the Exchange server.
3	If the production cluster is different from the DR cluster, update the DNS record for the virtual Exchange server's network name with the IP address at the production cluster. Note ————— Until you complete the Active Directory, DNS, and WINS replication to reflect the IP change and refresh the client cache, client connectivity issues might occur.
4	Using the Cluster Administrator, check the Network Name cluster resource in the Exchange DR cluster resource group to ensure that the correct name is in use. It must exactly match the network name that was in use for the Exchange virtual server at the production site.
5	If, when this DR site was brought online, the cluster resource group was not created and SnapManager for Exchange was not installed, do so now: - Locate the procedure "Bringing the DR sites online" on page 32. - Complete all the steps in the section "Create the cluster resource group and install SnapManager for Exchange" on page 33.

Step	Action
6	Using SnapDrive, do the following: a. Reconnect to the LUNs on the SnapMirror destination volume using the same drive letters that were used at the production site and, when prompted, specify a Virtual Disk Type of “shared.” If you do not use the same drive letters that were used at the production site, the SnapManager restore operation will fail. The drive letters will not be available if they are still configured as physical disk resources for any reason, even if they are not actually mapped to LUNs. If the production Exchange server with SnapManager is still available, the drive letter to LUN mappings can be found in the SnapManager Configuration reports that reside in a special shared directory under the SnapManager installation directory. b. When prompted, select the Exchange DR cluster resource group. This creates the shared physical disk resources on the cluster nodes.
7	Using the Cluster Administrator, add the Exchange System Attendant cluster resource. This creates the remaining resources automatically and uses all of the same drive letters. You will <i>not</i> be able to change them.
8	Install and configure SnapManager on all nodes of the cluster.

Step	Action
9	Make the cluster node you are working on the owner of the Exchange cluster resource group: - Use the Cluster Administrator to perform a “move group” operation. - When SnapManager prompts for a location for the MTA and SMTP files, place them on the separate LUN you created for the Exchange “data directory.” These files need to be kept on a separate LUN from the Exchange database, transaction logs, and the SnapManager SnapInfo directory. Specify the same path for the SnapInfo directory; otherwise, the backup sets will not be visible under the SnapManager Restore tab.
10	Perform a SnapManager for Exchange restore operation with the following options selected: ◆ “Use the most recent backup set” ◆ “Up-to-the-minute restore” ◆ “Mount databases automatically after restore”
11	Verify that the virtual Exchange server on the DR cluster is up and running: - Use the Cluster Administrator to verify that the Exchange virtual server is online. - Use the Exchange System Manager to verify that the Exchange databases are mounted.
12	If the cluster is configured with SMTP or HTTP virtual server cluster resources, these resources could fail shortly after you bring them online. To prevent this from happening, follow the steps in “Changing the IP addresses of SMTP and HTTP virtual server cluster resources” on page 55 before proceeding.
13	Create a SnapManager backup immediately.

Step	Action
14	If you expect the DR cluster to remain online for any length of time, use SnapManager to configure reoccurring scheduled backup jobs. See the <i>SnapManager 3.1 for Exchange Installation and Administration Guide</i> for details.

Here is an example of a configuration at the DR site:



Failing back to the production site

To fail back to the production site, complete the following steps.

Step	Action
1	If you are using SnapManager 3.1.1 with Data ONTAP 7.1, then before proceeding with this failback procedure, be sure that any LUN clone split operations have completed. The LUN clone split functionality, introduced in Data ONTAP 7.1, supports significantly faster online snapshot restore times when using SnapManager or SnapDrive to restore. This functionality is enabled by default. To check that any LUN clone split operations have completed, use the filer's <code>lun clone split status</code> command. For detailed information about this command, see the <i>Data ONTAP 7.1 Block Access Management Guide for iSCSI and FCP</i>. Attention — If you attempt a failback procedure immediately after a failover that uses a LUN clone split (such as a dry run of a failover and failback), the LUN clone split operation could interfere with SnapMirror when trying to resynchronize the data back to the production site.
2	Create a final SnapManager backup on the DR cluster.
3	Prevent further user access by bringing the Exchange cluster resources offline, but leave the physical disk cluster resources online for the next step.

Step	Action
4	To ensure that you can bring the Exchange databases back online at the production site without first having to perform a SnapManager restore operation, verify that each Exchange database is in a consistent state. To do this, use the Exchange Server Database Utilities (Eseutil.exe) tool with the /mh option to view the header of each Exchange database and then check the value displayed next to “State” in the command output. The following example shows the Eseutil /mh command run against the database priv1.edb, located in the directory I:\EXCHSRVR\mdbdata. Only the first part of the command output is shown here: <pre> C:\Program Files\Exchsrvr\bin> eseutil /mh I:\EXCHSRVR\mdbdata\priv1.edb Microsoft(R) Exchange Server Database Utilities Version 6.5 Copyright (C) Microsoft Corporation. All Rights Reserved. Initiating FILE DUMP mode... Database: I:\EXCHSRVR\mdbdata\priv1.edb File Type: Database Format ulMagic: 0x89abcdef Engine ulMagic: 0x89abcdef Format ulVersion: 0x620,11 Engine ulVersion: 0x620,11 Created ulVersion: 0x620,11 DB Signature: Create time:05/06/2005 16:35:18 Rand:2129456 Computer: cbDbPage: 4096 dbtime: 136725 (0x21615) State: Clean Shutdown </pre> Note If the database is in a consistent state, the information output under the “Initiating FILE DUMP mode” section includes the line “State: Clean Shutdown”. Repeat this step for every database you need to bring back online at the production site.

Step	Action
5	Use the Cluster Administrator to delete the Exchange System Attendant cluster resource in the Exchange DR cluster resource group. This deletes all of the Exchange cluster resources, but the Physical Disk, IP, and Network Name resources remain intact. Attention Do <i>not</i> select the Remove Virtual Exchange Server option (available by right-clicking the Exchange DR cluster resource group). This option takes the Exchange server out of Active Directory. The following error might appear in the Windows Application Event Log: <pre> Event Type: Error Event Source: MSExchangeCluster Event Category: Services Event ID: 1027 Date: 6/23/2005 Time: 4:46:46 PM User: N/A Computer: EXCHSRVR Description: SA: System Attendant resource has been deleted improperly. The objects in Active Directory corresponding to this Exchange Virtual Server have not been removed. If you unintentionally deleted the System Attendant resource, you can restore it and its dependent resources to their original configuration by re-creating the System Attendant resource using the same parameters as before. If you want to remove the Exchange Virtual Server corresponding to this System Attendant resource, you have to re-create the System Attendant resource with the same parameters as before and then select the option "Remove Exchange Virtual Server" in the context menu of the group or System Attendant resource using the Cluster Administrator tool. For more information, click http://www.microsoft.com/contentredirect.asp. Data: 0000: 00 00 00 00 </pre> This error is expected here.

Step	Action	
6	Mirror the modified Exchange data on the SnapMirror destination volumes at the DR site back to the SnapMirror source volumes at the production site.	
	If...	Then...
	The original SnapMirror source volumes and snapshots remain intact	Go to Step 7 .
	The data on the original SnapMirror source volume or the volume itself was lost	Go to Step 17 .
If the original SnapMirror source volumes and snapshots remain intact		
7	Mirror only the changed blocks on the DR filer volumes back over to the production filer volumes. To do this, go to the original SnapMirror source filer command line interface and, for every volume that is being used by this Exchange/SnapManager configuration, issue the <code>snapmirror resync</code> command to mirror only the changed data at the DR site back to the production site. Suppose you have an Exchange/SnapManager configuration with two volumes. In this example, the filers at the production site and the DR site are named <code>prod_filer</code> and <code>dr_filer</code>, respectively, and the volume names on both filers are <code>db_vol</code> and <code>logs_vol</code>. The following sequence of two commands illustrates how the <code>resync</code> command might be issued for this example configuration: <pre>prod_filer> snapmirror resync -S dr_filer:db_vol prod_filer:db_vol</pre> <pre>prod_filer> snapmirror resync -S dr_filer:logs_vol prod_filer:logs_vol</pre>	

Step	Action
8	Monitor the status of the operation by using the <code>snapmirror status</code> command on the production filer, and do not proceed until the SnapMirror “State” is “Snapmirrored” for all volumes in this configuration. Note _____ You can also check the status of the operation using FilerView on the production filer.
9	Use SnapDrive to update the mirror. You can do this using either the SnapDrive graphical user interface (MMC) or the SnapDrive command-line interface (<code>sdcli.exe</code>). Only one mirror update per filer volume is required; it is not necessary to perform an update for each drive letter. When SnapDrive is used to perform a SnapMirror update, updating a single LUN on a given volume actually updates all of the LUNs on the volume.
10	Monitor the status of the operation by using the <code>snapmirror status</code> command on the production filer, and do not proceed until the SnapMirror “State” is “Snapmirrored” for all volumes in this configuration.
11	At the production filer, break the reverse SnapMirror relationship. You can do this using either the <code>snapmirror break</code> command or FilerView. The data that changed at the DR site is now mirrored back to the production site.
12	Break the “resync” mirror in the reverse direction.

Step	Action
13	Reinstate the original SnapMirror relationship. To do this, issue another <code>snapmirror resync</code> command, but this time from the DR filer. The following sequence of two commands illustrates how the <code>snapmirror resync</code> command might be issued. Following is an example of how this command might look using the example filer and volume names used in Step 7. <pre>dr_filer> snapmirror resync db_vol dr_filer> snapmirror resync logs_vol</pre>
14	Confirm that the SnapMirror relationship has been re-created in the original direction: - Open a web browser on the filer that is the SnapMirror destination. - To bring up FilerView, enter <code>http://filename/na_admin</code> into the address field of the web browser, where <i>filename</i> is the name of the filer at the production site. For the example filer names used in Step 7, the URL would be <code>http://prod_filer/na_admin</code>. - After the page loads, click the FilerView link. - Click SnapMirror and then click Manage. Information about the SnapMirror relationships displays. - Be sure that the “State” is “Snapmirrored.”
15	Go to Step 23 to finish the failback to the production site.

Step	Action	
If the data on the original SnapMirror source volume or the volume itself was lost		
16	If...	Then...
	Only the data on the original source volume was lost	Go to Step 17 .
	The volume itself was lost	Do the following: a. Recreate the original SnapMirror source volume. b. Go to Step 17 .
17	Create a new SnapMirror relationship in the reverse direction (from the SnapMirror destination volume at the DR site back to the SnapMirror source volume at the production site) and then initialize the mirror. This transfers all data from the original SnapMirror destination volume at the DR site back to the original SnapMirror source volume at the production site. This can be done using the filer’s command line or by using the FilerView graphical user interface. To do this using FilerView, complete the following steps: a. Open a web browser on the filer that is the SnapMirror destination. b. To bring up FilerView, enter <code>http://<i>filename</i>/na_admin</code> into the address field of the web browser, where <i>filename</i> is the name of the filer at the production site. For the example filer names used in Step 7, the URL would be <code>http://prod_filer/na_admin</code>. c. After the page loads, click the FilerView link. d. Click SnapMirror and then click Manage. Information about the SnapMirror relationships displays. e. Be sure that the “State” is “Snapmirrored.”	

Step	Action
18	Using SnapDrive, update the mirror. This can be done using the SnapDrive GUI (MMC) or the command line (sdcli.exe). It is not required that an update be performed for each drive letter. Rather, only one update per filer volume is required. When SnapDrive is used to perform a SnapMirror update, updating a single LUN on a given volume actually updates all of the LUNs on the volume.
19	Confirm that all data has been mirrored back to the repaired original SnapMirror source volume.
20	Break the mirror using the <code>snapmirror break</code> command or FilerView.
21	Un-configure the reverse SnapMirror relationship. This can be done using the filer's a line or by using the FilerView graphical user interface. To do this using FilerView, complete the following steps: - Open a web browser on the filer that is the SnapMirror destination. - To bring up FilerView, enter <code>http://<i>filename</i>/na_admin</code> into the address field of the web browser, where <i>filename</i> is the name of the filer at the production site. For the example filer names used in Step 7, the URL would be <code>http://prod_filer/na_admin</code>. - After the page loads, click the FilerView link. - Click SnapMirror and then click Manage. Information about the SnapMirror relationships displays.

Step	Action
22	Reestablish the original SnapMirror relationship in the original direction so that data from the production filer is mirrored to the DR filer. This can be done using the filer's <code>snapmirror resync</code> command or by using the FilerView graphical user interface. Perform this task on the DR filer. - Open a web browser on the filer that is the SnapMirror destination. - To bring up FilerView, enter <code>http://<i>filename</i>/na_admin</code> into the address field of the web browser, where <i>filename</i> is the name of the filer at the production site. For the example filer names used in Step 7, the URL would be <code>http://dr_filer/na_admin</code>. - After the page loads, click the FilerView link. - After FilerView loads, click “SnapMirror” and then click “Manage.” Information about the SnapMirror relationships is displayed. - Create a SnapMirror relationship and then initialize it. - Be sure that the “State” is “Snapmirrored.”
Fail back to the production site	
23	Launch the Cluster Administrator on one of the nodes at the DR site: - Bring the Network Name and IP address cluster resources offline in the Exchange DR cluster resource group. After the original mirror is reestablished, the DR cluster's physical disk resources show as failed. - Use the Cluster Administrator to delete these failed cluster resources.

Step	Action	
24	If the DR cluster will take over the Exchange services <i>within one hour</i> of the time that the production site went offline, use the Active Directory Users and Computers MMC to reset the machine account for the Exchange virtual server. If you fail to do this, you might encounter client authentication issues. Attention _____ Do <i>not</i> delete and re-create this account. Doing so will make it impossible to recover the Exchange server.	
25	If the production cluster is different from the DR cluster, update the DNS record for the virtual Exchange server’s network name with the IP address at the production cluster. Note _____ Until you complete the Active Directory, DNS, and WINS replication to reflect the IP change and refresh the client cache, client connectivity issues might occur.	
26	Verify that the DR site is in the same state that it was in prior to the disaster: a. Use the Cluster Administrator to verify that the Exchange DR cluster group is ready. b. Use the filer console or FilerView to verify that the original SnapMirror relationship is back in place.	
27	To complete the failback, bring back online the LUNs belonging to the Exchange virtual server and the original MSCS cluster group.	
	If...	Then...
	The original Windows cluster at the production site was not lost	Proceed to “ Clean up the cluster physical disk resources ” on page 49.
	The original Windows cluster at the production site was lost	Proceed to “ Recreate the cluster resource group and the Exchange virtual server ” on page 52.

Clean up the cluster physical disk resources: Follow these steps to complete the failback if the Windows cluster at the production site is operational and both the Exchange cluster resource group and the Exchange cluster resources exist.

In this case, the cluster physical disk resources need to be cleaned up in case the cluster physical disk resources are in a failed state at the production site.

Step	Action
1	Using the Cluster Administrator, do the following: - Bring up the properties page for the Exchange System Attendant cluster resource. - Remove the dependencies for all but one physical disk resource (LUN). - Save the changes and exit the dialog box. The Exchange System Attendant cluster resource requires a dependency on at least one physical disk resource. This step will allow you to delete all but one of the physical disk resources.
2	If any of the LUNs that were removed as dependencies are still mounted, use SnapDrive to disconnect them
3	Using SnapDrive, do the following: - Reconnect to the LUNs on the SnapMirror source volume using the same drive letters as before and, when prompted, specify a Virtual Disk Type of “shared.” The drive letters will not be available if they are still configured as physical disk resources for any reason, even if they are not actually mapped to LUNs. - When prompted, select the Exchange cluster resource group. This creates the shared physical disk resources on the cluster nodes. - Connect all of the LUNs except the one that was left as a dependency in the previous step.

Step	Action
4	Using the Cluster Administrator, do the following: - Bring up the properties page again for the System Attendant cluster resource. - Replace the reconnected LUNs as dependencies and remove the one that was left over from last time. - Save the changes and exit the dialog box.
5	Using SnapDrive, do the following: - Reconnect the final LUN, using the same drive letter as before and, when prompted, specify a Virtual Disk Type of “shared.” The drive letters will not be available if they are still configured as physical disk resources for any reason, even if they are not actually mapped to LUNs. - When prompted, select the Exchange cluster resource group. This creates the shared physical disk resources on the cluster nodes.
6	Go back to the Cluster Administrator and replace the System Attendant dependency on the last LUN.
7	Verify that the configuration is correct by running through the SnapManager Configuration Wizard. Be sure to save any changes if they need to be made.
8	If the cluster is configured with SMTP or HTTP virtual server cluster resources, these resources could fail shortly after you bring them online. To prevent this from happening, follow the steps in “ Changing the IP addresses of SMTP and HTTP virtual server cluster resources ” on page 55.
9	Using the Cluster Administrator, bring the Exchange cluster group online.

Step	Action
10	If the MS Search Instance cluster resource fails to come online, use SnapDrive to restore the LUN that was configured for the Exchange “data directory.” These files need to be kept on a separate LUN from the Exchange database, transaction logs, and the SnapManager SnapInfo directory. Choose the most recent snapshot with the “e_loginfo__” prefix. Note The LUN containing the data directory is not restored as part of a SnapManager restore operation.
11	Perform a SnapManager for Exchange restore operation using the snapshot you created at the beginning of the failback procedure and with the following options selected: ◆ “Use the most recent backup set” ◆ “Up-to-the-minute restore” ◆ “Mount databases automatically after restore” Note If the database was verified to be in a “Clean Shutdown” state after Exchange was taken offline on the DR cluster, you can forgo the SnapManager restore.
12	Verify that the virtual Exchange server on the production cluster is up and running: a. Use the Cluster Administrator to verify that the Exchange virtual server and the cluster resources are online. b. Use the Exchange System Manager to verify that the Exchange databases are mounted.
13	Continue with the recurring scheduled backup jobs that were in place prior to the failover.

Recreate the cluster resource group and the Exchange virtual

server: Follow these steps to complete the failback if the Windows cluster at the original production site was lost and needs to be rebuilt from scratch.

In this case, the cluster resource group and the Exchange virtual server have to be re-created.

Step	Action
1	Install Windows Server on all nodes of the cluster.
2	Configure the default cluster group so that you have a working cluster without Exchange. Note _____ The quorum disk can be a NetApp LUN, but this is not a requirement. _____ For detailed information about configuring the cluster, refer to Microsoft documentation.
3	Using the Cluster Administrator, create Exchange cluster resource group.
4	Install SnapDrive on all cluster nodes, following the instructions in the <i>SnapDrive Installation and Administration Guide</i> .
5	If using iSCSI, establish an iSCSI connection from one of the cluster nodes at the production site to the production filer.
6	Using SnapDrive, perform the following steps: - Reconnect to all of the LUNs using the original drive letters and, when prompted, specify a Virtual Disk Type of “shared.” - Place the LUNs in the Exchange cluster resource group. This creates the shared physical disk resources on the cluster nodes.
7	Install Exchange plus any service packs on all nodes of the cluster. The same service pack must be applied that was in use at the original production cluster and the DR cluster.
8	Using the Cluster Administrator, create an “IP Address” cluster resource in the Exchange cluster group.

Step	Action
9	If this IP address is different from that of the DR cluster or the original production cluster, update the DNS record for the virtual Exchange server's network name. Note Until you complete the Active Directory, DNS, and WINS replication to reflect the IP change and refresh the client cache, client connectivity issues might occur.
10	Using the Cluster Administrator, do the following: a. Create a Network Name cluster resource in the Exchange cluster resource group, using the same Exchange server name as the original cluster and DR cluster. b. Create a new Exchange System Attendant cluster resource in the Exchange cluster resource group. This automatically creates all of the other Exchange cluster resources. c. When prompted by Exchange, specify the same drive letter for the system directory.
11	If the cluster is configured with SMTP or HTTP virtual server cluster resources, these resources could fail shortly after you bring them online. To prevent this from happening, follow the steps in “Changing the IP addresses of SMTP and HTTP virtual server cluster resources” on page 55 before proceeding.
12	Install and configure SnapManager on all nodes of the cluster.

Step	Action
13	Perform a SnapManager for Exchange restore operation using the snapshot you created at the beginning of the failback procedure and with the following options selected: ◆ “Use the most recent backup set” ◆ “Up-to-the-minute restore” ◆ “Mount databases automatically after restore” Note_____ If the database was verified to be in a “Clean Shutdown” state after Exchange was taken offline on the DR cluster, you can skip the SnapManager restore.
14	Verify that the virtual Exchange server on the production cluster is up and running: a. Use the Cluster Administrator to verify that the Exchange virtual server and the cluster resources are online. b. Use the Exchange System Manager to verify that the Exchange databases are mounted.
15	Use SnapManager to re-create the automated backup jobs, described in the <i>SnapManager for Exchange Installation and Administration Guide</i>.

Changing the IP addresses of SMTP and HTTP virtual server cluster resources

After a failover or failback, the SMTP and HTTP virtual server cluster resources might fail after being online for a few minutes if both of the following conditions are true:

- ◆ The cluster is configured with the SMTP virtual server cluster resources, HTTP virtual server cluster resources, or both.
- ◆ The IP address for the virtual Exchange server at the DR site is different from the IP address at the production site.

If these resources fail, the following events appear in the Windows application event log:

```
Event Type: Error
Event Source: MSExchangeCluster
Event Category: Services
Event ID: 1005
Date: 8/25/2005
Time: 3:44:04 PM
User: N/A
Computer: EXCHSRVR1
Description:
SMTP Virtual Server Instance (EVS1): The IsAlive check for this
resource failed.
```

```
For more information, click
http://www.microsoft.com/contentredirect.asp.
Data:
0000: 4c 27 00 00 L'..
```

```
Event Type: Error
Event Source: MSExchangeCluster
Event Category: Services
Event ID: 1005
Date: 8/25/2005
Time: 3:44:07 PM
User: N/A
Computer: EXCHSRVR1
Description:
Exchange HTTP Virtual Server Instance (EVS1): The IsAlive check for
this resource failed.
```

```
For more information, click
http://www.microsoft.com/contentredirect.asp.
Data:
0000: 4c 27 00 00 L'..
```

To prevent the SMTP or HTTP virtual server cluster resources from failing after a cluster failover or failback, update the IP address as described in the two procedures that follow.

SMTP resource: For the SMTP resource, complete the following steps.

Step	Action
1	Launch the Exchange System Manager.
2	Browse to the Exchange virtual server name.
3	Expand the Exchange server name, Protocols, and SMTP.
4	Right-click Default SMTP Virtual Server and select Properties.
5	On the “General” page, select the correct IP address from the drop down list.
6	Click OK and then close the Exchange System Manager.
7	Using the Cluster Administrator, bring the SMTP virtual server cluster resource online.

HTTP resource: For the HTTP resource, complete the following steps.

Step	Action
1	Launch the Exchange System Manager.
2	Browse to the Exchange virtual server name.
3	Expand the Exchange server name, Protocols, and HTTP.
4	Right-click “Exchange Virtual Serve” and select Properties.
5	On the “General” page, select the correct IP address from the drop-down list.
6	Click OK and then close the Exchange System Manager.
7	Now launch the Internet information Services Manager.
8	Expand the local computer name and then expand the “Web Sites” folder.
9	Right-click Exchange Virtual Serve” the select properties.

Step	Action
10	When the properties appear, select the “Web Site” page and then set the correct IP address.
11	When done, click OK and then close the IIS Manager.
12	Using the Cluster Administrator, bring the SMTP virtual server cluster resource online.

